Anatomy of a Security Operations Center

By John Wang, NASA SOC (soc@nasa.gov)

GFirst 2010

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.

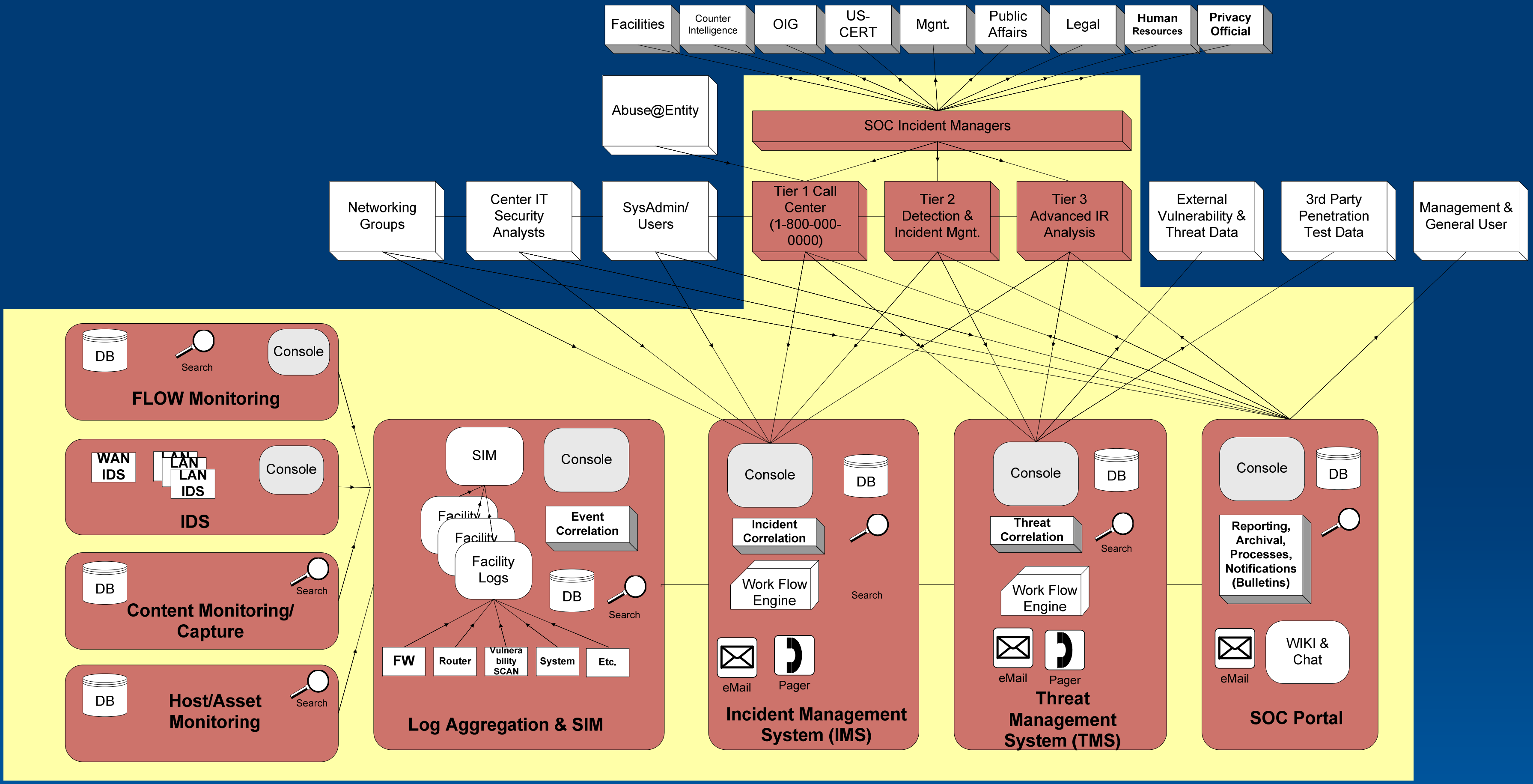
Sample Problem Statement:

- 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

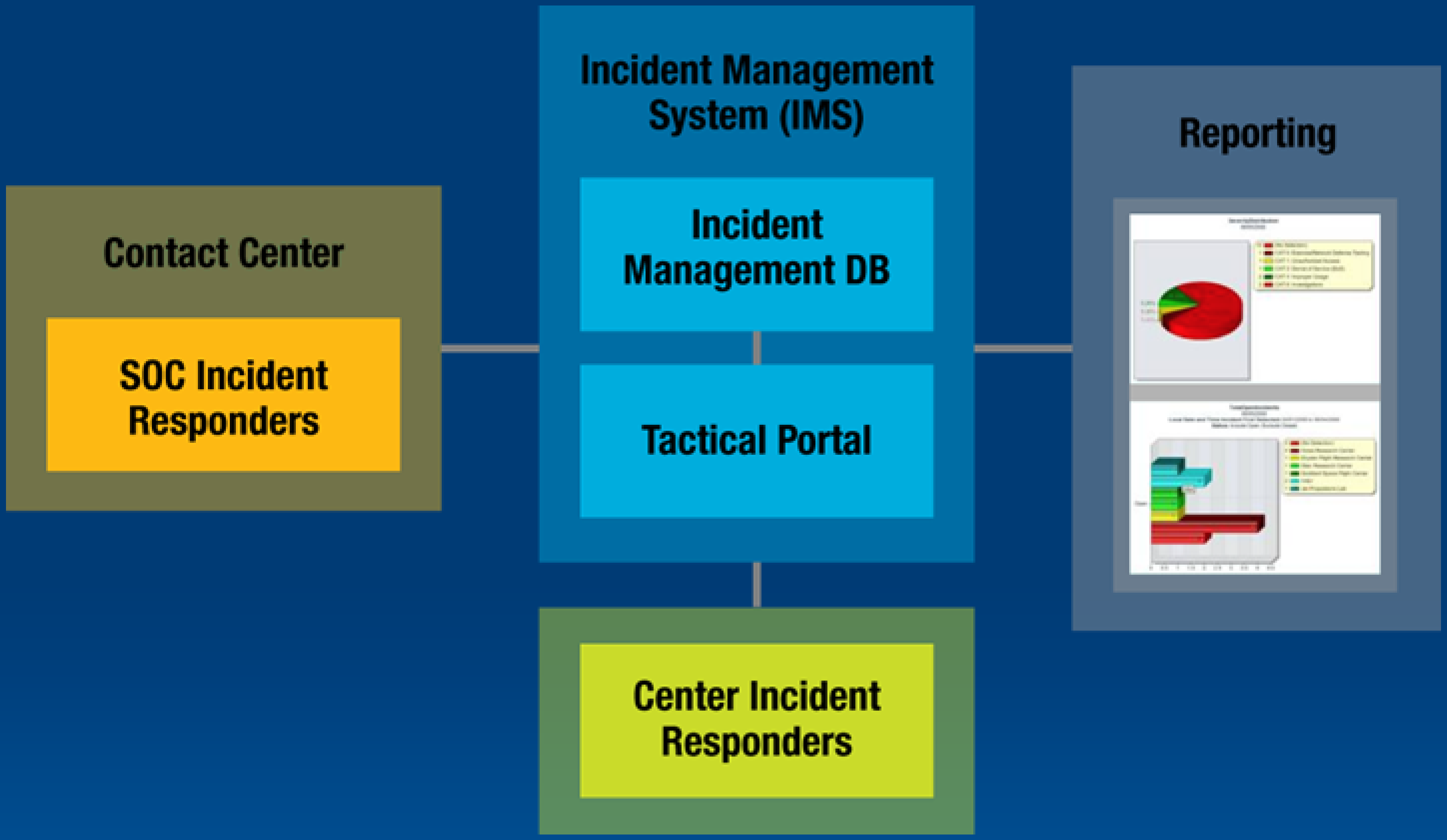
Sample SOC Architecture



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

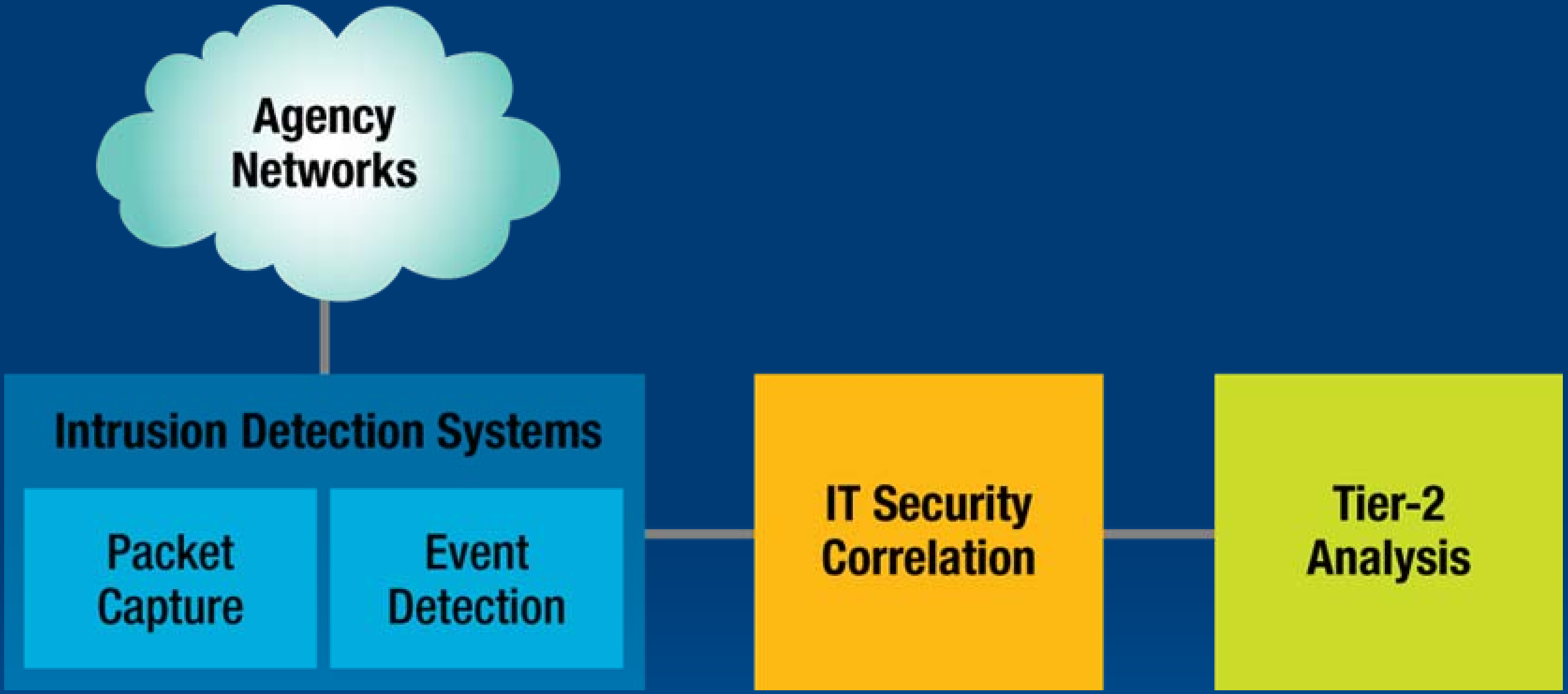


Centralized incident management system for incident response

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



24x7 monitoring and data correlation

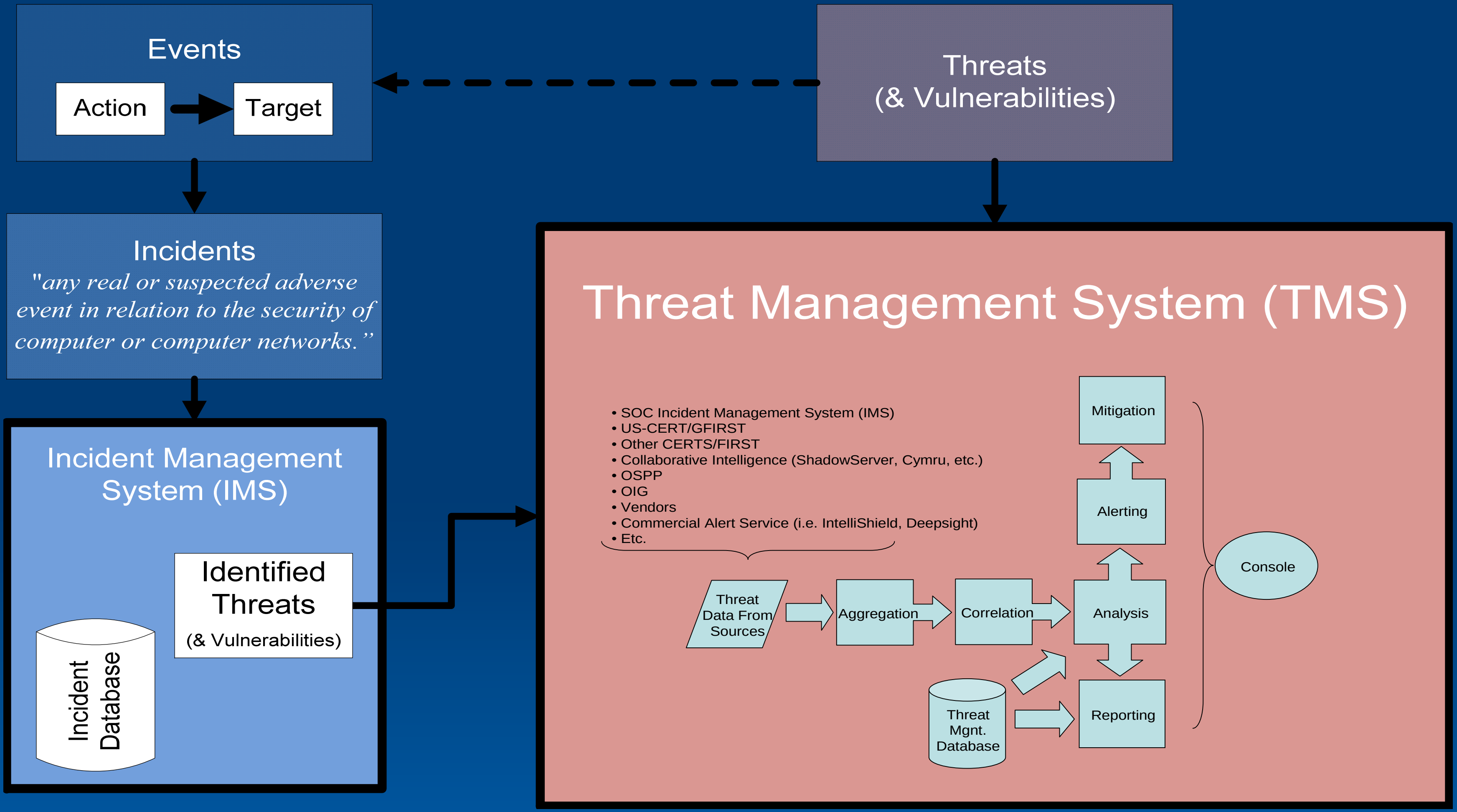
Threat Management Capability

- 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



Events

Action

Target

Threats
(& Vulnerabilities)

Incidents

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

Incident Management System (IMS)

Identified Threats

(& Vulnerabilities)

Incident Database

Threat Management System (TMS)

- 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.

