Building An OT Capable SOC

The ecosystem of skills and technology required for ICS security operations

MATT COWELL
mcowell@dragos.com
@m_p_cowell

The Dragos Offering

Technology, Intelligence, Expertise

DRAGOS

Today's Agenda

01 **Defining an OT capable SOC**

02 **Considerations to build an OT capable SOC**

03 **Example OT SOC workflow**

04 **Evaluating readiness & establishing a path to an OT SOC**

DRAGOS

What is a SOC?

What is a SOC?

- Focused team of trained & experienced individuals whose mission is to prepare for, detect and respond to security issues & incidents.
- Utilizing technology to analyze data gathered from intelligence sources AND data from within the environments they are protecting to perform security operations.

DRAGOS

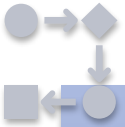
Core Components of a SOC

People

- Domain Expertise
- Multi-skilled
- Tiered support

Technology

- Collection
- Visibility
- Detection
- Workflows



Process

- Consensus based
- Tested
- Adaptable
- Defined Swimlanes

DRAGOS

Summary of SOC Functions

PREPAREDNESS

1. Collection & visibility
2. Threat intelligence
3. Firewall hardening

PROACTIVE

1. Hypothesis driven investigations (hunting)
2. Vulnerability assessments
3. Tabletop exercises

REACTIVE

1. Investigating alerts
2. Gathering forensics
3. Root cause analysis

DRAGOS

Defining an OT Capable SOC

- Focused team of trained & experienced individuals whose mission is to prepare for, detect and respond to security issues & incidents impacting OT systems.
- Utilizing technology optimized for OT to analyze OT relevant data gathered from intelligence sources AND data from within the OT environments they are protecting to perform security operations.

Defining an OT Capable SOC

Security Technology and Skills support:

- OT endpoint diversity & impact on data collection
- Dissection & interpretation of OT protocols
- OT Technology/Assets (PLC's, DCS, etc)
- OT Language & acronyms
- Consequence awareness
- Environment awareness
- OT Threat landscape awareness

