chi Cybersecurity Studio

Lab Report

Beyond CVSS – New Approaches to Vulnerability Management

Companies Need to Radically Prioritize Their Vulnerabilities

The number of IT vulnerabilities has risen by 411% since 2005, when CVSS scoring was first introduced. Legacy vulnerability management practices no longer work.

Technologies Mentioned

CyCognito
Kenna
Nucleus
Palo Alto Prisma Cloud
Rapid7
Splunk
Tanium
Tenable
Vulcan
Wiz

*If you are interested in connecting with a partner on any of these technologies, let us know.

Go Deeper

Work together on a new framework in upcoming sessions:

March 28: *OT Vulnerability Remediation*
April 04: *Approaches to Attack Surface Management*
Coming soon: *Radical Vulnerability Prioritization*
Coming soon: *Vulnerability Remediation Partner Relationship Management*

Why It Matters

Vulnerability Management is a relationship management job. There needs to be trust between Cybersecurity teams and their partners who manage the technology and are responsible for any remediations. Traditional vulnerability management programs do the exact opposite — they flood partners with thousands of vulnerabilities that cannot, and should not, all be remediated.

A new framework is needed that:

- **Radically prioritizes vulnerability remediation** based on the threat landscape and a company's exposure to those threats. This framework should differentiate between when there are vulnerabilities that pose an imminent threat to the organization, and then everything else.

- **Shifts mindsets** across the organization and governing bodies. Remediation partners embrace new behaviors built on the right sense of urgency. Executives and governing bodies embrace risk management, rather than risk elimination.

- **Includes a unified view of vulnerabilities** and remediation priorities across a vast technology footprint. This view can ease today's subject-matter expertise resourcing requirements across both cybersecurity teams, and remediation teams. While this unified view has proven elusive for most teams, it is a potential game-changer.

Quick Win

- **Implement a remediation hierarchy with no more than 3 tiers.** Put vulnerabilities from your Attack Surface at the top and define an aggressive timeframe and process for remediation, while lengthening timeframes for lower tiers. Consider invoking incident management to signal urgency. Be particularly vocal in recognizing remediation partners when SLAs are achieved.

Lab Report

Beyond CVSS – New Approaches Vulnerability Management

Shifts in Vulnerability Management Approaches

As the four lab participants outlined their transformation journeys a key theme emerged: success is achieved when you've aligned the resources, processes, and tools to responsibly allocate vulnerability identification and remediation labor.

Company 1 described their journey from "fix everything" to risk-based prioritization.

- The program started out heavily focused on numbers and efficiency — grabbing vulnerability data from all over the network and leveraging a third-party to run the operations.
- The combination of the two didn't work. Too much data was blindly passed to partners and was not resulting in remediation of the worst vulnerabilities.
- More recently, they have established a new scoring mechanism and remediation timelines for vulnerabilities based on exploitability and impact.
- Components of the risk score include: exploitability of the vulnerability and where the asset sits on the network.
- While they won't re-score older vulnerabilities, they do provide recommendations on how to prioritize the backlog.
- **Team structure:** Recently they've insourced the program and tied it more closely to the risk management function. The cybersecurity team currently does not manage Cloud vulnerabilities.

Company 2 is in the midst of a significant transformation to their vulnerability management program, introducing a new model for prioritization.

- This year the focus is on centralizing and normalizing vulnerabilities from multiple sources.
- Once consolidated, they will apply a new risk-based formula to score each vulnerability, which will drive a new remediation workflow.
- Components of the risk score include: asset value, accessibility from the internet, whether a vulnerability is on CISA's list, and age of hardware.
- The new workflow includes measurements for remediation teams' speed and ability to remediate on time.
- In the future they want to tackle building a risk acceptance process.
- **Team structure:** Infrastructure and Application vulnerabilities are managed under two different teams due to expertise, however the same risk-based framework will be applied. Currently the team does not manage Cloud vulnerabilities.

Lab Report

Beyond CVSS – New Approaches Vulnerability Management

Shifts in Vulnerability Management Approaches

Company 3 is working to implement scanning and management tools that help, rather than hinder, the program.

