Skyhawk Security and Amazon: Better Together Cloud Security

Skyhawk Security Overview

Skyhawk Security revolutionizes cloud security with a preemptive strategy, which enables enterprises to stop attacks and prevent cloud breaches, through all layers, from the application to cloud.

Skyhawk's **Continuous Autonomous Purple Team** SaaS platform, is built on two main pillars:

- **Cloud Threat Detection and Response** – an agentless CADR, provides cyber defense, built on a multi-layer machine learning and AI-based threat detection engine.
- **The AI-Based Red Team** - a Breach and Attack Simulation that simulates weaponized risks on the cloud environment and runs them against the CADR threat detection engine, to validate the company's security controls are ready to defend against company's specific weaponized risks.

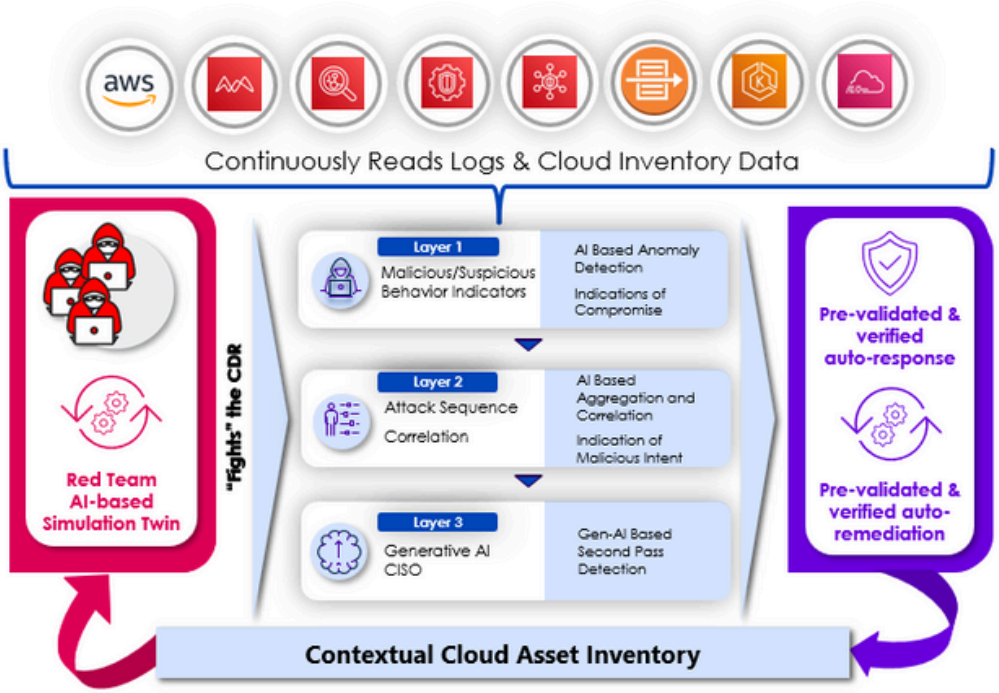

Figure 1: Skyhawk Synthesis Security Platform leverages feeds, logs, telemetries, and data sources for preemptive threat detection.

Skyhawk's analysis runs continuously in a Digital Simulation Twin so there is no disruption nor impact on production.

The solution proactively identifies weaponized risk in the cloud, across all layers of cloud applications (application, host vulnerabilities, and cloud level) and their interactions. The risks are prioritized based on the business value of the asset impacted by that weaponized risk (in CTEM terms: Scoping and Discovery). The coverage of application vulnerabilities, infrastructure vulnerabilities, cloud posture and misconfigurations, as well as sensitive data discovery are at the core of the data feeds going into the platform. This in-depth analysis allows customers to:

- Preemptively ensure accurate risk prioritization aligns with business priorities
- Automated creation of cloud security controls
- Drive operational efficiency by improving the ROI of other Amazon Security investments while reducing TCO as the Skyhawk Synthesis platform analyzes the data from these other tools (Cloud-Native Application Protection Platforms, Vulnerability scanners, data discovery scanners, etc.) and provides the conclusions, recommendations, and remediations

Skyhawk's AI-based Red Team, a cloud-native, agentless Breach and Attack Simulation module, produces a step-by-step attack scenario. It then maps a detection indicator for each step of the attack, therefore, providing a unified view of simulated attacks along with suggested preventative remediations, as well as security controls for threat detection and response (the layers of defense). This continuous autonomous process ensures there are compensating controls in place to detect threats while the application and DevOps teams implement the risk/path remediation steps. According to industry statistics, remediations can take up to four months on average to address high and critical Cloud-Native Application Protection Platform (CNAPP) findings. Threat actors are exploiting this time window and do not wait. This automated and continuous "tabletop" exercise ensures the platform has identified the attack and has a verified response should an unaddressed CNAPP finding be exploited in an incident.

