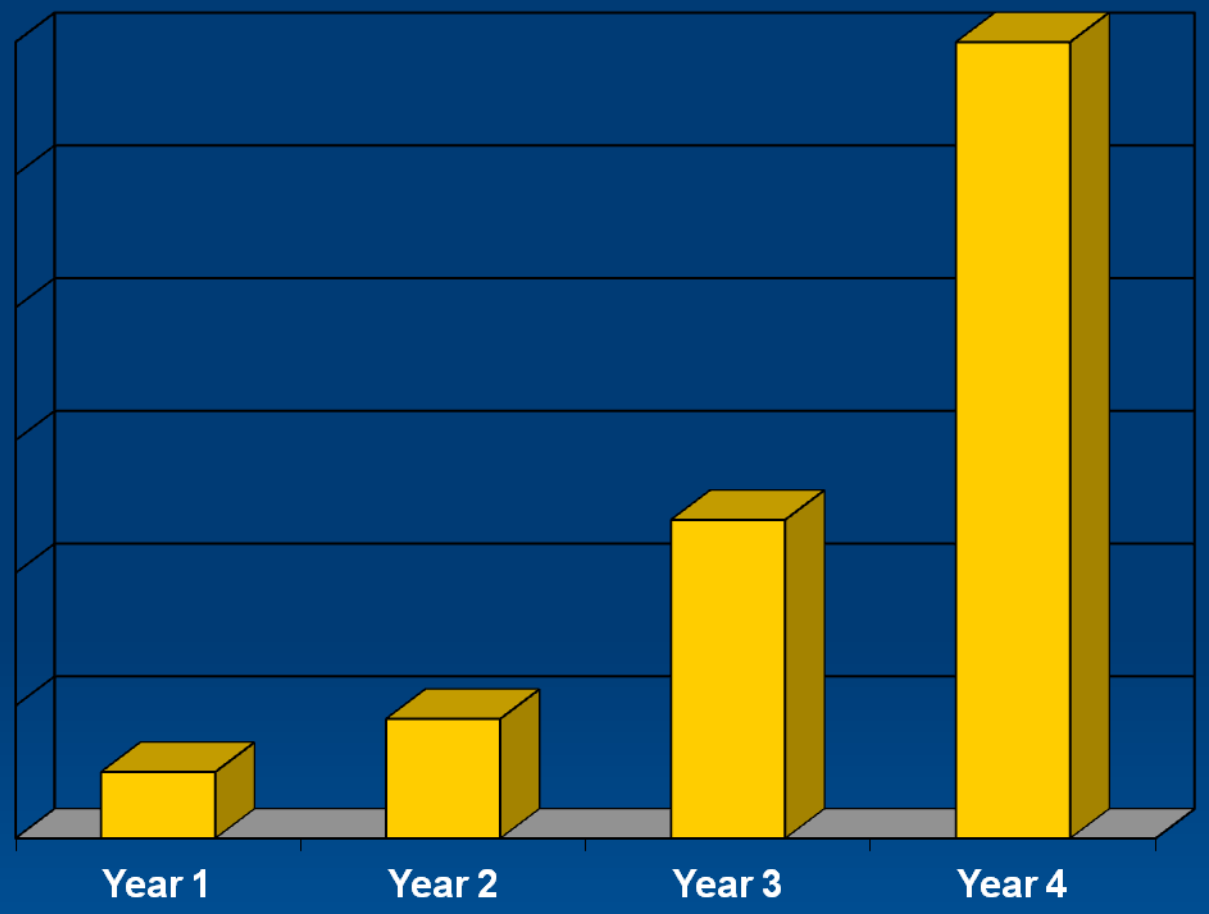
Analysis of CSIRT/SOC Incidents and Continuous Monitoring of Threats

By: John Wang, Katsutoshi C. Ishisoko (Chris)
NASA Ames Research Center

Incidents Per Year



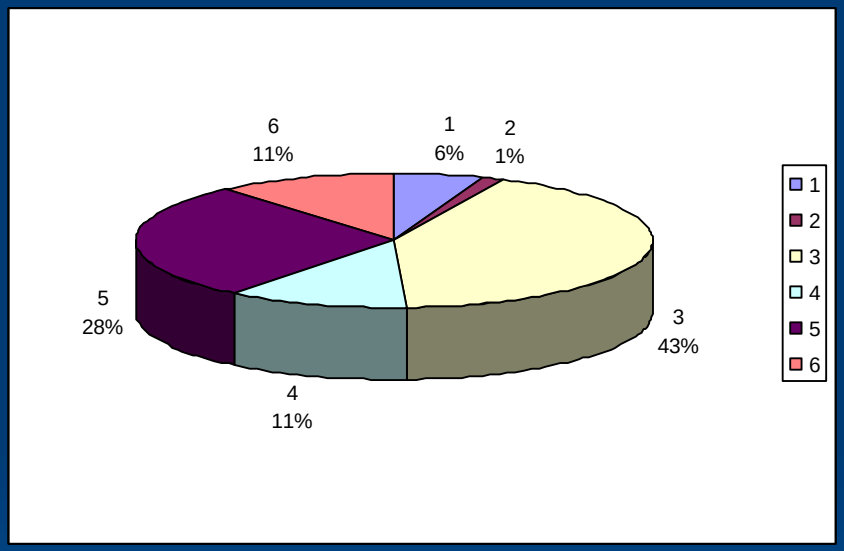
Note: Not Real Data! For illustrative purposes only.

