NXLog

NXLog Platform Helps Altice Portugal to Improve SOC Performance

altice

NXLog Platform Helps Altice Portugal to Improve SOC Performance

CUSTOMER PROFILE

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 over €5,000 million in revenue as of 2022.

RELATED INDUSTRIES

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

BUSINESS DEMANDS

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

CHALLENGES

Centralize security events from variety of sources and apply extensive pre-filtration events policy to boost real-time threat detection. Ensure complete log retention for all the critical systems.

SOLUTION

- NXLog Platform
- NXLog Professional Services

BUSINESS RESULTS

SOC performance and reliability increased with implementing cost-efficient agentless telemetry pipeline by NXLog for security log collection. Security posture improved with broader log collection coverage and centralized data retention.

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.

SOLUTION

According to ISO/IEC 27002:2013 – “Information Technology/Security Techniques – Code of Practice for Information Security Controls,” section 12.4 on “Logging and Monitoring,” organizations must establish procedures and controls to detect unauthorized access attempts, authentication failures, and privilege escalation. These measures are critical to ensuring sufficient evidence is available in the event of an incident. Additionally, the standard emphasizes the importance of defining baseline behavior models to enable the detection of anomalous scenarios effectively.

Under the enterprise security policy, Altice Portugal's Security Operations Center (SOC) is required to ensure uninterrupted event monitoring across critical systems and technologies, including the DMZ, security devices, and network elements. However, legacy log collection tools fell short, failing to retrieve data from certain key sources and leaving systems vulnerable to potential security gaps. Moreover, the outdated solution faced significant performance challenges, particularly with data sources like domain controllers, which inundated the SIEM with an overwhelming volume of events, hindering its efficiency.

The NXLog Platform provides a flexible telemetry pipeline architecture, enabling the implementation of agentless log collectors to retrieve events from diverse sources, such as Windows endpoints and network appliances. It was essential to forward these events to multiple destinations for real-time analysis and long-term retention. This requirement was seamlessly addressed, as NXLog supports a wide range of log destinations, including major SIEM platforms like Google Chronicle, Microsoft Sentinel, Elastic, Graylog, IBM QRadar, and Microfocus ArcSight. Additionally, it integrates with popular log retention solutions, such as its embedded storage and search engine, AWS, Azure, and Snowflake.

Another challenge was pre-filtering critical events for the SIEM to maintain optimal performance and enable rapid threat detection, all while ensuring that every captured log reached the security platforms. NXLog addressed this challenge effectively with its powerful parsing capabilities, enabling event filtering and normalization before forwarding them to their destinations. Additionally, engineers utilized local caching feature of NXLog agent to ensure that all logs were reliably delivered to the security systems without delay.

To build a new robust event collection pipeline, NXLog has been chosen over competitors, because of its lightweight, wide support of events sources, integration, and event parsing capabilities.

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 telemetry pipeline, 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,
Manager of Cybersecurity
Architecture & Engineering

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!