ICS CYBER THREATS AND A HUNTING WE SHALL GO

“TRADITIONAL” ENTERPRISE SECURITY

- “IT” or Enterprise Security ranges many topics and fields
- As a broad simplification though most of Enterprise Security falls into High Frequency, Low Impact Analysis
  - A high number of events, incidents, and threats impact the community at any given time and all security personnel can expect to deal with numerous incidents throughout their career; this influences strategy and mindset

2019 STATISTICS:

$3.5B USD REPORTED LOSSES FROM CONSUMER COMPLAINTS – FBI

157K+ INCIDENTS AND 3,950 CONFIRMED PUBLIC BREACHES – VERIZON DBIR

13B+ MALICIOUS EMAILS A YEAR – MICROSOFT

HIGH FREQUENCY, LOW IMPACT

When events are high frequency there is a natural tendency to spend resources triaging the events understanding that you will not get to all of them.

Low impact events can lead to risk acceptance and over time underestimating the impact of numerous low impact events.

TRIAGE MINDSET

Inherently reactive thought process that drives an acceptance that something will happen first to warrant your time

HARD LESSONS

Can be difficult to identify or even have the time to identify lessons learned and apply insights across numerous seemingly disconnected events

BURN OUT

Can become overly repetitive and lack intellectual stimulation for those responding to them while potentially being underappreciated by others

THE FREQUENCY & SOPHISTICATION OF THREATS ARE RISING

1998 - 2009

LACK OF COLLECTION

- Campaigns: APT1
- ICS Malware: None

2010 - 2012

PUBLIC INTEREST IN ICS

- Campaigns: Sandworm
- ICS Malware: Stuxnet

2013 - 2015

CAMPAIGNS TARGET ICS

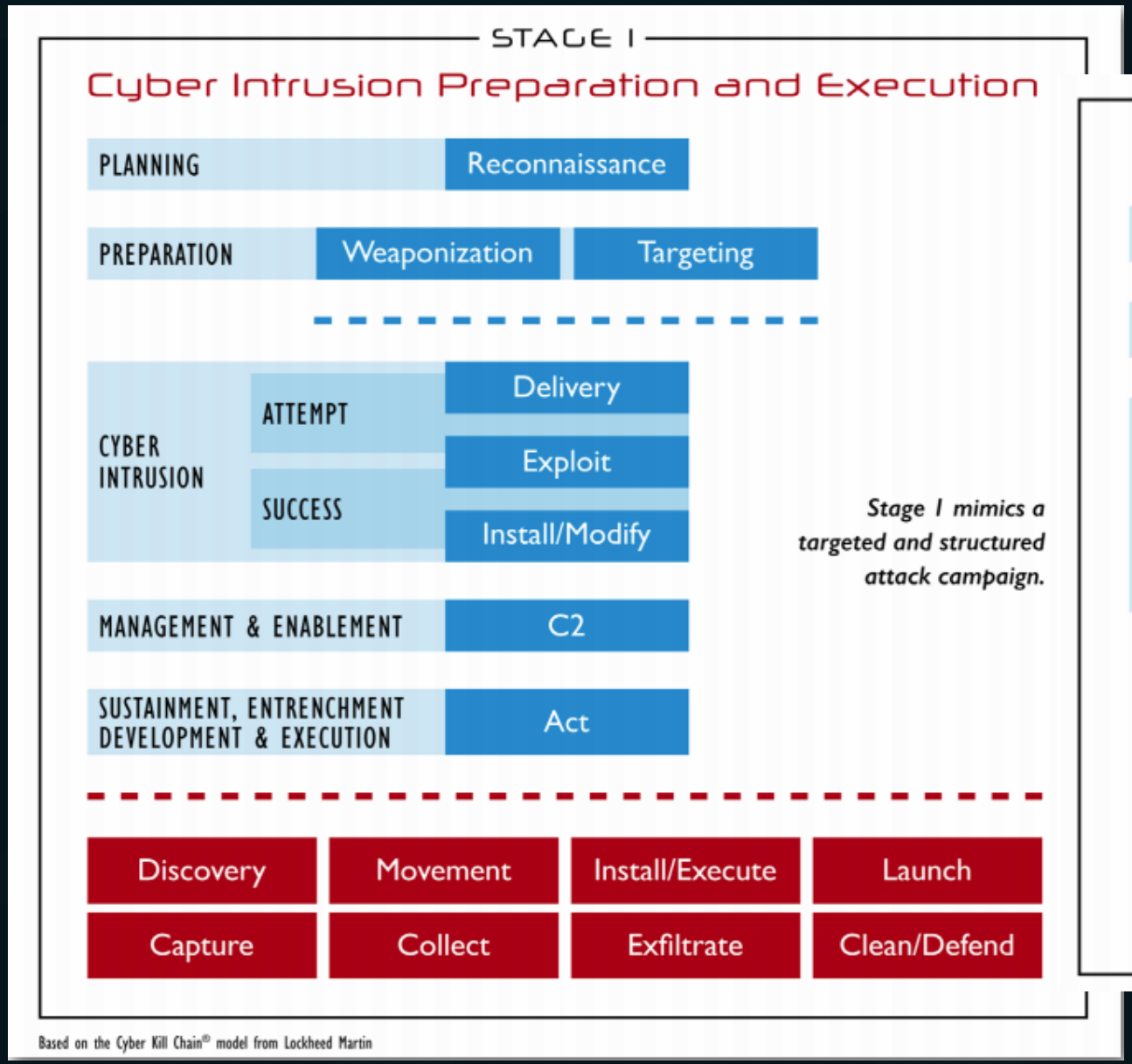
- Campaigns: Dragonfly
- ICS Malware: BlackEnergy 2 and Havex
- First attack to cause physical destruction on civilian infra-structure (German Steel)

