Palo Alto Networks Adds "Bring Your Own AI" Capability To Cortex XSIAM AI-driven Security Operations Platform

November 13, 2023

Cortex XSIAM now enables customers to add their own custom AI models on the XSIAM data lake in addition to the already existing 1,300+ models

SANTA CLARA, Calif., Nov. 13, 2023 /PRNewswire/ -- It used to take an attacker 44 days on average to exfiltrate data from an organization once it was compromised — now it's a matter of hours — and with companies taking an average of 5.5 days to initially contain an incident, legacy security operations solutions no longer work. Since its debut, Cortex XSIAM® has helped customers revolutionize their security operations center (SOC). One services company improved its median time to resolution from days to minutes — 270 times faster than before. Further improving the award-winning AI-driven security operations platform, Palo Alto Networks (NASDAQ: PANW) today unveiled Cortex XSIAM 2.0, which includes a new bring-your-own machine learning (BYOML) framework.

Palo Alto Networks collects more security data than any other cybersecurity company, with more than 5 petabytes of security data ingested daily, and with more than 1 exabyte stored in total. XSIAM offers robust, out-of-the-box AI models built for superior security analytics and protection against threats. In addition, many mature SOCs want the ability to customize and create their own ML models. The BYOML framework makes the vast security data stored in XSIAM available for the first time. This allows security teams to create and integrate their own ML models into XSIAM to enable unique use cases like fraud detection, security research and sophisticated data visualization.

In addition to the BYOML framework, XSIAM 2.0 includes new features that enable organizations to address today's security operations challenges through increased visibility and threat prioritization. The new XSIAM Command Center creates a seismic shift in how security teams monitor their security operations with a comprehensive view of data sources and alerts, enabling the effortless identification and prioritization of security incidents within a single unified platform. Additionally, with the new MITRE ATT&CK Coverage Dashboard, organizations can swiftly gauge their overall defense against a broad set of threat actor tactics and techniques, channeling their efforts toward strengthening their overall security posture.

Gonen Fink, senior vice president, Cortex products, Palo Alto Networks, said:
"Effective security operations are a major challenge for companies all worldwide. The speed at which attackers are moving, coupled with new regulatory requirements like the SEC Mandate requiring public companies to disclose material cybersecurity incidents within four days of discovery, make it impossible to handle cyberthreats with traditional manual approaches. Using artificial intelligence and automation, XSIAM 2.0 closes this gap by addressing operational complexity, stopping threats at scale, and speeding up incident remediation."

Further building on its recent success and recognition, Palo Alto Networks Cortex XSIAM was identified as a Leader and Outperformer in GigaOm's 2023 Radar Report on Autonomous SOC.*

Andrew Green, research analyst, GigaOm, said:
"As a solution built from the ground up with lessons learned from a suite of leading security products, XSIAM delivers a comprehensive autonomous SOC solution that scores high on a wide range of key criteria."

The outcomes achieved by XSIAM 2.0 cannot be met with multiple point products and siloed data. XSIAM converges SOC capabilities, including XDR, SOAR, SIEM and more, into a single platform to streamline security operations. It also continuously collects, stitches and normalizes raw data, all through a unified approach. Unified data, coupled with an AI-driven platform approach, is why customers have seen the following results:

- Oil and gas company: 75% reduction in incidents requiring investigation. This is from ~1,000 a day to ~250 a day, eliminating false positives and duplicates.
- Boyne Resorts: Added 20 more data sources into one platform, streamlining and improving investigations.
- Imagination Technologies: 10x improvement in incident closure rate, going from <10% to 100%.

Paul Alexander, director of IT operations at Imagination Technologies Group, said:
"One of our biggest pain points is information overload. Business growth is great, but it means we have more business operations to manage, and meanwhile, the threat actors are getting more sophisticated. XSIAM is helping because it effectively lets us cut straight to the real and serious incidents that we need to focus on and we're not wasting time on data that doesn't need our attention."

Mike Dembek, network architect at Boyne Resorts, said:
"Log collection was a huge weak point for us. Our SIEM was expensive, and it was difficult to integrate sources. We were hunting down alerts that weren't accurate; it was a hodgepodge of stuff that wasn't correlated together. With XSIAM, we have more visibility and faster investigations. Seamless data onboarding and automation setup are game changers."

Availability
XSIAM 2.0 is generally available to customers globally today.

*GigaOm Radar for Autonomous Security Operations Center (SOC), Green, Andrew; Nov 1, 2023

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, and the Palo Alto Networks logo are registered 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. Any unreleased services or features (and any services or features not generally available to customers) referenced in this or other press releases or public statements are not currently available (or are not yet generally available to customers) and may not be delivered when expected or at all. Customers who purchase Palo Alto Networks applications should make their purchase decisions based on services and features currently generally available.

View original content to download multimedia:https://www.prnewswire.com/news-releases/palo-alto-networks-adds-bring-your-own-ai-capability-to-cortex-xsiam-ai-driven-security-operations-platform-301985645.html

SOURCE Palo Alto Networks, Inc.

Matt Manturi, Palo Alto Networks PR, mmanturi@paloaltonetworks.com