What Deep Investigation Really Looks Like: A SOC Analyst's Perspective

Deep investigation in cybersecurity isn't just about watching dashboards and clicking "resolve" on tickets. It's an intricate process of piecing together attacker behavior across time, systems, and attack vectors to understand not just what happened, but how and why. Modern security operations centers rely on sophisticated network detection and response (NDR) platforms to enable this level of analysis, transforming raw network data into actionable intelligence that helps security teams identify suspicious activity and protect critical assets.

The Foundation of Deep Investigation: Advanced Threat Detection

Network Detection and Response platforms continuously scan network traffic and traffic metadata within internal networks (east-west) and between internal and external networks (north-south). These systems use signature and non-signature-based methods such as machine learning and behavioral analytics to identify threats and malicious activities on the network, helping security professionals detect potential threats before they can disrupt systems or compromise sensitive data.

Modern NDR solutions like Fidelis Network® establish baseline models of network behavior through machine learning and network behavior anomaly detection. The system continuously monitors network traffic in real time, comparing current activity against established baselines to detect anomalies and policy violations. When suspicious activity is detected, it alerts security teams and can perform automated actions such as blocking IP addresses or isolating compromised devices. This effective threat detection capability is essential for maintaining an organization's security posture against evolving threats.

Advanced platforms like Fidelis Network® capture over 300 metadata attributes from network traffic—significantly more than traditional NetFlow data. This comprehensive data collection includes network and application protocols, files, and content analysis through patented Deep Session Inspection technology. The system automatically decodes and analyzes traffic to detect advanced threats and unauthorized data transfers across all ports and protocols, providing security operations teams with the visibility needed to identify vulnerabilities and prevent future attacks.

Deep Session Inspection: The SOC Analyst's Secret Weapon

Fidelis Network®'s patented Deep Session Inspection technology provides unique visibility of deeply embedded content and context across all ports and protocols. This capability goes beyond traditional deep packet inspection by analyzing complete communication sessions rather than individual packets. It captures and stores over 300 attributes of standard metadata, plus enhanced metadata including custom tags, to provide rich information for automated and manual threat detection.

Deep Session Inspection bi-directionally scans all network traffic to reveal network and application protocols, files, and content. It automatically decodes and analyzes traffic to detect advanced threats and unauthorized data transfers, providing visibility into nested files and

encrypted traffic patterns that traditional security tools cannot detect. This session-level analysis enables the detection of threats distributed across multiple packets and provides context about entire conversations between systems, helping security teams understand sophisticated threats and advanced persistent threats that might otherwise remain undetected.

Automated Investigation: What Happens When Deep Investigation Begins

Studies show that advanced attacks require approximately 18 minutes from the time of initial detection to becoming indistinguishable from normal activity. As attackers begin to hide in plain sight, they can mask their objectives and behave within normal user patterns, leading to months of undetected dwell time. This rapid evolution of cyber threats demonstrates why security operations centers need automated threat response capabilities to mitigate security incidents effectively.

The role of playbooks enables automation of investigation across multiple network segments and user behaviors. Detection of anomalies, machine learning outputs, encrypted traffic analysis, and DNS detection lead to several investigative possibilities that previously consumed hours of analyst time. Automated playbooks investigate signals across all possible domains in the environment and present analysts with automated analysis, including remediation techniques that lead to file deletion, system rollback, endpoint isolation, and firewall modifications.

Modern NDR platforms like Fidelis Network® provide assisted and automated detection, investigation, and response capabilities. Detected advanced threats are presented as conclusions determined by automated validation, contextual enrichment, and correlated threat activity. This approach enables analysts to take rapid responsive and automated actions rather than spending time gathering evidence from various security systems and sources, significantly improving incident response capabilities and helping organizations strengthen their cybersecurity posture.

Why Leading SOCs Say Detection Alone Isn’t Enough

- Gain speed, clarity, and control with modern NDR.
- Go beyond detection-only strategies
- Slash dwell time with automated response
- Uncover hidden threats

Download the Whitepaper

Threat Investigation and Incident Analysis from the SOC

Detections are often granular events within the network that can generate thousands of individual alerts, creating an unending list of investigations. Advanced NDR platforms perform incident analysis where many detections are correlated to reduce the burden on response teams. Examples include incidents focused on specific assets or users, global analysis of similar detections, and anomalies connected to other detections across the enterprise. This correlation helps security professionals distinguish between legitimate network activity and potential security incidents.

Fidelis Network® automatically groups related alerts to save critical time and improve threat hunting capabilities. It provides sandboxing, network forensics, data loss prevention, threat intelligence, and automated security rules in one unified solution. The platform gives users aggregated alerts, context, and evidence for faster threat investigation, deeper analysis, and reduced alert fatigue, enabling security teams to focus on the most critical cybersecurity threats rather than being overwhelmed by false positives.

Deception Technology: A SOC Analyst's Advanced Detection Method

Fidelis Deception® automatically discovers environments and auto-generates decoys that have profiles, services, and activity matching the environment for active deception layers. The system deploys decoys of key assets, services, and fake data, then makes deception deterministic by setting up breadcrumbs on real systems likely to be compromised, leading attackers to decoys. This innovative approach helps organizations detect insider threats and unknown threats that traditional detection rules might miss.

High-fidelity alerts come from decoys, breadcrumbs, Active Directory credentials, man-in-the-middle traps, and poisoned data combined with network traffic analysis and telemetry data for investigations. The deception environment automatically adapts to network changes as they occur to remain synchronized with actual assets, resources, and services. Deception also provides detection for legacy systems, shadow IT, and enterprise IoT devices where security agents cannot be installed, extending protection to mobile devices and other endpoints that might lack traditional security controls.

