Anatomy of a Security Operations Center

By John Wang, NASA SOC (soc@nasa.gov)
Sample Problem Statement:

The Agency faces many challenges in protecting its data and IT infrastructure. The Agency is experiencing compromises on a daily basis. The threats are real and increasing, and now include sophisticated Advanced Persistent Threats.
Sample Problem Statement:

- Not responding to threats in a timely, consistent manner
- Lacking a coordinated operational, technical Agency approach to prevention, detection, and remediation
- Not following an organized system for knowledge sharing regarding threats and incidents (multiple centers are successfully hit by the same attack)
- Not having accurate incident and threat status from discovery to resolution
Goal of a SOC

- Improve the Agency’s Incident Detection and Response Capabilities
- Manages and Coordinates the Agency’s response to Cyber Threats and Incidents
- Monitors the Agency’s Cyber Security posture and reports deficiencies
- Coordinates with US-CERT and other Government and Non-Government entities
- Performs Threat and Vulnerability Analysis
- Performs Analysis of Cyber Security Events
- Maintains Database of Agency Cyber Security Incidents
- Provide Alerts and Notifications to General and Specific Threats
- Provide regular reporting to Management, Agency IT Security Officials, and Cyber Incident Responders
Sample SOC Architecture
Incident Management System

• Function
  • Continuous monitoring of Agency Incident Status & Total Life Cycle Incident Management and Tracking
  • Incident Data Sharing, Collaboration, Correlation, and Analysis
  • Improve Efficiency - Automated workflow, notification, and reporting
  • Role Based Access Control
  • Spot trends and issues
  • Root Cause Analysis
  • Searchable Database
  • Feed Threat Data to TMS
Accurate incident and threat status from discovery to resolution

Centralized incident management system for incident response

8/2/2010
24 X 7 Monitoring Staff

- Function
  - Call Center & Data Entry
  - 24x7 Monitoring (SIM, IDS, etc.)
  - Data Gathering, Correlation and Analysis
  - Triage
  - Incident Response
  - Incident Coordination & Management
Threat response in a timely, consistent manner

Agency Networks

Intrusion Detection Systems
- Packet Capture
- Event Detection

IT Security Correlation

Tier-2 Analysis

24x7 monitoring and data correlation
Threat Management Capability

• **Function**
  
  • Collect information on threats and methodology from Incidents, External Sources (Commercial, public, etc.), Partners, CI
  • Organize and correlate the information
  • Analyze the relevance of the information to the Agency
  • Determine the need and course of action
  • Act: Block; Watch; other
  • Assess the results
  • Utilize Database to Assess new Incidents
  • Provide Alerts & Notifications
Threat Management System

- **Unify Threat Management** -- Enable Consistent and repeatable threat management process.
- **Centralize and Structure Threat Database** -- Capture and consolidate vulnerabilities, malicious code and patches that affect critical technologies and processes. Centralize repository for threat and vulnerability data from trusted sources in a searchable, standards-compliant database.
- **Bring in Threat Content** -- Populate customized threat data with information from Agency’s own research, content from a commercial threat feed provider and threat advisories received via email.
- **Analyze and Refine Threat Data** -- Analyze and react to vulnerabilities and malicious code based on the impact to Agency
- **Alert Users to Emerging Threats** -- Automatically notify responsible personnel so they can proactively address emerging threats.
- **Report on Threat Levels and Activities** -- Produce real-time reports and user-specific dashboards to view threats by technology, severity, type and impact to Agency organization.
- **Validate Vulnerability Remediation** -- Reporting of activities related to threat remediation.
Threat Management System

- SOC Incident Management System (IMS)
- US-CERT/GFIRST
- Other CERTS/FIRST
- Collaborative Intelligence (ShadowServer, Cymru, etc.)
- OSPP
- OIG
- Vendors
- Commercial Alert Service (i.e. IntelliShield, DeepSight)
- Etc.

Incident Database

Identified Threats (& Vulnerabilities)

Incident Management System (IMS)

Events

- Action
- Target

Incidents

"Any real or suspected adverse event in relation to the security of computer or computer networks."

