

5 Considerations for ICS Incident Response

Kai Thomsen

Director, Global Incident Response Services, Dragos Inc.

whoami

- Director of Global Incident Response Services @ Dragos Inc.
- Certified SANS Instructor, ICS curriculum, teaching "ICS Active Defense and Incident Response" (ICS515)
- Spent ~7 years in the automotive industry and ~14 years in the steel industry in various security roles, including Incident Response and Business Continuity
- Have you noticed 2020 is somehow different? I compensate spending all my time in the home office with carving my neighborhood on my OneWheel





Agenda

1. **Preparing for an ICS IR Event**
2. **Assigning IR Decision Making Responsibility**
3. **Determining when a Shutdown of Operations is Justified**
4. **Getting to Root Cause**
5. **Engaging an IR Team**

Preparing for an ICS IR Event



Serious security incidents in ICS are low frequency, but high impact. The potential of physical impact is the most important differentiator of IT vs. ICS incidents. Regardless whether your ICS is considered critical infrastructure or not, it is critical to *your business*.

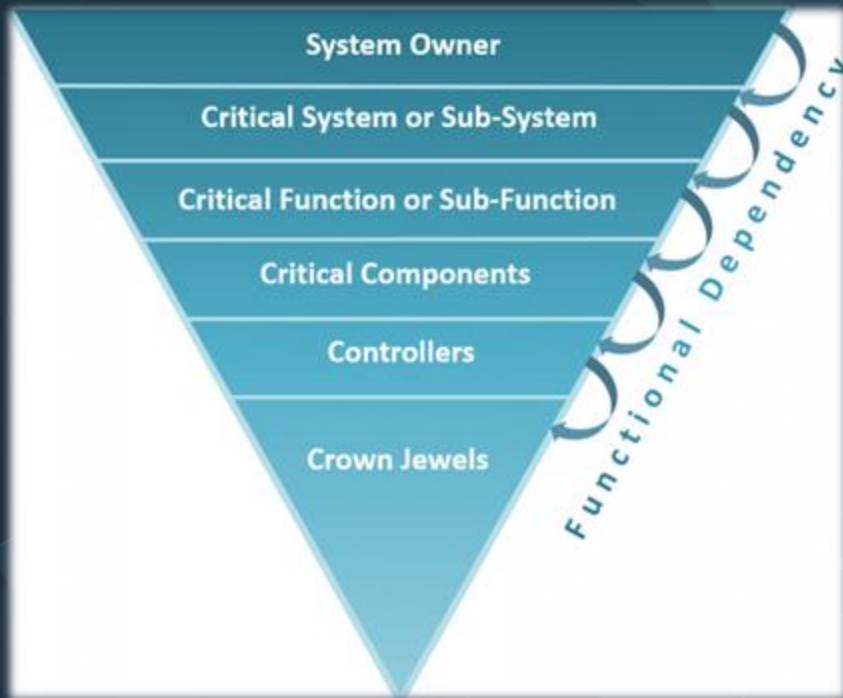
ICS IR – The Mission

- IT is a business enabler, not an end by itself. IT forgets that sometimes ;-)
- The mission of cybersecurity is to mitigate certain business risks
- The mission of ICS Incident Response is to counter cyber threats against the ICS
- The most important tasks of ICS IR during an incident are
 - Scoping the nature and extent of the compromise
 - Providing decision makers with a recommended course of action
 - Conducting Root Cause Analysis to identify how the adversary was able to compromise the ICS environment

Know Your Most Important Assets

Focus on the Crown Jewels

If you are aware what the most important systems are for your plant and business processes, you can focus your defense efforts on these, and the most likely path and adversary might take to reach them.



Know Your Adversary – Focus on Relevant Activity Groups

AL **ALLANITE**
since 2017

- MODE OF OPERATION**
Watering-hole and phishing leading to ICS recon and screenshot collection
- CAPABILITIES**
Powershell scripts, THC Hydra, SecuriDump, Inveigh, PSExec
- VICTIMOLOGY**
Electric utilities, US & UK
- LINKS**
Palmetto Fusion

Ch **CHRYSENE**
since 2017

- MODE OF OPERATION**
IT compromise, information gathering and recon against industrial orgs
- CAPABILITIES**
Watering holes, 64-bit malware, covert C2 via IPv6 DNS, ISMDOOR
- VICTIMOLOGY**
Oil & Gas, Manufacturing, Europe, MENA, N. America
- LINKS**
OilRig, Greenbug

