Cyber Exposure Management

logi-tech CYBERSECURITY

Do you have total confidence in your digital attack surface?

In today's smart facilities, your network is more than laptops and servers - it includes cameras, smart lighting, HVAC systems, and even the machinery on your production floor. Most traditional security tools only see a portion of these devices, leaving significant visibility gaps across unmanaged IoT, IIoT, and legacy OT assets.

Logi-Tech partners with Armis to deliver Armis Centrix™, a leading cyber exposure management platform that acts as an always-on digital security guard that never blinks.

Armis + Logi-Tech: The digital "eyes" on your entire network - IT, OT, and everything in between, so you can operate safely, efficiently, and with complete peace of mind.

ARMIS

Complete Visibility, Total Confidence

Think of Armis as an always-on digital security guard that never blinks. It automatically discovers every device on your network, knows exactly what it is, and immediately alerts you if something starts acting suspicious. Whether it's a contractor's tablet or a critical industrial machine, if it's connected, Armis is watching.

No blind spots, no guessing - just total confidence that your facility is protected.

Technical

With the convergence of IT and OT networks, traditional agent-based security solutions leave significant visibility gaps, particularly across unmanaged IoT, IIoT, and legacy OT assets. Armis, delivered through Logi-Tech, provides a passive, agentless platform that closes this gap by monitoring network traffic at the packet level and identifying devices by their unique behavioral signatures. Its global database tracks over 4 billion devices, enabling real-time detection and threat prevention.

Key Capabilities

- **100% Passive Monitoring:** Operates out-of-band to avoid disrupting sensitive OT equipment or PLCs.
- **Real-Time Asset Inventory:** Automatically generates a complete hardware and software inventory, including shadow and unauthorized assets.
- **Vulnerability & Risk Scoring:** Correlates device activity with CVEs and proprietary threat intelligence, prioritizing the highest risks first.
- **Automated Policy Enforcement:** Integrates with firewalls, NAC, or SIEMs to trigger quarantine or segmentation when a device violates security policies.
- **Essential Eight Gap Analysis:** Identifies unmanaged devices and enforces compliance with frameworks like the Essential Eight, including restricting administrative privileges and patching applications.

Streamline Cybersecurity Operations with Armis Centrix™, Cyber Exposure Management Platform

Armis Centrix™ is a leading cyber exposure management platform that delivers real-time visibility, risk assessment, and proactive protection of your entire digital attack surface. Powered by the Armis.

AI-driven Asset Intelligence Engine, it continuously discovers, monitors and secures every asset—including IT, OT, IoT, and IoMT devices—across complex environments. With automated risk scoring, vulnerability detection, and dynamic network segmentation, Armis Centrix helps organizations minimize cyber risk, enforce security policies, and remediate threats before they impact business operations.

This cloud-native, frictionless platform is designed to reduce your cyber exposure, streamline compliance reporting, and accelerate incident response with AI-powered asset intelligence and threat mitigation at scale.

sales@logitech.com.au | 61+ (08) 8152 4000 | logitech.com.au