

Observer Threat Forensics

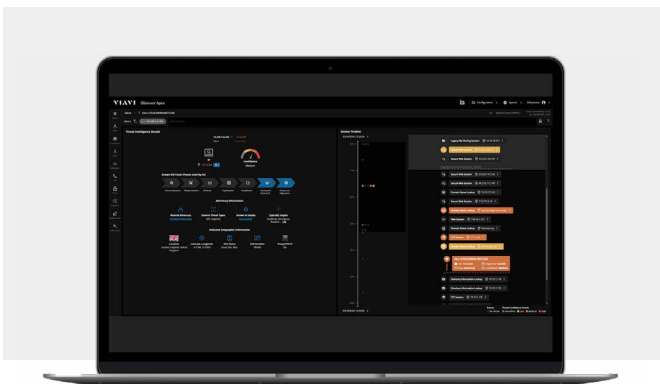
High-Fidelity Network Forensics with Threat Intelligence for NetSecOps

Bridging network visibility and threat intelligence to accelerate threat validation, investigation, and response.

Observer Threat Forensics with Threat Intelligence powered by CrowdStrike® bridges the gap between endpoint detection and network-layer evidence by delivering packet-level visibility, threat context, and forensic depth—all in one solution.

It correlates packet-based analytics, flow telemetry, and real-time threat context to enrich every alert with forensic-grade insight. By correlating end-user and service impact alongside threat intel detailing attacker intent, the solution enables security operations teams to validate incidents faster, reduce noise, and prioritize high-risk threats with precision.

VIAVI Observer delivers high-fidelity alerts derived from real network activity, such as protocol misuse, abnormal flow patterns, service degradations, and indicators of compromise (IOCs), enriched with contextual threat intelligence. Each alert is available within the platform and includes direct access to packet and enriched flow evidence, along with network activity timelines that provide visibility into events before, during, and after the alert. This enables analysts to validate threats, assess impact, and investigate suspicious activity with full forensic context. By correlating this data with security incidents and performance anomalies, the solution gives NetOps and SecOps shared visibility to collaborate more effectively, accelerate triage, and strengthen overall incident response.



Observer Threat Forensics with Threat Intelligence

viavisolutions.com/enterprise/threatforensics

Contact Us: +1 844 GO VIAVI | (+1 844 468 4284).

To reach the VIAVI office nearest you, visit viavisolutions.com/contact

© 2025 VIAVI Solutions Inc. Product specifications and descriptions in this document are subject to change without notice. Patented as described at viavisolutions.com/patents

viavisolutions.com

observerthreatforensics-ds-ec-nse-ae | 30194618 902 0326

Key Benefits

- Accelerate investigations by moving seamlessly from alerts to packet and enriched flow data for deeper analysis
- Reduce mean-time-to-resolve with high-fidelity, behavior-based alerts
- Investigate faster with linked workflows between alerts and data capture, in one platform
- Correlate related activity across multiple indicators, to understand how events connect and prioritize response
- Support strategic NetSecOps convergence with shared data and joint investigation paths

Key Features

- **Evidence-Backed Alerts:** Actionable insights from traffic behavior, enriched with adversary intelligence
- **End-User Experience Scoring:** Prioritize based on actual service disruption, not just severity labels
- **Built-In Threat Intelligence:** Access IOCs, TTPs, and adversary context directly within the investigation workflow
- **Network Activity Timeline:** Visualize activity before, during, and after an IOC to understand context and validate suspicious behavior
- **Layer-7 and DNS Intelligence:** Detect and investigate domain-based IOCs with deep application-layer visibility

Learn more about
our solutions:

