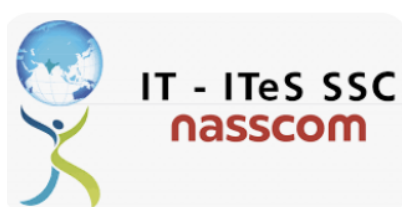


Information and Cyber Security Analyst (AI Integrated)

VERSION 1

CURRICULUM / SYLLABUS

SHRM Version	1.0
Date	01.02.2026
Course code	SHRM/FS/01/2026
Mapped to QP Codes	1. QP Name: AI – Analyst Application Security QP Code: SSC/Q0903 2. QP Name : Security Analyst QP Code : SSC/Q0901 QP Version: 3.0 NSQF Level: 5



Preamble

The "Information and Cyber Security (AI integrated)" program is designed to equip professionals with comprehensive knowledge and skills in the field of cyber security, emphasizing the integration of artificial intelligence (AI). This 440-hour program spans over six months, encompassing theory, practical sessions, and a capstone project. The curriculum is structured into four modules, progressing from fundamental concepts to advanced topics, preparing participants for professional careers in cyber security.

Course Objective and Learning Outcome

1. To provide a strong foundation in the principles and practices of cyber security.
2. To develop intermediate and advanced skills in identifying, analyzing, and mitigating cyber threats.
3. To integrate AI techniques and tools in enhancing cyber security measures.
4. To offer hands-on experience with real-world cyber security tools and scenarios by engaging in live projects.
5. To prepare participants for professional certifications and careers in cyber security.

Sl.No.	Learning Outcomes
1.	Demonstrate a comprehensive understanding of cyber security principles and practices
2.	Analyze and mitigate various types of cyber threats related to application security, Network Security and Information Security using advanced techniques.
3.	Integrate AI tools and techniques to enhance cyber security measures.
4.	Utilize industry-standard cyber security tools and technologies effectively.
5.	Apply their knowledge in real-world scenarios and contribute effectively to their organizations

Course Anatomy

Total duration of the course 308 hours (of theory and practical sessions) PLUS Capstone Project - 60 hours

Theory – 198 hours | Practical, Project assignments – 170 hours

Course structure Extensive demo and exercise
Several projects on use of various tools
Capstone project

Training Delivery In Hybrid Mode with offline classes from campus with remote access through smart classroom
Managed through a LMS platform with separate web page for each batch

Training Input All digital content available through web page of the batch

Lesson Planning Flexible structure customised each week while making the weekly roster.

Course Delivery

Program Delivery Pedagogy

- Interactive theoretical sessions to cover fundamental and advanced concepts.
- Practical sessions in a controlled environment to apply theoretical knowledge.
- Real-world scenarios to enhance problem-solving skills.
- Engagement in live projects
- Opportunity to get engaged in WEBEL Cyber Security Centre of Excellence
- Interactions with Industry Experts.
- A comprehensive project to apply learning in a practical, real-world context.
- Regular quizzes, assignments, and exams to evaluate understanding and progress.

Practical Sessions

Practical sessions will include hands-on exercises with cyber security tools and AI applications, such as:

- Network security simulations
- Ethical hacking and penetration testing
- AI-based threat detection and response
- Incident response and management
- Secure coding practices

Software and Hardware Requirements

- **Software:** Kali Linux, Wireshark, Metasploit, Nessus, Splunk, TensorFlow, PyTorch

- **Hardware:** Laptops/Desktops with minimum 8GB RAM, 500GB SSD, and i5 processor or higher; Network simulation equipment; Virtual lab infrastructure.

