splunk>

CASE STUDY

MBDA Germany Drives Security Intelligence With Splunk Enterprise Security

MBDA

Executive summary

MBDA Germany is the leading guided missile and air defence systems company in Germany. MBDA Germany is part of the European MBDA Group, a world leader in missiles and missile systems. The company has sites in Schrobenhausen, Aschau am Inn and Ulm. MBDA Germany needed a solution that would give it the visibility to identify and investigate the threats targeting the organization more effectively. Since deploying Splunk Enterprise and Splunk Enterprise Security (ES), the company has seen benefits including:

- Reduced time to investigate security incidents
- Improved identification and classification of security attacks
- Enhanced overall security posture

Why Splunk

MBDA Germany develops, manufactures and provides customer and product support for guided missile systems and air defense systems to the Air Force, Army and Navy. As a missile manufacturer, MBDA Germany is often the target of advanced threats and has to be able to identify these attacks, investigate where they come from and act to mitigate them. MBDA Germany needed to gain visibility into the security-relevant data across the organization, and selected a solution from the "leader" quadrant in the Gartner Magic Quadrant for Security Intelligence and Event Management (SIEM) solutions. Splunk Enterprise and Splunk Enterprise Security (ES) stood out because they offered a user-friendly interface, out-of-the-box content and fast time to value. This made it particularly suitable for MBDA Germany's small IT team, enabling the security operations center (SOC) team to work very efficiently.

The main goal of using Splunk Enterprise and Splunk ES is to quickly identify and investigate security threats and attacks. MBDA Germany analyzes data from over twenty families of systems in Splunk software, including the breadth of the network with approximately 2,500 endpoints, 350 servers, switches, gateways, AAA servers and WAN connections to France, Italy and the UK.

Industry

- Manufacturing

Splunk Use Cases

- Security

Challenges

- Lack of visibility across entire infrastructure
- Undetected security threats in the network

Business Impact

- Mean time to investigate security incidents reduced significantly
- Real-time alerts identify attacks that would previously have gone undetected
- Analysis of historical data informs future security measures, resulting in a more resilient security posture overall

Data Sources

- Network logs
- Endpoint logs
- Server logs
- Data from switches
- Data from gateways
- Authentication logs

Splunk Products

- Splunk Enterprise
- Splunk Enterprise Security

Mean time to investigate security incidents reduced to a twentieth

The biggest breakthrough for MBDA Germany is the reduction in time the SOC team needs to trace back indicators of compromise messages from different Computer Emergency Response Teams (CERT). Since deploying ES, the average time to analyze a CERT message has been reduced from an average of 372 minutes to just 15.

Real-time alerts identify attacks that would previously have gone undetected

Since deploying the Splunk platform as its security intelligence solution, MBDA Germany has been able to identify a greater number of attacks, many of which would previously have gone undetected. The SOC team has set up alerts around a number of critical events, such as if machines are infected with malware and communicate outside the company or if malicious outsiders try to enter the MBDA Germany network through specially prepared websites. As a result, MBDA Germany can identify potential malicious activity before it has any negative impact.

Analysis of historical data informs future security measures

It is important for MBDA Germany to understand where an attack came from, what it looked like and what the impact was, in order to be able to respond effectively. Splunk Enterprise and Splunk Enterprise Security enable the company to trace back the single stages of an attack in detail and identify existing holes. MBDA Germany can quickly assess a case, escalate if necessary, document and communicate on it.

"Splunk dramatically reduces security risks at MBDA Germany. The software helps us to work much more efficiently, gain visibility across our entire network, react more quickly to security breaches and use insights from our data analysis to inform our future security strategy."

Patrick Schwarz
Head of IT and Project Manager
Information Technology
MBDA Germany

In addition, MBDA Germany can use these insights from past incidents to create new measures against future attacks. The result is a more resilient security posture overall, shorter reaction times for cases, better tracability and valid information about security breaches.