

# RSA<sup>®</sup>Conference2019

San Francisco | March 4–8 | Moscone Center



**BETTER.**

SESSION ID: AIR-R11

## Incident Response beyond Enterprise IT

**Jason Escaravage**

Senior Vice President  
Booz Allen Hamilton

**Phil Hamill**

Principal  
Booz Allen Hamilton



#RSAC

# Introduction

## Agenda

- 1 **The IR Landscape is Changing**  
New challenges for today's IR capability
- 2 **Cloud IR Challenges**
  - Threats in the cloud
  - Differences with cloud IR
  - Jumpstart your Cloud IR Capability
- 3 **OT IR Challenges**
  - Threats to your OT environment
  - Differences with OT IR
  - OT IR Journey
  - Jumpstart your OT IR Capability
- 4 **Useful Reference Sources**

## By the end of this session, you will:

- ✓ Learn how threat actors have evolved their approach in targeting OT and Cloud
- ✓ Understand why IR looks different in these emerging domains
- ✓ Discover who the key “players” are in your organization to tackle IR in OT and Cloud
- ✓ Walk away with actionable steps to take when you get back to the office

# The World Looks Different Today

## Yesterday

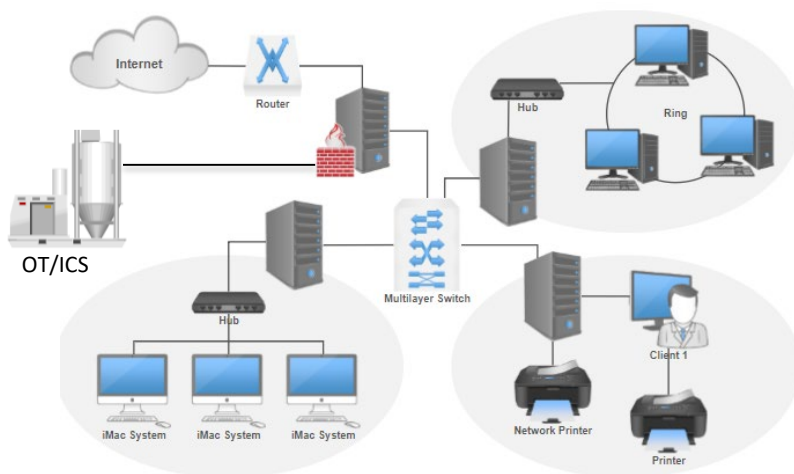
- **Scope** – Enterprise IT servers, workstations, and devices
- **Assets** – Mostly company owned and managed
- **Access** – IR staff had authority, access, expertise, and rights of way

## Today

- **Scope** – Now includes Enterprise, Cloud, OT, IoT, IIoT, Mobile...
- **Assets** – Assets not all owned/managed (ex. SaaS, Joint Ventures, BYOD Mobile)
- **Access** – New stakeholders and coordination across teams, geographies, and providers
- **Shifting Focus** – Adversaries are targeting weaknesses in emerging domains

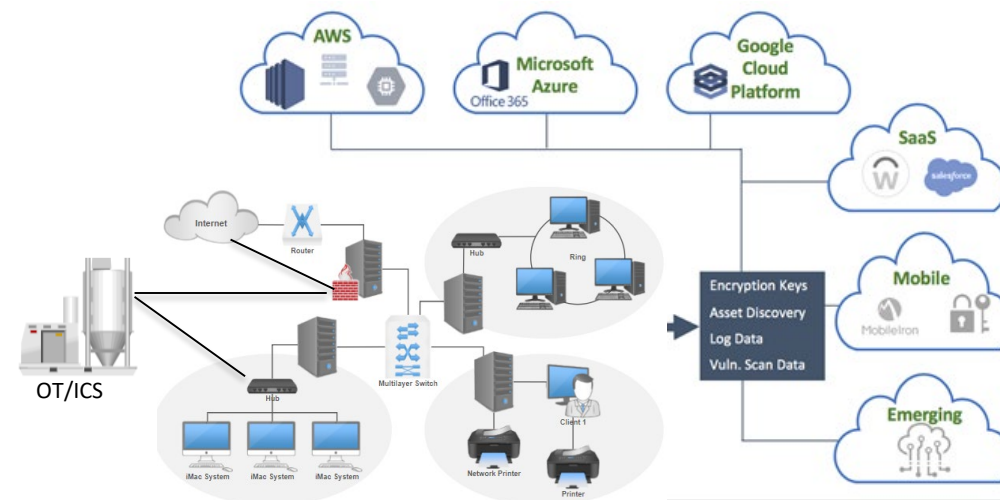
# Emerging Domains Are Shaping IR Strategy

