Building, Maturing & Rocking a Security Operations Center

Brandie Anderson
Sr. Manager, Global Cyber Security Threat & Vulnerability Management
Hewlett-Packard
Agenda

- To be or Not to be...
- What is a SOC?
- Use Case Creation
- People
- Process & Procedure
- Documentation
- Workflow
- Metrics
- I don’t want to grow up
- Rocking a SOC
- Questions
• Building a SOC is a business decision
  • Organization size
  • Compliance factors
  • Reduce the impact of an incident
  • ROI
  • Proactive reaction
What is a SOC?

Through people, processes and technology, a SOC is dedicated to detection, investigation, and response of log events triggered through security related correlation logic.
McAfee ePO

Malicious File Download Event

Tipping Point Alerts

Suspicious Network Activity

Possible Compromised Host or Insider Threat Activity
Use Case Creation

2012: The year malware surged 'dramatically'

91% of Targeted Attacks Start with Spear-phishing Email

Large-Scale Water Holing Attack Campaigns Hitting Key Targets

Microsoft's Patch Tuesday Leaves Out Crucial Internet Explorer Fix

Adobe Data Breach Exposes Military Passwords

Cyberattacks Against U.S. Corporations Are on the Rise
People

192.168.0.23:43987 → 203.45.65.201:1433 SQL Injection Attack 23Mar10 1930:003 user=jones
Roles and Responsibilities

- Level-1 and Level-2 Analysts
- Operations Lead
- Incident Handler
- SEIM Engineer
- Content Developer
- SOC Manager

Staffing Models

- Establishing coverage
- Determining the right number of resources
  - 8x5 = Min 2 Analyst w/ on-call
  - 12x5/7 = Min 4-5 Analysts w/on-call
  - 24x7 = Min 10-12 Analysts
- Finding the right skills
- Ensuring on-shift mentoring
- Continuous improvement
  - Resource Planning

- Security Device Engineers
- System Administrators
- Network Administrators
- Physical Security
### Training Plan

Listed below are the training modules, by week, to be completed by all analysts in the SOC. As part of Wiki training, analysts should create their own Training Plan Tracking page in the Wiki to keep track as they progress through this training.

#### Week 1
SOC Training Modules - SOC Training Overview
- SOC Training Modules - General Information Technology
- SOC Training Modules - Attacker Techniques
- SOC Training Modules - Defensive Methods
  - General Security - Reconnaissance: Activity

#### Week 2
SOC Training Modules - ArcSight Introduction & Components
SOC Training Modules - ArcSight Real-Time Detection and Analysis
  - ArcSight Event Correlation Whispers
- ArcSight Filter Exercises: How To Activity
- ArcSight Active List Exercises: How To Activity
- ArcSight Rule Exercises: How To Activity
- ArcSight Integration Command Exercises: How To Activity
- General Security - Exploit: General Security - Exploit Exercise
- General Security - Privilege Escalation: General Security - Privilege Escalation Exercise

#### Week 3
SOC Training Modules - ArcSight ESM Reporting and Logger Searching
  - ArcSight Query Exercises: How To Activity
  - ArcSight Report Exercises: How To Activity
  - ArcSight Trend Exercises: How To Activity
  - ArcSight Query Viewer Exercises: Activity
  - ArcSight Dashboard Exercises: How To Activity
  - General Security - Snort: General Security - Snort IOS Exercise
  - General Security - Packet Analysis: General Security - Packet Analysis Exercise

#### Week 4
Research and Present Topic
Wiki Review (Operations Section)
  - General Security: Malware General Security - Packet Analysis Exercise

---

### Training
- Information security basics
- On-the-job training
- SEIM training
- SANS GCIA and GCIH

### Career development
- Avoiding burnout
- Providing challenges
- Outlining career progression
  - Exactly how do I get from level 1 to level 2 to lead, etc
- Skill assessments
- Certifications
Process & Procedure

Operational
- Call Out
- Case Management
- Event Handling
- Monitoring
- On-boarding
- Shift Log
- Shift Turn Over
- Triage

Analytical
- Event Analysis
- Incident Response
- Reporting
- Research
- Threat Intelligence

Business & Technology
- Access Management
- Architecture
- Compliance
- DR/BCP
- Process Improvement
- Use Cases
### Microsoft SharePoint

**Pro**
- Approved by Policy
- Already deployed, supported both internal & by Microsoft
- Integrates with Active Directory & MS Office
- Allows for Calendars, Task Assignment, Notifications, Document Revision Tracking

**Con**
- Complicated to use
- Typically hard to find information (search)
- Not very flexible
- No real revision control

### File Shares

**Pro**
- Everyone has MS Office
- Everyone knows how to use a file share
- Does not require specific technology knowledge

**Con**
- Cluttered
- Overlap of information
- Nearly impossible to search for information
- Requires someone in charge of upkeep
- No revision control

### Wiki

**Pro**
- Open Source
- Editor utilizes Markup Language (HTML-like)
- Easy to Search
- Malleable
- Revision Control
- Plugins allow extensive customization

**Con**
- Open Source
- Not Vendor supported
Workflows

- Event
- Incident
- Case
- SOC
- Departmental
- Organizational
Metrics

How many events are coming in?
- Raw Events
- How many data endpoints are collected/monitored
- How many different types of data
- How many use cases

Further defined
- Per hour/day/week/month
- Per analyst
- Per hour of day/ per day of week
- Incident/ case category/ severity

What is coming out?
- Correlated Events
- Incidents/ Cases

How quickly are things handled?
- Event recognition
- Event escalation
- Event resolution
Maturing

- Understand the 80/20 rule
- Leverage metrics
- Expand senior leader dashboard view
- Institute CMM methodology
- Monitor organizational health
- Increase complexity
According to the book *Pragmatic Security Metrics – Applying Metametrics to Information Security*, an information security version of the Capability Maturity Model (CMM) looks loosely like this:

“**Level 1: Ad hoc:** information security risks are handled on an entirely informational basis. Processes are undocumented and relatively unstable.

**Level 2: Repeatable but intuitive:** there is an emerging appreciation of information security. Security processes are not formally documented, depending largely on employee’s knowledge and experience.

**Level 3: Defined process:** information security activities are formalized throughout the organization using policies, procedures, and security awareness.

**Level 4: Managed and measurable:** information security activities are standardized using policies, procedures, defined and assigned roles and responsibilities, etc., and metrics are introduced for routing security operations and management purposes.

**Level 5: Optimized:** Metrics are used to drive systematic information security improvements, including strategic activities.”

*Brotby & Hinson, 2013 p. 47

CMM – Capability Maturity Model is registered to Carnegie Mellon University
Rocking It

Preparation

Identification

Containment

Eradication

Recovery

Lessons Learned

Lessons Learned
Questions
Thank you!