Threats

(& Vulnerabilities)

Threat Management System (TMS)

- Mitigation
- Alerting
- Analysis
- Reporting

Threat Management System (TMS)

Threat Data From Sources

Aggregation

Correlation

Analysis

Reporting

Console
Security Data Sets

SMART Action

Cyber Threat Management

SOC Synergy

Vulnerability Management

Incident Management

NASA
Incident States & Work Elements

Incident States

Open

Confirmed

Contained

Recovered

Resolved

Closed

Incident Work Elements

Detection & Reporting

Analysis, Categorization & Triage

Containment

Eradication & Recovery

Post Incident Analysis, Reporting, Actions, and Recommendations

Review
SOC Incident Response Process

States:

1. Detection & Reporting
2. Analysis, Categorization, & Triage
3. Containment
4. Eradication & Recovery
5. Post Incident
6. Review/Closeout
<table>
<thead>
<tr>
<th>Credibility</th>
<th>Capability</th>
<th>Intent</th>
<th>Opportunity/Vulnerability</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High (2)</strong></td>
<td>Information from highly reliable</td>
<td>Actors possess Expert level knowledge and extensive resources indicative of organized efforts</td>
<td>Targeted confidentiality, integrity, or availability (CIA) attack of dataset or individuals. Disruption of critical Agency mission or function.</td>
<td>Significant impact to Agency Programs, Project, Operations, People, Data, Systems, or Cost.</td>
</tr>
<tr>
<td></td>
<td>source or has been independently confirmed</td>
<td></td>
<td>Systems vulnerable to known vectors or methodology and/or available to known Actors.</td>
<td></td>
</tr>
<tr>
<td><strong>Moderate (1)</strong></td>
<td>Information from normally reliable</td>
<td>Actors possess Moderate to high levels of sophistication with moderate resources</td>
<td>Non-targeted Attacks of Agency systems affecting confidentiality, integrity, or availability (CIA) of data. E.g. web defacement, botnets, etc.</td>
<td>Moderate impact to Agency Programs, Project, Operations, People, Data, Systems, or Cost.</td>
</tr>
<tr>
<td></td>
<td>source but unconfirmed</td>
<td></td>
<td>Systems potentially vulnerable to known vectors or methodology and/or potentially available to known Actors.</td>
<td></td>
</tr>
<tr>
<td><strong>Low (0)</strong></td>
<td>Information from unreliable source</td>
<td>Actors possess Low level of sophistication with little resources required. (or Unknown)</td>
<td>“Drive by” or opportunistic attacks (or Unknown)</td>
<td>Low impact to Agency Programs, Project, Operations, People, Data, Systems, or Cost. (or Unknown)</td>
</tr>
<tr>
<td></td>
<td>or source without established history (or Unknown)</td>
<td></td>
<td>Systems not likely vulnerable to known vectors or methodology and/or not likely available to known Actors (or Unknown)</td>
<td></td>
</tr>
</tbody>
</table>
## US-CERT Incident Categories

<table>
<thead>
<tr>
<th>CAT 0</th>
<th>Exercise/Network Defense Testing</th>
<th>This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAT 1</td>
<td>Unauthorized Access</td>
<td>In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.</td>
</tr>
<tr>
<td>CAT 2</td>
<td><em>Denial of Service (DoS)</em></td>
<td>An attack that <em>successfully</em> prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.</td>
</tr>
<tr>
<td>CAT 3</td>
<td><em>Malicious Code</em></td>
<td>Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been successfully quarantined by antivirus (AV) software.</td>
</tr>
<tr>
<td>CAT 4</td>
<td><em>Improper Usage</em></td>
<td>A person violates acceptable computing use policies.</td>
</tr>
<tr>
<td>CAT 5</td>
<td>Scans/Probes/Attempted Access</td>
<td>This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.</td>
</tr>
<tr>
<td>CAT 6</td>
<td>Investigation</td>
<td>Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.</td>
</tr>
</tbody>
</table>
Incidents Per Year

Note: Not Real Data! For illustrative purposes only.
Incidents By Category

Note: Not Real Data! For illustrative purposes only.
Incidents per Center/Facility

