BLACKHAWK ALERT

CYBER SECURITY SOLUTIONS

VIGILANCE PRODUCT WHITEPAPER

BLACKHAWK ALERT VIGILANCE

INTRO

Blackhawk Vigilance is a SIEM (Security Information and Event Management) solution. A SIEM is a type of software that helps organisations collect, analyse, and respond to security-related data from a variety of sources.

SIEM is a key part of technology for achieving compliance standards. Whether compliance required is for Sarbanes Oxley, Basel II, HIPAA, GLB, FISMA, PCI DSS, GDPR or NISPOM, Vigilance can assist you in meeting your regulatory requirements.

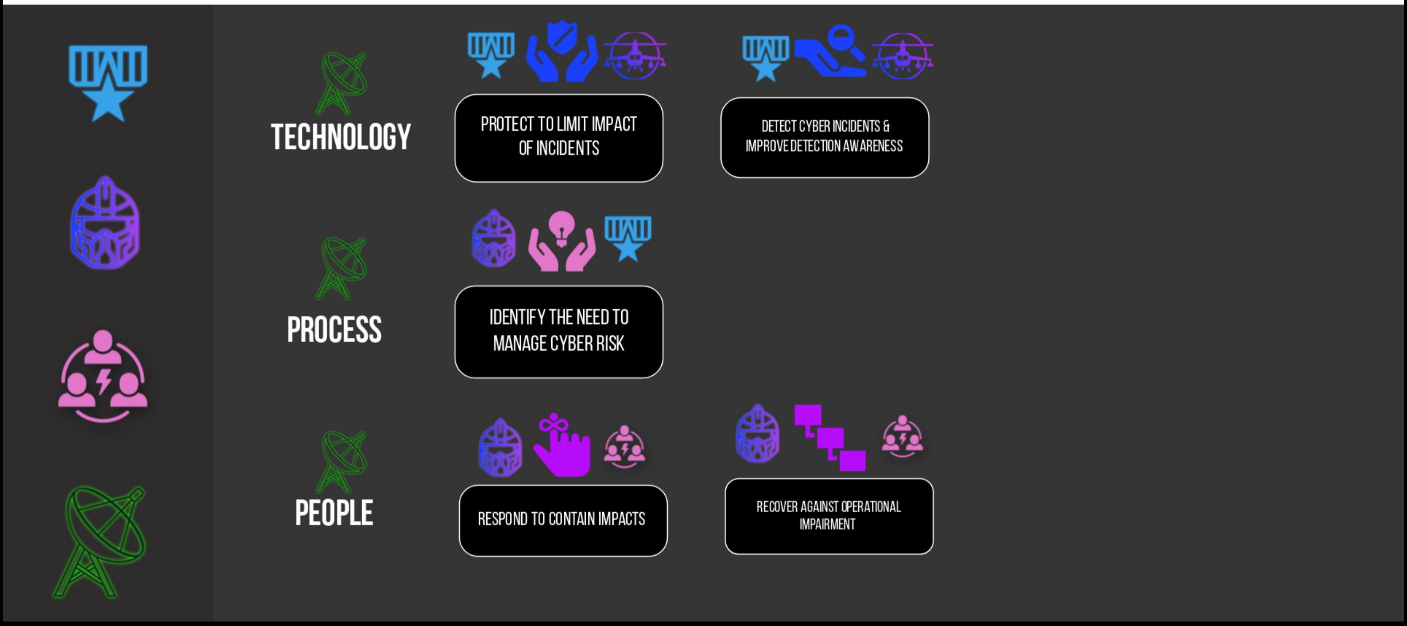
WHAT IS VIGILANCE?

Blackhawk Vigilance enables a comprehensive view of your organisation’s security posture, including potential threats and vulnerabilities, so we can take appropriate action to protect your systems and data.

Vigilance includes features such as real-time event correlation, alerting, and reporting, as well as integration with other Blackhawk security solutions such as endpoint protection and firewall through Blackhawk Fortress and Blackhawk Frontier.

A Security Information and Event Management (SIEM) system is a crucial component of an organisation’s security infrastructure, and it is required by a number of compliance and regulatory frameworks to ensure the security and confidentiality of sensitive information.

