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, and service degradations, providing the context security team's need. Each alert includes a direct link to packet or enriched flow evidence, allowing analysts to validate threats, assess impact, and perform deeper investigation with full forensic detail. By correlating network-derived intelligence with security incidents and performance anomalies, the solution gives NetOps and SecOps teams shared visibility to collaborate more effectively, accelerate triage, and strengthen overall incident response.

Observer Threat Forensics with Threat Intelligence

Key Benefits

- Accelerate incident response with immediate access to correlated threat intelligence and packet-level evidence
- Reduce mean-time-to resolve with high-fidelity, behavior-based alerts
- Investigate faster with linked workflows between alerts and data capture, in one platform
- Improve SOC and NOC collaboration with a unified view of threat and performance impact
- 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:** Observer Threat Intelligence enables direct access to IOCs, TTPs, and adversary context instantly
- **Linked Forensics:** Every alert includes click-through access to associated packets and enriched flows
- **Full-Fidelity Retention:** Long-term packet capture and meta data for retrospective forensics

Learn more about our solutions:

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