Powering Cybersecurity for a Critical Energy Infrastructure

About the Customer

The customer is a public sector energy utility specializing in power generation through both thermal and renewable sources. With operational facilities spread across multiple sites, including lignite-based thermal plants and solar energy parks, it plays a vital role in maintaining energy stability across industrial and residential zones. The organization also manages a range of digital assets for SCADA systems, smart grid integrations, procurement platforms, and administrative tools—all of which are integral to its operational continuity and regulatory commitments.

The Challenge

With its infrastructure designated as part of national critical information infrastructure (CII), the organization faced unique cybersecurity challenges:

Protecting operational technology (OT) systems such as SCADA, DCS, and PLC from cyber intrusions.	Securing real-time energy trading platforms and data exchanges with grid operators and regulators.	Ensuring availability and data integrity of monitoring systems at remote solar and thermal sites.
Mitigating the risks of phishing and credential abuse targeting plant operators and administrative staff.	Achieving compliance with national CII cybersecurity guidelines and energy sector-specific audits.	Managing vulnerabilities across hybrid IT-OT environments with minimal disruption to ongoing operations.

The convergence of IT and OT, combined with regulatory scrutiny, demanded an integrated, proactive cybersecurity posture.

Threat Deception with XDR+

Deception elements were deployed in key zones:

- Created decoy control servers in plant environments to detect unauthorized access attempts.
- Used honey credentials and fake VPN gateways to attract potential attackers and bots.
- Resulted in a 52% decrease in false-positive alerts and early detection of misconfigured vendor access.

Security Compliance Enablement with GSOS

GSOS enabled the team to:

- Align policies with CII protection guidelines for the power sector.
- Build an auditable control map with automated evidence collection across plant and HQ systems.
- Monitor real-time policy violations and report directly to compliance and executive teams.

CTEM in Action with Invinsense OXDR

CTEM Stage	Outcome
Scoping	Identified 3,800+ assets, including SCADA endpoints, plant control servers, vendor portals, and cloud admin dashboards.
Discovery	Detected 57 critical vulnerabilities, including outdated firmware in PLCs, default credentials, and exposed API keys.
Prioritization	Highlighted 22 vulnerabilities that could impact production uptime or expose plant controls.
Validation	Simulated threats in two test OT environments to validate lateral movement via old engineering workstations.
Mobilization	Achieved 92% patch closure in less than 25 business days through combined IT-OT remediation workflows.

Executive Quote

"In an industry where downtime is not an option, Invinsense has given us the confidence to run our energy operations securely. Their unified visibility across IT and OT has been a game changer."

– Head of IT & OT Security, Leading Public Sector Power Utility

Solutions Used

To address these sector-specific risks, the organization deployed the Invinsense platform:

- Invinsense XDR to monitor both IT and OT networks, ensuring centralized detection across SCADA systems, plant LANs, and cloud admin tools.
- Invinsense XDR+ to implement deception assets in OT zones and admin networks to trap lateral movement.
- Invinsense OXDR to continuously assess vulnerabilities across ICS devices, procurement applications, and third-party interfaces.
- Invinsense GSOS to operationalize and track cybersecurity policies aligned with national CII protection frameworks.

Key Results

- 92% remediation of critical vulnerabilities within 25 business days.
- 52% reduction in false positives via deception and context-aware detection.
- Full alignment with CII protection mandates and energy audit standards.
- Early detection of OT-specific threats including unauthorized remote access attempts.
- Strengthened resilience across hybrid infrastructure spanning plants and HQ systems.

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