CybrHawk
Transforming Cybersecurity

Threat Detect & Response (CybrHawk SIEM)

CybrHawk SIEM solutions provide a powerful method for the detection of threats, real-time reporting and long-term security logs and events analysis. This tool can be extremely useful to protect organizations of all sizes.

Enhanced performance

Detection of potential security risks

Reducing the effect of security breaches

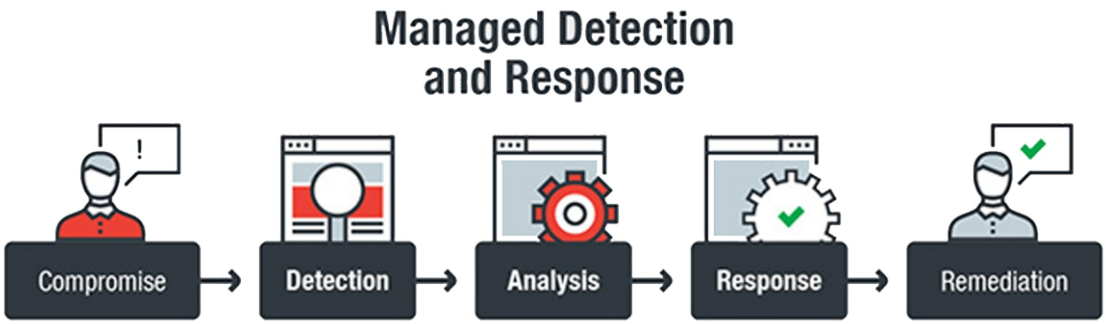
Better reporting, log review and IT enforcement with retention

Reducing costs

954-669-1960

www.cybrhawk.com

Security Information and Event Management (SIEM) software facilitates risk identification, enforcement and security incident management by collecting and analyzing safety incidents (both near-real and historical) as well as a wide range of other events and contextual data sources. The core capabilities area wide range of collection and management of log events, the ability to analyze log events and other data across different sources, and operational capabilities (such as incident management, dashboards and reporting).



CybrHawk SIEM platform provides visibility to the whole network and integrate below fields.

Information aggregation: Log management aggregates information from a wide variety of sources, including network, security, servers, databases, applications, allowing the collection of tracked information to help avoid missing critical events.

Correlation: searches for common attributes and connects events into meaningful bundles. This software provides the ability to perform a number of integration techniques to combine various sources and make information useful. Correlation is usually a feature of a full SIEM solution's Security Event Management component

Alert: Automated correlated event analysis

Dashboards: Software can take data from incidents and convert them into information graphs to help show trends and recognize things that do not follow a standard pattern.

Compliance: Software can be used to automate compliance data collection and reporting which adapts to existing processes of security, governance and auditing

Persistence: use of long-term historical data storage to enable data comparison over time and provide the persistence needed for compliance requirements. Long-term storage of log data is important in forensic investigations as it is unlikely that a network breach will happen when the breach happens

Forensic analysis: ability to search, based on specific parameters, through logs on various nodes and time periods. It eliminates the need to compile log data in your head or scan thousands and thousands of logs.

sales@cybrhawk.com

CybrHawk Inc, 6451 N Federal Hwy #105 Fort Lauderdale, FL 33308