2024

Vulnerability Management

Best Practices Guidance Document

V1.0
August 2024

A CyberRisk Collaborative Task Force Product

Contents

Vulnerability Management Task Force Members and Acknowledgements

The CyberRisk Collaborative would like to acknowledge the following member companies and individuals for their collaborative efforts which, through discussions, experience, and research, supplied the content for this document. **Please direct any questions to Dustin.Sachs@cyberriskalliance.com**.

Task Force Executive Leader:

Kristina Belnap, Senior Vice President, CISO, SILAC Insurance Company

Task Force Members (CISOs and Security Staff):

Kwesi Armah, Scientific Games
Paul Bivian, Kirkland & Ellis
Mike Flores, HealthEquity
Matt Higdon, Menards
Lou Klubenspies, CISO, Revvity
John Nagengast, Penn National Insurance
Parker Opar, CRISP Health
Jeremy Rowley, Motorola-Lenovo
Richard Rushing, CISO, Motorola-Lenovo
Brad Skrbec, Motorola-Lenovo
Travis Zeigler, Revvity

Introduction

Background and Purpose

In July 2023, members of the CyberRisk Collaborative organized a task force to find best practices for developing, implementing, and enhancing their Vulnerability Management Programs (VMPs). Challenges with identifying and prioritizing vulnerabilities in various environments (e.g., cloud, on premise, applications) as well as vulnerability remediation motivated members to collaborate on finding the most effective strategies for vulnerability identification, prioritization, and remediation.

Member discussions, experiences, and contributions, including sharing vulnerability management policies, contributed to developing the guidance shown in this document. CISOs can use this document to help design and improve the effectiveness of their VMPs.

During 2024, guidance was enhanced to include a Vulnerability Management Program Maturity Assessment Tool to help members find program weaknesses and to develop strategies for improving their programs.

This document addresses technical vulnerabilities only (e.g., OS, middleware, applications). The organization of this guidance document is as follows:

- "Vulnerability Management Definition and Scope" includes industry-based definitions of vulnerabilities, vulnerability management, and scope.
- "The Importance of Vulnerability Management to an Effective Cybersecurity Program" demonstrates that the exploitation of vulnerabilities is real and is concerning customers.
- "Vulnerability Management Program Components and Task Force Member Guidance" identifies the organizational resources, processes and tools required to operate an effective VMP.
- "Guidance for VM "On Prem", in the Cloud, Third Parties, App Development, and for Acquisitions" provides insights on how to manage vulnerabilities in different computing environments.
- "Summary" recaps key takeaways from this document.
- "Appendix: Member Comments About Vulnerability Management Tools" provides useful information about VM tools used by task force members.

Supplemental Tools

The CyberRisk Collaborative task force members created the following supplemental tools to support the guidance provided in this document. These are available to members under separate covers:

1. **Vulnerability Management Policy.** This policy template shows program objectives and goals, roles and responsibilities, and program specifics.
2. **Vulnerability Management Program Assessment Tool.** Leveraging the VMP organization, processes, and tools components of the CyberRisk Collaborative Vulnerability Program model, this tool allows members to assess the maturity of their programs and provides members with strategies for improving program effectiveness.

Vulnerability Management Definition and Scope

Definition

There are many definitions of vulnerabilities and vulnerability management offered by notable industry associations. *NIST SP-800-37, Rev 2, Appendix B,* defines vulnerabilities as "weaknesses in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source." Microsoft defines vulnerability management as "a continuous, proactive, and often automated process that keeps your computer systems, networks, and enterprise applications safe from cyberattacks and data breaches. As such, it is an important part of an overall security program. By identifying, assessing, and addressing potential security weaknesses, organizations can help prevent attacks and minimize damage if one does occur."

Furthermore, Microsoft describes the goal of vulnerability management as "to reduce the organization's overall risk exposure by mitigating as many vulnerabilities as possible", recognizing the challenges with doing so, "given the number of potential vulnerabilities and the limited resources available for remediation." Therefore, "vulnerability management should be a continuous process to keep up with new and emerging threats and changing environments."

Scope

As Table 1 below demonstrates, the vast scope of managing vulnerabilities in technology environments, computing assets, and software presents a significant challenge to most organizations.

Table 1: The Scope of the Vulnerability Management

Technology Environments	Computing Assets	Software
Data Centers	• End user devices. • Servers • Databases • Networks • Security Technologies	• Operating Systems • Middleware • Applications • Tools / Platforms
Cloud		
Development		
Third Parties		
Acquisitions		
Operational Technologies (OT)	ICS / SCADA	

The Importance of Vulnerability Management to an Effective Cybersecurity Program

Vulnerability Management is a key part of the overall Cybersecurity Program as evidenced by the daily reporting of entities whose systems have been breached by an unpatched vulnerability and by customers vetting the effectiveness of their suppliers' vulnerability management programs.

The Exploitation of Vulnerabilities is Real

The Verizon Data Breach Investigations Report

According to the 2024 Verizon Data Breach Investigations Report, the exploitation of vulnerabilities was one of the top vectors for all data breaches, as shown in Figure 1 below. The exploitation of vulnerabilities was the primary attack vector for supply chain breaches.

