Skyhawk's AI Autonomous Attack Simulation Took Control of an AWS Organization in Seconds

Skyhawk exposes a critical blind spot in traditional cloud security: Legitimate configurations and capabilities that can be dynamically chained into a full organizational takeover

What happened: Skyhawk's AI Red Team achieved full AWS Organization Take Over

Skyhawk Security recently engaged with a company to evaluate their readiness to prevent AI Autonomous attacks on their AWS cloud. Skyhawk's Agentic AI Red Team took control of a company's production AWS organization in seconds, starting with low-privileges and escalating to gaining control over a production organization.

The exercise revealed a class of threat that conventional security tooling is structurally unable to detect: attack built entirely from legitimate capabilities and configurations that no CNAPP will flag, chained together dynamically by Skyhawk's agentic AI autonomous attack simulation. There were no misconfiguration, no frontier models, no human in the loop, and no vulnerabilities used. The company carefully followed best practices and was part of the zero-critical club and yet, they were confronting Skyhawk's AI Red Team's Organization takeover. We were just as shocked as they were!

70%+
OF CLOUD ATTACKS USE IAM AS THE INITIAL ACCESS VECTOR

83%
OF CLOUD ATTACKS INVOLVE IAM OVERALL

89%
YEAR-OVER-YEAR INCREASE IN AI-ENABLED ATTACKS

The AI-enabled Adversarial View vs The Graph View: Why your CNAPP can't see it

The AI-enabled Adversarial View shows you what an AI Powered threat actor can do, and this is very different from just a graph. The AI-enabled Adversarial View shows how legitimate cloud constructs can be dynamically manipulated and chained together, just like a threat actor, to breach your cloud. In the case of this environment, Skyhawk's AI Red Team was able to take over the production AWS Organization — this is a company game over.

A traditional graph view of the environment would not surface this attack. A static attack graph analysis of the same environment showed no viable route from low privilege to organizational control, giving security teams a false sense of confidence.

This highlights the issue and why CNAPPs won't find the issue. When legitimate permissions, roles, and cloud assets are still not safe when an attacker has AI at their disposal.

Skyhawk Security Prevents Cloud Breaches and Takeovers

Skyhawk Security delivers mitigation that is specific to your cloud environment and updates continuously as your architecture and security controls evolve. It builds a live, digital model of your entire cloud estate and creates custom attacks based on the cloud security controls and architecture. Then, the platform rewrites the cloud's graph to lead to a breach or full account takeover long before a threat actor reaches their objective.

Are you ready for AI-driven attacks?

Book a 20-minute walkthrough on your own org → skyhawk.security/aws-cloud-org-takeover/