Optimized for an OT environment

DRAGOS

The Great Debate of 2018

https://www.youtube.com/watch?v=AB8J8CSvQas

Different SOC Approaches

- Build OT capabilities into existing IT SOC

- Build a dedicated OT SOC

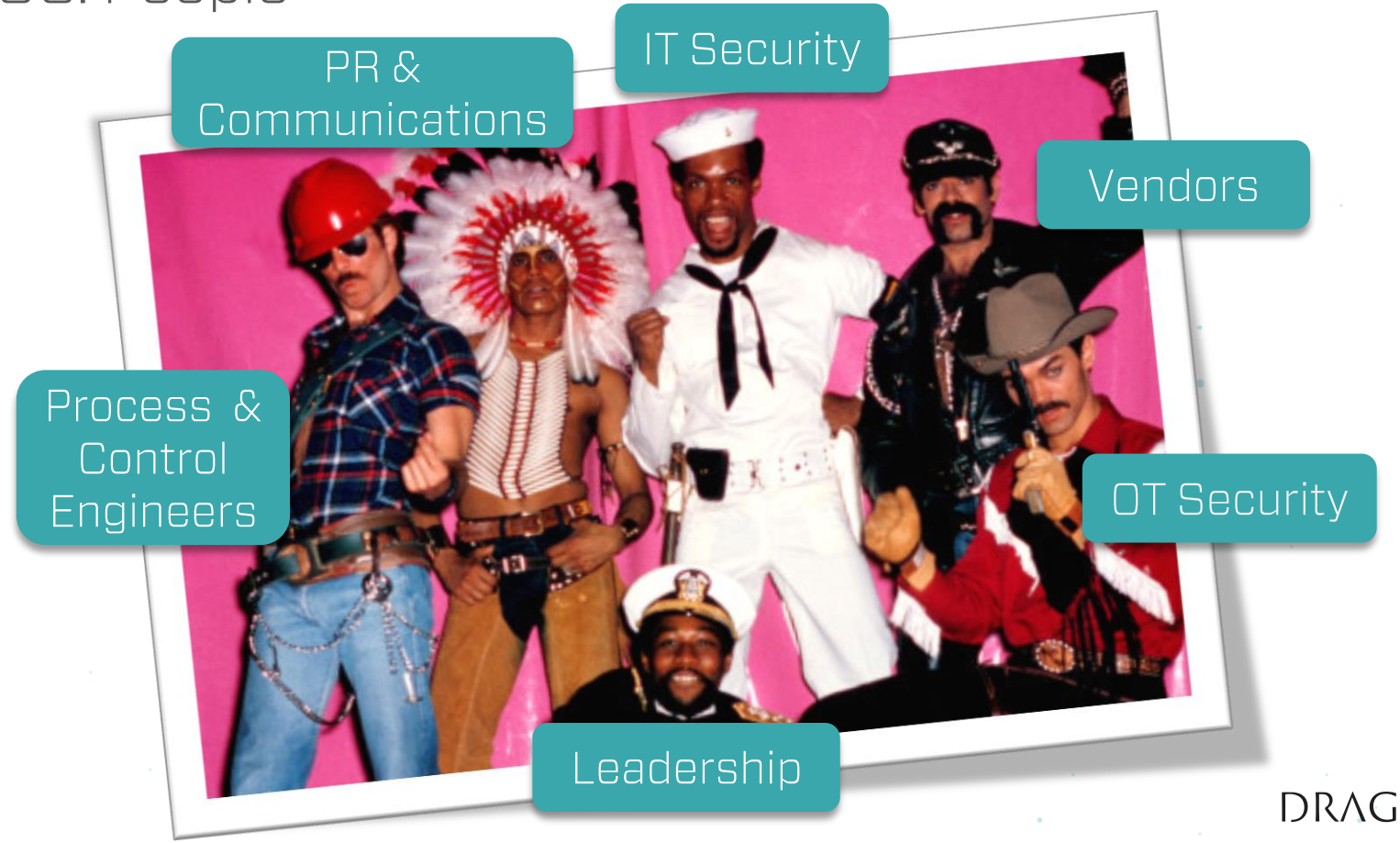
- Build OT security operations into existing control room operations
- Outsource OT SOC functions to 3rd party security team

