NXLog

NXLOG HELPS ALTICE PORTUGAL TO IMPROVE SOC PERFORMANCE AND SECURITY POSTURE

CUSTOMER CASE STUDY

NXLOG HELPS ALTICE PORTUGAL TO IMPROVE SOC PERFORMANCE AND SECURITY POSTURE.

Altice Portugal (former Portugal Telecom) is the largest telco in Portugal.

Altice Portugal is a subsidiary of Altice Group — a multinational cable and telecom company headquartered in Luxembourg, with a presence in France, Israel, Belgium & Luxembourg, Portugal, the French West Indies/ Indian Ocean Area, and the Dominican Republic.

Altice Group is a convergent leader in telecoms, content & media, entertainment, and advertising, with €5,029 million in revenue as of 2022.

FIXED INDUSTRIES

- Fixed line services
- Mobile 4G/5G communications
- Media, Entertainment & Advertising

BUSINESS DEMAND

Improve security posture of internal infrastructure, SOC performance, and reliability.

CHALLENGE

Implement agentless log collection to get events centralized into SIEM. Apply extensive pre-filtration of events to boost real-time threat detection. Ensure complete log retention for all the critical systems.

SOLUTIONS

- NXLog Enterprise Edition
- NXLog Agent Manager

BUSINESS RESULTS

- A cost-efficient agentless log collection pipeline has been built.
- Security posture improved with broader log collection coverage, and SOC performance/reliability increased.

BACKGROUND

Telecommunication companies operate highly sophisticated IT systems to provide customers with modern services and handle customer’s data. That makes them susceptible to various threats and a high-value target for cybercriminals. Compared to other enterprises, telecoms experience a wide range of attacks, from assaulting mobile infrastructure, hacking into customer accounts, and stealing customer data to disrupting services with DDoS and ransomware attacks.

Data is an essential and critical asset for Altice Group’s business, so it needs appropriate protection. The operational management of cybersecurity is carried out by an information security team from Altice Portugal, accredited by the TF-CSIRT Trusted Introducer (Europa-ENISA), which ensures the handling and coordination of computer security incidents and the dissemination of alerts. Internationally, Altice Portugal is part of the European CSIRT Network.

Information and Communication Technologies (ICT) security at Altice Portugal is ensured by implementing controls, including policies, processes, administrative procedures, software, and hardware. At Altice Portugal, audits are performed by internal and external auditors and via technical vulnerability assessment. All exposed external sites are subject to third-party penetration testing in case of a major change. External audits include ISO 27001 certification and compliance with ANACOM (national telecom sector regulation body). Internal audits include NIS1, and compliance of IT controls in the scope of the annual financial report audit, among others.

CHALLENGES & SOLUTION

According to ISO/IEC 27002:2013 – "Information Technology/Security Techniques – Code of practice for information security controls", section 12.4 "Logging and monitoring", it's necessary to establish procedures and controls to detect illegitimate entries, authentication failures, and privileges escalation; to ensure that sufficient evidence exists if any incident occurs; to define regular behavior models that allow detecting anomalous scenarios.

In line with the enterprise security policy, the most critical systems and technologies, DMZs, security devices, and network elements, must be under non-stop events monitoring by Altice Portugal Security Operations Center (SOC). Legacy log collection tools couldn't get data from certain critical sources, keeping systems in gray security areas. Also, with the old log collection solution, some sources, like domain controllers, posed performance challenges for SIEM, flooding it with excessive events.

NXLog offers flexible deployment architectures, and it was decided to implement agentless log collectors to pull events from different sources, including Windows endpoints and network appliances. It was then mandatory to forward events to multiple destinations – for real-time analysis and long-term retention. That task was easy to solve as NXLog supports a wide range of log destinations, including all the major SIEMs, like Google Chronicle, Microsoft Sentinel, IBM QRadar, Microfocus ArcSight, as well as popular solutions for log retention, including Elasticsearch, AWS, Graylog, Snowflake, and others.

Another challenge was pre-filtering critical events for the SIEM to keep its performance high for fast detection while ensuring all the logs captured reach the security platforms. NXLog has successfully solved this thanks to its potent parsing capabilities, which help filter events and normalize them before sending them to their destinations. Also, the engineers configured NXLog's local caching feature to ensure all the logs reach security systems as soon as possible.

> *"To build a new robust event collection pipeline, NXLog Enterprise Edition has been chosen over competitors, because of its lightweight, wide support of events sources, integration, and event parsing capabilities".*
>
> ***- Jorge Silva, Manager of CyberSecurity Architecture & Engineering***

> *"At Altice Portugal, the biggest Telco operating in the country, we were limited with getting some security logs to our SOC platforms.*
> *However, with the migration to NXLog Enterprise Edition, we are able now to get all security events for analysis, in a fast, resilient and reliable way.*
> *We are very pleased with the product capabilities, its support for various log types, and NXLog customer service timely providing solutions".*
>
> ***- Jorge Silva concludes***

SOLUTIONS

NXLog Enterprise Edition

NXLog Manager

NXLog Add-Ons

REQUEST A FREE TRIAL

*Visit our **website** to learn more about our products or get in touch with one of our dedicated representatives. should just say ‘get in touch’.*

Contact us: **nxlog.co** YouTube LinkedIn Twitter