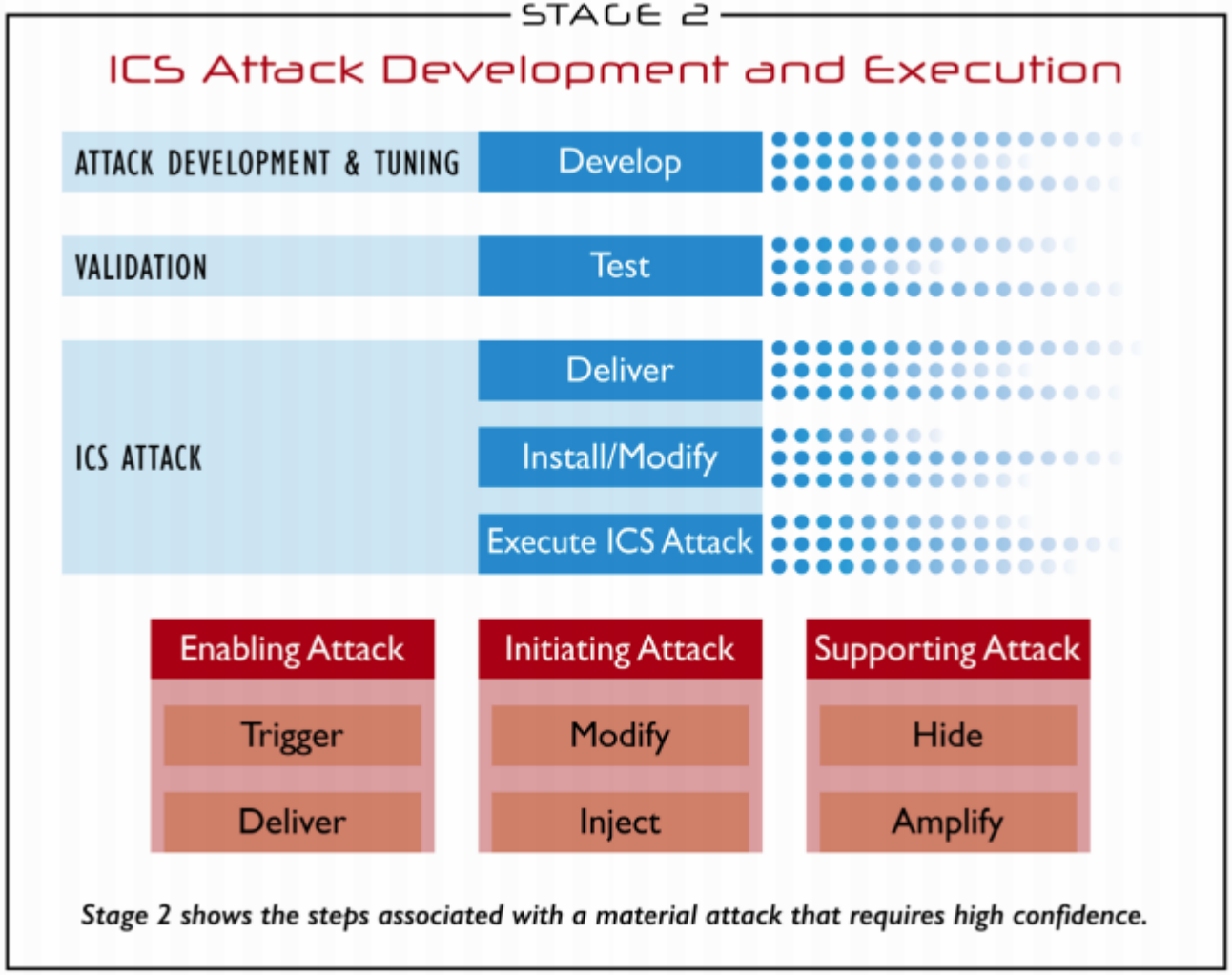
2016 – 2020

ADVERSARIES DISRUPT ICS

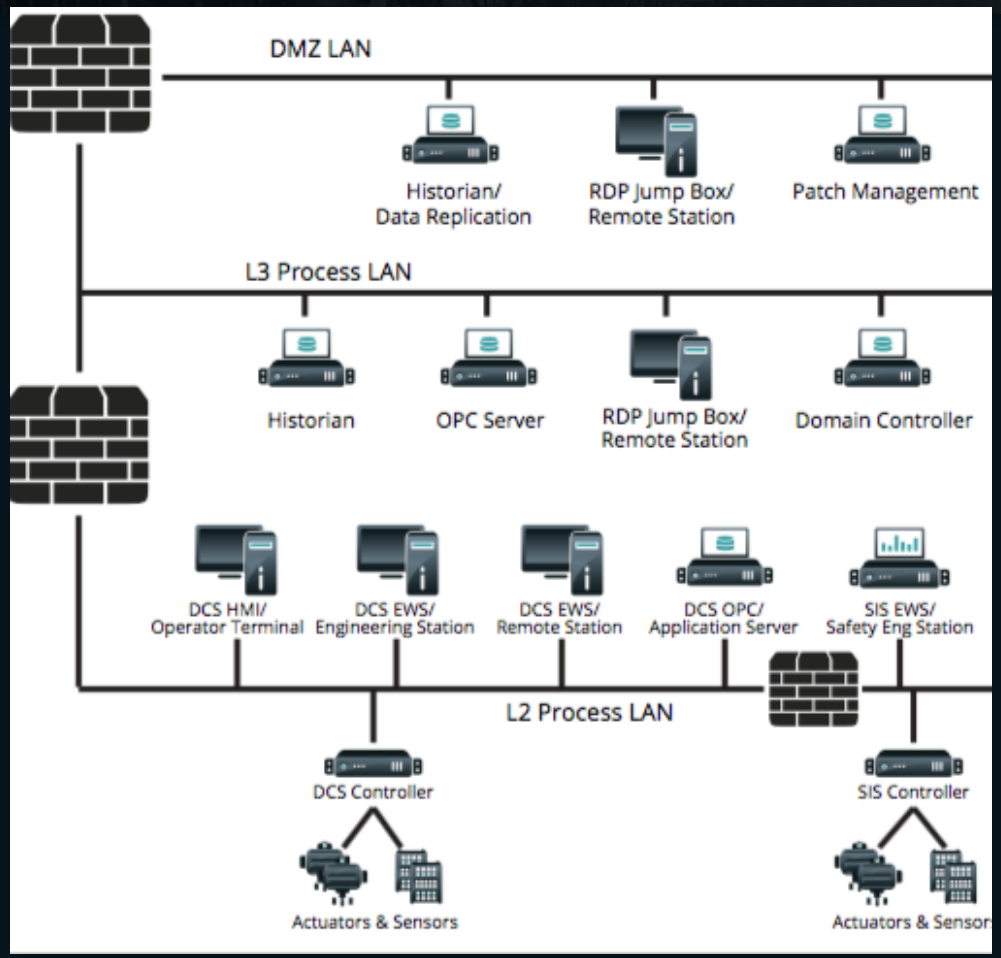
- Activity Groups: 12 unique state threats
- ICS Malware: CRASHOVERRIDE TRISIS, and EKANS
- Ukraine: first and second ever electric grid attacks that disrupt power
- Ransomware and destructive attacks
- First malware to target human life