DRAGOS MANAGED THREAT HUNTING

- Hybrid

DRAGOS

OT SOC: People



DRAGOS

OT SOC: Skills & Experience

PREPAREDNESS

1. Collection & visibility
2. Threat intelligence
3. Firewall hardening

PROACTIVE

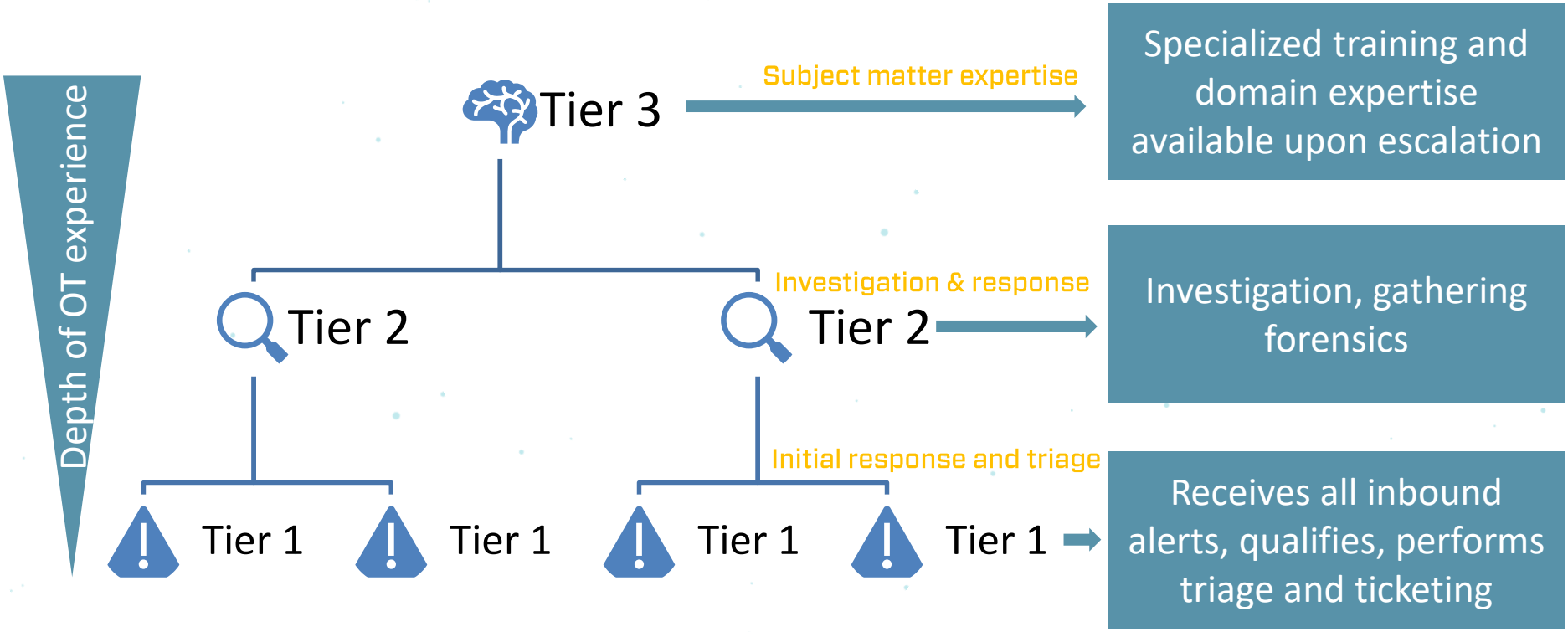
1. Hypothesis driven investigations (hunting)
2. Vulnerability assessments
3. Tabletop exercises

