bmc

Technical White Paper

# SecOps Response Service and Microsoft SCCM

Better together for improved analytics, reporting, and planning

# Table of Contents

# Executive Summary

The greatest challenge in improving the state of vulnerability management today is not vulnerability scanning: most vulnerabilities are known, with relatively high confidence. It's also not that you can't remediate the vulnerabilities effectively when you apply an extraordinary level of effort, either. For example, whenever a virus or ransomware exploit is sufficiently successful that it makes the front page of the Wall Street Journal, Slashdot, or Reddit, organizations rapidly call up a small army from within the ranks of IT to push fixes to every known corner of the enterprise. They're like the CDC or WHO doctors rushing to address an epidemic: effective, but expensive.

The key challenge is in closing the gap between efforts in security and operations: making the output of the security team's vulnerability assessment effort actionable and making the IT operations remediation process for those vulnerabilities faster, more effective, and more efficient.

Closing this gap is important to improving vulnerability management for organizations that rely on Microsoft System Center Configuration Manager (SCCM), a popular systems management suite for managing large groups of Windows servers and workstations. However, SCCM has some limitations related to vulnerability management that can make patching labor intensive and stressful. Today, SCCM is most often used only with the most recent patches. It is commonly used in ways that miss servers that are offline or being serviced. Fortunately, BMC SecOps Response Service helps by offering better analytics, planning, and reporting to improve protection and make SCCM more powerful.

**Read on to learn more about:**

- Why the SecOps gap can leave organizations more vulnerable and how to close that gap
- How to have fewer security-related emergencies
- How SecOps Response Service provides the visibility, analytics, and planning to help configuration management systems, such as SCCM, reduce the effort, time, and risk associated with vulnerability management

SecOps Response Service integrates seamlessly with Microsoft SCCM.

## THE SECURITY/IT OPERATIONS GAP AND COMPETING MISSIONS

Every organization has responsibilities to address security vulnerabilities and patch and configure production systems. They may collect, process, or store critical data about customers, patients, payment cards, or defense-related information. As a part of a comprehensive information security program, most IT operations teams must regularly apply security patches and configurations to systems.

However, there's a significant internal conflict here: the IT operations team's usual first mission is to maintain the highest possible availability of the systems they manage. Balanced with that mission is the requirement to also close vulnerabilities by applying security-related patches or configurations, which require brief outages, usually during agreed maintenance windows. Because those maintenance windows are so limited, patching gets delayed, and organizations leave themselves open to breaches.

### Patching and Configuration Management Hygiene

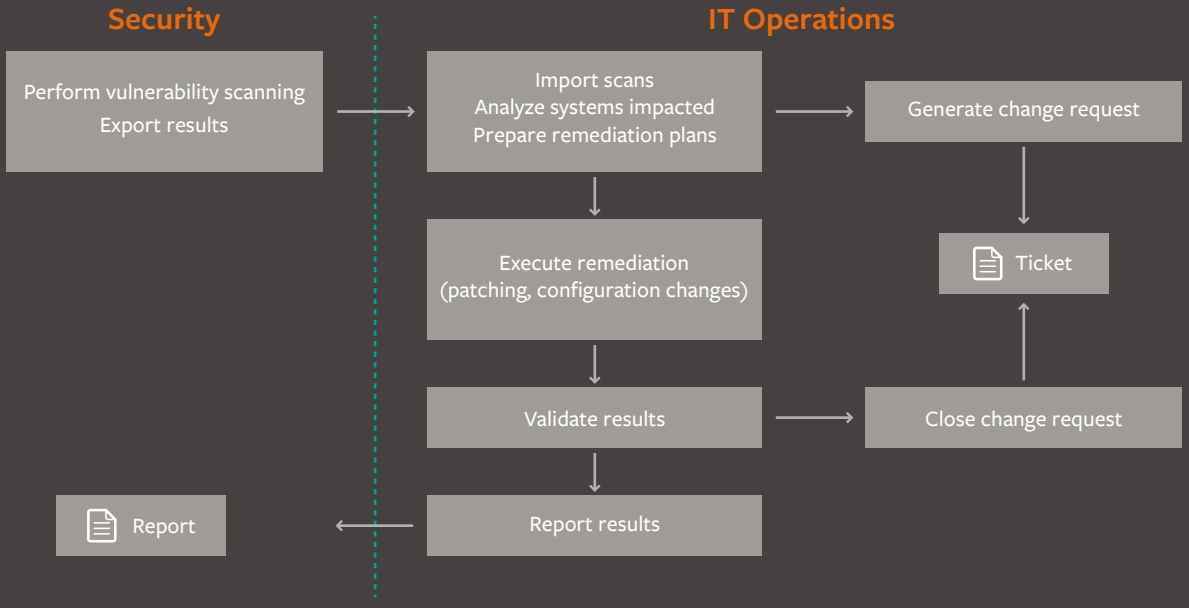
Good patching and configuration management practice is a kind of hygiene, like taking your car in for regular maintenance. Ideally, you're doing this frequently enough to keep the car running properly. If you don't service parts on time, such as not changing brake pads when needed or running out of oil, you run the risk of impeding the driving experience or causing an accident that can be serious and expensive. When organizations don't patch regularly enough, the results are similar: first, things are a bit uncomfortable, but they eventually can get fairly serious, and potentially expensive or time-consuming to fix.