ALIGNMENT TO THE NIST FRAMEWORK



TECHNOLOGY

PROTECT TO LIMIT IMPACT OF INCIDENTS

DETECT CYBER INCIDENTS & IMPROVE DETECTION AWARENESS

PROCESS

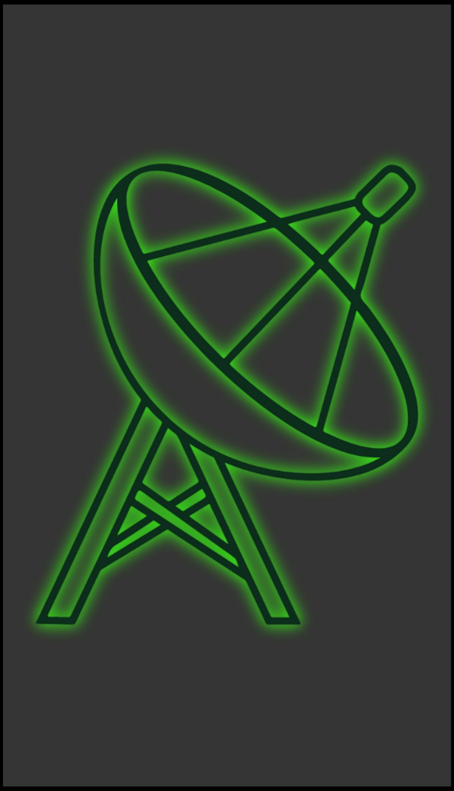
IDENTIFY THE NEED TO MANAGE CYBER RISK

PEOPLE

RESPOND TO CONTAIN IMPACTS

RECOVER AGAINST OPERATIONAL IMPAIRMENT

KEY FEATURES



BLACKHAWK VIGILANCE FEATURES

Network Activity Monitoring:
detection and response to security events, and generation of audit reports.

Log Collection and Management:
Collect, aggregate, and normalise log data from various sources, through automated log parsing, tagging, and categorization.

Real-Time Event Correlation and Analysis:
Analyses log data in real-time to identify potential security threats and suspicious activity for rapid detection and response

Threat Detection and Response:
Advanced analytics and machine learning algorithms detect potential security threats, such as malware, phishing attacks, and insider threats through machine learning, user and entity behaviour analytics (UEBA).

Incident Response and Forensics:
Provides incident response workflows and forensic investigation tools to help security teams investigate and respond to security incidents. Vigilance integrates with popular security tools and services to streamline incident response.:

Compliance Reporting and Audit Trails:
Vigilance SIEM generates compliance reports and audit trails to demonstrate compliance with regulatory requirements, such as PCI DSS, HIPAA, and GDPR.

Reduction of insurance premiums:
Blackhawk Vigilance SIEM helps organisations demonstrate that they have taken appropriate measures to protect their systems and data, which in turn reduces their premiums owed to cyber insurance providers - reducing their overall cost of cover.

Blackhawk Alert's 24/7 Security Operations Center (SOC) is tasked with forensic investigation on historical and present events related to your business's data. Our SOC team is responsible for the triage and investigation of all potential incidents detected by Blackhawk Vigilance.

Data Retention, of all information associated with tickets and alerts, like timestamps, authors, notes, status, resolutions, attachments and relevant related raw events are available for you to review any time for up to seven years from date of record. This information can be used as evidence in compliance with most required information security standards.

BLACKHAWK VIGILANCE'S SIEM ENABLES THE BLACKHAWK ALERT TO DELIVER SECURITY:

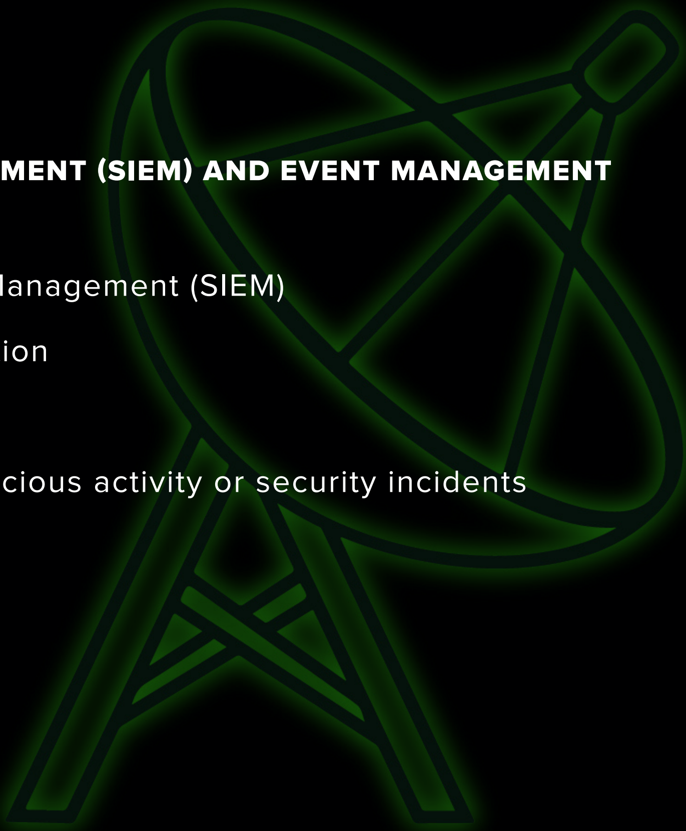
1. **Network Activity Monitoring:** detection and response to security events, and generation of audit reports.
2. **Log Collection and Management:** Vigilance SIEM systems collect, aggregate, and normalise log data from various sources, including network devices, servers, and applications. Vigilance supports a wide range of log sources and provides automated log parsing, tagging, and categorization.

3. **Real-Time Event Correlation and Analysis:** Vigilance SIEM analyses log data in real-time to identify potential security threats and suspicious activity. It provides real-time analytics and correlation of events across multiple sources to detect and respond to threats quickly.
4. **Threat Detection and Response:** Blackhawk Vigilance uses advanced analytics and machine learning algorithms to detect potential security threats, such as malware, phishing attacks, and insider threats. Vigilance offers advanced threat intelligence and detection capabilities, including machine learning, user and entity behaviour analytics (UEBA).
5. **Incident Response and Forensics:** Blackhawk Vigilance SIEM provides incident response workflows and forensic investigation tools to help security teams investigate and respond to security incidents. Vigilance integrates with popular security tools and services to streamline incident response.
6. **Compliance Reporting and Audit Trails:** Vigilance SIEM systems generate compliance reports and audit trails to demonstrate compliance with regulatory requirements, such as PCI DSS, HIPAA, and GDPR.
7. **Reduction of insurance premiums:** Blackhawk Vigilance helps organisations demonstrate that they have taken appropriate measures to protect their systems and data, which in turn reduces their premiums owed to cyber insurance providers - reducing their overall cost of cover.

ADDITIONAL FEATURES

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) AND EVENT MANAGEMENT SOLUTIONS:

1. Cloud-based Security Information & Event Management (SIEM)
2. Complete Event and Log Management Solution
3. 24/7 monitoring and remediation
4. Generating alerts and notifications for suspicious activity or security incidents
5. Automatically responds to incidents
6. Raw Events Retention - 6 months



THREAT INTELLIGENCE AND RISK MANAGEMENT:

7. Providing a comprehensive view of an organisation’s security posture

8. Exposes hidden risks

9. Blocks unknown threats

10. Gain intelligence about the cyber-threats targeting your business

11. Supports Business Continuity Planning

12. Comprehensive Risk Reporting

FORENSIC CAPABILITIES AND INCIDENT INVESTIGATION:

13. Forensics Data analysis

14. Offering forensic capabilities for incident investigation and response

15. Malware and Ransomware protection

COMPLIANCE AND REGULATORY MEASURES:

