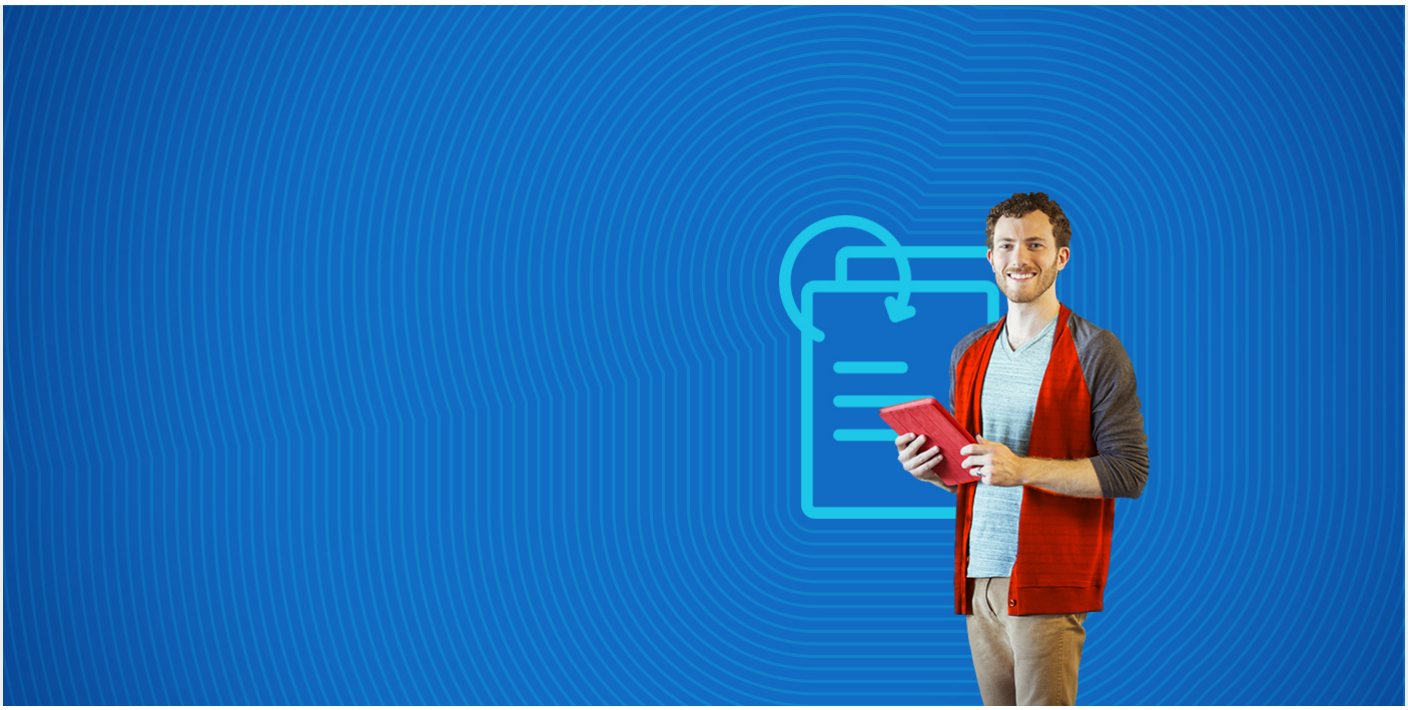
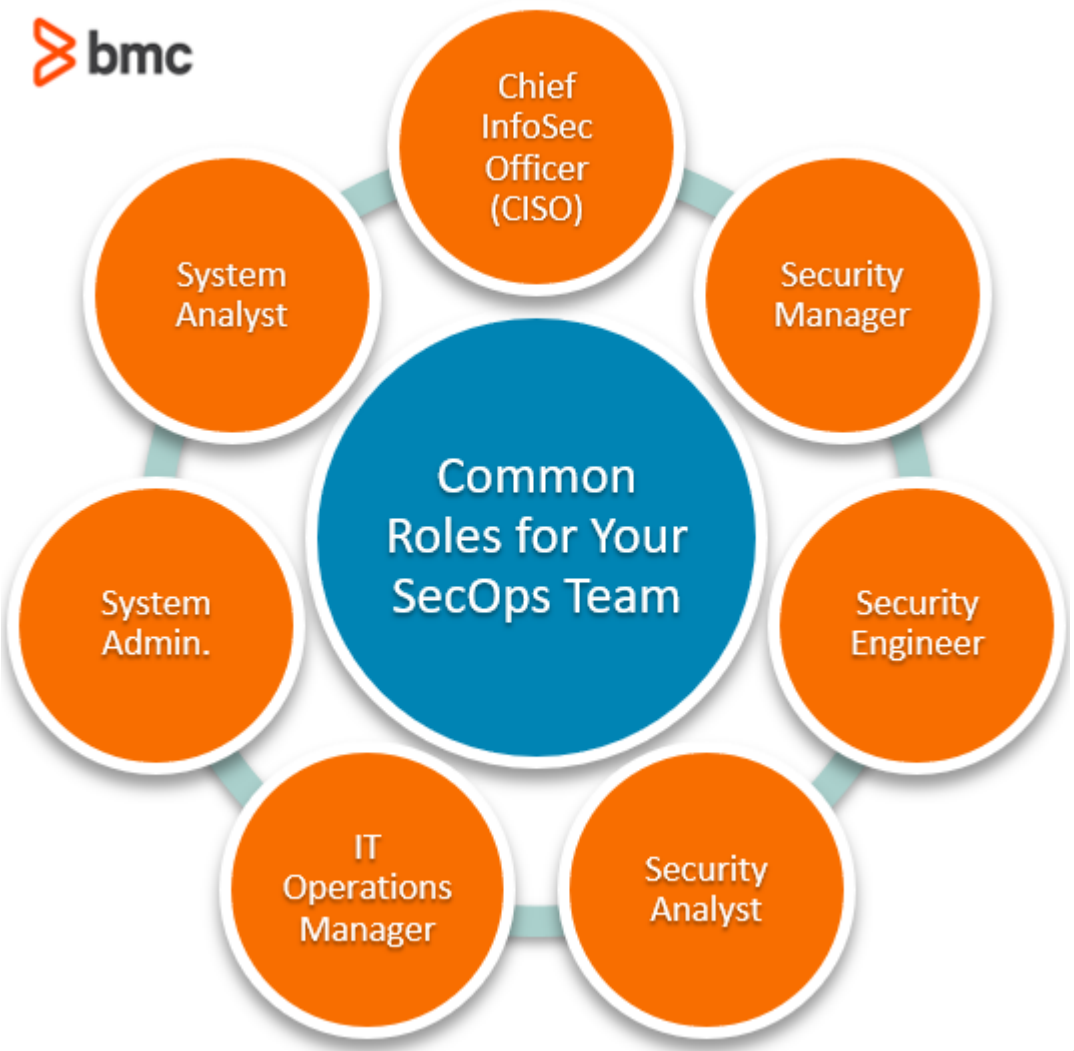
SECOPS ROLES AND RESPONSIBILITIES FOR YOUR SECOPS TEAM



