LOGPOINT

May 25, 2022 10:00 CEST

Logpoint poll highlights extent of insecure and unmonitored business-critical systems

- *Forty percent of those surveyed do not include business-critical systems such as SAP in their cybersecurity monitoring*
- *Almost 30 percent of poll respondents do not review SAP logs for cybersecurity events or cyberthreat activity*

COPENHAGEN, Denmark & BOSTON, May 25, 2022 – Logpoint has today announced findings from a recent poll to uncover the security and cost implications enterprises face with their existing IT infrastructure. The poll, issued on Twitter, was targeted at cybersecurity and IT professionals in both the U.S. and UK.

The poll revealed the extent of insecure and unmonitored business-critical systems, with 40 percent noting that they do not include business-critical systems such as SAP in their cybersecurity monitoring. In addition, a further 27 percent were unsure if it was included in their cybersecurity monitoring at all. This is concerning given that SAP serves as the core system behind every aspect of business operations. Not including this in the centralized security monitoring solution leaves organizations vulnerable and exposed to the risk of cyber threats.

“Considering that 77 percent of global transactions touch an SAP system, protecting it against cyber-attacks is vital. *Organizations store their most critical assets within SAP and this data must be protected. SAP systems require extensive protection and security monitoring, and b*usinesses need to ensure they have an integrated security operations platform that monitors all IT infrastructure to ensure they have complete visibility into their SAP system,” said Andrew Lintell, Logpoint VP for EMEA.

Furthermore, when asked how they currently review SAP logs for cybersecurity events or cyberthreat activity, almost 30 percent of respondents admitted to not reviewing SAP logs in any way, and again, nearly 30 percent said they didn’t know if this was being monitored. Failure to do so can create a blind spot for businesses and make it challenging to detect and quickly respond to fraud and threats within SAP.

To add to this, only 23 percent said the process of reviewing SAP logs for cybersecurity events or cyberthreat activity was automated through SIEM, with almost 19 percent still doing so manually.

“Bringing SAP systems under the remit of cybersecurity solutions can massively reduce the security risks and provide logs to aid any audit processes. Accommodating it within the SIEM, for example, can enable these applications to benefit from automation and continuous monitoring, as well as coordinated threat detection and response with log storage and log management, to assist in subsequent investigations,” commented Lintell.

“The problem though is that businesses are trying to fill the gaps in their cybersecurity stacks by devoting more spending to a growing litany of cloud security products, with many toolsets and features going unused or resulting in configuration failure and ultimately, data breaches that could be avoided,” Lintell added.

For those businesses looking to invest in cloud security, a near 40 percent of respondents regarded software licensing in the cloud as too expensive, with 24 percent declaring it led to unknown future costs. Lock-in or lack of control with software licensing was also flagged as an issue by 22 percent, along with a lack of user-based licensing options by 14 percent, as the predominant model of charging is data usage-based. The results indicate there's clearly some appetite for change in the way that cloud-based security services are offered, and businesses stand to benefit from a converged cost-effective form of cyber defense.

Lintell commented - "Businesses must continue to build out their cloud presence and the market is seeing some natural consolidation as complementary technologies such as SIEM and SOAR converge. There are cost-effective options available, and a SaaS all-in-one solution can limit the costs associated with licensing, particularly if it's based on the number of devices sending data rather than on the volume of your data, which is where businesses are seeing costs escalate".

Methodology:
Comprising five question and answer options and drawing 3,371 responses, the Logpoint Twitter poll was conducted during March 15-18, 2022.

About Logpoint
Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats. By combining sophisticated technology and a profound understanding of customer challenges, LogPoint bolsters security teams' capabilities while helping them combat current and future threats. Logpoint offers SIEM, UEBA, SOAR and SAP security technologies converged into a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more. Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company. For more information, visit http://www.logpoint.com

Contacts

Maimouna Corr Fonsbøl
Press Contact
Head of PR
PR & Communications
mcf@logpoint.com
+45 25 66 82 98