Co **COVELLITE**
since 2017

- MODE OF OPERATION**
IT compromise with hardened anti-analysis malware against industrial orgs
- CAPABILITIES**
Encoded binaries in documents, evasion techniques
- VICTIMOLOGY**
Electric Utilities, US
- LINKS**
Lazarus, Hidden Cobra

Dy **DYMALLOY**
since 2016

- MODE OF OPERATION**
Deep ICS environment information gathering, operator credentials, industrial process details
- CAPABILITIES**
GOODOR, DORSHEL, KARAGANY, Mimikatz
- VICTIMOLOGY**
Turkey, Europe, US
- LINKS**
Dragonfly2, Berserker Bear

EL **ELECTRUM**
since 2016

- MODE OF OPERATION**
Electric grid disruption and long-term persistence
- CAPABILITIES**
CRASHOVERRIDE
- VICTIMOLOGY**
Ukraine, Electric Utilities
- LINKS**
Sandworm

Ma **MAGNALLIUM**
since 2016

- MODE OF OPERATION**
IT network limited, information gathering against industrial orgs
- CAPABILITIES**
STONEDRILL wiper, variants of TURNEDUP malware
- VICTIMOLOGY**
Petrochemical, Aerospace, Saudi Arabia
- LINKS**
APT33, PARISITE

Pi **PARISITE**
since 2017

- MODE OF OPERATION**
VPN compromise of IT networks to conduct reconnaissance
- CAPABILITIES**
Exploiting known VPN vulnerabilities; SSH.NET, MASSCAN, and dnsmiff hacking tools
- VICTIMOLOGY**
US, Middle East, Europe, Australia, Electric, Oil & Gas, Aerospace, Government
- LINKS**
MAGNALLIUM

Ra **RASPITE**
since 2017

- MODE OF OPERATION**
IT network limited, information gathering on electric utilities with some similarities to CHRYSENE
- CAPABILITIES**
Service installer malware designed to beacon out to adversary infrastructure
- VICTIMOLOGY**
Electric Utilities, US, Saudi Arabia, Japan, Europe
- LINKS**
LeafMiner

St **STIBNITE**
since 2018

- MODE OF OPERATION**
Extensive use of Dynamic DNS providers, spoofed domains for government & tech entities, adversary-owned infrastructure
- CAPABILITIES**
Malicious document files, credential theft website, multi-stage Python scripts, PoE2RAT framework, publicly-available tools and scripts
- VICTIMOLOGY**
Wind Power, Government, Asia
- LINKS**
None

Ta **TALONITE**
SINCE 2019

ADVERSARY:

- Behavioral overlaps with APT10
- Potential links to Chinese state interests

CAPABILITIES:

- Phishing with malicious attachments
- Use of custom malware with multiple components
- Leveraging legitimate software for malicious activity

VICTIM:

- Focused targeting of U.S. Electric utilities from mid 2019 through 2020
- Indications of historical activity in Japan and Taiwan prior to 2019

INFRASTRUCTURE:

- Combination of adversary-owned and compromised infrastructure
- Infrastructure almost exclusively based in East Asia

Wa **WASSONITE**
since 2018

- MODE OF OPERATION**
IT compromise and information gathering
- CAPABILITIES**
DTrack RAT, Mimikatz, system tools for file transfer and lateral movement
- VICTIMOLOGY**
India, South Korea, Japan, Electric, Nuclear, Oil & Gas, Manufacturing, Research
- LINKS**
COVELLITE

Xt **XENOTIME**
since 2014

- MODE OF OPERATION**
IT compromise and information gathering
- CAPABILITIES**
TRISIS, custom credential harvesting, off the shelf tools
- VICTIMOLOGY**
Oil & Gas, Middle East, US, Europe
- LINKS**
None

<https://www.dragos.com/threat-activity-groups/>

Example: Adversaries based on Industry Vertical

Threat Activity Groups We're Tracking

The Threat Activity Group reports below are compiled by our expert practitioners to provide awareness about your threat landscape and evolving threats, so you can create defensive plans to protect your ICS environments.

