Red Education

CAREERS IN CYBER SECURITY EXPLAINED

WWW.REDEDUCATION.COM

Rededucation © 2026 All rights reserved.

PREFACE

The purpose of this guide is to assist individuals and organisations understand career pathways across the CYBER SECURITY Industry. This should provide insight across roles-based responsibilities including the necessary skills required to support a particular job function within a chosen field of expertise.

This knowledge should assist:

- existing employees within the sector understand advancement paths
- newly entering employees from university studies prior to entering the industry
- someone interested in a career transition from one industry to another and willing to upskill to become a Cyber Security Specialist

For your benefit, we've plotted a roadmap to assist career progression across specific fields of expertise, to plot future career progression.

Rededucation © 2026 All rights reserved.

INFORMATION TECHNOLOGY CAREERS

WHY CYBER SECURITY

The world changed irreversibly in 2020. Due to the global pandemic, society, as we knew it, collapsed almost overnight, and a cloud-driven explosion of new technologies followed. Five years of technological development were compressed into less than a year. Consider the magnitude of the cultural shifts that have occurred during this time period, including changes in health, travel, technology, commerce, hard currency, and social gatherings.

There has never been such a rapid and profound social transformation in human history. The pandemic of COVID-19 is to the twenty-first century as the Industrial Revolution was to the nineteenth. This century, and the early 2020s in particular, will be viewed by future generations as the golden age of a "New Technological Revolution."

Without diminishing the loss of life, one could argue that from a business standpoint we are now stronger. The pandemic has altered the social and economic structure of the world so that it is less dependent on the physical state and more dependent on the virtual plane. As the world continues to implement these innovative technologies in our communities and societies, historians of the future will examine and comment on this phenomenon.

Governments and corporations are exerting resource pressures on the IT Industry to support the explosion of new cloud-based technologies as businesses rush to adopt hybrid or fully virtualized cloud solutions. It is fascinating to observe the rapid change in behaviour that has been facilitated by IT technology and cloud services that support business processes.

As businesses scramble to address the new IT skills gap resulting from the rapid transition from old to new technologies, the need for specialised cybersecurity training has become critical and pressing. The widening skills gap in the ICT industry has provided cybercriminals and their organisations with new opportunities to exploit.

The pandemic precipitated a perfect storm. It compelled the world's economies to invest rapidly in the industry in order to transition from antiquated legacy systems to more advanced systems, to ensure the distribution and continuity of goods and services.

This rapid transition over a short period of time, which necessitates a skilled workforce to manage and administer I.T. networks, has resulted in an explosion of skilled-worker positions. This has led to an underresourced industry on a global scale.

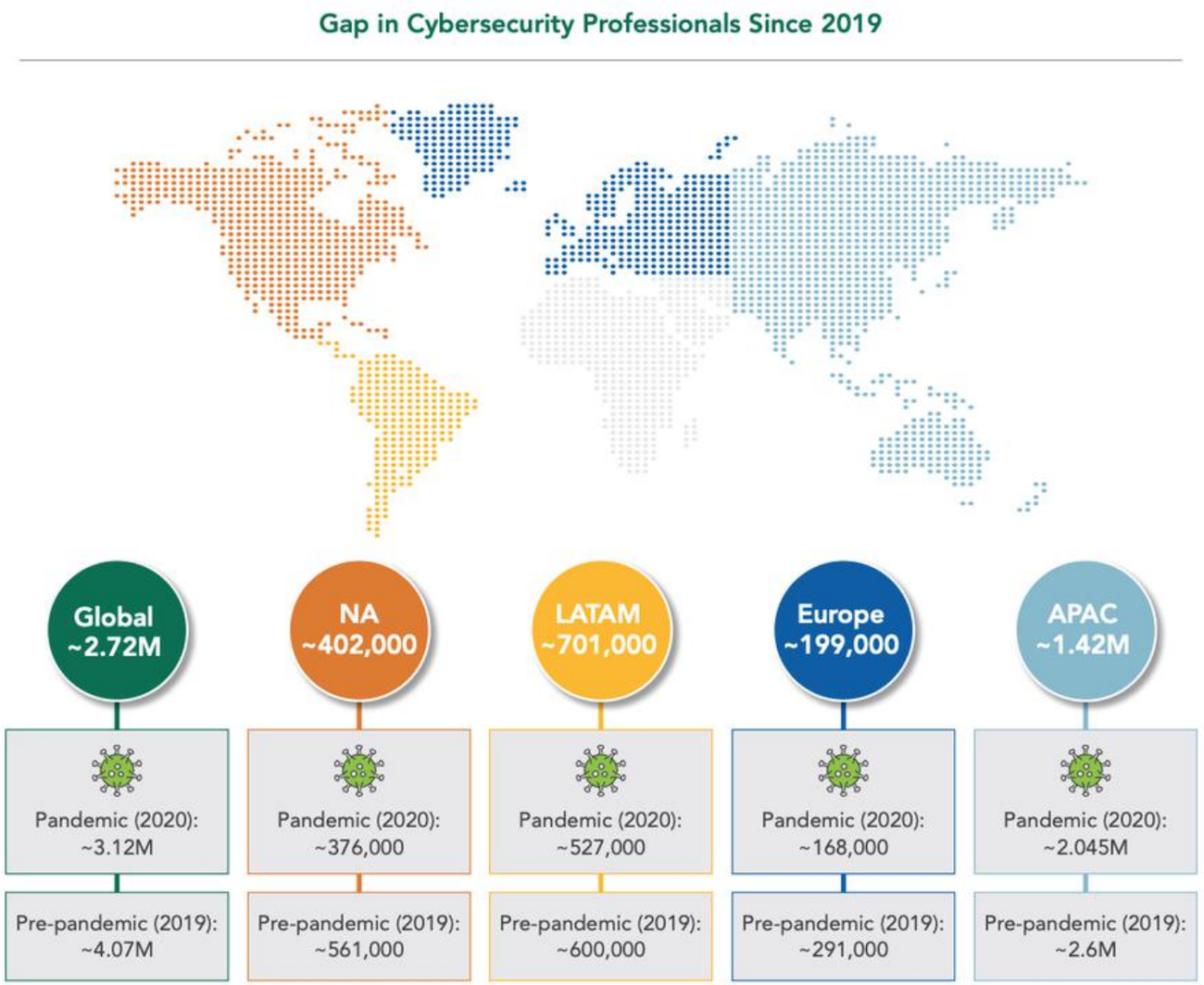
A reliance on insufficient personnel to manage these systems effectively.

Consequently, a lack of skilled workers required to manage systems and an uneducated population has resulted in an increasing number of well-publicised cybersecurity breaches that threaten vital infrastructure services and erode public confidence.

For CIOs in charge of teams of technical specialists, the significant skills gap in the IT industry is one of the most pressing issues. It is a major concern for all businesses, and the risks associated with it are significant.

In international organised crime networks, criminal elements are becoming more intelligent, sophisticated, and integrated. To stay ahead of these intruders, you must have a thorough understanding of the technology that will protect you; however, the effectiveness of these systems depends on the individuals who operate them. A dearth of qualified workers results in an overworked and underresourced industry.

Nonetheless, supply and demand issues have created opportunities. From new graduates to workers transitioning industries, and existing I.T. specialists willing to invest and acquire new skills to assume leadership roles and ultimately higher-paying positions.



https://fintechnews.ph/56130/security/cybersecurity-talent-shortage-puts-apac-organizations-at-risk/

The Information Technology Industry is a vital service desperately in need of qualified personnel. The industry provides excellent compensation, the opportunity to work in any part of the world, the option to work remotely or on-site alongside skilled personnel. With a global shortage of approximately 2.7 million workers, the current labour market offers exceptional opportunities.

Rededucation © 2026 All rights reserved.

THE IMPORTANCE OF CERTIFICATION TRAINING

Rededucation © 2026 All rights reserved

I.T. CERTIFICATION TRAINING

Rapid technological progress generates both opportunities and challenges.

The rapid technological advancement and product development of cybersecurity products provide both positive and negative consequences.

Since the Pandemic, rapid technological change has exceeded the capacity of the global I.T. community to provide and support a skilled labour force. Despite the difficulty of the present age, there are opportunities.

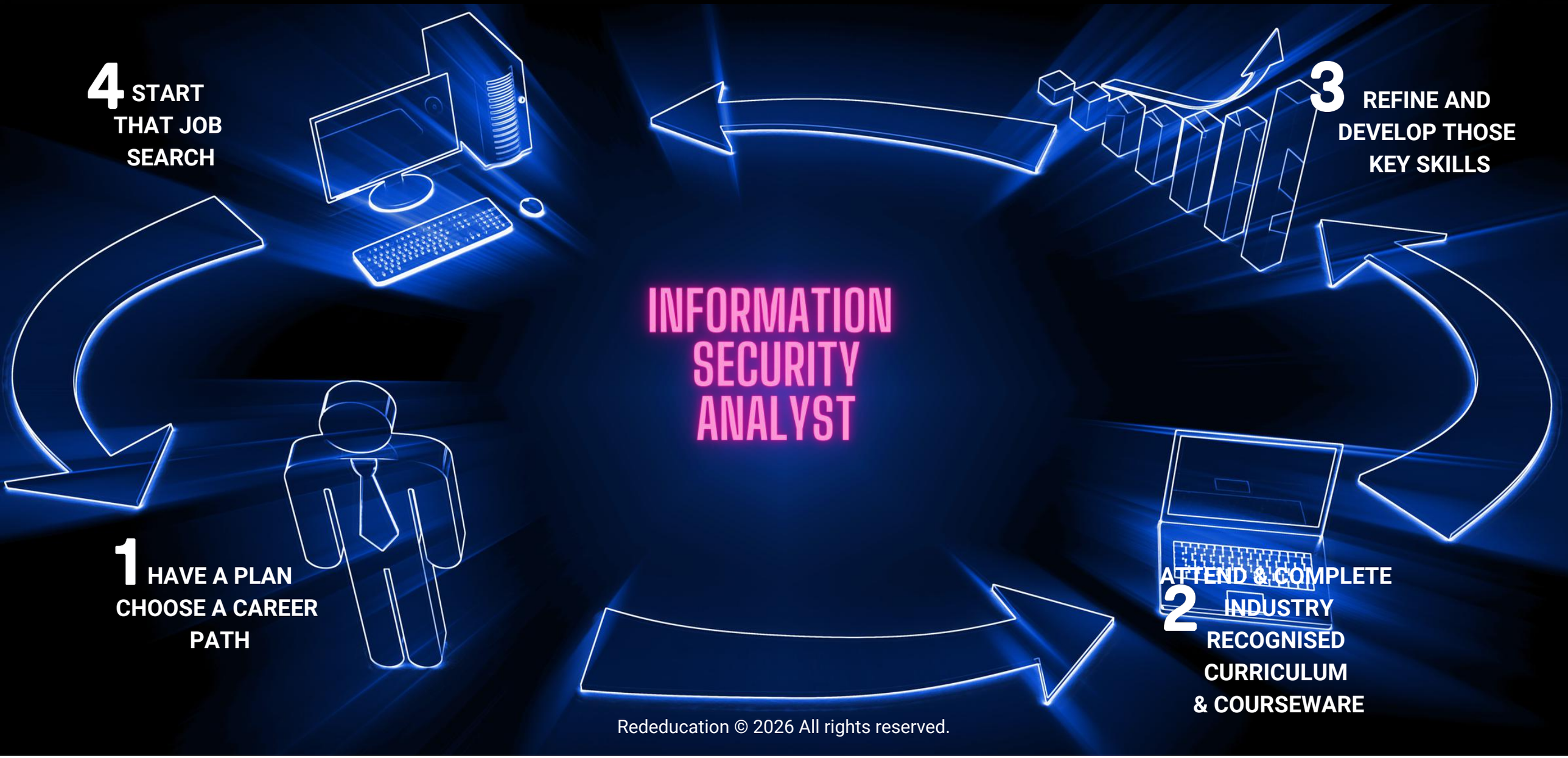
Continuous Certification Training is required in order to equip operators with the skills necessary to provide field support and overall protection of business services and processes. Without ongoing certification and recertification, employees risk becoming obsolete in today's society due to rapid technological change.

Continuous certification training improves the performance, job satisfaction, promotion and career advancement opportunities, and salary expectations of I.T. technicians.

