opentext™ | Cybersecurity

Case Study

Dubai Electricity and Water Authority

ArcSight supports sophisticated SOC, successfully bridging OT and IT to deliver unparalleled intelligent security.

Overview

Dubai Electricity and Water Authority (DEWA) provides Dubai's citizens and residents with a continuous and reliable supply of electricity and water. DEWA is one of the best utilities in the world, delivering world-class electricity and water services to over 900,000 customers in Dubai, according to the highest levels of quality, efficiency, and availability. DEWA's total installed capacity is 11,413MW of electricity and 470 million imperial gallons of water per day. For the second consecutive year, the UAE, represented by DEWA, ranked first in the world for getting electricity, according to the World Bank's Doing Business 2019 report.

Challenge

DEWA is a National Critical Infrastructure which presents some unique challenges in security management, as a cyber-attack could take down the entire city and would lead to a national emergency. Critical Infrastructure providers rely heavily on Operational Technology (OT) to control utility networks. These are typically isolated systems with no connection to the outside world. The assumption used to be that this would guarantee their security, but this is no longer the case, as Mr Jacob Jacob, Specialist Cyber Security for DEWA, explains: "We live in a world where millions of devices are connected through public ISP networks and to the Internet. The Internet of Things (IoT) is relevant for DEWA in smart homes, through solar power generators, car charging points, etc. When we started our cyber security journey, we wanted to find a solution to merge IT with OT, so that we can share data between systems, gain threat intelligence on OT devices, and provide improved monitoring of our IT devices."

> "With ArcSight we have a platform to monitor security events and manage incidents. We have seamless data integration, and are compliant with relevant security standards and controls. Improved asset visibility ensures 99 percent availability."
>
> **Mr Jacob Jacob**
> Specialist Cyber Security
> Dubai Electricity and Water Authority

DEWA has key security priorities to address: decrease the impact of any security events; detect and stop security threats; and reduce business downtime and non-compliance. With ever-increasing security data volumes, it was clear to DEWA that an intelligence-driven defence with enhanced data analytics is required to provide visibility and speed up investigation capabilities.

هيئة كهرباء ومياه دبي
Dubai Electricity & Water Authority

At a Glance

Industry

Energy and Utilities

Location

Dubai, United Arab Emirates

Challenge

Consolidate IT with OT, so that data can be shared between systems, to improve threat intelligence and device monitoring

Products and Services

ArcSight Data Platform
ArcSight Enterprise Security Manager
ArcSight Investigate

Success Highlights

- 30% security alarm reduction
- 98% risk mitigation rate
- Reduced meter fraud with AI-driven detection
- 99% device availability through increased visibility

“By taking a different approach to visualizing our risk themes, embracing modern, business-enabling technologies such as ArcSight, and establishing an advanced Security Operations Center (SOC), we have experienced a 30 percent reduction in alarms, ensuring our resources are directed most effectively.”

Mr Jacob Jacob
Specialist Cyber Security
Dubai Electricity and Water Authority

Connect with Us
www.opentext.com

Solution

DEWA’s research led to building an ecosystem that includes ArcSight by OpenText™, an open platform to transform data chaos into security insight. Mr Jacob was excited about several ArcSight features: “It can ingest data from a wide variety of sources and provide intelligent correlation for us to base our analysis on. We work with Elastic and were delighted to discover native integration between ArcSight and Elastic. This powers our analytics and gives us geographical context. With so many devices to monitor, capturing data from different sources is vital for us. We need to know for instance if a valve is being operated, or if areas of a pipeline are being disconnected from the network. These are network events that have a potentially serious impact on our service delivery.”

ArcSight Data Platform (ADP), ArcSight Enterprise Security Manager (ESM), and ArcSight Investigate are part of a sophisticated security ecosystem that can interface with the existing Hadoop, Spark, and Elastic. The ArcSight portfolio, combined with Artificial Intelligence (AI), provides data log management, data analysis, real time alerting and monitoring, security analytics, and intelligent security operations.

“We as cyber security professionals were called upon to detect meter fraud because we have a business use case that collects, correlates, and interprets meter data to highlight fraud,” says Mr Jacob. “ArcSight enabled us to combine various data sources where we could deploy AI on the data streams to analyze consumption patterns. So now, tampering cases are detected and flagged automatically.”

The analytics ecosystem with ArcSight helped create a next generation security operations model. Active event filtering and prioritization enables DEWA to focus on critical alarms. 12 state-of-the-art technologies are integrated to collect data from over 10 connected sources. The infrastructure covers 80 percent of DEWA-controlled devices and networks, and over 20 operational dashboards are automatically generated to provide real-time visibility into the security status.

Meanwhile, the OT has been merged into the security ecosystem as well. An intelligence-driven defence across 25 DEWA locations now means nearly 3,000 devices are fully monitored, with a risk mitigation rate of 98 percent.

Results

Water is a scarce and hard-won commodity for a city surrounded by desert. Leveraging technology, including ArcSight, an adaptive systems ecosystem, DEWA can now predict water network behaviour with AI-based event monitoring. This allows it to capacity-plan more accurately and reduce wastage.
Mr Jacob: “With ArcSight we have a platform to monitor security events and manage incidents. We have seamless data integration, and are compliant with relevant security standards and controls. Improved asset visibility ensures 99 percent availability. More sophisticated data connectivity will enhance this to the full 100 percent, which is our near-term goal.”

He concludes: “By taking a different approach to visualizing our risk themes, embracing modern, business-enabling technologies such as ArcSight, and establishing an advanced Security Operations Center (SOC), we have experienced a 30 percent reduction in alarms, ensuring our resources are directed most effectively. We have found a strategic partner in Micro Focus (now part of OpenText), and look forward to continuing our innovative cyber security journey together.”

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.