NXLog

PORTS OF AUCKLAND CHOOSE NXLOG FOR SECURITY LOGS COLLECTION

PORTS OF AUCKLAND CHOOSE NXLOG FOR SECURITY LOGS COLLECTION

PORTS OF AUCKLAND
TĀMAKI HERENGA WAKA

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 DEMAND

Improve overall security posture and save on SIEM costs.

CHALLENGE

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.

SOLUTIONS

- NXLog Enterprise Edition
- NXLog Agent Manager

BUSINESS RESULTS

- Security posture of IT/OT networks improved with unified and autonomous log collection pipeline
- 6-digit in savings reached on SIEM with events filtration powered by 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 aspect 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 sea port organization.

PROJECT & 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 Enterprise Edition has been planned to substitute 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 amount of events collected from endpoints make sense for security operations, while the others are just to pose a significant impact on overall SIEM performance and its 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 events forwarded to SIEM. To achieve that, an extensive filtration policy has been applied with NXLog, 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 helped to simplify log collection routines significantly and, being initially managed by security service provider, NXLog installation has been smoothly handed over to Ports of Auckland team.

> *"NXLog Community Edition was considered for PoC phase and finally NXLog Enterprise Edition has been chosen for production deployment because of its manageability and scalability."*
>
> ***- Lajos Varga, Head of Digital Technology, Ports of Auckland***

> *"NXLog allowed us to address technical challenges as the solution is non-blocking and most importantly supports native integration with our SIEM solution, so it was required for successful project implementation"*
>
> ***- Lajos Varga summarized -***
>
> *"One of the strong points of NXLog Enterprise Edition to highlight is its configuration granularity and filtration abilities that allowed us to ingest only valuable events resulting in expenditure saving on EPS volume."*

SOLUTIONS

NXLog Enterprise Edition

NXLog Manager

NXLog Add-Ons

REQUEST A FREE TRIAL

*For more information on NXLog visit our **website** , checkout our **integrations' page** or **schedule a meeting** with one of our representatives*