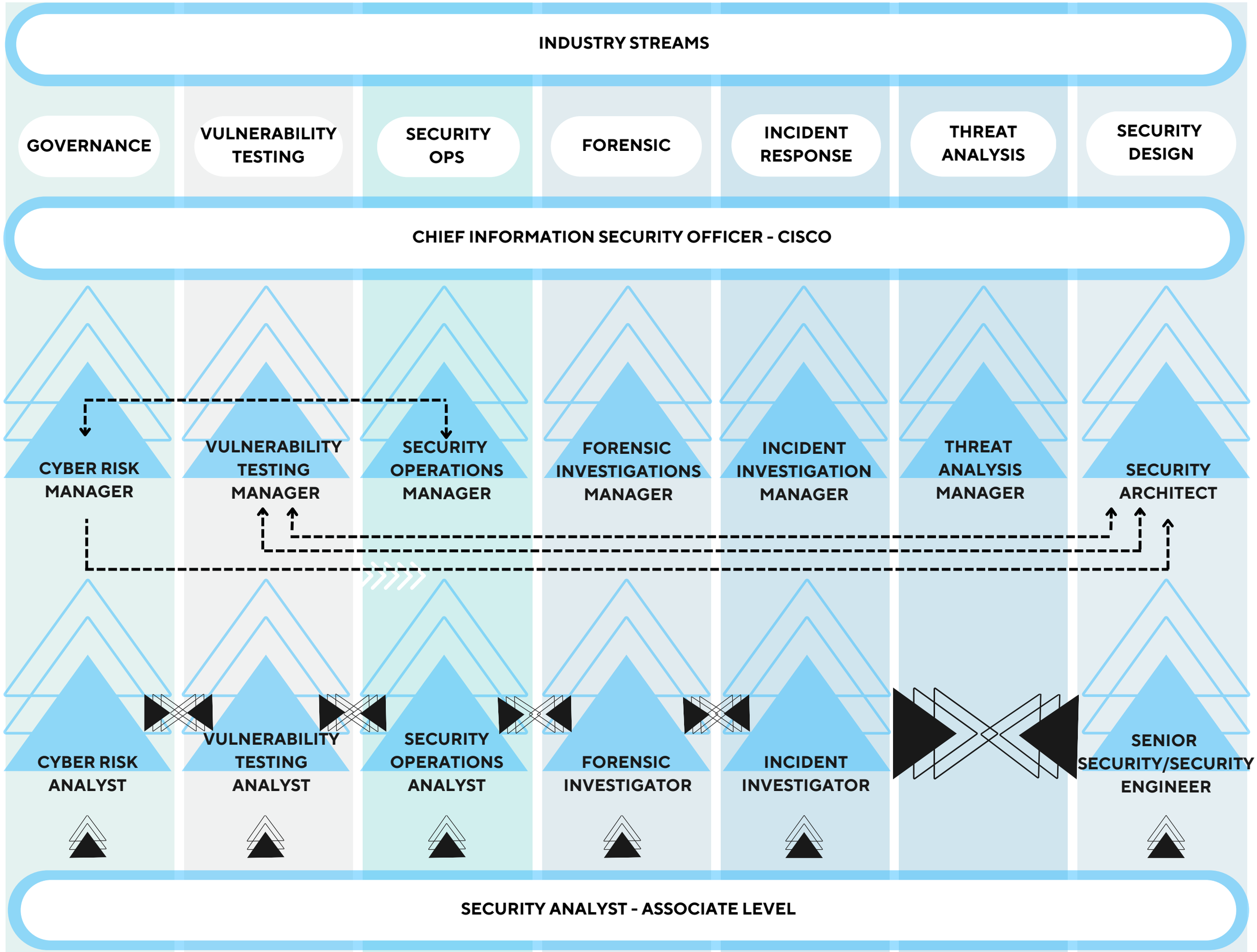
Increasing global demand for skilled labour ensures I.T. professionals are in high demand reducing the risk of redundancy across the span of their careers. This demand will create additional opportunities, and since businesses are desperate for skilled labour, this career choice will offer numerous advantages to qualified candidates entering this industry.

Rededucation © 2026 All rights reserved.

GETTING STARTED



Rededucation © 2026 All rights reserved.


INDUSTRY STREAMS
GOVERNANCE
VULNERABILITY TESTING
SECURITY OPS
FORENSIC
INCIDENT RESPONSE
THREAT ANALYSIS
SECURITY DESIGN
CHIEF INFORMATION SECURITY OFFICER - CISCO
CYBER RISK MANAGER
VULNERABILITY TESTING MANAGER
SECURITY OPERATIONS MANAGER
FORENSIC INVESTIGATIONS MANAGER
INCIDENT INVESTIGATION MANAGER
THREAT ANALYSIS MANAGER
SECURITY ARCHITECT
CYBER RISK ANALYST
VULNERABILITY TESTING ANALYST
SECURITY OPERATIONS ANALYST
FORENSIC INVESTIGATOR
INCIDENT INVESTIGATOR
SENIOR SECURITY/SECURITY ENGINEER
SECURITY ANALYST - ASSOCIATE LEVEL

A New Education for a Changing World

JOB ROLES EXPLAINED

Rededucation © 2026 All rights reserved.

SECURITY ANALYST ASSOCIATE LEVEL

JOB DESCRIPTION

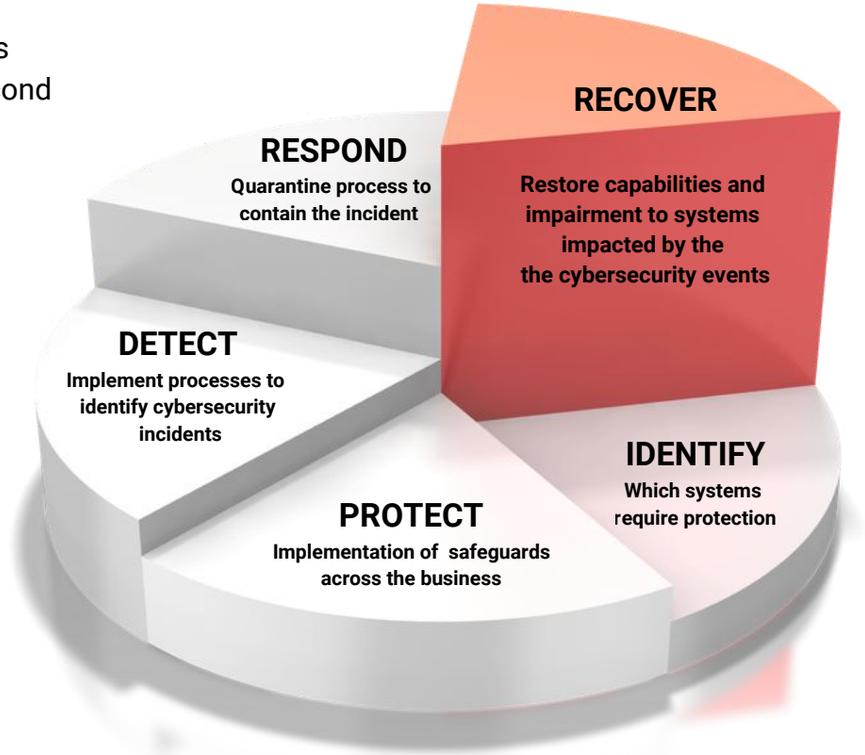
Security Analysts play a crucial role in securing the networks, systems, and data of an organisation. They collaborate with all departments within an organisation to identify, investigate, and report I.T. security system vulnerabilities. They defend an organisation against a variety of cyber security threats.

Behind a wall of hardware and cloud-based solutions designed to identify malicious activity, stand the second line of defence, Security Information Personnel.

Types of Cyber Attacks include a single incident or a series of repeated and strategic attacks.

Examples of these:

- Malware infections.
- Social manipulation attacks
- Attacks on software supply chains
- Advanced persistent threats (APT)
- Distributed denial of service (DDoS)
- Man in the middle (MitM) attacks
- Password attacks



The role of the security analyst is to manage alerts, incidents, and general system and system log maintenance. Due to the nature of their job, they may be required to work at any time of day, night, weekend, or holiday. They must be flexible and committed to the task at hand outside of standard business hours.

Rededucation © 2026 All rights reserved.

As part of their duties, the Security Analyst is constantly vigilant. They can quickly and methodically analyse and resolve security-related issues. They communicate effectively with others and coordinate efficiently within their team to carry out daily security operations. They are also viewed as educators of the general workforce when it comes to applying specific standards when opening attachments and links from unknown sources.

This personnel are trained and conversant with systems including network security monitoring systems, encryption, web vulnerability, penetration testing, antivirus software, network intrusion detection, and packet sniffers.

In order to enter this field, it is essential to have studied cybersecurity fundamentals, such as network architecture and protocol, routing and switching, firewalls, and other key cybersecurity elements. After becoming a Security Analyst, a variety of career paths are available.

Numerous Security Analyst positions call for a bachelor's degree, boot camps, or similar programmes in computer science, programming, or related fields. As the demand for cybersecurity increases in the future, companies are focusing more on hiring individuals with the necessary skills.

TECHNICAL SKILL	PROFICIENCY LEVEL
Business Needs	★★
Incident Management	★★
Forensics	★★
Infrastructure	★★★
Network Maintenance	★★
Problem Solving	★★★
Security Administration	★★
Assessment & Testing	★★
Education Awareness	★★★
Programme Management	★★★
Stakeholder Management	★★
Threat Analysis	★★★
Threat Intelligence	★★

PERSONAL QUALITIES	PROFICIENCY LEVEL
Communication	Basic
Creative Thinking	Basic
Problem Solving	Intermediate
Teamwork	Intermediate
Detect Patterns	Intermediate

Rededucation © 2026 All rights reserved.

KEY JOB FUNCTIONS

TASK DESCRIPTIONS

Monitor

- Observe cyber security measures
- Record security events
- Respond to alarms
- Compile and analyse analysis reports

Maintenance

- System modifications, policies, and practices
- Implement new cyber processes and applications as directed
- Conduct vulnerability and penetration tests as directed
- Align systems to Vendor systems recommendations
- Maintain documentation of system upgrades

Response

- Contribute to the response to security alerts
- Assist in forensic investigation
- Assistance in resolving security incidents
- Contribute to process simulations in order to enhance the process
- Recommend modifications to the cyber security systems and procedures
- Record cyber security events

Compliance

- Contribute to the response to security alerts
- Instruction on best practices for end users
- Assist in forensic investigation
- Assistance in resolving security incidents
- Contribute to process simulations in order to enhance the process
- Recommend modifications to the cyber security systems and procedures
- Record cyber security events

Performance Optimisation

- Prototype new systems and procedures
- Assist in the implementation of software and hardware Assist with system testing and scheduled updates
- Research and recommend the development of new products and processes

Rededucation © 2026 All rights reserved.

CYBER RISK ANALYST

THREATS

AI
CYBERSECURITY
RISKS DATA
POISONING
PROMPT
INJECTION
MODEL THEFT

JOB DESCRIPTION

The Cyber Risk Analyst has an in-depth understanding of cyber analysis tools and analysis techniques to determine RISK in order to mitigate cyber-related attacks.

Cyber Risk Analysts track, monitor, and oversee security policies and standards to ensure their adoption and compliance. They are capable of working independently using scientific and analytical procedures and have strong communication skills.

They design, update, and maintain the digital security systems of private businesses and government agencies.

Principal responsibilities include:

- Installation
- Investigation
- Identify Weaknesses Across Systems and Processes
- Ethical Hacking
- Creation and Implementation of Enterprise-Wide Policies and Procedures, Including Reporting

Rededucation © 2026 All rights reserved.

POINTS OF FAILURE

PEOPLE
PROCESS
PRODUCT

BUSINESS IMPACTS

FINANCIAL LOSS
IDENTITY THEFT
BUSINESS DISRUPTIONS
REPUTATIONAL DAMAGE
LOSS OF CLIENTS
CRITICAL SERVICES DISRUPTION
LEGISLATION
DATA ENCRYPTION
LOST CONTRACTS
LOST PRODUCTIVITY
3RD PARTY LIABILITY
PHYSICAL DAMAGE
DISTRACTIONS

They take pleasure in analysing data and identifying trends that could endanger the company.

The majority of Cyber Risk Analysts hold a bachelor's degree in the field (or a closely related field such as mathematics, computer science, or engineering).

TECHNICAL SKILL	PROFICIENCY LEVEL
Adherence to regulatory guideline	★★★
Business Needs Analysis	★★★
Data Breach Incident Managemer	★★★
Cyber Forensics	★★★
Cyber Risk Management	★★★★
IT Governance	★★★★
Security Administration	★★★
Security Educational Awareness	★★★★
Security Governance	★★★★
Security Programme Managemen	★★★★
Stakeholder Management	★★★
Strategy Implementation	★★★★
Strategic Planning	★★★★

PERSONAL QUALITIES	PROFICIENCY LEVEL
Digital Literacy	Advanced
Computational Logic	Advanced
Problem Solving	Advanced
Transdisciplinary Thinking	Intermediate
Problem Solving	Advanced

Rededucation © 2026 All rights reserved.

KEY JOB FUNCTIONS

TASK DESCRIPTIONS

Monitor

- Monitor risks and incidents involving cyber security systems
- Conduct research on new criminal tendencies and proposed countermeasures
- Evaluate existing systems and controls
- Conduct RISK assessment audits

Maintenance

- Reduce risk using document process techniques and supporting tools
- Creation of RISK assessment reporting documents
- Internal investigation to produce threat analysis reports
- Develop scope documentation

Response

- Analysis of the root cause of a cyber incident
- Recommending corrective actions and future processes to prevent the recurrence
- Implement precautions against known cyber security techniques
- Follow and record all efforts

Compliance SOP's

- Adoption and implementation of new cyber policy and documentation systems
- Examine existing procedures, policies, and documentation for holes
- Contribute to the formulation of updated and new policy doctrine
- Conduct compliance and risk assessments audits

Rededucation © 2026 All rights reserved.

JOB DESCRIPTION

The Security Operations Centre Analyst or SOC performs analyses of real-time data across a myriad of sources, reports and logs. The combination of this data identifies RISK.

Some of the challenges faced by SOC Departments are enough SOC analysts, to begin with, to make sense of the numerous data points to build a comprehensive threat landscape, knowing when and when not, to keep data and finally, the ability to competently manage a toolkit of monitoring tools, which are an aggregator of data, which working together, create actionable insight.

They play a significant role in flagging real-time threats and post-threat evaluation analysis, depending upon the severity of the alert they then trigger an equally weighted response.

SOC is typically found in larger organisations that operate 24/7 days a week. The majority of SOC Analysts have a Computer Science Degree or equivalent background. On call anytime, any day.

Rededucation © 2026 All rights reserved.

SECURITY OPERATIONS CENTRE ANALYST SOC

A SOC Analyst requires:

Knowledge of Security Information and Event Management in Practice (SIEM)

SQL, C, C++, C#, Java, or PHP programming language experience is required.

The Security Operations Analyst is analytical and diligent when performing real-time analyses. They are adept at synthesising trends and observations.

They implement procedures and policies and may be required to be on-call during the majority of their shifts, workdays, and weekends.

They are acquainted with a variety of monitoring tools.
and techniques.

