SECOPS VS OPSEC: WHAT’S THE DIFFERENCE?

If there’s one thing you can be certain of when you venture out into the wide world of technology, it’s that you are going to come across acronyms. A lot of them. While deciphering and remembering them can be complicated, add in the factors of constantly evolving and changing technology and systems and you are sure to get them mixed up at times.

Two of these commonly confused IT acronyms are SecOps and OPSEC. Each is vital to organizations in their own way, but it’s necessary to understand what they are as well as why they are beneficial to business and cybersecurity as we know it. Let’s look at SecOps and OPSEC.

What is SecOps?

In a traditional business environment, IT security teams and operations teams are two separate departments who work apart from each other and focus on their own duties and priorities.

With SecOps, these two entities are combined into a single team, injecting vital security into each layer of operations and production, while automating security tasks as much as possible. This type of methodology integrates the tools, processes, and technology of both the security and operations teams, providing the capability of more secure applications.

The joint effort of this proactive team provides greater visibility into any security risks or vulnerabilities while quickly catching and resolving security issues before they become a major problem. The entire IT operations becomes more streamlined in the process, as well, with more effective deployments, less downtime, and fewer compliance failures.

Adopting SecOps in an organization might include steps such as:

- Analyzing business goals and objectives
- Obtaining company-wide buy-in for the new philosophy
- Incorporating automation
- Deployment of the SecOps process
- Ongoing monitoring and improvement

Just like with any new methodology, SecOps is not a quick process that can be performed and completed overnight. It is a gradual adoption of new philosophies and workflows that must be agreed upon and utilized by all necessary staff for it to be effective. It must also be continuously evaluated and modified in order to ensure success.

What is OPSEC?

Originally coined by the U.S. military, operations security (OPSEC) is an analytical process by which public company data is assessed and protected from adversaries.

In the internet age, OPSEC has become vital for private organizations and government agencies alike, ensuring that all confidential and critical information is protected from cyber-attackers trying to obtain data and exploit it. One of the main components of OPSEC is to observe the specific data you want to protect from the lens of a hacker, being able to search through public or unclassified data to see if there are any holes or cracks in your security perimeter.

The OPSEC process includes five steps:

1. Identify critical information
2. Determine the threat
3. Assess any vulnerabilities
4. Analyze the risk
5. Develop and apply countermeasures

1. Identify critical information

The first step in OPSEC is to identify what, if any, data or information would be disastrous if acquired by a cybercriminal. Having this data fall into the wrong hands would cause harm to your organization, hurt clients, or damage the company reputation. This sensitive information could include:

- Intellectual property
- Financial records
- Confidential client information in any capacity whether it be social security numbers, financial information, personal data, or protected health information

2. Determine the threat

The next step is to determine who your specific adversaries may be. The type of threat to your organization will greatly vary depending on your industry as well as the kind of information you are privy to, but it could include anything, such as:

- Business competitors
- Criminal hackers
- Other governments or countries.

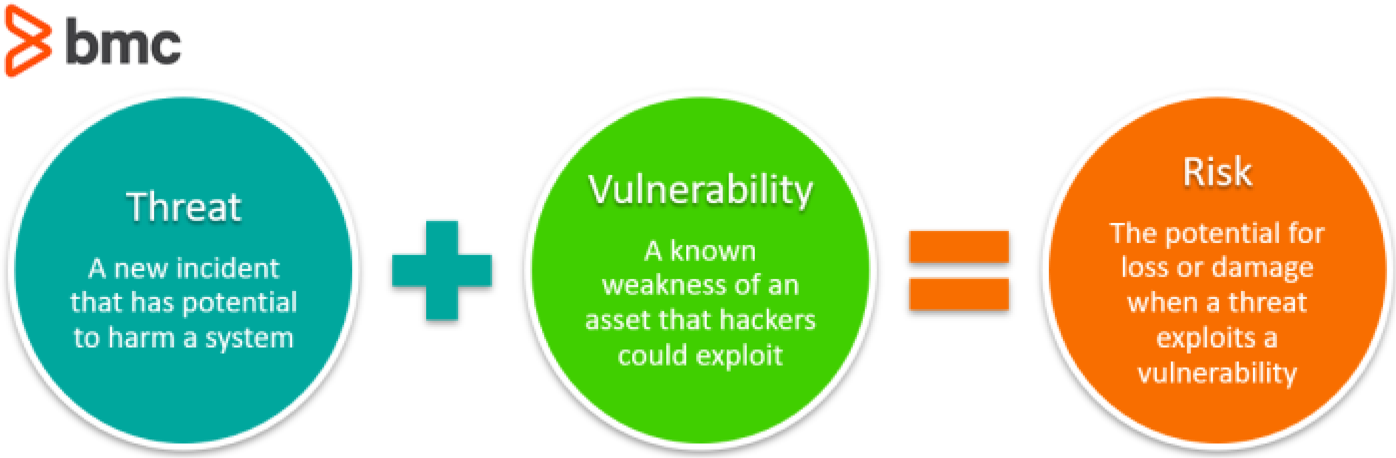
Different enemies will be targeting different data, so it's crucial to know your threats and understand what they might be looking for.

3. Assess any vulnerabilities

This third step should be considered central to any company's security posture as it is crucial to know what types of security holes might be in your infrastructure's perimeter as well as if there are any weak points. The best way to assess for vulnerabilities is through a complete security audit.

A full security audit will help you:

- Identify gaps and weaknesses in any current security practices
- Decide what measures must be taken for the future, such as:
  - Patching vulnerabilities
  - Implementing new software or better data encryption
  - Offering further security training for staff


bmc
Threat
A new incident that has potential to harm a system
Vulnerability
A known weakness of an asset that hackers could exploit
Risk
The potential for loss or damage when a threat exploits a vulnerability

4. Analyze the risk

After you know what potential vulnerabilities your system has, the next step of OPSEC is to determine the specific threat levels they pose. It is crucial to pinpoint the level of damage that could result from the weakness being exploited as well as how probably it is that it could be found in the first place. Assessing these threats provides a clear list of priorities for the organization to focus on first.

5. Develop and apply countermeasures

With important information collected and potential risks identified, it's time to create a plan for how the organization will move forward. This could include a number of activities, like:

- Updating hardware
- Developing new policies for staff regarding confidential and private data

- Adopting additional software
- Providing more security training for employees

Security for business

At the end of the day, both SecOps and OPSEC are important and necessary components to IT security in the modern business, each having their own specific benefits and functions.

No matter how you decide to incorporate these practices, they are sure to provide far more than just peace of mind; SecOps and OPSEC offer enhanced visibility, increased productivity, and of course, security. What more could you ask for in an IT acronym?

Additional resources

For more on this topic, check out the BMC Security & Compliance Blog or these articles:

- SecOps in Action: How You Can Benefit
- IT Security & Compliance Guide, with 10+ articles
- What is Security Threat Modeling?
- What is Security Orchestration, Automation, and Response (SOAR)?
- What is Security Information and Event Management (SIEM)?
- What is DevSecOps? The Role of Security in DevOps Architecture