NXLog

Securing the City That Never Sleeps: How NYC Cyber Command Bolstered its Cyber Resilience with NXLog Platform

NYC Cyber Command

Securing the City That Never Sleeps: How NYC Cyber Command Bolstered its Cyber Resilience with NXLog Platform

CUSTOMER PROFILE

Founded in July 2017, New York City Cyber Command protects the city and its residents from cyber threats by ensuring the resilience of essential services and data. Over the past seven years, it has enhanced its cybersecurity maturity across 100+ city agencies, collaborating with public and private partners to safeguard New York's digital ecosystem.

RELATED INDUSTRIES

- Government
- Regulations

BUSINESS DEMANDS

- Achieve compliance
- Security posture improvement

CHALLENGES

- Managing logs from diverse systems
- Achieving real-time visibility
- Scaling to handle increasing log volumes

SOLUTION

NXLog Platform

BUSINESS RESULTS

Enhanced network visibility, reduced incident response time, and implemented scalable log management – strengthening the city's cyber resilience and operational efficiency.

BACKGROUND

New York City Cyber Command (NYC3) is a critical technology organization tasked with safeguarding the city's digital infrastructure and ensuring the resilience of essential services. Managing a complex and diverse IT environment — including DNS servers, Windows servers, Centrify AuditTrail systems, AD FS servers, and DHCP servers — NYC3 generates massive volumes of logs in varied formats. As regulatory requirements have tightened and the cybersecurity landscape has grown increasingly complex, NYC3 faced the challenge of maintaining robust security and compliance by unifying real-time log collection across its heterogeneous systems.

The existing log collection solution fell short of meeting NYC3's operational and security needs, presenting several key challenges:

- **Diverse IT infrastructure:** The environment's mix of systems and log types required different protocols and mechanisms for log extraction, making centralized collection and processing a significant hurdle.
- **Limited real-time visibility:** The inability to extract certain logs (e.g., DNS) and forward them in a standardized format hindered the Security Operations Center's (SOC) visibility and delayed log parsing development, impacting incident response capabilities.
- **Scalability and performance:** As NYC3 expanded its operations to protect the city's vast digital ecosystem, the surge in log volume strained the existing system, necessitating a solution capable of high performance, scalability, and simplified management.

To address these challenges and ensure the city remained digitally resilient, NYC3 sought a logging solution that could deliver scalability, flexibility, and compliance while enhancing real-time visibility and operational efficiency.

SOLUTION

After evaluating the available logging solutions, NYC3 selected **the NXLog Platform** for its robust feature set, exceptional performance, and seamless integration capabilities across diverse environments. NXLog's proven track record in addressing complex log management challenges in highly regulated industries made it the ideal choice for NYC3's mission-critical operations.

Key Reasons for Choosing NXLog:

- **Comprehensive support for a heterogeneous environment:** NXLog provided unparalleled compatibility with NYC3's diverse infrastructure, supporting log collection from all major operating systems (e.g., Windows, Red Hat Linux, Ubuntu, macOS) and network devices. Its modular architecture also ensured seamless integration with critical systems, including DNS servers, DHCP servers, AD FS, and Centrify AuditTrail.

- **Enhanced syslog integration:** Native support for syslog enabled seamless log forwarding and real-time analytics. Logs were normalized and enriched before being sent to the syslog aggregators, streamlining threat detection and compliance reporting.

The deployment of NXLog Platform was a carefully orchestrated process, designed to ensure minimal disruption to NYC3's critical operations while maximizing efficiency. It began with integrating log sources across the organization's diverse infrastructure. Using NXLog Platform wizards, agents were swiftly deployed and configured across DNS servers, Windows servers, DHCP servers, and Centrify AuditTrail systems. The platform's ability to handle bulk installations with minimal human intervention allowed for a seamless and consistent rollout. NXLog agents immediately began capturing critical logs — ranging from DNS queries and DHCP lease information to system security events — laying the groundwork for a centralized and comprehensive log management system.

With the logs flowing in, the next step was to refine the data. Logs were enriched with contextual details like hostnames, timestamps, and consistent formatting. This process of normalization and enrichment transformed raw data into actionable insights, significantly improving the accuracy and efficiency of analytics within the SIEM and other third-party tools. It was a pivotal moment, as the team could now see a clearer, more unified picture of the network's activities.

As the system came to life, the focus shifted to continuous optimization. The team conducted rigorous performance tuning to ensure all necessary logs were captured, processed, and relayed with minimal latency. This meticulous attention to detail meant that the solution was not only functional but also finely tuned for real-time operations, meeting NYC3's high standards for speed and reliability.

The results of this phased implementation were transformative. With logs centralized from DNS, DHCP, and security systems, NYC3 achieved unprecedented end-to-end visibility of its network activities. Suspicious behaviors and anomalies were detected more efficiently, significantly reducing security risks. And the real-time relay of logs to security tools empowered the Security Operations Center (SOC) to identify and respond to threats with remarkable speed, minimizing potential damage.

Additionally, the agile architecture of NXLog Platform enabled scalability, so NYC3 could easily integrate additional data sources as its infrastructure evolved. This provided a future-proof solution that would grow alongside the city's cybersecurity needs.

RESULTS

The deployment of NXLog Platform marked a turning point for NYC3, delivering a robust, scalable, and future-ready logging solution that improved its network and security visibility. By seamlessly handling logs from heterogeneous systems and integrating effortlessly with syslog servers and SIEM, NXLog empowered NYC3 to centralize, normalize, and analyze data with unprecedented efficiency. This transformation not only streamlined operational processes but also strengthened NYC3's ability to detect and respond to threats in real time, strengthening the city's overall cyber resilience.

By choosing NXLog, NYC3 underscored its unwavering commitment to security, compliance, and innovation in the face of an ever-evolving threat landscape. The deployment of NXLog Platform wasn't just a technical upgrade — it was a strategic leap forward, equipping NYC3 with the tools and insights needed to protect New York City's digital ecosystem with greater confidence and resilience.

For more information about NXLog products and services, visit our website,contact us via the web form, or schedule a meeting.

Start free with the NXLog Platform now!