TECHNICAL SKILL	PROFICIENCY LEVEL
Adherence to regulatory guidelines	★★★
Business Continuity	★★★★
Data Breach Management	★★★
Cyber Risk Management	★★★★
DR Disaster Recovery	★★★★
Network Security	★★★
General Administration	★★★
Security Program Management	★★★★
Stakeholder Management	★★★
Threat Analysis and Defence	★★★★
Threat Intelligence and Detection	★★★

PERSONAL QUALITIES	PROFICIENCY LEVEL
Communication	Intermediate
Creative Thinking	Intermediate
Problem Solving	Intermediate
Sense Making	Intermediate
Teamwork	Intermediate

Rededucation © 2026 All rights reserved.

KEY JOB FUNCTIONS

TASK DESCRIPTIONS

Monitor

- Conducts security process evaluations, audits, and tests involving schedules and procedures.
- Performs real-time analysis and trending of software system security log data
- Analysis of data to detect suspicious and criminal behaviour
- Recommendations to the team for further enhancing the monitoring rules and alerts for security
- Observes and reviews
- Processes related to cyber security monitoring should always be documented

Maintenance

- Implement network security measures
- Creates a list of emergency response procedures requiring action
- Maintains input data sources for the logging system
- Plan security audits in accordance with reporting requirements.
- Compilation of status report information for management presentation

Response

- Review incident reports for security
- Assess the nature and gravity of cyber security incidents
- Assists management in establishing procedures for handling cyber security incidents that have been identified
- Provide business with updates throughout the lifecycle of a cyber security incident.
- Creates a final incident report detailing the cyber security incident's occurrence
- Supports business continuity, maintenance, and update plans and procedures

Rededucation © 2026 All rights reserved.

IDENTIFICATION

Digital Devices

PRESERVATION

Preservation of digital data

RECOVERY

Retrieval of "digital echo" from deleted devices

ANALYSIS

Observation, trends analysis of data

FINDINGS

Reporting and summary of investigation drawn from evidence

JOB DESCRIPTION

Digital forensics is the science of recovering, analysing and preserving digital data. This can come from either existing or deleted data that has been linked to cybercrime. Any device capable of storing digital data can serve as a data source.

The Forensics Investigator is accountable for the investigation processes following a cyber threat or cyber incident.

They understand various types of cyber threats, standards, processes and frameworks. They have sufficient knowledge of hardware products and systems to extract and analyse data from a variety of sources.

These may come from hard drives, laptops, USB drives, mobile phones, tablets, file servers, backup tapes, Gmail, Office 365, and other digital sources and footprints.

Forensic investigators have a solid background in analytics, which enables them to unearth the smoking gun that sheds light on a case. Then, they can develop processes and strategies to prevent future security incidents.

Rededucation © 2026 All rights reserved.

These individuals may have a previous background in law enforcement, government agencies, and the private security industry.

Computer forensic investigators assist in the recovery of data from computers and other digital storage devices. The retrieved data can then be utilised in criminal investigations or as evidence in cybercrime cases.

Evidence may involve determining the specifics of computer system intrusions, recovering data from encrypted or deleted files, or recovering deleted emails and passwords.

Upon completion of the investigation, it is their duty to present their findings to the executive team or the judicial system, outlining causality, business impacts, outcomes, and recommended mitigation plans to prevent future attacks.

A Bachelor's degree in Computer Science or a related field is advantageous, and investigators must receive ongoing training in rapidly evolving technologies, systems, and products.

Attending trade shows and seminars, as well as engaging in self-directed learning, keeps their skills current and relevant as technology extraction methods change.

TECHNICAL SKILL	PROFICIENCY LEVEL
Cyber Forensics	★★★
Cyber Risk Management	★★★★
Emerging Technologies	★★★
Failure Analysis	★★★
Network Security	★★★
Security Administration	★★★
Security Assessment and Testing	★★★
Stakeholder Management	★★★
Threat Analysis and Defence	★★★
Threat Intelligence and Detection	★★★

PERSONAL QUALITIES	PROFICIENCY LEVEL
Communication	Intermediate
Creative Thinking	Intermediate
Problem Solving	Intermediate
Sense Making	Intermediate
Teamwork	Intermediate

Rededucation © 2026 All rights reserved.

KEY JOB FUNCTIONS

TASK DESCRIPTIONS

Actions

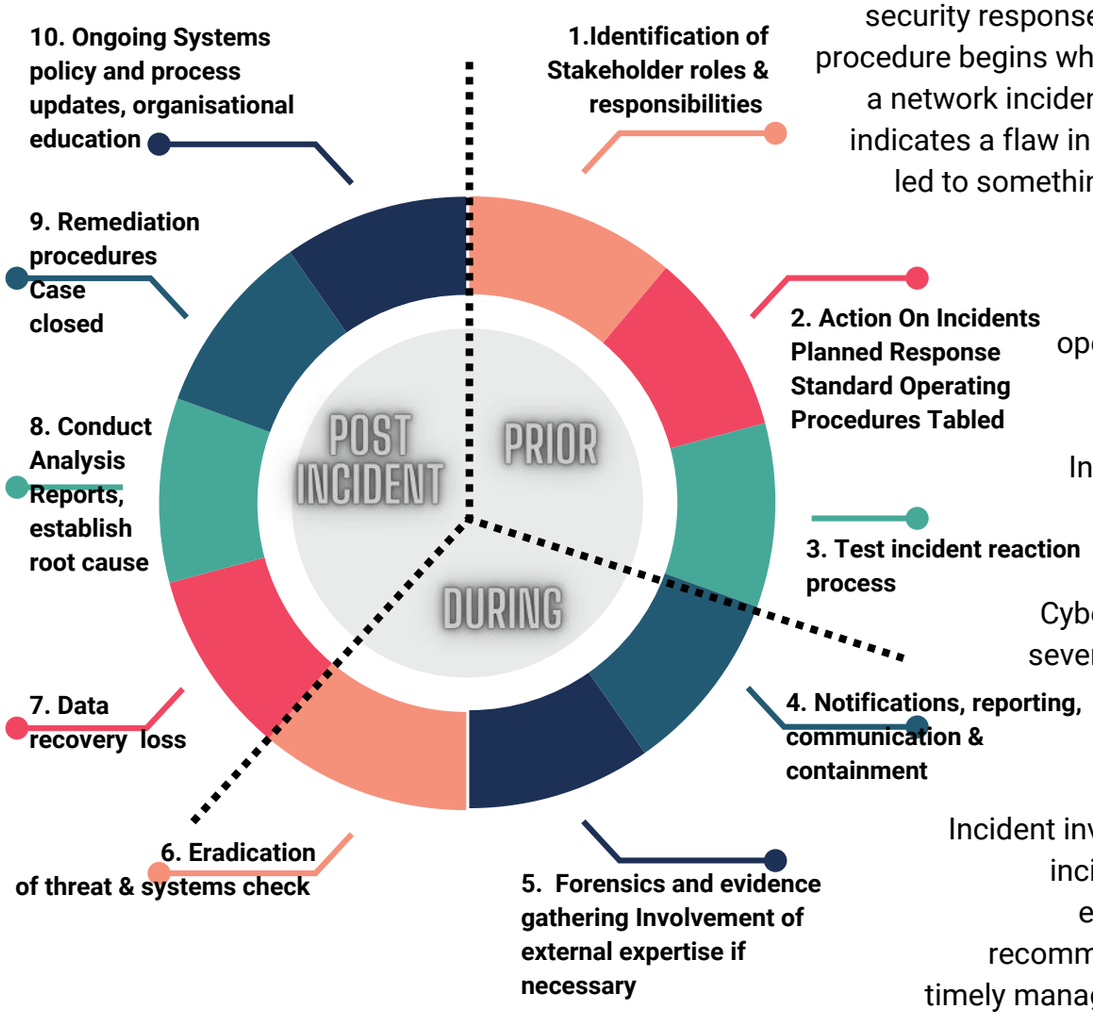
- Getting together with supervisors and managers
- Evidence collection
- Investigation and information collection from affected parties
- Analyze IT systems
- Information retrieval from storage and other electronic devices
- Gather and decrypt threat information from compromised IT systems
- Cross-analyse threat data in order to classify the threat

Response

- Repairing broken digital systems
- Conduct forensic analysis and investigations to determine the cause of the cyber-attack and to document its effects
- Extrapolate key insights and consequences from security incident analyses
- Limit the repercussions of security incidents
- Prepare reports detailing incident findings, analyses, and conclusions
- Based on the investigation findings, update the threat database
- Examining software for design defects
- Provide insights and recommendations to impacted parties regarding post-investigation findings and future cyberattack mitigation strategies

Rededucation © 2026 All rights reserved.

JOB DESCRIPTION



Investigation of incidents is only one component of the security response and management process. The overall procedure begins when the cyber security team is notified of a network incident. The occurrence of a security incident indicates a flaw in process or protection systems that has led to something negatively affecting the organisation.

It is frequently associated with a breakdown in technology, standard operating procedure, or employee conduct that contributes to the occurrence or exacerbates its severity. The Incident Investigator conducts a complex analysis to determine the root cause of the incident.

Cybersecurity incidents include the type and severity, loss of confidential information, and blocking of system access within the organisation.

Incident investigators produce reports that include incident timelines supported by evidentiary evidence, as well as their conclusion and recommendations. They are responsible for the timely management of cyber incidents, including the escalation and resolution of the situation

Rededucation © 2026 All rights reserved.

INCIDENT INVESTIGATOR

The process of documenting incidents is time-consuming, stressful, and, depending on the severity of the attack, extremely complex. If organisations are able to prepare in advance for the possibility of an attack, the administrative burden can be reduced while response plans are expedited.

It provides employees with recommendations for actions based on the likelihood of an incident occurring. Providing guidance and templates with this facilitates the emergency response plan and promotes a more uniform approach across the organisation or government agency.

Incident Investigators are required to be on call 24 hours a day, seven days a week, including nights, weekends, and holidays.

They are conversant with cyber security standards, protocols, and frameworks, as well as the application of various cyber security tools and techniques for incident resolution.

The Incident Investigator is extremely attentive to detail and utilises a critical and methodical approach to conducting investigations and analyses. They examine issues from a variety of business perspectives and actively disseminate their thoughts throughout the organisation.

TECHNICAL SKILL	PROFICIENCY LEVEL
Cyber Forensics	★★★
Cyber & Data Breach Management	★★★
Cyber RISK Management	★★★★
Security Assessment and Testing	★★★
Stakeholder Management	★★★
Threat Analysis & Defence	★★★
Threat Intelligence & Detection	★★★

PERSONAL QUALITIES	PROFICIENCY LEVEL
Communication	Intermediate
Creative Thinking	Intermediate
Problem Solving	Intermediate
Sense Making	Intermediate
Teamwork	Intermediate

Rededucation © 2026 All rights reserved.

KEY JOB FUNCTIONS

TASK DESCRIPTIONS

Compliance

- Identify roles and responsibilities and stakeholder guidelines
- Develop a strategy for combating cyber threats in order to reduce the risk of information system leakage and intrusion
- Create procedures and policies in response to cyber attacks
- Implement processes and guidelines to follow incident response protocols, including analysis techniques, and the creation of incident report templates
- Implement strategies to reduce cyber incident identification and action response times

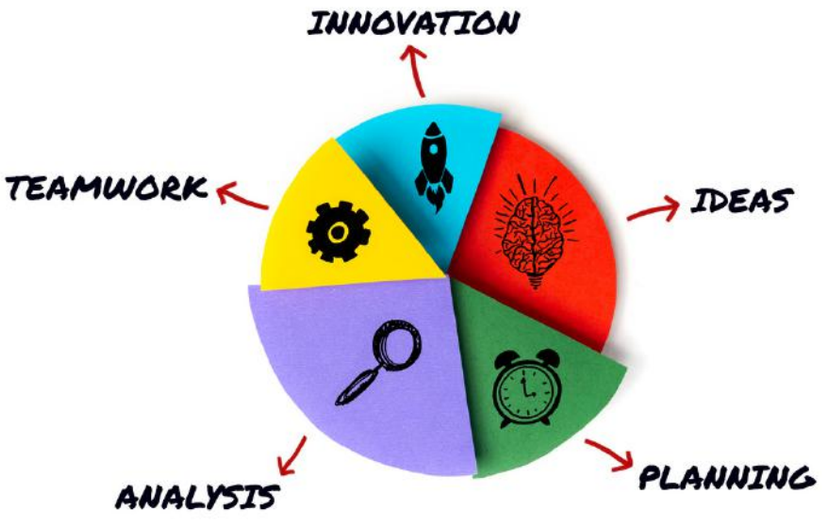
Response

- Handle responses to cyber security incidents immediately
- Following established processes and policies contain the threat and lead the recovery process of cyber security incidents
- Utilise appropriate cyber incident management techniques to resolve challenges

Performance Optimisation

- Collect, analyse, and store information on cyber threat intelligence
- Analyze system vulnerabilities that may pose cyber security risks
- Continuous system enhancements to future-proof the business and build IT system resilience for the present and future
- Propose mitigation techniques and countermeasures to ensure minimal cyber threats
- Analyze past cyber-attacks in order to gain organisational insights and formulate appropriate responses

Rededucation © 2026 All rights reserved.



JOB DESCRIPTION

In order to become a Senior Security Engineer, a bachelor's degree in cybersecurity, computer science, or a related field may be required. Employers may also require a master's degree in a related field and ten or more years of proven work experience for senior-level positions.

This level of employment requires a high level of expertise and specialised knowledge, skills, and experience. These employees frequently exercise discretion in the performance of their daily duties.

