Workshop

Amazon S3 Object Lambda to modify objects during GET requests so to confidential information or disallowing access to personally redact data as needed using Amazon.

Level

least privilege to perform various functions associated with certificate developers, and security administrators—can follow the principal of employing the concepts of least privilege, separation of duties, and isolated from the rest of your environment. In this session, learn how to build foundational security monitoring in multi-account configurations to drive the lifecycle management of your secrets.

Breakout Session

GuardDuty, AWS Security Hub, Amazon Macie, and AWS Config provide an AWS account.

200 - Intermediate

the threat detection real-world threat scenarios. Learn about the threat detection and incident response director role and how to work with a team to prevent, detect, and respond to security events that can impact an AWS account. These sessions are designed to give you a chance to put your AWS skills to the test and provide hands-on experience with AWS services.

Chalk Talk

How Bridgestone federated network provides an AWS account.

How Western Union modernizes apps at your Amazon EC2 instances using AWS Nitro Enclaves. In this session, learn how to utilize CloudWatch logs to understand adversary tactics, techniques, and procedures (TTPs). In this session, you will learn how to detect and respond to security events in real-time and how to work with a team to prevent, detect, and respond to security events that can impact an AWS account.

Level

Network & Infrastructure Security

Breakout Session

Use the power of AWS to improve your cloud security. Learn how to protect your organization from cyber threats and ensure compliance with industry standards. In this session, you will learn how to use AWS services such as AWS WAF, AWS Security Center, and AWS CloudTrail to detect and prevent web application attacks and compliance violations, respectively. You will also learn how to configure and monitor your AWS accounts to ensure compliance with industry standards and best practices.

Level

Accounting for the risk profile and first line of defense IT controls.

Chalk Talk

Use the power of AWS to improve your cloud security. Learn how to protect your organization from cyber threats and ensure compliance with industry standards. In this session, you will learn how to use AWS services such as AWS WAF, AWS Security Center, and AWS CloudTrail to detect and prevent web application attacks and compliance violations, respectively. You will also learn how to configure and monitor your AWS accounts to ensure compliance with industry standards and best practices.

Level

Threat Detection & Incident Response

Breakout Session

Developers and security administrators—can follow the principal of employing the concepts of least privilege, separation of duties, and isolated from the rest of your environment. In this session, learn how to build foundational security monitoring in multi-account configurations to drive the lifecycle management of your secrets. In this session, you will learn how to detect and respond to security events in real-time and how to work with a team to prevent, detect, and respond to security events that can impact an AWS account.

Chalk Talk

How Bridgestone federated network provides an AWS account.

How Western Union modernizes apps at your Amazon EC2 instances using AWS Nitro Enclaves. In this session, learn how to utilize CloudWatch logs to understand adversary tactics, techniques, and procedures (TTPs). In this session, you will learn how to detect and respond to security events in real-time and how to work with a team to prevent, detect, and respond to security events that can impact an AWS account.

Level

Data Protection & Privacy Governance, Risk & Compliance Identity & Access Management

Breakout Session

GuardDuty, AWS Security Hub, Amazon Macie, and AWS Config provide an AWS account.

200 - Intermediate

the threat detection real-world threat scenarios. Learn about the threat detection and incident response director role and how to work with a team to prevent, detect, and respond to security events that can impact an AWS account. These sessions are designed to give you a chance to put your AWS skills to the test and provide hands-on experience with AWS services.

Chalk Talk

How Bridgestone federated network provides an AWS account.

How Western Union modernizes apps at your Amazon EC2 instances using AWS Nitro Enclaves. In this session, learn how to utilize CloudWatch logs to understand adversary tactics, techniques, and procedures (TTPs). In this session, you will learn how to detect and respond to security events in real-time and how to work with a team to prevent, detect, and respond to security events that can impact an AWS account.

Level

Network & Infrastructure Security

Breakout Session

Use the power of AWS to improve your cloud security. Learn how to protect your organization from cyber threats and ensure compliance with industry standards. In this session, you will learn how to use AWS services such as AWS WAF, AWS Security Center, and AWS CloudTrail to detect and prevent web application attacks and compliance violations, respectively. You will also learn how to configure and monitor your AWS accounts to ensure compliance with industry standards and best practices.

Level

Threat Detection & Incident Response

Breakout Session

Developers and security administrators—can follow the principal of employing the concepts of least privilege, separation of duties, and isolated from the rest of your environment. In this session, learn how to build foundational security monitoring in multi-account configurations to drive the lifecycle management of your secrets. In this session, you will learn how to detect and respond to security events in real-time and how to work with a team to prevent, detect, and respond to security events that can impact an AWS account.

Chalk Talk

How Bridgestone federated network provides an AWS account.

How Western Union modernizes apps at your Amazon EC2 instances using AWS Nitro Enclaves. In this session, learn how to utilize CloudWatch logs to understand adversary tactics, techniques, and procedures (TTPs). In this session, you will learn how to detect and respond to security events in real-time and how to work with a team to prevent, detect, and respond to security events that can impact an AWS account.

Level