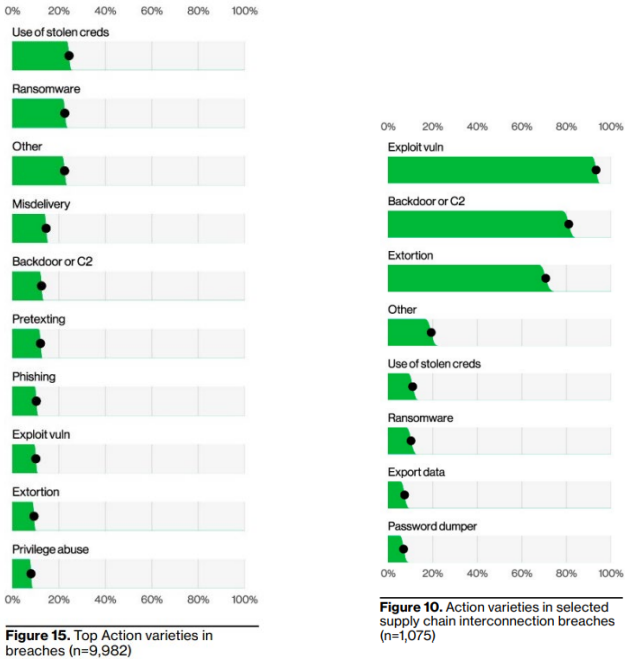
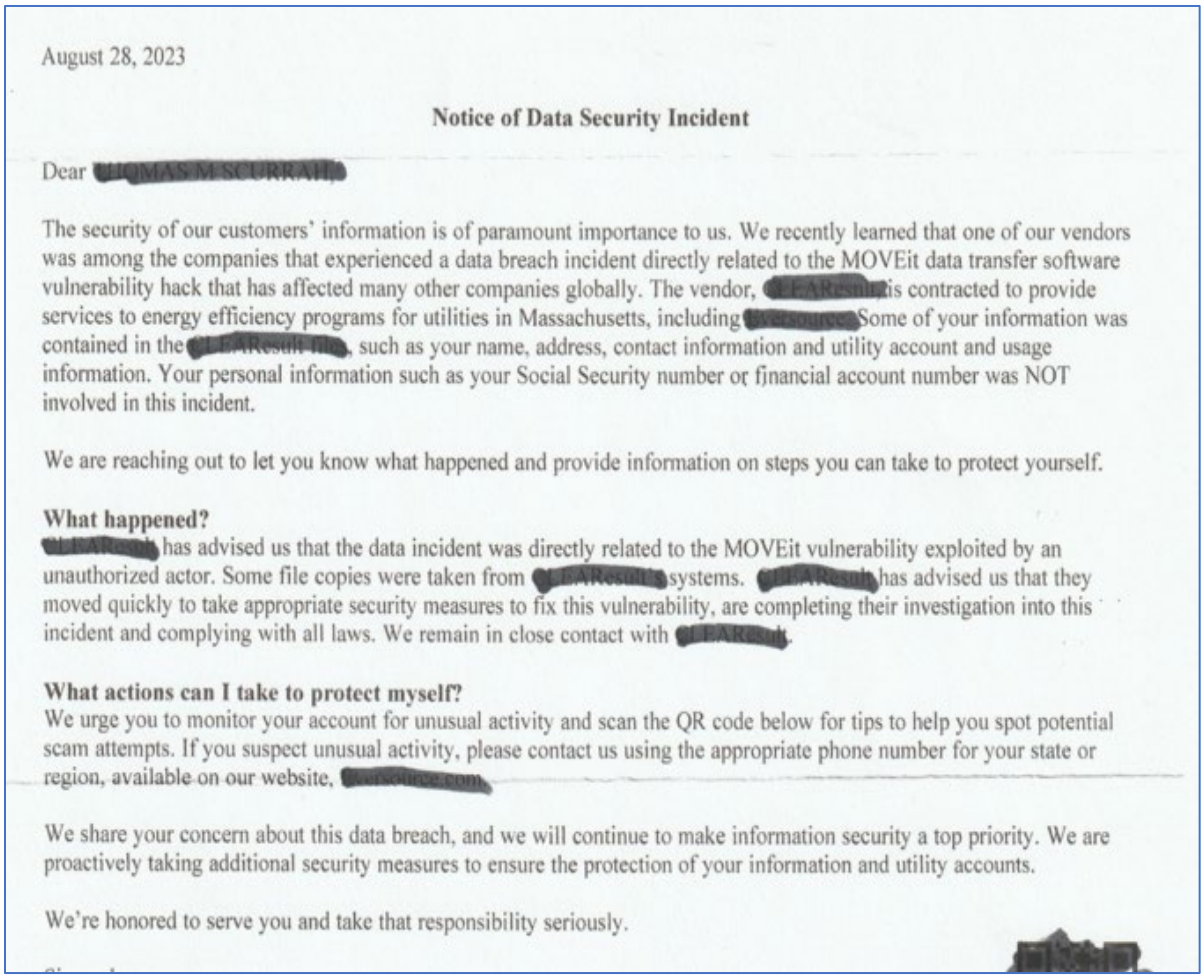


Figure 1: 2024 Verizon Data Breach Investigations Report: Vulnerability Exploitation

The MOVEit Breach and Its Impact on Consumers

Exploited vulnerabilities in widely used third party software and services can have far-reaching consequences often involving a compromise of consumer personal information. The MOVEit breach is a pertinent example. MOVEit is a widely used file transfer program. On May 31, 2023, Progress Software warned customers of an SQL injection (SQLi) vulnerability in MOVEit Transfer and MOVEit Cloud Software. This was a zero-day vulnerability actively exploited by a ransomware group, CLOP. This allowed the attacker to deploy a custom ASP.NET web shell (LEMURLOOT) to achieve persistence on a network for further attacks. SQLi attacks have been prevalent in the past, breaching notable organizations like Target, Yahoo, Zappos, Equifax, Epic Games, TalkTalk, LinkedIn, and Sony Pictures. The attacker's persistence on the MOVEit network allowed for the compromise of customer personal information, as shown by the notice in Figure 2 to the customers of a power company who employed MOVEit services.



