Stability | Security | Compliance

Scope of Work

CyberSecurity in AWS:
Assess, Identify and Deliver the best Cyber Security environment and Compliance framework's best practices for the Client's AWS presence

Digital Edge

Circumstances and Challenges

The Client has evolved from a centralized, stable and secure IT environment to a multi-dimensional business with multi-product oriented management for which the core infrastructure controls have become fragmented and as a result, not meeting the business' overall required compliance standards. The challenge is to restore centralized Security oversight and implement the required cybersecurity best practices to meet the Company's overall compliance requirements across all platforms and overcome the current threat environment.

Deliverables

1. Cloud readiness assessment report,
2. Recommendations for AWS Services Protecting Network & Host-Level Boundaries,
3. Recommendations for AWS Services for Security Configurations,
4. Recommendations for SDLC implementation and integration of automated vulnerability scanning into Continuous Development pipeline,
5. Recommendations for Monitoring, Alerting and Incident response,
6. Recommendations for Environment Hardening.

High Level Requirements

a) Assess existing IT environment's application architecture and infrastructure;
b) Review and understand Customers business goal's when including cloud operations into their processes;
c) Provide best practices' recommendations for adoption of secure AWS cloud environment based on various widely accepted security and compliance frameworks…
   - Systems hardening – CIS Benchmarks. Both L1 and L2 levels are considered, depending on system purpose and business requirement,
   - System Development Lifecycle – NISP SP 800-64, ISO 27001, OWASP Secure Coding Practices,
   - Cloud design – AWS Cloud Best Practices, NIST Cloud Computing Reference Architecture (SP 500-292),
   - Cloud security – NIST SP 500-299 Cloud Computing Security Reference Architecture, AWS alignment to NIST CSF.

Process

1. Discovery of Existing Environment

Conduct interviews to understand customers' vision, goals and objectives when including cloud operations into their processes. Our analysis will utilize these topics/points in order to develop a complete understanding of the existing environment in order to deliver optimal assessment value including design and build an integration path within the existing model for AWS-based operations that meets the Cloud strategy/vision/goals.

1.2 Current application architecture

Review all existing applications expected to be moved to the cloud environment and assess their readiness for migration. Identify which AWS services would be required or recommended for usage.
Explore/discuss viability of "containerized" benefits approach versus standard EC2 instances.
Topics covered:

- Applications list and their description,
- Utilized programming languages and frameworks,
- If Secure Development Lifecycle has been utilized and how,
- Application components,
- Data flow, application interfaces and data classification.

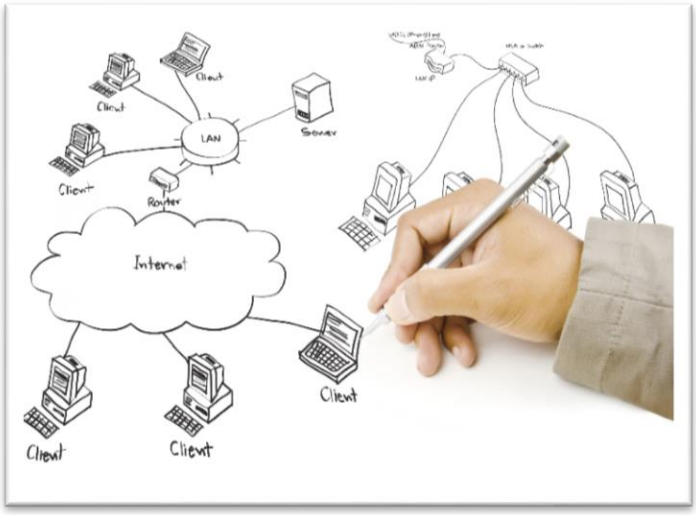
1.1 Current cloud state capability

- Description of existing IT infrastructure,
- On-site or off-site hosting,
- Development lifecycle,
- Existing frameworks,
- Current Risk Management program,
- Current Security Governance program,
- Cloud strategy/vision/goals,
- Availability of existing programs or initiatives that could impact cloud migration,
- Applicability of any legal or compliance regulations, privacy standards.

1.3 Current application architecture

Explore Identify requirements for identity management, user authentication and authorization…

- Existing authentication providers,
- Current principles of authorization; Is RBAC implemented? Control granularity?



1.4 Network design

Identify application networking requirements.

- Network design review,
- Network segmentation,
- Network and Host-Level Boundaries,
- SSL configuration… requirements, endpoints and termination points.

2. AWS Cloud Recommendations

Based on information received from previous activities, provide and discuss recommendations for AWS configurations.

2.1. Infrastructure hardening

Recommend and discuss best practices for implementing hardened AMIs following CIS benchmarks, applicable business requirements and AWS cloud computing specifics.

***Please note CIS hardened OS images, available from Amazon Marketplace, offer only partial compliance to CIS Benchmarks due

2.2. Integration of vulnerability scanning for web application continuous development lifecycle

- Recommend a proactive approach to security standards and vulnerability prevention.
- Explore and discuss integration of automated scanning tools (such as OWASP ZAP) and statistical code analyzers into the development pipeline.

2.3. Data protection

Our recommendations include approaches to ensure data protection, both in-transit and at rest using available AWS tools.

2.4. Audit and Monitoring

Based on environment, applications and the vision/goals' requirements, deliver recommendations for building a 24/7 monitoring solution, metrics to monitor, how to react to failures, and integration with incident response ticketing systems.