CYBER SILO

THREAT HAWK SIEM

INTRODUCTION

Threat Hawk SIEM aggregates and analyze activities for entire company's infrastructure. It helps organizations in detecting potential threats & vulnerabilities before attacker disrupt business. Threat Hawk SIEM collects security data from network devices, servers, domain controllers, mobile devices.

WHY THREAT HAWK SIEM?

1. Real-Time Threat Detection

Proactively identify and mitigate threats before they impact business operations.

2. Faster Incident Response

Minimize damage with rapid detection and automated response workflows.

3. Enhanced Threat Hunting

Leverage deep insights and actionable intelligence to uncover hidden threats.

4. Comprehensive Visibility

Gain full coverage across networks, endpoints, and cloud environments.

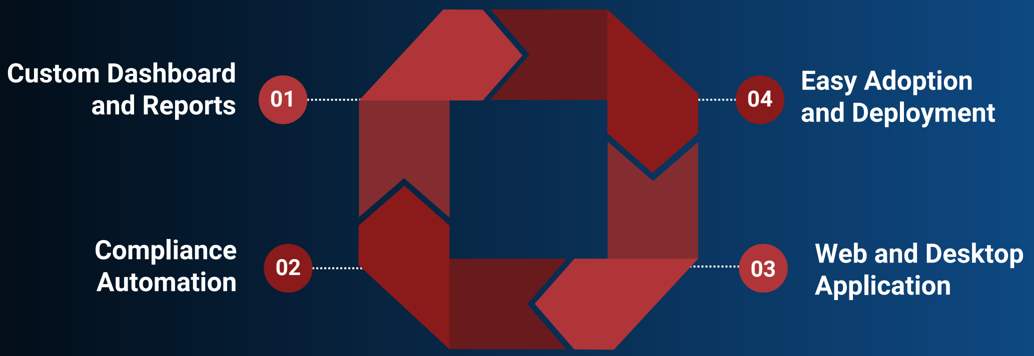
5. Streamlined Compliance

Simplify adherence to ISO 27001, GDPR, HIPAA, NIST, PCI DSS, and NESA standards.

6. Scalable for Growing Businesses

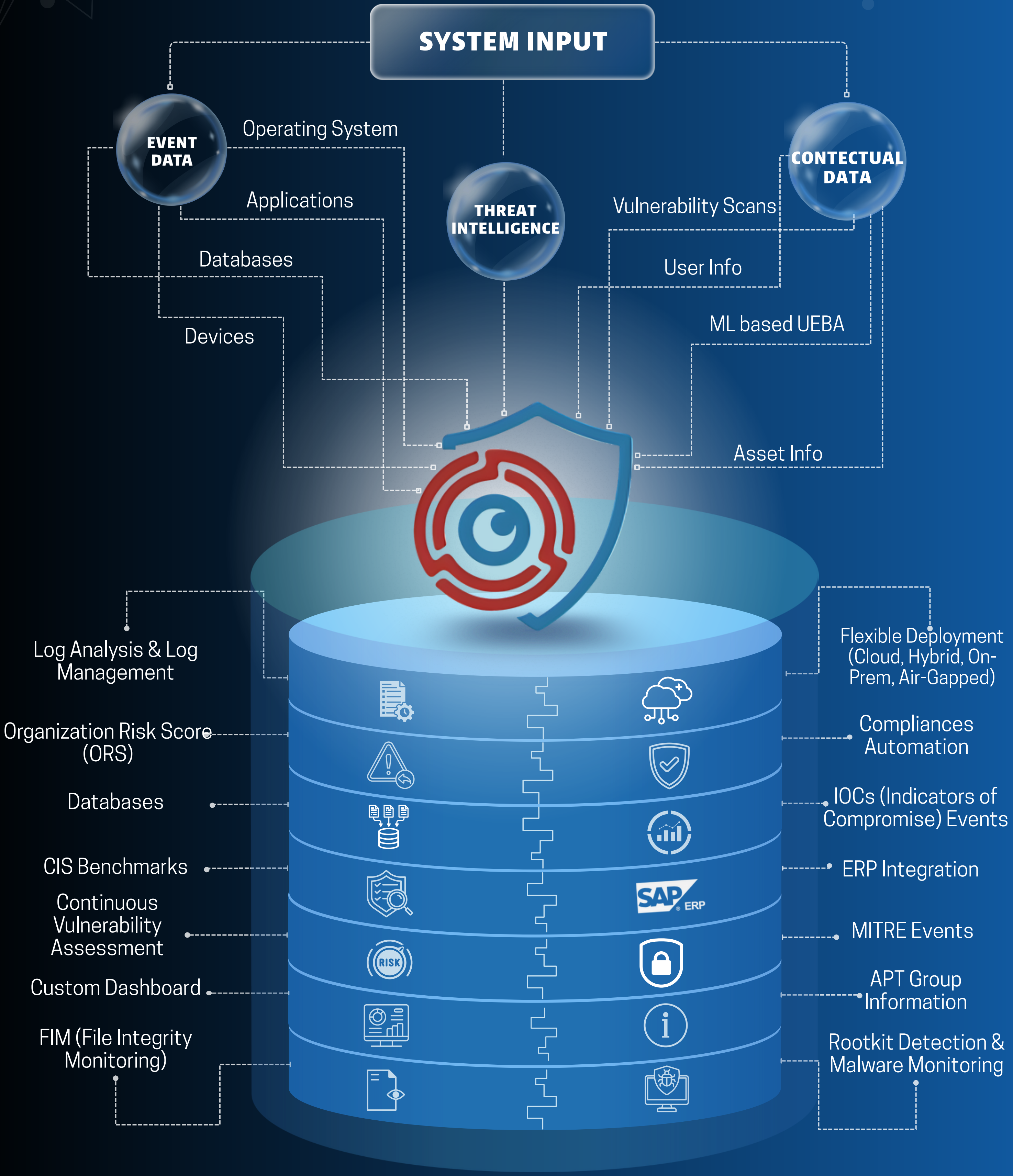
Adapts seamlessly to expanding IT environments without performance loss.

