

# 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

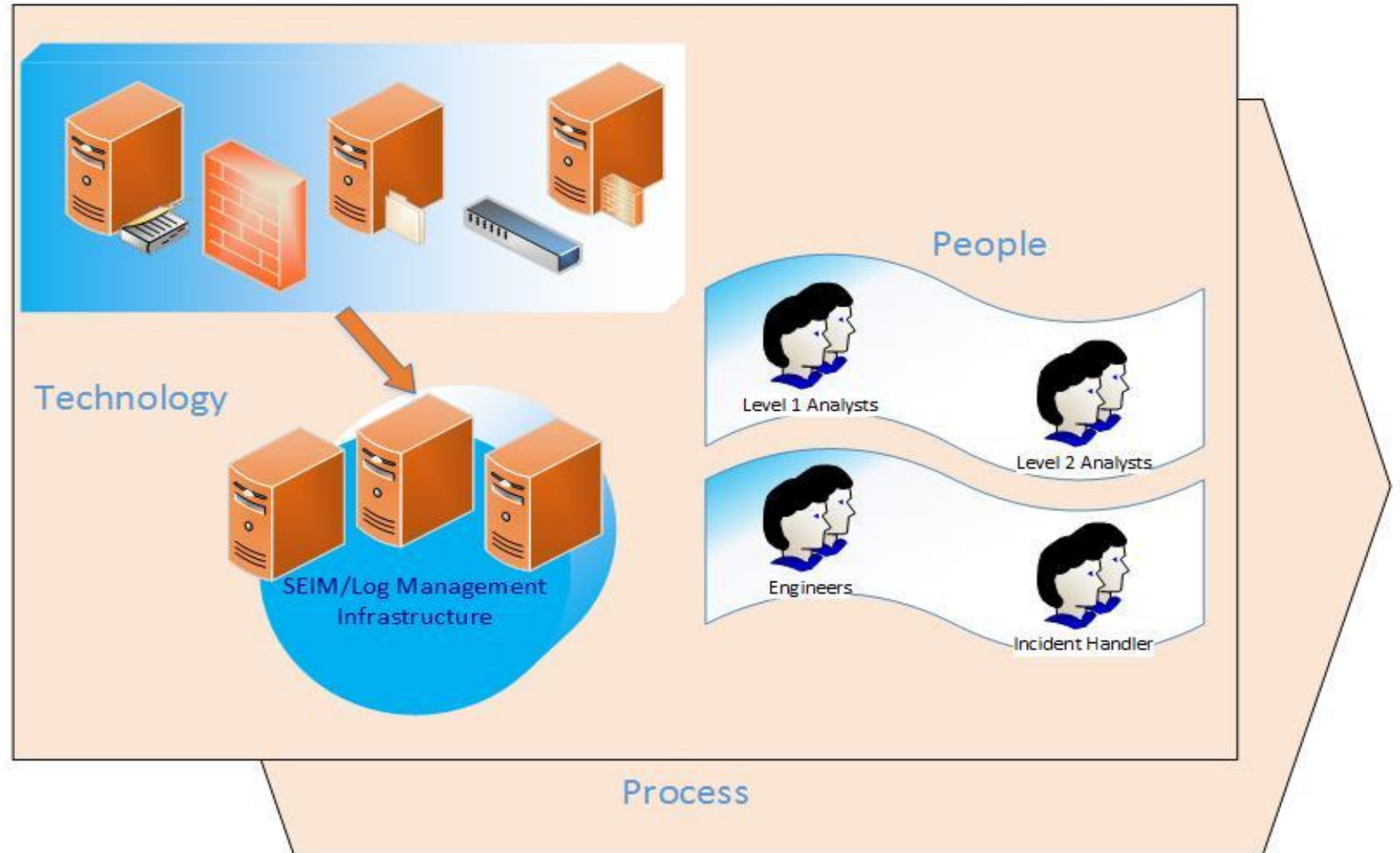
To be or  
Not to be...

