CASE STUDY

THREAT DETECTION AND ANALYSIS SOLUTION USES DATA SCIENCE, BIG DATA AND SELF-LEARNING

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.

The client recently purchased a security startup that pinpoints attacks before they can disclose and corrupt sensitive data. The solution analyzes web traffic, analyzes endpoint and network data, and then uses machine learning to identify malicious activity.

softserve

Business Challenge

Our client's initial goal was to scan and detect threats in the ecosystem using simple network snapshots and data science. However, the client did not have the expertise in-house and was looking for a team of professionals to help address the goal and take on the challenge of dealing with the technology's beta versions and its relatively new functionality.

Project Description

The client consulted with SoftServe to assist with its security tool, threat detection, and analysis solution that included hardcore data science, big data, and self-learning. Its main features tracked and detected abnormalities based on a snapshot of network traffic.

The SoftServe team focused on configuration, building the infrastructure, and monitoring. Additionally, the team led the migration from the on-premise model to the AWS cloud and container world. And the service of migration from the Monoliths architecture to Microservices.

SoftServe team—following Scrum—consisted of three DevOps engineers, one team lead (TL), and one project manager (PM). The team communicated regularly with daily sync-ups, weekly planning meetings, weekly demos, and HipChat.

The requirements were described by the technical project owner (PO) and the scope was divided into phases. The SoftSerServe team worked closely with the PO to translate the requirements into technical tasks. The migration phases consisted of:

- Planning
- Proof of concepts (PoCs)
- Production in a cloud
- Traffic switch

Technology Stack

- Boto3
- Python
- Bash
- Terraform
- Ruby
- IntelliJ IDEA
- Git
- TeamCity
- BitBucket
- ELK
- Docker
- Ingress Controller
- Prometheus
- Jira
- ElasticSearch
- Splunk
- Cloudwatch
- AWS
- Fluentd
- Metrics api
- Nginx

Value Delivered

The SoftServe team provided the client with the needed expertise and optimized the processes to meet the goals of the collaboration. Additionally, the trust and collaboration with the client's developer teams resulted in achieving the desired results in a short time period.

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