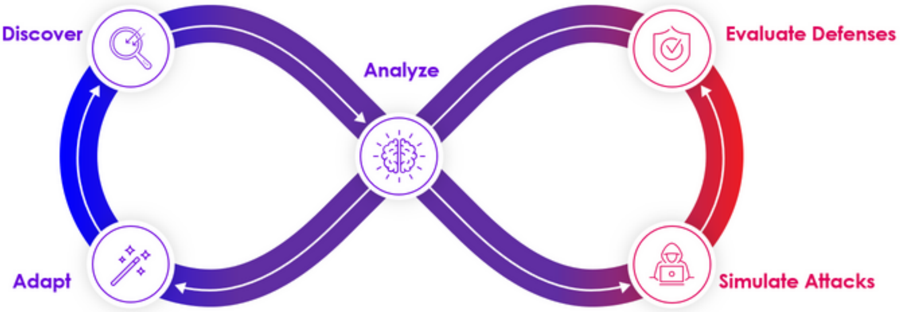
Preemptive Cloud Security: Continuous Autonomous Purple Team

Leverage the Continuous, Autonomous Purple Team to take a proactive approach to cloud security for the very first time.

Skyhawk revolutionizes CloudSecOps with proactive cloud threat detection and response (CDR) to help organizations sort through the overwhelming alerts, posture findings, and other events that traditional security tools throw at them to identify the actual threats. The Continuous Autonomous Purple Team preemptively identifies potential attack vectors to prevent cloud breaches.

How does it work:

- **Discover:** Identifies all cloud assets and maps out the paths threat actors could use to gain access.
- **Analyze:** the configuration, vulnerabilities, and security controls that are in place are fully analyzed and attack recipes are created.
- **Simulate Attacks:** Leveraging the attack recipes, the Simulation Digital Twin is used to fully execute the attacks.
- **Evaluate Defenses:** Where the attack is successful, is prioritized based on the business value of the asset that is vulnerable.
- **Adapt:** CDR machine learning models are updated for more accurate detections, pre-verified automated response is put in place for verified alerts.



Continuous Autonomous Purple Team Workflow

What does this mean for you?

- Preemptive security enables automated response thus reducing MTTD and MTTR to seconds
- Addresses the Progressive Technology-based Adversarial-Driven Risk
- Preemptive defense with Skyhawk runs continuously, adapting to changes in real time, ensuring newly introduced assets or configurations are always under protective assessment

Realize Compensating Controls for your Cloud Security

It can take up to 128 days to resolve posture findings. Threat actors will not wait for you to resolve these vulnerabilities before attacking your cloud. Skyhawk's Autonomous Continuous Purple Team identifies which threats need to be resolved now and updates your CDR to detect threats that are happening now, so your cloud is protected, event as you are resolving posture findings.

About Skyhawk Security

Skyhawk Security is the originator of Cloud Threat Detection and Response (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. Recently added Interactive CDR provides an out-of-band verification on cloud activities, incorporating principles of Zero Trust, so security teams can verify cloud events, and take action if needed. 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.