Project Obsidian

Cyber Threat Intelligence

Module 4: Operationalizing Threat Intelligence

Agenda

- **Objective**
- **Planning & Direction:** Intelligence-driven actions
- **Collection:** Industry-focused report
- **Processing:** Report data & information
- **Analysis & Production:** Produce outputs
- **Dissemination:** Share the report
- **Feedback & Evaluation:** Receive feedback

Objective

Objective - Module 4

Demonstrate how a report can be operationalized.

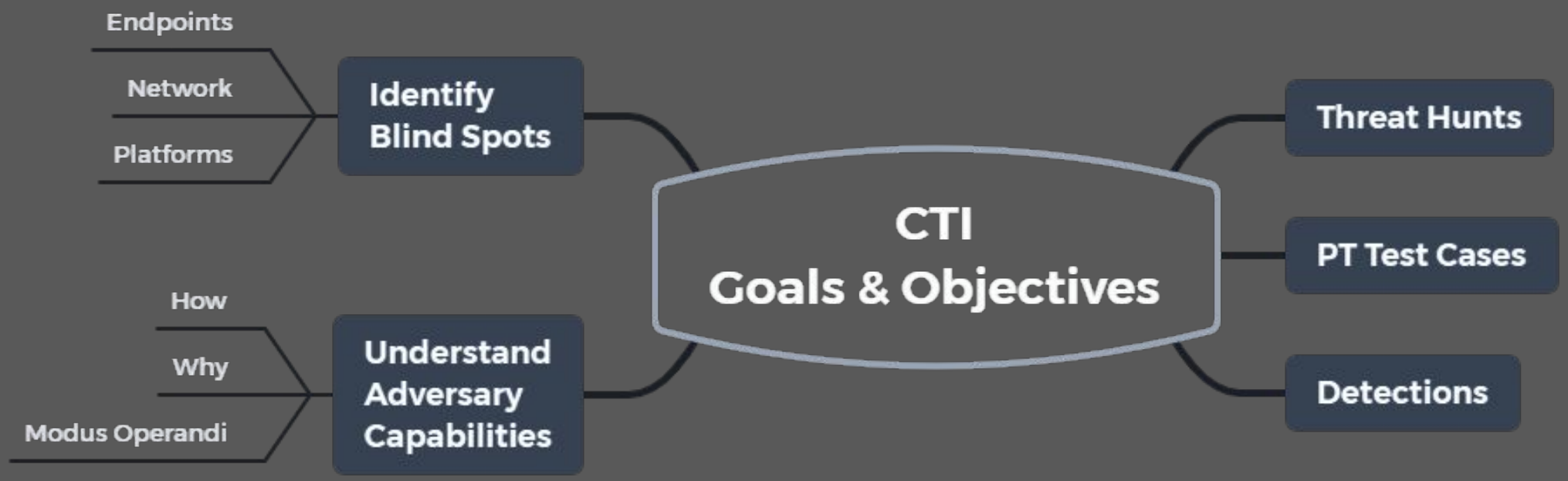
Planning & Direction

Planning & Direction

Goals & Objectives

- Sweep environment for IOCs
- SOC/IT: opportunities for blocks and detections
- Threat hunt team: new hunt
- Purple team: new test cases
- Forensics team: situational awareness
- Inform management & executives: situational awareness

Planning & Direction



Collection

Collection

Sourcing a report may require using a manual method of collection.

- Review the report
- Identify and extract data, information, and intelligence
- Store, tag, sort, etc

Automating report consumption may be a feature in some platforms.

Processing

Processing

- Identify data, information, and intelligence in the intrusion report
- Pull into your platform/storage of choice (can this be improved?)
- Sort intrusion data: TTPs, etc
- Automate IOC sweep: send data to SIEM and/or other platforms

Analysis and Production

Production - Report Summary

Report from a peer organization

- Executive summary
- TTPs
- Diamond model for intrusion analysis
- MITRE ATT&CK navigator layer
- Detections
- IOCs

Production - Beyond the Report

Get the required data to stakeholders in the appropriate format.

