ABOUT THE COURSE:

Cyber Security by Google:

Course Objectives	• Principles and components of Google Cloud's security infrastructure. • Implement effective identity and access management practices using Google Cloud IAM. Utilize Google Cloud's encryption tools to secure data at rest and in transit. • Configure network security settings to protect cloud resources from external threats. • Monitor and respond to potential security incidents using Google Cloud's threat detection tools. • Ensure compliance with relevant regulations and standards using Google Cloud's compliance features.
Course Outcomes	• Articulate foundational security principles, including confidentiality, integrity, and availability, and apply them within the context of cloud environments. • Develop and implement effective cloud security strategies using Google Cloud tools, focusing on identity and access management, data protection, and network security. • Identify and assess various cloud security risks, including data breaches, insider threats, and compliance issues, and formulate strategies to mitigate these risks. • Analyze and respond to different types of cloud cybersecurity attacks, such as DDoS, malware, and phishing, using Google Cloud's security features and best practices. • Evaluate and apply the role of a cloud security analyst, including monitoring cloud environments, performing security assessments, and ensuring compliance with industry standards. • Utilize practical skills in real-world scenarios to manage and secure cloud environments effectively, preparing for roles in cloud security and cybersecurity.

Course Duration: 45 Hours

Course Content:

UNIT I: Introduction to Security Principles in Cloud Computing

Essentials of cybersecurity - security lifecycle - digital transformation - key cloud computing concepts.

Lab Component & Outcome:

● Engage in exercises that explore the CIA triad, authentication mechanisms, and risk management techniques. This includes setting up and configuring secure user authentication and access controls.

● Gain a solid understanding of core security principles and learn to apply them to protect cloud environments against common security threats.

UNIT II: Strategies for Cloud Security Risk Management

Widely used cloud risk management frameworks - security domains - compliance lifecycles - IPAA, NIST CSF, and SOC.

Lab Component & Outcome

● Perform hands-on tasks to configure IAM policies, encrypt data using cloud tools, and set up secure network connections. This includes creating and managing secure cloud resources.

● Develop practical skills in implementing comprehensive cloud security strategies using Google Cloud tools, focusing on identity management, data protection, and secure networking.

UNIT III: Cloud Security Risks: Identify and Protect Against Threats

Principles of identity management - access control within a cloud environment - AAA (Authentication, Authorization, and Auditing)

Lab Component & Outcome

● Participate in risk assessment exercises, identify potential security vulnerabilities, and design mitigation strategies. This includes evaluating case studies and creating risk management plans.

● Gain the ability to identify, assess, and mitigate various cloud security risks, ensuring a proactive approach to managing and reducing potential threats in cloud environments.

UNIT IV: Detect, Respond, and Recover from Cloud Cybersecurity Attacks

Capabilities in logging - security - alert monitoring with techniques - mitigating attacks

Lab Component & Outcome

● Conduct labs on identifying and responding to various cybersecurity attacks, using Google Cloud's security tools for threat detection and incident response. This includes simulating attack scenarios and deploying defensive measures

●Develop the ability to analyze and respond to cloud cybersecurity attacks effectively, using Google Cloud's capabilities to detect threats and manage incidents in real-time.

UNIT V: Put It All Together: Prepare for a Cloud Security Analyst Job

Cloud security principles - risk management - identifying vulnerabilities - incident management - crisis communications.

Lab Component & Outcome

● Engage in security monitoring exercises, perform security assessments, and conduct audits using cloud-based tools. This includes developing reports and creating security strategies.

● Acquire practical experience in the duties of a cloud security analyst, preparing for a career in cloud security through hands-on activities in monitoring, assessment, and security management.

INDUSTRY USE CASE:

1. **Password Strength Checker:**

Task: Create a tool that assesses the strength of passwords based on criteria such as length, complexity, and uniqueness.

2. **Network Scanning Tool:**

Task: Develop a simple network scanning tool to discover active devices on a network.

3. **Basic Firewall Configuration:**

Task: Set up a basic firewall on a virtual machine to control incoming and outgoing network traffic.

4. **Security Awareness Website:**

Task: Build a website or web application that educates users on cybersecurity best practices, common threats, and ways to stay secure online.

5. **Encryption and Decryption Tool:**

Task: Develop a basic tool for encrypting and decrypting messages using classic encryption algorithms like Caesar cipher or substitution cipher.

6. **Malware Analysis Sandbox:**

Task: Create a simple malware analysis sandbox where users can safely analyse and understand the behaviour of basic malware samples in a controlled environment.

7. **Wireless Network Security Assessment:**

Task: Perform a basic security assessment of a wireless network, identifying common vulnerabilities and proposing security enhancements.

8. **Incident Response Plan Documentation:**

Task: Develop a simple incident response plan for a fictional organization, outlining steps to be taken in case of a security incident.

9. **Social Engineering Awareness Campaign:**

Task: Plan and execute a social engineering awareness campaign within a controlled environment, simulating phishing or other social engineering attacks.

10. **Password Policy Implementation:**

Task: Implement and document a strong password policy for educational systems, emphasizing user awareness.

11. **Secure File Sharing for Assignments:**

Task: Implement a secure file-sharing system for students submitting assignments,

ensuring confidentiality.

12. **Network Security Audit for Computer Labs:**

Task: Perform a basic security audit on computer labs, identifying and mitigating potential vulnerabilities.

13**. Secure Online Learning Platform:**

Task: Assess and enhance the security of an online learning platform used by students and teachers.

14. **Incident Response Plan for Institutions:**

Task: Develop an incident response plan specific to educational institutions, outlining roles and procedures.

15. **Basic Cybersecurity Training Module:**

Task: Develop a Cybersecurity Model system and training module for students.

16. **Phishing Detection System:**

Task: Develop a system that detects phishing emails by analysing email content, sender information, and links. Implement machine learning to improve detection accuracy over time.

17. **Data Leakage Prevention Tool:**

Task: Create a tool that monitors and prevents data leakage by analysing data transfer activities, identifying sensitive data, and blocking unauthorized transfers.

18. **IoT Device Security Assessment:**

Task: Conduct a security assessment of Internet of Things (IoT) devices, identifying vulnerabilities and proposing measures to enhance security.

19. **Web Application Vulnerability Scanner:**

Task: Develop a tool that scans web applications for common vulnerabilities such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF), providing detailed reports and mitigation suggestions.

20. **Advanced Persistent Threat (APT) Detection System:**

Task: Implement a system to detect advanced persistent threats by monitoring network traffic, analysing patterns, and identifying anomalies indicative of sophisticated cyber-attacks.