Palo Alto host networking event at Gazipur, promising cyber resiliency - In

Data: 2025-09-27 06:04:16

Autor: Inteligência Against Invaders

Palo Alto Networks, a leading cybersecurity company, recently hosted a significant networking event titled ” Raise the bar on Security with Prisma SASE” with over 100 IT and security experts. This exclusive gathering focused on sharing insights about the changing threat landscape and highlighted Palo Alto’s newest developments in cloud security and secure access solutions.

Chinmoy Maiti, a senior solutions consultant at Palo Alto, stated that the company is committed to enhancing hybrid work environments. At the event, attendees learned about new features in Prisma SASE (Secure Access Service Edge) that improve integration with identity-based access controls and visibility across networks. The session showcased how organizations use SASE for zero trust enforcement and secure user access.

Prisma Browser is a managed enterprise browser that requires no infrastructure changes or admin rights and provides unified visibility and policy across devices and Prisma Access. It supports all major platforms and is set to be the main secure productivity hub by 2030 for both managed and unmanaged endpoints. Currently, 85-100% of employee work occurs in the browser, yet 95% of organizations face browser-based security incidents, with 345 vulnerabilities reported in 2023. Over 60% of critical network data in browsers is not decrypted, reducing control over SaaS, web, and AI apps. Nearly 90% of organizations permit personal devices for corporate use, resulting in 85% of ransomware breaches from unmanaged endpoints.

Rafiqul Islam Badal, solution consultant give a strong emphasis placing on the urgent need to modernize Security Operations Centers (SOCs), highlighting that traditional endpoint security tools are no longer sufficient to counter today’s rapidly evolving threats. The company cited alarming statistics, including an average breach remediation time of six days, while threat actors are projected to exfiltrate data in as little as five days by 2025—contributing to an average breach cost of $4.88 million. This growing gap is attributed to the complexity of security operations, where fragmented tools like EDR, SIEM, and SOAR overwhelm analysts with thousands of alerts, resulting in fatigue and missed threats. To address these challenges, Palo Alto spotlighted its Cortex suite, particularly Cortex XDR and Cortex XSIAM. Cortex XDR was presented as an industry-leading, AI-powered detection platform offering unified protection across identity, network, endpoint, and cloud environments.

For organizations seeking full SOC transformation, the company positioned Cortex XSIAM as a next-gen solution designed to unify data, analytics, and automation in one platform, streamlining operations and accelerating threat response. Kalpajit Pal, Director of Sales, emphasized the need for security teams to move from manual methods to a proactive, AI-driven defense due to the rising threats from quantum computing that could undermine traditional cryptography. Central to this change is Palo Alto’s Zero Trust Platform, featuring the Strata Network Security and Cortex XSIAM

AI-Driven SecOps Platforms, designed for real-time threat prevention and automated security operations.

Kalpajit introduced the 5th Generation Next-Generation Firewalls (NGFWs) with Quantum Optimized Hardware offer up to 4X performance for Post-Quantum Cryptography (PQC) TLS decryption, which is vital as encryption standards change. He said, Cortex XSIAM helps simplify modern SecOps by combining data, analytics, and automation across the security stack. Actual deployments show it can cut the mean time to remediate (MTTR) from days to just one hour. The platform's future integration with CyberArk will enhance cybersecurity, providing better identity protection and stricter control over critical infrastructure.

In Q&A session, Kamrul hasan Babu committed to support the customer on call and promised better services making local talents. Industry Engagement: Participants took part in live demos, presentations, Q&A, and breakout sessions, allowing direct interaction with Palo Alto's product and engineering teams.

The ***event*** highlighted the increasing demand for integrated, AI-driven security platforms to address modern threats and protect cloud-native environments.

Palo Alto Networks is strengthening its position in the security arena by innovating promoting collaboration, and knowledge-sharing sessions continuously. This not only enhances their commitment to the customer but also supports the security community in staying proactive against threats.

Check Point Hosts "Securing the Hyperconnected World in the AI Era" in Dhaka