CASE STUDY

SECURITY CENTER OF EXCELLENCE AND DEVSECOPS FOR A LEADER IN LOYALTY BUSINESS

Improved infrastructure and application security with 20% reduced capital expenses

Client Background

Our client is a leading loyalty and customer engagement solutions company serving millions of consumers through their solutions and partner programs. They enable brands to connect, engage with their customers and expand the value of customer relationship. The client had acquired multiple small loyalty businesses that dealt customer critical data in the AWS cloud environment. However, the acquired companies lacked a consistent security standards & procedure. Besides, security vulnerabilities and threats were a part and parcel of their business applications and workflows.

The key objectives of the client included:

- Develop a coherent security and compliance practice for all the acquired companies to eliminate security blind spots
- Build a secure and resilient CI/CD pipeline with automated deployment of AWS infrastructure and multiple applications in their respective pipeline
- Build security service APIs to leverage consistent security posture across their business entities

Xoriant Solution | Key Contributions

The client engaged Xoriant for security assessments of their IT environment, build security solutions and services and be a part of their Security Center of Excellence (COE) team. Being a trusted security advisor, Xoriant was the chosen technology partner performing extensive cyber security assessments in the client's global customer engagement platform. They wanted to leverage Xoriant's capability in developing automated security solutions and

KEY BENEFITS

- Ensured consistency in usage of compliance and security standards.
- 20% reduction in capital and operational expenditure using services built on cloud serverless technology.

best practices to tackle the latest and evolving security threats besides making them efficient. Our key contributions included:

- Security Assessment of AWS Infrastructure, platform and applications
- Developed and deployed Serverless Access Management Solution
- Developed and deployed AWS Account Hardening Solution
- Developed and deployed Git Security Automated Code Scan Solution
- Developed and deployed SAST API Automated Code Security Scanning Solution
- Developed 45+ bots for CIS Notifications and Auto-Remediation
- Developed AWS S3 Bucket Scan for PII and PCI

Cyber Security Assessment: Xoriant performed an extensive cyber security assessment on the customer's AWS environment. The outcome included vulnerability details of infrastructure, platform, applications, and steps to remediate. Xoriant's security assessment methodology also defined risk score of the IT environment and recommended a plan to improve the Security Posture. This helped the client to plan for the risk and vulnerabilities mitigation strategy, plan remediation solutions, introduce additional security standards and risk controls for Instructure and Applications.

Serverless Access Management Solution: The client used manual provisioning and termination of temporary access to its IT resources. They lacked active cyber defence practice, cloud security training, automated reporting for compliance, data security implementation guidelines and detection, prevention and reporting capabilities. Xoriant developed and deployed a Serverless Access Management Solution that automated granting and revoking access through secured and encrypted communication channels.

AWS Account Hardening Solution: The client pursued manual provisioning of AWS accounts and infrastructure. Xoriant developed and deployed an Account Hardening Solution using AWS services and Jenkins. It included automated deployment of all the configuration steps with high levels of isolation of resources and security, thereby supporting the organization with multiple

KEY BENEFITS

- 90% improvement in TAT using automated and secured access grant/revoke.
- Secured and encrypted communications.
- Reduced security risk to AWS infrastructure, compliant with CIS standards.
- Improved security for PII and PCI.

AWS accounts. This increased the security of the AWS environment as per CIS standards and significantly dropped the risk of the cyber-attack.

Git Security Automated Code Scan Solution: The client lacked internal assessments such as code repository scanning. To ensure regular coding is done as per the best secured coding standards, Xoriant developed and deployed the Git Security Automated Code Scan Solution that scans repositories from GitHub, CodeCommit and BitBucket and redacts exposed secrets in the final report. This solution fixed the source code vulnerabilities related to identity and credential theft thereby protecting the organization from possible attacks.

SAST API Automated Code Security Scanning Solution: The client's development team did not exercise a standard secure SDLC practice and struggled with security outreach in product teams. Xoriant developed a SAST API Automated Code Security Scanning Solution using Veracode. This included just one secured API for all product teams to scan multiple apps in a single scan. Thus, ensuring consistency in scanning, reporting and improving application security runtime.

Bots for CIS Notifications and Auto-Remediation: The client lacked a secure AWS infrastructure and auto remediation. Xoriant security team developed and deployed 45+ operational bots for CIS notifications and auto-remediation using AWS SNS, Lambda and DivvyCloud Bot Factory. This resulted in cloud resources complying CIS L2 via auto-remediation. In case of any non-compliance, cloud owners get early notifications.

