Wohin geht Security bei Oracle?

Michael Fischer, ORACLE Deutschland B.V. & Co. KG

Security ist eine der Kompetenzen von Oracle. Bestehende Produkte werden um Sicherheitsfunktionen weiterentwickelt, neue Security-Services geschaffen und Firmen auch im Bereich „Security" akquiriert. Ziel ist die kontinuierliche Verstärkung der Absicherungsmöglichkeiten von Daten und Services. Um Silo-Landschaften entgegenzuwirken, erfolgt eine Vorintegration in eine Art Sicherheitsplattform, die optional genutzt werden kann. Dieser Artikel beschreibt den aktuellen Stand im Technologie-Portfolio von Oracle mit einem kurzen Ausblick in die Zukunft.

„Security needs automation" war eine der Schlüssel-Botschaften von Larry Ellison auf der Oracle Open World 2017. In seiner Keynote hatte er das plakativ mit dem Krieg der Systeme von Hackern gegen Menschen begründet, die ihre Systeme quasi manuell verteidigen. In diesem Wettrüsten kann nur Schritt gehalten werden, wenn auch bei der Verteidigung automatisiert wird. Weitere Gründe für eine Automatisierung sind:

- Mit der stetig wachsenden Zahl von Systemen in On-Premises- und Cloud-Umgebungen steigt der Aufwand, alle diese Umgebungen zu überwachen.
- Durch die zunehmende Intelligenz in Cyber-Attacken im Gegensatz zu den einfachen Datenabgriffen der Vergangenheit reicht die Funktionalität bisheriger Log-Auswertungen nicht mehr aus.
- Mit neuen Regularien wie der EU-Datenschutz-Grundverordnung und auch einem genaueren Blick auf die Einhaltung von Regularien sind mehr Sicherheitsnachweise erforderlich.

Neben der Automatisierung findet sich die Weiterentwicklung im Bereich „Security" in den einzelnen Technologien und in Security-Komponenten wie dem Monitoring. Monitoring-Komponenten haben zwei Entwicklungen Rechnung zu tragen; zum einen müssen Aktivitäten in und Konfigurationen von On-Premises-Systemen und Cloud-basierten Diensten überwacht werden. Zum anderen, bedingt durch immer intelligentere Cyber-Attacken, müssen Aktivitäten über Systeme hinweg und abweichend vom normalen Verhalten erkannt werden.

Laut Gartner-Analysten (siehe unter anderem Gartner CARPA 2017) wird das bisherige Security-Monitoring heute auf den Prüfstand gestellt, klassische „Security Information and Event Management"-Systeme (SIEM) erfüllen diese erweiterten Anforderungen nicht. Andere Umfragen von Sicherheitsverantwortlichen unterstreichen dies, indem die Mehrzahl angibt, mit den vielen separaten Sicherheitstools frustriert zu sein sowie Korrelationen und entsprechende Automatisierungzu vermissen (siehe auch Ponemon Institute Report, Challenges 2017).

Ist das eine rein akademische Betrachtung oder besteht hier tatsächlich Handlungsbedarf? Hilfestellungen bei dieser Überlegung liefern beispielsweise der „Oracle und KPMG Cloud Threat Report 2018", der Maßnahmen darstellt, die aktuell zum Schutz von On-Premises- oder Cloud-basierten Datenbanken eingesetzt werden. Diese zeigen, dass ein stärkerer Schutz durchaus möglich wäre. Die geschilderten Angriffsszenarien sind je nach Branche unterschiedlich, sodass unterschiedliche Schwerpunkte bei der Verteidigung sinnvoll sind. Der Report zeigt auch, dass die Mehrzahl der Kunden eine weitergehende Automatisierung bereits umgesetzt haben oder zumindest planen. Mit Bezug auf den aufgeführten Report sind im Folgenden die Punkte „Automatisierung" und „Security-Technologien" betrachtet.

Automatisierung

Automatisierung hilft bei der Sicherstellung von Security, sowohl beim Betrieb der Systeme als auch beim Incident beziehungsweise Security & Threat Monitoring. Die Automatisierung beim Betrieb lässt sich exemplarisch an der Oracle-Datenbank zeigen. Eine Weiterentwicklung bei der Oracle-Datenbank bezüglich eines möglichst automatisierten Betriebes umfasst automatisiertes Patching und eine automatisierte Aktualisierung beziehungsweise Anpassung verfügbarer Security und Betriebseinstellungen. Unterstützungen dazu gibt es seit Längerem unter anderem mit dem Oracle Enterprise Manager, der Basis-Mechanismen bereitstellt.

