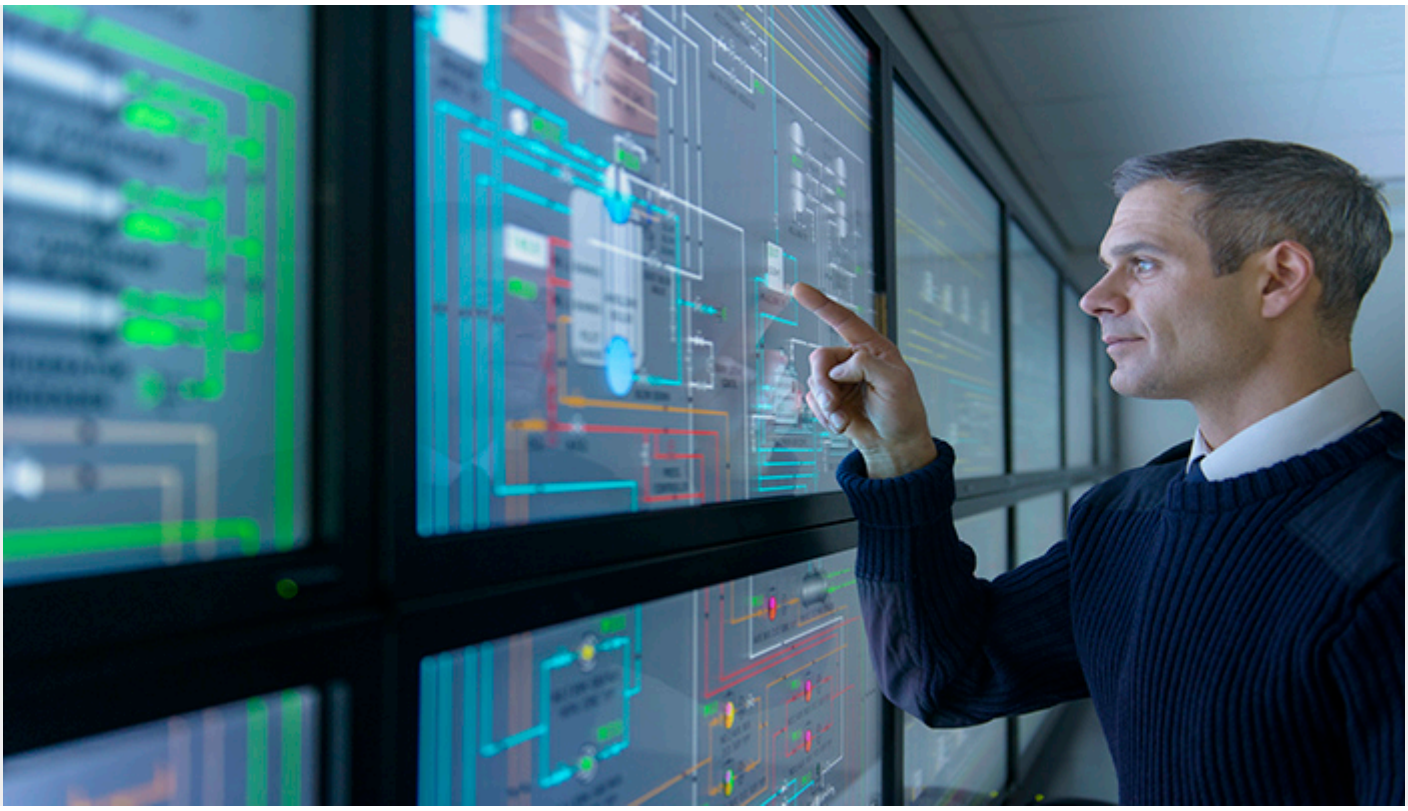
SYSTEM ADMINISTRATOR VS SECURITY ADMINISTRATOR: WHAT'S THE DIFFERENCE?



In today's economy, computer networks are crucial to nearly every single business organization, whether it's a large enterprise or a small business. As such a critical part of business – sometimes it's the product itself – computer networks require a dedicated employee or several employees to manage the day-to-day operations of the network. That's where system administrators come in.

Our reliance on computer networks is only getting stronger, so the information stored within them can be invaluable. Security administrators are employees who test, protect, and ensure the hardware, software, and, increasingly, the data within the computer networks. This security, therefore, is becoming more and more critical – especially at a time when individuals and sovereign nations threaten cybersecurity attacks.