## Yesterday



- Defense-in-depth strategy starting at a defined perimeter
- Slow-changing / static environment
- Logs feeding SIEM -> SOC -> IR
- EDR tools for live response
- Containment benefits from control / proximity / access
- OT “isolated” behind a firewall


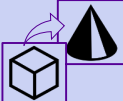



## Today



- Perimeter evaporated and cloud environment shifts rapidly
- Former on-prem services now in the cloud
- External logs may have reliability / availability issues
- EDR deployment complicated by volume and velocity
- Containment is hampered by volatility and lack of access
- OT / IT convergence and new connectivity requirements

# Emerging Domains Present Challenges for IR

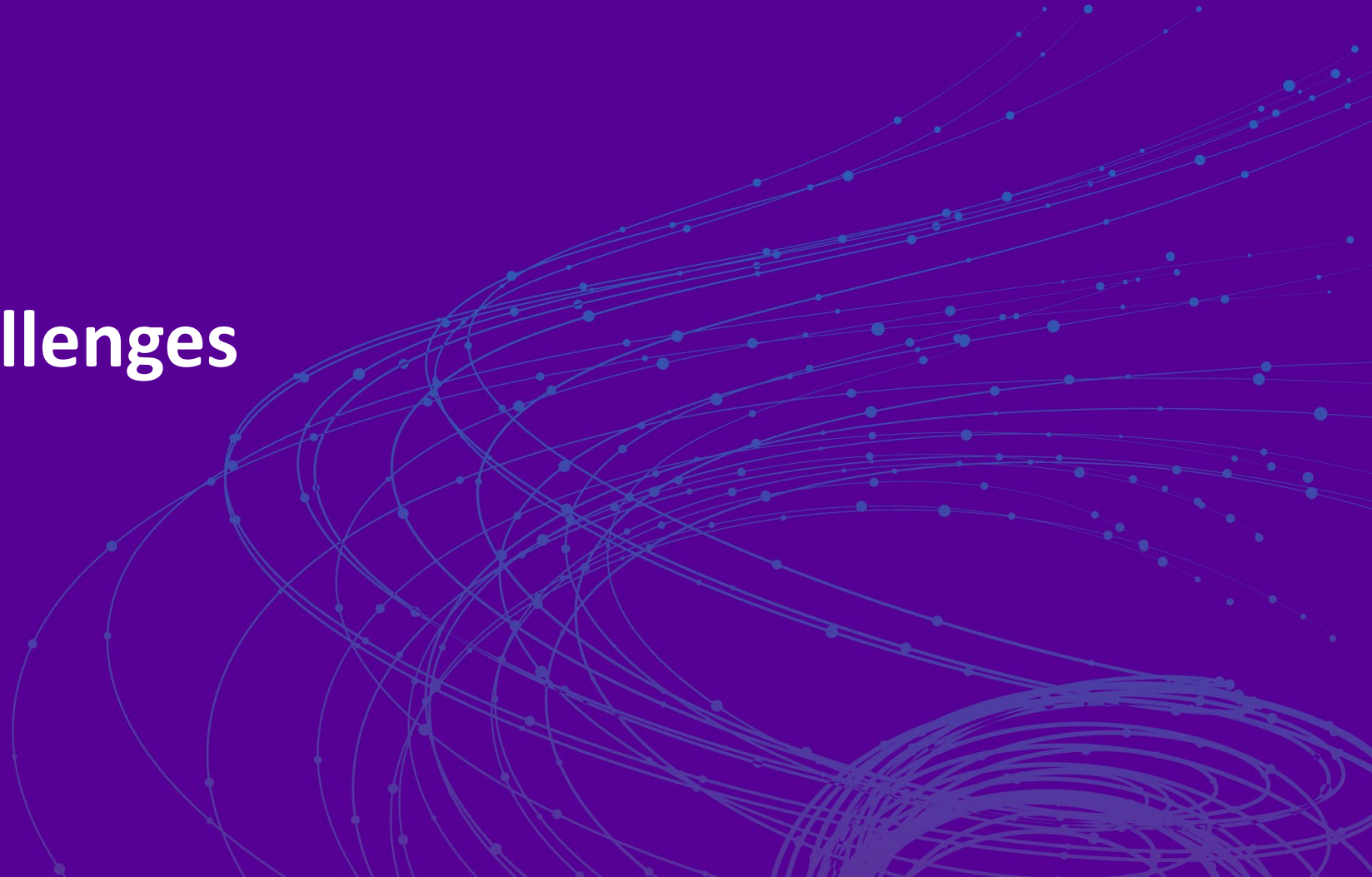
New domains introduce new efficiencies, and also added risks and challenges for IR

