HARMONY PURPLE
by Orchestra Group

Automated Red and Blue Teams Make It Purple

Next generation risk-based cyber defense within everyone's reach.

Cybersecurity is shifting from traditional penetration testing and abstract vulnerability scanning and assessment approaches towards effective risk-based cybersecurity management. Risk-based cybersecurity provides a business context for cyber defense, leveraging the understanding of the organization's asset criticality, policies, processes, and defenses in order to provide insights into critical asset vulnerabilities and the effectiveness of controls in place. Effective risk-based cybersecurity ensures that the organization's compliance requirements and security objectives to meet certain standards and guidelines are constantly measured, providing threat-led control testing and response prioritization against the organization's risk appetite.

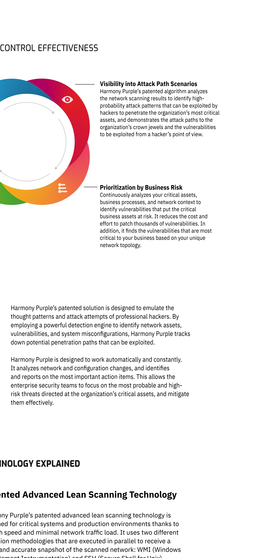
This understanding inevitably requires highly qualified (and expensive) red teams that provide deeper cyber risk insights through advanced hunting investigations. Therefore, it is usually only found in organizations that have the skilled resources and the budget to afford it and conduct these investigations regularly.

Cybersecurity blue teams design defensive measures against red teams' activities. Blue teams conduct systematic examinations of cybersecurity controls to assess effectiveness, identify security deficiencies, predict effectiveness of proposed security controls, and to confirm effectiveness of such controls after implementation. Like the red teams, they are very expensive and require highly skilled personnel.

Cybersecurity purple teams work in unision with red and blue teams to maximize their effectiveness. They do this by integrating the defensive tactics and controls from the blue team, with the threats and vulnerabilities found by the red team, into a single narrative that maximizes both.

AUTOMATED RED, BLUE AND PURPLE TEAM

Harmony Purple is an automated blue and red team that takes the best of both to ensure your cybersecurity controls are effective, at a cost that most organizations are able to afford.



Red Team

Harmony Purple's automated red team seeks out vulnerabilities and network misconfigurations and uses them to simulate how attackers would move in your environment to "capture the flag" of your critical assets.

Blue Team

Harmony Purple's automated blue team makes up the other side of the risk equation by closing the continuous improvement loop, leveraging the insights of the red team. The blue team leverages existing detective, preventative, and compensating controls to thwart the red team's attempts by enhancing control effectiveness, lowering risk, and pre-emptively protecting against attacks.

Purple Team

Harmony Purple's automated purple team tool, which combines red and blue team best of breed capabilities, provides the most effective continuous improvement methodology for cyber defense previously available only to the most advanced companies. The automated purple team puts the next generation of risk-based cyber defense within everyone's reach.

HARMONY PURPLE SOLUTION

AUTOMATED PURPLE TEAMS ENSURE CONTROL EFFECTIVENESS

Continuous Scanning
Continuous scanning of all the company assets' vulnerabilities including critical servers, web servers, endpoints, applications, network configuration weaknesses, and data connectivity flows. With patented advanced lean scanning technology, Harmony Purple is designed for critical systems and production environments thanks to its high speed and minimal network-traffic load.

Recommended Remediation
Reports on all critical assets at risk and recommends the best mitigation options that fit your critical asset risk, significance, and operational needs. It offers several remediation options, and validates vulnerability remediations over time.

Visibility into Attack Path Scenarios
Harmony Purple's patented algorithm analyzes the network scanning results to identify high-probability attack pathways that can be exploited by hackers to penetrate the organization's most critical assets, and demonstrates the attack paths to the organization's crown jewels and the vulnerabilities to be exploited from a hacker's point of view.

Prioritization by Business Risk
Continuously analyzes your critical assets, business processes, and network context to identify vulnerabilities that put the critical business assets at risk. It reduces the cost and effort to patch thousands of vulnerabilities. In addition, it finds the vulnerabilities that are most critical to your business based on your unique network topology.

Harmony Purple allows organizations to substantially reduce its attack surface with the least amount of time and effort and with the most efficient use of staff resources, helping organizations invest their time wisely on those vulnerabilities that threaten its mission-critical assets and business processes.

Harmony Purple's patented solution is designed to emulate the thought patterns and attack attempts of professional hackers. By employing a powerful detection engine to identify network assets, vulnerabilities, and system misconfigurations, Harmony Purple tracks down potential penetration paths that can be exploited.

Harmony Purple is designed to work automatically and constantly. It analyzes network and configuration changes, and identifies and reports on the most important action items. This allows the enterprise security teams to focus on the most probable and high-risk threats directed at the organization's critical assets, and mitigate them effectively.

