VULCAN | PULSE

How Are Businesses Mitigating Cyber Risk?

How are businesses mitigating cyber risk?

Companies are grappling with an increasing number of cyber threats across digital surfaces from traditional IT infrastructure, to cloud application environments. Security leaders are looking for ways to fine-tune their risk identification, prioritization and mitigation programs.

However, leaders are realizing that legacy vulnerability management efforts aren't getting the job done, and that risk and cybersecurity resources could be better utilized if focused on remediation outcomes. Pulse and Vulcan Cyber surveyed 200 cybersecurity leaders to learn more about their cyber hygiene regimens—in particular what their risk remediation and mitigation priorities and programs are.

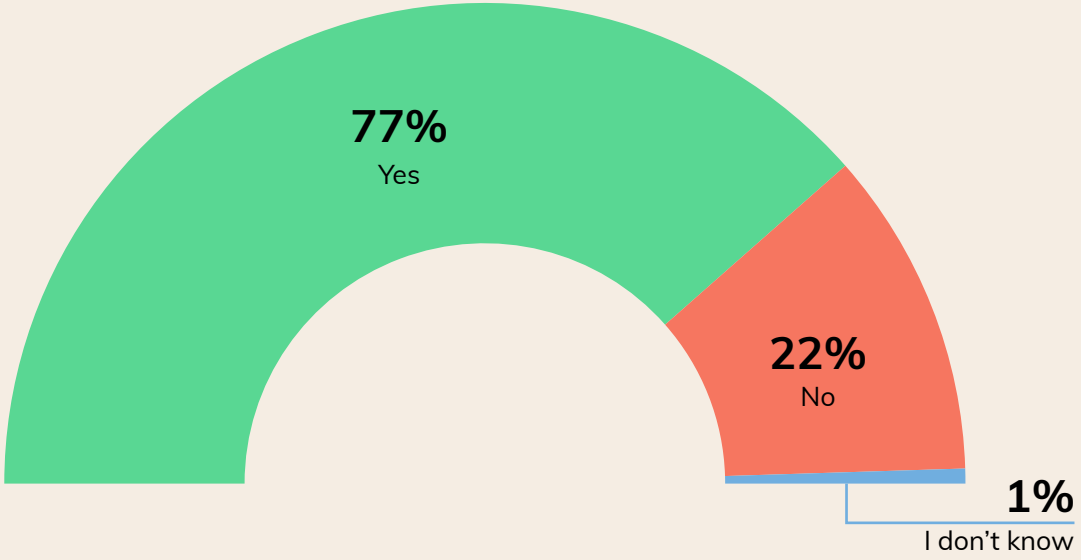
Data collected from July 1 - July 9, 2021

Respondents: 200 cybersecurity leaders

You are not alone: 77% of businesses have been impacted by unmitigated risk

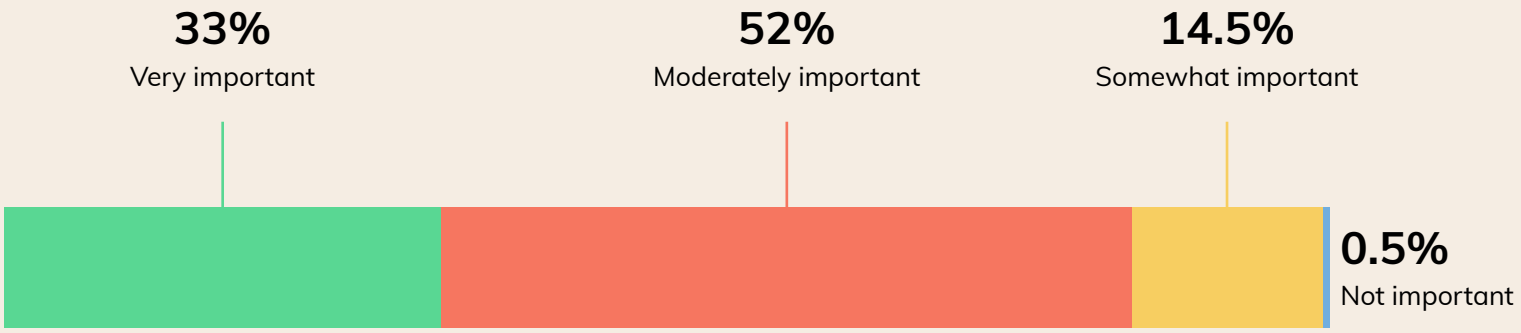
More than three-quarters (77%) of cybersecurity leaders have been impacted by a security vulnerability in the past year.

