APP SEC CBT COURSE CATALOG 2025

INFRARED SECURITY

Contents

APP SEC ESSENTIALS SERIES

Welcome to the App Sec Essentials Series. This Series of Courses provides participants with an understanding of key foundational concepts relating to application security including vulnerabilities and mitigation strategies covering industry-recognized taxonomies. Courses are organized based on a role and technical level to provide a tailored experience for the entire software team at all stages of development.

"select invoice from invoice_table where invoiceID = + data_from_user
Untrusted data could contain commands!

This series includes :

Integrating Security Throughout the SDLC

App Sec Foundations

App Sec Foundational Exam

App Sec Foundations for Managers

App Sec Foundational Exam for Managers

App Sec Foundations for Developers—*Learning Path*

Injection

Broken Authentication

Sensitive Data Exposure

XML External Entities

Broken Access Control

Security Misconfiguration

Cross-Site Scripting

Insecure Deserialization

Using Components with Known Vulnerabilities

Insufficient Logging and Monitoring

Server-Side Request Forgery

Securing the Supply Chain: Maintaining Software and Data Integrity

App Sec Foundational Exam for Developers

Mobile App Sec Foundations for Developers

Mobile App Sec Foundations for Managers

API Security

Integrating Security Throughout the SDLC

Audience: All

Duration: 1 hour

Course Description:

The Integrating Security Throughout the Software Development Life Cycle (SDLC) course raises awareness of the critical security activities necessary to build secure software for any product team members, providing resources to help formalize a secure SDLC and guidance on auditing existing activities to find gaps in your existing program.

Participants in this course will learn the following:

- What security activities should be performed during an application's lifecycle
- Provide resources to help guide the creation of a secure SDLC
- Documents with more detail on security activities
- Introduction to a security maturity model for your organization
- A method for gap assessment for your existing security activities

App Sec Foundations

Audience: Software Awareness, Introductory

Duration: 1 hour

Course Description:

This course focuses on the most common security vulnerabilities and attack vectors facing applications today. Participants will explore these vulnerabilities at a high level by analyzing real-world examples and rich visualizations. Upon completing the course, the participant will have knowledge of the risks inherent in web applications.

The course will cover the following topics:

- Introduction to Application Security
- Injection Attacks: SQL Injection
- Broken Authentication
- Sensitive Data Protection
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging and Monitoring

App Sec Foundational Exam

Audience: Software awareness, managers, and executives

Duration: 30 minutes

Exam Description:

Participants will be allowed to demonstrate their mastery of topics covered in the App Sec Foundations course via completing a 10-question graded exam.

App Sec Foundations for Managers

Audience: Software managers and executives

Duration: 1 hour

Course Description:

This course focuses on the most common security vulnerabilities and attack vectors facing applications today. Participants will explore these vulnerabilities at a high level by analyzing real-world examples and rich visualizations with specific product and project management guidance. Upon completing the course, participants will know the risks inherent in web applications.

The course will cover the following topics:

- Introduction to Application Security
- Injection
- Broken Authentication
- Sensitive Data Protection
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging and Monitoring

App Sec Foundational Exam for Managers

Audience: Software awareness, managers, executives

Duration: 30 minutes

Exam Description:

Participants will be allowed to demonstrate their mastery of topics covered in the "App Sec Foundations for Managers" course by completing a 10-question graded exam.

App Sec Foundations for Developers—*Learning Path*

Audience: Software developers, engineers, architects

Courses: 10+ courses

Duration: 4+ hours

Learning Path Description:

This ever-growing learning path focuses on the most common security vulnerabilities and attack vectors facing application developers today, as defined by industry leaders including topics addressed in the OWASP Top Ten and more! Participants of these courses will explore these vulnerabilities and challenges through a detailed analysis of real-world examples, rich visualizations of attacks, and comprehensive discussions of mitigation strategies with supporting code examples. After completing these modules, participants will be able to identify, mitigate, and prevent common security vulnerabilities within their applications more readily.

Courses Include:

Introduction to Application Security

Injection

Broken Authentication

Sensitive Data Protection

XML External Entities (XXE)

Broken Access Control

Security Misconfiguration

Cross-Site Scripting (XSS)

Insecure Deserialization

Using Components with Known Vulnerabilities

Insufficient Logging and Monitoring

Server-Side Request Forgery

Securing the Supply Chain: Maintaining Software and Data Integrity

**Course descriptions to follow individually*

Foundational Exam for Developers

Audience: Software developers, engineers, architects

Duration: 1 Hour

Exam Description:

Participants test their knowledge and have an opportunity to demonstrate their mastery of topics covered across the entire App Sec Essentials Series.