Electric United States →



XENOTIME

SINCE 2014

Focused on physical destruction and long-term persistence



COVELLITE

SINCE 2017

IT compromise with hardened anti-analysis malware against industrial orgs



MAGNALLIUM

SINCE 2017

IT network limited, information gathering against industrial orgs



RASPITE

SINCE 2017

IT network limited, information gathering on electric utilities with some similarities to CHRYSENE



PARISITE

SINCE 2017

VPN compromise of IT networks to conduct reconnaissance




ALLANITE

SINCE 2017

Watering-hole and phishing leading to ICS recon and screenshot collection

Learn about the Adversary and their TTP's

COVELLITE operates globally with targets primarily in Europe, East Asia, and North America. US targets emerged in September 2017 with a small, targeted phishing campaign directed at select U.S. electric companies. The phishing emails contained a malicious Microsoft Word document and infected computers with malware.



COVELLITE
since 2017

- > **MODE OF OPERATION**
IT compromise with hardened anti-analysis malware against industrial orgs
- > **CAPABILITIES**
Encoded binaries in documents, evasion techniques
- > **VICTIMOLOGY**
Electric Utilities, US
- > **LINKS**
Lazarus, Hidden Cobra



The malicious emails discovered in the fall masqueraded as resumes or invitations. They delivered a remote access tool (RAT) payload which was used to conduct reconnaissance and enable persistent, covert access to victims' machines.

COVELLITE's infrastructure and malware are similar to the hacking organization known as LAZARUS GROUP by Novetta and HIDDEN COBRA by the U.S. Department of Homeland Security.

LAZARUS GROUP is responsible for attacks ranging from the [2014 attack](#) on Sony Pictures to a number of Bitcoin heists in 2017. Technical analysis of COVELLITE malware indicates an evolution from known LAZARUS toolkits. However, aside from technical overlap, it is not known how the capabilities and operations between COVELLITE and LAZARUS are related.

COVELLITE remains active but appears to have abandoned North American targets, with indications of activity in Europe and East Asia. Given the group's specific interest in infrastructure operations, rapidly improving capabilities, and history of aggressive targeting, Dragos considers this group a primary threat to the ICS industry.

Identify Techniques

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 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	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
			Program Download							
			Rootkit							
	System Firmware									
	Utilize/Change Operating Mode									

Understand Your Detection Capabilities

Collection Management Framework

	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



Build out Detection Capabilities

Initial Access	Execution	Persistence	Privilege	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impact: Process Control	Impact
Local Windows Compromise	Change Program State	Hooking	Enumerate for Network	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Network Disruption Systems Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command Line Interface	Module Hijacking	Indicator Removal in Host	IO Module Hijacking	Exploitation of Remote Services	Data from Information Assets/Logs	Construction Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Location through API	Process Download	Misconfiguring	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Misconfiguring	Denial of View
Control Public Facing Application	Graphical User Interface	Project File	Human Master Service	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Main in the Middle	System Firmware	Rootkits	Network Sniffing	Remote File Copy	IO Image		Block Serial Control Port	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spool Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Redirection Through Removable Media	Project File		Write/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Severing/Disabling Attachment	Scripting					Point & Tap Identification		Device Restart/Shutdown	Require Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Exfiltration for Denial of Service	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Unresponsive I/O Image	Spool Reporting Message	Manipulation of View
						Screen Capture		Modify Alarm Settings	Denial and Command Message	Shift of Operational Information
								Modify Control Logic		
								Program Download		
								Block		
								Program Termination		
								Network/Change Operating Mode		

<https://www.dragos.com/resource/collection-management-frameworks-beyond-asset-inventories-for-preparing-for-and-responding-to-cyber-threats/>

Considerations for ICS IR Preparation

01

Collaborate

Ensure that there is routine honest and constructive dialogue between process operations (OT) teams, and IT and cybersecurity teams. Process engineers know more about operations than cybersecurity specialists ever will, and vice versa. Collaboration is essential.

02

Safety First

Confirm that all essential personnel for onsite IR have the necessary safety certifications and Personal Protection Equipment (PPE).
Ensure everybody on the team is aware of who is ultimately allowed to directly interact with ICS systems. OT operates, IR offers guidance!

03

Adjust

Be aware that IT IR techniques and procedures can't always be adapted 1:1 to ICS.
Acknowledge that access to important systems might be limited and prepare & train for acquisition and analysis within the constraints of your ICS environment.

