The Majority of Business Cyber Security Decisions are Made Without Insight into the Attacker, According to New Mandiant Report

Global survey of cyber security decision makers finds that while nearly all respondents are satisfied with the quality of their threat intelligence, nearly half struggle with effectively applying it

RESTON, Va., Feb. 13, 2023 /PRNewswire/ -- Mandiant Inc. today unveiled the findings of its "Global Perspectives on Threat Intelligence" report, which provides new insight into how organizations navigate the increasingly complex threat landscape. The report is based on a global survey of 1,350 cyber security decision makers across 13 countries and 18 sectors – including financial services, healthcare and government.

Operationalizing intelligence: an identified challenge

Despite the widespread belief that understanding the cyber threat actors who could be targeting their organization is important, 79% of respondents stated that their organizations make the majority of cyber security decisions without insights into the threat actor that is targeting them.

While the report found that nearly all respondents (96%) were satisfied with the quality of threat intelligence their organization is using, respondents declared effectively applying that intelligence throughout the security organization to be one of their greatest challenges (47%). Further, almost all (98%) of those surveyed said they need to be faster at implementing changes to their cyber security strategy based on available threat intelligence.

Underestimating the threat

According to the survey, 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.

However, despite these concerns, security decision makers remain optimistic regarding the effectiveness of their cyber defenses. When asked about confidence in whether their organization is fully prepared to defend itself against different cyber security events, respondents felt most confident in tackling financially motivated threats, such as ransomware (91%), followed by those conducted by a hacktivist actor (89%) and nation-state actor (83%). When asked to rank which countries their organization would be unable to fully defend itself against, more than half of respondents (57%) said Russia, followed by China (53%), North Korea (52%) and Iran (44%).

Further, just over half of respondents (53%) felt they could prove to their senior leadership team that their organization has a highly effective cyber security program.

Other key findings:

- Cyber security is only discussed on average once every four or five weeks with various departments within organizations, including the board, members of the C-suite and other senior stakeholders. This cadence is even less frequent for groups such as investors, where the average lowers to once every seven weeks.
- Only 38% of security teams share threat intelligence with a wider group of employees for risk awareness.
- A majority (79%) of respondents relayed that their organization could focus more time and energy on identifying critical trends.

Resources

Access the full "Global Perspectives on Threat Intelligence" report and analysis here:https://www.mandiant.com/global-perspectives-on-threat-intelligence

Quotes

Sandra Joyce, Vice President, Mandiant Intelligence at Google Cloud comments "A conventional, check-the-box mindset isn't enough to defend against today's well-resourced and dynamic adversaries. Security teams are outwardly confident, but often struggle to keep pace with the rapidly changing threat landscape. They crave actionable information that can be applied throughout their organization."

Joyce continued, "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."

Survey Methodology

Commissioned by Mandiant, the "Global Perspectives on Threat Intelligence" survey was conducted byVanson 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 1,000+ employees.

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.

About Google Cloud

Google Cloud accelerates every organization's ability to digitally transform its business. We deliver enterprise-grade solutions that leverage Google's cutting-edge technology – all on the cleanest cloud in the industry. Customers in more than 200 countries and territories turn to Google Cloud as their trusted partner to enable growth and solve their most critical business problems.

SOURCE Google Cloud

For further information: Mandiant-PR@google.com