DRAGOS


STAGE 1
Cyber Intrusion Preparation and Execution
PLANNING
Reconnaissance
PREPARATION
Weaponization
Targeting
CYBER INTRUSION
ATTEMPT
SUCCESS
Delivery
Exploit
Install/Modify
MANAGEMENT & ENABLEMENT
C2
SUSTAINMENT, ENTRENCHMENT DEVELOPMENT & EXECUTION
Act
Stage 1 mimics a targeted and structured attack campaign.
Discovery
Movement
Install/Execute
Launch
Capture
Collect
Exfiltrate
Clean/Defend
Based on the Cyber Kill Chain® model from Lockheed Martin


STAGE 2
ICS Attack Development and Execution
ATTACK DEVELOPMENT & TUNING
Develop
VALIDATION
Test
ICS ATTACK
Deliver
Install/Modify
Execute ICS Attack
Enabling Attack
Trigger
Deliver
Initiating Attack
Modify
Inject
Supporting Attack
Hide
Amplify
Stage 2 shows the steps associated with a material attack that requires high confidence.

TRISIS 2017



- XENOTIME compromised petrochemical facility in Saudi Arabia in 2014
- Profiled Safety Instrumented System (SIS) and left for 3 years
- Returned in 2017 and targeted SIS twice
- Root Cause Analysis failure led to second attempt by the adversary
- 1st cyber attack to specifically target human life

https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf

THREAT PROLIFERATION

KNOWN ACTIVITY GROUPS TARGETING ENERGY INDUSTRY

Ten activity groups targeting Energy:

- ELECTRUM
- XENOTIME
- MAGNALLIUM
- ALLANITE
- DYMALLOY
- CHRYSENE
- COVELLITE
- RASPITE
- PARISITE
- WASSONITE

THE INDUSTRIAL THREAT LANDSCAPE

RECENT OBSERVATIONS FROM THE FRONTLINES OF ICS/OT CYBERSECURITY

New Adversaries

Two new threat activity groups underscore the heightened risk and increasing threats to industrial environments as adversaries expand their reach geographically and to new sectors.

Growing Threats

Ransomware targeting ICS claimed multiple new victims this quarter, as organization-specific malware continues to disrupt ICS operations.

Increasing Exposure

A group of new vulnerabilities will have major impacts on the industrial sector in months and years to come as they impact a fundamental communication stack present in many industrial devices.