16. Enabling compliance with security regulations and industry standards

17. Improve regulatory & industry compliance measures

18. 7 years data log retention

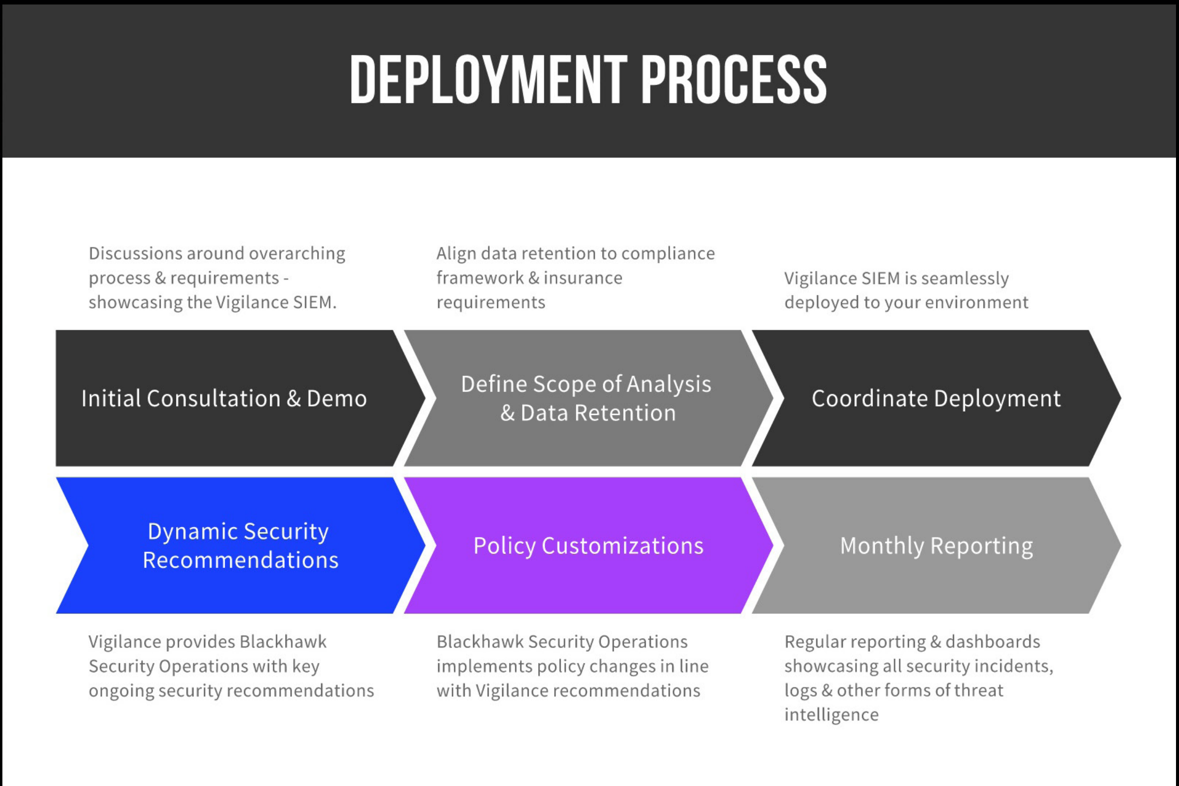
WEB AND APP ANALYSIS:

19. Web and App traffic Analysis

20. Executive Security Summary Report

DEPLOYMENT

Vigilance SIEM is seamless in deployment. Blackhawk Alert’s security team will install the software across all applicable devices.



DEPLOYMENT PROCESS

Discussions around overarching process & requirements - showcasing the Vigilance SIEM.

Align data retention to compliance framework & insurance requirements

Vigilance SIEM is seamlessly deployed to your environment

Initial Consultation & Demo

Define Scope of Analysis & Data Retention

Coordinate Deployment

Dynamic Security Recommendations

Policy Customizations

Monthly Reporting

Vigilance provides Blackhawk Security Operations with key ongoing security recommendations

Blackhawk Security Operations implements policy changes in line with Vigilance recommendations

Regular reporting & dashboards showcasing all security incidents, logs & other forms of threat intelligence

CONCLUSION

The primary function of Blackhawk Vigilance SIEM (Security Information and Event Management) is to collect, analyse, and respond to security-related data from a variety of sources, such as network devices, servers, and applications. This provides our security team a comprehensive view of your organization's security posture, including potential threats and vulnerabilities, so they can take appropriate action to protect your systems and data.

Other key functions of a SIEM include:

- Real-time event correlation: Analysing and correlating data in real-time to identify potential security threats and vulnerabilities
- Alerting and notifications: Generating alerts and notifications for suspicious activity or security incidents
- Incident investigation and response: Providing forensic capabilities for incident investigation and response
- Reporting and visualisation: Providing reporting and visualisation capabilities for security teams to monitor and analyse security data over time
- Compliance: Enabling compliance with security regulations and industry standards
- Integration: Integration with other security tools such as firewalls, intrusion detection systems, and vulnerability scanners
- Data retention up to 7 years

In summary, the primary function of a SIEM is to provide an organisation with the ability to detect, respond and report security incidents, threats and vulnerabilities in a centralised way as well as storing all data for compliance up to 7 years.