Introduction to Application Security

Audience: Software developers, engineers, architects, testers

Duration: 10 min

Course Description:

Welcome to the Introduction to Application Security course, where we introduce the App Sec Foundations for Developers Learning Path! In this course we will review the state of the web from a security perspective and explore how web vulnerabilities can be exploited and cause serious problems for organizations. Allowing Learners to prepare to dive into specific security vulnerabilities and security challenges covered in later courses within the Learning Path.

Injection

Audience: Software developers, engineers, architects, testers

Duration: 20 min

Course Description:

Welcome to the Injection eLearning course. Injection attacks are widespread and can occur whenever a user-defined input is utilized in conjunction with an interpreter. This course will raise awareness of the most common injection attacks facing our applications today. In addition, you will understand the secure programming patterns and practices needed to mitigate the risk of injection attacks.

Participants of this module will…

- Realize the wealth of interpreters used in web applications
- Understand common injection attacks such as SQL Injection
- Gain insight into the mitigation of vulnerability through variable binding

Broken Authentication

Audience: Software developers, engineers, architects, testers

Duration: 15 min

Course Description:

Welcome to the Broken Authentication eLearning course. This course will raise awareness of the most common attacks against authentication, identity management, and session management controls. In addition, you will get an understanding of the secure programming patterns needed to mitigate such risks in your own applications.

Participants of this module will…

- Be able to enumerate the most common attacks against authentication
- Understand how to mitigate those common attack vectors
- Realize how to manage sessions throughout the application lifecycle securely

Sensitive Data Exposure

Audience: Software developers, engineers, architects, testers

Duration: 30 min

Course Description:

Welcome to the Sensitive Data Exposure eLearning course. This course will raise awareness of the risks associated with the use of sensitive data within our applications. In addition, we will discuss techniques to handle sensitive data more securely as it is passed throughout the various layers of an application.

Participants of this module will…

- Hear about real-world examples of sensitive data exposure
- Understand the risk of sensitive data exposure at various application layers
- Discuss data classification and the basic application of cryptography

XML External Entities (XXE)

Audience: Software developers, engineers, architects, testers

Duration: 15 min

Course Description:

Welcome to the XML External Entities eLearning course. This course will discuss an inherent weakness in XML parsing and how a single type of default behavior can put your data and your users at risk.

Participants of this module will…

- Obtain a background on XML and XML parser capabilities
- Learn about external entities and how they are subject to abuse
- Understand how to configure XML parsers to prevent such abuse

Broken Access Control

Audience: Software developers, engineers, architects, testers

Duration: 30 min

Course Description:

Welcome to the Broken Access Control eLearning course. This course will raise awareness of the risks of using insecure direct object references and exposing privileged application functionality without the corresponding function level access control verifications. In addition, we will discuss techniques to properly manage and reduce this risk by using various secure programming patterns.

Participants of this module will…

- Learn about the dangers of relying on presentation layer access control
- Obtain strategies to implement function level access control
- Learn about the dangers of direct object references
- Obtain strategies to implement data level access control

Security Misconfiguration

Audience: Software developers, engineers, architects, testers

Duration: 25 min

Course Description:

Welcome to the Security Misconfiguration and Key Secure Configuration Principles eLearning course. This course will raise awareness of the most common security issues arising from misconfiguration. In addition, you will get an understanding of the secure configuration settings needed to mitigate such risks in your applications.

Participants of this module will…

- Understand the configuration concerns in the many layers of our application
- Discuss those fundamental secure configuration principles that can be applied to any environment
- Learn how to apply those secure configuration principles to a database and a web server

Cross-Site Scripting (XSS)

Audience: Software developers, engineers, architects, testers

Duration: 25 min

Course Description:

Welcome to the Cross-Site Scripting eLearning course. This course will raise awareness of the most common vulnerability facing web applications today… Cross-Site Scripting. In addition, you will get an understanding of the secure programming patterns needed to mitigate the risk of Cross-Site Scripting in your applications.