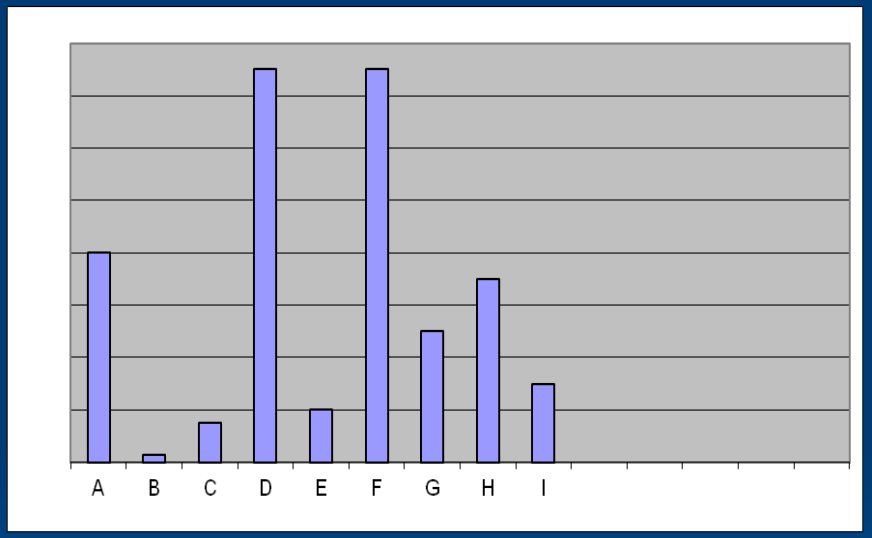
US-CERT Incident Categories

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 Organization 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 Organization 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.

Source: http://www.us-cert.gov/government-users/reporting-requirements.html

Incidents By Category & Facilities





Note: Not Real Data! For illustrative purposes only.

What do these data tell us???

- We are in Trouble!

Tracking Incidents by Categories

- Answers When? What? (Somewhat!) and How Often?
- Does not Answer Who? What? (Extended Version), Where? or Why?
- Not conducive to root cause analysis.
- Fails to reveal useful trends.

Does not lead to ACTION!

Practical Questions Unanswered

- How are you being attacked?
- How did you detect it?
- What are the Impacts?
- What did it cost?
- What do you need to fix?
- What controls work?
- What controls did not?

Everyone has an opinion…

SHOW ME THE DATA!!!

