IBM Guardium ile Sürekli Veri Güvenliği ve Denetim

Modern Veri Güvenliğinde Database Activity Monitoring (DAM) Yaklaşımı

IBM Guardium ile Gerçek Zamanlı İzleme, İç Tehdit Yönetimi ve Regülasyon Uyumluluğu

Yazan: Seyhan Tekelioğlu


IBM
GUARDIUM
VERİTABANI AKTİVİTE İZLEME, VERİ GÜVENLİĞİ, UYUM VE DENETİM REHBERİ
KAPSAMLI TEKNİK KAYNAK, EN İYİ UYGULAMALAR VE SAHA DENEYİMLERİYLE
GERÇEK ZAMANLI İZLEME
POLİTİKA TABANLI KONTROL
HASSAS VERİ KEŞFİ VE SINIFLANDIRMA
UYUMLULUK OTOMASYONU
DETAYLI RAPORLAMA
SIEM ENTEGRASYONU
RİSK ANALİZİ
OLAY YÖNETİMİ
VERİ GÜVENLİĞİ
UYUMLULUK
DENETİM
İZLEME & ANALİZ
ALARM YÖNETİMİ
HASSAS VERİ KORUMA
DASHBOARD
78%
AKTİVİTE İZLEME
RİSK ANALİZİ
KRİTİK 24
YÜKSEK RİSK 56
ORTA RİSK 128
DÜŞÜK RİSK 195
GUARDIUM
UYUMLULUK
KVKK
PCI DSS 4.0
ISO/IEC 27001
NIST CSF 2.0
VERİTABANI GÖRÜNÜRLÜĞÜ
YETKİ VE ERİŞİM KONTROLÜ
DENETİM KANITI ÜRETİMİ
SIEM & SOAR ENTEGRASYONU
BULUT VE HİBRİT DESTEĞİ
VERİNİZİ İZLEYİN, KORUYUN, YÖNETİN.
RİSKLERİ AZALTIN, GÜVENİ ARTIRIN.
YAZAN: SEYHAN TEKELİOĞLU

İçindekiler

Özet

Kurumların dijital dönüşüm yolculuğu, veriyi en kritik kurumsal varlıklardan biri hâline getirmiştir. Finans, sağlık, kamu, üretim ve telekomünikasyon gibi sektörlerde iş süreçlerinin büyük bölümü artık veritabanları üzerinde yürütülmektedir. Bu nedenle saldırganların odağı da sunuculardan ve uç noktalardan doğrudan veriye yönelmiştir.

Geleneksel güvenlik yatırımları; güvenlik duvarları, saldırı tespit sistemleri (IDS), saldırı önleme sistemleri (IPS), uç nokta koruma çözümleri (EDR/XDR) ve kimlik yönetimi platformları ile ağın ve sistemlerin korunmasını hedefler. Ancak bu çözümler, veritabanı içerisinde gerçekleşen her işlemi ayrıntılı olarak izlemek veya yetkili kullanıcıların faaliyetlerini denetlemek için tasarlanmamıştır.

Modern tehdit ortamında en kritik risklerden biri, **yetkili kullanıcılar tarafından gerçekleştirilen kötüye kullanım** veya **çalınmış kimlik bilgileriyle yapılan erişimlerdir**. Bir saldırgan, geçerli kimlik bilgileriyle veritabanına erişim sağladığında, yalnızca ağ trafiğini izleyen güvenlik çözümleri bu faaliyetleri her zaman tespit edemeyebilir. İşte bu noktada **Database Activity Monitoring (DAM)** çözümleri devreye girer.

IBM Guardium; veritabanı aktivitelerini gerçek zamanlı olarak izleyen, kayıt altına alan, analiz eden ve gerektiğinde otomatik aksiyon alabilen kapsamlı bir veri güvenliği platformudur. Çözüm, yalnızca SQL sorgularını kaydetmekle kalmaz; aynı zamanda hassas veri erişimlerini belirler, politika ihlallerini tespit eder, denetim raporları üretir ve kurumların KVKK, PCI DSS, ISO 27001 gibi düzenlemelere uyum süreçlerini destekler.

Bu makalenin amacı, IBM Guardium'un kurumlara sağladığı teknik ve operasyonel faydaları açıklamak, gerçek kullanım senaryolarını

incelemek ve modern veri güvenliği yaklaşımında neden kritik bir rol oynadığını ortaya koymaktır.

---

1. Giriş

1.1 Veri Artık Yeni Petrol Değil; İş Sürekliliğinin Temelidir

Son yıllarda "Veri yeni petroldür." ifadesi sıkça kullanılmaktadır. Ancak günümüz koşullarında bu benzetme yetersiz kalmaktadır. Çünkü veri artık yalnızca ekonomik değeri olan bir kaynak değil, aynı zamanda kurumların operasyonel devamlılığını sağlayan temel unsurdur. Bir finans kuruluşunda müşteri kayıtları, bir hastanede elektronik sağlık kayıtları veya bir üretim tesisinde üretim reçeteleri olmadan operasyonların sürdürülebilmesi mümkün değildir.

Bu nedenle saldırganlar da hedeflerini değiştirmiştir. Geçmişte sunucuların ele geçirilmesi ön plandayken, günümüzde amaç doğrudan veriye erişmek, hassas bilgileri çalmak veya veriyi manipüle etmektir. Fidye yazılımı grupları, veri sızıntısı odaklı tehdit aktörleri ve içeriden gelen riskler, kurumların güvenlik stratejilerini yeniden şekillendirmesine neden olmaktadır.

Birçok kurum; güvenlik duvarları, ağ segmentasyonu, çok faktörlü kimlik doğrulama ve uç nokta koruma çözümleri gibi katmanlı güvenlik önlemleri uygulamaktadır. Ancak bu önlemler, veritabanı içinde gerçekleşen her işlemi ayrıntılı biçimde görünür hâle getirmez. Örneğin, yetkili bir veritabanı yöneticisinin mesai saatleri dışında milyonlarca müşteri kaydını sorgulaması veya bir uygulama hesabının beklenmedik şekilde hassas tablolara erişmesi, yalnızca ağ seviyesindeki kontrollerle tespit edilemeyebilir.