Ziel bei der Automatisierung ist es, einen möglichst hohen Grad von Autarkie des Systems zu ermöglichen, die weit über die Basis-Mechanismen hinausreicht. Automatisierung ist keine reine Software-Lösung, sondern umfasst neben der Technologie auch die beteiligten Personen und festgelegten Prozesse. Oracle hat dies mit der Bereitstellung der Autonomous Database erstmalig eingeführt. Aufgabenstellungen, die dabei beispielsweise im Falle von Regularien adressiert werden, sind berücksichtigt. So sind hier ein „least privilege"-Management oder der Zugriff auf Audit-Daten zu nennen.

Bei Autonomous gelten die Rahmenbedingungen der Services, die als Teil der Unternehmenspolicies akzeptabel sein müssen. Die Verantwortlichkeiten des

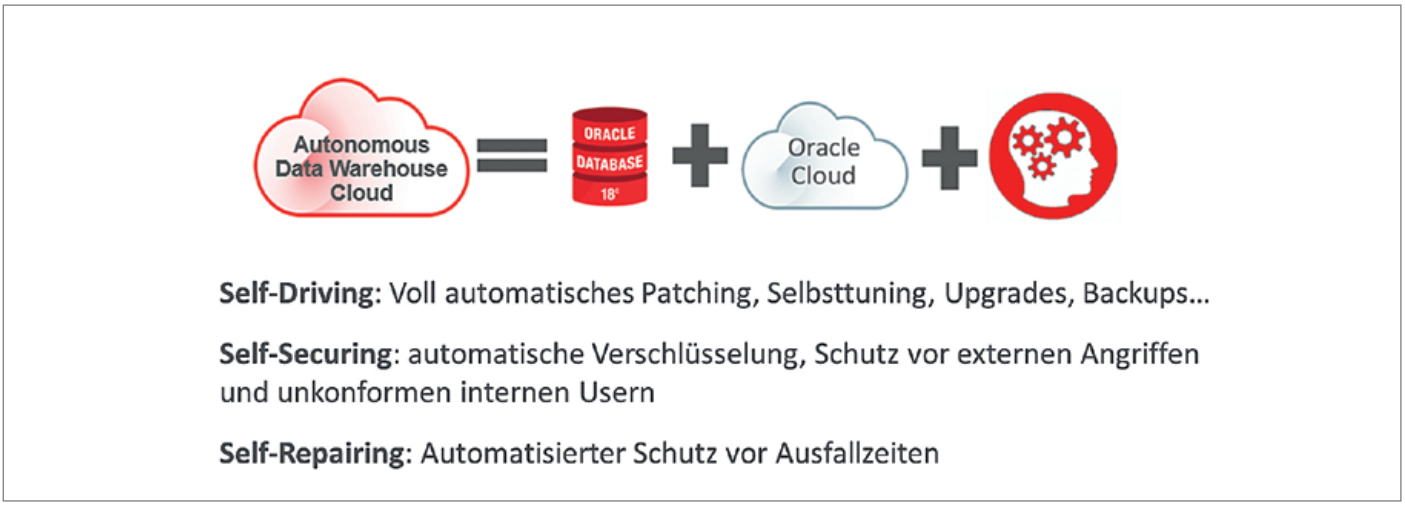

Abbildung 1: Oracle Autonomous Data Warehouse

Kunden sind gemäß den Unternehmensvorgaben umzusetzen, etwa Zugriffsberechtigungen, Schutz der Daten oder die Verarbeitung des Audit-Trails. Weitere Services sind zurzeit Oracle Autonomous Analytics Cloud, Oracle Autonomous Integration Cloud und Autonomous Visual Builder Cloud Service *(siehe Abbildung 1)*.

Die Automatisierung beim Security Monitoring kann durch ein Zusammenspiel verschiedener Oracle-Werkzeuge umgesetzt werden. Es kommen vier Komponenten zum Einsatz, die einzeln verwendet oder untereinander beziehungsweise in 3rd-Party-Systeme integriert werden können. Oracle stellt mit dem Oracle Enterprise Manager seit Längerem ein Werkzeug zum Monitoring der On-Premises- und Cloud-Installationen zur Verfügung. Der hier vorgestellte Ansatz legt andere, Cloud-basierte Werkzeuge von Oracle zugrunde, die weit über den Enterprise Manager hinausgehen. Zentrale Elemente des Monitorings bezüglich Security und Compliance sind:

- Die Überprüfung hinsichtlich der Aktionen in einzelnen Systemen und über Systeme hinweg.
- Eine fortwährende Prüfung der Konfiguration bezüglich der Unternehmens- und Compliance-Vorgaben.

