HUNKLER
GmbH & Co. KG

**ORACLE WHITEPAPER**
**SEPTEMBER 2018**

# ORACLE SECURITY MONITORING AND ANALYTICS CLOUD SERVICES

ORACLE

ORACLE DATA SHEET

*Disclaimer: This document is for informational purposes. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.*

# Oracle Security Monitoring and Analytics Cloud Service

ORACLE

SECURITY MONITORING AND ANALYTICS CLOUD SERVICE

Oracle Security Monitoring and Analytics (SMA) is the first integrated SIEM and UEBA platform for effective protection of evolving IT landscapes against modern threats. SMA combines universal data ingestion with next-generation analytics to enable early detection, rapid investigation and intelligent remediation of threats across heterogeneous on-premise and cloud infrastructure. SMA is delivered as a service from the Oracle Cloud to provide rapid time to value, greater scale and reliability, and reduced management overhead.

**KEY BUSINESS BENEFITS**

- Improved Security and Risk Posture
  - Lower risk and cost of data breaches and security incidents
  - Early detection of known and unknown threats
  - Visibility across heterogeneous infrastructure, cloud assets
- Greater SOC Efficiency
  - Fewer false positives and negatives
  - Faster time to detection and remediation
  - Reduced learning curve for SOC analysts
- Rapid Time to Value
  - Delivered as a next-gen, auto-scaling cloud based service
  - SOC ready content for security and compliance use cases
  - Runbook templates for automation of SOC operations

## The Security Monitoring Dilemma for Modern IT Teams

Consumerization, containerization, cloud, mobile, and IoT have multiplied the surface area of security risk exposure. Additionally, the snatch and grab attacks of yesterday have been replaced by advanced, multi-stage attacks that evade detection by signature based tools. Meanwhile DevOps and related CI/CD initiatives have created a perfect storm of faster infrastructure changes and shrinking threat detection windows. Legacy on-premise security monitoring solutions are deployment and infrastructure management intensive. They also lack the scale and reliability needed to effectively detect new threats. As a result, IT teams are unable to keep pace with the volume and sophistication of modern security threats.

## Oracle Security Monitoring and Analytics Cloud Service

Oracle Security Monitoring and Analytics (SMA) is a cloud service that addresses today's security monitoring challenges through comprehensive security threat detection, investigation and remediation. SMA provides integrated SIEM and UEBA capabilities to protect heterogeneous IT stacks across private and public clouds against modern, evolving threats. It includes out of the box security monitoring for a broad range of use cases that can be leveraged by both small security teams and large enterprise security operations centers.

## Universal Threat Visibility

Oracle Security Monitoring and Analytics Cloud Service (SMA) supports ingestion of any machine or user data from on-premise or cloud based infrastructure. Numerous log sources of security context (OS, DB, firewalls, web proxy etc.) are supported out of the box with new parsers provided on a monthly basis. These sources are mapped to a normalized and categorized event format for flexible, vendor and device independent analytics. A custom parsing toolkit enables easily extending data ingestion to custom

ORACLE

**KEY FEATURES**

- Data Access Anomaly Detection
  - Detect anomalous SQL queries by user, database or application
- Multi-dimensional Anomaly Detection
  - Develop rich user baselines across behavioral attributes
- User Session Awareness
  - Intelligent user identity awareness and attribution
- Kill Chain Discovery and Visualization
  - Intuitive visualization of common attack chain patterns
- Application Topology Awareness
  - Detect multi-tier or lateral movement in applications
- Integrated Threat Intelligence
  - Leverage up to date, global IOC data for detection and forensics

applications and other sources. Universal threat visibility also extends to contextual sources of data such as CMDB, user directory, threat intelligence feeds and vulnerability scanners.

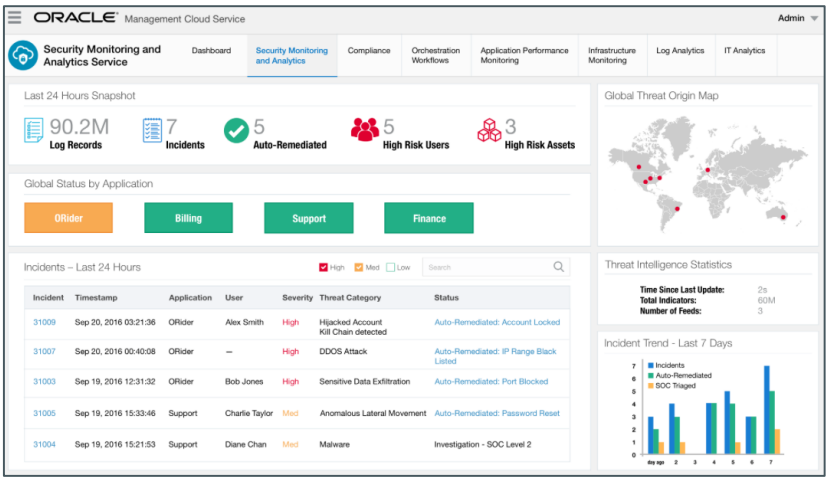


Figure 1: Security Overview Dashboard

## Machine Learning Based Anomaly Detection

Oracle SMA provides a powerful analytics engine that combines rules based correlation and machine learning driven anomaly detection for the broadest range of threat vectors.

Rich, multi-dimensional behavioral baselines can be developed for users, groups or other entities like applications. This enables detection of complex anomalies. For example, user anomalies can be detected at the intersection of an activity type (successful network logins) and various associated attributes such as time, location, and host. SMA can also go a level deeper than other UEBA tools and detect complex data layer anomalies. Specifically, SMA can baseline data query syntax patterns for a given user, database or application and then detect anomalous data access. This “data deep” analytical capability enables more effective detection of unauthorized data access and exfiltration. The analytics engine also supports state preservation and escalation in threat detection. This capability enables early detection of multi-stage, layered attacks like APT.

