How SecOps Can Benefit Your Agency

Industry
Perspective

bmc

Executive Summary

FBI Director James Comey said, "There are two kinds of big companies in the United States. There are those who've been hacked…and those who don't know they've been hacked."

If the private sector is under attack by hackers, should we also assume the federal government is as well? Managing a seamless and secure federal IT enterprise is no small feat in today's complex environment. Consider all of the systems and applications your agency uses to meet daily demands from internal and external customers. At the same time, agencies must defend against the constant barrage of cyberthreats aimed at disrupting those systems.

Behind the scenes, your agency's operations team is working diligently to keep these systems running and functional for the hundreds or thousands of people who depend on them. Equally important is the security team that must ensure the same systems are secure, up to date and compliant with federal standards.

Managing the balance between security and system performance is a high stakes battleground that operations and security teams must navigate carefully. Building consensus between these groups can be challenging, with one team focused strictly on security, while the other wants to ensure uptime and high performance for existing or new services. These competing priorities and lack of integration between security and operations can create gaps in the security posture that leaves agencies susceptible to increased risk and cyberattacks.

Security breaches in the federal government have potentially catastrophic consequences and must be blocked, but the two primary teams responsible for blocking them – security and operations – have different priorities, timelines, and objectives. In recognition of this challenge, agencies are investing in a new management approach known as SecOps to bridge the gap between security and operations teams and ensure that systems stay up and running, and secure all at the same time. SecOps links the security and operations teams together to work with shared accountability, processes and tools to ensure that agencies do not have to sacrifice security to maintain a commitment to agility. They can meet new service delivery models that enable an agency to move faster with a highly automated, coordinated, and secure approach to enable continuous innovation.

GovLoop partnered with experts at BMC to help agencies understand what this new paradigm offers and how it differs from government's traditional approach to security and operations. In this report, you'll glean insights from BMC's AJ LaForty, Senior Solutions Consultant; Michael Alonso, Principal Solutions Consultant; and Dejan Zdravkov, Federal Sales Executive, on what SecOps means for your agency.

But first, let's begin with an overview of current security and operations practices in government.

Government's Approach to Security and Operations

2 teams, 2 missions.

As the name implies, the security team oversees security to prevent hackers and malicious insiders from accessing sensitive government data and systems. This team is also charged with ensuring all IT systems follow federally mandated policies and compliance standards. Given their metrics and mission, their job stops at the level of identifying the threat, vulnerability or deficiency. They do not own the operational implementation of the changes to remediate or fix the issues – that role lies within the operations team. Part of the responsibility of the operations team is to carry out any corrective actions, such as patching, and ensure that any vulnerabilities are mitigated in a timely manner.

The operations team includes the people who run applications that are consumed by internal or external end users. They are responsible for maintaining uptime, stability and performance for current systems and for deploying new services, such as software code and features.

For operations personnel, much of their time is focused on keeping systems up and running, especially during high-peak times like open-enrollment season for Centers for Medicare and Medicaid Services, or tax season for the IRS.

"They're trying to ensure security and compliance tasks don't interfere with the systems operations," Zdravkov explained. "Since the primary mission of operations is to ensure uptime and stability, and not provide security, the security updates are frequently delayed or even tabled altogether. This situation can create a window of risk, or an attack surface, for hackers to exploit vulnerabilities in those systems."

Exacerbating the issue is the fact that, according to a WhiteHat Website Security Statistics Report, it takes an average of 193 days from the time an agency is aware of a vulnerability to the time it's remediated with a patch or other action, even when the systems aren't on lockdown.

Something else also contributes to this problem: interactions between security and operations teams are largely manual. When the security team runs automated scans of the IT environment for compliance issues, the results are often shared with the operations team via massive paper spreadsheets with thousands of lines of data. The information isn't prioritized, and often the data is provided to the operations team without the full context of the information. From there, the team must identify what issues need to be addressed, which is another manual process. Those updates are then scheduled into the production cycle and implemented. That process takes time, and again, it's highly manual.

A big part of why this process is so fragmented, manual, and disjointed is because security and operations teams may at times seem to speak two different languages with little understanding of one another's perspectives. A report by BMC and Forbes found that 60 percent of the 304 C-level executives who responded to the survey said that security and operations did not understand each other's requirements.

What if there were a way to break down the silos and reduce the burden of manual processes between these two teams? Through the power of SecOps automation, there is. The next sections explore what SecOps is and how agencies can benefit from it.

SECURITY TEAM

oversees security to prevent hackers and malicious insiders from accessing sensitive government data and systems.