S3 Bucket Scan for PII and PCI: The client missed data classification and security implementation guidelines for PCI and PII. Xoriant improved the security for PII and PCI by developing an S3 bucket Scan using AWS serverless services and DivvyCloud Bot Factory. The solution supports scan on text files, CSV files, notifies account owners for possible leaks in S3 buckets and improves security for ensuring files at S3 follow PCI compliance standards.

KEY BENEFITS

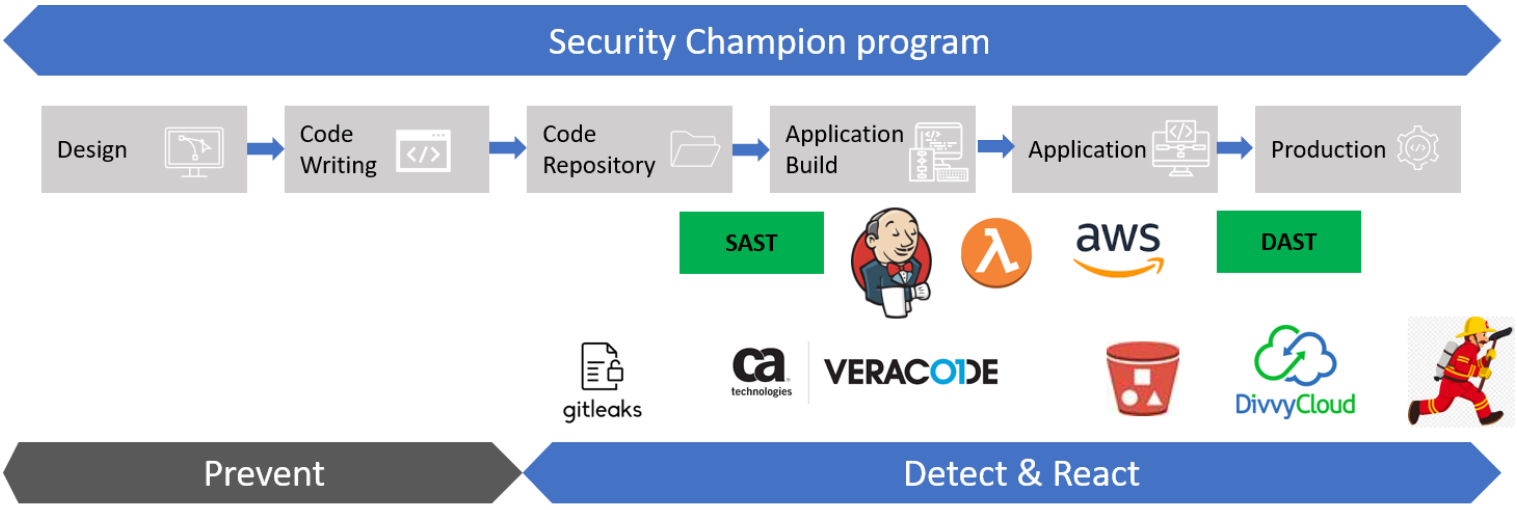
- Exhibited a fully secured and auditable process.
- Assurance of adherence to security processes via secure and automated CI/CD.
- Enhanced the application security runtime.
- Post implementation of the above solutions, risk score dropped from 4 to 3 as per the Xoriant's assessment methodology, resulting in improved Security Posture of infrastructure and applications.

Client Testimonial

Xoriant team's contribution in bringing the risks down and thereby improve the security posture of our IT organization by developing and implementing the remediation solutions are highly appreciated. Their capability in security space is making us ready to combat the cyber threat and vulnerabilities. The entire DevSecOps team and AWS CloudOps team were in unison right from the start in automating and building the security services.

- Senior Director, Application Security

High Level Architecture



Technology Stack

AWS Cloud Services: Serverless Lambda, API Gateway, RDS, CloudWatch, SNS, SES, Cloud Formation, DivvyCloud | Jira | Confluence | Jenkins | Ansible | Veracode | Python | Go Lang Groovy

Xoriant is a product engineering, software development and technology services company, serving technology startups as well as mid-size to large corporations. We offer a flexible blend of onsite, offsite and offshore services from our eight global delivery centers with over 3600 software professionals. Xoriant has deep client relationships spanning over 30 years with various clients ranging from startups to Fortune 100 companies.