Dieses Monitoring wird meist toolbasiert in SIEM-Systemen durchgeführt und durch ein Network Operation Center/Security Operation Center (NOC/SOC) betrieben. Traditionelle Ansätze sind typischerweise regelbasiert und arbeitsaufwendig. Dies birgt Herausforderungen, denen durch Automatisierung mithilfe von Machine Learning begegnet wird. Damit können viele der bisherigen manuellen Schritte im SOC automatisiert werden, sodass den SOC-Spezialisten mehr Zeit für komplexere Bewertungen und Analysen bleibt.

Automatisierung erfolgt beispielsweise beim Auffinden von Abweichungen durch automatisiertes User and Entity Behavior Analytics (UEBA), beim Aufspüren von Threats beziehungsweise Kill Chains oder bei Vorhersagen oder der Erkennung von allgemeinen Korrelationen und Mustern. Diese Funktionen werden von verschiedenen Oracle-Lösungskomponenten bereitgestellt. Sie bieten vorgefertigte Integrationen zu Systemen und nutzen einen unterliegenden Big-Data-Ansatz, um die beliebig wachsenden Daten in den Griff zu bekommen. Die Komponenten sind im Einzelnen:

- Oracle Management Cloud Security Monitoring Analytics (OMC SMA) zum Monitoring der Plattformen, ob On-Premises oder in der Cloud
- Oracle Management Cloud Compliance Control (OMC CC) zur Prüfung der Konfigurationen gegen Unternehmensvorgaben oder externe Regelwerke
- Oracle Cloud Access Security Broker (Oracle CASB) zum Entdecken einer Schatten-IT in der Cloud, dem Monitoring von Unternehmensvorgaben bezüglich Nutzung und Konfiguration von Oracle und 3rd-Party-Cloud-Diensten wie AWS, Salesforce, Azure, Box etc. sowie eine Data-Loss-Prevention-Funktionalität (DLP)
- Oracle Identity Cloud Service (Oracle IDCS) für das Bereitstellen eines Benutzerverwaltungs- und Authentifizierungssystems für On-Premises oder Cloud Services

Alle Komponenten zusammen bilden das im Jahr 2016 bei Gartner vorgestellte Oracle Identity Aware Security Operations Center (Identity SOC). Es vereint Identity, CASB, Security Monitoring & Analytics sowie Configuration Compliance und ermöglicht intelligente, risikobewusste Sicherheit in komplexen, hybriden Multi-Cloud-Umgebungen. In Kombination mit der Oracle Management Cloud bietet Oracle mit dem Security Monitoring ein einheitliches Dashboard für Management, Betrieb, Performance und Reporting *(siehe Abbildung 2)*.

Security-Best-Practices aus dem Report

Im „Oracle und KPMG Cloud Threat Report 2018" sind Security-Best-Practices aufgestellt. Diese tragen zwar Cloud-Security in der Überschrift, passen aber auch für On-Premises. On-Premises-Systeme haben die gleichen Problemstellen, sei es durch Mitarbeiter, eingeschleuste Maleware oder Zugriffsmöglichkeiten von außen. Die folgende Aufstellung aus dem Report ist keine umfassende Darstellung von Security-Best-Practices wie beispielsweise die CIS Controls, sondern dient zur Darstellung der von Oracle weiterentwickelten Security. Dabei kommen neue und

