AUJAS CYBERSECURITY
A NuSummit Company

aujas.com

SUCCESS STORY

Secure at Scale: A Manufacturing Leader's Cybersecurity Transformation

SECURITY VERIFICATION SERVICES

aujas.com

Business Need

The client is a leading name in the manufacturing sector, specializing in energy and environmental engineering solutions, with an annual revenue of ₹10,389 crore or approximately $1.25 billion USD for FY 2024–25. Operating in a hybrid cloud environment, the company faced increasing cybersecurity risks threatening its operational resilience and industry reputation.

To mitigate these risks proactively, the client aimed to strengthen its cybersecurity framework through continuous 24×7 SOC monitoring, robust vulnerability management, and enhanced application security practices. Before engagement, the company lacked mature incident response capabilities and was vulnerable due to limited investigation and oversight of security alerts.

Business Challenges

Multiple inefficiencies and systemic gaps affected the client's cybersecurity operations, including:

Limited Asset Coverage

Not all assets were integrated with the legacy SIEM (ArcSight), making the enterprise prone to cyberattacks.

Inadequate Monitoring

Existing dark web surveillance was limited to 8×5 support, risking a delayed response to critical data leaks.

Operational Gaps

Internal audits flagged key weaknesses in monitoring and asset coverage.

Urgency of Migration

A 60-day window was mandated to complete migration from the existing SIEM before offboarding.

Manual Processes and Alert Fatigue

Security alerts were not being investigated in detail, and key alerts were missed due to high volumes and a lack of actionable context.

Legacy solutions—including Arcsight SIEM and Cyble Dark Web monitoring—lacked advanced analytics, detailed investigation workflows, and full-time operational coverage, necessitating a rapid and robust transformation.

Solution Implementation

Aujas Cybersecurity implemented a full-stack cybersecurity operations solution anchored by QRadar SIEM to address these urgent needs. The transformation was structured across four critical phases: Kickoff and Information Gathering, SIEM Implementation and Log Source Integration, Use Case Validation and SOAR Enablement, and Operational Transition.

This phased approach ensured rapid, scalable deployment aligned with the client's security and compliance objectives.

Key Capabilities Delivered

As part of the engagement, Aujas Cybersecurity delivered the following key capabilities to enhance the client's detection, visibility, and response posture:

Advanced Detection Coverage

Over 400 custom use cases were developed, achieving 89% coverage of the MITRE ATT&CK framework tailored to the client's environment.

Asset-Wide Integration

All servers listed in the asset inventory were onboarded to SIEM, ensuring 100% monitoring coverage.

Custom Integration Engineering

Seamlessly ingesting logs from ERP systems and proprietary applications via custom parsers.

24×7 Monitoring

Aujas Cybersecurity extended Cyble dark web monitoring to 24×7, in collaboration with the client's internal teams, improving alert response times.

The implementation required coordination between Aujas Cybersecurity engineers and the client's InfoSec, Infrastructure (Cloud and On-Prem), and Application teams. Challenges related to infrastructure alignment and complex application integrations were addressed through structured collaboration and regular working sessions

Business Impact

1

100% Server Coverage

Complete SIEM integration for all critical assets.

2

89% MITRE Technique Coverage

Robust threat detection aligned to leading cybersecurity frameworks.

3

Improved Detection & Response

In-depth investigations, proactive alerting, and better executive-level threat visibility.

4

Compliance Readiness

Enhanced audit and incident monitoring prepared the client for future compliance audits and security assessments.

5

Asset Visibility Gains

Discovery scans revealed unsupported devices and missing assets in inventory, prompting remediation and updates.

The client now benefits from a security foundation capable of responding to modern threats such as ransomware, phishing, and insider attacks, especially those affecting manufacturing-specific systems.

Differentiators

The client selected Aujas Cybersecurity over competing cybersecurity vendors based on several key strengths, including:

Comprehensive Services Portfolio

Covering SOC monitoring, threat hunting, vulnerability management, and application security.

Technical Proficiency

Deep expertise in custom parser creation, OOTB integrations, and resolving ERP-specific challenges.

Framework-Driven Delivery

MITRE ATT&CK-based case engineering and structured transition management.

Client-Validated Value

Stakeholders highlighted in-depth alert investigations and seamless integration with various devices and applications as key success factors.

Aujas Cybersecurity's detailed analytical approach and operational agility made it an ideal partner for navigating complex security challenges under time and resource constraints.

Conclusion

In under 60 days, Aujas Cybersecurity enabled the client to modernize its cybersecurity operations, transition from legacy tools, and achieve strategic objectives across visibility, compliance, and cyber resilience. The client is now equipped with a scalable, compliant, and threat-ready security infrastructure by leveraging contextual analytics, extended monitoring, and a framework-driven approach.

About Aujas Cybersecurity

Aujas Cybersecurity - A NuSummit Company, helps build and transform cybersecurity postures to enable businesses to mitigate risks. We are a pure-play cybersecurity services company with deep expertise in Identity and Access Management, Risk Advisory, Security Verification, Managed Detection and Response, and Security Engineering services. Our unique products and services help businesses build and transform security postures while mitigating risks. Our focus is to strengthen security resilience by minimizing the occurrence of attacks, threats, and risks so that you can drive change, innovate, and accelerate growth.

For more information, visit us at www.aujas.com or write to us at contact@aujas.com.

Cupertino I Dallas I Jersey City I Ottawa I Riyadh I Dubai I Mumbai I New Delhi I Bangalore

For more information, visit us at **aujas.com**

All trademarks, logos and brand names are the property of their respective owners. All company, product and service names used are for identification purposes only. Use of these names, trademarks and brands does not imply endorsement

Follow us at: