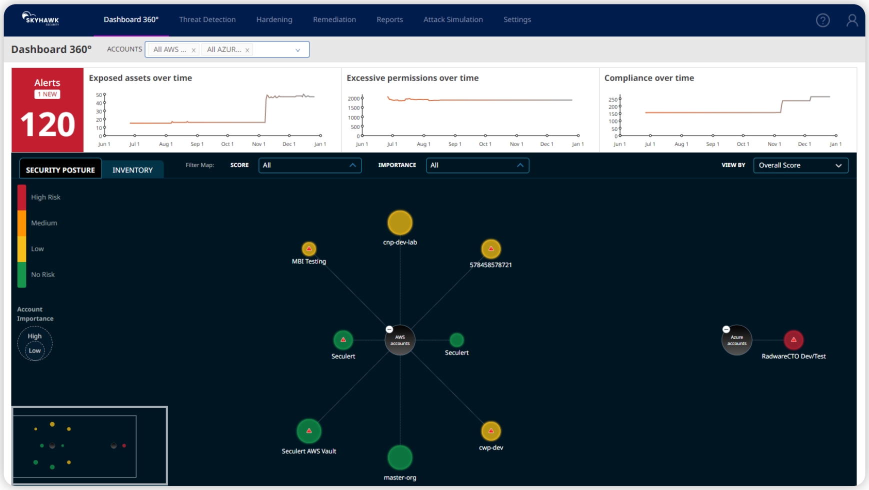
Skyhawk Synthesis Security Platform

Skyhawk Synthesis Security Platform delivers unique threat detection and response capabilities for multi-cloud environments by alerting you to actual threats and not noisy anomalies. Security Operations Center (SOC) and Cloud SecOps teams are overwhelmed with investigating and closing every "alert", most of which are not actual threats or incidents. Skyhawk Synthesis contextualizes the cloud, application, and user behavior in your environment and creates an attack storyline to identify actual threats. By focusing on actual threats in the runtime, Skyhawk improves productivity and morale of the SOC and reduces business risk.

In addition to Cloud Threat Detection and Response, Skyhawk Synthesis includes Cloud Security Posture Management (CSPM) and Identity Threat Detection and Response (ITDR). CSPM and ITDR, which are baseline cloud security features, are augmented by Skyhawk's runtime Cloud Threat Detection and Response (CDR) which monitors and analyzes all threat vectors of identity, permissions, exposed assets, and unauthorized access to identify real-time risk.

Skyhawk Synthesis Dashboard



ACCOUNTS All AWS ... All AZUR...

Filter Map: SCORE All IMPORTANCE All VIEW BY Overall Score

The simple dashboard provides a comprehensive visual describing the realerts, the trends across exposed assets, permissions, and compliance. Finally, users can easily see the cloud accounts, how they are connected, and the security posture based on risk.

Key Benefits

- Centralized runtime analysis and observability identifies risky behaviors to stop threats before they become a newsworthy incident
- Resolve issues fast with a full understanding of exactly how threat actors penetrated the environment with attack sequences
- Respond to actual incidents with contextualized models built to alert on behaviors that are atypical for your specific cloud, application, and users
- Reduce the cloud attack surface by understanding all permissions and their use so unused permissions can be safely eliminated without impacting productivity
- Support internal and external compliance initiatives with automated review
- Identify privilege escalation and other malicious uses of unsuspecting identities

Runtime Observability

This is a key differentiator for Skyhawk Synthesis – runtime observability. Other security tools will look at static points in time, evaluating configurations or permissions. This is not sufficient to detect threats. Skyhawk Synthesis looks at configurations, permissions, and activities in the environment – the runtime activities – so that you fully understand how a vulnerability was exploited. This level of monitoring shows the SOC how misconfigurations are being used to penetrate your environment. This is especially helpful with misconfigurations that cannot be addressed or take time to be addressed. This level of monitoring reduces the risk of misconfigurations that your business must tolerate.

Identifying real alerts with MBIs and the Attack Sequence and Eliminate Alert Fatigue

Skyhawk Security leverages malicious behavior indicators to create an attack sequence. Malicious behavior indicators (MBIs) are behaviors and activities that we flag over time and build into a sequence based on the metadata and logs we are collecting from the cloud. An MBI alone is not usually indicative of an attack, but it is indicative of an interesting activity. A string of MBIs creates an attack sequence and once the overall score of a sequence reaches a specific threshold it is determined to be an alert.

