SECURE AWS LANDING ZONE WITH OPENSEARCH AS A SIEM

CRITICAL SERVICES

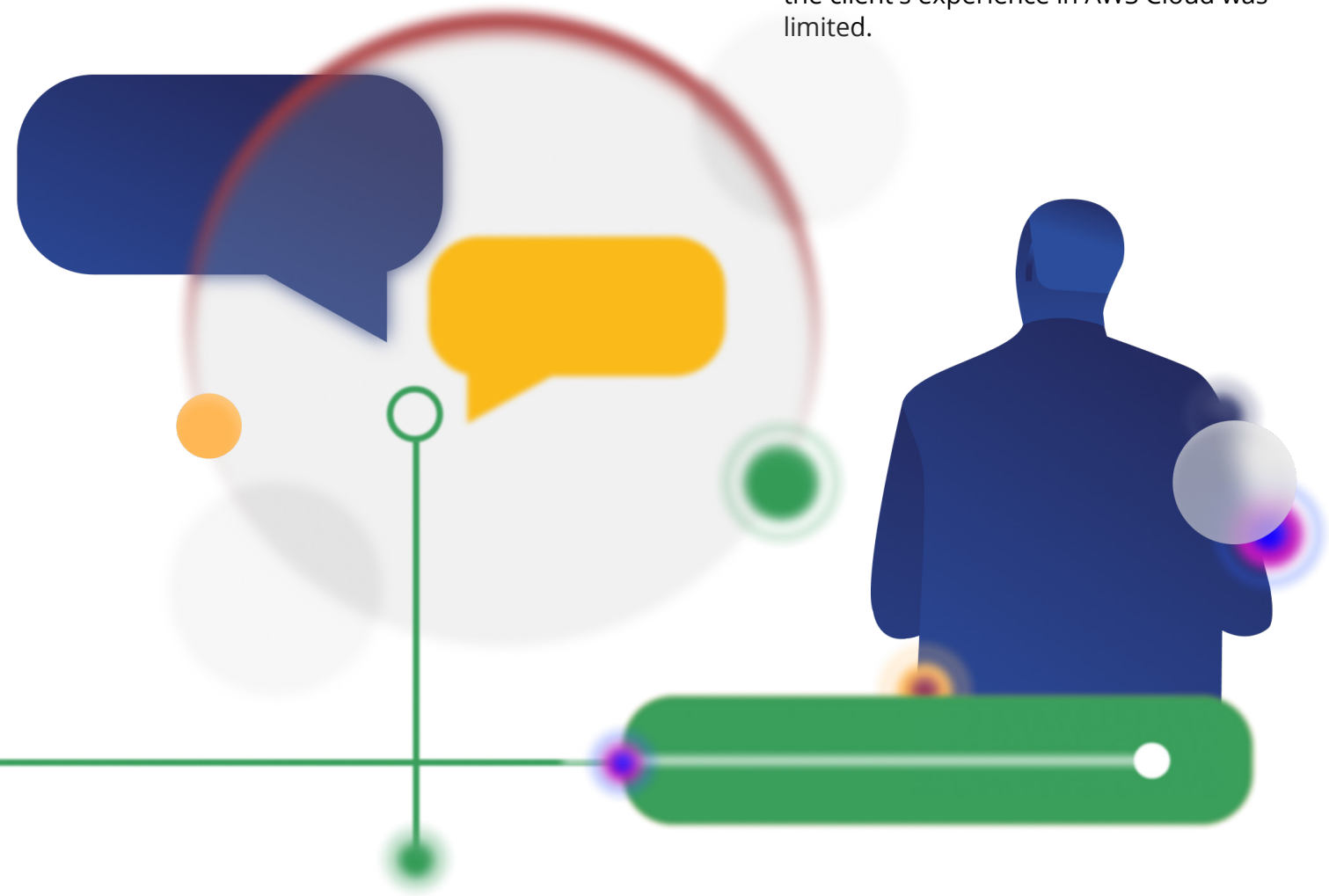
softserve

Client Background

Our client is a global innovation company creating products and services for complex data analysis.