Other Questions Unanswered

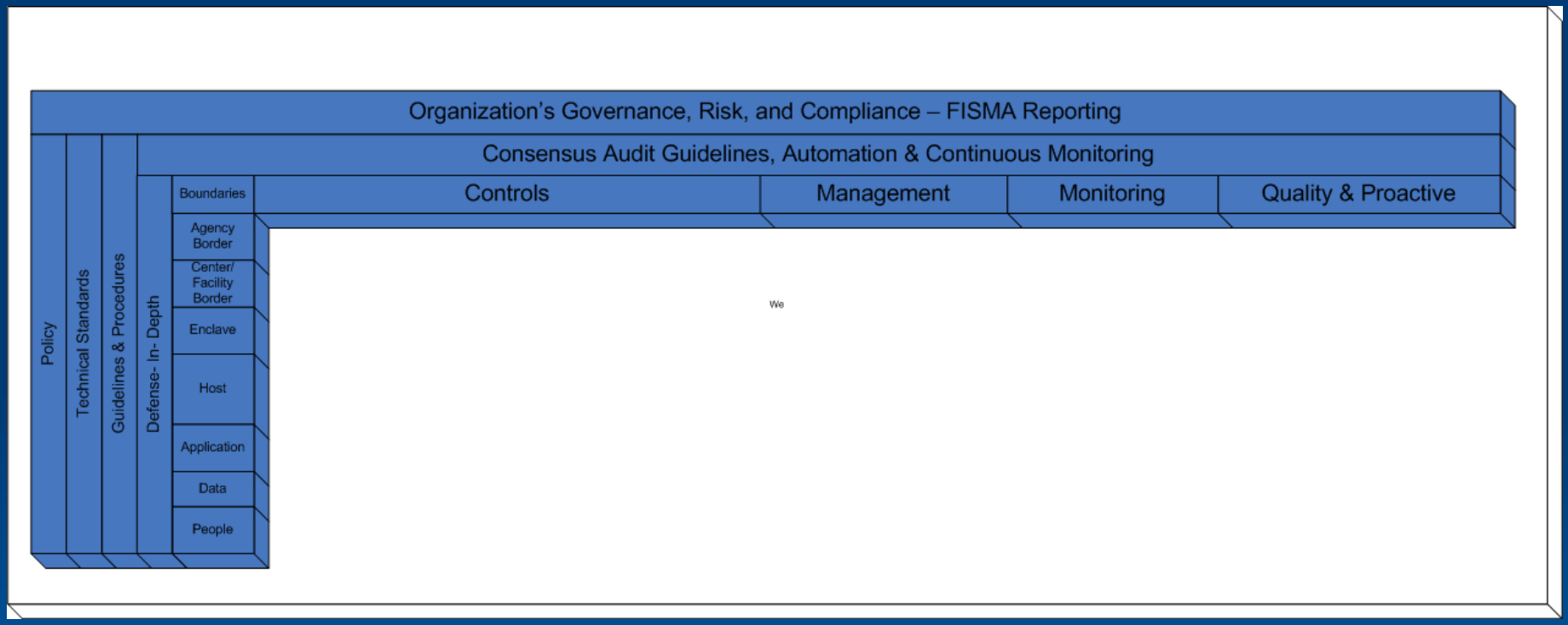
1) Were there any insider threats?
2) Were there any data ex-filtration by a Foreign Intelligence Entity (FIE)?
3) Were there any data obtained or ex-filtrated by hackers/hactivists?
4) Did you have any Spear Phishing incidents?
5) How many Cat 1 and Cat 3 were because of client side application vulnerabilities?
6) 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 you know what data was on the systems?
7) How many incidents were result of user inadvertently going to a bad/compromised site?
8) How many systems at the Organization were part of a Botnet?
9) How many instances of web defacement did you have? How did they get in?
10) Did we see any attacks from Social Networks? If so how many? Which social network?
11) Did you see any attacks on Mobile Devises?
12) How many Scareware incidents were there last year?
13) How many Cat1 & 3s used OS vulnerabilities?
14) Which Detection Systems were most effective?

What do we need to Get There?

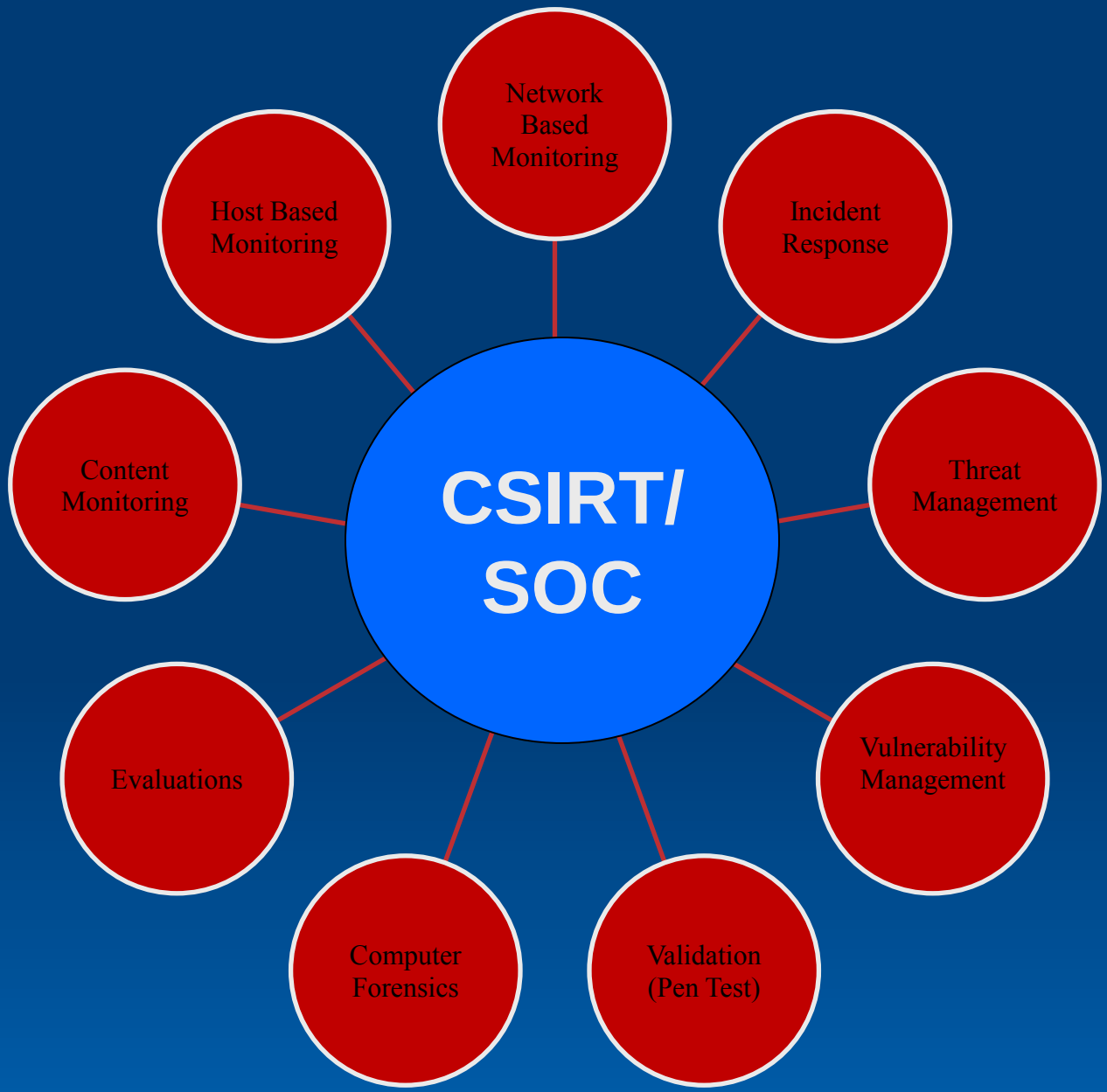
- Architecture
- Controls/Monitoring -> DATA
- CSIRT/SOC
  - Processes
  - Incident Taxonomy
  - Incident Management System
  - Threat Management

