
# 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

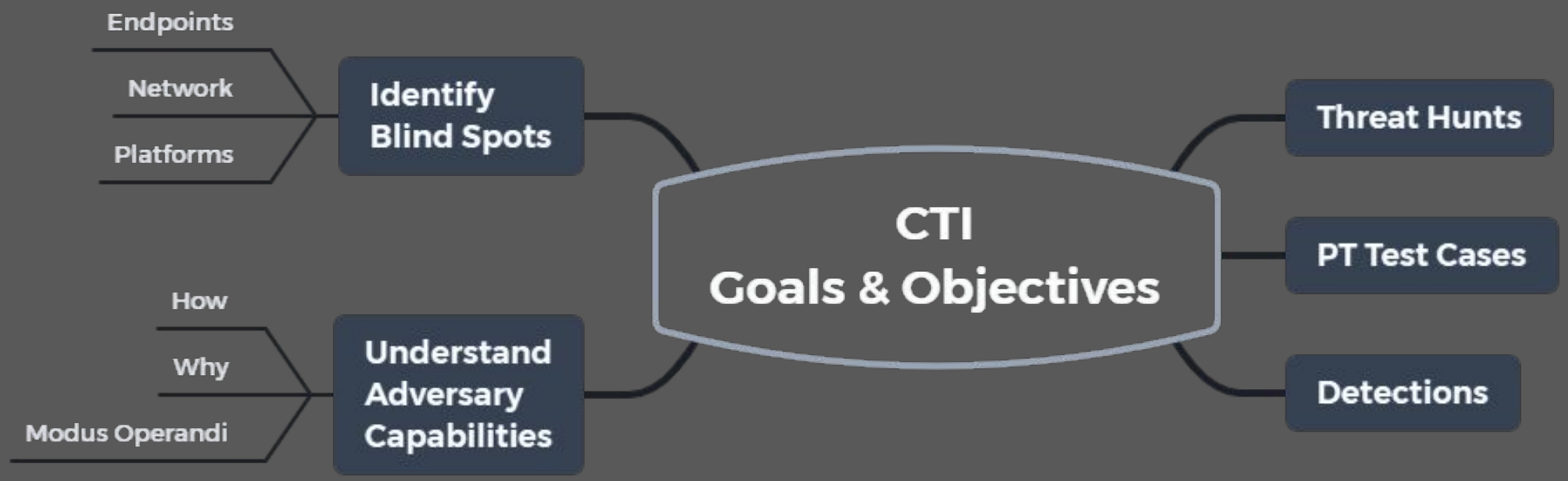
Overview of stakeholders, intelligence requirements, goals & objectives

