splunk>

CASE STUDY

MTR Goes the Extra Mile With Solution Providing Automated Real-Time Visibility

MTR

Executive summary

MTR Corporation Ltd. is a major public transport operator running 10 commuter railway lines, a Light Rail network and a high-speed Airport Express link on which about 5.8 million passenger trips are made on a normal weekday in Hong Kong. While enjoying a world-class level of safety and reliability in railway operation through the years, MTR is always striving for excellence. By deploying Splunk solutions, MTR has seen added values in the following areas:

- Real-time visibility into IT operations
- Enhanced operational efficiency and productivity; improved resource utilization
- Ultrafast threat tracking in minutes

Why Splunk

Nowadays, with cybersecurity being top of mind for companies around the world, the protection of systems, network and data in cyberspace has become a critical issue, and there is no exception for public transportation operators. Therefore, MTR saw a need to carry out a system upgrade to automate daily IT security management and threat detection, with a special focus on the tracking of access to the corporate network.

MTR would like to automate the access control process further by building a stronger link between the privileged account management system and the production systems. In 2017, MTR started replacing its old security information and event management (SIEM) system with Splunk Enterprise, Splunk Enterprise Security (ES) and Splunk IT Service Intelligence (ITSI) monitoring and analytics solution and has derived benefits from the flexibility and additional values the solutions offer.

Operational visibility and real-time monitoring redefine threat prevention

Splunk Enterprise matches searches on all data sources in the MTR information system to analyze potential threats. Data from the Active Directory, privileged account management system and other sources are well integrated, and user login information is matched to approved

Industry

- Travel & Transportation

Splunk Use Cases

- Security
- IT operations

Challenges

- Request for higher visibility into IT infrastructure to cope with business growth
- Rising demand to strive for excellence in risk and threat detection
- Intention to further automate security management

Business Impact

- Enhanced security management, thanks to proactive, real-time visibility and actionable IT operations insights
- Efficient threat tracking, turning manual work into minutes of automated operations
- Raised productivity and efficiency, due to the simplified operation and optimized resource utilization

Data Sources

- Active Directory
- Privileged account management system
- Production system

Splunk Products

- Splunk Enterprise
- Splunk Enterprise Security
- Splunk IT Service Intelligence

user records, enabling automatic user tracking and identification. Splunk Enterprise has converted manual investigations into simple, proactive and automated searches, facilitating real-time security monitoring through internal risks and threats analyses.

Flexible graphical interface brings convenience and boosts efficiency

According to the MTR team, user analysis is as simple as a Google search with Splunk Enterprise. Unsuccessful login attempts and incorrect passwords are automatically tracked and reported. Unauthorized accesses can be traced layer by layer, from a network location to account ID, and then to the user identity. This prevents users from being able to gain unapproved elevated privileges.

The interactive graphical dashboard makes the network status clear at a glance. Users have anomaly detection and threat monitoring at their fingertips, resulting in unprecedentedly efficient IT operations.

Network access tracking done in minutes; resource utilization highly improved

Using correlation and analytics, Splunk Enterprise detects high-risk activity, access and events, providing actionable insights to the MTR team in minutes. After identifying a threat to the network, Splunk Enterprise will alert the team, and they can search through historical event data to determine the scope, intent and severity of the actions. Splunk software functionality frees up valuable time and resources for MTR's IT team, enabling them to focus on value-added business activities.

> **"A turnkey analytics platform, Splunk offers us a rapid entry to actionable threat intelligence, giving us the visibility into potential risks in our production environment and a tool to monitor, investigate and report on them."**
>
> Ted Suen, Head of Information Technology
>
> MTR Corporation Ltd.

Creating new possibilities for the future

The IT team has already extended the use of Splunk Enterprise to manage service performance and availability. The team is also applying Splunk Enterprise for the detection of external threats.

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