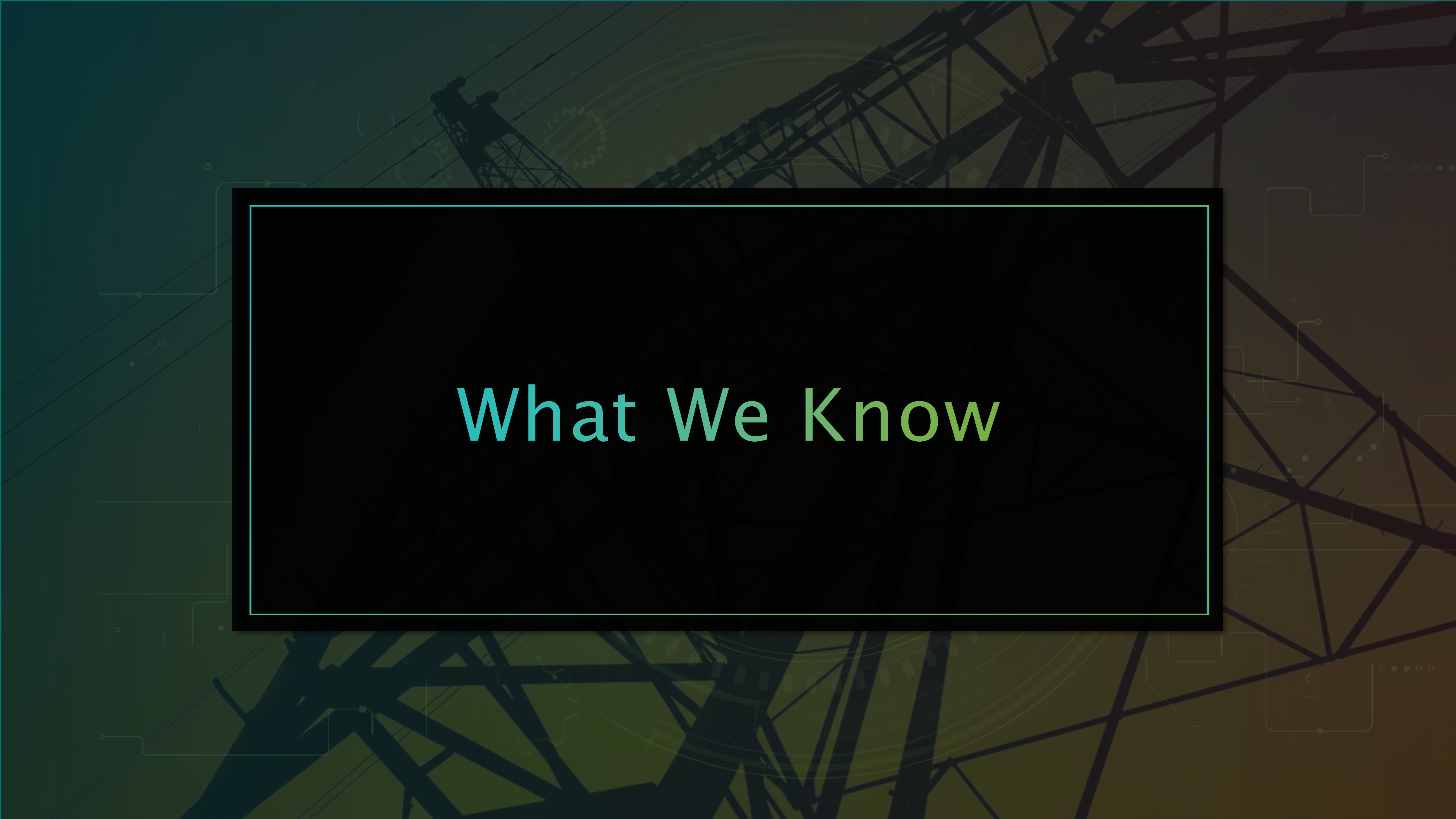
Do or Do Not

Fundamental First Steps in Industrial Rapid Response

Seth Enoka
Nate Pelz

About Us

- Seth:
  - Principal Responder
  - Dragos: ±3 years
  - Before: Middle East, Cisco, Clayton Utz, Klein & Co.
- Nate:
  - Senior Responder
  - Dragos: ±2 years
  - Before: PSIRT, Pres. Transition Team, Python Developer



What We Know

Safety and Haz Ops

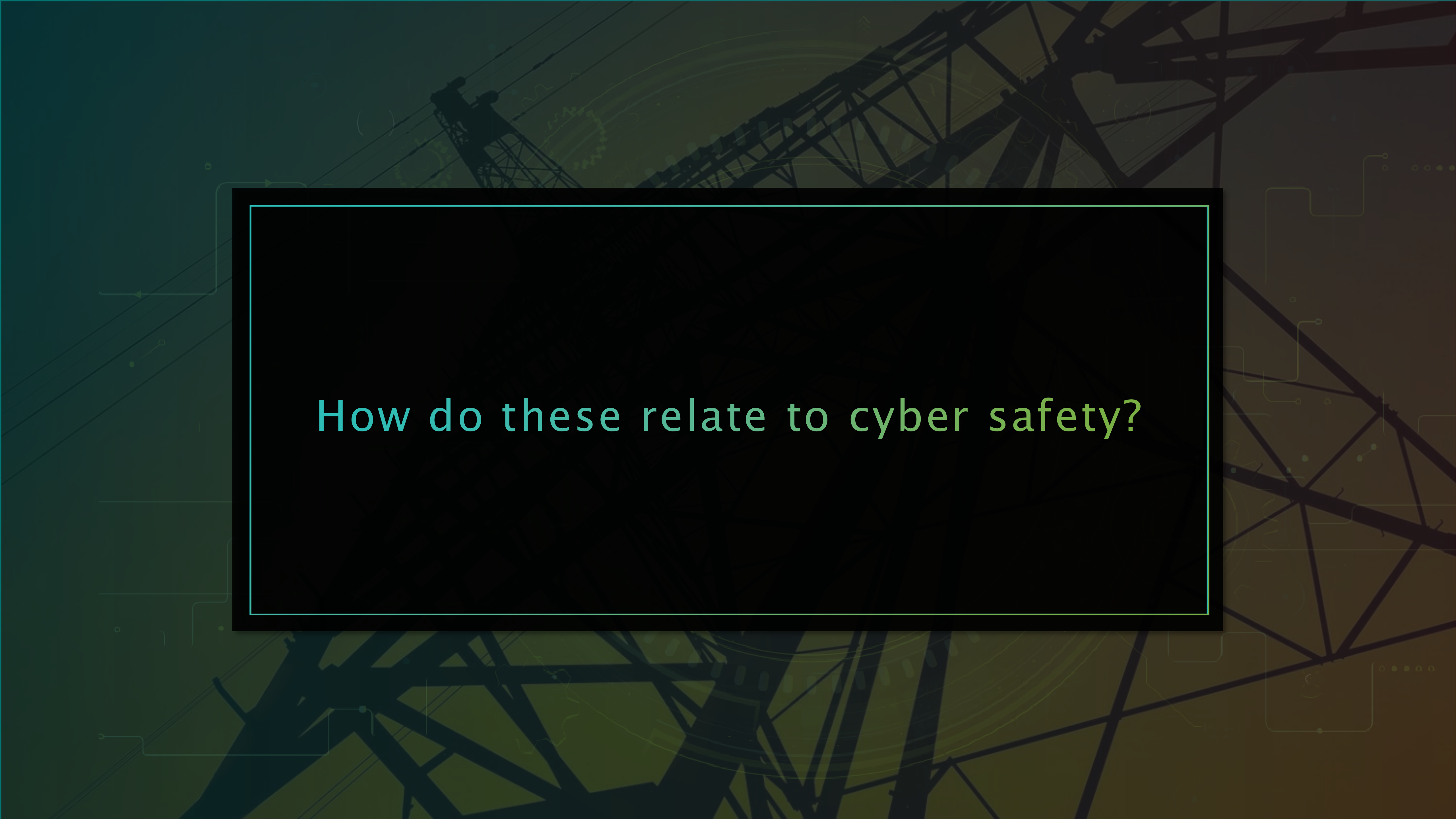
Physical Procedures

- Most are familiar with Job Hazard Analysis (JHA), a.k.a. ‘Take Five’
- Site personnel are aware of Immediate Emergency Actions
  - Safety: humans, facility, process integrity
  - Alert others in the immediate area
  - Communicate with emergency authorities
  - Provide details: name/location, nature of event, assistance required
  - Muster at designated location if unsafe
- ‘Site champions’ are currently less common
  - Similar to medical officer, fire warden, etc.