- 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



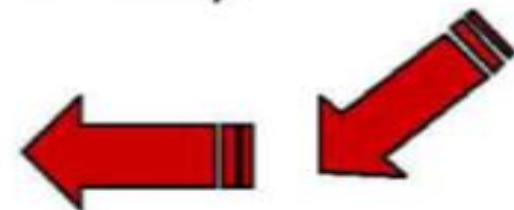
McAfee ePO

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

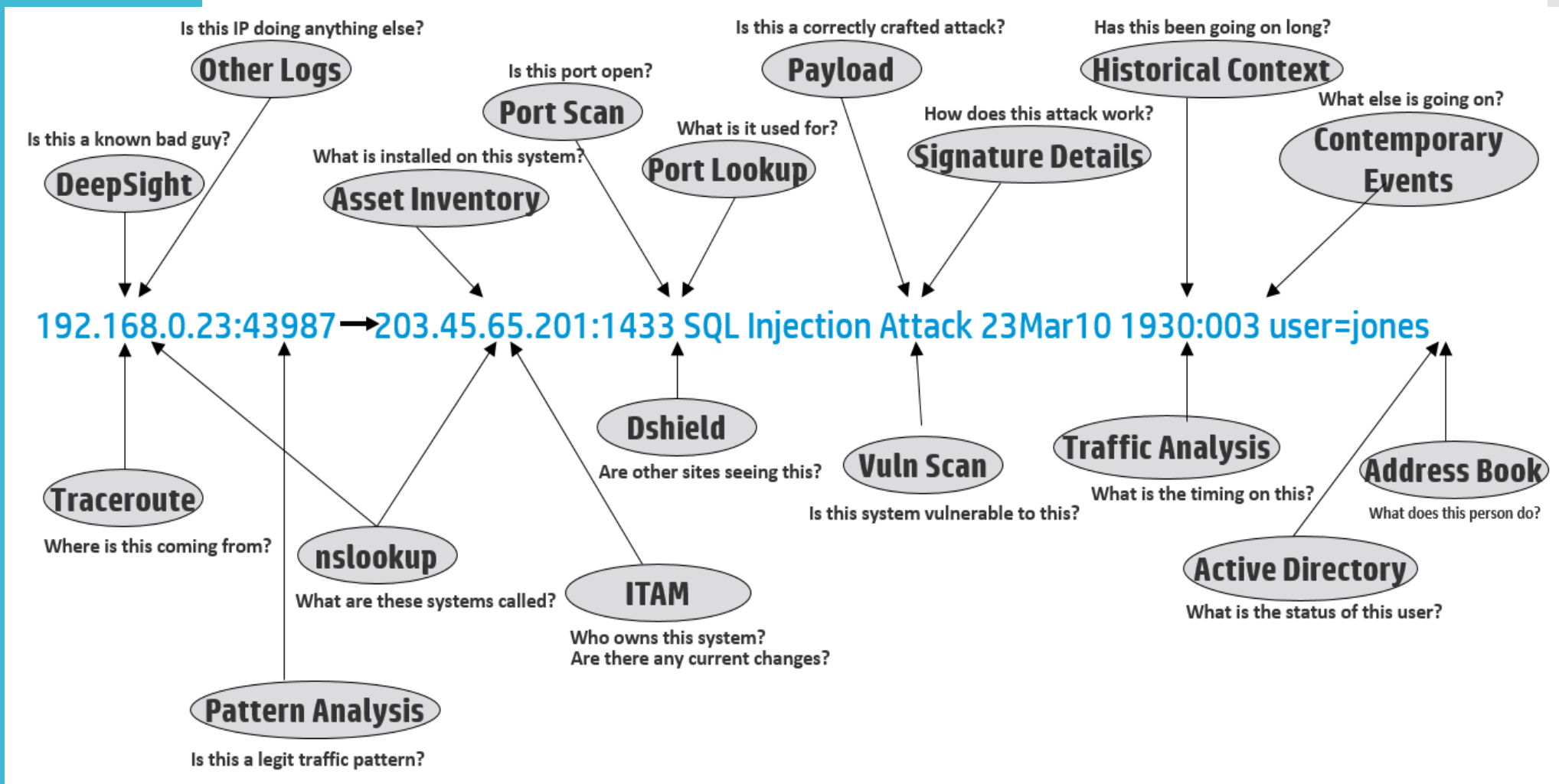
Microsoft's Patch Tuesday Leaves Out Crucial Internet Explorer Fix



