Cyber Threat Detection and Response

CTI and CDR in Military Environments

Authored by Matt Thorn & Mark Rogers

Agenda

- Instructor Introduction
- Cloud In Military Environments
- What is…?
  - Cloud Detection and Response (CDR)
  - Cyber Threat Intelligence (CTI)
- Incident Response for the Cloud
- Advanced Analytics
- Summary & Q&A

Instructor Introduction: Matt Thorn

- Palo Alto Networks Cortex Domain Consultant
- US Army Veteran - SATCOM Tech/MSQ GMF Controller
- Nearly 38 years of Telecom, Networking, and Cyber Security
- Former Personal Trainer
- Outdoorsman, sorta
- Father of two adults
- Drives a mean Audi RS5

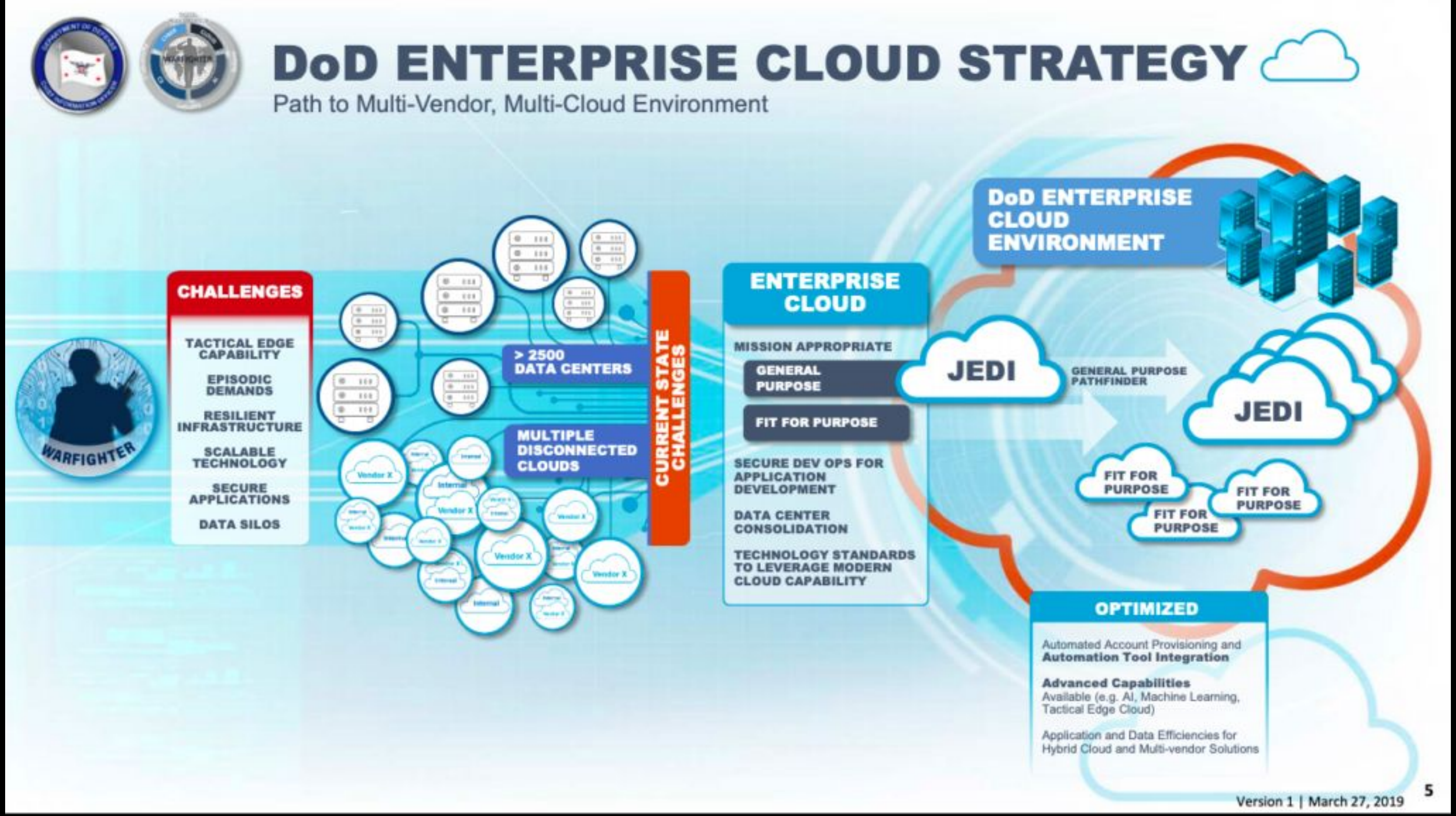
Cloud usage in the US Military

- Examples such as Cloud One, cARMY, Flank Speed, and Olympus.

- JEDi, Joint Enterprise Defense Infrastructure (JEDI) contract was a large United States Department of Defense cloud computing contract that was canceled and essentially replaced by Joint All Domain Command and Control (JADC2) and the Artificial Intelligence and Data Acceleration (ADA) initiative.

- DISA's Thunderdome is an example of a multi-cloud computing enabled environment.