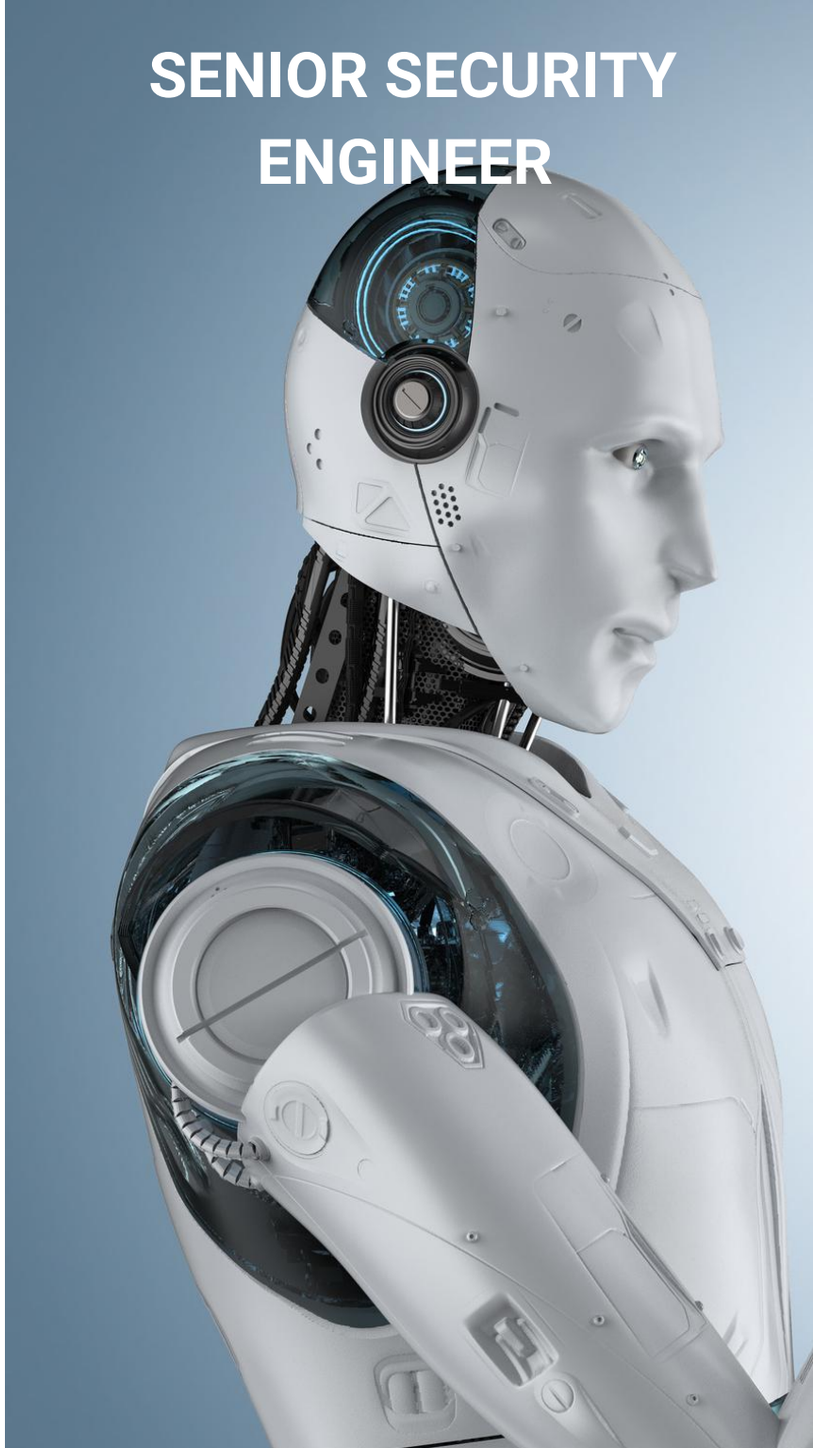
Their duties are frequently complex and require minimal direction when assigned projects or workloads.

They possess a significantly higher level of knowledge than their entry-level peers and exhibit discretion when identifying technical and complex issues.

The person, designs, implements, maintains and operates security controls and countermeasures for information systems. In the acquisition, development, and change management lifecycles of information systems, they evaluate and recommend security controls and procedures, and monitor compliance.

Rededucation © 2026 All rights reserved.

SENIOR SECURITY ENGINEER



They carry out routine tasks associated with periodic reviews and audits of infrastructure security systems and maintain documentation of security standards and procedures. They have a comprehensive understanding of cyber security standards, protocols, and frameworks.

The approach of the Senior Security Engineer/Security Engineer to designing and implementing secure system architectures is organised and methodical. They effectively communicate with their team and other stakeholders.

They analyse trends and the ever-changing threat environment. They provide guidance to senior management and develop and implement compliance strategies for RISK mitigation.

They coordinate and manage third-party RISK and compliance assessments to examine their company for identified I.T. Strategy gaps.

TECHNICAL SKILL	PROFICIENCY LEVEL
Business Needs Analysis	★★★
Incident Management	★★★
RISK Management	★★★★
Emerging Technology	★★★
Infrastructure Design	★★★
Network Security	★★★★
Security Administration	★★★
Security Architecture	★★★
Governance	★★★★
Programme Management	★★★
Strategy Implementation	★★★★
Strategic Planning	★★★★

PERSONAL QUALITIES	PROFICIENCY LEVEL
Communication	Basic
Computational Thinking	Basic
Problem Solving	Intermediate
Teamwork	Intermediate
Sense Making	Intermediate

Rededucation © 2026 All rights reserved.

KEY JOB FUNCTIONS

Monitor

Maintenance

Response

TASK DESCRIPTIONS

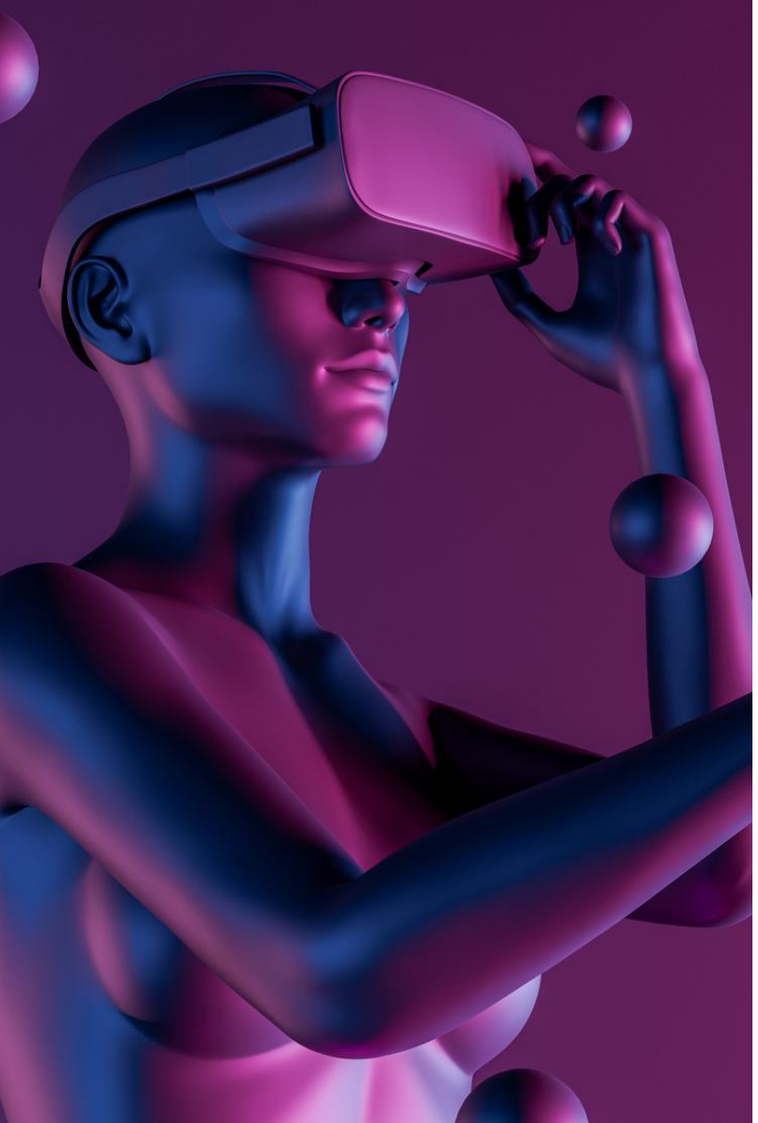
- Manage the upkeep of security platforms, systems, and software
- Develop and conduct individualised disaster recovery exercises
- Simulation tests of existing system Architectures
- Contribute to the resolution of issues and incidents

- Develop security systems in accordance with security standards
- Assist with the evaluation and testing of new security technologies and controls
- They suggest security products, services, and procedures to strengthen system architecture designs
- They record the design, operation, use, and anticipated outcomes of new systems

- Implement new architecture, technologies, and enhancements for enterprise security
- Identify scaling and automation techniques for security infrastructure and processes
- Resolve problems encountered during the implementation of new security systems
- Responds to incidents involving information system security, including the investigation, countermeasures, and recovery from computer-based attacks, unauthorised access, and policy violations
- Interacts and coordinates with third-party incident responders, including law enforcement
- Assess the strengths and weaknesses of security systems and suggest modifications to address the weaknesses

Rededucation © 2026 All rights reserved.

CYBER RISK MANAGER



JOB DESCRIPTION

The Cyber Risk Manager aids in the formulation, upkeep, and evaluation of an organization's security policies and procedures. They collaborate closely with engineering and operations teams to ensure that security requirements are met by system controls. Additionally, they manage and follow up on the results of system security audits.

A properly implemented RISK Assessment process and strategy can proactively identify and mitigate potential threats. A good manager and a thorough analysis of an organization's weak points will reduce security incidents and improve the business's compliance footprint and reduce the threat landscape, potentially preventing the company from incurring costly fines in the event of security breaches.

When attracting new customers, a robust compliance regime can enhance the organization's reputation and instil business confidence that privacy concerns will be handled in a secure manner.

They manage employees and are responsible for the team's performance and outcomes. They educate and advise stakeholders on security measures and protocols.

They understand cyber security standards, protocols, and frameworks, as well as compliance with local Cyber Security Acts. They are proficient in employing a variety of cyber security processes, tools and techniques, depending on the needs and requirements of the organisation.

Rededucation © 2026 All rights reserved.

A Cyber Risk Manager must conduct ongoing research and keep abreast of emerging technologies to combat future sources of RISK.

This individual is an effective communicator who understands how to explain concepts based on the audience's level of comprehension.

Cyber Risk Managers have a solid understanding of emotional intelligence concepts.

A leader in cybersecurity must have strong relationship-building skills to be effective.

The perception of a person's strength as a leader is dependent on knowledge, empathy, and, of course, professional ethics.

They foster a cooperative environment and positive relationships within and beyond their team.

The Cyber Risk Manager has a keen, analytical mind and can anticipate problems and risks in order to mitigate them in advance.

TECHNICAL SKILL	PROFICIENCY LEVEL
Audit and Compliance	★★★★★
Budgeting	★★★★★
Business Needs Analysis	★★★★★
Business Performance Management	★★★★★
CYBER Breach Management	★★★★★
Cyber Forensics	★★★★★
Cyber Risk Management	★★★★★
IT Governance	★★★★★
Learning & Development	★★★★★
Manpower Planning	★★★★★
Networking	★★★★★
People & Performance Management	★★★★★
Strategic Administration & Architecture	★★★★★
Education, Awareness, Governance	★★★★★
Security Programme Management	★★★★★
Security Strategy	★★★★★
Stakeholder Management	★★★★★
Strategy Implementation	★★★★★
Strategy Implementation	★★★★★

PERSONAL QUALITIES	PROFICIENCY LEVEL
Communication	Basic
Computational Thinking	Basic
Problem Solving	Intermediate
Teamwork	Intermediate
Sense Making	Intermediate

KEY JOB FUNCTIONS

TASK DESCRIPTIONS

Monitor

- Manage the strategic growth and enhancement of risk frameworks, methodologies, and requirements
- Recommend strategies to address key cyber security risk areas
- Contrast business requirements with cyber security concerns and legal and/or regulatory mandates
- Anticipate internal and external business obstacles as well as legal or regulatory issues
- Provide strategic risk guidance to stakeholders for the organization-wide implementation and execution of cyber risk strategies

Maintenance

- Establish governance procedures for documenting and revising the security policy, standards, guidelines, and procedures
- Plan the deployment of information systems and cyber security policies
- Develop the enterprise's Cyber Risk Maturity model
- Develop policies and frameworks for cyber security risk assessments and compliance audits

Response

- Advise on the formulation of methods and procedures for conducting cyber risk assessments
- Develop plans for enterprise-wide cyber risk assessment activities
- Coordination of the organization-wide ongoing cyber risk assessment activities
- Following the discovery of vulnerabilities in operating systems, provide strategic and technical recommendations
- Incorporate new security and risk management issues, trends, and alerts into the risk assessment framework
- Develop cyber risk mitigation strategies and organisational policies

Rededucation © 2026 All rights reserved.

KEY JOB FUNCTIONS CONTINUED

TASK DESCRIPTIONS CONTINUED

Compliance SOP's

- Establish governance procedures for documenting and revising the security policy, standards, guidelines, and procedures
- Plan the deployment of information systems and cyber security policies
- Develop the enterprise's Cyber Risk Maturity model
- Develop policies and frameworks for cyber security risk assessments and compliance audits
- Manage the documentation of methodologies and tools used to mitigate cyber risks
- Establish reporting guidelines for the results of cyber risk assessments
- Monitor the creation of internal threat awareness reports
- Provide technical and non-technical staff with threat awareness reports

RISK Mitigation

- Develop programmes and initiatives to bolster the organization's capacity to mitigate risks
- Supervise the planning and execution of cyber security exercises for the organisation
- Assume the role of subject matter expert for a cyber security incident and breach investigations and post-breach remediation efforts
- Propose measures for preventing future incidents and enhancing cyber security
- Maintain the cyber security operations training plans for all security personnel
- Manage responses to inquiries, inspections, and audits from regulatory agencies.

