NXLog

Enhancing Managed Security Service operations with **NXLog**

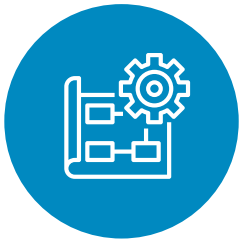
nxlog.co

In their effort to provide adequate security monitoring, management and response capabilities Managed Security Service Providers (MSSP) are heavily dependent on the reliability and accuracy of the data they are working with. This is especially true when it comes to log messages. As all major MSSP infrastructures at its core consist of a Security Operation Centre (SOC), which is powered by a robust Security Information and Event Management (SIEM) system. Provided MSSP services such as firewall management, intrusion detection, virtual private network control, vulnerability scanning and anti-viral services all heavily rely on data extracted from log messages. Lacking the necessary tools to collect and send the right log messages into their SIEM, MSSPs are incapable to ensure proper information security and business continuity for their customers.

The challenges

Proper log collection and distribution to the SIEM is an ongoing struggle for MSSPs which can originate from not addressing three main pillars.

Is the logging infrastructure suited for unhindered log collection and log enrichment?



Is the log transport adequately protected, and the metadata optimized and structured to be digestible by all systems?

Is the log collection optimized as to not negatively affect the performance of the systems handling the large volumes of logs?

By raising these questions, we can deep dive into what are the actual challenges that create these struggles and by addressing them finding the right solution can be made much easier.

Log Collection Challenges

Infrastructure	Data	Performance
Source	**In transit & at rest**	**Volume**
Log messages originate from scattered heterogeneous environments. These messages may be unstructured or semi-structured, with fields and data types that may not be normalized to the required SIEM fields. The challenge rests with a log collector that can draw from these varying environments, enrich the data and forward into SIEMs without losing data fidelity.	Logs hold metadata that is required to fulfil needs within the security, IT operational and business domains. As these logs traverse across networks, data security in transit need to be supported. Log data at rest should be considered. Built-in log rotation and retention can be used for compliance and archiving needs, as well as checksums for log message integrity.	Properly supporting log volume is an inevitable challenge for enterprise systems handling thousands of endpoints. These endpoints will also generate a wide variety of logs and in tremendous quantities, affecting system and memory performance of the log centralization server. A smart strategy to collect logs is needed to avoid poorly developed logging infrastructure.
Integration	**Format**	**Scaling**
SIEMs may be the core destination, but they are not the only destination for logs. Instead, a vendor neutral solution needs to be implemented, making it possible for MSSPs to use the same log collector to forward logs to several other destinations for log monitoring, analysis and visualization.	Depending on the source, logs are written in a number of formats, and presented as unstructured, semi-structured or structured with key value pairs. Log destination may also have its own requirements as the format that a log is ingested in will affect how it should be enriched and converted on the log collection stage.	Logs are written and presented in a number of different formats - CSV, JSON, Syslog, EventLog, etc. On top of that logs may arrive in numbers that many destination systems cannot necessarily handle. If the destination threshold exceeds due to the amounts of logs it receives at once it can result in an overload.

The solution

To tackle the described challenges many MSSPs incorporate a log collection solution into their SOC infrastructure which acts as a bridge between log sources and destinations. This allows optimized log flow and handling and ensures that the right data gets to the right place.

Log Collection Solutions

Infrastructure	Data	Performance
Source	**In transit & at rest**	**Volume**
Log collection solutions are vital for centralized log exchange and log management hubs. It collects all logs regardless of format or size from all available sources.	Log collection solutions ensure secure log transfer via encrypted channels and log message integrity at rest through cryptographic check summing on messages.	Log collection solutions are meant to operate with vast amounts of logs with features to deal with downtime of the log source.
Integration	**Format**	**Scaling**
Log collection solutions forwards logs to the right destinations. Even by distributing the same logs to multiple destinations in parallel.	Log collection solutions are capable in parsing and enriching logs with the necessary structured fields and convert logs into multiple formats.	Log collection solutions are meant to optimize log flow and forward only the amount the destination is capable digesting.

