McAfee
Together is power.

Oracle Unified Auditing - Was passiert mit meinen Daten?

Christian Deneke | 27. Juni 2018
Product Specialist

christian_deneke@mcafee.com

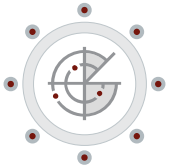
Top - Datenbanksicherheitsherausforderungen

Mangel an Transparenz und Kontrolle der Daten

Finden und Schützen der sensitiven Daten

Einhaltung gesetzlicher Vorschriften

Erfüllen bestehender oder neuer behördlicher Compliance-Anforderungen



Steigende Erfolgsrate von Malware-Angriffen

Schutz vor Zero-Day und bekannter Malware

Warum Auditing der Daten und Zugriffe?

- Compliance Anforderungen
- Interne Security Policy

Wo sind meine Daten …. überhaupt?

- Wenn ich nicht weiß wo meine zu schützenden Daten sind, wie soll ich diese denn schützen?

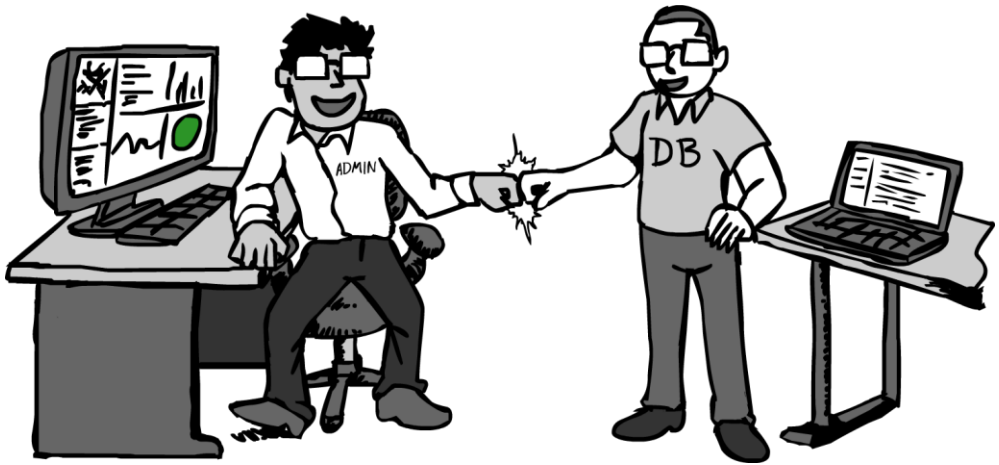
- Was sind meine zu schützenden Daten?

Was sind die Herausforderungen beim Audit-Regel erstellen?

- Wartbarkeit
- Übersichtlichkeit
- Aktualisierung
- Revisionsmöglichkeit

Wer darf und kann Regeln erstellen oder ändern?

- Der Datenbankadministrator
- Der Applikationsverantwortliche
- Das SOC Team
- Der Security Officer



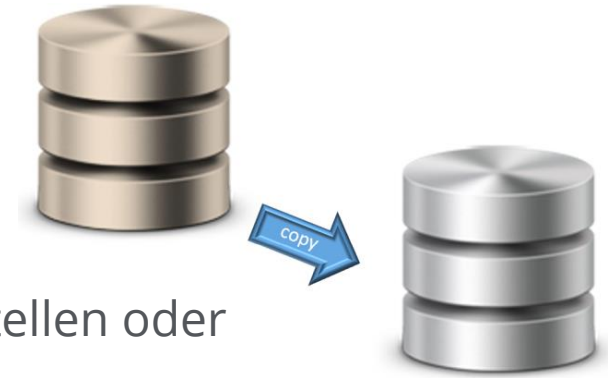
Wer wertet die Regeln aus und wer wird informiert?

- Wie verwalte ich die gewonnenen Daten?

- Wen informiere ich?
  - Den Datenbank - Administrator
  - Den Applikationsverantwortlichen
  - Das SOC Team
  - Den Security Officer

Wie kommen die Regeln auf eine neue Datenbank?

Was mache ich, wenn eine weitere Datenbank installiert wird?