# 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

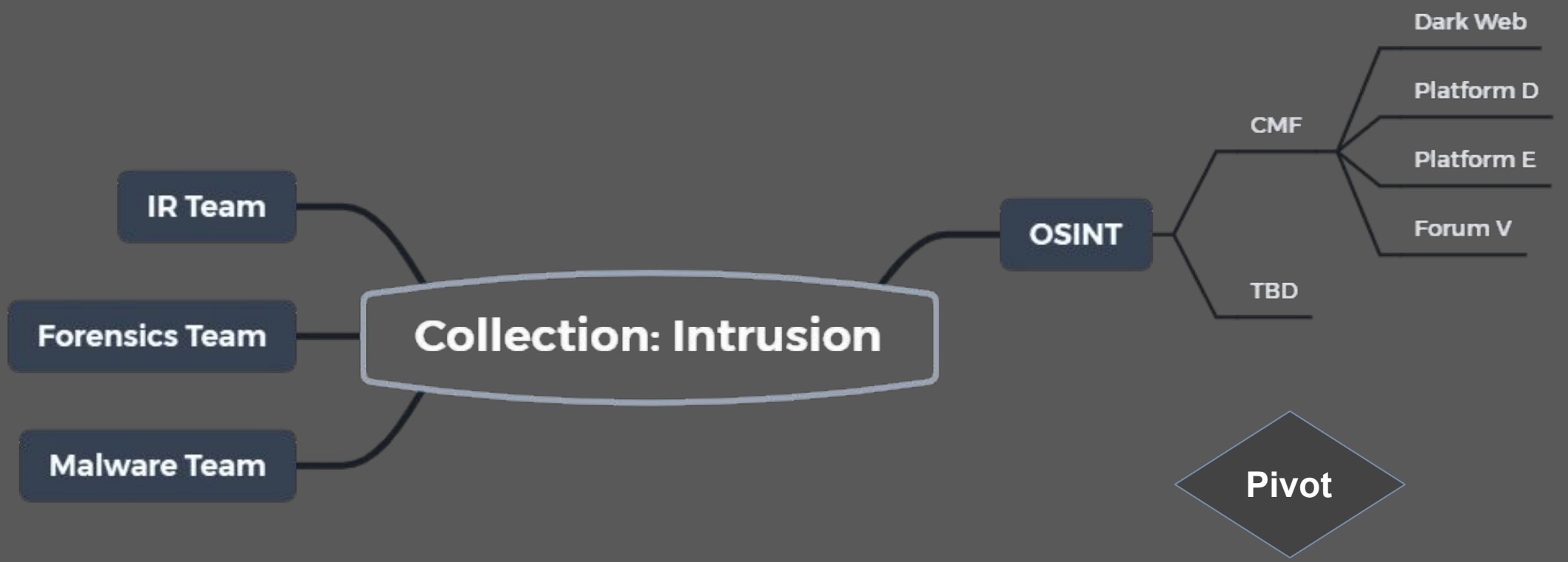
# Planning & Direction



# Collection

CTI analyst’s role during an incident

# Collection


IR Team
Forensics Team
Malware Team
Collection: Intrusion
OSINT
CMF
Dark Web
Platform D
Platform E
Forum V
TBD
Pivot

