Oracle Identity SOC Security Solution

Identity-Centric Security for the Cloud Era

Introduction

Today's attacks have increased in sophistication. The threat of zero-day exploits is expanding on a scale unseen before and putting a strain on researcher's ability to identify and prevent using signature-based techniques. This makes anomaly detection the only way to spot the needle in a haystack. Today's threats are now multi-vector by utilizing multiple entry points, and break apart the attack sequence into smaller segments that are re-packaged and executed. The attack surface is now targeted vs indiscriminate, which makes user awareness and attribution invaluable in detection. The ability to correlate anomalous events from the network, applications and user behaviors is key in early detection and containment.

This challenges the network-centric philosophy on defense, as tools are being asked to secure data and assets in ways that they are not capable of. Identity is now the bridge between the worlds of user, application and network controls. It is the identity context brought together with new technologies such as machine learning, big data, and advanced analytics that allows a security professional to centralize and normalize user activities. Then correlate and analyze those user events against cloud application, user and network based events to identify anomalistic and potentially risky behavior in near real-time. Last, the outcome of this leads to preventative actions to defend against current and future attacks across the affected planes.

The Advent of the New Identity SOC

The traditional SOC (Security Operations Center) provides device management and monitoring services for firewalls, intrusion protection systems, proxies, and other perimeter and preventative security technologies. Alongside change management and maintenance of security devices, monitoring system logs and events have primarily been done using a security information and event management (SIEM) platform.

The Identity SOC is an identity and context-aware intelligence and automation solution. It provides the agility that is needed to detect and respond to advanced threats and persistent attacks and to provide a feedback loop for adaptation and evolution. The Identity SOC must protect users, applications/APIs, content/data as well as workloads.

The Identity SOC utilizes optimized dashboards and risk console for security professionals that is bringing in feeds from throughout your environment…

Oracle Identity SOC correlates identity-context to identify security risks and enables actionable intelligence for automated response

BENEFITS OF AN IDENTITY SOC

- Actionable intelligence on incidents supports a proactive defense as well as post-event analysis for root cause.
- Closes the gap where network-centric tools cannot cover
- Extends monitoring capability without consuming additional resources by automating post-event, investigation and response

WHY NOW?

- New advanced data analytics tools allow real-time streaming and analysis
- Cloud solutions are needed as traffic by-passes traditional network-centric tools
- Identity attribution is best way to cross-correlate risky activity of sophisticated attacks

ORACLE

- Security tools including firewalls, IDS, IPS, Web Proxy, VPN, AV, DLP, DAM, WAF, VA Scanners
- Applications and Workloads whether on-prem or in the cloud
- Infrastructure such as IaaS, PaaS, EMM, middleware, database, webservers, hypervisors and hosts (Windows, Linux and Unix)
- Networking tools such as routers, switches, DNS, DHCP and load balancers

The Identity SOC takes advantage of modern data analysis tools such as advanced analytics, machine learning and sophisticated data science techniques that allow identifying and investigating in near real-time. Behavioral analytics is used to detect suspicious behavior indicators of an attack. Attack path modelling is used to predict the potential path an attacker can take to escalate privileges. Finally, Identity SOC includes automated orchestration and incident response. Bi-directional integrations allow it to be self-healing enabling different departments to work together through organized playbooks and processes.

Oracle Delivers the World's First Identity SOC

Oracle has recognized this shift in the security landscape and in our customer's needs. Not only do we need to protect our own cloud, but our customers are looking for modern techniques to help them provide consistent security controls across cloud and on-prem environments. A 2016 Right Scale study said enterprises plan to use an average of six (6) cloud services to run their workloads. More than ever, coordinated security management is needed.

Oracle is making a big investment in the world's first Identity SOC. With three new security cloud services that integrate several new technologies into a homogeneous set of services. The integrated technologies include Security Incident and Event Management (SIEM), User & Entity Behavior Analytics (UEBA), Identity Management (IDM), and Cloud Access Security Broker (CASB). Each of these new services will integrate with the rest of your security fabric, but when joined together they offer the full benefit of a true Identity SOC with bi-directional controls and actionable intelligence.

Oracle Security Monitoring and Analytics (SMA) Cloud Service, built on Oracle Management Cloud's secure big data platform, enables rapid detection, investigation and remediation of the broadest range of security threats across on-premises and cloud assets.

Oracle Identity Cloud Service is Oracle's next-generation comprehensive security and identity platform that is cloud-native and designed to be an integral part of the enterprise security fabric, providing modern identity for modern applications.

Oracle Cloud Security Service, a leading Cloud Access Security Broker (CASB), enables organizations to protect business-critical cloud infrastructure and data with combined threat detection, predictive analysis, security configuration management and automated incident response and remediation.

Preventive controls protect the front door, but detection and response are required to protect your entire home.

COMPONENTS OF AN IDENTITY SOC

» Optimized Dashboards and Risk Consoles

» Advanced Analytics, Machine Learning and Data Science

» Automated Orchestration, Incident Response, & Self-Healing

WHY ORACLE?

» Only vendor to offer combined SIEM, UEBA, CASB and IDM in an integrated solution

» Security is in our DNA. Leaders in Identity, Big Data, Analytics, and Data Security

» Take advantage of the tools that are used to protect the Oracle Public Cloud for yourself

CONNECT WITH US

blogs.oracle.com

facebook.com/oracle

twitter.com/oracle

cloud.oracle.com

FOR MORE INFORMATION

Contact: 1.800.ORACLE1

ORACLE

Integrated Cloud Applications & Platform Services