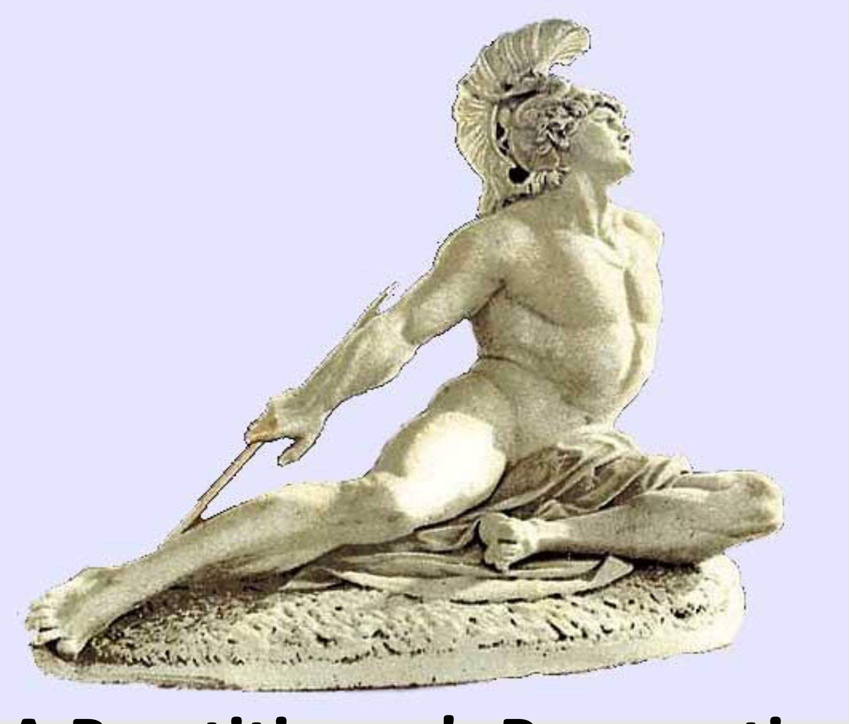
Vulnerability Management



A Practitioner’s Perspective

William Favre Slater, III
M.S., MBA, PMP, CISSP, SSCP, CISA, ITIL, IPv6
Senior IT Consultant in Cybersecurity
Chicago, Illinois
United States of America
slater@billslater.com
http://billslater.com/interview

EVOLVE
Security Academy

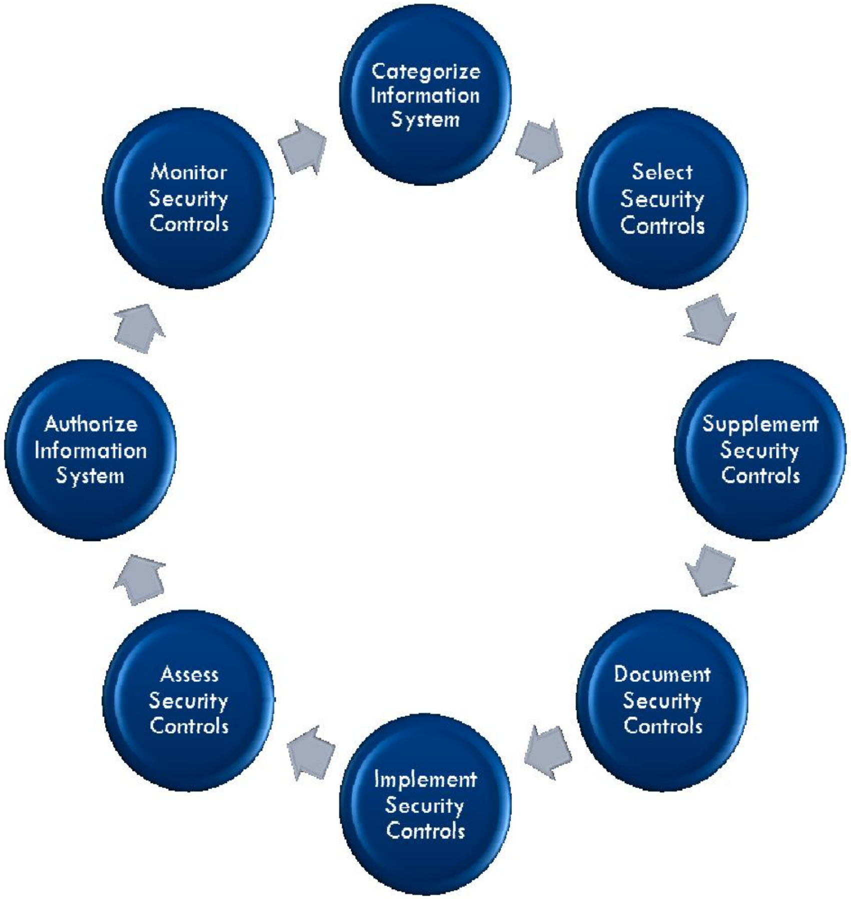
Agenda

- Introduction
- What are Vulnerabilities?
- What are Threats?
- Quick Story about David Brewer, Michael Nash, and the "Brewer Events".
- Tools
- Planning Your Scanning
- Vulnerability Management & Reporting
- Remediation Management & Reporting
- Vulnerability Aging Reporting
- Personal Insights from Experience
- Summary
- Conclusion
- Questions
- Resources

Introduction

- Vulnerability Management
  - Is an essential part of any modern Security Management Program
  - Is required now by all Security Frameworks
  - Requires careful planning, rigor, and discipline
  - Requires Diplomacy
  - Requires Strong Management Support
  - Is required to keep you out of lawsuits
  - Is required to help protect your organization from deadly attacks and data breaches

Information Security is a Continuous Process



Categorize Information System

Select Security Controls

Supplement Security Controls

Document Security Controls

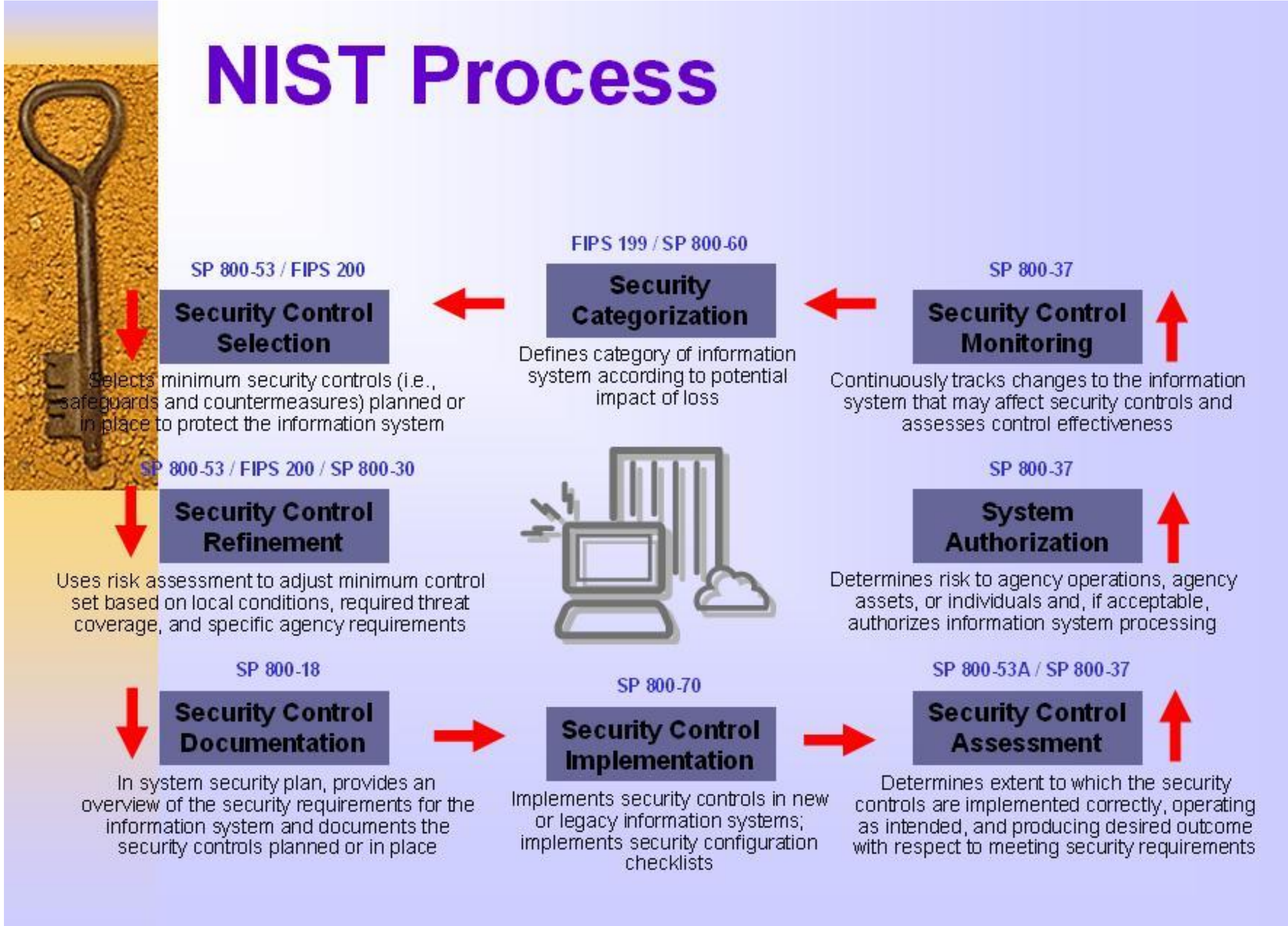
Implement Security Controls

Assess Security Controls

Authorize Information System

Monitor Security Controls

Information Security is a Continuous Process



NIST Process

FIPS 199 / SP 800-60

Security Categorization

Defines category of information system according to potential impact of loss

SP 800-53 / FIPS 200

Security Control Selection

Selects minimum security controls (i.e., safeguards and countermeasures) planned or in place to protect the information system

SP 800-53 / FIPS 200 / SP 800-30

Security Control Refinement

Uses risk assessment to adjust minimum control set based on local conditions, required threat coverage, and specific agency requirements

SP 800-18

Security Control Documentation

In system security plan, provides an overview of the security requirements for the information system and documents the security controls planned or in place

SP 800-70

Security Control Implementation

Implements security controls in new or legacy information systems; implements security configuration checklists

SP 800-53A / SP 800-37

Security Control Assessment

Determines extent to which the security controls are implemented correctly, operating as intended, and producing desired outcome with respect to meeting security requirements

SP 800-37

System Authorization

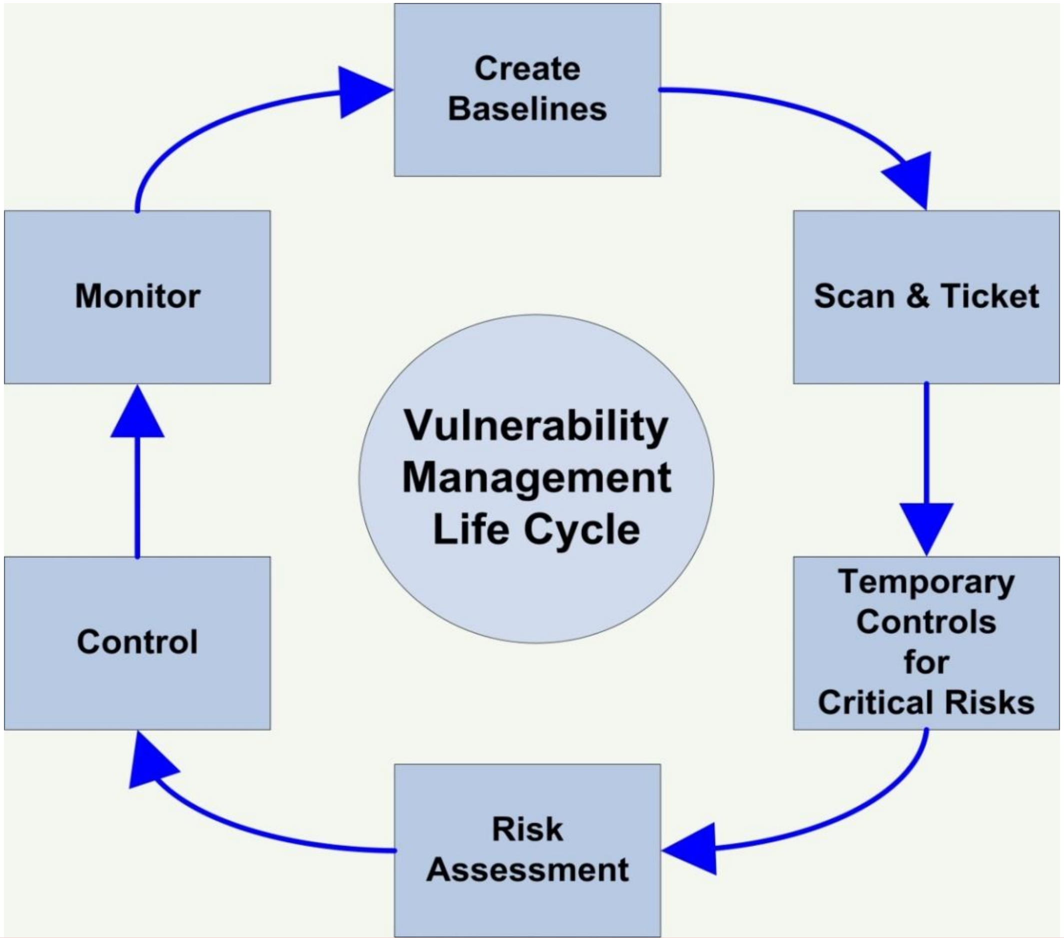
Determines risk to agency operations, agency assets, or individuals and, if acceptable, authorizes information system processing

SP 800-37

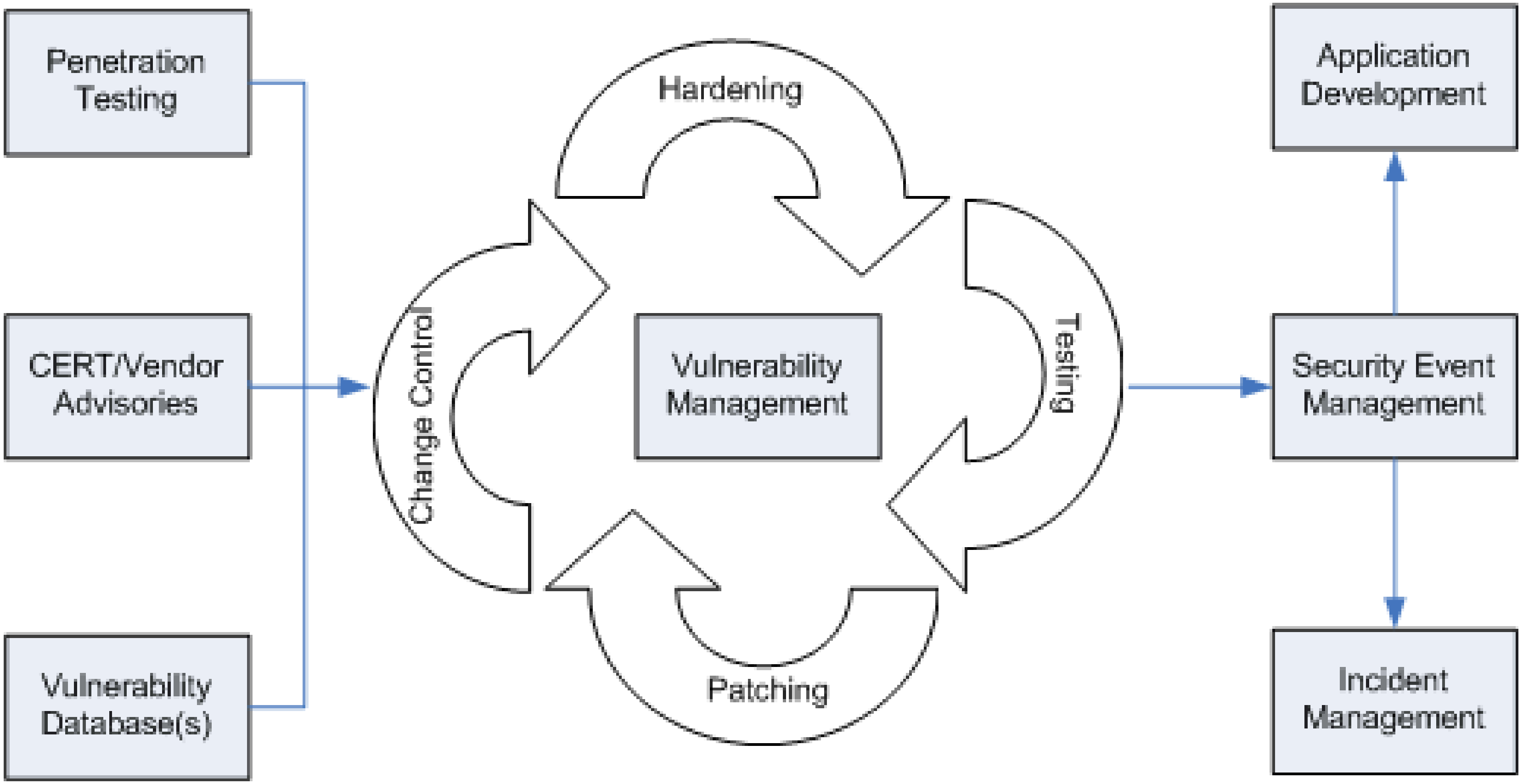
Security Control Monitoring

Continuously tracks changes to the information system that may affect security controls and assesses control effectiveness

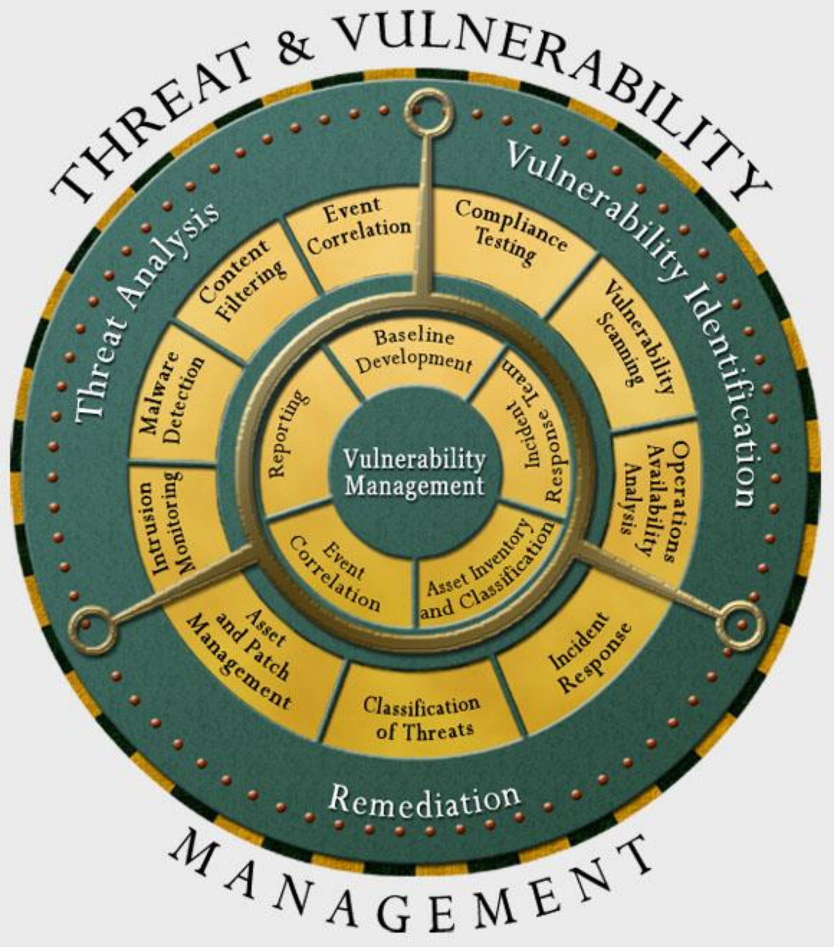
Vulnerability Management Life Cycle


Create Baselines
Scan & Ticket
Temporary Controls for Critical Risks
Risk Assessment
Control
Monitor
Vulnerability Management Life Cycle

Vulnerability Management Security Management

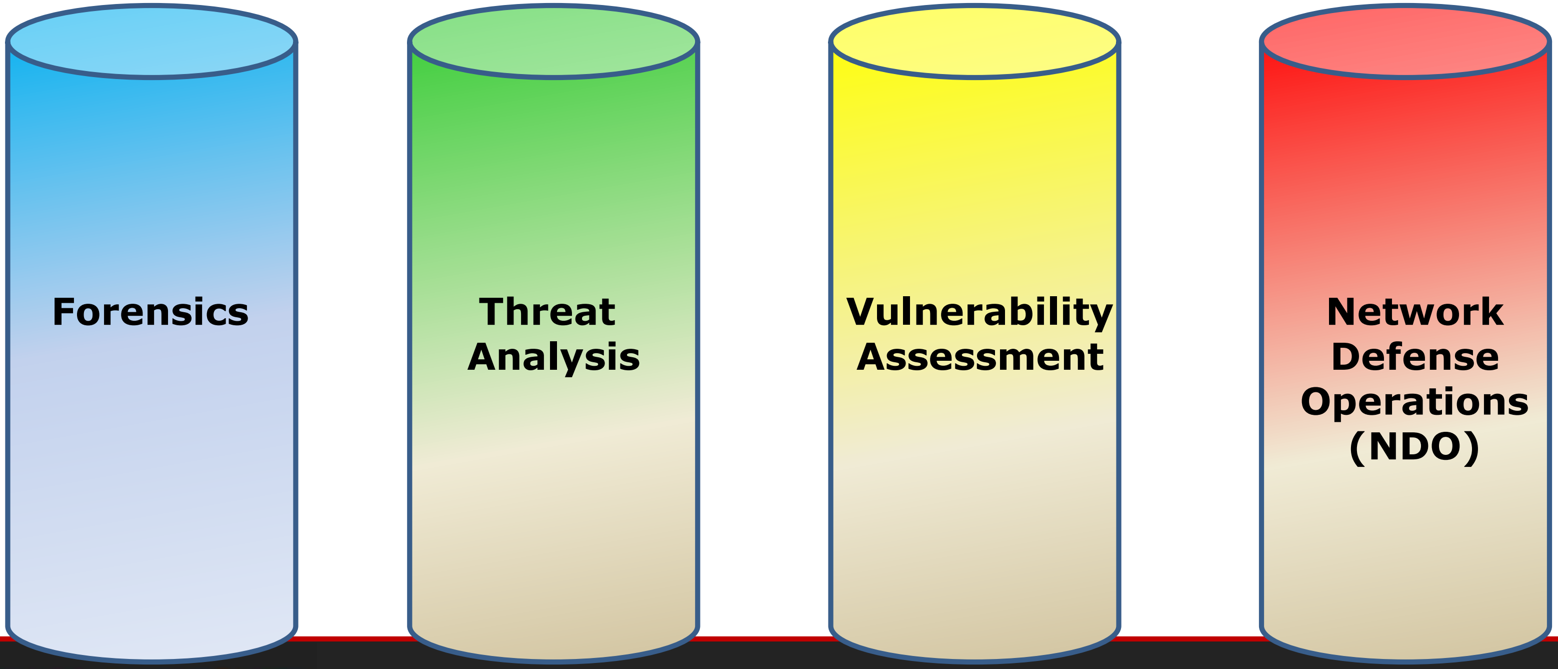


Vulnerability Management Security Management



Computer Network Defense (CND)

The Four Pillars



Forensics

Threat Analysis

Vulnerability Assessment

Network Defense Operations (NDO)