- Defenders
- IT
- Forensics team
- Incident Response team
- Threat Hunt team
- Purple Team team

Production - Data Management

How is data

- Documented
- Standardized
- Modeled

How is data quality measured?

https://threathunterplaybook.com/pre-hunt/data_management.html

Who is in charge of data management?

Production - IOC List

Type	Value
URL	https[:]//drive[.]google[.]com/file/d/1QwcBy3ukLWzRkDb7rmuSEHwQFVUYN2Fx/
Domain	https[:]//webwormhole[.]io
Domain	https[:]//app[.]interactsh[.]com
Domain	https[:]//transfer[.]sh
Domain	https[:]//file[.]pizza
URL	https[:]//raw[.]githubusercontent[.]com/puckiestyle/powershell/master/SharpHound[.]ps1
URL	https[:]//raw[.]githubusercontent[.]com/PowerShellMofia/master/Recon/Invoke-Portscan[.]ps1
URL	https[:]//raw[.]githubusercontent[.]com/PowerShellEmpire/PowerTools/master/PowerView/powerview[.]ps1
URL	https[:]//raw[.]githubusercontent[.]com/EmpireProject/Empire/master/data/module_source/credentials/Invoke-Kerberoast[.]ps1
URL	https[:]//raw[.]githubusercontent[.]com/BC-SECURITY/Empire/master/empire/server/data/module_source/credentials/Invoke-Mimikatz[.]ps1