Bu görünürlük eksikliği, yalnızca güvenlik açısından değil, denetim ve uyumluluk süreçleri açısından da önemli bir risk oluşturur. Denetçiler artık yalnızca "erişim kontrolü var mı?" sorusunu değil; "Kim, ne zaman, hangi veriye, hangi amaçla erişti?" sorularını da

sormaktadır. Bu soruların güvenilir ve değiştirilemez kayıtlarla cevaplanabilmesi, modern veri güvenliğinin temel gereksinimlerinden biridir.

Database Activity Monitoring (DAM) çözümleri, tam da bu ihtiyaca cevap vermek üzere geliştirilmiştir. Veritabanı üzerinde gerçekleşen işlemleri gerçek zamanlı olarak izleyen, analiz eden ve politika ihlallerini tespit eden bu teknolojiler, kurumlara hem güvenlik hem de denetlenebilirlik kazandırır. IBM Guardium ise bu alanda uzun yıllardır kullanılan, geniş veritabanı desteği ve gelişmiş politika yönetimiyle öne çıkan çözümlerden biridir.

Bu dokümanın devamında, veri güvenliği alanındaki güncel tehdit ortamı, IBM Guardium'un mimarisi, sağladığı faydalar ve regülasyonlara katkıları ayrıntılı olarak ele alınacaktır.

---

2. Günümüzde Veri Güvenliğinin Değişen Dinamikleri

2.1 Dijital Dönüşümün Yeni Güvenlik Paradigması

Son on yılda dijital dönüşüm, kurumların bilgi teknolojileri altyapılarında köklü değişikliklere neden olmuştur. Geleneksel veri merkezlerinin yerini hibrit bulut mimarileri alırken; mikro servisler, konteyner teknolojileri, API tabanlı uygulamalar ve yapay zekâ destekli iş süreçleri kurumsal BT'nin vazgeçilmez bileşenleri hâline gelmiştir.

Bu dönüşüm yalnızca uygulama mimarilerini değiştirmemiş, aynı zamanda **kurumsal verinin erişilebilirliğini ve saldırı yüzeyini de önemli ölçüde artırmıştır**. Günümüzde aynı veritabanına;

- Web uygulamaları,
- Mobil uygulamalar,
- ERP sistemleri,
- CRM platformları,
- İş zekâsı araçları,
- Harici entegrasyon servisleri,
- Bulut uygulamaları,
- API ağ geçitleri,
- Yapay zekâ servisleri

Eş zamanlı olarak erişebilmektedir.

Bu çeşitlilik, operasyonel verimliliği artırırken güvenlik açısından yeni riskleri de beraberinde getirmiştir. Artık yalnızca dış tehditlere karşı koruma sağlamak yeterli değildir; içeriden gelen

risklerin, yetkili kullanıcı faaliyetlerinin ve uygulama katmanındaki veri erişimlerinin de sürekli izlenmesi gerekmektedir.

2.2 Saldırganların Hedefi Artık Sistemler Değil, Veridir

Geçmişte siber saldırılar çoğunlukla sistemleri çalışamaz hâle getirmeye odaklanırken, günümüzde temel hedef doğrudan kurumsal verilerdir.

Bunun başlıca nedenleri şunlardır:

- Kişisel verilerin yüksek ekonomik değeri
- Finansal bilgilerin karaborsada satılabilmesi
- Fikri mülkiyet verilerinin stratejik önemi
- Sağlık kayıtlarının uzun süreli kötüye kullanılabilmesi
- Kimlik bilgilerinin başka saldırılarda kullanılabilmesi

Bir saldırgan için işletim sistemine erişim çoğu zaman nihai hedef değildir; amaç veritabanındaki kritik bilgilere ulaşmaktır. Bu nedenle başarılı saldırılar incelendiğinde, saldırının son aşamasında çoğunlukla yoğun SQL sorguları, toplu veri okuma işlemleri veya veri dışa aktarma (export) faaliyetleri görülmektedir.

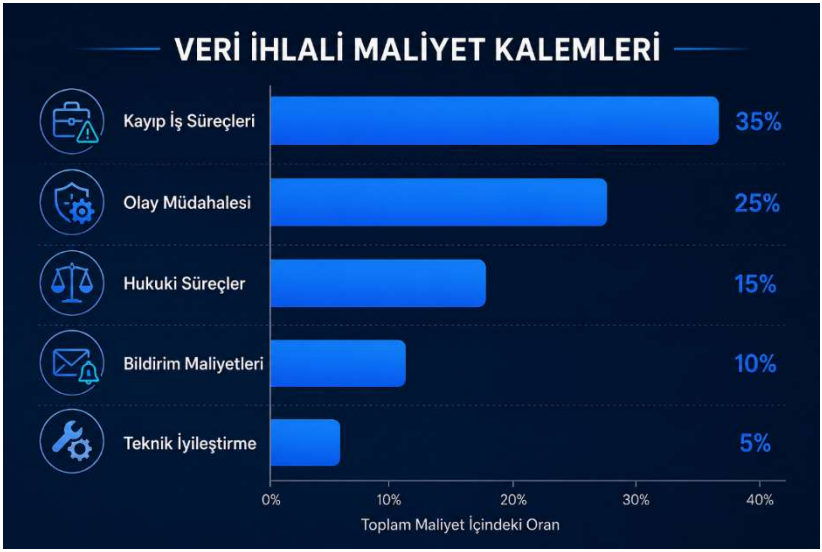
2.3 Veri İhlallerinin Ekonomik Boyutu

Veri ihlalleri yalnızca teknik bir güvenlik problemi değildir; aynı zamanda kurumların finansal performansını, marka itibarını ve yasal yükümlülüklerini doğrudan etkileyen stratejik bir risk unsurudur.

IBM ve Ponemon Institute tarafından yayımlanan **Cost of a Data Breach Report 2025** araştırmasına göre:

Bu veriler, ihlallerin yalnızca saldırı anındaki zarardan ibaret olmadığını göstermektedir. Maliyet; olay müdahalesi, hukuki süreçler, düzenleyici yaptırımlar, müşteri kaybı, operasyonel kesinti ve itibar zedelenmesi gibi birçok kalemden oluşmaktadır.

Şekil 2.1 – Veri İhlali Maliyet Dağılımı



2.4 İç Tehditler Neden Daha Tehlikelidir?

Çoğu kurum güvenlik yatırımlarını dış saldırganlara karşı planlamaktadır. Oysa birçok olayda saldırganlar, geçerli kullanıcı hesaplarını ele geçirerek veya yetkili kullanıcıları kötüye kullanarak veriye erişmektedir.