	<b>New stakeholders</b>	Must work with new internal stakeholders and external providers under a shared responsibility model
	<b>Connected but vulnerable OT Systems</b>	Increased connectivity presents new attack vectors
	<b>Lack of OT system expertise</b>	OT environments are often characterized by highly specialized systems and non-traditional IT components
	<b>Dynamic environments in cloud</b>	Speed and automation are critical, target state unknown, platforms and services may change quickly
	<b>Lack of cloud environment and tool expertise</b>	Cloud services are not one-dimensional – each model of cloud (IaaS, PaaS, SaaS) requires different approaches and tools



**RSA**Conference2019

## Cloud IR Challenges



# Threats in the Cloud

## New environments lead to new actors/threats

Commodity crime is leaning into cloud for resources/crypto-mining; APTs know critical data may be duplicated to poorly protected or unsupervised cloud environments, so why bother attacking hardened legacy corp net?

### Top Cloud Threats

#### Poor / Default Configs

Breaches are often due to a database or server exposed to the internet with no or minimal authentication, spilling massive amounts of (often regulated) data.

#### Poor Identity Control

Developers may expose sensitive credentials on public sites; org may fail to follow least privilege principles; or staff might be creating shadow IT via rogue accounts / environments.

#### API Abuse

Application developers prioritizing speed and functionality may not comprehend abuse potential of APIs, exposing customer data or infrastructure.

#### Availability Attacks

Massive IoT botnets can now target cloud-scale providers previously viewed as unsinkable. Incidents may also not be intentional but result of CSP failures affecting entire regions.

#### Side Channels

For now mostly academic, but compute and storage is (usually) not bare metal, which exposes resources to VM escapes, timing attacks, and other methods of leaking data in shared environments.

**These are not threats that map to a legacy IR model**

# What's different about Cloud IR



## Cloud Moves at Warp Speed

Everything happens way too fast for reactive IR to start when an alert comes in



## Dynamic resources require dynamic response capabilities

Playbooks / runbooks don't cut it - IR runbooks need to be CODE in order to respond to events in time (can't pull memory from a terminated instance, or isolate an infected lambda that already ran)



## Push left, integrate security in the space between SDLC and Prod

You must automate IR throughout deployment process

- Code environments for robust enforcement of security resources (ex. instances without EDR, insecure fw rules, or unencrypted storage get killed immediately and without appeal)



## Failure to adopt cloud native solutions, will leave you with legacy solutions

Taking a server, turning it into a VM and hosting in AWS is **NOT** cloud computing (but it is what many legacy enterprises do anyways)



# Getting the Right Players For Cloud IR

	Cyber Incident Response	DevOps Engineers	Cloud Service Providers (e.g. AWS, Azure, GCP)
Response Mission	<i>Architect and maintain robust visibility and response operations in the cloud</i>	<i>SMEs for building and integrating response capabilities with existing cloud environment</i>	<i>Provide unique high-level visibility, access, or assistance</i>
General Responsibilities	<ul style="list-style-type: none"> <li>Design monitoring requirements and determine alert/action thresholds</li> <li>Coordinate incident from alert to resolution</li> <li>Perform forensics on data isolated/retrieved by automated response tools/actions</li> </ul>	<ul style="list-style-type: none"> <li>Note/escalate irregular behavior within cloud environment</li> <li>Provide best practices/SMEs to help develop automated response tools/actions</li> <li>Integrate containment requirements into environment architecture</li> </ul>	<ul style="list-style-type: none"> <li>Alert on system-level/macro-scale events or issues</li> <li>Respond to requests for features/data to support response operations</li> <li>Support root cause analysis and troubleshooting</li> </ul>
<p><i>Though not inclusive of the entire team, these primary players form the foundation of the Cloud IR Response Team</i></p>			

# Understand Your Cloud Maturity

Cloud affects all areas of Incident Response

- People: Cloud-native skills required
- Processes: New playbooks designed around integration with deployment pipeline, new SLAs
- Technology: Forge new tools and fully automated/intelligent response capabilities

	Basic	Intermediate	Advanced
Indicators	<ul style="list-style-type: none"><li>• Direct port of legacy server-based resources to cloud hosting</li><li>• Basic network layout</li><li>• Discrete access controls/IAM</li></ul>	<ul style="list-style-type: none"><li>• DevOps team with scalable CI/CD pipeline</li><li>• Dynamic Networking</li><li>• Role-Based Access Control</li></ul>	<ul style="list-style-type: none"><li>• Containerized architecture on top of automated distributed compute system (ex. Kubernetes)</li><li>• Advanced/multi-cloud dynamic network</li><li>• Federated, per-user Single Sign-On</li></ul>
Traits	Legacy IR processes and tools may still be effective	Leverage DevOps team for additional monitoring capabilities; adjust SLAs	IR team with cloud-native skillset is required to build customized automated response tooling

# What's Next? Here's what you should do when you return to the office

## Jumpstart your Cloud Incident Response Program

Cloud IR migration is a journey. Where does your org sit? Where does it want/need to be?

1

### Legacy Transfer

**Direct port** of legacy server-based resources to cloud hosting. Old EDR/ and log forwarding could still be effective in this configuration.

2

### Access Control

Even with a basic network layout, attention must be paid to **enforce Role-Based Access Control**. This may or may not integrate with existing authentication systems.

3

### Dynamic Resources

Leverage the scalability of cloud resources to optimize your environment and **dynamically scale existing security policies and technologies**.

4

### Update TTPs

Ensure best practices in Cloud Incident Response by **updating and maintaining playbooks, policies, procedures, SLAs and tooling** to incorporate cloud resources.

5

### Dev Ops Integration

Using IR team members with cloud-native skillsets, **implement a full DevSecOps deployment pipeline** utilizing automation and advanced tools to enable intelligent response.

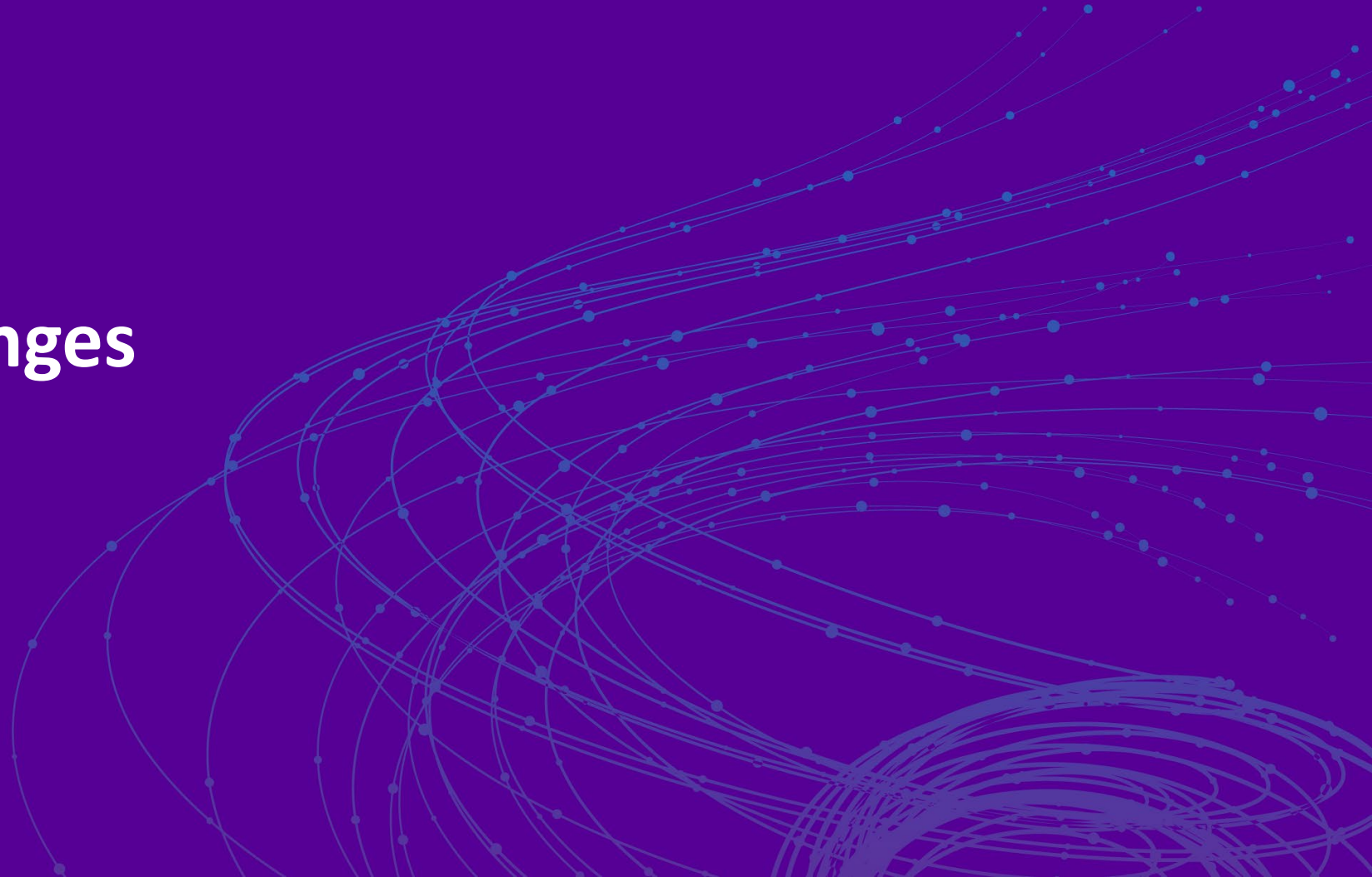
6

### Continuous Improvement

Cloud-native IR must **continue to adapt** as the business adopts new cloud services or develops new applications leveraging cloud resources.

