SECOPS TRENDS OF 2021

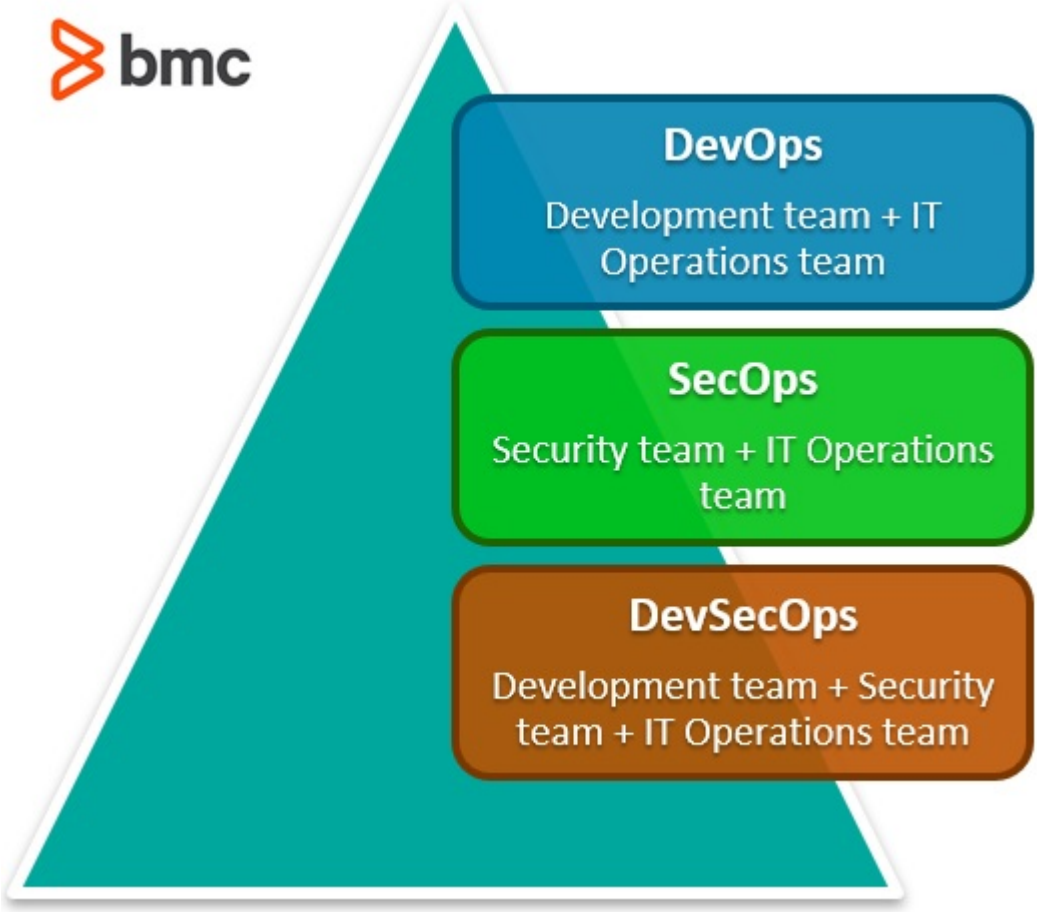
Rewind to just a couple years ago, when all you heard about was DevOps, the concept of combining the development team with the operations team. The idea behind this new culture was simple: developers would help take responsibility for putting things into production, breaking down silos, and enhancing collaboration. There was one thing missing from DevOps though—it didn't factor in security.

This is where SecOps comes in.

Given the success that companies who have added SecOps to their Security Operations Center (SOC) have already seen, it's no wonder so many other enterprises are following suit, making it one of the major IT trends of 2020. With this in mind, we have put together some of the latest findings in current SecOps trends.

SecOps in the enterprise

Similar to the core concept of DevOps, collaboration between teams is central to the SecOps methodology, fusing together the security and operations teams. With this joint effort, security is no longer added as an afterthought, but rather injected into the entire lifecycle. (A third iteration, DevSecOps combines all three teams.)



Although this new concept might appear to be fairly straightforward, there are many obstacles that teams face when they decide to switch to the SecOps methodology. Further, practitioners are facing extreme challenges as cybersecurity becomes more complex.

Current state of SecOps

Sumo Logic, leader in cloud-based machine data analytics, recently released its findings from a global survey of trends and findings of SecOps in 2020. The 2020 State of SecOps and Automation study illustrates some common themes, challenges, and solutions that a majority of organizations are facing when it comes to security in their industries.

