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

Red Team exercises help organizations understand whether security controls will hold under the pressure of threat actors or not. 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. Where the red team is able to penetrate the security controls is what should be prioritized for the security operations center (SOC).

Skyhawk Security's Purple Team enables an AI-based Red Team to simulate attacks leveraging Simulation Twin. There is no impact on people and infrastructure, while ensuring AI-driven accuracy. The Purple Team continuously performs Red Team exercises, providing updated breach data as the cloud architecture changes and security controls are updated. This ensures a consistent and up to date view of your cloud security.

Red Team Challenges

- **Resource intensive:** Entire teams are needed to evaluate the cloud architecture and design the right attacks
- **Disruptive:** If not done correctly, the SOC can receive many alerts indicating some full-scale assault by a threat actor, when really it is a controlled security exercise.
- **Security Team Immaturity:** If you do not have a mature team in place, this can also cause damage your cloud security controls and cause serious issues to be missed.
- **Point in time:** Red team exercises are executed once and then findings are reported. Cloud security architecture and controls are constantly changing and a point in time view is inadequate.

Red Team-as-a-Service delivers Attacker Insights in Real-time

Organizations use Red Team as a Service (RaaS) to gain a proactive and realistic assessment of their security posture. RaaS providers offer a subscription-based or continuous model for conducting these adversarial simulations, which is a powerful alternative to traditional one-off engagements.

- **Real-time vulnerability detection and remediation:** Understand which vulnerabilities are putting your most valuable assets at risk and therefore, your business, and understand how to remediate them fast.
- **Scalability across large, distributed environments:** An AI-based Red Team Service can easily analyze and process large amounts of data, such as logs, telemetry, architecture, and security controls to deliver accurate results.
- **Reduced human error and bias:** AI-based services ensure accuracy and speed.
- **Cost-effective:** An AI-based Red Team can be run continuously at a much lower cost 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.

Overview of Red Team-as-a-Service

Skyhawk's Continuous, Autonomous Purple Team and more specifically, the AI based Red Team, creates attack scenarios that helps identify which vulnerabilities are weaponized beyond exploitability. It identifies those that actually impact a crown jewel. The open platform analyzes information from many different security tools to analyze and uncover vulnerabilities that creates exposure and increase the cloud attack surface.

The AI-based Red team using Simulation Twin simulates attacks specific to your cloud architecture and security controls to determine how a threat actor could breach your cloud. This is done across the entire cloud architecture, at-scale, continuously, ensuring that as changes are made, the vulnerabilities, over-used permissions, and posture findings are always up-to-date to secure your business. The vulnerabilities that lead to a crown jewel are prioritized for remediation. One customer had tens of thousands of vulnerabilities to remediate, but using Skyhawk's breach and attack simulation analysis, less than ten were identified as being truly weaponized and exposing crown jewel assets.

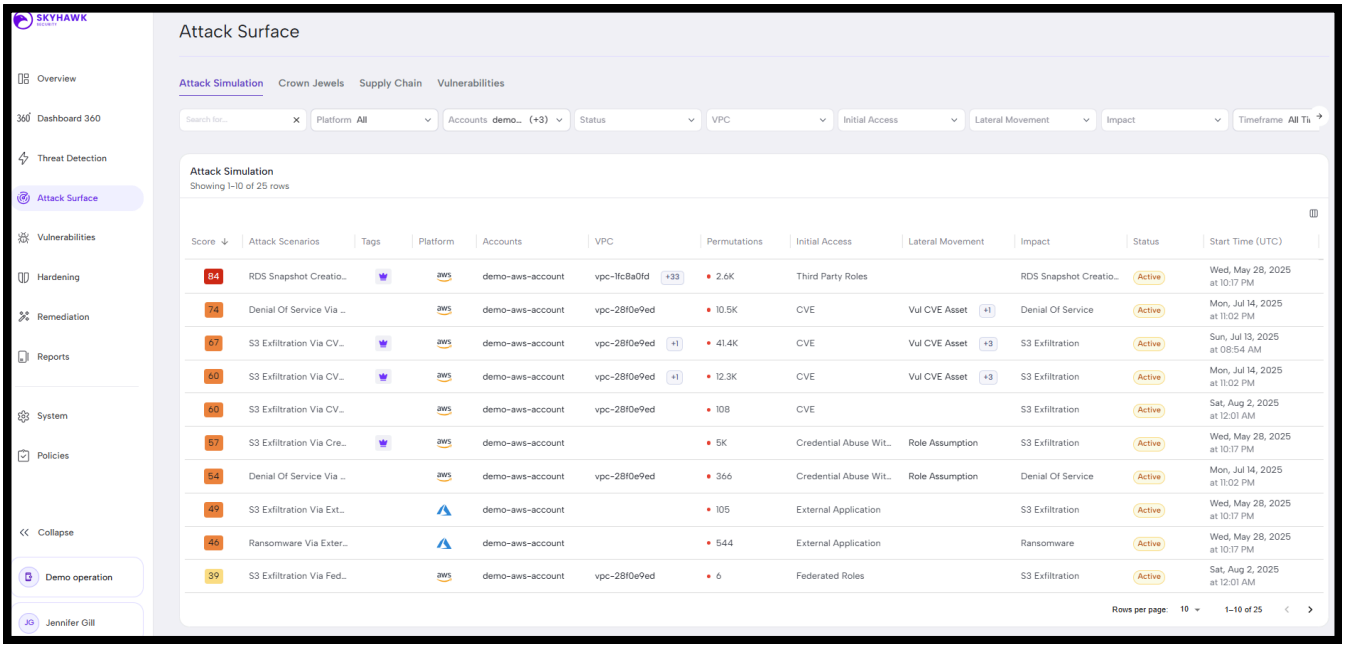

Figure 1: AI-designed attack simulations identify which attacks present the most risk as well as which crown jewels are impacted.

About Skyhawk Security

Skyhawk Security is the leader in Purple Team-Powered CDR, leveraging a multi-layer AI-based approach to identify and stop cloud threats before they become breaches. Skyhawk revolutionizes CDR 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. 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).