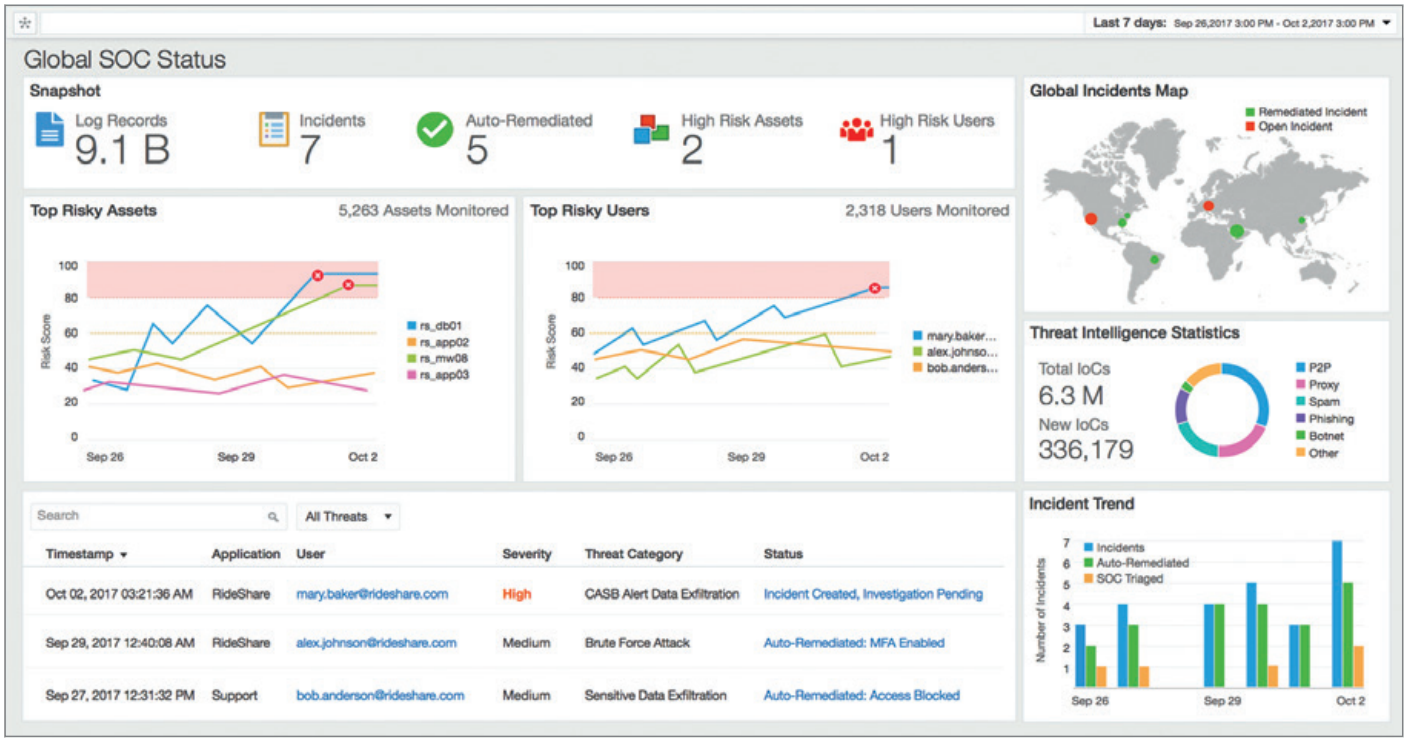

Abbildung 2: Oracle-Dashboard für das Security Monitoring

bekannte Mechanismen zum Tragen: Erstens müssen Policies für alle Umgebungen gelten und gesetzt werden – bei eigenen, externen oder Cloud-basierten Systemen oder Diensten. Um Policies in alle Umgebungen zu propagieren und durchzusetzen, können Provisionierungen und Enforcement Gateways/Proxys eingesetzt werden. Klassisches Identity und Access Management provisioniert Berechtigungen und stellt entsprechende Autorisierungen und SSO sicher. Werkzeuge von Oracle auch für hybride Umgebungen sind im IAM Portfolio. Erweitert wurde das IAM Portfolio um die Cloud-basierte Komponente, den Identity Cloud Service.

Zweitens bestimmt der Kontext der Daten deren Schutzbedarf mit, ein Aufruf von einem nicht registrierten Device beispielsweise ist unterschiedlich zu einem vertrauenswürdigen Device zu sehen. Kontextbasierte Autorisierung oder auch im Schritt vorher die kontextbasierte Anmeldemöglichkeit wird entweder in den Systemen umgesetzt (etwa während der Datenbank-Anmeldung) oder von einem zentralen Access-System durchgeführt (zum Beispiel mit Proxies). Werkzeuge von Oracle sind sowohl die eingangs gelisteten Komponenten als auch Funktionalitäten in den Produkten wie der Oracle-Datenbank.

