Threat Intelligence Efforts Stymied By Talent Shortages and Budget Constraints

Buyers seek solutions that automate threat intelligence processes to detect, respond to and remediate cyber threats

NEW YORK, NY, UNITED STATES, January 31, 2023 /EINPresswire.com/ -- Early, actionable access to credible intelligence is critical amid today's rapidly changing threat landscape. But according to research from CRA Business Intelligence, the research and content arm of cybersecurity data and insights company CyberRisk Alliance, internal obstacles and competing priorities like limited resources and lack of skilled staff are keeping organizations from effectively addressing threats to their network.

Automation was also a concern among the 200 U.S. security and IT executives, leaders, security administrators, and compliance professionals who responded to CRA BI surveys in June and November 2022. In the most recent survey, underwritten by security companies Ivanti and Mimecast, many expressed an inability to automate threat intelligence processes and trigger security responses related to the detection and remediation of attacks. Others claimed actionable intelligence is hard to find, while others grapple with threat data overload and collating and assembling critical attack data, along with controlling excessive alerts and false positives.

Regardless of the current limitations, the value of threat intelligence can't be understated. "Because threat intelligence feeds deliver threat data in real time, security teams will learn about potential issues as soon as they are discovered," said one survey respondent. "This is key because slower threat responses lead to larger data breaches and significant recovery costs."

Key takeaways from the June 2022 and October 2022 surveys:

- Virtually all respondents from the October survey indicated they use threat intelligence at some level within their organization. The top use cases for threat intelligence include security operations (70%), increasing the effectiveness of vulnerability management processes (64%), incident response (53%), and risk analysis (53%).

• Many respondents from the June survey pointed out that having access to early and credible intelligence is a core requirement for their organization. About 57% said they subscribe to up to 10 threat intelligence feeds while another quarter (26%) gather their intelligence from 11 to 50 feeds. The largest shares of respondents said they use threat data from malware analyses (75%) or indicators of compromise (IOCs) (72%).

• Respondents said they use a variety of information in their organization's threat intelligence program, according to the October survey findings. The most common types are data from IDS, firewall, endpoints, etc. (reported by 67%), network traffic analysis packs and flow (62%), incident response and live forensics (57%), application logs (56%) and email or spreadsheets (55%).

• In the June survey, respondents indicated the importance of having an automated action and response capability as part of their chosen solution now and in the future. Nearly half (46%) said they already incorporate automation in their threat intelligence strategies, and almost as many (41%) said they plan to add that capability, making this the top planned component of their threat intelligence strategies.

• About 66% of respondents from the June survey anticipated spending more on threat intelligence in the coming year. This bodes well for security operations centers hoping to boost defense capabilities through improved threat intelligence, particularly as it relates to patching security flaws in current software and responding more quickly to security events.

The full research report is available for download here.

About CyberRisk Alliance
CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community, and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA's brands include SC Media, Security Weekly, ChannelE2E, MSSP Alert, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, its research unit CRA Business Intelligence, the peer-to-peer CISO membership network, Cybersecurity Collaborative, and now, the Official Cyber Security Summit and TECHEXPO Top Secret. Click here to learn more.

About Ivanti
Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT applications and data over various networks to stay productive and work from anywhere. The Ivanti Neurons automation platform connects the company's indus¬try-leading unified endpoint management, cybersecurity, and enterprise service management solutions, providing a unified IT platform that enables devices to self-heal and self-secure and empowers users to self-service. Over 40,000 customers, including 96 of the Fortune 100, have chosen Ivanti to discover, manage, secure, and service their IT assets from cloud to edge, and deliver excellent end-user experiences for employees, wherever and however they

work. For more information, visit www.ivanti.com and follow @GoIvanti.

About Mimecast
Since 2003, Mimecast has stopped bad things from happening to good organizations by enabling them to work protected. We empower more than 40,000 customers to help mitigate risk and manage complexities across a threat landscape driven by malicious cyberattacks, human error, and technology fallibility. Our advanced solutions provide the proactive threat detection, brand protection, awareness training, and data retention capabilities that evolving workplaces need today. Mimecast solutions are designed to transform email and collaboration security into the eyes and ears of organizations worldwide.

Jenn Jones
CyberRisk Alliance
+1 857-328-0173
email us here