The reasons organizations don't patch frequently enough are often complicated, but they typically are related to a process breakdown: perhaps maintenance windows aren't documented or agreed to or the proposed changes are hard to manually link to a list of configuration items (CIs). Maybe the organization, having been burned by one too many "blanket" change controls, has slowed down the rate of change approvals for patching activities to drive better results when patches are applied.

## VULNERABILITIES, SCANNING TOOLS, AND 400 PAGES OF THE SECOPS GAP

Today, most organizations use at least one of the popular vulnerability scanning tools: Qualys ThreatProtect, Tenable's Nessus, or Rapid7's Nexpose. Most organizations are also scanning on a regular, scheduled basis, and generating a lot of vulnerability information. They may integrate the output of those scans into other tools, but the basic assessment of what vulnerabilities are in the environment usually starts with the scanning tools. The list of vulnerabilities that comes out of them is often in XML or another machine-readable format.

These scans can be as simple as the scan of a single newly provisioned system, a major zone/VLAN, all of the instances running in a particular cloud provider, Azure or AWS, or the bulk of the production network. Larger scans are common, and it's not atypical to generate a file that's the equivalent of 200-250+ MB of data or 400 or more printed pages. The scans are often passed directly to IT operations, in XML or PDF format.




A typical vulnerability detection and remediation process

There are integrations that will create incident tickets directly from these tools, but they often shift the burden to IT operations, who must parse the raw vulnerability data and work through potentially thousands of tickets. Instead of security asking IT operations to read through and make effective use of a 400-page PDF or XML file, security might create many individual change controls or incidents, all of which need to be assessed, have action plans built around them, and managed over a lifespan of a month or two.

Unfortunately, many IT operations groups are not in a position to make automated, fully-integrated use of this scan data, so they will often have to make an assessment of the information they can interpret, and may generally only be able to address the "top 5" or "top 10" vulnerabilities. Since this tends to be a highly tactical activity, it's easy to lose sight of last month's or last quarter's "top 10."

### When Fixing Vulnerabilities Doesn't Mean Patching

Patches are only part of the story. Many security-related vulnerabilities can be closed through configuration changes: either turning on or off a setting, or installing or uninstalling a software element. Configurations that require more than the most basic of configurations or that have potentially high impact to applications, are simply accepted by the client business unit. This acceptance is often due to a gap in understanding the real risk of the change versus the effective threat level. Other reasons an organization will accept risk they otherwise wouldn't is due to a gap in their ability to effectively pre-flight test, QA, and troubleshoot after a change has some impact on the application.

## 5 KEY REQUIREMENTS TO IMPROVE VULNERABILITY MANAGEMENT

**The goal and challenge for the SecOps team is to effectively communicate the priorities and exposures, and drive direct, timely action to close these vulnerabilities.** It is no longer sufficient to just communicate that the vulnerabilities are there. Businesses are asking what can be done to accelerate the closure of the most critical vulnerabilities. The more forward-thinking businesses are also asking how to do this effectively and efficiently, with fewer security-related emergency projects. BMC SecOps Response Service is designed to address this gap.

### Enable Blind Spot Detection

"You can't manage what you can't measure" and you can't fix what you don't know about. Vulnerability scanners are great at getting detailed information about every system they can get to and the network IP ranges passed into them. The lists, IP ranges, and other groupings that the SecOps team is working from may bear relatively little similarity to those being used by the IT operations teams. However, if there are new systems or networks/VLANs, shadow IT, hybrid cloud systems, or those otherwise not known or being scanned by your scanners, they may also not be patched. This situation makes these systems potentially some of the greatest liabilities in the organization.

To this day, organizations implementing automated discovery will regularly find some systems with years-old vulnerabilities, such as POODLE, Heartbleed, and Shellshock, that either aren't being regularly patched or aren't being regularly scanned for vulnerabilities to handle. This is known as a blind spot. By integrating discovery services into SecOps Response Service, you can help identify the gap between the systems that are well-managed, and those that are just waiting to be exploited. This capability ensures that:

- Hosts that are discovered on the network are included in an appropriate group for regular scanning and assessment.
- You take action on every identified system that has a known vulnerability by feeding this list back to the automation or deployment platform.

