Harmony Purple: A Better Solution for Vulnerability Management

Traditional vulnerability management is not working. It consumes too much time and resources from security and IT operations and causes too much maintenance downtime. The tools that were supposed to make vulnerability management easier and more efficient have only gotten more complex, more expensive and more difficult to use. Despite all the effort and expense, security has not improved. Organizations of all types and sizes keep falling victim to data breaches and ransomware.
A new approach is needed.

THE PROBLEM WITH TRADITIONAL VULNERABILITY MANAGEMENT

Traditional vulnerability management systems scan hosts and compare the patch level on each system with known vulnerabilities. In a typical scan, hundreds or even thousands of vulnerabilities are flagged as critical or high severity. The result is excess maintenance downtime and a lot of work on weekends and nights for IT personnel. Compliance reporting becomes difficult because unaddressed vulnerabilities must be justified. Meanwhile, businesses still get breached because the right systems were not patched.

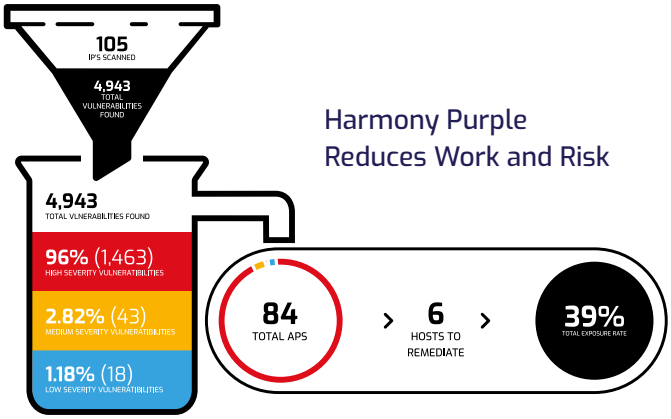
60%
of breaches would have been prevented by applying the right patch
Source: Ponemon Institute

Harmony Purple takes a new, holistic approach. It accounts for how the vulnerabilities could be exploited within the context of the IT environment and the value of the assets at risk. It then identifies the most effective mitigation strategies for minimizing both the risk and potential impact of being breached.

HARMONY PURPLE: A NEW APPROACH TO VULNERABILITY MANAGEMENT

Harmony Purple is an all-in-one vulnerability management and prioritization solution. It unifies scanning, adversarial attack path analysis, prioritization and remediation. It is easy to use, automated, and because it is low impact, scans can be run anytime on production systems. Harmony Purple takes a four step approach to deliver the results security and operations teams need:

1. Agentless discovery and scanning of all hosts. It identifies all open vulnerabilities and their severity.
2. Identifies if a vulnerability is exploitable on the host – whether the host has the prerequisite open ports, services or access an attacker needs to exploit the vulnerability.
3. Applies its patented Attack Path Scenario (APS) analysis to test all possible pathways an attacker could use to penetrate exploitable systems. It identifies all viable attack pathways and potential for lateral movement.
4. Provides recommended remediations based on penetration risk and asset value. This is a combination of patching and compensating controls that maximize security effectiveness.
   The result is a set of manageable tasks that deliver better security with less work.



Harmony Purple
Reduces Work and Risk

FEATURES AND BENEFITS

- ✓ **Agentless:** No need to install, maintain and troubleshoot agents on thousands of hosts.
- ✓ **Lean Scanning:** Run scans during production and on critical systems. No need to schedule downtime for scans.
- ✓ **Attack Path Scenarios:** Discovers the viable pathways from vulnerable hosts to other systems and assets on the network.
- ✓ **Automated Red Team:** Uses simulated penetration testing to identify exposures, without the expense of manual pen tests, and without the risk of disruption to production systems.
- ✓ **Automated Blue Team:** Analyzes existing defensive measures and compensating controls and provides recommended actions.
- ✓ **Recommended Remediations:** Provides mitigation options with few false-positives and reduces the amount of urgent maintenance patching. Result is less system downtime, less work for IT operations, and less risk.
- ✓ **Compliance and Reporting:** Detailed and executive summary reports keep auditors and oversight committees informed. Saves time preparing reports and explaining results.
- ✓ **Timely Threat Intelligence:** Harmony Purple uses multiple feeds from Orchestra Research Lab, Network Information Security & Technology News database (NIST), multi-vendor security update feeds, MITRE Att&ck, and more.
- ✓ **On Premises:** Harmony Purple runs on a virtual machine hosted in your network. It only needs external access to receive weekly threat feed and software updates.
- ✓ **Managed Services:** Harmony Purple supports managed security services, enabling VARs and MSSPs to deliver the best vulnerability solution to client businesses of all sizes.

WHY HARMONY PURPLE

We automate and combine security red and blue teams into a continuous improvement purple team. The purple team translates red team breaches into blue team corrective and preventative actions. This establishes a continuous improvement regime for security processes and controls - the most effective way to keep your organization protected from attacks.

WHAT CUSTOMERS ARE SAYING

"With Harmony Purple, we increased visibility into the potential attack surface of bank assets and at the same time prioritize the reduction process to correct and remediate those attack surfaces in an efficient and effective way."
Gil Hatam, Head of Cyber Defense Innovation Process and Methodology, First National Bank of Israel

"Protecting the hospital's network is very challenging. We have many portals, complex networks between other hospitals and government departments, dedicated medical equipment, and more. Using Harmony Purple, I can finally focus on what really matters."
Hospital CISO

ABOUT ORCHESTRA GROUP Orchestra Group's mission is to address the major roadblocks that make it difficult for CISOs, CIOs, and their teams to manage cybersecurity risk. Orchestra Group addresses these challenges by combining management and operations of IS, IT, Risk and Compliance into a single platform.
Visit us at www.orchestragroup.com