REACTIVE

1. Investigating alerts
2. Gathering forensics
3. Root cause analysis

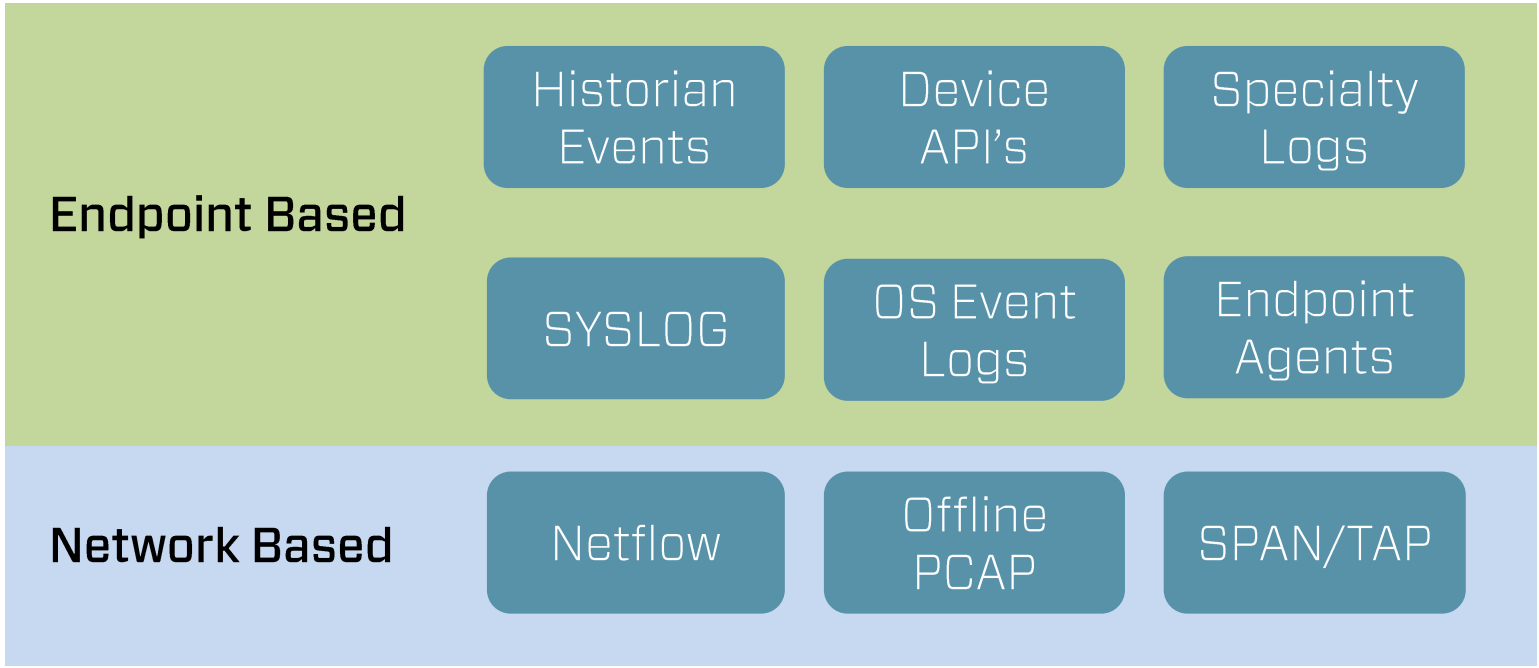
DRAGOS

OT SOC: Tiers



DRAGOS

OT SOC: Collection



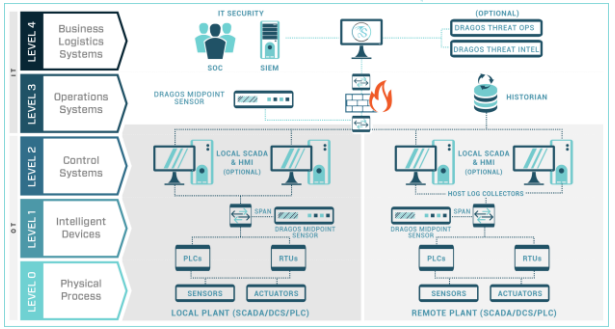
Define a Collection Management Framework

