VigilantMVDR

Managed Vulnerability Detection & Response

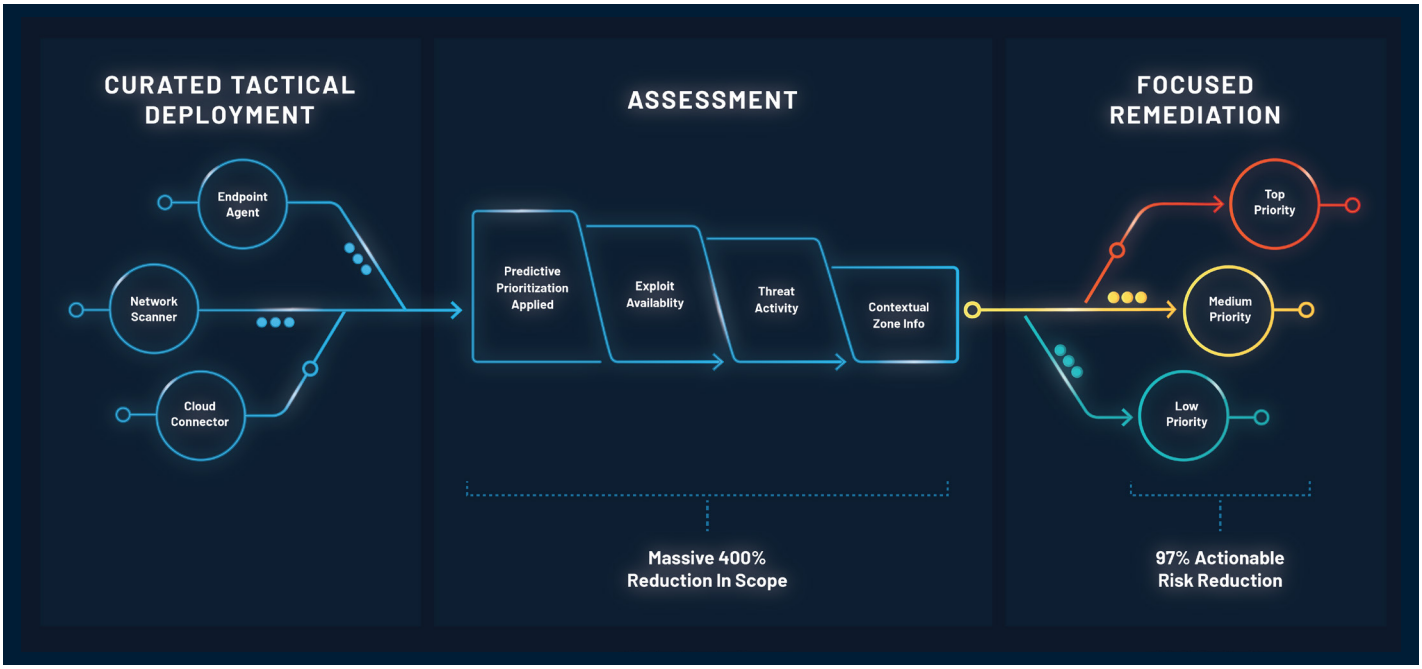
A Proactive and Strategic Approach to Vulnerability Management & Risk Reduction

Whether your goal is regulatory compliance, security maturity, or risk surface reduction, evolving from error-prone legacy vulnerability programs is more crucial than ever. Going beyond merely discovering and assessing vulnerabilities, Vigilant Managed Vulnerability Detection and Response (MVDR) is a powerful solution that solves the higher-order challenge of helping organizations effectively prioritize what matters most. By calculating key metrics, comparing progress against industry standards, and determining when and where to make adjustments, VigilantMVDR optimizes the strategy necessary to secure the higher ground.

An Intelligent Assessment and Remediation Strategy

VigilantMVDR's Risk Based Prioritization is our process of re-prioritizing vulnerabilities based on the probability that they will be leveraged in an attack. It combines over 150 sources, including vendor-based vulnerability data and third-party vulnerability and threat data. Vigilant studies the same "Exploit and Malware Kits" threat actors use and tests them with our own benevolent hackers (Penetration Testing) to reduce risk before a potential attack.

With Risk Based Prioritization, VigilantMVDR dramatically improves an organization's remediation efficiency and effectiveness by focusing first on the 3% of vulnerabilities that have been – or will likely be – exploited.



The Result: Visibility into your vulnerabilities, clear priorities to address first and attack surface reduction – improving efficiency and reducing risk.

A Complete Vulnerability Assessment and Remediation Lifecycle

Each phase of this Lifecycle is critical and Vigilant will collaborate with you in ongoing tactical sessions to ensure accurate and comprehensive deployment. We'll also review the overall health, success, and gaps together during strategy sessions.

COMPREHENSIVE DISCOVERY

Vigilant assesses clients' environments to identify and classify assets known or unknown. Each asset is then tagged based on subnet, as well as a list of identifiable factors like location, name, OS, zone, owner, or function. Vigilant also goes the extra mile to provide the foundation of an **Asset Management** mechanism, host identification, tagging, assignment of ownership, classification, and relational searching.

Outcome: A full and complete list of vulnerabilities – to ensure there are no surprises.

A CUSTOMIZED ASSESSMENT STRATEGY

Vigilant precisely assesses the security environment using a combination of data collection methods that may include:

- Internal scanner appliances to assess network devices and non-endpoints
- External cloud-based appliances to assess external IP space

Outcome: A customized strategy crafted specifically for your company – not an "off-the-shelf strategy" merely based on reports from the industry or general population.

RISK-BASED PRIORITIZATION

Since most CVSS scores are assigned within two weeks of vulnerability discovery, the score only employs a theoretical view of the risk a vulnerability could potentially introduce – leading security teams to waste much of their time chasing after the wrong issues while missing many of the most critical vulnerabilities that pose the greatest risk to the business.

Risk Predictive Prioritization implements factors such as real-time threat indicators, exploit availability, compensating controls and contextual security zone – in order to recommend the best effort remediation approach that goes over and above simple CVSS scores. High risk items are flagged as "Top Priority," and lower risk efforts are deprioritized.

Outcome: The right vulnerabilities are addressed, leading to focused efforts and immediate surface hardening.

REMEDIATION AND MITIGATION

Vigilant's expert ongoing guidance provides a highly-focused remediation plan that includes tactical working sessions that go beyond traditional patch management based purely on 'critical' or highest-score-first approach. Depending upon the subscription level you choose (e.g. single, quarterly, monthly), you will receive:

- **Tactical meetings** review findings and influence the patching process. Dashboards within your portal provide accessible details.
- **Live Dashboards access and automated reports** are provided to the assigned remediation lead\owner.
- **CISO-level review meetings** with Vigilant to discuss effectiveness, issue troubleshooting, as well as ad-hoc requests.
- **Executive reporting** tracks effectiveness of ongoing patching and remediation efforts providing statistical metrics and trends.

Outcome: Vigilant's collaborative "service-first" approach provides true, hands-on guidance vs. merely issuing a printed report.

Want The Full Story? Ask About Our Client Success Stories.

CLIENT IN THE SUPPLY CHAIN INDUSTRY

I appreciate VigilantMVDR's focus on continuous assessment. It fulfills all of our vulnerability management needs, from regulatory compliance requirements to security-first methodology, as well as internal/external risk reduction prerequisites in our organization.

*You can rest assured that Vigilant will never sell your data or reveal your identity. Ever.

VIGILANT

www.vigilantnow.com

25% of Vigilant's profits goes to defend and protect endangered children around the world.

Contact Us
855-238-4445
sales@vigilantnow.com