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

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

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?

- Yes: 66%
- No: 30%
- Not sure: 4%
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?

- Vulnerability management teams: 64%
- Application security teams: 62%
- SOC / Incident teams: 59%
- Security operations: 55%
- Cloud security teams: 42%
- Executive management: 21%
- IT analysts: 13%
- Other: 0%
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?

- Block bad IPs, URLs, domains, files, etc.: 64%
- Integrate threat intelligence feeds with other security products: 63%
- Analyze root cause to determine incident scope: 54%
- Use threat intelligence to enrich alerts: 49%
- Assess overall organizational threat levels: 40%
- Fine-tune security controls: 38%
- Link alerts together into incidents: 32%
- Support a security roadmap: 23%
- Better prioritization (based on severity and impact): 13%
- Other: 0%
The most used source of threat intelligence was reported as commercial feeds (78%).

What are your current sources of threat intelligence?

- Commercial threat intelligence feeds: 78%
- Community (OTX): 64%
- Social channels: 61%
- Dark web: 14%
- Other: 1%
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?

- **73%** Lack the skills
- **55%** Intelligence is not predictive enough
- **48%** Not enough dedicated personnel
- **36%** Siloed data
- **38%** Lack the tools
- **22%** Justifying investment
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)?

- Yes: 56%
- No: 17%
- Not sure: 27%
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?**

- **Weekly**: 45%
- **Daily**: 26%
- **Monthly**: 24%
- **More frequently than daily**: 4%
- **Yearly**: 1%
- **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?

- 75% Often
- 12% Very often
- 13% Rarely
- 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.

- 43% Above average
- 44% Average
- 10% Excellent
- 3% Below average

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?

- Data integration: 72%
- Data collection and processing: 61%
- Data enrichment: 48%
- Risk mitigation: 38%
- I don’t trust automating threat intelligence: 6%
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?

1 = least useful  2  3  4  5 = most useful

By my tech stack
By prevalence of
exploitations in vulnerabilities
By zero-day vulnerabilities
By sector (vertical)
By malware usage
By exploit maturity
By region
Anything on my feed
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
- North America 69%
- EMEA 22%
- EMEA 9%

Titles
- 75% Director
- 25% Manager

Company Size
- 44% 1,001 - 5,000 employees
- 36% 10,001+ employees
- 20% 5,001-10,000 employees
- 25% 20,001+

This content, which provides opinions and points of view expressed by users, does not represent the views of Gartner; Gartner neither endorses it nor makes any warranties about its accuracy or completeness.

Source: Gartner Peer Insights, Reliance on Threat Intelligence survey

© 2022 Gartner, Inc. and/or its affiliates. All rights reserved.