Security Architecture & Management

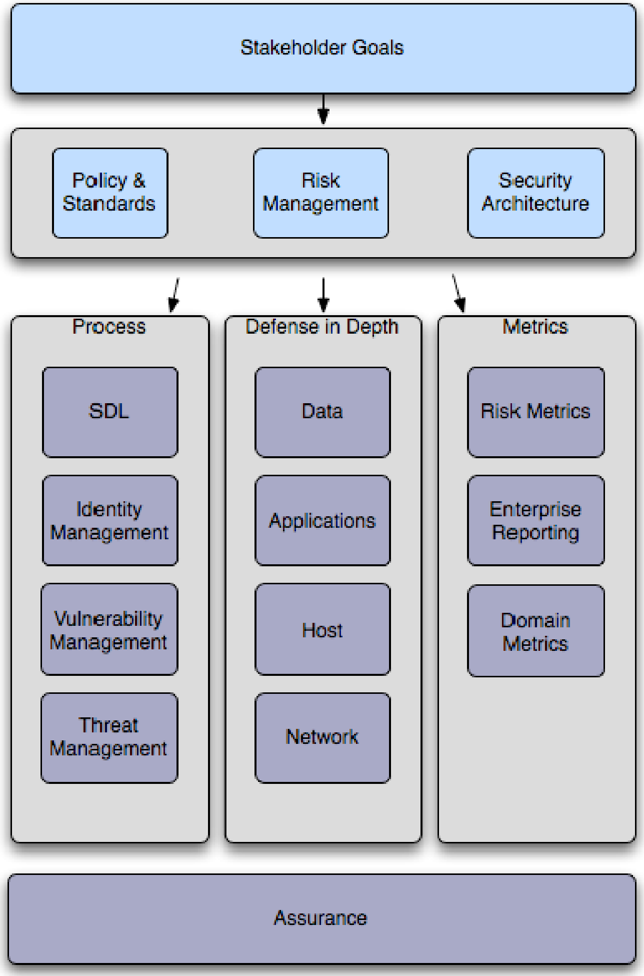
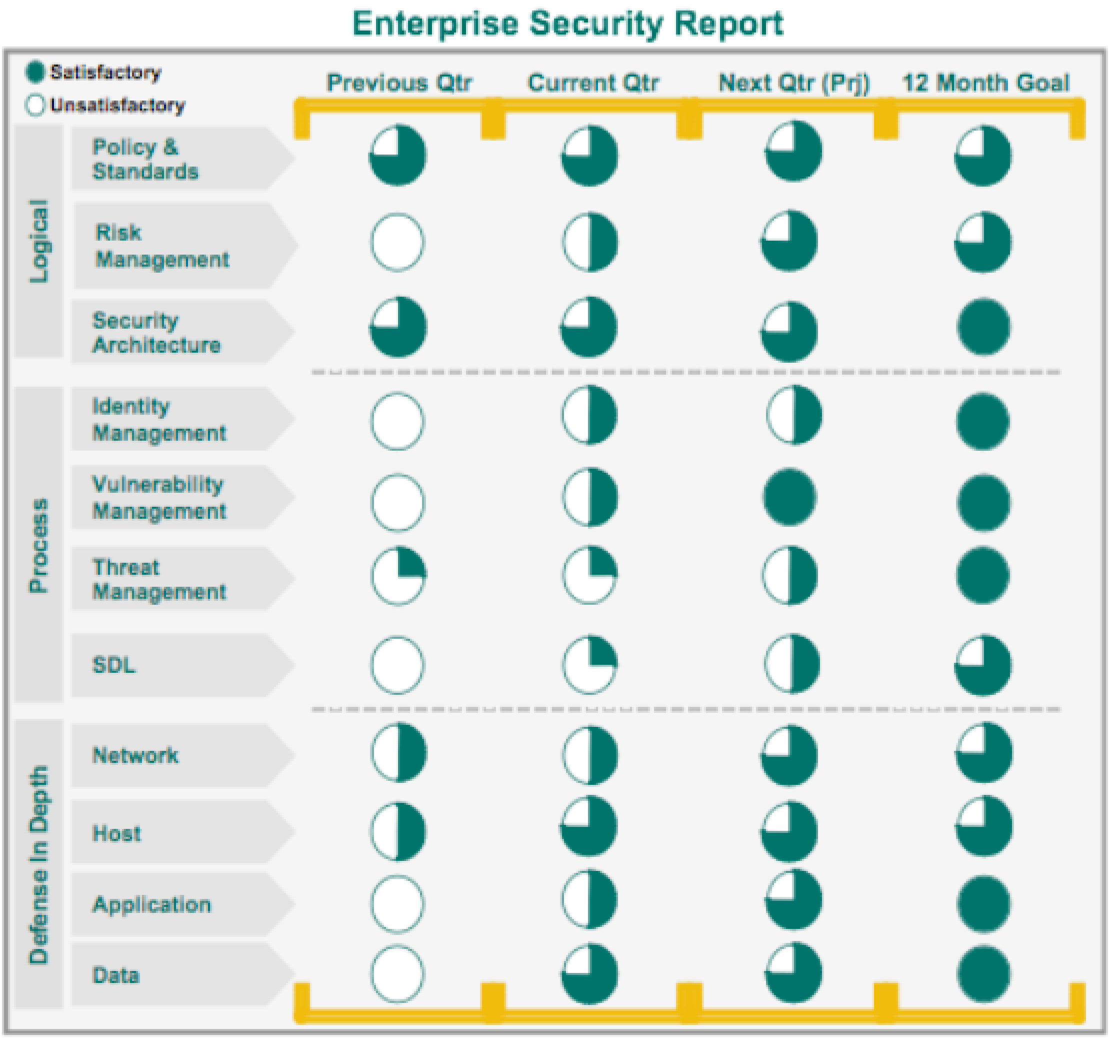


Figure 1: Security Architecture Blueprint

Measuring and Reporting on Security Architecture & Management



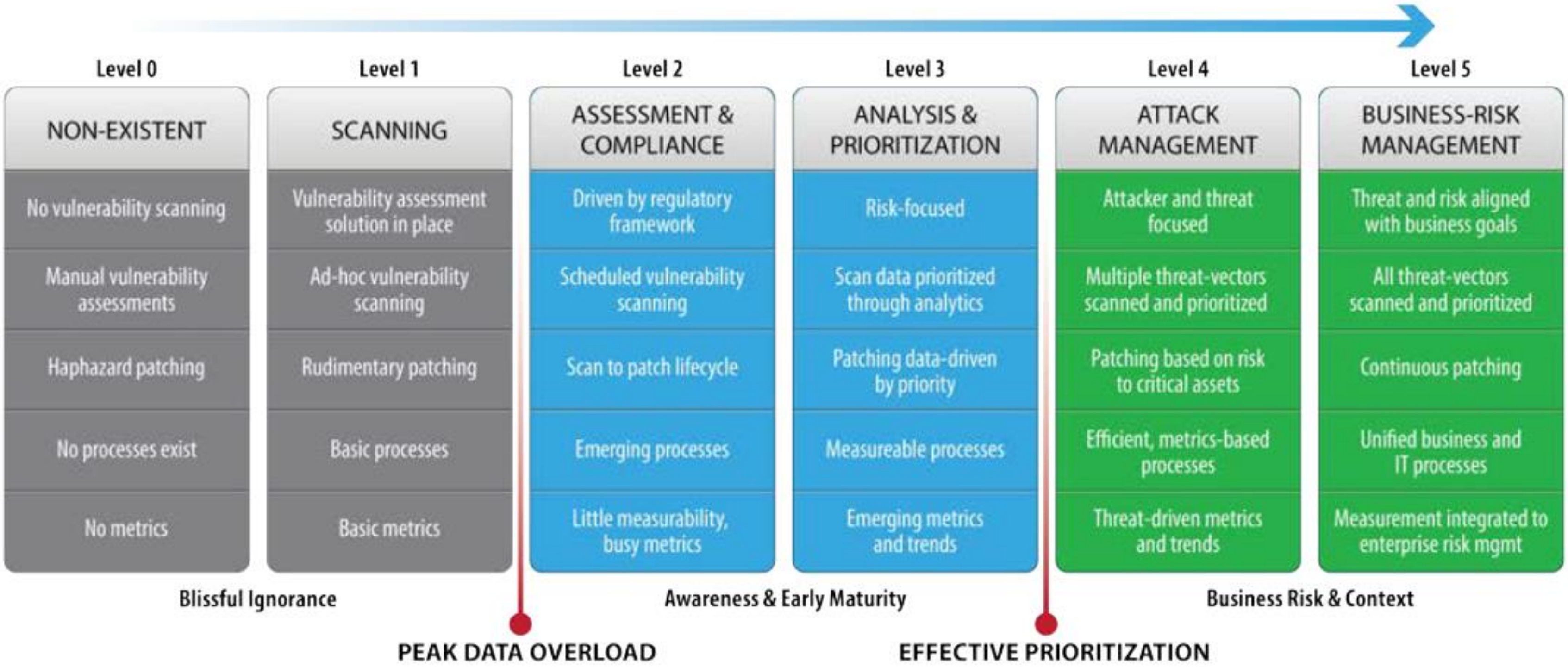
Enterprise Security Report

● Satisfactory
○ Unsatisfactory

		Previous Qtr	Current Qtr	Next Qtr (Prj)	12 Month Goal
Logical	Policy & Standards	◕	◕	◕	◕
	Risk Management	○	◑	◕	◕
	Security Architecture	◕	◕	◕	●
Process	Identity Management	○	◑	◑	●
	Vulnerability Management	○	◑	●	●
	Threat Management	◔	◔	◑	●
	SDL	○	◔	◑	◕
Defense In Depth	Network	◑	◑	◕	◕
	Host	◑	◕	◕	◕
	Application	○	◑	◕	●
	Data	○	◕	◕	●

Figure 6: Enterprise Security Executive Report

Is There a Capability Maturity Model for Threat and Vulnerability Management?



Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
NON-EXISTENT	SCANNING	ASSESSMENT & COMPLIANCE	ANALYSIS & PRIORITIZATION	ATTACK MANAGEMENT	BUSINESS-RISK MANAGEMENT
No vulnerability scanning	Vulnerability assessment solution in place	Driven by regulatory framework	Risk-focused	Attacker and threat focused	Threat and risk aligned with business goals
Manual vulnerability assessments	Ad-hoc vulnerability scanning	Scheduled vulnerability scanning	Scan data prioritized through analytics	Multiple threat-vectors scanned and prioritized	All threat-vectors scanned and prioritized
Haphazard patching	Rudimentary patching	Scan to patch lifecycle	Patching data-driven by priority	Patching based on risk to critical assets	Continuous patching
No processes exist	Basic processes	Emerging processes	Measureable processes	Efficient, metrics-based processes	Unified business and IT processes
No metrics	Basic metrics	Little measurability, busy metrics	Emerging metrics and trends	Threat-driven metrics and trends	Measurement integrated to enterprise risk mgmt

Blissful Ignorance

Awareness & Early Maturity

Business Risk & Context

PEAK DATA OVERLOAD

EFFECTIVE PRIORITIZATION

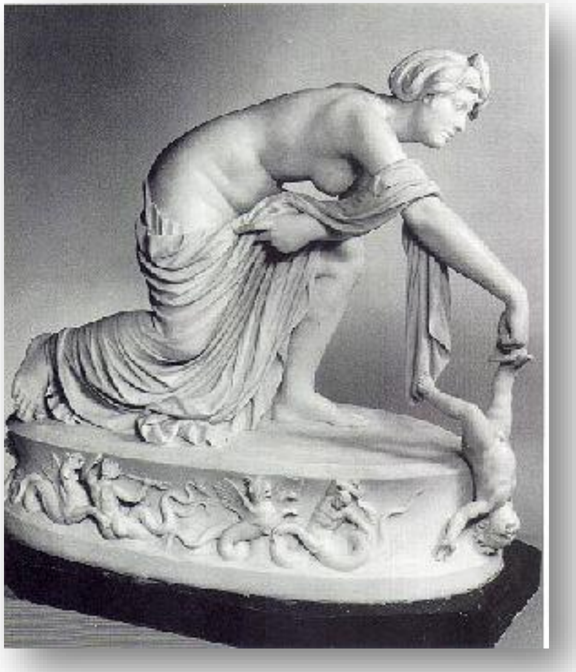
Figure 1. The Threat and Vulnerability Management Maturity Model

Source: https://blog.coresecurity.com/2014/10/21/the-threat-and-vulnerability-management-maturity-model/

WHAT ARE VULNERABILITIES?

Vulnerabilities

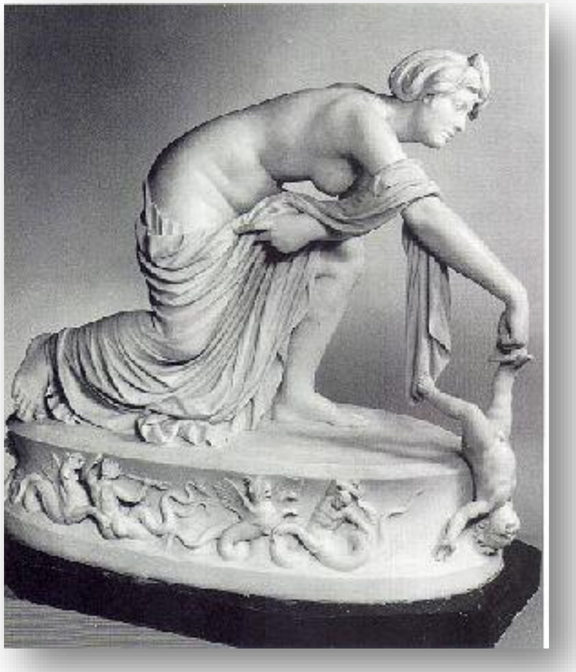
- Vulnerability – definition
- Vulnerability examples



Thetis dipping Achilles into the River Styx

Vulnerabilities

- What is a "vulnerability"?
  - A situation or condition that represents an opportunity for a threat to damage or for information to be stolen from the organization, IT Systems or network.
  - Comes from the Latin word, "vulnus", meaning "wound"
  - Sometimes called, ***"The Achilles Heel."***



Thetis dipping Achilles
into the River Styx

The Death of Achilles

Achilles was mortally wounded in the one place he was vulnerable: his heel.

Some Sources of Vulnerabilities

- Complicated user interface
- Default passwords not changed
- Disposal of storage media without deleting data
- Equipment sensitivity to changes in voltage
- Equipment sensitivity to moisture and contaminants
- Equipment sensitivity to temperature
- Inadequate cabling security
- Inadequate capacity management
- Inadequate change management
- Inadequate classification of information
- Inadequate control of physical access
- Inadequate maintenance
- Inadequate network management
- Inadequate or irregular backup
- Inadequate password management
- Inadequate physical protection

Some Sources of Vulnerabilities

- Inadequate protection of cryptographic keys
- Inadequate replacement of older equipment
- Inadequate security awareness
- Inadequate segregation of duties
- Inadequate segregation of operational and testing facilities
- Inadequate supervision of employees
- Inadequate supervision of vendors
- Inadequate training of employees
- Incomplete specification for software development
- Insufficient software testing
- Lack of access control policy
- Lack of clean desk and clear screen policy
- Lack of control over the input and output data
- Lack of internal documentation
- Lack of or poor implementation of internal audit
- Lack of policy for the use of cryptography

Some Sources of Vulnerabilities

- Lack of procedure for removing access rights upon termination of employment
- Lack of protection for mobile equipment
- Lack of redundancy
- Lack of systems for identification and authentication
- Lack of validation of the processed data
- Location vulnerable to flooding
- Poor selection of test data
- Single copy
- Too much power in one person
- Uncontrolled copying of data
- Uncontrolled download from the Internet
- Uncontrolled use of information systems
- Undocumented software
- Unmotivated employees
- Unprotected public network connections
- User rights are not reviewed regularly

WHAT ARE THREATS?

Threats

- Threat – definition
- Some sources of threats
- More threat examples

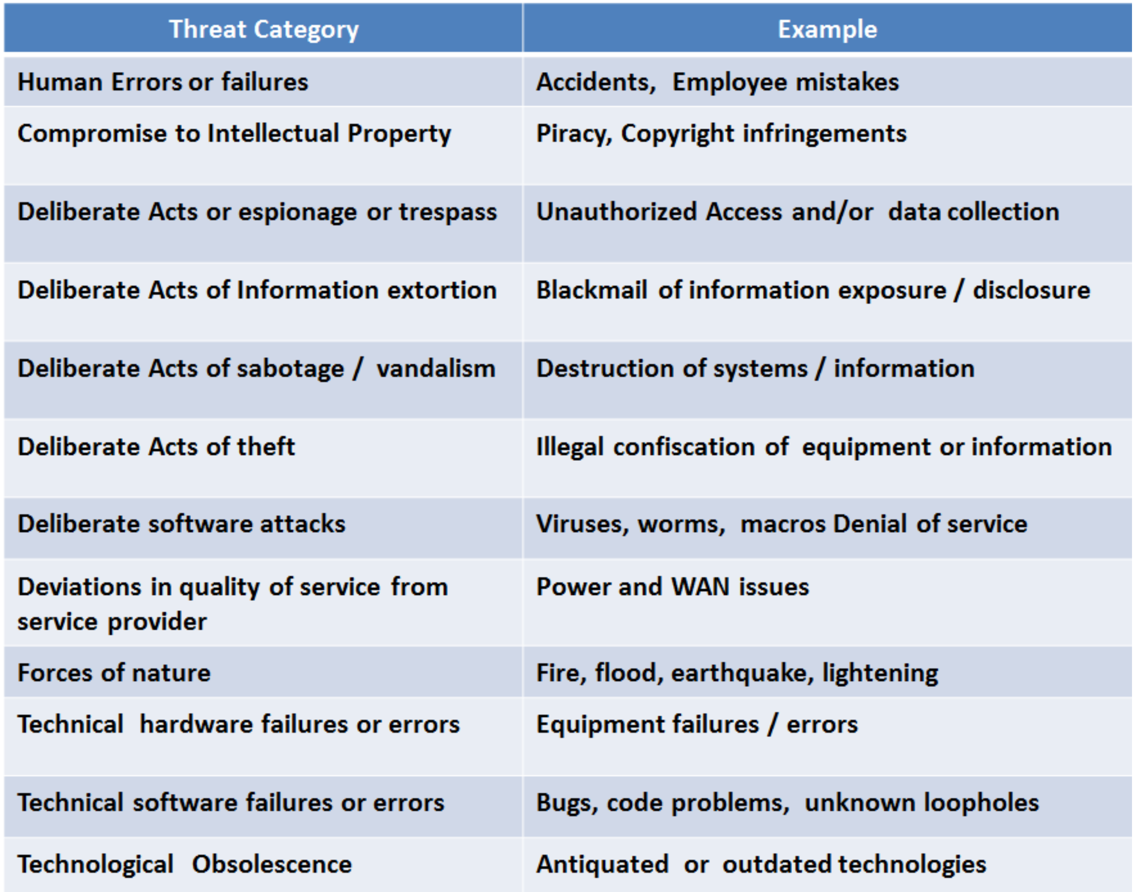
Threats

- What is a “threat”?
  - Something that can potentially cause damage or theft to the organization, IT Systems or network.

Some Sources of Threats

- Misguided Employees
- Mistakes by careless Employees
- External Parties
- Low awareness of security issues
- Lack of or lapse in security policy compliance
- Growth in networking and distributed computing
- Growth in complexity and effectiveness of hacking tools and viruses
- Natural disasters e.g. fire, flood, earthquake

Typical Threats that Represent Business Risks



Threat Category	Example
Human Errors or failures	Accidents, Employee mistakes
Compromise to Intellectual Property	Piracy, Copyright infringements
Deliberate Acts or espionage or trespass	Unauthorized Access and/or data collection
Deliberate Acts of Information extortion	Blackmail of information exposure / disclosure
Deliberate Acts of sabotage / vandalism	Destruction of systems / information
Deliberate Acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros Denial of service
Deviations in quality of service from service provider	Power and WAN issues
Forces of nature	Fire, flood, earthquake, lightening
Technical hardware failures or errors	Equipment failures / errors
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological Obsolescence	Antiquated or outdated technologies

QUICK STORY ABOUT DAVID BREWER AND THE "BREWER EVENTS".

So Let's Simplify This Stuff And Make it Easier, Achievable and More Manageable

Dr. David Brewer, FBCS, CITP

Note: with clients – he had to start using the Word, "EVENT", because he learned Executive Management got upset About the connotation of Words like ASSETS, THREATS and VULNERABILITIES

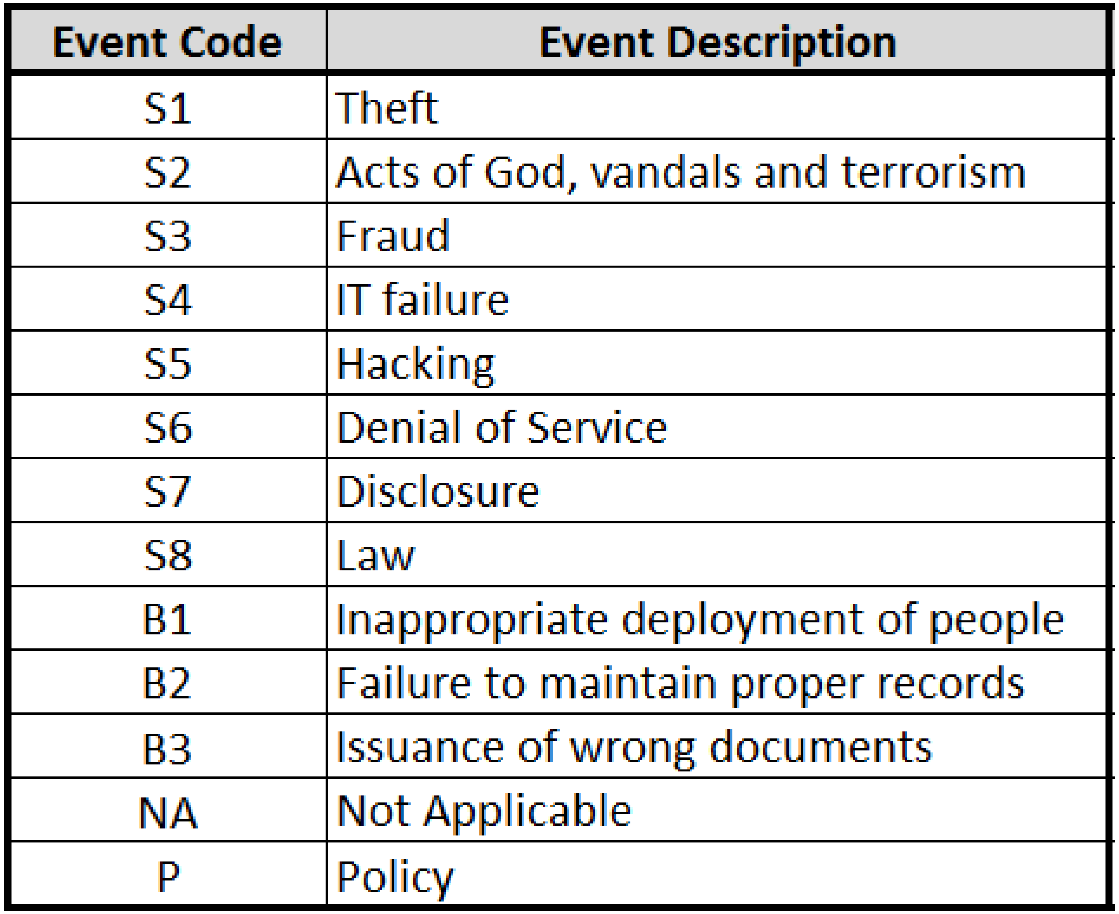
Co-author of the ISO 27001 standard security framework, October 2005
Co-author of ISO 27001 Annex A Insights, December 2010
Director, Gamma Secure Systems Limited
ISO/IEC 27001 and ISO 9001 Certified for the
Provision of Information Security Consultancy
www.gammassl.co.uk

