SKYHAWK
SECURITY

CLOUD THREAT DETECTION IN RUNTIME

Threat detection is a critical capability of a Security Operations Center (SOC). Organizations need to be able to detect and remediate threats in real-time. However, current threat detection tools take a "one-size fits all" approach and alert on every anomaly that occurs in your environment. This has your SOC wasting lots of time confirming that alerts are in fact, just anomalies. This causes alert fatigue and impacts the productivity of every SOC analyst.

Skyhawk Synthesis Security Platform contextualizes the cloud, application, and user behavior in your environment, and correlates this information to identify actual threats. Anomalies are easily ignored so the SOC focuses on activities that will actually cause a breach so the team can reduce the risk to the business.

THE 3 CHALLENGES OUR SOLUTION ADDRESSES FOR OUR CUSTOMERS ARE:

1. I have posture gaps and vulnerabilities that cannot be fixed or take too much time to fix impacting deployment priorities and deadlines.
2. Root-cause analysis of an attack takes weeks, piecing together all the suspicious and malicious behaviors. I don't have weeks, I have minutes. I need to do this fast.
3. Alerting on every anomaly is too time consuming and generates too many false positives. Our customers needed a solution that correlates multiple events that are connected into a single storyline that can validate the manifestation of an attack.

TO PROTECT YOUR CLOUD, THERE ARE SEVERAL QUESTIONS THAT YOU NEED TO ASK YOURSELF:

- What is going on in my environment?
- What is my threshold for risk?
- Is my cloud being accessed by unauthorized personnel or unrecognized networks?
- Have I configured my cloud correctly? Do I have ports exposed to the internet?

Skyhawk developed the only Cloud Threat Detection Solution that can help you answer those questions by providing observability into how an attack propagates by discovering and monitoring anomalous behavior in runtime throughout your organization's entire lifecycle. Our solution correlates multiple suspicious events into a graphical storyline providing the observability needed to determine how the attack is manifested in order to reduce your attack surface area, mitigate data leakage, eliminate account takeover, and thwart business disruption.

CLOUD SECURITY POSTURE MANAGEMENT (CSPM) & CLOUD PROVIDERS NOT ADDRESSING THREAT OBSERVABILITY:

CSPM vendors are scanning for vulnerabilities, misconfigurations and other static events within your cloud environment only during one particular moment in time. This in itself is useful, but as we are aware, not all misconfigurations can be fixed, or these misconfigurations may take time to be fixed. This means you are exposed until the misconfiguration is resolved. This is the real gap within CSPM tools. They do not provide observability regarding if an attack is being initiated and therefore you need runtime protection to ensure you are not being exploited. What is missing is the analysis of the behavior in the environment; runtime analysis is not part of CSPM solutions, leaving a significant gap in your threat detection and leaving your business exposed.

According to a research study, 54% of lateral movement goes undetected and represents 80% of the dwell time within an environment[1] . Cloud threat detection needs to provide observability within the runtime to provide immediate detection when multiple, correlated events occur. Identifying how the event started and how it traverses through your public cloud infrastructure allows you to identify exactly what to change in your environment.

[1] https://www.issp.com/post/3-reasons-you-can-t-fully-trust-your-security-tools-and-what-you-can-do-about-it

Some CSPM vendors and cloud providers are now touting that they include threat detection, but they lack detection breadth. In evaluating each of these vendors, make sure you look for these key capabilities.

1. AI and ML correlated events to deliver the attack sequence. Most breaches are not the result of a single event, but are made up of several events over time. When evaluating the solution, be sure it elevates the attack sequence so you are responding to actual threats. Anomalies and other events cause alert fatigue and distracting noise in the environment.

    a No existing solutions are able to identify the sequence of events that translates into graphical attack storyline on how an attack propagates thereby requiring weeks of forensic analysis. These vendors report each detected anomaly or suspicious event as an individual alert which should be investigated by Security or SOC teams. This is very noisy and causes alert fatigue.

    b Skyhawk monitors multiple malicious behavior indicators, correlates them together into an attack story and generates an attack alert only when a story reaches a high enough risk score. This greatly reduces the number of alerts and false positives while enabling security teams understand the end-to-end threat chain currently occurring in their cloud.