Adobe Data Breach Exposes Military Passwords

Cyberattacks Against U.S. Corporations Are on the Rise

# People



## Roles and Responsibilities

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

- 
- Security Device Engineers
  - System Administrators
  - Network Administrators
  - Physical Security

## 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



## 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.

<b>Week 1</b>	<a href="#">SOC Training Modules - SOC Training Overview</a>	
	<a href="#">SOC Training Modules - General Information Technology</a>	
	<a href="#">SOC Training Modules - Attacker Techniques</a>	
	<a href="#">SOC Training Modules - Defensive Methods</a>	
	General Security - Reconnaissance:	<a href="#">Activity</a>
<b>Week 2</b>	<a href="#">SOC Training Modules - ArcSight Introduction &amp; Components</a>	
	<a href="#">SOC Training Modules - ArcSight Real-Time Detection and Analysis</a>	
	<a href="#">ArcSight Event Categorization Whitepaper</a>	
	ArcSight Filter Exercises: <a href="#">How To</a>	<a href="#">Activity</a>
	ArcSight Active List Exercises: <a href="#">How To</a>	<a href="#">Activity</a>
	ArcSight Rule Exercises: <a href="#">How To</a>	<a href="#">Activity</a>
	ArcSight Integration Command Exercises: <a href="#">How To</a>	<a href="#">Activity</a>
	General Security - Exploit:	<a href="#">General Security - Exploit Exercise</a>
	General Security - Privilege Escalation:	<a href="#">General Security - Privilege Escalation Exercise</a>
<b>Week 3</b>	<a href="#">SOC Training Modules - ArcSight ESM Reporting and Logger Searching</a>	
	ArcSight Query Exercises: <a href="#">How To</a>	<a href="#">Activity</a>
	ArcSight Report Exercises: <a href="#">How To</a>	<a href="#">Activity</a>
	ArcSight Trend Exercises: <a href="#">How To</a>	<a href="#">Activity</a>
	ArcSight Query Viewer Exercises:	<a href="#">Activity</a>
	ArcSight Dashboard Exercises: <a href="#">How To</a>	<a href="#">Activity</a>
	General Security: Snort	<a href="#">General Security - Snort IDS Exercise</a>
	General Security: Packet Analysis	<a href="#">General Security - Packet Analysis Exercise</a>
<b>Week 4</b>	<a href="#">Research and Present Topic</a>	
	<a href="#">Wiki Review (Operations Section)</a>	
	General Security: Malware	<a href="#">General Security - Packet Analysis Exercise</a>

## 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

# Documentation Repository Choices

## 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

---

## 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

## 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

## August 2012 Log

### Navigation

[July2012Log](#) [September2012Log](#)

- [ShiftLogTemplateDays](#)

### Daily List View

Day	Day of Week	Day	Day of Week
<a href="#">Aug01Day</a>	Wednesday	<a href="#">Aug17Day?</a>	Friday
<a href="#">Aug02Day</a>	Thursday	<a href="#">Aug20Day?</a>	Monday
<a href="#">Aug03Day</a>	Friday	<a href="#">Aug21Day?</a>	Tuesday
<a href="#">Aug06Day</a>	Monday	<a href="#">Aug22Day?</a>	Wednesday
<a href="#">Aug07Day</a>	Tuesday	<a href="#">Aug23Day?</a>	Thursday
<a href="#">Aug08Day</a>	Wednesday	<a href="#">Aug24Day?</a>	Friday
<a href="#">Aug09Day</a>	Thursday	<a href="#">Aug27Day?</a>	Monday
<a href="#">Aug10Day</a>	Friday	<a href="#">Aug28Day?</a>	Tuesday
<a href="#">Aug13Day?</a>	Monday	<a href="#">Aug29Day?</a>	Wednesday
<a href="#">Aug14Day?</a>	Tuesday	<a href="#">Aug30Day?</a>	Thursday
<a href="#">Aug15Day?</a>	Wednesday	<a href="#">Aug31Day?</a>	Friday
<a href="#">Aug16Day?</a>	Thursday		

[Edit](#)

### Navigation

[< PREVIOUS\\_SHIFT](#) [NEXT\\_SHIFT > ?](#)

 NEVER create shiftlog topics from this page!!