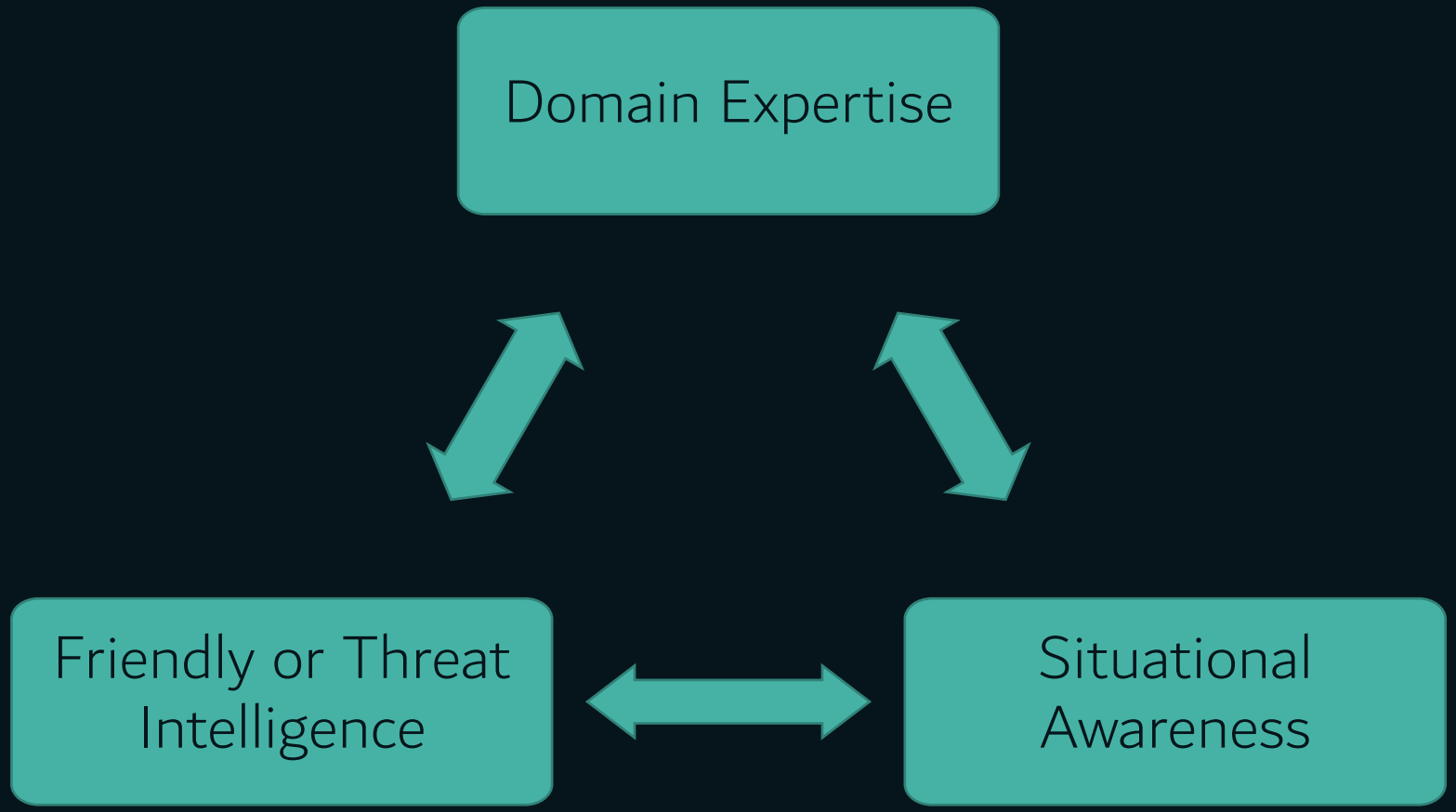
DRAGOS

FIGURE OUT WHAT YOU HAVE - CMF

	CONTROL CENTER	CONTROL CENTER	CONTROL CENTER	TRANSMISSION SUBSTATION	TRANSMISSION SUBSTATION
ASSET TYPE	Windows Human Machine Interface	Data Historian	Network Monitoring Appliance	Windows Human Machine Interface	Remote Terminal Units
DATA TYPE	Windows Event Logs	Alarms	Alerts	Windows Event Logs	Syslog
QUESTION TYPE (KILL CHAIN PHASES)	Exploration, Installation, Actions on Objectives	Actions on Objectives	Internal Reconnaissance, Command and Control, Delivery, Actions on Objectives	Exploitation, Installation, Actions on Objectives	Installation, Actions on Objectives
FOLLOW-ON COLLECTION	Registry Keys	Set Points and Tags	Packet Capture	Registry Keys	Controller Logic
DATA STORAGE LOCATION	Enterprise SIEM	Local	Enterprise SIEM	Local	Local
DATA STORAGE TIME	60 Days	120 Days	30 Days	30 Days	7 Days

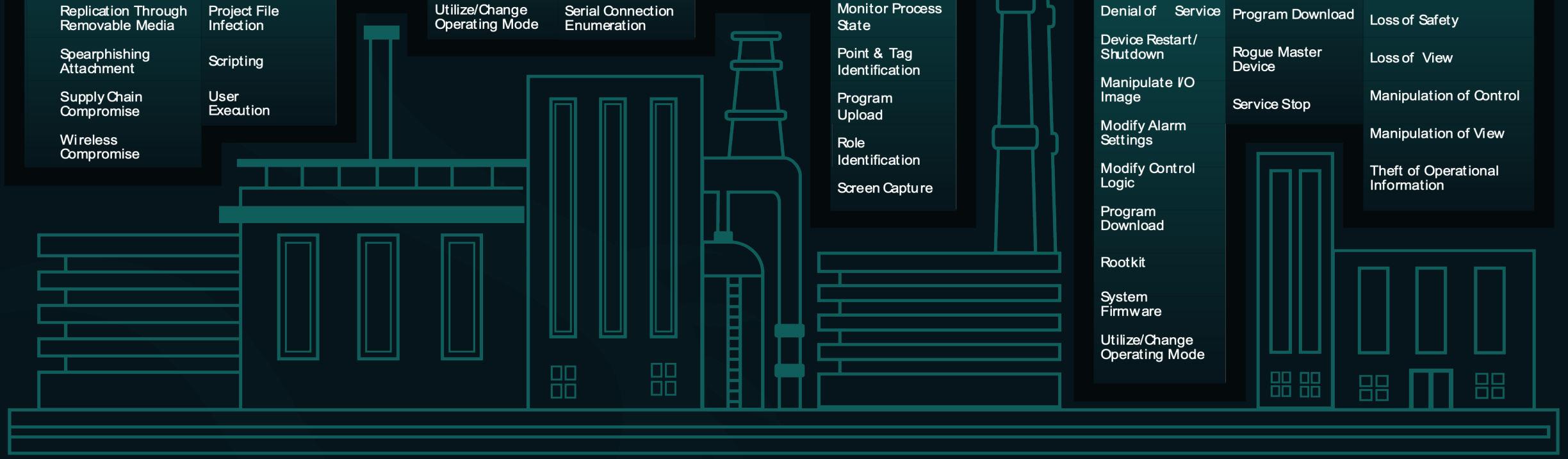
HTTPS://WWW.DRAGOS.COM/WP-CONTENT/UPLOADS/CMF_FOR_ICS.PDF

GENERATE HYPOTHESES



HTTPS://WWW.SANS.ORG/READING-ROOM/WHITEPAPERS/THREATS/GENERATING-HYPOTHESES-SUCCESSFUL-THREAT-HUNTING-37172

INITIAL ACCESS	EXECUTION	PERSISTENCE	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND & CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL	IMPACT
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network ConnectionEnumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/ Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings		Manipulation of View
						Screen Capture		Modify Control Logic		Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		



HTTPS://COLLABORATE.MITRE.ORG/ATTACKICS

DRAGOS

INITIAL ACCESS	EXECUTION	PERSISTENCE	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND AND CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL	IMPACT
Data Historian Compromise	Change Program State	Hooking	Exploitation For Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage To Property
Drive-By Compromise	Command-Line Interface	Module Firmware	Indicator Removal On Host	I/O Module Discovery	Exploitation Of Remote Services	Data From Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial Of Control
Engineering Workstation Compromise	Execution Through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial Of View
Exploit Public-Facing Application	Graphical User Interface	Project File	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss Of Availability
External Remote Services	Man In The Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial Comm Port	Modify Parameter	Loss Of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss Of Productivity And Revenue
Replication Through Removable Media	Project File		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial Of Service	Program Download	Loss Of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss Of View
Supply Chain Compromise	User Execution					Program Upload		Exploitation For Denial Of Service	Service Stop	Manipulation Of Control
Wireless Compromise						Role Identification		Manipulate I/O Image	Spoof Reporting Message	Manipulation Of View
						Screen Capture		Modify Alarm Settings	Unauthorized Command Message	Theft Of Operational Information
								Modify Control Logic		
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