August 28, 2023

Notice of Data Security Incident

Dear [redacted]

The security of our customers' information is of paramount importance to us. We recently learned that one of our vendors was among the companies that experienced a data breach incident directly related to the MOVEit data transfer software vulnerability hack that has affected many other companies globally. The vendor, [redacted] is contracted to provide services to energy efficiency programs for utilities in Massachusetts, including [redacted] Some of your information was contained in the [redacted], such as your name, address, contact information and utility account and usage information. Your personal information such as your Social Security number or financial account number was NOT involved in this incident.

We are reaching out to let you know what happened and provide information on steps you can take to protect yourself.

What happened?

[redacted] has advised us that the data incident was directly related to the MOVEit vulnerability exploited by an unauthorized actor. Some file copies were taken from [redacted] systems. [redacted] has advised us that they moved quickly to take appropriate security measures to fix this vulnerability, are completing their investigation into this incident and complying with all laws. We remain in close contact with [redacted].

What actions can I take to protect myself?

We urge you to monitor your account for unusual activity and scan the QR code below for tips to help you spot potential scam attempts. If you suspect unusual activity, please contact us using the appropriate phone number for your state or region, available on our website, [redacted].com.

We share your concern about this data breach, and we will continue to make information security a top priority. We are proactively taking additional security measures to ensure the protection of your information and utility accounts.

We're honored to serve you and take that responsibility seriously.

[redacted]

Figure 2: Letter from Power Company to Consumers Following MOVEit Breach

Your Customers and Cyber Insurance Companies Want Assurances

Your customers, prospective customers and cyber insurance underwriters are inquiring about your vulnerability management processes. Third party security risk questionnaires often include the following questions:

- *What is your patching cadence for critical, high, and medium vulnerabilities?"*
- *"Do you patch critical vulnerabilities ASAP?"*
- *"Please provide a copy of a latest scan and penetration test report showing that all critical and high vulnerabilities have been remediated."*

Task force members have noted that cyber insurance underwriters are asking more poignant questions around the management of vulnerabilities, including requiring more proof to back up questionnaire responses.

Vulnerability Management Program Components and Task Force Member Guidance

Introduction

A comprehensive Vulnerability Management Program (VMP) consists of the following components and subcomponents, shown in Table 2 below:

Table 2: Vulnerability Management Program Components and Subcomponents

Component	Subcomponent
Organizational Resources	• Vulnerability Management team • Budget • Stakeholders • Governance
Processes	• Six Vulnerability Management Lifecycle Processes • Remediation Service Level Agreements (SLAs) • Metrics
Tools	• Asset Discovery • Vulnerability Identification • Vulnerability Remediation

An effective VMP ensures that staffing resources are sufficient and engaged, processes are running continuously, and scanning and remediation tools are operating within computing environments.

The rest of this section describes each subcomponent of the VMP and provides task force member guidance for improving their effectiveness.

Organizational Resources

Description

As shown in Table 3 below organizational resources include staffing, budget and oversight bodies.

Table 3: Organizational Resources Required by the VMP

Sub-Component	Description
Vulnerability Management (VM) Team	• A full or part-time staff trained in vulnerability management. • The team typically reports to the CISO. • The team takes part in the operation and oversight of vulnerability management lifecycle processes.
Budget	• Staffing and tools costs must be included in a discrete or line-item budget.

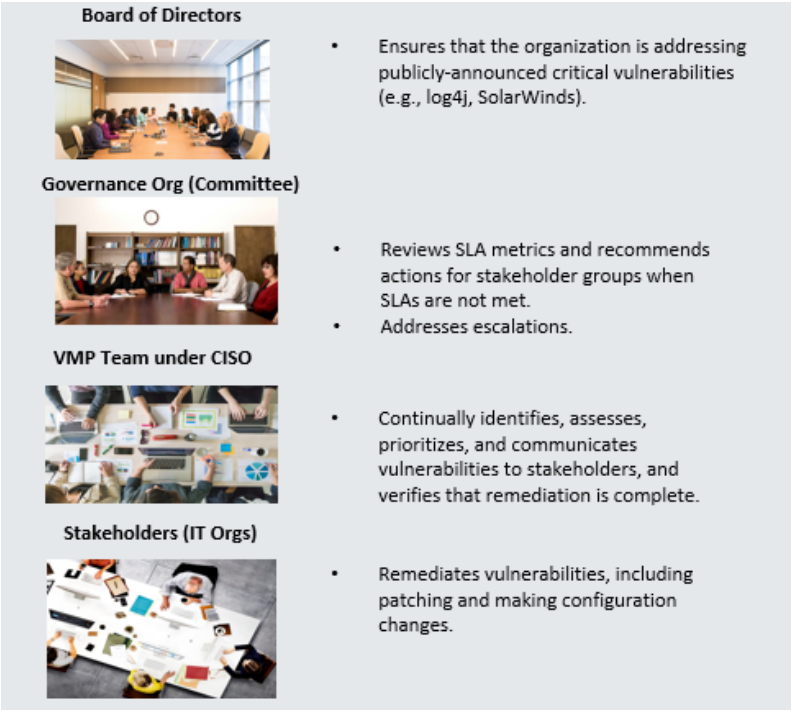
Sub-Component	Description
	• Budgetary needs span security and IT remediation groups.
Stakeholders	• Stakeholders are organizations and personnel responsible for vulnerability remediation activities. An example of a stakeholder is an end-user services group responsible for patching laptops. • Vulnerability roles and responsibilities must be defined for and accepted by all stakeholders.
Governance	• Policies, standards, and procedures must be approved and communicated to ensure that vulnerabilities are identified, categorized by risk, and addressed within specific timeframes. • Oversight of the performance of the VMP must occur to ensure it is effective in identifying and remediating vulnerabilities on time. A standing or solely purposed committee made up of IT and security management is typically established to oversee the VMP.