Source: http://www.gammassl.co.uk/research/27001annexAinsights.pdf

An "Event" is

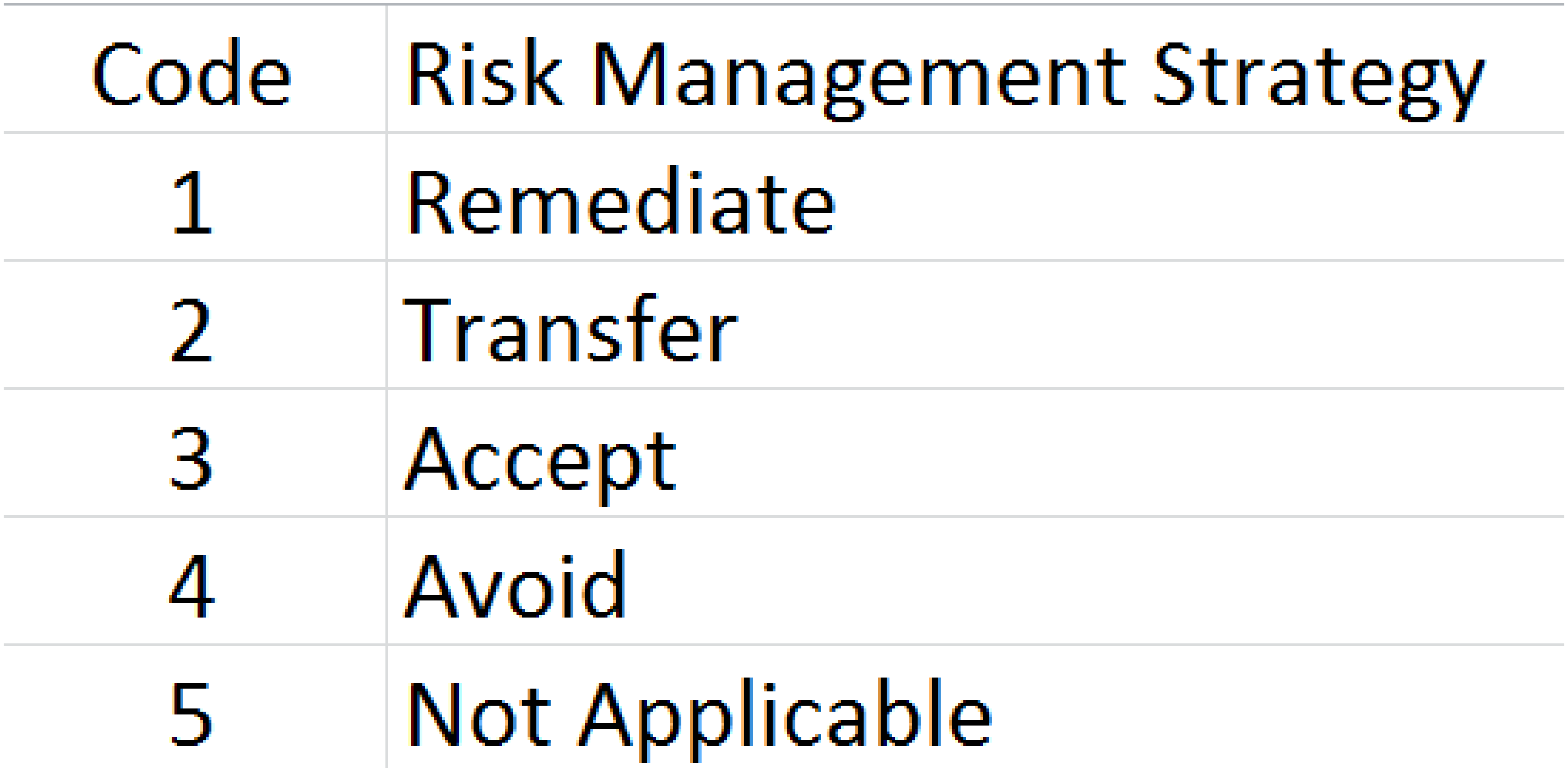
- When Threat Meets Vulnerability or
- When a Threat EXPLOITS a Vulnerability

Brewer Event List



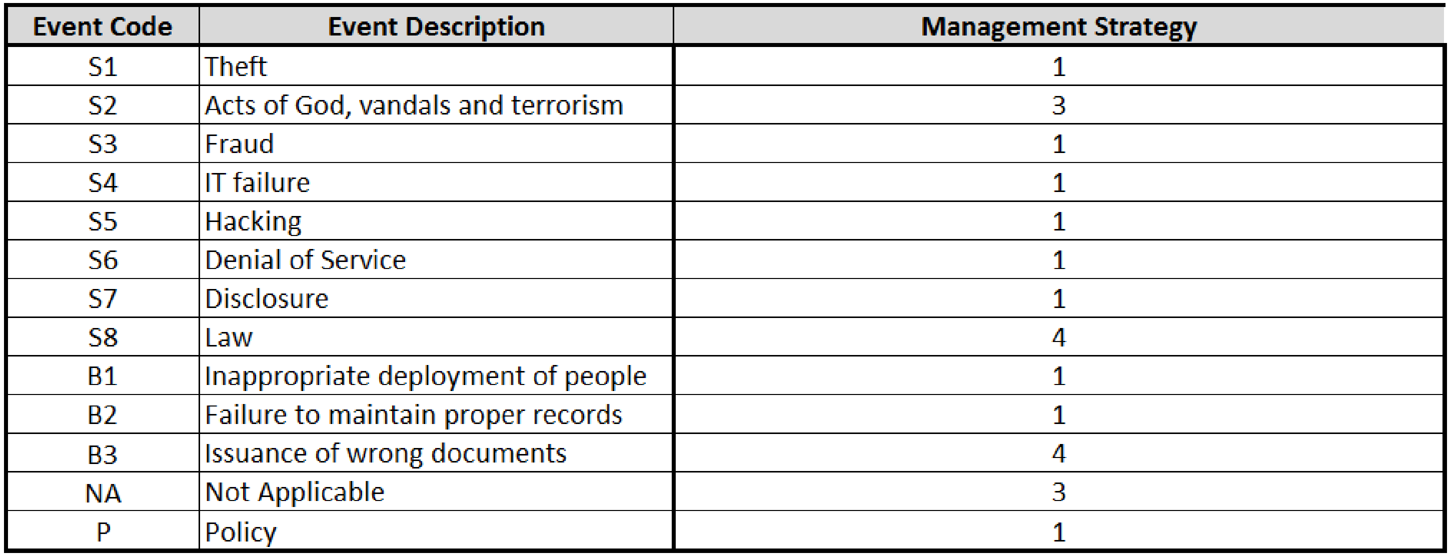
Event Code	Event Description
S1	Theft
S2	Acts of God, vandals and terrorism
S3	Fraud
S4	IT failure
S5	Hacking
S6	Denial of Service
S7	Disclosure
S8	Law
B1	Inappropriate deployment of people
B2	Failure to maintain proper records
B3	Issuance of wrong documents
NA	Not Applicable
P	Policy

Risk Management Strategies

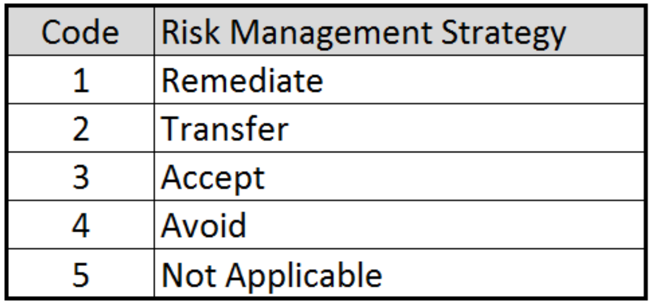


Code	Risk Management Strategy
1	Remediate
2	Transfer
3	Accept
4	Avoid
5	Not Applicable

Applying the Brewer Events with Risk Management Strategies



Event Code	Event Description	Management Strategy
S1	Theft	1
S2	Acts of God, vandals and terrorism	3
S3	Fraud	1
S4	IT failure	1
S5	Hacking	1
S6	Denial of Service	1
S7	Disclosure	1
S8	Law	4
B1	Inappropriate deployment of people	1
B2	Failure to maintain proper records	1
B3	Issuance of wrong documents	4
NA	Not Applicable	3
P	Policy	1



Code	Risk Management Strategy
1	Remediate
2	Transfer
3	Accept
4	Avoid
5	Not Applicable

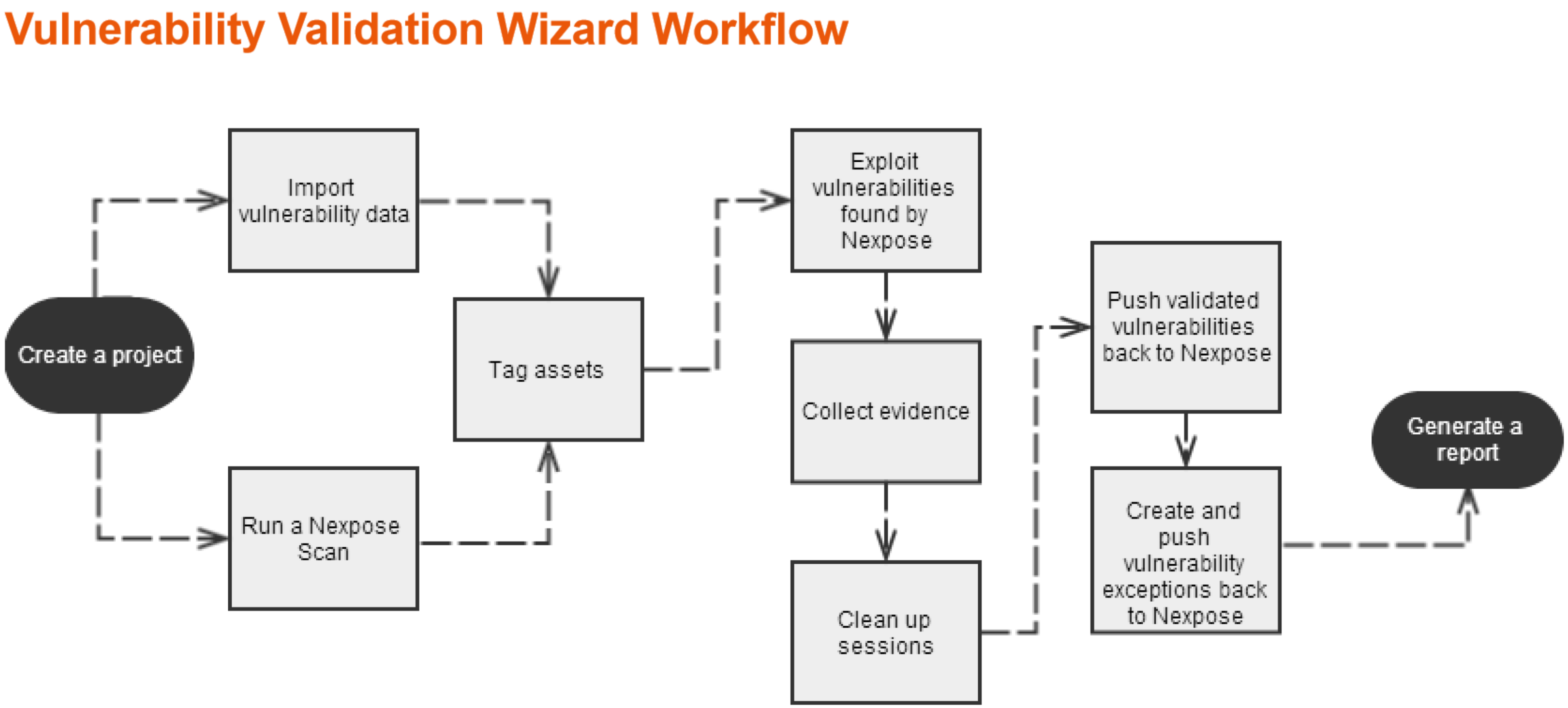
TOOLS

Tools:

- Scanners
  - Nexpose
  - IBM VMS
  - Nessus
  - Netcat

Tools:

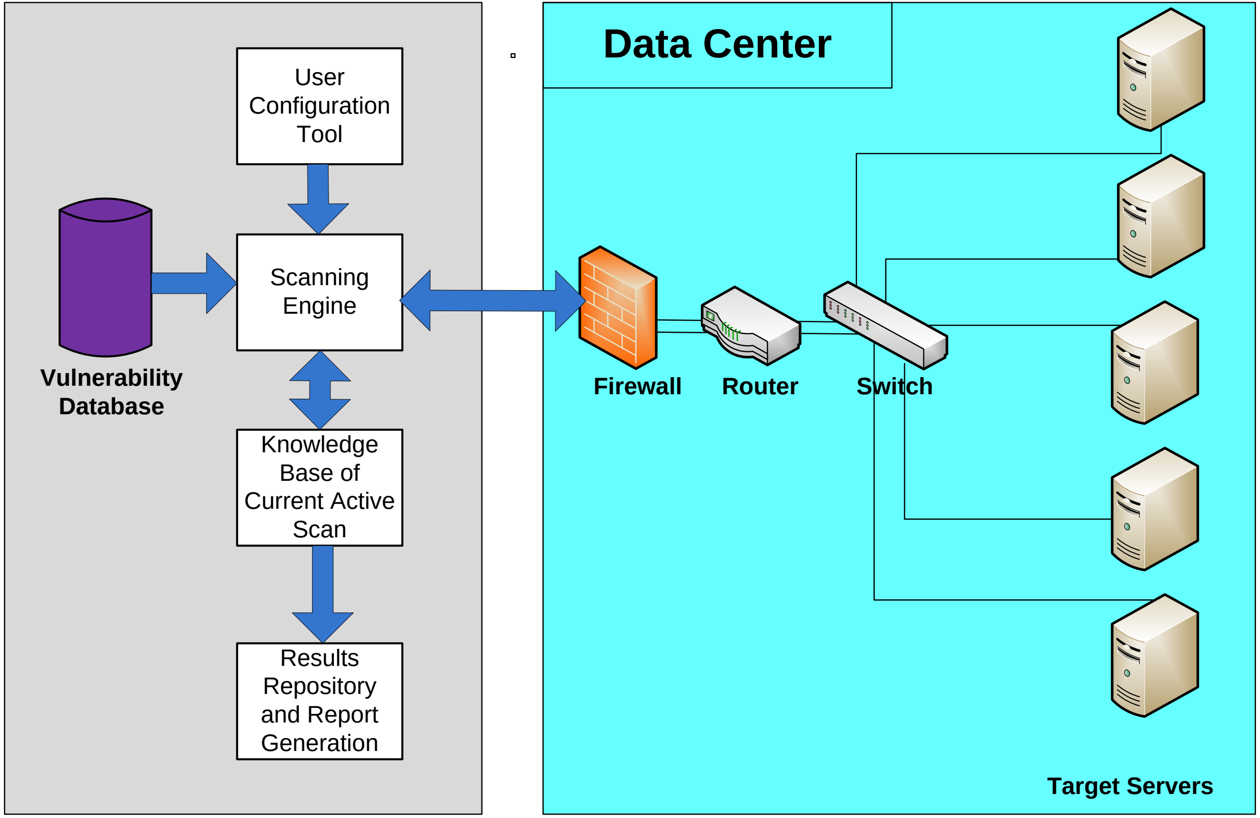
- Nexpose



Vulnerability Validation Wizard Workflow
Create a project
Import vulnerability data
Run a Nexpose Scan
Tag assets
Exploit vulnerabilities found by Nexpose
Collect evidence
Clean up sessions
Push validated vulnerabilities back to Nexpose
Create and push vulnerability exceptions back to Nexpose
Generate a report

Source: Rapid7

Tools: Generic Vulnerability Scanning



Generic Vulnerability Scanner Architecture on A Scanning Server

Technical Notes:
1) It is standard practice to *white list* the IP address of your scanner at the Firewall and other IDPS Devices.
2) The scanner probes for active IP addresses and open ports, and associates them with what it finds with the Vulnerability Database.

Source: Skoudis, E. (2006), Counter Hack Reloaded.

PLANNING YOUR SCANNING

Planning Your Scanning

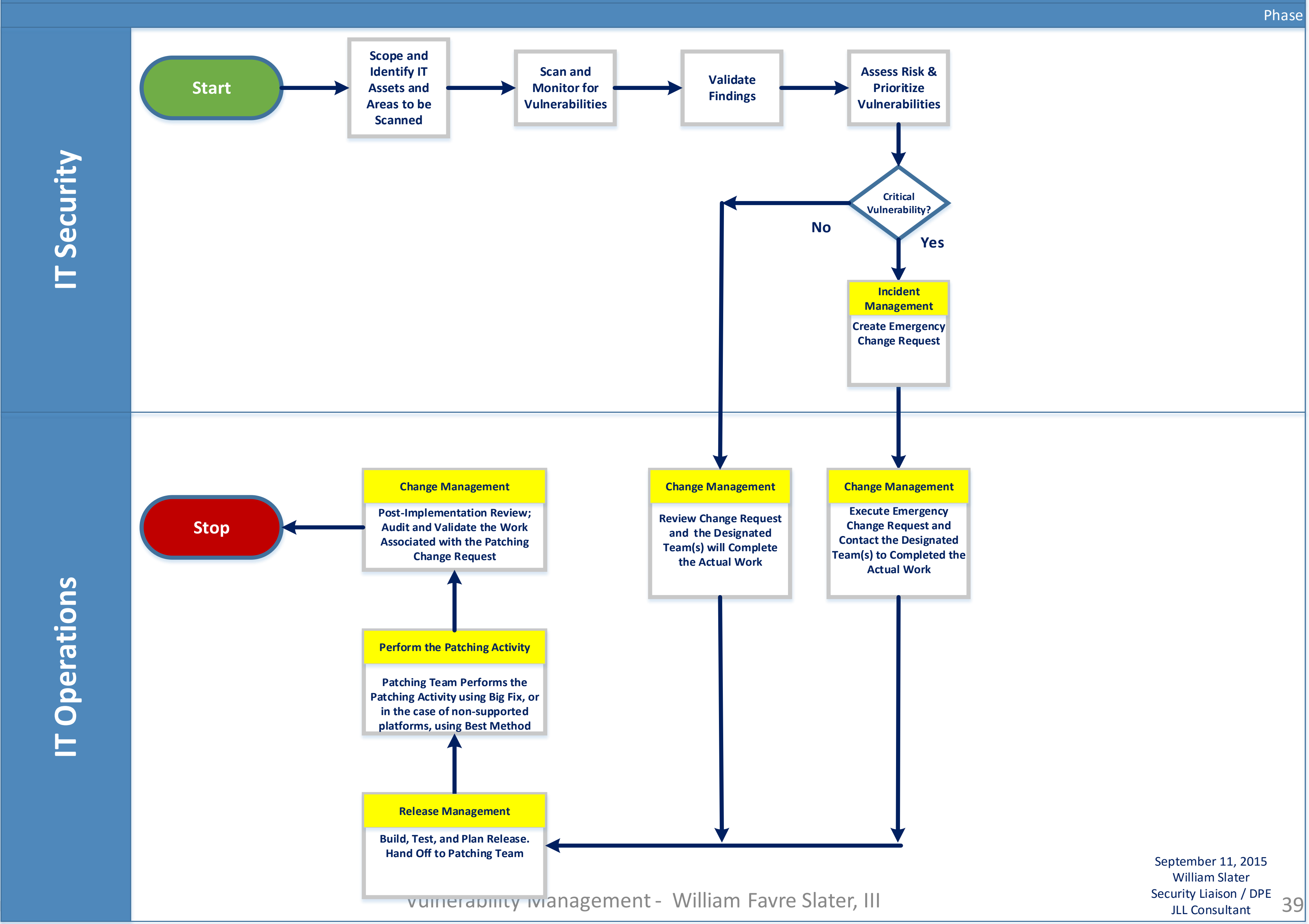
- Get Management Support
- Create a Project Plan
- Change Management Request and Approval
- Examples available upon request
- Publish organization-wide announcements before and after the scans complete.
- Do the Vulnerability Scan during the approved change window.
- Note: If a server or network device goes down during or shortly after your scanning, YOU WILL BE BLAMED FOR IT, so document EVERYTHING.

VULNERABILITY MANAGEMENT & REPORTING

Vulnerability Management

- Get Management Support
- Create a good Vulnerability Management Policy
- Create a good Vulnerability Management Program
- Create a good Remediation Management Program

Vulnerability Management



Phase

IT Security

IT Operations

Start

Scope and Identify IT Assets and Areas to be Scanned

Scan and Monitor for Vulnerabilities

Validate Findings

Assess Risk & Prioritize Vulnerabilities

Critical Vulnerability?

No

Yes

Incident Management

Create Emergency Change Request

Change Management

Execute Emergency Change Request and Contact the Designated Team(s) to Completed the Actual Work

Change Management

Review Change Request and the Designated Team(s) will Complete the Actual Work

Release Management

Build, Test, and Plan Release. Hand Off to Patching Team

Perform the Patching Activity

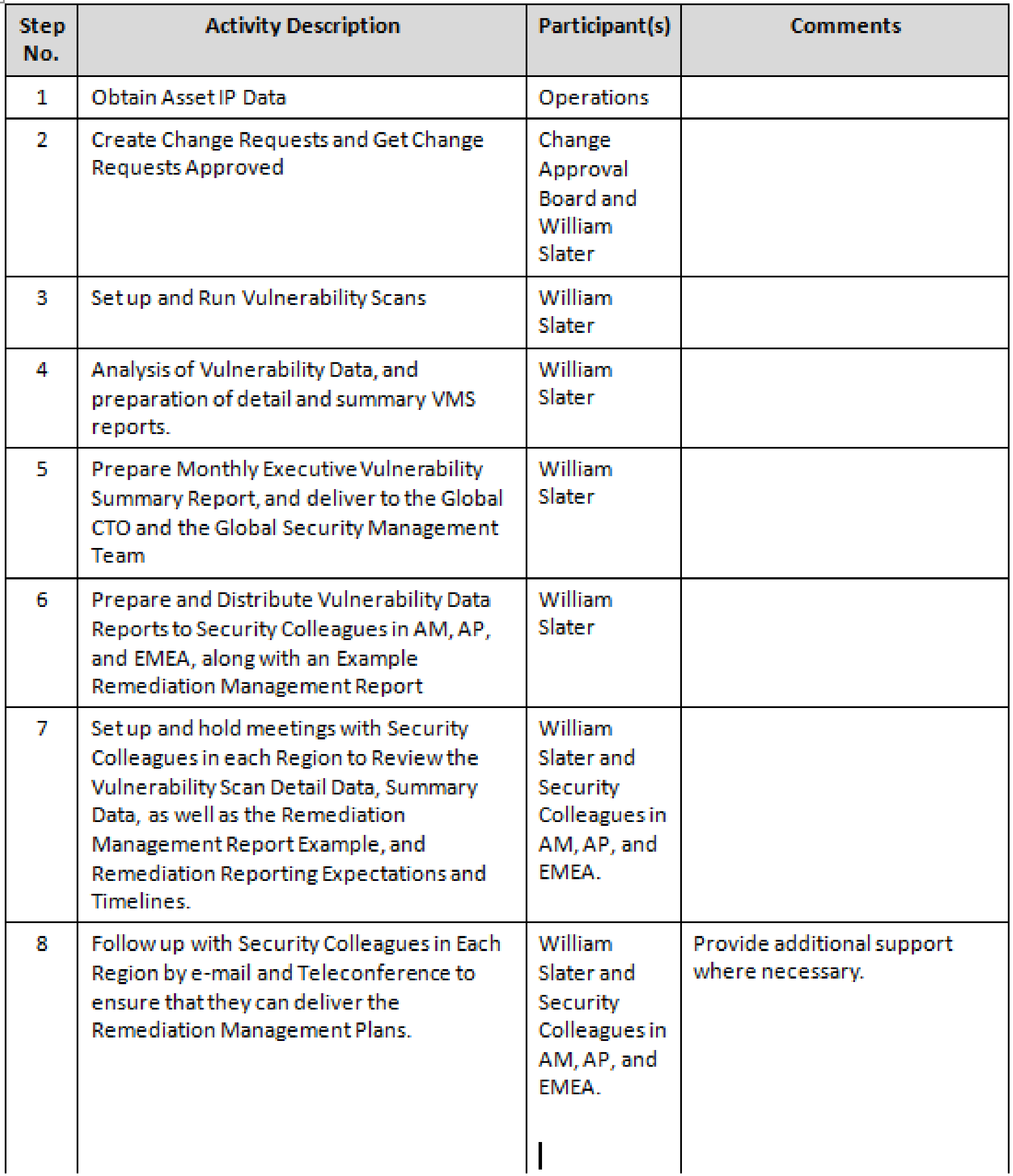
Patching Team Performs the Patching Activity using Big Fix, or in the case of non-supported platforms, using Best Method

Change Management

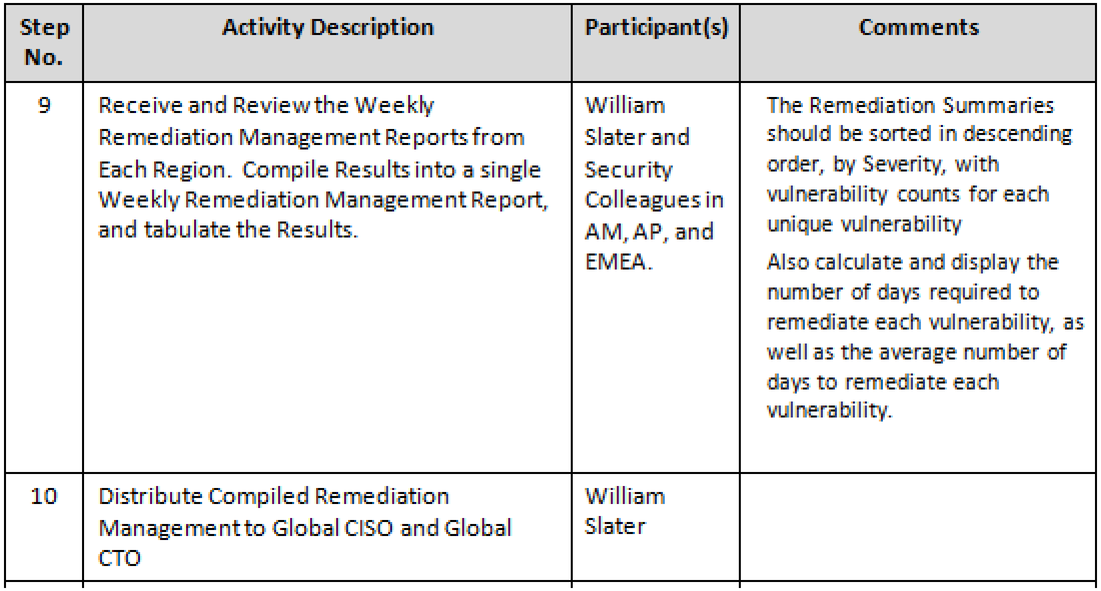
Post-Implementation Review; Audit and Validate the Work Associated with the Patching Change Request

Stop

September 11, 2015
William Slater
Security Liaison / DPE
JLL Consultant



Step No.	Activity Description	Participant(s)	Comments
1	Obtain Asset IP Data	Operations	
2	Create Change Requests and Get Change Requests Approved	Change Approval Board and William Slater	
3	Set up and Run Vulnerability Scans	William Slater	
4	Analysis of Vulnerability Data, and preparation of detail and summary VMS reports.	William Slater	
5	Prepare Monthly Executive Vulnerability Summary Report, and deliver to the Global CTO and the Global Security Management Team	William Slater	
6	Prepare and Distribute Vulnerability Data Reports to Security Colleagues in AM, AP, and EMEA, along with an Example Remediation Management Report	William Slater	
7	Set up and hold meetings with Security Colleagues in each Region to Review the Vulnerability Scan Detail Data, Summary Data, as well as the Remediation Management Report Example, and Remediation Reporting Expectations and Timelines.	William Slater and Security Colleagues in AM, AP, and EMEA.	
8	Follow up with Security Colleagues in Each Region by e-mail and Teleconference to ensure that they can deliver the Remediation Management Plans.	William Slater and Security Colleagues in AM, AP, and EMEA.	Provide additional support where necessary.



Step No.	Activity Description	Participant(s)	Comments
9	Receive and Review the Weekly Remediation Management Reports from Each Region. Compile Results into a single Weekly Remediation Management Report, and tabulate the Results.	William Slater and Security Colleagues in AM, AP, and EMEA.	The Remediation Summaries should be sorted in descending order, by Severity, with vulnerability counts for each unique vulnerability Also calculate and display the number of days required to remediate each vulnerability, as well as the average number of days to remediate each vulnerability.
10	Distribute Compiled Remediation Management to Global CISO and Global CTO	William Slater	

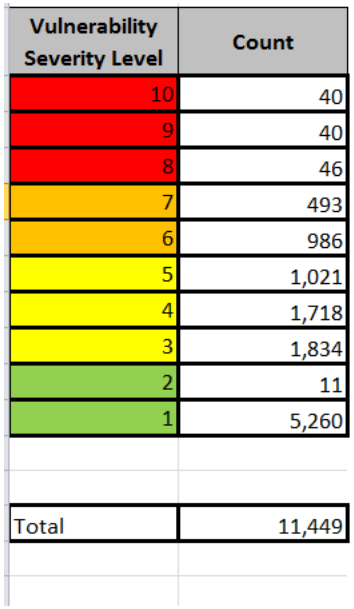
Vulnerability Reports

- **Detail reports**
  - To operations groups (Network Teams, and Server Teams)
- **Summary by region, device, and severity**
  - (To operations groups (Network Teams, and Server Teams)
- **Monthly Executive Summaries** (to Global CTO, Global CISO, Regional CIOs, CTOs, and CISOs)
- **Ad Hoc Reports** – for Auditors, Managers, etc.

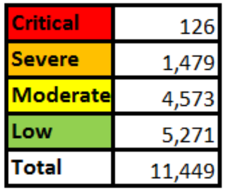
- **Strong Advice:** Keep all your Data, Queries, Reports, E-mails, Meeting Requests, Meeting Minutes, etc. And have naming standards so you can easily find stuff.

Vulnerability Reports

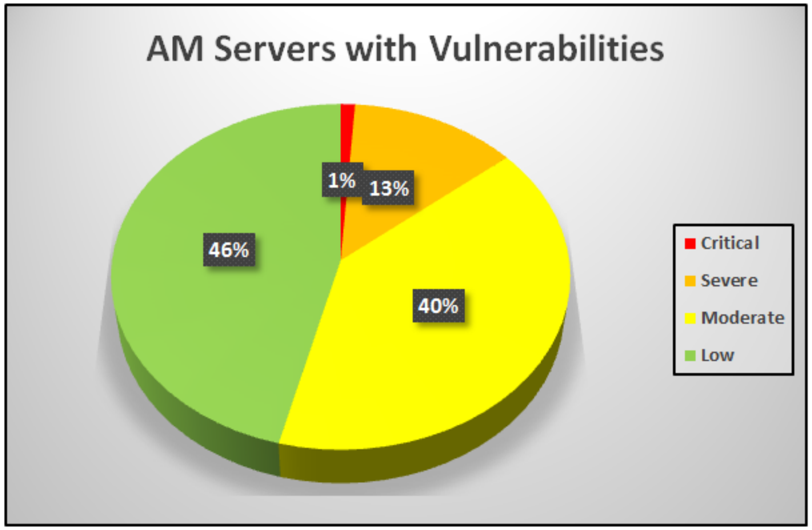
- Summary by region, device, and severity
  - (To operations groups (Network Teams, and Server Teams)



Vulnerability Severity Level	Count
10	40
9	40
8	46
7	493
6	986
5	1,021
4	1,718
3	1,834
2	11
1	5,260
Total	11,449



Critical	126
Severe	1,479
Moderate	4,573
Low	5,271
Total	11,449



AM Servers with Vulnerabilities

Vulnerability Reports

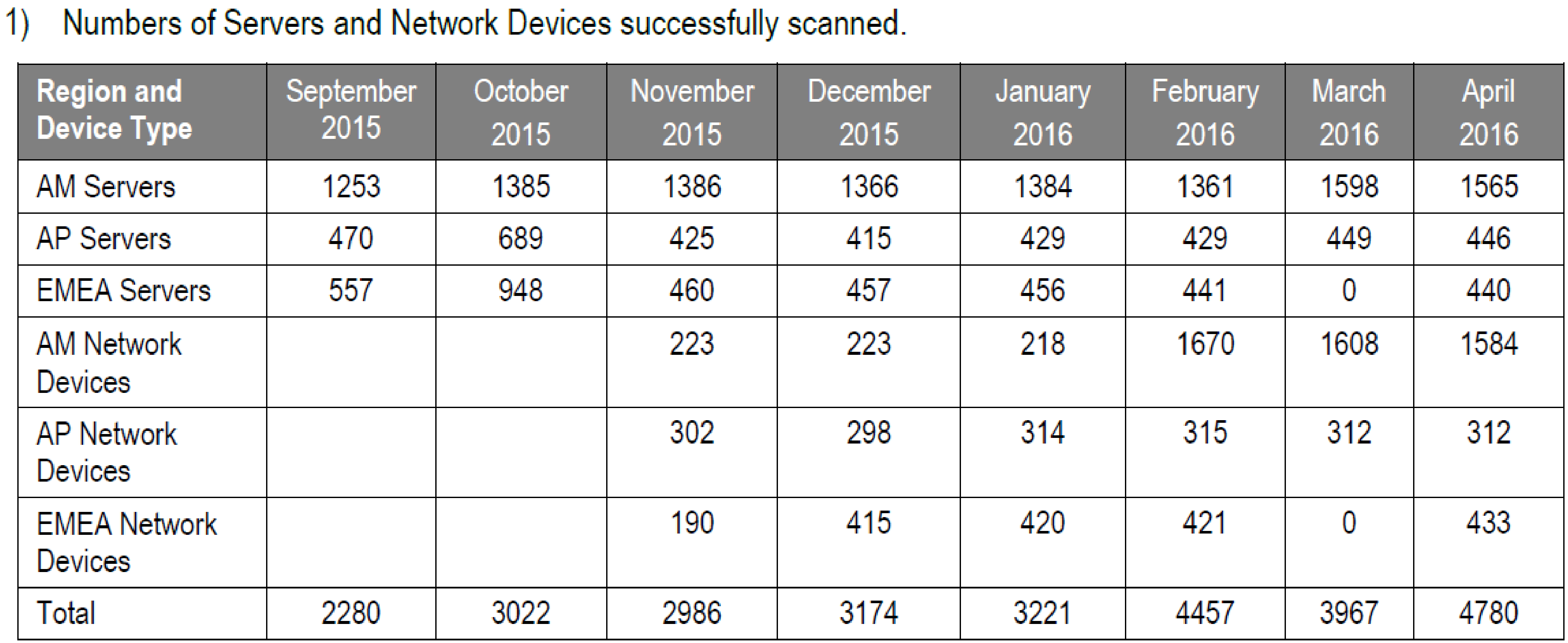
- Summary by region, device, and severity
  - To operations groups (Network Teams, and Server Teams)
  - SQL Statement (from MS Access):

```
SELECT DISTINCT AM_Servers_Combined_2016_0520_VULN.[Vulnerability Severity Level],
Count(AM_Servers_Combined_2016_0520_VULN.[Vulnerability ID]) AS
[CountOfVulnerability ID]
FROM AM_Servers_Combined_2016_0520_VULN
GROUP BY AM_Servers_Combined_2016_0520_VULN.[Vulnerability Severity Level]
ORDER BY AM_Servers_Combined_2016_0520_VULN.[Vulnerability Severity Level] DESC;
```

Query name: AM_Servers_with_VULN_Summary_Counts_2016_0520

Vulnerability Reports

- Executive Summaries (to CIO, CTO, CISO, etc.)

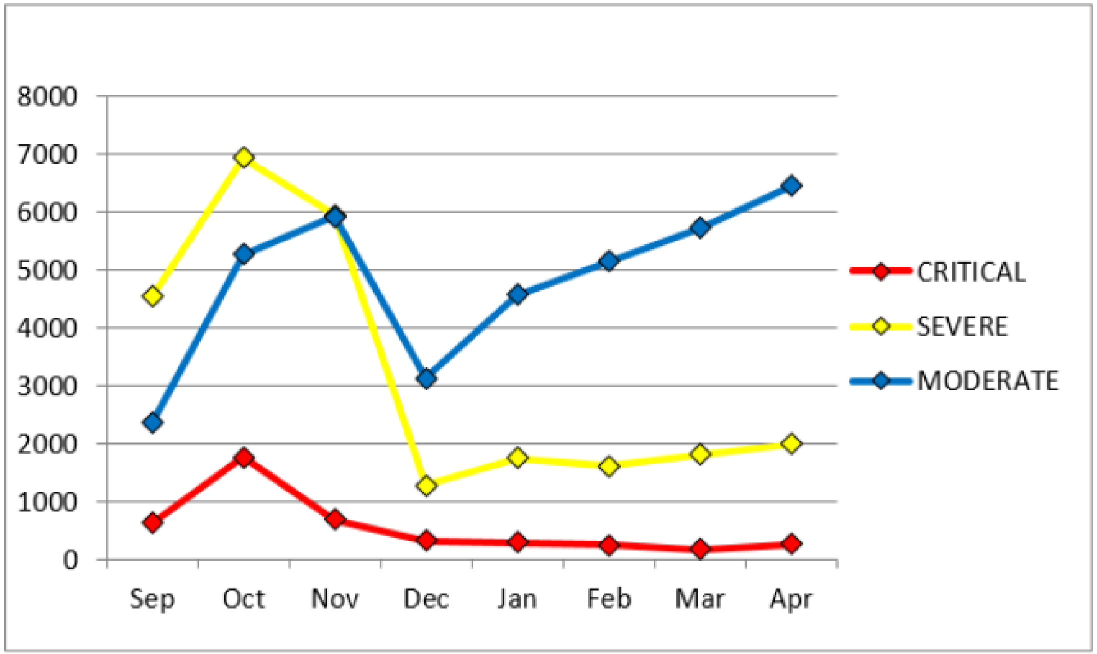


1) Numbers of Servers and Network Devices successfully scanned.

Region and Device Type	September 2015	October 2015	November 2015	December 2015	January 2016	February 2016	March 2016	April 2016
AM Servers	1253	1385	1386	1366	1384	1361	1598	1565
AP Servers	470	689	425	415	429	429	449	446
EMEA Servers	557	948	460	457	456	441	0	440
AM Network Devices			223	223	218	1670	1608	1584
AP Network Devices			302	298	314	315	312	312
EMEA Network Devices			190	415	420	421	0	433
Total	2280	3022	2986	3174	3221	4457	3967	4780

Vulnerability Reports

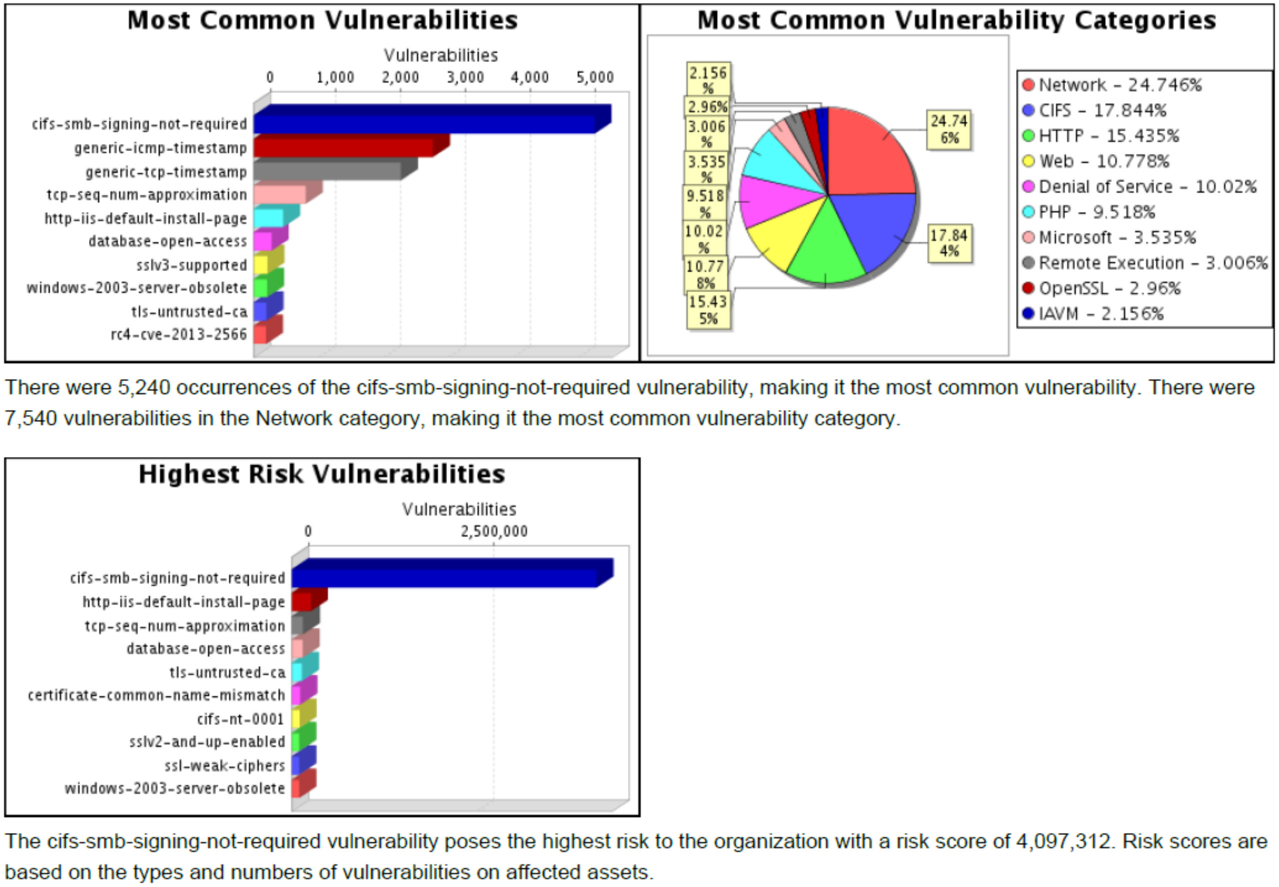
- Executive Summaries (to CIO, CTO, CISO, etc.)



Open Vulnerabilities on Servers by Severity

Vulnerability Reports

- Executive Summaries



Most Common Vulnerabilities

Most Common Vulnerability Categories

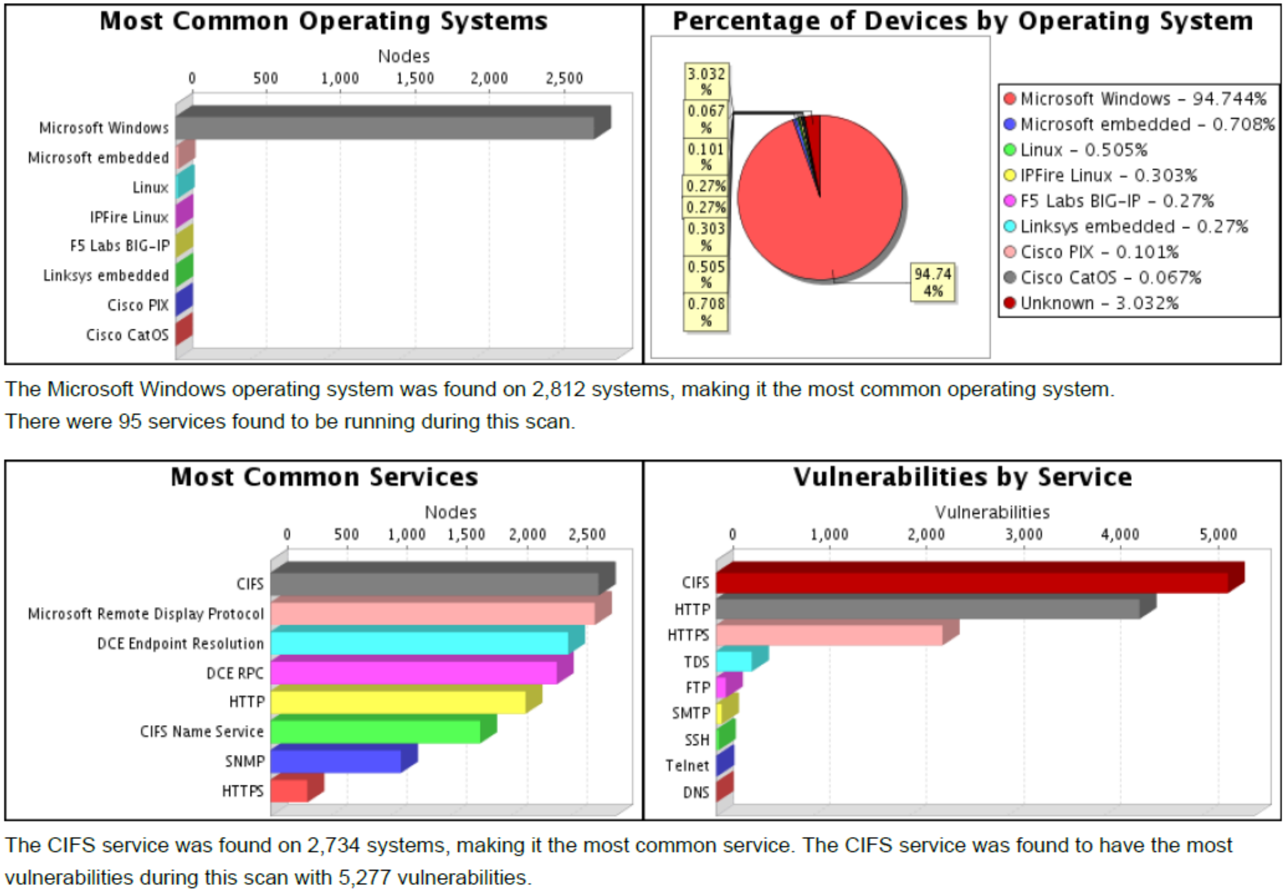
There were 5,240 occurrences of the cifs-smb-signing-not-required vulnerability, making it the most common vulnerability. There were 7,540 vulnerabilities in the Network category, making it the most common vulnerability category.

Highest Risk Vulnerabilities

The cifs-smb-signing-not-required vulnerability poses the highest risk to the organization with a risk score of 4,097,312. Risk scores are based on the types and numbers of vulnerabilities on affected assets.

Vulnerability Reports

- Executive Summaries



Most Common Operating Systems

Percentage of Devices by Operating System

The Microsoft Windows operating system was found on 2,812 systems, making it the most common operating system.

There were 95 services found to be running during this scan.

Most Common Services

Vulnerabilities by Service

The CIFS service was found on 2,734 systems, making it the most common service. The CIFS service was found to have the most vulnerabilities during this scan with 5,277 vulnerabilities.

REMEDIATION MANAGEMENT & REPORTING

Remediation Management & Reporting

- Vulnerabilities are remediated by:
  - Patching
  - Firmware updates
  - Hardening devices
  - Software Upgrades
  - Recommended Settings on Operating Systems and/or Applications
  - Retirement of a vulnerable device

Remediation Management & Reporting

- Remediation reports show what Summaries and Details of what vulnerabilities are getting remediated and how long, on average, it is taking from time of notification to remediation.
- Used to track Security Performance:
  - Critical = 30 days
  - Severe = 60 days
  - Moderate = 90 days
- Alternative to remediation: Have management review and accept the risk of not remediating. This is usually a formal process and must be requested and granted in writing.

Remediation Management & Reporting

- **Detail reports**
  - To operations groups (Network Teams, and Server Teams)
- **Summary by region, device, and severity**
  - (To operations groups (Network Teams, and Server Teams)
- **Monthly Executive Summaries** (to Global CTO, Global CISO, Regional CIOs, CTOs, and CISOs)
- **Ad Hoc Reports** – for Auditors, Managers, etc.

- **Strong Advice:** Keep all your Data, Queries, Reports, E-mails, Meeting Requests, Meeting Minutes, etc. And have naming standards so you can easily find stuff.