[Check In/Out Procedures](#) | [Shift Log Management](#)

[Daily Stand-up Meeting](#)

### ARCSIGHT Cases

Time	New or Existing Case	Case ID	Case Name	Callout?	Brief Description	Ticket Type	Incident Type	Action Required by Next Shift	Created By
------	----------------------	---------	-----------	----------	-------------------	-------------	---------------	-------------------------------	------------

[Edit](#)

<Case Name should be an EXACT match to the case name as listed in ArcSight. >

### New HPSM Problem Tickets

Time	Ticket No.	Priority	Team Assigned	Brief Description
------	------------	----------	---------------	-------------------

[Edit](#)

### Shift Log Entries

Time	Log Entry	By
------	-----------	----

[Edit](#)

### Filter Requests & Action Items

[More...](#)

### Analyst Status

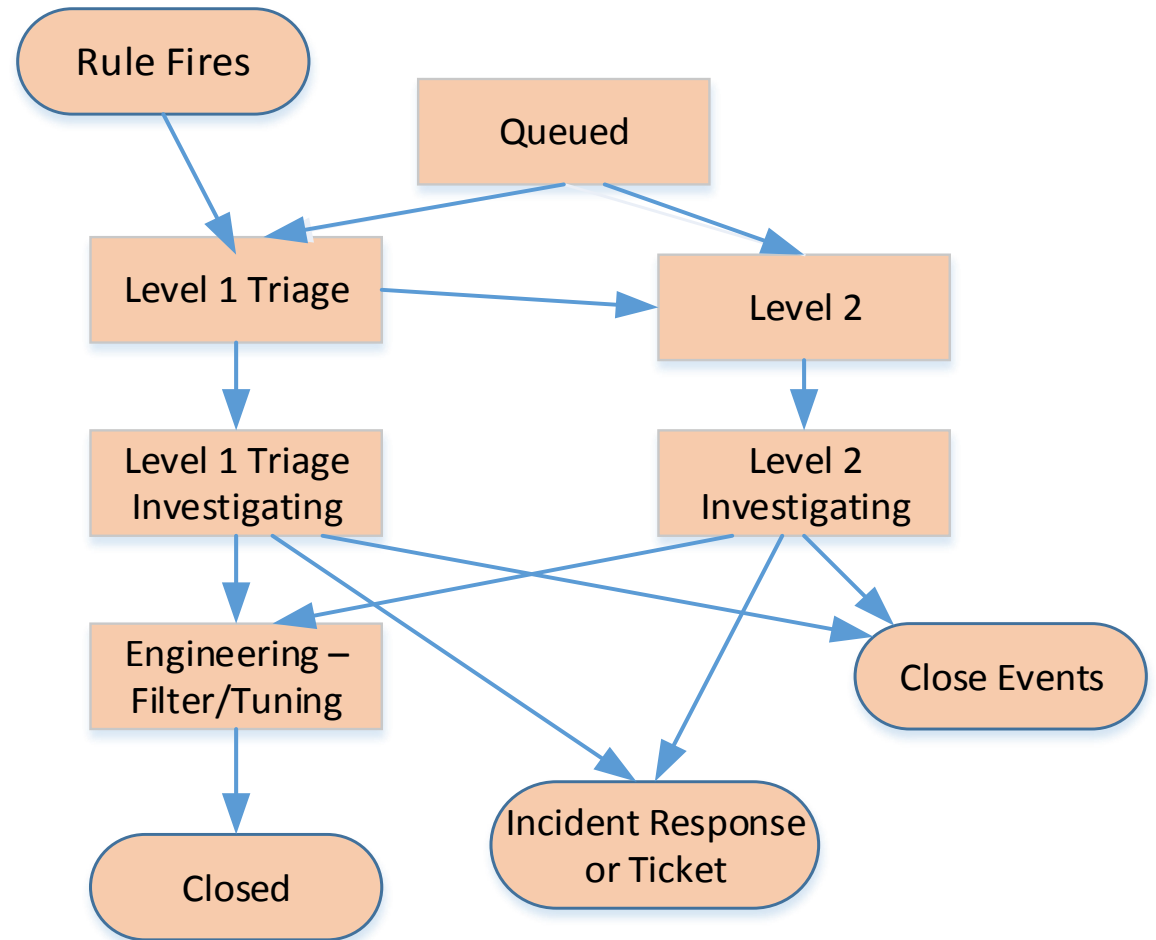
Date/Time	Analyst	Status
-----------	---------	--------