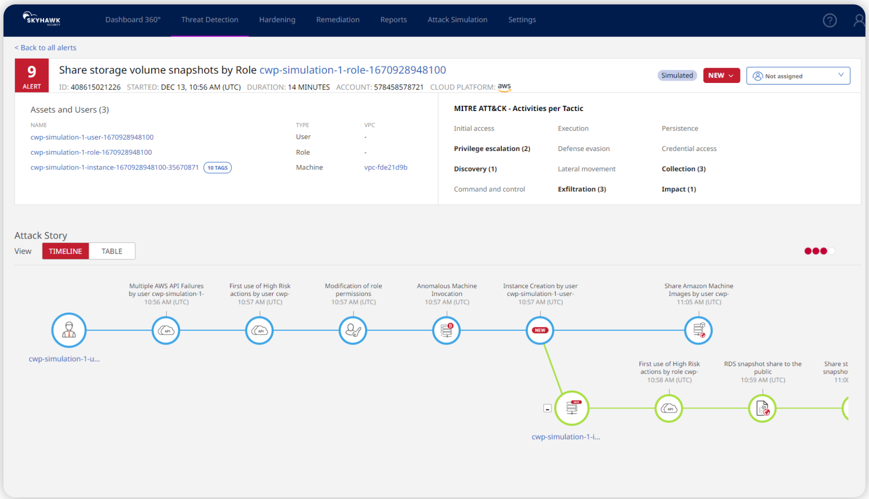
This is where we identify actual incidents which are real alerts that require your attention. The MBIs are sequenced into a storyline, which is then scored. The sequence is continuously evaluated as new MBIs are added to the sequence and scored. Once the score of the sequence is higher than 7, you get a *real*ert and you know you need to investigate. This ensures you respond to the riskiest alerts first.

Skyhawk's attack sequence provides a complete overview to the SOC of how the attacker got in and then moved around the organization. The SOC team, regardless of experience level, can easily identify the vulnerabilities and take steps to close these gaps in real-time.

Skyhawk's AI and ML are different, really.

Skyhawk Security leverages advanced machine learning (ML) techniques and artificial intelligence (AI) to build models for ongoing behavioral analysis of the runtime for more accurate threat detection. Models are trained and tuned every day on customer data at a global level. The output of the models is reviewed by security experts to ensure the model is accurate. This is done continuously to make sure the models are relevant. For more information, check out our blog, "The Science Behind our Security".

The Attack Sequence



Share storage volume snapshots by Role cwp-simulation-1-role-1670928948100

ID: 408615021226 STARTED: DEC 13, 10:56 AM (UTC) DURATION: 14 MINUTES ACCOUNT: 578458578721 CLOUD PLATFORM: aws

Assets and Users (3)

NAME	TYPE	VPC
cwp-simulation-1-user-1670928948100	User	-
cwp-simulation-1-role-1670928948100	Role	-
cwp-simulation-1-instance-1670928948100-35670871 10 TAGS	Machine	vpc-fde21d9b

MITRE ATT&CK - Activities per Tactic

Initial access	Execution	Persistence
Privilege escalation (2)	Defense evasion	Credential access
Discovery (1)	Lateral movement	**Collection (3)**
Command and control	**Exfiltration (3)**	**Impact (1)**

Attack Story

View TIMELINE TABLE

Multiple AWS API Failures by user cwp-simulation-1- 10:56 AM (UTC)
First use of High Risk actions by user cwp- 10:57 AM (UTC)
Modification of role permissions 10:57 AM (UTC)
Anomalous Machine Invocation 10:57 AM (UTC)
Instance Creation by user cwp-simulation-1-user- 10:57 AM (UTC)
Share Amazon Machine Images by user cwp- 11:05 AM (UTC)
cwp-simulation-1-u...
NEW
First use of High Risk actions by role cwp- 10:58 AM (UTC)
RDS snapshot share to the public 10:59 AM (UTC)
Share st snapsho 11:0
cwp-simulation-1-i...

Skyhawk Synthesis links together malicious behavior indicators to show how a threat actor penetrated and moved through your cloud.

Skyhawk Security helps ensure compliance with one-click reporting across a variety of common industry standards, with detailed visual reports on where you are successful and where you need to do some worksecurity experts to ensure the model is accurate. This is done continuously to make sure the models are relevant. For more information, check out our blog, “The Science Behind our Security”.

Eliminating Excessive Permissions

Access to cloud resources is granted through permissions and in order to ensure employee productivity is not impacted, many cloud teams will grant permissions broadly. Employees may only use one or two of these permissions to access the information they need, meaning the other permissions assigned to them are unused. This expands the attack surface and provides additional tools for hackers to use to penetrate your cloud.

Skyhawk Synthesis automatically detects all the permissions that are assigned to users/groups/roles and analyzes their usage. This information is presented to the SOC so they can revoke permissions if needed and reduce the attack surface.

