splunk>

CASE STUDY

DKB Upholds Customer Trust, Addresses Threats 90% Faster with Splunk

Key Challenges

As DKB embarked on its cloud migration journey, the financial institution struggled to monitor its complex systems and detect when its environment was compromised.

Key Results

After adopting Splunk and gaining full visibility into its infrastructure, DKB reduced the number of false positive alerts and accelerated threat detection and investigation by 90%.

DKB
Deutsche Kreditbank AG

Industry: Financial Services

Solutions: Splunk Security

In the world of banking, customer trust is paramount.

Four and a half million customers entrust Deutsche Kreditbank (DKB), the second-largest direct bank in Germany, with their loans, credit cards, savings and more. To ensure seamless transactions, payments and other processing, DKB has been migrating to the cloud as well as investing more in cybersecurity. The company initially used Splunk through a managed service provider, and then brought Splunk in-house.

DKB's move to the cloud grew more elaborate than they expected. It needed a solution to help it see into all parts of its hybrid infrastructure, from various security tools to cloud and on-prem environments alike. DKB needed full visibility to surface issues promptly – especially as the potential for a ransomware attack and other cybersecurity threats could endanger not just the stability of its systems, but also erode the trust of its customers.

Outcomes

- 90% faster threat detection and investigation
- Increased visibility across tools and environments
- Fewer false positives

Minimizing blind spots

DKB started using Splunk for security monitoring, incident management and, more recently, threat intelligence. The company already used a multitude of security tools, but Splunk let them aggregate all the different data from different tools and search it.

And this has saved time — a lot of it. Andreas Hennich, Head of the Security Operations Center at DKB, says, "The biggest advantage Splunk brought was the visibility. We see everything; we see every alert that pops up on the different security tools and in all the environments we have in the cloud and the on-prem environment. Because we have everything in one place, we're able to investigate and use this data that much faster."

No compromise undetected

DKB's teams improved network security by accelerating alert response; before, there were simply too many alerts to keep up with, and they were decentralized too, which meant delays and missed alerts. "In the past, we searched through log files to look for network issues, but it was time-intensive, and it was easy to miss alerts. Now that we have all components of our infrastructure connected to Splunk as our SIEM, there's a lot of different activities inside network security that are quickly visible and in a centralized, correlated database," says Hennich. "In the case of compromise, we can see the alerts more quickly and react faster."

When it comes to actual threats, DKB has reduced investigation and resolution time by 90%, Hennich reports. "Before Splunk, we had to search different log files, search additional data, write search queries and more. But it's so much faster with Splunk."

Now that we have all components of our infrastructure connected to Splunk as our SIEM, there's a lot of different activities inside network security that are quickly visible and in a centralized, correlated database. In the case of compromise, we can see the alerts more quickly and react faster."

Andreas Hennich, Head of the Security Operations Center at DKB

24-splunk- 133169 - EMEA DKB Customer Story-102