UNIQUENESS

- Approved by NASSCOM
- AI Integration to Cyber Security Analysis
- Blended mode with Online delivery and opportunity to get exposure in WEBEL Cyber Security centre of excellence
- Covers Information, network, application security and forensics
- Several assignments, Live Project Participation, Capstone Project
- Industry integration for the course

Eligibility and target group

- Graduates in any discipline
- IT professionals wishing to make career shift
- B Tech and MBA students
- Corporate professionals in related field to upscale
- Pan India with focus on digital audience

Dimension of the course

- Managing CYBER SECURITY THREATS
- Locating VULNERABILITY
- Threat DETECTION and Addressing
- INCIDENT RESPONSE AND MANAGEMENT
- CYBER SECURITY Connected to
 - Information Security
 - Network Security
 - Application security and
 - Forensic

Broad Coverage and Lesson Structure

The table lists the modules and their duration corresponding to the Compulsory NOS of the QP.

NOS and Module Details	Theory Duration (In Hours)	Practical Duration (In Hours)	Total Duration (In Hours)
SECTION A : INTRODUCTION TO INFORMATION, NETWORK AND CYBER SECURITY - (Total Duration - 85 hrs : Theory 55 + Practical 30) Aligned to QP Code: SSC/Q0903 - QP Name : Analyst Application Security QP Code: SSC/Q0901 - QP Name: Security Analyst			
Module 1: Bridge Module - Introduction to various operating systems, network systems, and digital forensics - (20 hours)	10:00	4:00	14:00
Module 2 (Bridge Module): Fundamental Concepts in Cyber Security Mapped to SSC/N0901	7:00	8:00	15:00
Module 3 : Introduction to Network Security Mapped to SSC/N0901 QP Code: SSC/Q0903	22:00	13:00	35:00
Module 4 : Cyber Security Policies, procedure, standards and Governance (10 hours) Mapped to SSC/N0909 (Version 1) QP Code: SSC/Q0903	6:00	0:00	6:00
Module 5 : Introduction of AI in Cyber Security	10:00	5:00	15:00
SECTION B : CYBER SECURITY THREATS, VULNERABILITY, DETECTION, INCIDENT RESPONSE AND MANAGEMENT (Total Duration - 83 hrs : Theory 55 + Practical 28) ALIGNED TO : QP Code: SSC/Q0903 - Analyst Application Security			
Module 6 : Identification of Cyber Security threats and vulnerabilities	20:00	5:00	25:00
Module 7 : Threats and vulnerability analysis Mapped to SSC/N0909 QP Code: SSC/Q0903	7:00	3:00	10:00

Module 8 : Incident Response and Management (20 hours) Mapped to SSC/N0903 QP Code: SSC/Q0903	10:00	5:00	15:00
Module 9 : Ethical Hacking and Penetration Testing (20 hours)	8:00	10:00	18:00
Module 10 : AI Techniques for Threat Detection	10:00	5:00	15:00
SECTION C : NETWORK SECURITY AND FORENSIC - (Total Duration - 45 hrs : Theory 27 + Practical 18) ALIGNED TO : QP SSC/Q0917			
Module 11 : Network Security	9:00	6:00	15:00
Module 12 : Forensic Analysis	9:00	5:00	14:00
Module 13 : Advanced Network Security Solutions	9:00	7:00	16:00
SECTION D : INFORMATION SECURITY, APPLICATION SECURITY (Total Duration - 77 hrs : Theory 48 + Practical 29) ALIGNED TO : QP SSC/Q0917			
Module 14 : Technological Developments in Application Security Mapped to SSC/N0909 (Version 1)	6:00	4:00	10:00
Module 15 : Web and cloud application security Mapped to SSC/N0909 (Version 1)	10:00	5:00	15:00
Module 16 : Information System Security features and management Mapped to SSC/N0901 (Version 2) and Mapped to SSC/N0903	6:00	4:00	10:00
Module 17 : Web Application Secure Configuration Mapped to SSC/N0910 (Version 1)	6:00	4:00	10:00
Module 18 : Monitoring Application Security (10 Hrs) Mapped to SSC/N0910 (Version 1)	5:00	3:00	8:00
Module 19 : Advanced Cryptography	9:00	5:00	14:00

