Remediation Services

Advanced Remediation Consulting Services

In the past decade the volume and sophistication of cyber attacks has increased dramatically. This increase has been matched by an exponential rise in the number of discovered vulnerabilities.

Security is a process, not a product. When it comes to successful vulnerability management, knowing what and where your vulnerabilities are is only half the battle. Choosing what and how to remediate is ultimately what defines your overall security success.

PRIORITIZATION
Understand business context to elevate issues that should be high priority.

Vulnerability discoverability informs strategic decision-making instead of reacting based solely on CVE risk scores.

Exploitation complexity defines how sophisticated an attacker must be to take advantage of a vulnerability.

Ease of remediation: If a simple fix–like changing a default password–is all that’s needed, implementing it (even if it isn’t especially critical) is good ROI.

OPTIMIZATION
Security configuration is critical because apps can introduce new conditions for exploitation. Attackers never stop researching and uncovering new methods of entry and exploitation, and patches and support for outdated software eventually end. Hundreds of things–literally, hundreds–can compromise your security posture so the best security is continuous security—which requires continuous vulnerability assessments and remediation.

REPORTING
Known assets are rarely the biggest problems – it’s the unknown exposures hiding in the shadows. Cloud, third-party and subsidiary environments have redefined the scope of your attack surface, so you must now manage elements you don’t own or directly manage, like partners and subsidiary assets.

Attacker innovation means tools, techniques and insights are all easier to acquire and implement than they used to be, too. If you can’t find your hidden assets, attackers will.
**VULNERABILITY REMEDIATION**

Optiv’s Remediation Services focus on the following areas:

- Detailed review and analysis of vulnerability reports from scans, assessments or incidents
- Ongoing remediation support, including vulnerability triage, remediation task ownership and coordination, across mixed teams of internal and third-party resources
- Assistance in prioritizing remediation activities
- Recommendations on remediation options and approaches
- Risk-based prioritization of vulnerabilities based on context and current threat intelligence
- Consulting guidance and assistance on network security control implementations within your IT operations environment
- Answering asset owner questions related to specific vulnerabilities
- Discussions on remediation options for specific vulnerabilities identified
- Monthly summary reports to show progress and trends

---

**PLAN**

**Summary:** Optiv consultant(s) work with you to review current VM capabilities and approaches. This includes an initial review of your most recent vulnerability identification results (from scans, penetration tests or incidents), followed by the creation of a remediation plan and recommendations on how to improve your overall VM program (and where you should prioritize and focus your remediation efforts).

**Service includes:**

- Current state analysis (CSA)
- Vulnerability Management & Remediation Program Plan Development, including recommendations on how to improve overall VM program performance and the remediation of vulnerabilities

---

**PLAN & GUIDE**

**Summary:** Optiv consultant(s) conduct a CSA and develop a custom remediation plan with recommended improvements. We work with your designated points of contact (POCs) in regularly scheduled, weekly consulting sessions and review vulnerability scan results, research remediation options and prepare/deliver remediation guidance documentation for your internal ops team(s).

**Service includes:**

- CSA
- VM & remediation program plan development
- Remediation project oversight and coordination
- 12 weeks of ongoing vulnerability triage support and remediation consulting

---

**PLAN, GUIDE, & SUPPORT**

**Summary:** Adds **hands-on** remediation support, as needed.

**Service includes:**

- CSA
- VM & remediation program plan development
- Remediation project oversight and coordination
- 12 weeks of ongoing vulnerability triage support and remediation consulting
- Up to 200 hours of custom hands-on support per month for working on identified remediation items
  
  **(Note:** custom hands-on support hours are 8-5 PM local time with some limited weekend and after-hours support. Additional hands-on remediation support hours may be added based on client-specific needs.)