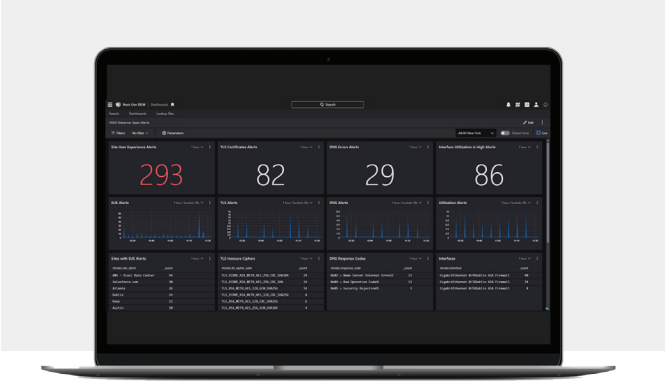
Observer + CrowdStrike Next-Gen SIEM

Integrated Network and Security Visibility for Unified Operations

Connect Observer with the CrowdStrike® Next-Gen SIEM to deliver network-based intelligence that drives unified visibility, smarter prioritization, and faster resolution, for stronger NetSecOps collaboration.

With the Observer Apex Data Connector, we integrate packet and flow-based analytics directly into the CrowdStrike Next-Gen SIEM to understand how issues detected by analyzing network traffic correlate with security events and posture. Observer helps answer key questions like: Is this security event impacting critical service performance? The Observer + CrowdStrike integration enables NetOps and SecOps to correlate, prioritize, and act on incidents more effectively.

Observer analytics and alerts reveal DNS errors, digital certificate issues, weak cipher suites, utilization spikes, and degraded End-User Experience (EUE) scores across sites and services. The Observer Apex Data Connector provides alerts with contextual links that take users directly to the relevant data within Observer, whether it's a DNS issue, degrading end-user experience, an expiring digital certificate, or unusual network utilization. Seamless launch-in-context enables efficient anomaly investigations, including direct access to forensic-level data. This unified visibility strengthens NetSecOps collaboration and accelerates incident response.



Observer brings the performance perspective to CrowdStrike Next-Gen SIEM

Key Benefits

- Unify network and security insights for a full understanding of business-impacting events
- Identify performance issues to prioritize resolution based on user and service impact
- Streamlined issue investigations help to reduce MTTR
- Improved collaboration between NetOps and SecOps teams
- Stronger threat response by transforming network data into action

Key Features

- **Embedded Contextual Links:** Pivot efficiently from CrowdStrike Next-Gen SIEM to Observer for deeper analysis
- **Multi-source Data Integration:** Leverage packets, metadata, and flows to assess performance, errors, and security-impacting events
- **Seamless Workflow Integration:** Embed Observer context into CrowdStrike Next-Gen SIEM investigation paths
- **Network Security Forensics:** Access high-fidelity packet and conversation-level data for event analysis

Contact Us: +1 844 GO VIAVI | (+1 844 468 4284). To reach the VIAVI office nearest you, visit viavisolutions.com/contact

observer-crowdstrike-siem-ds-ec-nse-ae
30194560 900 0825