**RSA**Conference2019

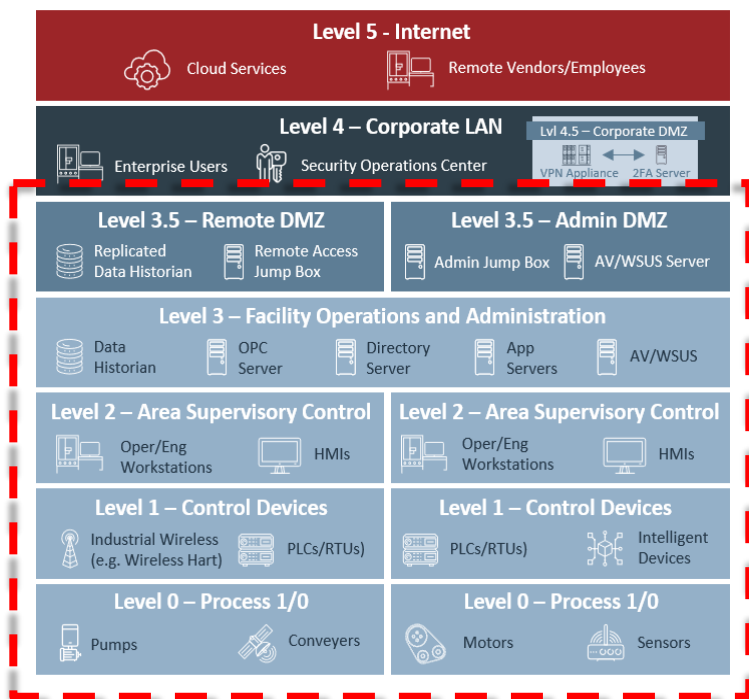
## OT IR Challenges



# Threats in OT

*OT incidents are likely to generate more attention than a typical IT incident.*

*Threat actors are targeting OT environments below Level 4*



- Target weaknesses in outdated industrial equipment
- Can leverage access through unsecure OT to gain access to broader company networks
- Targets the weakest link
- Can cause physical impacts through cyberattacks

## Crypto Mining Malware

2018 Crypto mining attack consumed the bandwidth of a water utilities HMIs causing security tools to fail

## TRITON Malware

2017 TRITON malware attack targeted a major manufacturing plant, disabling safety systems and leaving the plant vulnerable

## NotPetya

2017 Malicious actors use a C2 backdoor to execute malware on infected machines significantly impacting organizations

## WannaCry Ransomware

2017 cyber virus which locked down IT and OT assets globally, demanded system owners to pay a ransom to restore system operations.



# What's Different About OT



## Health and Safety factors

Incident responders need a full understanding of the consequences of their actions

- Shutting down key processes can result in unsafe conditions and disrupt access to life-safety critical systems (e.g. gas detectors, oxygen meters)



## Environment Challenges

Real-time OS's, non-traditional protocols, application and network dependencies that are unknown/undocumented



## Need for Specialized Response Tooling and Training

Special response tooling may be required (embedded devices, RTUs, and PLCs)



