MANDIANT

NOW PART OF Google Cloud

Global Perspectives on Threat Intelligence

As our 'Global Perspectives on Threat Intelligence' report demonstrates, security teams are concerned that senior leaders don't fully grasp the nature of the threat. This means that critical cyber security decisions are being made without insights into the adversary and their tactics.

Sandra Joyce
VP, Mandiant Intelligence
Google Cloud

This first-of-its-kind report offers insight into how organizations are navigating the global cyber security threat landscape. Findings are drawn from extensive interviews with 1,350 business and IT leaders who make security decisions for organizations with at least 1,000 employees. Respondents were based in 13 countries across three regions and in 18 sectors—including financial services, healthcare and government.

The quality and global reach of the responses provide a snapshot of how cyber security decision-makers at large organizations view and operationalize threat intelligence.

Findings

Responses confirm the initial supposition that although teams value threat intelligence and receive it from multiple sources, they often struggle to apply the information effectively throughout their organizations.

Security teams at the world's largest companies face not only enormous pressures but also challenges in communicating across their organization. And while security teams clearly understand the need for better intelligence on threat actors, many of them make decisions without a full understanding of who is attacking their organization and why. These visibility gaps mean that defenses may not meet their intended goals.

96% of respondents are satisfied with the quality of threat intelligence their organization is using

47% of respondents cited one of their greatest challenges to be effectively applying threat intelligence throughout the security organization

67% of respondents believe their senior leadership team underestimates the cyber threat to their organization

96% of security decision makers believe it is important to understand which cyber threat actors could be targeting their organization

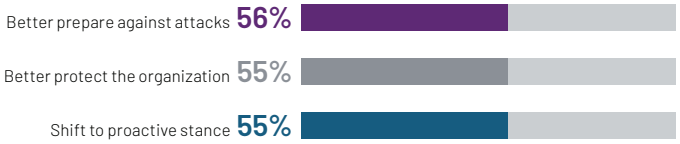
79% of respondents say that at least the majority of the time, they make decisions without adversary insights

Threat Awareness and Security Confidence of Practitioners

The report reveals a global discrepancy between the high level of confidence organizations have in dealing with cyber attacks and the tendency of security teams to make decisions without comprehensive information on the threat actors and their tactics, techniques and procedures (TTPs).

It also shows that a substantial majority (96%) of security decision makers believe it is important to understand which cyber threat actors could be targeting their organization.

As security decision makers, why do you believe it is important to understand which cyber threat actors are targeting your organization?

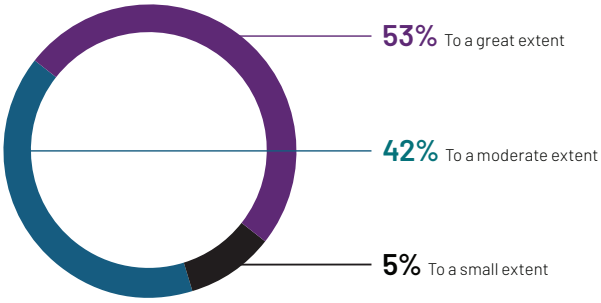


Despite the near-universal understanding of the importance of acquiring information on cyber threat actors—and 96% of respondents citing they are satisfied with the quality of their threat intelligence—79% of respondents said that they make most of their decisions on cyber attacks without insights on who could be targeting their organization. Only 35% say their organization has a comprehensive level of understanding about different threat groups and their TTPs.

Further, 67% of cyber security decision makers believe senior leadership teams still underestimate the cyber threat posed to their organizations, while more than two-thirds (68%) agree their organization needs to improve its understanding of the threat landscape.

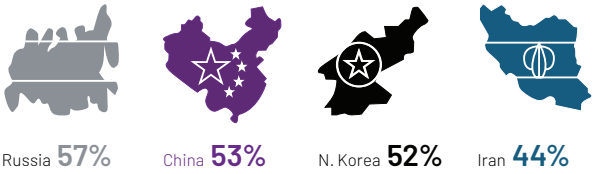
Regardless of these concerns, confidence is high among decision makers that their organization can contain security threats. Nearly all respondents (95%) say they feel they can prove to their senior leadership team that their organization has a moderate to highly effective cyber security program.

To what extent do you feel you can prove to your senior leadership team (such as board of executives or C-suite) that your organization has an effective cyber security program?

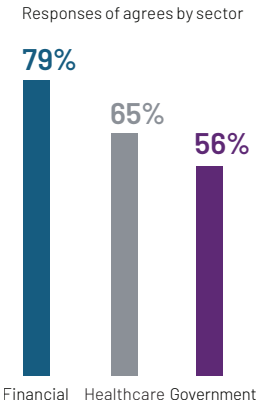


Many security decision makers are confident their organization is fully prepared to defend itself against a significant cyber security attack caused by a financially motivated actor (91%), a hacktivist actor (89%), or a nation-state actor (83%).

