Capgemini | aws

AWS LEVEL1 MSSP BY CAPGEMINI

The 24/7 Security Alarm For Your Cloud Environment

Let us take your cloud security weight off your shoulders. As an AWS Level 1 Managed Security Service Provider (MSSP), we have worked closely with AWS security experts to develop the required managed security service (MSS) specializations , covering 10 specific area of setting up your Security Posture The AWS Level 1 MSS is uniquely designed to protect and monitor your essential AWS resources, delivered to you as a fully managed service.

QUALIFICATIONS YOU CAN TRUST

Let us take your cloud security weight off your shoulders. As an AWS Level 1 Managed Security Service Provider (MSSP), we have worked closely with AWS security experts to develop the required managed security service (MSS) specializations , covering 10 specific area of setting up your Security Posture The AWS Level 1 MSS is uniquely designed to protect and monitor your essential AWS resources, delivered to you as a fully managed service.

Whether your company is new to security or already staffed with cloud security professionals, we are happy to either become your outsourced cloud security team or be integrated into your internal security teams' operations Either way, you will benefit from our close collaboration with AWS security experts in the integration of native AWS security services and AWS Security Competency Technology Partner tools that our staff of cyber professionals leverage to provide you AWS Level 1 MSS.

KEEPING CLOUD DATA SECURE 24/7

How We Address Cloud Security Challenges:

1. AWS Infrastructure Vulnerability Scanning

Routine Scanning of AWS infrastructure resources for known software vulnerabilities.

Benefits: Identifies infrastructure in your environment that is subject to known vulnerabilities. Helps to maintain external compliance standards.

2. AWS Resource Inventory Visibility

Continuous scanning and reporting of all AWS resources and their configuration details updated automatically with newly added or removed resources.

Benefits: Maintain full visibility into what AWS resources are being added, changed, or removed across your organization to help reduce business risk from unsanctioned activity.

3. AWS Security Best Practices Monitoring

Detect when AWS accounts and the configuration of deployed resources do not align to security best practices.

Benefits: Track and detect misconfigurations of AWS resources to improve cloud security posture and reduce business risk.

4. AWS Compliance Monitoring

Scanning your AWS environment for compliance standards on two or more of the following: CIS AWS Foundations, PCI DSS, HIPAA, HITRUST, ISO 27001, MITRE ATTACK, AND SOC2.

Benefits: Improve cloud security governance and compliance posture and reduce business risk.

5. Monitor, Triage Security Events

A combination of automated tooling and security experts continuously monitors aggregated AWS resource logs across network, host, and API layers to analyze and triage security events.

Benefits: Gain full visibility into security alerts related to your AWS environment, with a consolidated list of security events and recommended remediation guidance.

6. 24/7 Incident Alerting and Response

Receive notification of high-priority security events and expert guidance on recommended remediation steps 24/7.

Benefits: Respond quicker to high-priority security events, reducing event impact and business risk.

7. Distributed Denial of Service Mitigation (DDoS)

A system backed by technology and security experts monitoring 24/7 for Distributed Denial of Service attack against your AWS applications.

Benefits: Increase visibility and resilience to DDoS attacks and reduce the risk of availability, financial, and security impacts to your applications.

8. Managed Intrusion Prevention System

Protect your environment from known and emerging network threats that seek to exploit known vulnerabilities.

Benefits: Add a layer of security for your AWS-based endpoints, helping with defense against known threat patterns, increasing your overall security posture.

9. Managed Detection & Response for AWS Endpoints

A combination of technology and cloud security experts working to continuously detect, investigate, and remove threats from within your AWS endpoints.

Benefits: Free up internal resources and decrease your business risk with continuous detection, investigation, and remediation of AWS endpoint security events.

10. Managed Web Application Firewall

A firewall managed service designed to protect web-facing applications and APIs against common exploits.

Benefits: Maintain high web application and API availability and reduce risk of compromised security, or consumption of excessive resources

OUR EXPERTS

Ravi Khokhar
Vice President, Head of Cloud
Capgemini Financial Services
ravinder.khokhar@capgemini.com

Shashi Gupta
Senior Director, Head of AWS Center of Excellence
Capgemini Financial Services
shashi.gupta@capgemini.com

Ramandeep Singh
Senior Director, Platform Engineering,
Cloud Solutions, and Security
Capgemini Financial Services
ramandeep.singh@capgemini.com

Sales By Product
Services
Upgrades
Hardware
Software
Subscriptions
Last 30 days
Updated 15 Min ago
Retention
81%
69%
85%
Profit and Loss summary
Affiliates Sales
Last 24 Hours
Updated 1 Min ago

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of 270,000 team members in nearly 50 countries. With its strong 50 year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fuelled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2020 global revenues of €16 billion.

Get the Future You Want | www.capgemini.com