DRAGOS

OT SOC: Architecture

Plant Coverage

Enclave Coverage



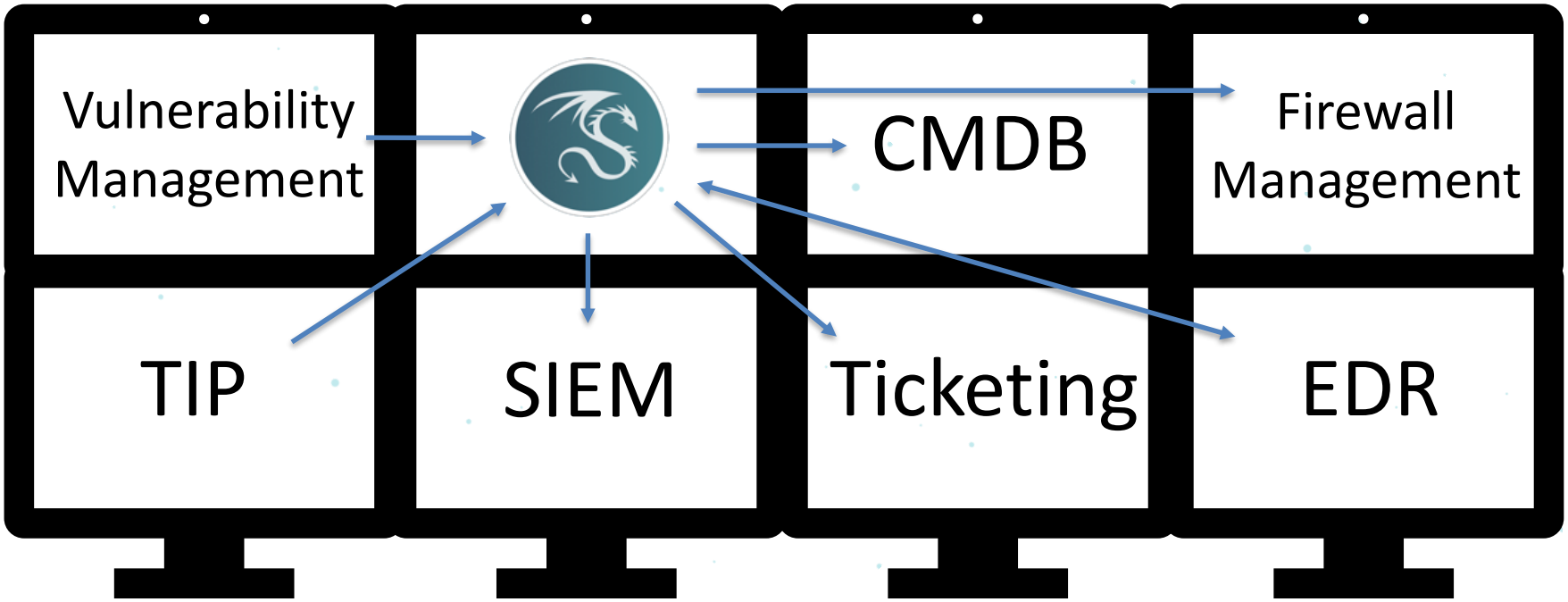
Network and Asset Coverage

DRAGOS

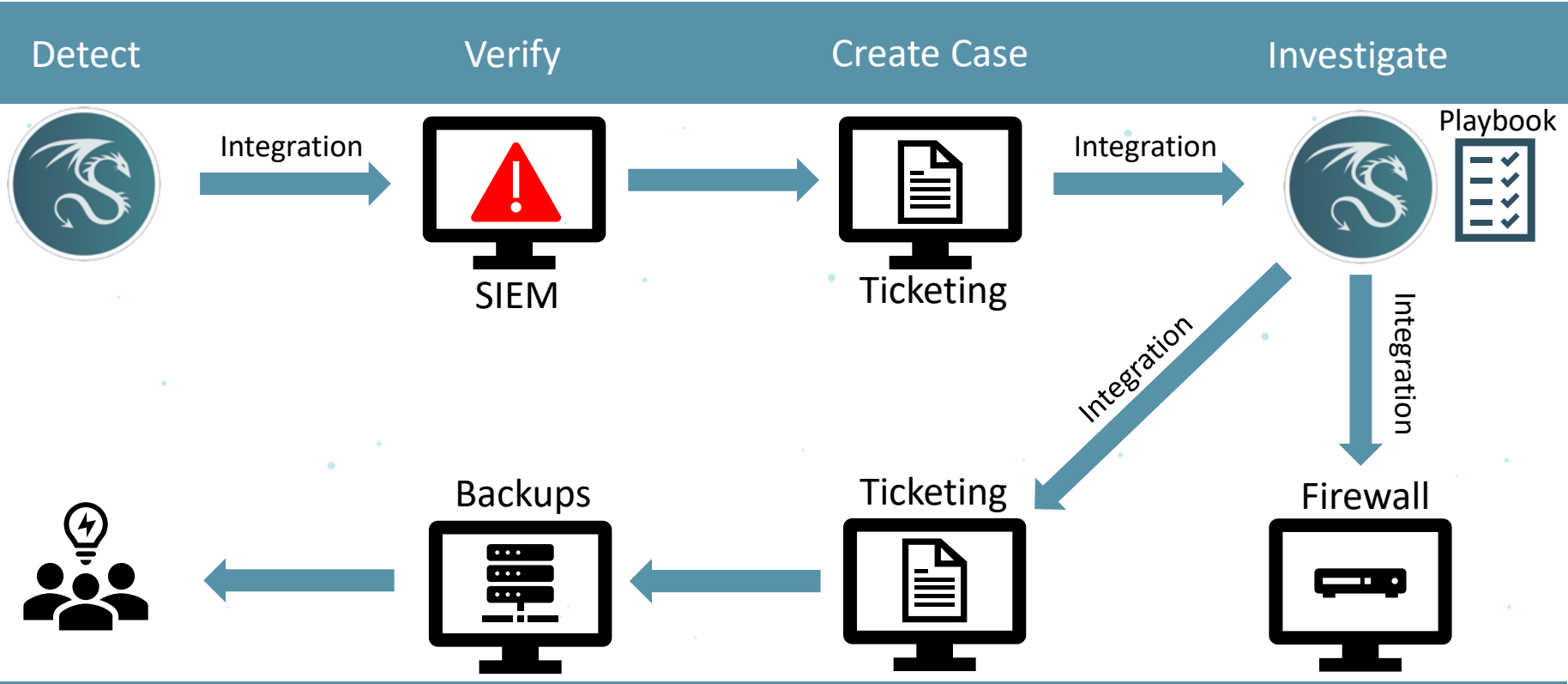
OT SOC: Technology

DRAGOS

OT SOC: Technology

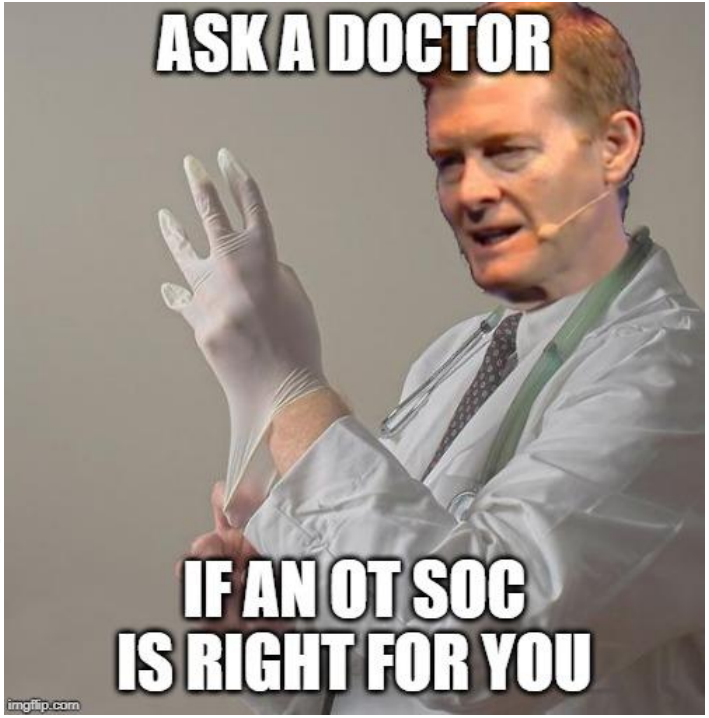


OT SOC: Example Response Process



OT SOC: Evaluating Readiness

1. Does your risk justify the investment?
2. Does your current infrastructure support the effort?
3. Do you have budget?
4. Do you have resources?
5. Are you mature enough today?
6. What are your objectives?



DRAGOS

Other Considerations

- SCALE/EXPAND
- INTEGRATIONS
- TRAINING & SUPPORT
- REDUNDANCY
- MEASURING SUCCESS

OT SOC: Where to Begin?

Define OT SOC goals

- Coverage
- Reactive
- Proactive

Evaluate capabilities & gaps

- Collection
- Technology
- Skills