Module 20 : AI-driven Security Operations	6:00	4:00	10:00
SECTION E : Employability Skill and PROJECTS			
Module 21 : Workplace data management, planning of work requirement Mapped to SSC/N9001 (Version 2)	4:00	4:00	8:00
Module 22 : Employability and basic communicative skills Mapped to SSC/N9002 (Version 2)	3:00	3:00	6 :00
Module 23 : Essential digital skills, Entrepreneurship, career development, goal setting and job readiness	2:00	2:00	4:00
Module 24 : Capstone Project (60 hours) To choose one project out of a list to be provided.	4:00	56:00	60:00
Total Duration	198:00	170:00	368:00

Module-wise Lesson and Session Plan

SECTION A : INTRODUCTION TO INFORMATION, NETWORK AND CYBER SECURITY

Aligned to

QP Code: SSC/Q0903 - QP Name : Analyst Application Security

QP Code: SSC/Q0901 - QP Name: Security Analyst

Module 1: Introduction to various operating systems, network systems, and digital forensics - (14 hours)

Bridge Module

Objective :

Discuss the fundamentals of programming and operating systems that are relevant to application security management.

- Introduction to Operating system
- Introduction to various network system
- Introduction to digital forensic
- Working with Windows and Linux OS Practical
- Discuss commonly used Unix/windows security commands

Theory: 10 Hrs Practical: 4 Hrs

Module 2 : Fundamentals of Cyber Security (15 hours)

Mapped to SSC/N0901

Objective: To build a strong foundation in cyber security concepts and practices.

- History and Evolution of Cyber Security (2 hours)
- Key Concepts and Terminologies (2 hours)
- Types of Cyber Attacks (3 hours)
- Cyber Security Landscape and Trends (3 hours)

Practical

- Demonstrate the working mechanism of malicious codes such as viruses, malware, logic bombs, ransomware, spyware, phishing, trojans, etc.
- Explain the various use cases of Cyber Security in the industry
- Explain various cyber threats associated with networks, devices, and remote access technologies

Theory: 7 Hrs Practical: 8 Hrs

Module 3 : Introduction to Network Security (55 hours)

Mapped to SSC/N0901 QP Code: SSC/Q0903

1. Network Security (8 hours)

- Commonly used ICT devices as well as list of web servers and web applications on sample network.
- Relevant networking concepts: load balancing, OSI, Data link Layer, Model/topology, TLS, SSL, etc.
- Devices: switches, routers, servers, transmission media
- Network Protocols and Architecture (5 hours)
- Firewalls: Types and Configurations (5 hours)
- Virtual Private Networks (VPNs) (5 hours)
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) (5 hours)

2. Network Security Solutions (18 hours)

- Explain common security solutions such as firewall, intrusion detection or prevention systems (IDS/IPS), anti-virus, web security gateways, email security, etc.
- Describe standard Systems Development Lifecycle (SDLC) practices and processes.
- Demonstrate the use of various Network Protocols and bandwidth management tools.
- Demonstrate the application of host network access controls; hubs; switches; routers; bridges; servers; transmission media IDS/IPS; application of SSL, VPN, 2FA, Encryption, etc.
- Demonstrate commonly used methods of data theft and unauthorized access
- Demonstrate the usage of basic methods/tools in preventing cyber-attacks.

Practical Sessions:

- Network setup and security configuration
- Basic encryption/decryption exercises

Theory : 10 Hrs Practical : 8 Hrs

3. Cryptography (9 hours)

- Principles of Encryption and Decryption
- Symmetric Cryptography
- Asymmetric Cryptography
- Cryptographic Applications

Theory: 4 Hrs Practical: 5 Hrs

Module 4 : Cyber Security Policies, procedure, standards and Governance (6 hours)

Mapped to SSC/N0909 (Version 1) QP Code: SSC/Q0903

Objective :

Understanding of the policies, standards, procedures, and guidelines related to application security.

