Palo Alto Networks Ushers in the Next-Generation Security Operations Center With General Availability of Cortex XSIAM -- the Autonomous Security Operations Platform

October 12, 2022

Early adopters reaping the benefits of improved SOC operations and efficiencies

SANTA CLARA, Calif., Oct. 12, 2022 /PRNewswire/ -- Delivering on the promise to help organizations leverage massive scales of data for their defenses, Palo Alto Networks (NASDAQ: PANW) today announced the general availability of Cortex® XSIAM, a breakthrough autonomous security operations platform powering today's modern secure operations center (SOC) and fundamentally changing the way data, analytics and automation are used across enterprise and cloud security operations.

Earlier this year, Cortex XSIAM was made available to a number of top organizations through the XSIAM Design Partner Program. The design partners spanned healthcare, logistics, design and manufacturing, technology, public sector, and entertainment verticals. The common challenges these organizations face include overwhelming alert volumes accompanied by a high number of false positives, lack of visibility across all parts of the organization, including cloud environments, and excessive manual overhead associated with managing numerous siloed tools.

"The SOC is where some of the best cybersecurity professionals work, and it is time that they have the right platform to get their jobs done effectively. We want to give our customers a new approach to SOC operations with a focus on results, efficiency and productivity," said Lee Klarich, chief product officer, Palo Alto Networks. "Cortex XSIAM establishes an autonomous SOC where organizations can respond to threats in a fraction of the time it takes today, and analysts can focus on the highest priority incidents. The SOC of the future will be built on AI and automation — any other approach is destined for failure."

Palo Alto Networks operates its own SOC on Cortex XSIAM and has seen the benefits of intelligent data integration, machine learning-based threat models, extensive automation and proactive analysis of the IT environment to reduce the attack surface. The Palo Alto Networks SOC processes over one trillion events per month, with Cortex XSIAM automatically handling the vast majority of those events. On average, the Cortex-powered SOC detects threats in 10 seconds and responds to high priority threats in one minute, with an 80% reduction in alerts that SOC analysts need to analyze.

The feedback on XSIAM has been strong. Design partners consistently reported improved visibility, fewer incidents, reduced false positives and reduced mean time to response. Paul Alexander, director of IT operations at Imagination Technologies Group, an international leader in the creation and licensing of semiconductor System-on-Chip Intellectual Property, said, "XSIAM is already helping us to resolve and address threats way more quickly and efficiently, reduce risk and track metrics."

"We see XSIAM as a platform that combines multiple capabilities into one unified ecosystem," said David Norlin, CISO at Lumifi. "For us, that means empowering analysts to move quicker on multiple datasets, detect threats more comprehensively, and deliver an even better service to our clients."

"From our first demo of XSIAM as part of the early access program, we were shocked and impressed with the maturity of the platform," said Randy Watkins, chief technology officer at Critical Start. "This was not a beta product, but a solution that customers would immediately be able to build their entire security operations program around. The data models within XSIAM are some of the best approaches we've seen to solving the lack of consistency with log management."

"XSIAM aims at much more than SIEM and provides the engine for the autonomous SOC," said Bobby Brillhart, vice president of engineering at Norlem. "XSIAM creates unprecedented opportunities for us as an MDR provider to scale our services and significantly decrease our MTTR."

Optimized for Cloud-Native Environments

By design, XSIAM operates across both cloud and enterprise security operations, providing true end-to-end management of threats, wherever they originate. Unlike most existing SIEM products, XSIAM comes with the ability to collect and integrate cloud telemetry that is unique to cloud-native systems. While companies born in the cloud benefit from the scale and automation of XSIAM and the ease of integration with public cloud and SaaS telemetry, organizations with legacy SIEM deployments can seamlessly transition to XSIAM as the next-generation autonomous SOC platform.

Availability

Cortex XSIAM is now available globally with full support across multiple cloud locations to comply with local regulations.

Additional Resources

- Register for Palo Alto Networks' November event: The Modern SOC, Reimagined.
- Join us at Ignite, Palo Alto Networks customer conference, to learn more and see XSIAM in action.
- Follow Palo Alto Networks on Twitter, LinkedIn, Facebook and Instagram.

About Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. We innovate to outpace cyberthreats, so organizations can embrace technology with confidence. We provide next-gen cybersecurity to thousands of customers globally, across all sectors. Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the Zero Trust Enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice.

At Palo Alto Networks, we're committed to bringing together the very best people in service of our mission, so we're also proud to be the cybersecurity workplace of choice, recognized among Newsweek's Most Loved Workplaces (2021), Comparably Best Companies for Diversity (2021)and HRC Best Places for LGBTQ Equality (2022). For more information, visit www.paloaltonetworks.com.

View original content to download multimedia:https://www.prnewswire.com/news-releases/palo-alto-networks-ushers-in-the-next-generation-security-operations-center-with-general-availability-of-cortex-xsiam--the-autonomous-security-operations-platform-301647198.html

SOURCE Palo Alto Networks, Inc.

Matthew Manturi, mmanturi@paloaltonetworks.com, 908-268-0512