TEKNOLOGISK INSTITUT

Virtuelt kursus
3 dage
Nr. 87925 P

DKK 23.999
ekskl. moms

Dato
28-05-2024

Sted
Virtuelt kursus

Security Engineering on AWS

Lær, hvordan du effektivt bruger AWS sikkerheds services til at forblive sikker og kompatibel i AWS skyen. Kurset fokuserer på best practices sikkerhedsanbefalinger fra AWS som du kan anvende til at styrke sikkerheden af din data og dine systemer. Kurset fokusere på de centrale services i AWS for compute, lagering, automatisering, overvågning, logning og reaktion på sikkerhedshændelser.

Lær i dine egne omgivelser

Lær med andre kursister

Spar tid og udgifter på transport

Adgang til undervisnings-materiale

Deltagerprofil

Teknologisk Institut
kurser@teknologisk.dk
+45 72 20 30 00

Dette kursus er for Security Engineers, Security Architects, Security Analysts, Security Auditors eller andre som er ansvarlige for styre, revidere og teste organisationens it-infrastruktur samt sikre, at den er i overensstemmelse med retningslinjer for sikkerhed, risiko og overholdelse af politikkerne.

Forudsætninger

Vi anbefaler at du inden du deltager på dette kursus har viden om AWS Security Fundamentals, erfaring med governance, risko og compliance samt arbejdet med it-sikkerhed i praksis, koncepter for it-infrastruktur og er bekendt med cloud computing koncepter.

Udbytte

- Assimilate and leverage the AWS shared security responsibility model
- Architect and build AWS application infrastructures that are protected against the most common security threats
- Protect data at rest and in transit with encryption
- Apply security checks and analyses in an automated and reproducible manner
- Configure authentication for resources and applications in the AWS Cloud
- Gain insight into events by capturing, monitoring, processing, and analyzing logs
- Identify and mitigate incoming threats against applications and data
- Perform security assessments to ensure that common vulnerabilities are patched and security best practices are applied

Det får du på arrangementet

- Erfaren underviser
- Materiale på engelsk
- Undervisning på engelsk

Indhold

Introduktion

- Welcome and introductions
- Introduction to Security on AWS

Identifying entry points on AWS

- Ways to access the platform
- IAM policies
- Securing entry points
- Incident response
- Lab - cross-account authentication

Security Considerations - Web Applications

- Security points in an AWS web application environment
- Analyse a three-tier application model and identify common threats
- Assess environments to improve security

Application Security

- Securing EC2 instances
- Assess vulnerabilities with Inspector
- Apply security in an automated way using Systems Manager
- Isolate a compromised instance
- Lab - Assessing Security with Inspector and Systems Manager

Securing Networking Communications - Part 1

Teknologisk Institut
kurser@teknologisk.dk
+45 72 20 30 00

- Apply security best practices to VPC
- Implement an ELB device as a protection point
- Protect data in transit using certificates

Data Security

- Protect data at rest using encryption and access controls
- AWS services used to replicate data
- Protect archived data

Security Considerations: Hybrid Environments

- Security points outside of a VPC
- Common DoS threats

Monitoring and Collecting Logs on AWS

- Monitor events and collect logs with CloudWatch
- Use Config to monitor resources
- AWS-native services that generate and collect logs
- Lab - Server Log Analysis Part 1 - collect logs

Processing Logs on AWS

- Stream and process logs for further analysis
- AWS services used to process logs from S3 buckets
- Lab - Server Log Analysis Part 2 - analyse logs

Securing Networking Communications - Part 2

- Identify AWS services used to connect on-premise to AWS
- Data protection between on-premise and AWS
- Securely access VPC resources in other accounts

Out-Of-Region Protection

- Use Route 53 to isolate attacks
- Implement WAF to protect applications
- Use CloudFront to deliver content securely
- Protect applications using Shield

Account Management on AWS

- Manage multiple accounts
- Use identity providers / brokers to acquire access to AWS services
- Lab - AWS Federated Authentication with ADFS

Security Considerations: Serverless Environments

- How to secure data in a serverless environment
- Use Cognito to authorize users
- Control API access with API Gateway
- Use AWS messaging services securely
- Secure Lambda functions
- Lab - Monitor and Respond with Config and Lambda

Secrets Management on AWS

- Manage key and data encryption with KMS
- Describe how CloudHSM is used to generate and secure keys

- Use Secrets Manager to authenticate applications
- Lab - Using KMS

Security Automation on AWS

- Deploy security-oriented AWS environments in a reproducible manner
- Provide management and control of IT services to end-users in a self-serve manner
- Lab - Security Automation on AWS with Service Catalog

Threat Detection and Sensitive Data Monitoring

- Threat detection and monitoring for malicious or unauthorized behaviour
- Leverage machine learning to gain visibility into how sensitive data is being managed in the AWS Cloud

Form

Dette virtuelle kursus foregår på din egen computer live via GoToMeeting med en engelsktalende underviser. Under kurset har du mulighed for at stille spørgsmål, deltage i diskussioner, se whiteboard på din skærm og lave lab øvelser.

Bemærkning

Please note: Effective 15th August 2022 the labs for all AWS courses will be delivered through AWS Builder labs. In order to access these labs you will need to have an Amazon account (used for Amazon.com/.co.uk retail). You can choose to use your existing Amazon account or you can elect to set up a new account utilising a new email address (such as Hotmail, Gmail, Yahoo etc etc). You can set up your new Amazon account here.
Please ensure that you have set up this Amazon account set up in advance of attending your class. Your Amazon account credentials will be used to access the AWS Builder lab environment that you will utilise during your course.
In order to access your digital course materials you are required to set up a Gilmore account in advance of attending your course. To do this please follow this link.

Søgte du et andet virtuelt kursus?

Vi tilbyder virtuelle kurser inden for mange forskellige områder. Kontakt os på tlf. 72203000 eller kurser@teknologisk.dk, så vi kan hjælpe med at imødekomme dit behov.

Læs mere om vores virtuelle kurser og se svar på dine spørgsmål (FAQ).

UNDERVISER

Undervisningen varetages af en erfaren underviser fra Teknologisk Instituts netværk bestående af branchens dygtigste undervisere.

Har du faglige spørgsmål så kontakt

Charlotte Heimann
+45 72203147
chhn@teknologisk.dk