Staff Management

- Analyze operational strategies, policies, and objectives across teams and initiatives
- Develop resource planning and utilisation strategies
- Examine the utilisation of assets
- Manage the creation of learning roadmaps for teams and functions
- Establish performance indicators to compare the efficacy of learning and development programmes to best practices
- Implement initiatives for key management position succession planning
- Develop certification training and educational programmes for system administration

VULNERABILITY & PENETRATION ASSESSMENT MANAGER

JOB DESCRIPTION

Infrastructure components, systems, and applications are tested and certified to determine compliance with standards for confidentiality, authenticity, access levels, and assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity. The Vulnerability & Penetration Assessment Manager plans and directs this procedure. The objective of a vulnerability management programme is to establish controls and techniques that will allow you to identify vulnerabilities in the company's information system components and technical infrastructure.

THE EVOLUTIONARY PROCESS REDUCING THE ATTACK SURFACE

Management of vulnerabilities is a prudent practice for safeguarding sensitive corporate data. Implementing a comprehensive vulnerability management strategy lays the groundwork for a complete programme that can assist you in enhancing your business's cybersecurity.

Vulnerability management is the continuous process of identifying, evaluating, repairing, and disclosing cybersecurity vulnerabilities in systems and the software that runs on such systems. After the vulnerability management method verifies that the fix was effective, the phase of discovery is resumed.

Products for scanning for vulnerabilities are widely available. While making recommendations and reporting on the test's activities and results, they strike a balance between stakeholder expectations. They ensure adherence to testing and evaluation protocols, methods, and instruments.

In addition to promoting knowledge management, they strengthen the testing competency of the organisation. They have extensive knowledge of a variety of testing tools and services, as well as cyber security guidelines, standards, and frameworks.

Due to their exceptional analytical and critical thinking, the Vulnerability Assessment and Penetration Testing Managers are capable of resolving and advising on highly complex issues.

They are also adept at presenting their findings to the appropriate parties. They have considerable experience managing resources.

Among the necessary skills are the following:

- Knowledge of network and application security
- Threat analysis programming languages, particularly scripting languages (Python, BASH, Java, Ruby, Perl) environments for Windows, macOS, and Linux
- A thorough understanding of the instruments used to assess security.
- The performance of platforms used to manage security risks
- Excellent technical writing and documentation abilities, including Cryptography

TECHNICAL SKILL	PROFICIENCY LEVEL
Audit and Compliance	★★★★
Budgeting	★★★★★
Business Performance Management	★★★★★
Cyber Risk Management	★★★★★
Emerging Technology Synthesis	★★★★★
Learning and Development	★★★★★
Manpower Planning	★★★★★
Network & Network Security	★★★★★
People and Performance	★★★★★
Security Assessment & Testing	★★★★★
Security Education & Awareness	★★★★★
Security Governance & Strategy	★★★★★
Strategy Implementation	★★★★
Stakeholder Communication	★★★★
Strategic Planning	★★★★★
Testing	★★★★★
Threat Analysis and Defence	★★★★★

PERSONAL QUALITIES	PROFICIENCY LEVEL
Computational Thinking	Advanced
Digital Literacy	Advanced
Global Mindset	Advanced
Sense Making	Advanced
Sense Making	Advanced

KEY JOB FUNCTIONS

Monitor

Maintenance

RISK Mitigation

Staff Management

TASK DESCRIPTIONS

- Establish test metrics to compare against requirements and best practices in the industry.
- Monitor the execution of certification examinations, audits, and inspections
- Provide guidance on the analysis of complex security test data to support security vulnerability assessment processes, including root cause analysis.
- Serve as an escalation point for security testing-related issues, dependencies, and risks
- Direct team members to continually enhance testing capabilities. Incorporate new security and risk management issues, trends, and alerts into penetration testing activities.

- Develop reporting frameworks and dashboards to support Vulnerability Assessment and Penetration Testing VAPT
- Inform the stakeholders of the outcome of testing initiatives and results.
- Recommend methods and strategies for mitigating identified risks
- Provide recommendations based on VAPT security considerations
- Accept certification documentation for penetration testing results
- Propose corrections and recommendations to facilitate and enhance software certification

- Develop security penetration testing policies and frameworks
- Establish policies based on certification for maintaining compliance
- Formulate governance procedures for documenting and revising security testing policy, guidelines, and procedures.
- Design service strategies and scope for security testing solutions.
- Recommend strategic and operational modifications to security testing in response to new threats.
- Promote cyber security awareness within the enterprise.

- Analyze operational strategies, policies, and objectives across teams and initiatives.
- Develop resource planning and utilisation strategies Examine the utilisation of assets
- Manage the creation of learning roadmaps for teams and functions.
- Establish performance indicators to compare the efficacy of learning and development programmes to identify gaps and reduce inefficiency
- Implement initiatives for key management position succession planning

SECURITY OPERATIONS MANAGER

JOB DESCRIPTION

The Security Operations Manager is responsible for developing strategies, putting them into action, and supervising the internal teams tasked with maintaining security operations. Expertise in security technology and forward-thinking security concepts are required and efforts made made to strengthen the security operations as a whole.

They are responsible for coordinating routine audits of all active security tools, procedures, and planned upgrades.

They develop disaster recovery (DR) plans and contingency plans, as well as escalation mechanisms for security incidents.

They are knowledgeable about cyber security procedures, frameworks, and regulations while adhering to local Cyber Security Policies. They are well-versed in a vast array of cyber security testing and monitoring techniques and tools.

The Security Operations Manager is extremely vigilant when it comes to keeping track of all security-related information.

Source Image : https://wsecservices.com/en/security-operations-center-soc/

They are a self-assured leader who actively engages and develops their team members and devises strategies for handling security incidents.

Among the responsibilities may be the creation of procedures within a Cyber Security Operation Center (CSOC).

Duties may include:

- The implementation of detection and response capabilities to support Vulnerability Management, Threat Hunting, Incident Reporting, and Cyber Threat Intelligence.
- They continuously develop the necessary personnel, processes, and software to support the CSOC.
- They offer the Cyber Security team effective leadership and knowledge.
- They guarantee that the Chief Information Security Officer and internal stakeholders receive timely and accurate information.
- They are a leader who is logical and meticulous driven by analysis, reports, and actionable insights.

TECHNICAL SKILL	PROFICIENCY LEVEL
Audit and Compliance	★★★★
Budgeting	★★★★★
Business Performance Management	★★★★★
Business Continuity	★★★★★
Cyber and Data Breach Incident	★★★★
Disaster Recovery Management	★★★★★
Emerging Technologies	★★★★★
Learning and Development	★★★★
Networking & Security	★★★★
People & Performance	★★★★
Security Administration	★★★★
Security Education & Awareness	★★★★★
Security Strategy	★★★★★
Employee Succession Planning	★★★★
Stakeholder Management	★★★★
Strategy Planning - Implementation	★★★★
Threat Analysis and Defence	★★★★★
Threat Intelligence & Detection	★★★★

PERSONAL QUALITIES	PROFICIENCY LEVEL
Communication	Advanced
Developing People	Advanced
Problem Solving	Advanced
Resource Management	Advanced
Sense Making	Advanced

KEY JOB FUNCTIONS

TASK DESCRIPTIONS

Monitor

- Plan the monitoring of security systems and the response to cyber security incidents.
- Monitor the identification and measurement of essential cyber security operations metrics
- Develop and implement cyber threat detection and incident alert rules
- Supervise the planning and coordination of round-the-clock security operations
- Observe adherence to security policies, regulations, rules, and standards.
- Promote the ongoing enhancement of security operations

Maintenance

- Coordinate ongoing assessments of existing security programmes, protocols, and planned enhancements
- Monitor cyber security service levels and provide management with periodic cyber security status reports
- Oversee the prioritisation of alerts and incident response resources

Response

- Formulate internal procedures for handling and reporting cyber security incidents
- Review reports on cyber security incidents and breaches
- Present final cyber security incident reports to senior management for approval.
- Recommend systems and procedures for cyber security breach prevention, detection, containment, and correction.

Rededucation © 2026 All rights reserved.

KEY JOB FUNCTIONS CONTINUED

Compliance SOP's

Staff Management

TASK DESCRIPTIONS CONTINUED

- Create the company's cyber security strategy
- Align security operations functions with the enterprise's overarching business goals
- Advise senior leaders on crucial issues that may affect the security objectives of the organisation
- Provide guidance on the formulation and implementation of security policy and controls
- Provide expertise on innovative security technologies and concepts
- Provide technical and operational oversight for the deployment and implementation of security tooling

- Analyse operational strategies, policies, and objectives across teams and initiatives
- Develop resource planning and utilisation strategies
- Examine the utilisation of assets
- Manage the creation of learning roadmaps for teams and functions.
- Establish performance indicators to compare the efficacy of learning and development programmes to best practices.
- Implement initiatives for crucial management position succession planning

Rededucation © 2026 All rights reserved.

JOB DESCRIPTION

The Forensics Investigation Manager is responsible for organising and directing investigation procedures and protocols following a cyber threat or incident. They must supervise the entire process of data collection and analysis. They classify the threat and recommend the next steps to the affected parties. They are also accountable for developing a forensics investigation strategy and supervising overall investigative procedures. They are familiar with the necessary hardware and software to analyse threat data from multiple sources.

The manager of Forensic Investigations exerts great effort and closely monitors all investigation-related activity.

They are a strong leader who thinks quickly on their feet, comes up with inventive ways to deal with security breaches, and enjoys mentoring and collaborating with their team members.

The forensic manager must have exceptional oral and written communication skills. They must be able to maintain composure under pressure while providing detailed accounts of incidents, followed by investigation-derived summaries and conclusions.

They are adaptable, and flexible, and have excellent social skills for collaborating with others and connecting with others.

Forensics Investigations Manager

They are skilled at organising and leading teams of specialists and delegating responsibilities as needed.

A degree in Computer Science or a related field, years of experience in the field, and extensive knowledge of electronic extraction methods, including appropriate investigative strategies and techniques, are required to lead a group of investigators competently.

TECHNICAL SKILL	PROFICIENCY LEVEL
Budgeting	★★★★★
Business Performance Management	★★★★★
Cyber Forensics	★★★★★
Cyber Risk Management	★★★★★
Emerging Technology Synthesis	★★★★
Failure Analysis	★★★★
Learning and Development	★★★★
Manpower Planning	★★★★
Networking Security & Networking	★★★★
People & Performance Management	★★★★
Security Administration	★★★★
Security Assessment & Testing	★★★★★
Security Governance & Strategy	★★★★★
Stakeholder Management	★★★★
Strategy Implementation	★★★★
Strategy Planning	★★★★★
Threat Analysis and Defence	★★★★
Threat Intelligence & Detection	★★★★

PERSONAL QUALITIES	PROFICIENCY LEVEL
Communication	Advanced
Developing People	Advanced
Problem Solving	Advanced
Resource Management	Advanced
Sense Making	Advanced

KEY JOB FUNCTIONS

TASK DESCRIPTIONS

Monitor

- Analyze operational strategies, policies, and objectives across teams and initiatives
- Develop resource planning and utilisation strategies
- Examine the utilisation of assets
- Manage the creation of learning roadmaps for teams and functions
- Establish performance indicators to compare the efficacy of learning and development programmes to best practices
- Implement initiatives for key management position succession planning

Response

- After cyber-attacks, direct forensic investigations and coordinate forensic teams to determine the incident's root cause
- Examine forensic incident trends to ensure that the appropriate investigative steps are taken
- Determine the strategies, tactics, and procedures employed in cyber attacks
- Manage the evidence and causal analysis of cyber threats, attacks, and incidents
- Report to senior management and key stakeholders on the results of investigations and legal proceedings.

