Technical Brief

STAMUS NETWORKS

Reduce the Costs of SIEM Data Retention with Clear NDR™

Conditional Logging & Pre-Correlation Reduce Data Volume without Sacrificing Security

Executive Summary

Security Information and Event Management (SIEM), data lake, and extended detection and response (XDR) platforms are essential for modern security operations but often come with significant costs tied directly to data ingestion volumes. This technical brief demonstrates how Clear NDR's conditional logging and pre-correlation capabilities can dramatically reduce SIEM ingestion costs while maintaining comprehensive security visibility. By comparing the data volumes from traditional approaches (IDS, NSM, NetFlow) with Clear NDR's optimized data, organizations can reduce data volume by as much as 97% and achieve substantial cost savings without sacrificing security effectiveness.

The SIEM Cost Challenge

SIEM platforms typically charge based on data ingestion volumes, making the management of log sources a critical cost factor for security teams. Traditional approaches to network security monitoring involve sending raw data from multiple sources to the SIEM:

- Intrusion Detection Systems (IDS) alerts
- Network Security Monitor (e.g. Zeek) logs (connection, DNS, HTTP, SSL/TLS, etc.)
- NetFlow/IPFIX records
- Packet capture (PCAP) files for investigations
- Extended detection and response (EDR) event logs
- Application logs
- Cloud workflow logs

While comprehensive, this approach results in extremely high data volumes that drive up SIEM costs significantly, often forcing security teams to make difficult tradeoffs between visibility and budget constraints.

Log Volume from Traditional Network Security Tools

When using separate tools to monitor network traffic, organizations typically ingest data from multiple sources, each generating its own set of logs. In this paper, we will focus on three of those tools:

IDS/IPS Systems

- Alert logs (1-5 GB per day per Gbps of monitored traffic)
- Rule match details (2-8 GB per day per Gbps)
- Packet captures of suspicious traffic (varies widely based on configuration)

Network Security Monitor (e.g. Zeek)

- conn.log: Basic TCP/UDP/ICMP connection details (10-20 GB per day per Gbps)
- dns.log: DNS query and response data (2-5 GB per day per Gbps)
- http.log: HTTP requests and responses (5-15 GB per day per Gbps)
- ssl.log: SSL/TLS handshake information (3-8 GB per day per Gbps)
- files.log: Metadata about files transferred (1-3 GB per day per Gbps)
- x509.log: Certificate information (0.5-2 GB per day per Gbps)

Additional protocol-specific logs (SMB, RDP, SMTP, etc.) adding 5-15 GB per day per Gbps per protocol

NetFlow/IPFIX

- Flow records (3-8 GB per day per Gbps of monitored traffic)
- Flow metadata and extensions (additional 1-3 GB per day per Gbps)

For a typical 10 Gbps network, these sources can collectively generate 300-800 GB of log data per day that would need to be ingested into a SIEM for comprehensive visibility. The challenge is compounded by:

- **Duplication:** The same network session may appear in IDS logs, Zeek conn.log, and NetFlow records
- **Correlation burden**: Analysts must manually correlate events across different log formats and timestamps
- **Varying retention needs**: Some logs are more valuable for long-term retention than others

This leads to significant SIEM ingestion costs without providing the pre-correlation and contextual advantages of an integrated NDR solution.

Clear NDR: Pre-Correlated, Optimized Data

Clear NDR offers two key capabilities that directly address SIEM ingestion costs:

- **Conditional Logging:** Instead of capturing every network transaction, Clear NDR can selectively store only the protocol transactions, flow records, and file transactions associated with critical detection events such as alerts, Sightings™, and policy violations.
- **Pre-Correlation:** Clear NDR performs correlation at the source, linking relevant network traffic data with security events before sending to the SIEM. This pre-correlation eliminates the need to ingest raw data streams for correlation within the SIEM itself.

