WHAT IS SECOPS AND HOW CAN YOU MAXIMIZE ITS POTENTIAL?

"SecOps" is the intersection of Security and Operations teams within an IT organization. Often there is a divide between these two groups called the "SecOps Gap", and it is more important than ever to reduce this gap to effectively fend off security threats. This post, the first in a two-part series, examines the SecOps gap, and how automated solutions can help close it and protect against security attacks.

What is the SecOps Gap?

In the past year alone, 56 percent of organizations reported a major security breach, and in 2019 total losses from cyber attacks are expected to exceed $2 trillion. In order to keep the barbarians at the gates, it has become more important than ever for security and operations to work closely together, and be armed with the most effective weapons to fight off attackers.

Unfortunately, there has been a long-standing, "SecOps" gap between security and operations teams. This gap exists because these groups have different priorities and objectives. For security teams, the focus is on preventing breaches and keeping sensitive data secure, whether it's housed internally or externally. On the other hand, operations teams are tasked with priorities like maximizing application and system uptime, keeping internal and external customers happy, and maintaining currency with the latest security patches and upgrades. This SecOps gap must be closed in order to maximize the effectivenss of security defenses.

To illustrate why, consider the way vulnerability scanning efforts work in many enterprises. A security team will be running vulnerability scanners that generate massive volumes of data. Typically, the data produced by these scanners is raw and difficult to parse.

These massive, raw data sets will be tossed over the fence to the operations staff members. These folks are then tasked with the effort of sifting through all this information, determining which specific servers have vulnerabilities, which services are affected, and prioritizing remediation efforts, which typically either require deploying a patch or making a configuration change.

Operations teams are never done, and it's virtually impossible for them to keep pace. Scanner data continues to pour in every time a new scan is complete. New reports come faster than vulnerabilities from previous reports can be closed out. Ultimately, many vulnerabilities are left unaddressed.

In addition to struggling to keep pace with vulnerability scanner data, additional challenges plague many teams:

- **Tasks are extremely labor intensive.** Tasks like patching require a lot of manual steps, such as sending emails, downloading files, determining how to work within maintenance windows, avoiding service disruptions and rollbacks, updating records (for example, the configuration management database), and so on.
- **Approvals are a big time sink.** Staff have to chase down approvers to get them to authorize changes. They also have to field a lot of questions, for example about the need, nature, and timing of changes. This ultimately leads to wasted time for a lot of people across the organization.
- **Reporting can be a headache.** Teams have to consolidate reporting information from various spreadsheets and other sources. They are constantly chasing open questions and loose ends. Was a patch successfully deployed? How many servers remain vulnerable?
- **Diverse environments increase operational complexity.** Today, it's common for an organization to be relying on a highly diverse range of services and platforms, including legacy on-premises infrastructure, multiple cloud service providers, microservices-based platforms, and more. Given all this diversity, teams have to contend with complexity that makes it difficult, time consuming, and labor intensive to maintain systems.

Compounding matters is that help is in short supply. Historically, security and operations have been resource constrained, often due to budgetary limitations. Now, those challenges are more pronounced, particularly in security, where experts are in high demand, but short supply. According to one report, there will be 3.5 million unfilled security jobs by 2021.

Not surprisingly, given the cumbersome processes and lack of collaboration, it's not uncommon for there to be points of contention among groups. One survey reported that 56 percent of respondents said there were tensions between operations and security.

Given all these obstacles, ongoing operation and administration is time consuming and costly, and inhibits business agility. Further, it means security vulnerabilities aren't addressed quickly enough—if they're handled at all.

How to Close the Gap: SecOps Solution Requirements

To contend with the challenges they're facing, security and operations teams need to adopt a new approach. They need to establish common processes and use integrated tools that enable

improved teamwork and efficiency.

Automation is an integral aspect to these efforts, offering a way for security and operations to streamline and accelerate many of their ongoing tasks. This includes capabilities for automated management of security vulnerabilities in servers and networking devices (routers, switches, load balancers, firewalls, IDS/IPS). Automation saves labor, and allows skilled resources to shift from maintenance to innovation, which can ultimately fuel competitive advantage and differentiation for the business.

In addition, to succeed long term, comprehensive solutions that integrate discovery with server automation and network automation are a necessity. With these capabilities, teams can gain improved visibility into the devices that need to be managed and eliminate blind spots, such as misconfigured servers that were missed by the latest vulnerability scan.

Conclusion

To keep pace with evolving threats and demands, security and operations teams simply can't continue to struggle with cumbersome workflows and siloed tools. Through combining advanced discovery with automation capabilities, Security and Operations teams can begin to establish true SecOps collaboration that fuels enhanced efficiency and security. In our next post , we'll look in more detail at specific vulnerabilities and how to address them.