CCEK – NSQF ALIGNED PROGRAM

COURSE SYLLABUS

FOR

Cyber Security

CCEK - NATIONAL SKILL DEVELOPMENT TRAINING PROGRAM

Cyber Security

CCEK – NSDC course package covers the following Qualification Packs and leads to the following NSDC certifications. The students who successfully completed the course programs are entitled to get NSDC certification after undergoing the assessment process of NSDC as per the rules and regulations stipulated by NSDC from time to time.

SL. NO.	QUALIFICATIONS PACK	QUALIFICATIONS PACK CODE	NSQF LEVEL
1	**Security Analyst** **Brief Job Description**: Individuals at this job are responsible for protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording, or destruction.	**SSC/Q8404**	**5**

COURSE DETAILS

Cyber Security

EXAMINATION DETAILS

COURSE NAME	COURSE CODE	ELIGIBILITY	DURATION
Cyber Security	G18	Pursuing degree/ BCA/ Bsc in Computer science/3 year Diploma	180

SL. NO.	EXAM	EXAM CODE	MAXIMUM MARK	INTERNAL	TOTAL MARK
THEORY PAPERS					
1	Fundamentals of Cyber Security, Network Security & Cryptography	T001	100	50	150
2	Ethical Hacking & Vulnerability Assessment	T002	100	50	150
3	Cyber Laws, Policies & Incident Response	T003	100	50	150
PRACTICAL PAPERS					
1	Network Configuration & Ethical Hacking Techniques	L001	100	50	150
TOTAL MARKS					
1	Total Examination Marks (Theory Online + Practical Examination)				400
2	Total Internal Marks				200
3	**Total Marks (Total Internal Marks + Total Examination Marks)**				**600**

Cyber Security

INTERNAL MARK CRITERIA FOR EACH

SL NO.	MODULE	MODULE CODE	MAXIMUM MARK	INTERNAL MARK	TOTAL MARK
1	Fundamentals of Cyber Security, Network Security & Cryptography	T001	100	50	150
2	Ethical Hacking & Vulnerability Assessment	T002	100	50	150
3	Cyber Laws, Policies & Incident Response	T003	100	50	150
4	Network Configuration & Ethical Hacking Techniques	L001	100	50	150
	TOTAL		400	200	600

ATTENDANCE	GENERAL PERFORMANCE	INTERNAL EXAMINATIONS/ PROJECTS/ ASSIGNMENTS	TOTAL MARKS
5	5	40	50

COURSE SYLLABUS

FOR

Cyber Security

COURSE	Cyber Security	
TOTAL MARKS	Mark: 600	Internal Mark: 200
TOTAL HOURS	180 Hrs	

DEFENITION OF CREDIT

1 Credit	15Hrs Theory/ 30Hrs Practical
Skill Components	60 – 70 % of Total Credit

MODULES INCLUDED IN THIS SUBJECT

SL NO	MODULE NAME	CREDIT BREAKUP
1	Module 1: Introduction to Security Analyst	**0.5**
2	Module 2: Real-Time Threat Detection and Response in Security Operations	**1**
3	Module 3: Digital Forensics and Incident Response	**1**
4	Module 4: Incident Response and Management	**1**
5	Module 5: Incident Response and Threat Management	**0.5**
6	Module 6: Incident Response and Vulnerability Management	**0.5**
7	Module 7: Cloud Security and Threat Management	**0.5**
8	Module 8: Data Security and Compliance in Cloud Environments	
9	Module 9: Phishing Threat Detection and Response	
10	Module 10: Phishing Incident Management and Prevention	
11	Module 11: Introduction to Employability Skills	

