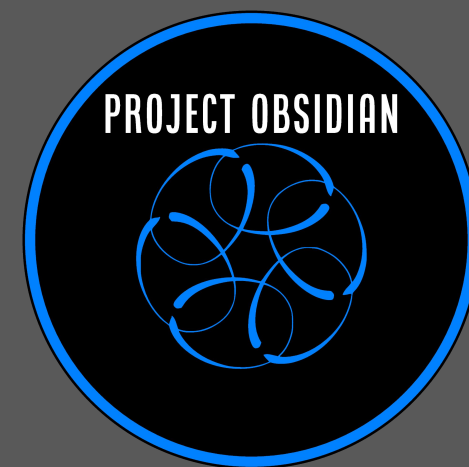




Project Obsidian

Cyber Threat Intelligence



Module 3: Generating Threat Intelligence from an Incident



Agenda

- **Objective**
- **Planning & Direction:** Stakeholders, requirements, goals & objectives
- **Collection:** CTI analysts role during an incident
- **Processing:** Intrusion data & information
- **Analysis & Production:** Research & Elements to include in a report
- **Dissemination:** Sharing the report with stakeholders
- **Feedback & Evaluation:** Methods for receiving feedback



Objective



Objective - Module 3

Demonstrate the important role CTI plays both during and after an incident.



Planning & Direction

Overview of stakeholders, intelligence requirements, goals & objectives



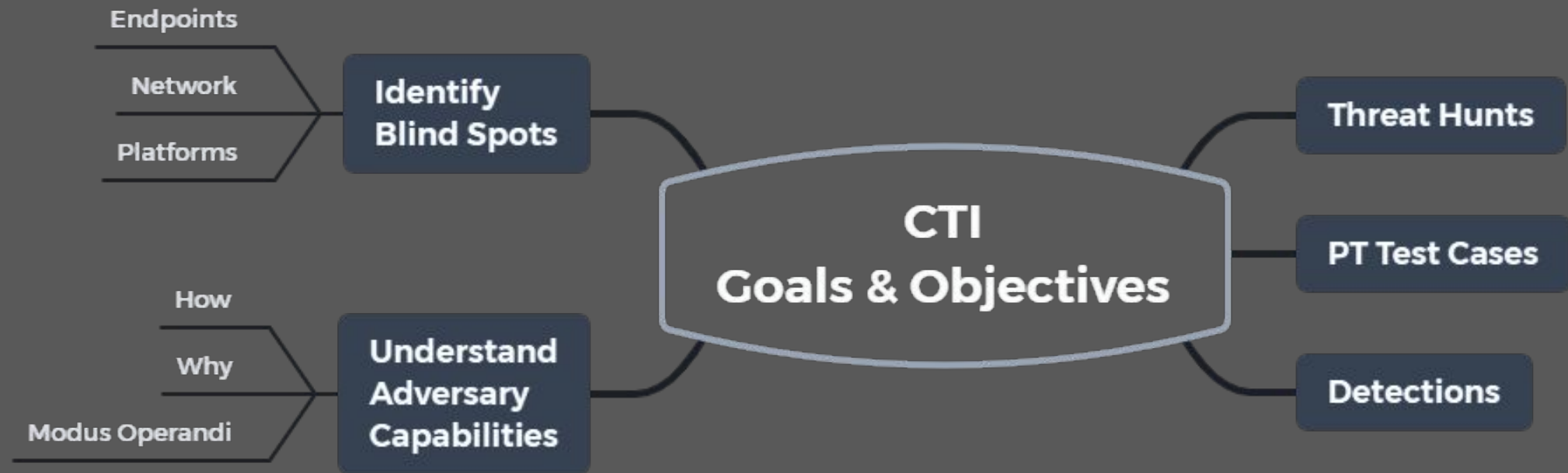
Planning & Direction

Stakeholders in our scenario include:

- CISO, CTO, CIO, Executive Board
- Security Operations Center (SOC)
 - Defenders
 - Forensics team
 - IR team
 - Malware analysis team
 - Threat hunting team
- SOC management
- IT team



Planning & Direction

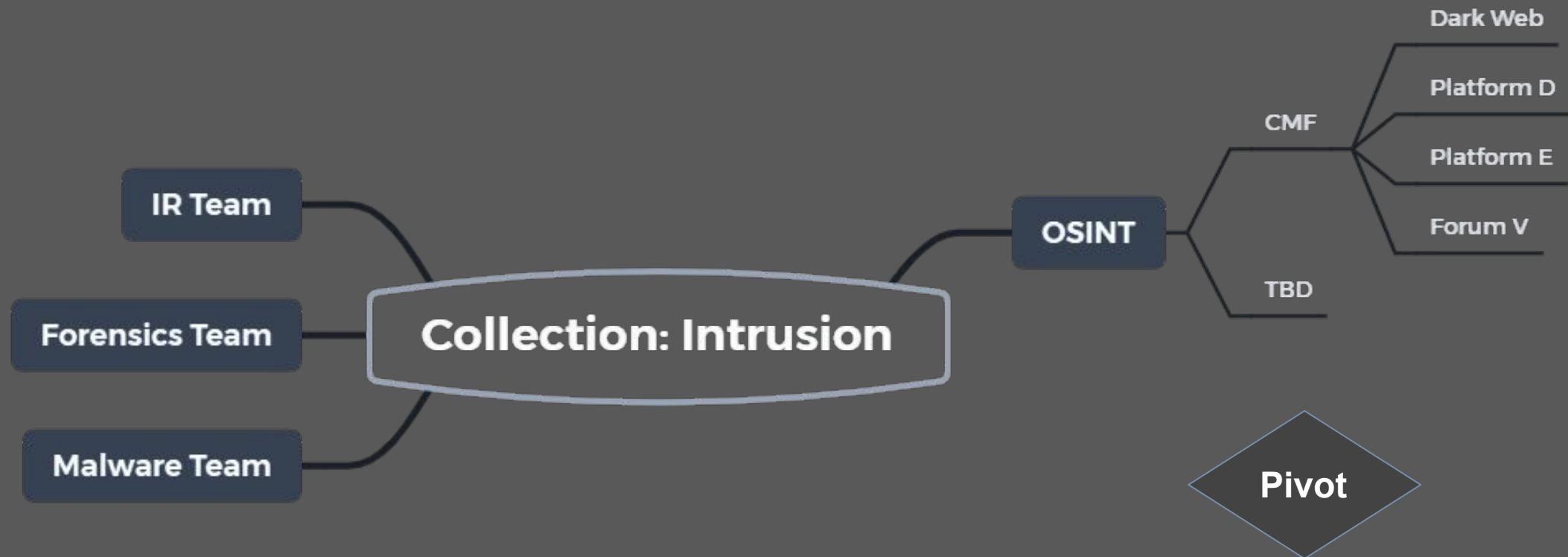


Collection

CTI analyst's role during an incident



Collection



Processing

Intrusion Data & Information



Processing

"[OpenCTI](#) is an open source platform allowing organizations to manage their cyber threat intelligence knowledge and observables. It has been created in order to structure, store, organize, and visualize technical and non-technical information about cyber threats."

"The data is structured using a knowledge schema based on the STIX2 standards. It has been designed as a modern web application including a GraphQL API and an UX oriented frontend."

OpenCTI can be integrated with other tools and applications such as:

MISP, <https://github.com/MISP/MISP>

The Hive, <https://github.com/TheHive-Project/TheHive>

MITRE ATT&CK, <https://github.com/mitre/cti>

and more



Analysis and Production

Research & Elements to include in a report



Demo - OSINT

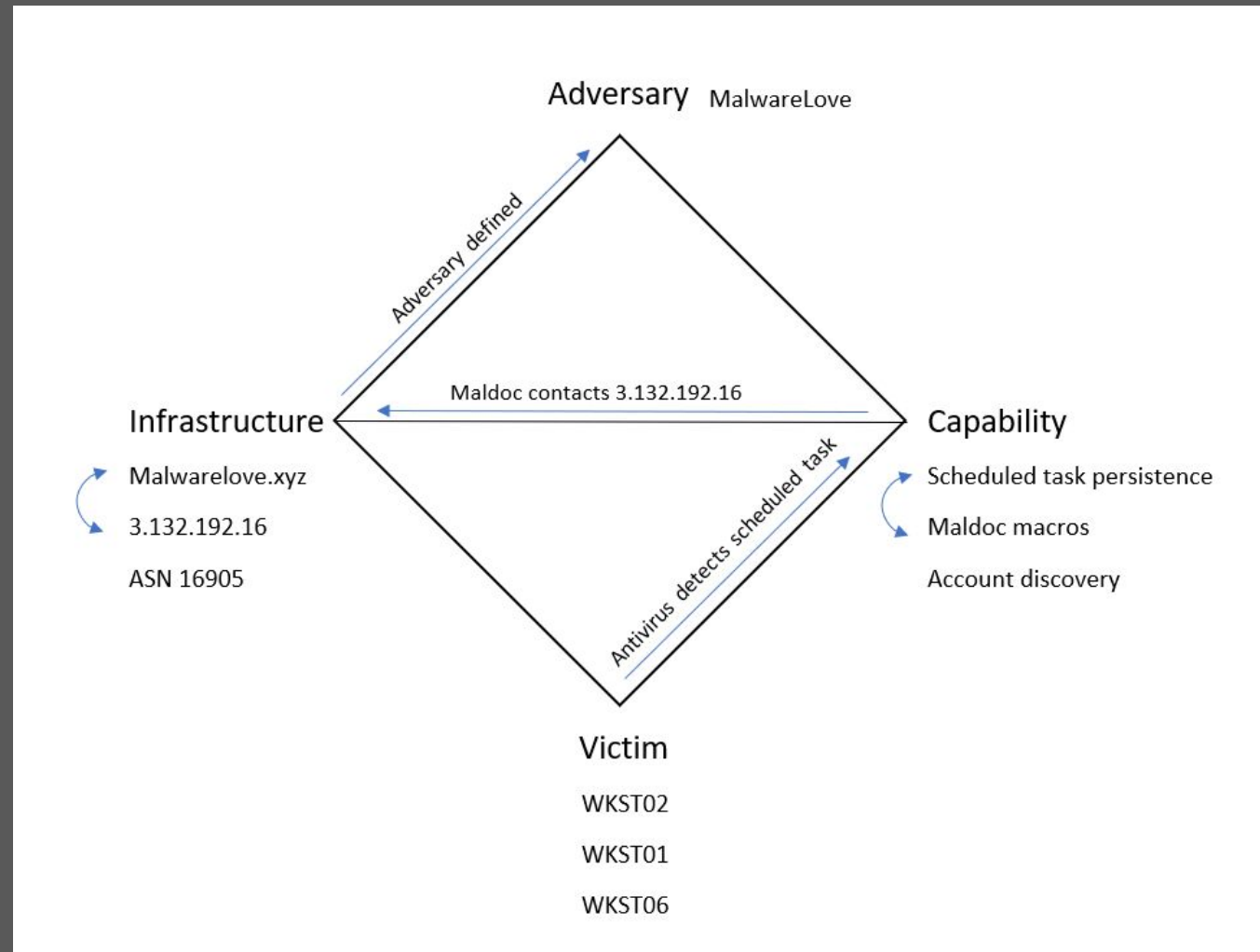
Pivoting using VirusTotal and Any.Run



Analysis and Production



Diamond Model for Intrusion Analysis



Intrusion Summary

- Best source of intelligence
- Diamond model for intrusion analysis
- Clustered on different criteria

| Victim | Infrastructure | Capability | Adversary (our definition) |
|----------------------------|--|--|----------------------------|
| WKST02 WKST01 WKST06 | 3.132.192.16 malwarelove.xyz ASN 16509 | Word Macro Account Discovery WinRM | MalwareLove |

