128 Days to Address Posture Findings - Threat Actors are not waiting.

Skyhawk Security delivers the compensating controls to secure your cloud, even when unresolved posture findings put you at risk.

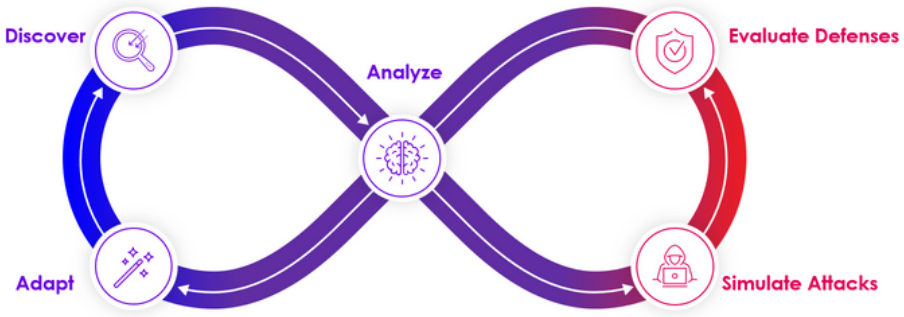
Recent industry experts have shared research that states it takes up to 128 days to resolve critical security posture findings. Threat actors will not wait for you to finish resolving these issues before they attack - so what do you have in place today to secure your cloud?

Skyhawk Security tackles this issue in two ways:
Cloud Threat Detection & Response and Continuous Autonomous Purple Team.

AI-based Autonomous Purple Team instantly analyzes customer cloud infrastructure, proactively runs attack simulation against it and uses the results to prepare verified detections, validated automated response and remediation recommendations to ensure the cloud has the most up to date security defenses in place. The security team is confident in using automated response as the attack has been rehearsed, and the team knows it is not what should happen, the alert is verified as true. Furthermore, the automated response has also been rehearsed, ensuring no production impact.

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.



How is this a compensating control?

While your security team works on updating the posture findings that other security tools identify, the purple team sees what the behavior will look like when a threat actor exploits these findings. The purple team verifies the alert and knows it does not want the activity to progress. The purple team then creates the associated automated response. As it is verified in Simulation Digital Twin, the security team can trust the automation to not impact production.

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.