2. Many vendors deliver threat detection on static information – but do not detect threats on activity and dynamic context. Skyhawk Synthesis monitors behaviors in the runtime. A few examples are:

    a Limited anomalous user behavior: Simply providing geo location and first time API usage

    b Limited anomalous role behavior: Many vendors do not detect anomalous behavior for nonhuman identities, like machine roles, functions roles, cross-account roles and other types of roles

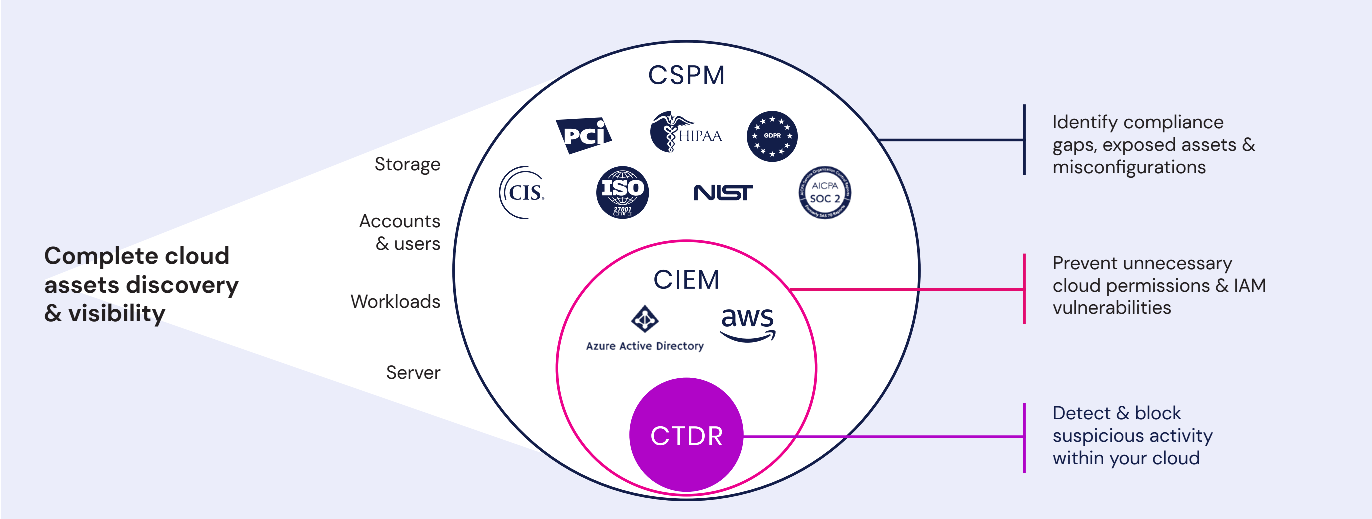
    c Limited anomalous North-South network communications

    d Limited anomalous East-West network communications

    e Limited anomalous access to S3 storage

3. The ability to detect and correlate from a large amount of data is lacking in these solutions. They do not have the scalability cloud environments need. Skyhawk has been built to scale for large enterprise accounts. One of our current customers correlates over 120 TB of data per month using our solution.

SKYHAWK SYNTHESIS SECURITY PLATFORM


Complete cloud assets discovery & visibility
Storage
Accounts & users
Workloads
Server
CSPM
PCI
HIPAA
GDPR
CIS
ISO 27001
NIST
AICPA SOC 2
CIEM
Azure Active Directory
aws
CTDR
Identify compliance gaps, exposed assets & misconfigurations
Prevent unnecessary cloud permissions & IAM vulnerabilities
Detect & block suspicious activity within your cloud

CLOUD THREAT DETECTION AND RESPONSE:

Skyhawk Security offers an accretive solution to your existing cloud security posture management tools. By utilizing our artificial intelligence and machine learning, our solution creates a baseline of typical behavior within your environment based on observed behaviors. In addition to metadata, our solution ingests your logs to gain a precise outlook on the activities within your environment. Leveraging this behavioral information within your environment, AI and ML create a contextualized baseline for what is normal for your environment so any alerts that are raised are actual alerts that require attention and not smaller one-off events.

