THE SECOPS ENGINEER: ROLE & RESPONSIBILITIES

As the culture of SecOps continues to spread globally, the demand for experienced professionals in this field will only grow. A major role on this team is that of the SecOps engineer.

The job duties and exact descriptions of SecOps engineers will greatly vary depending on your industry, the maturity of your security operations center, and the size of your organization. At its core, though, the position of SecOps engineer is generally consistent across the board.

We've put together this guide to the SecOps Engineer role that covers:

- SecOps engineer role
- Tasks
- How to become one
- More resources

What is a SecOps engineer?

A SecOps engineer is a security professional who is responsible for securing and protecting network systems, applications, and data. In short, a SecOps engineer supports enterprise security.

A SecOps engineer can go by a number of titles:

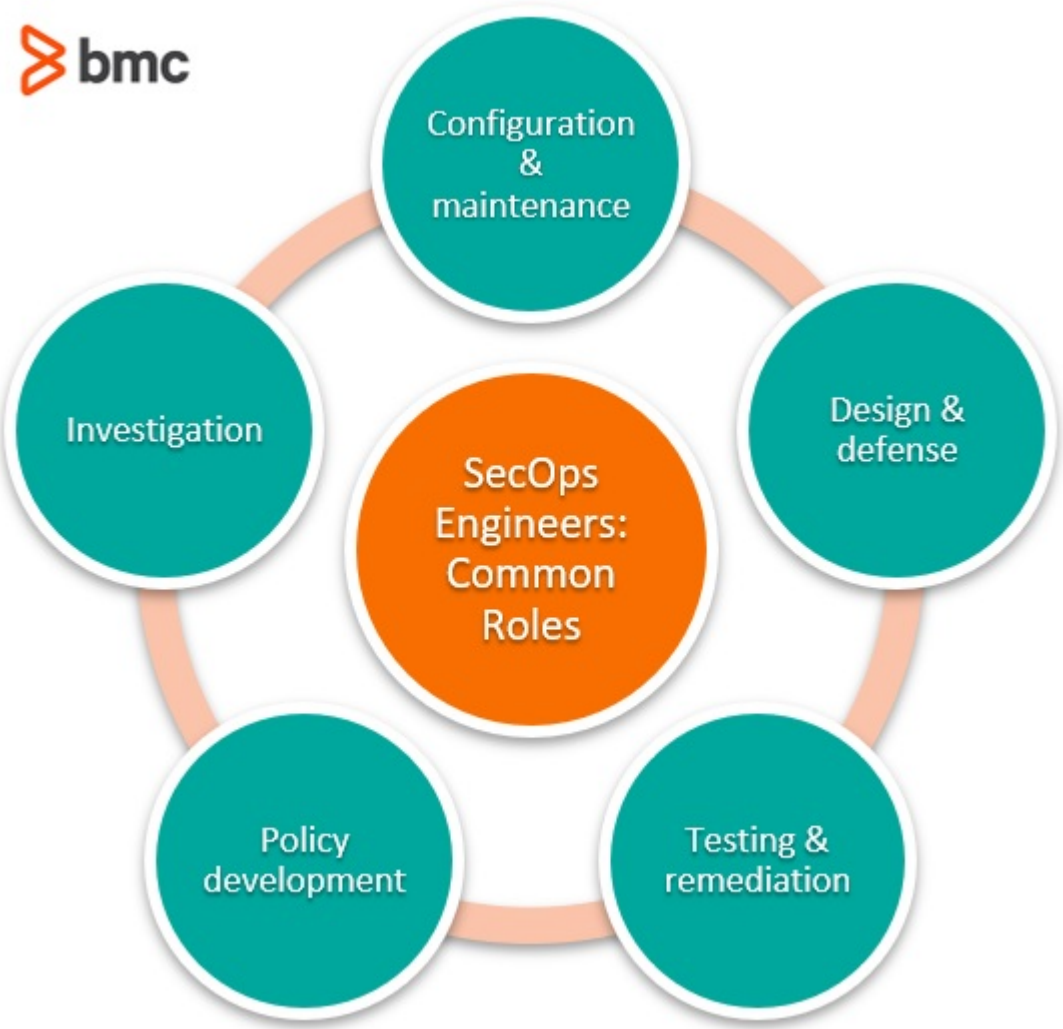
- Security Engineer
- Security Architect
- Security Device Engineer
- SIEM engineer
- Many similar titles

What does a SecOps engineer do?

Although it will vary, some essential job duties of SecOps engineers include:

- Configuration and maintenance
- Design and defense
- Testing and remediation
- Policy development
- Investigation

Let's take a look at each of these job duties.



