CybrHawk
Transforming Cybersecurity

Fusion Analytic Platform from CybrHawk

THE SOC SOLUTION FOR EVOLVING THREAT LANDSCAPE

Cybrhawk Investigate is a single pane of glass for visibility, correlation and threat hunting. Coupled with big data analytics it results in improved SOC efficiency and maturity.

Cybrhawk Investigate integrates with all SOC technologies for managing security incidents and investigations, built on a single big data repository, providing analytics, investigations and visualizations to decrease response time for incidents. It can be integrated with information sources such as threat intelligence to enrich information and decision making.

THE SOC ANALYST CHALLENGE

Cyber security incidents are becoming more prevalent and increasingly complex to manage. In today's world of global communication, companies often find themselves overwhelmed by the sophistication of cyber-attacks. These sophisticated attacks require organizations to effectively handle information overload across a range of different systems and teams to protect a wide array of assets.

With data feeds coming from different sources, SOC analysts must juggle between multiple security products, logs and data in order to respond to a security incident. The number of technologies is only going to grow with more and more data for analyst to study through, resulting in alert fatigue. With increasing data sources, correlating alerts for root cause analysis has become one of the major challenges of a SOC. Confusion with different dashboards for each technology increases time to respond to an incident and inefficiency. Slow investigation processes and no defined path towards analysis leads to incident being open for weeks to months, with different analysts working on it, eventually not meeting SLA's.

Another challenge is to keep up with SOC SLA and reduction in MTTR, however complex these threats are engineered. Need for a single point of visibility and investigation is not a good to have but a serious requirement with evolving and complex nature of cyber threats for the hour.

Cybrhawk Investigate addresses these challenges by combining data feeds and running intelligent correlation to provide sharp analysis and investigation to reduce Mean time to Respond to a security incident. Using intelligence powered big data solution, it provides real time visualization of a security event, granular drill down through a single click and searching for artefact across all workstations, servers and cloud technologies integrated with the platform.

KEY FEATURES AND BENEFITS

ESTABLISH CONTROL

Integrate different data sources to gain instant visibility and status of SOC.

POWERFUL RESEARCH

Enhance the capabilities of all team members with powerful research, investigation, and threat hunting.

VISUALIZATIONS

Visual maps of related incidents for quick detection of duplicates. Real-time view and customization of reports for tiered support.

AUTOMATIC DATA ENRICHMENT

Adds historical context and threat intelligence to incidents, enabling analysts to respond more effectively.

QUICKER RESPONSE TIME

Granular tracking of alarms and events across multiple data sources

AD-HOC DASHBOARDS & REPORTS

Converges and visualizes raw data from all security tools in the organization, such as O365, AWS, Servers, Workstations, IPS, Firewalls and threat intelligence feeds.

UNIQUE INSIGHTS

Provides insights within a clear and easy-to-use UI, to minimize analysis time and accelerate the investigation process.

FLEXIBLE AND SCALABLE DEPLOYMENT

Can be deployed both on premise and on cloud to support flexible businesses and Managed security providers.

VISIBILITY

Cybrhawk Investigate integrates with all SOC technologies to provide visibility from a single dashboard.

- It ingests data from servers, honeypots, cloud services, threat intel, ticketing tools and perimeter devices.
- Runs unparallel intelligent correlations to provide meaningful information on alerts.
- Simple navigation for SOC analysts that does not require training making them adapt quickly.
- Develop custom widgets and dashboards assisting resolution to incidents.

THREAT HUNTING

Cybrhawk Investigate provides simple and advanced investigation capabilities through varied search queries.

- Find triggers for alerts and threats by quickly searching through the data repository for incident response.
- Absolute visibility on data from endpoints and servers on different events and actions to support advanced threat hunting
- Develop your own threat hunting dashboards and visualizations based on incident category.

VISUALIZATIONS

Involve upper management into an incident response with simple visualizations and reports.

- Simple visualizations for escalations, explanations and inputs across different verticals
- Customize and export reports for SOC management and realize SOC metrics
- Introduce flexibility in day to daily activities as and when required.

DEPLOYMENT MODELS

CLOUD	ON-PREMISE
The most suitable model for Managed service providers, organizations and multi-location businesses giving visibility and threat hunting through a cloud dashboard	Organization requiring data and its responsibility to be managed and hosted by themselves.

AVAILABLE INTEGRATIONS