Architecture Building Blocks

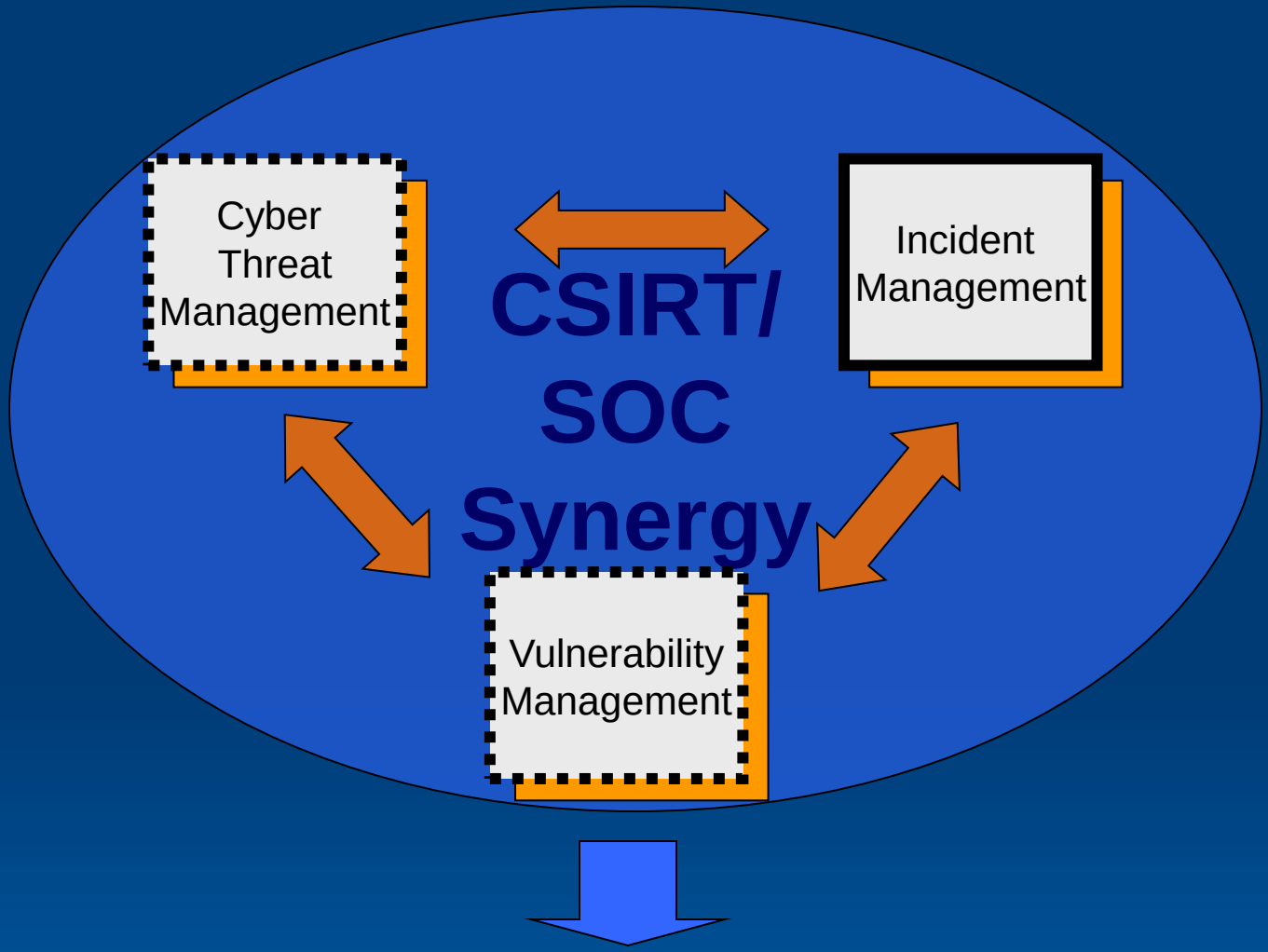
(Reference CAG Controls http://www.sans.org/critical-security-controls/guidelines.php)



