Deloitte.

A financial services organization automates security and reporting

CHALLENGE	A large financial services organization's information security team intended to transition from manual processes, which involved considerable processing and wait times for requestors, to on-demand automation and self service to facilitate app teams' cloud migration.
APPROACH	Informed by client workshops, Deloitte's solution architects and engineers designed a cloud-first automation and reporting capability and using an agile delivery methodology.
OUTCOME	More than 90% of their infrastructure security has been automated. Additionally, the team can create new production ready environments with supporting cybersecurity guardrails in less than 3 hours, streamlining operational processes and reducing costs.

Our client, a large financial services organization, was looking to streamline their operations and improve their security posture. Through a series of workshops, Deloitte identified the client's requirements and use cases that informed the automation and reporting capabilities which Deloitte's architects and engineers built using an agile methodology.

Security automation capabilities implemented a cloud-first and serverless application model, leveraging a combination of automated tooling and security specialists. Continuous monitoring also aggregated Amazon Web Services (AWS) resource logs across network, host, and application programing interface (API) layers to analyze and triage security events. Deloitte designed alert pipelines to

view, analyze, and remediate operational workflows. These capabilities also enabled routine scanning of AWS infrastructure resources for known software vulnerabilities, and newly added resources are automatically discovered and available for scanning. AWS metadata for scanned AWS infrastructure is available as part of scan results to better enable more effective reporting and decision making.

Deloitte also delivered cloud managed cybersecurity services across workstreams, including:

- AWS Infrastructure Vulnerability Scanning
- Distributed Denial of Service (DDoS) Mitigation
- Managed Intrusion Prevention System (IPS) , Managed Detection and Response for AWS Endpoints
- Managed Web Application Firewall (WAF)
- AWS Compliance Monitoring (Monitor, Triage Security Events)

Enabling automation

An agile team implemented a continuous integration/deployment (CI/CD) pipeline in DevOps, deploying the information security services to the client's cloud environments. Key workstream results enabled:

- Increased frequency and speed of releases to keep pace with business demands
- Automated security tasks to reduce delivery time and provide more consistent security services to further secure cloud environments
- Enabled the business to shift security left in software development life cycle (SDLC) processes by providing self-service capabilities for application teams to consume information security capabilities
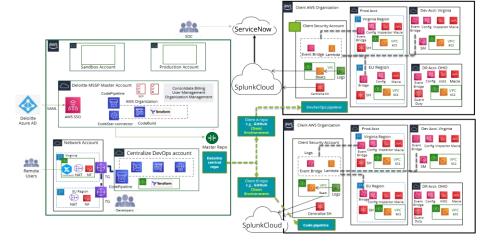
Scope and complexity

The project involved deploying, protecting, and managing:
AWS EC2 instances
AWS Firewall Manager
Lambda
AWS WAF
AWS Advance SHIELD
GuardDuty encryption keys and certificate manager
AWS Transit Gateway
Prisma Cloud

Cloud compliance frameworks for privacy and data protection criteria that meet standards and regulations like HIPAA, ISO 27001, SOC2, CCPA, PIPEDA, MITRE ATT&CK, CIS AWS Foundations Benchmark v1.3, CSA CCM, GDPR, HITRUST CSF V9.3, NIST-800, SOC2, ISO27001, and PCI DSS v3.

Industry compliance frameworks: Palo Alto Networks firewall, TrendMicro, Cloudstrike, Okta ASA/SSO, Prisma Compute, Nessus, Hashicorp Key vault, ServiceNow, etc.

Cloud reference architecture | Cyber cloud managed services

Illustrative architecture for securely deploying AWS to support multiple enterprise applications and user base

Contact us:

Aaron Brown
Cyber Cloud Managed Services Leader
Partner | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
aaronbrown@deloitte.com

Fiona Williams
Advisory AWS Alliance Leader
Partner | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
fwilliams@deloitte.com