Schaffhauser Kantonalbank is strengthening its cybersecurity with terreActive's Security Operations Center

Expansion of cyberdefense platform increases security maturity

Hackers don't care if a business is international or local, as long as the expected gain from the crime is large enough. That's why every bank in Switzerland needs the same protection. Schaffhauser Kantonalbank has expanded its security arsenal thanks to an efficient cyberdefense plan and the exploitation of synergies in SOC operations.

Background

Schaffhauser Kantonalbank (SHKB) already had good security solutions from Splunk and Vectra, among other providers. Log data was being recorded but not yet centrally analyzed, and a real-time overview of all systems and applications was not available. The bank needed a partner to develop a security operations center (SOC) to detect and handle incidents based on a cyberdefense platform. After developing the solution in 2020, the new partner will also provide individual SOC services in the future to reduce the burden on the bank's human resources. SHKB issued an official invitation to tender. terreActive won the contract based on the comprehensive solutions it offered and its outstanding customer focus.

Preparing for the project

Before the actual project start, a proof of concept (PoC) was provided, including an SOC workshop to discuss the first possible use cases (threat scenarios). In a kick-off meeting, SHKB and terreActive planned the resources, deadlines, and division of responsibilities and defined project milestones along the lines of the security monitoring cycle. Escalation pathways, access rights, and responsibilities – such as those in play during the incident-response process – were also addressed in a later workshop.

Approach

As the sum of all security measures, the cyber defense platform (CDP) is key to the SOC when it comes to detecting and handling incidents. For this reason, terreActive used the planning phase to test a number of variations of the CDP, taking Schaffhauser Kantonalbank's particular circumstances into account. «terreActive was able to quickly produce an initial CDP for us using existing security measures and then continuously develop it to cover an ever wider range of threat scenarios», says Andreas Glauser, Chief Security Officer of Schaffhauser Kantonalbank. «terreActive's extensive use case database helped get the project started quickly, since quite a few standard use cases could be activated immediately after considering our bank's threat landscape.»

«terreActive's experienced employees helped us select the most effective use cases. Regular, highly constructive meetings allow us to ensure the professionalism and continuing development of the cyberdefense platform.»

Andreas Glauser, Chief Security Officer

Schaffhauser Kantonalbank

Technical implementation

«To meet our high requirements for performance, capacity, and redundancy, we worked with terreActive to develop the existing Splunk infrastructure into a cyberdefense platform», says Rudolf Lenz, Director of Operations & IT at Schaffhauser Kantonalbank. Sensitive IT systems were linked to the SIEM (security information and event management) platform and now generate logs that are centrally stored and analyzed. Splunk Enterprise Security is the primary SOC tool for correlating log data and locating and visualizing threats. terreActive also integrated use cases and fine-tuned them to SHKB. Vulnerability management with Tenable was installed and linked to the SIEM to further enhance security.

Schaffhauser Kantonalbank

About Schaffhauser Kantonalbank

With over 300 employees and 8.7 billion francs in assets, Schaffhauser Kantonalbank is the leading financial institution in the Canton of Schaffhausen. The modern universal bank with five branch offices offers financial services to private individuals, companies, and public institutions. The bank was founded in 1883 and is wholly owned by the canton.

Daily operation and incident response

terreActive's flexible service catalog allows medium-sized enterprises in a range of industries to benefit from the same services as large corporations. The services terreActive offers Schaffhauser Kantonalbank include threat detection and threat intelligence – services that the Aargau-based company also provides to major global corporations. All customers benefit equally from terreActive's experience and synergies.

terreActive's SOC first reviews all reports generated by the cyberdefense platform. If necessary, incidents are investigated and clarified together with Schaffhauser Kantonalbank. If a security incident is triggered, a runbook specifies who does what.

terreActive's SOC operates from its sites in Aargau and Zurich, managing the cyberdefense platform together with the customer.

Benefits for the bank

- Detection and reaction times for security incidents have been reduced massively.
- SHKB receives comprehensive reporting, assessment principles, and recommendations.
- Because terreActive runs the SOC, the company's internal resources can be employed elsewhere, thus increasing efficiency.
- The centralized, non-modifiable log collection meets the compliance standards.
- SHKB's cyberdefense undergoes continuous improvements thanks to close collaboration with terreActive's specialists.

«Monthly review meetings help us constantly review and optimize our security standard», explains Andreas Glauser of Schaffhauser Kantonalbank.

Businesses that take precautions now will have an edge in countering future attacks by cybercriminals.