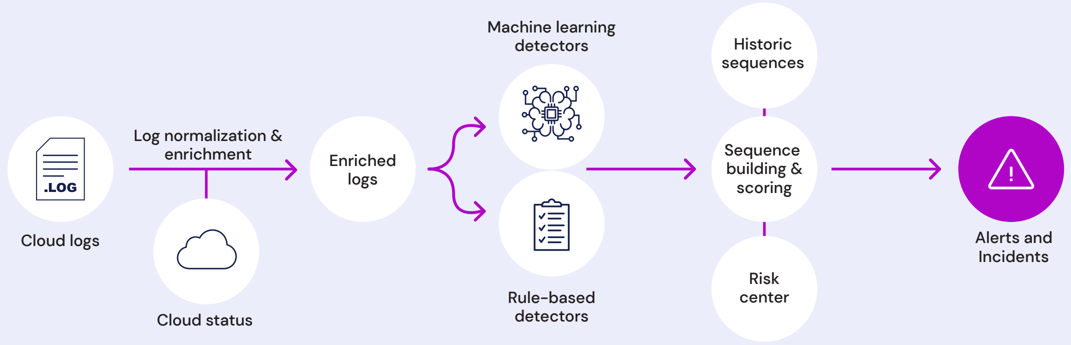
There are several anomalies that Skyhawk identifies across several factors. A few examples are:

- API: If the API is accessed at an unusual time of day, or by an unusual user
- Time of Day: Is the employee suddenly working at a new time?
- Machine invocations: Is a machine being invoked at an abnormal time or by a new user?
- Storage access: Is a new application or user accessing storage?

DETONATION OF MALICIOUS BEHAVIOR INDICATORS (MBIS):

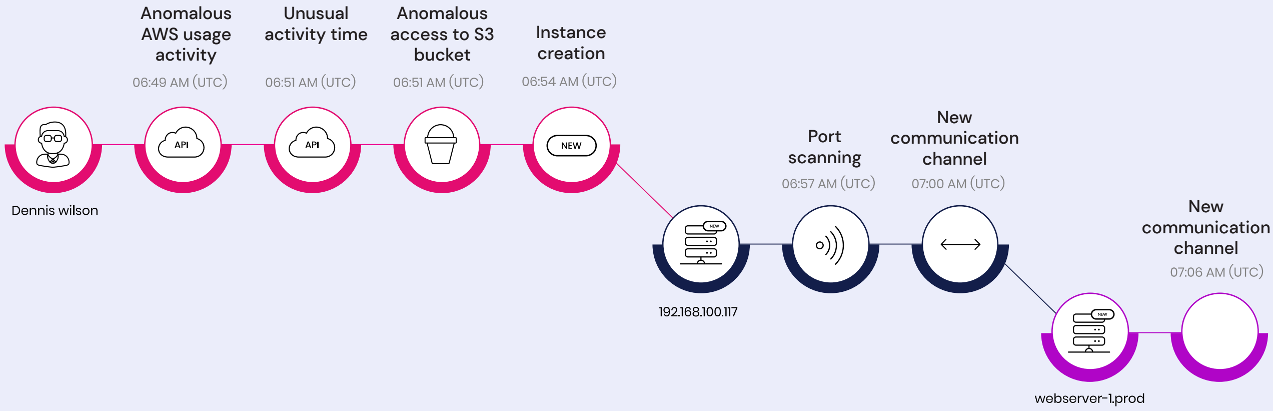
Machine learning and historical rules-based detectors analyze activities as they occur to create an MBI. MBIs are created when anomalies have been identified by deviating from the baseline or a very risky action has been executed which warrants further investigation. MBIs are single events which the solution correlates together into a sequence so security teams can understand the bigger picture, providing visibility into a hacker's path inside your cloud and potential next steps for stopping them. The sequence ensures that the bigger picture and overall threats are better understood, reducing false positives, and ensuring teams do not waste their time chasing non-events. Currently, there are over 70 MBIs which are used to characterize risky behaviors, and more are being developed everyday.

