Skyhawk Synthesis: Continuous Proactive Protection

Generative AI-Based Autonomous Purple Team

Cloud adoption is driven by the agility and accessibility it provides. Ironically, these are also two factors contributing the most to the challenges organizations face in securing clouds, given the constant nature of tension between agility and security, amplified by the lack of perimeter. The high pace of advancement in generative AI adds another new vector and complexity. Threat actors now leverage Gen-AI to continuously evolve, change tactics, techniques, and approaches which lowers the skills set required to deploy an attack.

Current cloud security solutions fall short because they are reactive, not proactive. Some, like CNAPP, only detect misconfigurations or vulnerabilities after they are deployed. CDR and CIRA solutions only react to suspicious behaviors after they happen and then respond, again too late.

Skyhawk Security's Continuous Proactive Protection turns that around with the industry's first proactive — not reactive —security solution. Using Skyhawk's proprietary generative AI and ML technology, the system proactively examines your cloud, evaluates your defenses and develops offense attacks from the perspective of an attacker. It then tests your responses to the attacks, before they actually do happen, to help you determine the best way improve your cloud's security.

Operating in a continuous cycle, Skyhawk is effectively delivering proactive protection through an Autonomous Purple Team that is constantly improving your cloud security. The result is nothing less than paradigm shift in cloud security.

Benefits

- **Prioritize threats** and alerts based on the business value of the asset
- **Operationalize CTEM** for cloud to manage and minimize your threat exposure
- **Adaptive threat detection** ensures detection engineering aligned to your cloud architecture
- **Leverage an AI-based Simulation Twin** to be 100% confident in your auto-response and auto-remediation

Continuous Proactive Protection

Continuous Proactive Protection ensures that your cloud is ready for a potential attack, with an adaptive security strategy built exactly for your cloud. It acts as a continuous automated, red, and blue team in a single platform. The platform continuously discovers your cloud's assets, monitors your configuration, vulnerabilities, topology and IAM to understand the least resistance paths to your most precious assets. In

addition, the platform uses various feeds of data on real tools, methods and the techniques of threat actors attacking cloud infrastructure. The system then uses this information to simulate attacks, defines specific and verified detections and generates automated responses. In addition, the system makes hardening recommendations which are prioritized against actual threats. This new capability delivers these key benefits:

- **Proactive security:** Many CDR solutions are passive waiting for suspicious indicators of compromise to happen. By utilizing Skyhawk's continuous autonomous purple team, you stay steps ahead of threat actors with the ability to predict the tactics that will be exploited, enabling security teams to be prepared with both validated, verifies responses (CIRA) as well as prioritize the remediation of weaponized risks and correct those issues first.
- **Continuous and Adaptive protection:** Clouds are always changing, the infrastructure, configuration, permissions, are being updated to support changing business requirements. This is one of the key benefits, but it also makes security extremely challenging. Skyhawk Synthesis is always monitoring your cloud and always identifying adjustments that should be made to your security strategy to prevent cloud breaches providing a security solution that is specific to your usage of the cloud. It delivers a completely customized security approach designed exactly for your cloud.
- **Detection you can trust for response automation:** The biggest inhibitor for customers to use response automation, is to trust the detection and response to make no harm. Providing a continuous autonomous purple team results in pre-validated, trusted detections, for each pre-validated tested response are prepared, validated, and trusted.

This new capability is built with the following key building blocks:

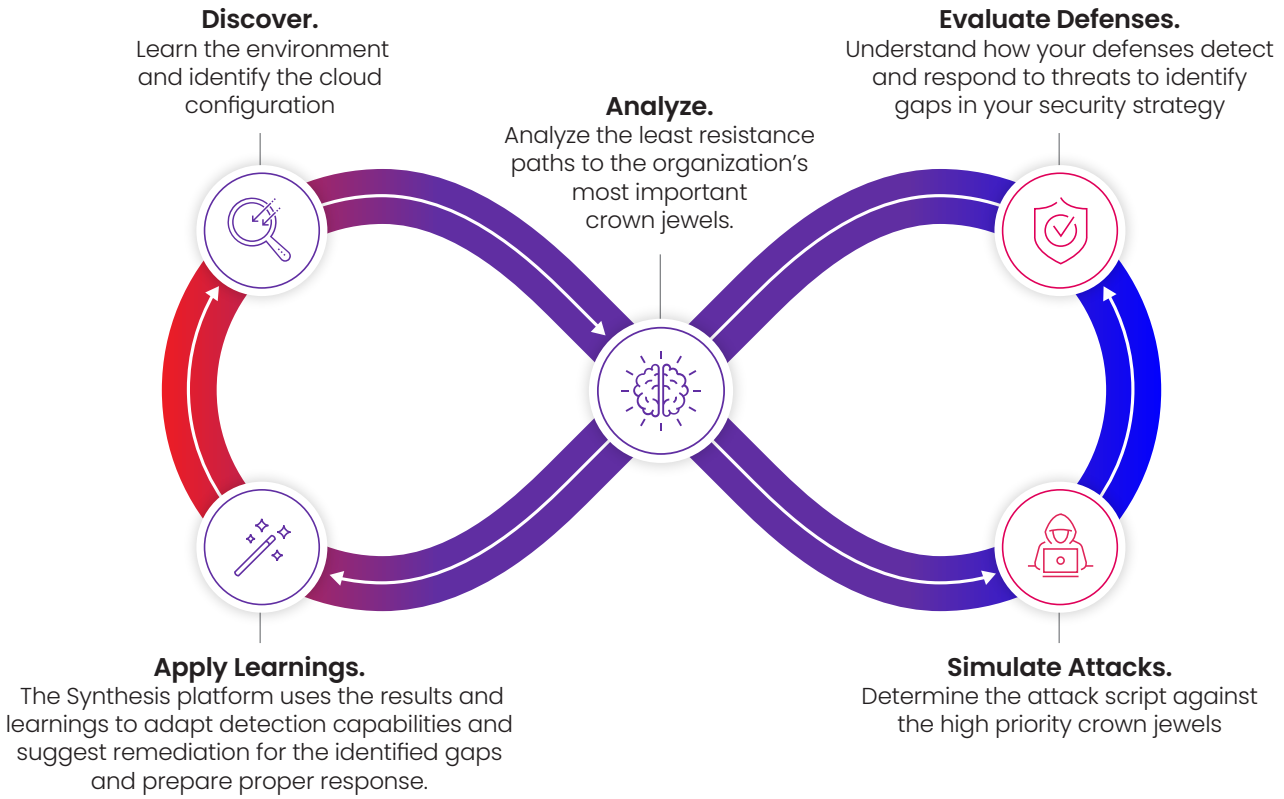
- **"Always Working" Purple Team:** Defend against attacks plans that are perpetually executed against your cloud to understand issues and weaknesses in your security posture so you can continuously improve your security.
- **Pre-validated automated response:** Not all misconfigurations, IAM privileges, or access can be completely addressed to minimize risk or closed off from exposure. Some configurations must be left due to architectural or legacy reasons. Skyhawk's pre-validated Automated response can be used to stop the progress of threat actors to prevent cloud breaches
- **Continuous learning:** Since the Skyhawk system acts as an automated purple team, AI learning techniques are being used, resulting in a continuously updating detection models, thus ensuring that new indicators are identified, minimizing the risk of threat actors learning how to evade detection.

Detection you can trust

Every business manager is looking to add more automation into their workstreams, and this is especially true for the CISO. Ensuring the fast and predictable remediation of a security issue is the ultimate goal. The only thing that is holding CISO's back from going full automation is trust. Is the triggered remediation action going to stop productivity? Shut down a website? Prevent a transaction from going through? CISOs need to trust that the remediation work will not negatively impact the business. With Project Purple, CISOs can trust the triggers. Project Purple is learning from your environment and takes the full context of the cloud, along with permissions, and normal work patterns before executing the remediation plan. Security teams can leverage automation to quickly respond to threats before the company's name ends up in the news or on social media.

How does this work?

