CASE STUDY

SIEM Transformation for a Major Utility

Resolving poor SIEM health, detection gaps, and empowering internal teams

Discovered Intelligence

CUSTOMER

Electric Utility Crown Corporation with over $6 billion in revenue and 6,000 employees.

ENVIRONMENT

Large Splunk environment running Splunk Enterprise Security.

USE CASE

Splunk Enterprise Security in poor health with insufficient security visibility.

OUR APPROACH

- HEALTH ASSESSMENT
- PERFORMANCE TUNING
- USE CASE WORKSHOP

CUSTOMER CHALLENGES

Poor SIEM Health and Low Visibility

The current Enterprise Security SIEM was in poor health, with limited use cases and alerting, resulting in detection gaps and insufficient security visibility.

Internal Resource Lacking Expertise

Limited in-house expertise in Splunk and Enterprise Security was preventing the solution from being fully leveraged and value realized.

Network Restrictions

The customer's network had strict security controls, which created challenges for efficient data collection and indexing.

HOW WE DELIVERED SUCCESS

Increased Enterprise Security Visibility

A Health Assessment of the Splunk environment enabled our team to pinpoint areas requiring tuning and remediation, resulting in improved search performance, improved data collection and complete detection coverage.

A security workshop and training sessions were conducted to define requirements and explore security use cases. This session revealed existing security gaps, fostered stronger collaboration among internal teams, and deepened their understanding of Splunk and Enterprise Security.

The customer ultimately gained significantly improved security visibility from Enterprise Security and strengthened their internal capability to manage the Splunk environment.

Discovered Intelligence

+ 1 877-605-0747
sales@discoveredintelligence.com
www.DiscoveredIntelligence.com