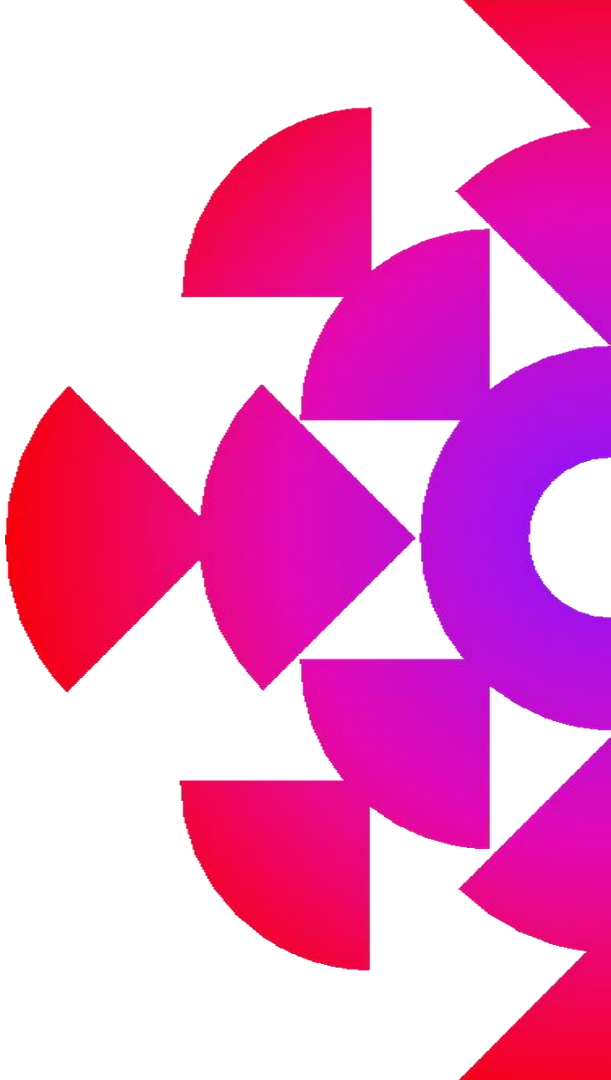
CLAROTY

FIVE ESSENTIAL STEPS FOR A CONVERGED IT/OT SOC

May 20, 2021



INTRODUCTION

Presented by-

Guilad Regev
Senior Vice President, Customer Care at Claroty

Don Weber
Instructor, SANS Institute

AGENDA

I. INTRODUCTION

A. Why OT Environments need SOC coverage

B. Making the case for a converged IT/OT SOC

II. THE FIVE ESSENTIAL STEPS FOR A CONVERGED IT/OT SOC

A. Appoint a designated IT/OT cybersecurity program manager

B. Achieve optimal alignment with existing cybersecurity capabilities

C. Gain visibility into IT and OT security alerts within the OT environment

D. Designate a cybersecurity site leader for each OT site

E. Establish a PSERT tasked with handling standard operating procedures

III. Q&A SEGMENT

Why OT environments need SOC coverage

The Question:

Should my organization create a separate Security Operations Center (SOC) for OT, or should we adapt our existing, IT-centric SOC to cover IT and OT in a consolidated manner?

Making the case for a converged IT/OT SOC

Performance Advantages

- **Enhanced visibility**, monitoring, and risk mitigation across the enterprise
- **Rapid configuration** changes and new policy implementation to enable secure digital transformation
- **Centralized incident response** and a singular, cohesive view of risk for the entire organization

Efficiency Advantages

- **People:** Leverages existing SOC rather than creating a separate team, minimizing the need for new hires
- **Technology:** Integrates existing tools with OT-specific technology to maximize ROI and enable centralized maintenance and upgrades

