Red Team-as-a-Service: Challenge Like an Attacker, No Overhead

Red Team exercises help organizations understand whether security controls will prevent a breach under the pressure of an attack. There is an incredible amount of value in each of these exercises, with the primary motivation being to test an organization's defenses against the tactics, techniques, and procedures (TTPs) of real-world attackers. However, these are typically completely manual and resource intensive. The typical approach requires building a test replica of the cloud which is both labor and cost intensive. These point-in-time exercises are rarely done due to the sheer effort and the more manual the exercise, the less likely it is executed effectively.

Skyhawk Security's AI-based Red Team simulates attacks on digital twins, non-disruptively, providing an adversarial view of your cloud security controls. Unlike Breach and Attack (BAS) solutions, Skyhawk's completely automated red team does not impact the infrastructure and is labor free, while ensuring 100% coverage and accuracy. With the automated simulation, the security team now has a full understanding of the true weaponized risk in their cloud and can pre-validate compensating security controls or indicators of compromise. In addition, remediation can be prioritized to use resources on validated scenarios.

Traditional Red Team and Breach & Attack Simulation Challenges

- **Resource intensive:** Entire teams are needed to evaluate the cloud architecture and design the right attacks.
- **Disruptive:** If not done correctly, this exercise can disrupt production, circumventing anomaly-based detections.
- **Point in time:** Red team exercises are executed periodically, between once a year to one a quarter in mature organizations. Cloud security architecture and controls are constantly changing and a point-in-time view is inadequate.

Skyhawk's Red Team-as-a-Service delivers Adversarial Insights in Real-time

Skyhawk's Continuous AI-based Red Team creates attack scenarios for your specific cloud configuration taking into account your specific security controls, unlike traditional BAS solutions which use pre-scripted attack scenarios that are limited in capability and scale. Skyhawk's Continuous AI-based Red Team uses non-disruptive digital twins to simulate attacks across the entire cloud architecture, at-scale, clearly identifying indicators or exposure based on the business risk. Skyhawk's Red Team-as-a-Service is always validating business risk, ensuring security teams are remediating the vulnerabilities and exposures that drive an overall cloud risk reduction.

- **Continuous, real-time vulnerability detection and remediation:** Continuously identify the weaponized vulnerabilities ensures security teams are always remediating the most pressing vulnerabilities and the cloud architecture and security controls change.
- **Comprehensive, customized attack scenarios:** An AI-based Red Team Service leverage automation to analyze and process large amounts of data to create custom attacks versus scenario-specific attacks to find the weaponized vulnerabilities specifically in your cloud.
- **Non-disruptive testing:** Automated AI-based services do not impact production in any way while ensuring accuracy and speed.
- **Effortlessly cost-effective:** An AI-based Red Team can be run continuously at a much lower cost and with significantly less effort than a human-based red team.
- **Document Compliance:** Testing reports demonstrate and prove support for frameworks like NIST and EU AI Act, reducing the burden on security and compliance teams and increasing ROI.

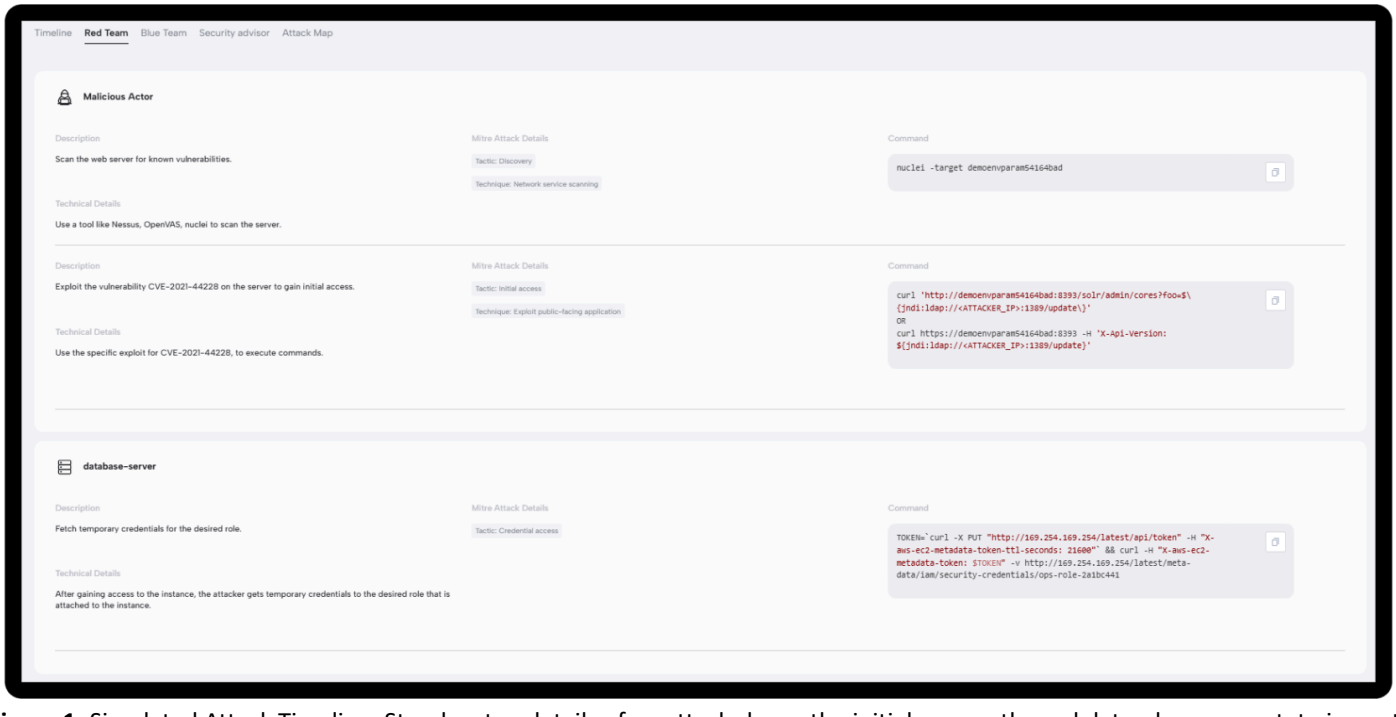

Figure 1: Simulated Attack Timeline: Step-by-step details of an attack shows the initial access, through lateral movement, to impact.

About Skyhawk Security

Skyhawk Security is the leader in Purple Team-Powered Cloud Security, leveraging a multi-layer AI-based approach to identify and preemptively stop cloud threats before they become breaches. Skyhawk revolutionizes cloud security with its Continuous Proactive Protection, an AI-powered Autonomous Purple Team, enabling security teams to take a proactive approach to cloud security for the very first time. The AI-based Red Team leverages digital simulation twins to deliver an adversarial view of the cloud, with no business impact. Led by a team of cyber security and cloud professionals who built the original CSPM category, Skyhawk's platform evolves cloud security posture management far beyond scanning and static configuration analysis, continuously adapting and improving threat detection so that it is always aligned with the cloud architecture. Skyhawk Security is a spin-off of Radware® (NASDAQ:RDWR).