



Security Administrator

Job Description

A cybersecurity team's point of contact is a security administrator. They are typically in charge of installing, administering, and troubleshooting a company's security solutions. They also create security policies and training documents for colleagues on security procedures. Security administrators oversee the entire system rather than specific components. While network and system administrators configure and maintain the system, security administrators step back to assess overall security. Unlike their counterparts, they work to defend the system as a whole and keep it secure from threats rather than focusing on hardware and software.

Security Administrator vs. Security Analyst

A Security Administrator's responsibilities range from entry-level to mid-level. The levels of responsibility associated with the Security Administrator role are frequently determined by the size of the company. In addition, the job occasionally requires analytics. In smaller organizations, the roles of Security Administrator and Security Analyst may be combined, whereas in larger organizations, they may be separate.

Key Responsibilities

- Preventing unwanted access, alteration, and/or destruction of systems.
- Checking and evaluating the network for weaknesses.
- Looking out for suspicious activities in the network flow.
- Establishing and maintaining firewalls, antivirus software, and patch management systems as security tools.
- Instituting access control, application security, network security rules, and corporate data protection measures.
- Educating co-workers about security awareness and procedures.
- Establishing and maintaining business continuity and catastrophe recovery procedures.

Qualifications Needed

- A degree in computer science, cyber security, or a similar discipline, either at the associate or bachelor level.

- A thorough knowledge of network, security, and computer systems.
- Excellent interpersonal, communication, and teaching abilities.
- Excellent analytical, critical-thinking, and problem-solving abilities
- Understanding of popular protocols including SSL, HTTP, DNS, SMTP, and IPsec.
- An in-depth knowledge of firewall technology.
- Understanding of packet shapers, load balancers, and proxy servers.
- Knowledge of intrusion detection and prevention systems ranging from intermediate to expert.
- Comprehensive knowledge of IT infrastructure, including protocols, operating systems, and networks.