Our Take 5

Cyber Procedures

- Our recommended Cyber Take 5 and roles:
  1. Keep Calm
  2. Assemble Your Team of Experts
  3. Activate Third Parties Early
  4. Spin up Out-of-Band Communications
  5. Collect Evidence & Scope the Incident



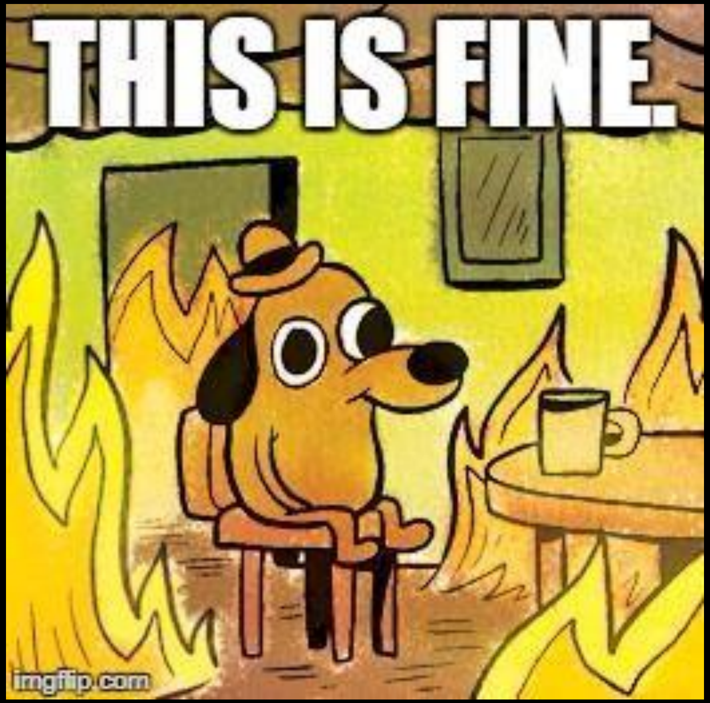
How do these relate to cyber safety?

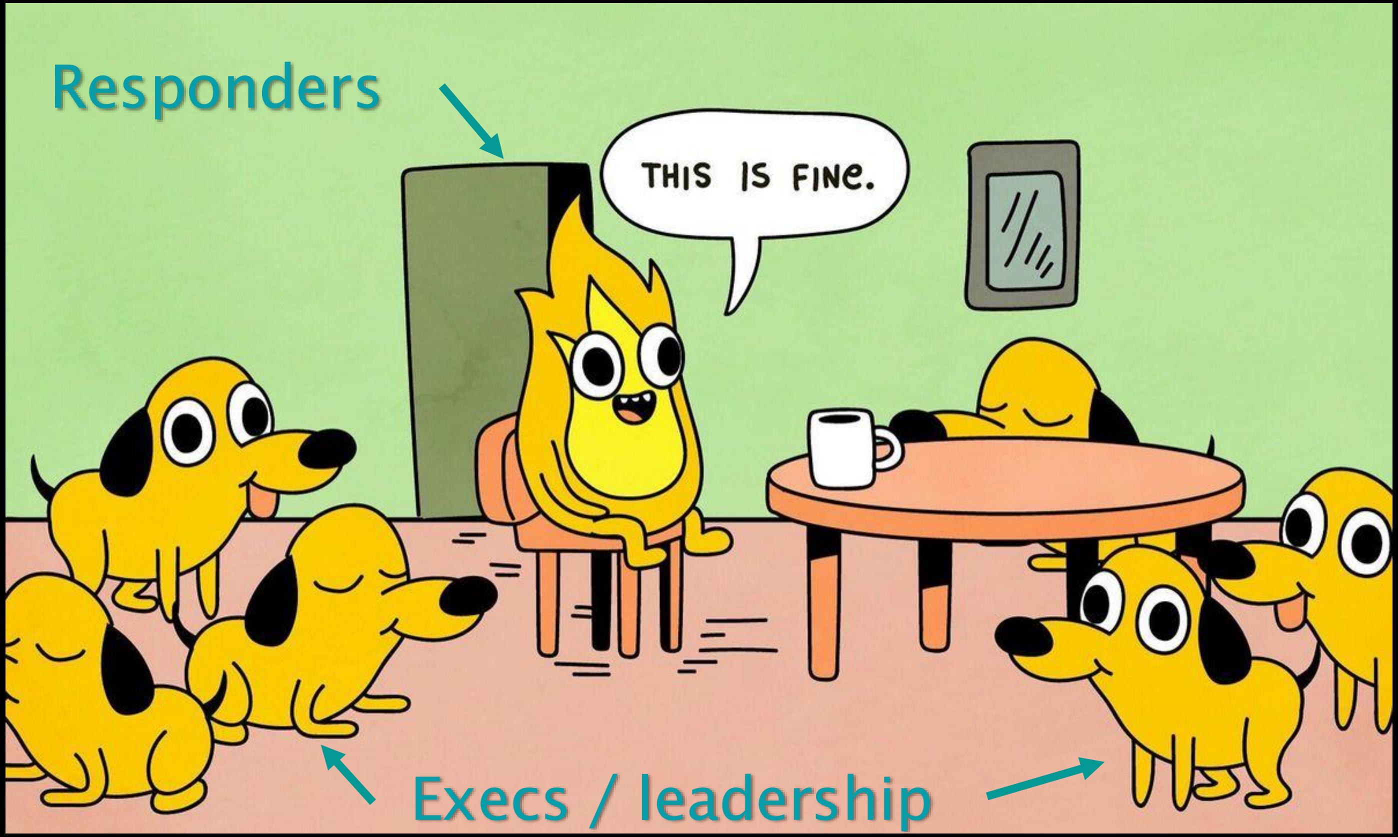
STEP #1

KEEP CALM

First: Keep Calm!

- DO: Stay calm (and keep everyone else calm)
- DO NOT: Match others' energy





- If- Rudyard Kipling:

If you can keep your head when all about you
Are losing theirs and blaming it on you,
If you can trust yourself when all men doubt you,
But make allowance for their doubting too;
If you can wait and not be tired by waiting,
Or being lied about, don't deal in lies,
Or being hated, don't give way to hating,
And yet don't look too good, nor talk too wise…"
You'll be an incident responder, my son!

STEP #2

ASSEMBLE YOUR TEAM

AKA…

- IRT (Incident Response Team)
- IMT (Incident Management Team)
- SIMT (Security Incident Management Team)
- CERT (Computer Emergency Response Team)
- CSIRT (Cyber Security Incident Readiness Team)
- *…whatever you call it…*

Tips for IRT Structure

- Employ an *expandable command structure*
  - Use FEMA’s Incident Command System for inspiration

- All roles should report to a single Incident Commander

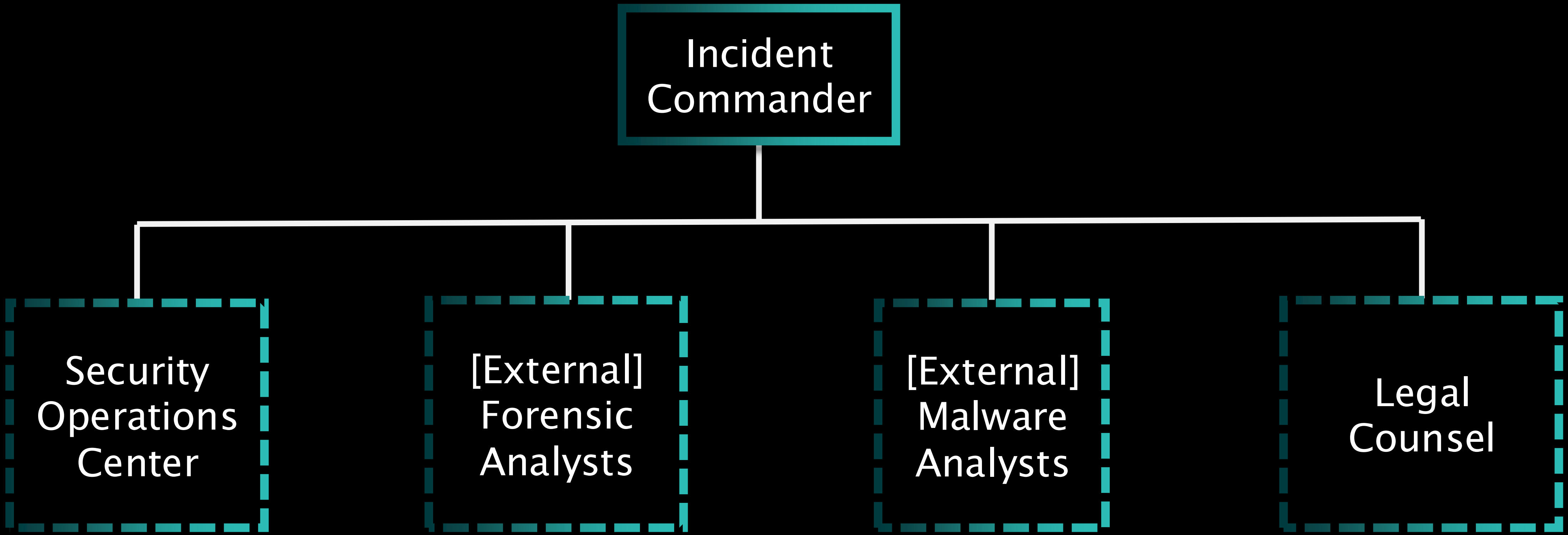
- Ensure OT specialists are driving response efforts

Incident Commander
mation
Safety Officer
aison Officer
erations Chief
Planning Section Chief
Logistics Section Chi

Severity 4: Employee reports possible phishing email

Incident Commander

Severity 3: Malware confirmed on end user device (IT)



