NETWITNESS

Whitepaper

The Modern Analyst Workflow

Connecting EDR, NDR, and SIEM for Faster Investigations

Executive Summary

Security operations centers today face a paradox. Organizations have deployed more detection tools than ever before, yet investigations often take longer than expected. Security teams rely on technologies such as Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), and Network Detection and Response (NDR) to monitor infrastructure, endpoints, and network activity.

Each of these technologies provides valuable insight into potential threats. However, when they operate independently, investigations become fragmented. Analysts must move between systems to gather evidence, correlate events, and reconstruct attack timelines.

This workflow slows response and increases operational burden on security teams.

The modern analyst workflow addresses this challenge by connecting EDR, NDR, and SIEM telemetry into a unified investigation process. Instead of navigating multiple tools, analysts can analyze security events across endpoints, network traffic, and log data within a single investigative framework.

This whitepaper explores:

- Why modern SOC investigations require unified visibility
- The investigative role of SIEM, EDR, and NDR technologies
- How integrating these capabilities accelerates investigations
- The operational benefits of a connected investigation model
- How the NetWitness platform enables a unified analyst workflow

For organizations seeking to reduce investigation time and improve security operations efficiency, integrating endpoint, network, and log telemetry has become a critical capability.

Table of Contents

Why Modern SOC Teams Struggle with Investigation Speed

Security operations teams generate large volumes of alerts every day. Behavioral analytics, detection rules, and threat intelligence feeds continuously monitor infrastructure and user activity.

Despite these advances, determining whether an alert represents a genuine threat often requires extensive investigation.

Analysts must answer several questions before initiating response actions:

- Did malicious code be executed on a system?
- Did the attacker move laterally within the network?
- Were additional endpoints affected?
- Was sensitive data accessed or exfiltrated?

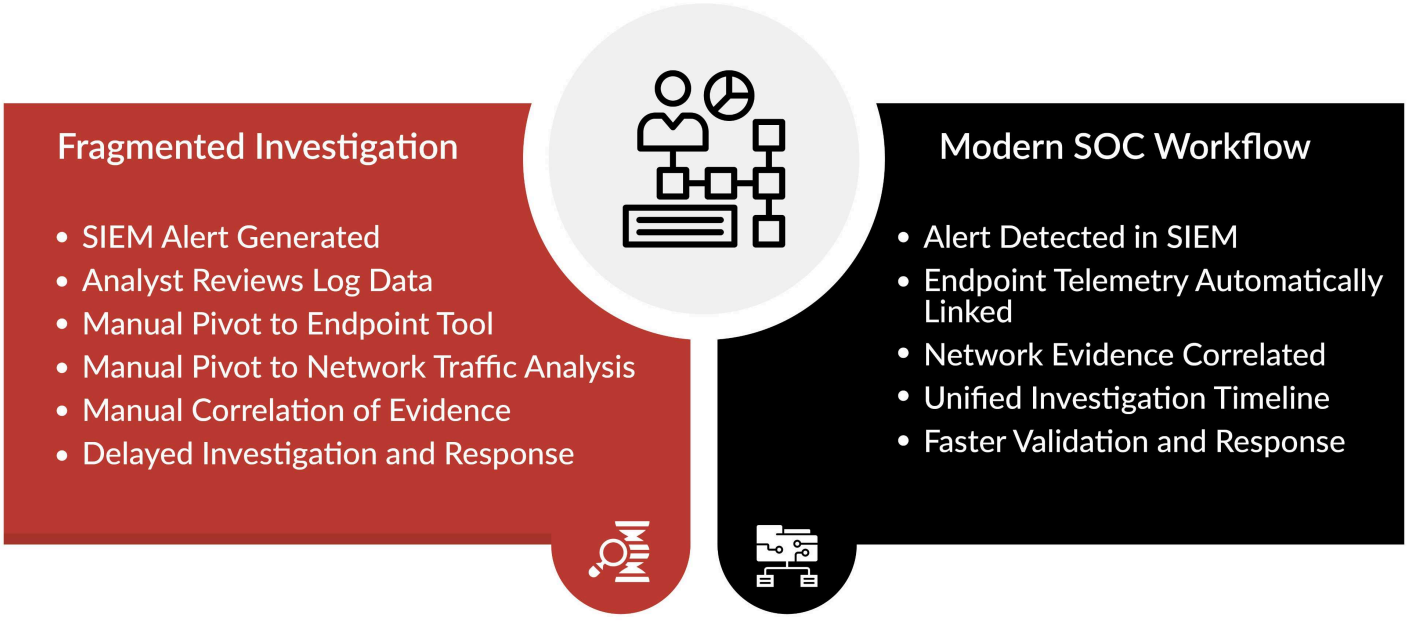
Each of these questions requires visibility into different parts of the environment.