UNIQUE PREPOSITIONS


Custom Dashboard and Reports
01
Compliance Automation
02
Web and Desktop Application
03
Easy Adoption and Deployment
04

CYBER SILO

ARCHITECTURE



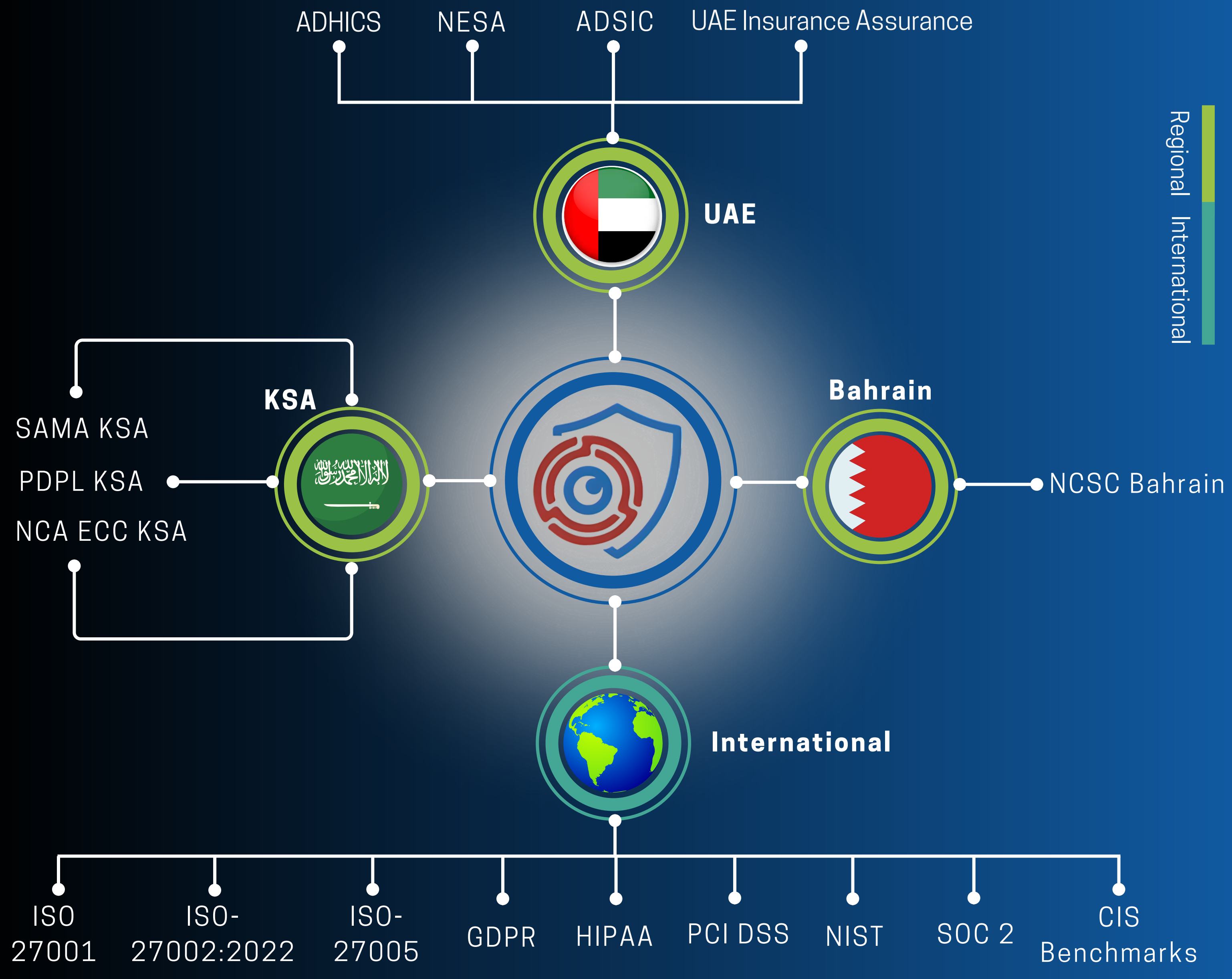
FEATURES

Sr#	Features	Description
1	Log Analysis & Log Management	Collects, normalizes, and analyzes log data from multiple sources for security insights.
2	Organization Risk Score (ORS)	Quantifies overall security posture with a dynamic risk assessment score.
3	Databases	Monitors and secures database activities for suspicious access or changes.
4	CIS Benchmarks	Ensures system configurations align with CIS security best practices.
5	FIM (File Integrity Monitoring)	Detects unauthorized file modifications in critical systems.
6	Custom Dashboard	Provides tailored views of security metrics.
7	Flexible Deployment	Supports cloud, on-premise, hybrid and Air-Gapped deployments based on organizational needs.
8	Compliances Automation	Automates compliance reporting for standards like ISO 27001, GDPR, and NIST.
9	Threat Intelligence	Identifies known threat patterns (IOCs) to detect breaches.
10	ERP Integration	Correlates security events with ERP systems like SAP, Salesforce, Zoho and Microsoft Dynamics 365, for holistic monitoring.
11	MITRE Events	Maps detected threats to the MITRE ATT&CK framework for tactical analysis.
12	APT Group Information	Tracks advanced persistent threat (APT) group tactics and indicators.
13	Rootkit Detection & Malware Monitoring	Identifies stealthy rootkits and malware activities in real time.