HTTPS://WWW.DRAGOS.COM/MITRE-ATTACK-FOR-ICS/

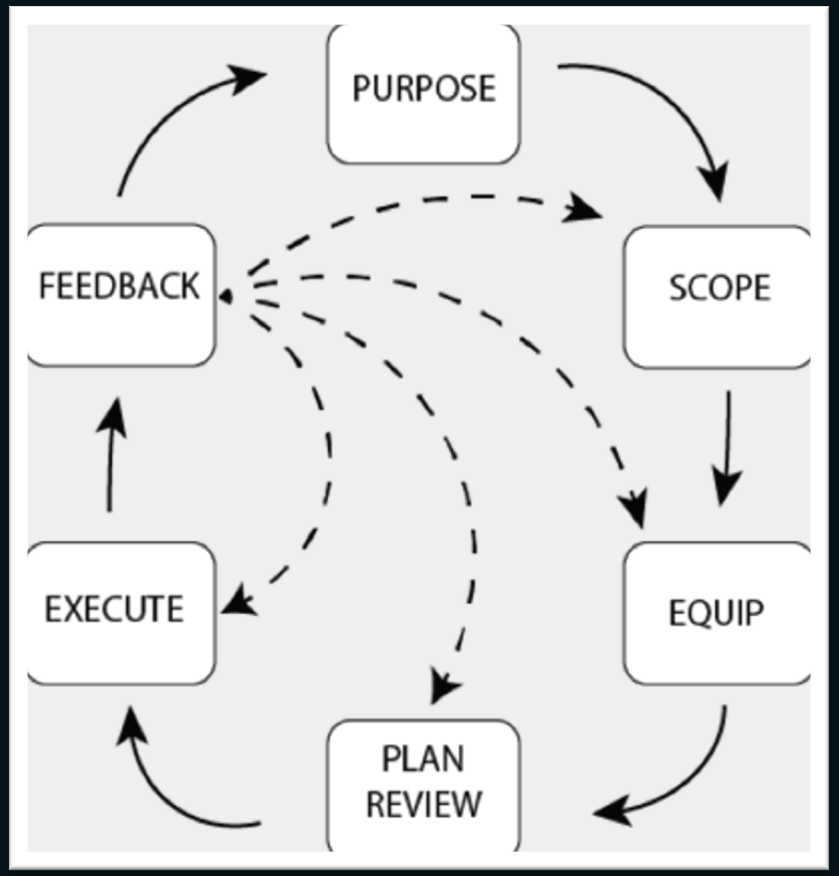
DRAGOS

INITIAL ACCESS	EXECUTION	PERSISTENCE	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND AND CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL	IMPACT
Data Historian Compromise	Change Program State	Hooking	Exploitation For Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage To Property
Drive-By Compromise	Command-Line Interface	Module Firmware	Indicator Removal On Host	I/O Module Discovery	Exploitation Of Remote Services	Data From Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial Of Control
Engineering Workstation Compromise	Execution Through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial Of View
Exploit Public-Facing Application	Graphical User Interface	Project File	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss Of Availability
External Remote Services	Man In The Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial Comm Port	Modify Parameter	Loss Of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss Of Productivity And Revenue
Replication Through Removable Media	Project File		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial Of Service	Program Download	Loss Of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss Of View
Supply Chain Compromise	User Execution					Program Upload		Exploitation For Denial Of Service	Service Stop	Manipulation Of Control
Wireless Compromise						Role Identification		Manipulate I/O Image	Spoof Reporting Message	Manipulation Of View
						Screen Capture		Modify Alarm Settings	Unauthorized Command Message	Theft Of Operational Information
								Modify Control Logic		
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

HTTPS://WWW.DRAGOS.COM/MITRE-ATTACK-FOR-ICS/

DRAGOS

HUNTING FOR XENOTIME: PURPOSE

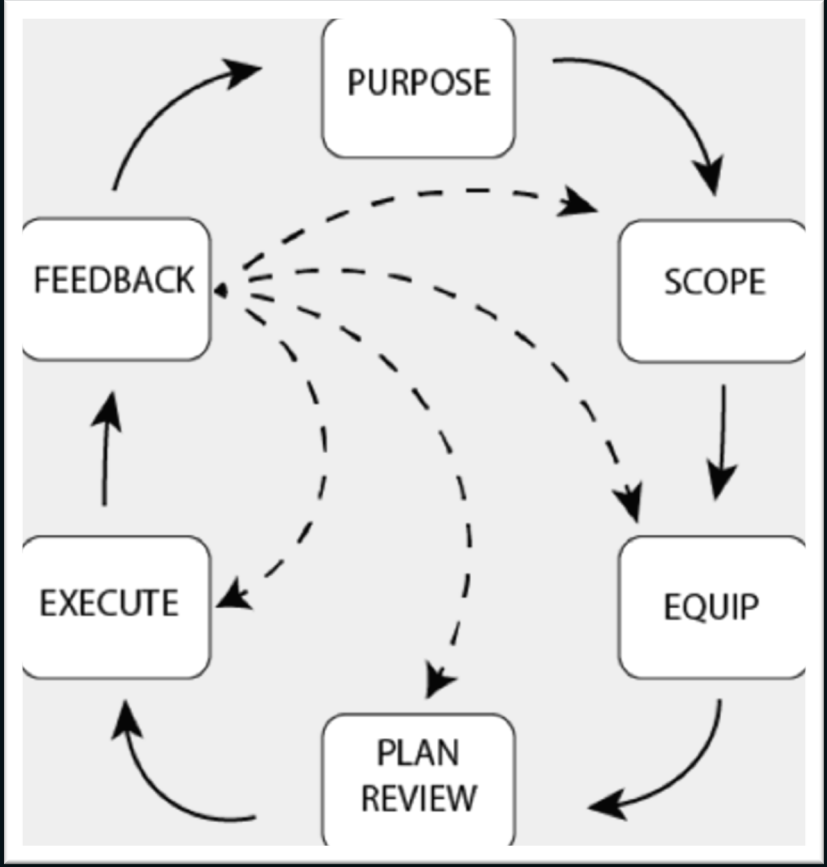


To uncover Xenotime behavior and activity currently present in and environment.