Log data may reveal suspicious authentication activity. Endpoint telemetry can show whether malware is executed on a device. Network traffic analysis may expose communication with command-and-control infrastructure.

Unfortunately, in many environments these data sources exist in separate tools. Analysts must manually collect and correlate information across multiple platforms before reaching a conclusion.

This fragmented workflow slows investigations and increases the likelihood that critical signals will be overlooked.

Fragmented vs. Unified Analyst Workflow



Fragmented telemetry increases investigation time. Unified telemetry enables faster threat validation.

The Role of SIEM in Detecting and Correlating Security Events

Security Information and Event Management platforms provide centralized visibility across enterprise infrastructure. They collect log data from operating systems, applications, authentication services, network devices, and cloud environments.

By aggregating these events, SIEM platforms enable security teams to detect suspicious patterns such as:

- Abnormal login activity
- Privilege escalation attempts
- Policy violations
- Anomalous user behavior

Correlation rules and behavioral analytics help identify relationships between events occurring across different systems.

However, logs typically provide summaries of activity rather than full evidence of how an attack unfolded. While a SIEM alert may reveal that suspicious behavior occurred, it does not always explain the underlying actions performed by an attacker.

To investigate these activities, analysts must examine endpoints and network telemetry.

The Role of EDR in Revealing Endpoint Activity

Endpoint Detection and Response technologies monitor activity on user devices and servers. These systems capture detailed telemetry related to process execution, file activity, registry changes, and script behavior.

Endpoint telemetry allows analysts to determine how suspicious activity occurred on a device.

During investigations, EDR systems help analysts identify:

- Which processes initiated malicious behavior
- Whether malware attempted persistence
- What files were created or modified
- Which users interacted with the system

Behavior-based analytics also enable EDR platforms to detect threats that do not rely on known signatures, including fileless malware and living-off-the-land techniques.

While endpoint telemetry reveals activity occurring on individual systems, it does not always provide insight into how attackers move across the network or communicate with external infrastructure.

This visibility gap is addressed through network detection technologies.

The Role of NDR in Detecting Network-Based Threat Activity

Network Detection and Response platforms analyze network communications to detect suspicious behavior across enterprise infrastructure.

Unlike log-centric monitoring tools, NDR technologies examine network traffic and metadata to identify anomalies and attacker movement.

Key capabilities include:

- Deep protocol analysis
- Network metadata inspection
- Threat intelligence correlation
- Behavioral detection of suspicious traffic patterns

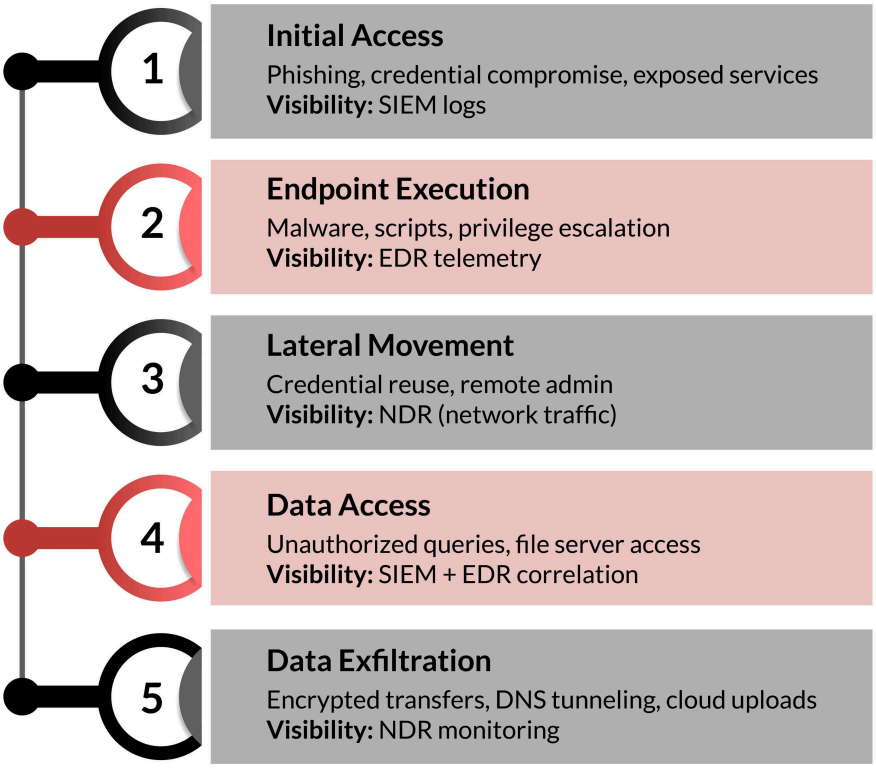
Advanced NDR platforms also support full packet capture, allowing investigators to reconstruct network sessions during forensic investigations.