[Edit](#)

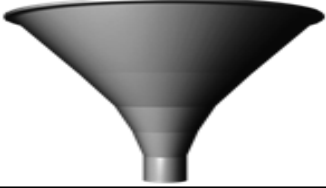
### Shift Change Signatures

# Workflows

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



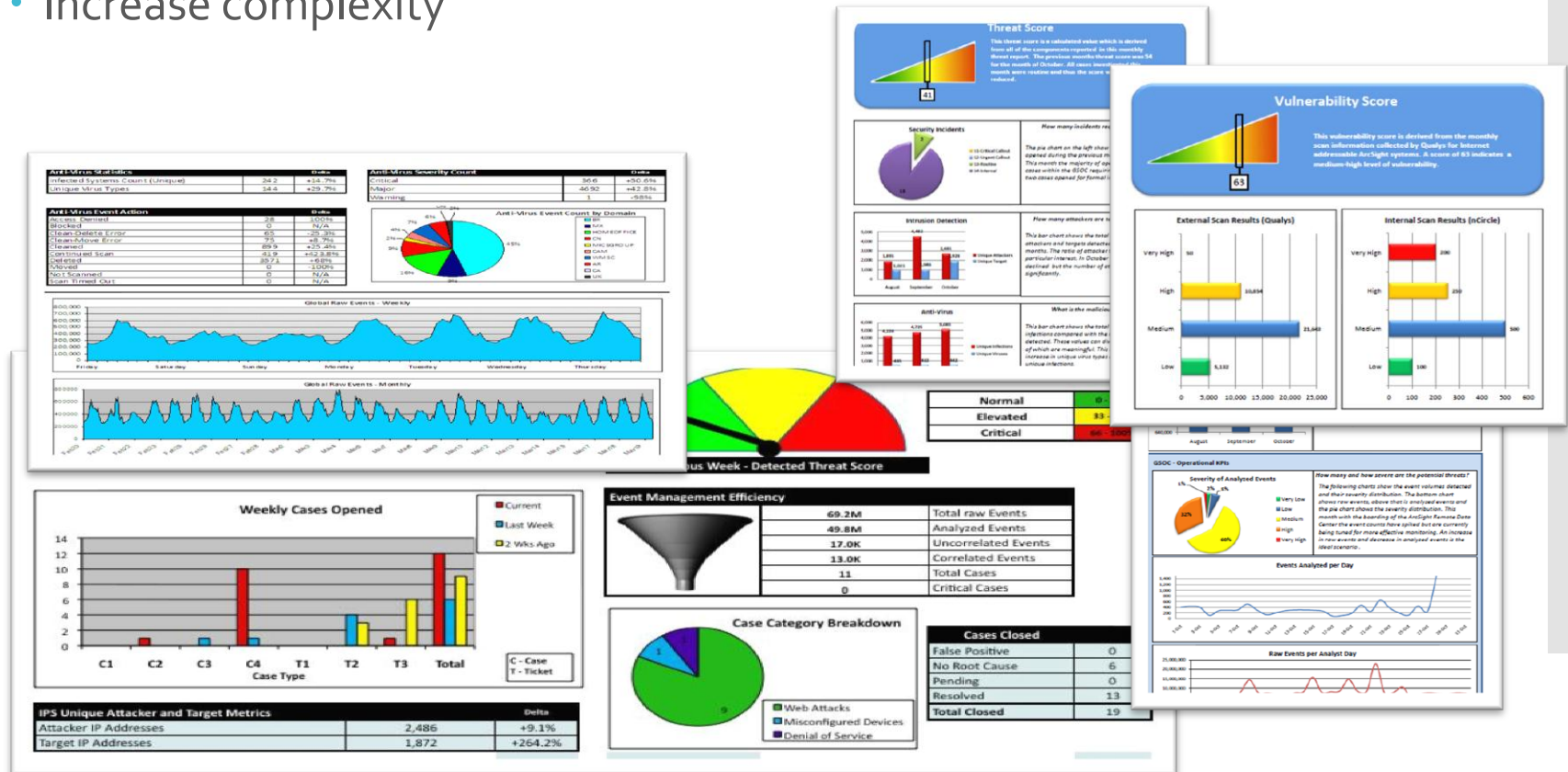
# Metrics

Event Management Efficiency		
	100 Million	Total Base (Raw) Events
	10 Million	Events Analyzed (Aggregated)
	25,000	Total Events of Interest (Correlated)
	750	Correlated Events of Interest (Console/Actionable)
	10	Cases Opened
		Critical Cases

- 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
- What is coming out?
  - Correlated Events
  - Incidents / Cases
- How quickly are things handled?
  - Event recognition
  - Event escalation
  - Event resolution
- Further defined
  - Per hour/day/week/month
  - Per analyst
  - Per hour of day/ per day of week
  - Incident / case category / severity

# Maturing

- Understand the 80/20 rule
- Leverage metrics
- Expand senior leader dashboard view
- Institute CMM methodology
- Monitor organizational health
- Increase complexity



# CMM Example

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.

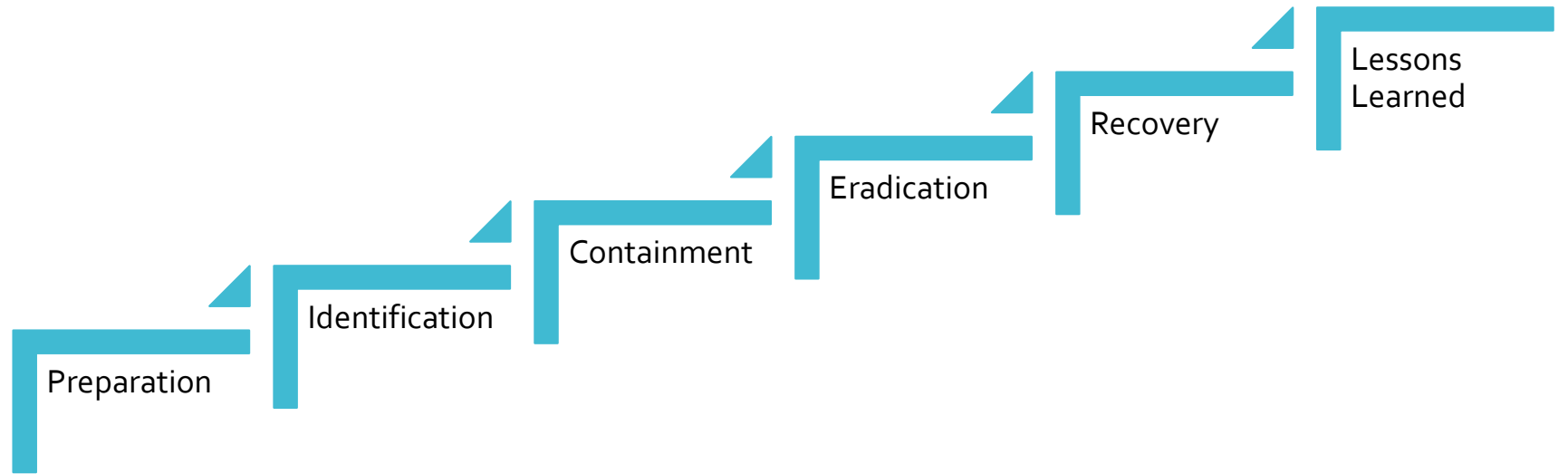
*Level 5: Optimized:* Metrics are used to drive systematic information security improvements, including strategic activities.”

\*Brotby & Hinson, 2013 p. 47

CMM – Capability Maturity Model is registered to Carnegie Mellon University



# Rocking It



Questions

Thank you!