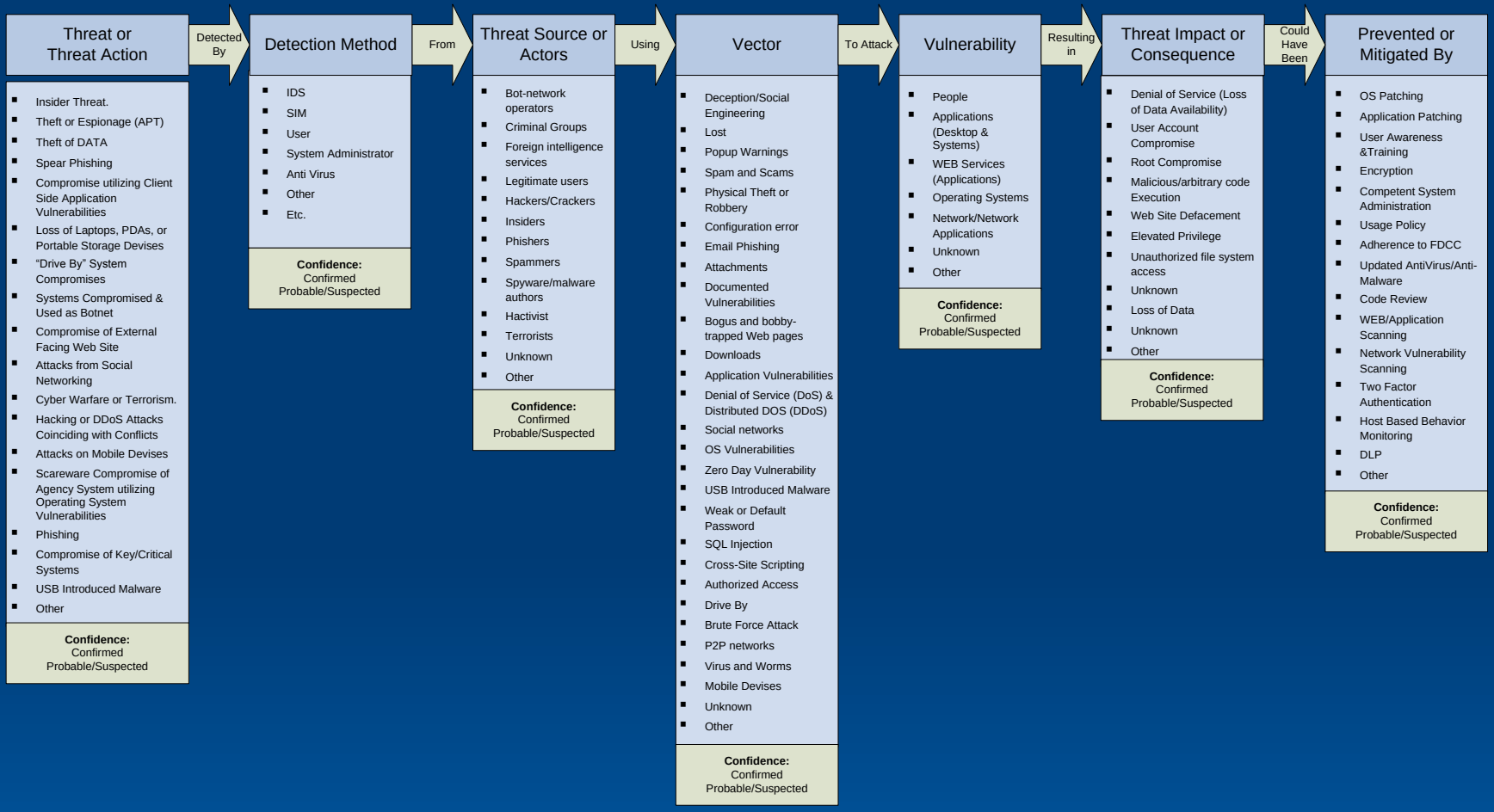
CSIRT/SOC as the HUB



Turning Disparate Data into Action!