Network visibility allows analysts to detect activities such as:

- Command-and-control communication
- Internal reconnaissance
- Lateral movement between hosts
- Data exfiltration attempts

These insights are essential for understanding how an attack spreads across the environment.

Security Visibility Across the Attack Lifecycle



How an Integrated Investigation Model Accelerates Incident Response

When endpoint, network, and log telemetry operate together, analysts gain the context required to investigate threats quickly and accurately.

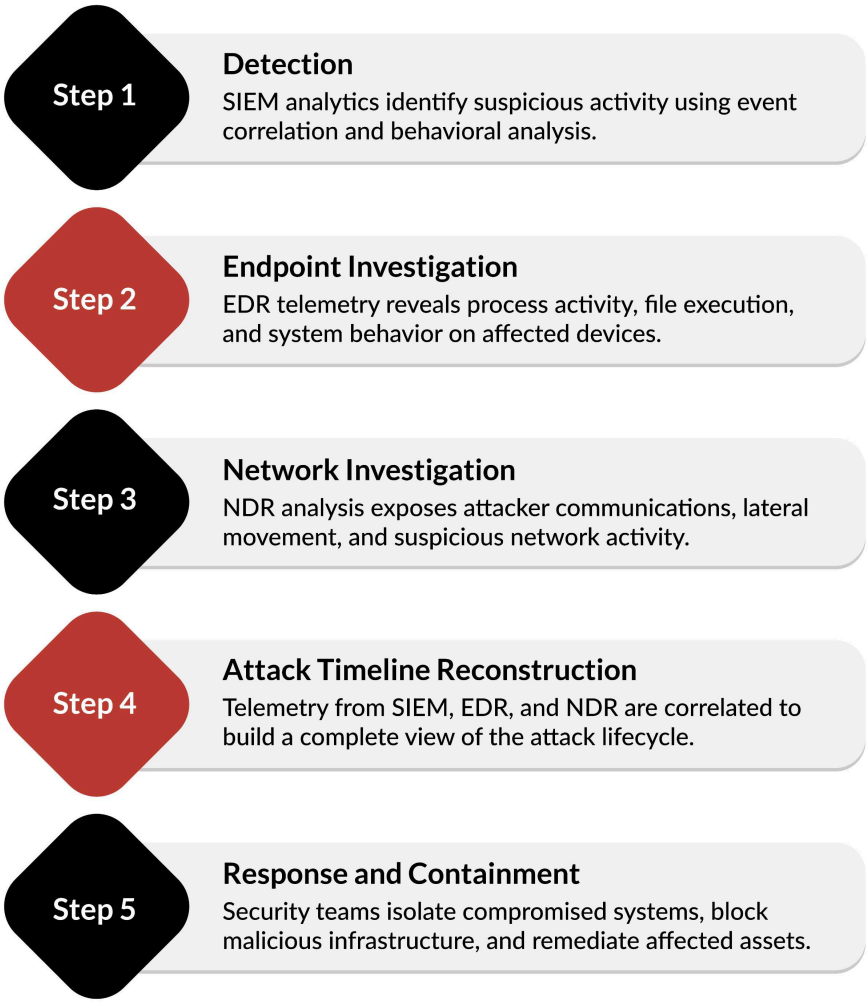
An integrated investigation model enables analysts to:

- Correlate events across multiple telemetry sources
- Reconstruct attack timelines more quickly
- Identify the scope of compromise
- Prioritize response actions based on accurate context

Instead of spending time gathering evidence from separate tools, analysts can focus on understanding attacker behavior and containing threats.

