Resolves complex security problems or breaches; conducts and initiates security scans and audits; performs risk assessments; acts as both a technical lead and liaison for interacting with third-party vendors, forensic specialists, auditors, law enforcement, and other investigators.

Creates and delivers training on information security for IT staff and end-users

Firewalls, intrusion detection and prevention systems, auditing and scanning systems, VPN, and remote access systems.
Vulnerability assessment tools including but not limited to Nessus, Metasploit, and Nmap.
Specific security issues associated with common operating systems, networking, and virtualization software.
Risk and threat assessment processes and practices.
Malware including computer viruses, worms, Trojan horses, spyware, and ransomware; phishing and other social engineering strategies.
Concepts, procedures,