1. Security Policies and Governance (6 hours)

- Importance of Security Policies
- Security Policy Development
- Compliance and Regulatory Requirements
- Information Security Management Systems (ISMS)

Practical Sessions

- Security policy development

Theory: 6 Hrs Practical 0 Hrs

Module 5 : Introduction of AI in Cyber Security (15 hours)

Introduction to AI in Cyber Security (15 hours)

- Basics of AI and Machine Learning
- AI Applications in Cyber Security
- AI Tools for Cyber Security
- Case Studies of AI in Cyber Security

Practical Sessions

- Demonstration

Theory: 10 Hrs Practical 5 Hrs

SECTION B : CYBER SECURITY THREATS, VULNERABILITY, DETECTION, INCIDENT RESPONSE AND MANAGEMENT

ALIGNED TO : QP Code: SSC/Q0903 - Analyst Application Security

Module 6 : Identification of Cyber Security threats and vulnerabilities (25 Hrs)

Mapped to Mapped to SSC/N0909 QP Code: SSC/Q0903

Objective: To deepen understanding and skills in identifying and mitigating cyber threats.

Topics:

1. Threats and Vulnerabilities
 - Common Cyber Threats and attacks
 - Define the types of vulnerabilities commonly found in applications.
 - Various vulnerability categories
 - Monitoring cyber threats and alert generation
 - Threat intelligence
 - Défense and access control
2. Identification of Application Vulnerabilities

- Types of vulnerabilities commonly found in applications, procedure to identify application vulnerabilities
- Importance of documentation review in identifying vulnerabilities
- How to distinguish false positives from genuine security threats
- Various methods to identify application vulnerabilities
- Explain the steps to gather relevant information for vulnerability assessment including:
 1. – source code
 2. – application type
 3. – security controls and application patching
 4. – application functionality and connectivity
 5. – application design and architecture
- Explain the methods to identify application vulnerabilities
- Describe the methods and tools used in application penetration testing

Theory: 20 Hrs

Practical 5 Hrs

Module 7 : Threats and vulnerability analysis (10 Hrs)

Mapped to Mapped to SSC/N0909 QP Code: SSC/Q0903

- Vulnerability Assessment Techniques (4 hours)
- Functionalities of commonly used vulnerability assessment tools and frameworks and best practices
- Assessing attacks related to upper OSI layers and data link layer
- Vulnerability Management Processes (3 hours)
- Case Studies on Threats and Vulnerabilities (3 hours)
- Practical
- Vulnerability scanning and analysis

Theory: 7 Hrs

Practical 3 Hrs

Module 8 : Incident Response and Management (15 hours)

Mapped to Mapped to SSC/N0903 QP Code: SSC/Q0903

- Incident Response Lifecycle
- Various stages of threat handling such as recording, classifying and prioritizing
- Maintaining organizational knowledge base in incident response.
- Forensics and Evidence Collection
- Incident Management Frameworks
- Describe the tools and templates used in reporting and documenting incident response.

- Prepare reports on security incident for consumption by appropriate stakeholders at various stages of incident management (identification, assignment, resolution, escalation, etc.)
- Sample incident response procedures using suitable tools.
- Case Studies on Incident Response
- Practical
- Incident response simulations

Theory: 10 Hrs

Practical 5 Hrs

Module 9 : Ethical Hacking and Penetration Testing (18 hours)

- Ethical Hacking Concepts
- Penetration Testing Methodologies
- Tools for Penetration Testing
- Practical Penetration Testing

Practical

- Penetration testing exercises

Theory: 8 Hrs

Practical: 10 Hrs

Module 10 : AI Techniques for Threat Detection (15 hours)

- Machine Learning Algorithms for Cyber Security
- Anomaly Detection Techniques
- AI-based Threat Intelligence
- Practical AI-based Threat Detection

