



THREE COMMON USE CASES FOR CLOUD THREAT DETECTION



Introduction

There are many different suspicious behaviors that we track in the Skyhawk Synthesis Security Platform that individually look suspicious but may or may not cause a breach. In this paper, we will look at what the outcome is when threat actors execute several of these suspicious behaviors in a row, and how we observe these behaviors, and identify create actual threat to your business. There are three main threats that hackers are attempting to execute:



Malicious usage of assets



Business Disruption



Exfiltration (theft) of data

Security teams are given an impossible task – be right 100% of the time. This is not possible, and it is for this reason that threat actors will penetrate your environment. Threat actors will get into your cloud with perfectly configured permissions, a perfectly configured cloud, and perfectly configured posture. Threat actors only need to be right once, and this is why you need threat detection and breach prevention. This does not mean you should abandon your prevention strategies – cloud security posture, managing permissions, and reducing the attack surface are critical components of your security. However, you need to make sure you can identify threat actors once they break through your first line of defense.

Skyhawk Synthesis Security Platform is a comprehensive cloud security platform that includes cloud security posture management, cloud identity and entitlement management, and cloud threat detection and response. It covers your security strategy from prevention to detection, to prevent breaches.

How are these incidents used for threat actor gain?

Threat actors compromise organizations for many reasons. The goals behind each of these threats are different and a single threat can help achieve several goals. For example, threat actors might be trying steal data for financial gain, espionage, leak the data to embarrass the organization, or even just to keep their hacking skills sharp. Each of the sections below provides detail on what hackers can achieve.

Skyhawk Synthesis Security Platform is a comprehensive cloud security platform that includes cloud security posture management, cloud identity and entitlement management, and cloud threat detection and response. It covers your security strategy from prevention to detection, to prevent breaches.

Malicious usage of assets

Threat actors are always on the hunt for compute and other resources that they can use for financial gain. Compute assets can be used to mine for crypto, which is called cryptojacking. Hackers mine for cryptocurrency and other assets that can be readily converted to money. These funds can then be used to further their other endeavors or be used as a salary to support their organization.

Your cloud assets can also be used to create more powerful botnets which are used to execute large scale cloud attacks. Botnets are groups of devices that run one or more bots and can be used to perform distributed denial-of-service attacks, steal data, send spam, and allow the threat actor to access a device and leverage its connection to access data. Disrupting the business can damage the brand and cause embarrassment for the organization. Stealing data can cause significant damage to the brand and embarrassment for the company. Sometimes specific data and IP is stolen for a competitor or to be sold to a competitor so the competitor can attempt to gain an advantage.

Business Disruption

Many threat actors simply want to damage the brand of a particular company and cause irreparable harm to their image so that people are weary to transact business with them. The disruption can take many forms, including hacking their social media accounts, taking down their website, or leveraging banking credentials to drain their bank accounts. Threat actors may also want to deliver a competitive advantage. For example, to execute an attack on a large e-commerce site during black Friday in order to create downtime for competition.

Many times, a business disruption is not for financial gain at all. A threat actor will attack a high-profile company to boost their own reputation. The hacker can then brag that they were able to penetrate a particular organization whether it is a well-known company, a government entity, or a person.

Stealing valuable data

There are many times a threat actor simply wants to steal valuable data for financial gain. The data is then returned to the company once a payment is made to the threat actor and their organization. The company then has to hope that a copy of the data has not been made and will be exploited even if they make the required payment. The hacker might want to embarrass the organization by leaking the data.

Another aspect to this is that the hacker may not be stealing the data just for themselves. They might be stealing this data to undermine a competitor or selling what they steal to the organization's competitor. This is another way to generate funds for their own organization.

How do we detect these threats before they become breaches?

At Skyhawk Security, we want to detect threats, but we do not want to overwhelm teams with alerts. At Skyhawk we avoid these distracting alerts with a multi-level AI approach. We build machine learning behavioral models to identify behaviors as they deviate from what is typical of your environment. These behaviors are analyzed using several machine learning strategies to sort through all the data to identify realerts.

How it works?

Logs and telemetry are collected from across your entire cloud environment. The collected data is enriched and cleaned so it can be used to create machine learning models to measure deviations from the baseline behaviors in the cloud. These advanced machine learning models monitor the runtime to find the behaviors that will eventually lead to an embarrassing cloud breach. Skyhawk Synthesis creates models across three main granularity levels within the cloud.