Staff Management

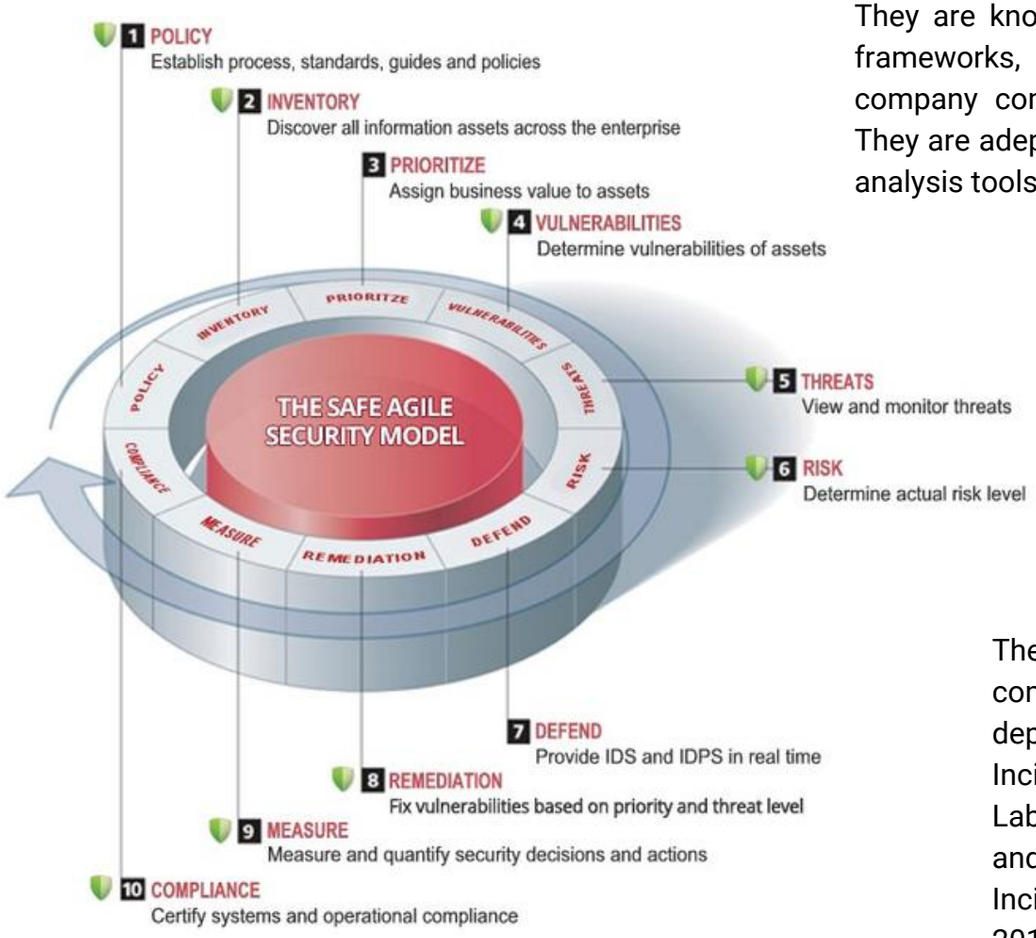
- Manage the creation of learning roadmaps for teams and functions
- Establish performance indicators to compare the efficacy of learning and development programmes to best practices
- Implement initiatives for key management position succession planning

Maintenance

- Create a plan to collect and analyse threat data following an incident
- Establish organisational policies and standards for digital forensic investigation
- After analysing the incident's root cause, develop threat mitigation processes and policies and update them as necessary
- Advise senior management on significant information security risks and forensics investigations policies and procedures

JOB DESCRIPTION

The Incident Investigation Manager is responsible for coordinating and monitoring the response in the event of a cyberattack. For the purpose of preventing future cyberattacks, they propose and develop mitigation techniques and countermeasures. They plan and execute countermeasures against cyberattacks. Informing upper management about cyber incidents is a crucial aspect of their job. They are required to work nights, weekends, and holidays, and must be available at all times.



https://www.yaacovapelbaum.com/2019/10/29/the-maginot-line-of-cyber-security/

They are knowledgeable about cyber security protocols, frameworks, and regulations, and he ensures that the company complies with the local Cyber Security Acts. They are adept at employing a vast array of cyber security analysis tools and techniques for problem-solving.

The Incident Investigation Manager is always on the lookout for suspicious behaviour and their investigations are extremely thorough. They are quick to offer solutions and make corrections when problems arise.

They are adept at navigating ambiguity, excellent communicators, and team builders. IT departments across all industries employ Incident Managers. According to the Bureau of Labor Statistics, the employment of computer and information systems managers, including Incident Managers, will increase by 15% from 2014 to 2024.

Incident Investigations Manager

This anticipated growth is primarily the result of continued upgrades to newer computer systems and an increased reliance on the operation of systems across all industries.

Incident Managers ensure that both employees and clients who utilise the technical products of a company receive technical support. They build technical teams and direct responses to technical software applications and system issues.

Managers of incidents are responsible for maintaining a log of all incidents. This aids them not only in tracking issues and ensuring their resolution but also in analysing incidents and establishing procedures to prevent or reduce the recurrence of similar issues.

A Situation Manager will establish operational procedures and policies for technical support teams.
These procedures will be implemented to assist with situations such as service interruptions and cyber security threats.
Additionally, they will instruct IT support personnel.

The Incident Manager will be an effective leader and team player who is also capable of working independently when necessary.
Additionally, Incident Managers must be attentive to the smallest of details and adept at handling crisis situations.

https://www.jobhero.com/

TECHNICAL SKILL	PROFICIENCY LEVEL
Budgeting	★★★★★
Business Performance Management	★★★★★
Cyber & Data Breach Incidents	★★★★
Cyber Forensics Management	★★★★
Cyber RISK Management	★★★★★
Learning & Development	★★★★
Manpower Planning	★★★★
Networking	★★★★
People & Performance	★★★★
Security Assessment Management	★★★★
Security Governance & Strategy	★★★★★
Stakeholder Management	★★★★★
Strategy Implementation & Planning	★★★★★
Threat Analysis & Planning	★★★★
Threat Intelligence & Planning	★★★★

PERSONAL QUALITIES	PROFICIENCY LEVEL
Communication	Advanced
Developing People	Advanced
Problem Solving	Advanced
Resource Management	Advanced
Sense Making	Advanced

KEY JOB FUNCTIONS

TASK DESCRIPTIONS

Monitor

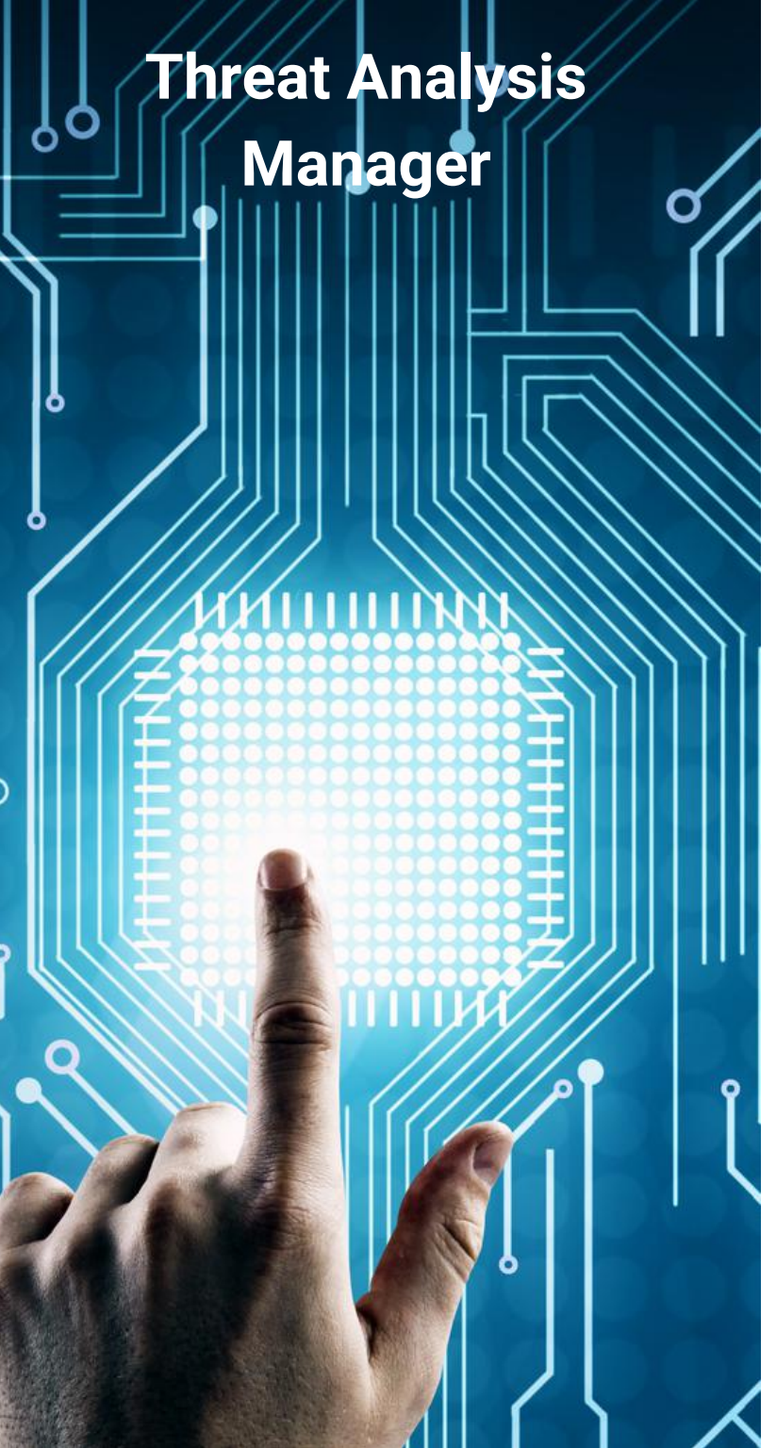
- Supervise the identification of security risks and system vulnerabilities
- Optimize data analytics models for cyber security to anticipate and detect suspicious activities
- Provide internal software and system design teams with risk analysis and security design guidance
- Monitor the dissemination of cyber threat intelligence to security partners, vendors, and law enforcement
- Supervise the creation of cyber security solutions to avert future cyber attacks.

Maintenance

- Analyze operational strategies, policies, and objectives across teams and initiatives.
- Develop resource planning and utilisation strategies
- Examine the utilisation of assets
- Manage the creation of learning roadmaps for teams and functions
- Establish performance indicators to compare the efficacy of learning and development programmes to best practices
- Implement initiatives for key management position succession planning

Compliance SOP's

- Develop emergency preparedness and disaster recovery plans specific to each security incident
- Establish organisational incident response policies and standards
- Develop incident response procedures and guidelines, revising them as necessary
- Provide guidance to senior management on the most significant information security-related risks and cyber incident response strategies



JOB DESCRIPTION

The Threat Analysis Manager devises strategies to protect a company's computer systems from potential cyber threats. It is his/her responsibility to determine which IT assets are vulnerable to cyber threats and attacks. The purpose of threat modelling is to provide defenders and the security team with an analysis of what security controls are necessary based on the current information systems and the threat landscape, the most likely attacks, their methodology, motivation, and target system.

https://www.eccouncil.org/threat-modeling/

They monitor the public Internet and identify potential threats and cyberattacking groups or individuals. Using testing and analysis, they guarantee the security of IT assets against cyberattacks.

Threat modelling requires collaboration between Security Architects, Security Operations, Network Defenders, the Security Operations Center (SOC), and the Threat Intelligence team in order to understand each other's roles, responsibilities, and challenges.

They are familiar with cyber security. They are accustomed to employing a wide range of cyber security analysis tools and techniques to monitor and detect potential incidents.

The Threat Analysis Manager constantly monitors, analyses and identifies potential security-related issues that may have a significant impact on security and operational systems.

A successful strategy for threat analysis can identify a wide range of threats within an organisation. The following classifications of threats are also included:

Accidental Threats

Whether it is a misconfiguration of a security procedure or an accident that leaves an organisation vulnerable, human error is one of the leading causes of cyberattacks today. By performing threat analysis, organisations are able to identify and rectify accidental errors prior to their exploitation by malicious actors.

Intentional Dangers

The threat that every organisation must consider is the intentional threat. Intentional threats are those perpetrated by malicious actors to gain access to sensitive data within an organisation and profit from it.

Internal Dangers

Unexpectedly, one of the most alarming threats is not what you might expect. Frequently, organisations worry about external threats and construct complex security architectures to keep bad actors out, but the real concern lies within the security perimeter of the organisation.

When an employee decides to act maliciously, the consequences can be disastrous because they may have easier access to sensitive information.

TECHNICAL SKILL	PROFICIENCY LEVEL
Audit & Compliance	★★★★★
Budgeting	★★★★★
Business Performance Management	★★★★★
Cyber & Data Breach Management	★★★★★
Cyber RISK Management	★★★★
Emerging Technology Synthesis	★★★★
IT Standards	★★★★
Learning & Development	★★★★
Networking Security & Networking	★★★★
People & Performance Management	★★★★
Security Architecture	★★★★
Security Assessment & Testing	★★★★★
Security Programme Management	★★★★★
Security Strategy	★★★★
Stakeholder Management	★★★★
Strategy Implementation	★★★★★
Strategy Planning	★★★★
Threat Analysis & Defence	★★★★
Threat Intelligence & Detection	

PERSONAL QUALITIES	PROFICIENCY LEVEL
Virtual Collaboration	Advanced
Transdiciplinary Thinking	Advanced
Problem Solving	Advanced
Leadership	Advanced
Global Mindset	Advanced

https://www.vmware.com/topics/glossary/content/threat-analysis.html#:~:text=Threat%20analysis%20is%20a%20cybersecurity,potential%20attack%20before%20they%20happen

KEY JOB FUNCTIONS

Monitor

Maintenance

Response

TASK DESCRIPTIONS

- Continuously scan and monitor external web applications and the dark web for potential threats.
- Conduct research into new and existing threats that could affect existing IT systems.
- Identify potential groups or individuals of attackers and implement preventative measures.
- Recommend and develop approaches or solutions to problems and situations for which there is insufficient information or no precedent.
- Monitor and report alterations in threat dispositions, activities, tactics, capabilities, and objectives associated with designated cyber operations warning problem sets.

- Develop and implement strategies for identifying assets vulnerable to cyber attacks and threats
- Deconstruct the application's architecture to identify potential threats and vulnerabilities in the application's design, implementation, deployment, or configuration.
- Conduct an in-depth analysis of existing threats and identify current cyber security weaknesses.
- Provide guidance on the design and implementation of security policy and asset controls
- Evaluate and provide feedback to enhance intelligence production, reporting, collection needs, and operations

- Utilizing knowledge of application and system vulnerabilities to identify potential threats that could affect applications and systems
- Test attacks and simulations on the systems to identify potential threats and the extent of potential damage.
- Prioritize and evaluate identified threats according to their severity.
- Provide timely notification of impending or hostile activities or intentions that may have an impact on the organization's objectives, resources, or capabilities.
- Utilize the existing threat and attack history database to anticipate and classify potential new threats.