To provide architecture modifications to deny Xenotime easy access to environment

Recommend areas of data visibility and monitoring improvement to detect abnormal behavior

HUNTING FOR XENOTIME: SCOPE: LOCATION



TOP 3 OIL REFINERIES BY PRODUCTION

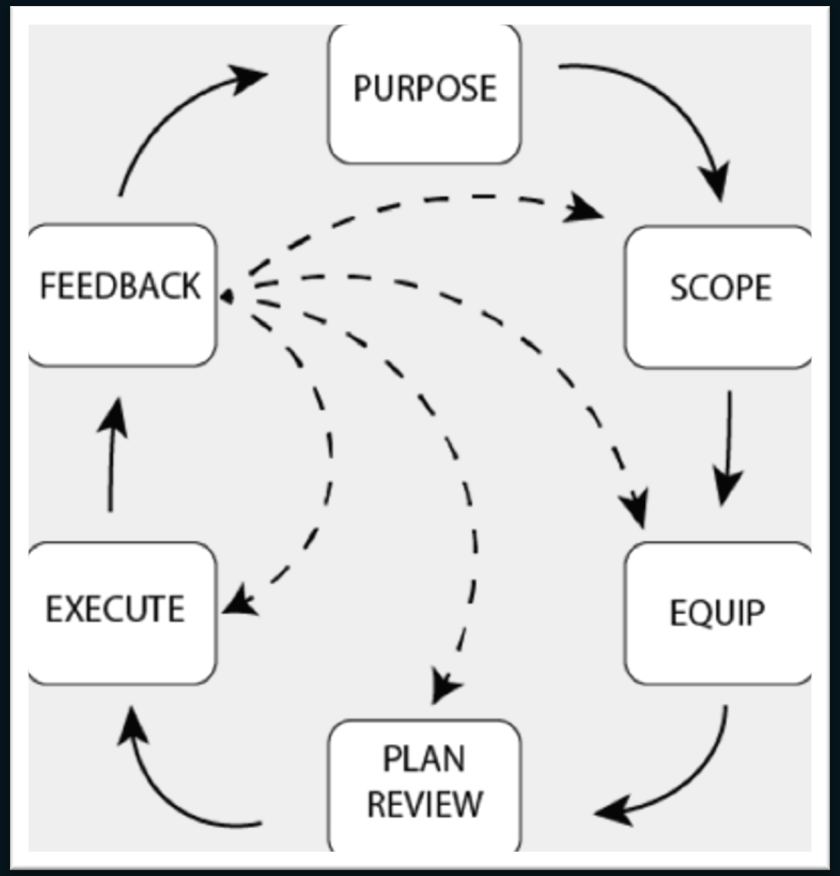
IT to OT Ingress/Egress Boundary

+ Remote Connections

OT Network

+ Safety Instrumentation System
+ Supporting Control Systems interacting with SIS

HUNTING FOR XENOTIME: SCOPE: HYPOTHESES

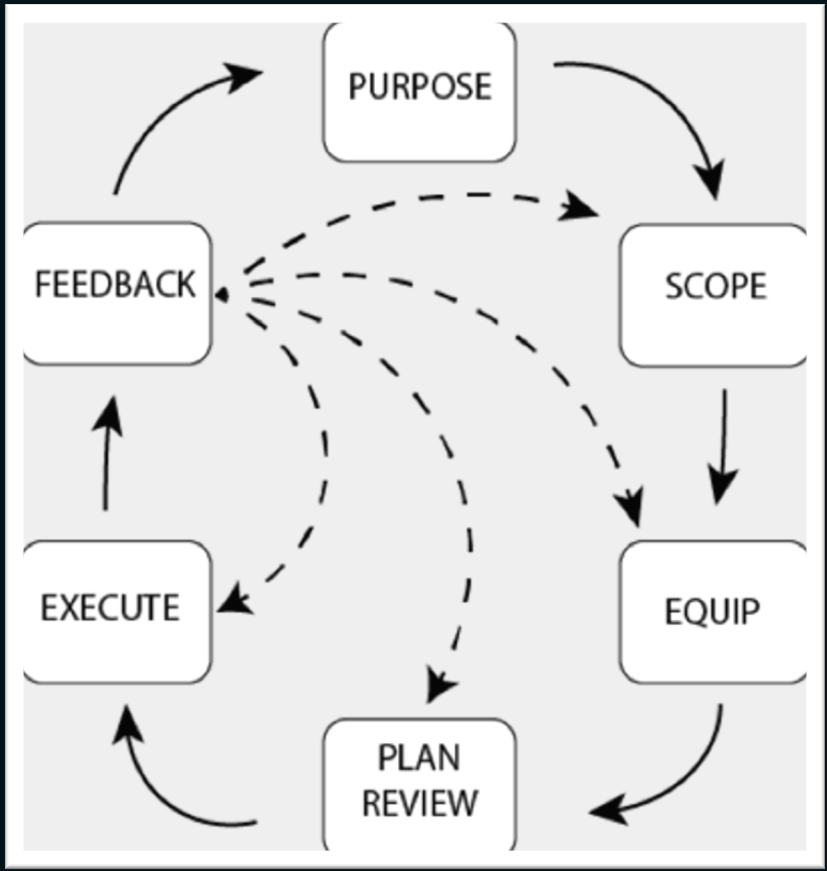


Adversary is leveraging approved remote connections (RDP and VPN) from the IT network to gain access to the OT network.

Adversary is sending malicious commands from the SIS workstation to the SIS controllers attempting to disrupt system functions.

Adversary is conducting reconnaissance by accessing internet enabled servers over SMB and RDP

HUNTING FOR XENOTIME: EQUIP: CMF



Data Source	Storage Duration
Perimeter Firewall Logs	~2 weeks
Windows Event Logs - Internet enabled servers	~4 days
Network Traffic – IT	~7 days
Network Traffic – OT (Including SIS)	~7 days
Host logs from SIS	None available
Process Historian	5 years
VPN Concentrator	~4 weeks
Intrusion Detection System	Deployed in IT, not OT

HUNTING FOR XENOTIME: EQUIP: CMF

Adversary is leveraging approved remote connections (RDP and VPN) from the IT network to gain access to the OT network.