İç tehditler üç ana grupta incelenebilir:

Kötü niyetli çalışanlar

- Veri hırsızlığı
- Rakip firmalara bilgi aktarımı
- Ayrılmadan önce toplu veri kopyalama

İhmalkâr kullanıcılar

- Yanlış SQL çalıştırılması
- Yetkisiz veri paylaşımı

- Güvenlik politikalarının ihlali

Ele geçirilmiş hesaplar

- Çalınmış DBA hesapları
- Servis hesapları
- Uygulama kullanıcıları
- API kimlik bilgileri

Bu tür faaliyetler çoğu zaman "geçerli kullanıcı" kimliğiyle gerçekleştirildiği için yalnızca ağ seviyesindeki güvenlik kontrolleriyle tespit edilmeleri zordur. Veritabanı üzerinde gerçekleşen işlemlerin ayrıntılı biçimde izlenmesi kritik önem taşır.

2.5 Yapay Zekâ ve Yeni Risk Alanları

2025 yılında yayımlanan IBM araştırması, yapay zekâ sistemlerinin güvenlik yönetişiminin birçok kurumda yeterince olgunlaşmadığını göstermektedir.

Araştırmanın öne çıkan bulguları:

- Küresel ortalama veri ihlali maliyeti **4,44 milyon USD** olarak ölçülmüştür.
- Kuruluşların önemli bir bölümü yapay zekâ yönetişim politikalarını henüz tamamlamamıştır.
- Güvenlik operasyonlarında yapay zekâ ve otomasyonu etkin kullanan kurumlar, ihlal başına ortalama **1,9 milyon USD** tasarruf sağlamıştır.

- Gölge yapay zekâ (Shadow AI) kaynaklı olaylar ise ihlal maliyetlerini artıran yeni bir risk alanı olarak öne çıkmıştır.

Yapay zekâ destekli uygulamaların kurumsal veritabanlarına erişmesi, bu erişimlerin de diğer kullanıcılar gibi izlenmesini gerekli hâle getirmektedir. Gelecekte DAM çözümlerinin yalnızca insan kullanıcıları değil, yapay zekâ ajanlarını ve otomatik servis hesaplarını da politika bazlı denetlemesi beklenmektedir.

2.6 Ağ Güvenliği Tek Başına Yeterli mi?

Birçok kurum aşağıdaki güvenlik yatırımlarını yapmaktadır:

- Yeni nesil güvenlik duvarları
- Web Application Firewall (WAF)
- EDR/XDR
- Çok faktörlü kimlik doğrulama (MFA)
- SIEM
- E-posta güvenliği
- Ağ erişim kontrolü (NAC)

Bu teknolojilerin her biri kritik öneme sahip olsa da ortak bir sınırlamaları vardır: **Veritabanı içinde gerçekleşen işlemleri SQL seviyesinde yorumlayamazlar.**

Örneğin aşağıdaki sorgu teknik olarak tamamen meşru görünebilir:

```
SELECT *
FROM CUSTOMER_CREDIT_CARD
WHERE COUNTRY='TR';
```

Ancak şu sorular yalnızca ağ güvenliği ürünleriyle cevaplanamaz:

- Bu sorguyu kim çalıştırdı?
- Normal görev tanımına uygun muydu?
- Daha önce bu tabloya erişmiş miydi?
- Aynı kullanıcı son bir saat içinde kaç kayıt okudu?
- Erişim mesai saatleri dışında mı gerçekleşti?
- Sonuçlar dışarı aktarıldı mı?

İşte **Database Activity Monitoring** çözümleri bu görünürlüğü sağlayarak güvenlik ekiplerinin olayları bağlamıyla değerlendirmesine yardımcı olur.

Bölüm Sonu Değerlendirmesi

Kurumların güvenlik stratejisi artık yalnızca çevre güvenliğine odaklanamaz. Gerçek risk, kritik verinin bulunduğu noktada başlar. Ağ katmanında görünmeyen ancak veritabanında gerçekleşen faaliyetlerin izlenmesi; hem güvenlik operasyonlarının etkinliği hem de denetim ve mevzuat uyumluluğu açısından vazgeçilmezdir.

IBM Guardium gibi DAM çözümleri, bu görünürlüğü sağlayarak kurumların yalnızca saldırıları tespit etmesine değil, aynı zamanda veriye kimlerin, ne zaman ve hangi amaçla eriştiğini kanıtlayabilmesine olanak tanır.

---

3. Dünya Genelinde Veri İhlalleri ve IBM Guardium Perspektifinden Analizi

3.1 Veri İhlalleri Neden Hâlâ Artıyor?

Son yıllarda güvenlik teknolojilerine yapılan yatırımlar önemli ölçüde artmasına rağmen, büyük ölçekli veri ihlallerinin sayısı azalmamıştır. Bunun temel nedenlerinden biri, saldırganların artık ağ altyapısını hedeflemek yerine **kimlik bilgilerini, uygulamaları ve doğrudan veriyi hedef alan** yöntemlere yönelmesidir.

Tipik bir modern saldırı zinciri şu şekilde ilerler:

Bu zincirin ilk aşamalarında EDR, SIEM veya ağ güvenliği ürünleri önemli rol oynasa da, saldırgan veritabanına ulaştığında **asıl görünürlük ihtiyacı Database Activity Monitoring çözümleriyle karşılanır**.

3.2 Equifax Veri İhlali (2017)

Olay Özeti

2017 yılında yaşanan Equifax veri ihlali, siber güvenlik tarihinin en büyük olaylarından biri olarak kabul edilmektedir.

Yaklaşık **147 milyon** kişinin kişisel bilgileri saldırganların eline geçmiştir.

Ele geçirilen bilgiler arasında;

- Kimlik numaraları
- Doğum tarihleri
- Adresler
- Kredi geçmişi
- Sürücü belgesi bilgileri

Bulunuyordu.

Saldırının başlangıç noktası, internet üzerinden erişilebilen bir web uygulamasındaki kritik bir güvenlik açığıydı. Ancak olayın en yıkıcı kısmı, saldırganların uygulama katmanını aşarak veritabanındaki hassas verilere erişebilmesiydi.

IBM Guardium Perspektifi

Guardium bu tür bir senaryoda;

✓ Hassas tabloların erişimini izleyebilir.

