SECOPS VS SOC: WHAT'S THE DIFFERENCE?

Security operations can look vastly different from company to company, greatly varying in size and maturity. Whether security functions are a simple incident and management device, or are full-fledged mission control centers with the highest levels of protection, each shares the same goal: to prevent, identify, and mitigate threats to the organization.

Although cybersecurity teams continue to evolve thanks to new technologies and philosophies, a few ideas have bubbled to the top here in 2020, namely SecOps and the present-day SOC. To decide if your organization should move forward with these, it's crucial to understand the differences between SecOps and SOC and how they can work together for the modern enterprise.

What is SecOps?

Security Operations (SecOps) is the seamless collaboration between IT Security and IT Operations to effectively mitigate risk. SecOps team members assume joint responsibility and ownership for any security concerns, ensuring that security is infused into the entire operations cycle.

Historically, security and operations teams often had different and conflicting business goals. Operations teams were focused on setting up systems in a way that would meet performance and uptime goals. Security teams were focused on complying with regulatory requirements, putting defenses in place, and responding to security concerns.

The downside to this model is that security was tacked on as an after-thought, sometimes even seen as a burden that slowed down operations—creating overhead. But as threats continue to increase and become more sophisticated, many organizations are recognizing that this environment of the past is no longer meeting the needs of the modern business.

By adopting SecOps, companies can inject security into the entire operations process, starting at the very beginning. Approaching security from square one ensures that you're meeting requirements and designing systems with security in mind. This "shift left" allows security to work cohesively in setting up a system. It also challenges operations team members to adjust how they create and develop.

What is SOC?

A Security Operations Center (SOC) is a group of security professionals working together to:

- Proactively identify and mitigate security risks against the enterprise
- Defend against any security breaches

In the past, this SOC was actually a physical facility with huge cyber protections. Inside an SOC, staff would monitor security stats and alerts. Although your SOC might be more virtual these days, the roles and responsibilities of the SOC have not changed.

For SOCs that are following best practices, some of their expected responsibilities include:

- Enforcing compliance
- Penetration testing
- Architecture planning
- Vulnerability testing
- Threat intelligence
- Analyzing log and event data
- Identifying and responding to incidents
- Identity and access management
- Key management
- Firewall administration
- Endpoint management

It's not hard to imagine how these teams might be feeling overloaded, with mounting pressure caused by data overload, skills shortages, and increasing remote teams and security concerns. However, by incorporating some modern methodologies, security teams can share the responsibility

with other members of the enterprise, enhancing their capabilities of proactively catching risks and mitigating threats.

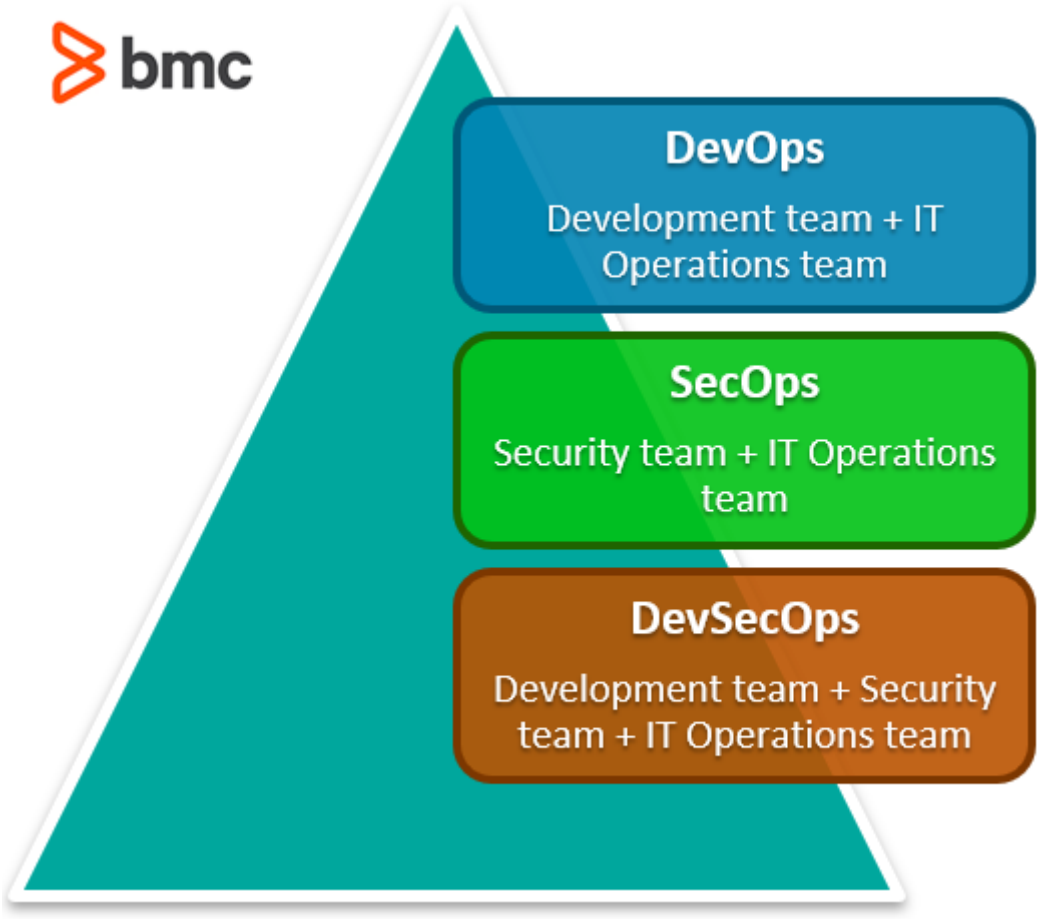
Integrating SecOps into the SOC

SecOps itself is a set of SOC processes, tools, and practices that helps enterprises meet their security goals more successfully and efficiently. However, the classic SOC is not compatible with the SecOps culture. In the past, the SOC would be completely isolated from the rest of the organization, performing their specific duties without much interaction with other parts of the business.

In today's culture, many decision makers understand that this is no longer beneficial. Today, security must be a joint effort. It is crucial for organizations to embrace the idea of the modern SOC: one that promotes collaboration and communication between the operations and the security teams.

There are a variety of ways that the SOC can begin to integrate its processes with both IT and development:

- **Distribute the SOC.** Start by taking security out of its silo and spreading out responsibilities among departments, specifically operations and security. (You can also incorporate the SOC into DevSecOps.)
- **Create a security COE (center of excellence).** Combine the SOC with select members from the dev and operations teams to ensure that security best practices are being understood and implemented
- **Establish a culture of collaboration.** Open the SOC to any staff member whose duties have a security impact, providing a simple way for workers to meet with and consult the organization's most advanced security experts on issues



SecOps and DevSecOps offer ways to embed security in the entire product lifecycle

SOC and SecOps

2020 is the year of SecOps. If you haven't already added it to your SOC, it's time to do so.

With more employees working remotely than ever before, and security operations already spread out, now is as good a time as ever to adopt the collaborative culture of SecOps, ensuring your SOC is up-to-date and ahead of the latest security threats.

SecOps 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. For more on this topic, explore our BMC Security & Compliance Blog and these articles:

- SecOps in Action: How To Benefit from SecOps
- SecOps vs OPSEC: What's The Difference?
- What is Security Threat Modeling?
- What is DevSecOps? The Role of Security in DevOps Architecture