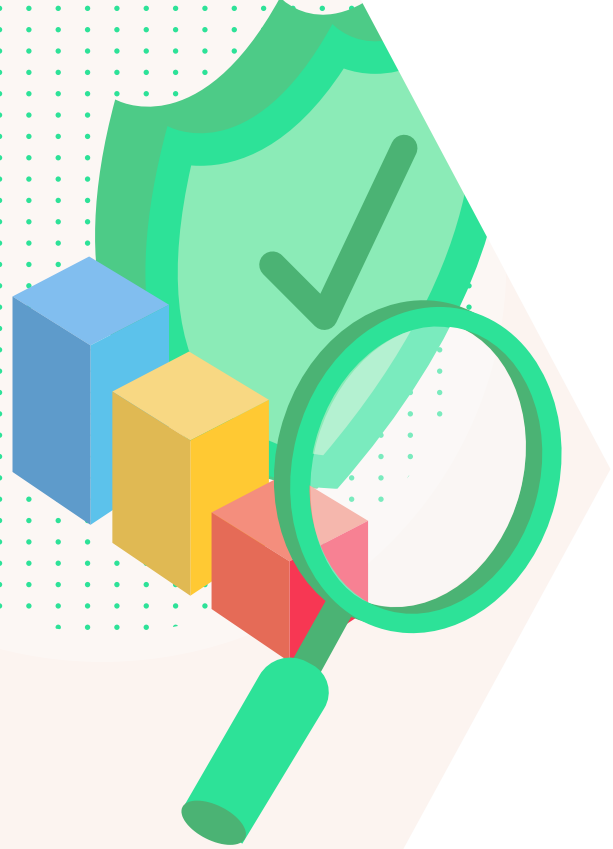


VULCAN. | Gartner Peer Insights™

Threat Intelligence Adoption Rises to Reduce Vulnerability Risk

Threat Intelligence Adoption Rises to Reduce Vulnerability Risk

Threat intelligence reduces vulnerability risk to optimize security posture by removing blind spots and providing crucial visibility. The goal for any security team is to more-effectively identify threats and prioritize the most-critical vulnerabilities.

Gartner Peer Insights and Vulcan Cyber surveyed 100 information security, vulnerability management, and threat intelligence executives and practitioners to understand how they approach threat intelligence at their organization. The survey and research exposes answers to questions such as:

- How are security managers relying on threat intelligence to keep attack surfaces secure?
- What are the most common threat intelligence use cases?
- Which threat intelligence challenges are the most concerning for security managers?

Data collection: June 8 - July 29, 2022

Respondents: 100 Information Security, Vulnerability Management, and Threat Intelligence Managers and Directors

With dedicated threat intelligence teams and budgets, information security leaders are tackling a wide range of security use cases

Nearly 75% of respondents' organizations have a dedicated threat intelligence team.

Do you have a team dedicated specifically to threat intelligence in place?

74%
Yes

21%
No

5%
Not sure

While many have dedicated teams, only two-thirds of information security managers and directors have a budget dedicated specifically for threat intelligence.

Do you have budget allocated specifically for threat intelligence?

