Auxis Builds Cybersecurity Operations from Scratch for **Global Aviation Leader**, Reducing Incidents by 30%

Client Profile

Our client, headquartered in Europe, is a global leader in the management and maintenance of Unit Load Device (ULD) containers and pallets for the aviation industry. The company operates in a highly distributed and regulated environment, with more than 800 employees across 40 locations and 550 airport partnerships.

Business Challenge

Setting up a robust cyber defense for carved-out aviation enterprise

Cybersecurity stands as the top business risk for the fourth consecutive year. In the aviation industry alone, cyberattacks surged 131% in just 12 months as growing reliance on digital infrastructure — combined with aging technology — created a prime opportunity for sophisticated threat actors to target high-value data and assets.

Overall, businesses confronted an average of 1,900+ weekly attacks in Q1 2025, a nearly 50% increase year-over-year. (Check Point's 2025 Global Cyber Attack report). The average cost of a data breach for U.S. enterprises: $9.36 million – the highest of any country (IBM's Cost of a Data Breach Report 2024).

Nearly 60% of data breaches are triggered by third-party risk, and pressure is mounting from airlines and global regulatory agencies for industry vendors like the client to strengthen their cybersecurity posture. When a change of ownership required the client to separate its IT infrastructure and processes from its former parent company, establishing a robust security strategy topped the priorities list.

To complete the carve out, the client was looking for an IT outsourcing provider who could serve as a true strategic partner, bringing greater flexibility, optimized processes, and nearshore advantages like similar time zones and cultural affinity that solved the challenges it had previously experienced outsourcing IT to Asia.

Auxis, a Latin America outsourcing pioneer with nearly 30 years of business and IT transformation experience, was hired to lead the client's IT carve out and set up its IT infrastructure, security processes, and security tools from scratch.

Key challenges included:

- **Establishing a strong cloud infrastructure** to support the client's users and business applications with the proper security mindset.
- **Creating strong security processes** from the ground up driven by best practices and the unique requirements of the aviation industry.
- **Choosing and implementing the best cybersecurity tools** for the organization in a crowded market of options.
- **Overcoming cybersecurity labor shortages in the U.S.** to build a dedicated security team capable of performing proactive, 24/7 monitoring and threat response.
- **The client's highly distributed operating conditions challenged protection,** including a global footprint spanning multiple time zones and airport locations bringing network complexities and limited connectivity.
- **A hybrid environment** combining legacy and modernized infrastructure further increased vulnerabilities.
- **Need for automation, visibility into security performance, and staff training** to keep pace with fast-changing threats.

As part of the carve out, Auxis was tapped to provide ongoing IT managed services across security, infrastructure management, and help desk support. Essential to its managed security service provider (MSSP) role: ensuring security tools and processes continuously adapt to the increasingly sophisticated landscape of cyberthreats.

Solution & Approach

Building a Security Operations Center infused with AI innovation in LATAM

With extensive experience delivering IT operations built on best practices and deep managed security service provider expertise, Auxis brought a highly collaborative and consultative approach to creating the client's security operations. The result: a comprehensive managed Security Operations Center (SOC) infused with AI innovation that ensures long-term resilience against cyber-risks.

Auxis came to the table with proprietary AI and automation solutions, partnerships with best-in-class technology providers, and a nearshore delivery model that offers access to top-tier, certified security talent at a fraction of U.S. costs. Unlike managed service providers who are just technical experts, Auxis also takes a business-led approach to IT transformation that ensures process optimization and an operational strategy aligned to business goals.

Today, Auxis provides 24/7 managed SOC services for the client that continuously adapt to a fast-evolving cybersecurity landscape. Monthly meetings assess and recommend action for plugging security gaps as new threats emerge. Auxis also stays up to date with the latest security advancements, providing agnostic recommendations for leveraging new technologies as needed: for instance, upgrading the client's malware protection to a modernized Extended Detection and Response (XDR) as a Service operation.

With complete visibility across the client's IT infrastructure and cybersecurity environment, Auxis' managed services team is uniquely positioned to resolve issues faster and coordinate security more effectively than providers limited to a single service area.