Note: Not Real Data! For illustrative purposes only.
Tracking Incidents by Categories

- Answers When? What? (Somewhat!) and How Often?
- Does not Answer Who? What? (Complete), Where? or Why?
- Not conducive to root cause analysis.
- Fails to reveal significant trends.
Practical Questions Unanswered

1) Were there any insider threats?
2) Were there any Theft or Espionage by Nation States?
3) Did we have any Spear Phishing incidents?
4) How many Cat 1 and Cat 3 were because of client side application vulnerabilities?
5) How many laptops and PDAs were lost or stolen? Was PII or SBU or ITAR involved in any of those? How many systems had data encrypted? Do we know what data was on the systems?
6) How many incidents were result of user inadvertently going to a bad/compromised site?
7) How many systems at the agency were part of a Botnet?
8) How many instances of web defacement did we have? How did they get in?
9) Did we see any attacks from Social Networks? If so how many? Which social network?
10) Did we see any attacks on Mobile Devises?
11) How many Scareware incidents were there last year?
12) How many Cat 1 & 3s used OS vulnerabilities?
13) Which Detection Systems were most effective?
What Do We Need?

• Need a means of categorizing incidents that will allow us to answer practical questions regarding, WHO, WHAT, WHERE, WHEN, HOW, and Impact, so that we can begin to understand Why it happened:
  • Root-causes?
  • Deficiencies?
  • Motive?
  • Trends.
• To do this, we need a Taxonomy for Incidents.
Evolution of Cyber Security

- Reactive
- Proactive
- Predictive
Definitions

- **Reactive Cyber Security** - Post incident detection, analysis, notification, containment, eradication, and remediation.
- **Proactive Cyber Security** - Avoiding or opposing threats against computers and networks through understanding the situation, assessing potential impacts, and implementing deterrence based on defensive methodologies.
- **Predictive Cyber Security** -- Anticipating and predicting future threats and vulnerabilities based on strategic analysis, threat intelligence, and correlation of disparate datasets to protect the confidentiality, integrity, and availability of data and IT infrastructure.
# Cyber Security Evolution

<table>
<thead>
<tr>
<th>Reactive</th>
<th>Proactive</th>
<th>Predictive</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOC</td>
<td>Incident Response, Notification, Tracking, Analysis, Containment, Eradication, and Remediation</td>
<td>Network Vulnerability Scanning: Network, systems,</td>
</tr>
<tr>
<td></td>
<td>Incident Detection Systems (IDS)</td>
<td>Vulnerability Handling</td>
</tr>
<tr>
<td></td>
<td>System</td>
<td>Email Filtering &amp; Blocking</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DNS Sinkhole</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Threat Tracking, Monitoring, &amp; Mitigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Patch/Asset Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Situational Awareness: Log Monitoring, Event Aggregation and Correlation (SIM)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Flow/Network Behavior Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Host Based Monitoring System (HBSS): Antivirus, Firewall, Anti-Malware, Application White listing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Active Protection: Intrusion Prevention System (IPS)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Web &amp; Application Scanning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Incident Scope Analysis &amp; Remote Forensics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Content Monitoring/Data Loss Prevention</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Red Team/Blue Team</td>
</tr>
</tbody>
</table>

8/2/2010
## Staffing

<table>
<thead>
<tr>
<th>Function</th>
<th>FTE</th>
<th>Hours of Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier 1</td>
<td>3 (Augmentation to Existing Call Center)</td>
<td>24 X 7</td>
</tr>
<tr>
<td>Tier 2</td>
<td>12</td>
<td>24 X 7</td>
</tr>
<tr>
<td>Tier 3</td>
<td>2</td>
<td>Business Hours</td>
</tr>
<tr>
<td>Implementation</td>
<td>6</td>
<td>Business Hours</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>3</td>
<td>Business Hours &amp; On Call</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>26</strong></td>
<td></td>
</tr>
</tbody>
</table>
Facilities

• On the Cheap!