OPERATIONS TEAM

responsible for maintaining uptime, stability and performance for current systems and for deploying new services.

What Is SecOps?

Think of SecOps as a management approach that bridges the gap to connect security and operations teams, in much the same way that DevOps unifies software developers and operations professionals.

SecOps links the security and operations teams together to work with shared accountability, processes and tools to ensure that agencies do not have to sacrifice security to maintain a commitment to uptime and performance.

This is certainly a cultural shift for many agencies, and one that requires them to first address the conflicting priorities between security and operations teams, according to BMC. IT Leaders need to step in and demonstrate that they are all accountable for ensuring the agency and its customers are protected.

When SecOps methods are embraced, security employees can no longer simply hand off results from a vulnerability scan to operations team members and think their work is done. The goal is to keep both teams engaged in the process and provide visibility into what changes need to be made and the possible impact of those changes to other parts of the business.

When these teams don't have an effective way to transfer and consume information, agencies can struggle to quickly remediate vulnerabilities. On average, it takes 193 days from the time an agency is aware of a vulnerability to the time it's fixed. Another chilling statistic is that 99.9 percent of vulnerabilities exploited have had a published CVE (Common Vulnerabilities Exposure) for over a year. Rob Joyce, Chief of Tailored Access Operations at NSA said, "There's so many more vectors that are easier, less risky and quite often more productive than [zero day excursions]. This includes, of course, known vulnerabilities for which a patch is available but the owner hasn't installed it."

BMC's aim is to help agencies confidently build a strong security posture by facilitating more effective communication between security and operations, so they can quickly and accurately prioritize and remediate threats. A strong SecOps solution transforms disconnected initiatives into a single, unified, secure, and comprehensive process that accelerates vulnerability resolution, controls the cost of remediation and mitigates risk.

This capability will enable security and operations teams to become more agile and move to a proactive security position for both cloud and on-premise systems. It will also allow the teams to more readily embrace key business initiatives related to managing the impact of digital transformation, the Internet of Things, and continuous delivery of services. These are vital to the performance of the agency but create significant security concerns if they are not managed with rigorous and adaptable controls.

Centralized management solutions can help facilitate coordination and collaboration between security and operations teams. According to the BMC/Forbes study, 60 percent of the respondents reported that they want tools for automating corrective actions and 59 percent want a centralized view into vulnerabilities and remediation actions.

SecOps empowers agencies to take a comprehensive and proactive approach to security issues rather than a reactive approach. Agencies can manage by policy and automatically address security issues to protect their agencies.

Key tenets of the BMC SecOps solution include:

AGILE EXECUTION TO MEET BUSINESS OBJECTIVES:

Automate the integration of security and operations data to accelerate remediation of vulnerabilities while driving operational excellence.

INTEGRATED VISIBILITY FOR HOLISTIC VIEW OF ENVIRONMENTS:

Collaboration between security and operations fueled by integrated and holistic visibility into risks, impacts, & operational plans.

RIGOROUS CONTROLS TO PROTECT CUSTOMERS:

Security and operations work collaboratively to support rigorous and vigilant controls while tools absorb some of the complexity so that agencies can get back to the fundamental services they deliver.

SecOps Solutions Reduce Manual Burdens

Today, network and systems administrators and IT staff are stretched thin and manual tasks consume key cycles and drive up costs. Automation technologies can help agencies reduce that burden.

"By using our tools and automating some of those manual tasks, like keeping the lights on, what used to take up to 80 percent of an IT staffer's time, is now just 20 percent," Zdravkov said. "As a result, the staffers can focus on more strategic and innovative projects."

For one BMC customer, it would have taken the agency about 17,000 hours to manually audit some 2,000 servers for compliance. This time estimate did not even entail fixing security issues or applying patches. It was only based on the time required for checking to understand if its systems met compliance standards.

"That's obviously not an option because they would need to hire a lot of systems administrators and the funding is not there," Zdravkov said. "That's one of the biggest challenges that we're addressing — the limitation of resources and funding in the federal government. Automation is the only way to get the job done, and there's where we come in."

One of BMC's customers at the Defense Department used to spend 15 hours applying patches to a Windows-based system. Now, using BMC's solutions, that number has decreased drastically to just 15 minutes.

"The good news is there isn't necessarily a steep learning curve for agencies that adopt BMC's SecOps tools," LaForty said. "Professionals who work in security and operations can be proficient in using the software solution within weeks. Users already understand how to apply patches and enforce configuration management prior to using the tool, and we're automating many of the things that they're already doing today." BMC also provides agencies with user-friendly dashboards and interfaces that make it easier for them to visualize security issues and quickly address those vulnerabilities.

