CRA Study: Enterprise-Level Weaknesses and System Exposures Prompt More Aggressive Vulnerability Management

Organizations are investing in more aggressive, proactive vulnerability management strategies to stay ahead of security flaws and attacker exploits.

NEW YORK, NY, UNITED STATES, September 6, 2022 /EINPresswire.com/ -- As organizations struggle to assess and patch systems fast enough to stay ahead of threats, they are investing in more aggressive, proactive vulnerability management strategies, according to a survey conducted by CRA Business Intelligence, the research and content arm of the cybersecurity data and insights company CyberRisk Alliance. The survey also reveals that organizations are embracing continuous security assessments and automated remediation processes to stay ahead of newfound flaws and attacker exploits. The report, co-sponsored by Invicti and Intruder, is based upon a survey of 213 security and IT leaders and executives, security administrators, and compliance professionals in the U.S.

Facing a changing threat landscape and constant stream of new vulnerabilities, respondents revealed many challenges in implementing and enhancing their vulnerability management programs. Even the best strategies and technology solutions were found to have specific issues including patch times and high false-positive rates, inefficient prioritization of vulnerabilities, and ineffective responses. The use of multiple vulnerability management vendors and tools instead of a single unified platform seems to be contributing to the underlying issues.

“Security teams have long struggled to stay on top of their vulnerability management efforts, and this survey shows that it remains a significant challenge,” said Bill Brenner, VP of Content Strategy at CyberRisk Alliance. “But the survey reveals some positives as well: Many are scanning more aggressively than they did just two years ago, and most plan to invest more on automated vulnerability management tools in the coming year."

Unfortunately for some organizations, the lack of budget, time, and qualified staff threatens their ability to acquire or implement an effective vulnerability management program.

Key takeaways from the survey:

- Virtually all respondents are concerned about current and future vulnerabilities and threats to their organizations. Nearly half (45%) said they are very or extremely concerned about vulnerabilities in the next 12 months. The time required to patch vulnerabilities is among their top three concerns, according to half of all respondents. A significant share (48%) also cited their concern about the expanding attack surface, while one-third (33%) said they are concerned about the high volume of vulnerabilities.

- For more than half (55%) of those surveyed, the driving force behind the evolution of their vulnerability management strategies is the fear of ransomware. Accordingly, organizations are taking a more aggressive and proactive stance towards vulnerability management compared to several years ago, implementing more robust vulnerability management programs that include increased scanning, expanded coverage of assets, improved patch management, continuous vulnerability monitoring, and automated solutions.

- As part of their vulnerability management programs, 9 out of 10 respondents reported their organization performs internal vulnerability scans; a large majority (70%) also perform external scans. The majority of respondents (52%) said they perform scans daily or multiple times per day, while another 22% said they perform weekly scans. On average, about one-third (32%) estimated their scanners detect up to 10 vulnerabilities per scan, while one in four respondents reported 11 to 50 vulnerabilities per scan. Of the vulnerabilities detected, a significant majority (72%) found one or more to be critical — roughly half (54%) estimated up to an average of 10 critical vulnerabilities and another 18% reported more than 10 critical vulnerabilities.

- Respondents are most likely to be equipped with patch management (75%), asset discovery/management (67%), continuous monitoring (66%), and configuration management (63%) capabilities. Only about one in four (26%) reported they currently have automated remediation — the lowest adoption rate among the list of capabilities. However, nearly half (46%) said they plan to add this to their vulnerability management programs, positioning this capability as potentially the most sought-after enhancement in vulnerability management for the near future.

In addition to these findings, organizations face various operational challenges in achieving fully effective vulnerability programs. In describing their challenges for vulnerability management implementation, respondents mentioned a lack of resources — including budgets and qualified staff — about 30% of the time. Some simply acknowledged that they don't know which tool is right for them or don't have the budgets to purchase them, more than two-thirds (69%) of all respondents said their budget or spending on vulnerability management will increase in the next 12 months.

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, 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.

About Invicti

Invicti Security is transforming the way web applications are secured. An AppSec leader for more than 15 years, Invicti enables organizations in every industry to continuously scan and secure all their web applications and APIs at the speed of innovation. Invicti provides a comprehensive view of an organization's entire web application portfolio, and powerful automation and integrations enable customers to achieve broad coverage of even thousands of applications. Invicti is headquartered in Austin, Texas, and serves more than 3,600 organizations of all sizes all over the world. For more information, visit Invicti's website or follow Invicti on LinkedIn.

About Intruder

Intruder is a cyber security company that helps organizations reduce their attack surface by providing continuous vulnerability scanning and penetration testing services. Intruder's powerful scanner is designed to promptly identify high-impact flaws, changes in the attack surface, and rapidly scan the infrastructure for emerging threats.

Trusted by more than 2,000 companies worldwide, with excellent ratings on G2, Intruder makes vulnerability management effortless for everyone. Visit Intruder's website to learn more and try their Pro service 30 days for free.

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

in today's world. Please see our Editorial Guidelines for more information.