X-Force Red

IBM **Security**

X-Force Red Vulnerability Management Services

Vulnerability Management Challenges

Whether it's due to compliance mandates, pressure from the Board of Directors, and/or an overall concern about the impact of a breach, most organizations have some form of a vulnerability management program in place. Many of those programs, however, solely focus on scanning which is not enough. With tens of thousands of published vulnerabilities in addition to new vulnerabilities being published on a daily basis, how can your security teams know which ones to fix first? And when they do decide what to fix first, what happens if the patch doesn't work or the system cannot be taken down for patching?

The X-Force Red team of veteran hackers has extensive expertise helping secure cloud environments, which includes AWS environments. X-Force Red Vulnerability Management Services (VMS) tracks new containers, assesses software versions in use, checks for secure provisioning, scans for known vulnerabilities in the EC2 or ECS framework, automatically ranks findings, and facilitates remediation.

X-Force Red Vulnerability Management Services for AWS

X-Force Red Vulnerability Management Services identifies, prioritizes, and manages the remediation of vulnerabilities that may expose some of your most important assets to an attacker. The service can include one or all of the following:

Self-Service or Managed Scanning
Using your Amazon Inspector, Qualys or Tenable scanning solution, X-Force Red provides deployment, support, and premium scanning services. The team can also leverage your existing scanning solution.

Scan Fundamentals
X-Force Red works with you to identify which applications and systems are the most important.

X-Force Red configures the scanning tools, profiles, schedules, and reports to identify vulnerabilities at the desired depth and meet your security and regulatory requirements.

Ad-hoc Scan Requests
X-Force Red can conduct out of schedule scanning, reporting, and/or scan profile updates.

Data Validation
X-Force Red validates identified vulne abilities to remove false positives and duplicates.

Prioritization
Scan results are inputted into X-Force Red's hacker-built automated ranking engine, which enriches and prioritizes findings based on weaponized exploits and key risk factors such as, but not limited to, asset value and exposure. The ranking method can be tailored to your environment based on your requirements.

Remediation Management
X-Force Red can facilitate the remediation process and provide subject matter expertise where needed to ensure the highest risk vulnerabilities are fi ed or compensating countermeasures are applied.

Read a client's story about how X-Force Red Vulnerability Management Services reduced the number of critical vulnerabilities by 60% in four months: **ibm.com/case-studies/large-global-bank-security**