AWS Security Best Practices – Intensive Training («AWSB09»)

Möchten Sie wissen, wie Sie eine sichere Umgebung in der AWS-Cloud aufbauen und aufrechterhalten können? Der Kurs AWS Security Best Practices hilft Ihnen, Lösungen zu entwerfen und zu implementieren, um Ihre Workloads sicher zu halten.

Dauer: 1 Tag
Preis: 900.– zzgl. 8.1% MWST
Kursdokumente: Digitale Original-AWS-Kursunterlagen

Inhalt

Derzeit können sich die durchschnittlichen Kosten einer Sicherheitsverletzung auf über 4 Millionen US-Dollar belaufen. AWS Security Best Practices bietet einen Überblick über einige der branchenüblichen Best Practices für die Verwendung von AWS-Sicherheits- und Kontrolltypen. Dieser Kurs hilft Ihnen, Ihre Verantwortlichkeiten zu verstehen, und bietet gleichzeitig wertvolle Richtlinien, wie Sie Ihre Arbeitslast sicher halten können.
Sie lernen, wie Sie Ihre Netzwerkinfrastruktur mit soliden Designoptionen sichern können. Sie lernen auch, wie Sie Ihre Rechenressourcen härten und sicher verwalten können. Schliesslich können Sie durch das Verständnis der AWS-Überwachung und -Warnungen verdächtige Ereignisse erkennen und melden, damit Sie im Falle einer potenziellen Gefährdung schnell reagieren können.

Modul 1: Überblick über die AWS-Sicherheit

- Modell der geteilten Verantwortung
- Kundenherausforderungen
- Rahmenwerke und Standards
- Etablierung von Best Practices
- Einhaltung der Vorschriften in AWS

Modul 2: Absicherung des Netzwerks

- Flexibel und sicher
- Sicherheit innerhalb der Amazon Virtual Private Cloud (Amazon VPC)
- Sicherheitsservices
- Sicherheitslösungen von Drittanbietern

Übung 1: Kontrolle des Netzwerks

- Erstellen einer Netzwerkinfrastruktur mit drei Sicherheitszonen
- Netzwerksegmentierung mit Hilfe von Sicherheitsgruppen, Network Access Control Lists (NACLs) und öffentlichen und privaten Subnetzen implementieren
- Den Netzwerkverkehr zu Amazon Elastic Compute Cloud (EC2) Instanzen mit Hilfe von VPC Flow Logs überwachen

Modul 3: Amazon EC2-Sicherheit

- Härtung von Rechenleistung
- Amazon Elastic Block Store (EBS) Verschlüsselung
- Sichere Verwaltung und Wartung
- Erkennen von Schwachstellen
- AWS Marketplace verwenden

Übung 2: Sichern des Startpunkts (EC2)

- Ein benutzerdefiniertes Amazon Machine Image (AMI) erstellen

- Bereitstellen einer neuen EC2-Instanz von einem benutzerdefinierten AMI
- Eine EC2-Instanz mit AWS Systems Manager patchen
- Ein EBS-Volume verschlüsseln
- Verstehen, wie die EBS-Verschlüsselung funktioniert und wie sie sich auf andere Vorgänge auswirkt
- Sicherheitsgruppen verwenden, um den Verkehr zwischen EC2-Instanzen auf den verschlüsselten Verkehr zu beschränken

Modul 4: Überwachung und Alarmierung

- Protokollierung des Netzwerkverkehrs
- Protokollierung des Benutzer- und API-Datenverkehrs (Application Programming Interface)
- Sichtbarkeit mit Amazon CloudWatch
- Verbessern der Überwachung und Alarmierung
- Überprüfen Ihrer AWS-Umgebung

Übung 3: Sicherheitsüberwachung

- Konfigurieren einer Amazon Linux 2-Instanz zum Senden von Protokolldateien an Amazon CloudWatch
- Erstellen von Amazon CloudWatch-Alarmen und -Benachrichtigungen zur Überwachung von fehlgeschlagenen Anmeldeversuchen
- Erstellen von Amazon CloudWatch-Alarmen zur Überwachung des Netzwerkverkehrs durch ein NAT-Gateway (Network Address Translation)

Key Learnings

- Entwurf und Implementierung einer sicheren Netzwerkinfrastruktur
- Entwurf und Implementierung von Rechensicherheit
- Entwurf und Implementierung einer Protokollierungslösung

Zielpublikum

Dieser Kurs richtet sich an folgende Job-Rollen:

- Solution Architect
- Cyber Security
- CloudOps
- DevOps

Warum sollten Sie an diesem Kurs teilnehmen? Welchen Nutzen bringt Ihnen diese Schulung? **The Voice of the Instructor beantwortet diese Fragen**. Wir haben unser Trainerteam gebeten, einen kurzen Text darüber zu verfassen, WARUM dieser Kurs für die jeweilige Jobrolle relevant ist und was Sie von der Teilnahme an diesem Kurs erwarten können. Sie finden diesen Abschnitt in der Kursbeschreibung unter *«Zusatzinfo»*.

