Protect 2014

Washington, D.C. September 8-11

Bridging the gap: SOC and CSIRT

Mitchell Webb, HP SIOC

Anthony Polzine, Protiviti

What is Incident Management?

- Incident Management involves preparing for, identifying and responding effectively to an incident [1]
- Mainly Security Operations - Intrusion Analysis (SOC), Incident Response (CSIRT) and Security Engineering
- Conducted by a group with expertise [2], defined process and effective technology

Preparation

- Developing an Incident Management program
- Founded on policy
- Built on people, process and technology

Detection

- Intrusion detection and analysis
- Triage and Mobilization
- Typically the task of the **SOC**

Containment

- Stop the bleeding by securing assets
- Typically fast passed leveraging technologies
- Typically the task of the **CSIRT**

Eradication and recovery

- Removal of the adversary from the environment
- Restoring normal operations
- Typically the task of the **CSIRT**

Response review

- Review actions and identify areas of improvement

The evolution and need for integration

- CSIRT capabilities have existed for many years in most organizations – focusing mostly on incident handling and forensics
- The concept of the SOC managing intrusion detection began to take hold around 2008 and many organizations began to train Analysts and implement core processes and technologies
- Traditionally SOC and CSIRT organizations have operated in silos executing only tasks relevant to their assigned incident management phase – with limited integration

Without effective integration, key information is missed resulting in non-optimal operations and greater risk to the organization

Integrating people

- People are critical to the success for both SOC and CSIRT operations – skill sets are similar while specialties exist on both teams
  - CSIRT teams typically contain greater forensic experience which can be leveraged by the SOC for improved detection content
  - SOC teams typically contain greater understanding of log management, including the retrieval of information from various information sources, which can be leveraged by the CSIRT for leads
- Core skills should be assessed for everyone in the Security Operations organization and cross training should occur as this greatly enhances the overall capability of the organization
- Additionally, both teams should regularly interact during incidents, scheduled operations meetings, lessons learned reviews and training sessions

Integrating process

- Each team should have an in-depth understanding of the others processes – a simple handover during the escalation phase is not optimal
- SOCs can often (and should) perform forensic level functions to provide thorough assessments during analysis and prep materials for CSIRT response activities
- Defined processes with an integrated incident management system is key to managing incident information and status for all stakeholders

Integrating technology

- Information must be available to all with a need to know, core technologies should be leveraged by both groups
  - **SIEM:** ArcSight is core to detection and response – Rapid Assessment and Triage content may be leveraged to provide quick retrieval of key information
  - **Network Forensics:** Packet captures are a must by the SOC for acquisition and analysis of network communications
  - **Host Forensics:** Memory acquisition and analysis is critical for accurate assessments by a SOC, even though this function has traditionally only existed within CSIRT
  - **Case management:** Information tracking for assessments, criticality, timeline and status must be shared – a single view of incident management tracking
  - **Indicator management:** Information for indicators used for detection and monitoring of an adversary must be made available and shared regularly

Effective operations

- Significant opportunities exist to integrate SOC and CSIRT teams resulting in substantial benefit to the larger incident management program
  - People: Leverage cross training and shadowing to develop and mature the entire security operations organization
  - Process: Integrate processes so that information is shared effectively and transitions are seamless
  - Technology: Develop systems that support the processes of both teams during investigation and response activities

References

1. http://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
2. https://www.sans.org/courses/

For more information

Attend these sessions

- TT3066, Leveraging HP ArcSight for Breach Response
- TT3052, HP ArcSight: Data Makes the Difference

Visit these demos

- SOC Demo

Your feedback is important to us.
Please take a few minutes to complete the session survey.

