CMS IT Services' transforms Managed Detection and Response with modern 24x7 security operations for Power Distribution giant

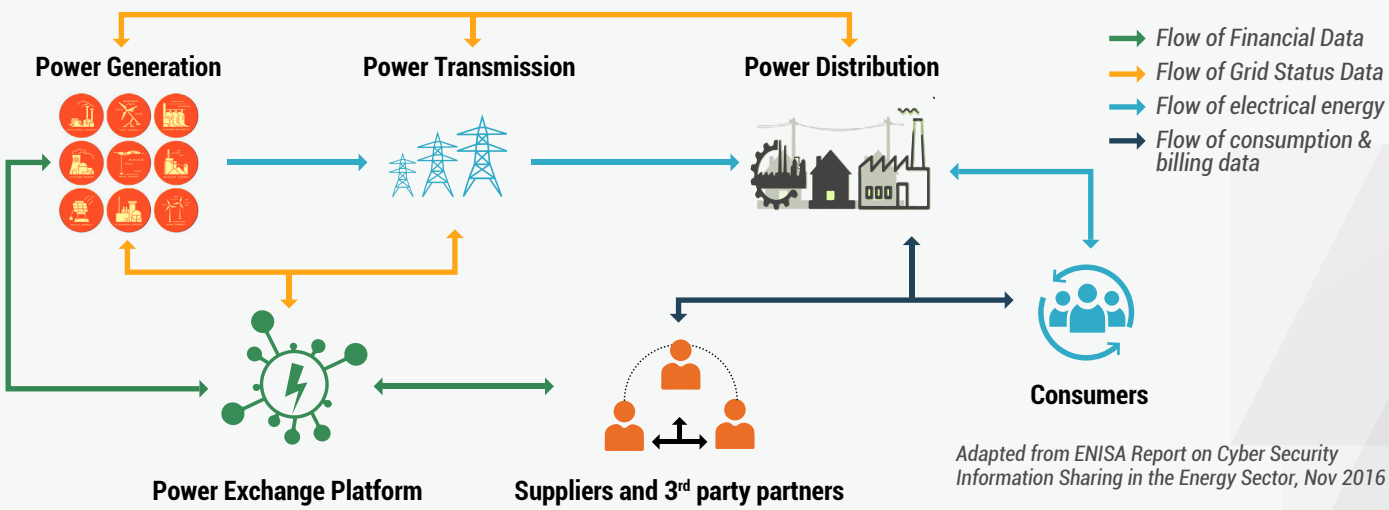
CUSTOMER

One of the largest power distribution corporations in India, the customer supplies power to more than 55 lakhs consumers per annum. They are part of the National Critical Information Infrastructure Protection Centre (NCIIPC) created under the provision of the Information Technology Act, 2000 by the Government of India. As part of their mission, to provide power supply to the consumers 24x365 and IT support to holding, generation, transmission, and trading companies, the customer has designed and implemented the latest holistic, comprehensive IT Security technologies integrated with defensible cybersecurity guidelines.

THE CHALLENGE

24x7 data privacy, critical system availability, and near real-time incident resolution are the cornerstones of Power Distribution companies. They are deeply linked with the other four primary national critical information infrastructures viz. banking, financial institutions and insurance, information and communication technology, transportation, and e-governance and strategic public enterprises.

The critical data flow between the various power generation, transmission, and distribution agencies connected with the customer are as follows:



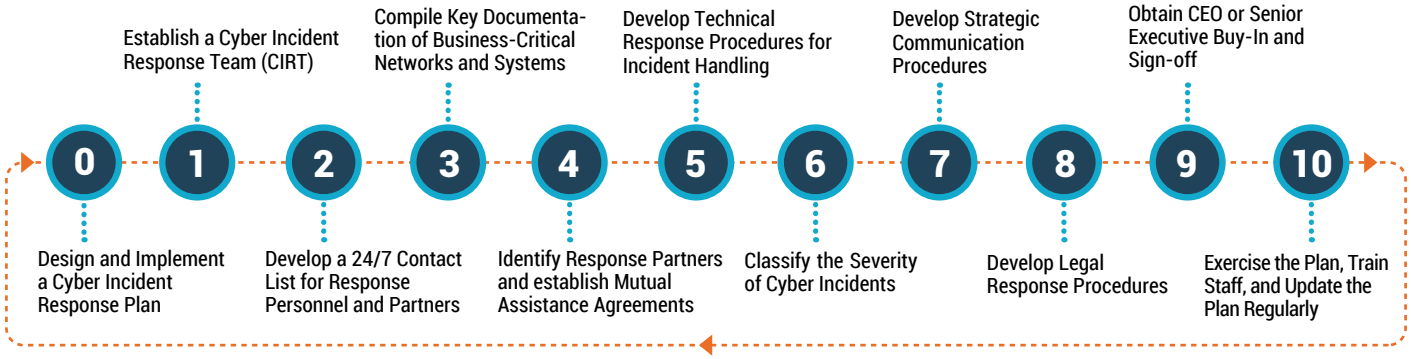
The customer needed essential products and services for the datacentre, disaster recovery centre, and integrated network and security operations and command centre.

THE SOLUTION

Leveraging four decades of demonstrated experience in winning against advanced attack tactics, techniques, and procedures by using a potent combination of intrusion cyber kill chain methodologies, Protect- Detect-Respond methodologies derived from NIST Cybersecurity Framework, CIS Controls, OWASP guidance, MITRE ATT&CK and RESPOND enterprise on the backdrop of program governance using ISO 27001, CMS IT designed, supplied, commissioned, and integrated the essential components.

The solution included integration of anti-advanced persistent threat solution, anti-virus and anti-spam solution, network data loss protection solution, comprehensive insider threat management solution, security incident and event management solution, identity and access management solution, network, web and content gateways, network security scanners, and next-generation firewalls. Deployment and integration were seamless.

For the 24x7 operations across the security and NOCs covering data centre, DR centre, centralised call centres, 375+ towns, 500+ WAN locations, and 850+ Offices (LAN), CMS IT brought in IT security triage specialists, incident responders, and threat hunters. Baselining and continuously improving business use-cases and incident management playbooks bolstered the SOC operations, procedures, metrics, and KPIs.



To provide continuous visibility, deep threat detection, rapid incident response, and Managed Detection and Response (MDR) with advanced AI/ML capabilities, was implemented in tandem with human threat hunting, data analytics and automation by our engineers.

BENEFITS

- Enhanced threat detection and response capabilities for complex attacks with adaptable TTPs
- 24x7 Advanced Security Monitoring, detection, and response integrates with security controls in IT/ OT/ IoT environment
- Continuously evolving business use-cases, playbooks and known error database
- Continuous visibility to Vulnerabilities and mitigation and immediate improvement of Cyber Defense Posture
- Continual compliance and risk assessments
- Complementing human-performed threat-hunting with real-time monitoring, detection, and response capabilities

We are a leading provider of System Integration and Managed Services. As one of India's top IT Services firms, we offer an integrated portfolio of products, solutions and services, built around Automation, Cloud, Cybersecurity & Digital. Currently, CMS IT Services has over 6500 employees and serves more than 300 leading enterprises across key industries.

www.cmsitservices.com
inquiry@cmsitservices.com
+91 80 4550 0300