bmc

Quicksheet

Vulnerability Management Maturity Model

Lifecycle Management

LEVEL 1

LEVEL 2

LEVEL 3

LEVEL 4

AD-HOC PATCHING

This is the initial patching process. Think of this as running Windows Update (WSUS) on your laptop for system scanning and installation of OS patches. Administrators run the process on servers at an ad-hoc time and execute manually. This is the general practice for small shops with limited to no IT departments.

BMC server automation solutions are the key offerings for Level 1.

PLANNED PATCHING

Organizations plan a patch window for servers on a regular basis, typically monthly. Deploying the patches, bringing down (pre-tasks) and up (post-tasks) of the applications will be executed manually. An ad-hoc manual testing of the application will be executed. Discovery tools are used to identify servers to be managed and blind spots.

BMC server automation solutions are the key offerings for Level 2.

SCRIPTED PATCHING (PRE / POST TASKS)

Scripting is implemented to help with the pre- and post-steps to the patching process. Patching is fully scheduled, and servers are defined for patch windows. A change request should be created with the documented servers that are patched.

BMC server automation solutions are the key offerings for Level 3. Orchestration can also suppose integrating change requests and a closed-loop change management system.

VULNERABILITY SCANS AND SCRIPTED PATCHING

The security team adopts a vulnerability practice and deploys a vulnerability scanner (i.e. Qualys, Nessus, Rapid7). Scans are executed on an ad-hoc basis and results are collected. Scan reports include ip addresses for servers and CVE identifiers vulnerabilities. Reports on vulnerabilities and risk are presented to executives for awareness. At this point, the organization is becoming more secure, but manual labor can increase due to the amount of time and effort spent on analyzing the scan reports.

BMC server automation solutions are the key offerings in Level 4. Orchestration can also support change requests and a closed-loop change management system.

LEVEL 5

MANUAL VULNERABILITY REMEDIATION AND SCRIPTED PATCHING

The security teams are sending scan reports over the wall to the operations teams to begin addressing the vulnerabilities. This is a pain-staking process as there is no business context for the vulnerabilities, only an IP address and vulnerability identifier (CVE). Operations teams are left trying to determine what to patch first and to develop remediation packages in an ad-hoc manner. Many vulnerabilities go unpatched due to the amount of manual effort involved. Scripts are used for patching, and vulnerability remediation is performed manually.

BMC server automation solutions are the key BMC offerings in Level 5. Orchestration can also support change requests and a closed-loop change management system.

LEVEL 6

INTEGRATED VULNERABILITY SCANNING, PLANNING, AND PATCH AUTOMATION

Data from discovery tools is used to cross-reference assets with vulnerability scanner data to identify blind spots (systems known to the discovery tool but were not scanned by vulnerability scanners). Systems are in place to tie vulnerability scan reports to available remediation options. Planning is supported, and includes assignment of patches to vulnerabilities and are tracked. There is an integrated solution of vulnerability scanning to automated patch deployments, and remediation efforts are tracked. Configuration changes to close vulnerabilities are also implemented using automation tools.

BMC server automation solutions are the key BMC offerings in Level 6. Orchestration can also support change requests and a closed-loop change management system.

LEVEL 7

CLOSED-LOOP VULNERABILITY MANAGEMENT AND PATCH AUTOMATION (VERIFIED)

Automation and Orchestration complete the loop of integration through the change management process. As vulnerability scans occur, they are integrated to the vulnerability management system which identifies remediation options. Orchestrated remediation can be scheduled which automates the creation of the necessary change requests with the associated servers and vulnerabilities to be patched, and schedules the remediation jobs in the appropriate maintenance windows per asset. Finally, a validation of success, inclusive of successful remediation deployment and application functionality, is integrated into the orchestrated process.

BMC server automation solutions are the key offerings in Level 7. Orchestration can also support change requests and a closed-loop change management system.

LEVEL 8

LEVEL 8 – SECDEVOPS INTEGRATION

As part of the CI/CD (Continuous Integration/Continuous Delivery) release process, developers have visibility to the vulnerabilities within their applications and can address them as part of their release cycle. The remediation packages and configuration changes are automatically scheduled with regular release cycles.