Incident Taxonomy



Threat Management System

- **Unify Threat Management --** Enable Consistent and repeatable automated threat management process
- **Centralize and Structure Threat Database --** 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 internal research, content from commercial threat feeds and threat advisories received via email
- **Analyze and Refine Threat Data --** Analyze and react to vulnerabilities and threats based on Risk
- **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 organization
- **Validate Vulnerability Remediation --** Reporting of activities related to threat remediation

Threat Management Goals

- Automation of Threat Mitigation
- Risk Assessment
- Campaign Tracking
- Vulnerability Tracking & Management
- IOC DB
- Trend analysis
- Alert and Reporting

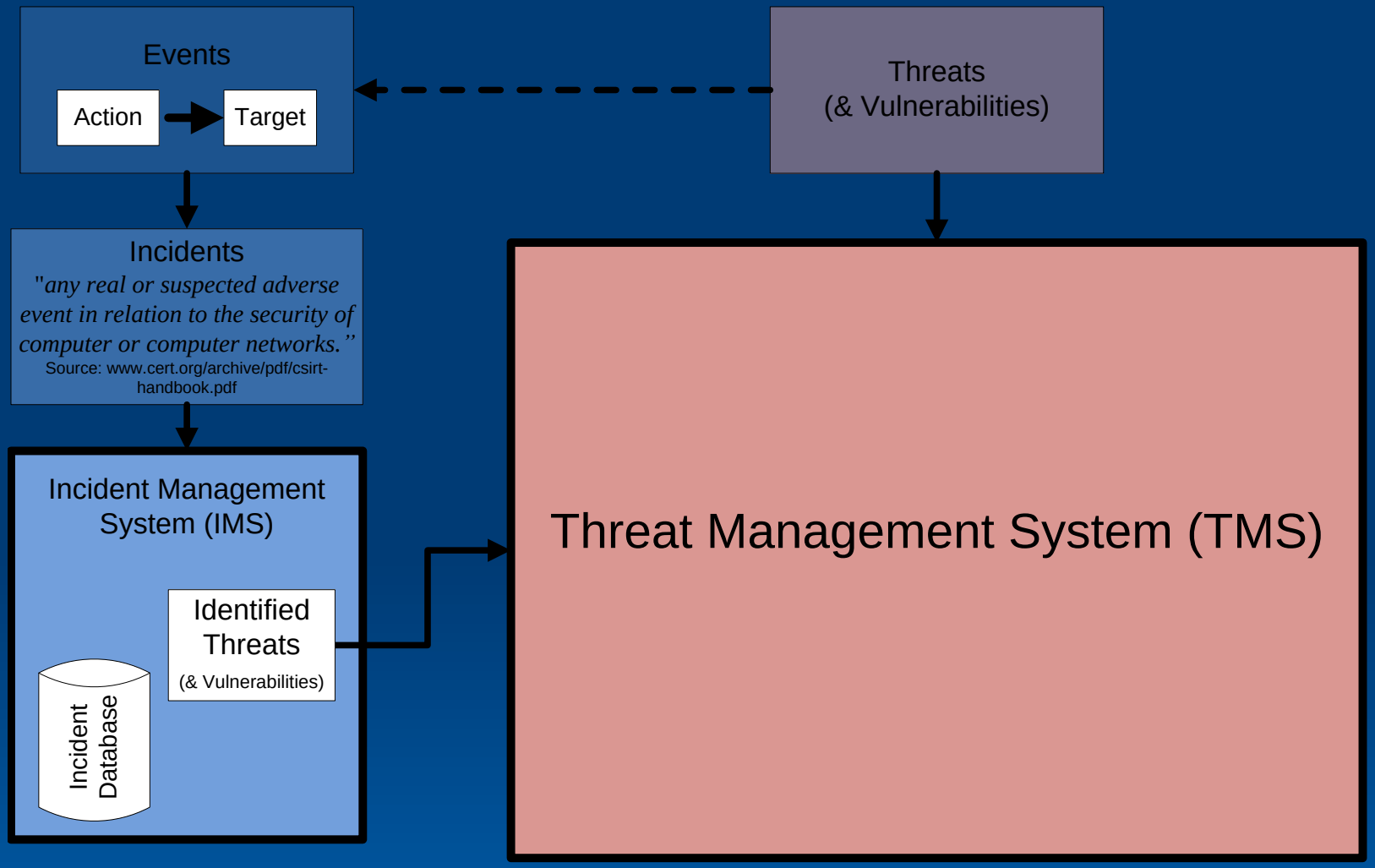
Inputs

- Incident Data
- Watch list
- Black list
- IOCs
- Threat feeds
- Vulnerability information
- Asset data
- Future: Shared Campaign information

