NOESIS

USE CASE

Enhancing Threat Detection and Response Across Critical Transportation Infrastructure

When a Transport and Logistic Operator moving over 145 million passengers a year needed to strengthen its cybersecurity, they turned to Noesis to help build a smarter, faster approach to detecting and responding to threats. The result was real-time visibility, faster incident response, and a noticeable step forward in infrastructure maturity.

Sector | Logistics & Transportation

Delivery Unit | IT Operations, Cloud & Security

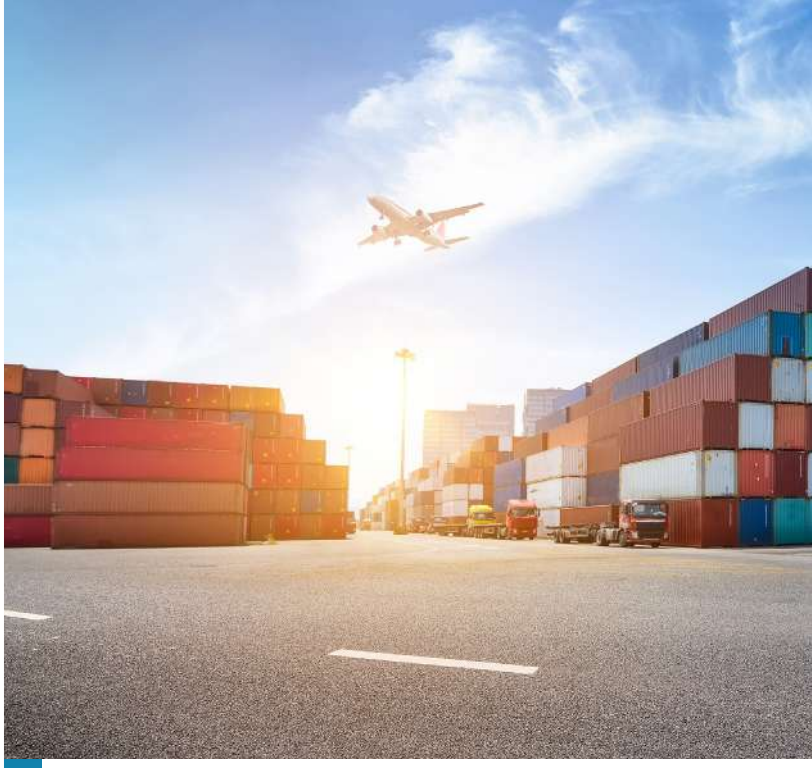
Solution | Network & Cybersecurity Assessment Services

145
Million passengers

+/- 4,000
Employees

+/- 175M
Daily System Events

400+
Offices & Kiosks



THE CHALLENGE

The organization struggled to anticipate emerging cyber threats, and its cybersecurity team faced multiple challenges:

- Security events (IT and IoT) were hard to detect in real time with little visibility and contextualization (Users, Assets, and IoC).
- Abnormal behavior from users and devices often went unnoticed.
- Alert fatigue made it difficult to separate real threats from false alarms.
- Critical systems weren't consistently monitored in a centralized way.
- Time lost between detection and response left gaps in protection.
- High number of legacy systems and use of 'Shadow" IT solutions.
- Patch management and vulnerability management programs not effective.

GOALS

- Collect and correlate security data from multiple sources (firewalls, proxies, DNS, Office 365, DHCP, DNS, domain controllers, and other).
- Design and implementation of efficient Threat Monitoring and Incident Handling processes.
- Bring threat intelligence into the detection process to improve accuracy.
- Monitor activity at the network perimeter and stop threats from spreading .
- Strengthen endpoint protection and response across the IT and IoT environment (automatic containment where possible).
- Behavioral monitoring of users (UEBA), in order to identify and respond to standard deviations (e.g., the user is performing unusual actions).

SOLUTION

Noesis worked closely with the organization to put a layered cybersecurity system in place - one that connected tools, intelligence, and processes into a unified approach.

- Opentext ArcSight ESM (SIEM) provided centralized event correlation and helped analysts detect anomalies with more context.
- Darktrace Immune System and Antigena brought real-time monitoring and AI-based response, learning the behavior of users and devices to stop threats early.
- Sophos Intercept X Advanced (EDR) gave IT teams visibility at the endpoint and tools to remotely isolate or remediate threats.
- Opentext Fortify (SAST and DAST) helped uncover vulnerabilities in both development and live web applications.
- SealPath IRM protected sensitive documents by limiting who could access or share them.
- Noesis also supported the design and rollout of SOC processes, helping teams move from reactive firefighting to structured incident

RESULTS

The team saw meaningful improvements in how quickly and effectively they could manage cyber risks.

- Security events that used to go unnoticed were now caught in real time.
- AI tools significantly reduced noise from false positives by learning what normal activity looked like and automatically
- Threats were stopped at the perimeter before they could spread internally.
- Infrastructure maturity improved, giving leadership greater confidence in their systems.
- Response times dropped as SOC workflows became more structured and repeatable.

NOESIS

Noesis is an international tech consulting company with 30 years of experience, delivering solutions to drive digital transformation and support business growth. It offers a wide portfolio of IT services, including areas such as IT Ops & Infrastructure, Cloud & Security, Enterprise Solutions, Low-Code Solutions, Data Analytics & AI, DevOps & Automation, Quality Management, Enterprise Application Integration, and Professional Services.

With more than 1.300 highly qualified talents, Noesis operates in eight countries: Portugal, Spain, the Netherlands, Ireland, the United Kingdom, Brazil, the USA, and the United Arab Emirates. As part of the Altia Group, listed on the Spanish stock exchange BME Growth, the company integrates a network of more than 4000 professionals, with operations in nine countries and a presence in more than 30 locations.