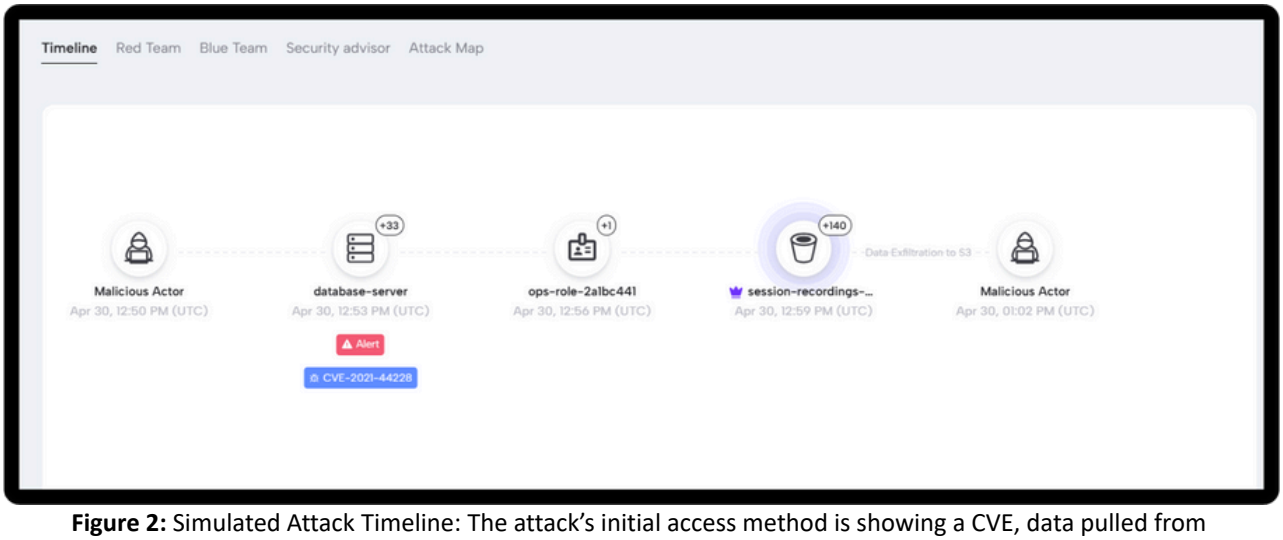

Figure 2: Simulated Attack Timeline: The attack's initial access method is showing a CVE, data pulled from Amazon Inspector, and the attack's impact on a crown jewel detected via Amazon Macie.

Figure 3: Simulated Attack Timeline: Step-by-step details of attack in Figure 2, shows the initial access, through lateral movement, to impact.

These simulations and analyses are done autonomously and continuously, without any human intervention, empowering customers to defend in hours against known exploits such as XZ Utils backdoor and the MOVEit Transfer exploit.

The results and benefits of the platform are:

- Addresses the **Progressive Technology-based Adversarial-Driven Risk**
- Bridging the gap between SOC and application teams before an attack happens
- Reducing MTTR to seconds by enabling trust in the detection and response
  - Resolving the two main inhibitors to automated response, trust in the alerts and in the response to ensure no negative impact to production and business operations
  - Preemptive security being the core which enables the trust required to reduce MTTD and MTTR to seconds
- Preemptively identifying risks and prioritizing the hundreds of thousands of vulnerabilities findings to a manageable list of true exploitable vulnerabilities by reachability analysis
- Understand true risk and reachability of vulnerabilities from the application to the cloud layers to empower the SOC to secure your business
- Preemptive defense with Skyhawk runs continuously, adapting to changes in real time, ensuring newly introduced cloud assets or configurations are always under protective assessment
- **Detecting threats in real-time to stop cloud incidents form becoming breaches**

In addition, **Skyhawk's Interactive CDR** introduces principles of Zero Trust, with an out of band verification of activities to further close the gap between SOC and application teams. When an alert is fired at the SOC, Interactive CDR sends an out of band suspicious activity notification to the cloud asset owner. The owner then confirms if they are aware of a specific activity or not. This provides additional contextual analysis between SOC and the application/DevOps teams, in real-time, to stop breaches fast.

Better together: Skyhawk and Amazon

As outlined above, the Skyhawk platform is fighting AI with AI. Combining AI-based Breach and Attack Simulations and AI-based Threat Detection, both fighting against each other on a Digital Twin, which is non-disruptive to the customer's cloud environments. To do so, the platform provides its own detections and simulations which also ingest and analyze feeds from vulnerability scanners (such as Amazon Inspector), logs and telemetries (such as Amazon Guardduty) and data classification services (such as Amazon Macie).