Participants of this module will…

- Learn the variants of XSS vulnerabilities
- Realize the many types of exploits that can be carried out using XSS
- Understand the importance of the browser context from both the attacker's perspective and the developer's perspective
- Learn how to mitigate the risk of XSS vulnerabilities by using contextual output encoding.

Insecure Deserialization

Audience: Software developers, engineers, architects, testers

Duration: 20 min

Course Description:

Welcome to the Insecure Deserialization eLearning course. This course will explain the dangers of insecure deserialization, explain how attackers can manipulate both the data and the structure of serialized objects, and go over countermeasures to protect your applications.

Participants of this module will…

- Understand the general concepts of serialization and deserialization
- Be able to exploit unsafe serialization using freely available tools
- Learn how to prevent unsafe serialization vulnerabilities in code

Using Components with Known Vulnerabilities

Audience: Software developers, engineers, architects, testers

Duration: 15 min

Course Description:

Welcome to the Using Components with Known Vulnerabilities eLearning course. This course will raise awareness of the risks of using third-party components containing publicly disclosed vulnerabilities within your applications. In addition, we will discuss techniques to properly manage and reduce this risk by using sources of information on the web to identify and update vulnerable components.

Participants of this module will…

- Hear about historical examples of risks identified in 3rd party components
- Learn of resources on the web that can be used to identify emerging and newly identified vulnerabilities
- Discuss strategies to catalog and update components used in applications properly

Insufficient Logging and Monitoring

Audience: Software developers, engineers, architects, testers

Duration: 20 min

Course Description:

Welcome to the Insufficient Logging & Monitoring eLearning course. This course will explain the dangers of insufficient logging and monitoring, explain the risks, and discuss how to implement proper logging and monitoring in your web applications.

Participants of this module will…

- Obtain a background on the reconnaissance phase of an attack
- Review the dangers of not collecting sufficient information for auditing
- Learn about key factors to consider when building a logging system

Server-Side Request Forgery

Audience: Software developers, engineers, architects, testers

Duration: 15 min

Course Description:

Welcome to the Server-Side Request Forgery course. Server-Side Request Forgery, also known as SSRF, is becoming more prevalent with the increased adoption of microservices and other distributed application architectures. SSRF exploits how your app makes outbound connections… the more outbound connections your app makes, the greater the likelihood that you'll suffer from SSRF. This course will explain how SSRF vulnerabilities are exploited today, what they look like in source code and corresponding mitigation strategies. This course uses .NET source code for illustration, but the concepts can be applied to any programming language.

Securing the Supply Chain: Maintaining Software and Data Integrity

Audience: Software developers, engineers, architects, testers, managers

Duration: 30 min

Course Description:

Welcome to the Securing the Supply Chain: Maintaining Software and Data Integrity course. Over the years, software has grown in complexity and increased its dependency on third-party resources, leading to the software supply chain becoming a major attack target. Ensuring the integrity of software and its data is essential to support a secure software supply chain. This course focuses on mitigating supply chain attacks that violate software and data integrity, emphasizing security controls across the development, build, and deployment phases of the SDLC.

Cross-Site Request Forgery

Audience: Software developers, engineers, architects, testers

Duration: 15 min

Course Description:

Welcome to the Cross-Site Request Forgery course. Cross-Site Request Forgery, also known as CSRF, is a common vulnerability facing web- and API-based applications today. CSRF exploits the inability of your application to correctly determine whether an authenticated and authorized request was legitimately submitted by the end-user or whether it was forged by a hacker. This course will provide you with an understanding of how CSRF vulnerabilities are exploited today, what they look like in source code and the corresponding mitigation strategies.

Open Redirect

Audience: Software developers, engineers, architects, testers

Duration: 15 min

Course Description:

Welcome to the Open Redirect course. Open Redirect vulnerabilities are commonly found in web-based applications and are frequently used to carry out sophisticated phishing attacks. The age-old guidance of hovering over a link to verify the destination domain name before clicking it is rendered moot with this vulnerability, making it an enticing target for hackers. This course will give you an understanding of Open Redirect vulnerabilities, how they're exploited, and how to spot and fix them in source code.