Task Force Member Guidance

Task force member guidance for ensuring that organizational resources are sufficient and effective is as follows:

Organizational Structure. Vulnerability management responsibilities must be shared among four organizations within the entity, as shown in Figure 3 below.

Figure 3: Organizations with Vulnerability Management Responsibilities



To bring current threat intelligence into the VM process, a task force member organization set up the Advanced Security Assessment Team (ASAT). Meeting monthly, the team examines the threat landscape for potential vulnerability exploits within the organization. The team is run by the information security organization and includes stakeholder organizations like client support, server support, and the architecture team. Ad hoc vulnerability remediation requirements, like Windows updates, are also discussed.

VM Team. A VM team should be established with a designated leader. The VM leader and team should report directly to the CISO. The VM Team manages vulnerability identification, assessment, prioritization and communication to stakeholder remediation teams. The VM team is NOT responsible for remediation but verifies that remediation has been completed.

Full and part-time staff may be employed as members of the team. As Table 4 below shows, for the task force group, there was no correlation between the size of the enterprise and the number of staff on the VM team.

Table 4: Enterprise Size vs. VM Team Staffing Levels for Task Force Members

Enterprise Size	VM Team Staffing Levels
3,000 employees	Dedicated team 1 manager, 2 analysts
3,500 employees	Dedicated team 1 manager + 1 backfill
10,000 employees	No dedicated team 6-12 individuals with multiple responsibilities
1,200 endpoints	No dedicated team 3-4 dedicated staff
3,700 endpoints, 1,600 servers	Dedicated team 1 full time + 1 support

Budget. Often organizations do not have a discrete budget for the VMP, as investments and staffing often span multiple organizations within information security and IT. Regardless, costs for staff time and tools should be tracked as a unique budget to ensure that funding for critical components is not removed from formal budgets.

Stakeholders. As groups within the IT organization responsible for remediating vulnerabilities, stakeholders must be held accountable to meeting remediation SLAs. Senior management must authorize and require stakeholders to perform their remediation responsibilities, and sufficiently resource these organizations with staffing and funding.

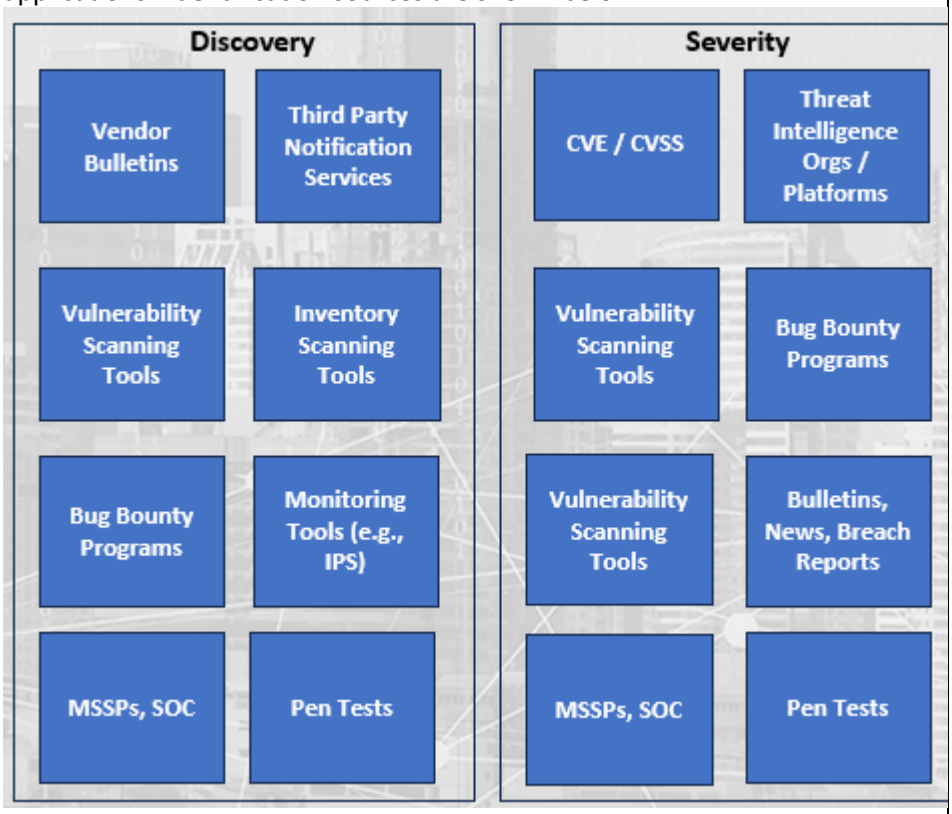
Governance. VMP governance is achieved through the implementation of policies and procedures and through the oversight of a governance organization. Leveraging an operational IT or Security steering committee can provide cost-effective oversight of the VMP. The governance organization should be empowered to address issues with meeting SLA requirements and handle other issues affecting the performance of the VMP.

Processes

Description

The VMP operates three key processes, as described in Table 3 below.

Table 3: Key VMP Operational Processes

Component	Description
VM Lifecycle Processes	The VMP operates six, continuous life cycle processes: 1. **Identify** – identify vulnerabilities in operating systems, middleware, and applications. Identification sources are shown below:  2. **Assess** --assess vulnerabilities in terms of their risks to the organization (likelihood of being exploited and impact if exploited); this typically requires assigning the vulnerability to a risk class (e.g., critical, high, medium, low). 3. **Prioritize** -- prioritize vulnerability remediation urgency based on risk.

