CASE STUDY

MONITOR AND PROTECT INTERNAL NETWORK THROUGH TRAFFIC DATA ANALYSIS

Client Background

Our client develops, manufactures, and sells networking hardware and other products related to the communication and information technology industry worldwide. Additionally, the company offers security products including cloud, email, endpoint, web, and network security; advanced malware protection; and next generation intrusion prevention systems.

Business Challenge

The client's goal was to assess the vulnerabilities and apply threat intelligence while simplifying access across wired, wireless and VPN connections. The company did not have the expertise in-house to address the peculiarities of the security field they were working in and needed a reliable partner that could cover a range of technical tasks.

softserve

Project Description

The client's solution—one of the most comprehensive visibility and network traffic analytics solutions available—uses enterprise telemetry from the existing network infrastructure. This hardware device provides advanced threat detection, accelerated threat response, and simplified network segmentation using multilayer machine learning and entity modeling. With advanced behavioral analytics, users always know who is on the network and what they are doing.

The service SoftServe provided related to monitoring and protecting the internal network through traffic data analysis. The team also developed the statistic rules criteria. There were event messages—not critical and could be ignored—and alarms that needed to be checked and fixed. Due to the fact that metadata does not have context and was challenging to analyze, the team decided to integrate the client's service engine to track the user sessions. This helped to gather information regarding who logged in and when so that quarantine regimes could be applied reducing risks and containing threats by dynamically controlling network access. Also, the integration made it possible to track non-user activities—Wi-Fi spot change, printers work.

Ten people were on the SoftServe team—two permanently worked from the US. The team followed the Scrum methodology, but switched to Kanban.

The project owner (PO) formed the requirements. However, as a result of the service peculiarities, the requirements were formed on demand. The team had full ownership over the tasks—determination and sizing.

The regular, stable communication included stand-up and planning meetings. The staffing process was implemented by SoftServe.

Value Delivered

Quality was a key point for our client and the main goal was to produce the high-quality code that worked perfectly and provided a better user experience for the client's customers. This not only expanded business relations but also saved costs because the code did not need to be fixed or rewritten. Additionally, the SoftServe team filled the technology gaps in expertise on the clients' side.

ABOUT US

SoftServe is a digital authority that advises and provides at the cutting-edge of technology. We reveal, transform, accelerate, and optimize the way enterprises and software companies do business. With expertise across healthcare, retail, media, financial services, software, and more, we implement end-to-end solutions to deliver the innovation, quality, and speed that our clients' users expect.

SoftServe delivers open innovation—from generating compelling new ideas, to developing and implementing transformational products and services.

Our work and client experience are built on a foundation of empathetic, human-focused design that ensures continuity from concept to release.

We empower enterprises and software companies to (re)identify differentiation, accelerate solution development, and vigorously compete in today's digital economy—No matter where you are in your journey.

Visit our **website**, **blog**, **Facebook**, **Twitter**, and **LinkedIn** pages.

NORTH AMERICAN HQ

Tel: +1 866 687 3588 (USA)
Tel: +1 647 948 7638 (Canada)

EUROPEAN HQ

Tel: +44 (0) 800 302 9436

info@softserveinc.com
www.softserveinc.com

softserve