This holistic approach not only ensures stronger protection but also aligns with broader industry trends: cybersecurity emerged as the #1 business function outsourced in 2024, with 77% of organizations outsourcing cybersecurity to third-party partners (Deloitte Global Outsourcing Survey 2024).

Auxis' managed security services solution includes:

1 Standing up a turnkey outsourced Security Operations Center (SOC)

With extensive experience serving as a managed security service provider for clients across industries at its Global Delivery Centers in Latin America, Auxis was able to quickly stand up a turnkey SOC operation infused with best practices; next-gen, AI-powered technologies; and optimized processes tailored to the client's specific business and industry needs. Auxis performs 24/7 security monitoring, threat detection, and rapid response across the client's global operations, ensuring full visibility and hyper-focus across systems, devices, and locations.

Auxis' nearshore delivery model further helped the client overcome the cybersecurity labor shortages that have caused salaries to surge in the U.S., providing instant access to a cost-effective team of certified and experienced professionals in Costa Rica and Colombia that function as a seamless extension of its IT team.

Latin America ranks as the #1 up-and-coming market for tech talent globally on CBRE's Scoring Tech Talent 2024 report, merging deep pools of skilled talent with the real-time collaboration, smooth communication, and cultural alignment needed to swiftly address and resolve urgent security issues.

In fact, IT services are now successfully delivered by 64% of shared services in Latin America, compared to 32% of shared services globally (2024 State of the GBS and Outsourcing Industry in Latin America report by SSON Research & Analytics and Auxis).

2 Implementing Extended Detection and Response (XDR) as a Service

Roughly 90% of successful cyberattacks and 70% of successful data breaches originate at endpoint devices, states the latest Verizon Mobile Security Index report. Auxis' XDR as a Service solution leverages **marketing-leading SentinelOne, Microsoft Sentinel, and other technologies** to help the client detect and contain endpoint threats, while Auxis' security experts perform operational overhead.

For this client, Auxis recommended the SentinelOne XDR solution to replace the client's traditional malware protection, recognizing its greater and more holistic capabilities. XDR not only focuses on detecting known malware signatures like traditional antivirus but also looks at broader patterns of behavior and data across systems. The SentinelOne technology further minimizes business impact with rapid, automated threat response, such as isolating infected machines without manual intervention. The result: a more comprehensive view of potential threats and a faster, more effective response.

Delivered as a turnkey solution to the client, Auxis handled everything from licensing and implementation of the SentinelOne technology to 24/7 monitoring and real-time alert response. The managed security operations center solution provides coverage across hundreds of endpoints ranging from workstations to mobile units, ensuring every device on the client's network is protected.

3 Strengthening the client's security posture with an advanced security toolset

Maintaining state-of-the-art cybersecurity infrastructure that can keep pace with today's security threats requires significant and ongoing investment in both hardware and software.

Auxis solved this problem by offering the flexibility to integrate with the aviation company's existing tools while also bringing its own suite of advanced cybersecurity solutions - enabling the client to access enterprise-grade and cutting-edge technology solutions that were costly and complex to implement on its own.

Key solutions include:

- **Multi-Factor Authentication (MFA) via Cisco DUO:** This adds a second layer of login verification, like a mobile push notification, making it significantly harder for attackers to access accounts.
- **Email filtering with Proofpoint:** Implemented to protect inboxes by identifying and blocking phishing, spam, and malware-laden messages before they reach users.
- **Web content filtering using Cisco Umbrella:** Auxis set this up for the client to block access to malicious or inappropriate websites, adding an additional layer of browsing protection.
- **Intrusion detection and log monitoring with Alert Logic:** Provided by Auxis to monitor server activity, identifying and flagging abnormal behavior that could indicate a security breach.
- **Security Awareness Training through KnowBe4:** Conducted for client employees, educating users on how to spot and avoid phishing scams and other common attacks.

4 Leveraging automation and AI SOC technology to rapidly respond to cyberthreats

With 75% of security professionals having to adjust their cybersecurity strategy in the past year due to the surge in AI-powered threats, automation holds the key to rapid identification and response. Organizations that leverage AI and automation extensively for proactive prevention experience 46% lower costs from a data breach than those that do not, IBM's Cost of a Data Breach report found.

