Case Study //

Implementation of Big Data Security Intelligence for a Financial Services Company

Initial situation

A financial services company with more than 10,000 employees in many different countries is striving to optimally protect its IT systems in accordance with its high traceability and security standards. It wishes to use active, traceable reporting not only to detect attacks early on, but also to identify potential targets and the likelihood of attacks being successful. Furthermore, the company wants to establish sustainable and technology-supported incident processes and therefore expand its security operations center (SOC).

Goals

- ✓ Optimized protection of the IT system against attacks
  - ✓ Active reporting
  - ✓ Early detection of attempted or actual attacks
  - ✓ Identification of possible targets
  - ✓ Determination of the likelihood of success
- ✓ Expansion of the security operations center
  - ✓ Establishment of sustainable and technology-supported incident processes

Approach

The first step in the project was to examine the entire IT environment and record possible data sources. At the same time, the complexity of integrating the different sources was assessed. The data gathered was used to perform an opportunities and benefits analysis that reflected the customer's specific infrastructure and served as the basis for a cost estimate and the definition of the multilevel procedure.

The subsequent initial requirements analysis was designed in agreement with data protection, security, operations, risk management, and the works council. The detailed procedure was worked out on the basis of the results of the opportunities and benefits analysis, taking into account existing solutions and their possible integration. A decision-support paper to implement the customer-specific solution to achieve big data security intelligence envisaged a step-by-step, cost-optimized implementation over a period of two years in line with mayato's maturity model.

Watch our predictions come true!

Reaching maturity level 1 of the IT environment

On the basis of logging data from a wide variety of network and security components, systems, and applications, initial findings about the environment were recorded and, with the help of rule sets, it was possible to produce the first reports and analyses.

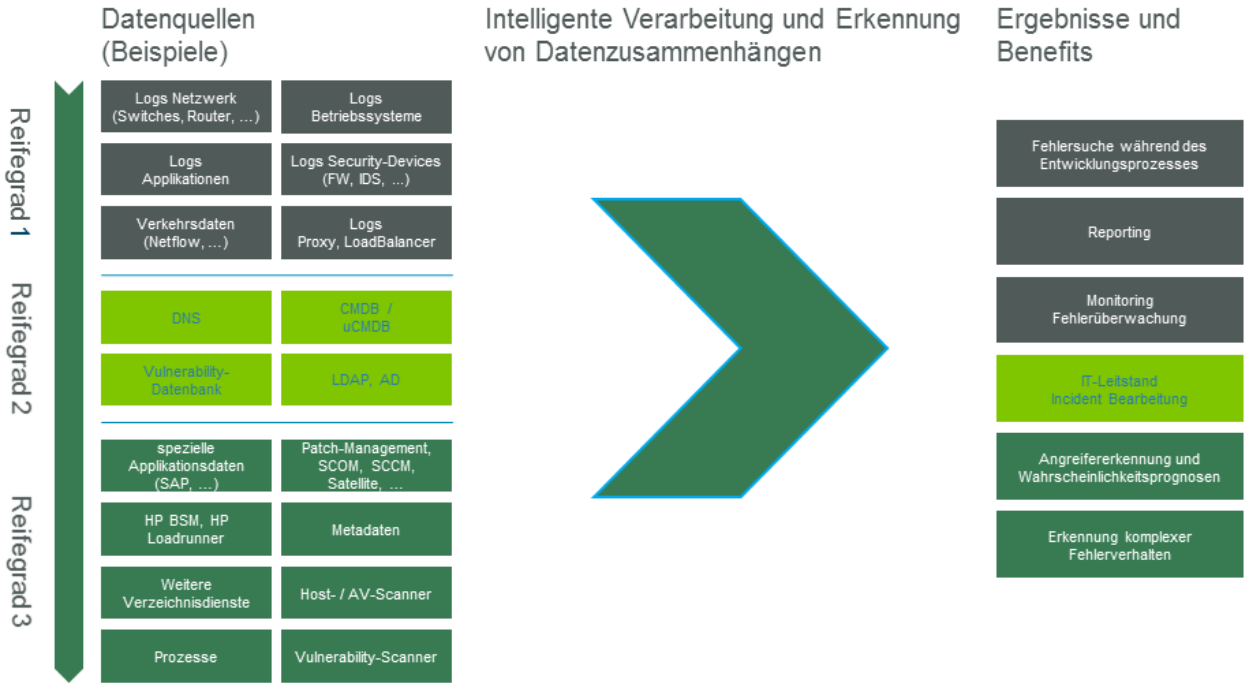
Reaching maturity level 2 of the IT environment

In the second step, the cornerstone was set for detecting correlations. Here, the live data recorded in step one was correlated with information from highly diverse tools and systems, such as directory services and inventory databases. A vulnerability database was incorporated to classify the security levels of systems. This meant search and report results could be refined and also enabled additional analysis options, particularly for the security operations center. With the completion of these activities, it became possible to integrate the system with the existing incident processes for the first time.

Reaching maturity level 3 of the IT environment

In the third and final step in the project, additional data sources from systems were included for patch management, monitoring, and antivirus and vulnerability scanning. This created clarity about which systems were susceptible to known weak points. By analyzing patch management, it was possible to differentiate between intentional and unintentional system changes.

In addition and with the help of mathematical analysis methods, evaluations were performed that made it possible to identify deviant behavior patterns, even for previously unknown and highly specific attack scenarios. This means the targets of attacks and attackers can be identified even if the tactics used are not mapped in the sets of rules defined in antivirus and security scanners.



Watch our predictions come true!

Results

The system that was set up and its fail-safe architecture, which is based on a standard industry product, enables the customer to detect attacks on IT systems at an early stage, even for previously unknown scenarios. The customer can also identify potential attackers and ensure forensic traceability across the whole IT infrastructure. What's more, evaluations can be performed about the likelihood of the success of attacks on potential targets, and these evaluations serve as the basis to harden and optimize the IT landscape.

About mayato

mayato GmbH empowers companies to capitalize on their information. Together with our customers, we develop and implement solutions in the areas of financial analytics, customer analytics, industry analytics, and IT security analytics.

A team of experienced process and technology consultants operates out of our offices in Berlin, Bielefeld, Mannheim, and Vienna. They analyze and optimize your business processes and work with you to determine the requirements for technical implementation. They assist you in selecting the right tools, develop successful strategies, and conceptualize tried-and-true modern architectures. And of course, mayato consultants also help with the practical side of implementing your chosen solutions. Technical standards and governance enable economical, effective projects and efficient operations in the long term.

Analysts and data scientists from mayato use these solutions on your behalf to establish connections between data from many different sources and to forecast trends and events. They devise convincing business cases and produce tangible monetary benefit from your processes and applications. Your employees learn how to use state-of-the-art data analysis methods, how to tackle data quality issues, and how to interpret and visualize results. Working with mayato future-proofs your company for the age of big data.

mayato GmbH was founded in 2007. Among mayato's customers are renowned large and midsize companies from a range of industries. As a partner of several software providers, mayato is committed to remaining neutral and – first and foremost – to delivering its own high-quality services. For more information, please visit www.mayato.com.

Contact us //

mayato GmbH
Am Borsigturm 9
13507 Berlin

info@mayato.com

+49 / 30 4174 4270 10