Anforderungen

Es wird empfohlen, dass die Teilnehmenden den folgenden Kurs besucht haben (oder über gleichwertige Kenntnisse verfügen):

- AWS Security Essentials – Intensive Training («AWSE04»)

Zusatzinfo

Voice of the Instructor

Die Teilnahme am Kurs «AWS Security Best Practices» kann Personen und Unternehmen viele Vorteile bringen. Hier sind einige Gründe, warum Sie eine Teilnahme in Erwägung ziehen sollten:

1. Erweitertes Sicherheitswissen: Der Kurs vermittelt Ihnen ein umfassendes Verständnis der AWS Security Best Practices. Sie lernen verschiedene Sicherheitskonzepte, Techniken und Tools kennen, die speziell für die AWS-Umgebung gelten. Mit diesem Wissen können Sie Ihre AWS-Infrastruktur und -Anwendungen effektiv schützen und das Risiko von Sicherheitsverletzungen und unberechtigten Zugriffen reduzieren.
2. Schutz von Daten und Vermögenswerten: AWS ist ein führender Cloud Service Provider, der eine grosse Menge sensibler Daten und kritischer Infrastruktur für Unternehmen weltweit hostet. Durch die Teilnahme an diesem Kurs erhalten Sie Einblick in die Sicherung Ihrer AWS-Ressourcen, den Schutz Ihrer Daten vor unbefugtem Zugriff, die Implementierung von Verschlüsselung und die Einrichtung sicherer Netzwerkkonfigurationen. Auf diese Weise können Sie Ihre Unternehmenswerte schützen, das Vertrauen Ihrer Kunden erhalten und relevante Sicherheitsvorschriften einhalten.
3. Reduzierung der Sicherheitsrisiken: Da sich die Cyber-Bedrohungen ständig weiterentwickeln, ist es wichtig, sich über die neuesten Sicherheitspraktiken auf dem Laufenden zu halten. Dieser Kurs behandelt häufige Sicherheitsrisiken und Schwachstellen, die speziell für AWS gelten, und zeigt Ihnen, wie Sie diese effektiv mindern können. Sie lernen Best Practices für Identity- und Access-Management, Netzwerksicherheit, Monitoring und Logging, Incident Response und vieles mehr kennen. Durch die Anwendung dieser Best Practices können Sie Sicherheitsrisiken proaktiv reduzieren und auf potenzielle Vorfälle angemessen reagieren.
4. Anerkennung in der Branche und beruflicher Aufstieg: AWS-Zertifizierungen und Schulungen haben in der IT-Branche einen hohen Stellenwert. Durch die Teilnahme am Kurs «AWS Security Best Practices» erwerben Sie wertvolle Kenntnisse und Fähigkeiten, die Sie in Ihrem Lebenslauf oder Berufsprofil ausweisen können. Dadurch können Sie sich von anderen abheben, Ihre Marktfähigkeit erhöhen und Karrieremöglichkeiten in den Bereichen Cloud-Sicherheit und AWS-Funktionen eröffnen.
5. Compliance und Auditfähigkeit: Viele Branchen haben spezifische Compliance-Anforderungen, wie z.B. HIPAA für das Gesundheitswesen oder GDPR für den Datenschutz. Der Kurs «AWS Security Best Practices» zeigt Ihnen, wie Sie Ihre AWS-Sicherheitsmassnahmen mit den relevanten Compliance-Standards in Einklang bringen. Sie erfahren, wie Sie die erforderlichen Kontrollen implementieren, Audits durchführen und die Dokumentation pflegen, um die Compliance Ihres Unternehmens sicherzustellen und Strafen zu vermeiden.

Denken Sie daran, dass sich die Sicherheitslandschaft ständig weiterentwickelt und dass es wichtig ist, über die neuesten Best Practices auf dem Laufenden zu bleiben. Durch die Teilnahme am Kurs «AWS Security Best Practices» erwerben Sie das Wissen und die Fähigkeiten, die Sie benötigen, um Ihre AWS-Infrastruktur zu sichern, Ihre Daten zu schützen und die Herausforderungen der Cloud-Sicherheit zu meistern.

Weiterführende Kurse

- Security Engineering on AWS – Intensive Training («AWSS04»)
- Advanced Architecting on AWS – Intensive Training («AWSA02»)
- Advanced Architecting on AWS with JAM – Intensive Training («AWSA2J»)
- AWS Security Governance at Scale – Intensive Training («AWSE07»)

Haben Sie Fragen oder möchten Sie einen Firmenkurs buchen?

Wir beraten Sie gerne unter 044 447 21 21 oder info@digicomp.ch. Detaillierte Infos zu den Terminen finden Sie unter www.digicomp.ch/weiterbildung-digital-transformation-technologies/cloud/amazon-web-services-aws/aws-devops/kurs-aws-security-best-practices-intensive-training