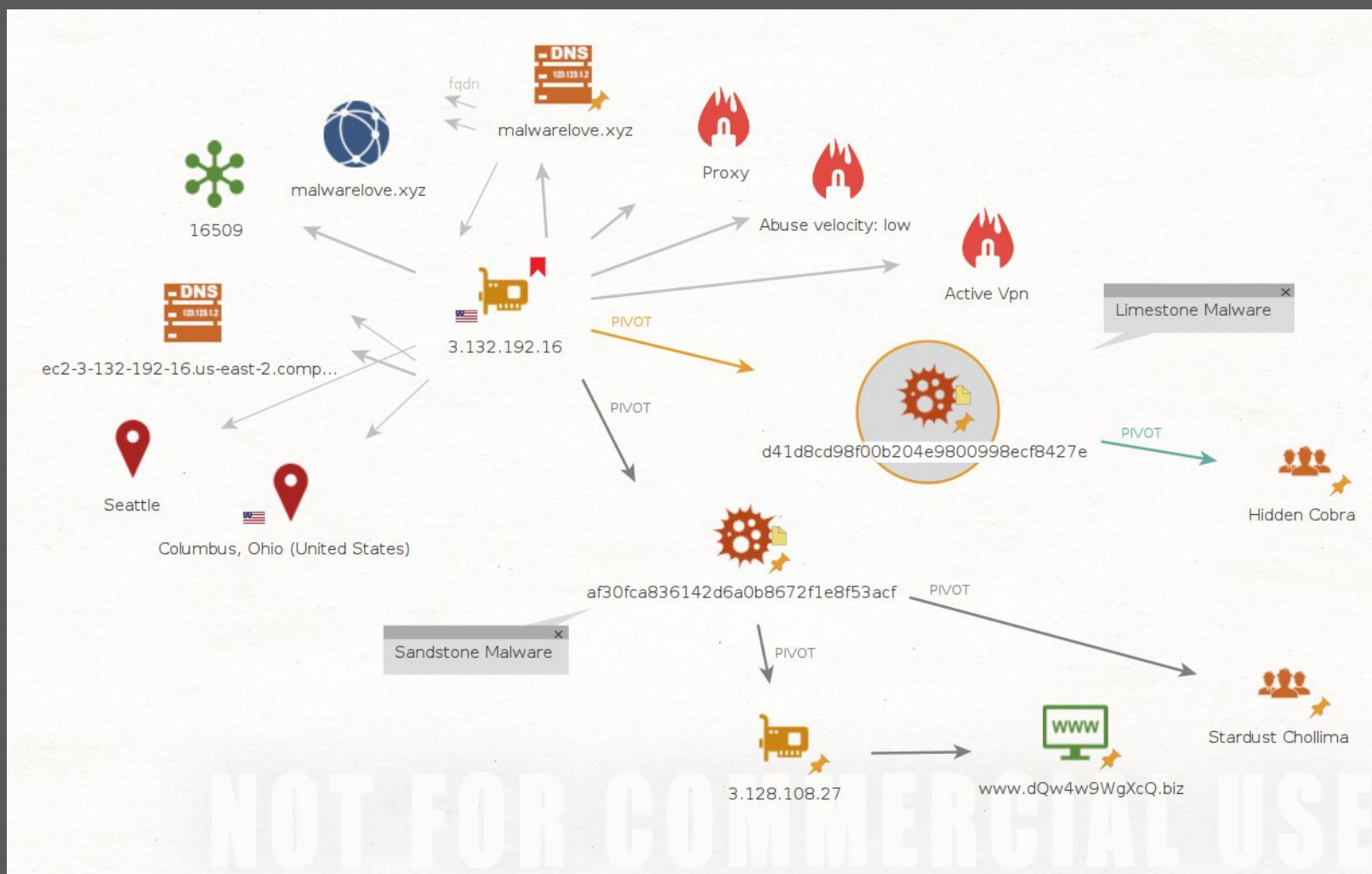


MITRE ATT&CK Navigator Layer

| Initial Access 9 techniques | Execution 12 techniques | Persistence 19 techniques | Privilege Escalation 13 techniques | Defense Evasion 42 techniques | Credential Access 16 techniques | Discovery 30 techniques | Lateral Movement 9 techniques |
|-------------------------------------|---|--|--|---|--|----------------------------------|--|
| Drive-by Compromise | Command and Scripting Interpreter (1/8) | Account Manipulation (0/5) | Abuse Elevation Control Mechanism (0/4) | Abuse Elevation Control Mechanism (0/4) | Adversary-in-the-Middle (0/3) | Account Discovery (0/3) | Exploitation of Remote Services |
| Exploit Public-Facing Application | Container Administration Command | BITS Jobs | Access Token Manipulation (0/5) | Access Token Manipulation (0/5) | Brute Force (0/4) | Application Window Discovery | Internal Spearphishing |
| External Remote Services | Deploy Container | Boot or Logon Autostart Execution (0/14) | Boot or Logon Autostart Execution (0/14) | BITS Jobs | Credentials from Password Stores (0/5) | Browser Bookmark Discovery | Lateral Tool Transfer |
| Hardware Additions | Exploitation for Client Execution | Boot or Logon Initialization Scripts (0/5) | Boot or Logon Initialization Scripts (0/5) | Build Image on Host | Exploitation for Credential Access | Cloud Infrastructure Discovery | Remote Service Session Hijacking (0/2) |
| Phishing (1/3) | Inter-Process Communication (0/3) | Browser Extensions | Create or Modify System Process (0/4) | Debugger Evasion | Forced Authentication | Cloud Service Dashboard | Remote Services (0/0) |
