Palo Alto Networks Unveils Enhanced Flexibility and Customization with Cortex XSIAM, the Precision AI Powered SOC Platform

May 7, 2024

News Summary:

- Cortex XSIAM shifts paradigm so that third-party EDR data is as easily ingestible as first-party data
- Cortex XSIAM's BYOML framework empowers custom ML models for tailored security solutions
- Cortex XSIAM expands cloud detection and response capabilities for complete visibility and protection

SANTA CLARA, Calif., May 7, 2024 /PRNewswire/ -- Cortex XSIAM® from Palo Alto Networks (NASDAQ: PANW) is the AI-driven security operations platform that enables organizations to transform their security operations with a unified platform that delivers all critical capabilities in one powerful solution. Today, the global cybersecurity leader announced the ability for customers to integrate their own custom machine learning models, seamlessly integrating third-party EDR data and also leveraging cloud detection and response capabilities. Cortex XSIAM now offers Palo Alto Networks customers the flexibility and customization to create a security solution that aligns perfectly with their organization's goals.

PREPARE FOR A BRAND-NEW FIGHT
with Precision AI™ by Palo Alto Networks
paloalto NETWORKS
CYBERSECURITY PARTNER OF CHOICE

"Data silos and manual repetition can't handle the speed of today's threats — a new approach is needed. Our customers are seeing transformative security outcomes; with Cortex XSIAM, large multinational companies have gone from a mean time to remediation (MTTR) of days down to minutes," said **Lee Klarich, chief product officer at Palo Alto Networks**. "From expanding our AI capabilities with BYOML, to opening data sources to treat third-party data as first party, and expanding to cloud, we continue to drive innovation with Cortex XSIAM to enable the SOC with the platform it needs to secure the entire enterprise."

Cortex XSIAM allows organizations to simplify security operations with an integrated platform: The integration of SOC capabilities, such as SIEM, XDR, SOAR and ASM, into a single platform is a game changer for security operations. With Cortex XSIAM, organizations get dramatically better security and turbocharged SOC performance.

XSIAM empowers organizations to take control of their security by offering a host of innovative features, including:

Cortex XSIAM for Third-Party EDR Telemetry allows qualifying organizations to adopt Cortex XSIAM without immediately replacing their existing EDR. This enables the ingestion of third-party EDR data into XSIAM, with the cost of ingestion credited for up to two years or until the EDR contract expires, when customers are able to migrate away from legacy EDR solutions and fully leverage the integrated XDR capability of Cortex XSIAM to realize optimal security outcomes.

Cortex XSIAM offers a Bring Your Own Machine Learning (BYOML) framework. Cortex XSIAM ingests vast amounts of security data across hundreds of supported sources to enable better out-of-the-box AI/ML analytics. For the first time, SOCs can take advantage of this data lake to create and customize ML models using a bring your own ML capability. Not every security use case is created equal, that's why enabling organizations to integrate custom ML models for those unique scenarios, incident management and data visualization requirements is key to their success.

Cortex XSIAM introduces Cloud Detection and Response (CDR) capabilities, providing visibility into cloud assets, incidents, coverage and vulnerabilities as well as integrations with Prisma® Cloud for enhanced incident grouping and navigation. With the unified user interface provided by XSIAM, security analysts can efficiently and effectively respond to cloud-based threats, enhancing situational awareness and bolstering their overall security posture.

At the heart of CDR are three major innovations that will be available to Cortex XSIAM customers:

- **Cloud Command Center**: Within the same unified UI that SOC analysts use for enterprise security in Cortex XSIAM, customers can now have full visibility into cloud assets, incidents, coverage, and vulnerabilities, enabling situational awareness and efficient and complete response to cloud threats.
- **Security Agent** across Cortex and Prisma Cloud platforms: The new agent combines Prisma Cloud's comprehensive vulnerability and compliance management capabilities with Cortex's best-in-class runtime security and threat protection. On top of improving security outcomes, the new agent drastically simplifies deployment and operations across the entire

security program.

- **Integration with Prisma Cloud**: Prisma Cloud further enriches the capabilities delivered through the Cloud Command Center with granular alerts and asset information, giving broader context, detailed incident grouping, and easier navigation to assets.

Moreover, XSIAM boasts over 1,000 integrations covering commonly used SOC tools for automated alert ingestion and orchestration of workflows, enabling SOCs to optimize processes and interactions across their entire security program.

"Our research indicates that despite continuing focus on consolidation efforts, 86% of security stacks still rely on ten or more tools, prompting 98% to continue efforts to further consolidate and integrate their security operations tools," said **Dave Gruber, principal cybersecurity analyst at Enterprise Strategy Group**. "Emerging security platforms like Cortex XSIAM are helping organizations achieve consolidation objectives, as they add the ability to ingest third-party EDR telemetry and even absorb migration costs from legacy EDR solutions."

Register to attend: *From 2:30-4 p.m. PDT today, May 7, 2024, join Palo Alto Networks Chairman and CEO Nikesh Arora for a virtual event:* ***Prepare for a Brand-New Fight****, and dive into these cutting-edge technologies and advancements in AI and cybersecurity.*

Cyber Defense Magazine this week recognized Palo Alto Networks, awarding 11 of its coveted Global InfoSec Awards for 2024 to the company. This included naming Cortex XSIAM as Hot Company in Cybersecurity AI and Cortex XDR® as Editor's Choice in Extended Detection and Response. Winners were named Monday, May 6, 2024, during the RSA Conference.

To learn more about Cortex XSIAM and its complete security solution, please visit www.paloaltonetworks.com/cortex/cortex-xsiam.

To learn more about Precision AI™ by Palo Alto Networks, please visit https://www.paloaltonetworks.com/precision-ai-security.

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 (2023, 2022, 2021), with a score of 100 on the Disability Equality Index (2023, 2022), and HRC Best Places for LGBTQ+ Equality (2022). For more information, visit www.paloaltonetworks.com.

Palo Alto Networks, Cortex, Cortex XSIAM, Cortex XDR, Prisma, Precision AI, and the Palo Alto Networks logo are trademarks of Palo Alto Networks, Inc. in the United States and in jurisdictions throughout the world. All other trademarks, trade names, or service marks used or mentioned herein belong to their respective owners.

This press release contains forward-looking statements that involve risks, uncertainties and assumptions, including, without limitation, statements regarding the benefits, impact, or performance or potential benefits, impact or performance of our products and technologies. These forward-looking statements are not guarantees of future performance, and there are a significant number of factors that could cause actual results to differ materially from statements made in this press release. We identify certain important risks and uncertainties that could affect our results and performance in our most recent Annual Report on Form 10-K, our most recent Quarterly Report on Form 10-Q, and our other filings with the U.S. Securities and Exchange Commission from time-to-time, each of which are available on our website at investors.paloaltonetworks.com and on the SEC's website at www.sec.gov. All forward-looking statements in this [press release are based on information available to us as of the date hereof, and we do not assume any obligation to update the forward-looking statements provided to reflect events that occur or circumstances that exist after the date on which they were made.

View original content to download multimedia:https://www.prnewswire.com/news-releases/palo-alto-networks-unveils-enhanced-flexibility-and-customization-with-cortex-xsiam-the-precision-ai-powered-soc-platform-302137928.html

SOURCE Palo Alto Networks, Inc.

press@paloaltonetworks.com