Incident Commander

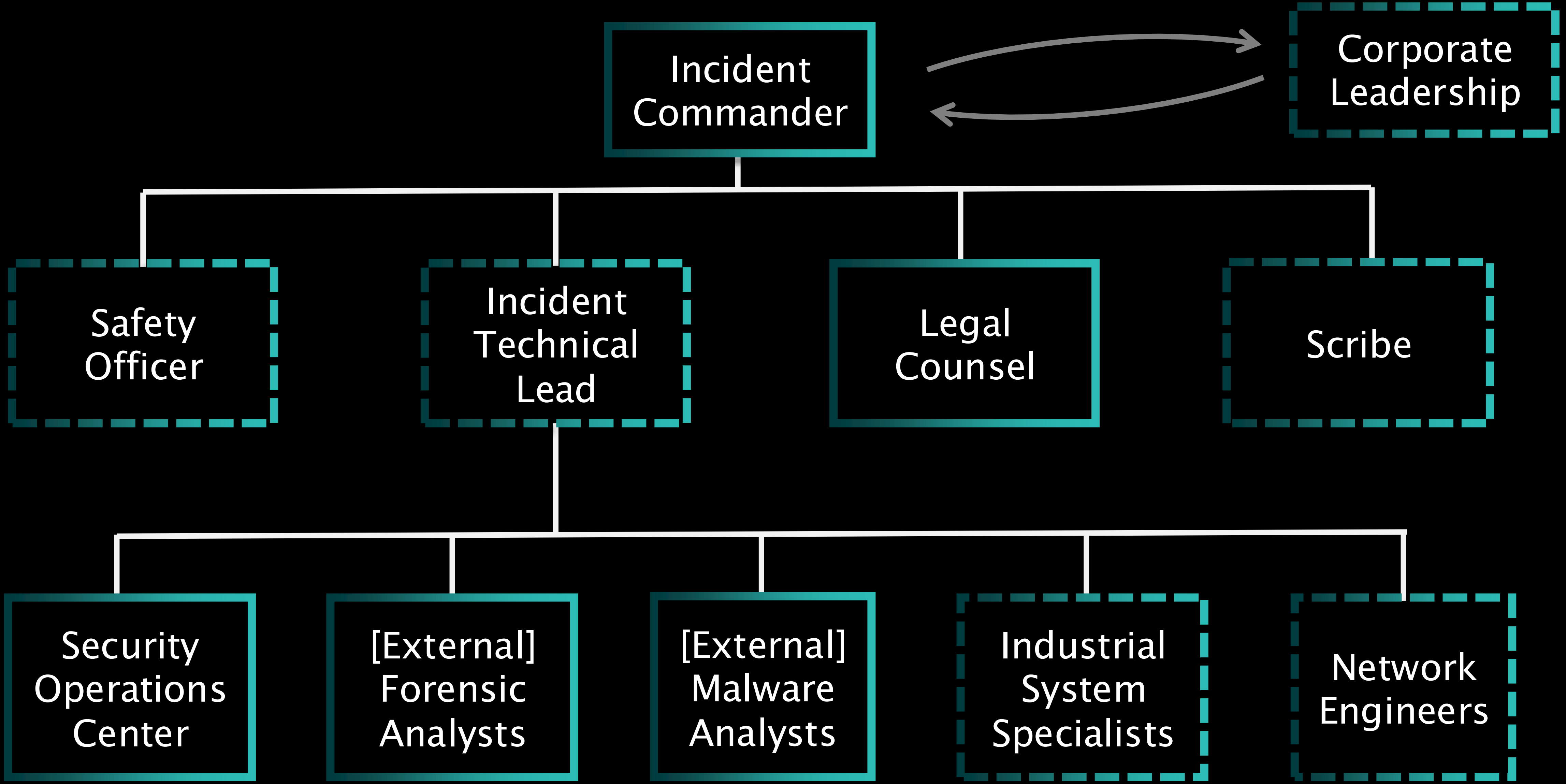
Security Operations Center

[External] Forensic Analysts

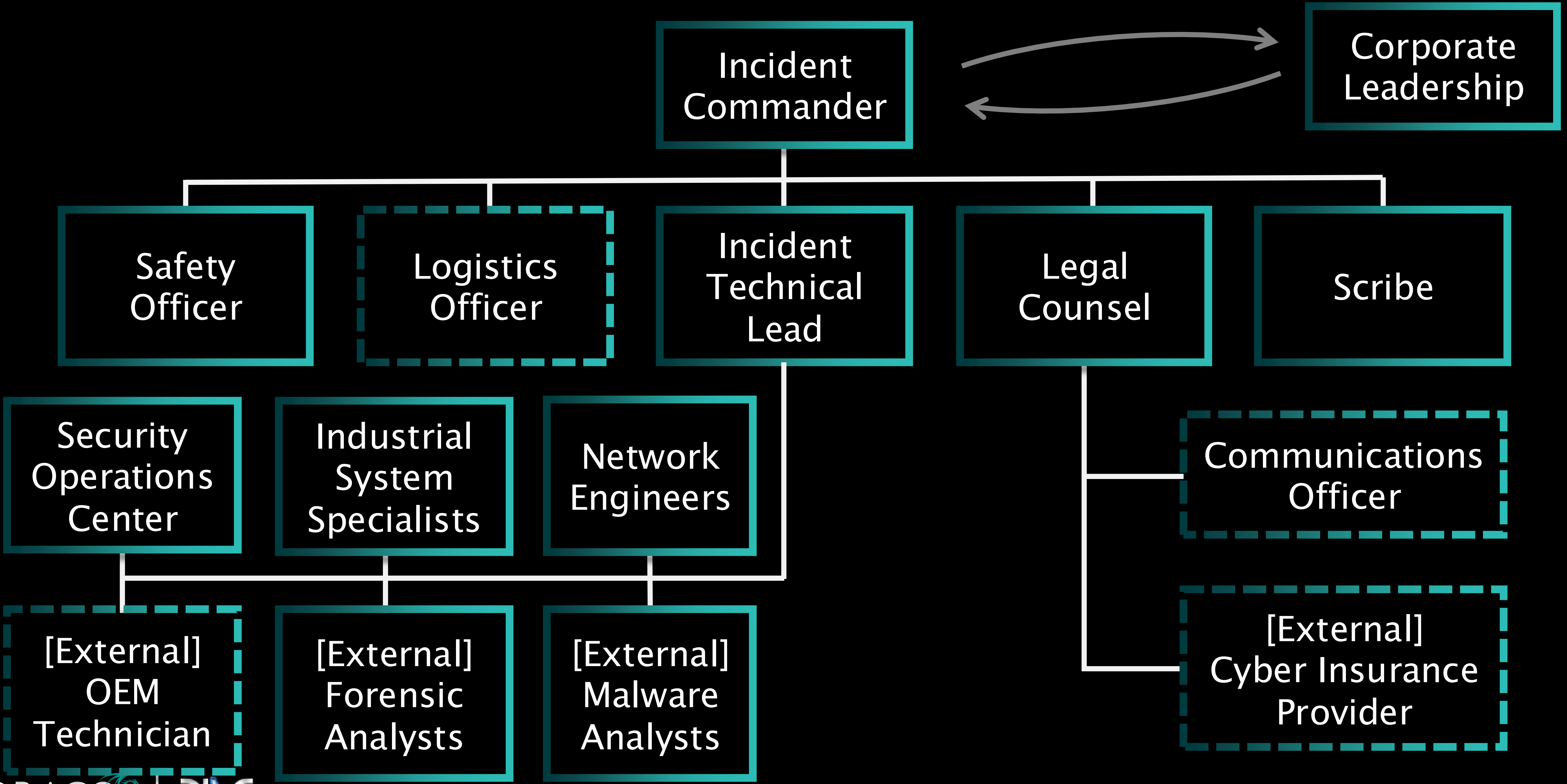
[External] Malware Analysts

Legal Counsel

Severity 2: SOC observes adversary has spread to control center



Severity 1: Ransomware locks hosts, causing production downtime


Incident Commander
Corporate Leadership
Safety Officer
Logistics Officer
Incident Technical Lead
Legal Counsel
Scribe
Security Operations Center
Industrial System Specialists
Network Engineers
Communications Officer
[External] OEM Technician
[External] Forensic Analysts
[External] Malware Analysts
[External] Cyber Insurance Provider

DRAGOS | DISC

HOW IT LIKES TO DO IR

WRONG WAY TO DO OT IR

You can’t perform OT IR without OT expertise:

1. Communicating how the process works, and what “normal” looks like

2. Determining safety & process impact of implementing potentially disruptive changes

3. Ensuring compliance with vendor support contracts

4. Performing collection on operating equipment

RIGHT WAY TO DO OT IR

Responders

OT Experts

STEP #3

ACTIVATE THIRD-PARTIES EARLY

Activate Third-Parties Early

- You have a lot of people available to help
  - DO: Engage support - Dragos and others, vendors, etc.
  - DO NOT: Feel like you need to suffer or get by alone