| Replication Through Removable Media | Native API | Compromise Client Software Binary | Domain Policy Modification (0/2) | Deobfuscate/Decode Files or Information | Forge Web Credentials (0/2) | Cloud Service Discovery | Replication Through Removable Media |
| Supply Chain Compromise (0/3) | Scheduled Task/Job (0/5) | Create Account (0/3) | Escape to Host | Deploy Container | Input Capture (0/4) | Cloud Storage Object Discovery | Software Deployment Tools |
| Trusted Relationship | Shared Modules | Create or Modify System Process (0/4) | Event Triggered Execution (0/15) | Direct Volume Access | Modify Authentication Process (0/5) | Container and Resource Discovery | Taint Shared Content |
| Valid Accounts (0/4) | Software Deployment Tools | Event Triggered Execution (0/15) | Exploitation for Privilege Escalation | Domain Policy Modification (0/2) | Multi-Factor Authentication Interception | Debugger Evasion | Use Alternate |
| | System Services (0/2) | External Remote | | Execution Guardrails (0/1) | | Domain Trust Discovery | |
| | User Execution (1/3) | | | Exploitation for Defense Evasion | | File and Directory Discovery | |
| | | | | File and Directory Permissions | | | |



Maltego Graph



Dissemination



Dissemination

For this module all of the teams were involved in the incident and are aware of the outcomes.

Aside from the IR report being delivered to stakeholders, dissemination is not required in this scenario.