KEY JOB FUNCTIONS CONTINUED

Compliance SOP's

Staff Management

TASK DESCRIPTIONS CONTINUED

- Document new threats based on a core set of attributes in order to develop protocols for threat mitigation
- Provide guidance on threat mitigation strategies and potential cyber threats and cyberattacks in order to ensure that the current cyber security standards and infrastructure are updated
- Support designated exercises, planning activities, and time-sensitive operations through intelligence analysis
- Provide evaluation and feedback to enhance intelligence production, reporting, requirements for collection, and operations

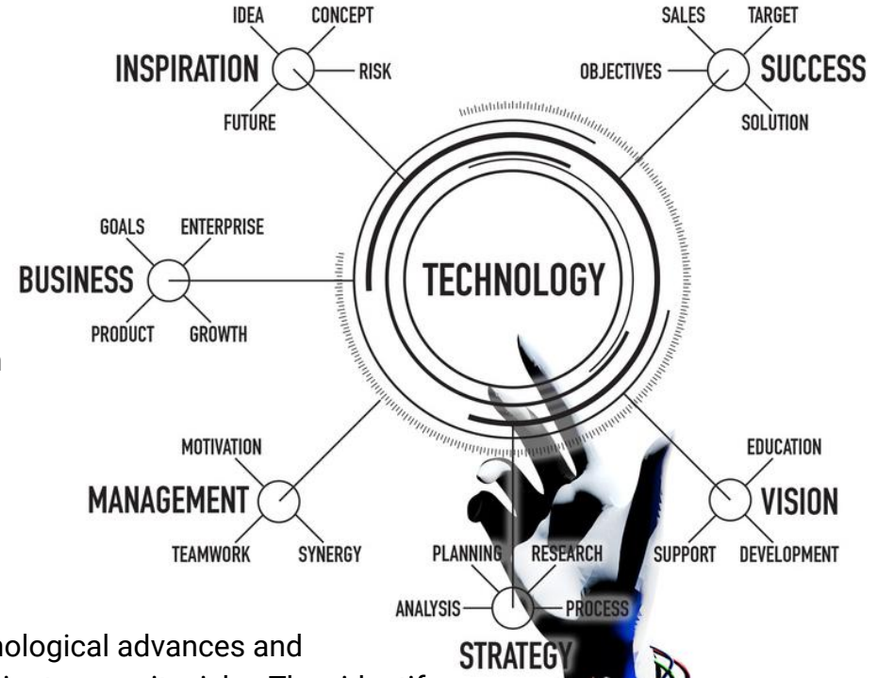
- Manage the budget allocation and expenditures across teams and projects
- Monitor and track the accomplishments and key performance indicators of the team
- Include targeted budgets, work allocations, and staff projections in your proposal for new operational plans
- Acquire, assign, and optimise resource usage
- Create learning roadmaps to support the team's professional development
- Manage the performance and development process, including maximising the potential of each individual through coaching and development opportunities

Security Architect

JOB DESCRIPTION

The Security Architect is responsible for overseeing projects involving the design, development, and implementation of complex, one-of-a-kind secure system architectures.

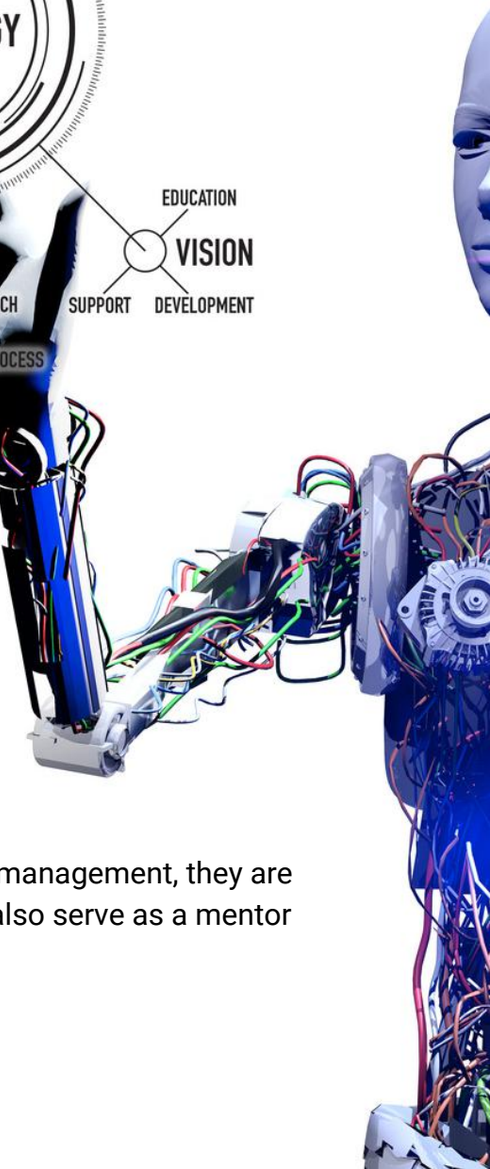
They plan and oversee the design of enterprise system artefacts that describe security principles and their relationship to the overall enterprise system architecture. They participate in the creation and deployment of new infrastructure security solutions.



They recommend and direct the adoption of new technological advances and best practices in infrastructure security systems to mitigate security risks. They identify and resolve unique and complex organization-wide and long-term issues.

They are experts in cyber security standards, protocols, and frameworks, and they ensure that the organisation complies with local security laws.

Numerous application and hardware-related technologies and services are familiar to them. The Security Architect possesses a creative and analytical mind and takes pleasure in identifying interconnections and interdependencies among the various system or architectural components.



Security Architects are technical experts however can relate and communicate well with staff and management, they are consultative by nature, and will actively engage stakeholders in the developmental systems. They also serve as a mentor to junior employees and provides technical leadership.

The Security Architect has knowledge of disaster recovery business continuity and continuity of operations plans. They can coordinate with system owners, common control providers, and system security officers regarding the allocation of security controls as a system-specific, hybrid, or common controls.

TECHNICAL SKILL	PROFICIENCY LEVEL
Business Needs Analysis	★★★★
Cyber Risk Management	★★★★★
Emerging Technology Synthesis	★★★★
Infrastructure Design	★★★★
Network Security	★★★★★
Security Administration	★★★★
Security Architecture	★★★★
Solution Architecture	★★★★★
Security Governance	★★★★★
Security Programme Management	★★★★
Security Strategy	★★★★★
Strategy Implementation	★★★★
Strategy Planning	★★★★★

PERSONAL QUALITIES	PROFICIENCY LEVEL
Communication	Advanced
Creative Thinking	Advanced
Developing People	Advanced
Problem Solving	Advanced
Sense Making	Advanced

KEY JOB FUNCTIONS

Monitor

Maintenance

Response

TASK DESCRIPTIONS

- Continuously scan and monitor external web applications and the dark web for potential threats
- Conduct research into new and existing threats that could affect existing IT systems
- Identify potential groups or individuals of attackers and implement preventative measures
- Recommend and develop approaches or solutions to problems and situations for which there is insufficient information or no precedent
- Monitor and report alterations in threat dispositions, activities, tactics, capabilities, and objectives associated with designated cyber operations warning problem sets

- Develop and implement strategies for identifying assets vulnerable to cyber attacks and threats
- Deconstruct the application's architecture to identify potential threats and vulnerabilities in the application's design, implementation, deployment, or configuration.
- Conduct an in-depth analysis of existing threats and identify current cyber security weaknesses.
- Provide guidance on the design and implementation of security policy and asset controls
- Evaluate and provide feedback to enhance intelligence production, reporting, collection needs, and operations

- Utilizing knowledge of application and system vulnerabilities to identify potential threats that could affect applications and systems
- Test attacks and simulations on the systems to identify potential threats and the extent of potential damage
- Prioritize and evaluate identified threats according to their severity
- Provide timely notification of impending or hostile activities or intentions that may have an impact on the organization's objectives, resources, or capabilities
- Utilize the existing threat and attack history database to anticipate and classify potential new threats

KEY JOB FUNCTIONS CONTINUED

Compliance SOP's

Staff Management

TASK DESCRIPTIONS CONTINUED

- Utilizing knowledge of application and system vulnerabilities to identify potential threats that could affect applications and systems
- Test attacks and simulations on the systems to identify potential threats and the extent of potential damage.
- Prioritize and evaluate identified threats according to their severity.
- Provide timely notification of impending or hostile activities or intentions that may have an impact on the organization's objectives, resources, or capabilities.
- Utilize the existing threat and attack history database to anticipate and classify potential new threats.

- Manage the budget allocation and expenditures across teams and projects
- Monitor and track the accomplishments and key performance indicators of the team
- Include targeted budgets, work allocations, and staff projections in your proposal for new operational plans
- Acquire, assign, and optimise resource usage
- Create learning roadmaps to support the team's professional development
- Manage the performance and development process, including maximising the potential of each individual through coaching and development opportunities

JOB DESCRIPTION

The Chief Information Security Officer or commonly known as the CISO designs the overall vision, to support the organisation's security platform. They are ultimately accountable for ensuring the security of corporate information and serve as the organization's security strategy, standards, and policy creator and enforcer.

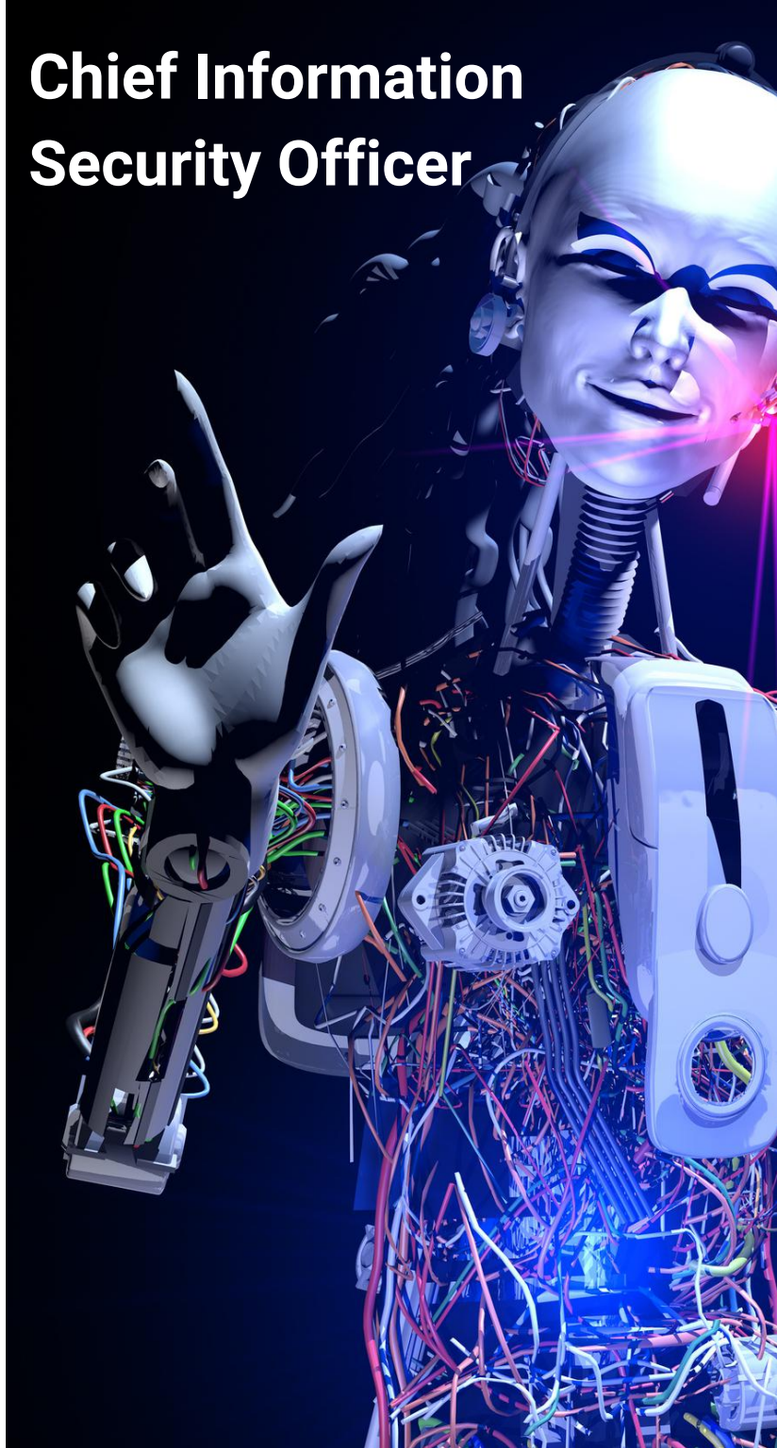
They oversee the design and ongoing development of a Cyber Risk Maturity Model and IT security architecture that strikes a balance between business requirements and security threats. They also establish compliance directives to support local and government regulatory policies, adherence to compliance, and audits.

https://www.nexor.com/a-day-in-the-life-of-a-ciso/

In addition to being an authority on cyber security compliance, they are the subject matter expert on all corporate responsibilities to ensure compliance with all State and Federal cyber security standards.

They keep abreast of cyber-related applications, hardware technologies, and services, and are constantly on the lookout for new technologies that can be used to enhance work processes or those that pose potential threats to the organisation.

Chief Information Security Officer



The Chief Information Security Officer is a visionary and influential leader who exhibits sound judgement and determination in ensuring the protection and security of corporate information. They are always strategic in nature when dealing with their team management including resource and skills development. The CISO is accountable for ensuring that the organization's cyber security and business objectives are aligned.

They facilitate communication between business and cyber security stakeholders to accomplish this.
This includes translating cyber security concepts and terminology into business concepts and terminology and ensuring that business teams consult with cyber security teams to determine the appropriate controls when planning new business projects.

In addition, since the CISO is responsible for the development of the organization's cyber security programme, they are in the best position to advise projects on the strategic direction of cyber security within the organisation.

The CISO is also accountable for managing the organization's response to cybersecurity incidents, including how internal teams respond and communicate during an incident. The CISO must be prepared to assume a crisis management position in the event of a significant cyber security incident. They must be capable of elucidating the situation and communicating effectively with internal and external stakeholders.

