EventTracker
Actionable Security Intelligence

EventTracker Vulnerability Scan

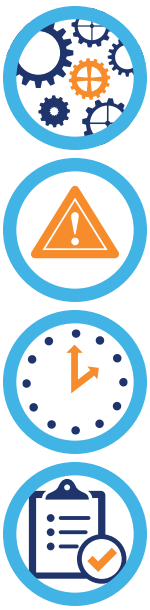
OVERVIEW

Attackers are constantly exploiting vulnerabilities as a means of making their way into their target networks. In fact, most malware is designed to attack vulnerabilities that have already been identified.

According to Gartner, 99.99% of exploits are based on vulnerabilities that have already been known to security and IT professionals for at least a year. And, it only takes 15 days from the time a vulnerability is announced before it's exploited.

Vulnerability scans are a critical component that can help reduce your network's attack surface and help you meet multiple compliance regulations that now require scans (like PCI-DSS, HIPAA, etc.).

But, vulnerability scans take time and discipline, and come with some other challenges:



- **Require technical skill** – vulnerarability scans require a great deal of technical resources and skill to be set up, secured, and maintained. If not managed and maintained, results can be filled with false-positives that can waste your time, and false-negatives that give you a false sense of security.
- **They can break your network** – if not done correctly, scans can do damage to your network by shutting down access to critical assets
- **Re-scanning** – if your scan fails for reasons like an asset that is missing from the network (i.e. an employee takes a laptop home), re-scans have to occur that waste time and effort
- **Reporting** – many vulnerability scanning tools lack the ability to produce reports that you need to measure and improve security, and meet compliance regulations

Organizations who don't have the time and processes to run regular vulnerability scans, but still want to become a harder target, trust EventTracker's Vulnerability Scanning Service, which is available through EventTracker's managed service offering, SIEMphonic. Our expert staff will identify risks within your environment, along with detailed recommendations to close these security gaps before attackers exploit them.

EventTracker
Actionable Security Intelligence

BENEFITS

Managed vulnerability scanning simplifies the process at a cost effective price. Some of the benefits you'll enjoy are:

1. **Experts on hand** – our vulnerability scans are backed by up-to-date intelligence and performed by our in-house security experts for the most effective scan
2. **Prioritization of what's exploitable** – we correlate your data with multiple threat intelligence feeds to monitor and prioritize vulnerability remediation while keeping in mind the value of your assets, so that you can plug the most important holes first
3. **Remediation recommendations** – after a scan is performed, our team of security experts will provide remediation recommendations so you know how to fix your vulnerabilities
4. **Scheduled scans** – you pick when you want your scans to occur so that they don't interfere, but still allow for continual monitoring
5. **Accurate results** – using an expert-backed solution means that you have the most accurate results, not false positives that waste your time
6. **Detailed reports and dashboard** – all of your scans and reports are integrated into a customized dashboard so that you can view and track results over time

HOW IT WORKS

1. EventTracker experts will work with you to identify and group assets. Assets include operating systems, applications, network devices, and more. We can perform a discovery scan and provide you with a list of assets, or we can accept your list.

2. You determine how often you want your vulnerability scans to occur (weekly, monthly, quarterly), plus you can schedule scans based on asset groups. Your vulnerability scan will show inadequate software patching, application defects, insecure configurations, architectural deficiencies, etc.

3. Detailed results, including remediation recommendations, are integrated into your customized Reports Dashboard.

4. Trend reports that show new, remediated or unchanged vulnerabilities are provided

The Vulnerability Scan component of the SIEMphonic service also includes the maintenance of the scanner system for signature, engine and platform updates.

SPECIFICATIONS

- Virtual Appliance on VMWare ESX 5.0 or higher
- CPU – 2.8 GHz minimum
- Memory – 4 GB
- VM Controller – LSI Logic RAID
- VM Hard Drive – SCSI type
- Disk – 60 GB
- Network Adaptor – 1
- Multi factor authentication bypass