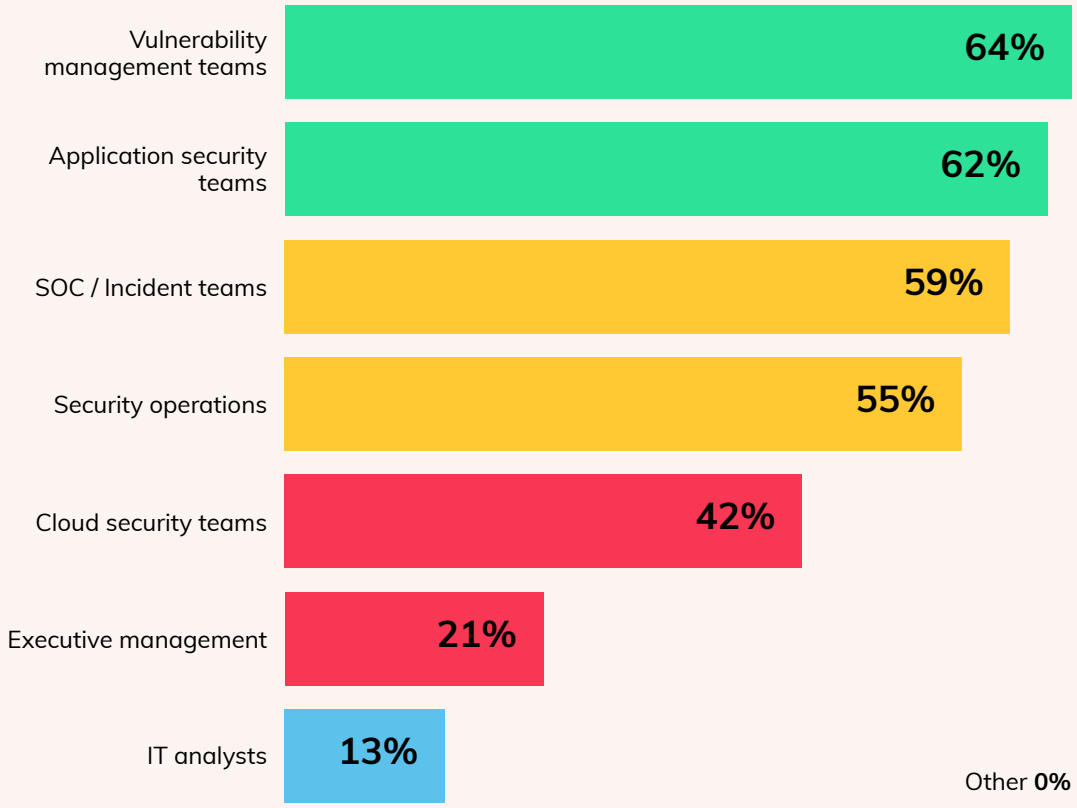
66%
Yes

30%
No

4%
Not sure

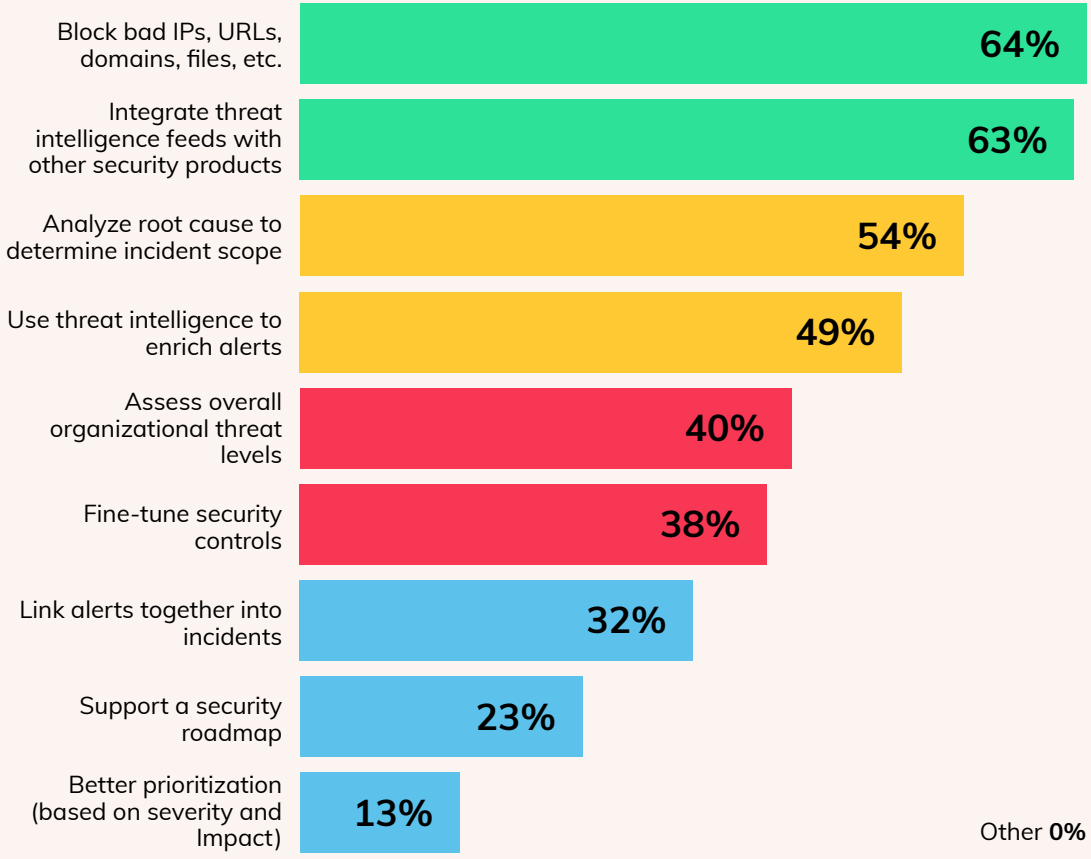
Information security managers and directors cite vulnerability management (64%), application security (62%), and SOC/incident teams (59%) as the top threat intelligence consumers in their organizations.