Configuration and maintenance

Whether it be large or small, a company's computer networks include:

- Intranets
- Wide area networks
- Local area networks (LANs)

SecOps engineers help to design and build all of these different computer networks and put tools into place to secure and protect them. These systems typically require regular maintenance, so SecOps engineers must keep them working and get them back up to speed when an issue arises. Security engineers are also responsible for deploying new security software and hardware, and

regularly updating it as needed.

Design and defense

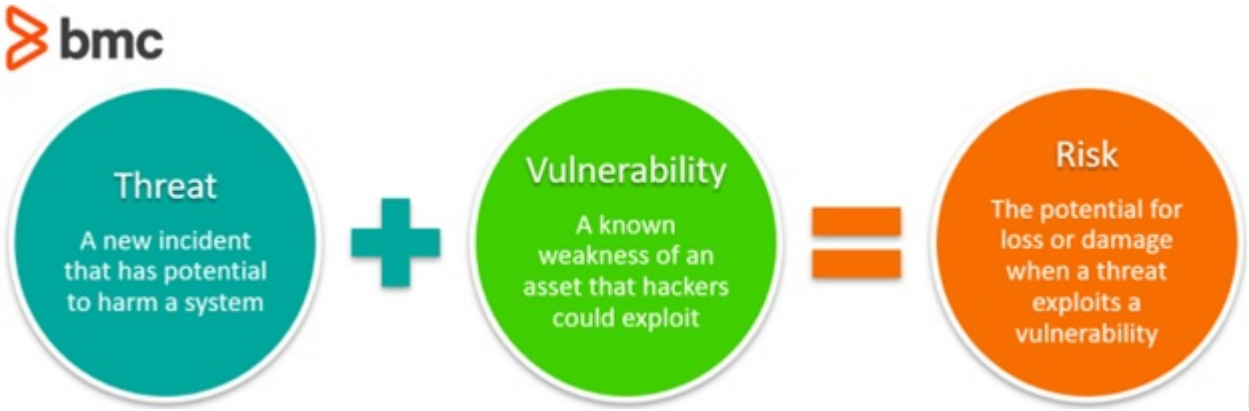
One of the biggest job duties of SecOps engineers is that of securing and protecting the network from malicious attacks. This can be completed in many ways, generally summed up in:

- Building intrusion detection systems and firewalls
- Designing security structures and tools

Given the ever-changing nature of cybersecurity threats, SecOps engineers must continuously learn about emerging technologies and security trends.

Testing and remediation

SecOps engineers are responsible for screening and testing the organization's security software for vulnerabilities, including existing systems and any new software they might obtain.



It is necessary to routinely check firewalls and data encryption technologies in order to determine when a replacement is needed. Security engineers also need a way to consistently monitor networks and systems for intrusions.

Policy development

A security operations center team is made up of many members. To ensure continuity, SecOps engineers must:

- Develop protocols that help all team members stay on top of their security needs.
- Create policies that ensure all systems follow regulatory security standards and compliance.

A SecOps engineer is likely directly involved in communicating all these plans to staff. You might even consider one-off or regular trainings.

Investigation

When a breach occurs—assume that it will—SecOps engineers must investigate to determine the root cause. As part of root cause analysis, the SecOps engineer can help write and distribute reports of their findings (known as postmortems) to share with key decision makers about how to improve security practices moving forward to prevent similar breaches.

Interested in becoming a SecOps engineer?

There are no specific guidelines or requirements that every company follows when recruiting security engineers. Still, there are a few different factors that are typically pretty standard across the board:

- A B.S. in Computer Science or similar field/experience
- A few years of experience working in information security
- Experience working with public cloud services, such as AWS, Azure, or GCP
- Expert knowledge in data structures utilized in distributed systems
- Some knowledge of security automation

There are also a variety of SecOps certifications available that can help you enhance your expertise in the industry and level the playing field. Some popular certifications include:

- CISSP: Certified Information Systems Security Professional
- CISM: Certified Information Security Manager
- CEH: Certified Ethical Hacker
- CompTIA Security+
- DSOE: DevSecOps Engineering

Reasons for certifying include learning more about your field, increasing your potential (and potential salary), and standing out among a field of candidates.

SecOps engineer roles in the enterprise

As organizations continue to enhance their security operations, the demand for talented SecOps engineers will only continue to increase. The roles and responsibilities of a SecOps engineer are crucial to the security of network systems and data.

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 security and IT roles, explore these resources:

- BMC Security & Compliance Blog
- State of SecOps in 2020
- What Does a Network Operation Center (NOC) Engineer Do?
- The Chief Information Security Officer (CISO) Role Explained
- Network Engineer vs Network Administrator: Roles & Responsibilities