THE DETECTION PROCESSES: HOW A SEQUENCE IS BUILT INTO AN INCIDENT



The sequences are dynamically scored, and high scoring sequences generate an alert which will reduce false positives and save your team’s time in investigating these incidents. The totality of the MBIs makes it clear when an attack is underway and also makes it clear when there are no threats.

ATTACK STORY



Along with the sequence of the attack, the Skyhawk Synthesis Security Platform includes information of what tactics and techniques of the MITRE ATT&CK framework are being exploited to enable teams to respond better.

HOW SKYHAWK SERVICES FLOW AND THE SECURITY OF THE INCIDENT DATA

Skyhawk Synthesis ingest logs from your cloud infrastructure in order to process the data and create a storyline of a possible attack. The key activities are described below and the image: "Skyhawk Services: From Data Ingestion to the Attack Sequence" shows the data flow.

STEP 01.

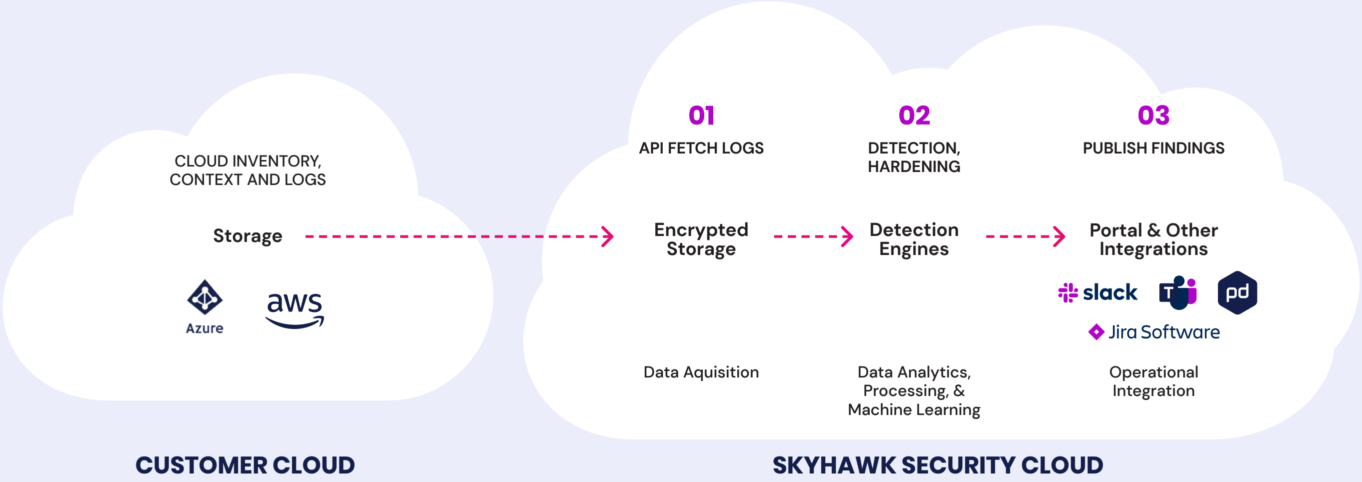
We collect data from two types of logs across the cloud environment.

- Meta data: This is simply a descriptive inventory data information. This data includes for example: Workloads info/managed services used/PaaS/ users/groups/permissions/ network definitions and more. Each type of data is collected in a different periodicity. The data is collected via the public cloud CLI/API and stored in our database. The data is used for CDR, CSPM, and CIEM needs, such as threat detection, misconfiguration, permission hardening, public exposure and for general visibility purposes.
- Log data: This is transactional event-based telemetry such as activity logs, flow logs, storage logs, and DNS Query logs. Log data is collected by the recommended AWS best practices in a form of notification mechanism updating us once a new file is available. The primary goal is to perform analysis to detect threats and excessive permissions. At a high level, the generated telemetries provide granular visibility to various activities, such as network transactions (east-west, north-south, vice-versa), API activity, access to data, identity administration and more.