Who would you consider as the primary threat intelligence "consumers" in your organization?



The most common use cases for threat intelligence are blocking bad IPs (64%), integrating threat intelligence feeds with other security products (63%), and analyzing root cause to determine scope (54%).

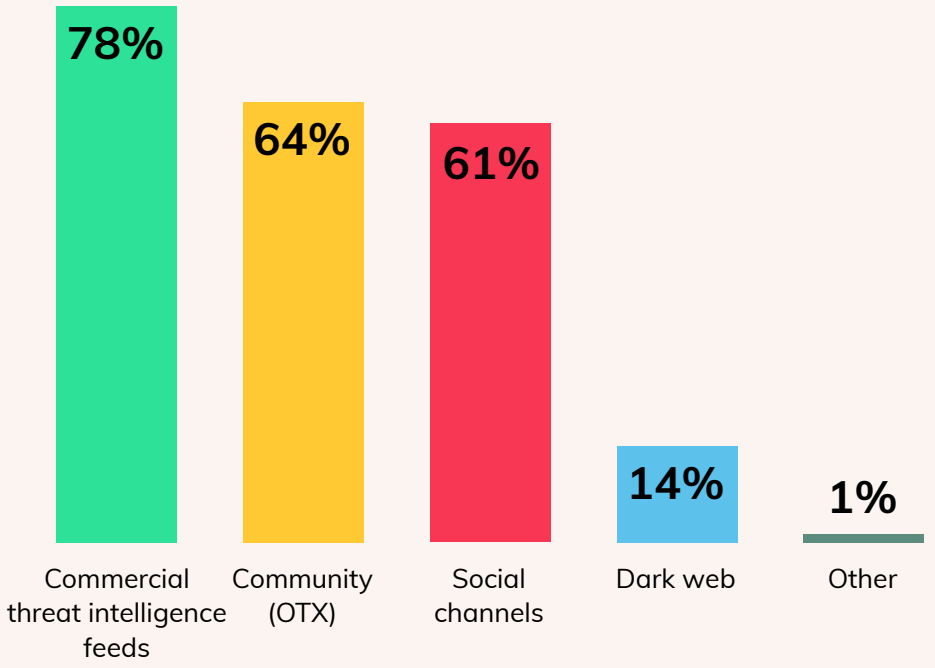
What are your main use cases for threat intelligence?



Many leaders rely on vendor threat feeds (3rd party vendors) as skills lack and intelligence is not predictive enough

The most used source of threat intelligence was reported as commercial feeds (78%).

What are your current sources of threat intelligence?



A lack of skills (73%) and threat intelligence not being predictive enough (55%) are the two biggest challenges respondents face.

What are your biggest threat intelligence challenges?

Despite challenges with threat intelligence predictiveness, 56% use or plan to use predictive models such as EPSS.

Do you, or are you planning to, use threat intelligence predictive models (such as EPSS)?