✓ Beklenmeyen SELECT yoğunluğunu tespit edebilir.

✓ Normal davranışın dışındaki kullanıcı aktivitelerini işaretleyebilir.

✓ Kritik tablo erişimlerinde gerçek zamanlı alarm üretebilir.

✓ SIEM platformuna olay aktarabilir.

✓ Olay sonrası adli analiz için ayrıntılı SQL kayıtları sağlayabilir.

Önemli Not: Guardium, web uygulamasındaki güvenlik açığını ortadan kaldırmaz; ancak saldırgan veritabanına eriştiğinde bu faaliyetleri görünür hâle getirerek olayın erken fark edilmesine katkı sağlayabilir.

3.3 Capital One Veri İhlali (2019)

Olay Özeti

Capital One olayında saldırgan, yanlış yapılandırılmış bulut servislerinden yararlanarak büyük miktarda müşteri verisine erişmiştir.

Yaklaşık **100 milyon** müşteri etkilenmiştir.

Erişilen veriler arasında:

- Kredi başvuruları
- Gelir bilgileri
- Kimlik bilgileri
- Banka hesap verileri

Yer almaktaydı.

Bu olay, yalnızca ağ güvenliğinin değil, **bulut üzerindeki veri erişimlerinin de sürekli izlenmesi gerektiğini** göstermiştir.

IBM Guardium Perspektifi

IBM Guardium'un bulut veri platformlarını destekleyen sürümleri sayesinde:

- Hassas veri erişimleri izlenebilir.
- Yetkisiz servis hesapları tespit edilebilir.
- Toplu veri okuma davranışları belirlenebilir.
- Politika ihlalleri gerçek zamanlı olarak raporlanabilir.
- Denetim kayıtları merkezi olarak saklanabilir.

3.4 Marriott Veri İhlali

Marriott olayı, saldırganların uzun süre fark edilmeden sistem içerisinde kalmasının ne kadar büyük risk oluşturduğunu göstermiştir.

Yaklaşık dört yıl boyunca devam eden yetkisiz erişim sonucunda yüz milyonlarca müşteri kaydı etkilenmiştir.

Bu olayın en önemli derslerinden biri şudur:

Bir saldırının gerçekleşmesi kadar, ne kadar süre boyunca fark edilmeden devam ettiği de kritik öneme sahiptir.

IBM Guardium Perspektifi

Uzun süre devam eden aşağıdaki davranışlar Guardium politikalarıyla izlenebilir:

- Aynı kullanıcının sürekli hassas tablo sorgulaması
- Mesai saatleri dışında erişimler
- Beklenmeyen IP adreslerinden bağlantılar
- Servis hesaplarının olağan dışı SQL çalıştırması

- Anormal veri hacimleri

Bu tür davranışlar tek başına saldırı kanıtı değildir; ancak güvenlik ekipleri için güçlü inceleme sinyalleri oluşturur.

3.5 LastPass Olayı

LastPass olayı, bulut tabanlı sistemlerde depolanan hassas verilerin korunmasının önemini ortaya koymuştur.

Yetkili erişimlerin kötüye kullanılması ve kritik sistemlere ulaşılması sonucunda önemli miktarda veri etkilenmiştir.

Bu olayın ardından birçok kurum şu soruyu sormaya başlamıştır:

"Yetkili kullanıcılarımız gerçekten yalnızca ihtiyaç duydukları verilere mi erişiyor?"

İşte DAM çözümlerinin temel amacı da bu soruya kanıtlanabilir kayıtlarla cevap verebilmektir.

3.6 Snowflake Ekosistemindeki Olaylar (2024)

2024 yılında çeşitli kuruluşlar, çalınmış kimlik bilgileri kullanılarak bulut veri platformlarındaki hesaplara yetkisiz erişim sağlanması nedeniyle veri kayıpları yaşadı. Ortak nokta, birçok olayda **geçerli kullanıcı hesaplarının** kullanılmasıydı.

Bu tür senaryoların öne çıkardığı ihtiyaçlar:

- Ayrıcalıklı kullanıcıların sürekli izlenmesi
- Çok faktörlü kimlik doğrulamanın yaygınlaştırılması
- Olağan dışı sorgu hacimlerinin tespiti

- Toplu veri dışa aktarma davranışlarının izlenmesi
- Denetim kayıtlarının merkezi ve değiştirilemez biçimde saklanması

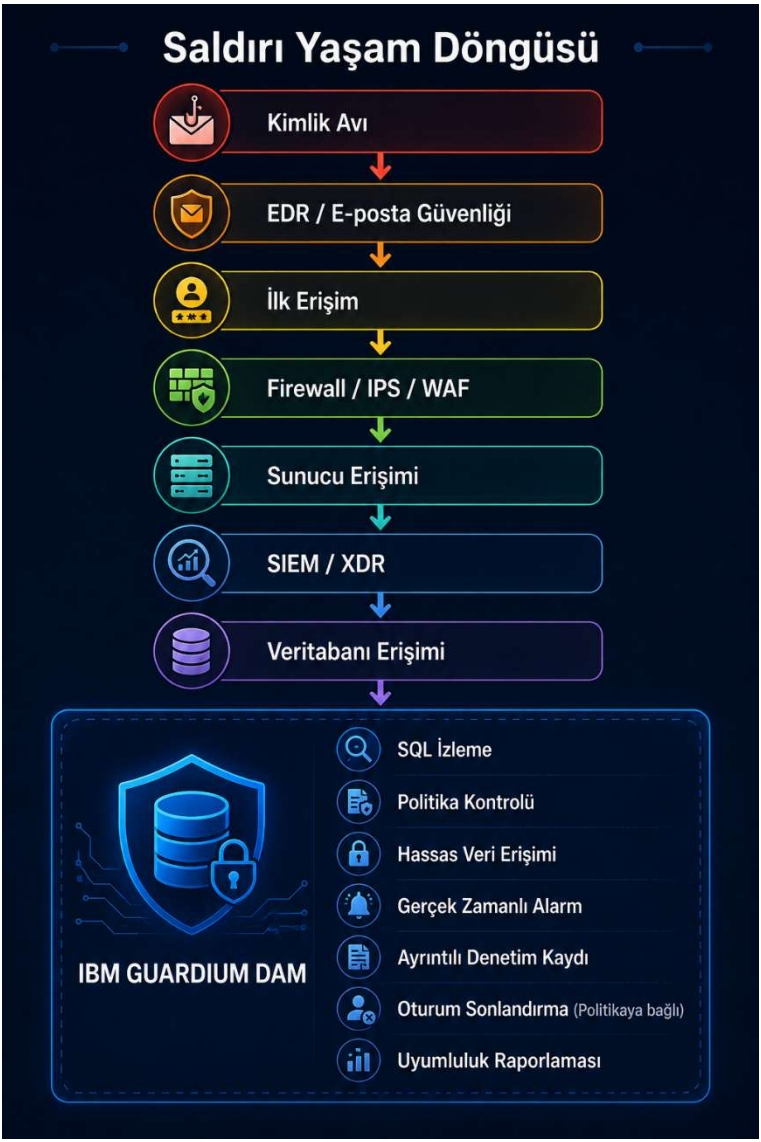
3.7 Ortak Nokta Nedir?