Practical

- Implementing AI-based threat detection models

Theory: 10 Hrs Practical: 5 Hrs

SECTION C : NETWORK SECURITY AND FORENSIC

ALIGNED TO : QP SSC/Q0917

Module 11 : Network Security (15 Hrs)

Topics:

- Evaluate functional requirements of network security
- Methods to assess network security of an organisation.
- Evaluate functional requirements for network security in sample systems
- Review Existing Network Security Measures

- Ways to conduct risk analysis and threat assessments of network security

Practical

- Describe the parameters used to evaluate the existing network security protocols

Theory: 9 Hrs Practical: 6 Hrs

Module 12 : Forensic Analysis (14 Hrs)

Topics:

- NETWORK FORENSICS
- OS FORENSICS
- CLOUD SERVICES FORENSICS
- FORENSICS AND ANTI FORENSIC

Practical

- Demonstrate some forensic illustration through case studies

Theory: 9 Hrs Practical: 5 Hrs

Module 13 : Advanced Network Security Solutions (16 Hrs)

Topics:

- Advanced Firewall Configurations
- Network Segmentation Strategies
- Network Traffic Analysis
- Advanced Network Monitoring
- How to explore potential vulnerabilities that could be technical, operational or management related and categorizing them
- Explain secure configuration and baseline configuration in the context of network security.

Practical

- Advanced network security configurations
- Demonstrate the process of evaluating security solutions in terms of metrics such as cost, benefits, and effectiveness

Theory: 9 Hrs Practical: 7 Hrs

SECTION D : INFORMATION SECURITY, APPLICATION SECURITY

ALIGNED TO : QP SSC/Q0917

Module 14 : Technological Developments in Application Security (10 Hrs)

Mapped to SSC/N0909 (Version 1)

Topics:

- Latest technological developments in application security

- Evaluate next generation techniques for controlling advanced threats to applications
- List popular sources and platforms to gather information related to technological developments in application security.

Theory: 6 Hrs Practical: 4 Hrs

Module 15 : Web and cloud application security (15 Hrs)

Mapped to SSC/N0909 (Version 1)

Topics:

- Investigating web attack
- Email security
- Working with cloud and IOT
- Case studies - web services security
- Endpoint and securing data

Theory: 10 Hrs Practical: 5 Hrs

Module 16 : Information System Security features and management (10 Hrs)

Mapped to SSC/N0901 (Version 2) and Mapped to SSC/N0903 (Version 2)

Topics:

- Discuss the features and functionalities of commonly used information security devices.
- Perform security assessment of sample information security systems using suitable tool
- Discuss the tools and templates used in installing, configuring, troubleshooting, and testing security devices

Theory: 6 Hrs Practical: 4 Hrs

Module 17 : Web Application Secure Configuration (10 Hrs)

Mapped to SSC/N0910 (Version 1)

Topics:

- Describe the methods to configure web applications securely across environments for minimum exposure and weaknesses.
- Discuss the best practices related to web application configuration.
- Demonstrate the process of securing web application configuration using tools and techniques such as application testing, code review, web application firewall, etc.
- Apply suitable programming tools and techniques to configure, modify and debug application codes

Theory: 6 Hrs Practical: 4 Hrs

Module 18 : Monitoring Application Security (8 Hrs)

Mapped to SSC/N0910 (Version 1)

Topics:

- Monitoring and Logging of Application Events and Alarms
- Explain the processes to monitor applications and solutions.
- Discuss the usage of Security Information and Event Management (SIEM) tools.
- Define prioritization and handling of Cyber Security incidents.
- Demonstrate Cyber Security Incident logging/reporting tools.

