How to build a successful SOC

Marcel Hoffmann, Manager
Cyber Defense Center Operations
Agenda

What is the Cyber Defense Center?

The challenge

Our solution
- Technology
- People
- Process

Lessons learned
What is the CDC?

HP’s internal Security Operation Center

The biggest test environment for HP security technologies

A live showcase for customers and partners
What is the CDC?
The challenge
SOC Engagement Matrix

- Cobble
- Build
- Rebuild
- Optimize

Non-existing
Reactive
Pre-existing
Proactive
Challenges

**Build ArcSight infrastructure**
In 9 months
- Sustain 3 billion EPD and more
- Fulfil HA/DR requirements
- Ready for compliance

**Hire and train 16 analysts**
In 3 months
- Develop training program
- Get everybody GCIA certified

**Complete physical construction**
In 6 months
- Design state-of-the-art watch floor
- Allow customer briefings

**Start 24x7 operations**
By November 2013
- Perform security monitoring
- Operate security mailbox and hotline
Our solution
Security Operations

Manufacturing success stories

→ Event → Alert → Incident

Security Operation Center

Platform
- Storage
- Raw events
- Event feeds
- Threat intelligence
- Normalization/categorization

Content
- Rules
- Correlation
- False positives

Incident Mgmt
- Investigation
- Incident
- Triage
- Incident Mgmt

External departments
- R&D
- Quality assurance

Success story
Technology

Security Operation Center

→ Event → Alert → Incident

Event feeds
Threat intelligence

Raw events

Platform
- Storage
- Normalization/categorization

Content
- Rules
- Correlation

© Copyright 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.
3 phase approach

- Detect insider threat
- Detect fraud
- Gain predictable intelligence

- Archive compliance
- Reduce potential impact

- Reduce attack surface
- Leverage threat intelligence

**SOC 3.0**
Secure the business

**SOC 2.0**
Secure the application

**SOC 1.0**
Secure the perimeter
ArcSight architecture

Global ESM Tier
- ESM Global Tier
- StoreEasy 5530 (NAS)
- L7500 Logger
- Local F5s
- Lancope Flow Replicators

Correlation ESM Tier
- ESM Correlation Tier

Relay Connector Tier
- Relay- and Syslog Connectors

API Connector Tier
- Trade or Hosted Data Centers
- API Connector Server
- MPLS
- VRF Tunnel

Active Stack
- Datacenter A
- Global ESM Tier
- Correlation ESM Tier
- Compliance Tier
- BU Stacks

Standby Stack
- Datacenter B
- Global ESM Tier
- Correlation ESM Tier
- Compliance Tier
- BU Stacks

Global Services Load Balancing (GSLB)

Remote Sites
- HP MPLS/Backbone
DC-DC
People

Security Operation Center

Platform - Platform Engineer
Content - Content Engineer

Incident Mgmt
- Incident Responder
  - Level-1 Analyst
  - Level-1 Analyst

Manager
- Level-2 Analyst

Event ➔ Alert ➔ Incident
Staffing

18+4 Intrusion Analysts
24x7 coverage, 10 hours/shift, 3 shifts/day

7 Incident Responders

6 Dedicated Senior Engineers

3 Managers

1 Senior Department Manager

Certifications held by CDC staff:

- SANS GCIA
- SANS GCFW
- SANS GCFE
- SANS GCIH
- CISSP
- CCNA
- AESA
- AEIA

Senior CDC staff have over a combined 80 years InfoSec experience

Extensive, customized 3-month training tailored to analysts’ strengths
Shift schedule

**Early shift**
- 3x L1
- 5:00 – 15:00

**Mid shift**
- 3x L1
- 10:00 – 20:00

**Night shift**
- 3x L1
- 19:30 – 5:30

Rotation every two months
New shift pairing every month

*Purple = Overlap time*
Hiring and training

Candidate backgrounds
• College graduates
• Administrators
• Tier-2/Tier-3 support

Focused on the analytical mindset

Analyst training
• Technical knowledge
• Tacit knowledge transfer
• Shadowing

Emphasis on individual training
Process framework

16 processes
40+ procedures

Subtle event detection
Incident management
Intrusion analysis
Reporting

Event management
Daily operations
Training

Process improvement
Metrics

BC/DR
Compliance

Business
The effort to run a security operation as a business - finance, metrics, service levels, etc.

Technology
Technical details associated with the technology deployment, configuration and architecture

Analytical
The intelligence and discipline used to collect information and use it to determine the discrete risk to an organization

Operational
The daily tasks and tempo associated with effective security operations

Service Management
Business Unit On-boarding

Design
Configuration management
System administration

Analytical Process
Operational Process
Technology Process
Business Process
Business Extended
Reporting and metrics

Security Operation Center

Event → Alert → Incident

Platform
- Storage
- Rules
Content
- Correlation
- Incident
Incident Mgmt
- Investigation
- R&D
- Quality assurance
External departments

Success story

Raw events
- Security systems
- Threat intelligence
- False positives
- Normalization/categorization

Content
- Rules
- Correlation
- Incident
- Triage
- Investigation

Platform
- Storage
- Rules
- Correlation

False positives
Lessons learned
Technology

Lessons learned

Own the whole stack
• Use appliances where possible
• Do not use standard builds
• Start with the deployment immediately

Minimize your number of ESM servers
• Cross-correlation between ESM difficult
• Content synchronization difficult
• Avoid multi-tier architecture as long as possible

Do not forget compliance
• ArcSight is an important part of audits
• Incorporate compliance requirements from the start
• Consider extended data retention requirements
People

Lessons learned

Prefer contract-to-hire for analysts
• Start with experienced analysts
• Extends the retention period

ArcSight Engineers are a critical hire
• Essential position already in the beginning
• 2-5 years of experience required

Maximize analyst retention
• Encourage participation
• Create a career path
• Give performance feedback

Continuous training
• Use shift overlaps for weekly training
• Develop your own training
Process

Lessons learned

Define a mission statement
• Clear statement to avoid “feature creep”
• Avoid secondary/tertiary tasks

Measure success
• Document success stories
• Show progress to leadership
• Perform maturity audits

Facilitate communication
• Daily or weekly news summaries
• Persistent chat rooms
• Solid shift turnover procedures

Keep feedback loops intact
• Analyst feedback important for content tuning
• Analysis and case quality feedback
• Threat intel fidelity feedback
Conclusion

How to make it successful

Gain attention
Avoid gaps in the assembly line
Measure quantitative and qualitative KPIs
Make it “their” SOC
For more information

Attend these sessions

• BB3055 - 5G/SOC: How the world's most advanced SOCs are leading the way

• BB3269 - Analysts assemble! Tips for successful security analyst recruitment, assessment, and retention

After the event


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

**Session** BB3270  **Speaker** Marcel Hoffmann

Please fill out a survey.

Hand it to the door monitor on your way out.

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