İncelenen olayların teknik detayları farklı olsa da ortak özellikleri dikkat çekicidir.

Bu tablo, güvenliğin yalnızca erişimi engellemekten ibaret olmadığını; erişim gerçekleştikten sonra da **kim, ne zaman, hangi veriye, hangi yöntemle erişti** sorularının cevaplanmasının kritik olduğunu göstermektedir.

3.8 IBM Guardium Bu Zincirde Nerede Konumlanır?

Aşağıdaki diyagram, farklı güvenlik teknolojilerinin saldırı yaşam döngüsündeki rollerini özetlemektedir.



Bu görsel, IBM Guardium'un diğer güvenlik ürünlerinin yerine geçen bir çözüm olmadığını; aksine, **veritabanı katmanında eksik kalan görünürlüğü tamamlayan** bir kontrol mekanizması olduğunu göstermektedir.

Bölüm Sonu Değerlendirmesi

Gerçek dünyadaki büyük veri ihlalleri incelendiğinde ortak sonuç nettir: Saldırganlar sonunda veriye ulaşmayı hedeflemektedir. Bu nedenle yalnızca çevre güvenliğine odaklanan bir yaklaşım yeterli değildir. Veritabanı katmanında gerçekleşen işlemlerin sürekli izlenmesi, politika ihlallerinin erken tespiti ve güvenilir denetim kayıtlarının tutulması; hem güvenlik operasyonlarının etkinliğini hem de düzenleyici uyumluluğu güçlendiren temel unsurlardır.

---

4. Database Activity Monitoring (DAM) Nedir?

4.1 Veritabanı Güvenliğinin Evrimi

Kurumsal bilgi sistemlerinin ilk dönemlerinde güvenlik anlayışı büyük ölçüde **çevre güvenliği (Perimeter Security)** üzerine kuruluydu. Güvenlik duvarları, ağ segmentasyonu ve erişim kontrol listeleri sayesinde kurum ağına yetkisiz erişimlerin engellenmesi yeterli görülüyordu.

Ancak dijital dönüşüm, bulut teknolojileri ve mobil erişimin yaygınlaşmasıyla birlikte bu yaklaşımın tek başına yeterli olmadığı ortaya çıktı. Günümüzde kullanıcılar, uygulamalar ve servisler farklı ağlardan, farklı cihazlardan ve farklı coğrafyalardan aynı veritabanlarına erişebilmektedir. Bu durum, saldırı yüzeyini genişletirken güvenlik kontrollerinin de veri merkezinden doğrudan veriye doğru kaymasını zorunlu hâle getirmiştir.

Veritabanları artık yalnızca uygulamaların veri sakladığı sistemler değil; müşteri bilgileri, finansal kayıtlar, sağlık verileri, fikri mülkiyet ve kritik iş süreçlerinin merkezidir. Dolayısıyla korunması gereken temel varlık sunucular değil, **verinin kendisidir**.

4.2 Database Activity Monitoring (DAM) Kavramı

Database Activity Monitoring (DAM), veritabanı üzerinde gerçekleşen tüm erişimlerin, SQL işlemlerinin ve kullanıcı aktivitelerinin **gerçek zamanlı olarak izlenmesi, analiz edilmesi, kayıt altına alınması ve gerektiğinde politika bazlı aksiyon alınmasını sağlayan** güvenlik yaklaşımıdır.

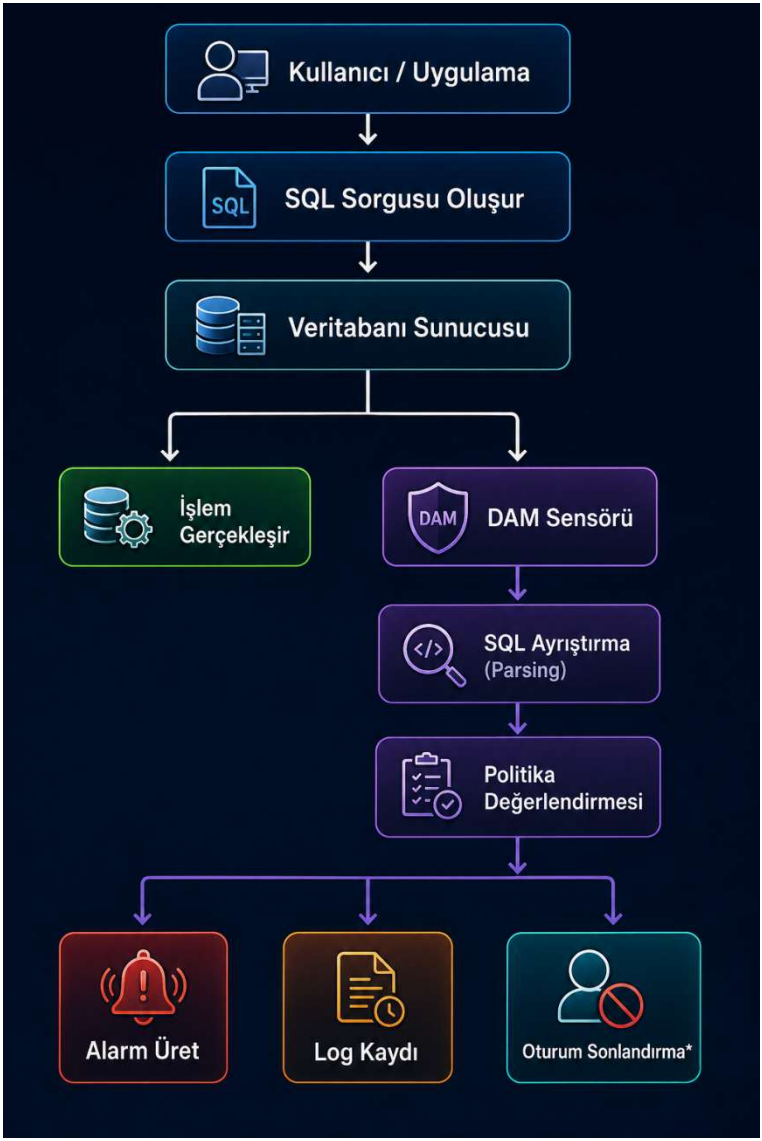
DAM çözümleri aşağıdaki temel sorulara cevap verir:

- Veritabanına kim bağlandı?
- Hangi kullanıcı hangi tabloya erişti?
- Hangi SQL sorguları çalıştırıldı?
- Hassas verilere kim erişti?
- Bu erişim normal davranışla uyumlu mu?
- Yetkisiz veya riskli bir işlem gerçekleşti mi?
- Bu olay ne zaman gerçekleşti?
- Olayın kaynağı hangi uygulama veya istemciydi?

Bu görünürlük, yalnızca güvenlik operasyonları için değil; denetim, mevzuat uyumluluğu ve adli bilişim süreçleri için de kritik öneme sahiptir.

4.3 DAM Çözümleri Nasıl Çalışır?

Genel olarak bir DAM çözümünün çalışma akışı aşağıdaki gibidir:



* Oturum sonlandırma (Kill Session) yalnızca kurumun tanımladığı politika ve desteklenen entegrasyonlar doğrultusunda uygulanır.

Bu mimari sayesinde veritabanındaki işlemler yalnızca kaydedilmez; aynı zamanda güvenlik politikalarına göre değerlendirilerek anlık aksiyon alınabilir.

4.4 DAM'in Temel Bileşenleri

Bir DAM çözümü genel olarak aşağıdaki işlevleri yerine getirir:

1. Gerçek Zamanlı İzleme

Veritabanına gelen SQL trafiğinin sürekli izlenmesi.

Örnek:

```
SELECT * FROM CUSTOMER;
```

Sorgu çalıştırıldığı anda;

- Kullanıcı,
- İstemci IP adresi,
- Uygulama,
- Veritabanı,
- Sorgu metni,
- Zaman bilgisi

Kayıt altına alınabilir.

---

2. SQL Ayrıştırma (SQL Parsing)

Bir SQL sorgusunun yalnızca metin olarak değil, anlamı ile analiz edilmesi önemlidir.

Örneğin:

```
DELETE FROM CUSTOMER;
```

İle

```
SELECT * FROM CUSTOMER;
```

Aynı şekilde değerlendirilmez.

DAM motoru;

- SELECT
- INSERT
- UPDATE
- DELETE
- ALTER
- DROP
- CREATE
- EXECUTE

Gibi komutları ayırt ederek farklı politikalar uygulayabilir.

---

3. Politika Motoru (Policy Engine)

DAM çözümlerinin en güçlü yönlerinden biri politika tabanlı çalışmalarıdır.

Örnek politika:

Maaş tablosuna DBA dışında biri erişirse alarm üret.

Başka bir örnek:

Mesai saatleri dışında PERSONEL tablosuna erişim gerçekleşirse kritik alarm oluştur.

Daha gelişmiş bir politika ise:

Son 10 dakika içinde aynı kullanıcı 500.000 satırdan fazla veri okursa SOC ekibine bildirim gönder.

Bu sayede yalnızca olaylar kaydedilmez; riskli davranışlar otomatik olarak tespit edilir.

---

4. Merkezi Kayıt ve Denetim

Birçok veritabanı kendi denetim kayıtlarını üretse de bu kayıtlar;

- Farklı formatlarda olabilir,
- Yerel sistemde tutulabilir,
- Yönetici yetkisine sahip kişiler tarafından değiştirilebilir veya silinebilir.

DAM çözümleri ise denetim kayıtlarını merkezi bir platformda toplayarak;

- Bütünlük,
- Erişilebilirlik,
- Uzun süreli saklama,
- Merkezi raporlama

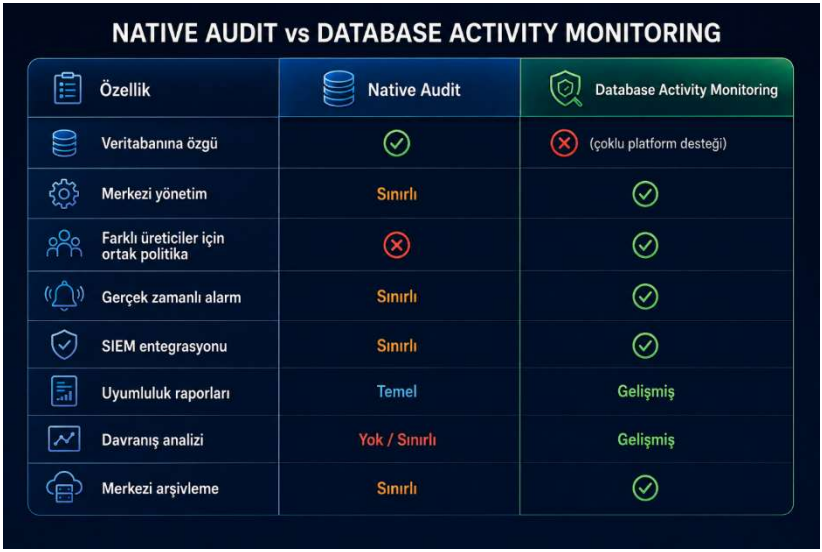
Gibi avantajlar sağlar.

4.5 Native Audit ile DAM Arasındaki Fark

Kurumlarda sıkça sorulan sorulardan biri şudur:

"Oracle Unified Auditing, SQL Server Audit veya PostgreSQL logları varken neden ayrı bir DAM çözümüne ihtiyaç duyuyoruz?"

Bu sorunun cevabı, iki yaklaşımın amaçlarının farklı olmasında yatmaktadır.



Native denetim mekanizmaları önemli bir güvenlik katmanıdır; ancak özellikle farklı veritabanı teknolojilerinin bulunduğu büyük ölçekli ortamlarda merkezi görünürlük ve tutarlı politika yönetimi sağlamakta yetersiz kalabilir.