12	Module 12: Constitutional values – Citizenship	**0.5**
13	Module 13: Becoming a Professional in the 21st Century	
14	Module 14: Basic English Skills	**0.5**
15	Module 15: Career Development and Goal Setting	
16	Module 16: Communication skills	
17	Module 17: Diversity and Inclusion	
18	Module 18: Financial and Digital Literacy	
19	Module 19: Essential Digital Skills	
20	Module 20: Entrepreneurship	
21	Module 21: Customer Service	
22	Module 22: Getting Ready for Apprenticeship and Jobs	
	Total	**6**

Training Outcomes

- Explain the use cases, common roles, and basic operating procedures followed by organizations in the context of cyber security.
- Evaluate the significance of network security protocols (e.g., SSL, TLS, IPSec) in safeguarding communications.
- Analyze the operational mechanisms of firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) in network protection.
- Demonstrate proficiency in interpreting security reports and alerts generated by monitoring tools to identify potential threats.
- Compare various cyber security frameworks (e.g., NIST, ISO/IEC 27001) and evaluate their applicability to organizational security measures.
- Evaluate the effectiveness of different cyber security tools (e.g., firewalls, SIEM, antivirus) in mitigating security risks.
- Design a basic security architecture for a small organization, considering potential threats and vulnerabilities.
- Identify and demonstrate various cyber security tools available for monitoring and protecting systems in a classroom setting.

MODULES

Module 1: Introduction to Security Analyst

THEORY

- Explain the importance of network security protocols such as SSL, TLS, and IP Sec.
- Describe the key components of a Security Operations Center (SOC) and their functions.
- Illustrate how firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) function to secure networks.
- Demonstrate how to interpret security reports and alerts generated by monitoring tools.
- Compare various cyber security frameworks (e.g., NIST, ISO/IEC 27001) and analyze how they apply to organizational security.
- Break down the incident response process and analyze the different phases involved.
- Assess the effectiveness of different cyber security tools (firewalls, SIEM, antivirus, etc.) in mitigating security risks.
- Evaluate the impact of security breaches on business operations and data confidentiality, integrity, and availability.
- Design a basic security architecture for a small organization, considering potential threats and vulnerabilities.

PRACTICAL

- Identify the various cyber security tools available for monitoring and protecting systems during a classroom demonstration (e.g., SIEM tools, antivirus software).
- Explain the steps involved in analyzing real-time network traffic during a practical session, using network monitoring tools such as Wire shark.
- Perform a basic configuration of a firewall in a classroom setting, including defining rules and setting up access control lists (ACLs).
- Use antivirus software to scan a system for malware and interpret the results in real-time.
- Analyze and interpret log files from a SIEM tool or IDS/IPS to identify patterns indicating a potential security breach.
- Compare network traffic before and after applying encryption protocols (e.g., SSL) during hands-on lab activities.
- Assess the security posture of a sample network by conducting a vulnerability scan using tools like Nessus or Open VAS in the classroom.

Module 2: Real-Time Threat Detection and Response in Security Operations

THEORY

- Explain how to monitor security alerts from various platforms, including firewalls, IDS, and SIEM, and the importance of continuous monitoring to detect potential threats.
- Analyze how security alerts can be correlated with system data to identify suspicious activities, recognizing common indicators of compromise.
- Explain the process of cross-verifying alerts with other logs such as network and application logs to validate the legitimacy of the threat.
- Categorize security threats based on severity, potential business impact, and the sensitivity of compromised data.
- Describe the MITRE ATT&CK framework and its use in classifying attack tactics, techniques, and procedures (TTPs).
- Apply a risk-based approach to prioritize threats based on urgency and business impact.

PRACTICAL

- Demonstrate the continuous monitoring of security alerts from firewalls, IDS, and SIEM platforms, identifying any immediate threats in a classroom lab setup.
- Perform real-time analysis of security alerts by correlating them with system data to detect suspicious activities in a controlled environment.
- Cross-verify security alerts with network and application logs, validating the legitimacy of identified threats through hands-on lab exercises.
- Classify security threats based on their severity, impact on business operations, and compromised data during practical scenarios or case studies.
- Apply the MITRE ATT&CK framework to classify and understand attack tactics and techniques in a practical lab session using real-world examples.
- Utilize a risk-based approach to determine the priority of threat response in a classroom exercise where students analyze different threat scenarios.