Remediation Management Guiding Principles – (1 of 5)

- Run Vulnerability Scans AFTER the Patch Updating Process
- Highest Risk: Confidential Data hosted
- Your Team should use and track metrics (i.e. how many vulnerabilities are getting fixed, etc.)
- You only need to go to the level of granularity where you can easily report
- Your Team needs to define what is “acceptable risk”
- Your Team needs to define its timelines for vulnerability scanning and remediation
- Your Team needs a vulnerability processes created and processes that are repeatable across sites, and easily implemented in the other Regions
- Create a Vulnerability Program Roadmap with a Remediation Plan that will extend into 2017 Q2
- Establish Roles and Responsibilities in the Vulnerability Management Program

Remediation Management Guiding Principles – (2 of 5)

- Create, use and maintain a RACI Chart
- Assign Patching and ensure that competent engineers are doing the patching
- Always review the Patching Cycle Results and the VMS Scan Results
- Find Missing Configurations and Unpatched devices
- Poor Governance and Oversight constitutes high risk
- You want Centralized Oversight with very closed loops (weekly, then semi-monthly)
- Hold engineers that patch servers accountable
- Use VMS to track the vulnerabilities for the Baseline
- Bottom Line: You have visibility so SHOW STEADY PROGRESS
- If possible, correspond attack history and patterns with vulnerabilities

Remediation Management Guiding Principles – (3 of 5)

- Group your VMS Policies by
  - Vendor
  - Servers
  - Routers
  - Switches
  - ASA
  - IDS/IPS
  - Wintel machines
- Add VMS Triage and Priorities because you will not be able to fix everything at once

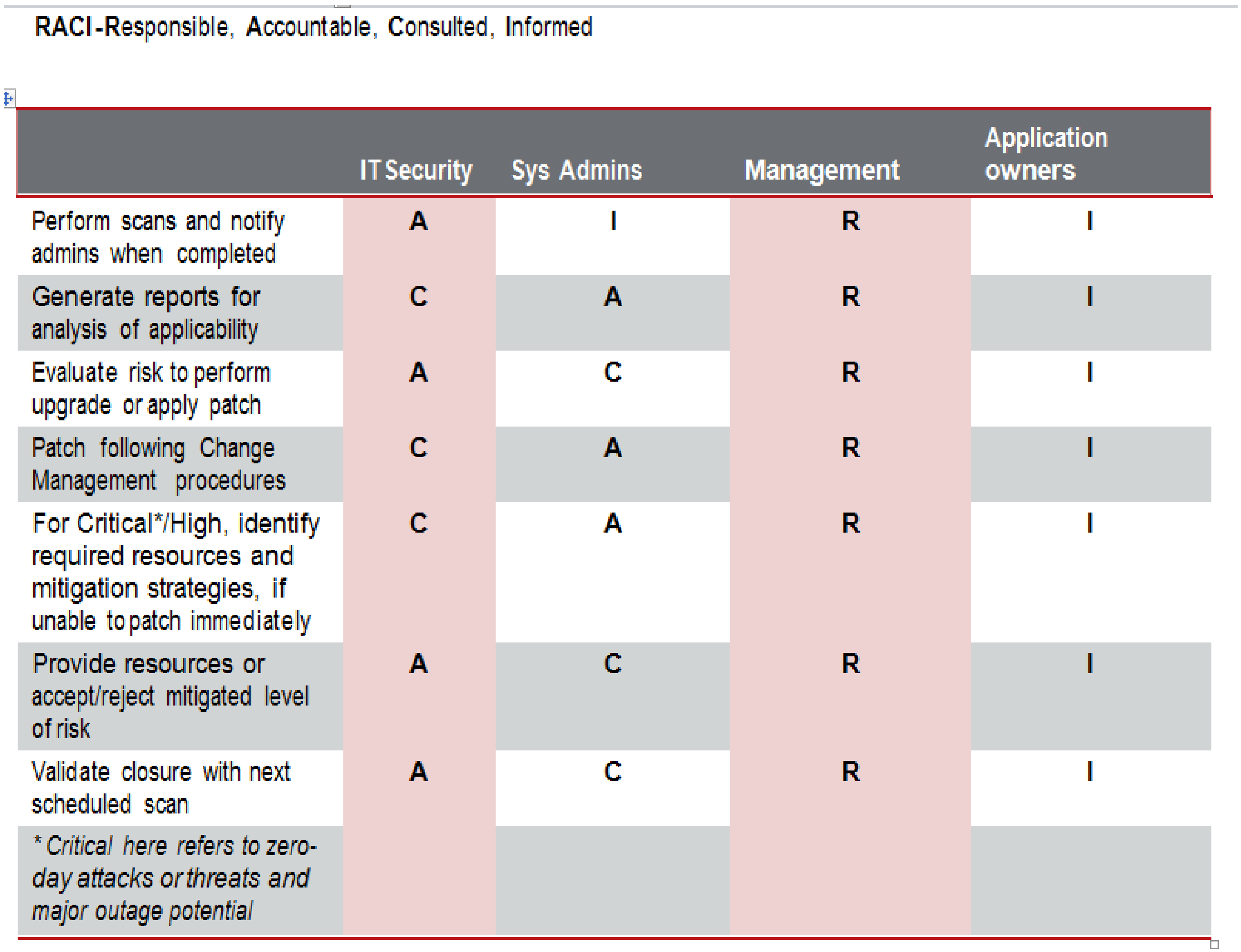
Remediation Management Guiding Principles – (4 of 5)

- Your goals
  - To Manage Risk
  - Improve Your Information Security Management Posture
- Nothing is EASY, especially when everything is MANUAL
- Learn how to Leverage for Reporting and more Management Vulnerability Management Processes
- Learn how to develop and maintain Vulnerability Management Tool Policies
- You will have problems with Bandwidth in terms of being able to manage the efforts that result in Vulnerability Remediation. It requires thoughtful planning and strategic use of resources, because the Enterprise and the Quantity of things to get done are both huge

Remediation Management Guiding Principles – (5 of 5)

- Go for the "Low Hanging Fruit" and get as much done as possible with single consoles like using Group Policy Objects to manage known critical vulnerabilities
- **Create a Project for the Vulnerability Remediations, and get a tough Sponsor – someone with the authority and influence to get results.**
- Have a well-designed Tactical Plan to go fix the vulnerabilities – make it easy to consume
- Make sure the Vulnerability Management Program reflects a well-designed Strategy – make it easy to consume

RACI Chart



RACI-Responsible, Accountable, Consulted, Informed

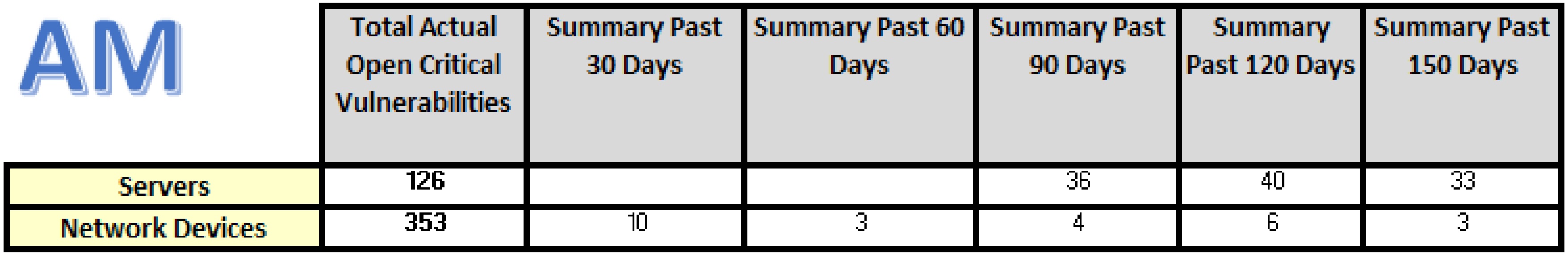
	IT Security	Sys Admins	Management	Application owners
Perform scans and notify admins when completed	A	I	R	I
Generate reports for analysis of applicability	C	A	R	I
Evaluate risk to perform upgrade or apply patch	A	C	R	I
Patch following Change Management procedures	C	A	R	I
For Critical*/High, identify required resources and mitigation strategies, if unable to patch immediately	C	A	R	I
Provide resources or accept/reject mitigated level of risk	A	C	R	I
Validate closure with next scheduled scan	A	C	R	I
** Critical here refers to zero-day attacks or threats and major outage potential*				

VULNERABILITY AGING REPORTING

Vulnerability Aging Reporting

- Vulnerability Aging Reporting tracks an organization security performance and shows how long, on the average, Teams are taking to remediate their vulnerabilities, by Region, Device Type, and Severity

Example:



AM	Total Actual Open Critical Vulnerabilities	Summary Past 30 Days	Summary Past 60 Days	Summary Past 90 Days	Summary Past 120 Days	Summary Past 150 Days
Servers	126			36	40	33
Network Devices	353	10	3	4	6	3

PERSONAL INSIGHTS FROM EXPERIENCE

Personal Insights from Experience

- A Vulnerability Management Program requires a strong project sponsor and continuous strong management report
- Be extremely organized, and set your own artifact naming standards.
- Be disciplined, reliable, accurate, and always conduct yourself with integrity.
- Stay cool, calm, and collected.
- Save *everything*.

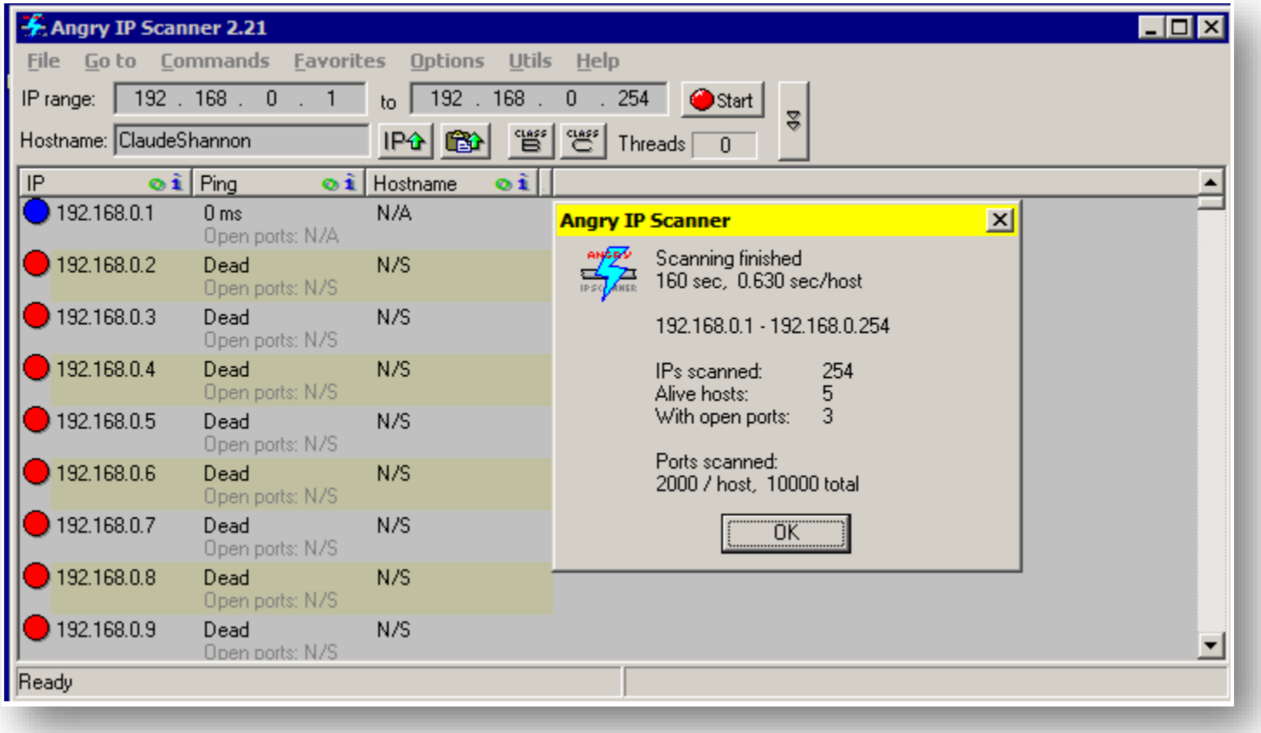
Personal Insights from Experience

- If you want to quickly get up to speed on port scanning, read this paper, Angry IP – An IP Scanner Tool - A Product Analysis and User Tutorial (well documented and fun!)
- Use Tools like Angry IP Scanner and Nexpose to attack your own home network.

Source: http://www.billslater.com/writing/Angry_IP__Scanner_W_F_Slater_2007_0716_.pdf

Personal Insights from Experience

- Angry IP – An IP Scanner Tool - A Product Analysis and User Tutorial



IP range: 192 . 168 . 0 . 1 to 192 . 168 . 0 . 254

Hostname: ClaudeShannon

Threads 0

IP	Ping	Hostname
● 192.168.0.1	0 ms Open ports: N/A	N/A
● 192.168.0.2	Dead Open ports: N/S	N/S
● 192.168.0.3	Dead Open ports: N/S	N/S
● 192.168.0.4	Dead Open ports: N/S	N/S
● 192.168.0.5	Dead Open ports: N/S	N/S
● 192.168.0.6	Dead Open ports: N/S	N/S
● 192.168.0.7	Dead Open ports: N/S	N/S
● 192.168.0.8	Dead Open ports: N/S	N/S
● 192.168.0.9	Dead Open ports: N/S	N/S

Angry IP Scanner

Scanning finished
160 sec, 0.630 sec/host

192.168.0.1 - 192.168.0.254

IPs scanned: 254
Alive hosts: 5
With open ports: 3

Ports scanned:
2000 / host, 10000 total

OK

Ready

Source: http://www.billslater.com/writing/Angry_IP__Scanner_W_F_Slater_2007_0716_.pdf

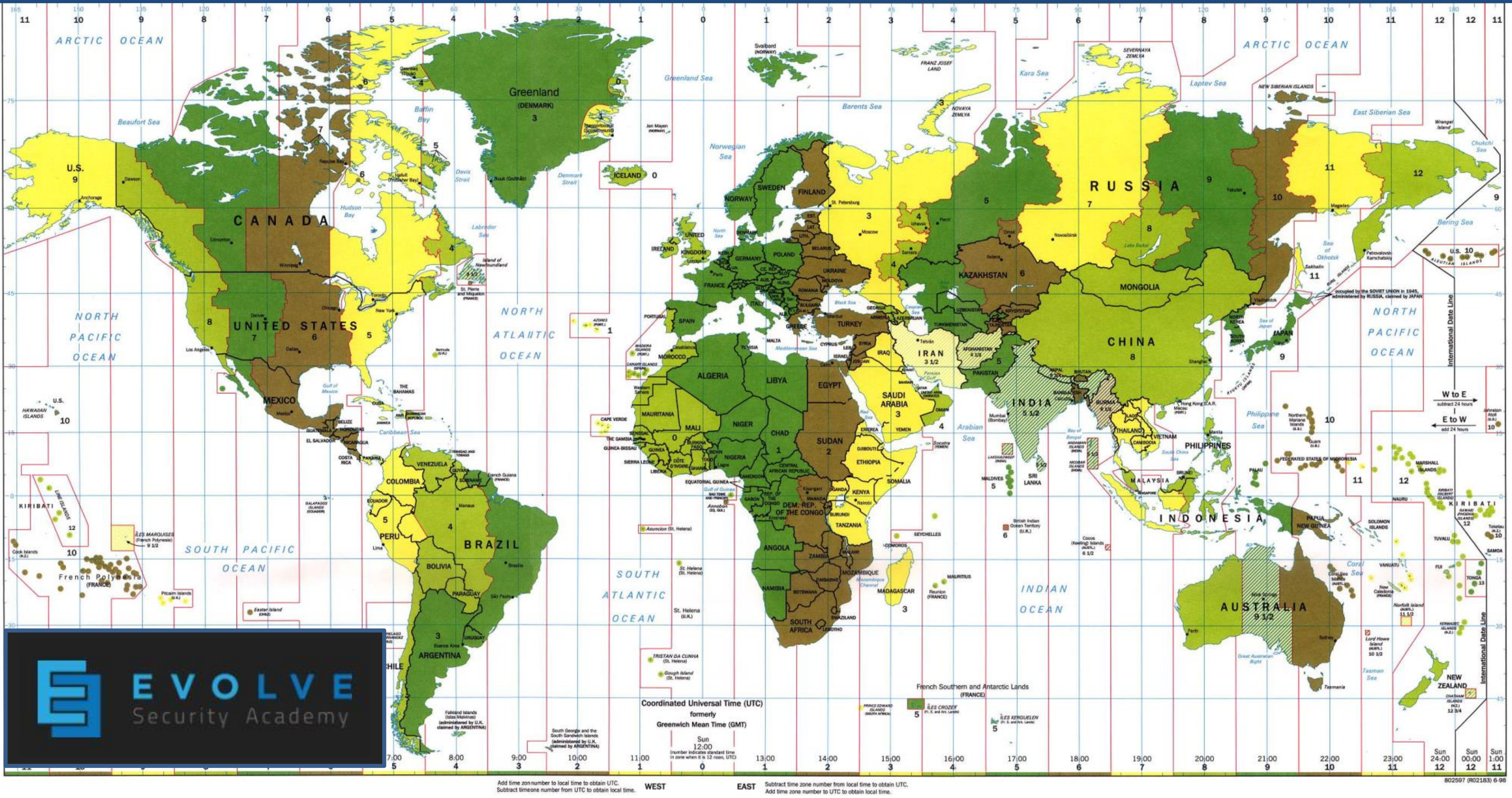
Summary

- Vulnerability Management is an essential part of information security.
- It is as much of a political task as it is a technical task.
- Keep up with your tasks, your schedule, and reporting.
- The ideas in this presentation will help you get on the right track and stay there.
- You will never have a dull day.

Conclusions

- Use ideas from this presentation to create or improve your own Vulnerability Management Program
- If you aren't identifying Vulnerabilities and methodically remediating them, you are leaving your organization exposed to many potential cybersecurity threats.
- Using a mature, organized approach, you can successfully improve your organization's security posture with a well-organized, well-executed Vulnerability Management Program and Remediation Management Program.
- Build strong Teams that will support your efforts in Vulnerability Management and Remediation Management.
- Keep everything because Management AND Auditors will definitely ask for your artifacts and data and documentation, and when you least expect it.

Questions?


ARCTIC OCEAN
Greenland (DENMARK)
Greenland Sea
Barents Sea
Kara Sea
Laptev Sea
East Siberian Sea
Beaufort Sea
Baffin Bay
Norwegian Sea
Hudson Bay
CANADA
U.S.
UNITED STATES
MEXICO
ICELAND
NORWAY
SWEDEN
FINLAND
UNITED KINGDOM
IRELAND
FRANCE
SPAIN
GERMANY
POLAND
UKRAINE
TURKEY
RUSSIA
KAZAKHSTAN
MONGOLIA
CHINA
JAPAN
IRAN 3 1/2
INDIA 5 1/2
PAKISTAN
AFGHANISTAN 4 1/2
SAUDI ARABIA
EGYPT
LIBYA
ALGERIA
MALI
NIGER
CHAD
SUDAN
NIGERIA
ETHIOPIA
KENYA
TANZANIA
DEM. REP. OF THE CONGO
ANGOLA
NAMIBIA
SOUTH AFRICA
MADAGASCAR
NORTH PACIFIC OCEAN
NORTH ATLANTIC OCEAN
SOUTH PACIFIC OCEAN
SOUTH ATLANTIC OCEAN
INDIAN OCEAN
Arabian Sea
VENEZUELA
COLOMBIA
PERU
BRAZIL
BOLIVIA
ARGENTINA
PHILIPPINES
INDONESIA
MALAYSIA
PAPUA NEW GUINEA
AUSTRALIA 9 1/2
NEW ZEALAND
KIRIBATI
French Polynesia (FRANCE)
International Date Line
W to E subtract 24 hours
E to W add 24 hours
Coordinated Universal Time (UTC) formerly Greenwich Mean Time (GMT)
Sun 12:00
WEST
EAST
Add time zone number to local time to obtain UTC. Subtract timeone number from UTC to obtain local time.
Subtract time zone number from local time to obtain UTC. Add time zone number to UTC to obtain local time.
802597 (R02183) 6-98
EVOLVE Security Academy

REFERENCES

References

- AngryIP.org. (2016). Home of Angry IP Scanner. Retrieved from http://angryip.org/ on August 2017.

- Core Security. (2014). The Threat & Vulnerability Management Maturity Model. Retrieved from https://blog.coresecurity.com/2014/10/21/the-threat-and-vulnerability-management-maturity-model/ on September 15, 2015.

- Forrester Group. (2010). The Forrester Wave™: Vulnerability Management, Q2 2010. retrieved from https://www.qualys.com/docs/wave_vulnerability_management_q2_2010.pdf on September 15, 2015.

- Foreman, P. (2009). Vulnerability Management. Auerbach Publications, Boca Raton, FL.

- Gartner Group. (2014). Vulnerability Assessment Technology and Vulnerability Management Practices. Retrieved from https://www.gartner.com/doc/2664022/vulnerability-assessment-technology-vulnerability-management on September 15, 2015.

- Mitre. (2016). Common Vulnerabilities and Exposures. Retrieved from https://cve.mitre.org/ on August 16, 2016.

- NIST. (2013). NIST SP 800-40r3 - Guide to Enterprise Patch Management Technologies. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf on September 13, 2015.

References

- Old Dominion University. (2011). Vulnerability Scanning and Management Procedure. Retrieved from http://www.odu.edu/content/dam/odu/offices/occs/docs/procedures/vulnerability-scanning-management-procedure.pdf on September 15, 2015.

- OWASP. (2016). OWASP Appendix_A: Testing Tools Retrieved from https://www.owasp.org/index.php/Appendix_A:_Testing_Tools August 16, 2016.

- Pondurance. (2011). SVM Part 1 – What is Security Vulnerability Management? Retrieved from https://www.pondurance.com/what-is-svm/ on August 16, 2016.

- Qualsys. (2013). Best Practices For Selecting A Vulnerability Management (VM) Solution. https://www.qualys.com/forms/whitepapers/best-practices-selecting-vulnerability-management-solution/ on September 13, 2015.

- SANS. (2013). Implementing a Vulnerability Management Process. Retrieved from https://www.sans.org/reading-room/whitepapers/threats/implementing-vulnerability-management-process-34180 on August 16, 2016.

- SANS. (2003). Vulnerability Management: Tools, Challenges and Best Bractices. Retrieved from https://www.sans.org/reading-room/whitepapers/threats/vulnerability-management-tools-challenges-practices-1267 on August 16, 2016.

References

- Skoudis, E. and Liston, T. (2006). Counter Hack Reloaded, second edition. Prentice Hall. Upper Saddle River, NJ.

- Skybox. (2014). Next Generation Vulnerability Management. Retrieved from https://www.skyboxsecurity.com/sites/default/files/Whitepaper_Next-Gen_Vulnerability_Management.pdf on August 16, 2016.

- Skybox. (2015). The State of Vulnerability Management Policy. Retrieved from http://blog.skyboxsecurity.com/vulnerability-threat-management/the-state-of-vulnerability-management-policy/ on August 16, 2016.

- Slater, W. F. (2007). Angry IP – An IP Scanner Tool - A Product Analysis and User Tutorial Retrieved from http://www.billslater.com/writing/Angry_IP__Scanner_W_F_Slater_2007_0716_.pdf on August 17, 2016.

- TechTarget. (2014). Vulnerability Management Programs: A Handbook for Security Pros. Retrieved from http://searchsecurity.techtarget.com/ehandbook/Vulnerability-management-programs-A-handbook-for-security-pros on September 13, 2015.