Component	Description
	Assessment & Prioritization Processes are: 1) Develop risk categories (Critical, High, Medium Low): a. Criteria (e.g., for Critical): b. CVSS Score of 8+ and exploitable. c. CVSS Score of 8+, Qualys risk of 4 or 5, and exploitable. d. Remediation SLAs (e.g., 72 hours for critical) 2) For high-risk items, run reports against top vulnerabilities to see what systems are impacted. 3) Group vulnerabilities by Asset. 4) Create a ticket and assign ticket to asset owner. 4. **Communicate** -- communicate to stakeholder remediation teams: (a) the nature of the vulnerability; (b) the computing assets it impacts; (3) the risk it poses to the organization; and (4) applicable remediation guidance, if known. 5. **Remediate** – stakeholder groups act immediately or plan to eliminate or reduce the risk imposed by the vulnerability through remediation efforts which include patches, configuration changes, and compensating controls. 6. **Verify** – verify that the vulnerability has been remediated, typically by means of a vulnerability scan. Verification processes include: a. Ensuring that patches have been applied successfully (validate your patch management program). b. Ensuring that all remediation actions have been taken for the vulnerability, including configuration or registry key changes. c. Reporting on successes and missed SLAs. d. Escalations to the senior management or governance committee when critical risks are not addressed through remediation.
Remediation Service Level Agreements (SLAs)	Remediation SLAs define the timeframes for remediating a vulnerability based on the risk class it has been assigned to. For example, the SLAs for critical vulnerabilities are often seven days or less.
Metrics	Metrics are used to help determine if SLAs are being met. An example is measuring (as a timeseries of monthly or cumulative values) the percentage of critical vulnerabilities that were remediated with the seven-day SLA timeframe.

Task Force Member Guidance

VM Lifecycle Processes.

Member guidance for improving the effectiveness of **IDENTIFYING** vulnerabilities is as follows:

1. Integrate VMP with the asset management program.
   - Build and leverage CMDB.
   - Allows you to know what assets to scan and what assets are vulnerable to a new threat.
2. Perform inventory scans.
   - Identify new assets for vulnerability management.
   - Identify assets that have been removed.
   - Use tools like ServiceNow and Ivanti.
3. Move toward authenticated and continuous scanning.

- Agents will tell you more but cost more financially and in terms of overhead.
- Will pick up current and timely vulnerabilities.
- More easily done in Windows environments, versus Linux.

4. Leverage a Third-Party Service for informing you of key vulnerabilities across multiple platforms.
    - Will ensure full coverage of vulnerability identification.
    - Will help with prioritization.
5. Employ virtual images to reduce scanning overheads.

Member guidance for improving the effectiveness of **ASSESSING and PRIORITIZING** vulnerabilities is as follows:

1. Perform automated, daily syncs with tickets for new vulnerability information.
2. Tie vulnerability remediation to a specific owner (asset owner).
3. Group findings into a single ticket by priority, by asset.
4. Integrate with existing ticketing systems like Jira.
5. Ensure that the ticket provides or references information to allow asset owner/remediation group to completely remediate the vulnerability.
6. If a vulnerability cannot be cost-effectively remediated, discuss at review venues and identify compensating controls.
7. Using agents on boxes will find more issues but give you fewer false positives.

Member guidance for improving the effectiveness of **COMMUNICATING and REMEDIATING** vulnerabilities is as follows:

1. Notify via a ticketing system.
2. Notification information should include:
    a. Asset Name
    b. Owner
    c. Vulnerability Name and Description
    d. Severity
3. All mitigation actions should be communicated (patching, registry key changes, configuration).
4. Establish remediation timeframes.
5. Tie remediation efforts into your patch management processes:
    a. Remediation of multiple vulnerabilities on an asset may be met by applying a patch or service pack.
    b. Automate your patching process as much as possible (Adobe, Chrome, Zoom will automatically apply patches.
6. Note that remediation may not be simply applying a patch (configuration change, change to registry keys).
7. Monitor remediation progress:
    a. Review progress in management meetings.
    b. Escalation when necessary.
    c. Use spreadsheets (or other tools) for tracking (includes remediation items and assigned dates).
8. Members suggest the following best practices:

a. Provide remediation teams with access to scanning tools that will provide remediation guidance.
b. Establish a dedicated remediation team.

Member guidance for improving the effectiveness of **VERIFYING** vulnerabilities is as follows:

1. Rescans are a primary and direct means of verification. Identify a tool as a "source of truth".
2. To verify that a vulnerability has been remediated, examine the version number of the asset.
3. In addition to scanners, rely on "indirect" yet important verification methods:
    a. Penetration Tests
    b. Bug Bounty Programs
    c. Identification of configuration changes required for full remediation.

Remediation Service Level Agreements (SLAs)

Member guidance for creating effective remediation SLAs is as follows:

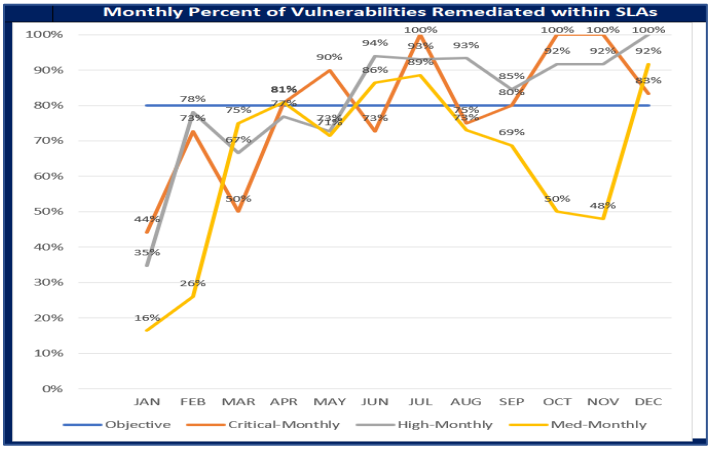
1. Set a remediation timeframe for each vulnerability risk category (e.g., Zero-Day: ASAP; Critical: 7 days; High: 30 days; Medium: 60 days; Low: 90+days).
2. Remediation timeframes should be based on customer and regulatory requirements and industry best practices.
3. SLAs should be documented and approved by senior management and accepted as requirements for the remediation teams.

