Case Study: Securing the Digital Backbone of Clean Industrial Heat

About the Customer

The customer is a pioneering energy technology company specializing in Electrified Thermal Energy Storage (ETES). Their flagship product, the Rondo Heat Battery, converts intermittent renewable electricity into continuous high-temperature heat, enabling industries to decarbonize processes traditionally reliant on fossil fuels. Operating across sectors like cement, chemicals, and textiles, the company collaborates with global partners to deliver zero-carbon industrial heat and power solutions.

The Challenge

As the company expanded its global footprint, several cybersecurity challenges emerged:

- Protecting proprietary technology and intellectual property from cyber-espionage and unauthorized access.
- Securing operational technology (OT) environments, including the Rondo Heat Battery systems deployed across various industrial sites.
- Ensuring the integrity and availability of cloud-based platforms used for remote monitoring and management of energy storage systems.
- Complying with international cybersecurity standards pertinent to the energy sector, such as NERC CIP and ISO 27001.
- Managing third-party risks associated with collaborations and integrations with industrial partners and suppliers.

Deception-Led Detection with Invinsense XDR+

- Deployed decoy systems and credentials mimicking critical components of the Rondo Heat Battery infrastructure.
- Detected and analyzed unauthorized access attempts, providing insights into potential threat actors and methodologies.
- Enhanced early detection capabilities, allowing for proactive threat mitigation.

Governance & Compliance with Invinsense GSOS

- Aligned cybersecurity practices with ISO 27001 and NERC CIP standards.
- Automated compliance reporting, reducing manual efforts and ensuring timely submissions.
- Established a centralized dashboard for real-time monitoring of compliance status and risk metrics.

CTEM in Action with Invinsense OXDR

CTEM Stage	Outcome
Scoping	Identified 850+ digital assets, including cloud platforms, OT devices, and partner integration points.
Discovery	Detected 45 vulnerabilities, including outdated firmware on OT devices and misconfigured cloud storage permissions.
Prioritization	Mapped 12 critical attack paths that could lead to unauthorized access to proprietary technology and operational systems.
Validation	Conducted simulated attacks to test the effectiveness of existing security controls and incident response procedures.
Mobilization	Implemented remediation measures, reducing the attack surface by 70% through patch management, access control enhancements, and network segmentation.

Executive Quote

"Implementing Invinsense has significantly enhanced our cybersecurity framework, ensuring the protection of our innovative technologies and the trust of our partners. Their comprehensive approach to threat detection and compliance has been instrumental in our continued growth and success."

— Chief Information Security Officer, Leading ETES Provider

Solutions Used

To address these challenges, the customer implemented the Invinsense cybersecurity platform:

- Invinsense XDR for comprehensive threat detection and response across IT and OT environments.
- Invinsense XDR+ to deploy deception technologies, creating decoy assets to detect and analyze unauthorized access attempts.
- Invinsense OXDR for Continuous Threat Exposure Management, simulating potential attack vectors and validating security controls.
- Invinsense GSOS to streamline governance, risk management, and compliance processes, ensuring adherence to industry standards.

Key Results

- 70% reduction in identified vulnerabilities within 60 days of implementation.
- Improved incident response times by 40%, enhancing the organization's ability to mitigate threats promptly.
- Achieved compliance with relevant industry cybersecurity standards, bolstering stakeholder confidence.
- Strengthened partnerships by demonstrating a robust cybersecurity posture to collaborators and clients.

Infopercept | INVINSENSE

About Infopercept - Infopercept is one of the fastest growing comprehensive cybersecurity companies in India, serving global clients. It provides platform led managed security services that covers all areas of cybersecurity, including defensive, offensive, detection and response, and security compliance. Infopercept has its own cybersecurity platform, 'Invinsense,' which integrates tools such as SIEM, SOAR, EDR, deception, offensive security, and compliance tools. Its cybersecurity and MDR services include dedicated teams of experts, ensuring that organizations have 24x7 cybersecurity operations support.

Imprint

Contact
sos@infopercept.com
www.infopercept.com/knowledge/casestudy