Radware AI SOC Xpert

A game changer for DDoS and application protection SOC operations

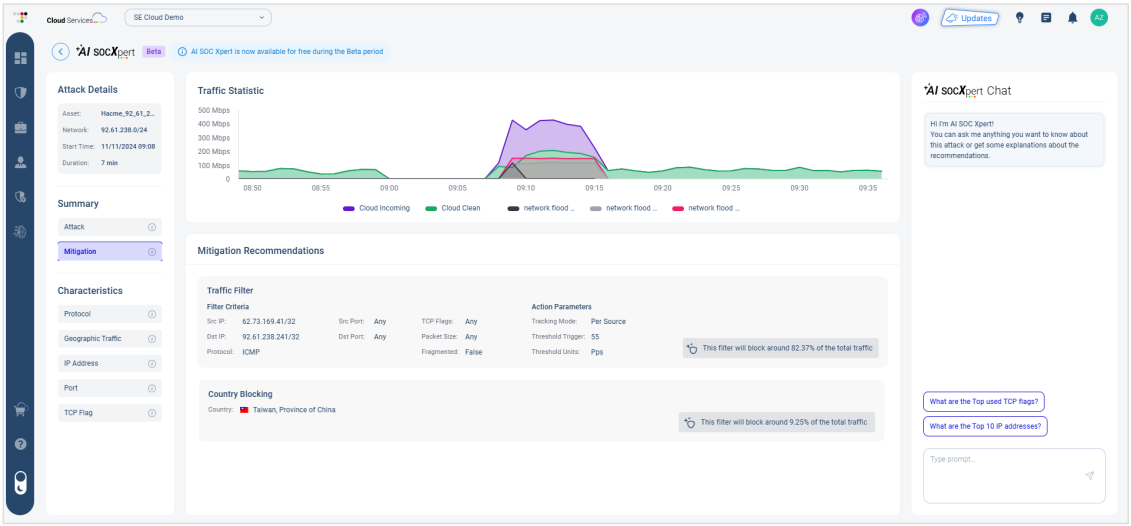
Security Operations Centers (SOCs) are crucial for cyber defense, yet many still rely on standard SIEM systems that struggle with DDoS and application security incidents. GenAI has transformed cyberattacks, enabling rapid zero-day exploits by cybercriminals and creating a critical time gap for SOCs. The shortage of cybersecurity experts only makes things worse for vulnerable businesses. To counteract these challenges, it's essential to use artificial intelligence (AI) to enhance threat prediction, detection and response. Proactive AI-based defenses allow for faster mitigation, reduced mean time to resolution (MTTR) and improved incident management efficiency.

Key Benefits of AI SOC Xpert

- Analyze and remediate instantly with automated AI algorithms
- Reduce root cause analysis lag from days to minutes
- Lower costs and delays with guided tuning and onboarding
- Raise the skill of all SOC analysts to expert level
- Access instant, intuitive forensic data from our AI assistant
- Receive mitigation strategies driven by live attacks, deception network data and crowdsourcing

Figure 1

Radware's unified cloud portal featuring AI SOC Xpert screens



Inside AI SOC Xpert

Automated and Instant Resolution of Incidents

Leaked attacks are detected in real time, leveraging AI-based analysis to generate optimized resolutions, adapting instantly as attacks evolve. Based on Radware's extensive expertise in mitigating real-world attacks, the recommended remediations are tailored to the specific incident and can be implemented automatically with a simple click of a button.

Accelerated Root Cause Analysis with up to 20X Reduction in MTTR

AI SOC Xpert ingests large data sets of security events and performs deep analysis to automatically generate RCAs and reduce MTTR from days to minutes.

Easily Accessible Data & Forensics via Intuitive AI Assistant

Provides instant access and full visibility to all required information, debriefing and ingestion of forensics through an intuitive, AI-prompt assistant. Get instant answers to questions, quick recommendations in real-time and a deeper investigation (if required) for the investigation of security incidents.

SOC Agents Empowered to Become DDoS and Application Security Experts

AI SOC Xpert enables regular SOC agents to effectively address significant application or DDoS threats, ensuring a seamless and efficient resolution that is accessible to SOC members of all levels of expertise.

Seamless Tuning and Onboarding for Lower TCO and Shorter Time-to-Value

Enhancing the accuracy of security policies via recommendations for policy tuning eliminates the need for manual rule-setting and human intervention, significantly lowering operational costs. Additionally, AI-powered tools expedite onboarding and integration with existing operations, ensuring rapid deployment. This seamless approach maximizes value in minimal time, shortening the overall time to value.

Enhancing SOC Efficiency and Effectiveness

In today's rapidly evolving threat landscape, SOC teams face immense pressure to detect and respond to incidents swiftly. AI SOC Xpert empowers SOC teams by providing real-time detection and adaptive responses, significantly reducing the time and effort required to manage incidents. This service allows SOC teams to quickly identify and resolve issues, minimizing downtime and enhancing overall security posture. The intuitive AI assistant streamlines data access and decision-making, allowing teams to focus on strategic tasks rather than manual processes. By lowering operational costs and expediting onboarding, it ensures that SOC teams can operate more efficiently and effectively, ultimately improving their ability to protect the organization.

RWI 389 | 11.18.2024