Metrics

Member guidance for creating effective metrics is as follows:

1. Metrics should be used to measure SLA performance, to ensure SLAs are met or that actions are implemented to meet SLA requirements.
2. Metrics should be reviewed regularly with remediation teams and with the VMP governance organization.
3. An example of metrics used to remediate SLAs is shown in Figure 4 below.

Figure 4: Vulnerability SLA Metrics Example



Tools

Description

Tools are essential to the operation of the VMP. Categories of tools are described in Table 4 below.

Table 4: Categories of VMP Support Tools

Component	Description
Asset Discovery	Tools that discover computing assets on the network that have not been inventoried and may pose a threat from vulnerabilities.
Vulnerability Identification	Vulnerability scanners and other tools used to identify vulnerabilities.
Vulnerability Remediation	Tools to help with remediation efforts. These include ticketing systems, project tracking software, and reporting and metrics tools.

Task Force Member Guidance

Members noted that tools can be "pricey", citing the following:

- "Tools like Wiz.io have transformed our Cloud vulnerability management program, but if you don't take care in how they are deployed, they can bankrupt you."
- "The asset discovery capabilities of ServiceNow are amazing but unaffordable."

Furthermore, because a single tool does not provide complete functionality for all VM lifecycle processes, several tools must be purchased and integrated. Thus, members are continuing to use spreadsheets for tracking purposes.

Tools that members have deployed are: AppOmni, Atlassian, AvePoint, CrowdStrike, Falcon Complete, Intune, Ivanti, Jira, Kenna Security, Netskope, NorthStar, Qualys, Rapid 7 / Nexpose. ServiceNow, Tanium, Tenable, and Wiz.io. Member comments made during task force meetings about some of these tools are documented in the Appendix.

By and large, members agreed that it is important to stay abreast of new features of tools that are used as well as new tools offered in the marketplace, especially those that operate in Cloud environments. A continuing investment in tools is required to improve the effectiveness of the VM Program.

Guidance for VM "On Prem", in the Cloud, Third-Parties, App Development, and for Acquisitions

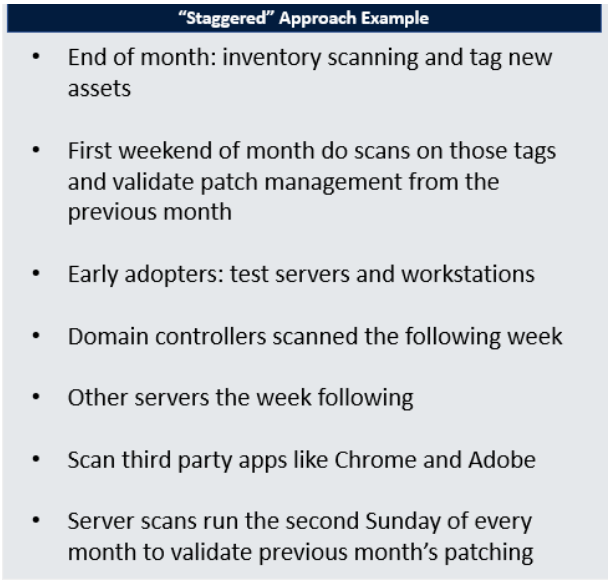
VM for Computing Assets "On Prem"

Computing assets "on prem" include laptops, office network equipment, and servers and databases within computing environments owned or leased by the entity. Member guidance is as follows:

1. **Adopt a "staggered" approach to periodic scanning.**

Periodic scanning occurs over planned intervals (e.g., monthly). Task force members recommend a "staggered" approach, as shown in Figure 5 below, to minimize potential disruptions to the environment and to validate the completion of patching from the previous month.

Figure 4: Example of a "Staggered" Periodic Approach to Scanning



Members cited different challenges to conducting periodic scans. The first challenge applies to global organizations. Scanning in global organizations requires adjusting tools to different time zones, which is often difficult to do. The second challenge is scanning endpoints in work-at-home environments when endpoints may not be connected to the network. This requires coordination and communication with end users. The third challenge is with scanning "pervasive middleware". Tomcat was cited as an example. Members recommended that a dedicated team, like the architecture group, performs scanning of "pervasive middleware."

2. **Move toward "continuous scanning."**

Members suggested that organizations should continuously (versus periodically) scan their environments, since agents on devices will identify more vulnerabilities. They cited the benefits of fewer false positives. However, a drawback is that this requires more agents on devices, which can

often compete with resources. Furthermore, with the identification of more vulnerabilities, the VM Team has more work prioritizing and triaging vulnerabilities.

VM for Computing Assets in Cloud Environments

Depending on the cloud service model adopted (e.g., SaaS, IaaS, PaaS), the responsibility for scanning computer assets may either be with the Cloud Service Provider (CSP) or the Cloud Service User (CSU). For example, scanning of IaaS environments is usually the responsibility of the CSU, whereas the scanning of SaaS tools is usually the responsibility of the CSP. Task Force Members gave the following guidance:

1. **Recognize that Cloud platform misconfigurations can introduce vulnerabilities to the CSU.**

   Regardless of the service model adopted, misconfiguring cloud settings can introduce vulnerabilities, such as exposing datastores to the Internet. Using CIS Cloud Security Benchmark tools can help identify configuration vulnerabilities. Automated Cloud configuration checking tools have been developed and are gaining use.