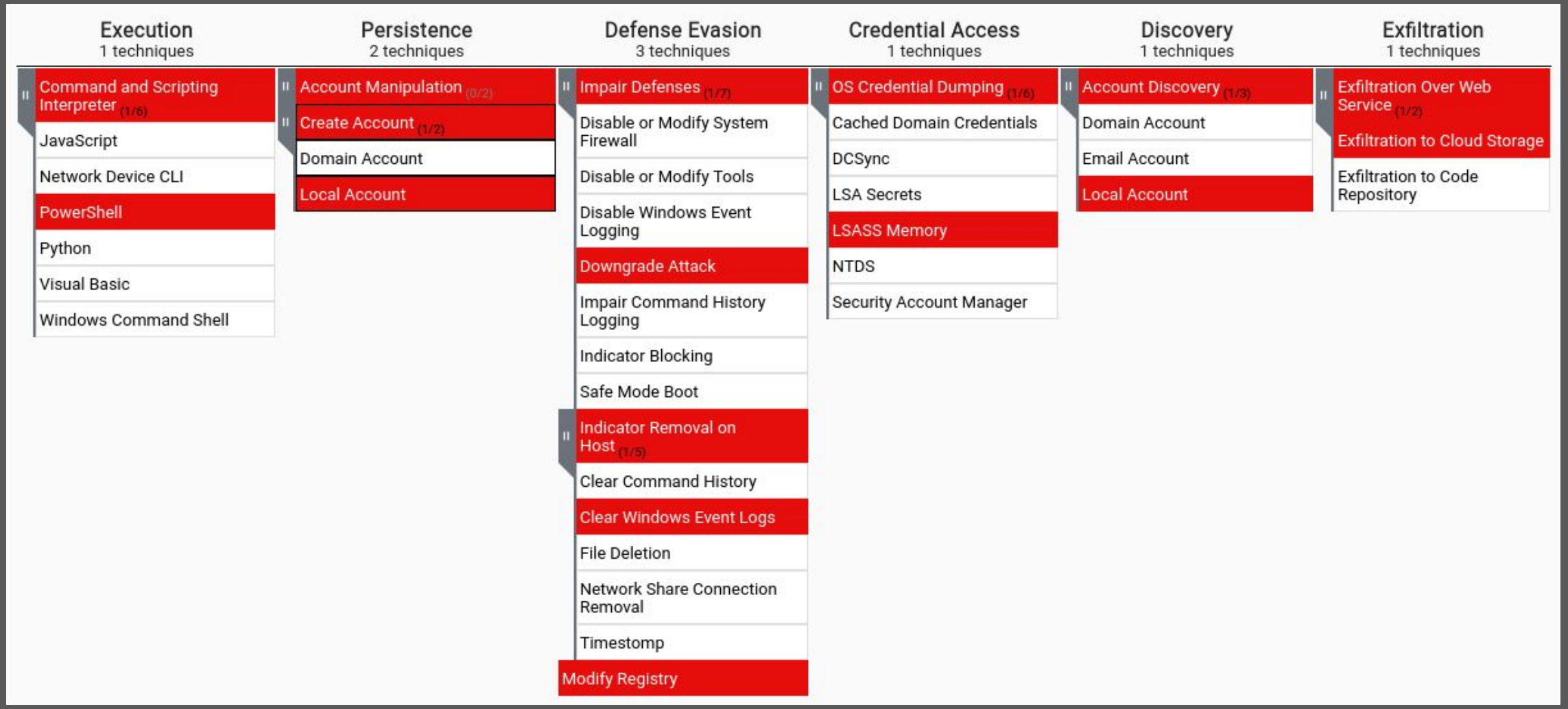
Production - Report Summary

Infrastructure	Victim	Capability	Adversary/Threat
https[:]//file[.]pizza https[:]//transfer[.]sh https[:]//app.interactsh[.]com https[:]//webwormhole[.]io	Financial organization	lsass dump using minidump bloodhound mimikatz smbscan portscan sharefinder comsvcs.dll psexec64.exe (lateral) psexecsvc (lateral) net user (discovery) whoami (discovery) lnk files powershell registry modifications - (NTLM Downgrade) clear-eventlog	?

Production - Report Summary

Tactic	Technique	Detail/Procedure
Credential Access	T1003.001	LSASS Dump
Execution	T1059.001	PowerShell
Discovery	T1087	net, whoami
Defense Evasion	T1562.010	Downgrade Attack
Defense Evasion	T1112	Modify Registry
Exfiltration	T1567	Exfil over Web Service
Persistence	T1098	Account Manipulation
Persistence	T1136.001	Create Account: Local Account
Defense Evasion	T1070.001	Indicator Removal on Host: Clear Event Logs
Discovery	T1135	Netwrok Share Discovery: Sharefinder

Production - MITRE ATT&CK Navigator Layer



Production - ATT&CK Navigator JSON

Production - Executive Summary

Provide a concise overview of the incident

- What happened?
- How did it happen?
- How can we prevent and detect similar intrusions?
- What was the goal/motivation of the intrusion?

Can you think of anything else that should be included?

