VULCAN | PULSE

How are Cyber Security Teams Prioritizing Vulnerability Risk?

How are Cyber Security Teams Prioritizing Vulnerability Risk?

Risk-based vulnerability management (RBVM) is essential to proactive defense against cyber threats, but many programs are too often ineffective and inefficient. Without an RBVM platform, security teams struggle to make the transition from simple vulnerability identification to meaningful response and mitigation. Ultimately, cyber security teams must deliver a common framework for risk visibility and work collaboratively with business leaders and IT teams to reduce cyber risk to the business.

According to this new research, security teams are not doing enough to correlate vulnerability data with actual business risk. Most vulnerability management programs are not giving business leaders and IT management professionals the risk insights they need to effectively protect valuable business assets, as opposed to any business asset regardless of relevance to the business.

Pulse and Vulcan Cyber surveyed 200 technology IT security decision-makers to find out how vulnerability risk is prioritized, managed and reduced.

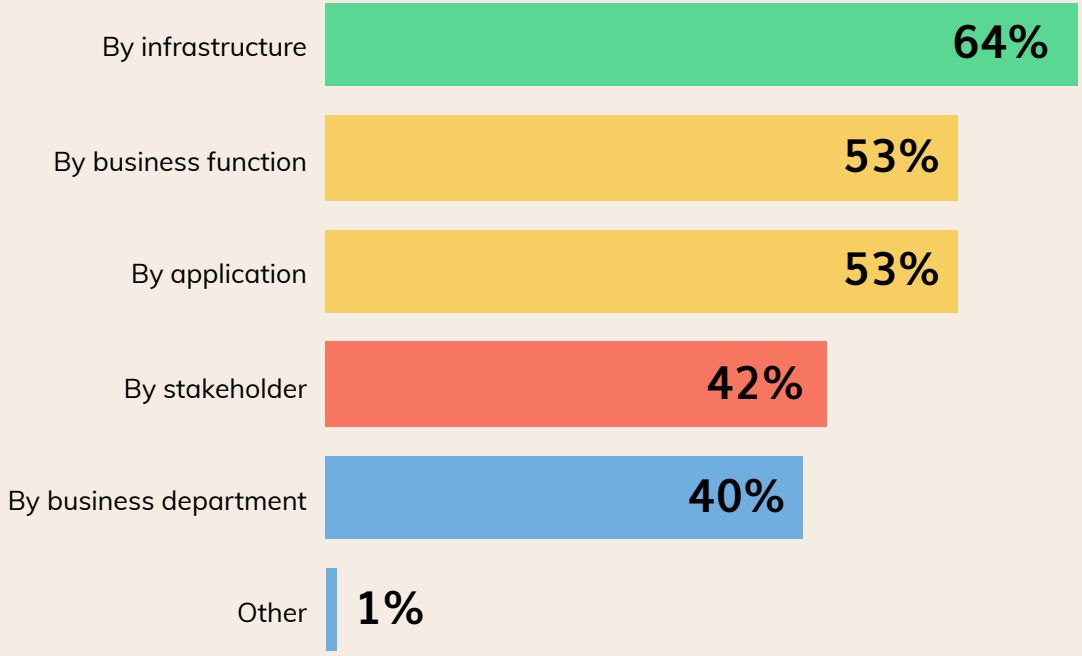
Data collection: September 23 - October 17, 2021

Respondents: 200 technology decision-makers

Most group vulnerabilities by infrastructure and prioritize based on third-party vulnerability severity data