Module 3: Digital Forensics and Incident Response

THEORY

- Explain the best practices for collecting and preserving digital evidence from compromised systems and network devices.
- Discuss the steps involved in performing a forensic analysis to reconstruct events leading to a security breach.

- Identify key attack vectors and vulnerabilities from forensic data to understand the cause of a security incident.
- Discuss the importance of collaboration with an incident response team in isolating affected systems and mitigating threats.
- Evaluate various remediation steps, such as patching vulnerabilities and hardening systems, to prevent future security breaches.

PRACTICAL

- Demonstrate how to collect and preserve digital evidence from a compromised system using forensic tools.
- Perform a forensic analysis on collected data to reconstruct the sequence of events leading to a breach.
- Analyze a set of compromised system logs or packet captures to identify the root cause of an attack.
- Collaborate with peers in a classroom environment to isolate an affected system and simulate incident mitigation.
- Recommend appropriate remediation actions for a given security incident based on the evidence gathered.

Module 4: Incident Response and Management

THEORY

- Explain the role and functionality of security tools such as IDS, firewalls, and SIEM in detecting and responding to cyber threats.
- Discuss various network protocols and their implications on security, including common system vulnerabilities and potential attack vectors.
- Analyze different threat categorization methodologies and their application in identifying security incidents.
- Describe the importance of data analysis in cyber security, including techniques for identifying patterns and anomalies indicative of security threats.
- Articulate effective communication strategies to convey cyber security findings to both technical and non- technical audiences.
- Explain emerging cyber threats, vulnerabilities, and security best practices, demonstrating an understanding of their implications for organizational security.
- Analyze past incidents to identify common vulnerabilities and recommend updates to incident response techniques based on lessons learned.
- Discuss the importance of continuous monitoring and defense strategies in adapting to evolving threat landscapes.

PRACTICAL

- Utilize IDS, firewalls, and SIEM tools to perform real-time monitoring and detection of cyber threats in a controlled environment.
- Conduct a hands-on analysis of network traffic using packet sniffers to identify vulnerabilities and potential attack vectors.
- Perform data analysis on provided security logs and datasets to detect anomalies or patterns that may indicate security incidents.
- Troubleshoot and resolve specific issues encountered during the detection and analysis of security incidents using appropriate tools and techniques.
- Prepare and present findings from practical analyses to a mixed audience, demonstrating the ability to adjust communication based on the audience's technical expertise.
- Research and present recent case studies on emerging cyber threats and vulnerabilities, applying findings to enhance real-time monitoring strategies in a classroom setting.
- Conduct a workshop to update incident response protocols, utilizing lessons learned from a real incident and incorporating feedback from peers

Module 5: Incident Response and Threat Management

THEORY

- Explain the importance of establishing and documenting clear escalation procedures for major security incidents.
- Describe effective communication strategies for conveying threat status, urgency, and required actions to relevant teams and management during an incident.
- Analyze the process of isolating a compromised system and its significance in incident response.
- Discuss the implementation and configuration of SOAR tools in automating threat detection, investigation, and containment processes.
- Review the organization's knowledge base for past information security incidents and evaluate the methods used to handle them.
- Assess the importance of allocating information security incidents to relevant personnel for effective investigation and response.
- Evaluate the criteria for determining the severity and potential impact of identified threats, prioritizing them based on organizational risk and criticality.
- Explain the process for monitoring the progress of investigations into information security incidents and the established standards or service level agreements (SLAs).

PRACTICAL

- Demonstrate device management procedures such as installation, configuration and testing using sample network/ information security devices.
- Demonstrate how to troubleshoot common issues in security devices.