- The Joint Warfighting Cloud Capability (JWCC) provides the DOD with a vehicle to acquire commercial cloud services directly from Cloud Service Providers.



DoD ENTERPRISE CLOUD STRATEGY

Path to Multi-Vendor, Multi-Cloud Environment

CHALLENGES

TACTICAL EDGE CAPABILITY

EPISODIC DEMANDS

RESILIENT INFRASTRUCTURE

SCALABLE TECHNOLOGY

SECURE APPLICATIONS

DATA SILOS

ENTERPRISE CLOUD

MISSION APPROPRIATE

- GENERAL PURPOSE
- FIT FOR PURPOSE

SECURE DEV OPS FOR APPLICATION DEVELOPMENT

DATA CENTER CONSOLIDATION

TECHNOLOGY STANDARDS TO LEVERAGE MODERN CLOUD CAPABILITY

DoD ENTERPRISE CLOUD ENVIRONMENT

OPTIMIZED

Automated Account Provisioning and **Automation Tool Integration**

Advanced Capabilities Available (e.g. AI, Machine Learning, Tactical Edge Cloud)

Application and Data Efficiencies for Hybrid Cloud and Multi-vendor Solutions

Version 1 | March 27, 2019

5

List of current CSO:
https://public.cyber.mil/dccs/cso/

Unique challenges to Cloud usage in the US Military

Cloud adoption in the US Military is slowly progressing because the controls

Commercial counterparts are less risk averse and require fewer checks and verifications

New versions or product deployments require extensive testing before being implemented or adopted fully. Software “bugs” are expected, as is “rapid patching”.

Cloud environments are far more ephemeral in nature and intent than the DoD is use to utilizing.

APT’s are rarely seen in a commercial environment. They are far more common in DoD.

Attacks such as Phishing are common in commercial side but not so in DoD.

What is Cyber Threat Intelligence

Threat Intelligence is a key to cyber security.

Understanding current attacks relative to an organization's security posture achieves prioritization.

DoD entities have extensive Threat Intelligence resources at their disposal.

Unfortunately, security teams rarely get the most value out of their threat intel investments, given the millions of indicators that come in daily.

