Palo Alto Networks Introduces Cortex XSOAR, Redefines Security Orchestration and Automation with Integrated Threat Intel Management

February 24, 2020
Cortex XSOAR simplifies security operations by unifying threat intelligence management with playbook-driven automation

SANTA CLARA, Calif., Feb. 24, 2020 /PRNewswire/ -- Palo Alto Networks (NYSE: PANW), the global cybersecurity leader, today introduced Cortex™ XSOAR, an extended security orchestration, automation and response platform that empowers security leaders with instant capabilities against threats across their entire enterprise. Cortex XSOAR is an evolution of the Demisto® platform, which was acquired by Palo Alto Networks in March 2019.

Palo Alto Networks is redefining the security orchestration, automation and response category by making threat intelligence management a core component. By tightly integrating threat intelligence management with SOAR capabilities — such as unified case management, automation and real-time collaboration — customers are now able to fully operationalize threat feeds.

"Customers are facing an overwhelming volume of alerts, threat intel sources, and security tasks," says Lee Klarich, chief product officer for Palo Alto Networks. "Both SOAR and threat intelligence management have developed over recent years as tools to help them, but existing product silos have led to even more manual work. Bringing threat intel data into Cortex XSOAR means security orchestration just got simpler for the customer. It makes no sense to have SOAR without native threat intel."

"The integration of threat management into security orchestration and automation is an inevitable evolution for improving security operations," notes Jon Oltsik, senior principal analyst and fellow at the Enterprise Strategy Group (ESG). "Cortex XSOAR brings the right pieces together. Until now, operationalizing vital threat intelligence data has been difficult or even impossible as it requires time, experience, and resources that are beyond the capabilities of many organizations. A platform like Cortex XSOAR acts as a security operations and analytics platform architecture, or SOAPA, for analyzing and operationalizing cyber threat intelligence. The benefit? Bringing the value of threat intel to the masses."

With Cortex XSOAR, customers are able to:

- **Standardize and automate processes for any security use case:** Easily automate hundreds of security use cases with playbooks that orchestrate response actions across more than 350 third-party products.
- **Adapt to any alert with security-focused case management:** Accelerate incident response by unifying alerts, incidents and indicators from any source within a single case management framework.
- **Boost SecOps efficiency with real-time collaboration:** Facilitate investigations across teams via a virtual War Room with built-in ChatOps and command line interface to execute commands across the entire product stack in real time.
- **Take action on threat intelligence with confidence and speed:** Take full control of threat data by aggregating disparate sources, customizing and scoring feeds, and matching indicators against a customer's specific environment, as well as leveraging playbook automation to drive instant action.

"Threat intelligence without context is just threat data. In order for threat intelligence to be of use, the original context of the threat intel has to be applied appropriately and mapped to internal incidents and policies," says Michael Poddo, director, Cyber Threat Analysis & Response, Emerson. "However, doing this at scale and speed to keep pace with real-time threat feeds is tough without automation. SOAR applied to threat intelligence can help fully integrate it into all aspects of your incident response program."

Cortex XSOAR will replace Demisto by Palo Alto Networks, subsuming and extending existing platform capabilities. Demisto customers will be migrated to Cortex XSOAR upon general availability, expected in March 2020, with an option to evaluate the new Threat Intel Management module at no additional cost.

For more information:

- Join the Palo Alto Networks Cortex XSOAR webcast on April 7.
- Visit the blog for additional details on Cortex XSOAR and the Cortex XSOAR ecosystem.

About Palo Alto Networks
Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

Palo Alto Networks, Cortex, Demisto, 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.

View original content to download multimedia:http://www.prnewswire.com/news-releases/palo-alto-networks-introduces-cortex-xsoar-redefines-security-orchestration-and-automation-with-integrated-threat-intel-

management-301009629.html

SOURCE Palo Alto Networks, Inc.