Table 1: Examples of Machine Learning Models

Machine Learning Model Granularity	Examples of Models Built
Skyhawk Security Cloud	Risk scoring – Assesses overall risk so that sequences are appropriately scored and only raised to a realert when there is actual malicious activity in your cloud.
Customer Cloud	Network Behavior – Models typical data volumes which are moved throughout the environment.
User, role, asset, or function – models are created for each of these cloud assets	Network Traffic – Monitors what network traffic each asset typically generates over the course of the day.
Identity Management	API Usage – Monitors which APIs each asset typically uses.

These models are constantly trained with new logs and data and are examined and updated on a daily basis to eliminate drift. This ensures the models are accurate, and that means the threat detection is accurate. Skyhawk Synthesis does not want to overwhelm you with meaningless alerts that are just anomalies and one-off events. When the platform raises an alert – it is something you and your team should be investigating immediately. It is not “maybe an issue” or “something you might want to investigate,” if the platform raises this alert, it needs your attention now.



Figure 1: An overview of machine learning model environment

The output of the models is examined. One-offs and anomalies are singled out and further analyzed and suspicious behavior indicators are identified. The first output from the models is a malicious behavior indicator. Malicious behavior indicators (MBIs) are activities that Skyhawk has identified as risky behaviors that require an investigation and may pose a threat to your business based on our own AI and ML modeling of what is normal for your cloud.

Table 2: Examples of Malicious Behavior Indicators

Types of MBIs	Description
Malicious Communications	Anomalous and abnormal communications to an unusual IP address
Log Activity	Anomalous and abnormal log activities, for example logs are no longer collected from specific sources
RDS Activity	Changes to RDS databases that weaken their security
Share to Unknown	Changes or behaviors of S3 assets that are anomalous
Identity Management	Changes in user credentials, especially when viewed frequently

The malicious behavior indicators are correlated into an attack sequence. The models look at the various MBIs in the environment and begin to sort them into storylines. The stories show how threat actors are moving about the environment to access your crown jewels.

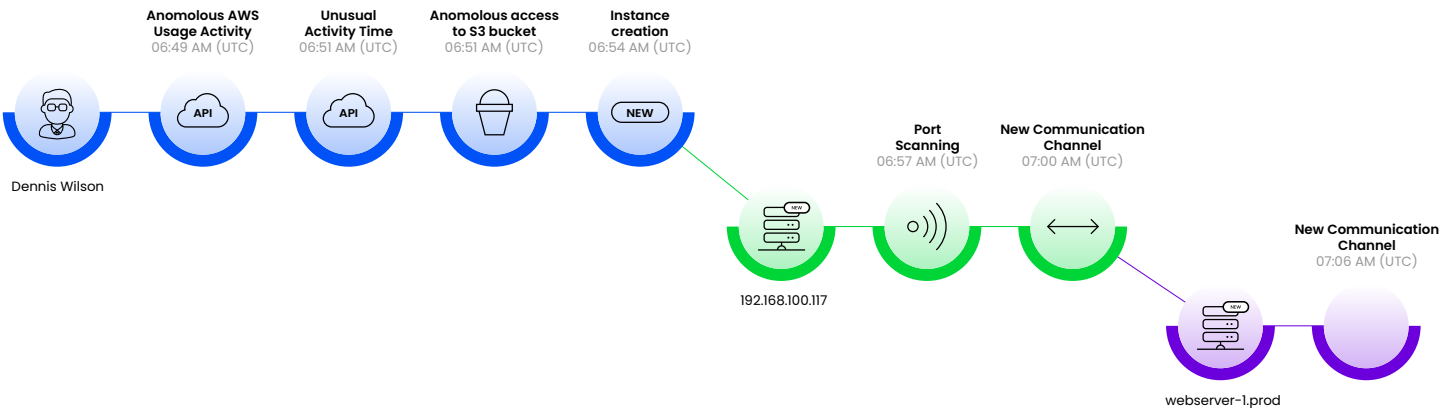


Figure 2: Example of an Attack Sequence

Finally, the models score the attack sequence. Across the entire cloud environment, the models measure risk to give an accurate assessment of the attack sequence to determine if it is an alert or not. Once a threshold is reached, it is raised to a real alert. Leveraging our integration with ChatGPT, the platform is able to determine if the attack sequence needs to be raised to an alert faster. To learn how ChatGPT works in Skyhawk Synthesis, see Appendix A.