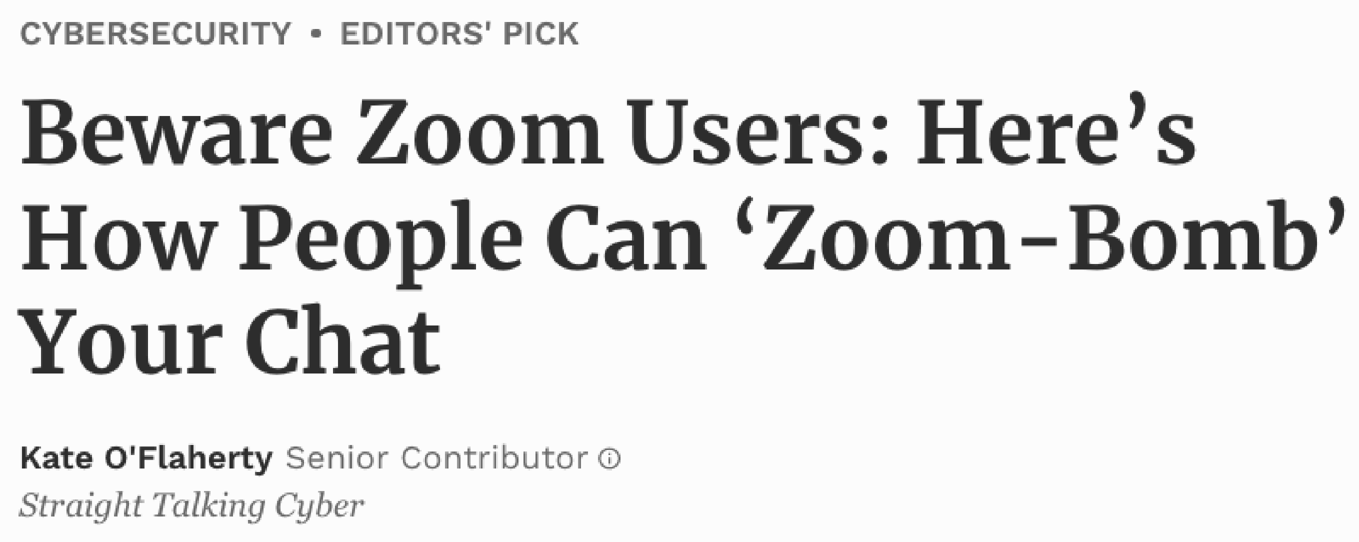
- Ideally:
  - Have relationships set up in advance
  - Work with Legal and operate under privilege
  - Have your admin sorted before incidents occur

STEP #4

SPIN UP OUT OF BAND COMMUNICATIONS

Spin Up Out of Band Communications

- Why OOB?

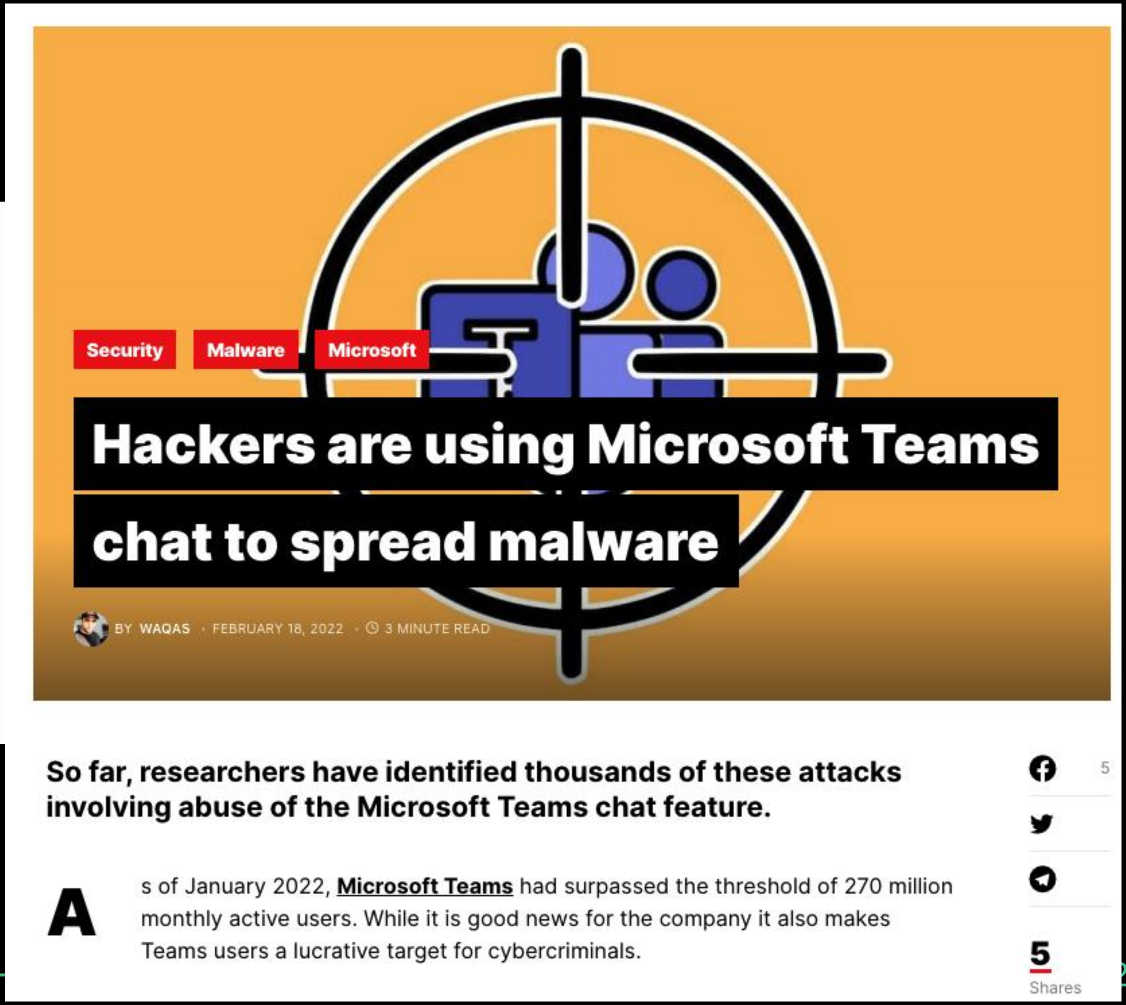


CYBERSECURITY • EDITORS' PICK

Beware Zoom Users: Here's How People Can 'Zoom-Bomb' Your Chat

Kate O'Flaherty Senior Contributor ⓘ

Straight Talking Cyber



Security Malware Microsoft

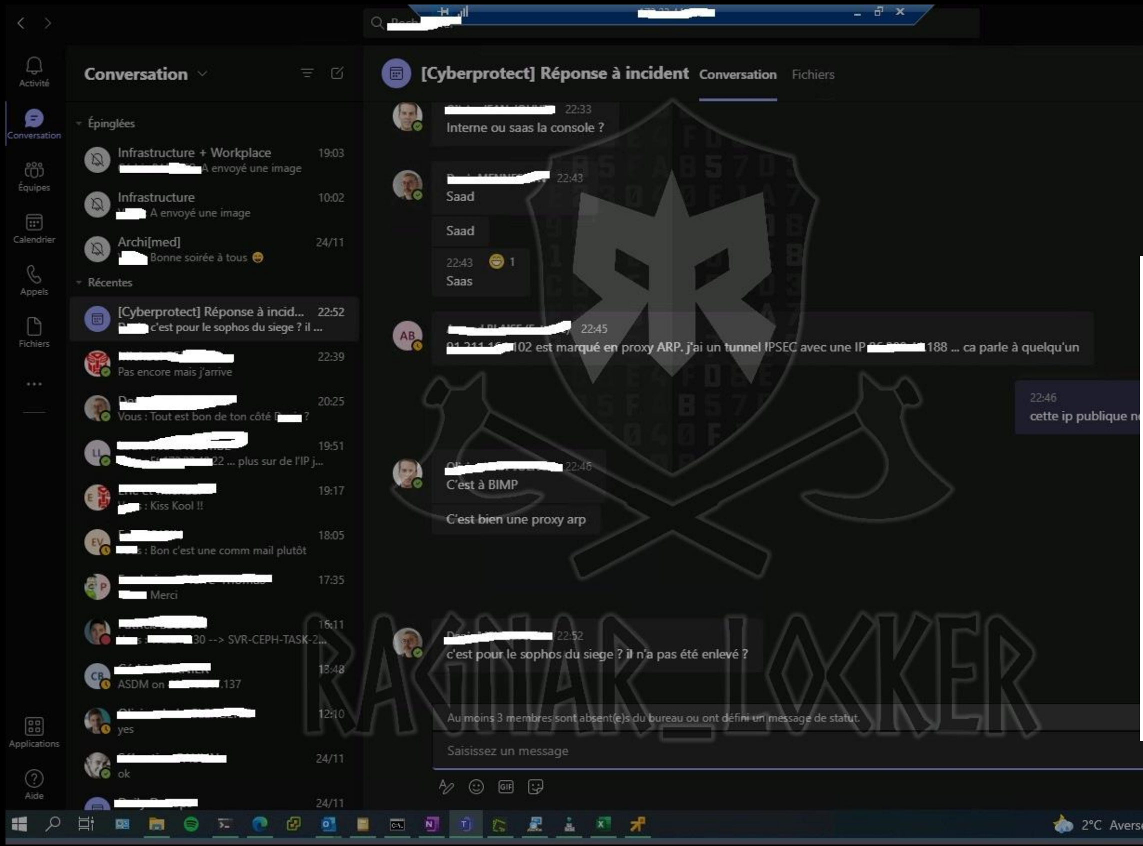
Hackers are using Microsoft Teams chat to spread malware

BY WAQAS · FEBRUARY 18, 2022 · 3 MINUTE READ

So far, researchers have identified thousands of these attacks involving abuse of the Microsoft Teams chat feature.

As of January 2022, **Microsoft Teams** had surpassed the threshold of 270 million monthly active users. While it is good news for the company it also makes Teams users a lucrative target for cybercriminals.