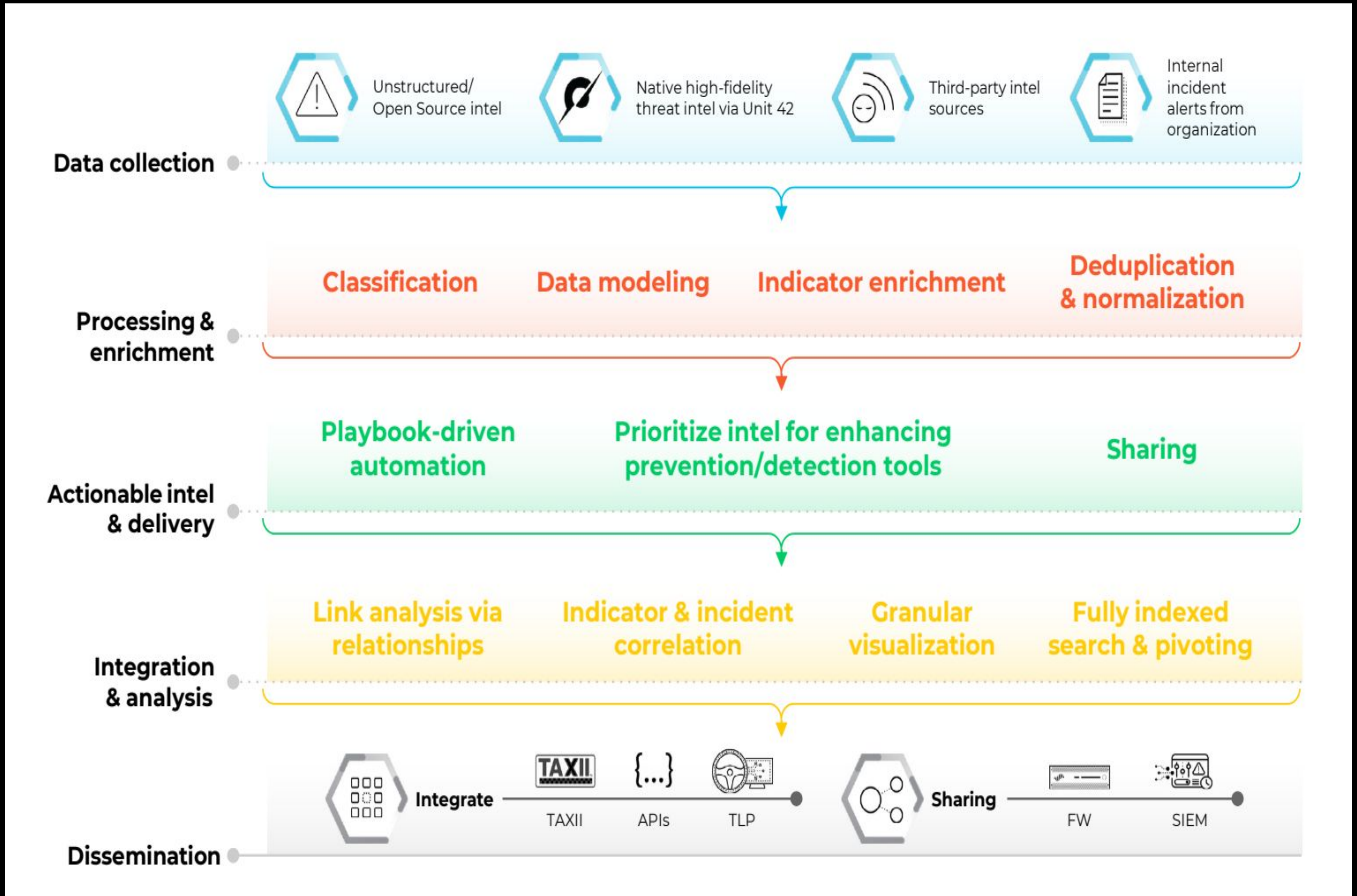

Data collection
Unstructured/ Open Source intel
Native high-fidelity threat intel via Unit 42
Third-party intel sources
Internal incident alerts from organization
Processing & enrichment
Classification
Data modeling
Indicator enrichment
Deduplication & normalization
Actionable intel & delivery
Playbook-driven automation
Prioritize intel for enhancing prevention/detection tools
Sharing
Integration & analysis
Link analysis via relationships
Indicator & incident correlation
Granular visualization
Fully indexed search & pivoting
Dissemination
Integrate
TAXII
{...}
TAXII
APIs
TLP
Sharing
FW
SIEM

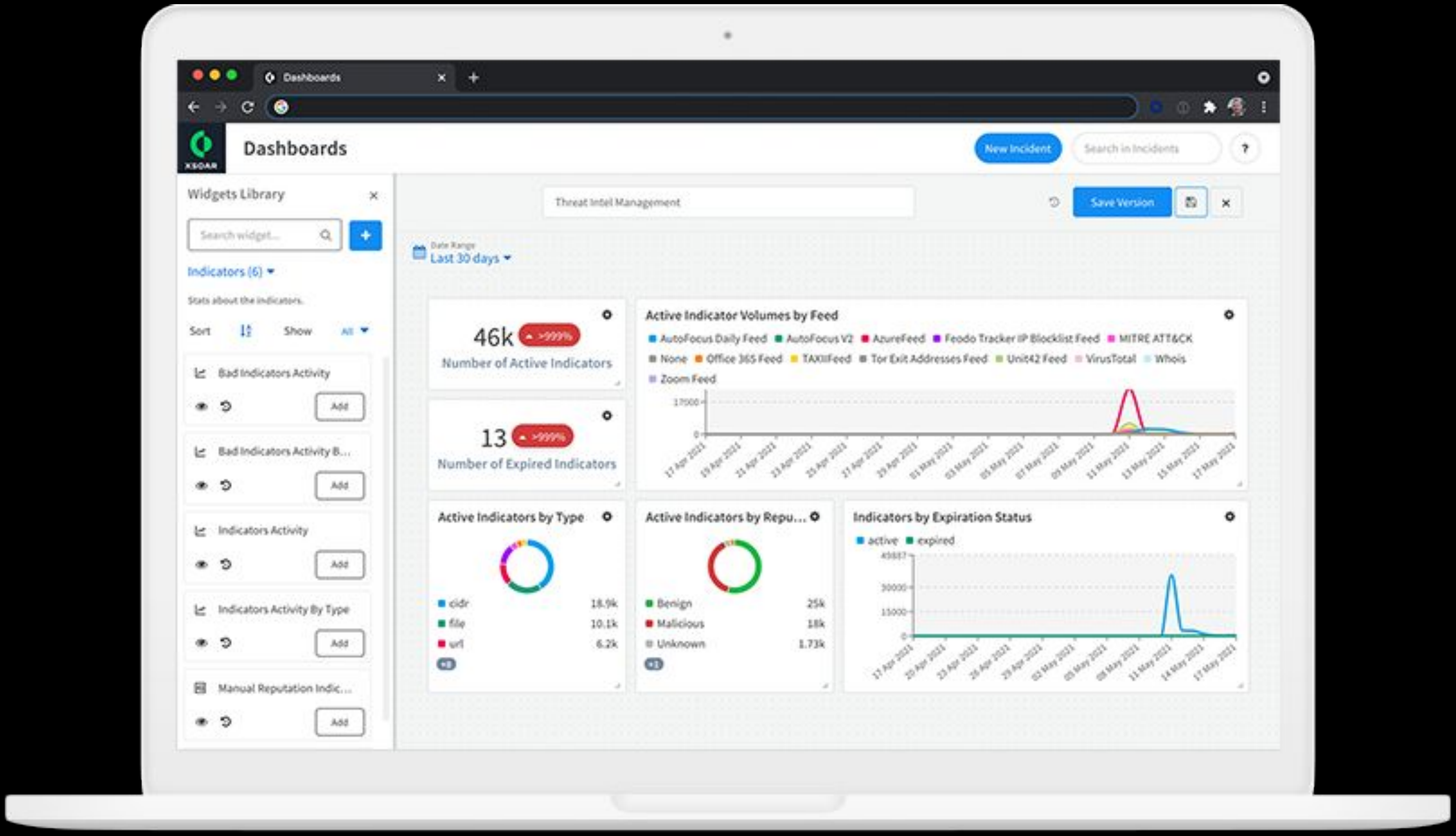
Figure 1: The lifecycle of threat intelligence platform

