Bright Star Institute

302.335.8868

admissions@brightstarinstitute.com

Cyber Security Cloud Analyst

Duration: 480 hours

Prerequisites: Rudimentary knowledge of computer systems. Students should know how to basically operate a computer, browse the world wide web, send and receive email messages, and write and print memos.

Description: The Cyber Security Cloud Analyst course is tailored for professionals aiming to excel in securing cloud environments. The course first educates students on fundamental principles and topics in cloud computing, and provides them with hands on experience in a cloud environment. Afterwards, they will learn general IT security concepts and fundamentals, and then will take a deeper dive into applying those principles in a cloud software environment.

Course attendees will begin their training by learning how cloud computing is implemented, and how to handle basic design and management issues when utilizing cloud computing services. Attendees will obtain the skills required to determine when a cloud solution is appropriate for an organization, develop cloud infrastructure, implement the cloud development life cycle, manage cloud operations, and understand cloud resource governance. Upon completion of this portion of the course, attendees will have a working-level proficiency with cloud computing.

Next, students will learn about the important task of securing cloud environments. After an introduction to fundamental security concepts, students will dive into the complexities of cloud security, covering key areas such as risk management and compliance in the cloud, data protection and encryption, cloud architecture, cloud network security, and more. Upon completion of this part of the course, the student will be prepared to become a certified IT Specialist in Cloud Computing and will be able to perform the basic responsibilities of an entry-level professional in the field.

Featuring a mix of detailed video lessons, practical lab exercises, and case studies, the course provides hands-on experience with the latest cloud security tools and techniques. The course offers flexibility through a self-paced format, allowing you to learn on your own schedule. Expert instructors are on hand to provide personalized support and ensure a deep comprehension of advanced cloud security concepts. This cloud security analyst course is ideal for aspiring cloud security professionals or those looking to

enhance their expertise in cloud protection. This course will also prepare students for the Certificate of Cloud Security Knowledge (CCSK) exam, so they can graduate from the course with an added certificate to boost their resume.

Course Overview

Fundamentals of Cloud Computing

- Essential Concepts in Cloud Computing
- Planning a Cloud Computing Project
- Selecting Cloud Solutions
- Defining Cloud Solution Requirements
- Determining Hardware and Storage Requirements for a Cloud Project
- Designing Cloud Apps and Solutions
- Developing and Testing Cloud Apps
- Integrating and Deploying a Cloud Solution
- Managing Cloud Operations
- Evaluating Cloud Governance

Introduction to Cybersecurity

- Overview of Cybersecurity
  - Definition and Scope of Cybersecurity
  - Historical Evolution
  - Current Trends and Technologies
- The Importance of Cybersecurity
  - Impact on Personal and Financial Information
  - Consequences of Cyberattacks
  - Role in National Security
- Cybersecurity Roles and Career Paths
  - Key Cybersecurity Roles
  - Required Skills and Qualifications
  - Career Development and Growth

Understanding Cyber Threats

- Types of Cyber Threats
  - Malware and Ransomware
  - Phishing and Social Engineering
  - Advanced Persistent Threats (APTs)
- Common Attack Vectors
  - Email Attachements and Links
  - Unpatched Software and Vulnerabilities
  - Insider Threats
- Case Studies
  - Notable Cybersecurity Breaches
  - Successful Cybersecurity Defenses
  - Emerging Threats and Responses

Basic Cybersecurity Concepts

- The CIA Triad
  - Confidentiality, Integrity, Availability
- Security Policies and Procedures
  - Developing Effective Security Policies
  - Incident Response Procedures
  - Compliance and Regulatory Requirements
- Introduction to Risk Management
  - Risk Assement Processes
  - Risk Mitigation Strategies
  - Risk Communication
- Understanding Risks
  - Types of Risks
  - Risk Management Frameworks
  - Risk Monitoring and Review

Fundamentals of Network Security

Introduction to Cloud Security

- Introduction to Networks
  - Basic Networking Concepts
  - Types of Networks
  - Network Devices and Protocols
- Network Security Basics
  - Firewalls and Intrusion Detection Systems (IDS)
  - Network Segmentation and VLANs
  - Encryption and Secure Communication
- Wi-Fi Security
  - Common Wi-Fi Vulnerabilities
  - Securing Wi-Fi Networks
  - Public Wi-Fi Risks and Precautions

- Understanding Cloud Computing
  - Overview of Cloud Computing Models (IaaS, PaaS, SaaS)
  - Key Cloud Service Providers (AWS, Azure, Google Cloud)
  - Cloud Deployment Models (Public, Private, Hybrid)
- Cloud Security Fundamentals
  - Basic Principles of Cloud Security
  - Shared Responsibility Model
  - Key Security Concepts
- Cloud Security Architecture
  - Cloud Security Architecture Components
  - Network Security in the Cloud (VPC, Subnets, Security Groups)
  - Intro to Identity and Access Management (IAM)
- Cloud Compliance and Governance
  - Understanding Compliance Frameworks (GDPR, HIPAA, PCI-DSS)
  - Cloud Governance Practices
  - Data Protection and Privacy Considerations

Cloud Network Security

- Network Security Fundamentals
  - Basic Networking Concepts (IP, DNS, TCP/IP)
  - Network Security Principles
  - Cloud-Specific Networking Components
- Securing Cloud Networks
  - Configuring Virtual Private Cloud (VPC) and Subnets
  - Implementing Security Groups and Network ACLs
  - Setting Up VPNs and Private Connections
- Advanced Network Security
  - Intrusion Detection and Prevention

Identity and Access Management (IAM)

- IAM Concepts and Architecture
  - Identity Management and Authentication
  - Authorization Models (RBAC, ABAC)
  - Federation and Single Sign-On (SSO)
- Implementing IAM in Cloud Environments
  - Configuring IAM Roles, Policies, and Permissions
  - Managing User and Group Access
  - Implementing Multi-Factor Authentication (MFA)
- Security and Best Practices
  - Least Privilege Principle
  - IAM Policy Management Best Practices

Systems (IDPS)
    - Network Segmentation and Micro-Segmentation
    - Security in Serverless Architectures
    - Auditing and Monitoring IAM Activities

Security Operations and Incident Response

- Security Monitoring and Logging
    - Cloud-Native Logging and Monitoring Tools
    - Setting Up Alerts and Dashboards
    - Analyzing and Interpreting Security Logs
- Incident Response
    - Incident Response Lifecycle
    - Cloud-Specific Incident Response Strategies
    - Case Studies and Lessons Learned
- Vulnerability Management and Penetration Testing
    - Identifying and Managing Vulnerabilities
    - Cloud-Specific Penetration Testing Tools and Techniques
    - Best Practices for Securing Cloud Applications

302.335.8868

admissions@brightstarinstitute.com

Copyright© Bright Star Institute