- Create reports on troubleshooting, configurations and deployment using standard templates and tDevelop and document an escalation procedure for a major security incident during a classroom exercise.
- Conduct a role-play exercise to effectively communicate threat status, urgency, and required actions to relevant teams and management.
- Demonstrate the process of isolating a compromised system using actual system configuration tools in a controlled environment.
- Implement a SOAR tool configuration scenario to automate threat detection and containment processes in the classroom.
- Review case studies of past information security incidents and discuss the lessons learned in small groups.
- Allocate real or simulated information security incidents to team members in a classroom scenario for investigation and response.
- Create a threat assessment report they evaluates the severity and potential impact of identified threats, presenting it to peers for feedback
- Monitor and report on the progress of an ongoing incident investigation in a simulated environment, identifying when escalation is necessary based on predefined SLAs.

Module 6: Incident Response and Vulnerability Management

THEORY

- Explain the principles and importance of conducting post-incident investigations to identify root causes of security breaches or attempted intrusions.
- Analyze security trends and incident data to contribute to the development and enforcement of organizational security policies.
- Describe the process and significance of regular vulnerability assessments in identifying potential weaknesses within systems, networks, and applications.
- Discuss the role of collaboration with IT teams in prioritizing and applying timely security patches to mitigate known vulnerabilities.
- Interpret complex data sets to detect patterns of suspicious activity, contributing to enhanced security breach detection.
- Discuss the organizational policies, standards, procedures, guidelines, and service level agreements (SLAs) that govern responses to information security incidents.

PRACTICAL

- Develop typography for different text elements (such as titles, subtitle, heading, tec.)
- Create samples to showcase proposed typography, colour palette and placement of design elements.
- Design guidelines for developing different user interface elements (such as Icons, toolbars, dialog box etc.)
- Conduct a comprehensive post-incident investigation in a simulated environment to identify root causes of a security breach, documenting findings and recommendations.

- Collaborate with peers to analyze real security incident data and present recommendations for policy enhancements based on identified trends.
- Perform a vulnerability assessment on an assigned system or application, documenting potential weaknesses and suggesting remediation strategies.
- Collaborate with IT teams to apply security patches to designated systems in real-time, demonstrating the prioritization of addressing known vulnerabilities.
- Analyze provided data sets in a classroom setting to identify patterns indicative of suspicious activity or potential security breaches, and present findings to the class.
- Adhere to organizational policies while managing a mock information security incident, ensuring compliance with established standards and SLAs.

Module 7: Cloud Security and Threat Management

THEORY

- Explain the features and functionalities of threat protection, information protection, and identity protection within the Microsoft 365 Defender Suite.
- Describe the deployment and management processes for Azure Security Center, Azure Firewall, and Azure Key Vault.
- Analyze security configurations and identify best practices to address emerging threats and vulnerabilities.
- Discuss the significance of implementing security measures across multiple cloud providers and servers.
- Evaluate the role of SIEM tools and threat intelligence feeds in continuous monitoring of cloud environments.
- Identify common indicators of suspicious activities or anomalies in cloud security.
- Outline the steps involved in investigating security incidents, including documentation and remediation.
- Assess the impact of security incidents and formulate strategies for corrective actions to prevent recurrence.
- Explain the principles of user account management, including role-based access control and the importance of timely de- provisioning.
- Discuss the principles and implementation of Multi-Factor Authentication (MFA) to enhance user account security.

PRACTICAL

- Configure and manage threat protection, information protection, and identity protection features within the Microsoft 365 Defender Suite in a live environment.
- Deploy and manage Azure Security Center, Azure Firewall, and Azure Key Vault in a hands-on lab setup.
- Conduct regular reviews and updates of security configurations to mitigate emerging threats and vulnerabilities using real-time tools.
- Implement security measures across multiple cloud providers and servers in a collaborative classroom project.