Threat Data From Sources

Aggregation

Correlation

Analysis

Alerting

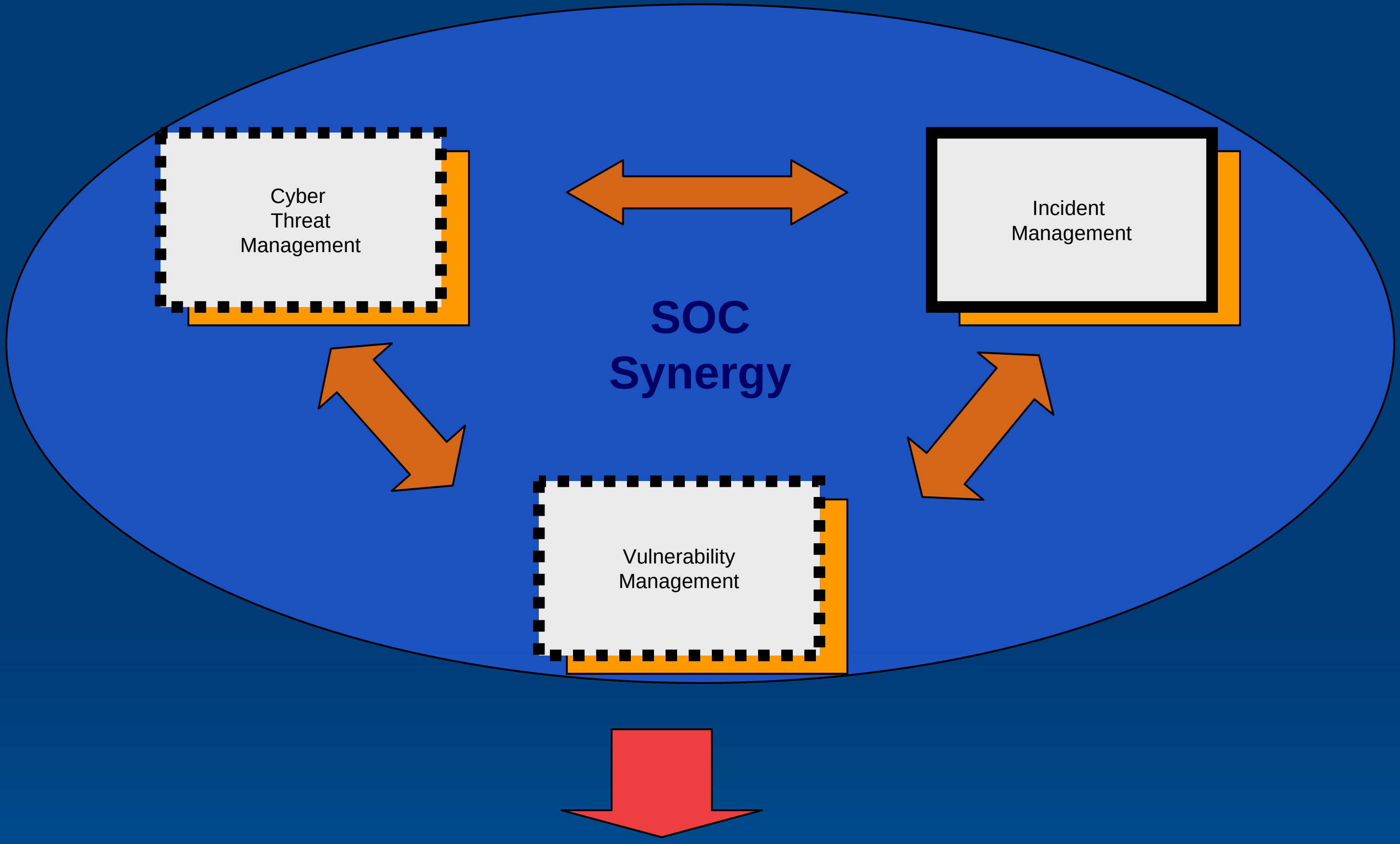
Mitigation

Reporting

Threat Mgnt. Database

Console

Security Data Sets

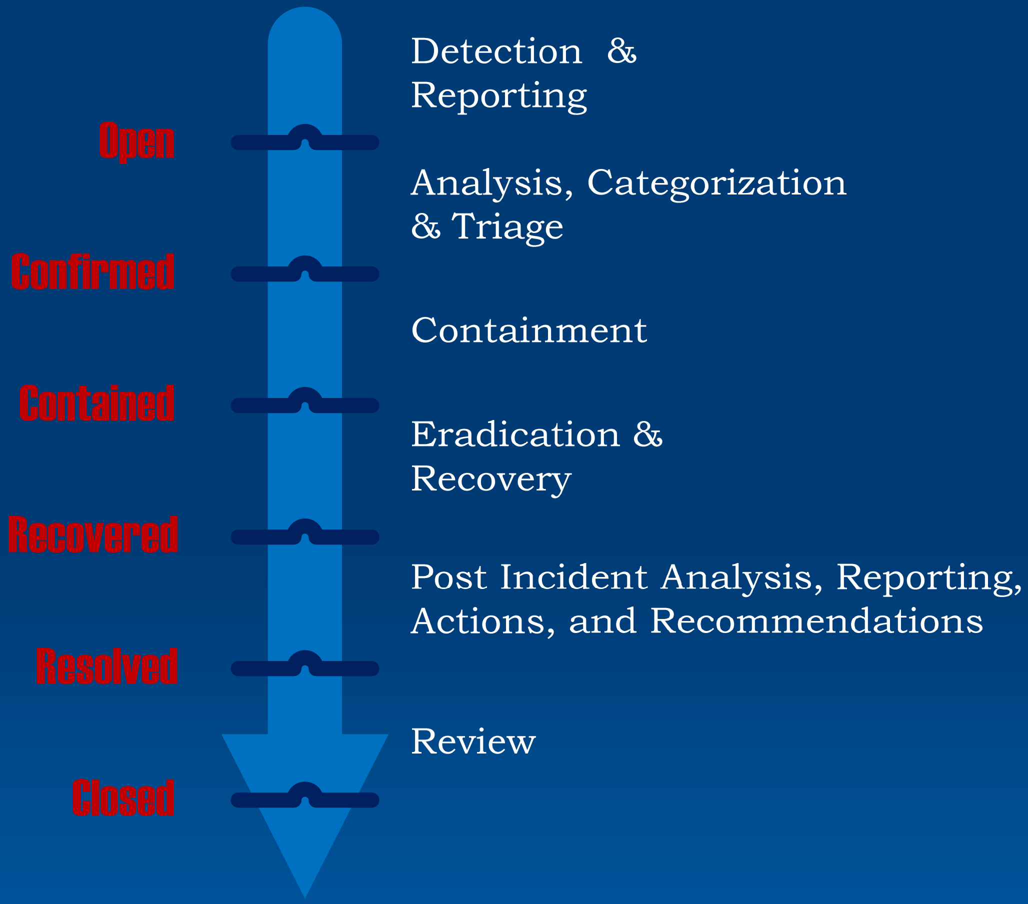


SMART Action

Incident States & Work Elements

Incident States

Incident Work Elements



Detection & Reporting

Open

Analysis, Categorization & Triage

Confirmed

Containment

Contained

Eradication & Recovery

Recovered

Post Incident Analysis, Reporting, Actions, and Recommendations

Resolved

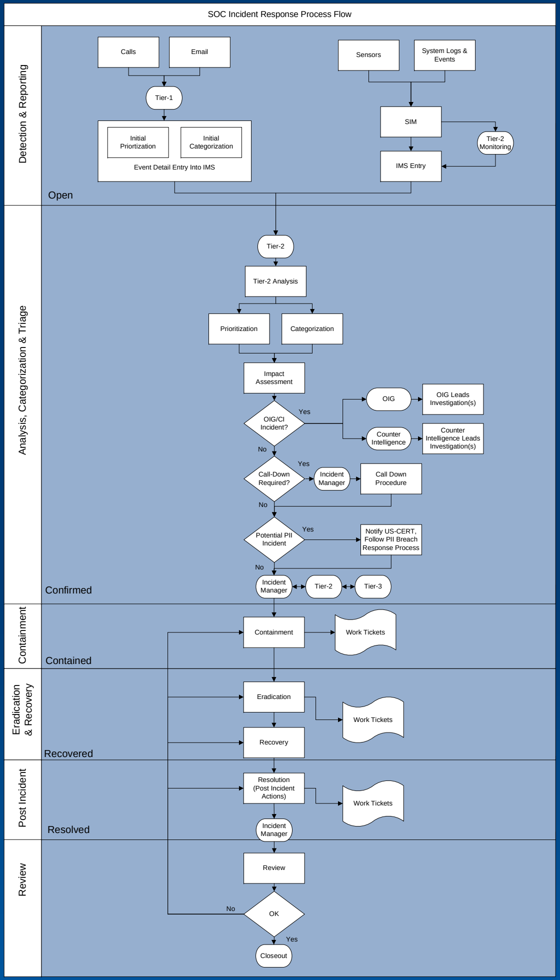
Review

Closed

SOC Incident Response Process

States:

1. Detection & Reporting
2. Analysis, Categorization, & Triage
3. Containment
4. Eradication & Recovery
5. Post Incident
6. Review/Closeout



SOC Incident Response Process Flow

Detection & Reporting

Calls
Email
Tier-1
Initial Priortization
Initial Categorization
Event Detail Entry Into IMS
Sensors
System Logs & Events
SIM
Tier-2 Monitoring
IMS Entry
Open

Analysis, Categorization & Triage

Tier-2
Tier-2 Analysis
Prioritization
Categorization
Impact Assessment
OIG/CI Incident?
Yes
OIG
OIG Leads Investigation(s)
Counter Intelligence
Counter Intelligence Leads Investigation(s)
No
Call-Down Required?
Yes
Incident Manager
Call Down Procedure
No
Potential PII Incident
Yes
Notify US-CERT, Follow PII Breach Response Process
No
Incident Manager
Tier-2
Tier-3
Confirmed