This shift significantly improves security operations efficiency.

The Modern Analyst Investigation Model



Outcome- Faster investigations | Improved analyst productivity | Reduced attacker dwell time

The Challenge with Traditional SIEM, EDR, and NDR Deployments

Many organizations deploy SIEM, EDR, and NDR technologies from different vendors. While each solution provides valuable capabilities, operating them as separate tools introduces operational challenges.

Security teams often encounter:

- **Investigation silos** - Telemetry remains isolated within separate platforms.
- **Data normalization challenges** - Different tools use different data formats and analysis models.
- **Manual correlation -** Analysts must manually assemble attack timelines across systems.
- **Limited forensic visibility -** Some tools rely primarily on summarized logs rather than full telemetry.

To address these challenges, security teams require a platform designed to correlate telemetry across security layers.

How NetWitness Enables a Unified Investigation Platform

NetWitness was designed with investigation in mind. The platform integrates SIEM, Network Detection and Response, and Endpoint Detection and Response capabilities within a unified threat detection and response architecture.

This integration allows analysts to investigate threats across endpoints, networks, and infrastructure logs without switching tools.

Rather than functioning as separate technologies, these capabilities operate as part of a single investigative environment.

Deep Network Visibility Through Full Packet Capture

One of the defining capabilities of the NetWitness platform is deep network visibility.

Unlike many NDR solutions that rely solely on network flow data, NetWitness captures and analyzes full packet data across the environment.

This allows analysts to reconstruct network sessions and examine communications in detail during investigations.

Packet-level visibility enables security teams to identify:

- Command-and-control communication
- Suspicious protocol behavior
- Lateral movement between systems
- Data exfiltration attempts

This forensic capability provides critical evidence when investigating sophisticated attacks.

Advanced Endpoint Visibility for Investigating System Activity

NetWitness Endpoint Detection and Response provides detailed visibility into activity occurring on user devices and servers.

Lightweight endpoint agents capture telemetry related to process execution, file activity, and system behavior.

This allows analysts to quickly determine:

- How malicious code executed
- Whether persistence mechanisms were installed
- What actions occurred on compromised systems

By correlating endpoint telemetry with network and log data, investigators can understand how attacks progressed across the environment.

Scalable Log Analytics and Threat Correlation

NetWitness SIEM provides centralized log collection and advanced analytics across hybrid infrastructure. The platform collects logs from a wide range of enterprise systems, including applications, cloud services, authentication platforms, and network devices. Metadata is generated during ingestion, enabling analysts to rapidly search and correlate events across large datasets.

This capability allows security teams to quickly identify relationships between events and detect suspicious patterns across the environment.

Unified Visibility Across Security Telemetry

Where NetWitness differentiates itself most clearly from traditional SIEM, EDR, and NDR deployments is in how these capabilities are integrated.

Rather than requiring analysts to move between separate tools, NetWitness correlates telemetry across network traffic, endpoint activity, and log data within a single investigation interface.

Analysts can:

- Pivot seamlessly between telemetry sources
- Reconstruct attacker timelines
- Analyze communications at packet level
- Investigate endpoint activity and user behavior
- Identify the full scope of compromise

Correlating telemetry across endpoints, networks, and logs enables a unified data model where evidence is enriched with business context and threat intelligence. This allows analysts to move beyond alert validation and quickly extract meaningful insights, reducing the time required to investigate and respond to threats.

Conclusion: Building the Modern Analyst Workflow

Security operations are increasingly defined by investigation speed. Organizations must be able to quickly determine whether suspicious activity represents a genuine threat and understand the full scope of an attack. Achieving this level of visibility requires an integrated approach to security telemetry.

By connecting EDR, NDR, and SIEM capabilities, organizations can transform fragmented detection tools into a unified investigation platform. This connected analyst workflow enables faster investigations, improved operational efficiency, and more effective incident response.

For enterprises seeking to strengthen security operations, building this integrated investigation model has become an essential step toward defending modern infrastructure.

Accelerate Your Security Investigations

Unify endpoint, network, and log telemetry in one platform to accelerate threat detection and response with NetWitness.

Request a Demo

Contact Information

Email for customer Service
support@netwitness.com

Website
www.netwitness.com

Follow us for regular updates

NETWITNESS