Figure 3: An Overview of the Cloud Breach Prevention Process

Malicious use of assets

In order to detect malicious use of assets, Skyhawk Synthesis examines multiple data points to identify malicious usage of assets like cryptomining. For example, if the platform detects any amount of network traffic to a mining pool, there is a high degree of certainty that there is crypto activity in the machines. It is highly unusual for a business machine to have any network traffic flowing to a mining pool. The platform also learns how machines are initiated in the environment. If a user is initiating many instances in an anomalous region or different types of machines with a higher price per instance – this also raises events in the platform. The ML models will then correlate these activities into a sequence which shows how the attack unfolded, so the security teams know which events to look for in the future, to make sure it doesn't happen again.

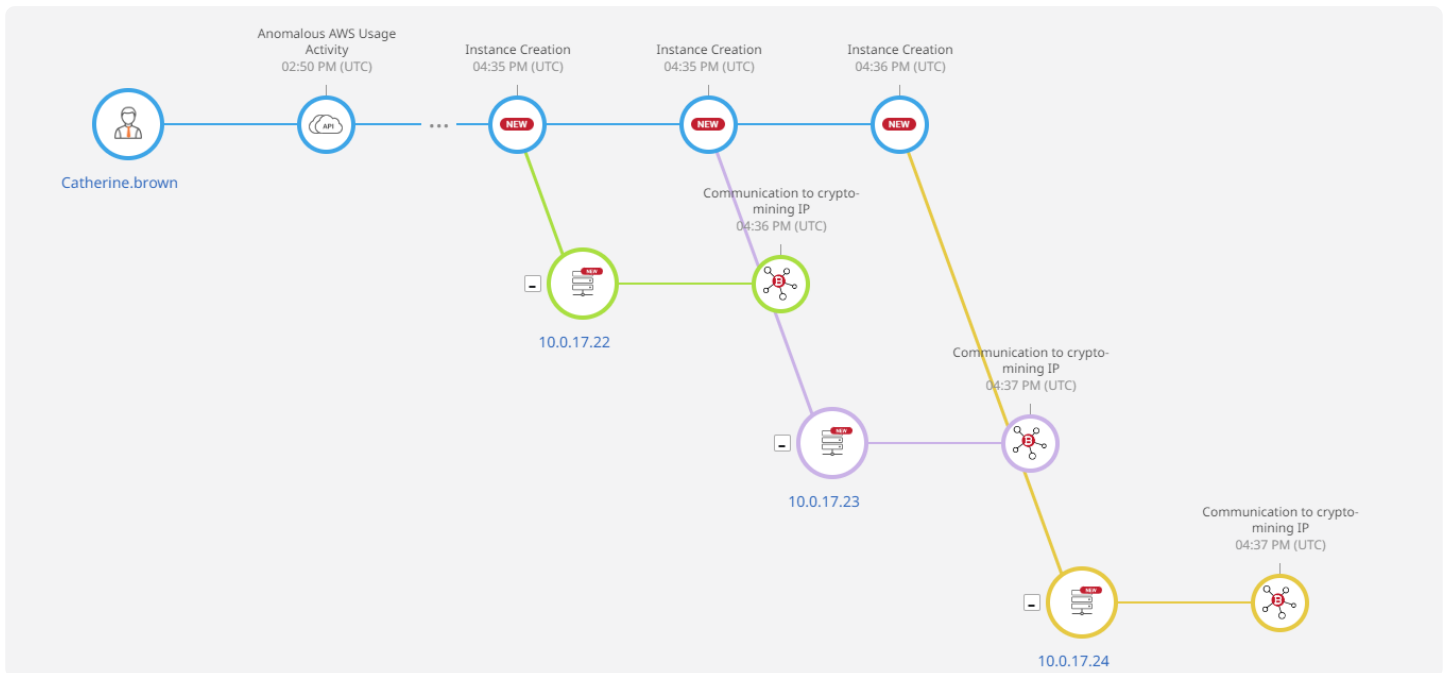


Figure 4: An attack sequence depicting cryptomining.

Business Disruption

Detecting a business disruption can be challenging because there are so many actions that can disrupt a business. Deleting data, rerouting network traffic, and taking down the website can all lead to business disruption. However, these can also be normal activities that occur over the course of the workday. When looking for activities that would lead to a business disruption, the platform looks for events that are out of the ordinary for a user. Additionally, one event is not enough, the platform will look for several anomalous events executed over time.

Using advanced threat detection techniques, the platform will look for a user that doesn't normally delete data suddenly starts to delete vast amounts of data. This anomalous behavior would raise an activity in the Skyhawk Synthesis Security Platform that it would track to see if it evolves to an incident.