CLAROTY

THE FIVE ESSENTIAL STEPS FOR A CONVERGED IT/OT SOC

Appoint a designated IT/OT cybersecurity program manager

Direct report to CISO

Lead the IT/OT initiatives

Leverage existing relationships

IT/OT middle ground

CLAROTY

Achieve optimal alignment with existing cybersecurity capabilities

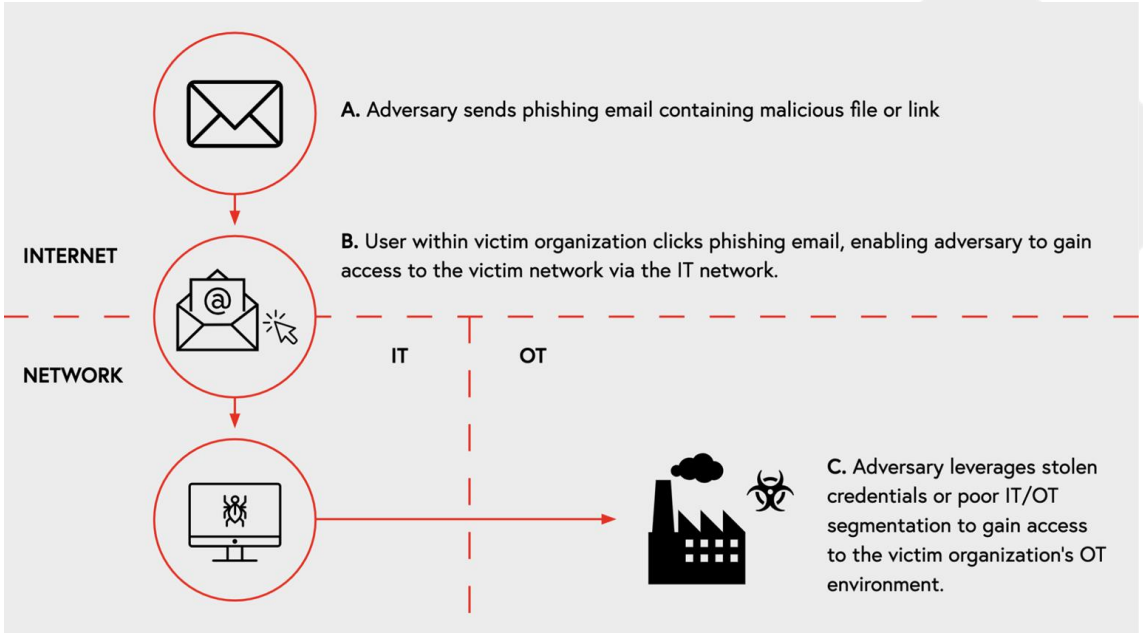
Leverage Existing Cybersecurity Infrastructure + Implement New

Assess Current Capabilities

Identify Gaps

Goal: To create a centralized system - easy access to all resources: SIEM, SOAR, and full restful API.

Gain visibility into IT and OT security alerts within the OT environment



- IT/OT convergence creates opportunities for threat actors to gain access to OT via the IT network.
- Cyber threats to OT typically enter the victim organization's network via the IT environment, so it's crucial to have unified visibility across IT and OT.

Gain visibility into IT and OT security alerts within the OT environment

Core dimensions of OT visibility:

- **Asset visibility**
- **Network visibility**
- **Process visibility**

Designate a cybersecurity site leader for each OT site

What CSLs need to succeed:

- Understanding of OT assets, systems, and security risks
- Familiarity with the network infrastructure of their plant
- Clear expectations for communicating with the SOC, PSIRT, and other relevant parties.
- Initial CSL training, followed by additional trainings to familiarize them with new standard operating procedures (SOPs).

Establish a PSERT tasked with handling standard operating procedures

PSERT (Production Security Emergency Response Team)

OT Security Practices

Standard Operating Procedures

Holistic IT/OT cybersecurity

Unfamiliar Situations

Q&A SEGMENT

CLAROTY

THANKS FOR JOINING US!

To learn more about the five steps detailed in this presentation, read our new white paper.