Palo Alto Networks Delivers the Industry's First Cloud-Optimized SOC Platform

April 11, 2024

As businesses invest in the cloud, new Cortex XSIAM features enable SecOps teams to identify and remediate cloud threats in real-time

SANTA CLARA, Calif., April 11, 2024 /PRNewswire/ -- Palo Alto Networks (NASDAQ: PANW), the global cybersecurity leader, today announced a new milestone in how security operations centers (SOC) secure the cloud. The new innovations as part of Cortex XSIAM® for Cloud bolster the Palo Alto Networks [Cortex XSIAM](#) platform to natively deliver Cloud Detection and Response capabilities in one unified solution, making Cortex XSIAM the industry's first SOC platform optimized for the cloud.

Many organizations now run a large portion of their business in the cloud, yet traditional SOC security tools weren't designed for the cloud. Palo Alto Networks new Cortex XSIAM for Cloud innovations delivers cloud security operations capabilities through one platform for faster, better security outcomes. It incorporates the unique architecture of cloud-based applications, understands the distinct characteristics of cloud-related threats, and provides the necessary real-time monitoring and response capabilities for SOC analysts.

Gonen Fink, SVP of Products for Cortex and Prisma Cloud, said:
"The evolution of our Cortex XSIAM platform to integrate Cloud Detection and Response capabilities underscores the reason we created Cortex XSIAM – to provide a comprehensive security operations platform powered by AI and automation. This approach eliminates data silos, increases efficiency, and nets optimal experiences for SecOps teams. Cortex XSIAM for Cloud represents our commitment to providing a unified security solution in one platform, leading to greater speed and better security."

As part of the new Cloud Detection and Response capabilities, Cortex XSIAM provides customers:

- **Comprehensive UI and workflows:** Within the same unified platform for enterprise security in Cortex XSIAM, SOC analysts can now utilize a new Cloud Command Center for complete visibility into cloud assets. This visibility enables security teams to identify and respond to cloud threats quickly.
- **An expanded security agent:** An expanded version of the Cortex XDR® Agent augments Cortex's best-in-class runtime security and threat protection with Prisma® Cloud's powerful vulnerability and security compliance management capabilities to deliver a complete Cloud Detection and Response solution. These new capabilities not only eliminate the necessity for two agents but also significantly enhance visibility while streamlining deployment and operations across the entirety of a security program.
- **Native integration with Prisma Cloud:** The new Prisma Cloud integration further enriches the capabilities delivered through the cloud SOC with broader context and security posture information about cloud assets for detailed incident grouping and more straightforward navigation.

Dave Gruber, Principal Cybersecurity Analyst at Enterprise Strategy Group, said:
"Our research shows that 89% of SOC teams either play a major role or have complete ownership of cloud security operations. Yet current SOC tools often fall short in providing the level of visibility and context needed to support cloud investigations. The addition of native, cloud SecOps capabilities within Cortex XSIAM narrows this gap, enabling cloud and security teams to work more collaboratively to see, understand, and mitigate attacks involving cloud resources."

To learn more about these and other innovations from Cortex®, register to attend [Symphony 2024 on April 17](#).

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, 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.

C View original content to download multimedia:https://www.prnewswire.com/news-releases/palo-alto-networks-delivers-the-industrys-first-cloud-optimized-soc-platform-302114495.html

SOURCE Palo Alto Networks, Inc.

Matt Manturi, mmanturi@paloaltonetworks.com