Although the primary dimension of security analytics has shifted from hosts to users, the reality is that most log sources lack the user context critical to threat detection. SMA combines user directory based identity awareness with user attribution extrapolated from VPN, DHCP and other activity sources to inject user context into security event streams. This capability is critical to early detection and false negative reduction around user centric threat vectors like insider threats or hijacked accounts.

## Intuitive Threat Hunting and Investigation

Oracle Security Monitoring and Analytics (SMA) is designed to optimize SOC efficiency by expediting threat hunting and investigation. Intuitive SOC analyst workflows ensure seamless navigation from high-level dashboard views to user or threat specific activity details. Similarly, analysts can leverage dynamic object linking functionality to pivot into user, asset, or threat intelligence browser views for on-demand investigative context.

### ORACLE MANAGEMENT CLOUD

- Oracle Security Monitoring and Analytics Cloud Service is part of Oracle Management Cloud
- Oracle Management Cloud (OMC) is a suite of next-generation, integrated monitoring, management and analytics solutions delivered as a service on Oracle Cloud. It is designed for today's heterogeneous environments across on-premises, Oracle Cloud and third-party cloud services. OMC is built on a horizontally scalable big data platform with high throughput data processing for providing real-time analysis and deep insights across technical and business events.
- Data in OMC is automatically analyzed using machine learning and is correlated across all OMC services, thereby eliminating multiple information silos across end-user and infrastructure data, enabling faster trouble-shooting and providing the ability to run IT like a business.
- OMC eliminates the human effort associated with traditional management toolsets while achieving better performance. Autonomously monitor, detect, triage and proactively resolve issues across hybrid cloud environments, including heterogeneous technology on-premises, in Oracle Cloud and in third-party clouds.

### TOP THREE CAPABILITIES

- Comprehensive, intelligent management platform
- Zero-effort operational insights
- Automated preventative and corrective actions

Greater SOC efficiency is also enabled by the SMA event taxonomy that enables analysts to view security activity in a vendor and device agnostic manner. By providing natural language event categorization, SMA cuts the need for analysts to intimately understand the vast number of unique log syntaxes. Additionally, for advanced multi-stage threats, SMA converts its awareness of common kill chain patterns (such as hijacked account behavior) into a logical attack phase oriented timeline view for rapid triage.

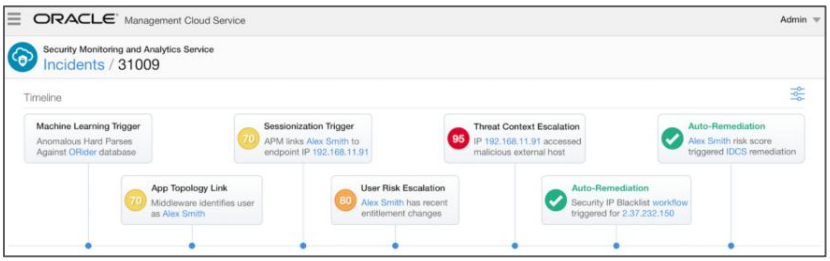


Figure 2: Attack Chain Timeline Visualization

## Enhanced Security Monitoring with OMC Platform

Oracle Security Monitoring and Analytics is part of Oracle Management Cloud (OMC), a suite of next-generation, integrated monitoring, management and analytics solutions delivered as a service on Oracle Cloud. OMC extends essential platform benefits of data ingestion and processing scale, overall reliability, and security to all services including SMA.

Additionally, cross service leverage enhances detection capabilities around specific threat vectors. For example, the OMC platform has application topology awareness that enables the SMA service to detect lateral movement within applications or multi-tier attacks against specific applications. Functionality in the broader OMC platform also provides configuration drift monitoring context. This enables SMA to connect suspicious access activity with specific configuration changes. The OMC platform also extends a rich orchestration framework for SOC remediation workflows to be instrumented in any IT stack, including in heterogeneous cloud platforms.

ORACLE

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

CONTACT US

For more information about Oracle Security Monitoring and Analytics Cloud Service, visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

Integrated Cloud Applications & Platform Services

## ÜBER HUNKLER

Das Karlsruher Systemhaus HUNKLER wurde 1988 erster offizieller Partner von Oracle in Deutschland. Ein Team von rund 20 Mitarbeitern unterstützt Kunden aus Industrie, öffentlicher Verwaltung, Gesundheits- und Finanzwesen mit Beratung, Lösungsentwicklung und Managed Services.

Im Fokus von HUNKLER stehen leistungsfähige, wirtschaftliche Infrastrukturen für Oracle-datenbanken mit den Schwerpunkten Hochverfügbarkeit, Ausfallsicherheit und Zero Downtime Migration. Die integrierten Komplettlösungen der Produktfamilie Oracle Engineered Systems sowie der Datenbank-/Anwendungsbetrieb in der Oracle Cloud sind weitere Themenfelder, die das Unternehmen umfassend abdeckt.

HUNKLER GmbH & Co. KG

**Hauptsitz Karlsruhe**
Bannwaldallee 32, 76185 Karlsruhe
Tel. 0721-490 16-0, Fax 0721-490 16-29
**Geschäftsstelle Bodensee**
Fritz-Reichle-Ring 6a
78315 Radolfzell
Tel. 07732-939 14-00, Fax 07732-939 14-04
**info@hunkler.de, www.hunkler.de**