Containment

Containment
Work Tickets
Contained

Eradication & Recovery

Eradication
Work Tickets
Recovery
Recovered

Post Incident

Resolution (Post Incident Actions)
Work Tickets
Incident Manager
Resolved

Review

Review
OK
No
Yes
Closeout

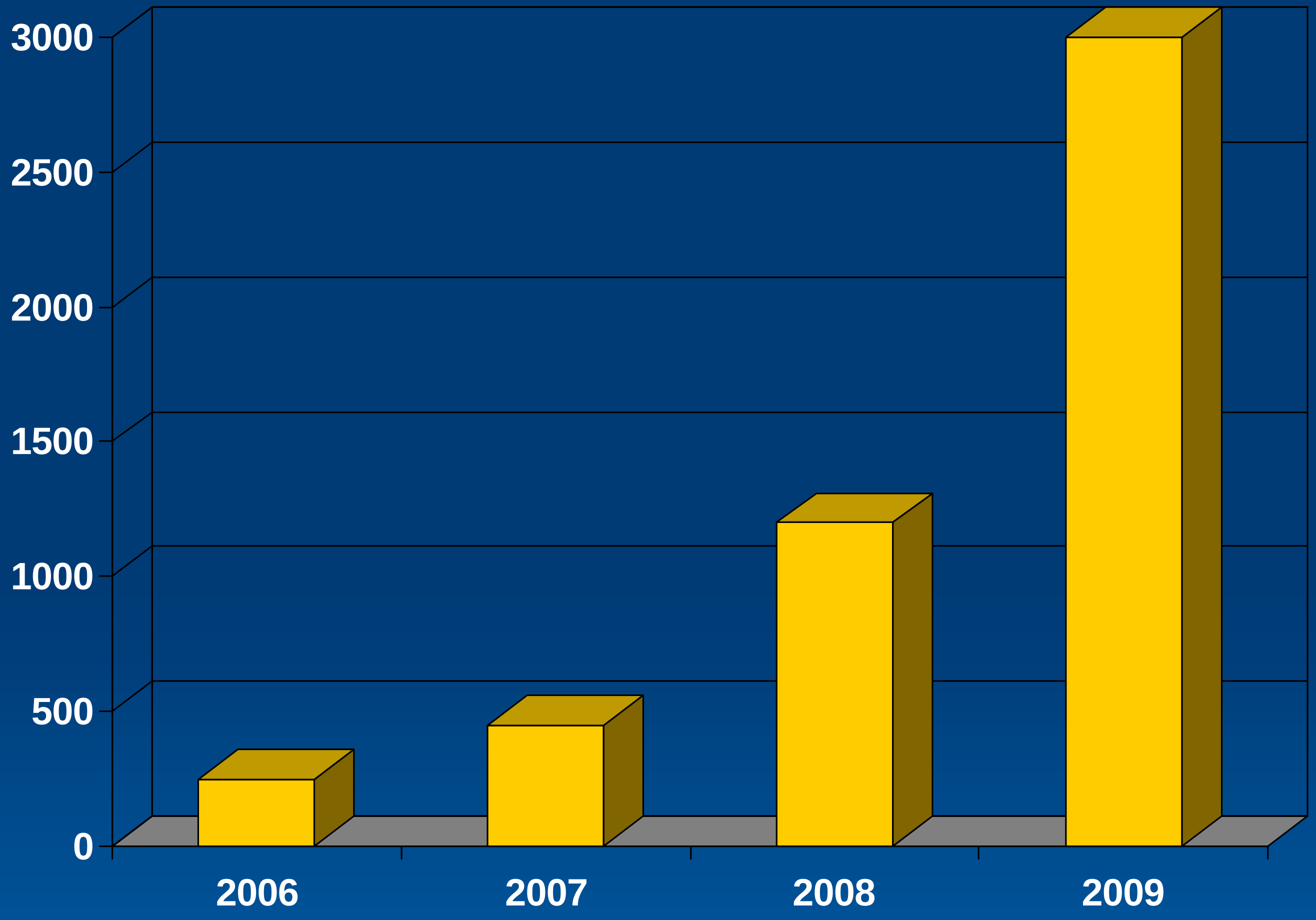
Cyber Threat Risk Assessment

	Threat			Opportunity/ Vulnerability	Impact
	Credibility	Capability	Intent		
High (2)	Information from highly reliable source or has been independently confirmed	Actors possess Expert level knowledge and extensive resources indicative of organized efforts	Targeted confidentiality, integrity, or availability (CIA) attack of dataset or individuals. Disruption of critical Agency mission or function.	Systems vulnerable to known vectors or methodology and/or available to known Actors.	Significant impact to Agency Programs, Project, Operations, People, Data, Systems, or Cost.
Moderate (1)	Information from normally reliable source but unconfirmed	Actors possess Moderate to high levels of sophistication with moderate resources	Non-targeted Attacks of Agency systems affecting confidentiality, integrity, or availability (CIA) of data. E.g. web defacement, botnets, etc.	Systems potentially vulnerable to known vectors or methodology and/or potentially available to known Actors.	Moderate impact to Agency Programs, Project, Operations, People, Data, Systems, or Cost.
Low (0)	Information from unreliable source or source without established history (or Unknown)	Actors possess Low level of sophistication with little resources required. (or Unknown)	"Drive by" or opportunistic attacks (or Unknown)	Systems not likely vulnerable to known vectors or methodology and/or not likely available to known Actors (or Unknown)	Low impact to Agency Programs, Project, Operations, People, Data, Systems, or Cost. (or Unknown)

US-CERT Incident Categories

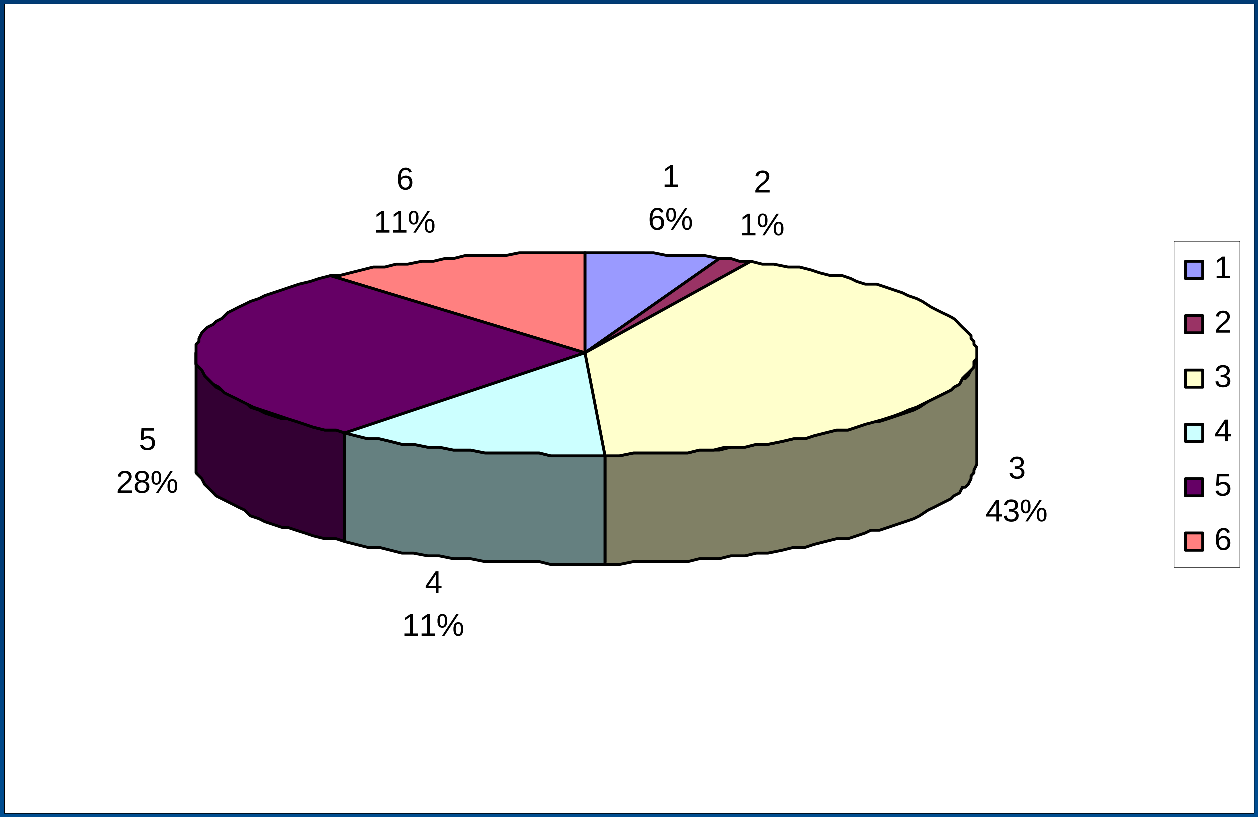
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.
CAT 1	Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource
CAT 2	*Denial of Service (DoS)	An attack that *successfully* 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.
CAT 3	*Malicious Code	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.
CAT 4	*Improper Usage	A person violates acceptable computing use policies.
CAT 5	Scans/Probes/Attempted Access	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.
CAT 6	Investigation	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

