**Persona Descriptions:**

**Vendor Security Specialist:**

Vendor security specialists are responsible for assessing and managing the cybersecurity posture of third-party vendors as well as the vendor’s products and services. These specialists work to identify potential security vulnerabilities and risks of potential vendors during the process of selecting vendors for an IT organization. Vendor security specialists conduct thorough evaluations of the security practices and compliance standards of vendors, focusing on reviewing integration processes, data security practices, and compliance with industry standards like SOC 2 and ISO 27001. These specialists focus on risk assessment and management, vendor audits, and creating strategies to mitigate risks from external vendor vulnerabilities. Vendor security specialists also frequently collaborate with legal teams in IT organizations to ensure that contracts include vendor security clauses and that vendors are contractually obligated to comply with organizational and industry security standards.

**Network Security Analyst:**

Network Security Analysts are primarily responsible for securing data transmission within an organization’s IT and network infrastructure, both on-premises and in the cloud. These analysts design and implement network security strategies and solutions in order to protect an organization from unauthorized access, data breaches, ransomware, and other cybersecurity threats. The primary responsibilities of network security analysts include configuring and maintaining firewalls, intrusion detection and prevention systems (IDS/IPS), and other network security tools. These analysts also conduct regular network traffic monitoring, vulnerability assessments, and penetration testing in order to identify weaknesses in an organization’s IT security posture. These analysts enforce encryption, network segmentation, and access control policies within an organization and play a critical role in securing communications between on-premises networks and cloud environments. These analysts are also primarily involved in cloud network security (AWS, Azure), VPNs, zero-trust models, incident response, and security for hybrid and multi-cloud networks.

**Cyber Risk Analyst / Chief Information Security Officer (CISO) / Information Security Officer (ISO)**

Cyber Risk Analysts, CISOs, and ISOs collectively cover a wide array of cybersecurity concerns across an organization, from assessing and mitigating risks to overseeing the creation of security policies and frameworks. Cyber Risk Analysts primarily focus on identifying and prioritizing potential risks within an organization’s IT environment, including evaluating how various vulnerabilities could impact an organization’s business model and SLAs. Cyber Risk Analysts are skilled in risk management and are often responsible for analyzing potential threats in various environments such as network security, application security, and data security.

Chief Information Security Officers (CISOs) and Information Security Officers (ISOs) are primarily responsible for managing the strategic direction of an organization’s overall cybersecurity policies and posture. This includes funding for security personnel and software as well as oversight of overall security operations and threat intelligence. CISOs and ISOs are also responsible for ensuring that an organization’s cybersecurity practices align with its business objectives, primarily through ensuring compliance with industry standards and regulations like GDPR. CISOs and ISOs are the primary roles for incident response execution and planning and crisis management, making them the ‘first responders’ of a data security or cybersecurity incident within an organization.