Auxis leverages automated workflows that triage alerts, enrich data with contextual information, and take predefined response actions — such as isolating devices or blocking IP addresses —without human intervention. This not only reduces alert fatigue for analysts but also accelerates response times and improves overall threat detection and management efficiency.

A 2024 Vectra AI survey found that IT staff are overwhelmed by an average of 3,800+ security alerts per day – causing 62% to be ignored due to excessive workload and inefficiencies in security tools. By leveraging automation, Auxis ensures genuine threats are not missed amid the noise.

Key AI and automation solutions include:

> **Auxis deploys critical automation SOC technologies** to significantly reduce the volume of alerts, streamline investigations, and ensure rapid response, including Security Information and Event Management (SIEM), Extended Detection and Response (XDR), and Security Orchestration, Automation, and Response (SOAR) platforms. These tools use predefined rules, threat intelligence, and machine learning to filter out false positives and correlate events across multiple systems, helping to prioritize and respond quickly to real threats.

> **Auxis developed proprietary AI-powered automation to enhance the capabilities of security tools.** That includes AI automation capable of pre-screening phishing and monitoring alerts, allowing SOC analysts to triage and respond to threats more quickly and accurately. Auxis also built an AI chatbot to automate the creation and routing of tickets and speed issue resolution.

Results

Partnering with a top MSSP SOC leads to a scalable, future-ready security operation

Auxis built a mature, security-first organization for the global aviation enterprise from the ground up, complete with optimized processes, a dedicated managed security operation center, best-in-class technology, and the flexibility to quickly adapt to today's fast-evolving threats. Auxis' managed security services continue to exceed the client's expectations across threat response, operational efficiency, and user satisfaction.

Key results include:

99.9% SLAs & 96% customer satisfaction

With security SLAs and customer satisfaction scores **surpassing client targets,** the global aviation leader benefits from proactive protection in an increasingly complex threat environment **– freeing internal IT resources to focus on innovation and strategy.** Regular monthly service reviews provide **clear visibility** into security performance metrics, identifying **continuous improvement** opportunities.

90% automated analysis of suspicious emails

Auxis' proprietary automation can assess 90% of reported emails, taking **12 seconds to perform analysis** that previously took security analysts about 17 minutes per email. This greatly accelerates timelines for investigating and responding to phishing reports. The bot's **accuracy is currently 85%** and that continues to increase as AI machine learning helps it learn.

56% alert automation

With automation managing more than half of alerts and filtering false positives, Auxis' MSSP team can focus on priority issues and problem management instead of reactive monitoring **– ensuring critical incidents don't slip through the cracks.**

30% reduction in security ticket volumes

The combination of dedicated resources, proactive monitoring, improved security systems, and advanced security tools have reduced the client's ticket volumes by about 30% since the start of the managed security services provider partnership with Auxis. The client has also seen a **significant drop in outages and false positives** due to automation, next-gen monitoring, and streamlined triage.

24/7 protection across time zones

Unlike internal IT teams working fixed schedules and juggling multiple responsibilities, the Auxis managed security operation center focuses on cybersecurity 24 hours a day, 7 days a week, 365 days a year. This constant vigilance ensures **potential threats are detected and addressed in real-time,** minimizing the window of opportunity for attackers and reducing the potential impact of security incidents. Auxis' solution supports the client's locations **across 24 countries,** including coordination with users in Asia, Europe, and North America.

30-50% cost savings

Nearshoring to Latin America achieves average labor cost savings of 30-50% compared to hiring similar resources in the U.S. while overcoming the severe shortage of top-tier cybersecurity professionals in the U.S. Partnering with Auxis as its managed security service provider further **eliminated the overhead of recruitment, training, and retention** that plague in-house operations. With automation and other optimizations, Auxis has also been able to expand device coverage for the client without a proportionate increase to costs.

Scalability & flexibility

With a deep bench of security talent and standardized processes, the Auxis SOC enables the client to **easily adjust security resources and services up or down** based on evolving needs. Auxis also stands out in the cybersecurity market with the flexibility to tailor services to the client's unique business and industry needs, **continuously adapting its services to today's emerging threats.** As security demands continue to evolve, Auxis stands ready to help the organizations scale smarter, stay compliant, and operate with confidence around the world.