The Skyhawk Synthesis Security Platform is a constantly working purple team for your cloud. The platform is constantly simulating attacks on your cloud, while constantly defending your cloud, to get a complete assessment of how threat actors will exploit your least resistance paths to get access to your precious data assets. Security gaps are easily identified so security teams know what to secure first and fast.



And then the entire process repeats itself, so new learnings are always used to update the security of your cloud to prevent cloud breaches.

The Business Value of the Purple Team

Simplify the CISO's Discussion regarding Exposure with the Executive Team

The CISO can now easily to go to the board and discuss in a simple way how exposures and risk was reduced to business-critical applications and crown jewel data assets. The AI-based Autonomous Purple team prioritizes threats based on the business value of the asset, and how simply a threat actor can gain access to it. The purple team is always mapping out attack exposures and scenarios so as the architecture and threat landscape changes, the purple team is able to identify which security issues to fix first to minimize exposure. to crown jewels. This will prove to auditors, regulators, and others, that there is robust security in place that is reducing threats and weaponized exposures to the most valuable business assets.

Operationalize CTEM for Cloud

Continuous Threat Exposure Management takes a programmatic approach to identifying exposures that can be weaponized by threat actors to penetrate your cloud environment and prioritize those exposures based on the business priorities and requirements. This aligns extremely well with Skyhawk Security's AI-based Autonomous Purple Team, as this innovative capability identifies security exposures in the cloud and then prioritizes them based on the business value of the asset. With Skyhawk, you can find and fix security exposures that are threatening your most valuable data assets.

Effective Exposure Hunting
The AI-based Autonomous Purple Team effectively identifies exposures and weaknesses in your cloud security and then prioritizes those threat exposures by how easily the threat actor can weaponize them to gain access to your valuable business assets. The Simulation Twin leverages AI to simulate a comprehensive attack to determine where the weaknesses in the cloud security is. This does not impact production, and is done continuously, and addresses these exposures before a threat actor can weaponize them to gain access to your crown jewels.

Adaptive Cloud Threat Detection
Organizations go to the cloud as it is agile and flexible and can adapt to changing business needs. Cloud Security tools need to also be agile and flexible or your valuable cloud data assets will be exposed. This is why CSPM, CNAPPs, and SIEMs are not well-suited to protect clouds – static tools cannot adequately protect dynamic environments. Skyhawk Security's Continuous Proactive Protection is constantly evaluating the changing cloud architecture and updating the threat detection, making recommendations to fix the posture, and identity remediation, as well as creates pre-validated auto-remediation and auto-response. This complete cloud security platform ensures the cloud security and cloud architecture are always in alignment, even as the cloud architecture changes to meet new business requirements.

Validated Security Auto-response and Auto-Remediation
Many organizations would like the opportunity to improve the efficiency of their security teams by leveraging auto-response and auto-remediation, but they cannot trust it. There is no way to do a full tabletop test without impacting production, so many do not have the infrastructure to test auto-response and auto-remediation. In the event of a security incident, nothing can be left to chance, these automated activities need to be tested and confirmed to work – the SOC cannot put the business at risk with unverified and unvalidated automations. The Simulation Twin provides pre-validated and pre-verified response and remediation. The SOC can now confidently implement these powerful automations to stop threat actors in their tracks and prevent cloud breaches. The SOC now has full confidence that their automations will work and will help reduce the risk and exposure to their business.

AI-based Tabletop Exercises
Many organizations leverage Tabletop exercises to understand how processes and procedures will hold up in the event of an attack. The issue is, a full tabletop exercise execution, if not done correctly, can give the appearance of a serious security breach! With Skyhawk Security, you can execute a comprehensive security tabletop exercise to understand exposures, vulnerabilities, and risk in your cloud within Skyhawk Security's AI-based Simulation Twin. This enables organizations to completely understand how their security platforms, processes, and people will react in the event of a breach. As mentioned, this information will be used to create verified and validated automated remediation and automated response.

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. 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).

Contact us today to learn more at skyhawk.security

SKYHAWK SECURITY