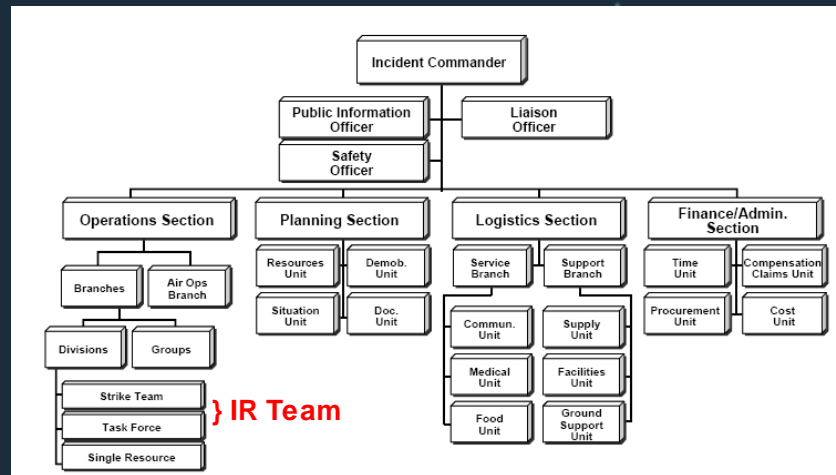
Assigning IR Decision Making Responsibility



The business-critical nature and complexity of ICS systems demand safety & reliability of operations and business continuity take precedence over some IR requirements. Collaboration, chain of command, and a clear assignment of authority to make decisions regarding OT operations and shutdown are key.

The Incident Command System

- The potential of physical impact requires ICS Incident Responders to be integrated into the overall crisis response organization.
- Depending on the duration of the incident, the IR team will be a Strike Team or Task Force.
- The Incident Commander must have the authority to make decisions on pausing or shutting down OT operations.
- Flow of communications and decisions need to be documented in the overall Incident Response Plan (IRP) *and exercised regularly*
- See also Megan Samford's talk ICS4ICS from the 2020 S4 conference at <https://youtu.be/s-71vkOw0Nw>



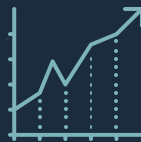
https://en.wikipedia.org/wiki/Incident_Command_System

ICS IR Decision Making Considerations



IC

The Incident Commander (IC) should be selected from the organization's top leadership. Being well respected within the organization and having prior experience with managing critical situations are required.



MTTR

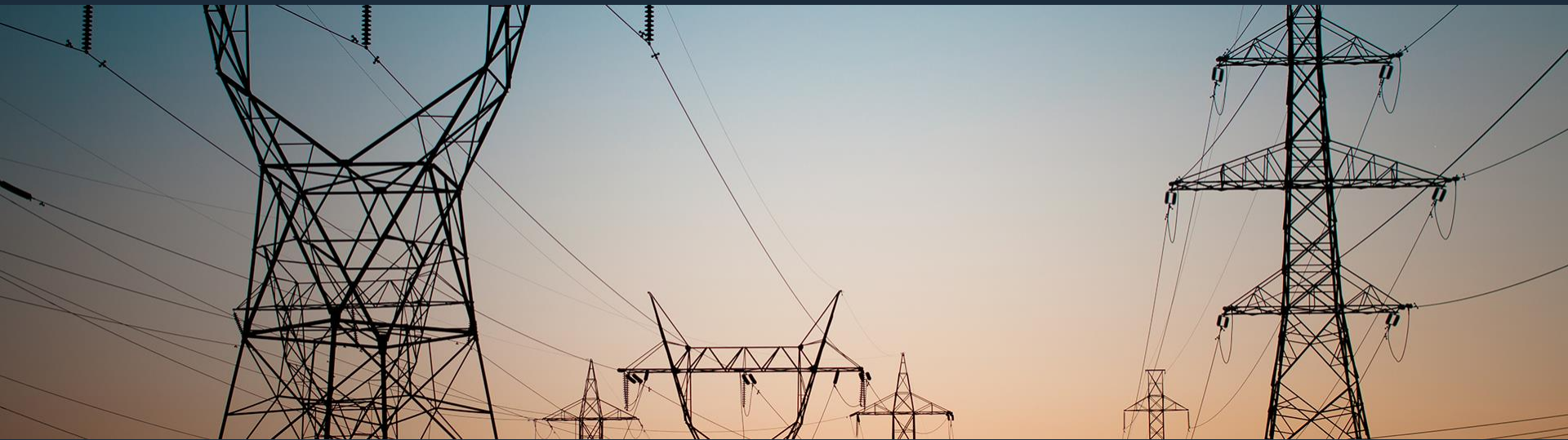
The mean time to recovery (MTTR) needs to be defined by executive leadership. This requirement will drive many aspects of ICS IR, including team size, in-house vs. outsourced, and skillsets.