TECHNICAL SKILL	PROFICIENCY LEVEL
Audit and Compliance	★★★★★
Budgeting	★★★★★
Business Continuity	★★★★★
Business Needs & Performance	★★★★★
Cyber Breach Management	★★★★★
Cyber Forensics	★★★★★
Cyber Risk Management	★★★★★
Disaster Recovery Management	★★★★★
Emerging Technology Synthesis	★★★★★
IT Standards	★★★★★
Learning & Development	★★★★★
People & Performance Management	★★★★★
Network Security	★★★★★
Networking	★★★★★
Partnership Management	★★★★★
Security Architecture	★★★★★
Security Governance	★★★★★
Security Strategy & Implementation	★★★★★
Stakeholder Management	★★★★★
Threat Analysis & Defence	★★★★★
Threat Intelligence & Detection	★★★★★

PERSONAL QUALITIES	PROFICIENCY LEVEL
Leadership	Advanced
Global Mindset	Advanced
Decision Making	Advanced
Transdisciplinary Thinking	Advanced
Sense Making	Advanced

KEY JOB FUNCTIONS

TASK DESCRIPTIONS

Monitor

- Supervise the formulation of information security and risk management policies, business continuity and disaster recovery plans
- Evaluate current information security practices to guarantee conformity with IT standards and industry standards
- Supervise the implementation of appropriate plans to ensure adherence to regulatory, industry, and regional requirements
- Establish and implement legal risk rules and guidelines for cyber security in accordance with industry norms and standards
- Promote awareness programmes for information security and risk management

Maintenance

- Establish the organization's cyber security vision, strategy, and any underlying initiatives or programmes
- Align information security and risk management strategies with business objectives
- Provide strategic, budgetary, and administrative guidance for information security strategy implementation
- Drive information security education and awareness throughout the organisation
- Provide guidance to senior management and key constituencies on information security issues

Response

- Serve as an expert in cyber security investigation and analysis
- Motivate the resolution of major security incidents
- Direct the development of plans to address system weaknesses
- Provide counsel regarding responses to regulatory inquiries, inspections, and audits
- Present evidence for legal action in response to cyber security incidents

Rededucation © 2026 All rights reserved.

KEY JOB FUNCTIONS CONTINUED

Compliance SOP's

Staff Management

TASK DESCRIPTIONS CONTINUED

- Supervise the formulation of information security and risk management policies, business continuity and disaster recovery plans
- Evaluate current information security practises to guarantee conformity with IT standards and industry standards
- Supervise the implementation of appropriate plans to ensure adherence to regulatory, industry, and regional requirements
- Establish and implement legal risk rules and guidelines for cyber security in accordance with industry norms and standards
- Promote awareness programmes for information security and risk management

- Supervise the development of risk assessment frameworks for cyber security
- Advise business stakeholders on cyber risks and incidents, as well as cyber security compliance standards
- Manage the development and testing of business continuity and disaster recovery plans
- Facilitate compliance with international and national information security and privacy regulations Serve as the organization's liaison with external agencies regarding cyber security risk issues

Rededucation © 2026 All rights reserved.

Red Education

ABOUT RED EDUCATION

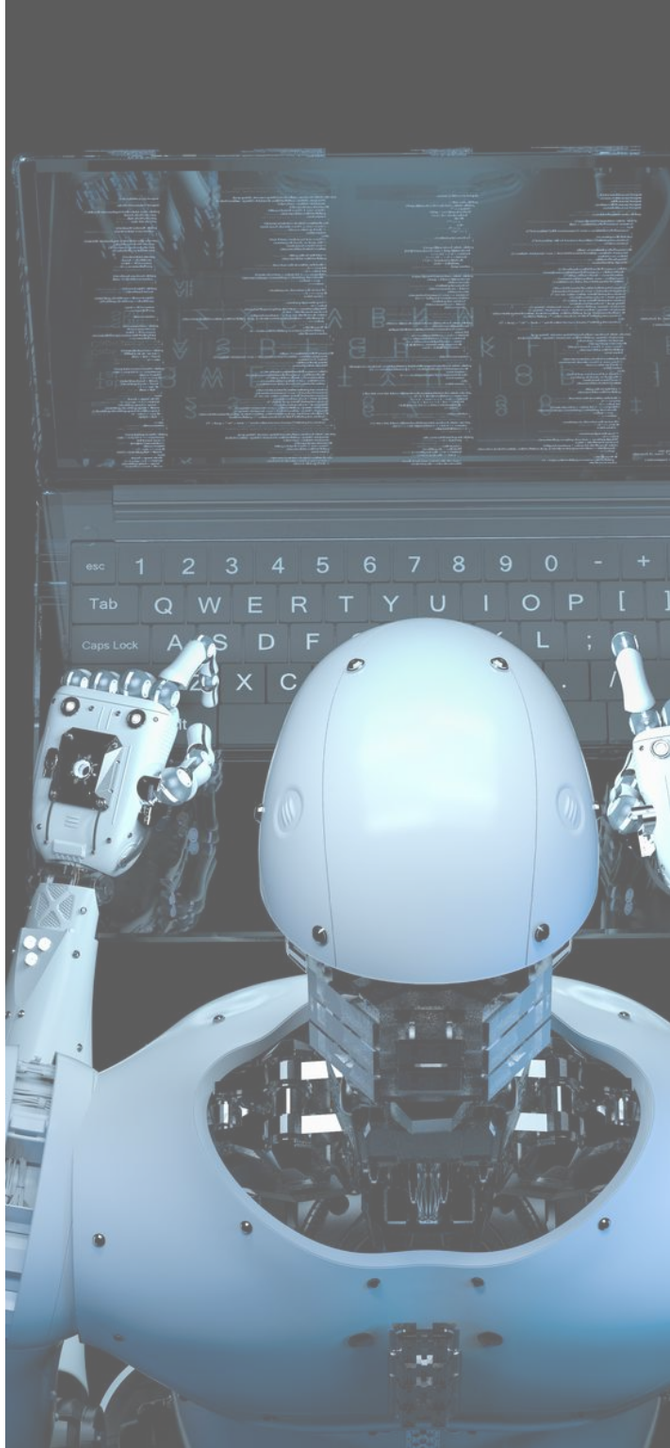
Red Education is a multi-award-winning global information technology Accredited Certification Training Company (ATC) headquartered in Sydney, Australia. With training hubs across ANZ, ASIA, SAARC, the Americas, the Middle East and Europe, more than 70 Red Education instructors across multiple regions and time zones deliver technical training programs to the IT community in local languages.

We began operations to support multinational technology provider F5, specialising in firewall technologies to protect against cyberattacks. F5 asked us to help train their clients due to the complexity of the technology. We said yes. From these humble beginnings, we have upskilled over 100,000 students to date across the globe

For over 20 years, providing training and certification to the world's leading technology brands: Palo Alto Networks, F5, Check Point, AWS, ForgeRock, AlgoSec, Nutanix, Avaya, Arista, Paessler, VMware, RedHat, epi, Fortinet, Symantec, Wilson Learning, Riverbed and Infoblox. And yes, we are still proudly working with F5.
You never forget your first!

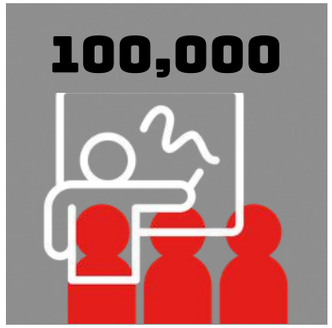
Our awards

We continue to be recognised for excellence across the cybersecurity training industry. In 2026, Red Education earned multiple honours including a Gold Stevie Award for Global Partnership of the Year, a Gold Stevie Award for Achievement in Certification Programs, and a Bronze Stevie Award for Achievement in Organisational Culture. We were also named Best Cybersecurity Education Provider and Cybersecurity Instructor Team of the Year at the Cybersecurity Excellence Awards, along with Gold wins for Best Cybersecurity Education Provider and Customer Satisfaction at the Globee Cybersecurity Awards.



Our technology partners

Since 2005 Red Education has assisted the IT industry with the certification process and the upskilling of IT technicians.

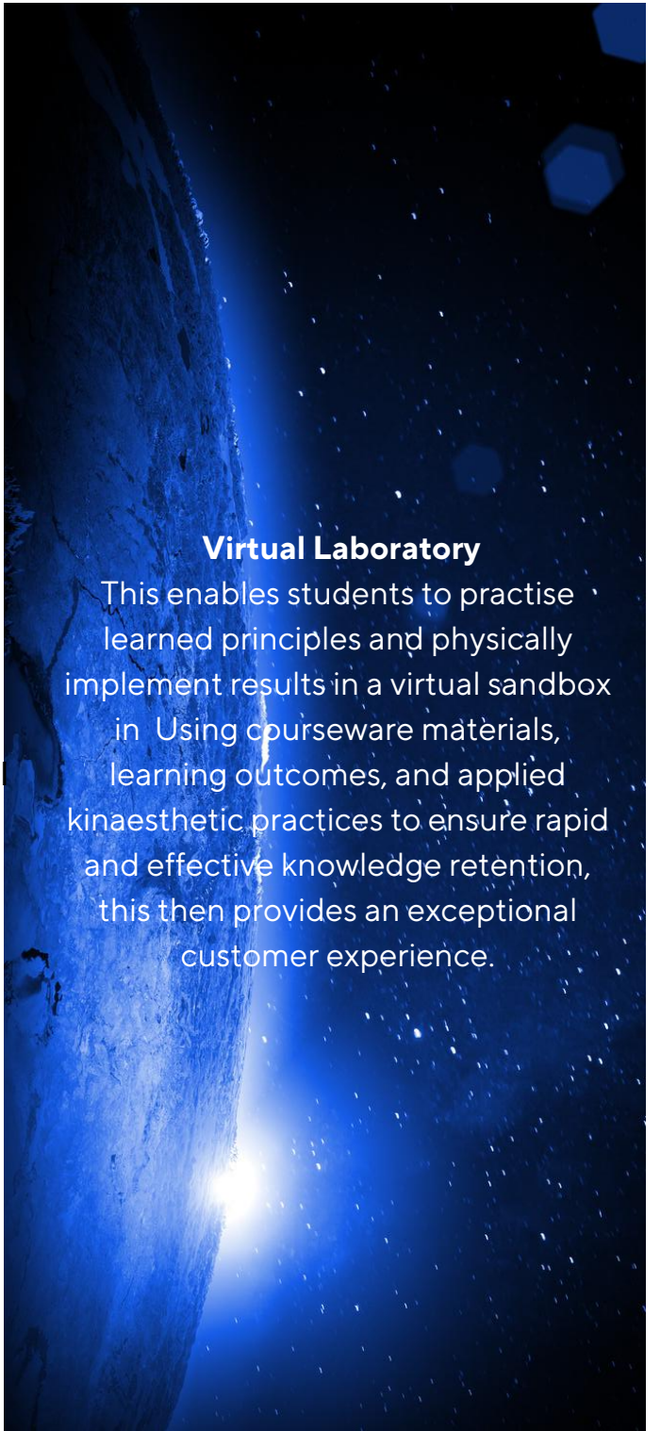


What our students say

We survey our students after the delivery of each training course and we invite feedback through Reviews.io and Google Reviews. Each student review is read and receives a reply, irrespective of rating or comment, from our Managing Director. We are proud to have earned an NPS score of 94 from our students and a 98% customer satisfaction rating.

Our virtual labs

Winning Red Education our spot on the AFR BOSS Top 10 Most Innovative Companies List, we are pretty sure that our custom-built virtual labs are better than anything else that is out there in the market. Our labs simulate real-world software environments and are used during Red Education training courses.



We believe that this is the best method to reinforce learning, enabling students to test workflows and resilience to cyber-attacks safely before implementation in their workplaces, building confidence and competence and reducing risk.

Our instructor team

Our global team of expert instructors is our superpower. Red Education instructors need at least 10 years of IT experience with the necessary technical skills to deliver a premium training experience. They must also be great communicators and exceptional teachers. Today, thanks to our Virtual Instructor-led Training model, students anywhere in the world can benefit from the expertise of these unicorns, the world's leading instructors, training virtually in the student's time zone and language.

In pursuit of excellence

Red Education has an absolute commitment to delivering superior results for our students, the organisations they work for, and our vendor partners.

Behind the scenes, Red Education follows the Kaizen methodology, with continuous process improvement in pursuit of excellence. We commit to continuous change as we constantly enhance our student's learning experience and outcomes.with continuous process improvement in pursuit of excellence. We commit to continuous change as we constantly enhance our student's learning experience and outcomes.

Corporate Social Responsibility

When a student enrols with us, we donate to an important cause in their region. In Australia and New Zealand, we work with GreenFleet, to help restore the native forests and ecosystems that provide habitat for endangered wildlife, help counter the devastating impact of bushfires, and reduce the effects of climate change. We plant five native trees for every student enrolled.
In the SAARC region, training with Red Education supports the Sri Sathya Sai Annapoorna Trust, providing much-needed free morning nutrition for disadvantaged school children across India. Thanks to Red Education students, 10 children are fed for every student enrolled.

Training with Red Education helps build a better future for our students, the global business community and the planet. And with our flexible payment plans, you can start now.

Payment Options

References

https://www.eccouncil.org/threat-modeling/

https://fintechnews.ph/56130/security/cybersecurity-talent-shortage-puts-apac-organizations-at-risk/

https://www.imda.gov.sg/cwp/assets/imtalent/skills-framework-for-ict/index.html

https://www.jobhero.com/

https://www.nexor.com/a-day-in-the-life-of-a-ciso/

https://www.vmware.com/topics/glossary/content/threat-

analysis.html#:~:text=Threat%20analysis%20is%20a%20cybersecurity,potential%20attack%20before%20they%20happen

https://wsecservices.com/en/security-operations-center-soc/

https://www.yaacovapelbaum.com/2019/10/29/the-maginot-line-of-cyber-security/

THE END

Rededucation © 2026 All rights reserved.