Stealing Valuable Data

When the goal of the threat actor is to steal data, there are certain behaviors you will see in the environment. For example, you will see a threat actor trying to determine the limits of the compromised user's permissions. How far can they get into your cloud? They will start moving about using API calls, etc. to see what assets they can access.

Threat actors might also reroute traffic between instances and resources. For example, they might redirect end-customers to a different website. Threat actors can enforce static IP addresses and then move the static IP from the company's account to their own cloud account. The experience of the end-customer is the same, so they simply put in their credentials and now the threat actor has them. In this case, the platform will look for static IP moving to different accounts to detect the impending disruption.

Here is an example of what an attack sequence looks like when the goal is data exfiltration.

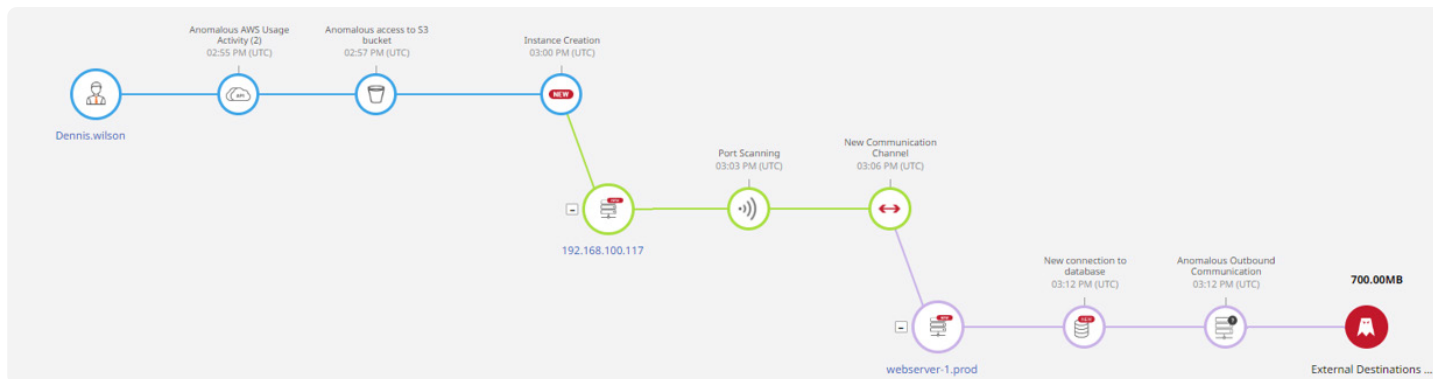


Figure 5: An example of a sequence that ended with data exfiltration.

Conclusion

The threats that security teams are dealing with are increasingly complex. Single events that are deemed suspicious could be just employees doing their job but are just doing something out of the ordinary for them or their role for many reasons. Security teams can be overwhelmed researching these suspicious activities. Skyhawk Synthesis helps security teams by correlated these events and looking at the sum of the risk to determine if something is truly a threat or risk to the business. The platform looks at the intent behind these behaviors to accurately identify threats, so security teams can stop these activities before they become full-blown breaches that harm your employees, your customers, and your organization.

About Skyhawk Security

Skyhawk Security is the originator of Cloud threat Detection and Response (CDR), helping hundreds of users map and remediate sophisticated threats to cloud infrastructure in minutes. Led by a team of cyber security and cloud professionals who built the original CSPM category, Skyhawk Security evolves cloud security posture management far beyond scanning and static configuration analysis. Instead, using advanced AI sequencing of context-based behaviors, Skyhawk provides CDR in the 'Runtime Hub'. The sequence of these events elevates the awareness of actual alerts, or realerts, which pose a threat to the business, reducing the noise and alert fatigue that other tools create. Threat detection gives organizations the observability they need to fully understand the business impact to mitigate risk, so security analysts can quickly detect and remediate malicious activities across multiple cloud platforms *as they happen*.