RoE

Clear Rules of Engagement (RoE) guide the ICS IR team on the Do's and Don'ts during an incident. They need to be strictly followed to ensure safety & reliability of operations. Adaption or a planned escalation procedure might be necessary depending on the incident.

Determining When Shutdown of Operations is Justified



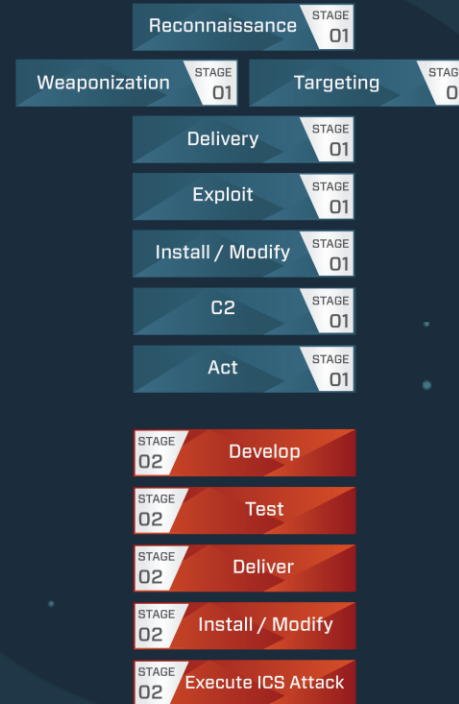
Serious security incidents in ICS are low frequency, but high impact. The potential of physical impact is the most important differentiator of IT vs. ICS incidents. Regardless whether your ICS is considered critical infrastructure or not, it is critical to *your business*.

ICS Cyber Kill Chain Considerations

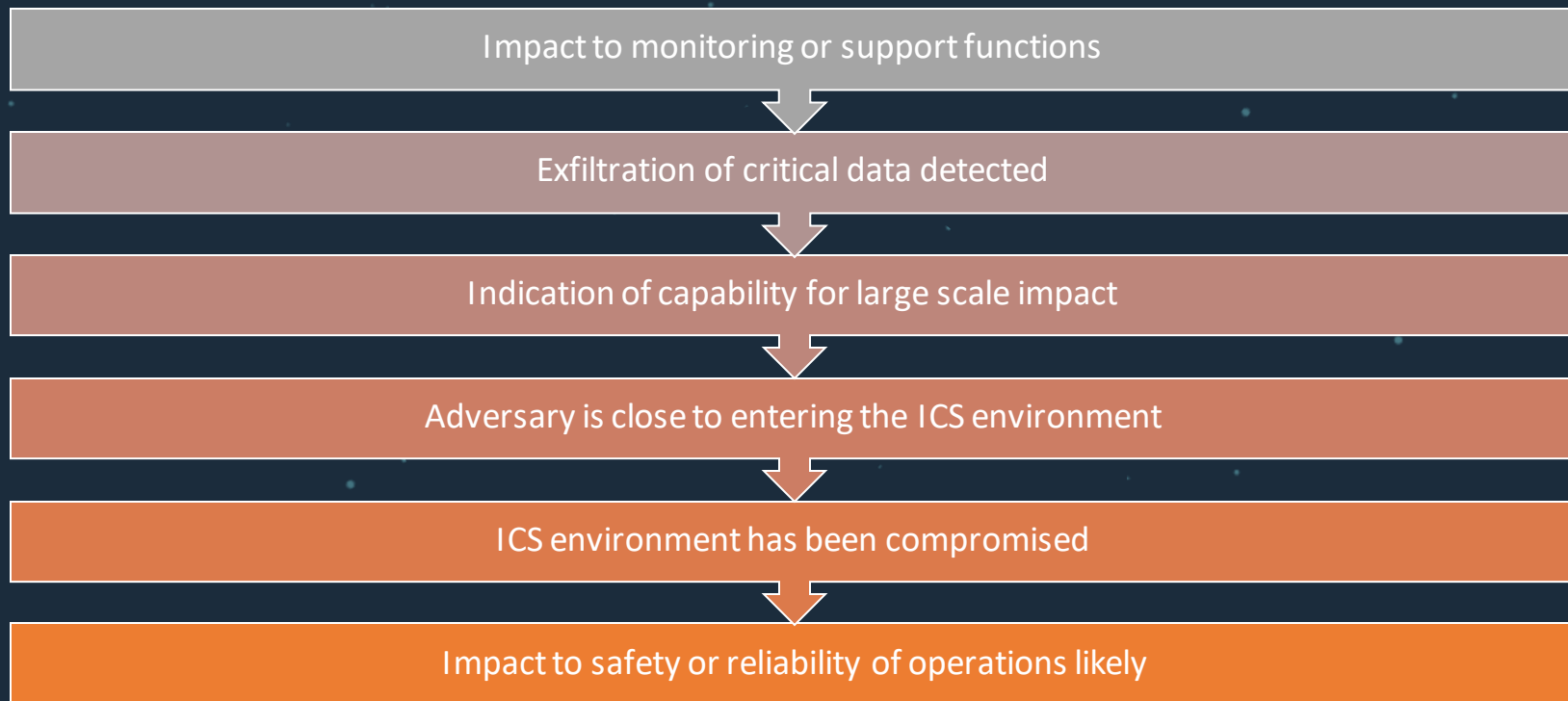
Where in the Kill Chain is the Adversary?