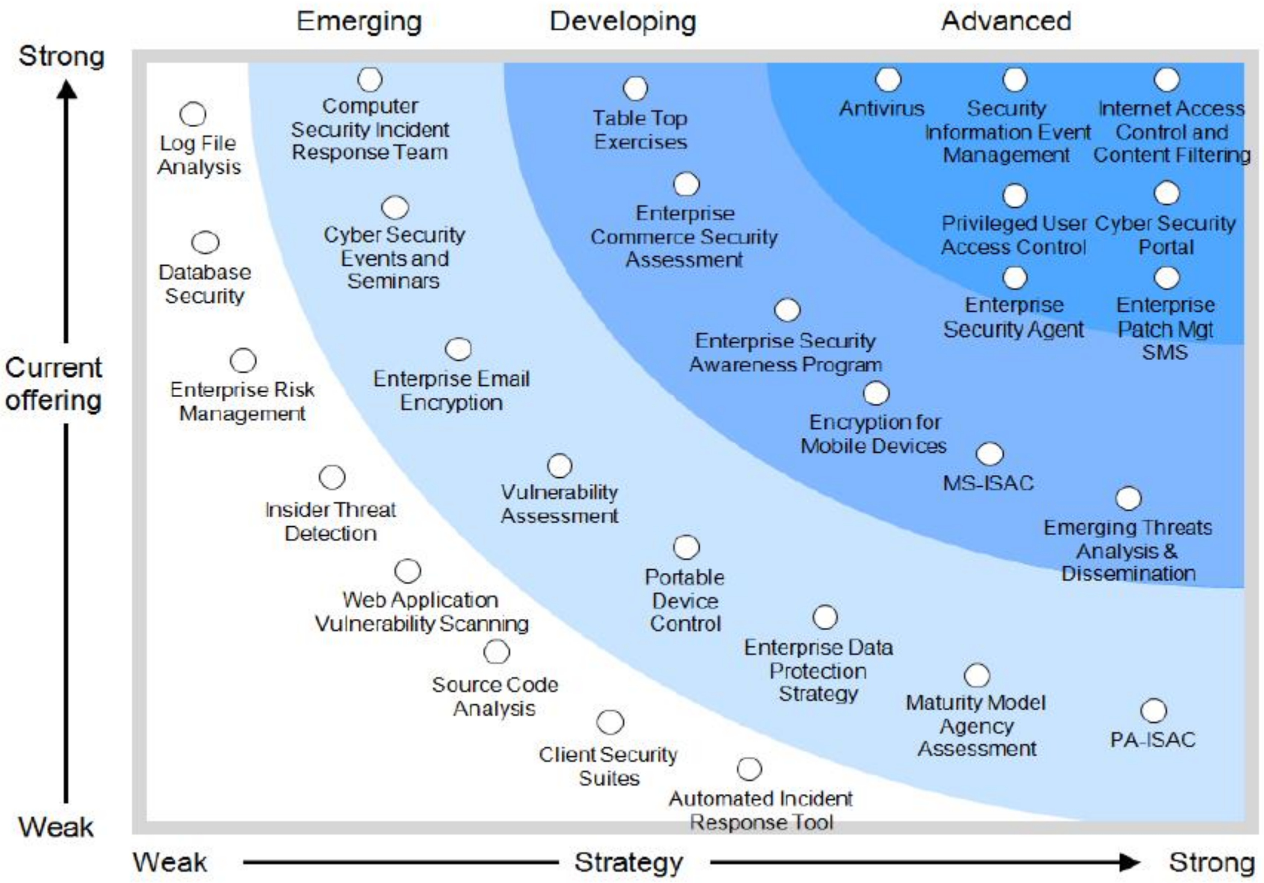
SUPPLEMENTAL SLIDES

National Association of State Chief Information Officers

NASCIO 2012 MIDYEAR CONFERENCE **Navigating IT Challenges**

NASCIO

2008 – 2010 Transition Period

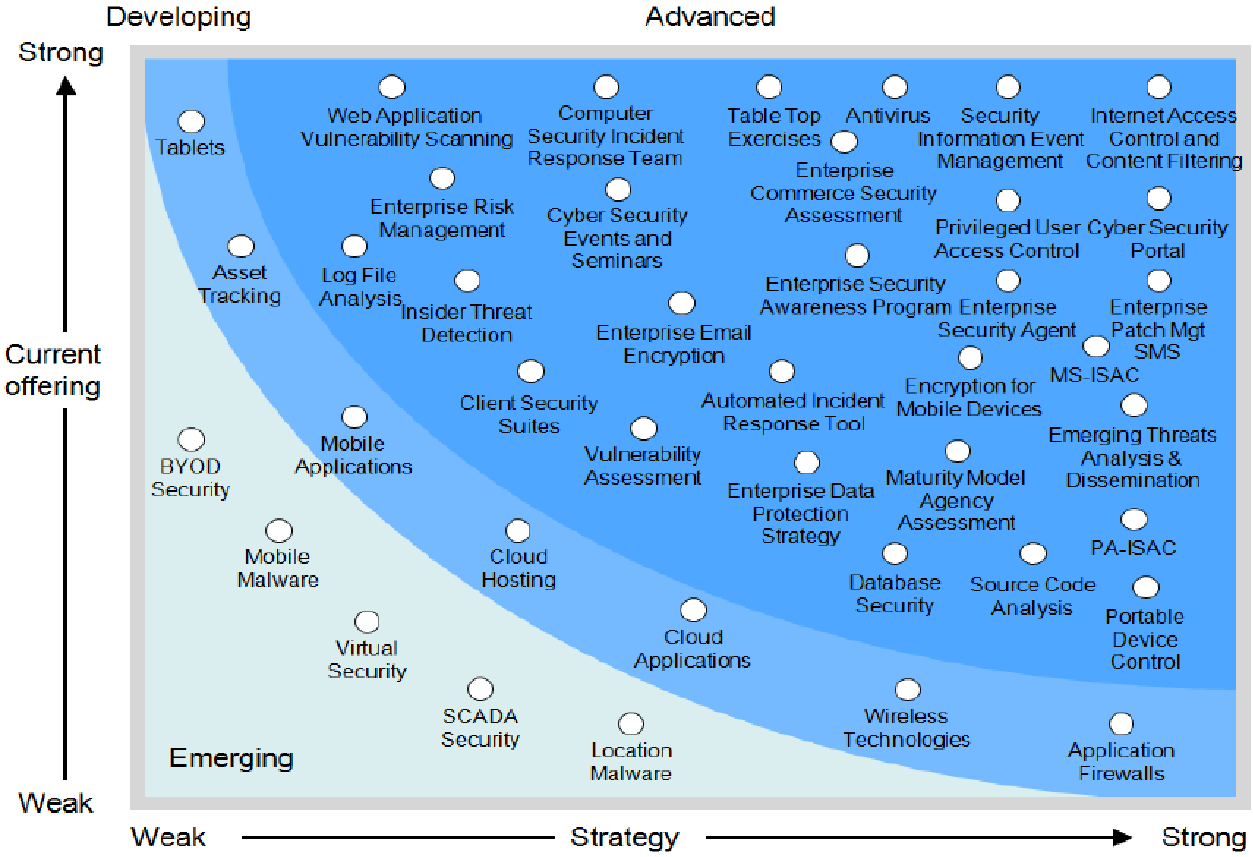

Emerging
Developing
Advanced
Strong
Current offering
Weak
Log File Analysis
Computer Security Incident Response Team
Table Top Exercises
Antivirus
Security Information Event Management
Internet Access Control and Content Filtering
Database Security
Cyber Security Events and Seminars
Enterprise Commerce Security Assessment
Privileged User Access Control
Cyber Security Portal
Enterprise Security Agent
Enterprise Patch Mgt SMS
Enterprise Risk Management
Enterprise Email Encryption
Enterprise Security Awareness Program
Encryption for Mobile Devices
MS-ISAC
Insider Threat Detection
Vulnerability Assessment
Emerging Threats Analysis & Dissemination
Web Application Vulnerability Scanning
Portable Device Control
Source Code Analysis
Enterprise Data Protection Strategy
Maturity Model Agency Assessment
PA-ISAC
Client Security Suites
Automated Incident Response Tool
Weak
Strategy
Strong

National Association of State Chief Information Officers

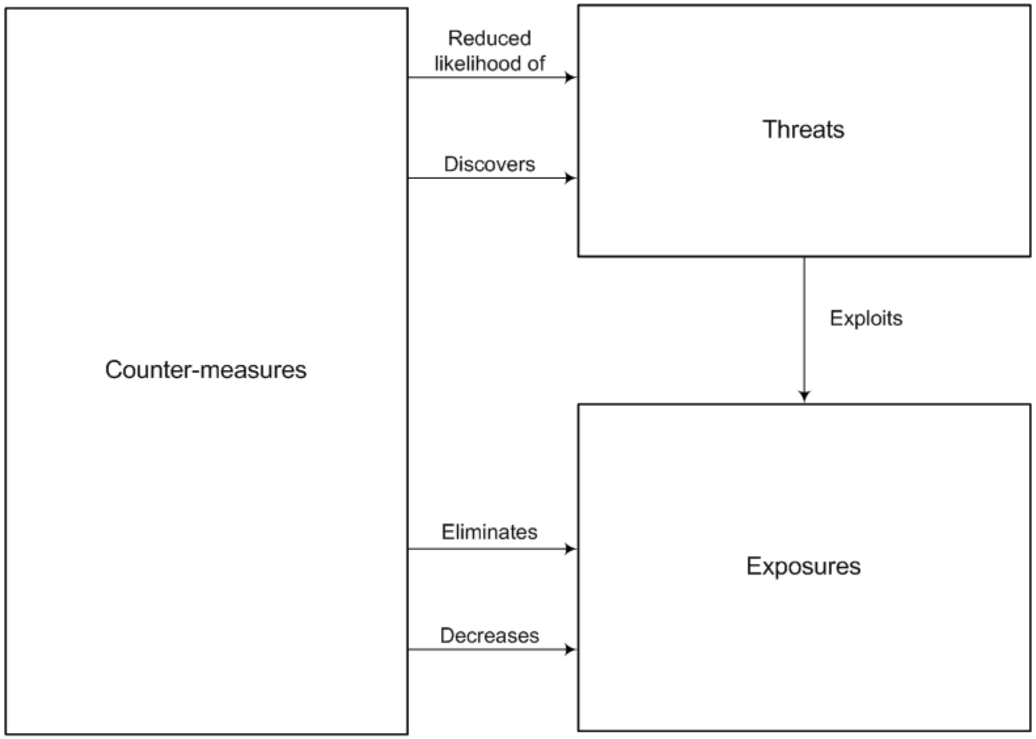
NASCIO 2012 MIDYEAR CONFERENCE

Navigating IT Challenges

2010 – 2012 Post GRC/SOA Implementation



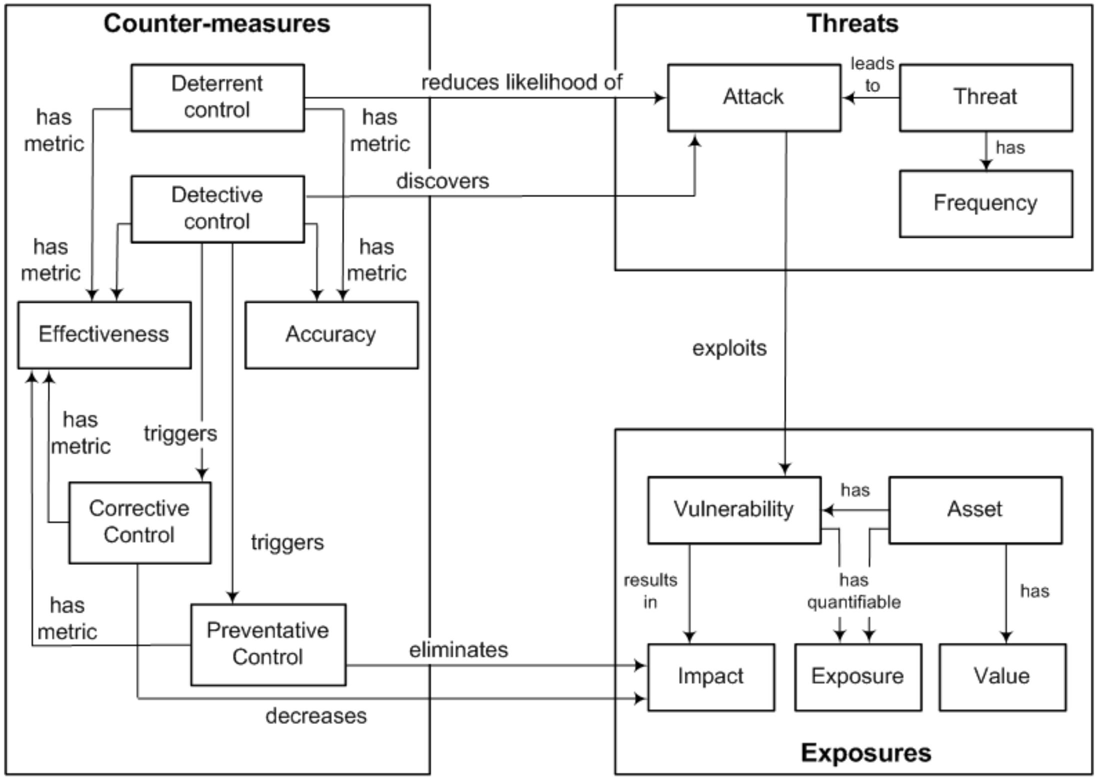
Logical Model for IT Security Management Controls – Level 1



Logical Model of IT Security Management Controls (Level 1)

From Security Metrics by Andrew Jaquith, published by Addison-Wesley, 2007

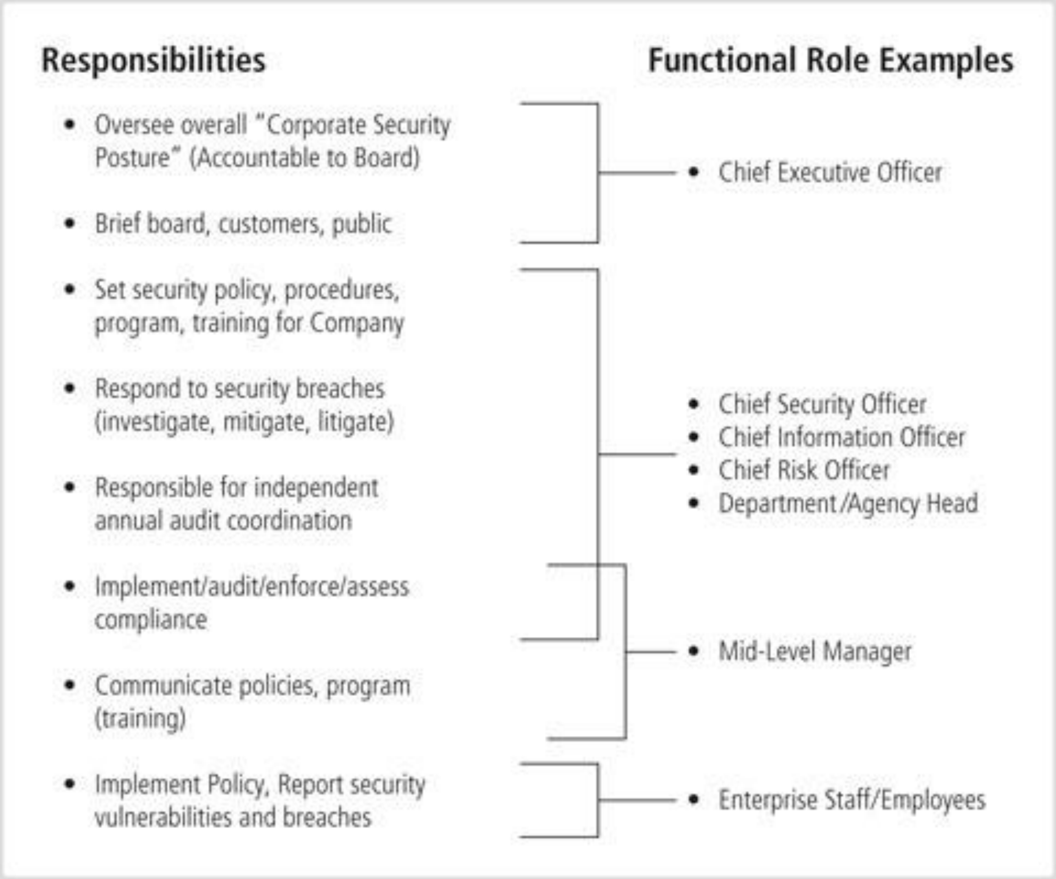
Logical Model for IT Security Management Controls – Level 2



Logical Model of IT Security Management Controls (Level 2)

From Security Metrics by Andrew Jaquith, published by Addison-Wesley, 2007

Planning for Information Security Implementation



Responsibilities

- Oversee overall "Corporate Security Posture" (Accountable to Board)
- Brief board, customers, public
- Set security policy, procedures, program, training for Company
- Respond to security breaches (investigate, mitigate, litigate)
- Responsible for independent annual audit coordination
- Implement/audit/enforce/assess compliance
- Communicate policies, program (training)
- Implement Policy, Report security vulnerabilities and breaches

Functional Role Examples

- Chief Executive Officer

- Chief Security Officer
- Chief Information Officer
- Chief Risk Officer
- Department/Agency Head

- Mid-Level Manager

- Enterprise Staff/Employees

Figure 2-8 Information security governance responsibilities

Source: Course Technology/Cengage Learning (adapted from Whitman, 2013)

Source: *Information Security Governance: A Call to Action*

Planning For Information Security Implementation (cont'd.)

- Implementation can begin
  - After plan has been translated into IT and information security objectives and tactical and operational plans
- Methods of implementation
  - Bottom-up
  - Top-down

Source: Course Technology/Cengage Learning (adapted from Whitman, 2013)

Introduction to the Security Systems Development Life Cycle

- An SDLC is a methodology for the design and implementation of an information system
- SDLC-based projects may be initiated by events or planned
- At the end of each phase, a review occurs to determine if the project should be continued, discontinued, outsourced, or postponed

Source: Course Technology/Cengage Learning (adapted from Whitman, 2013)

Introduction to the Security Systems Development Life Cycle (cont'd.)

- SecSDLC methodology is similar to SDLC
  - – Identification of specific threats and the risks they represent
  - – Design and implementation of specific controls to counter those threats and manage risks posed to the organization

Source: Course Technology/Cengage Learning (adapted from Whitman, 2013)c

Introduction to the Security Systems Development Life Cycle (cont'd.)

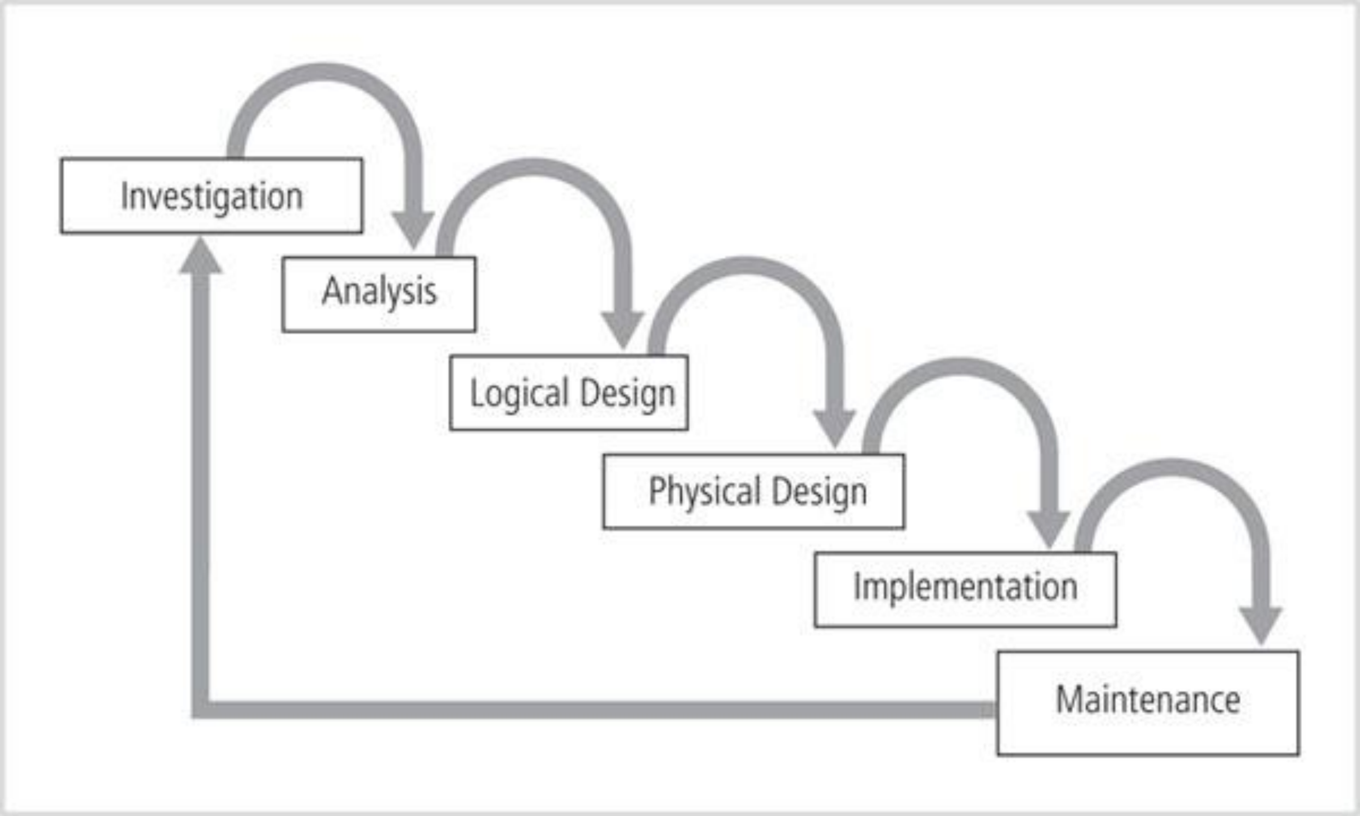


Figure 2-10 Phases of the SecSDLC

Source: Course Technology/Cengage Learning (adapted from Whitman, 2013)c

Introduction to the Security Systems Development Life Cycle

- Analysis in the SecSDLC
- Analyze relevant legal issues that could affect the design of the security solution
  - Risk management begins in this stage
    - The process of identifying, assessing, and evaluating the levels of risk facing the organization, specifically the threats to the information stored and processed by the organization
    - A threat is an object, person, or other entity that represents a constant danger to an asset

Source: Course Technology/Cengage Learning (adapted from Whitman, 2013)

Introduction to the Security Systems Development Life Cycle (cont'd.)

- An attack
  - A deliberate act that exploits a vulnerability to achieve the compromise of a controlled system
  - Accomplished by a threat agent that damages or steals an organization's information or physical assets
- An exploit
  - A technique or mechanism used to compromise a system

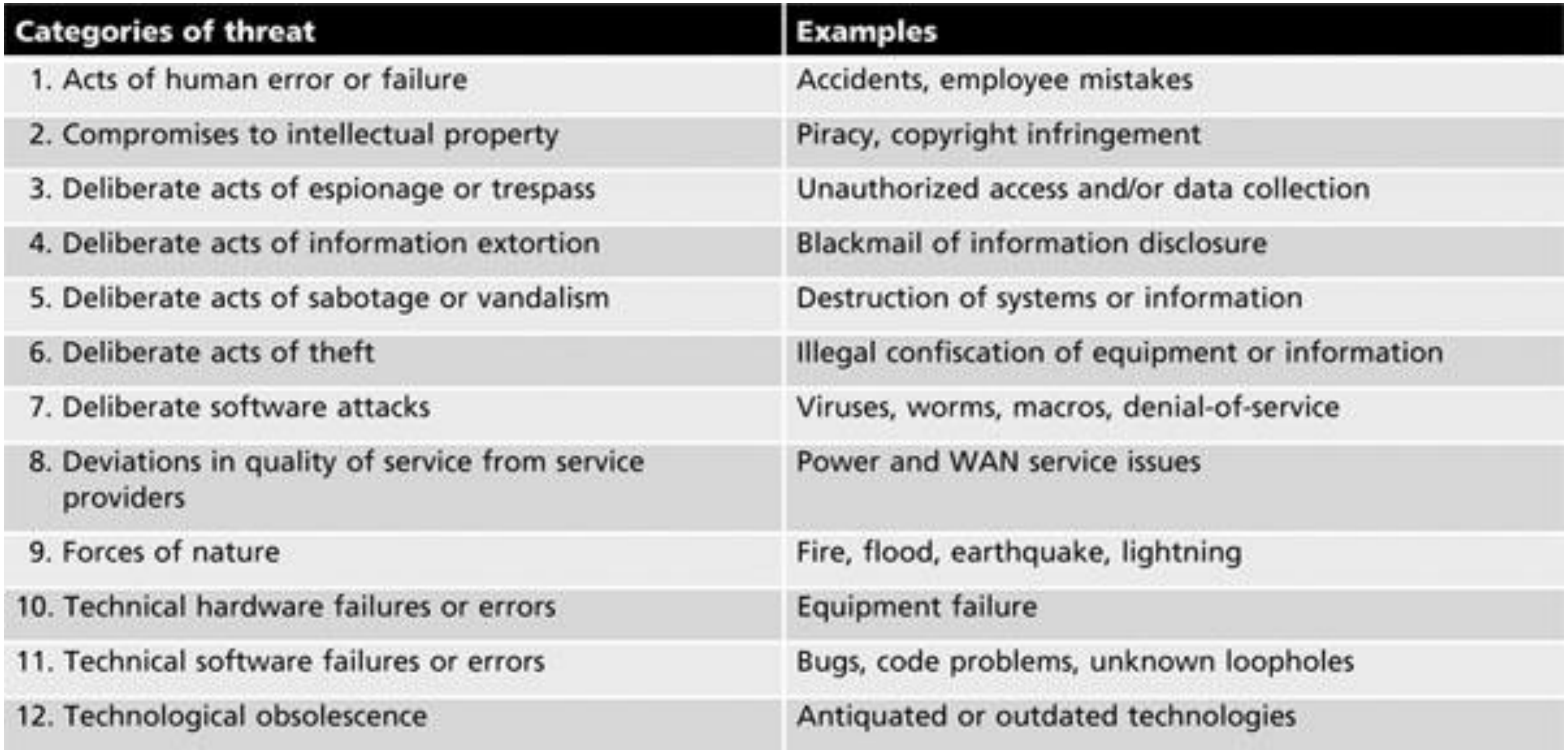
Source: Course Technology/Cengage Learning (adapted from Whitman, 2013)

Introduction to the Security Systems Development Life Cycle (cont'd.)