Has an IT security vulnerability impacted your business within the last year?



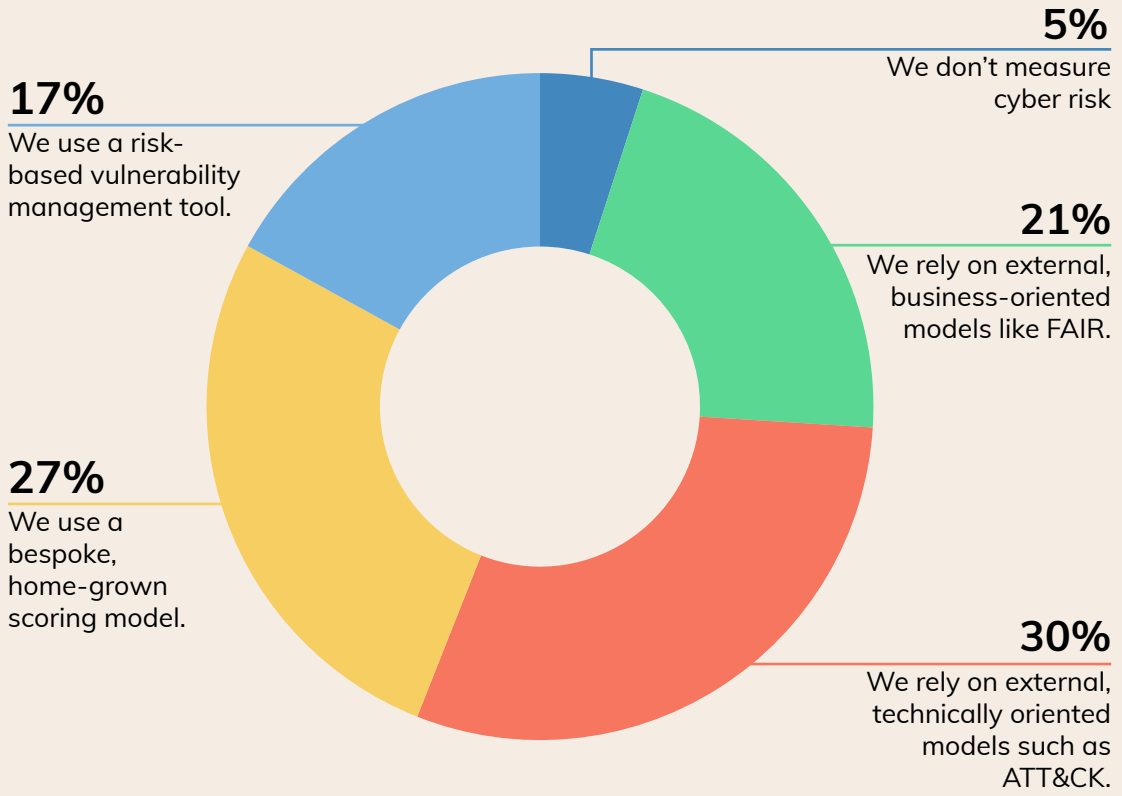
As most cybersecurity leaders experienced a security breach recently, 85% deem it moderately or very important to manage and prioritize vulnerabilities with a risk-based approach.

How important is risk-based vulnerability management and prioritization to your organization?



Only 5% of the survey respondents don't measure cyber risk, with more than 51% using external risk models such as FAIR and ATT&CK. Twenty-seven percent use a risk scoring model developed in-house and 17% use a purpose-built risk-based vulnerability management tool.

How do you measure cyber risk to your business?



A majority of the cybersecurity leaders (76%) apply the same risk scoring and prioritization model for infrastructure as they do for application surfaces.

Do you use the same prioritization (risk score) model for both infrastructure and application security?