### Overcome Challenges in Vulnerability Scan Processing and Prioritization

Security teams in every modern organization assess the applications and infrastructure of that organization, whether it's on-premises, in a data center hosting environment, or in a multi-cloud environment. While this can include implementing best practices like active penetration testing, advanced application code security reviews, and security and regulatory compliance audits, one of the most common starting points is using vulnerability scanning. Once gaps are identified, these are usually prioritized, focusing on the most sensitive systems, especially those that are public- or internet-facing, or those that safeguard the most important information in that organization.

Once those vulnerabilities have been identified and prioritized by the SecOps teams, a list of the vulnerabilities is typically passed to the IT operations team for assessment and closure. The resolution of some of these vulnerabilities may lie entirely within the application domain and are commonly sent to the experts in those groups. However, many vulnerabilities can be closed either through the application of common security patches or configuration changes, like disabling unneeded services, requiring authentication, or providing more effective encryption. Effectiveness requires a system that can automate the comparison of the scans against the systems and provide plans for remediation that are actionable.

### Achieve Repeatable Action and Deployment

Identifying how to fix any one vulnerability can require a fair amount of effort and introduce risk in and of itself. This is especially true if there are not good systems for preserving and reusing these decisions once they are made. The assessment and fix preparation process can take a week or two of time for action on any given vulnerability, especially if the team is busy. Some Microsoft patches may have more than a dozen hotfixes, depending on OS version, edition of Windows, etc. As a result, it's important to identify and capture the appropriate fix for a given vulnerability and make it easy for the team to pick the right fix.

The last major challenge is getting the remediation packages to the endpoints and successfully executed in a timely fashion. Historically, particularly on certain deployment systems, it has been difficult to package and stage individual remediation packages for any given target. It was much more common to make up a few "bundles" of patches and deploy that "approved bundle" broadly, potentially to almost every system within a large common group.

This process has caused a number of challenges:

- It was more difficult to deploy patches that could have had a good preventative effect, due to the potential negative impact these patches might have on another system. This problem made it more challenging for any given patch to be included and often restricted the selection of patches to just critical patches.
- Since the bundle would go to many systems, it would often restrict the total number of patches that could be included, due to deployment bandwidth, and space constraints on the systems with the smallest staging areas. So, it's common that only this month's critical patches might be included, and potentially a few patches from last month as well.
- If a managed system were down for a few weeks, for extended maintenance, a hard to obtain part, or other issues, it could potentially miss a fair number of patches. If space is tight on the distribution point infrastructure in the environment, those patches might not be redeployed or audited for potentially a relatively long window.

### Reduce Time Pressure

Executing under pressure to meet a quick deadline is often a key issue for IT operations. While some systems can drive initiation and execution quickly within a few minutes, it's not uncommon for patch execution to happen, perhaps hours later. This can mean that if a system requires a large number of patches to be deployed, or if the bundle is relatively large in size, the deployment might get delayed.

Maintenance windows are tight and the time required for the system to be out of service can be fairly long, even to the point of making patching unattractive or untenable at all to the line of business owner. No matter how much they respect the need for good security practices, most business units want required maintenance to occur fast, with low impact and high certainty. They need to return the applications and systems to productive service, so they can continue to serve the needs of the business.

### Enrich SCCM/WSUS Standalone with More Knowledge About the Vulnerability and Prioritize Patching

The key challenge of software deployment-focused systems like SCCM's Windows Server Update Services (WSUS) function is that while they provide information about common vulnerability and exposure (CVE) information, it can require effort to relate vulnerability scan information to the specific hotfixes that can close those vulnerabilities. It can be a challenge to identify the related Windows bulletin and knowledgebase article, and the specific hotfixes that can then address or close the vulnerability. In addition, they don't facilitate prioritization of those patches by severity beyond "critical." In a time-constrained world, most organizations don't get to deploy all of the patches they would like: it's important to quickly prioritize and address the most important vulnerabilies first.

Providing reporting with dashboards and trends of vulnerabilities and missing patches is not a core strength for these tools. Given that software distributions are primarily done by OS collections or groups, versus addressed to or tailored for individual systems, these systems effectively are good at getting the most common set of patches to the most machines. However, they can be a blunt instrument in a world that increasingly demands precision, accuracy, and "do no harm."