What is Cyber Threat Intelligence

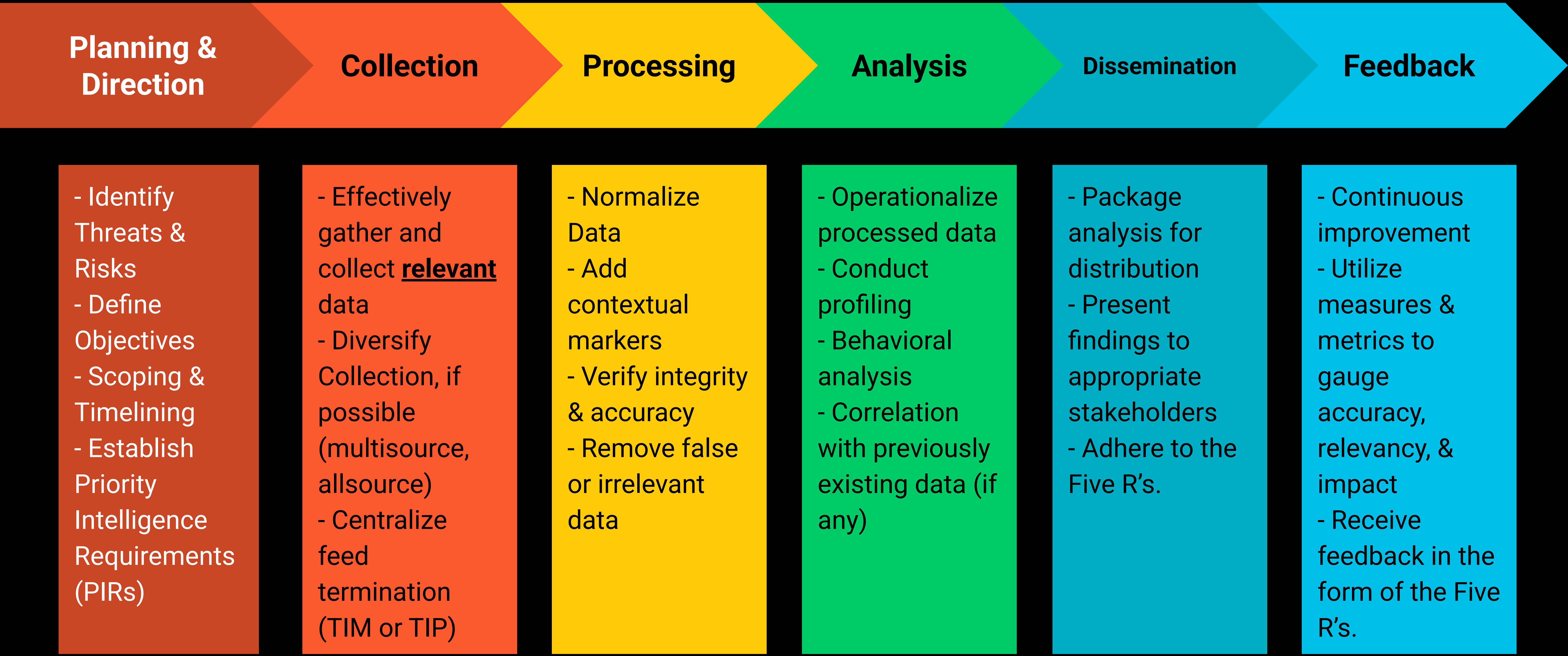
Automatically map threat information to incidents

Take automated action

Enrich and prioritize



CTI: The Threat Intelligence Cycle



Planning & Direction	Collection	Processing	Analysis	Dissemination	Feedback
- Identify Threats & Risks - Define Objectives - Scoping & Timelining - Establish Priority Intelligence Requirements (PIRs)	- Effectively gather and collect **<u>relevant</u>** data - Diversify Collection, if possible (multisource, allsource) - Centralize feed termination (TIM or TIP)	- Normalize Data - Add contextual markers - Verify integrity & accuracy - Remove false or irrelevant data	- Operationalize processed data - Conduct profiling - Behavioral analysis - Correlation with previously existing data (if any)	- Package analysis for distribution - Present findings to appropriate stakeholders - Adhere to the Five R’s.	- Continuous improvement - Utilize measures & metrics to gauge accuracy, relevancy, & impact - Receive feedback in the form of the Five R’s.