# 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

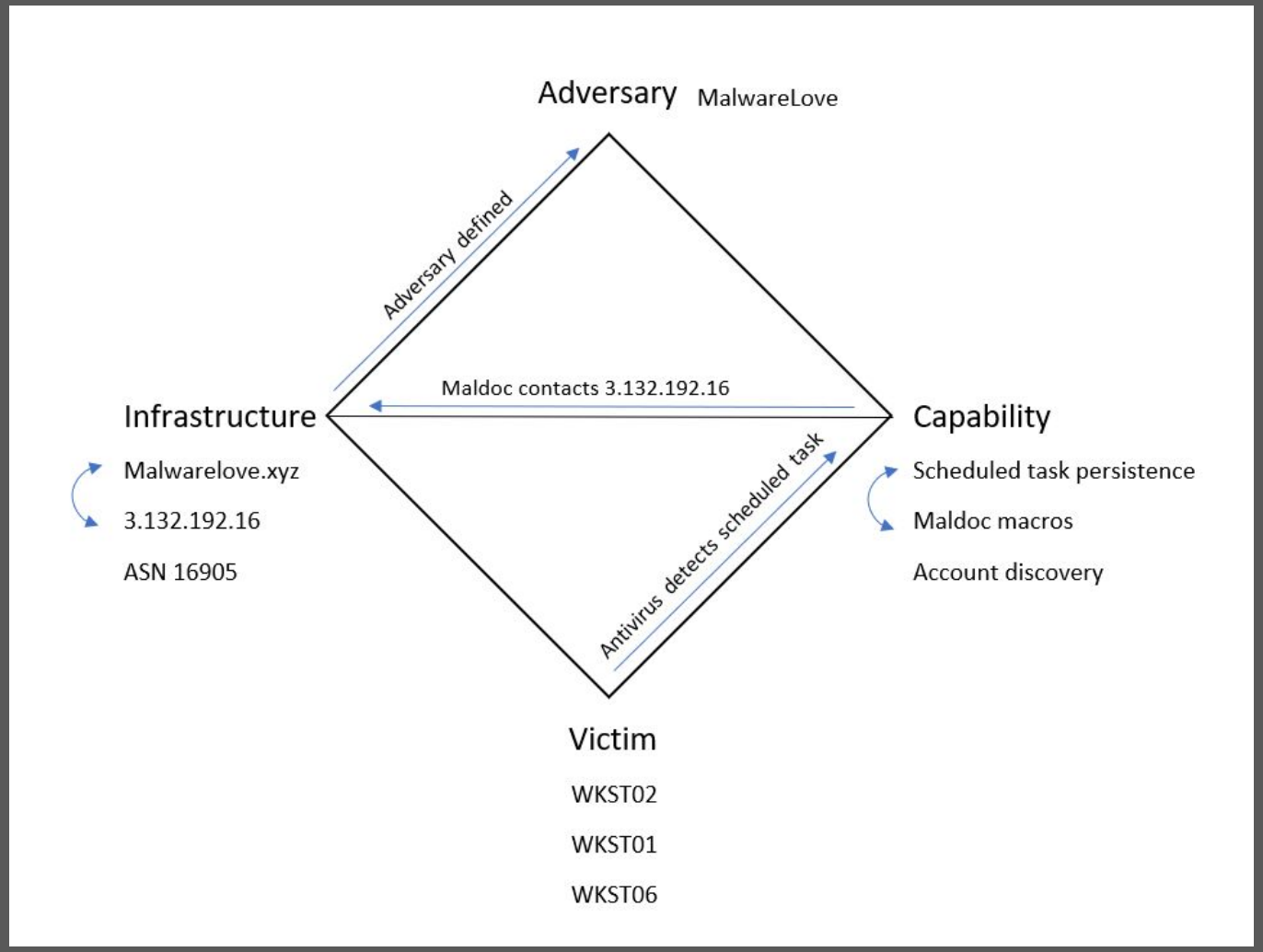
Research & Elements to include in a report