Tonight's party

@ Newseum

Time

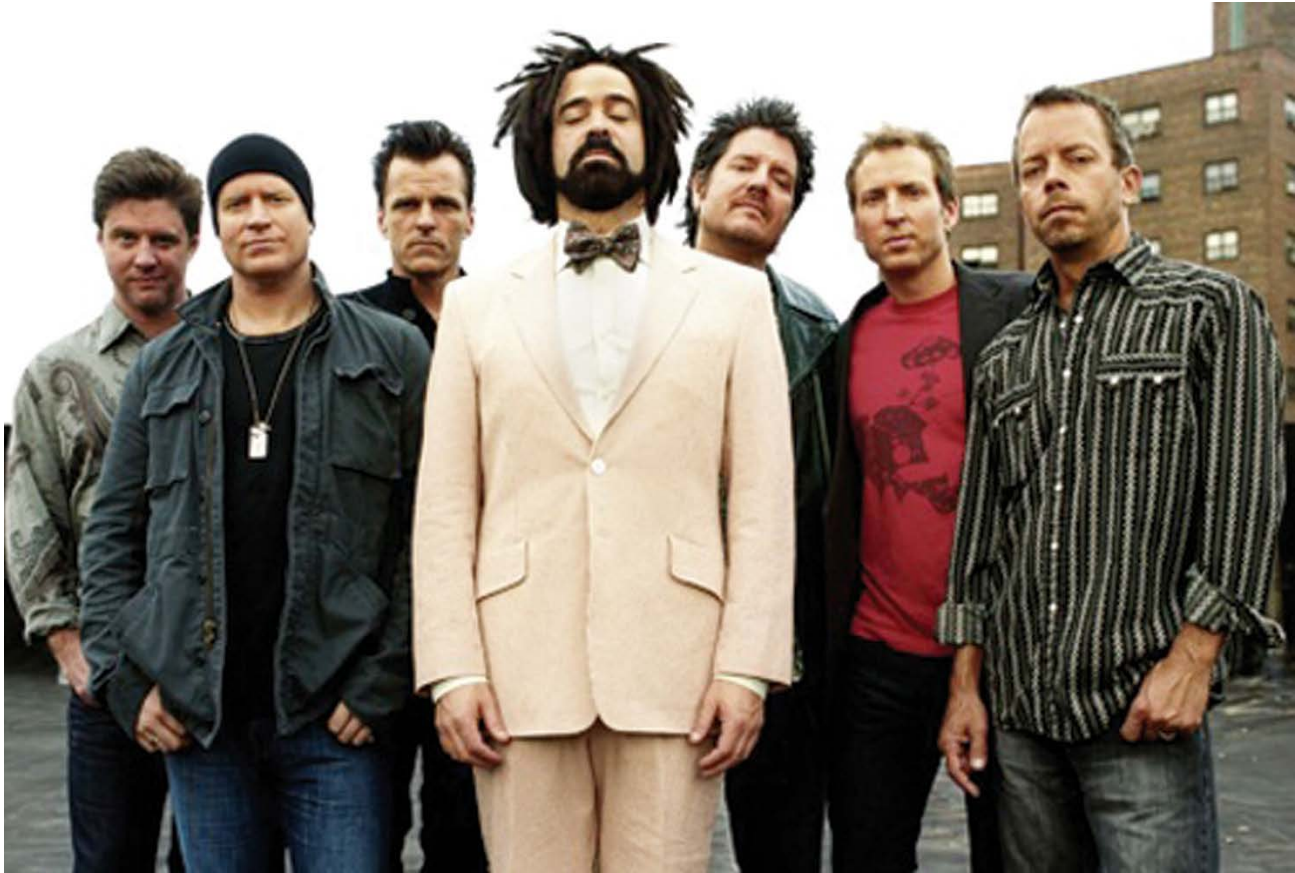
7:00 – 10: 00 pm

Shuttles run between hotel's Porte Cochere (Terrace Level, by registration) and Newseum from **6:30 - 10:00 pm**

Questions?

Please visit the Info Desk by registration

Enjoy food, drinks, company, and a private concert by Counting Crows



Please give me your feedback

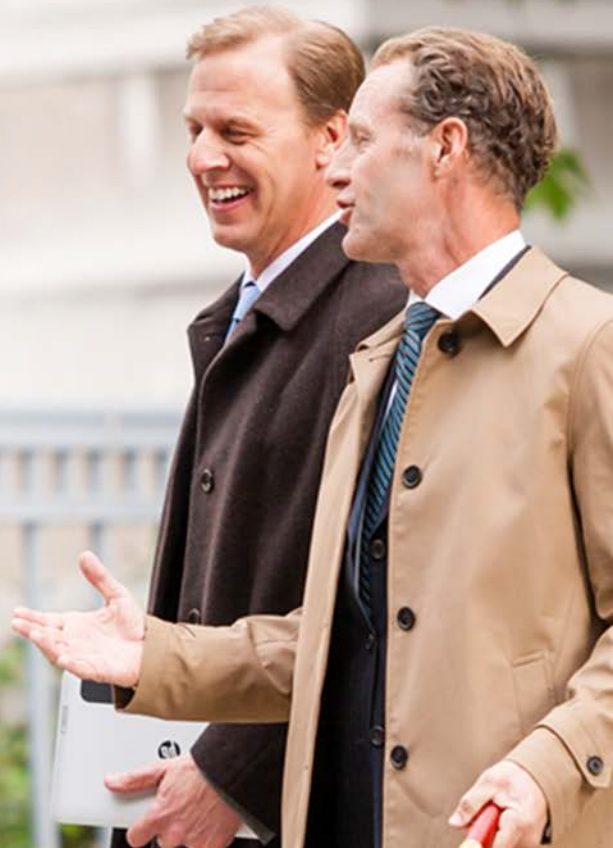
Session TT3035 **Speaker** Mitchell Webb and Anthony Polzine

Use the mobile app

1. Click on **Sessions**
2. Click on **this session**
3. Click on **Rate Session**

Or use the hard copy surveys

Thank you for providing your feedback, which helps us enhance content for future events.



Thank you

Make it matter.