4.6 Database Firewall ile DAM Aynı Şey midir?

Hayır.

Bu iki kavram sıklıkla karıştırılır.

Database Firewall

Temel amacı;

Engellemektir.

Örneğin;

```
DROP DATABASE;
```

Komutunu engelleyebilir.

Database Activity Monitoring

Temel amacı;

- Görmek,
- Analiz etmek,
- Raporlamak,
- Alarm üretmek,
- Gerektiğinde politika doğrultusunda aksiyon almaktır.

Modern veri güvenliği mimarilerinde bu iki yaklaşım birbirini tamamlayabilir.

4.7 DAM'in Sağladığı Temel Kazanımlar

Bir DAM çözümü kurumlara aşağıdaki başlıklarda değer katar:

Güvenlik

- Yetkisiz veri erişimlerinin görünür hâle gelmesi
- İç tehditlerin tespiti
- Ayrıcalıklı kullanıcıların izlenmesi
- Hassas veri erişimlerinin denetlenmesi

Operasyon

- Merkezi raporlama
- Standart politika yönetimi
- Farklı veritabanlarının tek platformdan izlenmesi

Denetim

- Değiştirilemez denetim kayıtları
- Kanıt niteliğinde loglar
- Uyumluluk raporları
- Denetim hazırlık süresinin kısalması

Olay Müdahalesi

- Gerçek zamanlı alarm
- SIEM entegrasyonu
- Olay geçmişinin ayrıntılı incelenmesi
- Adli bilişim süreçlerinin desteklenmesi

4.8 IBM Guardium'un DAM Yaklaşımındaki Konumu

IBM Guardium, klasik DAM yaklaşımını daha geniş bir veri güvenliği platformuna dönüştürmektedir. Temel yetenekleri arasında:

- Gerçek zamanlı veritabanı aktivite izleme
- Ayrıcalıklı kullanıcı denetimi
- Hassas veri keşfi ve sınıflandırması
- Güvenlik açığı değerlendirmesi (Vulnerability Assessment)
- Uyumluluk raporlaması
- Politika tabanlı uyarılar
- Merkezi denetim kayıt yönetimi
- SIEM ve SOAR entegrasyonları
- Hibrit ve çoklu bulut veritabanı desteği

Yer alır.

Bu yaklaşım, DAM'i yalnızca bir log toplama çözümü olmaktan çıkarıp kurumun veri güvenliği stratejisinin önemli bir bileşeni hâline getirir.

Bölüm Sonu Değerlendirmesi

Database Activity Monitoring, modern veri güvenliğinde yalnızca "veritabanı loglarını toplamak" anlamına gelmez. Asıl değeri; veritabanı üzerinde gerçekleşen işlemleri bağlamıyla birlikte yorumlayabilmesi, riskli davranışları erken aşamada görünür kılması ve güvenlik ile denetim ekiplerine güvenilir kanıtlar sunabilmesidir.

IBM Guardium, bu yaklaşımı gelişmiş politika motoru, merkezi yönetim, kapsamlı raporlama ve geniş platform desteğiyle bir üst seviyeye taşıyarak kurumların hem güvenlik operasyonlarını hem de regülasyon uyumluluğunu güçlendirmeyi hedefler.

---

5. IBM Guardium Mimarisi ve Temel Bileşenleri

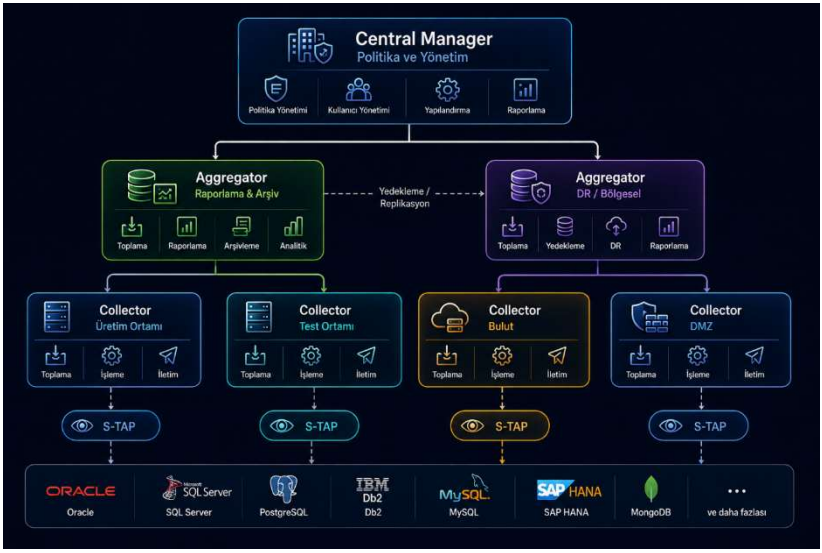
5.1 IBM Guardium Mimarisine Genel Bakış

IBM Guardium, yalnızca veritabanı aktivitelerini izleyen bir yazılım değildir. Kurumsal ölçekte binlerce veritabanını, yüzlerce uygulamayı ve farklı coğrafyalara yayılmış veri merkezlerini merkezi olarak yönetebilen ölçeklenebilir bir platformdur.

Mimarinin temel hedefleri şunlardır:

- Veritabanı aktivitelerini gerçek zamanlı izlemek
- Performans üzerinde minimum etki oluşturmak
- Merkezi politika yönetimi sağlamak
- Denetim kayıtlarını güvenli biçimde saklamak
- Alarm üretmek ve olay yönetimini desteklemek
- Uyumluluk raporlarını otomatik oluşturmak
- Büyük ölçekli yapılarda yatay büyümeyi desteklemek

Aşağıdaki şema, tipik bir Guardium dağıtımını göstermektedir.



Bu mimari sayesinde farklı veritabanları tek bir güvenlik ve denetim platformu altında yönetilebilir.

5.2 Collector

Collector, IBM Guardium mimarisinin temel bileşenidir.

S-TAP ajanlarından veya desteklenen diğer veri toplama yöntemlerinden gelen veritabanı trafiğini alır, analiz eder ve politika motorundan geçirir.