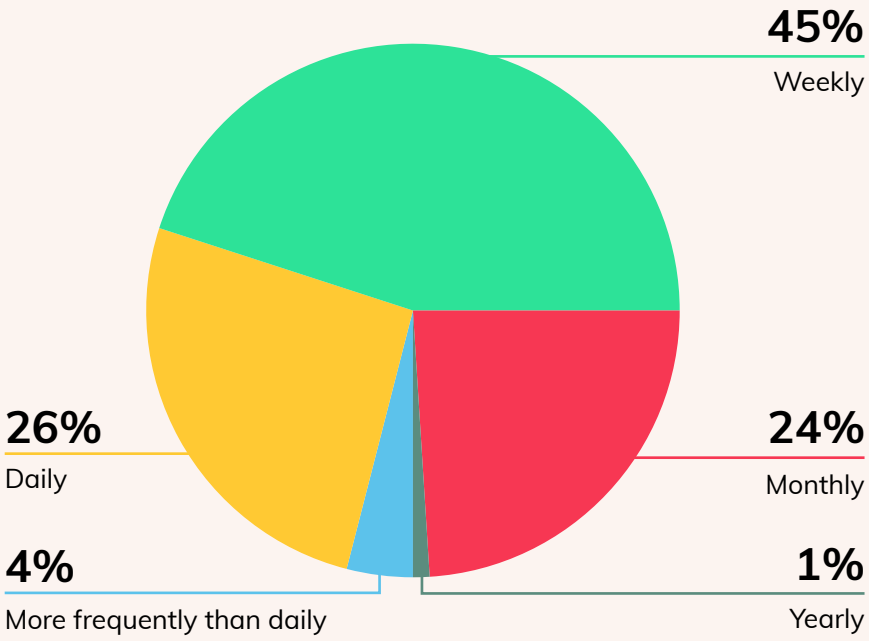
56%
Yes

17%
No

27%
Not sure

Respondents use threat intelligence to identify and prioritize risks more often than ever

75% of respondents say threat intelligence helps their team identify threats at least weekly.



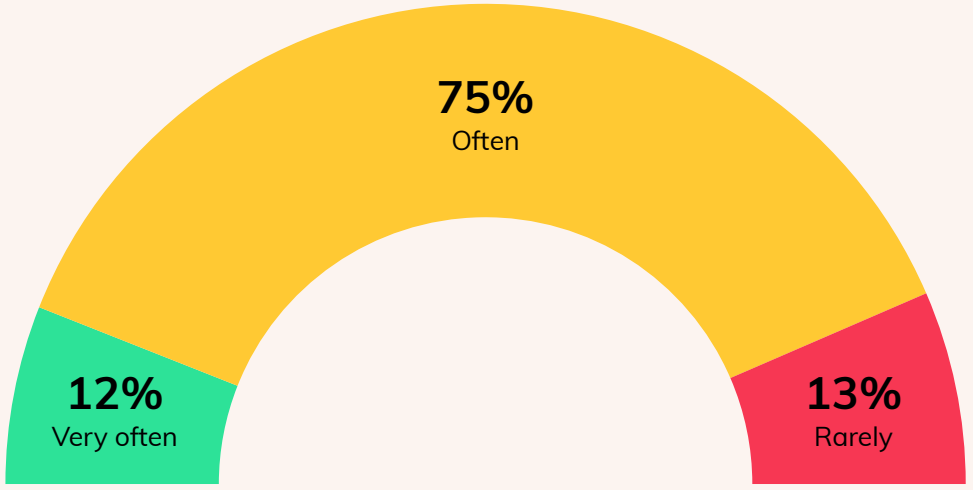
How often does threat intelligence help your team identify potential threats or prevent incidents?

Less frequently than yearly **0%**

Never **0%**

87% of decision makers rely on threat intelligence often or very often for vulnerability prioritization.

How often does your organization rely on threat intelligence for vulnerability prioritization?