Drittens sind Data Discovery und Klassifikation notwendig, um zu wissen, welche Daten im Unternehmen vorliegen und wie hoch der Schutzbedarf ist. In diesem Prozess wird die Anwendungslandschaft mit Hinblick auf verwendete Daten analysiert. Oracle bietet Hilfestellungen mit Werkzeugen bei der Inventarisierung und mit einem automatisierten Datenabgleich (Konsistenz der Datenquellen). Eine Analyse kann über das DBSat-Tool *(siehe "http://www.oracle.com/technetwork/database/security/dbsat/overview/index.html")* oder Application Data Modelling vom Enterprise Manager erfolgen, wenn neben den Dictionary-Funktionen auch Daten analysiert werden sollen. Die Data-Integration- und Enterprise-Quality-Data-Management-Werkzeuge können eingesetzt werden, wenn es um das Unternehmensdatenmodell und Datenabgleich geht. Die Werkzeuge von Oracle heißen wie in der Beschreibung in diesem Absatz aufgelistet.

Viertens ist die Verlässlichkeit des Schutzes durch Monitoring der gesetzten Konfiguration von Systemen und Einstellungen sicherzustellen. Die Konformität hinsichtlich der Konfiguration ist die Domäne von IT-Compliance. Werkzeuge von Oracle sind dazu der Enterprise Manager oder das „Configuration & Compliance"-Modul des Oracle Management Cloud Service. Vorhandene Regelwerke (STIG, CIS, Best Practices) können ausgewählt und auch angepasst werden. „Configuration & Compliance" hilft auch, ähnliche Datenbank-Umgebungen über Clustering zu erkennen, um Regelwerke individuell anzupassen.

Fünftens ist ein Schutz gegen Angriffe notwendig, um neben dem zuvor beschriebenen Schutz auch die Ausnutzung von Lücken in Systemen und Missbrauch von Accounts zu verhindern oder zumindest zu entdecken. Für Threat Prevention, hier durch das aktive, systemübergreifende Monitoring von Oracle und 3rd-Party-Komponenten, stellt Oracle Security Monitoring und CASB-Service zur Verfügung. Beide können Threats erkennen sowie die einzelnen Stufen von Kill Chains wie Lateral Movements.

Sechstens braucht es Data Loss Prevention, um einen ungewünschten Abfluss von Daten zu verhindern. Data Loss Prevention (DLP) wird vorrangig durch Unternehmenspolicies adressiert. Vergebene und regelmäßig überprüfte Berechtigungen beschreiben den Kreis der legalen Zugriffe. Unrechtmäßige Versuche werden im Vorfeld verhindert (Fehlkonfigurationen entdecken, bevor sie genutzt werden) oder beim Zugriff geblockt. Für dieses Blocken kann die starke Authentifizierung der Datenbank genutzt werden, die die Umgebungspa-

rameter auswertet, Tools auf dem Client oder ein Zugriff über einen Proxy. Im Fall von Datenbank-Zugriffen über Database Activity Monitoring (DAM) und im Falle von webbasierten Services über einen DLP-CASB-Proxy.

Siebentens ist Monitoring des tatsächlichen Verhaltens eines Benutzers oder Systems (UEBA) erforderlich, um herauszufinden, inwieweit Abweichungen vom normalen Verhalten vorhanden sind, um damit erkennen zu können, dass beispielsweise ein Account in fremde Hände gelangt ist oder der Mitarbeiter nicht unternehmenskonform agiert. Cloud Access Security Broker und Security Monitoring enthalten Policy-Monitoring, Threat-Erkennungen und UEBA-Komponenten. Alle drei Funktionen tragen zur Verhaltensanalyse bei. Threat-Erkennung kommt beispielsweise bei Brute-Force-Log-in-Versuchen zum Tragen oder beim Zugriff von wechselnden Orten in kürzester Zeit. UEBA vergleicht den Benutzer oder das System mit seinem normalen Verhalten oder dem Verhalten einer Vergleichsgruppe. So können Unregelmäßigkeiten bei SQL-Befehlen erkannt werden oder Systeme, die für andere Aufgaben zweckentfremdet werden.

Status quo der Installation bei Datenbanken

Laut dem Status quo bei Datenbanken („Oracle und KPMG Cloud Threat Report 2018“) nutzt lediglich die Hälfte der Befragten Datenbank-Firewalls, Verschlüsselung, Web-Application-Firewalls (WAF) und übergreifendes Monitoring. Etwa ein Viertel der Befragten nutzt beim Monitoring auch weiterentwickelte Technologien wie Machine Learning. Eine Annäherung an die Einführung des automatisierten Betriebs, hier Security Automation, ist erfolgt, aber noch nicht umgesetzt.

