MINISTRY OF HUMAN RESOURCES

HRD CORP
HUMAN RESOURCE DEVELOPMENT CORPORATION

IndSF | INDUSTRIAL SKILLS FRAMEWORK

2nd Edition 2023

CYBERSECURITY

MDEC™ PIKOM CyberSecurity MALAYSIA
Company No. 200601006881 (726630-U)
Malaysian National Computer Confederation
MPC PERBADANAN PRODUKTIVITI MALAYSIA
MCMC

ACKNOWLEDGMENT

We would like to thank all subject matter experts and validators who have contributed to the development and enhance the Industrial Skills Framework document Digital Technology - Cybersecurity

MR. SHAIFUBAHRIM MOHD SALEH

MR. SIVA CHANDRAN A/L P. GOVINDA SAMY

TS. LEE HWEE HSIUNG

DR. PRAKASH CHRISTIANSEN A/L ANTHONY THOMAS

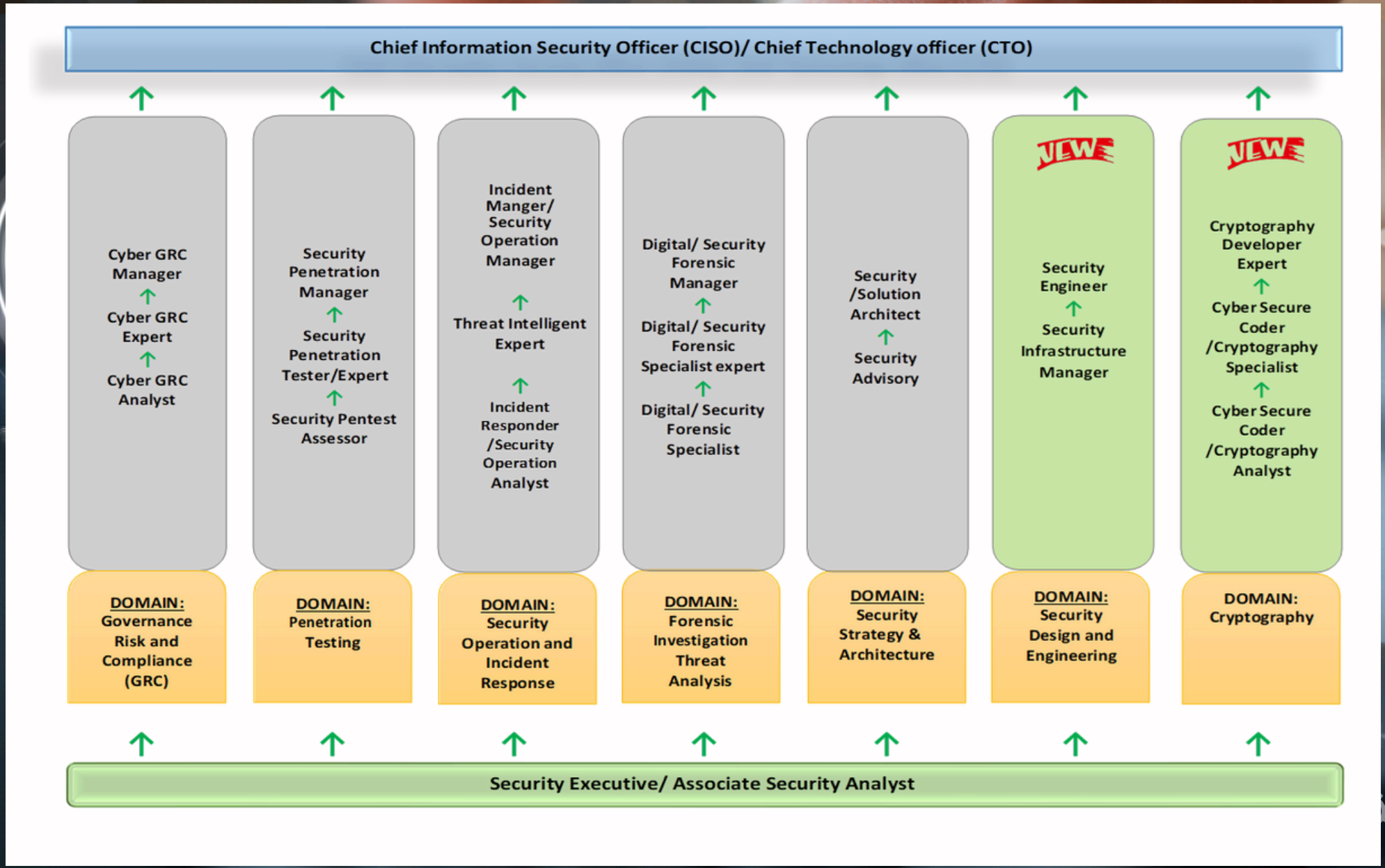
MS. ZAFREIDA BINTI ZAHRULLAYALI

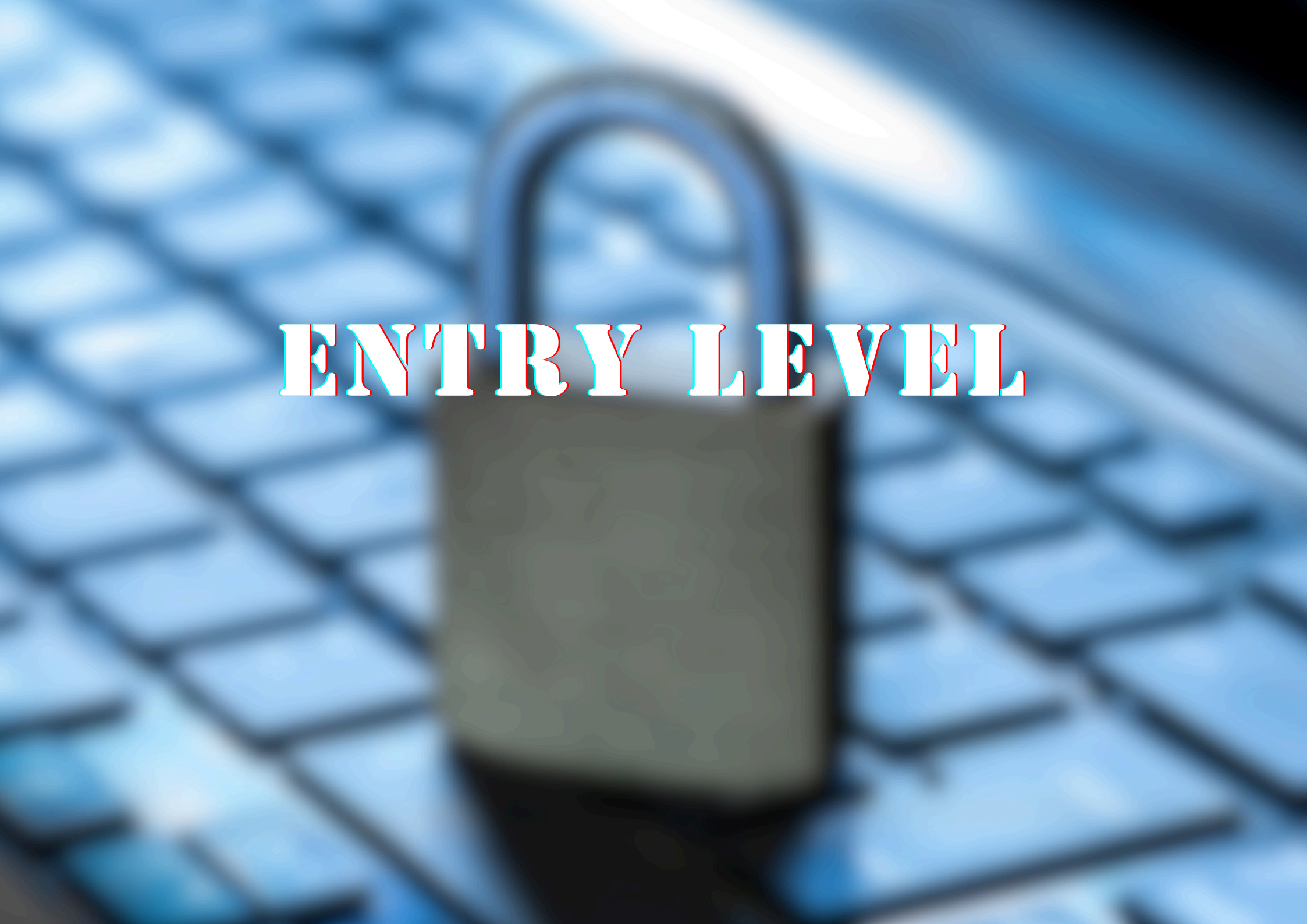
MR. MOHAMED ANWER YUSOFF

MS. KHANEEZA BINTI KHALID

MR. RAJ KUMAR A/L KUNHIRAMAN

Career Pathway




ENTRY LEVEL

Security Analyst/ Associate Security Analyst

Job Description

- To support administration, monitoring, and maintenance of security systems and operations.
- To monitor security alerts and events.
- To collect and document contextual information following established practices.
- To support the preparation and publishing of security advisories.
- To conduct vulnerability assessments and penetration testing to identify system and network vulnerabilities.
- To monitor and analyze security alerts and reports to identify potential security breaches.
- To provide incident response support.
- To implement security policies, procedures, and standards.
- To configure and manage security tools, including firewalls, antivirus software, and intrusion detection systems.

Common Certification

- A bachelor's degree in a relevant field such as Computer Science, Information Systems, Cybersecurity or other related field.
- ISACA CSX Fundamental Certificate (For Beginner)
- CompTIA A+ (For Beginner)
- EC-Council Certified Network Defender (CND) (For Beginner)
- Cisco Certified Entry Networking Technician (CCENT) (For Beginner)
- GIAC Security Essentials Certification (GSEC) (Level 1)
- Cisco Certified Network Professional Security (CCNP Security)
- CompTIA Security+
- EC-Council Certified Ethical Hacker (CEH)
- (ISC)² Systems Security Certified Practitioner (SSCP)
- EC-Council Certified Incident Handler (E|CIH)
- ITIL V4 Foundation for IT Service Management
- ISO/IEC 27001:2013 Information Security Management System Requirements
- Certified Information Security Management System Auditor (CISMSA)
- Certified Penetration Tester (Security Tools)
- Certified Incident Handling and Network Security Analyst
- Certified Digital Forensic for First Responder (Foundation)
- Certified Cryptography Foundation

Security Analyst/ Associate Security Analyst

Essential Skills

- Information Security Knowledge
- Risk Management
- Legal and Compliance Understanding
- Ethical Hacking Skills
- Technical Proficiency / Analytical Skills / Problem Solving Skills

Common Used Tools/ Technologies

- Programming and Scripting Tools
- Scanner (Network, Vulnerability)
- Governance, Risk and Compliance (Platforms)
- Security Information and Event Management (SIEM)
- Threat Intel

Soft Skills

- Communication
- Creative Thinking
- Teamwork
- Stakeholder Management

Competencies

- Cyber Incident Management & Problem Management
- Cyber Forensics
- Infrastructure Support
- Security Administration
- Security Assessment & Testing
- Security Education & Information Security Awareness
- Project Management
- Threat Intelligence & Detection
- Programming


GOVERNANCE
RISK &
COMPLIANCE

Cyber GRC Analyst

Job Description

- To assist and maintain cybersecurity governance frameworks and policies.
- To assist in developing cybersecurity standards, procedures, and guidelines aligned with industry best practices and regulatory requirements.
- To assist in conducting cybersecurity risk assessments within the organization.
- To identify potential vulnerabilities, analyze their impact, and report incidents.
- To contribute to minimizing threats to the organization's information systems and data.
- To play a key role in monitoring and detecting cybersecurity incidents.
- To investigate security breaches and coordinate response efforts.
- To participate in testing incident response plans and procedures for effective mitigation and recovery.

Common Certification

- A bachelor's degree in a relevant field such as Computer Science, Information Systems, Cybersecurity or other related field.
- Certified Information Systems Security Professional (CISSP)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Information Privacy Professional (CIPP)
- Certified Information Security Management System Auditor (CISMSA)
- Certified Information Systems Auditor (CISA)
- Certificate of Cloud Security Knowledge (CCSK)

Competencies

- Information Security and Cybersecurity Domain Knowledge
- Understanding and Awareness on ISO Standards and Industry Best Practices
- Understanding and Awareness on Malaysian Laws and Regulations related to Cybersecurity

Cyber GRC Analyst

Essential Skills

- Analytical Skills
- Communication Skills
- Attention to Detail
- Problem-Solving
- Collaboration and Relationship Building
- Continuous Learning
- Program Management (Audit Risk Compliance)

Soft Skills

- Communication
- Critical Thinking
- Problem-Solving
- Adaptability
- Collaboration
- Attention to Detail
- Time Management
- Ethical Conduct

Common Used Tools/ Technologies

- Governance, Risk, and Compliance Platforms
- Risk Assessment Tools
- Compliance Management Tools
- Security Information and Event Management (SIEM) Systems
- Vulnerability Management Tools
- Data Loss Prevention (DLP) Solutions
- Compliance and Risk Assessment Frameworks
- Documentation and Policy Management Tools
- Project Management and Collaboration Tools

Cyber GRC Expert

Job Description

- To establish and oversee security policies, standards, and procedures within the organization.
- To lead the organization's cybersecurity risk management program, conducting regular risk assessments and implementing effective risk mitigation strategies.
- To collaborate with business units to integrate risk management into decision-making processes.
- To ensure alignment of security practices with business objectives.
- To identify, assess, and prioritize risks related to information security.
- To develop risk mitigation strategies and action plans.
- To monitor risk exposure and adjust strategies as needed.
- To ensure compliance with relevant regulations, industry standards, and internal policies.
- To conduct regular audits and assessments to verify adherence.
- To provide guidance to teams on compliance requirements.
- To plan and execute internal and external cybersecurity audits, working collaboratively with audit teams.
- To address audit findings and implement improvements to enhance cybersecurity controls.
- To engage in research and development activities to enhance investigative techniques in the digital forensics field.
- To develop and deliver cybersecurity awareness and training programs for employees.
- To cultivate a culture of cybersecurity awareness and responsibility throughout the organization

Common Certification

- A bachelor's degree in a relevant field such as Computer Science, Information Systems, Cybersecurity or other related field.
- Minimum 5 years of experience in cybersecurity, risk management, or compliance.
- Certified Information Systems Security Professional (CISSP)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Information Security Manager (CISM)
- Certified Information Privacy Professional (CIPP)
- Certified Information Privacy Manager (CIPM)
- ISO 27001 Lead Implementer or Lead Auditor
- ISACA COBIT
- Certified Information System Auditor (CISA)
- Certified of Cloud Auditing Knowledge (CCAK)

Competencies

- Strategic Thinking
- Leadership
- Business Acumen
- Analytical and Problem-Solving Skills
- Communication and Influencing
- Collaboration and Relationship Building
- Regulatory and Industry Knowledge
- Change Management
- Ethical Conduct

Cyber GRC Expert

Essential Skills

- Strong Knowledge of Information Security and Cybersecurity Domain
- Governance, Risk, and Compliance (GRC) Expertise
- Risk Management
- Compliance Management
- Analytical and Problem-Solving Skills
- Communication and Stakeholder Management
- Leadership and Influence
- Ethical Conduct
- Continuous Learning
- Program Management (Audit Risk Compliance))

Soft Skills

- Communication
- Critical Thinking
- Problem-Solving
- Adaptability
- Collaboration
- Attention to Detail
- Time Management
- Ethical Conduct

Common Used Tools/ Technologies

- Governance, Risk, and Compliance Platforms
- Risk Assessment Tools
- Compliance Management Tools
- Security Information and Event Management (SIEM) Systems
- Vulnerability Management Tools
- Data Loss Prevention (DLP) Solutions
- Compliance and Risk Assessment Frameworks
- Documentation and Policy Management Tools
- Project Management and Collaboration Tools

Cyber GRC Manager

Job Description

- To develop, drive and direct the cybersecurity GRC strategy aligned with overall business objectives.
- To understand the organization's risk appetite, define long-term goals, and create a roadmap for achievement.
- To ensure the cybersecurity GRC program supports the organization's strategic direction and effectively manages risks
- To oversee the identification, assessment, and management of cybersecurity risks.
- To coordinate risk assessments, vulnerability assessments, and penetration tests.
- To develop risk treatment plans and ensure appropriate controls are in place for effective risk management.

Common Certification

- A bachelor's degree in a relevant field such as Computer Science, Information Systems, Cybersecurity or other related field.
- Minimum 7 years of experience in cybersecurity, risk management, or compliance.
- Certified Information Systems Security Professional (CISSP)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Information Security Manager (CISM)
- Certified in the Governance of Enterprise IT (CGEIT)
- Certified Information Privacy Professional (CIPP)
- ISO 27001 Lead Implementer/Lead Auditor
- Project Management Professional (PMP)

Competencies

- Cybersecurity Knowledge
- Governance, Risk, and Compliance Expertise
- Leadership and Management Skills
- Risk Management
- Compliance Management
- Communication and Influencing Skills
- Stakeholder Management
- Analytical and Critical Thinking
- Business Acumen
- Continuous Learning

Cyber GRC Manager

Essential Skills

- Strong Knowledge of Information Security and Cybersecurity Domain
- Governance, Risk, and Compliance (GRC) Expertise
- Risk Management
- Compliance Management
- Analytical and Problem-Solving Skills
- Communication and Stakeholder Management
- Leadership and Influence
- Ethical Conduct
- Continuous Learning
- Program Management (Audit Risk Compliance))

Soft Skills

- Communication
- Critical Thinking
- Problem-Solving
- Adaptability
- Collaboration
- Attention to Detail
- Time Management
- Ethical Conduct
- Decision Making Skills
- Conflict Resolution Skills

Common Used Tools/ Technologies

- Governance, Risk, and Compliance Platforms
- Risk Assessment Tools
- Compliance Management Tools
- Security Information and Event Management (SIEM) Systems
- Vulnerability Management Tools
- Data Loss Prevention (DLP) Solutions
- Compliance and Risk Assessment Frameworks
- Documentation and Policy Management Tools
- Project Management and Collaboration Tools


PENETRATION
TESTING

Security Pentest Assessor

Job Description

- To perform security assessments on computer systems, networks, and applications.
- To identify vulnerabilities, weaknesses, and potential security risks using various tools and techniques to simulate real-world attacks.
- To conduct penetration tests on target systems.
- To identify vulnerabilities and attempt exploitation for unauthorized access or data compromise.
- To Identify potential attack vectors, executing test scenarios, and documenting findings.
- To utilize vulnerability scanning tools for identifying and assessing vulnerabilities.
- Conducting automated scans to discover weaknesses like misconfigurations or unpatched software.
- Documenting assessment steps, techniques used, and potential impact of identified vulnerabilities.
- To provide detailed recommendations for addressing and mitigating identified vulnerabilities.
- To stay updated with the latest security threats, attack techniques, and countermeasures.
- To keep abreast of new vulnerabilities, exploits, and emerging security technologies.
- To apply industry best practices and follow ethical hacking guidelines.
- To understand system architecture, application design, and relevant security requirements.
- To utilize effective communication skills to explain technical concepts, discuss findings, and provide clear recommendations.
- To assist in the remediation process by providing guidance and clarification on identified vulnerabilities.
- Collaborating with the organization's IT and security teams to ensure proper implementation of security measures.
- To consider compliance requirements and regulatory frameworks applicable to the organization.
- To ensure alignment of security assessments with standards, legal, and ethical guidelines.
- To stay updated with the latest security technologies, tools, and techniques.
- To engage in continuous learning, attending conferences, and obtaining relevant certifications.
- To enhance expertise in security assessments and penetration testing methodologies.

Security Pentest Assessor

Common Certification

- Certified Ethical Hacker (CEH)
- Offensive Security Certified Professional (OSCP)
- Certified Penetration Testing Engineer (CPTE)
- GIAC Penetration Tester (GPEN)
- Certified Information Systems Security Professional (CISSP)
- Certified Web Application Penetration Tester (CWAPT)
- Certified Mobile and Web Application Penetration Tester (CMWAPT)

Competencies

- Technical Proficiency
- Penetration Testing Methodologies
- Vulnerability Assessment
- Ethical Hacking Techniques
- Security Tools
- Risk Assessment and Management
- Compliance and Regulatory Knowledge
- Documentation and Reporting
- Continuous Learning
- Professionalism and Ethics

Security Pentest Assessor

Essential Skills

- Technical Proficiency
- Ethical Hacking Techniques
- Vulnerability Assessment
- Penetration Testing Methodologies
- Security Tools and Technologies
- Risk Assessment and Management
- Critical Thinking and Problem-Solving
- Attention to Detail
- Documentation and Reporting

Soft Skills

- Communication Skills
- Active Listening
- Problem-Solving Abilities
- Analytical Thinking
- Adaptability
- Time Management
- Attention to Detail
- Client-Focused Approach
- Collaboration and Teamwork
- Ethical Conduct
- Continuous Learning

Common Used Tools/ Technologies

- Network and vulnerability scanning tools
- Software security application software
- Penetration testing frameworks and tools
- Network packet analysing tools
- Password cracking and testing tools
- Wired and wireless network security tools
- Web application scanning tools
- Advanced penetration testing and security auditing operating systems

Security Penetration Tester

Job Description

- To collaborate with clients or project stakeholders.
- To define the scope of the penetration testing engagement.
- To understand goals, objectives, and constraints.
- To develop a testing plan and methodology based on the defined scope.
- To identify target systems, networks, or applications for testing.
- To gather necessary information about the target environment.
- To conduct vulnerability assessments using various tools and techniques.
- To provide technical expertise and support during complex assessments.
- To scan target systems, networks, and applications for potential vulnerabilities and misconfigurations.
- To work closely with clients to understand security requirements.
- To utilize ethical hacking techniques to exploit identified vulnerabilities.
- To gain unauthorized access to systems or applications.
- To simulate real-world attacks and assess the effectiveness of existing security controls.
- To adhere to legal and ethical guidelines.
- To perform social engineering tests to assess the human element of security.
- To conduct phishing attacks, physical security bypass, or other tactics.
- To test the organization's ability to defend against social engineering attacks.
- To prepare comprehensive reports detailing identified vulnerabilities and their potential impact.
- To provide actionable recommendations to address identified vulnerabilities.
- To offer support and guidance during the remediation process.
- To ensure that penetration testing activities and deliverables comply with applicable legal, regulatory, and industry standards.
- To address questions or concerns regarding identified vulnerabilities and recommended mitigation strategies.
- To stay updated with the latest security threats, attack techniques, and security technologies.
- To engage in continuous learning and professional development.
- To enhance skills and stay at the forefront of the field.
- To maintain a high level of ethical conduct throughout the testing process.
- To respect client confidentiality and ensure assessments are conducted within agreed-upon boundaries.

Security Pentest Tester

Common Certification

- Certified Ethical Hacker (CEH)
- Offensive Security Certified Professional (OSCP)
- Certified Penetration Testing Professional (CPENT)
- Certified Information Systems Security Professional (CISSP)
- GIAC Penetration Tester (GPEN)
- Certified Penetration Tester (CPT)
- eLearnSecurity Certified Professional Penetration Tester (eCPPT)
- Certified Web Application Penetration Tester (CWAPT)
- Offensive Security Certified Professional (OSCP)
- A bachelor's degree in a relevant field such as Computer Science, Information security, Cybersecurity or other related field. A master's degree is an added advantage.
- Minimum 3 years of experience in penetration testing.

Competencies

- Technical Knowledge
- Penetration Testing Methodologies
- Vulnerability Assessment
- Exploitation Techniques
- Security Tools and Technologies
- Risk Assessment
- Reporting and Documentation
- Industry Knowledge
- Problem-Solving and Analytical Thinking
- Communication and Collaboration
- Ethical Conduct

Security Pentest Tester

Essential Skills

- Technical Proficiency
- Ethical Hacking Techniques
- Vulnerability Assessment
- Penetration Testing Methodologies
- Security Tools and Technologies
- Risk Assessment and Management
- Critical Thinking and Problem-Solving
- Attention to Detail
- Documentation and Reporting

Soft Skills

- Communication Skills
- Active Listening
- Problem-Solving Abilities
- Analytical Thinking
- Adaptability
- Time Management
- Attention to Detail
- Client-Focused Approach
- Collaboration and Teamwork
- Ethical Conduct
- Continuous Learning

Common Used Tools/ Technologies

- Network and vulnerability scanning tools
- Software security application software
- Penetration testing frameworks and tools
- Network packet analysing tools
- Password cracking and testing tools
- Wired and wireless network security tools
- Web application scanning tools
- Advanced penetration testing and security auditing operating systems

Security Penetration Manager

Job Description

- To lead and manage a team of Security Penetration Testers.
- To recruit, hire, and train team members.
- To provide guidance, mentoring, and performance evaluations.
- To oversee the planning, execution, and delivery of penetration testing projects.
- To coordinate with clients, understand project requirements, and assign resources.
- To ensure timely and high-quality project deliverables.
- To effectively communicate with stakeholders, including clients, senior management, and other teams.
- To communicate assessment findings and recommendations to clients or project stakeholders in a clear and understandable manner.
- To build and maintain strong client relationships.
- To develop and implement strategies to enhance the effectiveness and efficiency of the penetration testing process.
- To define testing methodologies, frameworks, and best practices.
- To continuously improve the team's skills and capabilities.
- To provide guidance on penetration testing scope and objectives.
- To ensure the quality and accuracy of penetration testing activities and deliverables.
- To review and validate assessment reports.
- To conduct technical reviews of methodologies.
- To implement quality control measures.
- To manage risks associated with penetration testing activities.
- To evaluate potential impacts and develop risk mitigation strategies.
- To ensure compliance with legal and ethical standards.
- To provide technical leadership and guidance to the team of Security Penetration Testers.
- To improve the security posture of tested systems, networks, or applications.
- To collaborate with stakeholders to prioritize and implement remediation measures
- To stay updated with the latest security trends, technologies, and vulnerabilities.
- To drive continuous improvement initiatives within the penetration testing team.
- To identify areas for improvement and implement process enhancements.
- To foster a culture of innovation and learning.
- To present assessment findings and explain technical concepts in a non-technical manner.
- To advise on security strategies and recommendations.
- To understand and adhere to relevant regulations, such as PCI DSS or GDPR.
- To manage the budget allocated for penetration testing projects.

Security Pentest Manager

Common Certification

- Certified Ethical Hacker (CEH)
- Offensive Security Certified Professional (OSCP)
- Certified Penetration Testing Professional (CPENT)
- Certified Information Systems Security Professional (CISSP)
- GIAC Penetration Tester (GPEN)
- Certified Penetration Tester (CPT)
- eLearnSecurity Certified Professional Penetration Tester (eCPPT)
- Certified Web Application Penetration Tester (CWAPT)
- Offensive Security Certified Professional (OSCP)
- A bachelor's degree in a relevant field such as Computer Science, Information security, Cybersecurity or other related field. A master's degree is an added advantage.
- Minimum 3 years of experience in penetration testing.

Competencies

- Technical Knowledge
- Penetration Testing Methodologies
- Vulnerability Assessment
- Exploitation Techniques
- Security Tools and Technologies
- Risk Assessment
- Reporting and Documentation
- Industry Knowledge
- Problem-Solving and Analytical Thinking
- Communication and Collaboration
- Ethical Conduct
- Strategic thinking
- Business Acumen

Security Pentest Manager

Essential Skills

- Technical Proficiency
- Ethical Hacking Techniques
- Vulnerability Assessment
- Penetration Testing Methodologies
- Security Tools and Technologies
- Risk Assessment and Management
- Critical Thinking and Problem-Solving
- Attention to Detail

Soft Skills

- Leadership
- Communication
- Collaboration
- Problem-Solving
- Time Management
- Adaptability
- Emotional Intelligence
- Ethical Conduct
- Client Relationship Management
- Continuous Learning

Common Used Tools/ Technologies

- Network and vulnerability scanning tools
- Software security application software
- Penetration testing frameworks and tools
- Network packet analysing tools
- Password cracking and testing tools
- Wired and wireless network security tools
- Web application scanning tools
- Advanced penetration testing and security auditing operating systems
- Post exploitation tools
- Adversary simulation tools


INCIDENT RESPONDER
/
SECURITY OPERATION
ANALYST

Incident Responder / Security Operation Analyst

Job Description

- To continuously monitor and track various sources of threat intelligence.
- Including open-source feeds, internal data sources, and vendor reports.
- To identify emerging threats.
- To gather and compile data related to known threats, vulnerabilities, and attacks.
- Including malware indicators, attack techniques, and attacker profiles.
- To analyze collected data to understand the potential impact of threats.
- On the organization's systems, data, and operations.
- To evaluate severity, relevance, and potential exposure.
- To identify patterns, trends, and developments in the threat landscape. Including tracking changes in attack methods, tactics, techniques, and procedures (TTPs).
- To create and distribute threat intelligence reports and alerts.
- To relevant stakeholders within the organization.
- Providing actionable recommendations for mitigating threats.
- To collaborate with the vulnerability management team.
- To assess the organization's systems and infrastructure for vulnerabilities and potential weaknesses.
- To support incident response teams.
- To participate in threat information sharing forums.
- To collaborate with external organizations, such as ISACs.
- To exchange threat intelligence.
- To utilize and manage threat intelligence platforms and tools for data collection, analysis, and dissemination.
- To conduct training and awareness programs for staff.
- To enhance their understanding of cybersecurity threats and best practices.
- To stay up-to-date with cybersecurity regulations and compliance requirements ensuring that the organization remains in compliance with relevant standards.

Incident Responder / Security Operation Analyst

Common Certification

- GIAC Cyber Threat Intelligence (GCTI)
- GIAC Certified Intrusion Analyst Certification (GCIA)
- GIAC Certified Incident Handler (GCIH)
- GIAC Penetration Tester (GPEN)
- (ISC)² Certified Information Systems Security Professional (CISSP)
- EC-Council Certified SOC Analyst (CSA)
- EC-Council Certified Threat Intelligence Analyst (CTIA)
- EC-Council Certified Incident Handler (ECIH)
- EC-Council Certified Network Defender (CND)
- EC-Council Certified Ethical Hacking (CEH)
- CompTIA PenTest+
- CompTIA Cybersecurity Analyst (CySA+)
- ISO/IEC 27001 ISMS Lead Implementer/ Lead Auditor
- ISO/IEC 22301 BCMS Lead Implementer/ Lead Auditor
- CREST Certification

Competencies

- Cyber Incident Management
- Cyber Risk Management and Assessment
- Disaster Recovery Management
- Threat Analysis & Defense
- Threat Intelligence & Detection
- Enterprise Architecture
- Cyber Crisis Management
- Cyber Forensic
- Surveillance and Incident Response
- Operations Management

Incident Responder / Security Operation Analyst

Essential Skills

- Incident Management
- ITIL
- Troubleshooting

Soft Skills

- Communication
- Creative Thinking
- Problem Solving
- Sense Making
- Teamwork
- Stakeholder Management
- Analytical Thinking

Common Used Tools/ Technologies

- Security Information and Event Management (SIEM) systems
- Network/ Packet Analyzer tools
- Vulnerability Assessment and Penetration Testing (VAPT) tools
- Malware Analysis tools
- Multi OS platform software
- Network/ Packet Analyzer tools
- Vulnerability Assessment and Penetration Testing (VAPT) tools
- Malware Analysis tools
- Incident Management Ticketing systems
- Virtual Environment

Threat Intelligence Expert

Job Description

- To continuously monitor and track various sources of threat intelligence.
- Including open-source feeds, internal data sources, and vendor reports.
- To identify emerging threats.
- To gather and compile data related to known threats, vulnerabilities, and attacks.
- Including malware indicators, attack techniques, and attacker profiles.
- To analyze collected data to understand the potential impact of threats.
- On the organization's systems, data, and operations.
- To evaluate severity, relevance, and potential exposure.
- To identify patterns, trends, and developments in the threat landscape. Including tracking changes in attack methods, tactics, techniques, and procedures (TTPs).
- To create and distribute threat intelligence reports and alerts.
- To relevant stakeholders within the organization.
- Providing actionable recommendations for mitigating threats.
- To collaborate with the vulnerability management team.
- To assess the organization's systems and infrastructure for vulnerabilities and potential weaknesses.
- To support incident response teams.
- To participate in threat information sharing forums.
- To collaborate with external organizations, such as ISACs.
- To exchange threat intelligence.
- To utilize and manage threat intelligence platforms and tools for data collection, analysis, and dissemination.
- To conduct training and awareness programs for staff.
- To enhance their understanding of cybersecurity threats and best practices.
- To stay up-to-date with cybersecurity regulations and compliance requirements.
- Ensuring that the organization remains in compliance with relevant standards.

Threat Intelligence Expert

Common Certification

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified Information Systems Security Professional (CISA)
- CompTIA Security+
- Certified Ethical Hacker (CEH)
- GIAC Certified Incident Handler (GCIH)
- GIAC Cyber Threat Intelligence (GCTI)
- EC-Council Certified Security Analyst (ECSA)
- Certified Threat Intelligence Analyst (CTIA)
- Cisco Certified CyberOps Associate
- A bachelor's degree in a relevant field such as Computer Science, Information Technology, Cybersecurity or other related field. A master's degree is an added advantage.
- Minimum 7 years of experience in with a focus on threat intelligence

Competencies

- Cybersecurity Knowledge
- Threat Analysis
- Information Gathering
- Data Analysis
- Risk Assessment
- Communication Skills
- Incident Response
- Tool Proficiency
- Continuous Learning
- Security Compliance
- Technical Skills

Threat Intelligence Expert

Essential Skills

- Malware analysis
- Network analysis
- Data collection and analysis tools
- Security information and event management (SIEM) systems
- Threat intelligence platforms
- Encryption and authentication protocols
- Open-source intelligence (OSINT) tools
- Digital forensics tools
- Intrusion detection and prevention systems (IDS/IPS)
- Programming and scripting (e.g., Python, PowerShell)
- Vulnerability assessment tools

Soft Skills

- Critical thinking
- Attention to detail
- Problem-solving
- Analytical skills
- Communication skills
- Adaptability
- Teamwork
- Time management
- Emotional intelligence
- Cross-functional collaboration
- Report writing
- Continuous learning

Common Used Tools/ Technologies

- Security Information and Event Management (SIEM)
- Multi OS platform software
- Network/ Packet Analyzer tools
- Vulnerability Assessment and Penetration Testing (VAPT) tools
- Malware Analysis tools
- Incident Management Ticketing systems

Incident Manager / Security Operation Manager

Job Description

- To manage, develop, and implement capabilities for SOC comprised of both outsourced and in-house resources structured to efficiently and effectively respond to incidents.
- To lead the operations of the security monitoring and intelligence team.
- To ensure optimal identification and resolution of security incidents.
- To manage outsourced and in-house security monitoring and intelligence team services.
- To ensure quality performance and fulfilment of Service Level Agreements (SLA).
- To direct the functions, processes, and operations of the security monitoring and intelligence team.
- To ensure policies, procedures, and objectives align with company goals.
- To oversee the monitoring, identification, and resolution of security incidents.
- To ensure threats detection through analysis, investigations, and prioritization of incidents based on risk/exposure.
- To develop, maintain, and lead an incident response management program including incident detection, analysis, containment, eradication, recovery, and chain of evidence/forensic artifacts required for additional investigations.
- To conduct scheduled and ad hoc training exercises to ensure staff are adequately prepared for incidents.
- To ensure adherence to regulatory compliance and laws governing information security, personal identifiable information, and assets.
- To identify potential threats/compromises targeting the company.
- To develop proactive strategies to minimize the impact of these threats.

Common Certification

- EC-Council Information Security Manager (EISM)
- Certified Information Systems Security Professional (CISSP)
- Projects In Controlled Environments (PRINCE2)
- Project Management Professional (PMP)
- GIAC Security Operation Manager (GSOM)
- GIAC Certified Incident Handler (GCIH)
- GIAC Cyber Threat Intelligence (GCTI)
- Certified Information Security Manager (CISM)
- CREST Certification
- ISO/IEC 27001 ISMS Lead Implementer/ Lead Auditor
- ISO/IEC 22301 BCMS Lead Implementer/ Lead Auditor

Competencies

- Cyber Incident Management
- Cyber Risk Management and Assessment
- Disaster Recovery Management
- Threat Analysis & Defense
- Threat Intelligence & Detection
- Enterprise Architecture
- Cyber Crisis Management
- Cyber Forensic
- Surveillance and Incident Response
- Operations Management
- Emerging Tech

Threat Intelligence Expert

Essential Skills

- Security Information and Event Management (SIEM)
- Multi OS platform software
- Network/ Packet Analyzer tools
- Vulnerability Assessment and Penetration Testing (VAPT) tools
- Malware Analysis tools
- Incident Management Ticketing systems
- Virtual Environment
- Security Audit and Risk Assessment

Soft Skills

- Communication
- Creative Thinking
- Problem Solving
- Teamwork
- Stakeholder Management
- Analytical Thinking
- Leadership Skills

Common Used Tools/ Technologies

- Security Information and Event Management (SIEM) systems
- Network/ Packet Analyzer tools
- Vulnerability Assessment and Penetration Testing (VAPT) tools
- Malware Analysis tools
- Encryption tools


FORENSIC
INVESTIGATION
THREAT ANALYSIS

Digital/Security Forensic Specialist

Job Description

- To assist in conducting forensic analysis on complex cases
- To assist in conducting digital evidence preservation at field site for complex cases
- To assist in conducting research on forensic acquisition and analysis of emerging technologies.
- To execute analysis methods for complex cases and new, emerging technologies to solve incoming cases.
- To assist in implementation of guidelines and best practices for acquistion, analysis and presentation of digital evidence
- To utilize tools to assist forensic acquisition and analysis of digital evidence
- To produce forensic reports

Common Certification

- Fundamentals of Incident Response, Threat Hunting, and Digital Forensics
- Enterprise Cloud Forensics and Incident Response
- Reverse-Engineering Malware: Malware Analysis Tools and Techniques
- Fundamentals of Network Forensics: Threat Hunting, Analysis, and Incident Response
- Smartphone Forensic Analysis In-Depth
- Mac and iOS Forensic Analysis and Incident Response
- AccessData Certified Examiner (ACE)
- IACIS Certified Forensic Computer Examiner (CFCE)
- GIAC Certified Forensic Analyst (GCFA)
- EnCase™ Certified Examiner (EnCE)
- EC-Council Computer Hacking Forensic Investigator (CHFI)
- GIAC Certified Forensic
- Magnet Axiom certification

Digital/Security Forensic Specialist

Essential Skills

- Network, Firewall, WAF, SIEM, EDR, AV and Penetration Security
- Operating System and Architecture
- Computer Forensics
- Scripting
- Forensic Analysis
- Cloud, Mobile, Technology Infrastructure

Common Used Tools/ Technologies

- Digital Forensics Tools
- Digital Identity Tools
- Data protection Tools
- Secure Infrastructure Tools
- Scripting Tools
- Security Information and Event Management (SIEM) tools
- Open Source Tools

Competencies

- Cyber Forensic
- Cyber Risk Management
- Cyber Incident Management
- Security Assessment & Testing
- Threat Analysis & Defense
- Threat Intelligence & Detection
- Enterprise and Device Architecture
- Law and regulation
- IT and Network Domain
- Cloud Security
- Mobile and IoT Security
- Malware Analysis / Reverse Engineering

Soft Skills

- Communication
- Creative Thinking
- Problem Solving
- Teamwork
- Stakeholder Management
- Analytical and Investigation Skills
- Ethics and Trust

Digital/Security Forensic Expert

Job Description

- To conduct systematic investigations and collect digital evidence from various sources.
- To ensure data integrity and chain of custody while preserving evidence from computers, mobile devices, networks, and cloud environments.
- To collaborate with incident response teams to identify and analyze security incidents.
- To determine the extent of breaches and develop strategies for containment, eradication, and recovery.
- To provide guidance and support in incident handling and reporting.
- To utilize advanced digital forensic tools and methodologies for analyzing digital evidence.
- To extract relevant information, including recovering deleted files, examining system logs, analyzing network traffic, and decrypting encrypted data.
- To perform data recovery operations on compromised systems and devices.
- To retrieve valuable evidence or data intentionally or unintentionally deleted, encrypted, or hidden.
- To prepare detailed reports and documentation of findings and investigative methods.
- To present findings in a clear and concise manner suitable for technical and non-technical audiences.
- To collaborate with legal teams and provide expert testimony in court proceedings.
- To prepare and present technical evidence supporting legal arguments.
- To assist in drafting affidavits and search warrants and stay updated on relevant laws and regulations.
- To stay current with emerging digital forensic tools, technologies, and methodologies.
- To engage in research and development activities to enhance investigative techniques in the digital forensics field.
- To stay current with emerging digital forensic tools, technologies, and methodologies.

Digital/Security Forensic Expert

Common Certification

- ITIL Foundation: ITIL (Information Technology Infrastructure Library).
- Certified Incident Manager (CIM):
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Project Management Professional (PMP).
- Certified Business Continuity Professional (CBCP)
- Certified Incident Handling Engineer (CIHE)
- Certified Information Privacy Professional (CIPP)
- Certified Forensic Computer Examiner (CFCE)
- EnCase Certified Examiner (EnCE)
- Certified Computer Examiner (CCE)
- GIAC Certified Forensic Analyst (GCFA)
- Certified Digital Forensic for First Responder (CDFFR)
- GIAC Certified Incident Handler (GCIH)
- EC-Council Certified Incident Handler (ECIH)
- Certified Cyber Forensics Professional (CCFP)
- A bachelor's degree in a relevant field such as Computer Science, Digital Forensics, Cybersecurity or other related field. A master's degree is an added advantage.
- Mininum 7 years of experience in digital forensics.

Competencies

- Incident Management Expertise
- Technical Knowledge
- Problem-Solving Skills
- Stakeholder Management
- Adaptability and Resilience
- Documentation and Reporting
- Customer Focus

Digital/Security Forensic Expert

Essential Skills

- Proficiency in using digital forensic tools and software.
- In-depth understanding of computer systems, file structures, and network protocols.
- Strong analytical and problem-solving skills.
- Knowledge of legal and ethical considerations in digital forensics

Soft Skills

- Communication
- Creative Thinking
- Problem Solving
- Teamwork
- Stakeholder Management

Common Used Tools/ Technologies

- Cyber Defense Tools
- Digital Identity Tools
- Data protection Tools
- Secure Infrastructure Tools
- Scripting Tools (eg. Python)
- Security Information and Event Management (SIEM) tools

Digital/Security Forensic Manager

Job Description

- To drive and direct forensic acquisition and analysis work.
- To ensure the right methods and tools are being applied to the forensic acquisition and analysis work.
- To ensure the right methods and tools are applied to forensic acquisition and analysis work.
- To review and endorse forensic results and/or patterns.
- To ensure consistency, accuracy, and the quality of work.
- To attend meetings and provide inputs on forensic findings.
- To assist in investigation and strategic decisions.
- Develop and implement strategic plans for the digital forensics function.
- To provide input for improving the competency development and continuous education program for the digital/security forensics team.
- To provide expert testimony in court.

Common Certification

- Certified Information Systems Security Professional (CISSP)
- Project Management Professional (PMP)
- Certified Forensic Computer Examiner (CFCE)
- EnCase Certified Examiner (EnCE)
- Certified Computer Examiner (CCE)
- GIAC Certified Forensic Analyst (GCFA)
- Certified Digital Forensic for First Responder (CDFFR)
- GIAC Certified Incident Handler (GCIH)
- EC-Council Certified Incident Handler (ECIH)
- Certified Cyber Forensics Professional (CCFP)
- A bachelor's degree in a relevant field such as Computer Science, Digital Forensics, Cybersecurity or other related field. A master's degree is an added advantage.
- Mininum 7 years of experience in digital forensics.

Competencies

- Digital Forensics Expertise
- Cybersecurity Knowledge
- Incident Response Management
- Governance, Risk, and Compliance Expertise
- Leadership and Team Management
- Analytical and Critical Thinking
- Communication Skills
- Stakeholder Management
- Continuous Learning

Digital/Security Forensic Manager

Essential Skills

- Digital Forensics
- Cybersecurity Knowledge
- Incident Response Management
- Compliance Management
- Leadership and Team Management
- Analytical and Critical Thinking
- Communication
- Continuous Learning

Soft Skills

- Communication Skills
- Leadership Skills
- Teamwork and Collaboration
- Problem-Solving and Analytical Thinking
- Adaptability and Flexibility
- Emotional Intelligence
- Time Management
- Decision-Making Skills

Common Used Tools/ Technologies

- Cyber Defense Tools
- Digital Identity Tools
- Data protection Tools
- Secure Infrastructure Tools
- Scripting Tools (eg. Python)
- Security Information and Event Management (SIEM) tools


SECURITY STRATEGY
&
ARCHITECTURE

Security Advisor

Job Description

- To develop and implement cybersecurity policies, procedures, and standards.
- To conduct regular risk assessments and vulnerability tests.
- To identify security threats and address security weaknesses.
- To stay up-to-date on industry trends and emerging threats.
- To ensure the organization's security measures remain effective.
- To provide training and guidance to employees on cybersecurity standards and best practices.
- To develop and manage incident response plans and protocols.
- To ensure a timely and effective response to threats.
- To collaborate with IT and other departments.
- To ensure security measures are integrated throughout the organization's systems and networks.
- To review and assess third-party security vendors.
- To ensure they meet the organization's security requirements.
- To maintain cybersecurity standards and documentations.
- To coordinate and advise control owners on the organization's cybersecurity implementation.
- To test and evaluate security controls.
- To ensure they meet the desired outcome of the organization's security requirements.

Common Certification

- Certified Information Security Awareness Manager
- Certified Information Security Management System Auditor
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- CompTIA Security+
- GIAC Security Essentials Certification (GSEC)
- Certified Information Systems Auditor (CISA)
- ISO 27001 Lead Auditor
- Certified in Risk and Information Systems Control (CRISC)
- Certified Cloud Security Professional (CCSP)
- A bachelor's degree in a relevant field such as Computer Science, Information Systems, Cybersecurity or other related field. A master's degree is an added advantage.
- Minimum 5 years of experience in cybersecurity, with a focus on assurance validation and compliance.

Security Advisor

Competencies

- Expert in cybersecurity domains such as security assurance, incident handling response, digital forensics, governance, risks, compliance, cryptography.
- Analytical Skills
- Technical Skills - various programming languages, operating systems, and network protocols.
- Problem-Solving Skills
- Technical knowledge on firewalls, intrusion detection systems, encryption, and malware analysis.
- Compliance - familiar with compliance regulations such as GDPR or HIPAA, depending on the industry they work in.

Essential Skills

- Risk Management
- Compliance Knowledge
- Leadership Skills
- Strategic Planning
- Incident Response
- Policy and Procedure Development
- Security Awareness and Training
- Vendor and Third-Party Risk Management
- Project Management
- Technical Skills
- Data Analysis
- Legal and Ethical Understanding
- Vendor and Tool Evaluation

Common Used Tools/ Technologies

- Firewall and intrusion detection systems (IDS)
- Vulnerability scanning and assessment tools
- Security incident and event management (SIEM) systems
- Antivirus and anti-malware software
- Network access control (NAC) systems
- Data loss prevention (DLP) tools
- Identity and access management (IAM) systems
- Encryption and decryption technologies
- Two-factor authentication (2FA) and multi-factor authentication (MFA) technologies
- Mobile device management (MDM) tools
- Security Awareness and Training Systems
- Authentication and Identity Management Tools
- Reporting Systems
- Risk Assessment and Management Tools
- Compliance and Policy Management Tools

Soft Skills

- Communication skills
- Critical thinking and problem-solving
- Flexibility and adaptability
- Collaboration and teamwork
- Attention to detail
- Ethics and integrity

Security/Solution Architect

Job Description

- To identify security risks and vulnerabilities.
- To develop strategies to mitigate identified risks.
- Developing Security Architecture and Systems:
- To develop and design security architecture and systems.
- To meet business requirements and security standards.
- To develop and implement security policies and procedures.
- To ensure compliance with regulatory requirements and industry standards.
- To collaborate with other IT teams.
- To integrate security solutions into existing systems and networks.
- To conduct security assessments and audits.
- To identify vulnerabilities and gaps in security systems.
- To provide technical leadership and guidance. To cybersecurity teams and other IT departments.
- To research and stay up-to-date on the latest trends and technologies in cybersecurity.
- To develop and maintain documentation related to security architecture and solutions.

Common Certification

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified Cloud Security Professional (CCSP)
- Certified Ethical Hacker (CEH)
- Cisco Certified Network Associate - Security (CCNA Security)
- CompTIA Security+
- GIAC Information Security Fundamentals (GISF)
- (ISC)² Certified Cloud Security Professional (CCSP)
- Certified Information Systems Auditor (CISA)
- A bachelor's degree in a relevant field such as Computer Science, Information Security, Cybersecurity or other related field. A master's degree is an added advantage.
- Minimum 5 years of experience in digital forensics.

Security/Solution Architect

Essential Skills

- Cybersecurity expertise
- Technical skills
- Problem-solving skills
- Communication skills
- Project management skills
- Risk management skills

Soft Skills

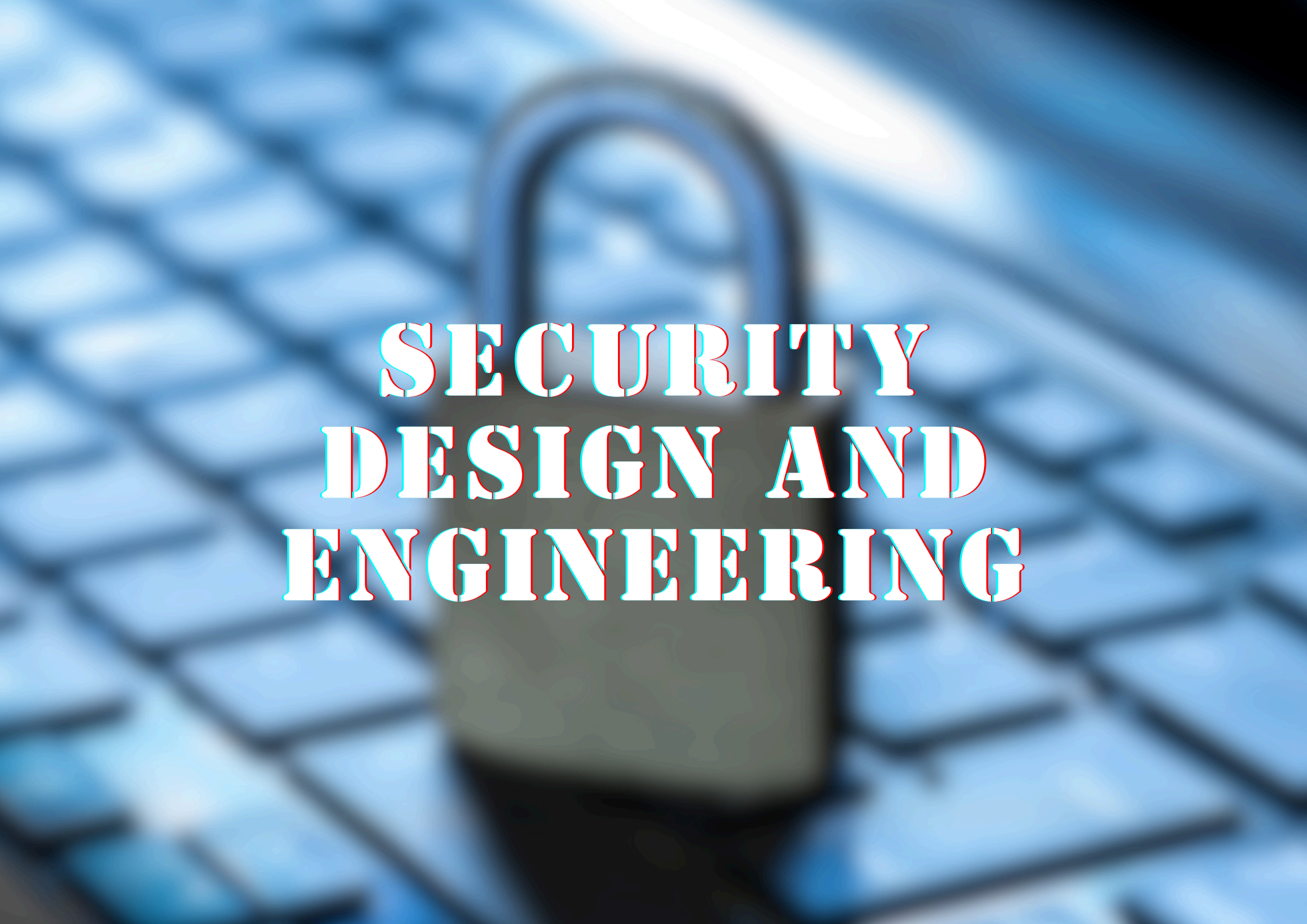
- Communication
- Leadership
- Problem-solving
- Adaptability

Competencies

- Technical expertise
- Communication skills
- Analytical and problem-solving skills
- Project management skills
- Creativity
- Business acumen

Common Used Tools/ Technologies

- Security Information and Event Management (SIEM) systems
- Intrusion Detection and Prevention Systems


SECURITY
DESIGN AND
ENGINEERING

Cybersecurity Infrastructure Manager

Job Description

- To develop and implement security policies and procedures.
- To safeguard the organization's assets.
- To oversee the installation, configuration, and maintenance of security infrastructure.
- Including firewalls, intrusion detection systems, and other security tools.
- To identify potential security risks and to develop strategies to mitigate the risks.
- To conduct regular security audits.
- To ensure the organization's security infrastructure is up-to-date and effective.
- To manage security incidents which includes responding to security breaches and coordinating with law enforcement agencies.
- To manage a team of security professionals.
- To provide guidance and support to ensure effective performance of duties.
- To keep up-to-date with the latest security trends and technologies.

Common Certification

- Certified Penetration Tester
- Certified Incident Handling and Network Security
- Certified Information Security Management System Auditor
- Certified Information Systems Security Professional (CISSP):
- Certified Ethical Hacker (CEH)
- CompTIA Security+
- Certified Cryptography Expert (CCE)
- A bachelor's degree in a relevant field such as Computer Science, Information Systems, Cybersecurity or other related field. A master's degree is an added advantage.
- Minimum 7 years of experience in with a focus on infrastructure management.

Cybersecurity Infrastructure Manager

Common Used Tools/ Technologies

- Vulnerability Assessment and Scanning Tools
- Security Information and Event Management (SIEM) Systems
- Security Analytics and Threat Detection Tools
- Penetration Testing Tools
- Risk Assessment and Management Tools
- Compliance and Policy Management Tools
- Incident Response and Forensics Tools
- Network Security Tools
- Cloud Security Tools
- Collaboration and Communication Tools
- Security Awareness and Training Systems
- Authentication and Identity Management Tools
- Mobile Device Management (MDM) Tools
- Reporting Systems

Competencies

- Expert in cybersecurity domains such as security assurance, incident handling response, digital forensics, governance, risks, compliance, cryptography.
- Analytical Skills
- Technical Skills - various programming languages, operating systems, and network protocols.
- Problem-Solving Skills

Essential Skills

- Risk Management
- Compliance Knowledge
- Leadership Skills
- Strategic Planning
- Incident Response
- Policy and Procedure Development
- Security Awareness and Training
- Vendor and Third-Party Risk Management
- Project Management
- Technical Skills
- Data Analysis
- Legal and Ethical Understanding
- Vendor and Tool Evaluation

Soft Skills

- Communication skills
- Collaboration
- Attention to detail
- Critical thinking
- Adaptability
- Collaboration and Team Building
- Crisis Management

Cybersecurity Engineer

Job Description

- To design and implement security measures to protect computer networks and systems from cyber attacks.
- To conduct vulnerability assessments and penetration testing to identify potential security issues.
- To develop and implement security policies, procedures, and standards to ensure compliance with regulations and industry best practices.
- To monitor network traffic and system logs for signs of suspicious activity.
- To respond to security incidents and conduct forensic investigations to determine the cause and scope of the breach.
- To collaborate with other IT professionals to identify and implement security solutions that meet the needs of the organization.
- To stay up-to-date with the latest trends and technologies
- To create solutions for pre-existing security issues
- To configure and install firewalls and intrusion detection systems (IDS)
- To respond to data security issues
- To oversee any changes in facilities, software, hardware, user needs and telecommunications.
- Conducting network maintenance
- To ensure the security configuration of end-user devices.

Common Certification

- Certified Information Systems Security Professional (CISSP)
- Certified Ethical Hacker (CEH)
- CompTIA Security+ Advance
- GIAC Security Essentials (GSEC)
- Offensive Security Certified Professional (OSCP)
- Certified Information Security Manager (CISM)
- A bachelor's degree in a relevant field such as Computer Science, Information Systems, Cybersecurity or other related field. A master's degree is an added advantage.
- Minimum 5 years of experience in cybersecurity field.

Cybersecurity Engineer

Common Used Tools/ Technologies

- Firewalls
- Intrusion Detection/Prevention Systems (IDPS)
- Security Information and Event Management (SIEM) Systems
- Vulnerability Scanners
- End Point Detection EDR
- DDOS
- Network Defence
- 8.Penetration Test
- 9.Encyrption Tool
- 10.SOAR

Essential Skills

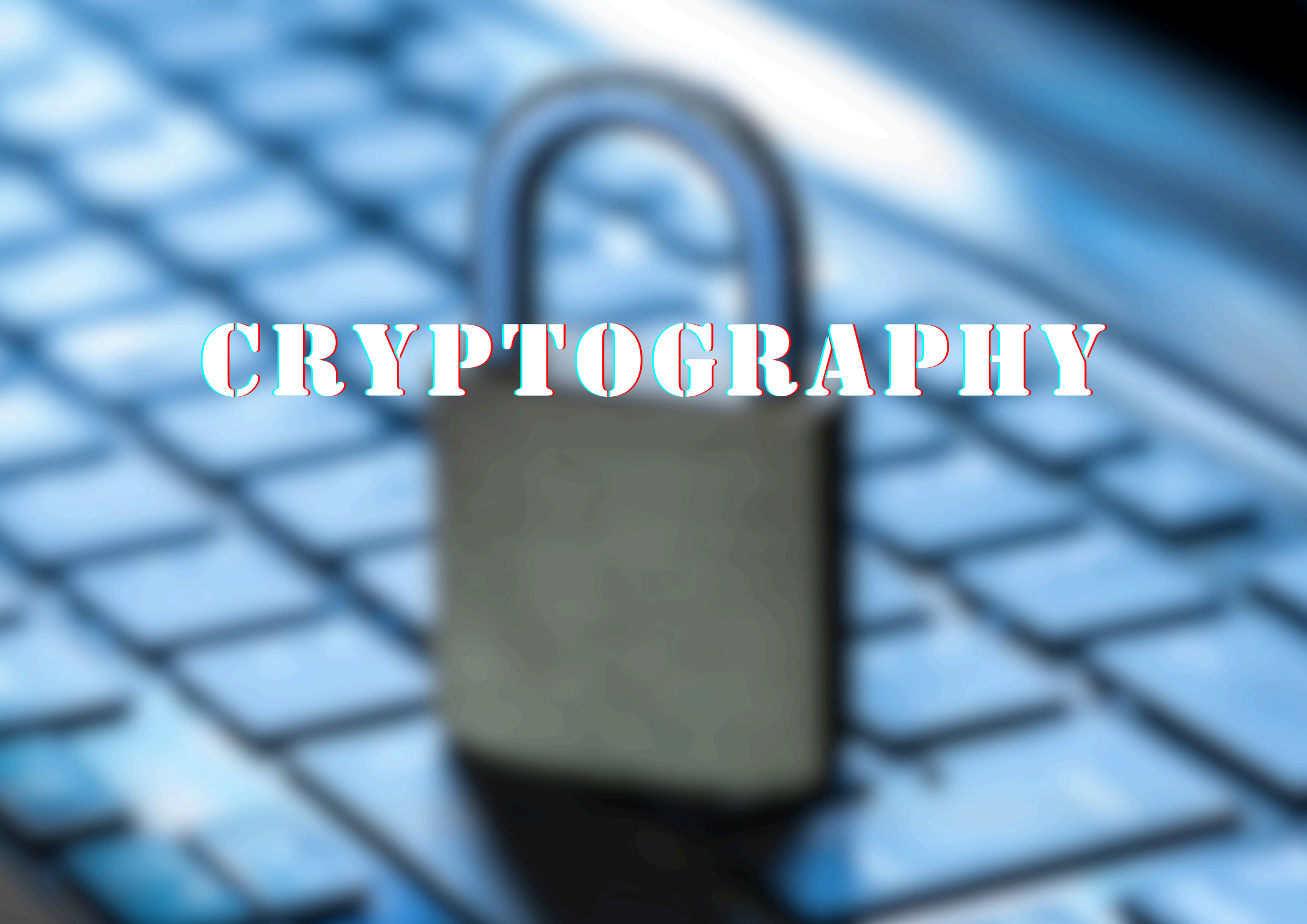
- Analytical skills
- Problem-solving skills
- Communication skills
- Attention to detail
- Continuous learning
- Leadership skills

Competencies

- Technical knowledge on cybersecurity product
- Communication skills
- Collaboration
- experience with incident detection, incident response, and forensics.
- Experience with Firewalls (functionality and maintenance
- Proficiency in Programming Languages
- Ability to work under pressure in a fast-paced environment
- Strong attention to detail with an analytical mind and outstanding problem-solving skills
- Great awareness of cybersecurity trends and hacking techniques

Soft Skills

- Communication
- Problem-solving
- Collaboration
- Adaptability
- Attention to detail
- Ethics


CRYPTOGRAPHY

Cyber Secure Coder/Cryptography Analyst

Job Description

- To analyze and assess the security of cryptographic systems and algorithms including encryption methods, key management, and cryptographic protocols.
- To identify vulnerabilities and weaknesses in cryptographic systems that could potentially be exploited by attackers.
- To stay informed about emerging threats and new cryptographic techniques.
- To develop and implement cryptographic solutions for data protection including encryption and decryption processes for various applications.
- To manage cryptographic keys, including key generation, distribution, rotation, and storage and to ensure their security and integrity.
- To evaluate and implement cryptographic protocols such as SSL/TLS, IPsec, and others to secure network communications.
- To conduct security audits and assessments of cryptographic systems.
- To ensure compliance with security policies and industry standards.
- To participate in incident response efforts.

Common Certification

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified Information Systems Security Professional (CISA)
- Certified Encryption Specialist (CES)
- Certified Cryptography Expert (CCE)
- Certified Cryptographic Architect (CCA)
- Certified Secure Software Lifecycle Professional (CSSLP)
- GIAC Certified Encryption Specialist (GCES)
- CompTIA Security+
- EC-Council Certified Encryption Specialist (ECES)
- Certified Cryptography Engineer (CCE)
- Bachelor's degree in mathematics, Computer Science, Information Technology, or a related field. A master's degree's degree is an added advantage.

Cyber Secure Coder/Cryptography Analyst

Essential Skills

- Cryptographic Algorithms
- Encryption and Decryption
- Key Management
- Public Key Infrastructure (PKI)
- Hash Functions
- Digital Signatures
- Secure Protocols (TLS, SSL)
- Cryptanalysis Techniques
- Cryptographic Libraries (e.g., OpenSSL)
- Secure Socket Layer (SSL) Analysis
- Blockchain and Distributed Ledger Technologies

Soft Skills

- Analytical thinking
- Attention to detail
- Problem-solving
- Communication
- Adaptability
- Collaboration
- Critical thinking
- Time management
- Integrity and ethics
- Continuous learning

Common Used Tools/ Technologies

- Cryptography tools
- Project Management and Collaboration Tools

Competencies

- Strong understanding of cryptographic algorithms and protocols.
- Analytical and problem-solving skills.
- Mathematical and statistical proficiency.
- Cryptographic implementation and vulnerability assessment.
- Familiarity with security standards and compliance.
- Programming and scripting knowledge.
- Risk assessment and mitigation.
- Communication and documentation skills.
- Security research and continuous learning.

Cyber Secure Coder/Cryptography Specialist

Job Description

- To creating, implementing, and maintaining cryptographic protocols and systems that protect sensitive information from unauthorized access and manipulation.
- To design and implement cryptographic algorithms and protocols for secure communication and data protection.
- To develop secure coding practices can protect organization against various types of vulnerabilities.
- To identify and minimize software and security vulnerabilities, handle exploits and attacks as they occur, and develop secure code and programming practices that can help prevent exploitation in an application.
- Identifying security risks
- Eliminating vulnerabilities
- Designing secure software architecture
- Implementing security measures
- Testing for and correcting security defects
- Maintaining the security of deployed software
- To introduce secure coding methodologies before the software or application is transferred into a production environment.
- To conduct research to stay up to date with current cryptographic practices.

Common Certification

- Certified Cryptography Expert (CCE)
- Certified Information Systems Security Professional (CISSP)
- Certified Ethical Hacker (CEH)
- CompTIA Security+
- SC2 CSSLP
- Certified Ethical Hacker (CEH)

Cyber Secure Coder/Cryptography Specialist

Essential Skills

- Cryptographic Algorithms
- Encryption and Decryption
- Key Management
- Public Key Infrastructure (PKI)
- Hash Functions
- Digital Signatures
- Secure Protocols (TLS, SSL)
- Cryptanalysis Techniques
- Cryptographic Libraries (e.g., OpenSSL)
- Secure Socket Layer (SSL) Analysis
- Blockchain and Distributed Ledger Technologies

Soft Skills

- Analytical thinking
- Attention to detail
- Problem-solving
- Communication
- Adaptability
- Collaboration
- Critical thinking
- Time management
- Integrity and ethics
- Continuous learning

Common Used Tools/ Technologies

- Cryptography tools
- Project Management and Collaboration Tools

Competencies

- Strong understanding of cryptographic algorithms and protocols.
- Analytical and problem-solving skills.
- Mathematical and statistical proficiency.
- Cryptographic implementation and vulnerability assessment.
- Familiarity with security standards and compliance.
- Programming and scripting knowledge.
- Risk assessment and mitigation.
- Communication and documentation skills.
- Security research and continuous learning.

Cryptography Developer Expert

Job Description

- To design and develop cryptographic algorithms and protocols to secure data and communications.
- To analyze and evaluate existing cryptographic systems and identify vulnerabilities.
- Develop and implement security solutions to protect against attacks and unauthorized access.
- To collaborate with other security professionals, software developers, and system administrators to ensure the security of systems and applications.
- To conduct research and stay up-to-date with the latest developments
- To decrypt and dissect ciphers and algorithms used to encrypt data.
- To create security systems to guard against unauthorized access and protect data.
- To develop protections to ensure critical information can't be edited, copied, or deleted.
- To analyze mathematical or statistical codes to solve security issues
- To test data security systems to identify vulnerabilities.
- To learn advanced coding strategies and new encryption programming techniques
- To provide technical support for hardware and software engineers
- To design cryptographic solutions for data protection, ensuring they align with industry standards and organizational security requirements.

Common Certification

- Certified Information Systems Security Professional (CISSP)
- Certified Ethical Hacker (CEH)
- Certified Cryptography Expert (CCE)
- Certified Secure Software Lifecycle Professional (CSSLP)
- GIAC Certified Encryption Specialist (GCES)
- CompTIA Security+
- Certificate of Cloud Security Knowledge (CCSK)
- Certified Network Defense Architect (CNDA)
- Certified Encryption Specialist (ECES)
- Certified Cryptography Engineer (CCE)
- Bachelor's degree in mathematics, Computer Science, Information Technology, or a related field. A master's degree's degree is an added advantage.

Cryptography Developer Expert

Essential Skills

- Strong knowledge of cryptography algorithms, protocols, and standards.
- Proficiency in programming languages
- Information Security and Cybersecurity Domain

Common Used Tools/ Technologies

- • Cryptography libraries and APIs
- • Cryptographic protocols
- • Hashing algorithms
- • Symmetric encryption algorithms
- • Asymmetric encryption algorithms
- • Digital signature algorithms
- • Key management and distribution systems
- • Secure communication protocols
- • Cryptanalysis tools
- • Programming languages

Soft Skills

- Analytical thinking
- Attention to detail
- Communication skills
- Collaboration
- Adaptability
- Problem-solving
- Ethical behaviour

Competencies

- Strong understanding of cryptographic algorithms and protocols, including symmetric and asymmetric key cryptography, hashing, digital signatures, and key exchange protocols.
- Experience with programming
- Knowledge of cryptographic libraries and frameworks
- Familiarity with cryptographic hardware
- Understanding of security threats and vulnerabilities related to cryptography and how to mitigate them.
- Ability to design and implement secure cryptographic solutions for various applications, such as secure communication, data storage, and authentication.
- Knowledge of regulatory and compliance requirements related to cryptography,
- Expertise in cryptographic algorithms, protocols, and key management.
- Proficient in secure coding practices and secure software development lifecycle (SDLC).


MANAGEMENT LEVEL

Chief Information Security officer

Job Description

- To create and execute a comprehensive cybersecurity strategy aligned with organizational goals and risk tolerance.
- To identify, assess, and prioritize cybersecurity risks.
- To develop strategies to mitigate or manage risks effectively.
- To ensure organizational compliance with industry regulations and data protection laws. Such as GDPR, HIPAA, or PCI DSS.
- To establish and enforce security policies, standards, and procedures.
- To develop and implement training programs to educate employees about security best practices and create a culture of security awareness.
- To oversee the selection, implementation, and management of security technologies such as firewalls, intrusion detection systems, encryption, and antivirus software.
- To assess and manage security risks associated with third-party vendors and service providers.
- To provide regular updates and reports to the board and executive leadership on the state of cybersecurity within the organization.
- To act as the primary point of contact for external entities.
- To stay current with the latest cyber threats, security technologies, and industry trends.
- To develop and manage the security budget, and reporting on the effectiveness of security controls and the status of security incidents to the board.

Common Certification

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified Chief Information Security Officer (CCISO)
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified Cloud Security Professional (CCSP)
- GIAC Security Leadership (GSLC)

Chief Information Security officer

Competencies

- In-depth knowledge of information security principles, practices, and technologies.
- Understanding of cybersecurity threats, vulnerabilities, and risk management.
- Familiarity with security frameworks and standards (e.g., NIST, ISO 27001, CIS).
- Strong leadership skills to lead the security team and foster a culture of security awareness within the organization.
- Strategic thinking and the ability to align security initiatives with business goals and risk management strategies.
- Effective project and program management skills to oversee security-related projects.
- The ability to identify, assess, and prioritize security risks to the organization.
- Skills in developing and implementing risk mitigation strategies and security policies.
- Knowledge of industry-specific regulations (e.g., GDPR, HIPAA) and the ability to ensure organizational compliance.
- Experience in handling compliance audits and reporting.
- Proficiency in incident response planning and execution.
- Skills in managing security incidents and minimizing their impact.
- Understanding of security architecture design and implementation to safeguard information systems and data.
- Knowledge of network and application security.
- Excellent communication skills to interact with both technical and non-technical stakeholders.
- The ability to convey complex security issues in a clear and understandable manner.
- Skills in assessing and managing security risks associated with third-party vendors and service providers.
- The ability to develop and implement security awareness programs for employees.
- Financial management skills to oversee the security budget and allocate resources effectively.
- Understanding of legal and regulatory aspects of cybersecurity, including privacy laws, data breach notification requirements, and liability.
- Stay up-to-date with the latest cybersecurity threats, trends, and emerging technologies in the industry.
- A commitment to maintaining the highest ethical standards and professional conduct.
- The ability to adapt to evolving threat landscapes and learn continuously to stay current in the field.
- Skills in presenting security matters to the board and executive leadership, translating technical issues into business terms.
- Proficiency in various security technologies and tools, such as firewalls, intrusion detection systems, encryption, and identity and access management solutions.

Chief Information Security officer

Essential Skills

- Technical Expertise
- Risk Management
- Leadership
- Strategic Thinking
- Communication Skills
- Regulatory and Compliance Knowledge
- Incident Response
- Security Awareness and Training
- Security Architecture
- Vendor and Third-Party Risk Management
- Financial Management
- Legal and Regulatory Knowledge
- Ethical and Professional Conduct:
- Business Acumen
- Adaptability and Continuous Learning
- Crisis Management
- Stakeholder Engagement

Common Used Tools/ Technologies

- Security Information and Event Management (SIEM) systems
- Intrusion Detection and Prevention Systems (IDPS)
- Firewall and Network Security Appliances
- Vulnerability Scanning and Assessment tools
- Antivirus and Anti-Malware software
- Encryption tools and technologies
- Access Control and Identity Management solutions
- Incident Response and Forensics tools
- Security Assessment and Penetration Testing tools
- Security Awareness and Training platforms
- Risk Management and GRC (Governance, Risk, and Compliance) software
- Secure File Transfer and Data Loss Prevention (DLP) solutions
- Cloud Security and CASB (Cloud Access Security Broker) tools
- Security Analytics and Threat Intelligence platforms
- Mobile Device Management (MDM) and Endpoint Security tools
- Secure Communication and Collaboration platforms
- Security Policy and Compliance Management software
- Secure Password and Credential Management solutions
- Secure Email Gateways and Email Filtering tools

Chief Information Security officer

Soft Skills

- Leadership
- Communication
- Strategic thinking
- Adaptability
- Collaboration
- Problem-solving
- Decision-making
- Ethics and integrity
- Empathy
- Conflict resolution
- Time management
- Influencing and persuading
- Emotional intelligence
- Stakeholder engagement
- Team building
- Negotiation skills
- Critical thinking
- Stress management
- Creativity