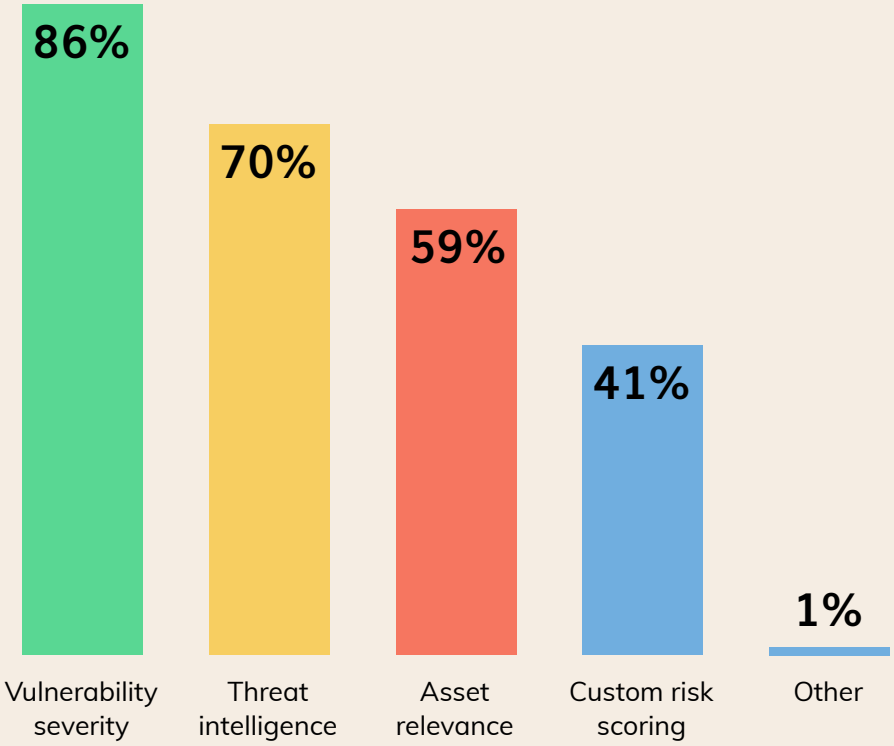
Decision-makers group by infrastructure (64%), business function (53%), and application (53%) when prioritizing vulnerabilities.

How do you group vulnerabilities when prioritizing?



Respondents use vulnerability severity (86%), threat intelligence (70%), and asset relevance (59%) data to prioritize vulnerabilities.

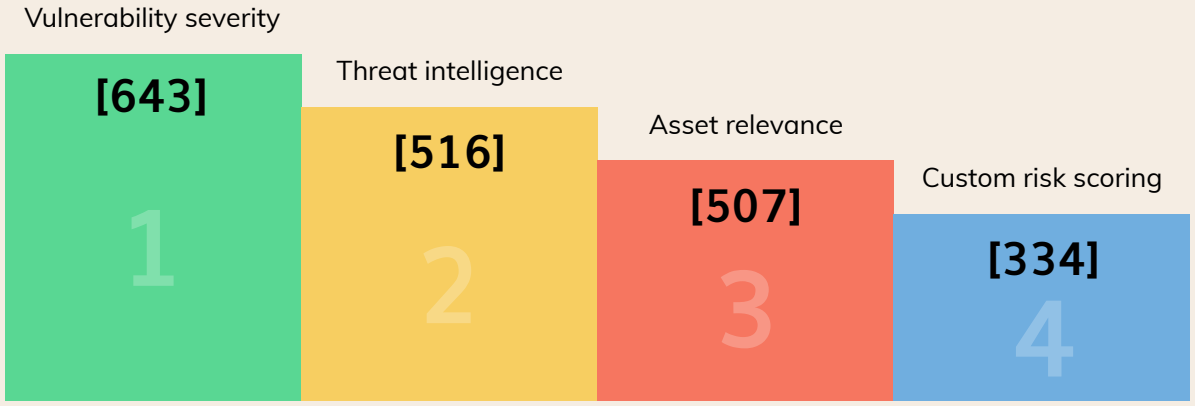
What data would you use to prioritize vulnerabilities identified by your business?



