HARMONY PURPLE

Cybot next generation

June 2020

Confidential

Risk based cyber security provides a business context for cyber defense. It shifts cyber defense from abstract vulnerability scanning and assessment towards effective risk based cyber controls. Risk based cyber security uses an organization's current security context, business needs and external intelligence to provide the context of business loss needed to ensure effective security controls.

Measuring Cyber Risk

Vulnerability scanning, penetration testing and red teams are the main mechanisms for measuring residual cyber risk – the risk that remains given 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.

Blue teams make up the other side of the risk equation by closing the continuous improvement loop. Blue teams leverage existing detective, preventive and compensating controls to thwart red teams attempts in order to enhance control effectiveness, lower risk and preemptively protect against attack.

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 for most companies.

That is until today. CyBot's automated purple team, i.e. **Harmony-Purple**, combines red and blue team capabilities to provide 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 in everyone's reach.

Harmony-Purple – Automated Purple Teams Ensure Control Effectiveness

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 is the brain that prioritizes the most effective way to minimize cyber risks to your applications and devices (servers, endpoints and mobile).

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 risk, or compensating controls of firewall configuration depending on cyber intelligence and business considerations.

Harmony-Purple – Next Generation Risk Centric Vulnerability Control

Harmony-Purple's can be configured either to recommend action – or automatically take action based on risk and business constraints. 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.