SecOps, the fusion of both the security team and operations team, is no longer a far-fetched idea; in fact, it's now the norm. With companies bringing SecOps into their Security Operations Centers (SOCs), it's crucial to be able to understand the roles and responsibilities of the SecOps team.

We've put together this list of common roles you can expect to include when outlining your SecOps team, including what responsibilities each position owns. Of course, these positions will vary depending on the size of your organization and the maturity of your SecOps team.



(This article is part of our Security & Compliance Guide. Use the right-hand menu to navigate.)

Chief Information Security Officer (CISO)

One of the most crucial members of the SecOps team is the person who is responsible for defining the entire organization's security position. Whether this is the CISO or the more general Chief Information Officer (CIO), they should be the one who establishes the security strategy and policies, as well as any procedures necessary to ensure the company's infrastructure and data is protected. This role might also include compliance, which requires additional policies, strategies, and procedures.

CISO responsibilities:

- Develop the entire security strategy
- Communicate interests and activities to the C-suite
- Oversee any compliance needs
- Ensure security strategy covers prevention along with detection and response
- Deeply know and understand the threat landscape

Security Manager

No matter the official title, often the Security Manager but not always, this individual oversees the

security operations center as a whole. If your company doesn't have a dedicated SOC, then this would be the person who is responsible for managing the security team, such as the Security Director or SecOps Lead.

The security manager creates a vision for developing the technology stack, hiring new members, and building updated processes. They should have significant experience with leading a security team and be able to offer both managerial supervision and technical guidance. For companies who do not have a designated CISO, the security manager would also have the responsibilities that are typically under the CISO umbrella.

