Enhancing SAP ERP Security by Integration with Threat Hawk SIEM

Whitepaper

According to a report by **IBM**, the average cost of a data breach involving ERP systems is **$4.24 Million**, highlighting the significant financial impact of security incidents.

Introduction

SAP ERP is a mission-critical enterprise application managing financials, supply chains, human resources, and other core business processes. Given its significance, SAP ERP is a high-value target for cyber threats, making security monitoring essential.

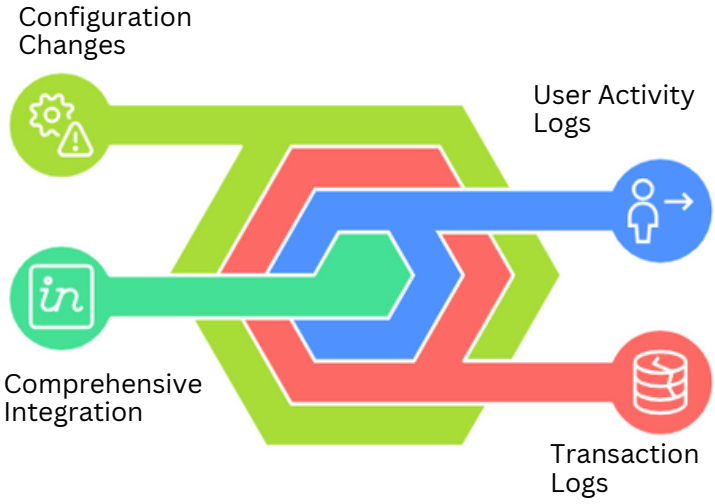
Integrating SAP ERP logs into Threat Hawk SIEM enables real-time threat detection, compliance enforcement, and proactive risk mitigation. This whitepaper explores the benefits, key log sources, and implementation strategies for SAP ERP and Threat Hawk SIEM integration.

SAP ERP Integration with Threat Hawk

Threat Hawk SIEM solution provides comprehensive integration with SAP ERP systems, capturing a wide range of log types to ensure thorough monitoring and analysis. Key log types include:

1. User Activity Logs:

Track user login and logout activities, providing insights into who accessed the system and when. This helps in identifying unauthorized access attempts and unusual user behavior.



2. Transaction Logs:
Monitor transaction activities within SAP ERP, capturing detailed records of all transactions performed. This ensures that all financial and operational transactions are logged and can be reviewed for compliance and security purposes.

3. Configuration Changes:
Detect and log any changes made to the system configuration. This includes modifications to user roles, access permissions, and system settings, helping to maintain a secure and compliant environment.

Why Integrate SAP ERP with Threat Hawk SIEM?

Integrating SAP ERP with Threat Hawk SIEM provides organizations with:

1. Real-time Threat Detection:
Identifies unauthorized access, privilege misuse, and fraudulent transactions.

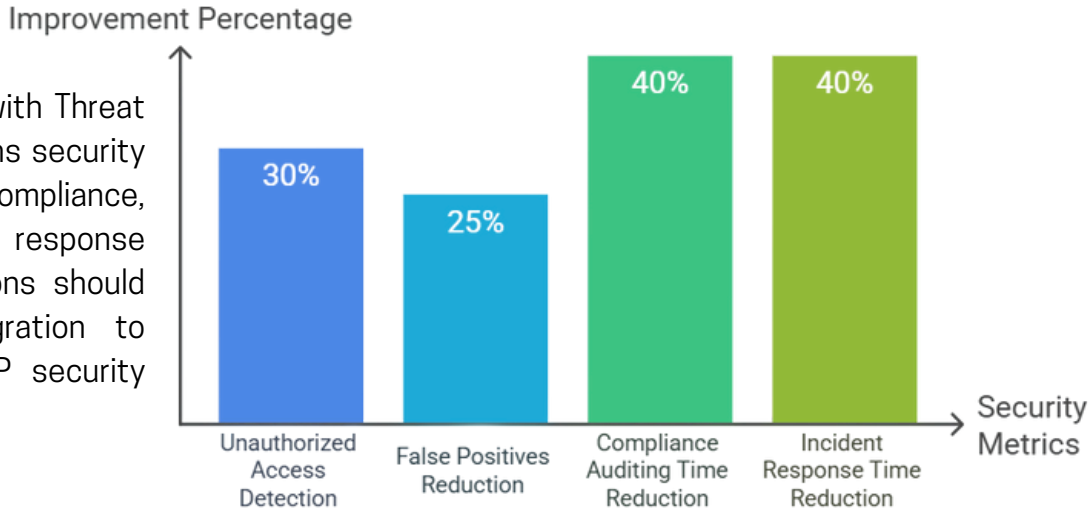
2. Anomaly Detection:
Analytics to identify abnormal user and transaction behavior.

3. Improved Incident Response:
Correlates SAP ERP events with enterprise-wide security logs for rapid investigation.

4. Centralized Data Security
ERP is attacker's Jackpot as it centralize sensitive data, financials, and operational controls, making them a one-stop shop for devastating breaches.

Benefits of SAP ERP and Threat Hawk SIEM Integration

Integrating SAP ERP with Threat Hawk SIEM strengthens security visibility, enhances compliance, and improves incident response efficiency. Organizations should prioritize SIEM integration to mitigate evolving SAP security risks.



Threat Hawk SIEM Monitors the Following SAP Logs

- SAP Security Audit Log
- SAP System Log
- SAP HANA Audit Log
- SAP Gateway Log
- SAP Java Audit Log
- SAP Profile Parameters

Key SAP ERP Events for SIEM Integration

To maximize security insights, the following SAP ERP events should be ingested into Threat Hawk SIEM:

Sr#	SAP Event	Description
1	Excessive Failed Login Attempts	Detects brute force or unauthorized login attempts.
2	Anomalous Login Location	Flags suspicious login activity from a new location.
3	Privileged Account Usage	Alerts when a user gets full SAP system access.
4	Possible Account Takeover	Indicates an attempted brute force attack.
5	Suspicious Finance Data Access	Detects unauthorized attempts to view financial records.
6	Data Exfiltration Attempt	Flags potential insider threats exporting bulk data.
7	Potential Fraudulent Account Changes	Detects modifications to banking details for fraud prevention.
8	Unauthorized User Creation/Deletion	Flags unauthorized user management actions.
9	Privilege Escalation Detection	Alerts when sensitive roles are assigned.
10	Security Configuration Tampering	Detects unauthorized changes to SAP security settings.
11	Unexpected System Restart	Detects unauthorized or unusual SAP system restarts.
12	Unusual Resource Utilization	Flags performance degradation that may indicate an attack.
13	Potential Denial of Service (DoS)	Detects excessive lockouts affecting system availability.
14	Audit Trail Tampering Attempt	Detects attempts to erase audit trails.
15	Policy Violation Detection	Flags transactions that bypass standard approval workflows.