# Demo - OSINT

Pivoting using VirusTotal and Any.Run


# Analysis and Production

# Diamond Model for Intrusion Analysis

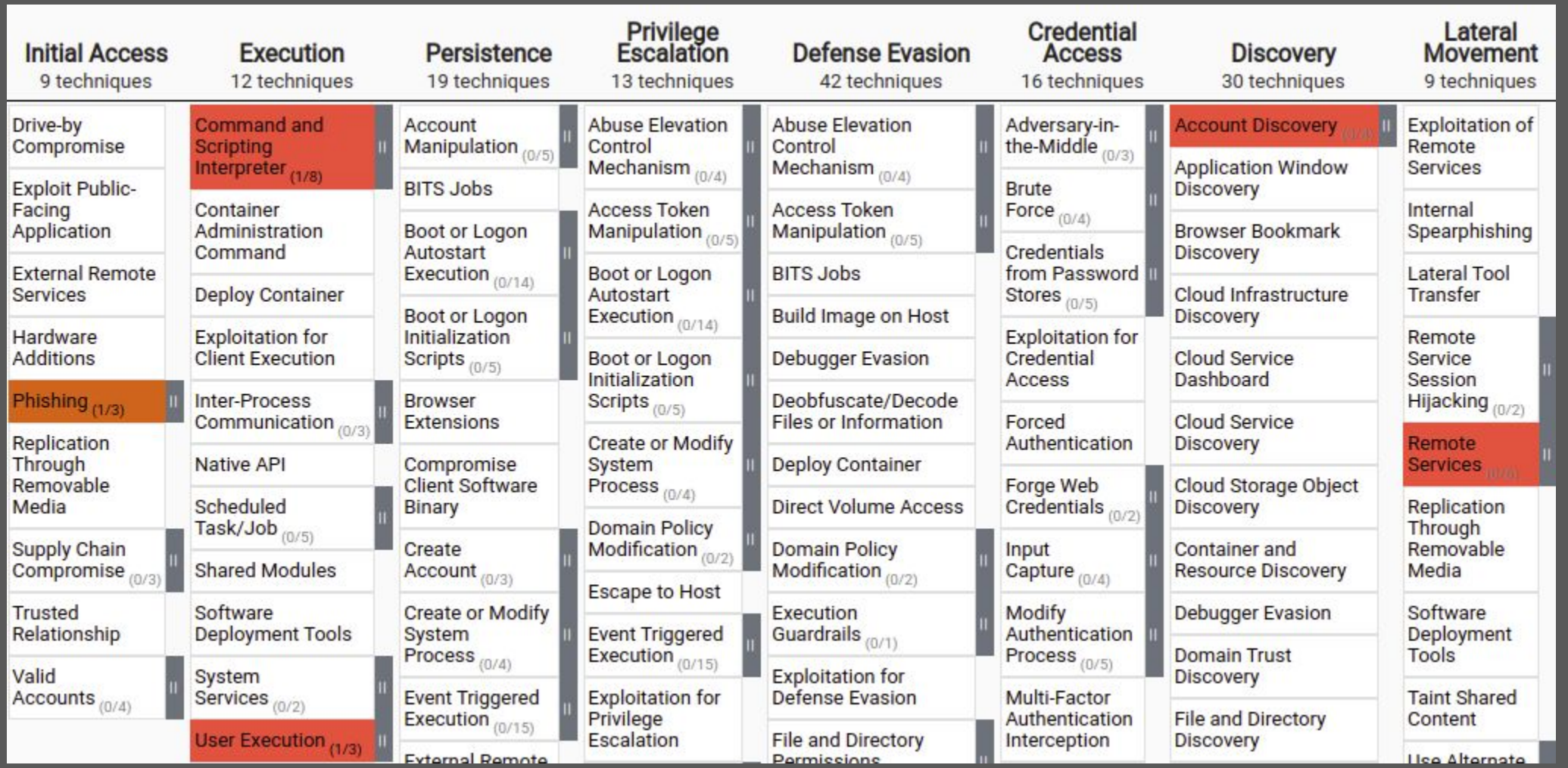