Theory: 5 Hrs Practical: 3 Hrs

Module 19 : Advanced Cryptography (14 hours)

Mapped to

Topics:

- Quantum Cryptography
- Cryptographic Protocol Analysis
- Advanced Encryption Techniques
- Cryptographic Applications and Case Studies
- Practical
- Cryptographic protocol implementation

Theory: 9 Hrs Practical: 5 Hrs

Module 20 : AI-driven Security Operations (10 hours)

Mapped to

Topics:

- AI in Security Operations Centers (SOC)
- Automated Threat Intelligence and Response
- AI Tools for Security Operations
- Practical AI-driven SOC Exercises
- Practical
- AI-driven SOC simulations

Theory: 6 Hrs Practical: 4 Hrs

Module 20 : Workplace data management, planning of work requirement (8 hours) ₹

SECTION E : Employability Skill and PROJECTS

Module 21 : Workplace data management, planning of work requirement
Mapped to SSC/N9001 (Version 2) - 8 hours

- Workplace data management, data structure and control system for data security
- Data privacy
- Planning work and defining scope of work
- work requirements and work area prioritization
- Work scheduling and execution
- Accuracy of work and completion

Module 22 : Employability and basic communicative skills

Mapped to SSC/N9002 (Version 2) - 6 hours

- Communicating with colleagues, associates, customer
- Basic Communicative English
- Managing workplace stress
- Making oneself ready beyond domain skill
- Presenting oneself

Module 23 : Essential digital skills, Entrepreneurship, career development, goal setting and job readiness - 4 hours

- Essential digital skill
- Preparation for career, interview preparation and job readiness
- Writing CV
- Entrepreneurship

Module 24 : Capstone Project (60 hours)

Objective: To apply theoretical and practical knowledge in a real-world project.

Project Plan:

- Project Selection: Choose a real-world cyber security problem.
- Project Proposal: Define objectives, scope, and methodology.
- Implementation: Develop and implement the solution using cyber security and AI techniques.
- Evaluation: Assess the effectiveness and impact of the solution.
- Presentation: Present the project findings and outcomes.

Practical Sessions:

- Regular project reviews and feedback sessions
- Collaboration with industry mentors
- Final project presentation and evaluation

Choice of projects :

- A list of projects will be provided (some samples indicated)
- To choose one
- Candidates can select project on its own and get the same vetted by the Institute.

SAMPLE Capstone Project Titles and Scope of Work for Cyber Security Program

1. Advanced Threat Detection and Mitigation Using Machine Learning

Scope of Work:

- **Objective:** Develop and implement machine learning models to detect and mitigate advanced persistent threats (APTs) in a simulated network environment.
- **Tasks:**
 - Collect and preprocess network traffic data.
 - Train and evaluate machine learning models (e.g., anomaly detection, clustering).
 - Implement real-time threat detection using the trained models.
 - Develop and test mitigation strategies to respond to detected threats.
 - Document the process and results, including model performance and effectiveness of mitigation strategies.

2. Developing a Comprehensive Incident Response Plan Using AI

Scope of Work:

- **Objective:** Create an AI-driven incident response plan to automate and enhance the effectiveness of responding to cybersecurity incidents.
- **Tasks:**
 - Research and identify key components of an effective incident response plan.
 - Design and implement an AI-based system for detecting, classifying, and responding to incidents.
 - Simulate various cybersecurity incidents to test the response system.
 - Evaluate the system's performance and refine the response strategies.
 - Document the incident response plan, system architecture, and findings.

3. Penetration Testing and Security Auditing of IoT Devices

Scope of Work:

- **Objective:** Conduct a comprehensive security audit and penetration testing of Internet of Things (IoT) devices to identify vulnerabilities and recommend mitigation strategies.

- **Tasks:**
 - Select a set of IoT devices for testing.
 - Perform vulnerability assessments using tools available in Kali Linux.
 - Execute penetration testing techniques to exploit identified vulnerabilities.
 - Analyze the security posture of the IoT devices and recommend mitigation strategies.
 - Document the findings, including detailed vulnerability reports and remediation steps.