76%
Yes

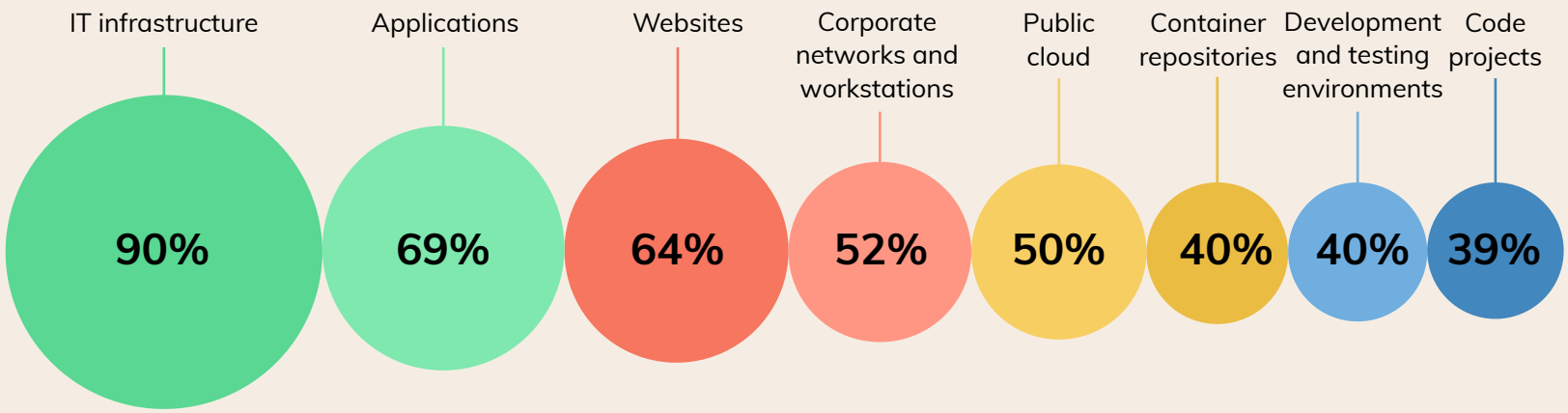
21%
No

3%
I don't know

A scanner for every surface

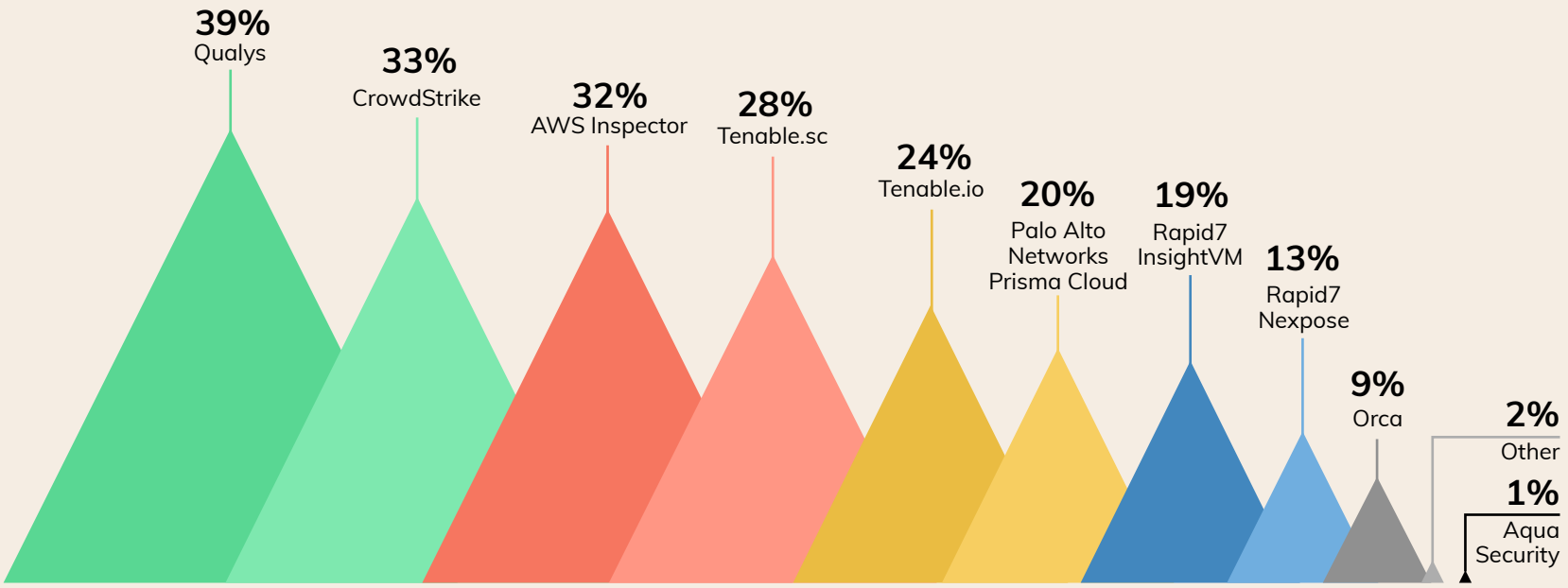
The top three surfaces cybersecurity leaders scan for vulnerabilities are infrastructure (90%), applications (69%), and websites (64%). Only 39% of respondents scan their code projects.