# Intrusion Summary

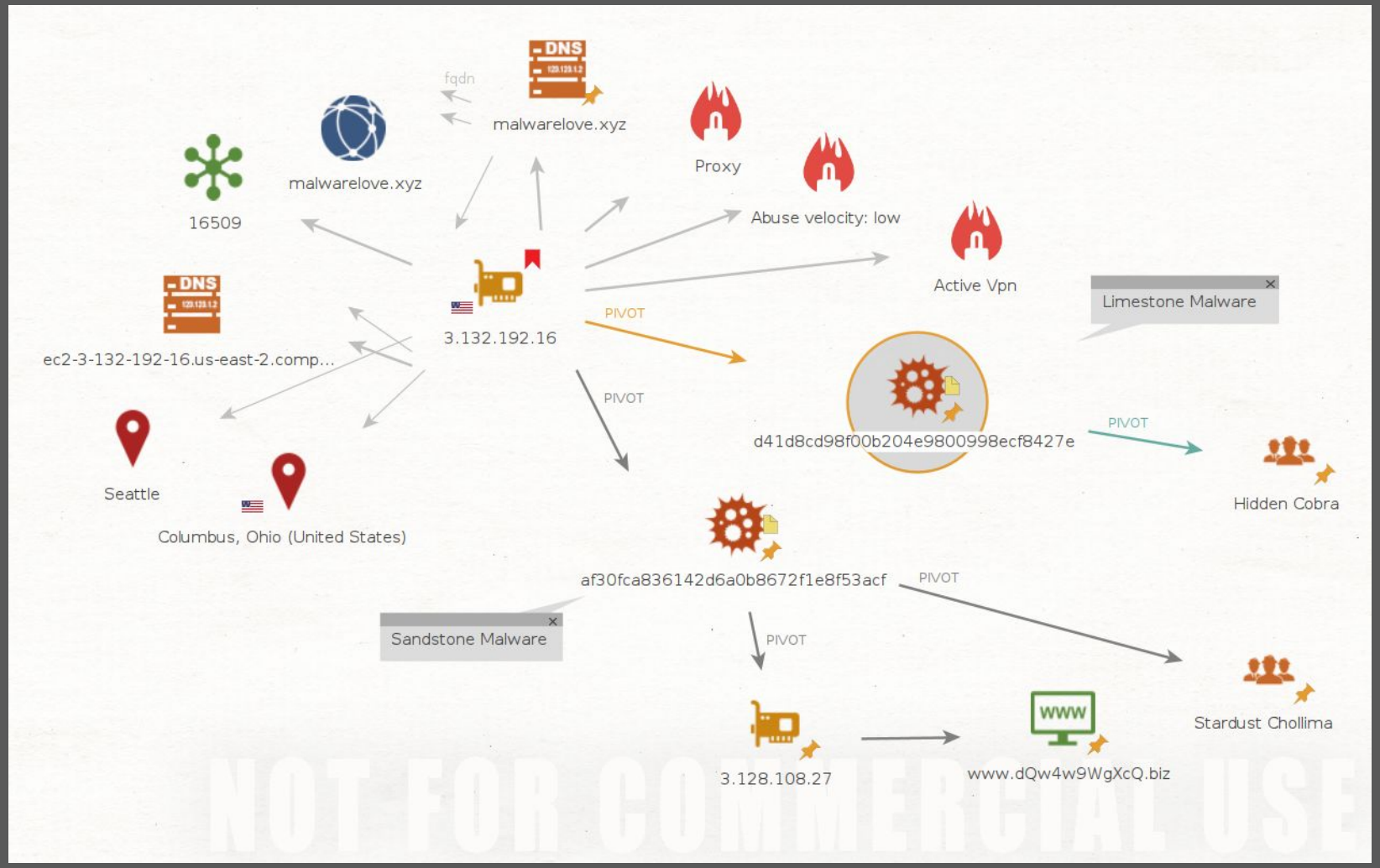
- Best source of intelligence
- Diamond model for intrusion analysis
- Clustered on different criteria