Devise multi-year plan

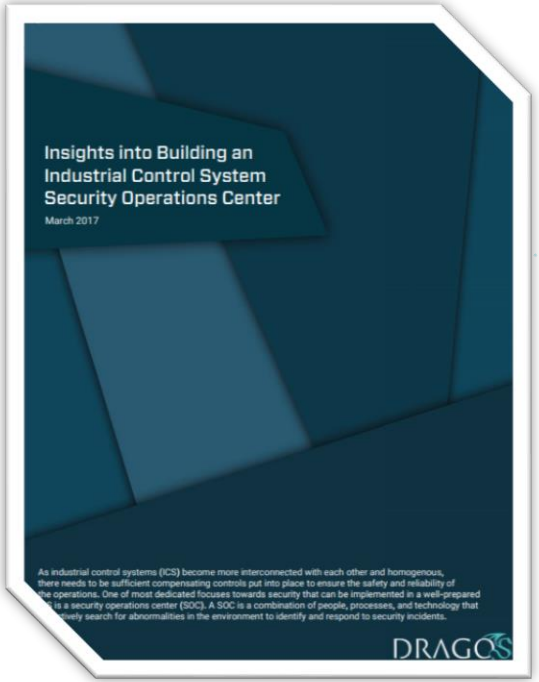
- Investments
- Address gaps
- Leverage partners/vendors

Iterate and expand

- Increase coverage
- Process optimizations
- Deeper capabilities

DRAGOS

Additional Resources



https://dragos.com/resource/insight-into-ics-soc-pdf/

https://dragos.com/blog/industry-news/building-a-collection-management-framework-for-industrial-control-systems/

DRAGOS

Summary

1. No one size fits all approach
2. Evaluate what you need to be effective to YOUR needs now and as you grow. Focus on the mission.
3. Success will require a combination of people, technology & process together
4. Visibility and collection will determine overall success
5. Know how to measure success.
6. Evolve & streamline with maturity

Thank you

MATT COWELL
mcowell@dragos.com
@m_p_cowell