- A vulnerability
  - An identified weakness of a controlled system in which necessary controls that are not present or are no longer effective

Source: Course Technology/Cengage Learning (adapted from Whitman, 2013)

Introduction to the Security Systems Development Life Cycle (cont’d.)



Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Deviations in quality of service from service providers	Power and WAN service issues
9. Forces of nature	Fire, flood, earthquake, lightning
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

Table 2-1 Threats to Information Security

Source: Course Technology/Cengage Learning
(adapted from Whitman, 2013)

Introduction to the Security Systems Development Life Cycle (cont'd.)

- Some common attacks
  - Malicious code
  - Hoaxes
  - Back doors
  - Password crack
  - Brute force
  - Dictionary
  - Denial-of-service (DoS) and distributed denial-of-service (DDoS)

Source: Course Technology/Cengage Learning (adapted from Whitman, 2013)

Introduction to the Security Systems Development Life Cycle (cont’d.)

- Some common attacks (cont’d.)
  - Spoofing
  - Man-in-the-middle
  - Spam
  - Mail bombing
  - Sniffer
  - Social engineering
  - Buffer overflow
  - Timing

Source: Course Technology/Cengage Learning (adapted from Whitman, 2013)

Introduction to the Security Systems Development Life Cycle (cont'd.)

- Investigation in the SecSDLC
  - Phase begins with directive from management specifying the process, outcomes, and goals of the project and its budget
  - Frequently begins with the affirmation or creation of security policies
  - Teams assembled to analyze problems, define scope, specify goals and identify constraints

Source: Course Technology/Cengage Learning (adapted from Whitman, 2013)

Introduction to the Security Systems Development Life Cycle (cont'd.)

- Investigation in the SecSDLC (cont'd.)
  - Feasibility analysis
    - Determines whether the organization has the resources and commitment to conduct a successful security analysis and design
- Analysis in the SecSDLC
  - Prepare analysis of existing security policies and programs, along with known threats and current controls

Source: Course Technology/Cengage Learning (adapted from Whitman, 2013)

Introduction to the Security Systems Development Life Cycle (cont'd.)

- Prioritize the risk posed by each category of threat
- Identify and assess the value of your information assets
  - Assign a comparative risk rating or score to each specific information asset

Source: Course Technology/Cengage Learning (adapted from Whitman, 2013)

U.S. Department of Veterans Affairs Computer Network Defense Workflows

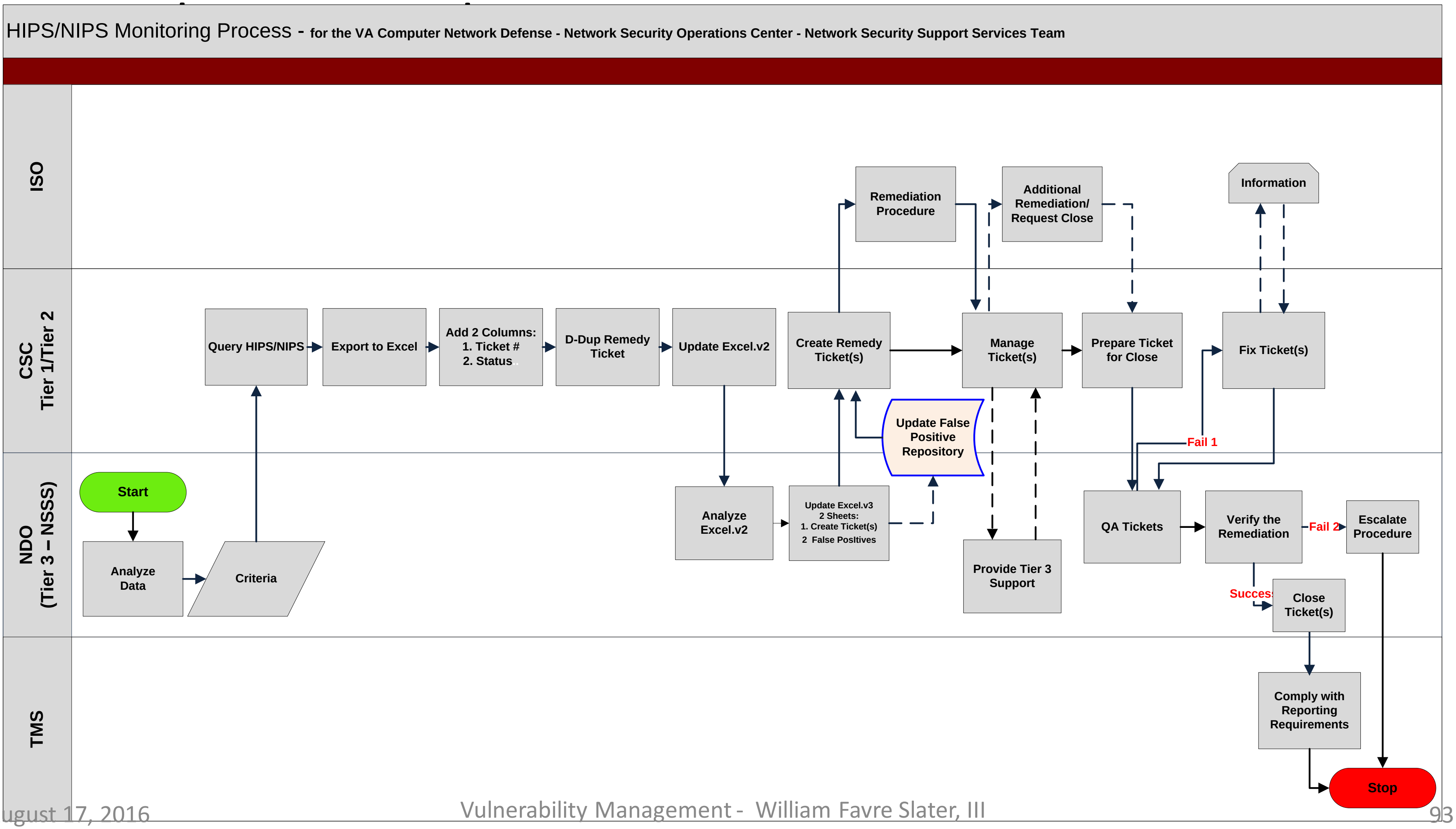
Computer Network Defense (CND)

Four Pillars

- Forensics
- Threat Analysis
- Vulnerability Assessment
- Network Defense Operations (NDO)
  - NSSS Team
- Enterprise Technical Security Officers

Challenges

- The new Custer Support Center – Network Security Support Services (Tier 3) Cooperative Workflow



HIPS/NIPS Monitoring Process - **for the VA Computer Network Defense - Network Security Operations Center - Network Security Support Services Team**

ISO

CSC Tier 1/Tier 2

NDO (Tier 3 – NSSS)

TMS

Start

Analyze Data

Criteria

Query HIPS/NIPS

Export to Excel

Add 2 Columns:
1. Ticket #
2. Status

D-Dup Remedy Ticket

Update Excel.v2

Analyze Excel.v2

Update Excel.v3
2 Sheets:
1. Create Ticket(s)
2 False Positives

Update False Positive Repository

Create Remedy Ticket(s)

Remediation Procedure

Additional Remediation/ Request Close

Manage Ticket(s)

Provide Tier 3 Support

Prepare Ticket for Close

Information

Fix Ticket(s)

Fail 1

QA Tickets

Verify the Remediation

Fail 2

Escalate Procedure

Success

Close Ticket(s)

Comply with Reporting Requirements

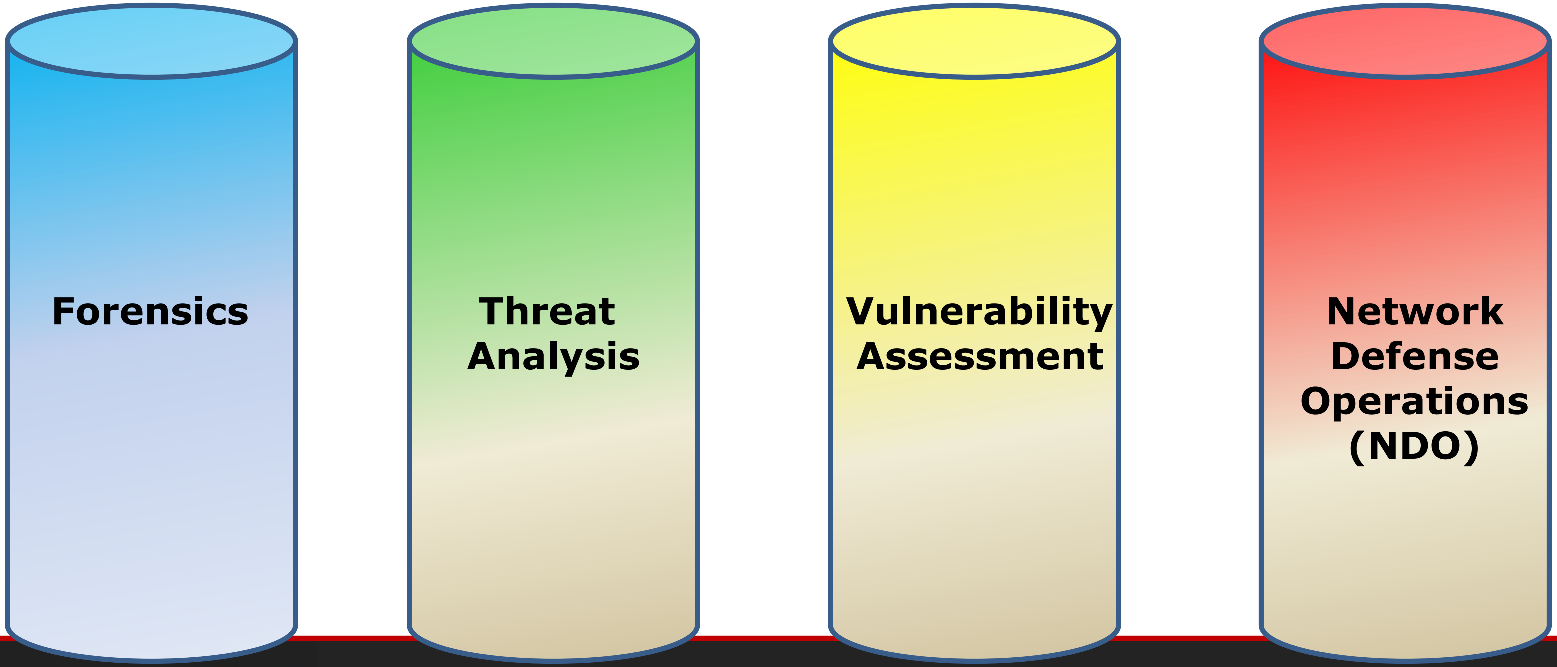
Stop

Network Security Operations Center (NSOC) Mission Statement

The Critical Infrastructure Protection Service, through the VA Network and Security Operations Center (NSOC), defends, manages, and monitors the network operating status and cyber security posture of the Department by providing the day to day management, operation and configuration of the enterprise network infrastructure, internet gateways, the delivery of enterprise security systems and services, the monitoring and reporting of security incidents, the conduct of threat and vulnerability analysis, the validation of adequate security controls within the enterprise and the full range of functions across the spectrum of activities relating to incident management, incident response and enterprise network management.

Computer Network Defense (CND)

The Four Pillars



Forensics

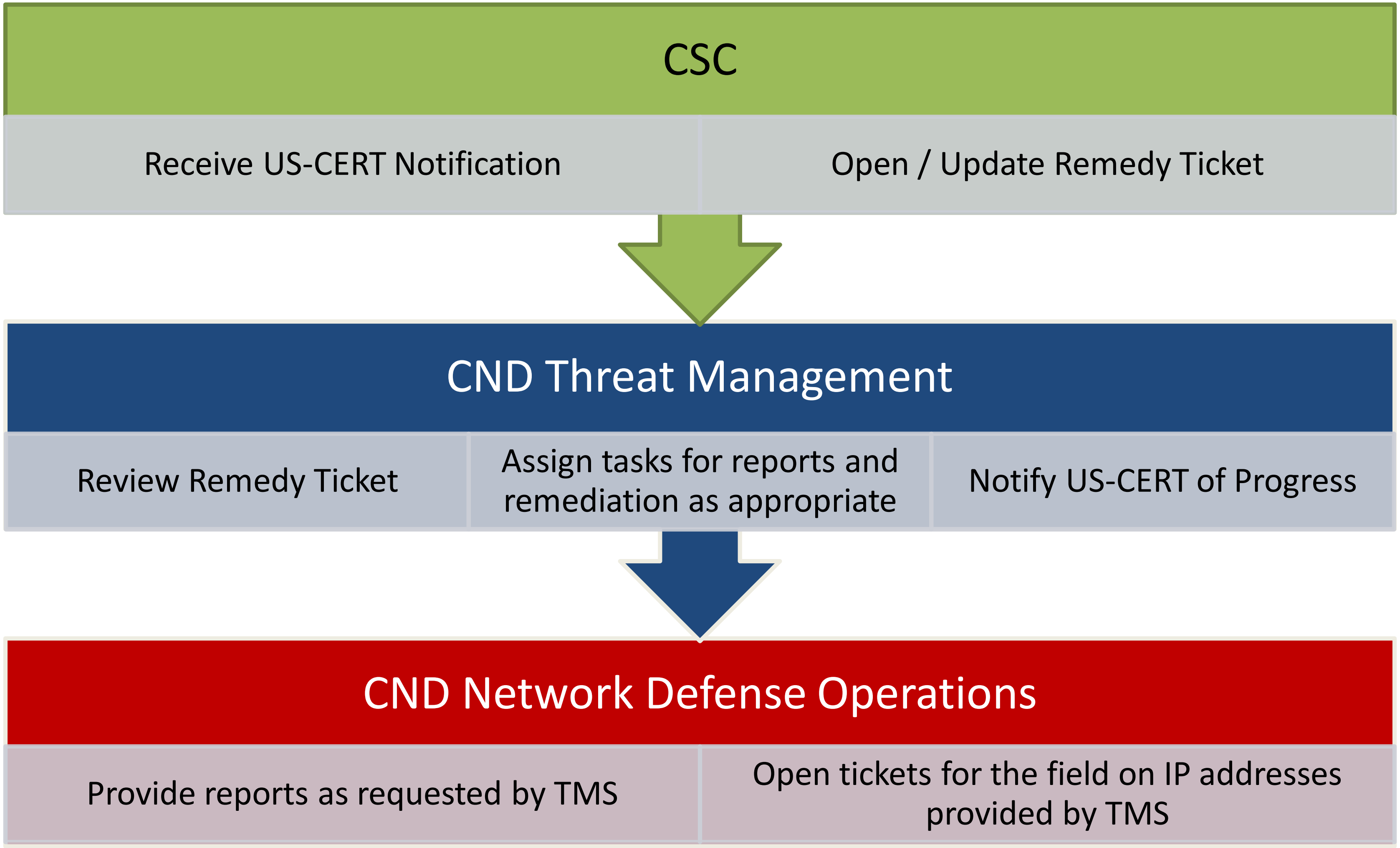
Threat Analysis

Vulnerability Assessment

Network Defense Operations (NDO)

VA-NSOC

US-CERT Incident Notification Ticket Processing



CSC

Receive US-CERT Notification

Open / Update Remedy Ticket

CND Threat Management

Review Remedy Ticket

Assign tasks for reports and remediation as appropriate

Notify US-CERT of Progress

CND Network Defense Operations

Provide reports as requested by TMS

Open tickets for the field on IP addresses provided by TMS

CSC

- Review notification to determine if this is a new notification or an update to an existing notification
  - If New : A new ticket will be opened
  - If Update: Existing ticket will be updated
- Assign the ticket to Computer Network Defense: Threat Management
- Input the US-CERT Incident Number field on the CSC Incident Management tab
- Ticket Priority set to HIGH

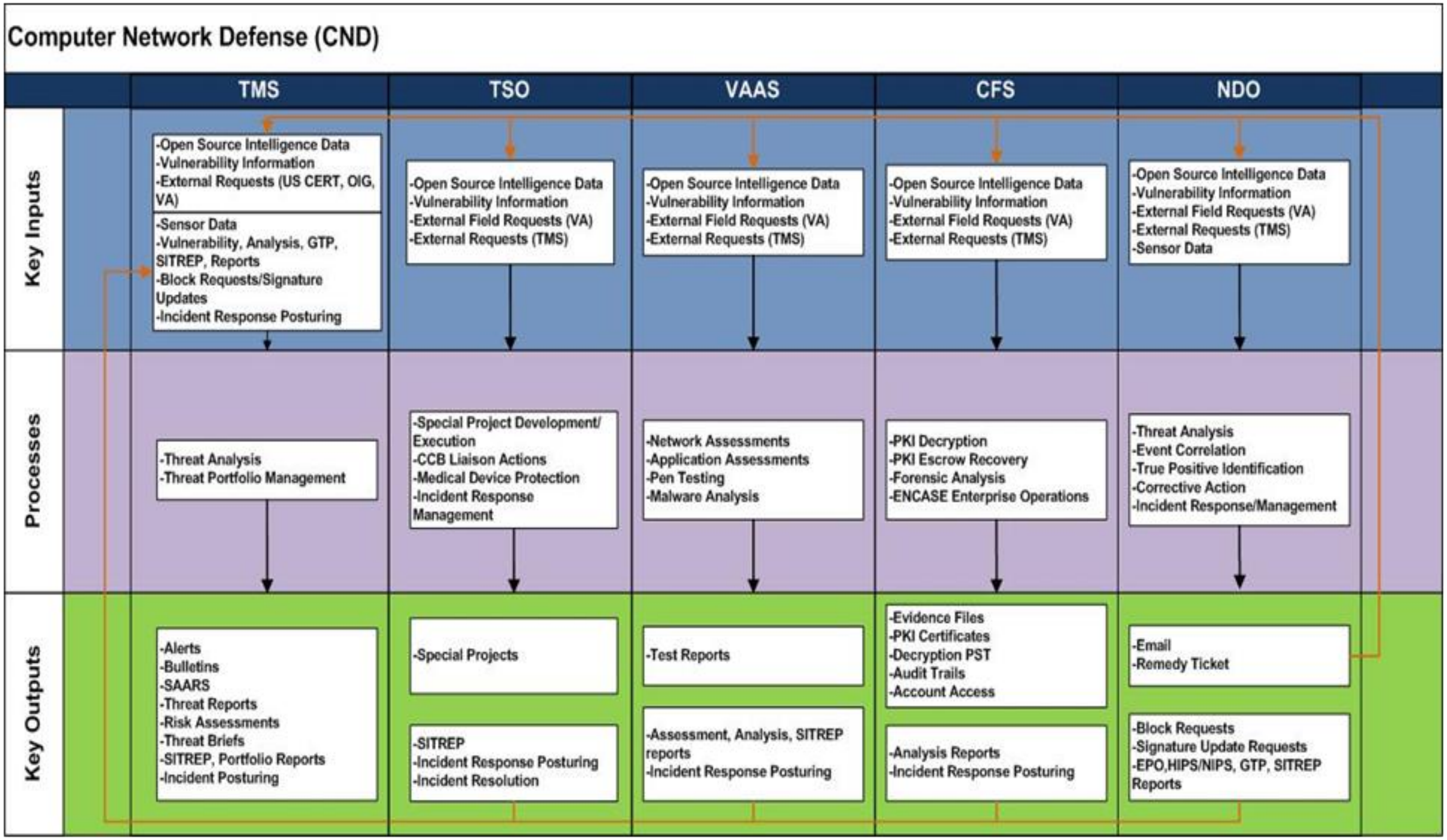
CND Threat Management

- TMS will review ticket
  - TMS will request reports as needed from NDO
  - TMS will notify US-CERT of VA ticket number
- TMS will analyze the log events and correlate to other sensor logs as necessary
- TMS will keep US-CERT updated on progress
- TMS will send a list of internal IP addresses to NDO for ticket creation and remediation activity
- TMS will maintain parent ticket through remediation of all child tickets managed by NDO
- TMS will close the parent ticket after successful closure of all child tickets by NDO

CND Network Defense Operations

- NDO will run reports as requested to support the TMS analysis
- NDO will open tickets for field operations remediation activities
  - Tickets will be linked to the original ticket as child tickets allowing TMS to track progress of activity
- NDO will follow up and track all field tickets through remediation as per normal NDO SOP
- NDO will manage all child tickets to the field and close them as appropriate.

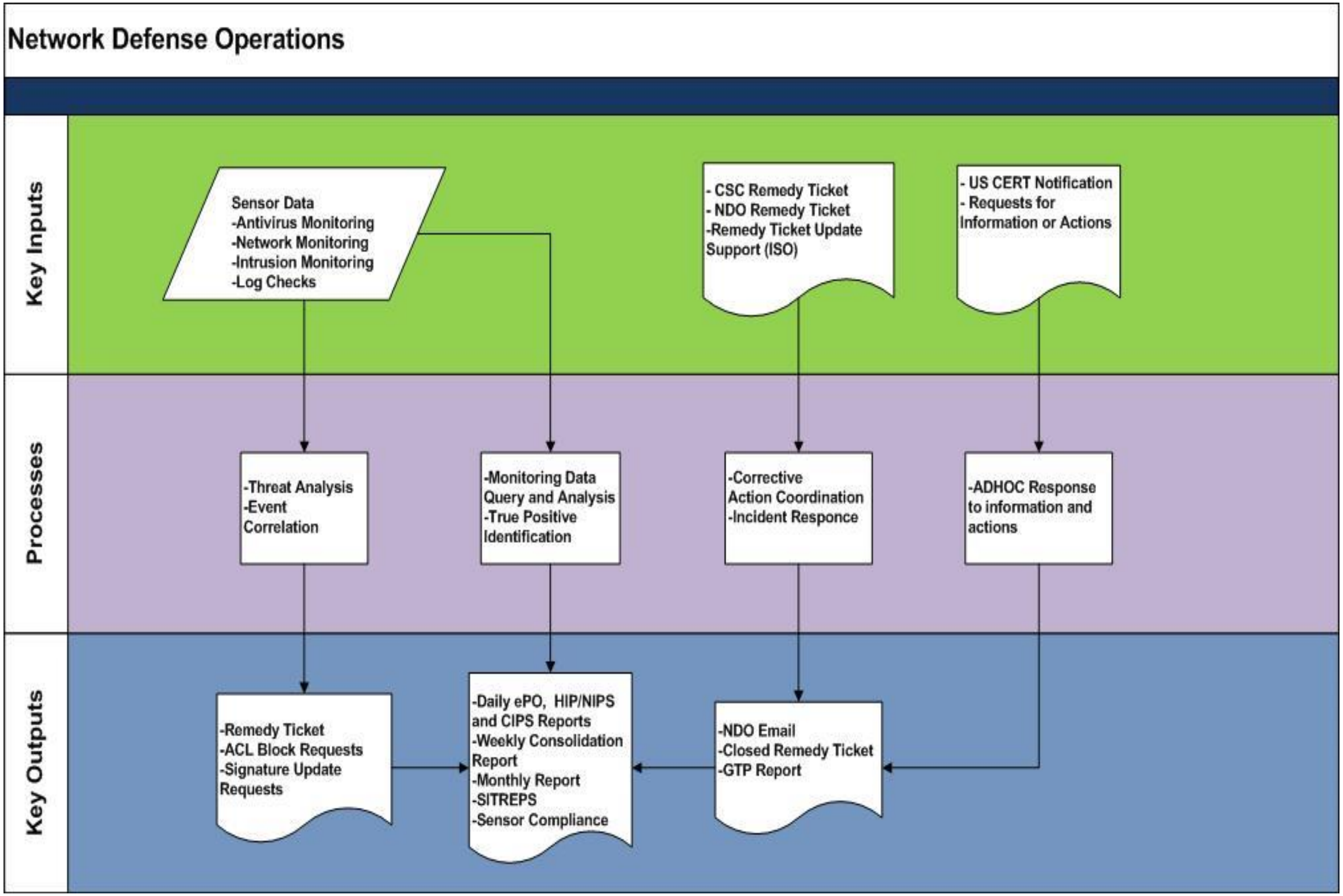
Computer Network Defense



Computer Network Defense (CND)