Spin Up Out of Band Communications



[Cyberprotect] Réponse à incident Conversation Fichiers

Épinglées

- Infrastructure + Workplace 19:03
  [redacted] A envoyé une image
- Infrastructure 10:02
  [redacted] A envoyé une image
- Archi[med] 24/11
  [redacted] Bonne soirée à tous 😄

Récentes

- [Cyberprotect] Réponse à incid... 22:52
  [redacted] c'est pour le sophos du siege ? il ...
- [redacted] 22:39
  Pas encore mais j'arrive
- [redacted] 20:25
  Vous : Tout est bon de ton côté [redacted] ?
- [redacted] 19:51
  [redacted] 22 ... plus sur de l'IP j...
- [redacted] 19:17
  [redacted] : Kiss Kool !!
- [redacted] 18:05
  [redacted] : Bon c'est une comm mail plutôt
- [redacted] 17:35
  [redacted] Merci
- [redacted] 16:11
  [redacted] 30 --> SVR-CEPH-TASK-2...
- [redacted] 13:48
  ASDM on [redacted].137
- [redacted] 12:10
  yes
- [redacted] 24/11
  ok
- [redacted] 24/11

[redacted] 22:33
Interne ou saas la console ?

[redacted] 22:43
Saad

Saad

22:43 😄 1
Saas

[redacted] 22:45
[redacted]102 est marqué en proxy ARP. j'ai un tunnel IPSEC avec une IP [redacted]188 ... ca parle à quelqu'un

22:46
cette ip publique n

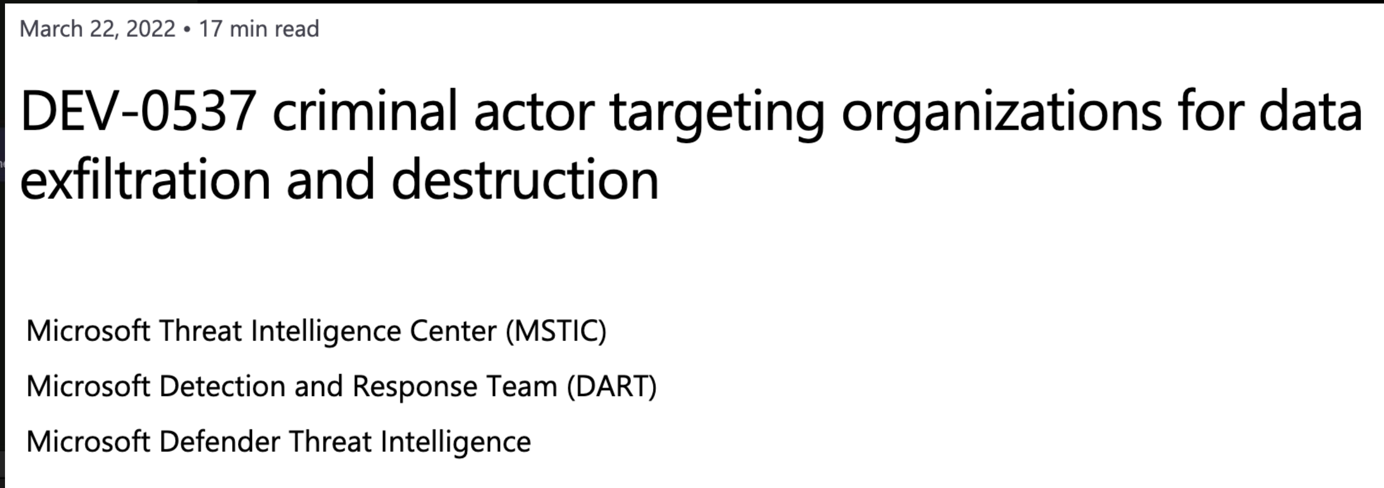
[redacted] 22:46
C'est à BIMP

C'est bien une proxy arp

[redacted] 22:52
c'est pour le sophos du siege ? il n'a pas été enlevé ?

Au moins 3 membres sont absent(e)s du bureau ou ont défini un message de statut.

Saisissez un message



March 22, 2022 • 17 min read

DEV-0537 criminal actor targeting organizations for data exfiltration and destruction

Microsoft Threat Intelligence Center (MSTIC)

Microsoft Detection and Response Team (DART)

Microsoft Defender Threat Intelligence

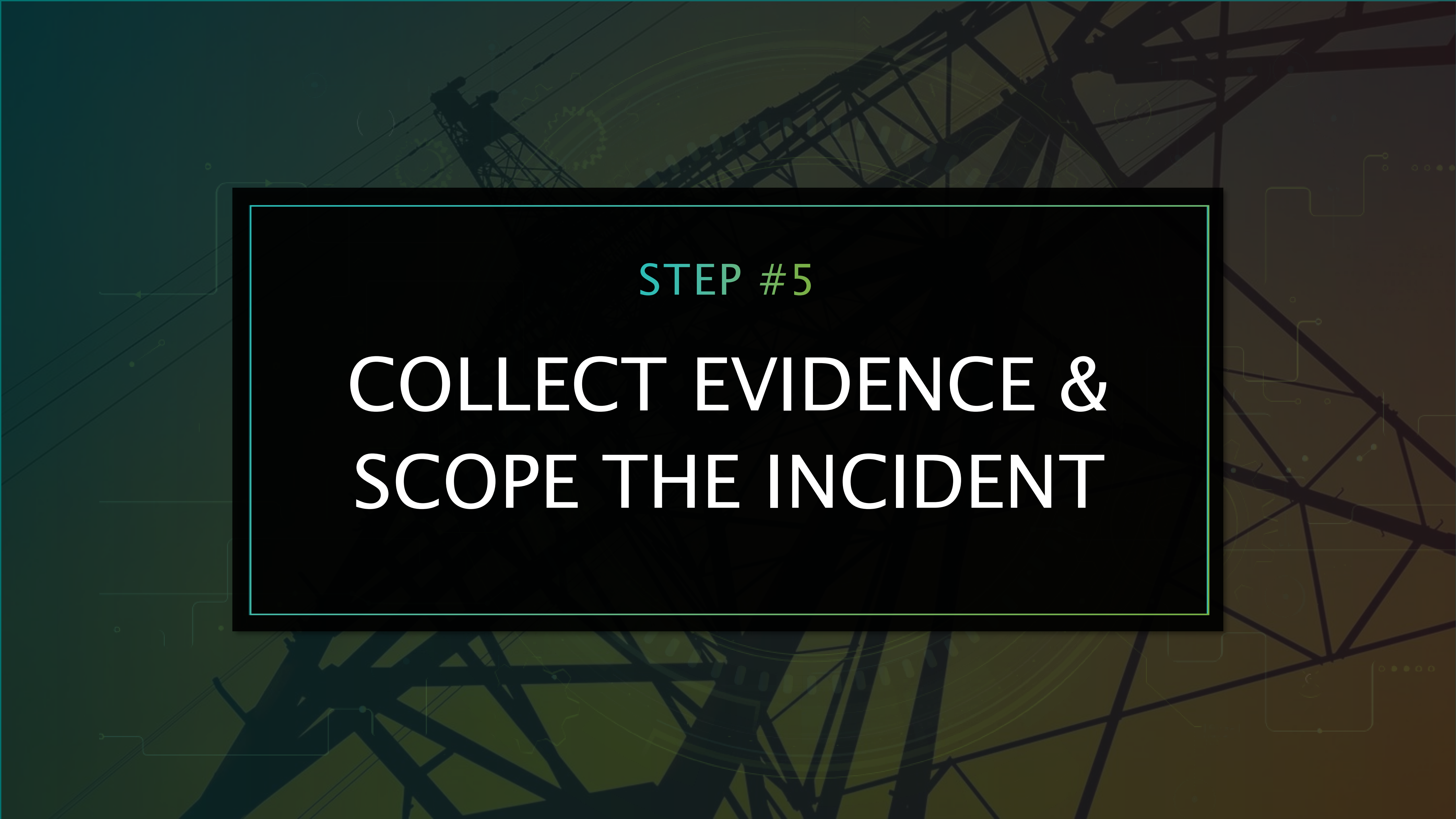
Spin Up Out of Band Communications

- Too often, organisations don’t use OOB comms
  - Not a consideration during IR planning
  - ‘Too busy’ responding to the incident

- When should you use OOB comms?
  - Once an event is escalated to an incident
  - Use your IRP documentation as a guide

Spin Up Out of Band Communications

- What comms are available?
  - 4/5G?
  - CB? Two-way radio?
  - Satellite?
  - Smoke signals?
- Ideally:
  - End-to-end encrypted: in transit and at rest
  - Not on corporate devices!
  - Consider multiple forms: SMS, email, file transfer, etc.