Extended Detection and Response: The Complete Investigation Picture

Fidelis Elevate® integrates network visibility with sensors for gateways, internal networks, email and web gateways, and cloud VMs into one unified solution to deliver automated threat detection and response. The platform provides unmatched visibility and threat intelligence with content and context to help organizations quickly address cyberattacks across the entire threat lifecycle—from initial intrusion to exploitation and lateral movement to data theft.

When combined with endpoint detection and response data from solutions like SentinelOne, the integrated solution provides an XDR platform that combines endpoint and network data to easily understand current risks and respond to new and ongoing attacks. Alert validation provides analysts with high-fidelity information that would require significant manual effort to triage through thousands of alerts and hunt through multiple products to determine active threats. This extended detection capability enables organizations to implement a comprehensive incident response plan that addresses emerging threats across all attack vectors.

Cyber Terrain Mapping: Understanding the Investigation Battlefield

When Fidelis sensors analyze network traffic, they gain understanding of assets communicating over the network, including operating systems, asset roles based on protocol analysis, and users augmented by Active Directory data. The collection of all assets and communication paths constitutes the Cyber Terrain of the environment, providing security teams with critical visibility into their organization's systems and potential attack surfaces.

Risk assessment throughout the Fidelis interface highlights asset risk with color-coded numbers

ranging from 1 (low risk) to 10 (critical risk). Risk calculation considers severity (Fidelis alerts, network anomalies, and endpoint vulnerabilities), coverage (security components including network sensor placement and EDR), and importance based on asset role. This multi-dimensional risk calculation enables proactive security measures and helps prioritize response efforts, ensuring that security operations teams can focus their limited resources on protecting the most critical data and systems from cybersecurity risks.

Retrospective Analysis: Learning from Past Investigations

Advanced NDR platforms require solutions that can hunt and automate information analysis of past behavior. New information becomes available constantly through new detections and threat intelligence from industry and internal experts. The ability to connect dots between current events and past behavior represents a crucial aspect of NDR capabilities, enabling security professionals to identify patterns that might indicate advanced persistent threats or sophisticated attack campaigns.

Fidelis Network® supports up to 360 days of retrospective analysis, enabling organizations to apply new threat intelligence to historical data and uncover previously missed attack patterns. Stored protocol, application, and content-level metadata allows discovery of past attacks through retroactive analysis triggered by key indicators derived from new threat intelligence, machine learning, sandbox results, and threat research. This real time threat intelligence capability helps organizations understand how attackers gain access to their systems and develop more effective threat response strategies.

Deep Investigation Best Practices: The SOC Analyst’s Playbook

Effective deep investigation requires systematic timeline reconstruction and comprehensive visibility across network, cloud, email, and endpoint metadata. Organizations need real-time and retrospective analysis capabilities for 30, 60, or 90 days minimum, combined with threat intelligence from multiple third-party sources and internally cultivated intelligence. This extended visibility is essential for identifying advanced persistent threats that may operate over extended periods while attempting to remain undetected.

Automation eliminates manual correlation steps that previously consumed analyst time. Rather than being reactive and piecing together evidence from multiple disparate systems, security analysts can focus on understanding adversary intentions and making strategic decisions under pressure. With comprehensive network detection providing visibility into deeply embedded content across all ports and protocols, analysts can concentrate on attribution and strategic assessment rather than data collection.

The most effective investigations combine cutting-edge artificial intelligence and machine learning with experienced analyst judgment. Understanding attacker behavior patterns and making decisions under pressure define successful response capabilities. Modern NDR platforms enable this approach by providing rich metadata, automated correlation capabilities, and integrated deception technologies that transform network security from reactive monitoring to proactive threat hunting.

Through advanced NDR capabilities, security operations centers can shift from alert fatigue to intelligence-driven investigation, reducing mean time to detection and response while providing the contextual awareness necessary for effective cyber defense in today’s evolving threat landscape. By implementing comprehensive threat detection and response solutions that protect both critical assets and sensitive information, organizations can maintain strong cybersecurity

posture while enabling their security teams to focus on preventing future attacks rather than simply responding to incidents after they occur.

Frequently Ask Questions

What makes Deep Session Inspection different from traditional deep packet inspection?

Deep Session Inspection analyzes complete communication sessions rather than individual packets, providing context about entire conversations between systems. This patented technology goes beyond traditional DPI by examining streaming traffic across network, email, and web to detect threats hidden in nested files, encrypted traffic patterns, and distributed across multiple packets that conventional tools miss.

How does Fidelis Network®’s 300+ metadata attributes enhance investigation capabilities?

Fidelis Network® captures over 300 metadata attributes from protocols, files, and content—significantly more than traditional NetFlow data. This rich metadata includes protocol and application data, content-level information, custom tags, and enhanced metadata that enables retrospective analysis up to 360 days. This comprehensive data collection provides security teams with the detailed context needed for thorough threat investigations.

How do automated playbooks change SOC investigation workflows?

Automated playbooks eliminate manual correlation steps by investigating signals across multiple network segments simultaneously. Studies show advanced attacks require approximately 18 minutes from initial detection to becoming indistinguishable from normal activity. Playbooks automate investigation across all possible domains, presenting analysts with pre-analyzed conclusions including recommended remediation techniques like file deletion, system rollback, and endpoint isolation.