Case Study: Healthcare

SKYHAWK SECURITY

Ibex Medical: Protecting Pathology Services with Skyhawk Security

Skyhawk Synthesis enables the Ibex Medical Security Team to get insight into malicious activity in their AWS cloud, better utilize AWS GuardDuty, reducing their overall security costs without impacting the productivity of the security team.

Ibex Medical is pioneering AI-based cancer diagnostics in pathology. Ibex services assist pathologists by creating reports to locate pathological anomalies to help increase the accuracy of patient diagnosis. These powerful services reside on AWS and securing this environment is critical for their business. The team knows the value of the data that resides in the logs but did not have the tools and manpower to extract the value themselves. In order to allow the team to focus on their core solution and utilize their resources in the most cost-effective manner, they turned to Skyhawk Synthesis Security Platform.

IBEX

Environment Overview

- A complex, multi-VPC environment.
- Multiple security tools and best practices implemented.
- Heavy compute usage and the nature of the services required meticulous design to ensure high performance and robust security.

The Situation

The team recognized the value of the information within the logs but did not have the manpower to mine and correlate all the relevant information themselves. They knew they were blind to a potential malicious activity that was happening in their cloud and there was no observability into the runtime. Ibex understood that in order for any solution to achieve their goals, they could not rely just on predetermined pattern, combination, or rule-based detection methodology. As an ML/AI company themselves, they understood the value and the potential impact of implementing these technologies in a security platform. Additionally, they wanted to maximize the investment they had made in AWS GuardDuty. Skyhawk Synthesis leverages many data sources, with Amazon GuardDuty being one of the data sources.

Proving the Value

Early in our relationship, during the product's proof of value, Skyhawk Synthesis detected a complicated event sequence and prevented it from escalating into a security incident. While the set of operations put in motion were extremely similar to what an insider can do with no malicious intent, as in this case they were done by an insider, Skyhawk Synthesis detected this event and prevented an incident. Skyhawk Synthesis proved its value while also helping Ibex team to improve their internal operational processes as a result. The attack sequence provided all the evidence the security team needed to have a complete understanding of what happened, and how to address it.

Results

The team at Ibex was incredibly relieved that the alert that was raised was an insider error detected in run time, and not a threat actor. Not only the incident itself was detected and prevented, but the product also surfaced potential procedural improvements, and provided the comfort that the Skyhawk Synthesis will ensure that future malicious activities will be detected and prevented. They will be able to see a clear, correlated attack storyline which allows them to respond in time to prevent cloud breaches. The value presented by Skyhawk Synthesis Security Platform and the synergy between these two products allows Ibex to make the most of their GuardDuty investment.

The integration with Amazon GuardDuty delivered a powerful solution:

- **Correlate alerts and improve productivity.** Skyhawk Synthesis goes beyond anomaly and event detection to reduce the number of alerts security teams see – typically our customers have fewer than 20% of the alerts that other tools provide. Skyhawk Synthesis aggregates and correlates alerts from GuardDuty and machine learning models, scoring them to only alert on sequences of behaviors that represent real-time threats. This reduces the impact on the already strained Ibex team as the know when an alert is raised by the combined solution, it needs attention.
- **Context is King.** Skyhawk Synthesis connects the dots, providing visibility and simple explanations for correlated, relevant threats in runtime that represent actual incidents. The security team no longer needed to wade through hundreds of log files to understand what is happening in the environment, Skyhawk provides contextualized evidence so that security analysts can understand the root-cause of alerts and resolve them - fast.
- **Reduce the cost of data ingestion.** When Amazon GuardDuty is used with Skyhawk, VPC flow logs are becoming optional, improving customers' TCO. Synthesis ingests and analyzes information and processes this information, reducing the burden on the Ibex security team.

How do Skyhawk Synthesis and Amazon GuardDuty work together?

- Skyhawk Synthesis ingests data from several data sources across the environment, including Amazon GuardDuty.
- Machine learning baseline models are created, and suspicious and malicious behaviors are identified.
- Skyhawk identifies risky behaviors that require an investigation – but these are not yet alerts! Only correlated Malicious Behavior Indicators (MBIs) – sometimes themselves made up of dozens of alerts – are identified.
- These IOCs (Skyhawk MBIs) are scored and correlated on an Attack Sequence – scoring is done using ML and now ChatGPT – and alerts are generated only when a threat threshold is reached.
- Skyhawk identifies actual runtime behaviors meaning the alerts are real – they indicate a threat actor's actual activity.

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 cybersecurity 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 generative AI and ML sequencing of context-based behaviors, Skyhawk provides CDR within a 'Runtime Hub' to quickly detect and remediate malicious activities across multiple cloud platforms as they happen. Skyhawk Security is a spin-off of Radware® (NASDAQ:RDWR).

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

SKYHAWK SECURITY