CTI: The Five R's of Dissemination & Feedback

- **Right Time**
  - Intelligence is delivered in a timely manner to afford maximum reactionary time and impact
    - Routine briefings, emergency bulletins...
- **Right Place**
  - Intelligence is presented in a manner accessible to proper stakeholders
    - Meetings, Delivered Reports...
- **Right Format**
  - Intelligence is delivered in a manner that is digestible and understandable for the given audience
    - Readable, ingestable...
- **Right Audience**
  - Intelligence is presented to the appropriate stakeholders who can utilize the data effectively
- **Right Data**
  - Intelligence contains all relevant information that is accurate, vetted/verified, and contextualized to achieve maximum situational awareness for the given audience

- *What is **Impact**? It is the means of which the intelligence is utilized in its fullest capacity to achieve maximum effectiveness upon its dissemination and use. Examples–*
  - *People: Stakeholders are engaged to make informed decisions to some action or plan*
  - *Processes: Engaged or modified based on the new data which optimizes flows and reactions*
  - *Technology: Detection and Prevention Systems are loaded with data that allows them to act on the new intelligence*

CTI: Levels of Intelligence

Tactical

- The *What*
- Indicators of Compromises
  - IPs
  - Domains
  - Hashes
  - Etc…
- Most rapidly changing data
  - IOCs can expire within hours of deployment
- Using only tactical intel makes environments reactionary.

Operational

- The *How* and *Where*
- TTPs
  - Tactics
  - Techniques
  - Procedures
- MITRE ATT&CK
- Behaviors and Activity less-frequently changed
- *"Humans tend to be lazy"*
- Threat Actors can have SOPs; often reuse attacks and methods
- *Modus Operandi*

Strategic

- The *Who* and *Why*
- Motives & Objectives
  - Nation-States & Geopolitics
  - Cybercriminals & Financial Gain
  - Militaries & Kinetic Effects
  - Cyberterrorism & Influence
- *"There is a Reason for Everything"*
- *Where there is a Will, There is a Way* Theory
  - Given enough time and resources, any system can be breached

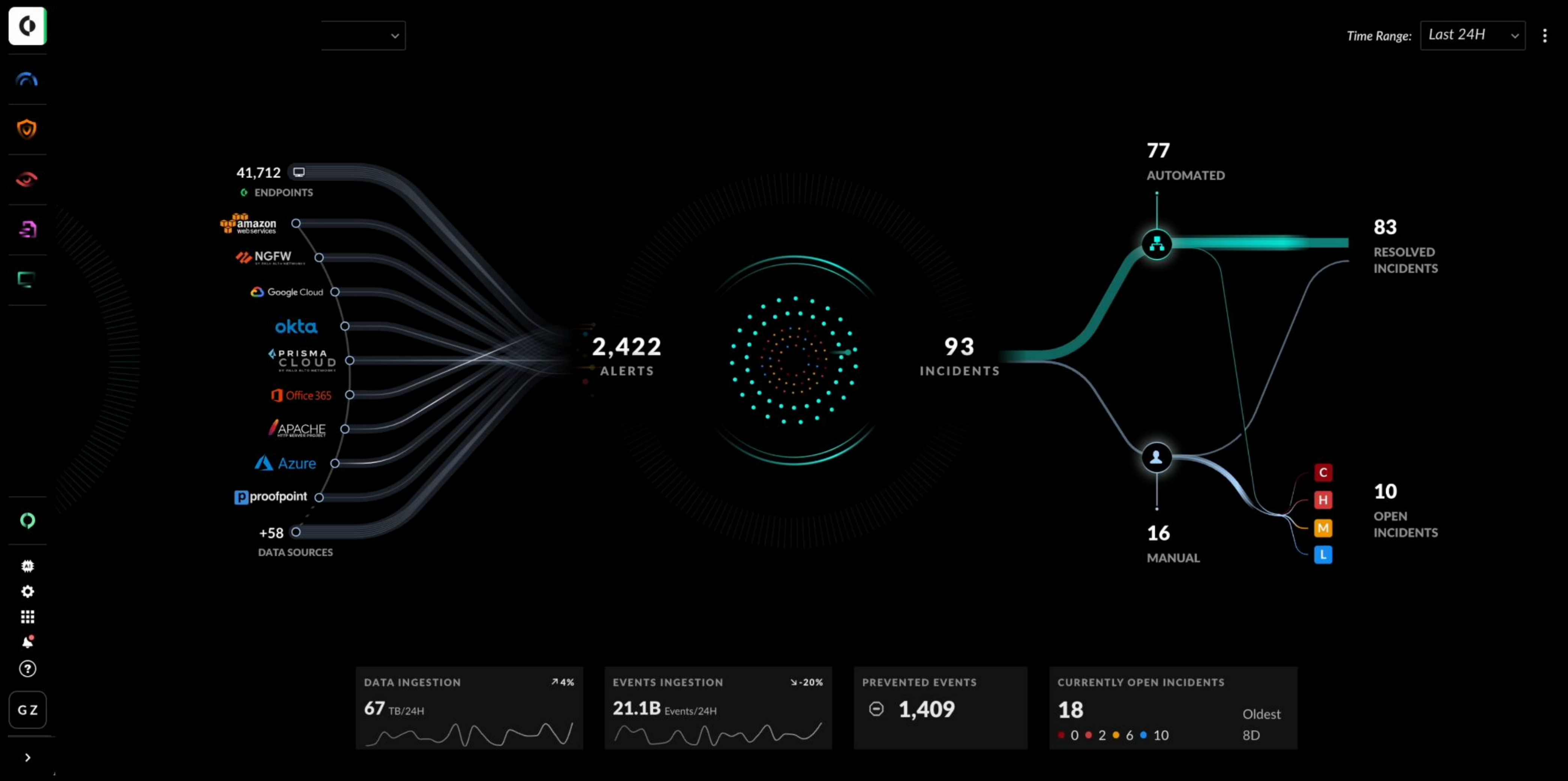
What is Cloud Detection and Response, or CDR?