STEP 2.

The collected data is aggregated, enriched, and analyzed for machine learning and AI.

SKYHAWK SERVICES: FROM DATA INGESTION TO THE ATTACK SEQUENCE



STEP 3.

The analysis engines within the platform process the log data to draw conclusions and provide remediation recommendations.

- Misconfiguration and Permission Hardening: This analysis is run every hour for constant security gaps identification.
- Rule-based detectors: Responsible in generating MBIs, in different layers: the network or cloud native. Detectors ranging between simple rules to algorithms running in different periodicity.
- Machine Learning detectors: Responsible for advanced and complex detections to generate MBIs. Learning and prediction processes are entirely built-in.
- Sequence Builder: Each generated MBI (Malicious Behavior Indicator) is tentatively correlated to either existing sequence or to a new attack sequence.
- Scoring, Risk center: This module is responsible to prioritize each of our different findings: Misconfigurations, public exposure, permission hardening warnings, threat detection alerts and MBIs.

STEP 4.

Users can connect to the system, via our web portal or via API.

Portal – presents role-based access control (RBAC) functionalities, that can be administered from our portal.

API – authenticated RESTful API, to be used for integration with 3rd party systems (SIEM, ticketing system, collaboration tools, IR tools, more).

STEP 5.

Integration with customer 3rd party systems can be achieved via native integration or our open source integration modules and currently have integration with:

- Mail
- Teams
- Slack
- Jira
- PagerDuty
- Azure Sentinel
- S3 Logger – this module allows easy integration with any SIEM system that supports consumption of data from S3 bucket

SKYHAWK CLOUD RUNTIME SECURITY PLATFORM: COMPREHENSIVE CLOUD SECURITY

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

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. Our team of data scientists is constantly updating the data to continuously update the model so that we can more accurately predict real threats versus one-off behaviors. The overall productivity of the security team is greatly improved as they are focus on activities executed by real threat actors.

ATTACK SIMULATION

Attack simulation capabilities allow for the simulation of advanced attack scenarios to quickly surface vulnerabilities and areas of weakness. The attack simulation catalog includes cloud-native data exfiltration and crypto-mining with a full description of the attack steps. These simulations enable organizations to understand how their environment would respond and what they need to do to address any areas of weakness.

FOUNDATIONAL SECURITY CAPABILITIES: CIEM AND CSPM

Our platform also includes foundational security capabilities: Cloud Security Posture Management (CSPM) and Cloud Infrastructure and Entitlement Management (CIEM). The platform includes compliance verification, detection of cloud misconfigurations, identifying publicly exposed assets and automatic governance enforcement to ensure your cloud environment is secure.

Detailed, one-click compliance reports for a wide range of industry and national compliance standards, including PCI DSS, SOC2, CIS Foundations, NIST Cyber

Security Framework, ISO 27001 and more, provide both high-level verification of your compliance status and line-by-line assessment of each individual criterion in the standard. CSPM also supports customized governance reports via a built-on query language, tailored to your specific needs.

Our CIEM capabilities discover, monitor, and remediate entitlement misconfigurations throughout your organization's entire CI/CD process within your infrastructure, applications, IAC templates and policies to reduce your attack surface area, mitigate data leakage, eliminate account takeover, and thwart business disruption. It takes a unique approach to hardening permissions by analyzing the gap between defined and used permissions and it provides coverage for all permission types, including users, machines, roles, groups, cross-account and federated roles.

The platform includes shift-left security capabilities as well. For companies interested in assessing their threat landscape during the development phase, Skyhawk's attack simulation capabilities offer an assessment of unknown network communications after an M&A event or simply getting observability in the architecture design of an account infrastructure prior to deployment. Providing observability into the design phase will help your DevSecOps team eliminate flaws prior to production, optimizing overall cost and security.

Skyhawk Synthesis delivers delivers a comprehensive security solution for your cloud environment in a simple to use interface making it easy to understand the security relationship between your cloud assets.

TO REVIEW OUR SOLUTION,
PLEASE VISIT US AT WWW.SKYHAWK.SECURITY