SECOPS IN ACTION, AND HOW YOU CAN BENEFIT FROM IT

In my previous post "What is SecOps and how can you maximize its potential?", I defined SecOps as the intersection of Security and Operations teams within an IT organization. However, these two teams typically have different objectives, priorities, and measurements which can create a divide between them, sometimes called the "SecOps gap", and it can be detrimental to the organization. However, this gap can be reduced and even eliminated using automation solutions designed to improve security, increase teamwork, close vulnerabilities faster, and maximize efficiency to save labor.

SecOps Solutions: Key Requirements and Capabilities

To build more effective collaboration between Security and Operations, organizations need integrated, automated solutions that have strong capabilities in the following areas:

Automated Vulnerability Management. Most organizations have security scanners in place to scan servers and networking devices on a regularly scheduled basis. These scanners typically generate reports with hundreds of pages of vulnerability data that must be analyzed and turned into usable information. This report is (hopefully) compared with BMC Helix Discovery information to identify devices missed by the scanners ("blind spots"). Blind spots are then scanned and the consolidated vulnerability data is passed from Security to Operations. In Operations, the tedious, time-consuming task of analyzing the vulnerabilities and planning their remediation is performed. This includes mapping the vulnerabilities to the servers or networking devices involved, mapping them to a patch (or configuration change), analyzing vulnerability severities, determining which business services are

at risk, setting priorities, initiating the change management and approval process, deploying the patch (or configuration change), verifying successful installation, and closing it out in the change management system.

Server and/or Network Automation. Automated vulnerability management needs to be one of the capabilities of a server or network automation solution. These solutions automate the deployment of security patches or configuration changes, ensure they are successfully installed, and generate reports. They should also have the ability to automate compliance with external regulations or internal policies, provision/deprovision a device, distribute software, and automate device lifecycle management. Automation increases efficiency, improves the quality of deployments and reduces rollbacks, and saves labor, allowing staff to be shifted from maintenance to more strategic projects.

Automated Compliance

Compliance with relevant regulatory mandates (such as CIS, SOX, HIPAA) and internal policies is also a requirement. If something is out of compliance, teams need real-time visibility to the problem, and the ability to use automation to fix it with the click of a button so they can always be audit-ready.

Automated Change Management. Automation of the change management process is needed so teams don't have to manually create tickets, communicate via email, manually obtain approvals, etc. Instead, integration between server and network automation, and the change management system, is required to speed up the management of vulnerabilities, increase efficiency, and save labor.

SecOps Solutions in Action

Hardly a day goes by when a new security breach is not in the news. And they can be costly, the average cost of a data breach now stands at $3.9M according to the Ponemon Institute. Many of these breaches are the result of a vulnerability that has been exploited. Fortunately, most vulnerabilities can be addressed with a patch, configuration change, or image update. Often the major obstacle is the time and manual effort involved. Use of SecOps automation solutions from BMC can help streamline this process, speed up remediation efforts, and save labor at the same time.
Here are examples of some recent vulnerabilities that SecOps automation solutions, combined with closed-loop change and configuration management, can help with:

EternalBlue: This server vulnerability originated in 2017 and is serious because it can help malware to spread. At the end of 2018, millions of systems were vulnerable to EternalBlue, and it has been involved in $1+ billion worth of damages in over 65 countries. Fortunately it can be remediated with Windows security patches deployed using server automation solutions.

WannaCry: This is ransomware attack targeted Windows computers, it encrypted data and then demanded ransom payments. It is believed to have spread to over 200,000 computers and may have caused over $1 billion in damages. Again, the remediation can be done using Windows security patches which could be deployed using server automation solutions.

Docker Doomsday: The Docker Doomsday vulnerability affects almost any organization using Docker and containers. It is very serious because it exploits a flaw in runc, which is the container runtime utility for Docker and Kubernetes. It can quickly spread to thousands of containers on the infected host, ultimately spreading further to many interconnected production systems. Again, the remediation can be done using patches that can be deployed using server automation solutions.

Conclusion

The short list of vulnerabilities above illustrate the kinds of security risks, and potential damages, faced by organizations today. Fortunately, automated solutions that help close the SecOps gap can address them, and deliver many benefits to Security and Operations teams. They increase the productivity of staff, allowing them to improve security by detecting and remediating more vulnerabilities in less time. SecOps automation also saves labor and allows it to be shifted from maintenance to innovation, delivering customer benefits and competitive advantage. They can also increase compliance with regulatory mandates and boost employee morale (and retention) by giving existing staff more interesting projects to work on. Finally, they can incease efficiency , lower costs, and improve collaboration across teams to the benefit of the organization as a whole.