Specifically designed for cloud environments

Typical issues to investigate: Data breaches, insider threats, misconfigurations, advanced persistent threats (APTs)

Incident response requirements for CDR

CDR for military environments



CDR: Don’t Forget the Fundamentals

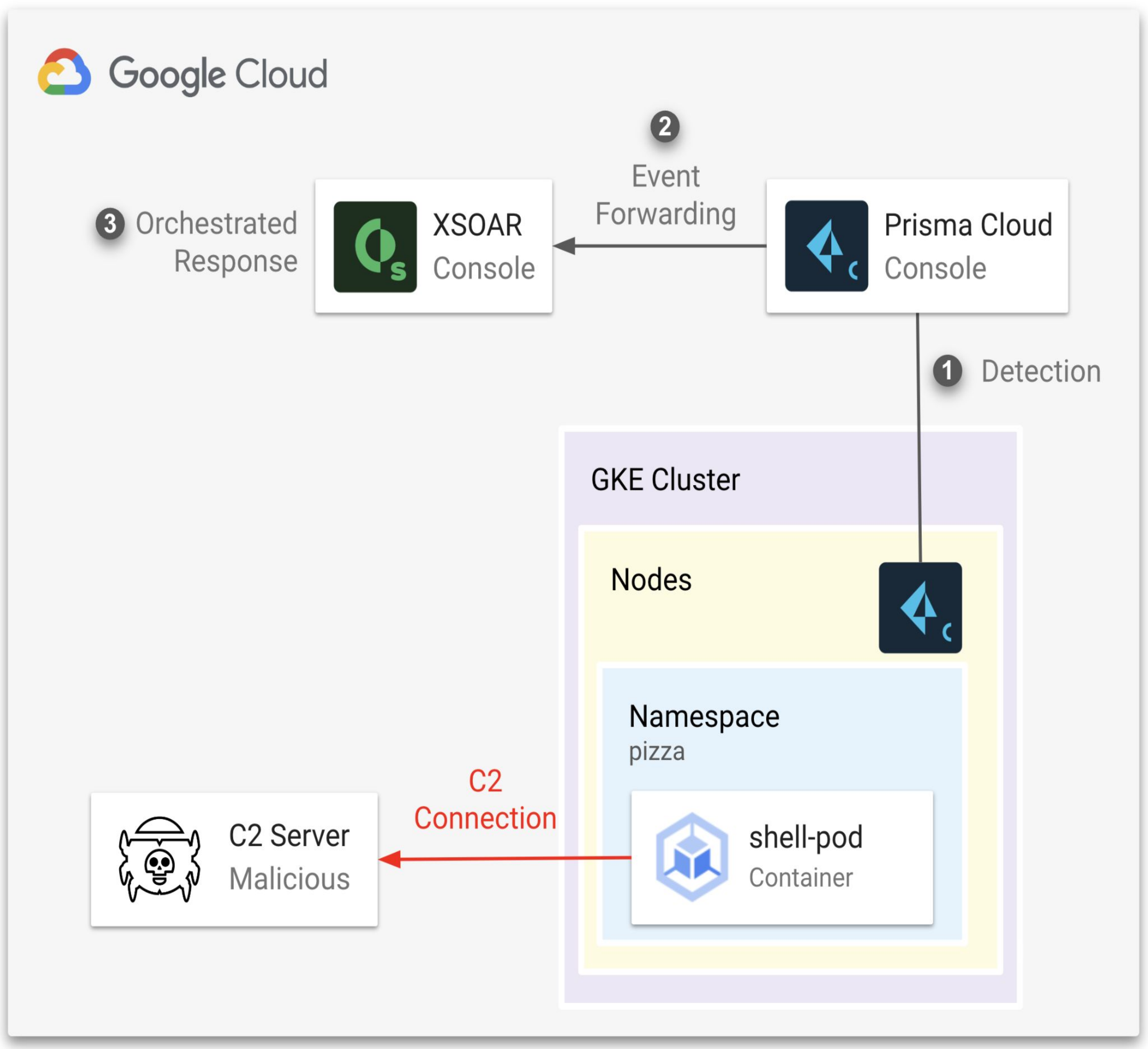
- While Cloud has its own specific needs, some key principles don’t change:
  - **Prepare** - Know what you have, know how important it is to you, and know where it is
  - **Identify** - If it looks like a duck, walks like a duck, and quacks like a fish…
  - **Contain** - … You need to immediately prevent it from walking and quacking any further than it already has.
  - **Eradicate** - Ensure you’ve isolated then remove the threat from your environment.
  - **Recover** - Bring back operations to their normal state
  - **After-Action Review** - What was suppose to happen, what did happen, what went right, and what went wrong?
- All Detection and Response relies on the first two actions to be able to do the rest.
  - Preparation and Identification ensure the remaining steps run smoothly
- Cloud Considerations:
  - Cloud uniquely presents the opportunity to build from the ground up with security in mind
  - Bring in security early to establish visibility and understand system design
  - This enables them to prepare effectively as things are deployed
  - Identification of what’s not normal through baselining and deviations from expected behavior
  - Routine checks against compliance needs and configuration best-practices