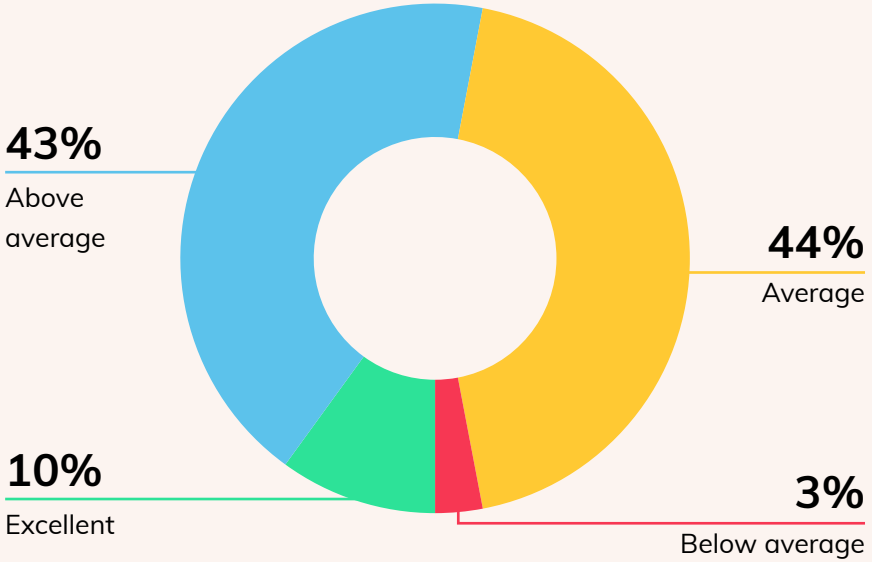
Not at all **0%**

Leaders are more responsive to their threat intelligence feeds and may look to automation for help

Just 3% of respondents felt their organization's ability to take action based on threat intelligence was below average.

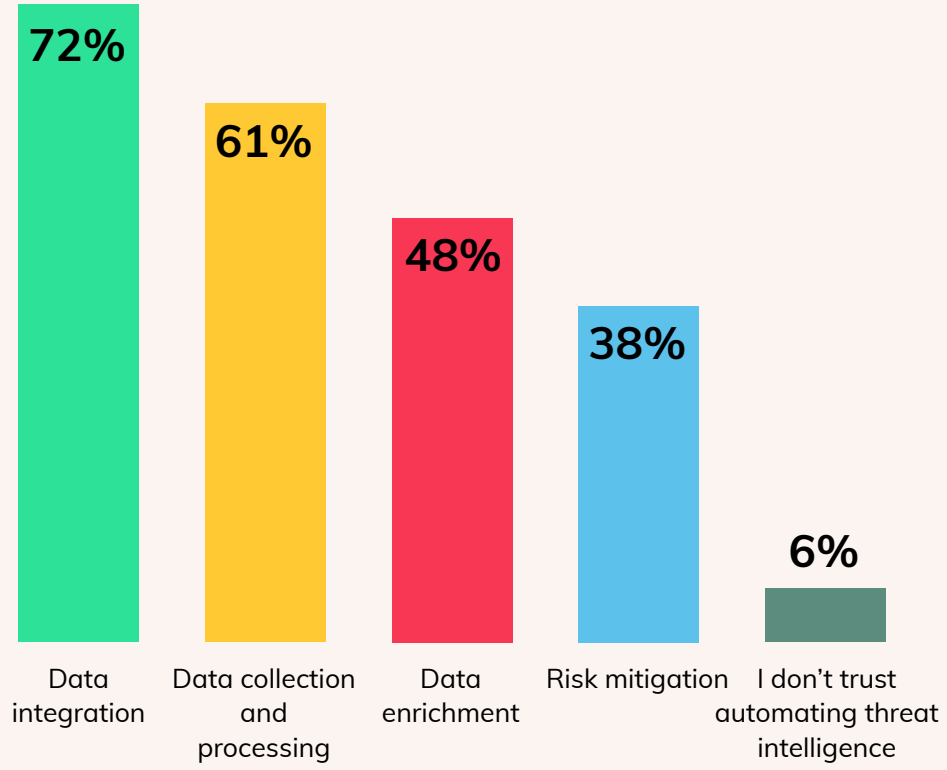
Please rate your organization's ability to take action based on threat intelligence.