Vulnerability testing is also integrated with the CI/CD release process to help prevent the reoccurrence of potential vulnerabilities. SecOps integration refers to a situation where Security team and Operations teams have bridged the “SecOps Gap” and have integrated tools that enable them to collaborate on setting priorities for vulnerability management. They also have visibility to the actions of each other,

and support the rapid and automated remediation of vulnerabilities in an agreed-to, prioritized sequence that optimizes organizational security, achieves

SLA's, and maximizes the vulnerability "burn-down" (closure) rate.

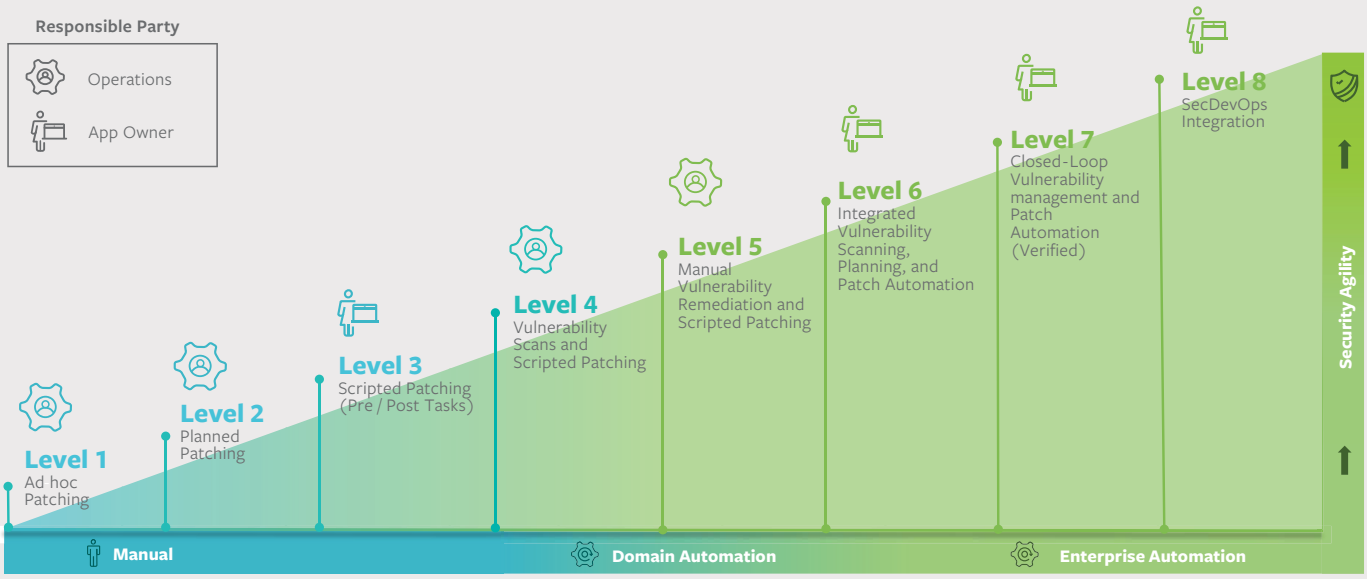
BMC server automation solutions and BMC Helix Cloud Security are the key BMC offerings in Level 8. Orchestration can also support change requests and a closed-loop change management system.

***Note:** BMC Helix Cloud Security can be adopted at any maturity level (Levels 1-8) because it gives developers visibility to vulnerabilities within their applications that they can correct as part of their release cycle, before they are deployed in production environments.

FOR MORE INFORMATION

To learn more about managing security vulnerabilities **https://www.bmc.com/it-solutions/truesight-server-automation.html**

VULNERABILITY MANAGEMENT MATURITY LEVELS



About BMC

BMC delivers software, services, and expertise to help more than 10,000 customers, including 92% of the Forbes Global 100, meet escalating digital demands and maximize IT innovation. From mainframe to mobile to multi-cloud and beyond, our solutions empower enterprises of every size and industry to run and reinvent their businesses with efficiency, security, and momentum for the future.

BMC – Run and Reinvent **www.bmc.com**