TIPPED MICRO

TIPPINGPOINT® ENTERPRISE VULNERABILITY REMEDIATION (EVR)

Quickly remediate vulnerabilities by integrating your vulnerability assessment into the TippingPoint product portfolio

EVOLVING THREAT LANDSCAPE

Organizations operate in an ever-changing threat landscape today, with new software updates, patches, and applications. On top of that, there is a constant stream of security advisories and threat bulletins, so IT security teams are constantly under a lot of pressure. They have to be able to understand and digest this information, and also implement and execute security policies based on threats that could affect their organization. One of the major challenges these teams face is mapping vulnerabilities to their assets and knowing how they can protect against known vulnerabilities discovered that are no longer under support from the asset vendor. Security teams spend enormous amounts of time and manual effort sifting through Common Vulnerabilities and Exposures (CVE) data and correlating their own security audits to identify the affected assets.

Another challenge that security teams face is scaling the remediation process across their entire enterprise. This is complicated by the added risk of waiting for the change window to apply a patch, and the need to support legacy systems and critical applications when there is no patch available from the software vendor for the identified vulnerability.

Key Benefits:
• Quickly optimize your network security protection with virtual patches for the CVEs in your network
• Improve compliance processes
• Simplify policy decisions
• Simple solution to deploy and manage
MAKING THREAT INTELLIGENCE ACTIONABLE

The Center for Internet Security (CIS) publishes the CIS Critical Security Controls for Effective Cyber Defense as part of the CIS Controls Version 6.0. One of the top five controls is “Continuous Vulnerability Assessment and Remediation.” The purpose of this critical control is to continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

Enterprise Vulnerability Remediation (eVR) addresses the “Continuous Vulnerability Assessment and Remediation” control by allowing customers to pull in information from other third party vulnerability management and incident response vendors, map CVEs to Digital Vaccine filters for the TippingPoint Threat Protection System (TPS) and next-generation IPS, and take action based on the enhanced threat intelligence to increase their security coverage. TippingPoint has collaborated with Qualys and Rapid7 to bring industry-leading vulnerability assessment solutions into the TippingPoint Security Management System (SMS). The key benefits of eVR include:

- A detailed view that shows what vulnerabilities, listed by CVE, have been discovered in your network, which assets are impacted by those vulnerabilities, and which TippingPoint Digital Vaccine security intelligence can defend those assets from the discovered vulnerabilities
- The ability to select your enterprise’s TPS/IPS security profile to quickly highlight Digital Vaccine security filters that can protect these assets from the discovered vulnerabilities
- Enables flagging of CVEs for follow-up, tracks policy changes and deploys tuned security policies to protect your assets all from the same workflow

This powerful tool empowers security teams to make the right decision on how to remediate the vulnerability. It might involve updating the asset, scheduling a change window to execute the patch, or turning the Digital Vaccine filter on in absence of an update from the software vendor. This enables security teams to maintain integrity of their systems at all times, regardless of what path they choose.

HOW IT WORKS

- Step 1: Run the vulnerability assessment report using different supported vulnerability management products from Qualys and Rapid7
- Step 2: Export the result of the vulnerability assessment to a supported file format
- Step 3: Import the file into the TippingPoint IPS or TPS from the Security “Profiles” tab of the Security Management Console, select “Vulnerability Scans” and import the exported report from the third party vendor
- Step 4: Select a set of imported vulnerability scans to analyze
- Step 5: Review the detailed scan results by asset and CVE mapped to Digital Vaccine filter coverage and overview of your current enforcement settings
- Step 6: Click “Profile Tuning” and select a security profile to show a focused list of Digital Vaccine filters that may be enabled to protect your enterprise
- Step 7: Optionally deploy your new security policy settings for immediate enforcement to your global IPS and/or TPS deployment

Customers will receive policy adjustment recommendations tuned against their specific deployment that will ultimately reduce administration time, increase security coverage, reduce unnecessary notifications, and provide a big picture view into their overall security posture. eVR is available today to all TippingPoint customers.

https://www.sans.org/critical-security-controls