• State of Art!
## Cyber Security from Different Perspectives

<table>
<thead>
<tr>
<th>CIO</th>
<th>Programs &amp; Projects</th>
<th>Law Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect the Enterprise</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident Response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proactive Response to Threats</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure Availability of IT Infrastructure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Conduct Business)</td>
<td>Ensure Mission Success</td>
<td>Catch the Bad Guys!</td>
</tr>
<tr>
<td></td>
<td>(Risks Vs. Rewards)</td>
<td></td>
</tr>
<tr>
<td>Access Control (Confidentiality &amp;</td>
<td>Ensure Availability of Mission</td>
<td>Protect National Security Interests</td>
</tr>
<tr>
<td>Integrity)</td>
<td>Critical Systems &amp; Applications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protect Intellectual Property</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protect Revenue Stream</td>
<td></td>
</tr>
<tr>
<td>Regulatory Compliance &amp; Reporting</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Different Priorities -> Different Requirements -> Different Solutions**

8/2/2010
Implementation Challenges

- **Budgets** - Never enough. Original request 2X funded.
- **Time** - Rush to implement, rush to Operational Readiness
- **Training**
- **Technology** -- Complicated
- **Change** - Change is hard!
- **Staffing** - Quality Staff is hard to find, hard to retain, Don’t Settle!
- **24 X 7** - Difficult to achieve
- **Funded Tasks Vs. Expectations of SOC**
Other Challenges

• With the Threat of APT, most perimeters are simply too porous - A defense-in-depth strategy is needed more than ever! If you are just guarding/monitoring the perimeter, you will never see it coming - or going.
• Perimeters also don’t help you against insider threats.
• We must balance our resources and efforts - shift more away from perimeter only monitoring and defenses to more focus on protecting what is important within those perimeters.
• Comprehensive Defense-in-Depth is an order of magnitude more expensive than perimeter based approach!
• SOC Needs visibility down to the Host Level.
Possible Shopping Lists

• Hosts:
  • Firewalls
  • IDS/IPS
  • Data Loss Prevention
  • Behavior Based Detection
  • Anti-Spyware
  • Rogue Host Detection
  • Policy Auditor
  • Devise Control (USBs, etc.)
  • Asset Management
  • Baseline Monitoring (FDCC)
  • Application White listing
  • Patch Management
  • Remote Forensics
  • Etc.
Possible Shopping Lists

- Network
  - Log Aggregation and SIM
  - Flow Monitoring
  - Full Packet Capture
  - Next Generation Firewalls - shift from blocking IPs and Ports to controlling applications
  - Web Application Firewall
  - Web Proxy
  - Content Monitoring (Network Based DLP)
  - New IDSs - Code Behavior/ Reputation
  - Continuous Vulnerability Scanning
  - Honeypot
Possible Shopping Lists

• Other
  • SOC -- provide Incident Response, Forensics Capabilities, Threat Monitoring, Intelligence Gathering
  • Continuous Monitoring
  • Better User Training and Awareness - First line of defense: Informed Users!
  • Contingency Planning
  • Red Team/Blue Team (inc. Third Party Penetration Testing & Web/Application Testing)
  • Encryption
  • 2 Factor Authentication
  • Identify, classify, and tag what you need to protect, what are your crown jewels, what will affect your organizational viability.

• MORE FUNDING & RESOURCES!!!
Recommendations for Building a SOC

- Commitment from the highest level of management
- Don’t underbid, don’t accept less $$$ than is necessary for success.
- Focus on quality - Start with Good People!
- Don’t over consolidate - Can’t do everything, still need boots on the ground!
- Manage Expectations - Change takes time, SOC does not solve all IT Security problems.
- Partner internally and externally.
- Don’t reinvent if you don’t need to -- Get help from others who have been through it.
- Share With the community!
Conclusion:

- SOC will help your Agency/Organization deal with incidents more efficiently and effectively.
- If SOC is funded only to be REACTIVE, your incident rates will not significantly decrease!
- Passive Monitoring and Reactive SOC is a starting point...Ultimately, SOC needs to be Active, Proactive, and Predictive and be part of a Comprehensive Defense-in-Depth approach.