Effectively Implement Security Best Practices

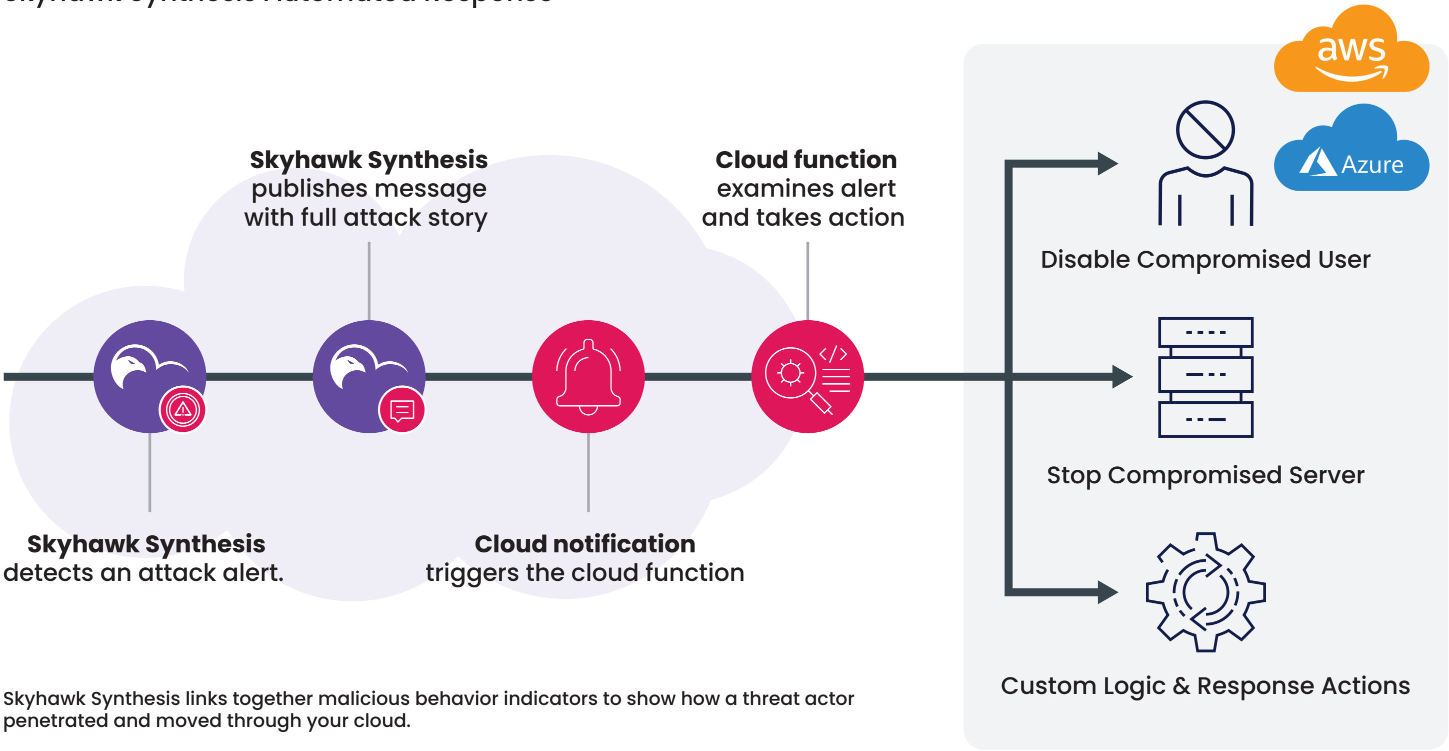
Managing security processes to ensure that your cloud security framework adheres to best practices is not an easy task. Skyhawk Security helps ensure compliance with one-click reporting across a variety of common industry standards, with detailed visual reports on where you are successful and where you need to do some work. An additional layer of protection is delivered with custom governance enforcement via a query language for custom rules.

Skyhawk Security’s misconfiguration detection and enforcement against a wide array of cloud security misconfigurations such as public exposure of assets, authentication misconfigurations, password policy, logging, networking, monitoring, and encryption. Misconfiguration alerts deliver granular details about the alert, including the affected assets, users, and the compliance rules which it violates.

User-Defined Automated Response

Automated response within Skyhawk Synthesis addresses compliance/governance issues (aka misconfigurations), public exposures, and *real*ert. You define rules within the Skyhawk Synthesis platform and only execute them if all the criteria are met. Security analysts create remediation rules with specific configurations to resolve various issues such as public exposures or misconfigurations. Auto-remediation is an optional capability, and is rule based allowing you to decide if and when to execute remediation actions.

Skyhawk Synthesis Automated Response



Skyhawk Synthesis publishes message with full attack story
Cloud function examines alert and takes action
Skyhawk Synthesis detects an attack alert.
Cloud notification triggers the cloud function
aws
Azure
Disable Compromised User
Stop Compromised Server
Custom Logic & Response Actions

Skyhawk Synthesis links together malicious behavior indicators to show how a threat actor penetrated and moved through your cloud.

A Complete Picture Of Cloud Risk

Skyhawk Synthesis takes a comprehensive approach to threat detection and response. It analyzes the configuration of your environment and all enabled permissions to fully assess the attack surface. It then analyzes the runtime within the environment, so SOC teams can see which misconfigurations or permissions are compromised and are being exploited – shutting down these vulnerabilities is where the SOC team needs to start. This is the level of security analysis that Skyhawk Synthesis provides that is a clear differentiator from all other platforms. **Understanding where your vulnerabilities are, clarifies how and when your vulnerabilities are being exploited.**

Skyhawk Synthesis not only provides a complete analysis of static configurations, it reveals risky behavior in the runtime so you can stop attacks in their tracks fast. AI and ML driven models create the right context for your business for your cloud, applications, and users, so that alerts are actual threats and not just anomalies or one-offs. The overall productivity of the team is greatly improved as they are focusing on *real*ert, and not chasing random activities.

Please visit skyhawk.security to learn more.

SKYHAWK
SECURITY