What is NXLog?

NXLog is a highly reliable and adaptable log collection solution that offers superior log collection including log enrichment (parsing, filtering, and conversion) and log forwarding. The suite is supported and certified on all major operating systems, is compatible with SIEM and log analytics products, and can handle data sources that other tools cannot cope with, providing more visibility into systems and operations.

NXLog Solution

Infrastructure	Data	Performance
Source	**In transit & at rest**	**Volume**
Deploy on multiple platforms - Linux (RHEL, CentOS, Debian, Ubunut), Windows, BSDs (FreeBSD, OpenBSD), major variants of Unix (AIX, Solaris, and macOS) and Docker. Implement either as agent-based, agent-less or a combination of both. Collect logs from files, databases, Unix domain sockets, network connections, and other sources. BSD Syslog, IETF Syslog, the Snare Agent format, Windows Event Log, JSON, and other formats are all supported.	NXLog provides features throughout the application to maintain the security of your log data. TLS/SSL is supported for encrypted, authenticated communications and to prevent data interception or alteration during transmission. When NXLog receives a log message it stores it in its original format as a raw event data. Stored logs can be encrypted, timestamped and digitally signed.	With an event-based architecture for processing tasks in parallel, non-blocking input and output where possible, and a worker thread pool for incoming log messages, NXLog is designed for high performance on modern multi-core and multi-processor systems. The input/output readiness notifications provided by most operating systems are used to efficiently handle large numbers of open files and network connections.
Integration	**Format**	**Scaling**
NXLog can integrate and inject logs in parallel into multiple technologies such as SIEM and Log Analytics Suites, Log Management Suites, SaaS and more. **SIEM:** IBM QRadar, RSA NetWitness, Rapid7 InsightIDR, Splunk Enterprise, McAfee ESM, FireEye Helix, Micro Focus ArcSight, Securonix. **Log Management:** Graylog, Solarwinds Loggly, Splunk, Datadog, Elastic Search with Kibana. **SaaS Destinations:** Nagios Log Server, Amazon S3 Cloud Storage, Azure Operations Management Suite (OMS), and NetApp.	Depending on the source, logs are written in a number of formats, and presented as unstructured, semi-structured or structured with key value pairs. Log destination may also have its own requirements as the format that a log is ingested in will affect how it should be enriched and converted on the log collection stage.	Logs are written and presented in a number of different formats - CSV, JSON, Syslog, EventLog, etc. On top of that logs may arrive in numbers that many destination systems cannot necessarily handle. If the destination threshold exceeds due to the amounts of logs it receives at once it can result in an overload.

NXLog integration with MSSPs

Nuspire Networks provides solutions in IT for franchises, industrial, healthcare and finance sectors.

Quadrant Security provides monitoring, notification and remediation services by cybersecurity professionals.

RadarServices is Europe's leading technology company in the field of Detection & Response.

T-Systems Austria provides information and communications technology (ICT) infrastructure and networking services.

"Managed security services providers (MSSPs) form an integral part of NXLog's clientele. The association with an MSSP running Europe's largest cyberdefence center proves to be an exemplification of how technology partners can benefit from NXLog. The MSSP is able to monitor security events without any data leaving the customer premises, while being able to remotely manage the logging pipeline."

Quote from the enterprise security magazine interview

In conclusion

MSSP should make sure that logs are collected in a reliable way, are always available and in the right format for their chosen SIEM solution to ingest. To make sure logs are adequately utilized, it is highly recommended to front end the SIEM solution with a robust log collection solution capable of forwarding and enriching the metadata at the log collection stage.

NXLog

For more information on NXLog visit our **website**, check out our **integration page** for the major integrations or schedule a **personal meeting** with one of our professionals.