NOESIS

USE CASE

Cybersecurity strategy design and implementation services

As a leading international provider of packaging, components, and insulation solutions in over 35 countries, with a strong aptitude for growth through acquisitions, the company must identify and mitigate cybersecurity risks as quickly as possible to avoid or reduce the impact on the business and brand. These risks include operational outages, system unavailability, loss of sensitive data, and even industrial espionage.

Sector | Packaging, Components and Insulation Solutions

Delivery Unit | IT Operations, Cloud & Security

Solution | Cybersecurity Services

104
Facilities/Sites

+3,000
Users

30
Acquired companies

28
Noesis Team

THE CHALLENGE

The organization has experienced sustained growth by entering new markets and introducing new products through various mergers and acquisitions. This growth has introduced key cybersecurity challenges.

- Inconsistent cybersecurity maturity levels, processes, and technologies across acquired companies with minimal standardization.
- A significant footprint of legacy, non-enterprise, and unsupported systems and platforms alongside widespread use of shadow IT solutions, hindering poor exposure assessments.
- Distributed teams and third-party partners operating across multiple geographic regions complicate unified security governance and coordination.
- Abnormal user and device behavior often goes undetected due to limited visibility and a lack of baseline activity profiling.
- Limited visibility and poor contextualization of security events across users, assets, and IoC hindering real-time detection and containment across both IT and IoT environments.
- Ineffective asset inventory, endpoint management and protection (EDR/XDR), server security, user access management, email and browser security, patch management, and vulnerability management programs, due to outdated or missing procedures and insufficient technology.
- Reliance on insecure authentication protocols (such as NTLMv1) and outdated communication protocols (e.g., HTTP, FTP, SMB1, and Telnet), increases exposure to attacks.

GOALS

- Achieve comprehensive visibility across the ecosystem by centralizing, aggregating, correlating, and prioritizing security events from multiple sources, including firewalls, proxies, VPN, DHCP, DNS, Office 365, domain controllers, XDR, and others.
- Design and implement security guidelines and policies covering critical areas such as remote user access, vulnerability management, threat monitoring, and incident response.
- Enhance endpoint protection and response capabilities across both IT and OT environments, enabling automatic containment of threats wherever feasible.
- Strengthen perimeter monitoring to detect and block threats early, through automatic threat containment measures where possible.
- Implement user and entity behavior analytics (UEBA) to continuously monitor user activities and detect deviations from normal behavior for timely response.

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.

- Cybersecurity assessment for the different domains (Workplace, Datacenter, Network and corporate/collaborative applications) and cybersecurity verticals, guided by the CIS framework. The first assessment considered implementation group 1 (Essential cyber hygiene) and annual assessments are now conducted to evaluate the implementation of previous recommendations and identify new initiatives to increase maturity and reduce exposure.
- Implementation of quick wins to reduce the organization's cyber exposure (password policies, configuration of MFA, configuration of DMARC and DKIM in the e-mail solution, OS updates for workplace devices, User Onboarding and Offboarding processes standardization, configuration of Microsoft Defender for Office 365 security capabilities) as well as business continuity measures (O365 backup, Active Directory backup, Disaster Recovery plan and DR testing in critical environments).
- Strategy to strengthen security and monitor remote access points to the organization's resources, reducing reliance on vulnerable shadow IT solutions.
- Strategy to improve security on "Internet-exposed systems and devices".
- Implementation of Darktrace Immune System and Antigena, delivering real-time monitoring and AI-based response, learning the behavior of users and devices to stop threats early.
- Implementation of Microsoft Defender for Endpoint, providing IT teams with endpoint visibility and tools to remotely isolate or remediate threats.
- Support of the design and implementation of guidelines & procedures, ensuring visibility over all security events (Threat Monitoring) and a structured incident response process in order to "simplify" the response to critical incidents (war room, communication plan to customers, suppliers and authorities) and enrich it with the lessons learned from each response.
- Implementation of the SIEM solution (Securonix) in order to centralise security events from the different sources (Domain Controllers, VPN, DNS, DHCP, Firewall and others) with integrations identity directory, CMDB and CTI feeds in order to prioritize and contextualize events automatically.
- Design and implementation of a patch management and vulnerability management program. Vulnerability management is carried out using Tenable VM.
- Development and delivery of customized cybersecurity roadmaps and initiatives, adapted to the customer's context and evolving security needs.

RESULTS

The organization saw meaningful improvements in its cybersecurity posture, achieving faster detection, more effective response, and overall reduced risk exposure:

- Previously undetected security events, such as unauthorized access attempts and suspicious operations, are now detected and mitigated in real time.
- AI tools significantly reduced false positives by learning normal user and device behavior, automating the blocking of suspicious/malicious activity and improving SOC efficiency.
- Threats are now intercepted at the perimeter, preventing lateral movement and internal spread.
- Cybersecurity maturity has improved steadily through ongoing assessments and structured initiatives, leading to reduced exposure.
- Incident response times have decreased significantly as SOC workflows were formalized and standardized, enabling a more agile and consistent reaction to security incidents.
- Visibility and control over endpoints, networks, and cloud environments has increased, supporting threat hunting and faster remediation.
- Cybersecurity roadmap ensures continuous alignment with evolving business needs and emerging threats, aiding in strategic decision-making.

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.