splunk> turn data into doing™

CASE STUDY

Sapura Energy Berhad Investigates Incidents 10x Faster for Seamless 24/7 Operations

Key Challenges

Detecting and investigating incidents efficiently to stay ahead of cyber threats was an arduous task for a small team, especially without centralized visibility across distributed operations.

Key Results

Security management is 10 times faster and requires fewer resources — and data-driven visibility helps clear all obstacles for maintaining seamless operations round the clock.

Industry: Energy & Utilities

Solutions: Security, IT Operations

Security isn't just the absence of danger — it's also the presence of peace of mind.

A leading integrated energy and solutions provider, Sapura Energy Berhad operates globally in more than 20 countries. Though cybersecurity was a top priority, the company faced challenges in formulating a proactive strategy to monitor the ever-evolving security landscape.

"At that time, we were unable to bring together all necessary information for efficient anomaly analysis. We needed to go through a huge volume of logs one by one and inspect various machines manually, all while consulting different people to understand the root cause of problems. It usually took days," says Md Harmizam Md Aris, manager of IT operations at Sapura Energy Berhad. "What we needed was a centralized data analytics platform to speed up investigations and drive better, faster security decisions."

Harmizam and his team found the right solution – Splunk, the Data-to-Everything Platform.

Data-Driven Outcomes

10x
faster incident detection and investigation

Fewer
resources required for cybersecurity management

24/7
operations activated for even better customer support

Efficiency Up, Pressure Down, Labor Halved

The Splunk solution achieves Sapura Energy Berhad's goals by helping the IT team eliminate all data silos and integrate logs from distributed sources into a single, shareable platform for centralized monitoring.

"Splunk impressed us with its reputation across industries, and has exceeded our expectations with its functionality," says Harmizam. "The Data-to-Everything Platform is flexible enough to accommodate our heterogeneous log data — which includes appliance, network, security and server logs, as well as logs from operating systems, Azure and Office 365 —, bringing us unprecedented convenience."

The Splunk analytics engine correlates and analyzes the data, unearthing actionable insights presented with rich visualization on an intuitive Splunk dashboard. "With full-stack visibility into our entire IT infrastructure, we now review all anomalies on a single pane of glass, while drilling down into potential risks and resolving issues effectively," Harmizam adds.

In measurable terms, Sapura Energy Berhad identifies and investigates incidents 10 times faster. Now the team can handle a single incident — that once took two or three days to analyze — in just three to four hours. "We no longer need to bury ourselves in different logs and bother various analysts, system administrators and application teams to fix a problem. The analysis is done proactively on the Splunk platform and clearly reported on the dashboard," Harmizam explains.

> Splunk enables us to leverage a single source of truth to turn data into better, faster security decisions."
>
> **Md Harmizam Md Aris,** Manager, IT Operations of Sapura Energy Berhad

Beating Expectation With a Wider Scope of Applications

While Sapura Energy Berhad had initially only planned to mitigate cyberattacks with Splunk, the solution has quickly proven to have a wider scope of application. The team now also uses Splunk to manage daily traffic, server resources and cloud usage, as well as uptime and downtime of their IT infrastructure.

Thanks to Splunk, Sapura Energy Berhad can anticipate future workload needs with data-driven analytics in order to make better IT decisions and plan network capacity more efficiently. They can also conduct statistical analysis to uncover data trends that reflect anomalous user and system behaviors. "With Splunk, we easily spot incidents that may hinder user experience, and empower 24/7 IT operations to support our business, bringing real value to end users," Harmizam says.

Sapura Energy Berhad is also grateful for Splunk's human connections. "With the support of the Splunk team, we can customize our dashboards really easily," says Harmizam. "This makes particular sense when we have such a small IT team."

Scaling Into the Future

With Splunk, Sapura Energy Berhad is ready to sustainably grow its IT infrastructure. "The Splunk platform is scalable enough to accommodate our constantly increasing log size, and its subscription-based operation model lets us step up investment according to actual needs," says Harmizam. "For instance, the volume of logs we put into the Splunk platform has gradually increased from 10GB to 100GB in six years' time, all matching the real pace of business growth."

Sapura Energy Berhad will also continue using the diverse range of Splunk apps that they can download for free to maximize the functionality of the analytics platform, such as compliance enhancement. Furthermore, the team is now planning to kick-start a new IT initiative with Splunk — security automation. "We are exploring bringing in Splunk Phantom to improve security orchestration, automation and response, especially in automating search and analytics processes so that we can take prompt action on every unexpected change in the IT environment."

Download Splunk for free or get started with the free cloud trial. Whether cloud, on-premises, or for large or small teams, Splunk has a deployment model that will fit your needs.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

Splunk, Splunk>, Data-to-Everything, D2E and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2021 Splunk Inc. All rights reserved.

21-15535-Splunk-Tier2-Sapura Energy Berhad-CS-103