Vulnerability severity has the greatest impact on prioritization and most use multiple models to score vulnerabilities

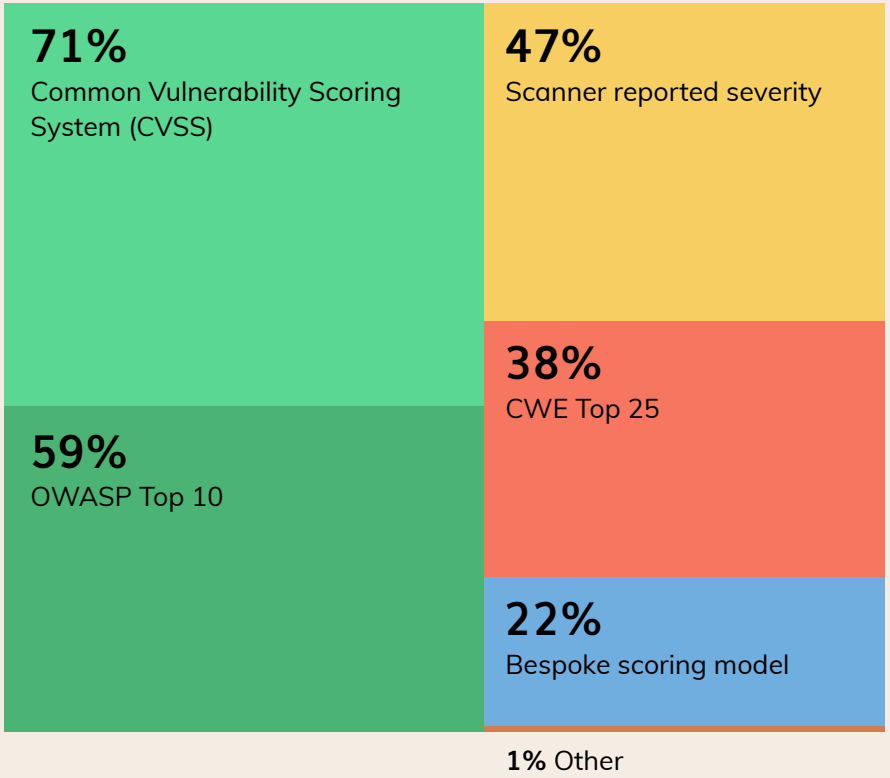
Decision-makers rank vulnerability severity, threat intelligence, and asset relevance as the most impactful on their vulnerability prioritization.

Rank the following inputs in order of impactfulness on your vulnerability prioritization.



To score and prioritize vulnerabilities, decision-makers use the common vulnerability scoring system (CVSS) (71%), OWASP top 10 (59%), and scanner reported severity (47%).

What model(s) does your organization use to score and prioritize vulnerabilities?