TECHNOLOGY EXPLAINED

Patented Advanced Lean Scanning Technology

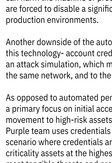
Harmony Purple's patented advanced lean scanning technology is designed for critical systems and production environments thanks to its high speed and minimal network traffic load. It uses two different detection methodologies that are executed in parallel to receive a quick and accurate snapshot of the scanned network: WMI (Windows Management Instrumentation) and SSH (Secure Shell for Unix) network credentials to gain access to the computers and devices in the scanned network. The solution uses the second and third network-layers protocols to perform a light-weight multi-scan process to detect all connected devices in the network and collect crucial system and configuration data from the device's OS, services, and installed software applications, for further analysis.

During this analysis, the collected data from each device is correlated with Harmony Purple's threat repository according to each device's assets (vendor, version, build, configuration, etc.). The repository, powered by Orchestra's Cyber Threat Intelligence (CTI), contains a tremendous amount of up-to-date threat knowledge, hacking techniques, and know-hows, constantly fed from multiple resources including Orchestra Research Lab, Network Information Security & Technology News database (NIST), multi-vendor security update feeds, MITRE Attack, and more.

Attack Path Scenario

Harmony Purple's patented algorithm analyzes the network scanning results to predict how an adversary would actually attack your network and most critical assets.

The attack patterns, as defined by Orchestra's research team, represent possible attack steps to penetrate the network and reach critical assets. For example, an attack targeting a domain controller as a first stage towards a multi-stage data exfiltration attack on critical assets containing sensitive data. Harmony Purple builds a set of penetration paths in the network and produces a prioritized list of the most probable attack paths that hackers may use. These attack paths may consist of several steps, each of them described in detail by Harmony Purple.



Vulnerability Verification

After all possible attack path scenarios (APSs) are created, Harmony Purple performs a simulated attack on the network system in order to examine the vulnerability points (weak links) that were discovered. By verifying the validity of the attack, Harmony Purple eliminates false positives and points only to viable and existing attack paths.

Prioritizing threats by asset criticality, attack probability, and risk, reduces false-positive alerts to the bare minimum, optimizing the effectiveness of your blue team, reducing time to patch and operational costs, while dramatically improving your overall security posture.

HARMONY PURPLE SOLUTIONS VS. AUTOMATIC PENETRATION TESTING

Several solutions on the market resemble automated penetration testing by utilizing "black box" methodologies. These are offered mainly by Breach and Attack Simulation (BAS) vendors. These approaches promise to expose vulnerabilities and misconfigurations with the primary focus on initial access or on audit equipment, lowering the cost of penetration testing through automation. Unfortunately, BAS automation also has a dark side- automated exploitation of vulnerabilities in a live production system can cause unplanned outages and can harm the machine or process that hosts the vulnerability. For that reason, BAS solutions are forced to disable a significant portion of their attack simulation strength when running in production environments.

Another downside of the automated penetration testing approach stems from the nature of this technology- account credentials found on production systems actually get tested during an attack simulation, which may result in sensitive data exposure to anyone with access to the same network, and to the scanning tool in particular.

As opposed to automated penetration testing, purple team automation does not place a primary focus on initial access or on audit, but rather on the potential impact of lateral movement to high-risk assets, which could have serious consequences when compromised. Purple team uses credentials ("white box") to identify the potential threats in advance of the scenario where credentials are compromised, while keeping the operational safety of high criticality assets at the highest priority. This approach enables the blue team to focus on the most tangible threats and provide proactive, even predictive, protection.

Harmony Purple's approach combines red and blue teams into a continuous improvement purple team. The purple team's job is to translate red team test failures (breaches) into blue team corrective and preventative actions (or CAPA, using the terminology of process improvement). The purple team provides continuous improvement for your security processes and controls. Continuous improvement is the most effective way to provide proactive security and protect your organization from cyber attack.
Harmony Purple's scanning technology is designed for critical systems and production environments, ensuring high speed, minimal network traffic load, and maximum security.

ABOUT ORCHESTRA GROUP

Orchestra Group's mission is to addresses the major roadblocks that make it difficult for CISOs, CIOs, and their teams, to manage cybersecurity such as:

1. Fragmented technologies using different paradigms for each slice of the cybersecurity puzzle leading to a cyber stack of 100+ different technologies in every large organization.
2. Lack of standard metrics to measure, manage, and benchmark cyber defense. This is crucial to drive efficiency, effectiveness, and continuous improvement of the organization's security.
3. Constant change is now the norm for business and IT. Cybersecurity requires constant tuning of the trade-offs between shifting IT/ business needs and cyber risk.

Orchestra Group addresses these challenges by combining management and operations of IS, IT, Risk and Compliance into a single platform.