Outputs

- Actions
  - Blocks (IP, Domains, e-mail, applications, etc.)
  - Signatures/monitoring (SIM, IDS)
  - IOCs
  - Notifications
  - Alerts
- Reports
  - Situation Awareness Reports
  - Mitigation Action Requests
  - Detailed threat reports
  - Campaigns
  - Trends

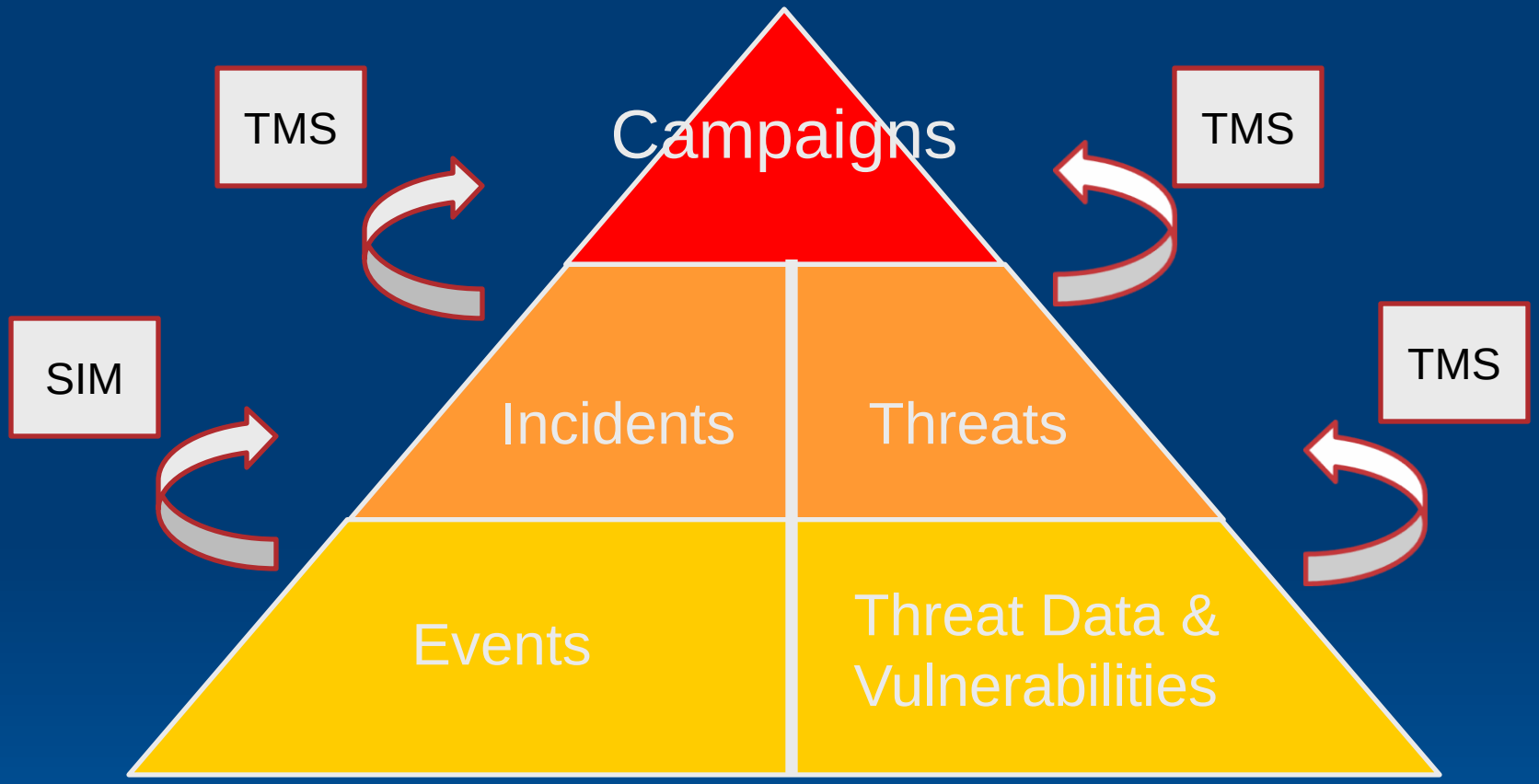
TMS Relationship to IMS



Campaigns

- Definition: A series of related adverse incidents which compromise the confidentiality, integrity, or availability of YOUR ORGANIZATION'S data, systems, networks, or the personal information of YOUR ORGANIZATION'S personnel
- These campaigns may include anything from state sponsored Advance Persistent Threats (APTs), to Denial of Service (DOS) attacks, to a multitude of other general threats aimed at stealing information for financial gain
- A group of related incidents are elevated to a Campaign when collectively the events pose a significant and persistent threat to YOUR ORGANIZATION and share common characteristics such as: known patterns of behavior (including techniques, persistence, sophistication, etc.), adversaries, tools, indicators-of-compromise, or motive(s)

