CYBER SECURITY TEAM

A cybersecurity team is typically composed of a variety of roles, each specialising in different aspects of security. Here are the primary roles that commonly make up a cybersecurity team:

- Chief Information Security Officer (CISO):
  - Responsible for overall cybersecurity strategy and implementation.
  - Reports to senior management and ensures alignment with business goals.
- Security Operations Manager:
  - Manages the day-to-day security operations and incident response.
- Security Analyst:
  - Monitors networks and systems for security breaches or intrusions.
  - Analyses security alerts and provides detailed reports.
- Security Engineer:
  - Designs and implements security solutions and infrastructure.
  - Maintains and upgrades security systems.
- Security Architect:
  - Develops the security architecture and framework.
  - Ensures that new projects and technologies integrate securely.
- Incident Responder/Incident Response Team (IRT):
  - Handles security breaches and incidents.
  - Conducts forensic analysis and coordinates remediation efforts.
- Penetration Tester/Ethical Hacker:
  - Conducts simulated attacks to identify vulnerabilities.
  - Provides recommendations to strengthen security measures.
- Security Consultant:
  - Provides expert advice on security best practices and strategies.
  - Often works on a contract basis to address specific security concerns.

- Compliance Manager:
  - Ensures that the organisation complies with relevant laws, regulations, and standards.
  - Conducts regular audits and assessments.
- Security Administrator:
  - Manages and configures security tools and policies.
  - Administers user access and controls.
- Threat Hunter:
  - Proactively searches for threats and vulnerabilities that may not have been detected by automated systems.
  - Uses intelligence and analytics to predict and prevent attacks.
- Security Awareness Trainer:
  - Educates employees about security policies, procedures, and best practices.
  - Develops training programs to mitigate human error.
- Data Protection Officer (DPO):
  - Manages data privacy and protection efforts.
  - Ensures compliance with data protection regulations like GDPR.
- Cloud Security Specialist:
  - Focuses on securing cloud environments and services.
  - Implements cloud-specific security measures and policies.
- Identity and Access Management (IAM) Specialist:
  - Manages user identities and access permissions.
  - Implements authentication and authorization mechanisms.
- Malware Analyst:
  - Studies and analyses malware to understand its behaviour and impact.
  - Develops strategies to detect and mitigate malware threats.
- Application Security Engineer:
  - Ensures that software applications are designed and coded securely.
  - Conducts code reviews and security testing on applications.

These roles work collaboratively to ensure a comprehensive security posture for the organisation, addressing both proactive and reactive aspects of cybersecurity.

CHIEF INFORMATION SECURITY OFFICER (CISO)

Responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected. Will direct staff in identifying, developing, implementing, and maintaining processes across the business to reduce information and information technology (IT) risks. This role ensures the organisation's compliance with relevant laws and regulations, and works to protect the confidentiality, integrity, and availability of the company's information.

QUALIFICATIONS/SKILLS

- Bachelor's degree in Computer Science, Information Technology, Cybersecurity, or a related field.
- Master’s degree preferred.
- Minimum of 10 years of experience in information security, with at least 5 years in a senior leadership role.
- Proven track record of developing and implementing information security programs.
- Professional security management certification, such as CISSP, CISM, or CISA.
- Strong understanding of information security frameworks, standards, and best practices.
- Excellent leadership, communication, and interpersonal skills.
- Strong analytical and problem-solving abilities.
- Ability to manage multiple priorities and projects in a fast-paced environment.

KEY COMPETENCIES

- Strategic Vision
- Risk Management
- Decision Making
- Leadership

- Communication
- Technical Proficiency
- Regulatory Knowledge
- Incident Management

OPERATIONS MANAGER

Responsible for overseeing the day-to-day operations of the cybersecurity team to ensure the effective implementation of security measures and protocols. This role involves managing security operations, incident response, threat management, and ensuring compliance with security policies and regulations. The Operations Manager will work closely with various stakeholders to enhance the organisation's security posture and mitigate risks.

QUALIFICATIONS/SKILLS

- Bachelor's degree in Computer Science, Information Technology, Cybersecurity, or a related field
- Master's degree or relevant professional certification (e.g., CISSP, CISM) is preferred
- Minimum of 5 years of experience in cybersecurity operations, with at least 2 years in a management or leadership role
- Proven experience in incident response, threat management, and security operations
- Strong knowledge of cybersecurity principles, practices, and tools.
- Excellent problem-solving and analytical skills.
- Strong communication and interpersonal skills.
- Ability to manage multiple tasks and priorities in a fast-paced environment.
- Proficiency in using security tools and technologies (e.g., SIEM, IDS/IPS).

KEY COMPETENCIES

- Leadership
- Strategic Planning
- Risk Management
- Communication

- Problem-Solving
- Team Collaboration
- Time Management
- Adaptability

SECURITY ANALYST

Responsible for protecting the company's information assets by identifying, analysing, and mitigating security threats. This role involves monitoring the network for security breaches, investigating violations, and ensuring compliance with security policies and procedures. The Security Analyst works closely with other IT and business teams to maintain a secure environment.

