CYBALT

Why Vulnerability Management as a Service?

Cybalt Inc. Suite #510, 2701,
North Dallas Parkway, Plano, TX

discover@cybalt.com

Why Vulnerability Management as a Service?

The Log4Shell Internet vulnerability identified in December 2021, affected millions of computers that used a piece of software, called Log4j, which records all manner of activities across a wide range of computer systems. Log4j is open source software provided by the Apache Software Foundation that records events such as errors and operational conditions and communicates these diagnostic messages to system administrators. When the Log4Shell vulnerability was identified, the CVE scored a perfect 10.0 on NIST's Common Vulnerability Scoring System (CVSS), the maximum possible criticality for a vulnerability.

The identified CVE was a Remote Code Execution (RCE) class of vulnerability allowing the attacker to execute code and potentially take full control of the system. What made the CVE especially dangerous was the ease of exploitation; even an inexperienced hacker could successfully execute an attack. According to Jen Easterly, Director of the U.S. Cybersecurity & Infrastructure Security Agency, there were likely millions of attempts to exploit the Log4Shell vulnerability.

Adding to the heightened risk of the Log4Shell vulnerability was Log4j's position in the software ecosystem. Logging is a fundamental feature of most software, which made Log4j very widespread. Log4j logging services are used in popular games like Minecraft, cloud services like Amazon Web Services, and in popular software development and security tools. Although the vulnerability first came to widespread attention on December 10th, 2021, at the time of writing this article the industry is still identifying new ways to cause harm through attacks using Log4Shell exploits.

A New Approach to Vulnerability Management is Needed

The Log4j attacks have identified many challenges to the current approach of vulnerability patching and remediation efforts practiced by many organizations. Log4j is often bundled as part of other software packages making it difficult to determine if the service is being used. You can't fix a problem if you are not aware of it.

The Log4Shell vulnerability also identified that there is no one-size-fits-all solution for patching and remediation. The remediation effort differed per family of the device and even within the actual application running on the device. For some devices like an edge router, a complete system update is required while on other platforms, updating to a new version of software applies the corrective actions. Making the remediation efforts even more troublesome, some software installations require the vulnerable code to be removed manually as pushing out updates is unsuccessful. The Log4Shell vulnerability has helped identify for the IT and information security industries that a new approach to vulnerability management is necessary – Vulnerability Management as a Service (VMaaS).

Outsourcing Vulnerability Management

Compliance and other business drivers require businesses to perform vulnerability scanning regularly. Having immediate, global visibility into your assets and vulnerabilities, is a security priority for mature risk management programs. Deploying scanners, physical and virtual, in the right places in the network and scheduling and tuning the scanners properly based on proven processes requires a depth of expertise and experience. Many security programs lack this expertise and don't have the talented resources to provide the necessary remediation promptly. The solution is Vulnerability Management as a Service.

With Vulnerability Management as a Service (VMaaS), your organization does not require expertise or the resources to identify your IT security vulnerabilities. With VMaaS all vulnerability management is handled for you including the configuration and setup of physical and virtual scanning tools, best practices implementation, and ongoing vulnerability management.

A wide range of vulnerability scans can be performed with VMaaS including privileged and non-privileged, internal, external, and agent-based. The regularly scheduled scans can trigger proactive alerts giving you insight into critical vulnerabilities. And vulnerability scanning should become an essential part of the software development lifecycle including during development, integration testing, user acceptance testing, and post-implementation into production.

Vulnerability Management as a Service and its patching technology services can be integrated into a 24x7 Global SOC (GSOC) team of security experts. The GSOC team will analyze your vulnerability management results and provide recommended actions, prioritized to help you address the most serious issues while making optimal use of your resources.

The Benefits of VMaaS

There are many benefits to VMaaS when compared to standing up vulnerability management platforms internally using your own IT resources:

- Tailor a vulnerability program to meet your organization's unique requirements (no more one-size-fits-all) approach to risk management.
- Scale your scanning and vulnerability management to any size up and down as your business dictates.
- On-premise, cloud, protect your assets anywhere and everywhere.
- Identify real, exploitable vulnerabilities while satisfying regulatory compliance requirements.
- Supplement your team with dedicated vulnerability management experts.
- Solves the two biggest problems of vulnerability management; how to prioritize vulnerabilities identified by scanning tools and how to ensure timely remediation of the biggest threats.

And like all "As a Service" offerings, a properly implemented solution such as VMaaS should simplify and streamline the operational life cycle of the services it promises to deliver.

The vulnerability management lifecycle includes the discovery of all an organization's assets, prioritizing them, assessing their risk profile, measuring risk (reporting) according to security policy, remediation, and verifying that threats have been eliminated.

Modern risk-based vulnerability management improves the vulnerability management lifecycle by keeping your team efficiently focused on reducing the biggest risks to your business. Every network is hit on an ongoing basis by a tidal wave of vulnerabilities. You can't fix them all. Relying on the threat intelligence of a leading VMaaS provider that utilizes artificial intelligence and machine learning allows you to cut costs and save time by prioritizing data-driven remediation decisions.

Scanners Are Like Service Providers – Not All Are Created Equal

Vulnerability scanning and VMaaS are essential tools in the fight against cyber threats. But no solution and no solution provider for that matter are perfect. Vulnerability scanners rely on a database of known weaknesses and are only as good as the latest updates. Conducting scans using outdated or inferior tools can lead to a false sense of security as you may miss critical vulnerabilities. There can be weaknesses that the scanner won't pick up because the vulnerability is newly discovered, or because the exploit is too complex to be detected by an automated tool. And tools might mistakenly flag something that looks suspicious when it isn't, a false positive that leads to inaccurate results.

It is because of challenges like false positives and ensuring that only the best and most current vulnerability databases are used during scanning, are reasons to hold your vulnerability management solution provider accountable. Does your provider have their own SOC and threat analysts, or are their tools only subscribing to common vulnerability databases? Does your partner's security operations center track the security alerts that an organization might encounter, including potential threat notifications via technologies, tools, employees, partners, and external sources? And does the SOC team investigate and validate reported threats to make sure they are not false positives?

It takes a sophisticated combination of expertise, process, and organization to effectively run a Vulnerability Management program. That's why every organization may not be able to support or resource Vulnerability Management in-house. Information security vulnerabilities can exist almost anywhere in the network from hardware devices and infrastructure to operating systems, firmware, applications, and APIs. Tens of thousands of software bugs are discovered every year. Details of these are posted on websites like cve.mitre.org and nvd.nist.gov. Responsible vendors publish timely corrections to vulnerabilities but zero-day vulnerabilities are discovered for which no patch yet exists.

Vulnerability Management as a Service can reduce the complexity of information security risk management by helping organizations accurately assess and remediate risk. Cybalt is a global cybersecurity practitioner assisting organizations with all their cybersecurity needs including security consulting, best-in-class security technologies, global SOC, Vulnerability Management as a Service, and Device Management as a Service.