- Besitzt diese zu schützende Daten?
- Muss ich das Regelwerk komplett neu erstellen oder kann ich ein vorhandes kopieren?

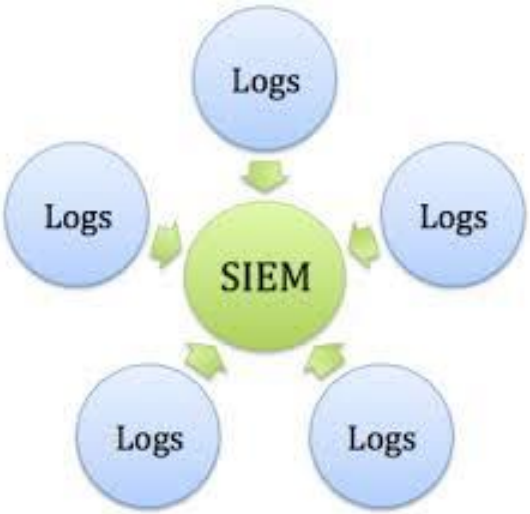
Was passiert bei einem Datenbank - Software Update?

- Hat sich etwas an meiner Syntax geändert?
- Hat sich etwas an meinen Regeln geändert?
- Sind meine Regeln noch aktiv, wie prüfe ich das?
- Was mache ich bei einem Mischbetrieb mit unterschiedlichen Datenbank - Software Versionen?

Integration mit SIEM

Korrelation von Events

- Oracle 12c unified auditing unterstützt kein Syslog, kommt erst mit 18c



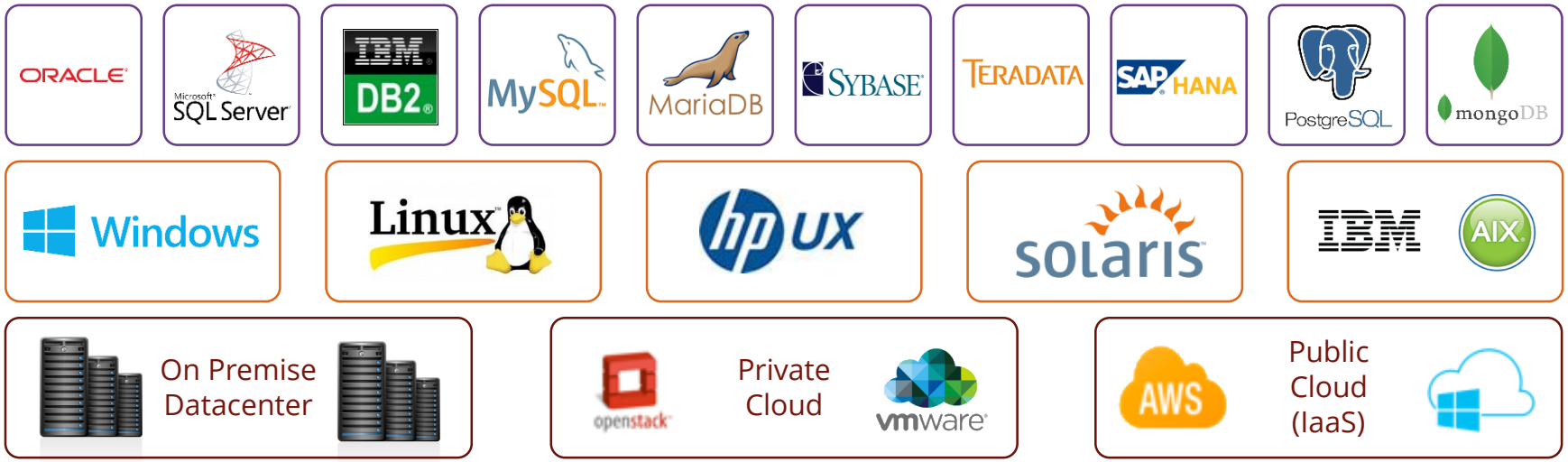
Housekeeping & Testing

- Audit-Log aufräumen
- Wird meine Regel noch benötigt?

- Triggert meine Regel noch?

Was mache ich einer multivendor Umgebung?

Was mache ich, wenn es mehr Datenbanken gibt als nur Oracle?



Beispiel für eine einfache Regel

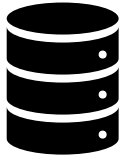
Einfaches Beispiel für eine Regel

Erlaubter Zugriff

Mitarbeiter
aus dem AD

IP Adresse(n)
statisch oder DHCP

Bekannte Application



Benötigte Instanz(en)

Rule Object (dynamic)
Bekommt die Benutznamen
Dynamisch aus dem AD

Rule Object
IP Adressen
Informationen

Rule Object
Freigegebene
Software

user not in $HR_user AND client_ip not in $HR_IP AND application not in $HR_Appl AND instance not in $SAP_DB
=> sendet ein Alarm und/oder blockieren des Zugriffs

Wie könnte eine mögliche Lösung aussehen?

McAfee Database Security

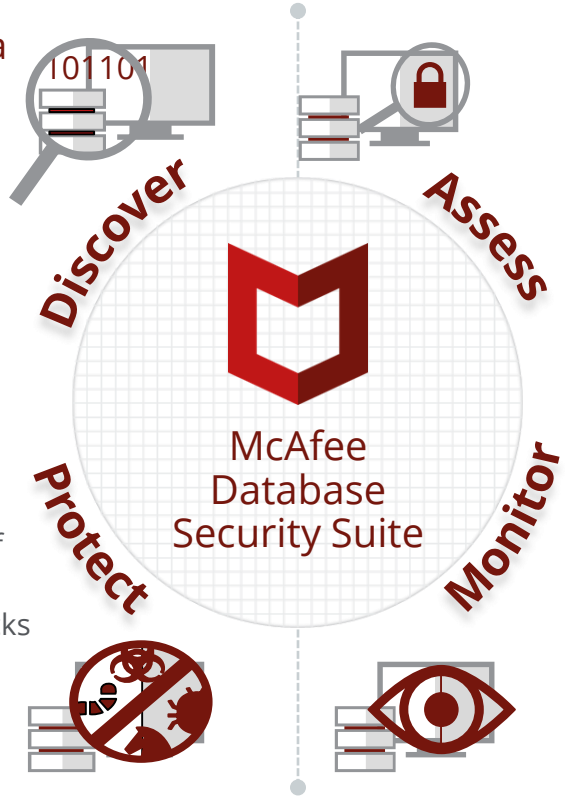
What we deliver

Database Discovery & Data Classification

- Database Discovery
- Sensitive Data Discovery
- User Rights Management
- GDPR, BSI, CIS Specific

Protection and Virtual Patching

- Identification and Prevention of Exploitation Attempts
- Protection Against Known Attacks
- Generic Pattern
- Abnormal Activity



Security Assessment

- Vulnerabilities
- Misconfiguration
- Missing Patches
- Vulnerable Code
- More than 6000 Checks

Activity Monitoring

- Real-Time Monitoring
- Policy Enforcement
- Audit, Alert or Block Activity

McAfee Database Security

Best of Breed

Security Research	Most credited security research team for discovered vulnerabilities that increase customers' security posture.
Software-Only Solution	Simple and intuitive deployment. Does not require additional hardware or network changes which keeps total cost of ownership low.
Fully Distributed Architecture	Does not require remote components which makes maintaining and management easy.
Autonomous Sensors	Autonomous architecture allows sensors to receive policies and enforce locally in real-time. Enables high level of security independent of Management Server.
Wide vPatch Protection	Automatically updated virtual patching for continuous virtual patching protection.
Unique In-Memory Monitoring	Patented in-memory monitoring technology makes it possible to see obfuscated or local statements.
Most Comprehensive Assessment Checks	More than 6000 pre-built security and data discovery checks makes risk assessment and data discovery fast and reliable.
Non-Intrusive Zero Risk Design	Developed with performance and uptime in mind. Zero-risk deployment, no reboot required. Greatly reduces risk and downtime.

McAfee, the McAfee logo and [insert <other relevant McAfee Names>] are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the U.S. and/or other countries.
Other names and brands may be claimed as the property of others.
Copyright © 2017 McAfee, LLC.