What IT assets do you scan for vulnerabilities?

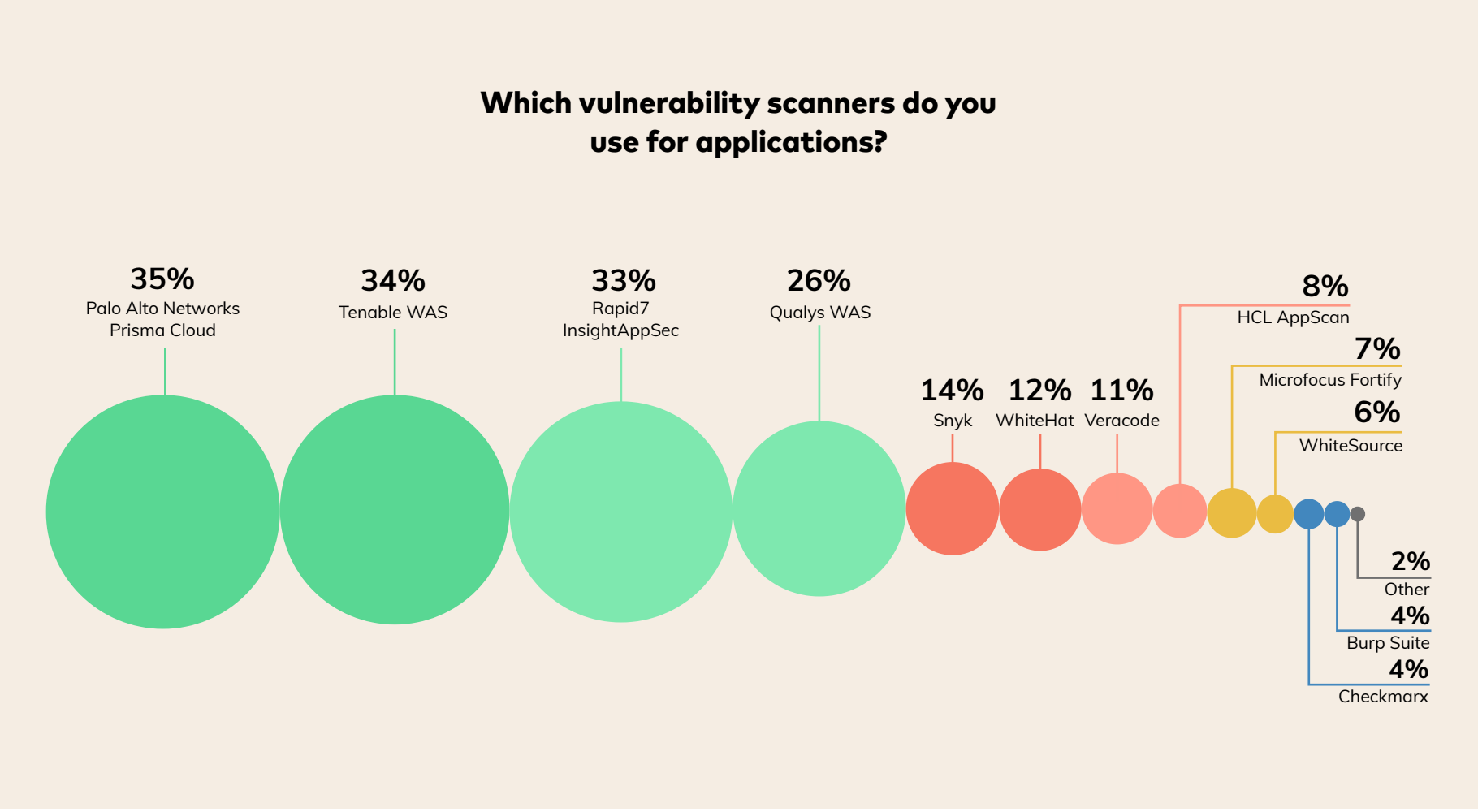


The most popular vulnerability scanners used for IT infrastructure are Qualys (39%), CrowdStrike (33%), AWS Inspector (32%), Tenable.sc (28%) and Tenable.io (24%).

Which vulnerability scanners do you use for IT infrastructure?



