Enhancing Security by Integrating Oracle Database with Threat Hawk SIEM

60% of breaches involve compromised credentials, with databases being a prime target (Source: Verizon DBIR).

INTRODUCTION

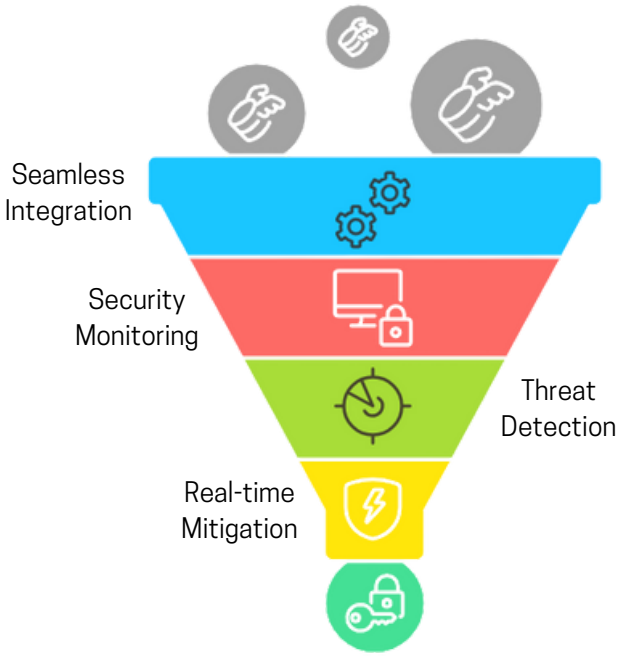
Oracle Database is a widely used enterprise database that stores critical business data, making it a prime target for cyber threats. Integrating Oracle logs into Threat Hawk SIEM enhances security by providing real-time monitoring, threat detection, and compliance enforcement.

This whitepaper explores the benefits, key log sources, and implementation strategies for Oracle and Threat Hawk SIEM integration.

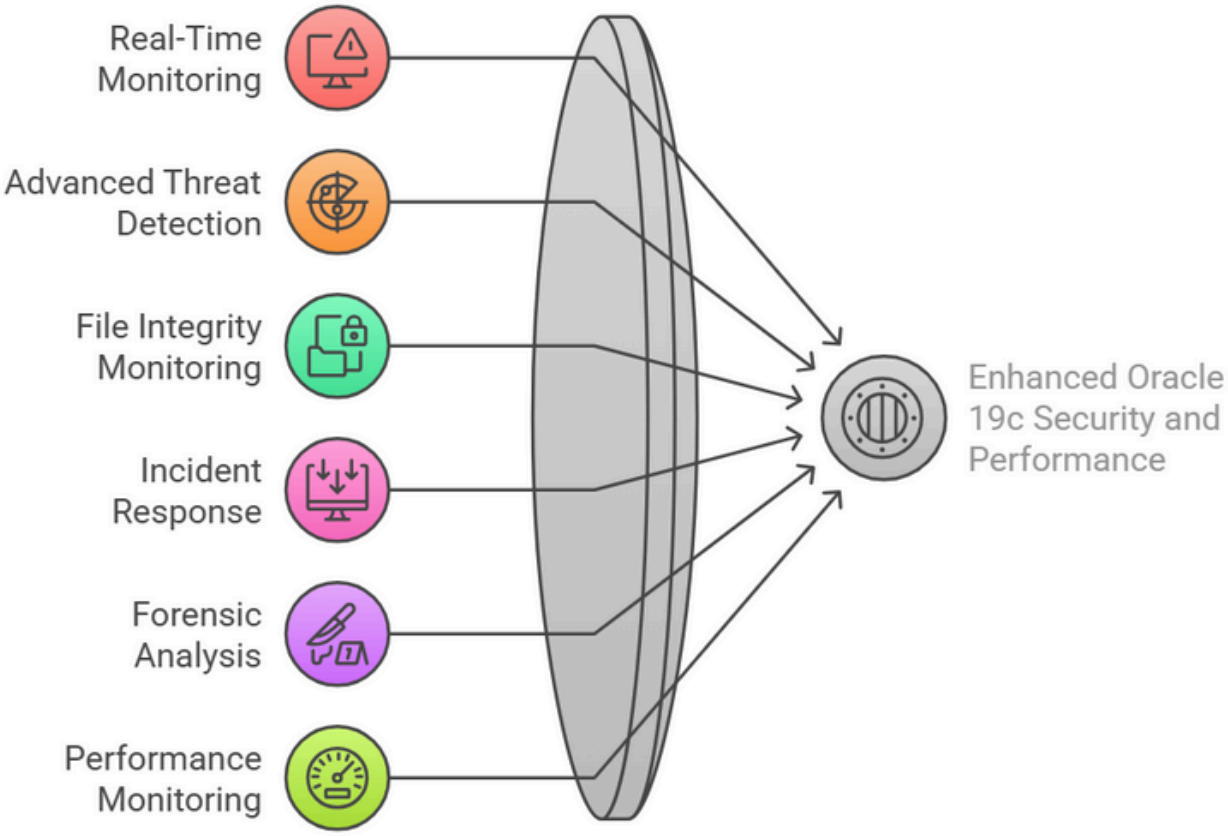
WHY INTEGRATE ORACLE WITH THREAT HAWK?