- Utilize SIEM tools and threat intelligence feeds to perform continuous monitoring and generate reports on cloud environments.
- Identify and report suspicious activities or anomalies in a simulated environment within specified response times.
- Investigate security incidents in a practical setting, documenting findings and remediation steps based on real scenarios.
- Develop and implement corrective actions to mitigate the impact of incidents and demonstrate their effectiveness in a practical exercise.
- Manage user accounts by configuring roles and responsibilities within a classroom lab, ensuring appropriate access is granted.
- Maintain accurate records of user access changes and perform de-provisioning of inactive accounts as part of a practical lab session.
- Implement and manage Multi-Factor Authentication (MFA) for all relevant user accounts in a live demonstration, achieving specified compliance rates.

Module 8: Data Security and Compliance in Cloud Environments

THEORY

- Explain the significance of conducting regular access reviews and describe the process of identifying and revoking unnecessary user permissions.
- Identify different types of sensitive data (e.g., PII, PHI) and discuss their implications in cloud environments.
- Classify data according to established sensitivity levels and articulate the necessary protection measures for each classification.
- Describe the principles and importance of Data Loss Prevention (DLP) policies in preventing unauthorized access and transmission of data.
- Analyze industry regulations (e.g., GDPR, HIPAA, PCI DSS) and evaluate their impact on data security practices within organizations.
- Discuss the elements and objectives of effective security awareness training programs for employees.

PRACTICAL

- Conduct an access review of user permissions in a classroom setting, identifying and documenting unnecessary permissions, and demonstrate how to revoke them effectively.
- Perform a classification exercise where participants identify and categorize various data types as PII or PHI using real-world examples provided during the training session.
- Categorize a set of sample data according to its sensitivity level and recommend appropriate protection measures that can be implemented in a cloud environment.
- Implement a mock DLP policy by configuring settings in a simulated cloud environment, and monitor for unauthorized data access or transmission.

- Conduct a mini-audit of compliance with industry regulations, utilizing checklists to assess adherence and document findings in a collaborative classroom activity.
- Develop and present a short security awareness training module to peers, achieving a targeted participation rate and gathering feedback for improvement.
- Carry out a vulnerability assessment on a provided cloud environment scenario, documenting findings and proposing remediation actions in a structured report format.

Module 9: Phishing Threat Detection and Response

THEORY

- Discuss how to employ advanced tools such as Phishme to analyze and assess the risk level of incoming emails.
- Recognize phishing attempts by identifying common red flags, including suspicious sender addresses, urgent requests, and grammatical errors.
- Explain the factors to consider when conducting risk assessments for potential phishing threats, including data sensitivity and employee vulnerability.
- Explain the design principles and importance of phishing simulation exercises for educating employees on phishing tactics.
- Comprehend digital forensic techniques used to trace the origin of suspicious emails, including the utilization of IP addresses, DNS records, and metadata

PRACTICAL

- Demonstrate the use of Phishme or similar tools to assess the risk level of incoming emails in a real-time environment.
- Identify phishing attempts by thoroughly examining sample emails for suspicious elements such as sender addresses, urgency, and inconsistencies.
- Perform risk assessments by analyzing potential phishing emails and determining the level of threat based on the sensitivity of information and employee vulnerability.
- Develop and conduct a phishing simulation exercise to educate employees on recognizing phishing attempts.
- Analyze and interpret employee responses to phishing simulations, identifying areas where knowledge gaps exist.
- Apply digital forensic techniques in the classroom by tracing the origin of suspicious emails, utilizing available IP addresses, DNS records, and metadata.

Module 10: Phishing Incident Management and Prevention

THEORY

- Identify the key damage indicators from successful phishing attacks and determine appropriate corrective actions to prevent recurrence.
- Explain phishing prevention policies in alignment with industry standards and

relevant regulations.