When an alert indicates a targeted intrusion, analysts need to determine how far along the adversary has come in reaching their objective.

The further along the Kill Chain, the swifter and more decisive the defender's response needs to be.



Escalation Factors



Define Thresholds for (Un-)acceptable Risk

The clearer the guidelines are for an Incident Commander to take decisions concerning the throttling or shutdown of operations, the faster these decisions can be made, and damage avoided.

These are *business decisions* and must be supported by the business stakeholders.



Getting to Root Cause



Regulations often include 'Lessons Learned' as part of the incident closeout. Root Cause Analysis (RCA) is key to identifying how the adversary compromised the environment, but not explicitly mentioned as a requirement. Without RCA though, an environment is prone to falling victim to the same attack again.

On the downside, RCA can require extensive resources and depending on visibility of the environment and forensic data available is not always possible to successfully complete.

RCA Considerations



01

Prioritize

It is important to first focus on scoping the incident and containing the compromise. If possible, dedicate one or two analysts to work on RCA. Especially data acquisition should be done quickly to retain as much as possible. As always, this needs to be synced with OT to be performed in a safe manner.



02

Prepare

Spending time during IR preparation on forensic data acquisition techniques and procedures helps scoping and RCA efforts. Assigning dedicated roles to different analysts will also make the acquisition and analysis run more effectively and timely.



03

Improve

Especially if an organization does not have effective monitoring of their ICS environment, the result of RCA will be “we don’t know”. Ensure that the reasons for not knowing get communicated clearly and addressed by stakeholders to enable improvement.

Engaging an IR Team



In ICS Incident Response, the stakes are much higher than in IT IR. This necessitates more caution in selecting the right model for incident response services, but also ensuring that there is effective collaboration between all parties involved (e.g. responders, internal staff, vendors, etc.).

IR Team Considerations

Outsourced vs in-house

- Depends mostly on MTTR requirements
- At minimum you should provide internal staff capable of leading external teams
- If you consider external partners, outsourcing IR is more sensible than Network Security Monitoring

Team size

- Consider that for 3-4 onsite responders you'll need ~10 staff
- Even in internal IR teams, not all functions need to be staffed internally
- If you decide to have a non-permanent internal IR team, consider how to maintain proficiency of IR skills

Experience

- Verify that your ICS isn't your IR provider's first ICS
- Since "ICS" isn't really a thing, ensure that your IR provider has experience with *your industry vertical*
- A good IR partner provides experienced incident responders. A *great* partner will coach you along the path of maturing your ICS cybersecurity organization

Preparation and Training

- ICS IR requires multi-team collaboration. Successful collaboration requires planning and exercise.
- Regular tabletop exercises with all parties involved in ICS IR are highly recommended

Thank you

Get our new ICS IR Whitepaper:

<https://www.dragos.com/resource/preparing-for-incident-handling-and-response-in-ics/>

Feedback?

Twitter: @kaithomsen

Email: kthomsen@dragos.com

