Managed Security Services and DevSecOps for an International Publishing Company

Business Scenario

The customer needed a strategic partner to deliver managed cloud services for applications and cloud infrastructure hosted in AWS. As part of the engagement, the customer wanted the partner to enhance the security posture in application development life cycle and provide managed security services as it's important for the customer to safeguard sensitive data like PII data hosted in the cloud environment.

Our Solution

To address customer business challenge, Tech Mahindra Security team performed a due-diligence of an existing security controls deployed. Post due-diligence outcome we have proposed the security controls to improve an application security and development life cycle by adopting DevSecOps model.

As part of the DevSecOps cycle, we performed Threat Modelling while building application architecture, integrated secure code scanning and application vulnerability scanning through CI/CD pipeline for continuous scanning and Runtime Application Self-Protection. This has helped the customer to reduce the application turn around cycle and enhance the security posture.

The following services are provided to the customer as part of Managed Security services:

- **Next-Generation Firewall:** Managing Fortinet's Fortigate as Next-Generation Firewall and protecting the network, applications and infrastructure from external adversaries. Reviewing and fine tuning of security policies on an ongoing basis to accommodate the ongoing business application changes.
- **DDoS & WAF:** Managing Cloud Front as landing zone which includes AWS Shield as DDoS protection and AWS WAF as Web Application Firewall to protect OWASP Top 10 attacks to secure hosted application in cloud environment. Managing the alerts from WAF and DDoS and fine tuning the security policies to improve the security posture.
- Investigates alerts from AWS shield and WAF to proactively detect and mitigate cyber threats. Critical incidents are resolved on priority and reports are shared with the customers.
- **Compliance**: Performing Continuous Compliance on AWS infrastructure leveraging Cloud Custodian compliance tool, integrated with AWS Config to provide the compliance view and remediating the identified misconfigurations and deploying the best practices.
- **SOC**: Security professional experts monitoring the logs from CloudTrail, CloudWatch, Compliance monitoring from AWS Config.

About the Company

Leading International Publishing Company –
One of largest publisher and learning enabler changing students' lives through learning, which is a great and inspiring responsibility. By linking research to learning practice, they develop engaging content and pioneering products for students that are empathetic, highly effective, and help students learn better.

AWS Services Volume

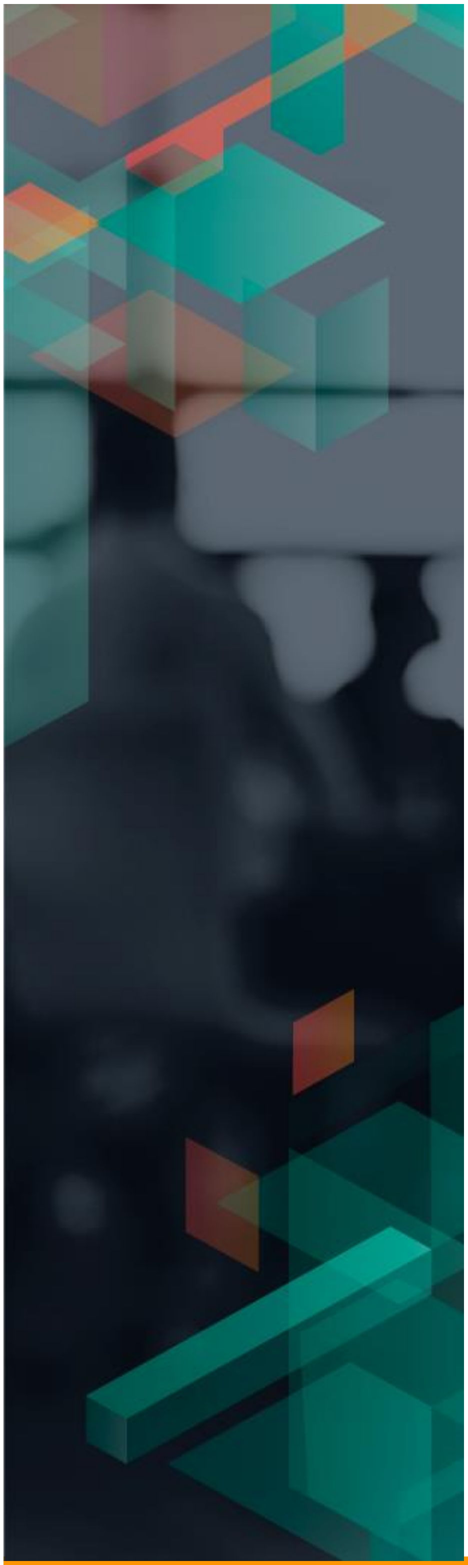
- 800 EC2 Instances
- 300 Production instances
- 50+ Database services

AWS Services Consumed

- Amazon Cloud Watch
- AWS Cloud Trail
- AWS VPN Services
- AWS Route53
- AWS Shield
- AWS WAF
- AWS Config

AWS Marketplace

- Fortinet Fortigate Next-Generation Firewall
- Cloud Custodian
- Micro Focus Fortify
- Qualys



- **Vulnerability Assessment:** Performing vulnerability assessment on a monthly basis to secure and reduce threats and risks.
- **Coordination:** Coordinated with application and infrastructure stakeholders to remediate the identified vulnerabilities proactively.
- **Remediations:** Remediating the highly critical vulnerabilities on the AWS EC2 instances through timely patching. The security patches for the Operating System are applied through AWS Systems Manager that gets deployed to Non-Production servers and then to production servers as per the Tech Mahindra Managed Cloud Operations (mCOPS) process.
- **Application Security Testing:** Performing Dynamic Application Security Testing (DAST) and Static Application Security Testing (SAST) using Micro Focus Fortify Application Security tools as per defined intervals in the application change cycles.
- **DevSecOps:** Managing CI/CD pipeline to ensure the development and operations are securely performed across life cycle of SDLC. Also, implemented threat modeling to ensure that all application or websites to reduce the attack surface from adversaries.

Value Delivered

- ✓ Protecting customer's AWS cloud environment using multi-layered defense with a combination of AWS native and third-party security controls
- ✓ Enhanced Security posture
- ✓ DevOps to DevSecOps - Security embedded in application development cycle itself
- ✓ Cloud Compliance and Configuration management using automation tools and scripts
- ✓ Proactive Threat Management through Vulnerability Assessment Services
- ✓ Hassle-free process for vulnerabilities remediation and patching the cloud services

About Tech Mahindra

Tech Mahindra's Enterprise Security & Risk Management Services team, with 18+ years of Cyber Security experience, act as a trusted advisor – consultant, system integrator and managed security service provider. We help customers to secure their digital transformation journey by, addressing all their cloud security needs by protecting their cloud environment, providing unified visibility, and ensuring compliance.

Tech
Mahindra