Palo Alto Networks Takes On Identity Attacks, Extends its Cortex XSIAM Platform with AI-driven Identity Threat Detection and Response

March 6, 2023

XSIAM enables security teams to further consolidate disparate SOC products

SANTA CLARA, Calif., March 6, 2023 /PRNewswire/ -- Palo Alto Networks (NASDAQ: PANW), the global cybersecurity leader, announced today the availability of its new Identity Threat Detection and Response (ITDR) module for Cortex® XSIAM ™. ITDR enables customers to ingest user identity and behavior data and deploy state of the art AI technology to detect identity-driven attacks within seconds. The module further strengthens XSIAM's ability to consolidate multiple security operations capabilities into a unified, AI-driven security operations center (SOC) platform.

Identity-driven attacks, which target user credentials to access confidential data and systems, are one of the most common methods cyber criminals use to breach organizations' networks. For example, in recent years Lapsus$ Group has used privileged user credentials to attack multiple government agencies, as well as multiple large technology companies.

"Today, customers who want to detect identity-related attacks must deploy multiple tools – UEBA, Insider Risk Management, endpoint-based ITDR, etc. – each providing a partial view into user activities," said Gonen Fink, senior vice president, Cortex Products at Palo Alto Networks. "Such disjointed approaches result in poor security outcomes, alert overload, and time wasted on triage. With the addition of ITDR, the XSIAM platform now integrates all identity data sources into a single security data foundation spanning endpoints, networks and cloud. This allows our customers to run comprehensive AI-driven threat detection to protect against stealthy identity-driven attacks."

The ITDR module ingests and integrates user behavior data, such as what times an employee typically works, and which applications and data they usually access. It processes data from a variety of sources, including authentication services, endpoint logs, cloud identity data, email and HR data, as well as network, OS, and custom sources. The built-in AI models can then be trained to flag suspicious activity based on irregular user behavior, getting ahead of prominent insider risks such as configuration manipulation, file manipulation, modification of permissions.

In addition to yielding stronger security outcomes, the addition of ITDR to Cortex XSIAM further reduces complexity in the SOC by tightly integrating identity analytics into a unified SOC platform. Cortex XSIAM already natively integrates security information and event management (SIEM), endpoint detection and response (EDR), network detection and response (NDR), security, orchestration and response (SOAR), Threat Intelligence Management (TIM) and Attack Surface management (ASM) capabilities, replacing the need for multiple point solutions.

"The ability to process large amounts of data and handle potential threats in real-time has become a major problem as the cybersecurity landscape has evolved," said Michael Kearns, CISO of Nebraska Methodist Health System. "The integration of AI and automation has become an absolute must for organizations to keep up with growing threats to ensure they can proactively and effectively mitigate cyber risks. Palo Alto Networks is the gold standard for innovation, which is why their AI and automation capabilities from Cortex are the powering force behind our security operations."

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 and 2022), 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-takes-on-identity-attacks-extends-its-cortex-xsiam-platform-with-ai-driven-identity-threat-detection-and-response-301762982.html

SOURCE Palo Alto Networks, Inc.

Media Contact: mmanturi@paloaltonetworks.com