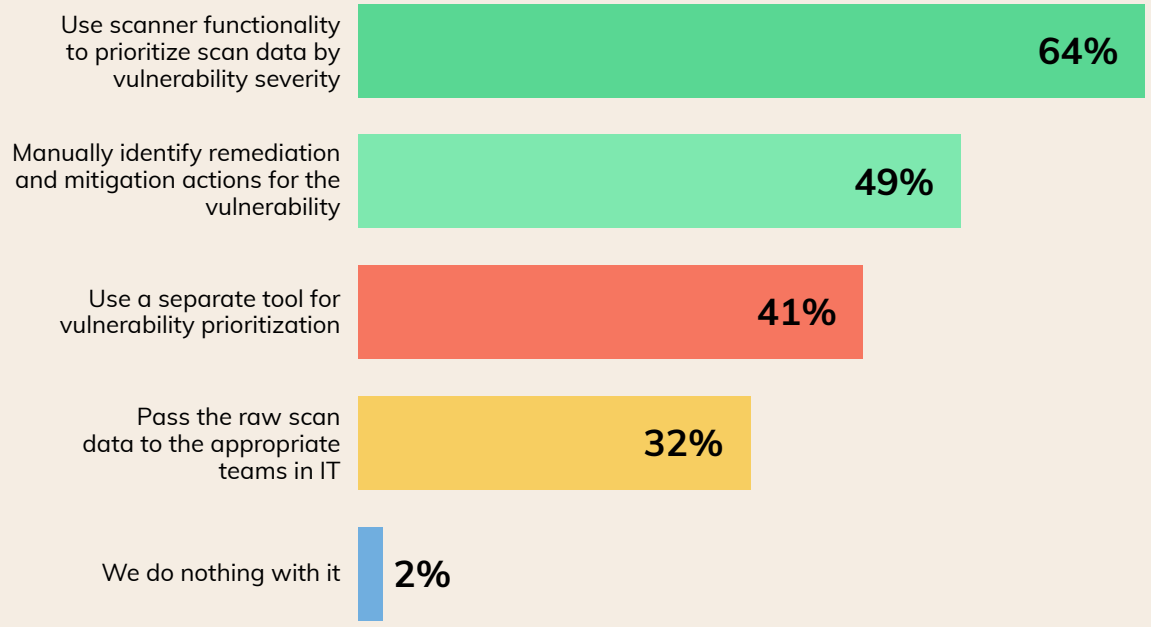
A different set of scanners are used for applications; the most popular ones are Palo Alto Networks Prisma Cloud (35%), Tenable WAS (34%), Rapid7 InsightAppSec (33%) and Qualys WAS (26%).



Manual processes and IT leader stakeholders heavily influence risk prioritization and mitigation

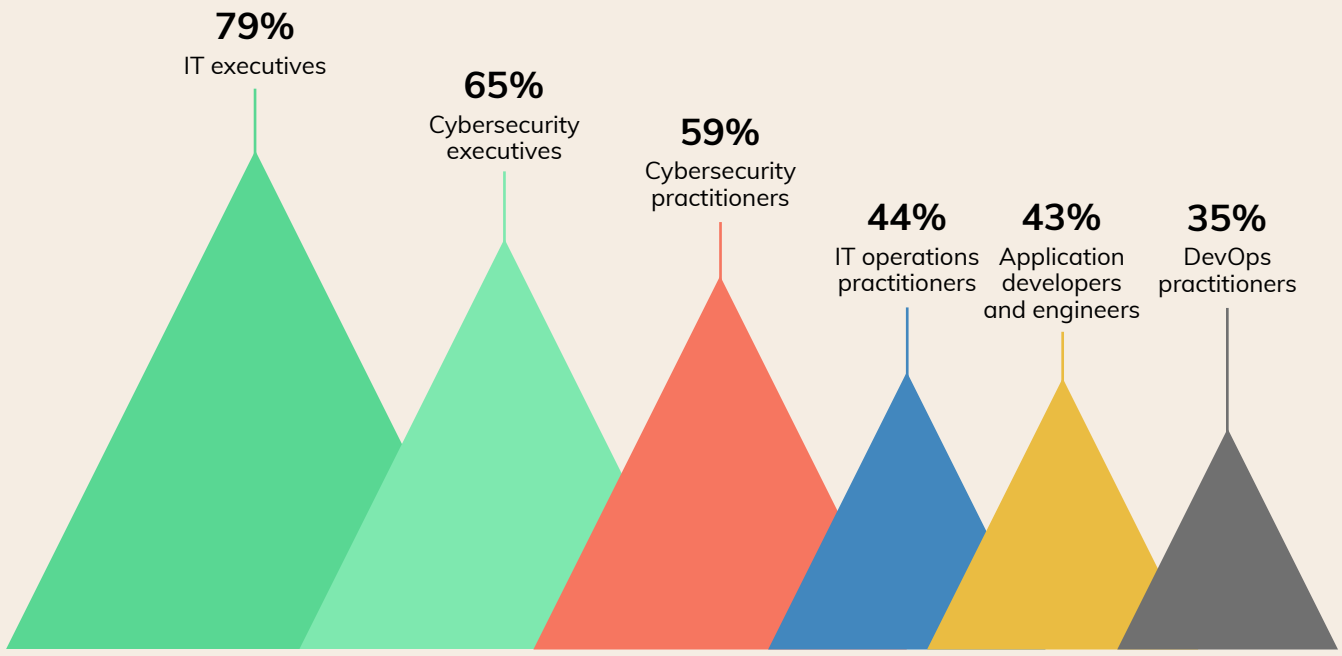
Once cybersecurity leaders have collected the data from a vulnerability scan, 64% use their scanners to identify AND prioritize vulnerabilities, while 49% rely on manual processes to identify remediation and mitigation actions. Forty-one percent use a separate tool to prioritize risk.

What do you currently do with your vulnerability scan data?



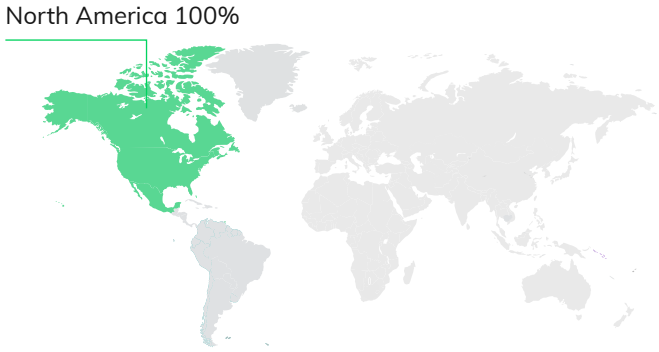
Cybersecurity executives (65%) and IT executives (79%) have the most sway when it comes to influencing the vulnerability and risk prioritization efforts. Meanwhile, IT operations (44%), developers (43%), and DevOps (35%) have a reduced influence.

What stakeholders are involved in your vulnerability prioritization effort?

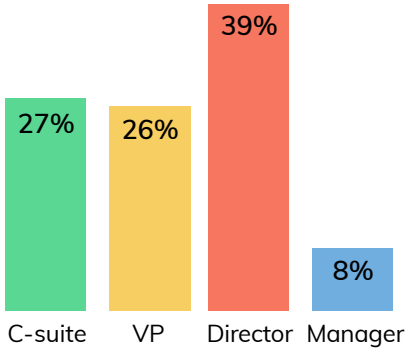


Respondent breakdown

Location



Titles



Company Size