NXLog

Ports of Auckland Choose NXLog Platform for Security Operations

PORT OF AUCKLAND
TĀMAKI HERENGA WAKA

Ports of Auckland Choose NXLog Platform for Security Operations

CUSTOMER PROFILE

Ports of Auckland is New Zealand's largest container port with a total breakbulk volume 7.293 million tonnes in 2022. It provides container terminal handling, bulk cargo handling, freight hubs, cruise industry facilities, and other services.

RELATED INDUSTRIES

- Container terminal handling services
- Cargo handling services
- Marine services
- Cruise ship services

BUSINESS DEMANDS

Improve security posture and save on SIEM costs.

CHALLENGES

Establish unified log collection pipeline to get events from various network sources. Implement pre-filtering of events on agents and forwarders to decrease EPS volume.

SOLUTION

- NXLog Platform
- NXLog Professional Services

BUSINESS RESULTS

- Security posture of IT/OT networks improved with unified and autonomous log collection pipeline
- 6-digit in savings reached on SIEM noise reduction

NXLog

BACKGROUND

Commercial sea ports face the challenge of non-stop operations. And that challenge gets more complicated nowadays: to remain competitive, ports have both to maintain existing operations and adapt quickly to evolving maritime environment, including new assets, policies and regulations. Ports of Auckland is not an exception, it has an extensive IT and OT infrastructure that ought to operate flawlessly 24 hours a day, 7 days a week, 365 days a year and its cybersecurity is a crucial component that helps to support business continuity while timely aligning with business needs.

Security events logging and analysis is one of the key aspects of a solid defense-in-depth strategy required for port's security operations. However, a vast array of interconnected endpoints and a wide structure of stakeholders introduce certain challenges for log management systems' adoption across any seaport organization.

SOLUTION

To improve its security posture, Ports of Auckland required security design transformations, including those on networks segregation and security logs management level. For effective cybersecurity operations it was necessary to implement Security Information and Event Management (SIEM) solution across all the infrastructure.

While a SIEM solution has been selected and deployed for testing stage, project delivery team discovered various limitations with existing log aggregation tools. So, it was decided to implement a parallel host logging with NXLog that has a wide integration list, featuring selected SIEM as well.

After the tests NXLog telemetry pipeline has been planned to replace old log collection tools and successfully rolled out across the infrastructure, including hundreds of host agents and collectors to forward events to SIEM system both from IT and OT networks.

It's a small number of events collected from endpoints make sense for security operations, while the others are just to pose a significant impact on SIEM performance and its recurring costs (usually a SIEM is priced by events per second (EPS) model).

So, the next challenge for Ports of Auckland was to decrease amount of noise forwarded to SIEM. To achieve that, an extensive filtration policy has been applied by NXLog agents, thanks to its flexible configuration options, parsing and event transformation capabilities. Eventually, Ports of Auckland managed to reach 6-digit in savings on SIEM by filtering events with NXLog.

NXLog significantly simplified log collection routines. Initially overseen by a dedicated security service provider, the telemetry pipeline was smoothly handed over to the Ports of Auckland team for ongoing management.

The NXLog free tier was initially used during the proof-of-concept phase. Ultimately, the full-featured NXLog Platform was selected for production deployment due to its exceptional manageability and scalability.

One of the key strengths of NXLog Agent is its granular configuration and advanced filtration capabilities, which allowed us to ingest only valuable events, significantly reducing expenditure on EPS volume.

NXLog enabled us to overcome technical challenges thanks to its non-blocking design and, most importantly, its native integration with our SIEM solution — an essential factor for the project's success.

Lajos Varga,
Head of Digital Technology,
Ports of Auckland

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!