Comparative Analysis: Traditional vs. Clear NDR Approach

The table below compares the data volumes generated by traditional raw data ingestion versus Clear NDR's optimized approach:

	10 Day Results				
	Traffic Rate	Hosts Observed	Events (all) per second	Detection Events	Log Volume
Traditional Raw Data Ingestion with IDS + NSM + NetFlow	5 Gbps	130,000	101,100	21,000,000	4.5 TB
Clear NDR with Conditional Logging & Pre-Correlation	5 Gbps	130,000	600	5,300,000	115 GB
		Savings	99 %	75 %	97 %

SIEM Cost Savings Across Network Scales

The impact on SIEM ingestion costs scales with network size. The table below demonstrates the potential savings at various network data rates, comparing the data volumes generated by traditional raw data ingestion versus Clear NDR's optimized approach:

Network Data Rate	Example Total Storage (gigabytes) Required for 10 Days		Verbose (full logging)	With Conditional Logging
	Raw Data Volume for SIEM with IDS+NSM+Netflow	With Clear NDR and Conditional Logging		
1 Gbps	900 GB	40 GB	95.56%	$10,320
5 Gbps	4.5 TB	115 GB	97.44%	$52,620
10 Gbps	9 TB	250 GB	97.22%	$105,000
25 Gbps	23.5 TB	600 GB	97.45%	$274,800
40 Gbps	37 TB	1 TB	97.30%	$432,000
100 Gbps	95 TB	2 TB	97.89%	$1,116,000

* Based on industry average SIEM pricing of $4 per GB/day ingested. Actual savings will vary based on specific SIEM pricing models.

Benefits Beyond Cost Savings

Clear NDR's approach delivers additional benefits beyond direct SIEM cost reduction:

1. **Improved Analysis Efficiency:** Pre-correlated data means analysts spend less time manually connecting events across multiple data sources.
2. **Faster Query Performance:** Reduced data volumes in the SIEM lead to quicker search and investigation times.
3. **Extended Retention:** Organizations can afford to retain security data for longer periods within the SIEM.
4. **Preserved Threat Detection:** Unlike simply truncating data sources, Clear NDR maintains full threat detection capabilities while optimizing data volumes.

Implementation Considerations

Security teams can implement this approach through:

- Configuring Clear NDR for conditional logging mode
- Setting up SIEM integration using Clear NDR's API or direct integration connectors
- Eliminating redundant raw data sources from SIEM ingestion
- Maintaining a small subset of critical raw logs if required by compliance needs

Summary

By leveraging Clear NDR's conditional logging and pre-correlation capabilities, security teams can dramatically reduce SIEM data ingestion costs while maintaining comprehensive security visibility. With data volume reductions averaging 97% across various network sizes, organizations can realize significant operational cost savings without compromising security effectiveness.

The approach is particularly valuable for organizations with high-speed networks, where traditional raw data ingestion would make SIEM costs prohibitively expensive. Clear NDR's model enables security teams to focus their SIEM budget on extending retention periods and adding additional security data sources rather than processing redundant network traffic data.

Introducing Clear NDR

Detection you can Trust, with Results you can Explain

Clear NDR is an open and transparent Network Detection and Response that delivers:

- Clear Visibility - Monitor activities across your entire attack surface
- Clear Detection - Multi-layer, transparent detections you can understand
- Clear Evidence - Everything you need to quickly resolve the incident
- Clear Response - The confidence you need to automate your response

ABOUT STAMUS NETWORKS

Stamus Networks believes that cyber defense is bigger than any single person, platform, company, or technology. That's why we leverage the power of community to deliver the next generation of open and transparent network defense. Trusted by security teams at the world's most targeted organizations, our flagship offering – Clear NDR™ – empowers cyber defenders to uncover and stop serious threats and unauthorized network activity before they harm their organizations. Clear NDR helps defenders see more clearly and act more confidently through detection they can trust with results they can explain.

STAMUS NETWORKS

5 Avenue Ingres
75016 Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

contact@stamus-networks.com
www.stamus-networks.com

