Building a Cyber Security Operations Center

Kevin Charest, Chief Information Security Officer, U.S. Department of Health and Human Services
Allison Miller, Senior Director of InfoSec Response Team, UnitedHealth Group
Damir Matanic, Senior Manager, Information Security Threat Response, Blue Cross and Blue Shield of IL, TX, NM, OK, MT
Tom Baltis, Deputy Chief Information Security Officer, Blue Cross and Blue Shield of IL, TX, NM, OK, MT
Advancing Agency Security Operations Overview

- Security Operations Considerations
- Security Ops Components
- Advancement through Optimization
- CSO In Motion
- Recommendations
Security Operation Considerations

- Technical Capabilities
  - IT Operations
  - Security Engineering

- Business
  - Resources
  - Internal Obstacles
  - Internal Support
  - Contracting
  - Budget
Security Operation Components

Traditional SOC/CSIRC Components:

- Security Monitoring
  - Intrusion Detection/Prevention Systems
  - Anti-Virus
  - Data Loss Prevention
  - Vulnerabilities
  - Incident Tracking
- Vulnerability Management
  - Vulnerability Mitigation
- Incident Management
- Communications and Reporting

- Event and incident investigations
- Incident Handling
  - Incident Analysis
  - Incident Response
- Vulnerability Handling
  - Vulnerability Analysis
  - Vulnerability Response
- Forensics Analysis
  - Evidence Handling
  - Evidence Analysis
- Penetration Testing

Components are Agency specific.
FOC and Optimization

Goal: Advancement through Optimization

In an effort to optimize operations, we conducted a gap analysis to develop recommendations.

- Where Strategy and Tactics Converge. This approach promotes:
  - Risk based decision making.
  - Prioritizes and resolves security deficiencies.
  - Creates a security foundation with measurable security improvement.

- We wanted Strategic and Tactical Recommendations to drive momentum.
HHS Cybersecurity Operations Momentum

Develop plan and focus intensity.

1. Identify issues: service goals, objectives, resources.
2. Prioritize top 3-5 issues and develop a timeline for each.
3. Clearly articulate the achievements to the program.
4. Define tasks with descriptions that need immediate execution.
4. CSO realigned their capabilities to services.
5. Capture how the recommendations will enhance the program.
6. Develop project plan and ensure team buy-in.
7. Strategic Recommendation Benefits
8. Strategic Recommendations
9. Tactical Recommendations
10. Service Recommendations
11. Recommendations Project Plan
12. Program Enhancements

Advancing Agency Security Operations
HHS Cybersecurity Operations In Motion

Data Sources

- OpDiv Reporting and Information Sharing
- HHS IOCs
- Mercury
- HSIN
- Closed Research
- Partner Agencies
- Open Research
- Monitoring Correlation

Processes

- Taxonomy code mapping
- Encrypt tool feed files
- Incident Handling process
- De-duplicate and whitelisting
- Department-wide Cyber IR process
- Incident Reporting (internal/external)
- Automated push of new feed files
- Scripts normalize data
- Two man rule

Real-time Monitoring

Advancing Agency Security Operations
HHS Cybersecurity Operations In Motion

- Automation of threat feeds improves our detection of nefarious activity and reduces our turn around time on notifying the OpDiv IRTs.
- Routine review of capabilities and processes drives efficiencies into normal operations that enhances our support to our customers.
- Conduct anomaly and threat research and investigations to detect OpDiv or Department-wide targeted threats.
- Maintain up to date on nation state and transnational cyber actor Tactics, Techniques, and Procedures (TTPs) used for awareness and feed into our Department-wide tool(s).
HHS Cybersecurity Operations Recommendations

Recommendations to create optimal security postures

- Conduct an analysis of your program at least once a year.
- Develop Department-wide Incident Response documentation.
- Develop Security Operations Information Sharing relationships with other Organizations.
- Fuse traditional intelligence information with security monitoring and reporting information.
- Strive to find technical efficiencies through the use of new technologies.
Questions

Kevin Charest  Ph.D., CISSP, PMP
Chief Information Security Officer
U.S. Department of Health and Human Services

Email: Kevin.Charest@hhs.gov

“Driving secure solutions through innovation and sustainable business practices”
Cyber Threat Management Capabilities
Overview and Key Lessons Learned

HITRUST 2014 Health Cyber Security Summit

Damir Matanic, Senior Manager, Information Security Threat Response
Tom Baltis, Deputy Chief Information Security Officer
Our Enterprise

Our Customers
Fourth largest US payer, serving nearly 14 Million members with $55B in annual revenue

Our Accolades
Gartner Security Innovation Award, CSO40 Award, Information Week 500

Our Strategy
Balanced market presence with group, retail, and government focus

Our People
More than 24,000 employees and contractors

Our Presence
60 office locations worldwide

Our IT Environment
Over 400 custom, COTS, cloud-based, mobile, and SOA-based business applications
Our Cyber Threat Management Program

24/7 enterprise coverage

- Close integration with Physical Security, Legal, and Compliance departments

Redundant, dedicated labs with isolated networks

Mobile device forensic capabilities

State of the art tools: Encase Enterprise, AccessData FTk, Cellebrite, FRED SC...

Nine dedicated fulltime resources

24/7 on-site monitoring

- Avg. raw security events per year: 52,000,000,000
- Avg. correlated events per year: 36,000

24/7 enterprise coverage

- Nine dedicated fulltime resources
- 24/7 on-site monitoring

Avg. raw security events per year: 52,000,000,000
Avg. correlated events per year: 36,000

Uses internal and external sources of IOC data (e.g. FS-ISAC)

- Incorporates 0-day vulnerabilities from internal risk assessments and vendor notifications
- Proof of concept implementation to measure business value

Leverages industry and cross-industry relationships, and proprietary sources and methods

Dynamic Tuning

- “Respond”
- “Tune”
- “Collect and detect”

Forensic Analysis

- “Analyze”

Security Event Analysis

- “Predict”

Incident Response
Lessons Learned

• **Design the incident investigation process to decompose the entire “kill chain”** of an incident, enabling a comprehensive set of recommendations to address vulnerabilities and control gaps that have contributed to each incident phase.

• **Develop specific response methodologies for each type of threat scenario.** This allows for a “plug and play” response that is more agile than a single, all encompassing methodology.

• **Perform live Red Team tests** of cyber threat management capabilities in addition to paper-based simulations. Tabletop exercises are insufficient to accurately evaluate the effectiveness of your capabilities.

Quick Tips: Staffing Strategy

The most effective cyber threat management organizations are staffed with dedicated teams of professionals possessing deep skills in incident response, digital forensics, executive communications and relationship building. In order to identify and select these resources, implement a rigorous, multidisciplinary interview process, and weigh work experience more heavily than certifications.
Lessons Learned Continued

• Where appropriate, deviate from conventionally held IT best practices to ensure availability of tools and preserve integrity of investigations. For example, integrating evidence collection tools with enterprise technology solutions may put evidence at risk of tampering.

• Partner with other cyber security teams to take advantage of their specialized knowledge and economies of scale. For example, leverage resources from the risk analysis and vulnerability research teams to reverse engineer malware.

• Share cyber threat knowledge within and across industries, and collaborate with your peers. The evolving threat landscape has created an environment where a single organization is no longer able to effectively manage many cyber threats.

Quick Tips: Relationships

Don’t underestimate the power of relationships in your investigations. At least 50% of your information will come from people who know and trust you. Incorporate data feeds from HR, Compliance, the helpdesk and other organizations into your threat intelligence and investigation capabilities.
Questions?