Campaign Approach:



Tracking Campaigns

Named Campaigns	Threat Status	Methods	Indicators-of-Compromise	Attribution (s)	Motive(s)	Outside Reference	Incident Tracking No.(s)
Campaign #1							
Campaign #2							
Campaign #3							

Indicators of Compromise

- OpenIOC.org
  - “IOCs allow you to describe a wide variety of indicators, including attacker activities, movement, and methodology, as well as specific forensic artifacts of malicious executables and exploits.” – Mandiant
- Mitre.org
  - Cyber Observable eXpression (CybOX)
  - Malware Attribute Enumeration and Characterization

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 Organization mission or function.	Systems vulnerable to known vectors or methodology and/or available to known Actors.	Significant impact to Organization 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 Organization's 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 Organization's 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 Organization's Programs, Project, Operations, People, Data, Systems, or Cost. (or Unknown)

SO What does Actionable Data Look Like???

Attacks: Primary

Attacks	Total
Social Engineering (Phishing)	
Drive By Malware -> Vulnerable System	
Insider Threat (Failure to Comply With Security Procedures)	
Insider Threat (Malicious Acts or Theft, Insider Enabled Attack or Compromise)	
Attack Web Applications	
Disclosure of Sensitive Information	
Attack DMZ System -> pivots to internal	
Account compromised from use of external system (vulnerable) to access Account	
Scan for weak Systems, vulnerable Software, or mis-configuration	
DOS	
Bruce Force Attack	
Other	
Unknown/Undetermined	

Attacks: Secondary

Attacks: Secondary	Total
Lateral Attack	
Utilize compromised system to attack Windows infrastructure	
Utilize compromised system/account to propagate SPAM	
Utilize system to attack External Systems	
Prolonged Undetected Attacker	
Other	

Vulnerabilities

Vulnerabilities	Total
OS Microsoft	
Browser	
FLASH	
Acrobat	
OS Apple	
Java	
MS Office Application	
OS Unix/Linux	
Other	
Unknown	

System Types

System Types	Total
Desktop	
Portable Computer	
External System	
Guest Network System	
Mobile Computing Devises	
IPhone	
IPad	
Blackberry	
Android	
External Storage	
USB FOB	
Web	
FTP	
Windows Domain Controller	
Sharepoint	
Database	
Other	

Detection Methods

Detection Methods	Total
IDS	
Sinkhole/Honeypot	
Email Monitoring	
User Report	
External Source	
Host – Anti Virus	
Other	

Motives

Motives	Total
Monetary	
Hactivism	
BotNet	
Disgrunteled	
Espionage/Advanced Persistent Threat	
Other	
Unknown	

Associated CAG Controls

Mitigated, Failed, or Could Have Prevented	Total
Critical Control 1: Inventory of Authorized and Unauthorized Devices	
Critical Control 2: Inventory of Authorized and Unauthorized Software	
Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	
Critical Control 4: Continuous Vulnerability Assessment and Remediation	
Critical Control 5: Malware Defenses	
Critical Control 6: Application Software Security	
Critical Control 7: Wireless Device Control	
Critical Control 8: Data Recovery Capability	
Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps	
Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	
Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services	
Critical Control 12: Controlled Use of Administrative Privileges	
Critical Control 13: Boundary Defense	
Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	
Critical Control 15: Controlled Access Based on the Need to Know	
Critical Control 16: Account Monitoring and Control	
Critical Control 17: Data Loss Prevention	
Critical Control 18: Incident Response Capability	
Critical Control 19: Secure Network Engineering	
Critical Control 20: Penetration Tests and Red Team Exercises	

Impact

Impact	Total
COST	
Confidentiality	
Integrity	
Availability	
Reputation	
Lost Productivity	
IR/Remediation Hours	
Other	
Unknown	

COSTS

- Cost of specific incident
- Average cost per incident
- Total Organization's cost for incidents
- Remediation Cost
- Legal Cost
- Cost impact of fixing and implementing a given control
- Etc.

Take Away

- Incident counts by categories are almost useless
- Management need actionable data based on incidents and threats
- You most likely already have the data, but it might not be in a useful form
- Before you spend $$$ on a control, you need to understand what the benefit will be in terms of incidents, impacts, and $$$