Integrating Oracle with Threat Hawk SIEM provides organizations with:

1. **Real-time Threat Detection:**
   Identifies unauthorized access, SQL injections, and suspicious database activities.
2. **Compliance Enforcement:**
   Ensures adherence to regulatory frameworks like PCI-DSS, GDPR, and ISO 27001.
3. **Anomaly Detection:**
   Advance analytics to identify abnormal data access patterns.
4. **Improved Incident Response:**
   Correlates database events with system-wide security logs for faster investigations.



ENHANCEMENT OF DATABASE SECURITY AND EFFICIENCY



BENEFITS OF INTEGRATING ORACLE DATABASE WITH THREAT HAWK SIEM

Detection Efficiency

30% improvement in threat detection efficiency.

False Positives

25% reduction in false positives through intelligent log correlation.

Remediation Time

40% decrease in vulnerability remediation time.

Misconfiguration

35% reduction in misconfiguration vulnerabilities compared to systems lacking deep SIEM integration.

Incident Response

40% faster incident response times reported by enterprises using SIEM for database security.

KEY ORACLE EVENTS FOR SIEM INTEGRATION

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

Sr#	Module	Oracle Event	Description
1	User Authentication & Privilege Escalation Monitoring	Excessive Failed Login Attempts	Detects brute force or unauthorized login attempts.
		Privileged Account Usage	Flags unauthorized or unexpected privileged logins.
		Possible Account Takeover	Indicates a brute force attack followed by a successful login.
2	Data Access & Modification Tracking	Excessive Failed Login Attempts	Detects brute force or unauthorized login attempts.
		Privileged Account Usage	Flags unauthorized or unexpected privileged logins.
		Possible Account Takeover	Indicates a brute force attack followed by a successful login.
3	Database Configuration & Structural Changes	Mass Data Extraction Attempt	Detects potential data exfiltration.
		INSERT, UPDATE, DELETE on Critical Tables	Alerts on unauthorized or mass changes in sensitive data.
		Unauthorized Schema Changes (ALTER, DROP, CREATE)	Identifies unauthorized structural changes.
4	System & Performance Monitoring	Unauthorized User Creation/Deletion	Detects unauthorized changes in user accounts.
5	Security & Compliance Monitoring	Privilege Escalation Detection	Triggers an alert when a non-admin user gets privileged access.
		Database Configuration Tampering	Identifies unauthorized system configuration changes.
		Unexpected Database Restart	Detects unauthorized database shutdowns or restarts.