LINKSHADOW

Industry

LEADING REGIONAL ENERGY COMPANY

EMPLOYEES - 4000+

CASE STUDY

A leading regional energy company collaborated with LinkShadow to secure their IT environment and create a cyber resilient environment.

CHALLENGES

The LinkShadow experts in coordination with the client SOC team identified the below challenges:

- Limited visibility of Users on the SIEM log data.
- Static Rule based threat detection on SIEM
- Inability to detect and respond to cyber threats quickly and effectively.
- Inability to protect sensitive data such as customer data, financial information, and intellectual property from external and insider threats due to inadequate encryption, access controls and monitoring systems and protocols.
- Absence of strict security standards and controls to contain vulnerabilities from third-party risks.

Industry I **LEADING REGIONAL ENERGY COMPANY**

SOLUTION

The solution was based on Network Throughput not limiting to division or IP addresses. Here LinkShadow Extended Detection & Response (XDR), Network Detection & Response (NDR), User Entity Behaviour Analytics (UEBA) – all three solutions where integrated into the client's IT environment:

- LinkShadow NDR tool was deployed to integrate and collect data from various sources across the client's network, endpoints, cloud locations, and applications to provide their security teams with enhanced visibility and a holistic view of the threat surface to identify potential threats or suspicious activities.
- For advanced threat detection, the LinkShadow XDR tool with AI/ predictive analytics, machine learning, and behavioural analytic techniques was applied to detect anomalies such as malware and ransomware in real-time. Followed by continuous monitoring of activities across different systems and dynamic correlation of events, LinkShadow XDR would enable identification of indicators of compromise and alert security teams on potential security incidents before impacting the business.

BENEFITS

To summarize, LinkShadow Next-Generation Analytics Platform support client to adopt a effective cyber resilience strategy with enhanced threat detection, SOC optimization, and visibility into security risks across their organization. By implementing NDR with XDR capability solution, client was able to improve their cyber security analytics capabilities and mitigate the risks associated with cyber threats. They were able to:

Remediate threats with quicker incident response capabilities thereby minimising the risk of damage or data loss.

Uncover threats by adopting a proactive approach to cybersecurity with advanced threat detection and user behaviour analytics.

Helped enhance the client's security posture with actionable intelligence through improved visibility.