CRA Study: Threat Intel Leveraged to Secure Systems and Educate Executives

Early actionable access to credible threat intel is critical in making informed decisions and thwarting the theft of confidential data.

NEW YORK, NY, UNITED STATES, August 11, 2022 /EINPresswire.com/ -- Organizations understand the important role threat intelligence solutions play in maintaining a strong cybersecurity posture, particularly with the rise of ransomware. According to findings in a survey from CRA Business Intelligence, the research and content arm of the cybersecurity data and insights company CyberRisk Alliance, they also leverage threat intel to educate executives.

In today's rapidly changing threat landscape, early actionable access to credible threat intel is critical. According to the respondents surveyed, which included 183 security and IT leaders and executives, security administrators, and compliance professionals in the United States, threat intelligence is critical to arm Security Operations Center (SOC) and Incident Response teams with the data needed to make timely, informed decisions that prevent system downtime, thwart the theft of confidential data, and protect intellectual property.

Many also credited threat intelligence for helping to protect their company and customer data — and potentially saving their organization's reputation. There's also no better way to keep leadership informed, maintained some respondents, so that security efforts can be prioritized. "Without threat intelligence you would be chasing ghosts," commented one respondent.

"What's striking about these survey responses is how threat intelligence has become such a powerful tool to communicate threats and needed solutions to executives," said Bill Brenner, VP of Custom and Research Content Strategy in CRA's Business Intelligence Unit. "Respondents see the automation of detection and response as key to uncovering and stopping attacks quickly, but also in painting a picture executives can understand."

Additional key takeaways:

- About two-thirds (64%) said they are very or extremely concerned about cyberthreats in the next 12 months. Their main concerns are ransomware (70%), followed by expanding attack surfaces (55%). Accordingly, for most respondents (62%), a fear of ransomware attacks is the top strategic driver of their threat intelligence strategies, followed by regulatory requirements (49%) and recommendations from industry experts (39%).

- Respondents reported their top use cases for threat intelligence are vulnerability management (68%), security operations (66%), and incident response (62%). Technical (73%) and operational (71%) threat intelligence are more common than the more difficult strategic or more basic tactical use cases. Only 5% said they did not use any threat intelligence.

- Many respondents pointed out that having access to early and credible intelligence is a core requirement for their organization. About six in ten participants 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 (IOC) (72%).

- 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 just as many (41%) said they plan to add that capability, making this the top planned component of their threat intelligence strategies.

Increased spending is also anticipated, as 66% of respondents expect their organizations to invest more on threat intelligence in the coming year. This specific trend 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.

For further insights, the full research report is available for download.

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, SecurityWeekly, ChannelE2E, MSSP Alert, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, its research unit CRA Business Intelligence, and the peer-to-peer CISO membership network, Cybersecurity Collaborative. Click here to learn more.

Jenn Jones
CyberRisk Alliance

+1 857-328-0173
press@cyberriskalliance.com