Incidents Per Year



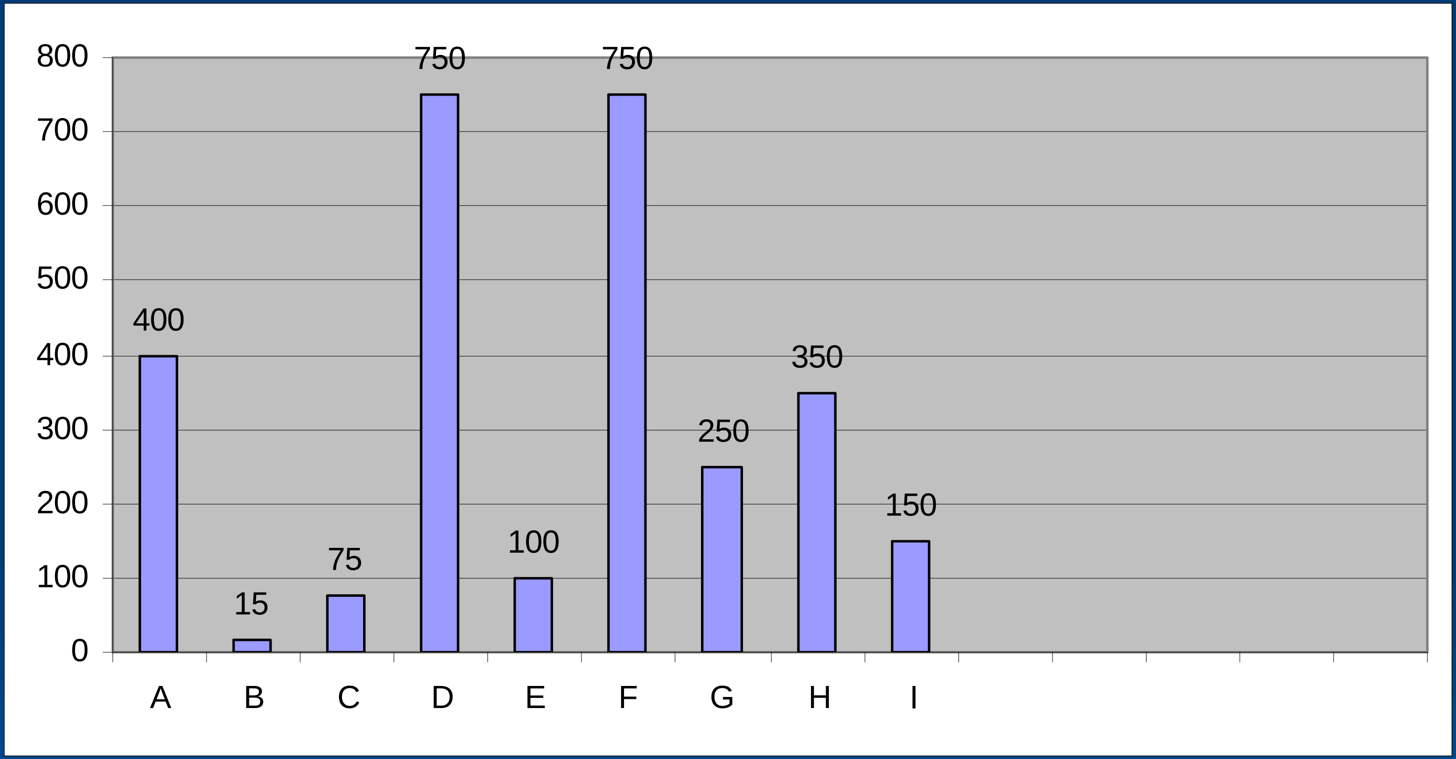
Note: Not Real Data! For illustrative purposes only.

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.