2. **Leverage Cloud vulnerability management tools.**

   Task force members with dedicated Cloud VM Teams have stated that managing vulnerabilities in the Cloud is easier than managing vulnerabilities in on-prem environments because of the higher quality of vulnerability management tools for Cloud use. Tables 5 and 6 below provide examples of Cloud vulnerability and configuration management tools.

Table 5: Member-Cited Cloud Vulnerability and Configuration Management Tools

Tool	Description
AppOmni	• For SaaS applications. • Helps with configuration management. • Has catalog of SaaS services with streamlined configuration management guidelines.
AvePoint	Governance of SharePoint, OneDrive, and Teams; cuts down sprawl; allows approvals from centralized teams.
AWS Injector Module	Identifies CIS configuration vulnerabilities.
Microsoft Secure Score	• Checks overall health of Cloud and Governance tools. • Comes with E5 license.

Wiz.io	• Identifies exactly what is running on the instance, including vulnerabilities. • Works in Azure and AWS. • Sits over Guard Duty and Control Tower as a CSPM (Cloud Security Posture Management).

Table 6: Key Configuration & Vulnerability Management Tools Provided by Major CSPs

CSP	Tool	Description
AWS	AWS Config	Assesses, audits, and evaluates the configurations of AWS resources. Continuously monitors and records AWS resource configurations.
	AWS Trusted Advisor	Analyzes AWS environment and provides recommendations for cost optimization, security, performance, and fault tolerance.
	Amazon Guard Duty	Managed threat detection service that monitors for malicious activity and unauthorized behavior in your AWS environment.
	AWS Security Hub	Provides a comprehensive view of security alerts and compliance status across all AWS accounts. It aggregates findings from various AWS security services and third-party tools.
	AWS IAM Access Analyzer	Analyzes resource-based policies in the AWS environment and helps identify and remediate unintended access to resources.
Azure	Azure Policy	Allows the tenant to define and enforce policies on resources in the Azure environment to ensure compliance with the organization's standards and requirements.
	Azure Security Center	Provides advanced threat protection across all Azure workloads, as well as security recommendations and integration with Azure policies.

	Azure Blueprints	Enables tenant to define a repeatable set of Azure resources and policies as a blueprint for the organization's compliance and security requirements.
	Azure Sentinel	Cloud-native security information and event management (SIEM) service that helps you detect, investigate, and respond to security threats across your Azure and on-premises environments.
	Azure Policy Guest Configuration	Assess and enforces configuration settings inside virtual machines (VMs), ensuring they meet security and compliance requirements.
Google Cloud	Google Cloud Security Command Center	A security management and data risk platform that helps tenant aggregate and analyze security data from across all Google Cloud services.
	Google Cloud Security Scanner	Scans your Google Cloud applications for common vulnerabilities, such as cross-site scripting (XSS) and SQL injection.

VM for Third Party Vulnerabilities

Task force members stated that their VM Teams were not responsible for addressing third party vulnerabilities. They noted that their development groups reached out to third party application providers to address any code vulnerabilities that were publicly identified as threats, such as Log4j. Procurement or the third-party risk management team was responsible for addressing vulnerability management practices in third parties that provided business services. However, members offered the following guidance:

1. **The VM Team should communicate relevant vulnerabilities to organizations responsible for third party risk management and offer guidance, when feasible.**

   Critical vulnerabilities affecting widely adopted computing platforms should be communicated to development and third-party risk management teams with remediation guidance, if available.

2. **The VM Team should advocate for the use of security report card tools like RiskRecon and SecurityScorecard.**

   Although these tools do not provide complete visibility into the third party's VM program, they do provide insight to patching externally facing computing assets.

3. **The VM Team should advocate for the use of third-party risk management tools that support vulnerability communication and remediation activities.**

Third party risk management tools are becoming more robust, enabling third party risk management organizations to communicate vulnerabilities to third parties and to oversee risk remediation activities.

VM for Applications

While development teams are usually responsible for identifying and mitigating vulnerabilities in code, the VM team may provide support through vulnerability notification, consultation, and remediation oversight.

Task force members recommended the use of vulnerability management tools as "far left" (early on) in the development process. Verbatim member comments are as follows:

- "Veracode is too far to the right."
- "Shifted to Snyk which identifies vulnerabilities earlier in the pipeline."
- "Wiz.io integrates with CI/CD to identify vulnerabilities."

VM for Acquisitions

Security organizations are often brought into the tail end of the acquisition due diligence process, making it difficult to gain insight into or oversee the vulnerability management practices of newly acquired businesses. Therefore, task force members recommended leveraging security report card services, like BitSight and SecurityScorecard, to help ensure that acquisitions are minimally addressing externally facing vulnerabilities.

Use of Bug Bounty Programs

Bub bounty programs, like BugCrowd, can help identify exploitable vulnerabilities and provide insights to penetration testers. However, members engaging bug bounty services recommend dedicating internal staff resources to maximize their value and to establish and carefully manage a bug bounty budget.

Summary

Vulnerabilities in operating systems, middleware, and applications have been exploited since the early days of the Internet. Vulnerabilities are still a primary means for exploitation of computer assets.

Vulnerabilities exist in all computing environments – cloud computing, third parties, on premises, and in companies being acquired.

Because vulnerabilities are prevalent in all computing environments and are significant exploit targets, entities must establish a Vulnerability Management Program (VMP). A comprehensive VMP requires organizational resources (VM Team, Budget, Stakeholders, Governance), Processes (VM Lifecycle Processes, Remediation SLAs, Metrics), and Tools (Asset Discovery, Vulnerability Identification, Vulnerability Remediation).