Business Challenge

The client has recognized the need to define and establish a secure environment for their infrastructure because of having security issues in the past. As the company has moderated its work using AWS console only, it aimed to get the resources being deployed using automated pipelines and to keep all the infrastructure as code (IaC) in GitLab repositories. SoftServe got the request to design an efficient security solution as the client's experience in AWS Cloud was limited.



Solution

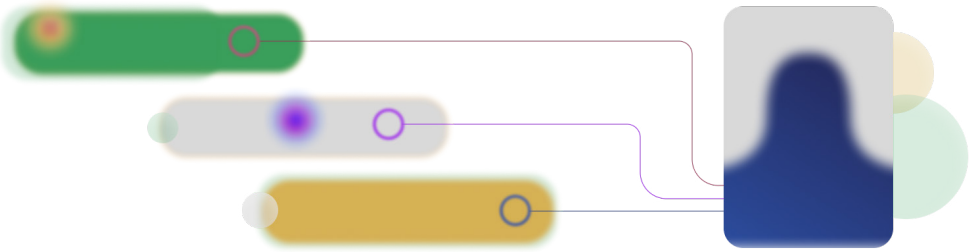
SoftServe analyzed the client's infrastructure and business goals and devised the exact action plan. During the verification stage, our team of experts focused on corresponding to the requirements of all security standards. This helped us to propose a powerful and workable solution for the client.

As the company had only two AWS accounts, the most efficient practice was to build a multi-account structure in AWS, where it wanted to migrate both — the new company infrastructure and its existing assets. The SoftServe team started by designing the secure architecture solution preparation.

Our next big step was creating the IaC secure AWS Landing Zone code in Terraform, where we could place every minor configuration. For this, our team of experts built a secure pipeline with KMS encryption, where only permitted users could have access and enforce changes to the production. Having deep experience in the security cloud domain, we used a significant number of AWS Services in the Terraform code: AWS GuardDuty, AWS Security Hub, AWS Security Control Policy, AWS Organization, AWS SSO, AWS KMS, AWS Secret Manager, AWS System Manager, AWS Config, AWS VPC, EC2, S3. The SoftServe security team also designed architecture for security information and event management (SIEM) service using OpenSearch built in AWS. AWS OpenSearch has all the logs gathered in one place from the entire organization. With the usage of Lambda functions and Kinesis Data Streams, the security data logs were pushed straight forward to the OpenSearch from many services like AWS CloudTrail, GuardDuty, SecurityHub, and VPC flows.