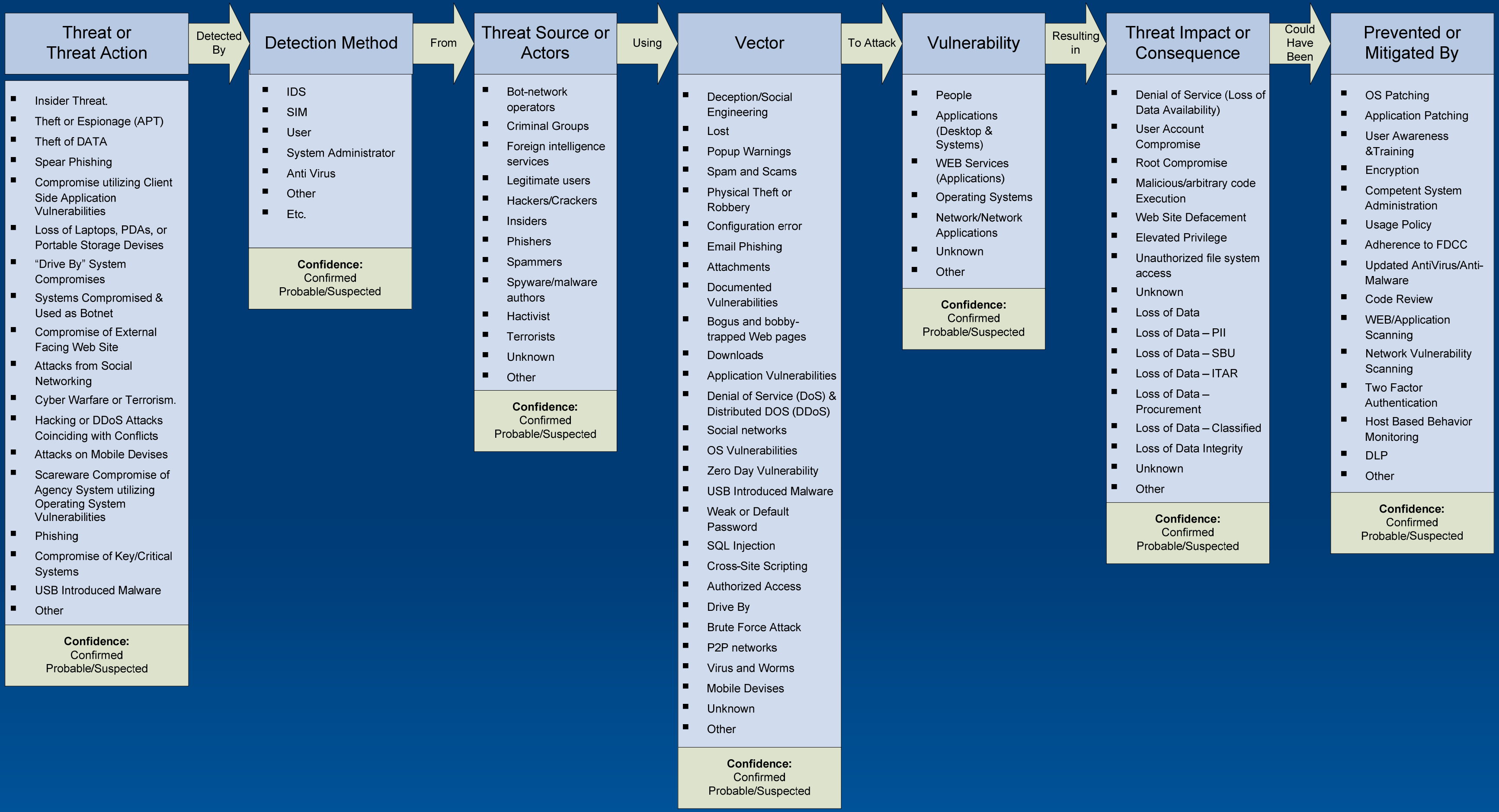
Practical Questions Unanswered

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 may 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 Cat1 & 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.

Incident Taxonomy



Threat or Threat Action

- Insider Threat.
- Theft or Espionage (APT)
- Theft of DATA
- Spear Phishing
- Compromise utilizing Client Side Application Vulnerabilities
- Loss of Laptops, PDAs, or Portable Storage Devises
- "Drive By" System Compromises
- Systems Compromised & Used as Botnet
- Compromise of External Facing Web Site
- Attacks from Social Networking
- Cyber Warfare or Terrorism.
- Hacking or DDoS Attacks Coinciding with Conflicts
- Attacks on Mobile Devises
- Scareware Compromise of Agency System utilizing Operating System Vulnerabilities
- Phishing
- Compromise of Key/Critical Systems
- USB Introduced Malware
- Other

Confidence:
Confirmed
Probable/Suspected

Detected By

Detection Method

- IDS
- SIM
- User
- System Administrator
- Anti Virus
- Other
- Etc.

Confidence:
Confirmed
Probable/Suspected

From

Threat Source or Actors

- Bot-network operators
- Criminal Groups
- Foreign intelligence services
- Legitimate users
- Hackers/Crackers
- Insiders
- Phishers
- Spammers
- Spyware/malware authors
- Hactivist
- Terrorists
- Unknown
- Other

Confidence:
Confirmed
Probable/Suspected

Using

Vector

- Deception/Social Engineering
- Lost
- Popup Warnings
- Spam and Scams
- Physical Theft or Robbery
- Configuration error
- Email Phishing
- Attachments
- Documented Vulnerabilities
- Bogus and bobby-trapped Web pages
- Downloads
- Application Vulnerabilities
- Denial of Service (DoS) & Distributed DOS (DDoS)
- Social networks
- OS Vulnerabilities
- Zero Day Vulnerability
- USB Introduced Malware
- Weak or Default Password
- SQL Injection
- Cross-Site Scripting
- Authorized Access
- Drive By
- Brute Force Attack
- P2P networks
- Virus and Worms
- Mobile Devises
- Unknown
- Other

Confidence:
Confirmed
Probable/Suspected

To Attack

Vulnerability

- People
- Applications (Desktop & Systems)
- WEB Services (Applications)
- Operating Systems
- Network/Network Applications
- Unknown
- Other

Confidence:
Confirmed
Probable/Suspected

Resulting in

Threat Impact or Consequence

- Denial of Service (Loss of Data Availability)
- User Account Compromise
- Root Compromise
- Malicious/arbitrary code Execution
- Web Site Defacement
- Elevated Privilege
- Unauthorized file system access
- Unknown
- Loss of Data
- Loss of Data – PII
- Loss of Data – SBU
- Loss of Data – ITAR
- Loss of Data – Procurement
- Loss of Data – Classified
- Loss of Data Integrity
- Unknown
- Other