In the event of a nation-state attack, which of the following countries do you believe your organization would be unable to fully defend itself against?

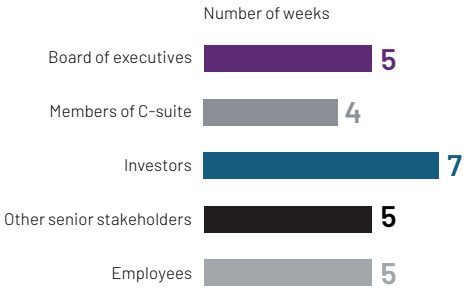


Do you agree or disagree? My organization needs to improve our understanding of the threat landscape.



One likely explanation for the lack of information on threat actors is infrequent communication between security decision makers and their wider organization. Respondents indicated that cyber security is only discussed on average once every 4-5 weeks with groups outside the security team, including the board, C-suite and other senior stakeholders. Discussion are even less frequent with investors, where the average lowers to once every seven weeks.

How often does your department discuss cyber security with the following groups? (average across all regions)

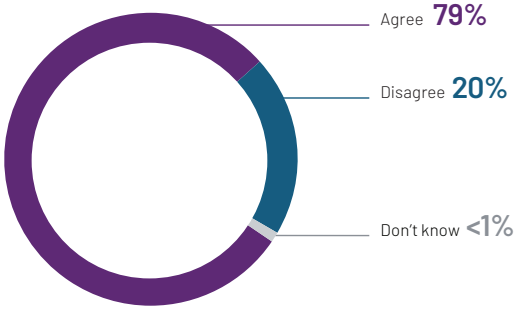


Challenges to Operationalizing Intelligence and Related Risks

The importance of threat intelligence was well understood. A large majority of the respondents deemed it important to identify the attacker (85%); the tools and techniques used by the attacker (88%); and the attacker's motivation (87%). Despite the appreciation for detailed threat intelligence, security teams reveal they do not follow through. Only 34% say they always consider the source of a potential attack when testing cyber security defenses and operations.

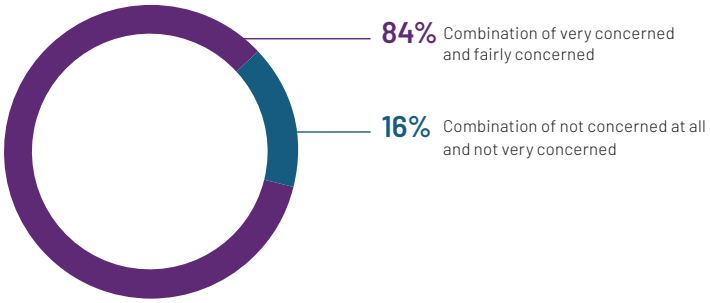
Security teams also do not spend the requisite time on identifying and acting on threats. A substantial majority of respondents (79%) said their organization could focus more time and energy on identifying critical trends within cyber security, while almost all (98%) said they need to be faster at implementing changes to their cyber security strategy based on the latest threat intelligence.

Do you agree or disagree? My organization could focus more time and energy on trends within cyber security that are critical



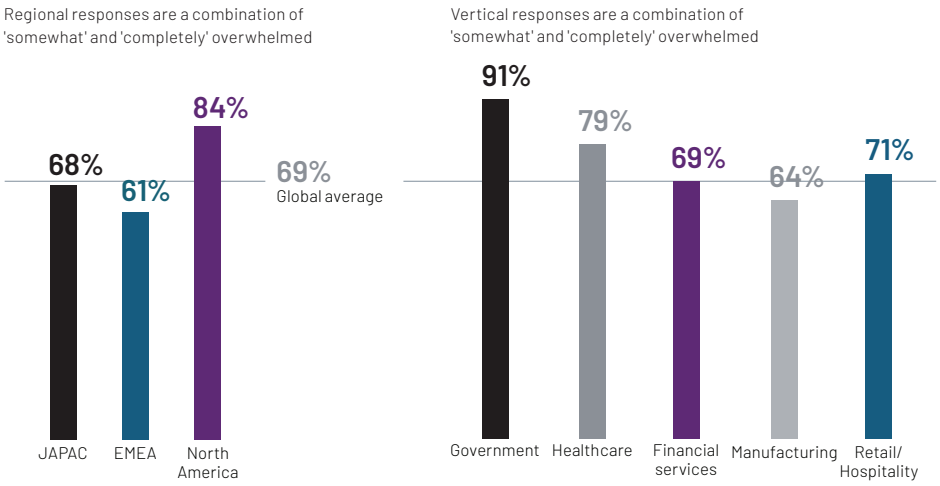
To acquire more actionable threat intelligence, security teams must process a vast amount of data every day. A large majority (84%) of respondents said that they are concerned they may be missing out on threats or incidents because of the number of alerts and data they are faced with. This information overload also impacts the well-being of personnel: more than two-thirds (69%) of security teams admit feeling overwhelmed.

What level of concern do you have that your organization might be missing real threats/ incidents due to the amount of alerts and data you are faced with?



North America respondents were most at risk of burnout, faced with the volume of data and alerts relating to threat intelligence. Among the industry verticals, government respondents were the most likely to feel overwhelmed.

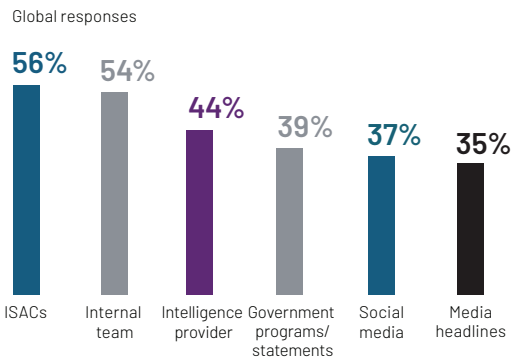
To what extent do you feel your IT security employees feel overwhelmed by the amount of data and/or alerts that have to be dealt with?



While information overload was clearly identified as a challenge for almost every organization, nearly half (47%) of respondents said applying intelligence effectively throughout an organization was one of the biggest challenges they faced when using threat intelligence and 38% said another was knowing what to do with the information. More than half (53%) said the global talent shortage in cyber security threatened their ability to stay ahead of the latest trends, while 42% pointed to the ever-evolving nature of threats.

Although teams struggle to operationalize the threat intelligence they receive, they continue to gather intelligence from a broad range of sources.

What sources does your organization use to keep up to date with the threat landscape?



Information gathered by security teams is frequently kept within those teams or not shared widely across the organization. Sixty-one percent of respondents said they shared threat intelligence with either IT teams to address infrastructure and application vulnerabilities, or with IT security leadership to prioritize security efforts. A much smaller percentage (38%) shared intelligence with other employees for risk awareness.

To operationalize cyber threat intelligence effectively and maximize the value from your investments:

Evaluate the data you rely on to ensure it is trustworthy, timely and actionable

A dependable threat intelligence program must be built on solid foundations; these attributes are an essential starting point.

Understand active threats specific to your organization and industry

Build up a clear picture of the adversaries, their motives, and tactics, techniques and procedures (TTPs) to best adapt your defenses.

Communicate with your stakeholders

Develop a regular cadence of feeding relevant intelligence (tactical, operational or strategic) to the right stakeholder group to drive optimal security and business decisions all the way through to the senior leadership and board level.

Prioritize resources to address what really matters

Leverage intelligence to understand what threats matter most to your organization right now. Assess vulnerabilities and exposures, give them a risk rating based on criticality and then tackle issues in the right order.

Test your defenses

Proactively test the organization's response to typical attack tactics from the adversaries you have identified. Validate your protection against these specific groups and measure improvements in your program over time.

Take action

Leverage the threat intelligence across your security systems and processes to proactively protect against potential threats.

Conclusion

In a rapidly evolving threat landscape, organizations must not only defend themselves against rogue cyber criminals motivated by financial gain, but also nation-states intent on economic disruption, espionage and the targeting of critical infrastructure.

In this context, threat intelligence can be used by decision makers to anticipate threats before they become a problem and deal with them more effectively. Indeed, the vast majority of security decision makers understand the importance of threat intelligence and are able to make better decisions when they have it.

Despite almost unanimous appreciation for the value threat intelligence can bring, security teams do not reliably bring it to bear against threats. At least half of security decisions are made without threat intelligence on potential attackers.

Security teams believe they are missing real threats because their teams are struggling to cope with the data they must process, sometimes lacking sufficiently skilled personnel and not always knowing what to do with the information they have. Until organizations begin to better process intelligence on threat actors, they will remain vulnerable to the always-increasing number of destructive and disruptive cyber attacks.

Survey Methodology: Commissioned by Mandiant, the "Global Perspectives on Threat Intelligence" survey was conducted by Vanson Bourne, a global market research firm, between August and September 2022. Feedback was obtained from 1,350 IT security decision makers across EMEA, North America and JAPAC at organizations with 1000+ employees.

Learn more at www.mandiant.com

Mandiant

11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant

Mandiant is a recognized leader in dynamic cyber defense, threat intelligence and incident response services. By scaling decades of frontline experience, Mandiant helps organizations to be confident in their readiness to defend against and respond to cyber threats. Mandiant is now part of Google Cloud.

MANDIANT
NOW PART OF Google Cloud