To implement an effective VMP:

- Senior management must endorse the VMP and authorize funding for support personnel and tools.
- Remediation SLA timeframes must be established based on vulnerability risk categories.
- Stakeholder organizations responsible for remediating vulnerabilities must strive (and be held accountable) to remediate vulnerabilities within SLA timeframes.
- SLA performance must be measured and reviewed, and corrective measures implemented.
- The VMP cannot operate without vulnerability scanning tools and will not scale without communication and remediation tracking and support tools.

Appendix: Member Comments About Vulnerability Management Tools

Tool	Member Comments
AppOmni	• For SaaS applications. • To understand how SaaS applications are implemented. • The fear is how we configure these apps.
Atlassian	Using this as a ticketing system
AvePoint	• Governance of SharePoint, OneDrive, and Teams environments • Allows approval from a Centralized Team to say we already have this capability. • Cuts down on sprawl. • Collects metadata. • Attestation workflows. • Can add a tab into Teams client and can do a self-service which sends a request to the Centralized Team.
CrowdStrike	• Leverage CrowdStrike, Falcon (Netskope), Qualys. • CrowdStrike/Falcon – can use the same agent for doing scans. • Limited in what they discover.
Falcon Complete (Netskope)	• Leverage CrowdStrike, Falcon (Netskope), Qualys. • CrowdStrike/Falcon – can use the same agent for doing scans.
Intune	• Infrastructure/ops doing its own patching (Intune, SCCM).

Ivanti	• Ivanti is used as the patching product as a second pass or security check on patched data.
	• Ivanti
	  ○ Can provide input to asset management program (Neurons).
	  ○ Can inventory software, service tags and has a Qualys connector.
	  ○ Has an agent and a ticketing system.

JIRA	• Can do custom integration with JIRA. • Ticketing system makes it easy to collaborate (Jira, Atlassian).
Kenna Security	• Nexpose feeds into Kenna Security and then can report vulnerabilities based on risk; will also tell the Apps team of their vulnerabilities. Kenna takes vulnerability scans and assigns a score for you based on risk.
NorthStar	• Tool that collects log from different scanners (e.g., NorthStar) takes in logs from other scanners to have other areas connect and identify assets; use this to ensure that all controls are in place and tells of devices not in the CMDB.

Qualys	• Qualys – can classify agents.
	• Risk-based identification is done within Qualys.
	• Run Qualys Reports.
	  ○ Can do asset searches.
	  ○ E.g., look at the top 10 vulnerabilities based on risk (three criteria: CVSS 8+ + Severity 4-5 in Qualys, and if exploitable; Qualys has its own database.
	• Has a link to the Qualys database to tell how to fix it.

Tool	Member Comments

	• Qualys is used to validate patching (vulnerability management scans by the end of the month.
	• Tomcat is used in many applications; Qualys will find many older versions; Tomcat does not get patched automatically.
	• Can inventory software, service tags and has a Qualys connector.
	• At the end of each month, we scan all IP subnets with Qualys and tag them and then scan them.
	• Leverage CrowdStrike, Falcon (Netskope), Qualys.
	• Leverage Qualys agent for certain environments; Qualys has more applications.
	• There is more to addressing a vulnerability sometimes than simply installing a patch (e.g., updating registry keys). Qualys will pick up that a registry key is missing.
	• Issue with Qualys ticketing system.
	• Monthly scans of networks / servers (Qualys – no agent).
	• Qualys has a database of vulnerabilities for scanning access.
	• Qualys can do discovery with IP to identify vulnerabilities (reactive)
	• Use Qualys:
	  ○ Does a decent job of knowing applications.
	  ○ 1000's of vulnerabilities.
	  ○ Knows about all CVEs out there for all applications – this is reactive.
	• Qualys:
	  ○ Can show all assets that have vulnerabilities, but if the scan was done three weeks ago, may miss a new asset.
	  ○ Does well with authenticated scans to determine version numbers.

Rapid7/Nexpose	• Very invested in Rapid 7
	  ○ Started to do this is the Cloud.
	  ○ Security tool is "everything to everybody".
	  ○ Need to buy an additional tool.
	  ○ This becomes extremely expensive.
	• Rapid 7 shop.
	• Rapid7 owns Metasploit.
	• Nexpose feeds into Kenna Security and then can report vulnerabilities based on risk; will also tell the Apps team of their vulnerabilities. Kenna takes vulnerability scans and assigns a score for you based on risk.

ServiceNow	Building a CMDB and are formalizing it in ServiceNow.
Tanium	• Bring in application tools to interrogate assets (Tanium). • Tanium has an agent-based solution to does discovery. • Tanium is a distributed model where endpoints talk to each other. • Tanium provides full coverage. • Use Tanium; can do automated patching (combination of things).
Tenable / Nessus	• We use agents with Tenable. • Want to track performance through Tenable. • Teams use Tenable API to build their own spreadsheets.

Tool	Member Comments
	• Missing patches: Patch management is not the source of truth; must go through Tenable as the source of truth, not simply tracking their patching tool. • Use Tenable. • Continuous Nessus scans. • Nessus agent across all endpoints (twice daily scanning).
Wiz.io	• Wiz.io can bankrupt your company because it looks at exactly what is running on the instance, getting into Java vulnerabilities. • Wiz is focused on AWS; buy workloads. • Cost of Wiz workloads is $55K for 700 workloads . • "Best in class" product. • Have fully operationalized Wiz.io. • Wiz is moving to data protection. • Coming out with advanced licenses. • In AWS & Azure. • Manages our Cloud environments. • Wiz costs $85 per workload. • Wiz pulls together insights. • Can easily onboard Amazon and Azure accounts in the tool. • Takes 15 minutes to get it up and running. • Implemented Wiz, which looks for the worst of the worst: will provide a list and alert. • Link for DAS which integrates with Wiz.