RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: **SBX4-R2**

A SOC in the Sandbox

Thomas VanNorman
Director of Application Engineering
Veracity Industrial Networks
@Tom_VanNorman

VERACITY
INDUSTRIAL NETWORKS

A SOC in the Sandbox

Today you will learn:

- Get an introduction to ICS SOCs.
- Learn from a sandbox demonstration.
- Understand the effects of attacks on ICS systems.

A SOC in the Sandbox

What is a OT Security Operations Center anyway?

Do I really need one?

A SOC in the Sandbox

- Are they…
- Anomaly Detection Solutions?
- Security Information and Event Management (SIEM)?
- Intrusion Detection Systems (IDS)?
- Cyber Attack Maps aka Pew Pew Maps?

A SOC in the Sandbox

- Or are they really a unicorn?

A SOC in the Sandbox

- No they are not unicorns , they really do exist.
- But who has them?
- Many fortune 1000 companies operate OT SOCs.
- Some companies have multiple OT SOCs.
- Some companies outsource Enterprise SOC and operate OT SOCs in house.

Ok so what exactly is an OT SOC?

A SOC in the Sandbox

- A SOC is a combination of people, processes, and technology that proactively search for abnormalities in the environment to identify and respond to security incidents.

A SOC in the Sandbox

The people part:

- Throwing people at a problem is never a solution.
- Good people at various skill level are needed with unique talents
- Three tiers of people are a must!

A SOC in the Sandbox

Tier 1 analysts who search logs and process, alerts, and other categorized events to identify and escalate abnormalities.

Tier 2 analysts are the incident responders who triage the events, analyze the accompanying activity, and apply appropriate mitigations.

Tier 3 analysts are there to act as subject matter experts when deeper analysis is required; especially against new threats. <u>These are the people that are the closest to the process.</u>

A SOC in the Sandbox

The processes part:

- Documentation and procedures are a must!
- Document everything that happens
- Follow procedures every time. If one does not exist make one.

A SOC in the Sandbox

The technology part:

NO SILVER BULLET

- Problem- Complete network visibility
- Solution- Software Defined Networking
- Problem- What do I do with this data now?
- Solution- Input to a threat detection solution

A SOC in the Sandbox

- Problem- Coloration of data from multiple systems
- Solution- Integrate the various platforms to a SIEM

A SOC in the Sandbox

Important take away:

- 100% of detection should be a false positive or detection.
- Many options are available for running an OT SOC
  - Managed Security Services Provider (MSSP)
  - In house
  - Hybrid, Tier 1-2 MSSP, Tier 3 in house
- More data the better
- Technology is not a replacement for people.

A SOC in the Sandbox

What are we doing in the ICS Sandbox?

- We have built an area where you can interact with SME's on this topic and many other OT / IOT topics.
- You can test your skills at several challenges.
- You can can avoid sales pitches and see how things actually work.

Questions?

Thank you for your time!

Tom VanNorman

@Tom_VanNorman

info@icsvillage.com

Reference for this presentation can be found at : https://dragos.com/media/Dragos-Insights-into-Building-an-ICS-Security-Operations-Center.pdf