- The team relies primarily on agent-based scanning for IT solutions, but has been through several in the last few years that haven't met their needs.
- They have been searching for a solution that makes it easy for remediation teams to address identified vulnerabilities.
- Earlier in their journey, the team implemented accelerated remediation timelines for vulnerabilities identified by their attack surface management program. This has proven effective to get attention on the highest-priority vulnerabilities.
- **Team structure:** Infrastructure, Application, OT/ICS, and Cloud vulnerabilities are managed under different teams due to expertise. They plan to invest in training around knowledge gaps, particularly Cloud security, in an effort to eventually combine the team.

Company 4 is exploring new vulnerability prioritization frameworks and preparing for the next big vulnerability, like Log4j.

- The team is evaluating new vulnerability scoring approaches like Exploit Prediction Scoring System (EPSS) from FIRST.
- During Log4j, the team invoked the IT incident response team to manage urgent remediation activities and to ensure the work was tracked to completion. This model proved effective and they are now creating repeatability for similarly significant vulnerabilities.
- This company implemented a Unified Vulnerability Management platform in 2021 and continues to optimize its use. They have found the most value in the self-service and workflow capabilities of the platform which benefit remediation partners. However, the quality of data from asset inventories has limited its effectiveness.
- **Team structure:** Infrastructure and Cloud vulnerabilities are managed under one team, while Application vulnerability fall under another.

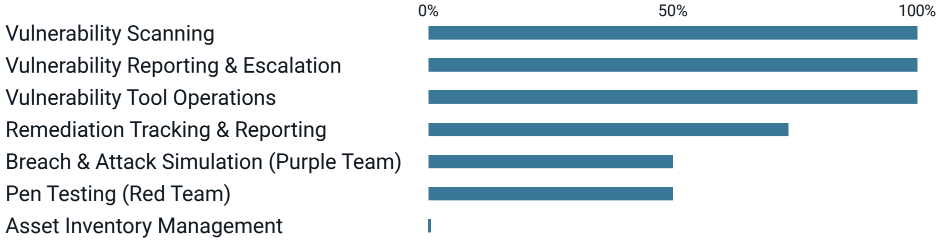
Lab Report

Beyond CVSS – New Approaches Vulnerability Management

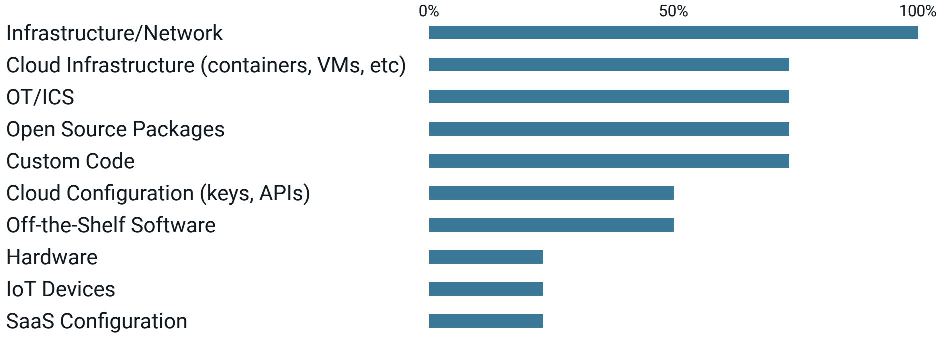
Participant Surveys

We asked the lab participants three questions about the day-to-day activities of their teams, and where they would look to grow.

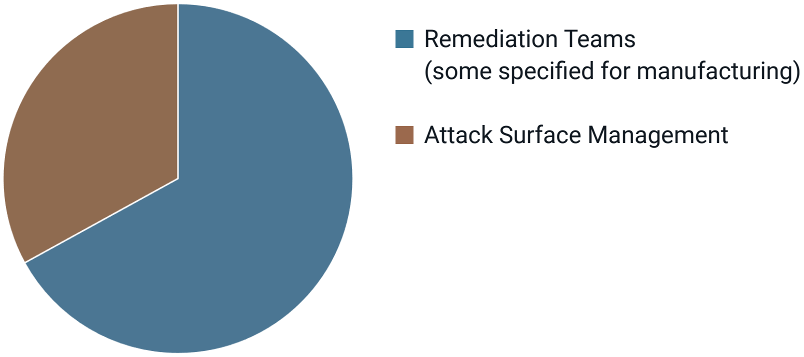
1. Which functions fall under your Vulnerability Management program today?



2. What types of vulnerabilities are you tracking in your program?



3. Where would you allocate 5 new headcount to get maximum benefit for reducing the organization's vulnerabilities??


Remediation Teams
(some specified for manufacturing)
Attack Surface Management