"Today's security operations teams are faced with constant threats of security breaches that can lead to severe fallout including losing customers, diminished brand reputation, and reduced revenue. To effectively minimize risk and bridge the gap, many companies rely on automated solutions that provide real-time analysis of security alerts," said Diane Hagglund, principal for Dimensional Research. "These findings highlight the challenges SOC teams are facing in a cloud-centric world, but more importantly why enterprises are aggressively looking to cloud-native alternatives for security analytics and operations."

Some of the top themes that played out in this survey, along with other research revealed by top security experts, are that SecOps needs to focus on:

- Automation
- Prioritization
- Aggregation

Let's take a look.

Enhancing automation

One of the major topics discussed in the report was automation. While steps towards automating security systems have increased over the years, the sheer volume of alerts that SecOps teams receive on a daily basis is simply becoming too much to handle:

- 93% of security teams reported that they cannot address all of their security alerts each day.
- 31% of the security pros said they can barely get to half of their alerts in the same day.

Obviously, this leads to major concerns when dealing with potentially devastating security threats, when the damage caused by even one missed breach could be catastrophic.

"The modern SOC needs tools to automate responses and cut down the amount of manual investigation time that ends up looking into false positives," said Gil Shulman, vice president of products at Illusive Networks.

For organizations that have a mature SOC, this looks like:

- Tier 1 analysts find themselves spending about 20 minutes per incident evaluating threat data, with up to 25 of these incidents per day.
- Tier 2 analysts spend between 60-80 minutes per day triaging and investigating alerts with about six of these per day.

"This leaves essentially no time for any other activity, with a significant portion of those workdays devoted to incidents that turn out to be false positives," Shulman continued. "Decreasing time wasted on ticket enrichment will allow analysts to perform to their strengths and provide a much more satisfying job experience for them."

There are a variety of cloud-native solutions available that address these challenges by automating

manual processes and freeing up analysts' valuable time for more complex matters. Companies can utilize technologies for improved automation., such as:

- UEBA
- SOAR tools (Security orchestration, automation, and response)
- AI and machine learning

Prioritizing alerts

Once teams take major strides toward efficient automation, the next big trend in SecOps is to find ways to prioritize the alerts and threats that are being received. According to the report, 70% of companies stated that the number of security alerts they receive on a daily basis has doubled, if not more, over the past five years.

"Enterprises are arguably dealing with more data today than ever before, and the pain security operations teams are feeling is significant. There's never been a more important time to ensure IT security operations are up to par," said Greg Martin, general manager for the security business unit at Sumo Logic. "Companies need to adopt solutions that let them quickly identify, prioritize and respond to only the most critical warning signals, so that they're not left drowning in alert overload with no direction."

Given the overwhelming amount of alerts, and the associated alert fatigue, companies must begin seeking tools immediately that can triage and prioritize alerts and flag those that need immediate attention. Finding innovative SIEM solutions that can monitor and correlate threats for on-premise and cloud environments will greatly benefit SecOps teams and ensure they find the most harmful threats first.

Security tool aggregation

Another major SecOps trend and focus is that of the aggregation and integration of security tools. According to a recent report released by Panaseer, responding organizations are on average running 57 separate security tools. 57!

Even more alarming? Over a quarter of the respondents claimed to be using more than 75 different security products.

Although the idea behind these numerous tools is to make the organization safer, running this many services quickly overwhelms, leaving larger blind spots than what they began with. And when it comes to security tool sprawl, redundancy makes you weaker, not stronger.

"There have been a lot of research studies that find the whole issue of interoperability and scalability is largely ignored, so as a result the technologies don't actually work together and you have more than you need," said Dr. Larry Ponemon, president of the Ponemon Institute. "So many things are generating reports ... you are in a state of information overload pretty quickly."

Security vendors must recognize that they need to decrease the number of tools available, ensuring they are integrated and have fewer platforms for customers to navigate. By reducing and prioritizing services, customers will have to work with fewer interfaces, resulting in more efficient processes and improved workflows.

SecOps trends

Although 2020 might be the year of SecOps, many organizations still have a long way to go before their methods reach peak efficiency. Understanding some of the current SecOps trends, as well as the challenges, will allow enterprises to continue to enhance their security postures and teams.

Additional resources

For more on this and related topics, explore these resources:

- BMC Security & Compliance Blog
- SecOps Roles and Responsibilities for Your SecOps Team
- SecOps vs SOC: What's The Difference?
- DevOps Trends: How Industry Changes Affect DevOps Teams