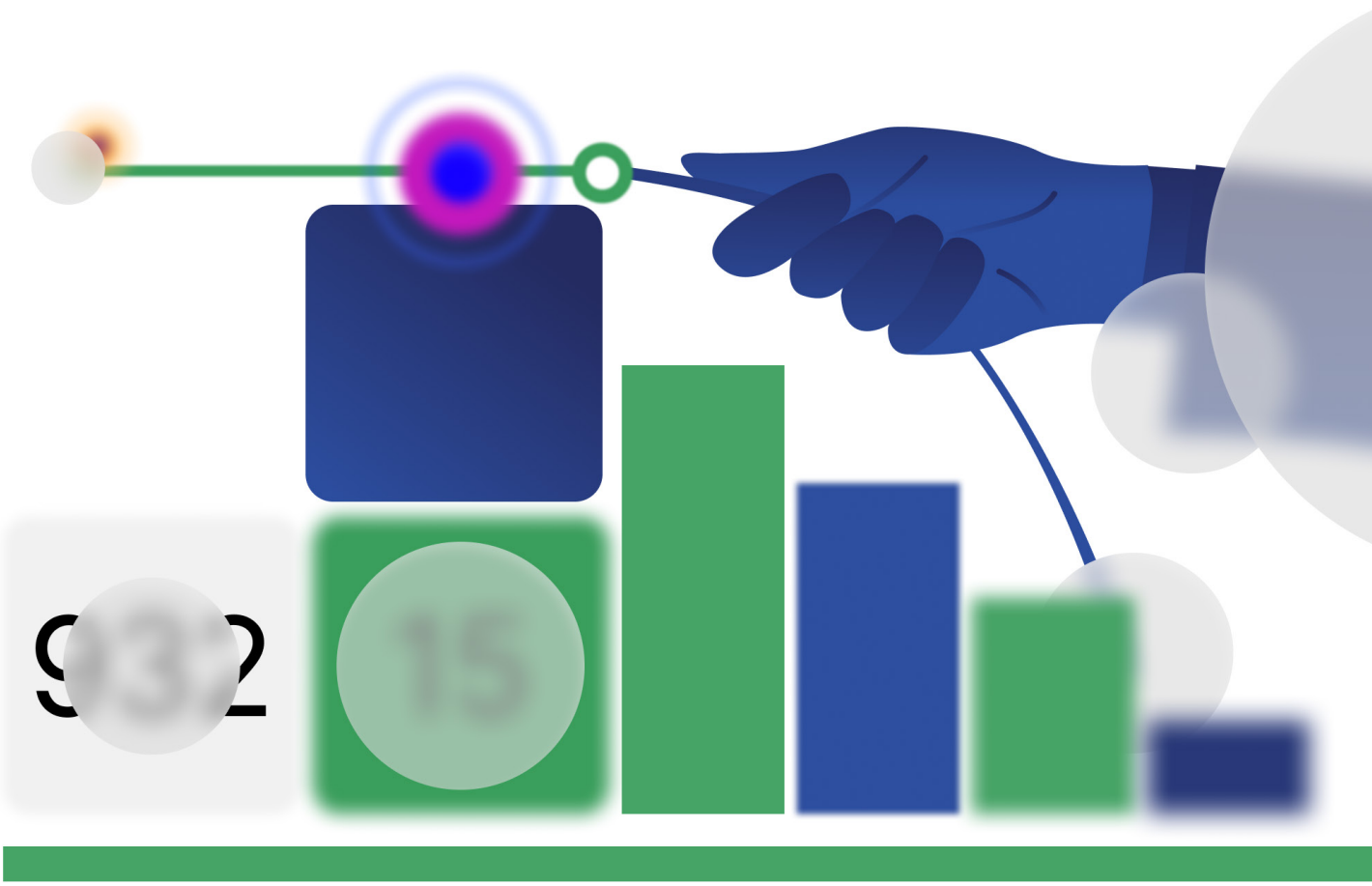
To detect any potential incidents on the client's infrastructure, the SoftServe developers designed two Slack channels: one for security audit notifications and another for providing details about the guard duty findings. In this way, we were able to form an incident notification center that facilitated identifying any attack attempts. This solution was highly profitable as our client was not experienced in AWS Cloud.

Within the process, SoftServe encountered the dilemma of a short period for the implementation — up to five months. Nevertheless, our experts enabled us to enroll a dozen of high-standard security tools.



Value Delivered

As a result of our partnership, the client reached the initial goal of getting a fully protected security environment. With the set of frameworks installed, SoftServe provided a solution with high automation capabilities. Our client got the possibility to make changes quickly and monitor the entire system from one place. All these steps brought the client's infrastructure to a new level of security allowing them to maximize their business goals and increase scalability.



ABOUT SOFTSERVE

We are a digital authority made up of advisors, engineers, and designers who deliver innovation, quality, and speed to elevate and accelerate our clients' digital journeys.

Our approach is built on a foundation of empathetic, human-focused experience design that ensures value and continuity from concept to release.

WE IDENTIFY WHERE YOU ARE.

WE PREPARE YOU FOR THE ROAD AHEAD.

WE TAKE YOU WHERE YOU NEED TO GO.

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

NORTH AMERICAN HQ

201 W. 5th Street, Suite 1550
Austin, TX 78701
USA +1 866 687 3588 (USA)
+1 647 948 7638 (Canada)

EUROPEAN HQ

30 Cannon Street
London EC4M 6XH
United Kingdom
+44 333 006 4341

info@softserveinc.com
www.softserveinc.com

softserve