Contact us today to learn more!
skyhawk.security/get-free-cspm/

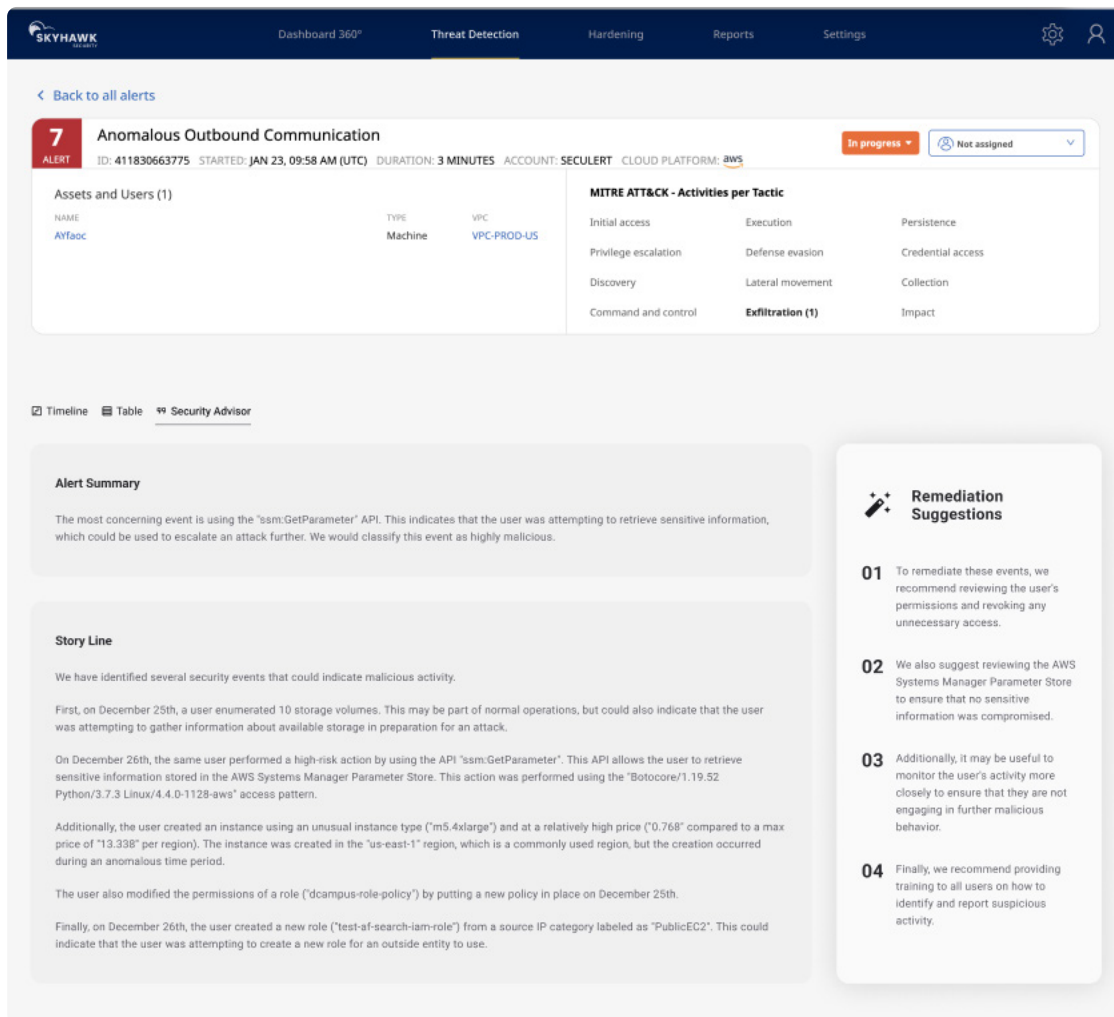
Appendix

Appendix A: Integration with ChatGPT

Machine learning and Artificial Intelligence can provide additional insights with advanced data processing and by processing large volumes of information and drawing insights. Skyhawk Security recognized the value of incorporating Chat GPT into the product to improve the accessibility of security and to detect threats and incidents faster, so organizations realize their goal – to prevent cloud breaches.

Security Advisor

Skyhawk Synthesis Security Platform leverages ChatGPT in two ways. The first is Security Advisor, which leverages ChatGPT to provide a simplified explanation of realerts. This improves the accessibility of security to all members of the security team so they can more easily understand the realert and how to fix it.