Data Source	Storage Duration
Perimeter Firewall Logs	~2 weeks
Windows Event Logs - Internet enabled servers	~4 days
Network Traffic – IT	~7 days
Network Traffic – OT (Including SIS)	~7 days
Host logs from SIS	None available
Process Historian	5 years
VPN Concentrator	~4 weeks
Intrusion Detection System	Deployed in IT, not OT

HUNTING FOR XENOTIME: EQUIP: CMF

Adversary is sending malicious commands from the SIS workstation to the SIS controllers attempting to disrupt system functions.

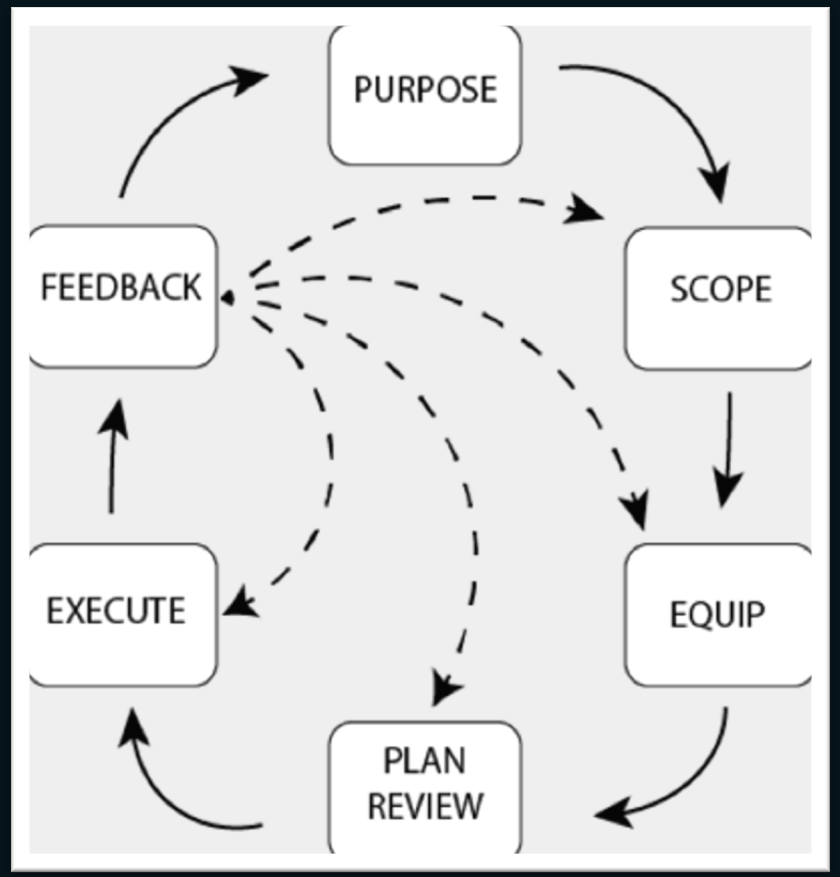
Data Source	Storage Duration
Perimeter Firewall Logs	~2 weeks
Windows Event Logs - Internet enabled servers	~4 days
Network Traffic – IT	~7 days
Network Traffic – OT (Including SIS)	~7 days
Host logs from SIS	None available
Process Historian	5 years
VPN Concentrator	~4 weeks
Intrusion Detection System	Deployed in IT, not OT

HUNTING FOR XENOTIME: EQUIP: CMF

Adversary is conducting reconnaissance by accessing internet enabled servers over SMB and RDP

Data Source	Storage Duration
Perimeter Firewall Logs	~2 weeks
Windows Event Logs - Internet enabled servers	~4 days
Network Traffic – IT	~7 days
Network Traffic – OT (Including SIS)	~7 days
Host logs from SIS	None available
Process Historian	5 years
VPN Concentrator	~4 weeks
Intrusion Detection System	Deployed in IT, not OT

HUNTING FOR XENOTIME: EQUIP: RESOURCES



TEAM RESOURCES

Senior and Junior Analysts

OT Operators

Network Admins

Any SME on Network

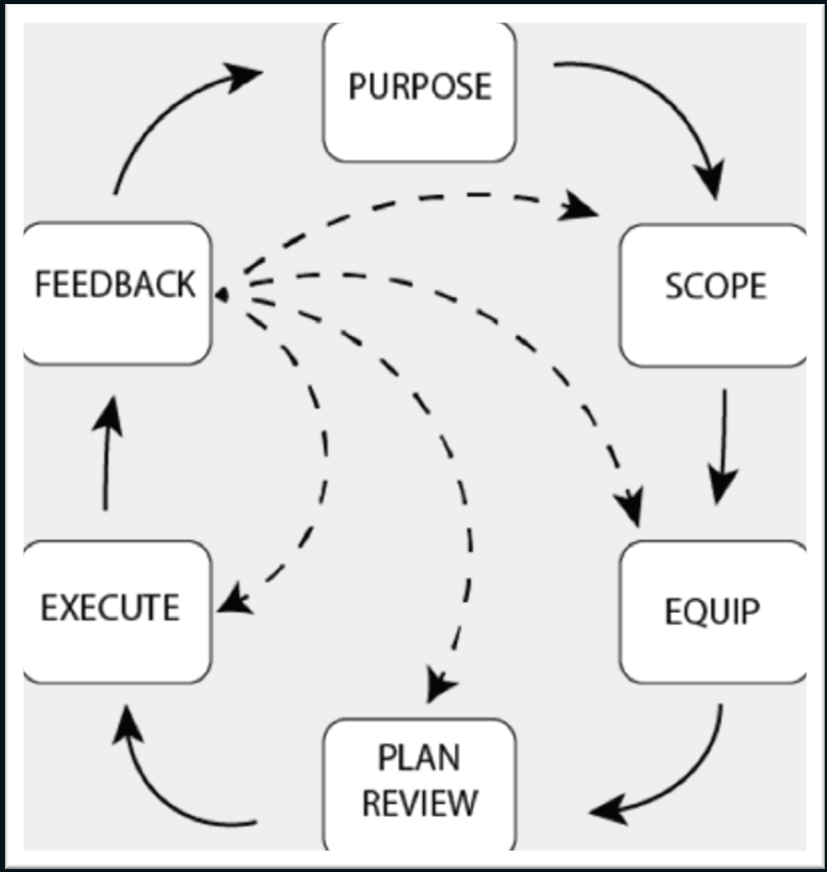
TOOLS

ICS Security Technology (Dragos Platform…obviously)