Dissemination



Feedback and Evaluation

Methods for receiving feedback



Feedback & Evaluation

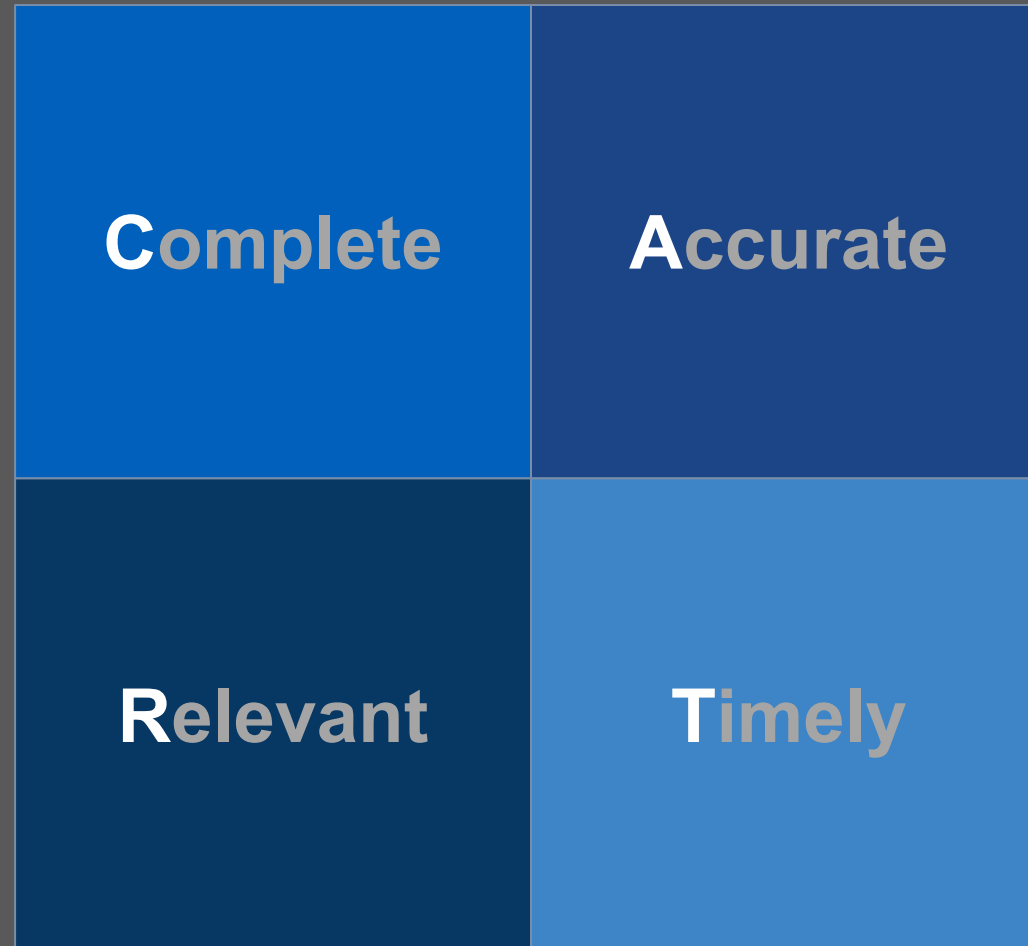
During the planning and direction phase, a process for providing feedback to the CTI team needs to be:

- Defined
- Documented
- Socialized

Ongoing feedback is critical to the success of any CTI program.



Feedback & Evaluation



Feedback & Evaluation

Complete

CTI must provide sufficient detail to enable a proper response

- How comprehensive is the CTI?
- Are all required data attributes present?
- Does CTI incorporate vulnerability analysis?
- Does CTI correlate across the entire organizational threat landscape and incorporate non-cyber intelligence and events to produce a complete threat profile?

Accurate

Quality CTI must be accurate and free from error

- What data sources corroborate threat intelligence to ensure accuracy?
- Is CTI updated when new information is learned or when knowledge changes?
- Is CTI time-bound to ensure that stakeholders understand the limited nature of the information?



Feedback & Evaluation

Relevant

CTI must address relevant threats to the organization and be delivered in a method that allows for effective action

- Does CTI map to threat intelligence requirements?
- How do stakeholders submit requirements and provide feedback to support more relevant intelligence?

Timely

CTI must be produced and delivered quickly so it can be used fast enough to make a difference

- How is threat intelligence delivered to ensure quick consumption?
- How long between the discovery of a threat and stakeholder notification?
- Is CTI released to stakeholders as it is learned or is dissemination paused until more data is discovered so that a more complete assessment can be shared?



Resources

Maltego

<https://www.maltego.com/>

Any.run

<https://app.any.run>

VirusTotal

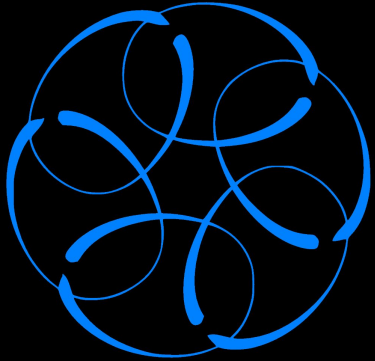
<https://virustotal.com>

Mitre ATT&CK Navigator

<https://mitre-attack.github.io/attack-navigator/>



PROJECT OBSIDIAN



Thank you

Join the conversation

<https://discord.blueteamvillage.org>