Mobile App Sec Foundations for Developers

Audience: Software developers, engineers, architects

Duration: 3 hours

Course Description:

This course focuses on the most common security vulnerabilities and attack vectors facing mobile application developers today. Participants will explore these vulnerabilities by analyzing real-world examples, rich visualizations of attacks, and discussions of mitigation strategies with supporting code examples. After completing this course, participants will be able to more readily identify, mitigate, and prevent common security vulnerabilities within their mobile applications. The course will explore the following topics:

- Improper Platform Usage
- Insecure Data Storage
- Insecure Communication
- Insecure Authentication
- Insufficient Cryptography
- Insecure Authorization
- Client Code Quality
- Code Tampering
- Reverse Engineering
- Extraneous Functionality

Mobile App Sec Foundations for Managers

Audience: Software managers and executives

Duration: 1 hour

Course Description:

This course is designed to enable managers of mobile application development teams to enhance their understanding of the threats against mobile applications and their corresponding security controls. This course will explore the following categories:

- Improper Platform Usage
- Insecure Data Storage
- Insecure Communication
- Insecure Authentication
- Insufficient Cryptography
- Insecure Authorization
- Client Code Quality
- Code Tampering
- Reverse Engineering
- Extraneous Functionality

API Security

Audience: Software managers and developers

Duration: 1 hour

Course Description:

The API Security course helps define and categorize those specific risks to the design, implementation, and deployment of APIs. This course references API Security concerns referenced by the OWASP API Top Ten and more! This course will provide you with an understanding of these risks and how they can be mitigated by using secure programming practices. Participants will assess real-world examples, explore rich visualizations of attacks, and engage in thorough conversations of mitigation approaches with supporting code examples. After completing this course, participants will be able to more readily identify, mitigate, and prevent common security vulnerabilities within APIs. The course will explore the following topics:

- Broken Object Level Authorization
- Broken User Authentication
- Excessive Data Exposure
- Lack of Resources & Rate Limiting
- Broken Function-Level Authorization
- Mass Assignment
- Security Misconfiguration
- Injection
- Improper Asset Management
- Insufficient Logging & Monitoring

OWASP Top Ten at a Glance

Audience: All

Duration: 15 minutes

Course Description:

Welcome to the OWASP Top Ten at a Glance mini-course. This course intends to briefly introduce some of the most common application vulnerabilities as defined by the OWASP Top Ten taxonomy and give a general overview of why these vulnerabilities are important.

Software Security Compliance – Developer Focused Approach

Audience: Software Managers and Developers

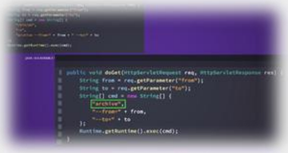
Duration: 30 minutes

Course Description:

Welcome to the Software Security Compliance – Developer Focused Approach course. In it, we'll explore why software security compliance matters, the major frameworks that govern it, and the crucial role developers play in safeguarding sensitive data. Such compliance frameworks referenced in this course include, but are not limited to, PCI-DSS, HIPPA, GDPR, NIST, and more!

BUILDING SECURE APPLICATIONS SERIES

Welcome to the Building Secure Application Series. This series of courses provides a thorough language-specific assessment of common vulnerabilities facing applications today. This series assumes participants have experience building applications with the specified language and the content reviewed within the App Sec Essentials courses. We recommend participants complete the App Sec Essentials for Developers Learning Path before beginning any of the Building Secure Applications courses for completeness.



```
public void doGet(HttpServletRequest req, HttpServletResponse res) {
    String from = req.getParameter("from");
    String to = req.getParameter("to");
    String[] cmd = new String[] {
        "archive",
        "--from=" + from,
        "--to=" + to
    };
    Runtime.getRuntime().exec(cmd);
}
```

resource and either hang permenantly in an infinite loop or crash with an out of memory error. Talk about denial of service!