Bestehende Mechanismen oder Funktionalitäten werden noch nicht vollständig ausgeschöpft und bieten, auch wenn sie systemübergreifend eingesetzt werden, viel Potenzial für eine stärkere Absicherung. Dies ist jedoch nicht das Ende der Entwicklung der Datenbank; die aktuelle Version 18c bringt weiterentwickelte Security-Mechanismen, die in dieser Ausgabe im vorangegangenen Artikel vorgestellt sind.

Die Cloud

Cloud ist nochmal ein anderer Blickwinkel. Die bisher beschriebenen Mechanismen, Services oder Technologien können alle ebenfalls in einem Cloud-Szenario genutzt werden. Darüber hinaus bietet die Cloud weitere Sicherheitsmerkmale, die eigenständig weiterentwickelt werden. Beginnend mit dem Security-Paradigma „secure by default“ werden instanziierte Komponenten wie Datenbanken oder Storage verschlüsselt aufgesetzt und die Berechtigungen nach dem „least privilege“-Prinzip initial so zugewiesen, dass die Nutzung durch den Cloud-Verantwortlichen des Kunden erst freigeschaltet werden muss.

Services nutzen die Basis-Infrastruktur der Cloud, die unter Sicherheitsgesichtspunkten aufgesetzt und stetig weiterentwickelt wird. Nur zwei Merkmale davon sind die Off-Box-Netzwerk-Virtualisierung, um das Netzwerk zu definieren und abzusichern (SDN ohne zentralen Controller), und die exklusiven Nutzungsmöglichkeiten von dedizierten Servern. Mehr Informationen dazu stehen im Artikel zum Frankfurter Oracle Datacenter in dieser Ausgabe auf Seite 58.

Fazit und Ausblick

Security von, mit und bei Oracle bleibt ein spannendes Thema. Oracle erweitert im Security-Umfeld sein Portfolio kontinuierlich mit Eigenentwicklungen und Zukäufen, zuletzt mit der Akquise von Dyn (DNS-Service) und dem noch nicht vollständig durchgeführten Zukauf von Zenedge, einer Web-Application-Firewall inklusive Service-Management.

Die vergangenen Jahre brachten einen Ausbau des Portfolios um Sicherheitsfunktionen wie im Datenbank-Bereich, Sicherheits-Komponenten im Identity und Access Management mit speziellen Cloud Security Services sowie durch den Aufbau von Cloud-Rechenzentren der nächsten Generation. Der Portfolio-Ausbau ist natürlich nicht abgeschlossen, kommende Services bringen Erweiterungen in DLP oder im Bereich „Governance in der Cloud“.

In die Weiterentwicklung eingebracht wurde eine weitere Automatisierung sowohl für den Betrieb von Komponenten (wie Datenbank) als auch für das Monitoring. Entscheidenden Beitrag dazu leistet das jeweils integrierte Machine Learning. Die Hürde für potenzielle unrechtmäßige oder unbeabsichtigte Zugriffe wird höher gelegt, Unregelmäßigkeiten werden weitgehend automatisiert erkannt. Fehlkonfigurationen, vernachlässigtes Einspielen von Patches oder Probleme bei Verfügbarkeit, Backup und Restore werden unwahrscheinlicher. Die Automatisierung wird weiter vorangetrieben und ist für weitere Services geplant.

Dem Wandel des Betriebsmodells wurde ebenfalls Rechnung getragen. DevOps und Cloud-Native-Development werden unterstützt, ebenso wie der Umbau der SIEM- oder Netzwerk-Monitoring-Teams mit der Einführung von Security Operation Centers (SOC). Hier ist der SOC-Spezialist nicht mehr allein, um die Drehscheibe um SIEM-Informationen beziehungsweise Alarme zu bewerten. Algorithmen aus dem Bereich „Machine Learning“ oder aus der Daten-Analyse übernehmen nun das Aussortieren relevanter Daten und leiten gegebenenfalls eine automatisierte Behandlung ein.

Die Weiterentwicklung beim Thema „Sicherheit“ erfolgt bei Oracle unter verschiedenen Aspekten: mehr Automatisierung, mehr künstliche Intelligenz, Erweiterung der Sicherheitsfunktionen in vorhandenen Komponenten und weiteren neuen Komponenten sowie Cloud Services. Um hier Silo-Landschaften entgegenzuwirken, erfolgt parallel die Integration in eine Art Sicherheits-Plattform, die optional genutzt werden kann.

Weitere Informationen

- Securitykomponenten von Oracle: *https://www.oracle.com/security*
- Autonomous Services: *https://www.oracle.com/autonomouscloud/index.html*

Michael Fischer
michael.fischer@oracle.com