IBM® X-Force® Red Vulnerability Management Services (VMS)

Identifying, prioritizing and remediating the vulnerabilities that matter most

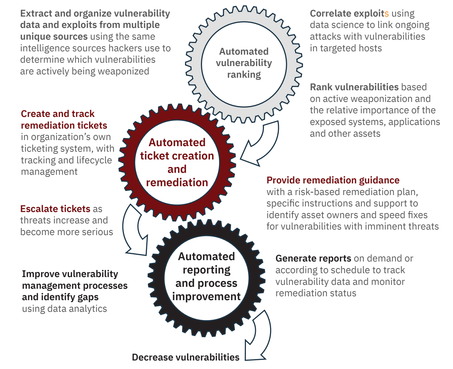
Every day, security teams waste time and resources remediating vulnerabilities that pose minimal risk to the organization while high-risk vulnerabilities go unattended. Identifying and prioritizing the most critical vulnerabilities requires a broader, more scientific and automated approach. IBM X-Force Red VMS correlates threat and vulnerability data from a variety of sources, identifies vulnerabilities that are actively being weaponized and ranks the most severe vulnerabilities in a matter of minutes.

Current vulnerability management challenges can be formidable

- **Too much lag time between vulnerability scans and remediation**, leaving the door open for exposure
- **Lack of manpower and resources** to mitigate and fix vulnerabilities expediently
- **Massive volume of vulnerability data**, potentially millions of records to sort through
- **Inability to quickly and accurately identify and prioritize the most critical vulnerabilities**
- **Slow processing due to manual methods**

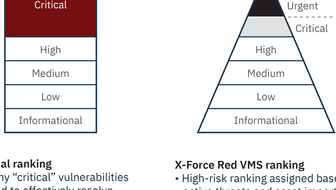
PURPOSE-BUILT AUTOMATION IS THE DIFFERENTIATOR

With manual methods, it can take organizations 3-5 days to prioritize vulnerabilities. X-Force Red VMS does it near instantaneously, then accelerates the remediation process by simplifying ticket management.



MORE PRECISE VULNERABILITY RANKING

Most vulnerability ranking processes rely on Common Vulnerability Scoring System (CVSS) ratings that do not factor in weaponization or asset importance. By continuously correlating threat and vulnerability data which includes this additional content, X-Force Red VMS is able to prioritize vulnerabilities more precisely, pare down the number of critical vulnerabilities and single out the ones that carry the highest risk to the organization.



Traditional ranking
- Too many "critical" vulnerabilities detected to effectively resolve
- High degree of false positives
- Time and resources spent remediating vulnerabilities that pose minimal risk

X-Force Red VMS ranking
- High-risk ranking assigned based on active threats and asset importance
- Fewer false positives by validating whether vulnerabilities are real
- Prioritized, risk-based remediation

ANY SCANNER, ANY LEVEL OF SERVICE

Flexible deployment
Choose any scanning tool, either IBM- or client-provided, with a significant discount for Qualys products. Own responsibility for deployment and support or, in certain cases, turn it over to X-Force Red.

Remediation service packs
Choose a remediation pack of 20, 40 or 60+ fixes. X-Force Red experts help guide the remediation process by providing how-to instructions, verifying each vulnerability is fixed and continuously prioritizing the next to be fixed.

Modular service options
- First-time discovery scanning and scan profile setup
- Data validation, including monthly false positive removal
- Vulnerability ranking
- Remediation lifecycle management, from ticket creation to completion
- Ad hoc scan requests
- Executive vulnerability management workshops

WHY X-FORCE RED VMS?

Rapid identification and ranking enables in-house security teams to remediate the most dangerous vulnerabilities quickly, reducing attackers' window of opportunity to strike.

Labor shortage relief
- Automated vulnerability prioritization, requiring less in-house staff and resources

Vulnerability differentiation
- Ranking based on active exploitation and the importance of exposed assets

Vulnerability validation
- False positive verification, eliminating unnecessary remediation

Remediation recommendations
- Consulting from true subject matter experts in vulnerability identification, prioritization and remediation
- Faster, more accurate remediation

With increased scrutiny placed on managing security vulnerabilities efficiently, it's more important than ever to identify, prioritize and remediate truly critical vulnerabilities as they emerge. X-Force Red VMS provides the expertise, tools and intelligence to help organizations find and fix the vulnerabilities that elevate risk the most.

LEARN MORE

64019164USEN-00