	TMS	TSO	VAAS	CFS	NDO
Key Inputs	-Open Source Intelligence Data -Vulnerability Information -External Requests (US CERT, OIG, VA) -Sensor Data -Vulnerability, Analysis, GTP, SITREP, Reports -Block Requests/Signature Updates -Incident Response Posturing	-Open Source Intelligence Data -Vulnerability Information -External Field Requests (VA) -External Requests (TMS)	-Open Source Intelligence Data -Vulnerability Information -External Field Requests (VA) -External Requests (TMS)	-Open Source Intelligence Data -Vulnerability Information -External Field Requests (VA) -External Requests (TMS)	-Open Source Intelligence Data -Vulnerability Information -External Field Requests (VA) -External Requests (TMS) -Sensor Data
Processes	-Threat Analysis -Threat Portfolio Management	-Special Project Development/ Execution -CCB Liaison Actions -Medical Device Protection -Incident Response Management	-Network Assessments -Application Assessments -Pen Testing -Malware Analysis	-PKI Decryption -PKI Escrow Recovery -Forensic Analysis -ENCASE Enterprise Operations	-Threat Analysis -Event Correlation -True Positive Identification -Corrective Action -Incident Response/Management
Key Outputs	-Alerts -Bulletins -SAARS -Threat Reports -Risk Assessments -Threat Briefs -SITREP, Portfolio Reports -Incident Posturing	-Special Projects -SITREP -Incident Response Posturing -Incident Resolution	-Test Reports -Assessment, Analysis, SITREP reports -Incident Response Posturing	-Evidence Files -PKI Certificates -Decryption PST -Audit Trails -Account Access -Analysis Reports -Incident Response Posturing	-Email -Remedy Ticket -Block Requests -Signature Update Requests -EPO,HIPS/NIPS, GTP, SITREP Reports

NDO Flows



Network Defense Operations

Key Inputs

Sensor Data
-Antivirus Monitoring
-Network Monitoring
-Intrusion Monitoring
-Log Checks

- CSC Remedy Ticket
- NDO Remedy Ticket
-Remedy Ticket Update Support (ISO)

- US CERT Notification
- Requests for Information or Actions

Processes

-Threat Analysis
-Event Correlation

-Monitoring Data Query and Analysis
-True Positive Identification

-Corrective Action Coordination
-Incident Responce

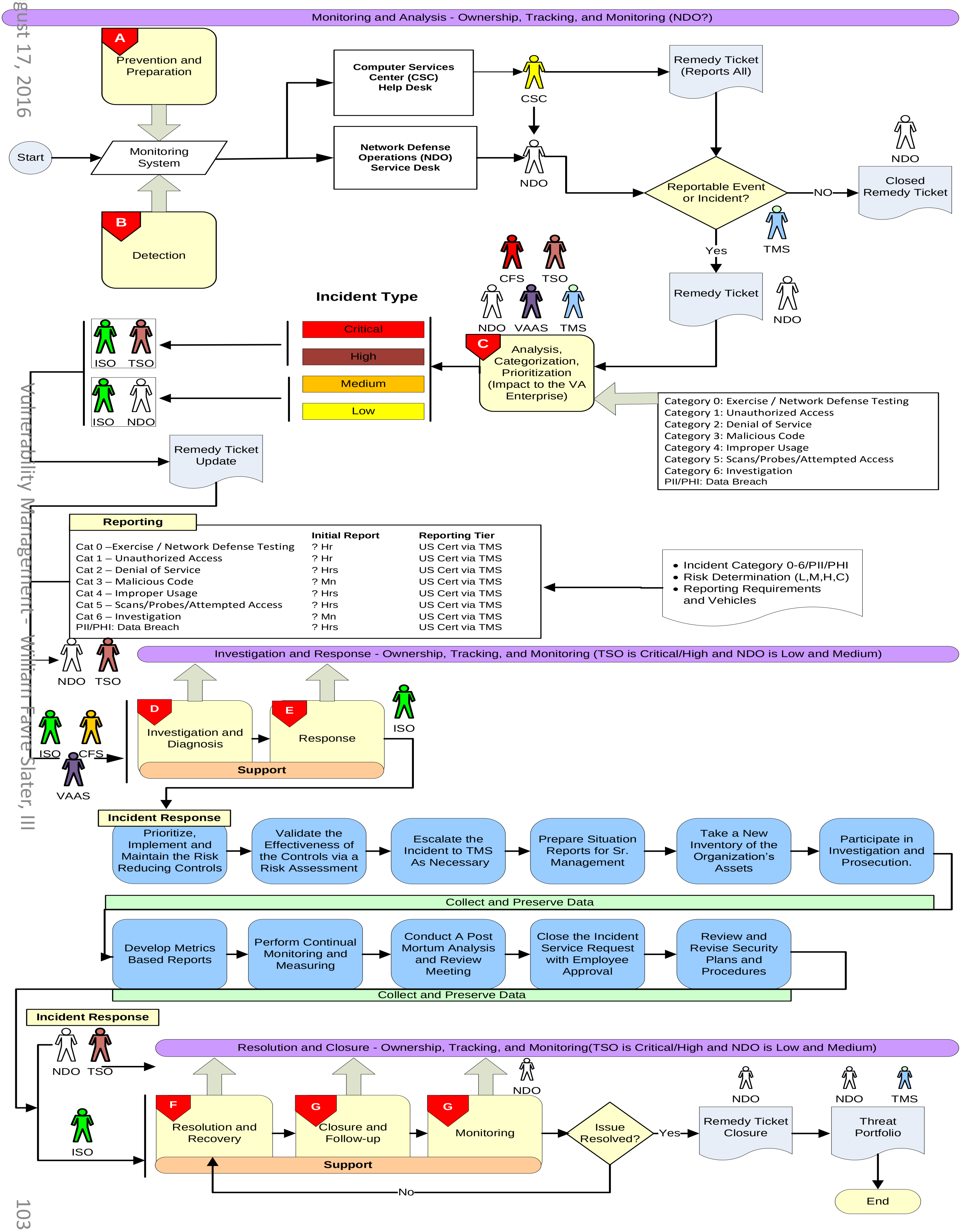
-ADHOC Response to information and actions

Key Outputs

-Remedy Ticket
-ACL Block Requests
-Signature Update Requests

-Daily ePO, HIP/NIPS and CIPS Reports
-Weekly Consolidation Report
-Monthly Report
-SITREPS
-Sensor Compliance

-NDO Email
-Closed Remedy Ticket
-GTP Report



Monitoring and Analysis - Ownership, Tracking, and Monitoring (NDO?)
Start
A
Prevention and Preparation
Monitoring System
B
Detection
Computer Services Center (CSC) Help Desk
Network Defense Operations (NDO) Service Desk
CSC
NDO
Remedy Ticket (Reports All)
Reportable Event or Incident?
NO
NDO
Closed Remedy Ticket
TMS
Yes
Remedy Ticket
NDO
CFS
TSO
NDO
VAAS
TMS
C
Analysis, Categorization, Prioritization (Impact to the VA Enterprise)
Incident Type
Critical
High
Medium
Low
ISO
TSO
ISO
NDO
Remedy Ticket Update

Category 0: Exercise / Network Defense Testing
Category 1: Unauthorized Access
Category 2: Denial of Service
Category 3: Malicious Code
Category 4: Improper Usage
Category 5: Scans/Probes/Attempted Access
Category 6: Investigation
PII/PHI: Data Breach

Reporting

	Initial Report	Reporting Tier
Cat 0 –Exercise / Network Defense Testing	? Hr	US Cert via TMS
Cat 1 – Unauthorized Access	? Hr	US Cert via TMS
Cat 2 – Denial of Service	? Hrs	US Cert via TMS
Cat 3 – Malicious Code	? Mn	US Cert via TMS
Cat 4 – Improper Usage	? Hrs	US Cert via TMS
Cat 5 – Scans/Probes/Attempted Access	? Hrs	US Cert via TMS
Cat 6 – Investigation	? Mn	US Cert via TMS
PII/PHI: Data Breach	? Hrs	US Cert via TMS

- Incident Category 0-6/PII/PHI
- Risk Determination (L,M,H,C)
- Reporting Requirements and Vehicles

Investigation and Response - Ownership, Tracking, and Monitoring (TSO is Critical/High and NDO is Low and Medium)
NDO
TSO
ISO
CFS
VAAS
D
Investigation and Diagnosis
E
Response
Support
ISO
Incident Response
Prioritize, Implement and Maintain the Risk Reducing Controls
Validate the Effectiveness of the Controls via a Risk Assessment
Escalate the Incident to TMS As Necessary
Prepare Situation Reports for Sr. Management
Take a New Inventory of the Organization's Assets
Participate in Investigation and Prosecution.
Collect and Preserve Data
Develop Metrics Based Reports
Perform Continual Monitoring and Measuring
Conduct A Post Mortum Analysis and Review Meeting
Close the Incident Service Request with Employee Approval
Review and Revise Security Plans and Procedures
Collect and Preserve Data
Incident Response
NDO
TSO
ISO
Resolution and Closure - Ownership, Tracking, and Monitoring(TSO is Critical/High and NDO is Low and Medium)
F
Resolution and Recovery
G
Closure and Follow-up
G
Monitoring
NDO
Support
Issue Resolved?
Yes
No
NDO
Remedy Ticket Closure
NDO
TMS
Threat Portfolio
End

Controls

- Control – definition
- Information system controls
- More on Information systems, controls and security
- More examples of controls

Controls

- What is a “control”?
  - A control is something that provides some level of protection for an asset in order to prevent negative consequences of a threat.

More on Information Systems and Security

- Passwords – safeguard them
- Use Virtual Private Network (VPN) for secure remote access
- Use Secure software for secure data transfers
- Use encrypted systems to avoid data compromise
- Encrypt portable storage media when possible
- Don't store protected or restricted data on your local computer disk storage

NEVER STORE PERSONAL OR PROTECTED DATA ON LOCAL MACHINES

Examples of Information Security Controls

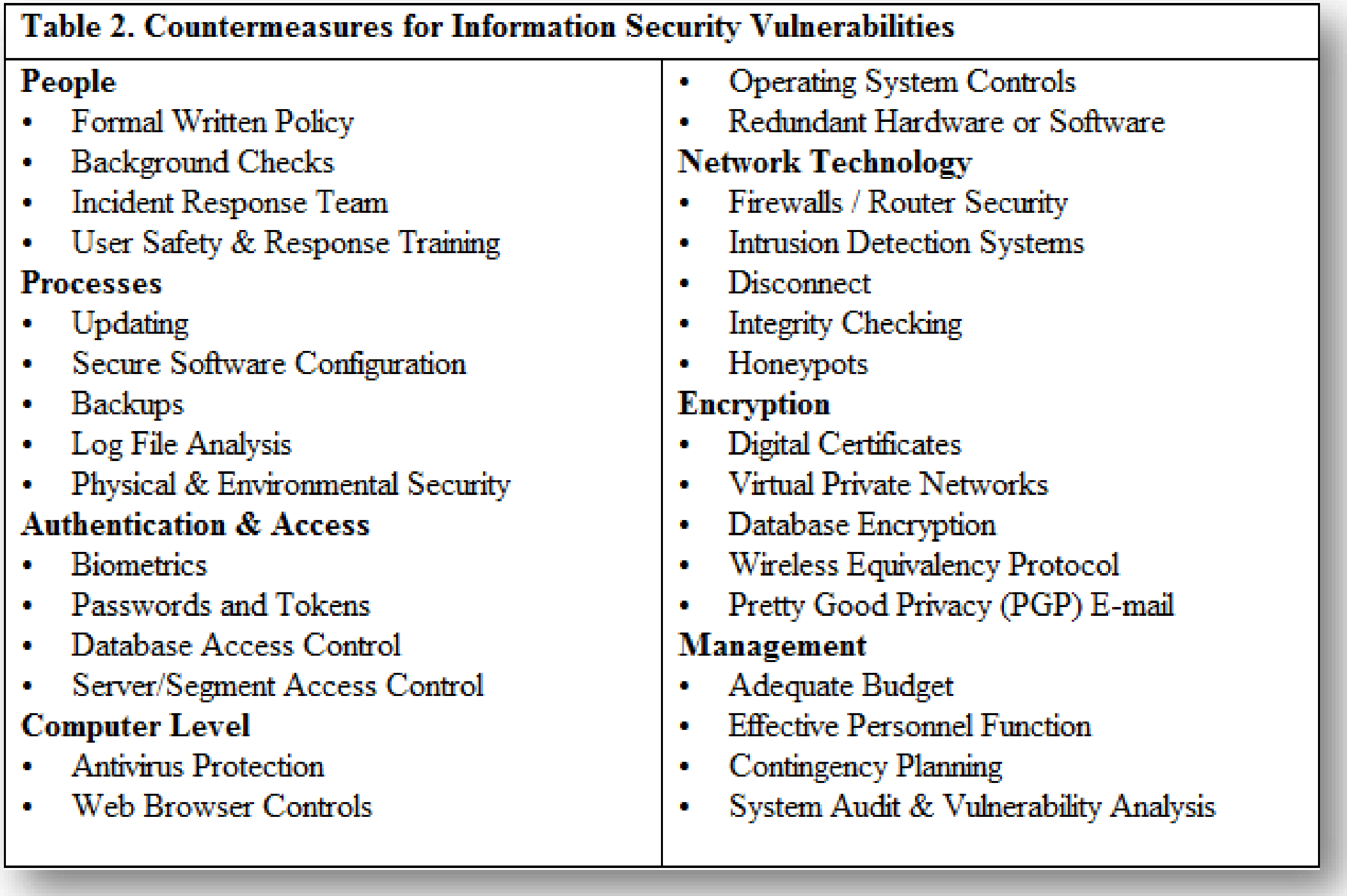


Table 2. Countermeasures for Information Security Vulnerabilities

People

- Formal Written Policy
- Background Checks
- Incident Response Team
- User Safety & Response Training

Processes

- Updating
- Secure Software Configuration
- Backups
- Log File Analysis
- Physical & Environmental Security

Authentication & Access

- Biometrics
- Passwords and Tokens
- Database Access Control
- Server/Segment Access Control

Computer Level

- Antivirus Protection
- Web Browser Controls
- Operating System Controls
- Redundant Hardware or Software

Network Technology

- Firewalls / Router Security
- Intrusion Detection Systems
- Disconnect
- Integrity Checking
- Honeypots

Encryption

- Digital Certificates
- Virtual Private Networks
- Database Encryption
- Wireless Equivalency Protocol
- Pretty Good Privacy (PGP) E-mail

Management

- Adequate Budget
- Effective Personnel Function
- Contingency Planning
- System Audit & Vulnerability Analysis

Source: http://www.johnsaunders.com/papers/riskcip/RiskConference.htm

OTHER SPEAKER INFORMATION

William F. Slater, III

❖ **Current Positions –**

Project Manager / Sr. IT Consultant, President & CEO of Slater Technologies, Inc., and Adjunct Professor at the Illinois Institute of Technology - Working on projects related to

- Lead Information Security Engineer at a Chicago-based FinTech Company
- Subject Matter Expert in Risk Management and Security
- Security reviews and auditing
- ISO 27001 Project Implementations
- Global Cybersecurity Manager at a $4.5 Billion company
- Software Development and Migration
- Created an eBook with articles about Security, Risk Management, Cyberwarfare, Project Management and Data Center Operations
- Providing subject matter expert services to Data Center product vendors and other local businesses.
- Also Developing and presenting technical training materials for undergraduate and graduate students at the Illinois Institute of Technology in the areas of Data Center Operations, Data Center Architecture, Cyber Security Management, and Information Technology hardware and software.

Contact Information & Other Information

William Favre Slater, III
MBA, M.S., PMP, CISSP, SSCP, CISA, ISO 27002, ISO 20000, ITIL v3, IP v6
Project Manager / Program Manager
slater@billslater.com
williamslater@gmail.com
Career Page: http://billslater.com/career
LinkedIn: https://www.linkedin.com/profile/in/billslater
Twitter: @billslater
SKYPE: billslater (by pre-arrangement reservation)
773 - 235 - 3080 - Home Office
312 - 758 - 0307 - Mobile
312 - 275 - 5757 - FAX
1337 N. Ashland Ave. No. 2
Chicago, IL 60622
United States of America

http://billslater.com/career

http://billslater.com/certifications

http://billslater.com/interview

http://billslater.com/writing

http://billslater.com/datacentermanager

http://billslater.com/iso27001

http://billslater.com/ms_cybersecurity

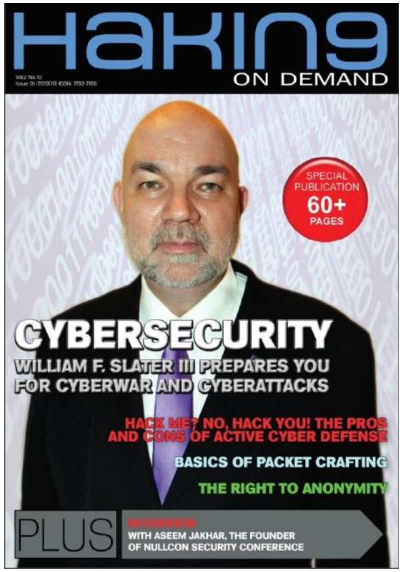
http://on.fb.me/fW3wH0

http://on.fb.me/vfGRVi

Then & Now

- A career Information Technology (IT) professional since July 1977 , starting as a young computer systems staff officer in the United States Air Force supporting the command control information systems that provided real-time war plan asset information to the Strategic Air Command Battle Staff (http://billslater.com/myusaf)
- Current a Sr. IT Consultant / Sr. IT Project Manager / Sr. Program Manager in Cybersecurity, Compliance, Auditing, and Data Centers
- Since October 2012, 18 published articles and one ebook (http://billslater.com/ebook1)

July 1977


Hakin9
ON DEMAND
SPECIAL PUBLICATION 60+ PAGES
CYBERSECURITY
WILLIAM F. SLATER III PREPARES YOU FOR CYBERWAR AND CYBERATTACKS
HACK ME? NO, HACK YOU! THE PROS AND CONS OF ACTIVE CYBER DEFENSE
BASICS OF PACKET CRAFTING
THE RIGHT TO ANONYMITY
PLUS
INTERVIEW WITH ASEEM JAKHAR, THE FOUNDER OF NULLCON SECURITY CONFERENCE

January 2013

1977 - First Job Out of College

Strategic Air Command Headquarters
Offutt Air Force Base, NE
Circa late 1970s – UNCLASSIFIED Configuration

2LT William F. Slater, III
United States Air Force
Computer Systems Staff Officer
July 1977

ILLINOIS INSTITUTE
OF TECHNOLOGY

The Microsoft Chicago Data Center - Microsoft's Flagship Cloud Data Center

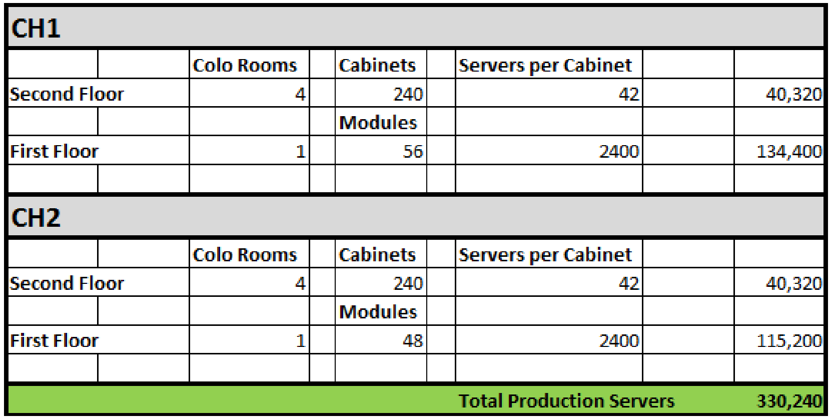
Microsoft Chicago Data Center in Northlake, IL. Actual street view photo from Google Maps

CH1 CHICAGO DATA CENTER

William F. Slater, III was the first Data Center Manager of this Facility in 2008

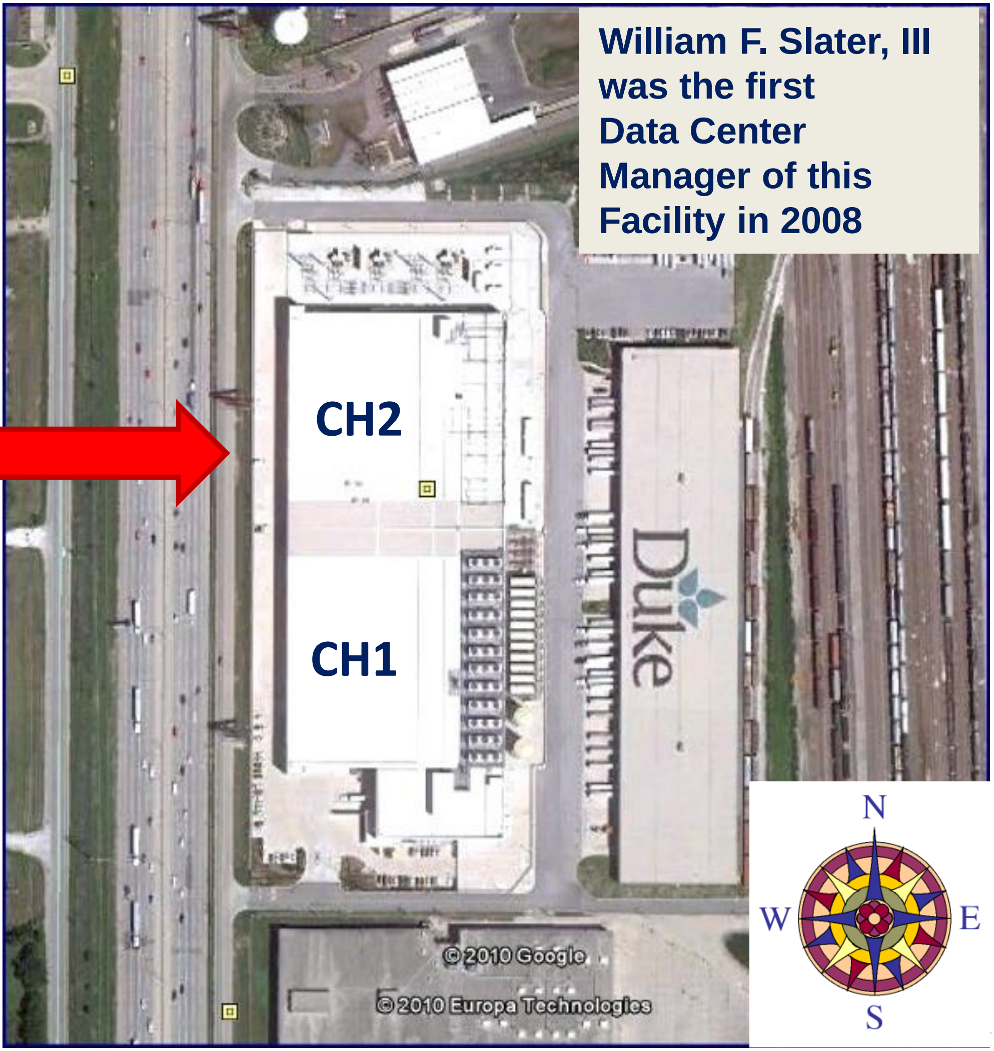
Microsoft Chicago Data Center in Northlake, IL. Actual architect's drawing from 2007 - 2008

The Microsoft Chicago Data Center - Microsoft's Flagship Cloud Data Center



	Colo Rooms	Cabinets	Servers per Cabinet	
CH1				
	Colo Rooms	Cabinets	Servers per Cabinet	
Second Floor	4	240	42	40,320
		Modules		
First Floor	1	56	2400	134,400
CH2				
	Colo Rooms	Cabinets	Servers per Cabinet	
Second Floor	4	240	42	40,320
		Modules		
First Floor	1	48	2400	115,200
			Total Production Servers	330,240

Size:	705,000 square feet
Power:	120 MW (enough to power 87,000 homes)
Critical Load for IT Equipment:	60 MW
No. of Physical Servers:	> 330,000 Servers



William F. Slater, III was the first Data Center Manager of this Facility in 2008

601 Northwest Hwy, Northlake, IL

CH1 CHICAGO DATA CENTER

Microsoft Chicago Data Center Operations Team Summer 2008