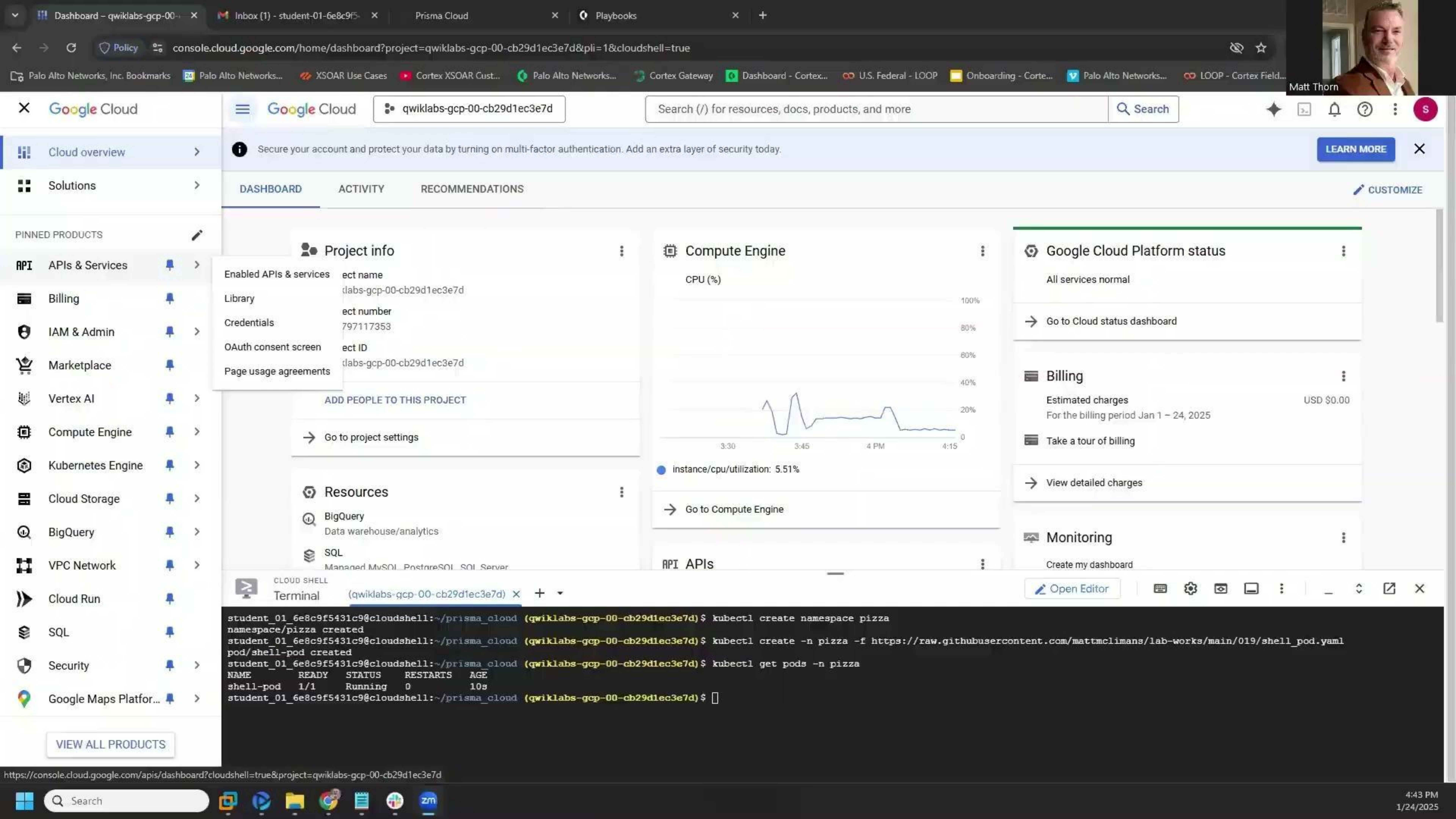
Incident Response in the Cloud

The process used to manage cyber attacks in a cloud environment is one simple definition of Cloud incident response.

The tools and techniques are similar to those for traditional environments, but are typically developed and hosted in the cloud, SaaS.

The ephemeral nature of cloud environments are make IR more challenging.





Secure your account and protect your data by turning on multi-factor authentication. Add an extra layer of security today.

