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.

Cloud Threat Detection and Response

Skyhawk Synthesis Security Platform leverages three layers of AI and machine learning to sort through thousands of alerts and events to find suspicious and malicious behaviors in your cloud - now. These models are updated daily to ensure they align with the cloud architecture as it changes. The cloud is never unprotected with Skyhawk Security.

- **Malicious Behavior Indicators (MBIs):** AI-based anomaly detection is the first indication of compromise. This first level of analysis identifies events that could indicate a threat. One MBI represents dozens of events that are indicative of a malicious behavior.

- **Attack Sequence:** As threat actors move through the cloud, the MBIs begin to fall into a single attack vector where the goal of the attack is clear: exfiltrate data, leverage resources for cryptomining.

- **Generative AI CISO:** One of our evaluations of risk is our AI-based CISO. It is trained based on your cloud threats, and behaviors, and can promote an attack sequence to an alert up to 78% faster without increasing false positives.

What does this mean for you?

- Significant reduction in threat exposure
- Reduce the impact of unresolved posture findings as once threat actors take advantage of them, Skyhawk Security will find the threat
- Manage the risk from posture findings that cannot be addressed as they will impact CloudDevOps productivity
- Improve team productivity as the CDR analyzes tens of thousands of events to prioritize a dozen alerts for your security team to address

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.