Dissemination

Dissemination

Feedback and Evaluation

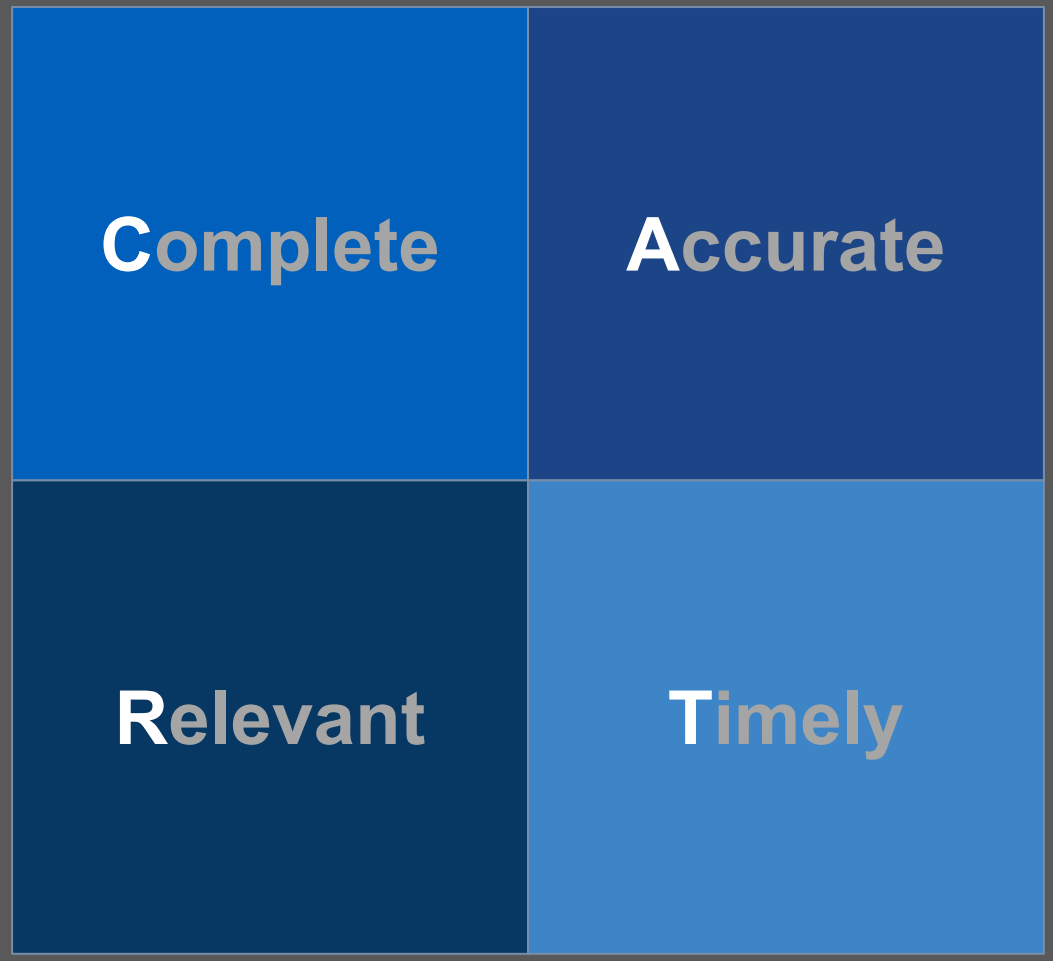
Feedback & Evaluation

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.

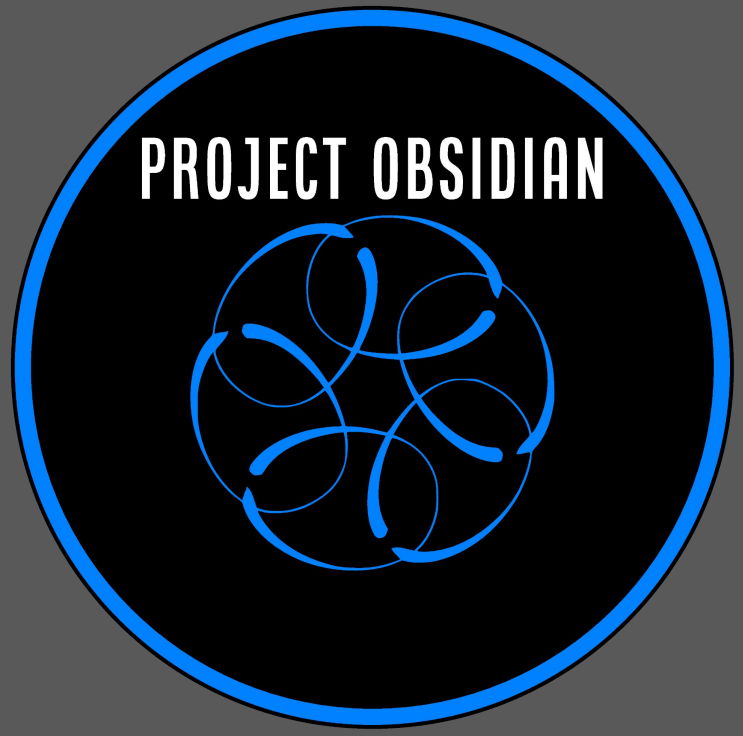
Feedback & Evaluation



Resources

Mitre ATT&CK Navigator

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



Thank you

Join the conversation

https://discord.blueteamvillage.org

Appendix

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?