## Varying Response Motivations

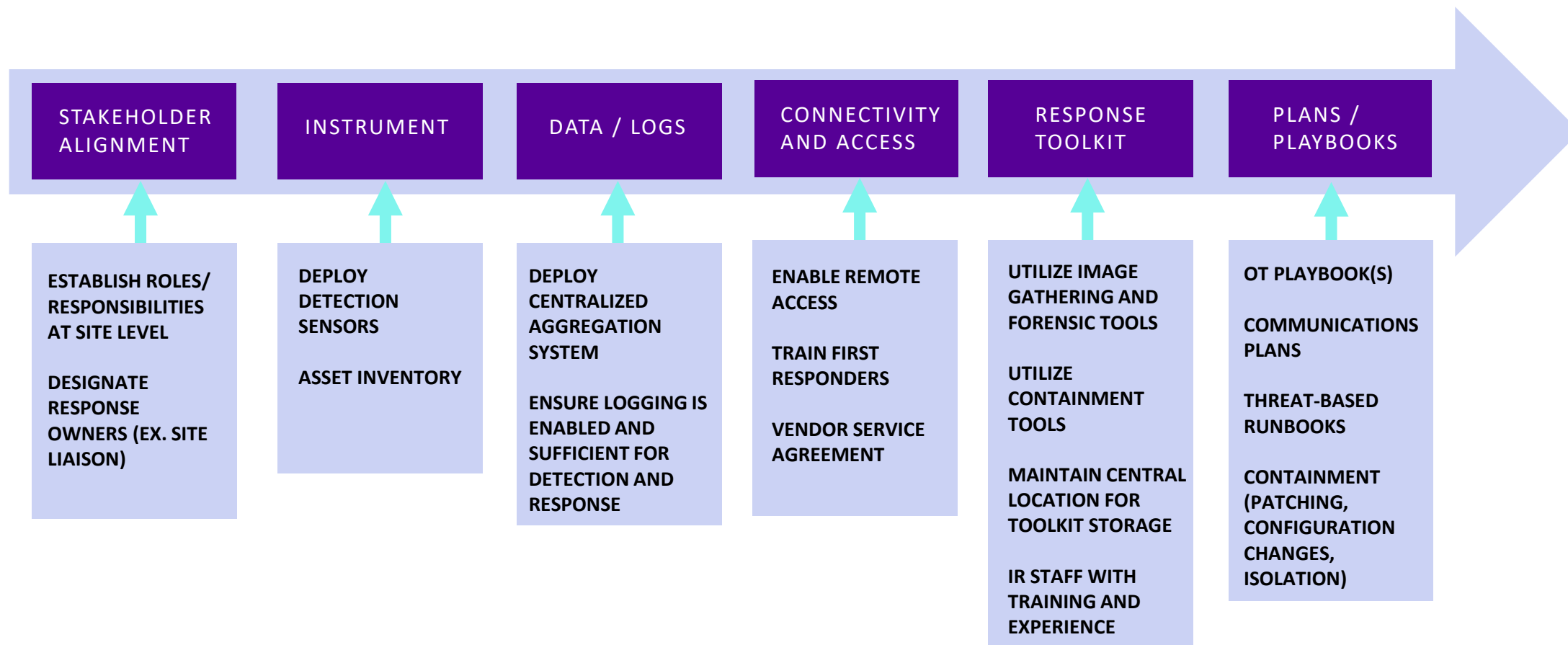
Response stakeholder motivation may vary – Response objective of OT engineers/operators may not align to Cyber IR objectives

# Getting the Right Players For OT IR

	Cyber Incident Response	Site / Process Engineers	Vendors (e.g. Honeywell, Rockwell, Emerson)
Response Mission	<i>Enable successful incident response</i>	<i>Provide permissions, access and site expertise</i>	<i>Assist in troubleshooting and replacement of vendor components/systems</i>
General Responsibilities	<ul style="list-style-type: none"> <li>• Coordinate incident functions and facilitate information sharing</li> <li>• Identify containment / remediation activities for critical vulnerabilities</li> <li>• Perform forensics and containment</li> </ul>	<ul style="list-style-type: none"> <li>• Report system irregularities occurring onsite</li> <li>• Provide access and permissions to investigate infected systems and embedded devices</li> <li>• Provide expertise regarding site operations</li> </ul>	<ul style="list-style-type: none"> <li>• Assist site personnel in performing troubleshooting</li> <li>• Repair or replace infected systems</li> <li>• Support root cause analysis and troubleshooting</li> </ul>
<p><i>Though not inclusive of the entire team, these primary players form the foundation of the OT IR Response Team</i></p>			

# OT IR Transformation Journey

*"Standard cyber incident remediation actions deployed in IT business systems may result in ineffective and even disastrous results when applied to ICS cyber incidents, if prior thought and planning specific to operational ICS is not done." - DHS*



# What's Next? Here's what you should do when you return to the office

## Jumpstart your OT Incident Response Program

1

### Response Playbooks

Develop **IR playbooks** for events impacting the OT domain. Identify and engage with new stakeholders.

2

### Emergency Remediation Planning

Develop IR playbook to **facilitate options for emergency containment**, patching, or the deployment of remediation actions.