14	Reports	Generates detailed security reports for audits and stakeholder reviews.
15	Security Events	Aggregates and prioritizes security alerts for faster response.
16	User Management	Controls access permissions and monitors user activities for insider threats.
17	Audit Logs	Maintains tamper-proof logs of all system actions for accountability.
18	In-App & Off-App Releases for SIEM	Supports seamless updates and patches without disrupting operations.
19	Task Management	Assigns and tracks incident response tasks within the SIEM platform.
20	Log & Network Flow Collection	Captures logs and network traffic data for comprehensive analysis.
21	Security and logs data Analytics	Applies ML to analyze logs for hidden threats and anomalies.
22	Intrusion & Vulnerability Detection	Identifies exploits and weaknesses in the IT environment.

CYBER SILO

COMPLIANCE STANDARDS AUTOMATION

Threat Hawk SIEM simplifies regulatory adherence by automating compliance monitoring and reporting for major global and country based standards. It supports ISO 27001, GDPR, HIPAA, NIST, PCI DSS, NESA, CIS, SOC2 and many more, ensuring organizations meet audit requirements with minimal effort.



CYBER SILO

Schedule a Demo Today to see explore Threat Hawk SIEM's Features in real time.

For queries and trials, contact us at **info@cybersilo.tech**

Visit our website: **https://cybersilo.tech**

For More Details Visit us

in **@Cyber Silo**

▶ **@CyberSiloHQ**

@Cybersilo.official

☎ **@Cyber Silo**