4. Enhancing Web Application Security Using AI-Based Intrusion Detection Systems

Scope of Work:

- **Objective:** Develop and deploy an AI-based Intrusion Detection System (IDS) to enhance the security of web applications against cyber-attacks.
- **Tasks:**
 - Research and select appropriate AI algorithms for intrusion detection.
 - Collect and preprocess web application traffic data.
 - Train and validate AI models for detecting web-based attacks (e.g., SQL injection, XSS).
 - Integrate the IDS with a web application and monitor its performance.
 - Evaluate the system's effectiveness in detecting and preventing attacks.
 - Document the development process, model performance, and security improvements.

5. AI-Powered Phishing Detection and Prevention System

Objective: Develop a system using AI to detect and prevent phishing attacks by analyzing email content and metadata.

- **Tasks:**
 - Collect a dataset of phishing and legitimate emails.
 - Preprocess the data by extracting relevant features.
 - Train machine learning models (e.g., decision trees, neural networks) to classify emails.
 - Implement real-time email filtering and alerting mechanisms.
 - Test the system's effectiveness using simulated email traffic.
 - Document the methodology, model performance, and prevention strategies.

6. Comprehensive Security Assessment of Cloud Infrastructure

Scope of Work:

- **Objective:** Conduct a thorough security assessment of a cloud-based infrastructure to identify vulnerabilities and recommend improvements.
- **Tasks:**
 - Inventory cloud resources and configurations.
 - Perform vulnerability scans and penetration testing on cloud services.
 - Assess compliance with security standards and best practices.

- Develop and recommend strategies for mitigating identified risks.
- Create a security assessment report detailing findings and recommendations.
- Document the tools and methodologies used in the assessment.

7. Development of a Secure Mobile Payment Application

Scope of Work:

- **Objective:** Design and implement a secure mobile payment application with robust security features to protect user data and transactions.
- **Tasks:**
 - Research security requirements for mobile payment applications.
 - Design the application architecture with security best practices in mind.
 - Implement security features such as encryption, biometric authentication, and secure storage.
 - Conduct security testing, including penetration testing and code reviews.
 - Deploy the application in a test environment and evaluate its security.
 - Document the design, implementation, and security measures.

8. Network Segmentation and Zero Trust Architecture Implementation

Scope of Work:

- **Objective:** Design and implement a network segmentation strategy and a Zero Trust architecture to enhance the security of an enterprise network.
- **Tasks:**
 - Research Zero Trust principles and network segmentation strategies.
 - Analyze the existing network infrastructure and identify segmentation opportunities.
 - Design and implement network segmentation using VLANs, firewalls, and access controls.
 - Develop and enforce Zero Trust policies, including identity and access management.
 - Test the new architecture for security, performance, and compliance.
 - Document the implementation process and its impact on network security

9. Forensic Analysis and Incident Response for Ransomware Attacks

Scope of Work:

- **Objective:** Conduct forensic analysis and develop an incident response plan for handling ransomware attacks in a corporate environment.
- **Tasks:**
 - Research ransomware attack vectors, behavior, and impact.
 - Set up a simulated environment to conduct ransomware attacks.
 - Develop an incident response plan, including containment, eradication, and recovery steps.
 - Conduct tabletop exercises to test the incident response plan.
 - Document the forensic analysis findings and incident response procedures.

10. Cybersecurity Risk Assessment and Management for Critical Infrastructure

Scope of Work:

- **Objective:** Conduct a comprehensive risk assessment of a critical infrastructure system and develop a risk management plan to enhance its security posture.
- **Tasks:**
 - Identify and define the scope of the critical infrastructure system (e.g., power grid, water supply).
 - Conduct a thorough risk assessment to identify potential threats, vulnerabilities, and impacts.
 - Use risk assessment tools and methodologies such as threat modeling and risk matrices.
 - Develop a risk management plan, including risk mitigation strategies and contingency plans.
 - Simulate various attack scenarios to test the effectiveness of the risk management plan.
 - Document the risk assessment findings, management plan, and recommendations for improving security.