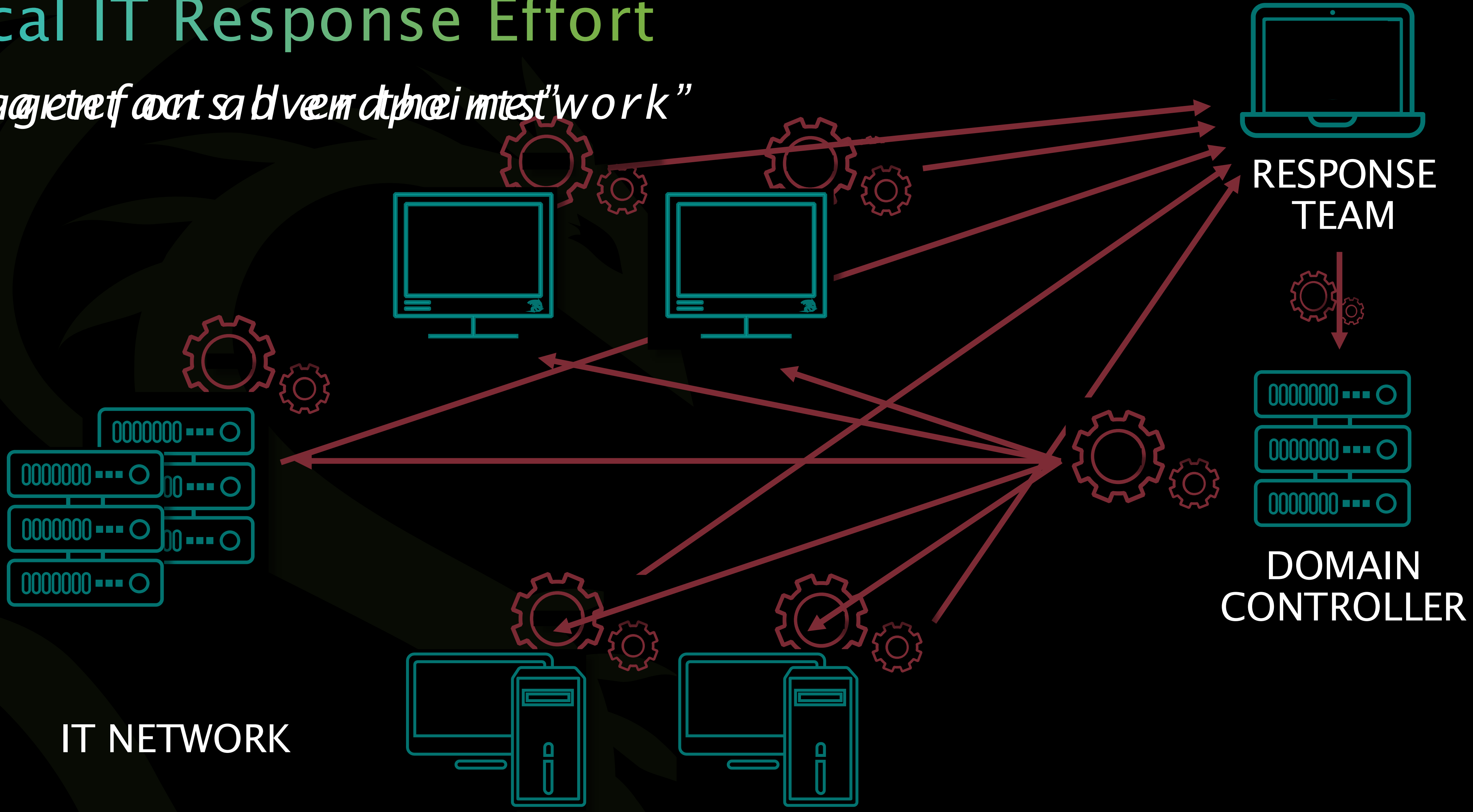


STEP #5

COLLECT EVIDENCE & SCOPE THE INCIDENT

Typical IT Response Effort

“Bemdaagetefoatsabvendpoeimtst’work”



Difficulties with running an agent on all endpoints:

- Incompatible endpoints running proprietary OS
- Incompatible endpoints running legacy OS
- OEM support contracts may be voided by installing software
- Deploying software via network may be difficult or infeasible…

Difficulties with sending artefacts over the network:

- OT networks have limited connectivity to WAN or internet *(which is good!)*

- Real-time production traffic is extremely sensitive to latency

- Remote networks may have limited bandwidth

Collection is *harder* in OT

Collecting from OT Networks

FOCUS

on the most valuable hosts and datasets

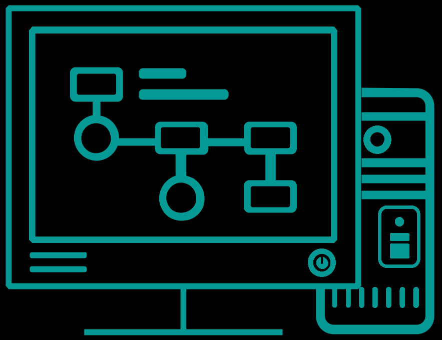
- Strategic hosts:
  - Devices involved in an incident
  - Network chokepoints
  - Crown jewels

- Strategic datasets:
  - Network PCAP
  - Firewall logs
  - EWS access logs
  - PLC status logs
  - Project file comparison
  - etc.

Guiding Questions

“The adversary has compromised my Engineering Workstation (EWS)”

- Did the adversary open engineering software?
- Did the EWS communicate with other assets within the relevant time window?
- What projects are available on the EWS? When were they last updated? By whom?
- Have projects running on controllers been altered?
- Have projects running on HMIs been altered?
- Are the engineering software binaries legitimate?



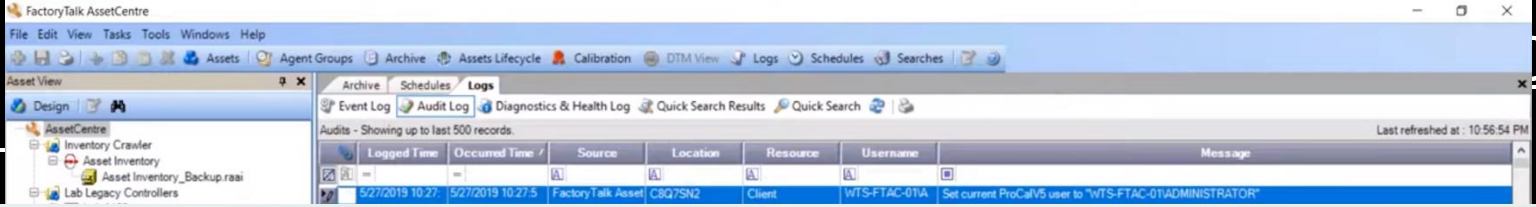
Guiding Questions

“The adversary has compromised my HMI”

- When was the HMI project last updated? By whom?
- Are there concerns with the integrity of the HMI project logic?
- Did the HMI communicate with other assets within the relevant time window?
- Have any tags or set points changed within the relevant time window?
- What operator actions have been taken on the HMI?
- Are the HMI binaries legitimate?

Accessing Strategic Datasets: Rockwell Automation

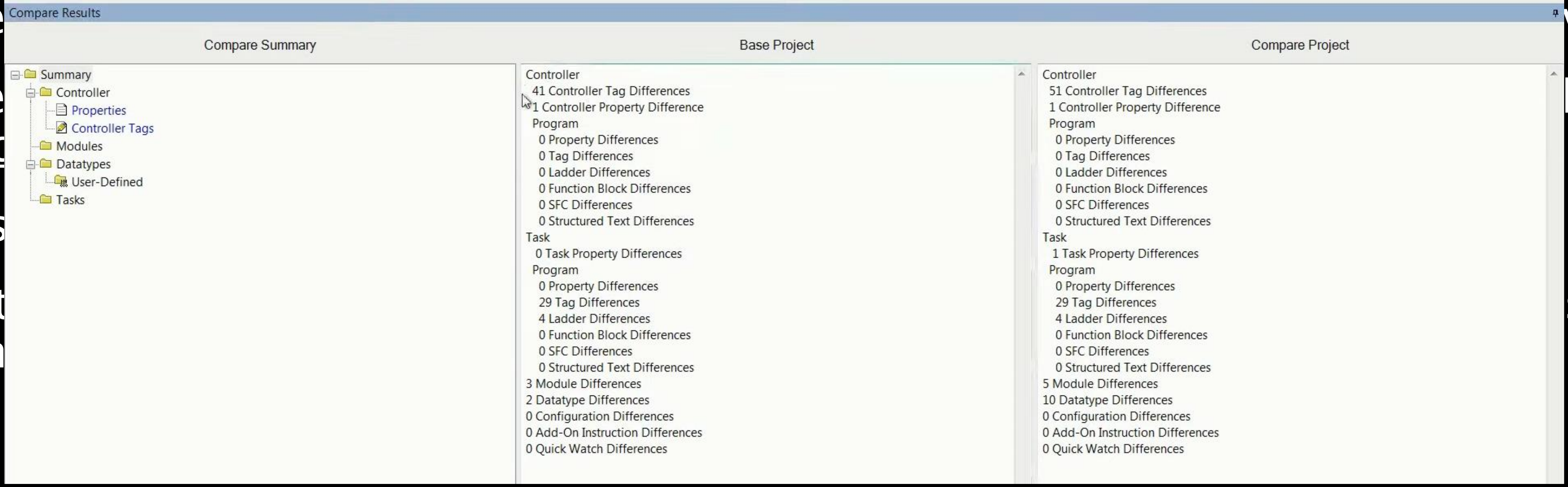
- Look for observed project changes within the FactoryTalk AssetCentre Audit Log
- Compare o) Logix Designer C
- Ide vice
- Ide he Fac
- Dis
- Ret s to a n


FactoryTalk AssetCentre

Audits - Showing up to last 500 records.