Security Manager responsibilities:

- Oversee the SOC
- Create the vision for hiring strategies, technology, and security processes
- Establish the incident response plan
- Establish a vulnerability management program
- Hire necessary security personnel
- Communicate security and technology needs to the CISO
- Analyze and optimize orchestration and automation

Security Engineer

The type and amount of security engineers or architects on your SecOps team will greatly vary, depending on the size and needs of your organization. While the most general title for this role is Security Engineer, many other titles fall under this category, including

- Security Architect
- Security Device Engineer
- SIEM Engineer
- Those who specialize in endpoint security

Security engineers are responsible for building both engineering security systems and security architecture, along with working closely with developers to ensure both the speed and continuity of releases. This role also requires the engineer to be able to define and document any protocols or procedures of the security systems they create.

Security Engineer responsibilities:

- Create, implement, and monitor all security systems
- Develop orchestration and automation between security tools
- Troubleshoot infrastructure

- Develop solutions to mitigate security vulnerabilities
- Communicate any security incidents with the team and necessary staff
- Report on evaluations and recommendations for improvement

Security Analyst

When you think of the security team, the role that probably comes to mind is that of the security analyst. Security Analysts are the ones who detect, investigate, and respond to any types of security incidents, from malware infections to full-blown breaches. They are also usually involved in the decision-making process of what preventative security measures to put into place, implementing them, and creating disaster recovery plans.

Many companies organize security analysts according to different levels according to skill level or experience, ensuring that more skilled analysts are the ones handling more complex incidents.

Security Analyst responsibilities:

- Plan preventative measures and procedures
- Create a plan for how to respond to threats
- Establish and implement security measures
- Monitor alerts
- Investigate and respond to any security incidents
- Provide training on information security and network security procedures

IT Operations Manager

An IT Operations Manager oversees the general daily activities within the IT department and maintains control over IT services and any of the connected infrastructure. They will make sure that all networks, servers, and computer systems are regularly monitored for performance issues and irregularities, and they will also assess error logs and system data to determine areas that need repaired or improved.

The IT operations manager will direct IT staff on general day-to-day tasks, including regular maintenance, workload scheduling, restoring systems should there be outages, and creating data back-ups. They will also support the end-user side of things, resolving any specific user issues that may arise and continually monitoring the performance of business-critical systems.

IT Operations Manager responsibilities:

- Manage and guide IT technicians
- Monitor IT systems and servers
- Develop department procedures and policies
- Oversee installations and upgrades
- Negotiate vendor contracts
- Resolve help desk escalations

System Administrator

System administrators, or sysadmins, are in charge of maintaining and configuring servers and computer systems, ensuring efficient, reliable operations. Sysadmins are responsible for installing

any needed software and hardware, and continuously researching the newest technologies and strategies to keep the IT business needs of the organization up to date. System administrators also actively resolve issues with servers or computer systems to limit potential disruptions.

System Administrator responsibilities:

- Install and update hardware and software
- Maintain and configure network servers and computer systems
- Integrate automation procedures and processes
- Run diagnostics and troubleshoot errors
- Lead help desk efforts
- Provide training and documentation to staff regarding new IT infrastructure

System Analysts

While system administrators usually focus on daily user performance, system analysts perform more research-based work, determining how IT systems are incorporated in the organization and how they can be optimized. They are typically at the forefront of researching emerging technologies and putting together documentation on the benefits and costs of these new systems. System analysts may also decide on the hardware and software for these new systems, overseeing the installation, configuration, and any necessary training.

System analyst responsibilities:

- Install, maintain, and troubleshoot information and computer systems
- Research innovative technologies and make recommendations for the organization
- Monitor current systems and analyze automation
- Review and backup systems regularly

Building a SecOps team

Sharing company responsibilities across teams is always beneficial, but especially so when it concerns security. When silos are broken down, processes are completed more efficiently, and teams can collaborate more effectively. By building a strong SecOps team with all of the critical team members, you will be putting your organization ahead of the game, ensuring security is never an after-thought again.

SecOps Solutions from BMC

BMC SecOps solutions enable your teams to prioritize and remediate critical vulnerabilities, and systematically address compliance violations through an integrated and automated approach across your multi-cloud environment.

Additional resources

For more on this topic, explore these resources:

- BMC Security & Compliance Blog
- Top 21 IT Security, InfoSec, & CyberSecurity Conferences of 2020

- SecOps vs DevSecOps: What's The Difference?
- SecOps in Action: How To Benefit from SecOps