Incorporating these data feeds from Amazon Services into the Skyhawk Synthesis Security Platform delivers additional value and creates a strong business case to incorporate them into the customer's cloud security strategy.

Better together with Amazon Macie

Security is first and foremost a business problem, therefore, prioritization needs to be given to the crown jewels as defined by the business. Skyhawk's business priority rules take feeds from Amazon Macie (Macie) to continuously discover crown jewels with sensitive data. Skyhawk customers have provided feedback that integration with Macie provides a use case to adopt it over Wiz's Data Security Posture Management (DSPM), due to Wiz's limitations in discovering only PII, whereas healthcare customers are also looking for PHI.

The results of the Skyhawk-Macie analysis provide the justification security teams need to incorporate Macie into their overall security strategy as more comprehensive results are achieved when compared with Wiz's DSPM.

Once the data classification and discovery are analyzed by Skyhawk, there are two outcomes for customers:

- Skyhawk prioritizes Threat Detection alerts based on the potential blast radius and crown jewels at risk. This capability predicts whether an incident might put crown jewels at risk before lateral movement gets to these assets. This context guides the SOC on which alerts need to be analyzed first and the potential impact to the business of a threat detection alert.

- Second, Skyhawk's Continuous Autonomous Purple Team prioritizes the results of the simulated attacks and provides analysis of which attacks are putting the business at the most risk. This allows the security team to either prioritize remediation or build the right detections and security controls, solving the most critical business problem in security, ensuring the protection of business-critical applications.

Better together with Amazon Inspector

The Continuous Autonomous Purple Team incorporates Amazon Inspector (Inspector) vulnerability scanning to create comprehensive attacks. This information ensures the simulated attacks are leveraging CVEs information as initial access and lateral movement techniques. This analysis helps customers to prioritize the real weaponized CVEs. A Skyhawk customer, who was using Wiz, had **500,000 critical and high vulnerabilities**, which was not manageable. This customer turned on Amazon Inspector in order to leverage Skyhawk's integration. The customer reduced the number of vulnerabilities to fewer than 300—a greater than 1000-fold improvement of the better together solution over Wiz.

Better together with Amazon Guardduty

The key to cloud threat detection and response is Skyhawk's machine learning models which analyze behaviors in the runtime. These baseline models identify risky behaviors indicators, which in turn are correlated into sequences of malicious intent. Skyhawk analyzes row data such as logs and also gets feeds from services such as Amazon Guardduty (Guardduty), which are included in the corelated attack sequence. This approach allows customers to achieve optimal TCO by combining various detectors based on risk tolerance and detection coverage, especially given that Guardduty consumes flowlogs from the backbone, which avoids duplicate charges whenever possible.

In addition, Skyhawk's Continuous Autonomous Purple Team allows organizations to verify that their security controls are in place and are able to detect adversaries in every step of their attack. The AI-based Red Team demonstrates for every step of the attack, which security control will fire an alert therefore, validating the security controls for the Guardduty alerts.

The result is the aggregate of detections, Skyhawk and Guardduty, which can be pre-verified prior to an attack even starting, therefore reducing MTTD. In addition, the combined solution eliminates alert fatigue experienced by customers from Guardduty alerts as they are preemptively verified with end-to-end detections improving the confidence of the security team in the alerts and their automated responses, reducing MTTR to seconds.

Skyhawk's approach is, and has been, to be an open platform which empowers the customer to achieve the best TCO by combining multiple feeds, optimizing spend for logs, telemetry, and cloud data based on the business definition of risk versus cost.

Customer Case Study: A Fortune 100 Company improves cloud security with Amazon and Skyhawk

A Fortune 100 Skyhawk Security customer started using Inspector on all their accounts for vulnerability management instead of Wiz due to the value the security team achieved using Skyhawk's AI-based Purple Team. Skyhawk Security increased Amazon service consumption as a direct result of the value gained from these combined services.

Summary: Better Together Security for Operational Efficiency and an Optimized TCO
Skyhawk Synthesis Security platform delivers preemptive cloud security, from the application to the cloud, built on the strengths of multi-tiered AI, driving the Continuous Autonomous Purple Team.

In addition, Skyhawk's open platform approach takes feeds from Amazon security services in the customer's environment, providing another layer of security analytics, driving customer value from Amazon security services investments. This joint solution further drives ROI, enabling customers to get more value from their Amazon security services investments, as it ranks and maps weaponized threats to the business, enabling the security team to effectively prioritize the correct, targeted action.

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.