Last refreshed at : 10:56:54 PM

Logged Time	Occurred Time	Source	Location	Resource	Username	Message
5/27/2019 10:27:	5/27/2019 10:27:5	FactoryTalk Asset	C8Q7SN2	Client	WTS-FTAC-01\A	Set current ProCalV5 user to "WTS-FTAC-01\ADMINISTRATOR"


Compare Results

Compare Summary

- Summary
  - Controller
    - Properties
    - Controller Tags
  - Modules
  - Datatypes
    - User-Defined
  - Tasks

Base Project	Compare Project
Controller	Controller
41 Controller Tag Differences	51 Controller Tag Differences
1 Controller Property Difference	1 Controller Property Difference
Program	Program
0 Property Differences	0 Property Differences
0 Tag Differences	0 Tag Differences
0 Ladder Differences	0 Ladder Differences
0 Function Block Differences	0 Function Block Differences
0 SFC Differences	0 SFC Differences
0 Structured Text Differences	0 Structured Text Differences
Task	Task
0 Task Property Differences	1 Task Property Differences
Program	Program
0 Property Differences	0 Property Differences
29 Tag Differences	29 Tag Differences
4 Ladder Differences	4 Ladder Differences
0 Function Block Differences	0 Function Block Differences
0 SFC Differences	0 SFC Differences
0 Structured Text Differences	0 Structured Text Differences
3 Module Differences	5 Module Differences
2 Datatype Differences	10 Datatype Differences
0 Configuration Differences	0 Configuration Differences
0 Add-On Instruction Differences	0 Add-On Instruction Differences
0 Quick Watch Differences	0 Quick Watch Differences

Collecting from OT Networks

FOCUS

on the most valuable systems and datasets

PRIORITISE

collection of volatile, time-sensitive or time-consuming datasets

- Collect volatile evidence first
- Use a Collection Management Framework (CMF) to identify data at risk of expiration, or which requires significant manual work to collect

Collecting from OT Networks

FOCUS

on the most valuable systems and datasets

PRIORITISE

collection of volatile, time-sensitive or time-consuming datasets

COLLECT

from individual systems via removable media

- Collection scripts can be executed directly without installation from USB thumb drives or even DVDs
- Data should be saved back onto the removable media

LEVEL 4

Corporate Network

LEVEL 3

Operations Systems

LEVEL 2

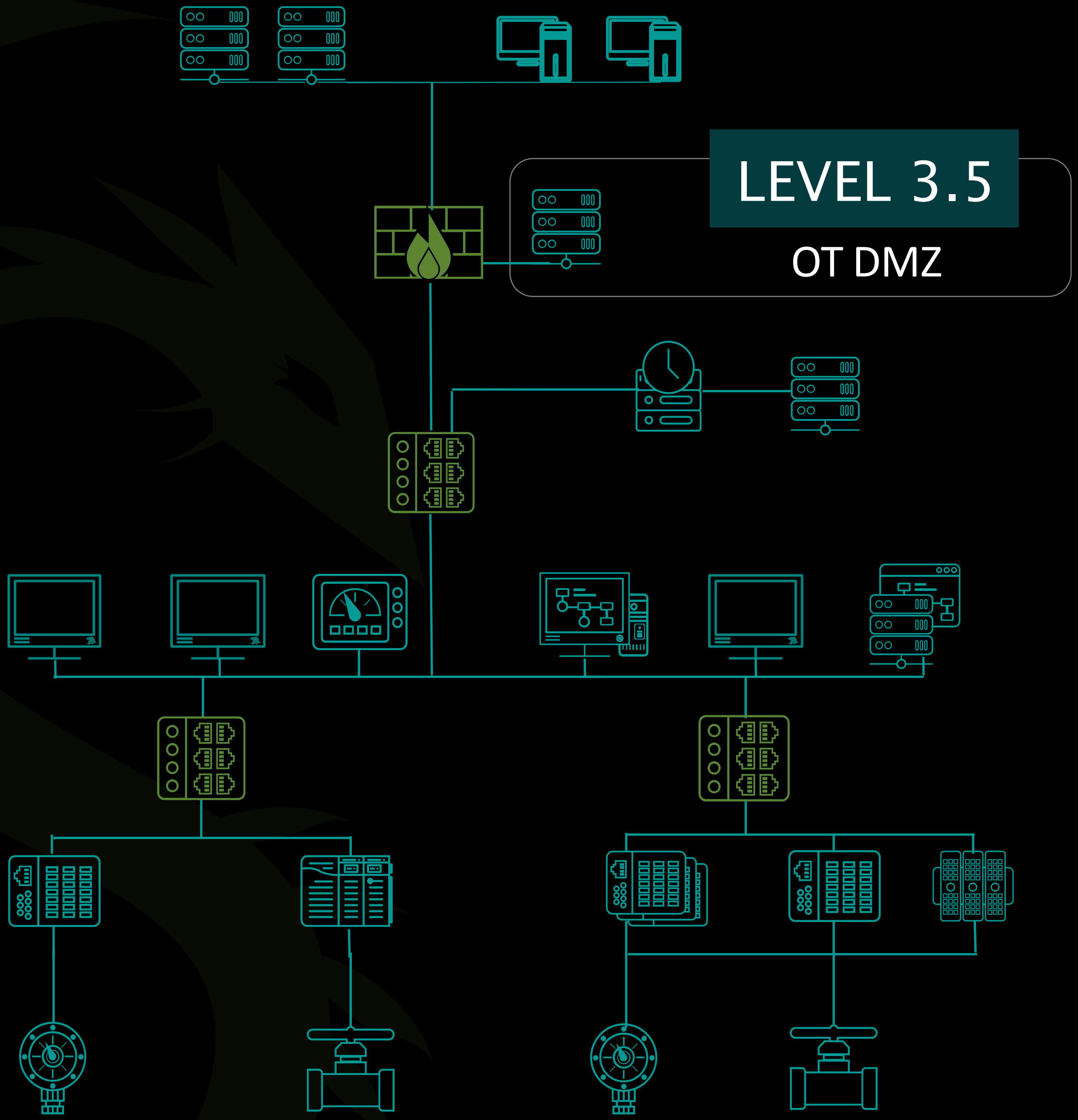
Supervisory Control

LEVEL 1

Basic Control

LEVEL 0

Physical Process



LEVEL 3.5

OT DMZ

LEVEL 4

Corporate Network

LEVEL 3

Operations Systems

LEVEL 2

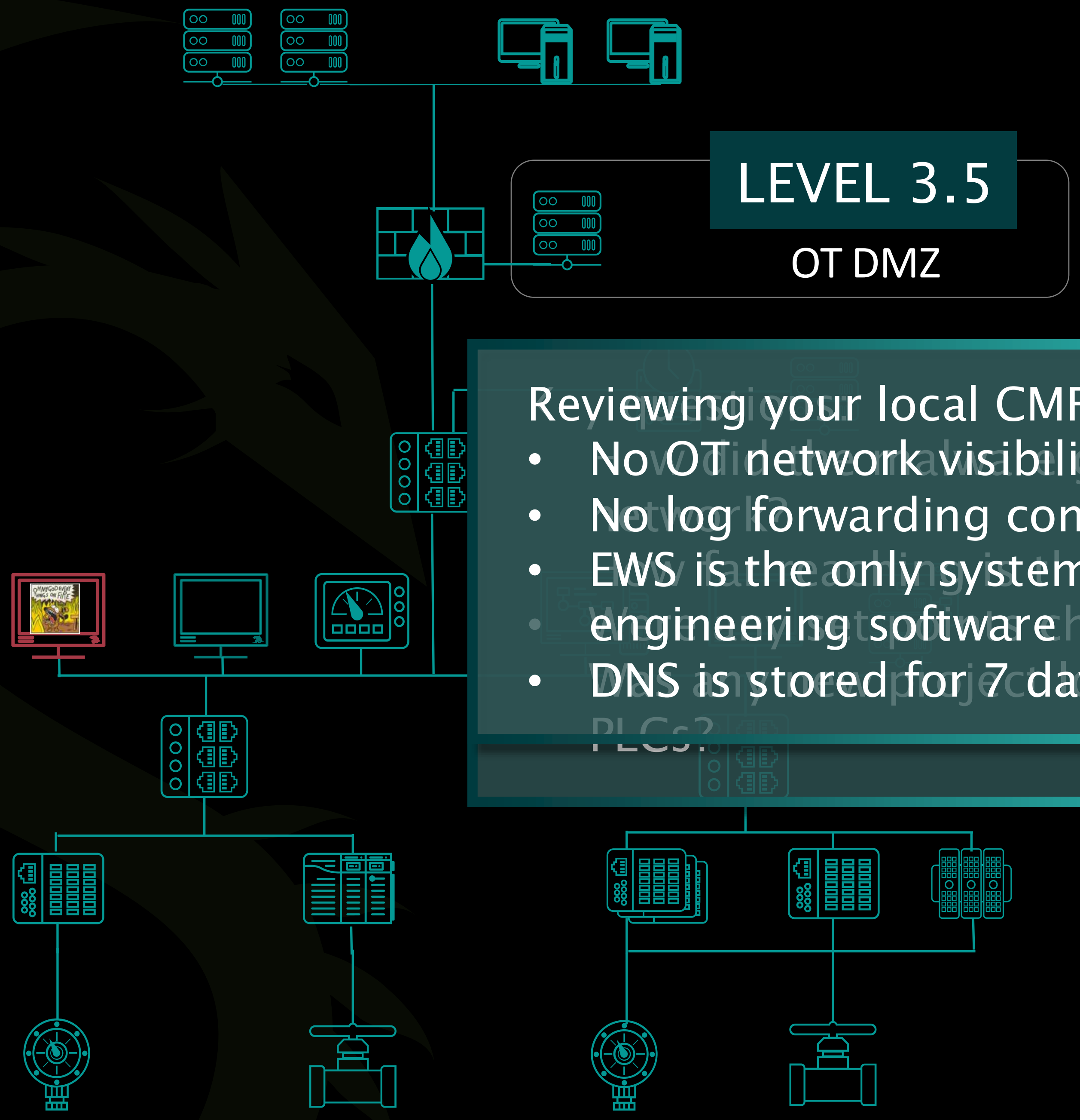
Supervisory Control

LEVEL 1

Basic Control

LEVEL 0

Physical Process



LEVEL 3.5

OT DMZ

Reviewing your local CMF:

- No OT network visibility
- No log forwarding configured
- EWS is the only system running engineering software
- DNS is stored for 7 days

LEVEL 4

Corporate Network

LEVEL 3

Operations Systems

LEVEL 2

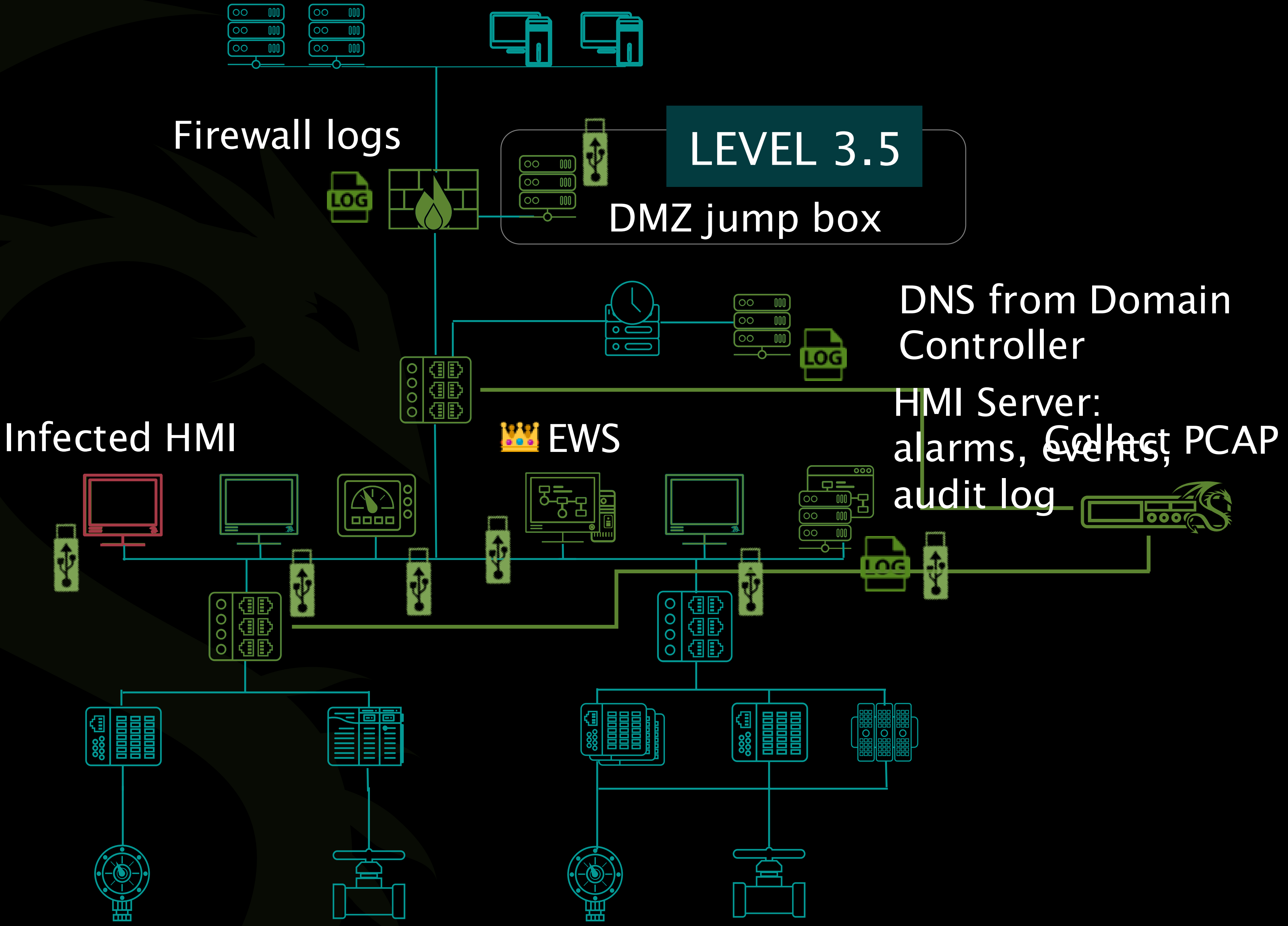
Supervisory Control

LEVEL 1

Basic Control

LEVEL 0

Physical Process



Firewall logs

DMZ jump box

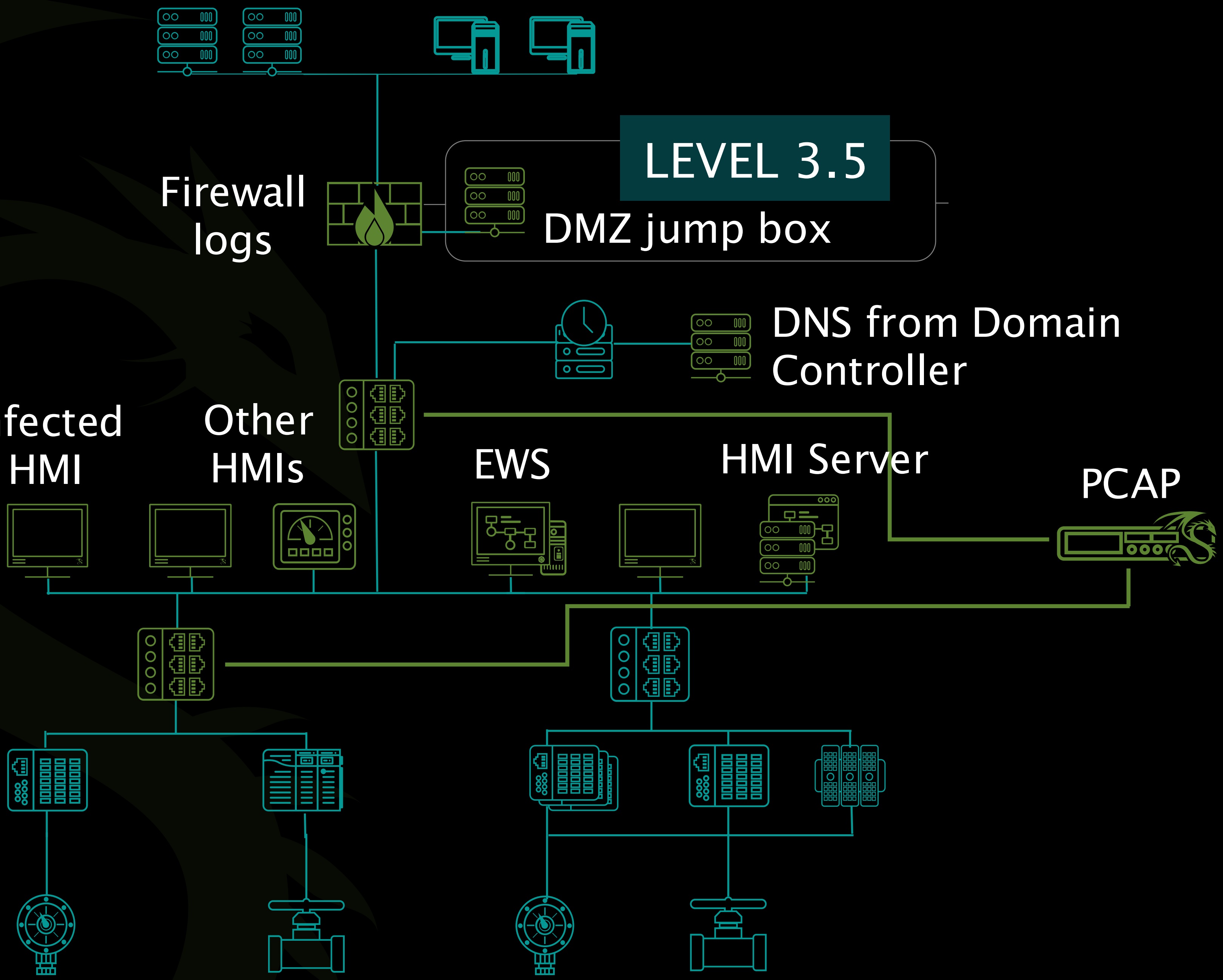
DNS from Domain Controller

HMI Server: alarms, events, audit log

Collect PCAP

Infected HMI

👑 EWS



LEVEL 4
Corporate Network
LEVEL 3
Operations Systems
LEVEL 2
Supervisory Control
LEVEL 1
Basic Control
LEVEL 0
Physical Process
Firewall logs
LEVEL 3.5
DMZ jump box
DNS from Domain Controller
Infected HMI
Other HMIs
EWS
HMI Server
PCAP

In Summary

The ‘Take 5’ of OT IR

1. Keep Calm
2. Assemble Your Team
3. Activate Third Parties Early
4. Spin Up Out-of-Band Comms
5. Collect Evidence & Scope

Thank You

Seth Enoka – senoka@dragos.com

Nate Pelz – npelz@dragos.com