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE order [
<!ENTITY my_entity SYSTEM "file:///dev/random">]>
<order>
    <id>&my_entity;</id>
</order>
```

This series includes :

Building Secure .NET Applications

Building Secure Java Applications

Building Secure JavaScript Applications

Building Secure Python Applications

Building Secure Ruby Applications

Building Secure Mobile Applications

Building Secure C/C++ Applications

Building Secure Go Applications

Building Secure .NET Applications

Audience: Software developers, engineers, architects

Duration: 1 hour

Course Description:

This course will provide participants with the secure programming practices necessary to build secure .NET applications resilient to frequent attacks, including but not limited to directory traversal, cross-site scripting, and injection. Finally, we will discuss several essential .NET security controls that can be used to mitigate some of the most prevalent attacks facing applications today.

Participants of this course will learn about the following vulnerabilities in .NET…

- HTTP Header Injection
- OS Injection
- SQL Injection
- Insufficient Certificate Validation
- Use of Insecure Ciphers
- Use of Insecure Digests
- XML External Entities
- Directory Traversal
- Cross-Site Scripting
- Insecure Deserialization
- Using Components with Known Vulnerabilities

Building Secure Java Applications

Audience: Software developers, engineers, architects

Duration: 1 hour

Course Description:

This course will provide participants with the secure programming practices necessary to build secure Java applications resilient to common attacks. This course will examine several essential Java security controls that can be used to diminish some of the most prevalent attacks facing applications today.

Participants of this course will learn about the following vulnerabilities in Java…

- HTTP Header Injection
- OS Injection
- SQL Injection
- Insufficient Certificate Validation
- Use of Insecure Ciphers
- Use of Insecure Digests
- XML External Entities
- Directory Traversal
- Cross-Site Scripting
- Insecure Deserialization
- Using Components with Known Vulnerabilities

Building Secure JavaScript Applications

Audience: Software developers, engineers, architects

Duration: 1 hour

Course Description:

This course will provide participants with the secure programming practices necessary to build secure client-side and server-side JavaScript applications resilient to conventional attacks. This course will examine several crucial JavaScript security controls that can be used to mitigate some of the most prevalent attacks facing applications today.

Participants of this course will learn about the following vulnerabilities in JavaScript…

- HTTP Header Injection
- OS Injection
- SQL Injection
- Insufficient Certificate Validation
- Use of Insecure Ciphers
- Use of Insecure Digests
- XML External Entities
- Directory Traversal
- Cross-Site Scripting
- Insecure Deserialization
- Using Components with Known Vulnerabilities

Building Secure Python Applications

Audience: Software developers, engineers, architects

Duration: 1 hour

Course Description:

This course will provide participants with the secure programming practices necessary to build Python applications resilient to widespread attacks. This course will examine many major Python security controls that can be used to mitigate some of the most prevalent attacks facing applications today.

Participants of this course will learn about the following vulnerabilities in Python…

- HTTP Header Injection
- OS Injection
- SQL Injection
- Insufficient Certificate Validation
- Use of Insecure Ciphers
- Use of Insecure Digests
- XML External Entities
- Directory Traversal
- Cross-Site Scripting
- Insecure Deserialization
- Using Components with Known Vulnerabilities

Building Secure Ruby Applications

Audience: Software developers, engineers, architects

Duration: 1 hour

Course Description:

This course will provide developers with the secure programming practices necessary to build Ruby and Ruby on Rails applications resistant to common attacks. This course will examine several Ruby security controls that can be implemented to mitigate some of the most prevalent attacks facing applications today.

Participants of this course will learn about the following vulnerabilities in Ruby…

- HTTP Header Injection
- OS Injection
- SQL Injection
- Insufficient Certificate Validation
- Use of Insecure Ciphers
- Use of Insecure Digests
- XML External Entities
- Directory Traversal
- Cross-Site Scripting
- Insecure Deserialization
- Using Components with Known Vulnerabilities

Building Secure Mobile Applications

Audience: Software developers, engineers, architects

Duration: 1 hour

Course Description:

This course will provide participants with the secure programming practices necessary to build secure mobile applications. Finally, we will summarize numerous key mobile security controls that can be used to avert some of the most prevalent attacks facing applications today.

Participants of this module will…

- Review the various types of mobile application architectures
- Understand the mobile application threat model
- Discuss the implications of weak server-side controls
- Highlight the risks of poor authentication and authorization
- Dive into the risks associated with managing sensitive data on mobile devices
- Fundamental security principles that help improve the security of mobile applications

Building Secure Go Applications

Audience: Software developers, engineers, architects

Duration: 1 hour

Course Description:

Welcome to the Building Secure Go Applications course. This course will provide you with the secure programming practices necessary to build secure Go applications resilient to frequent attacks and will summarize numerous key security controls that can be used to avert some of the most prevalent attacks facing applications today.