3

### Enterprise Alignment

Develop **"rights of way"** between Cyber Defense Ops, IT, third-party providers, and site engineering.

4

### Access and Privileges

**Secure remote accesses** and **elevated privileges** for IR staff designated to handle OT incidents.

5

### IR for Offsite OT Assets

Define a strategy for **deploying IR fly-away teams and tools** to "off estate" assets (e.g., contractor, joint-venture operated site).

6

### IR Workbench

Implement an **IR response workbench** with Admin/remote access, live response, tools/scripts, forensic tools, etc.

7

### Training

**Train IR staff on the OT environment** landscape, OT investigative methodologies, and enable test environments for staff to practice IR on simulated control system workstations and components.

8

### IR Exercises

Conduct periodic IR exercises of varying levels of complexity, and **inclusive of cyber, domain-specific, and enterprise stakeholders**.

# Case Study

## Global Oil Field Services organization that sought to enhance detection and response capabilities for its OT facilities

### Challenges

- **Silos** – No agreement between OT and Cyber to enable detect and respond responsibilities
- **Limited Access** – First responders had limited remote access to respond to incidents at OT sites
- **Insufficient Visibility** – Detection capabilities were not deployed consistently across all OT sites
- **Knowledge Gap** – Cyber responders lack working knowledge of OT systems; OT personnel lack understanding of cyber capabilities

### Activities

- Multiple **workshops** to identify key stakeholders (internal and external to the organization)
- Documented the process and **workflows** to understand the operating environment
- Conducted incident **scenario exercises** to develop functional response activities
- Established **Severity Criteria** and target state requirements for visibility, detection, and response  
Drafted **actionable** Incident Management Plan and IR Playbooks

### OUTCOMES

An agile and adaptable cyber security organization able to effectively respond and contain unknown threats to the organization

Delivered new shared responsibility models for teams which had not worked together in the past

Defined strategic direction for further maturing the organization's detection and incident response capabilities



# References and Helpful Sites

## OT Incident Response

- <https://dragos.com/resource/lessons-learned-from-threat-hunting-responding-to-industrial-intrusions/>
- <https://www.boozallen.com/c/insight/publication/top-8-cybersecurity-trends-for-2019.html>
- [https://www.researchgate.net/publication/266477470\\_Developing\\_Cyber\\_Forensics\\_for\\_SCADA\\_Industrial\\_Control\\_Systems](https://www.researchgate.net/publication/266477470_Developing_Cyber_Forensics_for_SCADA_Industrial_Control_Systems)
- <https://www.boozallen.com/s/insight/thought-leadership/industrial-cybersecurity-threats-are-on-the-rise.html>
- <https://www.langner.com/ot-security-incident-management/>
- [https://ics-cert.us-cert.gov/sites/default/files/recommended\\_practices/final-RP\\_ics\\_cybersecurity\\_incident\\_response\\_100609.pdf](https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf)

## Cloud Incident Response

- <https://www.sans.org/reading-room/whitepapers/incident/incident-response-amazon-ec2-first-responders-guide-security-incidents-cloud-36902>
- <https://aws.amazon.com/blogs/publicsector/building-a-cloud-specific-incident-response-plan/>
- <https://www.okta.com/security-blog/2018/04/incident-response-in-the-cloud-%E2%80%93-is-your-security-team-ready/>
- [https://d1.awsstatic.com/whitepapers/architecture/AWS\\_Well-Architected\\_Framework.pdf](https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf)

# QUESTIONS

# THANK YOU

FOR MORE INFORMATION, PLEASE CONTACT:

**JASON ESCARAVAGE**

SENIOR VICE PRESIDENT

[ESCARAVAGE\\_JASON@BAH.COM](mailto:ESCARAVAGE_JASON@BAH.COM)

**PHIL HAMILL**

PRINCIPAL – OT CAPABILITY LEAD

[HAMILL\\_PHILLIP@BAH.COM](mailto:HAMILL_PHILLIP@BAH.COM)