The screenshot displays the Skyhawk Security Platform interface. At the top, there's a navigation bar with links to Dashboard 360°, Threat Detection, Hardening, Reports, and Settings. Below this, a breadcrumb trail shows 'Back to all alerts'. The main content area features an alert titled 'Anomalous Outbound Communication' with a red '7 ALERT' badge. The alert details include ID: 411830663775, STARTED: JAN 23, 09:58 AM (UTC), DURATION: 3 MINUTES, ACCOUNT: SECULERT, and CLOUD PLATFORM: AWS. A status bar indicates 'In progress' and 'Not assigned'. Below the alert details, there's a table for 'Assets and Users (1)' with columns for NAME, TYPE, and VPC. The table shows one entry: 'AYTaoC' (Machine) in 'VPC-PROD-US'. To the right of the table is a 'MITRE ATT&CK - Activities per Tactic' section with a grid of activities: Initial access, Execution, Persistence, Privilege escalation, Defense evasion, Credential access, Discovery, Lateral movement, Collection, Command and control, and Exfiltration (1). Below the table, there are tabs for 'Timeline', 'Table', and 'Security Advisor'. The 'Security Advisor' tab is active, showing an 'Alert Summary' and a 'Story Line'. The 'Alert Summary' states: 'The most concerning event is using the "ssm:GetParameter" API. This indicates that the user was attempting to retrieve sensitive information, which could be used to escalate an attack further. We would classify this event as highly malicious.' The 'Story Line' provides a detailed narrative of the events, starting with a user enumerating storage volumes on December 25th, followed by a high-risk action using the 'ssm:GetParameter' API on December 26th, and finally, the user creating a new role ('test-af-search-iam-role') from a source IP category labeled as 'PublicEC2'. On the right side of the 'Security Advisor' tab, there's a 'Remediation Suggestions' section with four numbered items: 01. Review user permissions, 02. Review AWS Systems Manager Parameter Store, 03. Monitor user activity, and 04. Provide training to all users.

Figure 6: Security Advisor powered by ChatGPT

Security Advisor provides three key components:

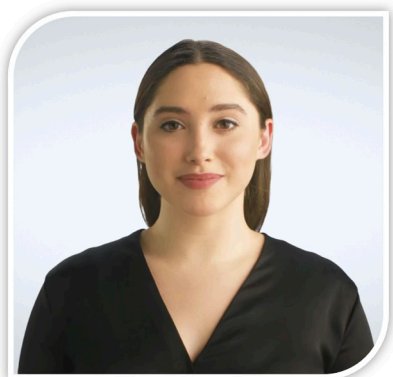
- Alert Summary: Provides a simplified explanation of the realert so you can better understand the problem and how to solve it.
- Story Line: The story line gives a detailed description of the attack sequence. It provides details on when each MBI occurred and when and the order of events that make up the attack.
- Remediation Suggestions: Finally, suggestions are made for how to ensure the attack does not happen again.

Earlier Detection of Threats with Collective Intelligence-Driven Second Opinion (CISO)

The second impact of integration with ChatGPT is it allows for earlier detection. Skyhawk Synthesis leverages CISO to assess the overall risk of the attack sequence to raise it to a realert earlier. This allows organizations to stop threats before a breach is realized.

How does this work?

The platform engages with Artificial Intelligence Agents (AI agents) to get their opinion on the attack sequence. Here are two examples of our AI agents. We have two AI agents, Sky and Hawk, who will evaluate the sequence.



"Hi, my name is Sky. I would score the sequence as 7 out of 10 in terms of maliciousness because a combination of events in it make it look suspicious, but other events make it more benign in my view."

"Hi, my name is Hawk. I would score it as 8 out of 10 because this combination of events is much more suspicious in my view and I don't think the events that Sky pointed out make it more benign."



The platform asks many, many AI agents to see how they would score the sequence. Each answer is plotted along a curve. We can then compute the average and variance which gives us a lot of confidence that the threat we have promoted to an alert is, in fact, an alert and requires attention. This threat detection is done with fewer MBIs so security teams can act much faster. Additionally, it ensures that security teams are not wasting their resources. Once the platform flags an alert as requiring attention, the security team knows this should be taken seriously. This is not a potential issue; it is a threat that is in progress and action needs to be taken to prevent a breach.



Figure 7: Results from hundreds of AI Agents are plotted and the agreed upon score is calculated.

ChatGPT enriches our own machine learning techniques and helps us accelerate our threat detection to prevent breaches. Our analysis shows that in 78% of the cases, Chat GPT helped alert truly suspicious incidents faster. It did so while not adding false positives to the system. We conducted many tests to benign sequences of events. Additionally, the true positive rate was increased by more than 20%, which was confirmed on tests conducted on actual attacks.

To learn more about Skyhawk Synthesis's integration with ChatGPT, please visit our website:
www.skyhawk.security

- Video: https://www.youtube.com/watch?v=Zj__2l-bgc8&t=61s
- Webinar: <https://www.youtube.com/watch?v=6JH3nsAPec0>
- Press release: <https://skyhawk.security/news/skyhawk-first-cloud-security-co-to-embed-chat-gpt-into-threat-detection/>