Participants of this course will learn about the following vulnerabilities in Go…

- OS Injection
- SQL Injection
- Insufficient Certificate Validation
- Use of Insecure Ciphers
- Use of Insecure Digests
- Directory Traversal
- Cross-Site Scripting
- Using Components with Known Vulnerabilities

Building Secure C/C++ Applications

Audience: Software developers, engineers, architects

Duration: 30 minutes

Course Description:

This course will provide you with the secure programming practices necessary to build secure applications resilient to vulnerabilities commonly introduced using C/C++.

Participants In this course will review the following topics in C/C++:

- Buffer Overflow
- Format String
- Memory Corruption
  - Use After Free
  - Double Free

OPERATIONS SERIES

This series of courses provide specific guidance on operational topics to support software development teams in creating safe and secure applications. Each of these courses covers a stand-alone security process with specified advice.

If your application would be attacked, how would you know?
What would be the key monitors or indicators that would inform you?
If a successful attack occurred, how would you recreate and understand what happened?

Courses within this Series include:

- Deriving Security Requirements within the SDLC Planning Phase
- Threat Modeling
- Docker and Application Container Security

Deriving Security Requirements within the SDLC Planning Phase

Audience: All

Duration: 20 minutes

Course Description:

Welcome to the Deriving Security Requirements within the SDLC Planning Phase course. Deriving security requirements from business requirements is an essential step in improving the security of the software delivered by your team. This course will review the concept of a security requirements practice and a security requirements framework and explore an example of how a product team may work through the creation of security requirements applicable to their business needs.

Threat Modeling

Audience: Architects, Testers

Duration: 1 hour

Course Description:

This course will provide participants with a foundational understanding of identifying, classifying, and rating threats that face our application architectures. In addition, participants will gain exposure to capturing threat modeling diagrams using Microsoft's Threat Modeling Tool. Topics reviewed include:

- Understanding the significance of Threat Modeling in the SDLC
- Defining Threat Modeling terminology and risk tolerance
- Discussing the various phases of the Threat Modeling process
- Utilization of Microsoft's Threat Modeling Tool
- Discuss Threat Quantification and highlight additional resources

Docker and Application Container Security

Audience: Software developers, engineers, architects

Duration: 30 minutes

Course Description:

This course is designed to introduce the fundamental security activities that can help improve the security of Docker containers and their running applications. After completing this course, learners will understand:

- The importance of scanning Docker images and applications running within the container for security vulnerabilities
- How Linux kernel security features help improve Docker security
- How to enforce resource constraints on Docker images to reduce the impact of vulnerability exploitation

INFRASTRUCTURE AS CODE SERIES

This series of courses provides in-depth guidance on implementing standard security controls within the cloud via infrastructure as code.

Courses within this Series include:

- IaC: Identity and Access Management in AWS
- IaC: Identity and Access Management in GCP

IaC: Identity and Access Management in AWS

Audience: Developer, Architect

Duration: 1 Hour

Course Description:

Welcome to the Infrastructure as Code: Identity and Access Management in AWS course. AWS offers several technologies to assist you in moving forward with Infrastructure as Code, including CloudFormation, Cognito, and Lambda, to name a few. CloudFormation delivers the ability to write templates, in either JSON or YAML, that automate the provisioning and configuration of various services and resources, including AWS Cognito and AWS Lambda. This course will provide learners with an understanding of how to implement multiple Identity & Access Management controls using Infrastructure as Code.

The Identity & Access Management controls covered in this course are driven by emerging research and industry-recognized standards and practices. Such controls include:

- Multifactor Authentication
- Cryptographic Authentication
- Single Sign-On
- Passwordless Authentication
- Adaptive Authentication
- Deny Resource Access by Default
- Enforce Level of Least Privilege

IaC: Identity and Access Management in GCP

Audience: Developer, Architect

Duration: 1 Hour

Course Description:

Google Cloud Platform offers several technologies to assist you in moving forward with an Infrastructure as Code strategy for Identity and Access Management, including Google Cloud SDK, Google Cloud Admin SDK, Anthos Service Mesh, and Identity-Aware Proxy, to name a few. Throughout this course, we will make frequent use of the Cloud SDK, which provides “tools and libraries for interacting with Google Cloud products and services” in a way that allows us to implement Infrastructure as Code. This course will give learners an understanding of how to implement various Identity & Access Management controls using Infrastructure as Code.

The Identity & Access Management controls covered in this course are driven by emerging research and industry-recognized standards and practices. Such controls include:

- Multifactor Authentication
- Cryptographic Authentication
- Single Sign-On
- Passwordless Authentication
- Adaptive Authentication
- Deny Resource Access by Default
- Enforce Level of Least Privilege