## HOW SECOPS RESPONSE SERVICE HELPS EXTEND THE STRENGTH OF SCCM AND WSUS

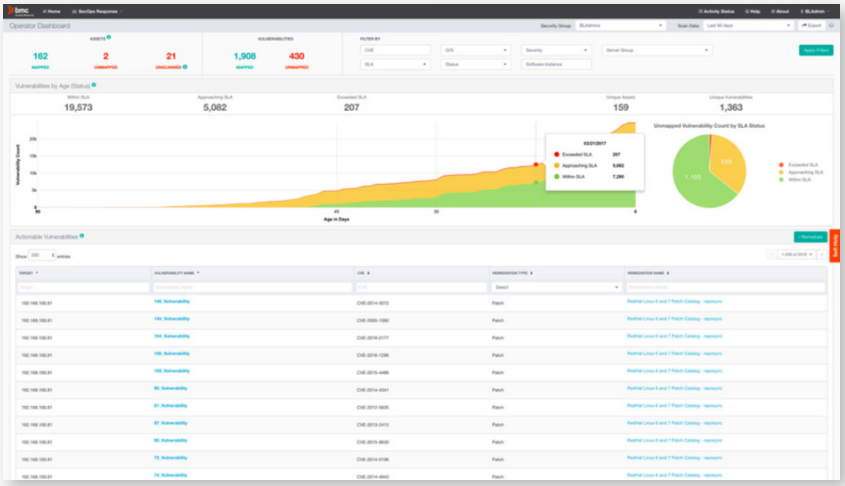
SecOps Response Service enhances SCCM, giving organizations the ability to import vulnerability and asset group information from scanners, map it to the appropriate remediation activity, and translate it into action. SecOps Response Service extends its support for BladeLogic Server Automation to now cover the most popular software distribution tool in the Windows-friendly data center: Microsoft System Center Configuration Manager.

Once vulnerability scan information is imported, it's easily mapped to hotfixes or patches, whether they include individual hotfixes or a patch rollup. SecOps Response Service provides good visibility into the severities of the Microsoft security bulletins, enabling it to automatically work from a prioritized list and address the most critical vulnerabilities first.

- By working from more focused list of vulnerabilities that are known to exist on specific individual systems, you can either leverage or improve upon the whitelist, to potentially pick up more patches in areas that have less exposure on the most critical vulnerabilities.
- You can also get the most important patches deployed in less time, shortening the overall maintenance window, and reducing risk and the burden on your staff.

SecOps Response Service also provides visibility back to the security team as to what remediation work has been planned against the discovered vulnerabilities, and the schedule to execute. This capability enables the security team to focus on the next critical vulnerability, which helps improve the operational tempo of the Security Operations Center, and lets the IT operations team focus on getting hotfixes distributed successfully and more easily.

The operator dashboard provides a holistic view of all known threats.




SecOps Response Service also has native capability with BladeLogic Server Automation to leverage BMC Discovery to find blind spots—those unscanned hosts that are not being checked for vulnerabilities at all—and enable change integration with solutions, such as Remedy, to automate the time-consuming process of change request management. These capabilities can save significant time for operations teams, while driving better processes and helping avoid change conflicts.

| SECOPS RESPONSE SERVICE AND SCCM | USE CASE |
|---|---|
| Deliver service-aware vulnerability management | View dashboards in the context of application service groups, leveraging existing device collections. When creating remediation distributions, you can do it in the context of specific collections. For example, you can say, "patch only my Prod SQL servers." |
| Manage an asset (that came in via a scan) that is mapped to multiple targets | Map devices behind load balancers to common IPs, and multiple detected IP addresses to a common device. |
| Create vulnerability exclusions for false positives or non-critical vulnerabilities | Give more power to the users to make decisions in the context of what's relevant for their business and eliminate irrelevant vulnerabilities. |

By working with your existing deployment architecture, including an installed and functional SCCM environment, you can leverage the deployment strengths of SCCM and the existing installed infrastructure and agents. You can do this while also setting up and scheduling more focused distributions, and closing vulnerabilities that will help your CISO, security, and IT operations organizations meet their business goals.

## CONCLUSION

Vulnerabilities to the enterprise won't go away but they can be controlled with the right technology and a plan to accelerate execution. SecOps Response Service extends the power of SCCM by natively integrating vulnerability scan data with operations data and allowing for automatic, enterprise-grade remediation. IT operations and security teams have the data they need to prioritize and remediate threats based on the potential impact to the business. They can address vulnerabilities by policy and impact, ensuring the most critical issues are fixed first, while protecting uptime and maintaining stability. In short, SecOps Response Service helps make security scans actionable so that IT operations can better support digital transformation initiatives.

## FOR MORE INFORMATION

To learn more about SecOps Response Service, please visit **bmc.com/it-solutions/secops-response-service**



*493911*