Or Open-Source Tools (Zeek/YARA)

TIME ALLOTMENT

HUNTING FOR XENOTIME: PLAN REVIEW



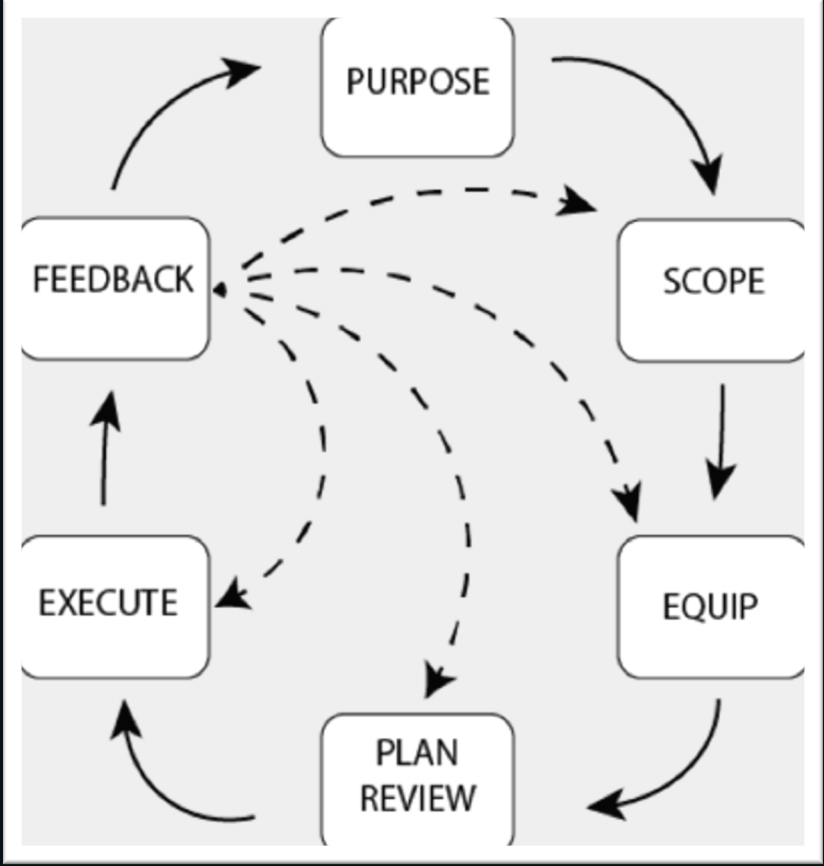
Does the plan achieve the purpose?

Are more resources required?

Is management okay with plan moving forward?

Has anything changed?

HUNTING FOR XENOTIME: EXECUTE

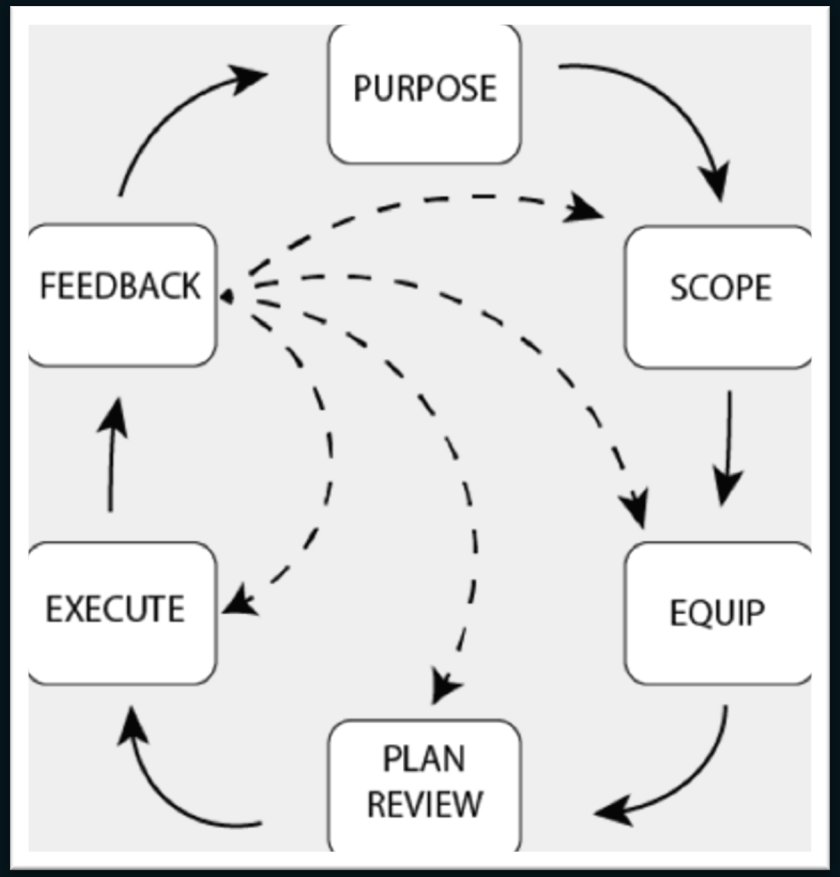


Analyze data sources for Xenotime behaviors as observables across all hypotheses

Create a report summarizing all findings

Report should be focused on conveying how the hunt achieved the “Purpose”

HUNTING FOR XENOTIME: FEEDBACK



Was 3 facilities too large a project for time allotment?

Is it possible to automate this hunt into stable detections?

How can we be more efficient?

THANK YOU

DRAGOS

RLEE@DRAGOS.COM
@ROBERTMLEE