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

# MITRE ATT&CK Navigator Layer



# 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

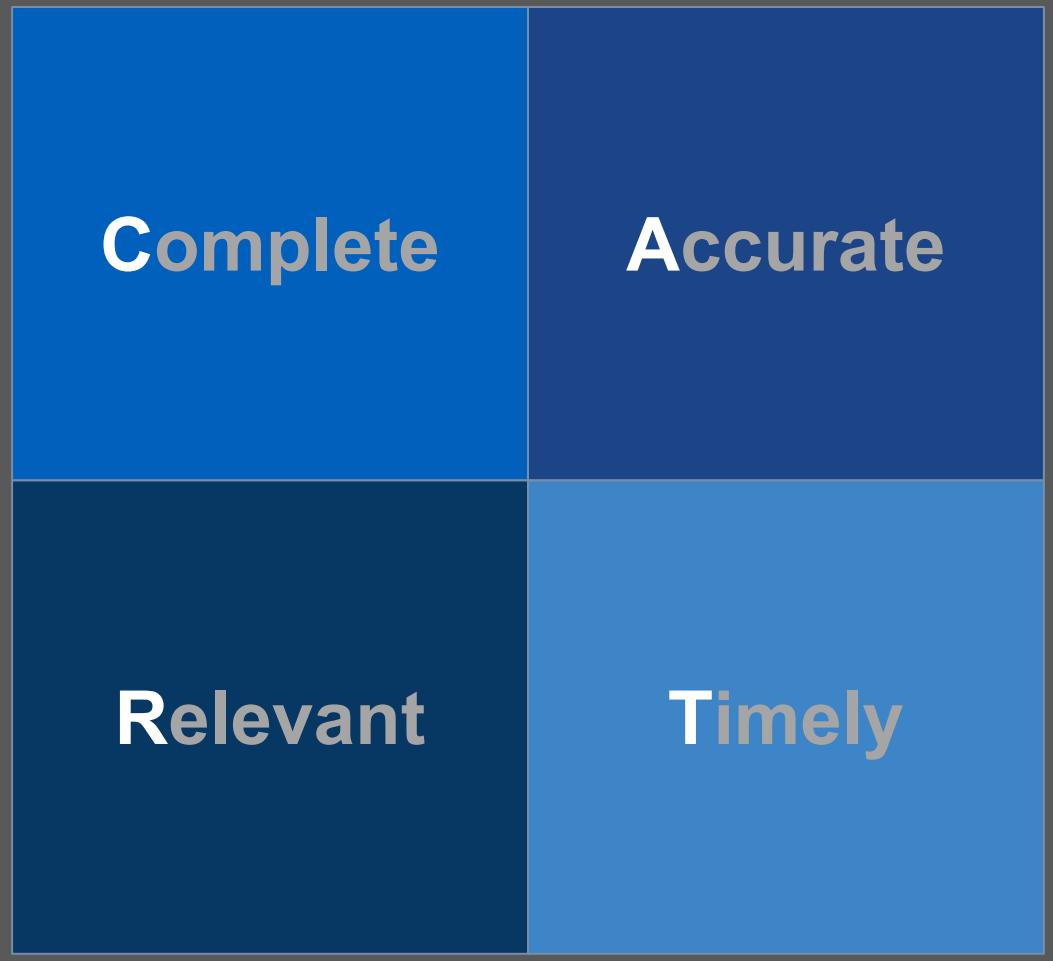
# Feedback & Evaluation

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/

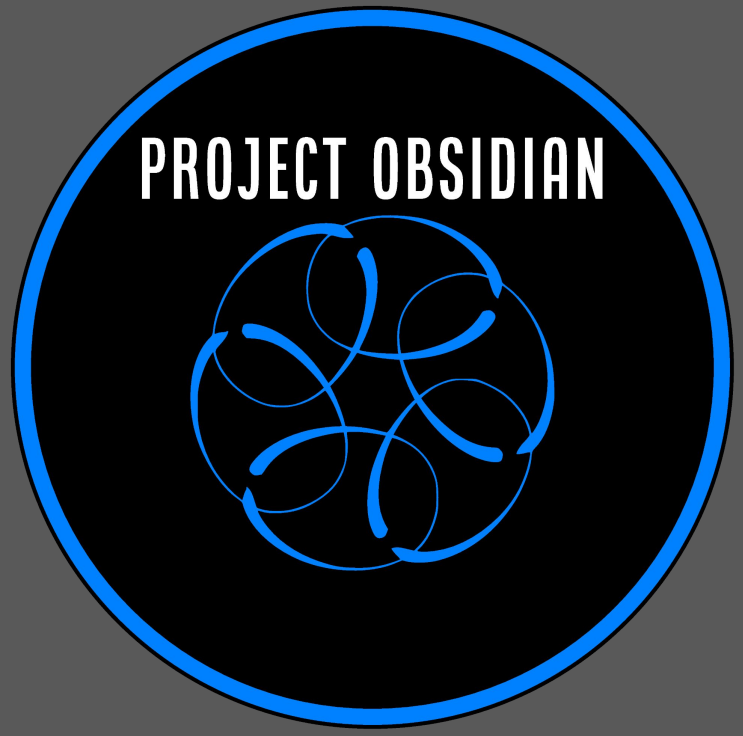
Any.run

https://app.any.run

VirusTotal

https://virustotal.com

Mitre ATT&CK Navigator
https://mitre-attack.github.io/attack-navigator/




# Thank you

Join the conversation

https://discord.blueteamvillage.org