Project info

ect name
:labs-gcp-00-cb29d1ec3e7d

ect number
797117353

ect ID
:labs-gcp-00-cb29d1ec3e7d

Compute Engine

instance/cpu/utilization: 5.51%

Google Cloud Platform status

All services normal

Billing

Estimated charges USD $0.00
For the billing period Jan 1 – 24, 2025

Monitoring

Resources

BigQuery
Data warehouse/analytics

SQL
Managed MySQL, PostgreSQL, SQL Server

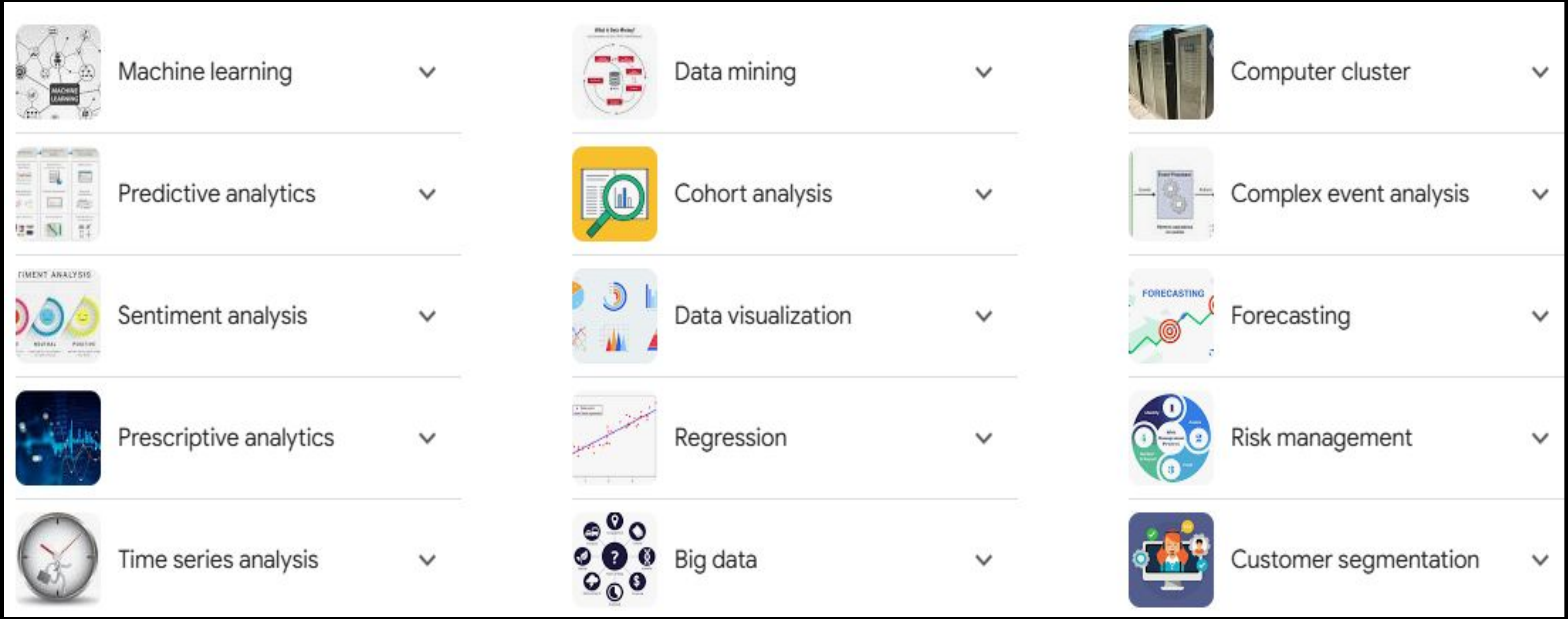
APIs

```
student_01_6e8c9f5431c9@cloudshell:~/prisma_cloud (qwiklabs-gcp-00-cb29d1ec3e7d)$ kubectl create namespace pizza
namespace/pizza created
student_01_6e8c9f5431c9@cloudshell:~/prisma_cloud (qwiklabs-gcp-00-cb29d1ec3e7d)$ kubectl create -n pizza -f https://raw.githubusercontent.com/mattmclimans/lab-works/main/019/shell_pod.yaml
pod/shell-pod created
student_01_6e8c9f5431c9@cloudshell:~/prisma_cloud (qwiklabs-gcp-00-cb29d1ec3e7d)$ kubectl get pods -n pizza
NAME        READY   STATUS    RESTARTS   AGE
shell-pod   1/1     Running   0          10s
student_01_6e8c9f5431c9@cloudshell:~/prisma_cloud (qwiklabs-gcp-00-cb29d1ec3e7d)$ 
```

https://console.cloud.google.com/apis/dashboard?cloudshell=true&project=qwiklabs-gcp-00-cb29d1ec3e7d

Advanced Analytics

Advanced analytics are techniques that use data to identify patterns, trends, and relationships. They can be used to make predictions, improve decision-making, and gain insights into customer behavior.



- Machine learning
- Predictive analytics
- Sentiment analysis
- Prescriptive analytics
- Time series analysis
- Data mining
- Cohort analysis
- Data visualization
- Regression
- Big data
- Computer cluster
- Complex event analysis
- Forecasting
- Risk management
- Customer segmentation

Summary

Cloud environments offer a distinct security challenges for all customers, but especially military organizations

Cyber Threat Intelligence when implemented correctly can provide keen in sites for an organizations SOC

Remember the 5R’s

Cloud IR is the process used to manage cyber attacks in a cloud environment is one simple definition of Cloud incident response.

Advanced analytics are techniques that use data to identify patterns, trends, and relationships.

Thank you