IBM **Consulting**

IBM Security Services for Cloud:

Rapid AWS Assessment

As you accelerate your migration to AWS Cloud, how can you ensure your environment is secure and compliant?

99%

of cloud failures through 2023 will be the customer's fault[1]

66%

Of security decision makers see cloud security best practice frameworks as very valuable[2]

Dive deep into your AWS environment's security posture with IBM Security

Our Rapid Cloud Security Assessment can bring visibility into security misconfigurations, traffic analysis, and your compliance posture against security and data privacy frameworks (such as NIST, ISO, CCPA, HIPAA, and PCI) across your AWS environment. This assessment walks through the security findings in an interactive, structured session which provides key recommendations to closing those gaps in a security assessment report.

This assessment is performed within a 2-week period and provides a comprehensive analysis of:

- **Your existing cloud architecture** for security implementation
- **Account structure** including subscriptions and resource tagging
- **Monitoring and log management** including AWS Security Hub, Amazon CloudWatch and Amazon GuardDuty
- **Compliance checks** for PCI DSS, HIPAA, CIS Benchmarks, NIST CSF/800-53, etc.
- **Data encryption** including AWS Key Management Service, Amazon Macie, and storage objects
- **Network and application security** including AWS Network Firewall, AWS Web Application Firewall, and AWS Shield
- **Identity and access management** including SSO, conditional access, MFA, and rotation of credentials
- **Monitoring controls** for AWS Security Hub, insights and recommendation
- **Your incident response plan** along with recommendations based on what is uncovered

[1] Gartner, Innovation insight for Cloud Security Posture Management , 2019

[2] Forrester Cloud Security Spotlight Report, 2021

Format and deliverables

- A typical rapid assessment is completed over a 2-week period and can be delivered in person or virtually
- The format is an interactive session combined with automated analysis
- This assessment is facilitated and reviewed by cloud security specialists – ensuring contextualized and tailored recommendations

Client success story

IBM Security led a large automotive manufacturer's modernization initiative with a 2-week Rapid Cloud Security Assessment.

The assessment provided clear visibility of cloud inventory and resource configurations across the cloud estate; identified compliance posture, gaps and risk analysis across key cloud areas; provided visibility into network exposure to the external world; and prioritized remediation actions to harden cloud environments.

Leading with a successful Security assessment resulted in the client's decision to accelerate their modernization to AWS Cloud.

Key benefits

- Get a deep understanding of your vulnerabilities to cyber attack and risk of business loss across your AWS environment
- Align compliance policies to industry standards, AWS recommend best practices, CIS benchmarks, NIST CSF, MITRE ATT&CK, etc.
- Remediation recommendations based on analysis of your organization's security posture by evaluating vulnerabilities, identity, and compliance risks.

aws PARTNER Premier Tier Services

- L1 MSSP Services Competency
- Security Services Competency
- Security Software Competency

IBM Security

Clients are responsible for ensuring their own compliance with various laws and regulations. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.