QUALIFICATIONS/SKILLS

- Bachelor's degree in Computer Science, Information Technology, Cybersecurity, or a related field.
- Minimum of 2-4 years of experience in information security or a related field.
- Hands-on experience with security monitoring, incident response, and vulnerability management.
- Relevant security certifications such as CompTIA Security+, CEH (Certified Ethical Hacker), or CISSP (Certified Information Systems Security Professional) are preferred.
- Strong understanding of security principles, techniques, and technologies.
- Proficiency in using security tools and software.
- Excellent analytical and problem-solving skills.
- Strong communication and interpersonal skills.
- Ability to work independently and as part of a team.

KEY COMPETENCIES

- Attention to Detail
- Analytical Thinking
- Problem-Solving
- Communication

- Technical Proficiency
- Team Collaboration
- Initiative and Proactivity
- Adaptability

SECURITY ENGINEER

Responsible for designing, implementing, and maintaining the security infrastructure of the organisation. This role involves developing security solutions, performing system hardening, and ensuring that the organisation's network, systems, and data are protected against threats. The Security Engineer collaborates with other IT teams to integrate security measures and responds to security incidents.

QUALIFICATIONS/SKILLS

- Bachelor's degree in Computer Science, Information Technology, Cybersecurity, or a related field.
- Minimum of 3-5 years of experience in information security, with hands-on experience in security engineering.
- Proven experience with network security, system hardening, and security technologies.
- Relevant certifications such as CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker), or CompTIA Security+ are preferred.
- Strong knowledge of security principles, practices, and technologies.
- Proficiency in using security tools and software.
- Experience with scripting and programming languages (e.g., Python, PowerShell).
- Excellent problem-solving and analytical skills.
- Strong communication and interpersonal skills.

KEY COMPETENCIES

- Technical Proficiency
- Analytical Thinking
- Problem-Solving
- Attention to Detail
- Communication
- Team Collaboration
- Initiative and Proactivity
- Adaptability

INCIDENT RESPONDER

Responsible for responding to and managing security incidents within the organisation. This role involves identifying, investigating, and mitigating cybersecurity threats and incidents, ensuring a swift and effective response to minimise impact. The Incident Responder will work closely with other cybersecurity team members to enhance the organisation's security posture and develop strategies to prevent future incidents.

QUALIFICATIONS/SKILLS

- Bachelor's degree in Computer Science, Information Technology, Cybersecurity, or a related field.
- Relevant certifications such as GCIH (GIAC Certified Incident Handler), CEH (Certified Ethical Hacker), or CISSP are preferred.
- Minimum of 3-5 years of experience in cybersecurity, with a focus on incident response or security operations.
- Proven experience in responding to and managing security incidents in a complex environment.
- Strong understanding of cybersecurity principles, threats, and attack vectors.
- Proficiency in using security tools and technologies (e.g., SIEM, IDS/IPS, EDR).
- Excellent problem-solving and analytical skills.
- Strong written and verbal communication skills.
- Ability to work effectively under pressure and in high-stress situations.

KEY COMPETENCIES

- Incident Response
- Threat Analysis
- Communication
- Problem-Solving
- Attention to Detail
- Team Collaboration
- Adaptability

PENETRATION TESTER/ ETHICAL HACKER

Responsible for identifying and exploiting security vulnerabilities in the organisation's systems, networks, and applications. This role involves conducting regular penetration tests, security assessments, and red team exercises to simulate real-world attacks and improve the organisation's security posture. The Penetration Tester / Ethical Hacker collaborates with other security and IT teams to implement effective security measures and provides detailed reports and recommendations.

QUALIFICATIONS/SKILLS

Bachelor's degree in Computer Science, Information Technology, Cybersecurity, or a related field.

- Minimum of 2-4 years of experience in penetration testing, ethical hacking, or a related field.
- Proven experience with penetration testing tools and methodologies.

Relevant certifications such as OSCP (Offensive Security Certified Professional), CEH (Certified Ethical Hacker), or GPEN (GIAC Penetration Tester) are preferred.

- Strong knowledge of security principles, practices, and tools.
- Proficiency in using penetration testing tools such as Metasploit, Burp Suite, Nmap, and Wireshark.
- Experience with scripting and programming languages (e.g., Python, Bash).
- Excellent problem-solving and analytical skills.
- Strong communication and interpersonal skills.

KEY COMPETENCIES

- Technical Proficiency
- Analytical Thinking
- Problem-Solving
- Attention to Detail
- Communication
- Team Collaboration
- Initiative and Proactivity
- Adaptability

SOFTWARE DEVELOPER

Responsible for designing, coding, testing, and maintaining software applications that meet the needs of the organisation and its clients. This role involves working collaboratively with other developers, analysts, and stakeholders to deliver high-quality software solutions. The Software Developer must be proficient in various programming languages and development tools, and demonstrate a strong understanding of software development principles and methodologies.

QUALIFICATIONS/SKILLS

- Bachelor's degree in Computer Science, Software Engineering, or a related field.
- Minimum of 2-4 years of experience in software development.
- Proven experience with one or more programming languages (e.g., Java, C#, Python, JavaScript).
- Strong knowledge of software development principles and methodologies (e.g., Agile, Scrum).
- Proficiency in using development tools and environments (e.g., IDEs, version control systems).
- Experience with databases and SQL.
- Excellent problem-solving and analytical skills.
- Strong communication and interpersonal skills.

KEY COMPETENCIES

- Technical Proficiency
- Analytical Thinking
- Problem-Solving
- Attention to Detail

- Communication
- Team Collaboration
- Initiative and Proactivity
- Adaptability