Associate Security Analyst/ Security Operations Analyst

HIGH

IN 3-5 YEARS

As Security Orchestration, Automation and Response (SOAR) continues to mature and increasingly automate and orchestrate workflows, core tasks of these job holders will be replaced. Job holders will face potential displacement and move into more specialized or experienced roles to manage SOAR.

KEY TRENDS

- AI & Analytics
- Evolving IT Ecosystem

FUTURE TASK-LEVEL VIEW

- Automated control assessment tools assist job holders in assessing security controls by providing real-time updates on the enterprise's security posture
- SOAR (Security Orchestration, Automation and Response) will take over manual tasks in cyber monitoring activities and reporting, leaving job holders to use their technical expertise and discretion in analysing insights from log data and reports
- SOAR will potentially replace core tasks such as managing cyber security systems and operations by orchestrating processes, policy execution and reporting, thereby reducing the manpower required for these tasks
- ML will assist job holders in automating security alerts and response prioritisation by adapting from previous cyber security incidents

POSSIBLE JOBS TO MOVE INTO

For Associate Security Analyst

- Incident Investigator (Easy)
- Cyber Risk Analyst (Easy)
- Forensics Investigator (Moderate)
- Vulnerability Assessment & Penetration Testing Analyst (Moderate)

For Security Operations Analyst

- Incident Investigator (Easy)
- Security Engineer (Moderate)
- Forensics Investigator (Moderate)
- Vulnerability Assessment & Penetration Testing Analyst (Moderate)

Click here to find out more on the programmes and support available to close skills gaps and gain future skills

Possible job roles to move into for:
Associate Security Analyst

POSSIBLE MOBILITY OPPORTUNITIES

Incident Investigator 

Cyber Risk Analyst 

RATIONALE

- Job holders can make use of their experience in **monitoring security alerts and events, and documenting information based on established practices**, which helps them transit into this role to **identify and define cyber threats and root causes, and develop reports that detail cyber incident details**.

- Job holders have experience in **analyzing security-related information and events, as well as preparing and publishing security advisories**, which will enable them to **identify IT related risk** and **determine appropriate controls to mitigate risks** in this role.

TOP SKILLS MATCH

- Cyber Forensics
- Cyber and Data Breach Incident Management
- Security Assessment and Testing
- Stakeholder Management
- Threat Analysis and Defence
- Threat Intelligence and Detection
- Business Needs Analysis
- Cyber Forensics
- Cyber and Data Breach Incident Management
- Security Administration
- Security Education and Awareness
- Security Programmme Management
- Stakeholder Management

TOP SKILLS GAP

- Cyber Risk Management
- Audit and Compliance
- Cyber Risk Management
- IT Governance
- Security Governance
- Strategy Implementation
- Strategy Planning

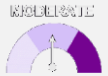
Click here to find out more about the programmes and support available to close skills gaps

Possible job roles to move into for:
Associate Security Analyst

POSSIBLE MOBILITY OPPORTUNITIES

Forensics Investigator

Vulnerability Assessment & Penetration Testing Analyst



RATIONALE

- Job holders can leverage their skills to **collect and analyse threat data** and transit into this role by upskilling and gaining additional skills to **investigate the root cause of cyber attacks post mortem.**

- Job holders can leverage their **understanding of cybersecurity systems, operational and maintenance vulnerabilities** to learn how to **design and perform tests on systems that might be vulnerable to attacks in this role.**

TOP SKILLS MATCH

- Cyber Forensics
- Security Administration
- Security Assessment and Testing
- Stakeholder Management
- Threat Analysis and Defence
- Threat Intelligence and Detection
- Security Assessment and Testing
- Threat Analysis and Defence
- Stakeholder Management

TOP SKILLS GAP

- Cyber Risk Management
- Emerging Technology Synthesis
- Failure Analysis
- Network Security
- Cyber Risk Management
- Emerging Technology Synthesis
- Network Security
- Security Strategy
- Test Planning

Click here to find out more on the programmes and support available to close skills gaps