LevelBlue

SERVICE BRIEF

REDUCE YOUR CUSTOMERS' CYBER RISKS

LevelBlue Managed Vulnerability Scanning for Partners

LevelBlue PARTNER PROGRAM

LevelBlue

LevelBlue Managed Vulnerability Scanning

Continuous monitoring for vulnerabilities is challenging. Your customers' attack surface continues to expand with new devices, software, and access points. Their IT environments are dynamic and introduce vulnerabilities. Meanwhile, cyber attackers are always on the hunt to exploit security weaknesses, and limited resources can slow your ability to address them.

LevelBlue's Managed Vulnerability Scanning Service for partners simplifies the process of determining the extent to which customers' critical systems and sensitive information are vulnerable to compromise or attack. LevelBlue consultants manage the vulnerability scanning of both internal and external environments. This scanning is conducted from an external perspective using a cloud-based web portal to manage scans and track remediation workflows. A virtual scan engine and/or host agents will be deployed within the customers' environment to scan the internal hosts.

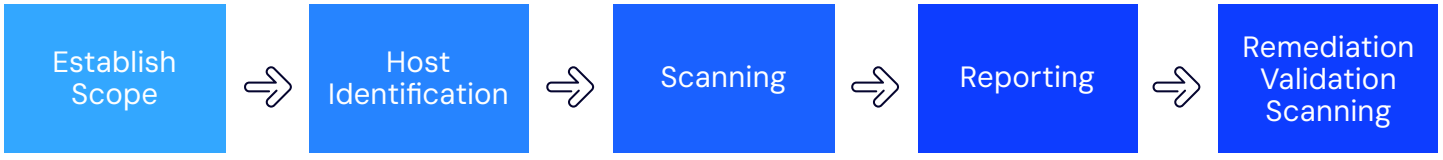
How It Works

LevelBlue cybersecurity consultants will initiate both ad-hoc and scheduled automated scans, producing vulnerability scanning reports as required by your customers and defined in the kick-off meeting. Information provided by your customers about the target environment will service as input for the automated scanning phase.

This diagram illustrates the workflow associated with Vulnerability Scanning:

Benefits of LevelBlue Managed Vulnerability Scanning for Partners:

- Automatically detect vulnerabilities and critical misconfigurations in your customers' assets
- Reduce your customers' attack surface and improve their security posture through ongoing risk reduction
- Validate and document vulnerability patching for your customers
- Accelerate compliance with consolidated audit planning, data collection, and reporting
- Receive expert remediation guidance from LevelBlue consultants with decades of industry-specific experience
- Enhance overall operational efficiency through proactive vulnerability management



Establish the networks to be evaluated

Perform discovery scans to identity live hosts

Execution of scans using automated tools

Analysis of hosts discovered and report generation

Execution of remediation validation scans using automated tools

LevelBlue

Establish Scope

Prior to starting the assessment, LevelBlue cybersecurity consulting conducts a project initiation meeting to mutually establish the rules of engagement. These rules will define the hours of testing, identify hosts specifically excluded from testing, and will generally guide the efforts to perform a thorough test while minimizing business disruptions.

Host Identification

The scan solution uses host and service identification activities to gather specific system and application information on targeted hosts and networks. It collects data on features such as open ports, operating system types, software versions, available services, and the applications providing those services. Utilizing this information, the scanner then compiles lists of known or emerging vulnerabilities, establishing a foundation for further testing.

Vulnerability Scanning

The objective of this phase is to identify hosts, services, and vulnerabilities in the target environment using a suite of customized tools. The scanner performs vulnerability identification after identifying all hosts, ports, and available services. The result of the vulnerability identification step is an enumeration of possible vulnerabilities obtained through a combination of the various scanning and analysis tools.

LevelBlue's scanning servers can be white-listed in any intrusion prevention system to allow the scans to be conducted without interference.

Vulnerability Reporting

During the reporting phase, LevelBlue cybersecurity consultants will thoroughly analyze the information gathered during the assessment. This analysis will include identifying vulnerabilities, assessing their potential impact, and assigning risk ratings to each finding. Based on these insights, LevelBlue will provide detailed remediation recommendations to address and mitigate the identified risks. These recommendations will be tailored to your customer's specific environment and prioritized based on the severity of the vulnerabilities, ensuring that the most critical issues are addressed promptly.

Remediation Validation Scanning

During the remediation validation scanning phase, automated tools will be utilized to verify the effectiveness of the implemented fixes. These scans will ensure that previously identified vulnerabilities have been successfully addressed and no new issues have been introduced.

Scalability

LevelBlue Managed Vulnerability Scanning service ensures scalability to support your customers. Partners can offer five different pricing tiers, categorized by the number of IP addresses, as outlined below:

- 64 IPs
- 128 IPs
- 256 IPs
- 514 IPs
- 1024 IPs

*one block per customer

LevelBlue

About LevelBlue

At LevelBlue, we simplify cybersecurity through award-winning managed services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence, which enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.

Contact us to learn more, or speak with your LevelBlue sales representative.

LevelBlue
PARTNER PROGRAM