Red and Blue Teams Operations Are Not as Simple as They Seem

Risk-based cybersecurity provides a business context for cyber defense. It shifts cyber defense from abstract vulnerability scanning and assessment towards effective risk-based cyber controls. Harmony Purple is an automated blue and red team that takes the best of both to ensure your cybersecurity controls are effective. The heart of the system is how Harmony Purple layers its patented Attack Patch Scenario (APS™) engine on top of your existing cyber capabilities.

MEASURING CYBER RISK

Vulnerability scanning, penetration testing, and red teams are the main mechanisms for measuring residual cyber risk – the risk that remains even with existing controls already in place.

Vulnerability scanning and penetration testers find potential cyber weaknesses, while red teams map cyber weaknesses to business risk for existing applications and devices.

Purple teams combine red and blue approaches to ensure control effectiveness. The value of purple teams is well known, the only problem is that the purple team approach has been too expensive in terms of resources and costs for most companies. That is, until today!

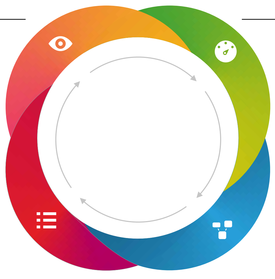
Harmony Purple's automated purple team tool, which combines red and blue team best of breed capabilities, provides a level of continuous cyber defense previously available only to the most advanced companies. Automated purple teams put the next generation of risk-based cyber defense within everyone's reach.

Blue teams make up the other side of the risk equation by closing the continuous improvement loop. Blue teams leverage existing detective, preventative, and compensating controls to thwart red teams' attempts by enhancing control effectiveness, lowering risk, and preemptively protecting against attack.

Harmony Purple
AUTOMATED PURPLE TEAMS ENSURE CONTROL EFFECTIVENESS

Visibility
Continuous visibility to all company assets current vulnerabilities including:
- Critical assets.
- Application and Web Servers.
- Endpoints.
- Network configuration weaknesses.
- Data connectivity flows.

Mitigation, Remediation and Reporting
- Recommend best mitigation options.
- Prioritize remediation of riskiest vulnerabilities.
- Report on all critical assets that are at risk.



Intelligent Assessment
- Continuously analyzes your critical assets, business processes, and network context to identify vulnerabilities that put the critical business assets at risk.
- Reduce the cost and effort to patch thousands of vulnerabilities.
- Find the vulnerabilities that are most critical to your business based on your unique network topology.

Attack Path Scenarios
- Visualize all Attack Path Scenarios and focus on those vulnerabilities that matter most.
- Continuously validate critical controls on the "crown jewels" of the company's assets.

Harmony Purple's automated red team simulates how a red team would act in your environment. It seeks out vulnerabilities and uses them to simulate how attackers would move in your environment to "capture the flag" of your critical resources. Harmony Purple's patented Attack Path Scenario engine prioritizes the most effective way to minimize cyber risks to your applications and devices (servers and endpoints).

Attack Path Scenarios enable Harmony Purple to recommend the most effective controls at the lowest cost, combining cyber intelligence and business considerations to optimize control effectiveness. For example, Harmony Purple might recommend a patch to a high-risk server to lower the risk or changing configuration based on cyber intelligence and business considerations.

HARMONY-PURPLE
NEXT GENERATION RISK-CENTRIC VULNERABILITY CONTROL

Harmony-Purple can be configured either to recommend an action, or remediate through SOAR solution integration. Harmony-Purple provides proactive management of cyber risk based on business impact, not abstract vulnerabilities.

Harmony-Purple works in unison with your existing cyber capabilities to provide next-generation security effectiveness that was previously available only to the largest companies.