"Something as simple as generating a report and getting people communicating is helping secure the environments because those groups weren't always in synch before," Alonso said. "Now that security and operations are more closely linked to communicate with each other, they have the ability to work together more effectively and secure the agency."

The next section reviews some of the key benefits that make BMC's SecOps solutions a game-changer for agencies.

> **"By using BMC tools and automating some of those manual tasks, like keeping the lights on, what used to take up to 80 percent of an IT staffer's time, is now just 20 percent. As a result, the staffers can focus on more strategic and innovative projects."**
>
> Dejan Zdravkov, Federal Sales Executive, BMC

How SecOps Can Benefit Your Agency

Government agencies can no longer afford to continue business as usual when it comes to executing security and operations missions because they fall victim to gaps in security. These gaps can leave them susceptible to increased risk.

The combination of increasing cyber threats and limited funding is forcing agencies to invest in solutions and management practices that will empower them to better secure IT systems with modest resources.

That's where SecOps comes in. This comprehensive approach to security and operations enables agencies to proactively respond to vulnerabilities and quickly remediate them. Highlighted here are some of the key benefits agencies are reaping from SecOps tools.

You become proactive versus reactive.

Many agencies are reactive in their approach to delivering security patches and compliance and configuration management across the agency because they lack a SecOps solution. Using SecOps, they can adopt a proactive approach that enables them to ensure tasks are done quickly, properly and in an automated manner. The ultimate goal is to remediate vulnerabilities and prevent data breaches. SecOps empowers IT professionals to do the innovative jobs they were meant to do, rather than spending time manually auditing and fixing individual machines, routers and switches.

You know your security status at all times.

Most agencies are required to scan their IT environments once a week and report on their security status once a month. But with an automated solution, you know your security status 24 hours a day, seven days a week because the scans are continuous. There are dashboards that help agencies to consume and prioritize the data. "If you're just following the letter of the law and scanning once a week, there are six other days of the week that you don't know what's going on inside your system," Alonso said. "That is a security awareness gap." By using an automated tool, agencies can identify and close those gaps.

You become more agile and responsive to security issues in the cloud and on-premise.

BMC's SecOps tools do not differentiate between private clouds in government data centers and public clouds in third-party facilities. "We manage the security from a simple platform that allows you to do security in the same fashion that you would for on-premise solutions or in a public cloud," LaForty said. That way, you can ensure everything is set up properly and aligned with compliance standards.

"It really doesn't matter if the system is running in a public or private cloud," LaForty said. "They should still technically be hardened and secured in the same fashion. As long as you can talk to the system, you can assure the compliance and security of that system."

Conclusion

The real value of SecOps is the opportunity it provides agencies to move beyond manual compliance exercises and embrace SecOps to maintain a posture of audit readiness all the time, foster collaborative decision-making between security and operations teams and swiftly close windows of risk reducing the attack surface.

For too long, silos between the operations and security teams have not only bogged down agency processes but also created gaps in security. These gaps in remediation leave IT systems and data vulnerable to hackers and malicious insiders. Defending against these types of attacks has become increasingly challenging as the threats grow more advanced and persistent.

Agencies cannot keep pace with these threats using manual efforts to check the security of their IT assets, install security patches, and quickly remediate any deficiencies that could make them susceptible to an attack.

That's why a growing number of agencies are embracing the benefits that SecOps can offer. Through partnerships with BMC, agencies have reduced the time they spend fixing known vulnerabilities, completed more frequent audits in less time and reduced their security risks. The tools are also easy to use.

> **Not everybody has 20 years of SecOps experience protecting the IT environment. That's why we bring a SecOps solution to our government customers that is easy to use and helps to ensure security and compliance while meeting the needs of operations teams and the people that agencies support."**
>
> Michael Alonso, Principal Solutions Consultant, BMC

About BMC

BMC is a global leader in software solutions that help IT transform traditional business sin to digital enterprises for the ultimate competitive advantage. Our Digital enterprise Management set of IT solutions is designed to make digital business fast, seamless, and optimized. From mainframe to mobile to cloud and beyond, we pair high-speed digital innovation with robust IT industrialization —allowing our customers to provide intuitive user experiences with optimized performance, cost compliance and productivity. BMC solutions serve more than 15,000 customers worldwide including 82 percent of the Fortune 500.

About GovLoop

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 250,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please email us at: info@govloop.com

www.govloop.com | @GovLoop

govloop

1152 15th St NW, Suite 800
Washington, DC 20005

Phone: (202) 407-7421 Fax: (202) 407-7501

www.govloop.com | @GovLoop