opentext™ | Cybersecurity

Case Study

Large Energy Company

ArcSight suite gives full industry regulation compliance and the flexibility to protect against a variety of cyber attacks.

Sophisticated Regulation Compliance Required

As an energy provider this organization needs to comply with NERC (North American Electric Reliability Corporation) CIP (Critical Infrastructure Protection) regulations, to mitigate disturbances to electrical service delivery. To do this, its security team needs to provide robust event handling, real-time event correlation, offline analytics, and the flexibility to understand and protect against several attack frameworks. Deployment flexibility was an important factor for this organization as they wanted to minimize time managing the infrastructure, to free up man hours for value-add security activities. Supported by OpenText™ Professional Services, ArcSight ESM by OpenText and ArcSight Logger by OpenText were implemented on-premises as the foundation of a sophisticated program to empower the security operations team.

"ArcSight has enabled us to fully comply with the NERC CIP regulations."

Data Security and Compliance Engineer
Large Energy Company

The team's Data Security and Compliance Engineer comments: "Over the years we have taken advantage of ArcSight's ability to normalize events, using categorization within our content to take ever changing technology within our environment into account."

Moving to MITRE ATT&CK Support for Further Flexibility

The organization is looking to modernize its security operations further and is interested in the ArcSight Intelligence features to provide better insight into their operations, automate repetitive tasks, and improve operational efficiencies. It currently leverages the 'cyber kill chain' method for pre-empting attacks. This follows a clearly defined linear sequence of phases. Adopting ArcSight Intelligence would give them the opportunity to support the MITRE ATT&CK framework, which is a matrix of intrusion techniques that is not confined to a specific order of operations and which is regularly updated with industry input to keep up with the latest techniques.

At a Glance

Industry

Energy

Location

USA

Challenge

Comply with stringent industry regulations and provide flexible protection against cyber attacks

Products and Services

ArcSight Enterprise Security Manager (ESM)
ArcSight Logger

Critical Success Factors

- Full NERC CIP regulation compliance
- Security appliance approach frees up valuable time
- ArcSight event normalization and categorization guards against technology changes

768-000029-002 | O | 08/23 | © 2023 Open Text