Minimal / none **0%**



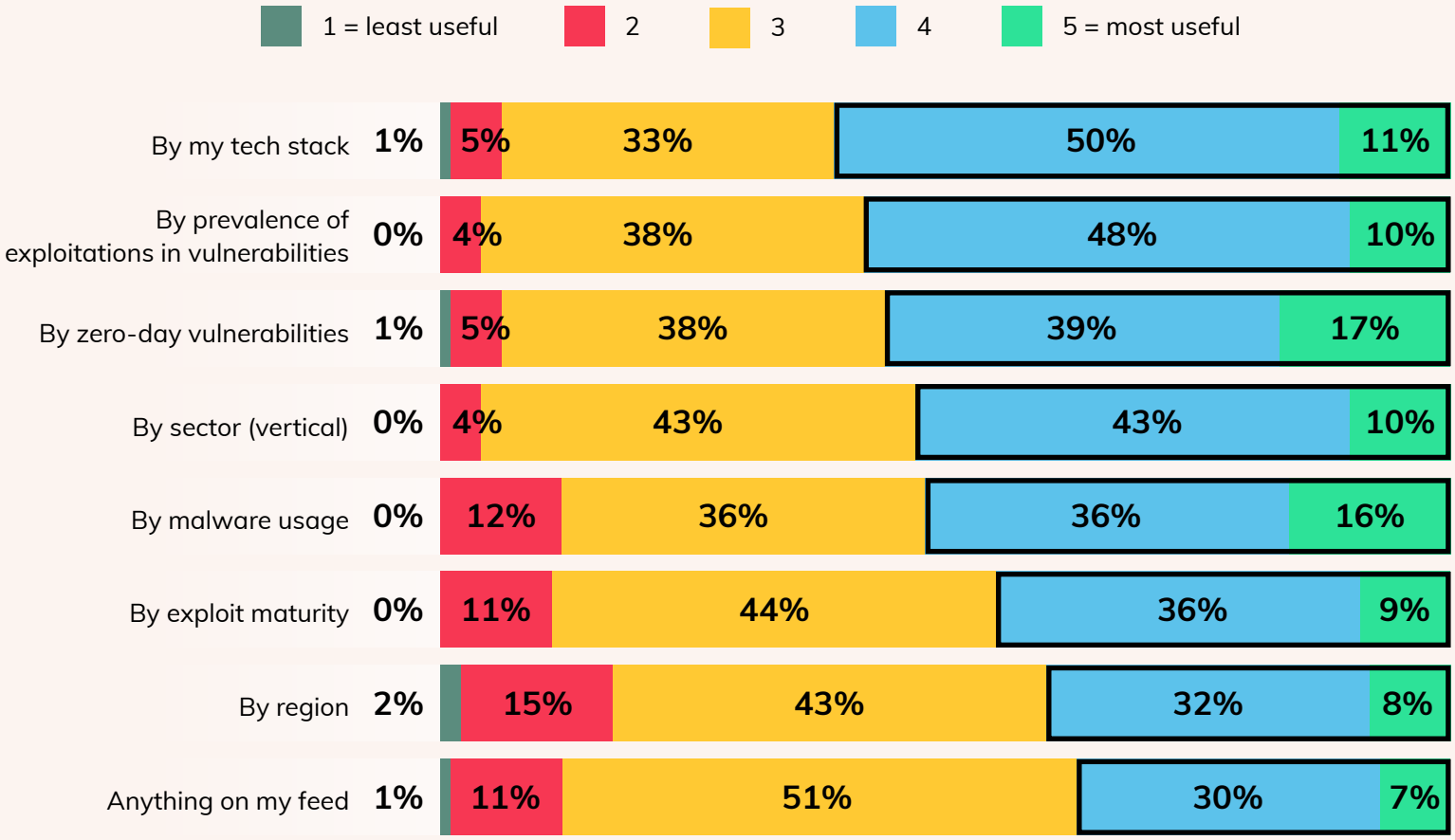
Data integration (72%) and data collection and processing (61%) are the elements of threat intelligence decision makers are most comfortable with automating.

What elements of the threat intelligence lifecycle are you comfortable automating?



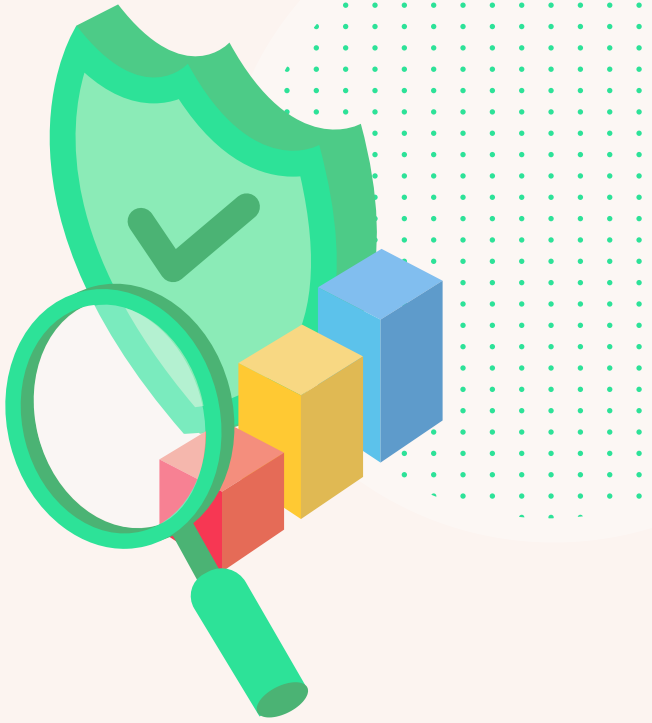
The most useful parameters for filtering threat intelligence are “by tech stack”, “by prevalence of exploitations in vulnerabilities”, and by “zero-day vulnerabilities”.

What parameters are most useful in filtering your threat intelligence data?



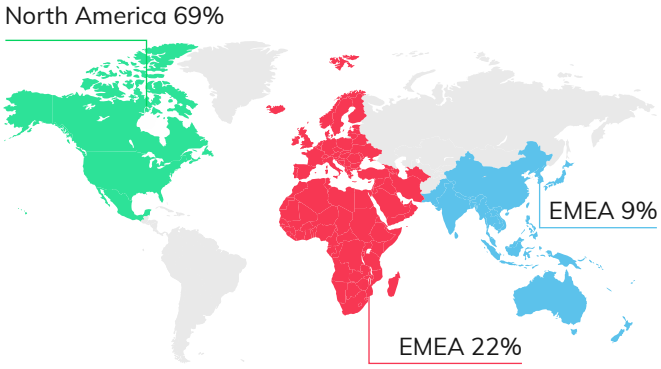
Enriching vulnerability scan results with data derived from various threat intelligence sources is key for contextual and efficient risk-based prioritization.

To see Vulcan Cyber vulnerability enrichment and prioritization capabilities in action, start your 30-day trial of Vulcan Enterprise, or request a demo.

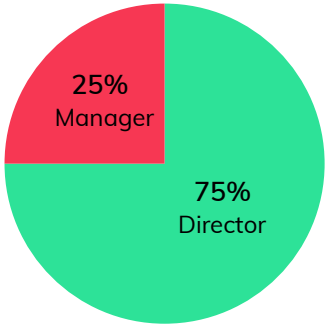


Respondent breakdown

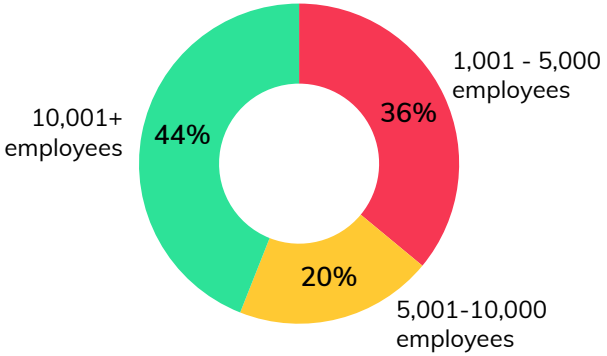
Location



Titles



Company Size



Gartner

Source: Gartner Peer Insights, Reliance on Threat Intelligence survey