- Describe the components of an incident response plan specifically designed for phishing and social engineering attacks.
- Discuss the importance of stakeholder involvement and coordinated response efforts during phishing incidents.
- Evaluate the regulatory requirements related to data privacy and security in phishing incident prevention and response.
- Interpret trends in phishing threats and assess the effectiveness of employee training programs.

PRACTICAL

- Analyze a real-world phishing attack case to assess damage and identify corrective actions during a group discussion.
- Draft a phishing prevention policy based on industry standards and regulatory requirements, ensuring all key elements are included.
- Collaboratively develop a segment of an incident response plan for phishing attacks, highlighting roles and responsibilities.
- Perform a role-play exercise simulating a coordinated response to a phishing incident, involving key stakeholders and utilizing predefined protocols.
- Conduct a mock audit of an organization's phishing prevention strategies, focusing on data privacy and security compliance.
- Create and present a report on phishing threat trends and training effectiveness, using real-world data provided during the training session.

Module 11: Introduction to Employability Skills

THEORY

- Discuss the Employability Skills required for jobs in various industries
- List different learning and employability related GOI and private portals and their usage

Module 12: Constitutional values - Citizenship

THEORY

- Explain the constitutional values, including civic rights and duties, citizenship, responsibility towards society and personal values and ethics such as honesty, integrity, caring and respecting others that are required to become a responsible citizen
- Show how to practice different environmentally sustainable practices

Module 13: Becoming a Professional in the 21st Century

THEORY

- Discuss importance of relevant 21st century skills.
- Exhibit 21st century skills like Self-Awareness, Behaviour Skills, time management, critical and adaptive thinking, problem-solving, creative thinking, social and cultural awareness, emotional awareness, learning to learn etc. in personal or professional life.
- Describe the benefits of continuous learning

Module 14: Basic English Skills

THEORY

- Show how to use basic English sentences for everyday conversation in different contexts, in person and over the telephone
- Read and interpret text written in basic English
- Write a short note/paragraph / letter/e -mail using basic English

Module 15: Career Development and Goal Setting

THEORY

- Create a career development plan with well-defined short- and long-term goals

Module 16: Communication skills

THEORY

- Demonstrate how to communicate effectively using verbal and nonverbal communication etiquette.
- Explain the importance of active listening for effective communication
- Discuss the significance of working collaboratively with others in a team

Module 17: Diversity and Inclusion

THEORY

- Demonstrate how to behave, communicate, and conduct oneself appropriately with all genders and PwD
- Discuss the significance of escalating sexual harassment issues as per POSH

Module 18: Financial and Digital Literacy

THEORY

- Outline the importance of selecting the right financial institution, product, and service
- Demonstrate how to carry out offline and online financial transactions, safely and securely

Module 19: Essential Digital Skills

THEORY

- Describe the role of digital technology in today's life
- Demonstrate how to operate digital devices and use the associated applications and features, safely and securely
- Discuss the significance of displaying responsible online behaviour while browsing, using various social media platforms, e-mails, etc., safely and securely
- Create sample word documents, excel sheets and presentations using basic features
- utilize virtual collaboration tools to work effectively

Module 20: Entrepreneurship

THEORY

- Explain the types of entrepreneurship and enterprises
- Discuss how to identify opportunities for potential business, sources of funding and associated financial and legal risks with its mitigation plan
- Describe the 4Ps of Marketing-Product, Price, Place and Promotion and apply them as per requirement
- Create a sample business plan, for the selected business opportunity

Module 21: Customer Service

THEORY

- Describe the significance of analysing different types and needs of customers
- Explain the significance of identifying customer needs and responding to them in a professional manner.
- Discuss the significance of maintaining hygiene and dressing appropriately

Module 22: Getting Ready for Apprenticeship and Jobs

THEORY

- Create a professional Curriculum Vitae (CV)
- Use various offline and online job search sources such as employment exchanges, recruitment agencies, and job portals respectively
- Discuss the significance of maintaining hygiene and confidence during an interview