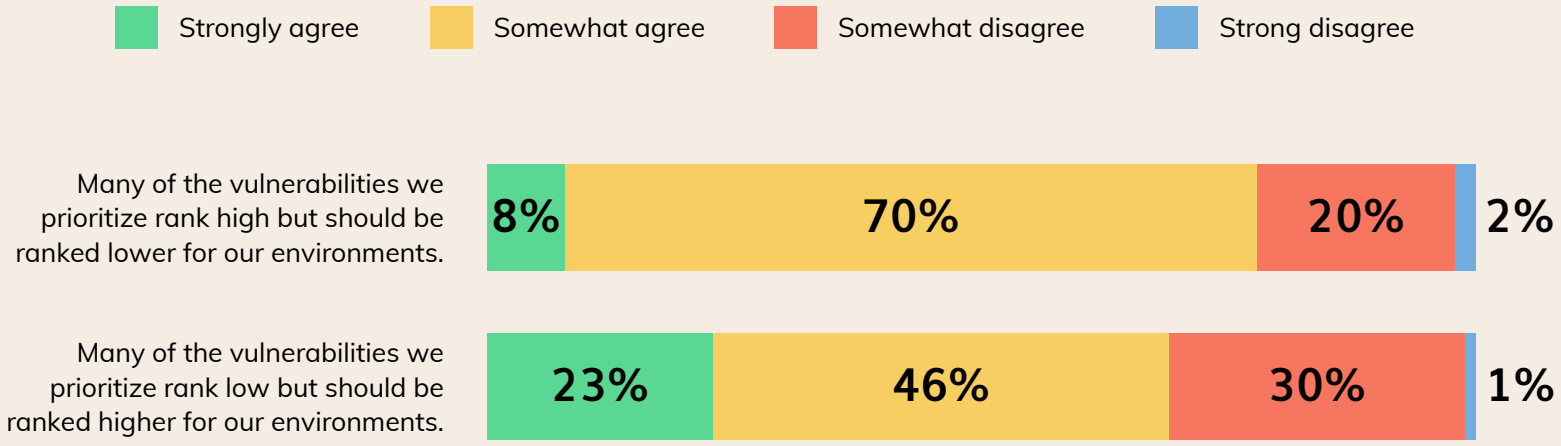
1% Other

In addition, 77% of respondents use at least 2 models to score and prioritize vulnerabilities.

Most agree they should adjust their prioritization of vulnerabilities

78% of respondents agree that high ranked vulnerabilities should be ranked lower, while 69% of respondents agree that low ranked vulnerabilities should be ranked higher.

To what extent do you agree or disagree with the following statements?

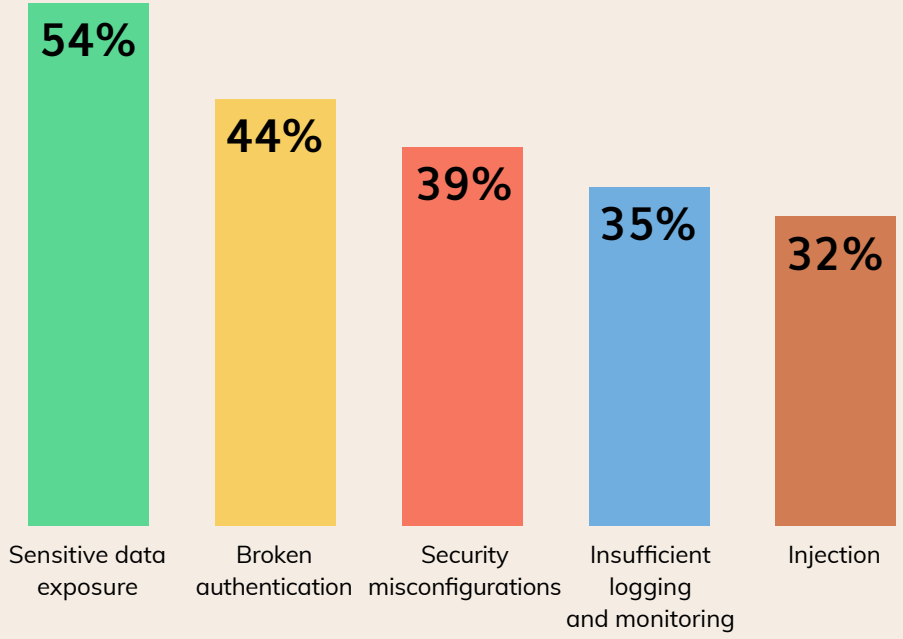


Leaders are most concerned about sensitive data exposure and MS14-068 (Microsoft Kerberos unprivileged user accounts)

Decision-makers say that sensitive data exposure (54%), broken authentication (44%), and security misconfigurations (39%) are the application vulnerability types most concerning to their organization.