In this article, we're talking about the roles and responsibilities of system administrators and security administrators. Though the names and jobs are similar, there are distinct differences in these IT-focused administrator roles.

Terminology

System administrator is often shortened to the buzzy title of sysadmin. More formally, some companies refer to their sysadmin as a network and computer systems administrator.

A security administrator, on the other hand, can have several names, including security specialist,

network security engineer, and information security analyst.

As always, the job title is less important than the specific roles and responsibilities that a company may expect from the position.

System Administrator

Roles & Responsibilities

As their responsibilities focus on daily network operations, system administrators are charged with a wide swath of computer work: organizing, installing, and supporting the computer systems, which can include local area networks (LANs), wide area networks (WANs), network segments, intranets, and other data communication systems. Several metrics, like uptime, performance, resources, and security, can help a sysadmin determine that the system meets the users' needs within the company's budget.

Responsibilities of a system administrator may include:

- Anticipating needs of the network and computer systems before setting it up
- Installing network hardware and software
- Ensuring and implementing upgrades and repairs in a timely manner
- Maintaining network and computer system security
- Understanding and solving problems as automated alerts occur
- Collecting data to help evaluate and optimize performance
- Adding and assigning users and network permissions, as determined by the organization
- Training users in proper use of hardware and software

Peers & Reporting

A system administrator likely reports to an IT department head.

Unlike some IT positions, sysadmins have a unique responsibility to communicate and problem solve with colleagues both within and beyond the IT team. Because a sysadmin solves problems for and trains all users, including non-IT employees, communication is imperative.

Job Requirements

Some businesses may require that a system administrator hold a BS in a computer-related field is helpful, though some companies may only require a post-secondary degree. Specific training and certifications alongside hands-on experience can strengthen a candidate's position, especially when he or she hasn't earned a BS. Common training and certifications for system administrators are offered by Microsoft and Cisco.

Beyond formal education, strong system administrators will also possess several vital skills, including analytical, communication, multitasking, and problem-solving skills.

Outlook

The U.S. Bureau of Labor Statistics (BLS) projects that the employment of system administrators will grow by 8 percent by 2024 – which is the average growth rate across all national occupations. This

projection is based on companies investing in newer technologies and, increasingly, mobile networks. The healthcare industry and businesses that turn to cloud computing are expected to lead this growth.

Security Administrator

Roles & Responsibilities

Where a system administrator knows a lot about many sectors of IT, a security administrator specializes in the security of the computers and networks.

In general, computer security, also known as IT security or cyber security, includes protecting computer systems and networks from the theft and/or damage to hardware, software, or information. It also includes preventing disruption or misdirection of these services. This should include knowledge of specific security devices, like firewalls, Bluetooth, Wi-Fi, and the internet as things. This also includes general security measures and an ability to stay abreast of new security sector developments.

Specific roles and responsibilities of a security administrator may include:

- Monitoring networks for security breaches, investing violations as occurs
- Developing and supporting organizational security standards, best practices, preventative measures, and disaster recovery plans
- Conducting penetration tests (simulating cyberattacks to find vulnerabilities before others can find them)
- Reporting on security breaches to users, as necessary, and to upper management
- Implementing and updating software to protect information
- Staying up-to-date on IT security trends and information
- Recommending security enhancements to management and C-suite executives

Peers & Reporting

Due to the necessity of network and data security, security administrators often report directly to upper management, which could be a CIO or CTO.

Security administrators frequently partner with sysadmins for implementing new changes to the network for security purposes.

Job Requirements

At a minimum, security administrators are expected to hold a BS in computer science, programming, or similar field. Some companies prefer to hire candidates that hold a MS in computer systems or an MBA in information systems.

In addition, companies frequently prefer candidates who are certified in specific security fields. A common certificate is the Certified Information Systems Security Professional. Other certificates focus on more specific areas, such as systems auditing or penetration testing.

Work skills are just as important to formal education. Candidates should be detail-oriented and analytical, as security vulnerabilities are often tiny, hard-to-notice parts of the program or network.

Problem-solving and communication skills are necessary, especially when training or helping non-IT colleagues.

Outlook

The BLS anticipates a significant growth in the security administrator role – predicting the industry will expand by 18 percent by 2024, a significant increase of 10 percentage points over the average for all jobs nationwide. As our economy relies more on hardware, software, and information, the need to protect them grows exponentially.