Confidence:
Confirmed
Probable/Suspected

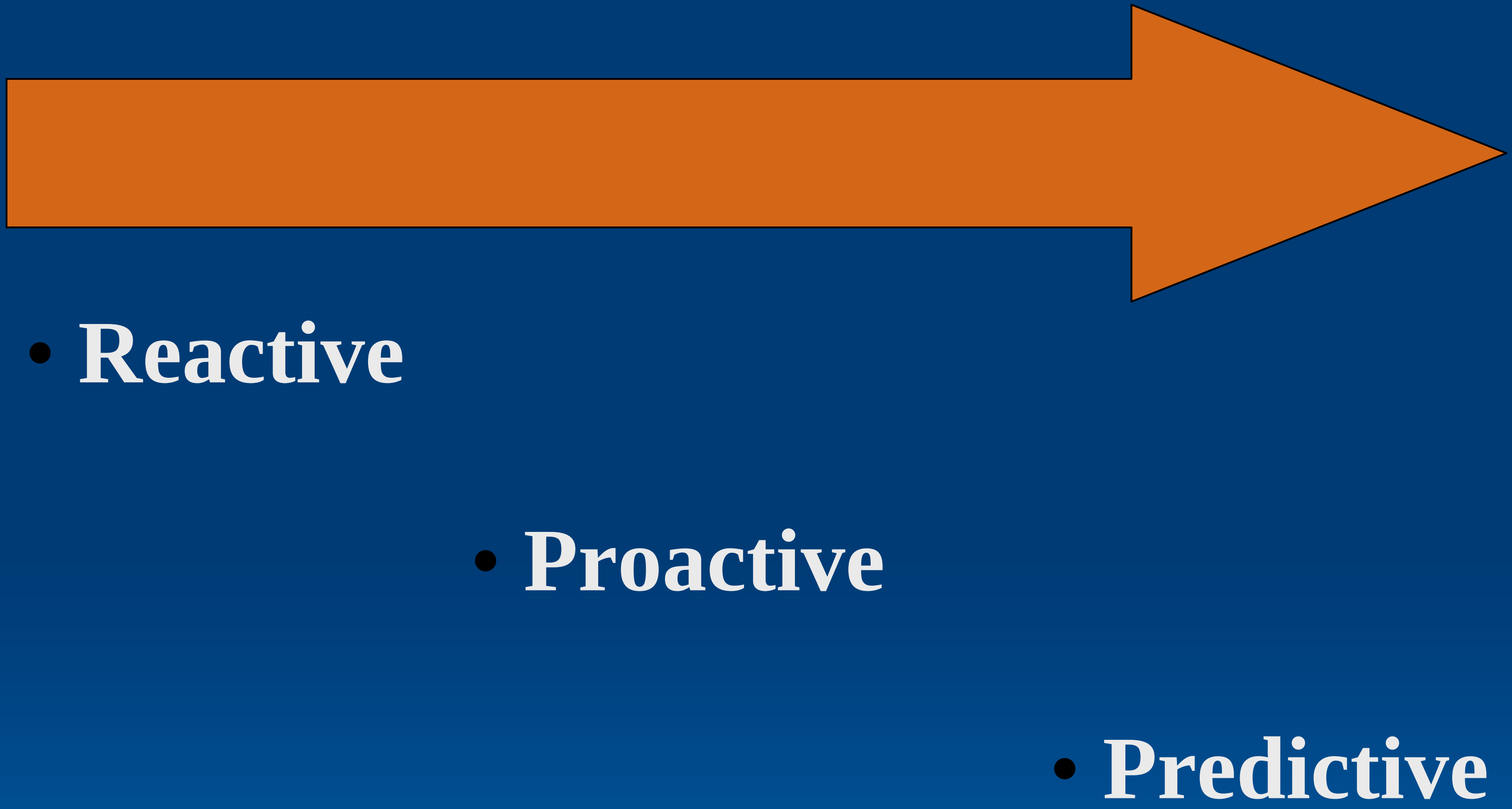
Could Have Been

Prevented or Mitigated By

- OS Patching
- Application Patching
- User Awareness &Training
- Encryption
- Competent System Administration
- Usage Policy
- Adherence to FDCC
- Updated AntiVirus/Anti-Malware
- Code Review
- WEB/Application Scanning
- Network Vulnerability Scanning
- Two Factor Authentication
- Host Based Behavior Monitoring
- DLP
- Other

Confidence:
Confirmed
Probable/Suspected

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

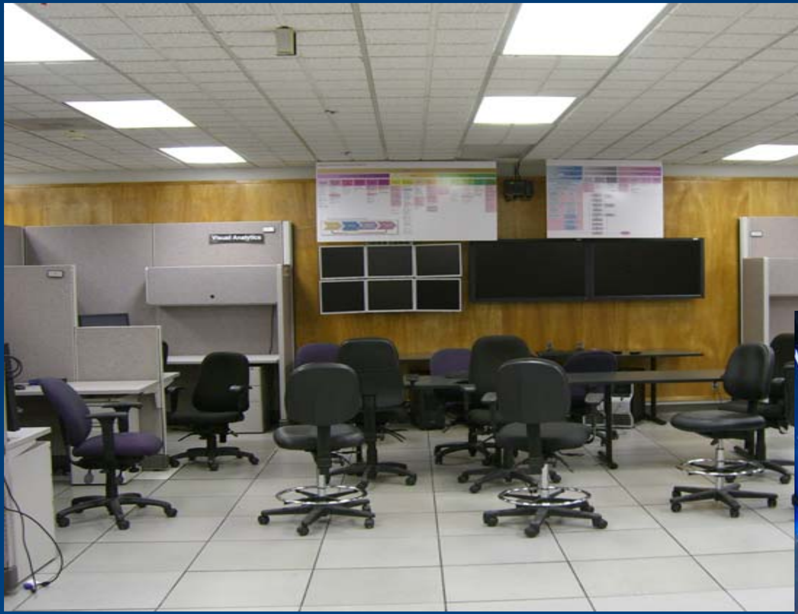
<table>
<tr><th colspan="2">Reactive</th><th>Proactive</th><th>Predictive</th></tr>
<tr><td rowspan="3">SOC</td><td>Incident Response, Notification, Tracking, Analysis, Containment, Eradication, and Remediation</td><td>Network Vulnerability Scanning: Network, systems,</td><td>Strategic Analysis</td></tr>
<tr><td>Incident Detection Systems (IDS)</td><td>Vulnerability Handling</td><td>Threat Management & Correlation System</td></tr>
<tr><td>Computer Forensics & Malware Analysis</td><td>Third-Party Pen. Testing (3rd Party)</td><td></td></tr>
<tr><td colspan="2"></td><td>Email Filtering & Blocking</td><td></td></tr>
<tr><td colspan="2"></td><td>DNS Sinkhole</td><td></td></tr>
<tr><td colspan="2"></td><td>Threat Tracking, Monitoring, & Mitigation</td><td></td></tr>
<tr><td colspan="2"></td><td>Patch/Asset Management</td><td></td></tr>
<tr><td colspan="3">Situational Awareness: Log Monitoring, Event Aggregation and Correlation (SIM)</td><td></td></tr>
<tr><td colspan="3">Flow/Network Behavior Monitoring</td><td></td></tr>
<tr><td colspan="3">Host Based Monitoring System (HBSS): Antivirus, Firewall, Anti-Malware, Application White listing</td><td></td></tr>
<tr><td colspan="3">Active Protection: Intrusion Prevention System (IPS)</td><td></td></tr>
<tr><td colspan="2"></td><td>Web & Application Scanning</td><td></td></tr>
<tr><td colspan="3">Incident Scope Analysis & Remote Forensics</td><td></td></tr>
<tr><td colspan="3">Content Monitoring/Data Loss Prevention</td><td></td></tr>
<tr><td colspan="2"></td><td colspan="2">Red Team/Blue Team</td></tr>
</table>

Staffing

Function	FTE	Hours of Operation
Tier 1	3 (Augmentation to Existing Call Center)	24 X 7
Tier 2	12	24 X 7
Tier 3	2	Business Hours
Implementation	6	Business Hours
Infrastructure	3	Business Hours & On Call
Total	26	

Facilities

- On the Cheap!



- State of Art!

Cyber Security from Different Perspectives

CIO	Programs & Projects	Law Enforcement
Protect the Enterprise		
Incident Response		
Proactive Response to Threats		
Ensure Availability of IT Infrastructure (Conduct Business)	Ensure Mission Success (Risks Vs. Rewards)	Catch the Bad Guys!
Access Control (Confidentiality & Integrity)	Ensure Availability of Mission Critical Systems & Applications	Protect National Security Interests
	Protect Intellectual Property	Gather Information about Those who are Gathering Information About You
Regulatory Compliance & Reporting	Protect Revenue Stream	

Different Priorities -> Different Requirements -> Different Solutions

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.