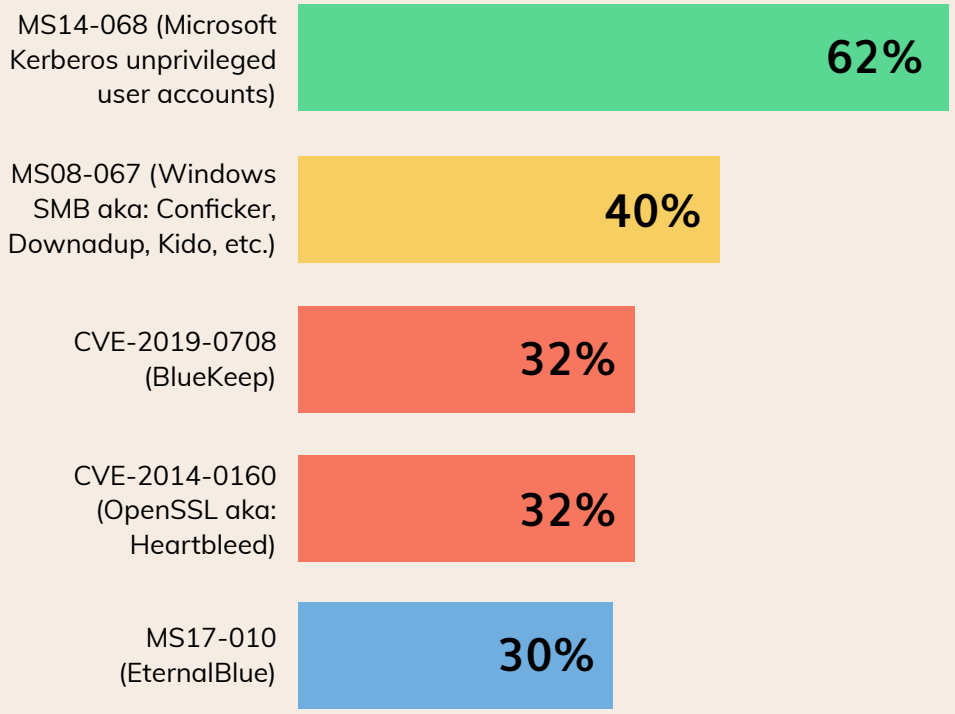
Of the most common application vulnerability types, which three are the most concerning to your organization?

Cross-site scripting (XSS) **31%**,
Using components with known vulnerabilities **30%**,
Broken access control **29%**,
XML external entity (XXE) **17%**,
Insecure deserialization **5%**,
Don't know **1%**



Respondents say that MS14-068 (62%), MS08-067 (40%), and CVE-20190-0708 (32%) are the most concerning vulnerabilities to their organization.

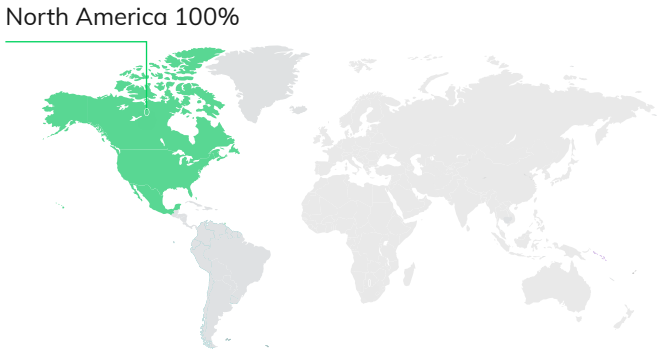
Of these specific vulnerabilities and common vulnerabilities and exposures (CVEs), which are most concerning to your organization?



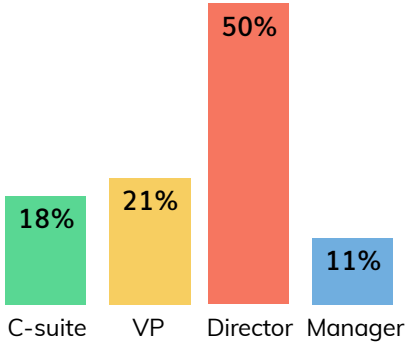
MS01-023 (Microsoft IIS aka: Nimda) **30%**, Spectre / Meltdown (CPU vulnerabilities) **29%**, CVE-2008-1447 (DNS aka: Kaminsky) **24%**, CVE-2014-6271 (Bash aka: Shellshock) **13%**, MS02-039 (SQL Slammer) **13%**

Respondent breakdown

Location



Titles



Company Size