Başlıca görevleri:

- SQL trafiğini toplamak
- SQL ayrıştırma (Parsing)
- Politika değerlendirmesi
- Gerçek zamanlı alarm üretimi
- Full SQL kayıtlarının tutulması

- Yerel raporların oluşturulması
- Verinin Aggregator'a aktarılması
- Arşivleme işlemlerini yönetmek

Collector, Guardium'un "karar verme" katmanıdır. Bir SQL sorgusunun yalnızca kaydedilip kaydedilmeyeceğine değil; alarm üretimi, raporlama veya belirli politikalara göre aksiyon alınmasına da bu katmanda karar verilir.

Tasarım Notu: Üretim ortamlarında Collector'ların kapasitesi; veritabanı sayısı, saniyedeki SQL hacmi, Full SQL Logging gereksinimi ve saklama süresine göre planlanmalıdır. Yanlış boyutlandırılmış Collector'lar performans sorunlarına ve raporlama gecikmelerine neden olabilir.

5.3 Aggregator

Aggregator, çok sayıda Collector'dan gelen veriyi merkezi olarak toplar ve kurum genelinde raporlama ile uzun süreli saklama işlevini üstlenir.

Başlıca görevleri:

- Collector'lardan veri almak
- Merkezi raporlama
- Kurumsal denetim raporları
- Uzun süreli veri saklama
- Arşiv yönetimi
- Uyumluluk raporları
- Trend analizleri
- Adli inceleme süreçlerine destek

Örneğin, farklı veri merkezlerinde çalışan 20 Collector bulunduğunu düşünelim. Her bir Collector kendi ortamını izler; ancak denetçi "Son 6 ay içinde kredi kartı tablolarına kim erişti?" sorusunu tek bir noktadan yanıtlamak ister. Aggregator bu merkezi görünürlüğü sağlar.

En İyi Uygulama: Büyük yapılarda günlük raporlar ve denetim sorguları doğrudan Collector yerine Aggregator üzerinden çalıştırılarak operasyonel yük dengelenebilir.

5.4 Central Manager (CM)

Collector ve Aggregator'ların ayrı ayrı yönetilmesi, büyük ölçekli ortamlarda ciddi operasyonel zorluklar doğurur. Central Manager bu ihtiyacı karşılamak için geliştirilmiştir.

Başlıca görevleri:

- Merkezi politika dağıtımı
- Appliance yönetimi
- Lisans yönetimi
- Yazılım güncellemelerinin koordinasyonu
- Konfigürasyon standardizasyonu
- Sağlık (Health) durumunun izlenmesi
- Envanter yönetimi

Örneğin, "Mesai saatleri dışında PERSONEL_MAAS tablosuna erişildiğinde kritik alarm üret" politikasının onlarca Collector'a tek tek tanımlanması yerine CM üzerinden merkezi olarak dağıtılması hem zaman kazandırır hem de yapılandırma tutarlılığını artırır.

5.5 S-TAP (Software TAP)

S-TAP, IBM Guardium'un veritabanı sunucularına kurulan hafif ajanıdır. Veritabanına ulaşan SQL trafiğini Collector'a iletir.

S-TAP'ın başlıca özellikleri:

- SQL trafiğini yakalama
- Kullanıcı bilgisi toplama
- İstemci IP adresi ve uygulama bilgisini ilişkilendirme
- Şifrelenmiş bağlantılarla çalışabilme (desteklenen senaryolarda)
- Düşük kaynak tüketimi
- Geniş veritabanı desteği

Neden S-TAP? Birçok ortamda yalnızca veritabanı günlüklerini okumak yeterli değildir. S-TAP, SQL isteğini uygulama ve istemci bağlamıyla birlikte görebildiği için olayların analizinde daha zengin veri sağlayabilir.

5.6 GIM (Guardium Installation Manager)

Büyük ölçekli kurumlarda yüzlerce hatta binlerce S-TAP ajanını tek tek yönetmek pratik değildir.

GIM bu süreci merkezi hâle getirir.

Başlıca yetenekleri:

- Toplu ajan kurulumu
- Merkezi ajan güncelleme
- Konfigürasyon dağıtımı
- Versiyon takibi

- Ajan durumunun izlenmesi

Örneğin 500 veritabanı sunucusunun bulunduğu bir ortamda yeni bir S-TAP sürümüne geçiş, GIM sayesinde planlı ve merkezi olarak gerçekleştirilebilir.

5.7 Policy Engine

Policy Engine, IBM Guardium'un en kritik bileşenlerinden biridir. Toplanan SQL aktivitelerini tanımlanan kurallara göre değerlendirir.

Bir politika aşağıdaki kriterlerden biri veya birkaçı üzerine kurulabilir:

- Kullanıcı
- Veritabanı
- Tablo
- Şema
- SQL komutu
- Uygulama
- İstemci IP adresi
- Gün ve saat
- Veri hacmi
- Sonuç satırı sayısı
- Nesne sınıflandırması

Örnek Politikalar:

- İnsan Kaynakları tablolarına yalnızca yetkili kullanıcılar erişebilir.
- Mesai saatleri dışında finans verilerine erişim kritik alarm üretir.
- Aynı kullanıcı 100.000 satırdan fazla veri okursa olay SIEM'e gönderilir.
- DROP TABLE komutu çalıştırıldığında yüksek öncelikli olay oluşturulur.

Politika motoru sayesinde Guardium yalnızca pasif bir izleme sistemi olmaktan çıkar; risk odaklı ve bağlamsal kararlar alabilen bir denetim platformuna dönüşür.

5.8 Inspection Engine

Inspection Engine, SQL ifadelerini ayrıştırarak içeriğini analiz eder ve politika motoruna anlamlı bilgiler sağlar.

Bu katmanda:

- SQL komut türü belirlenir.
- Hedef tablo ve şema tespit edilir.
- Hassas veri nesneleri ile eşleştirme yapılabilir.
- Politika koşulları değerlendirilmek üzere hazırlanır.

Bu sayede basit bir metin kaydı yerine, olayın güvenlik açısından anlamı ortaya çıkar.

5.9 Full SQL Logging

Kurumlar çoğu zaman yalnızca "kim bağlandı?" sorusunun değil, "tam olarak hangi SQL çalıştırıldı?" sorusunun da yanıtını ister.

Full SQL Logging özelliği ile:

- SQL metni
- Parametreler (desteklenen senaryolarda)
- Çalıştırma zamanı
- Kullanıcı
- Uygulama
- İstemci IP bilgisi

Kayıt altına alınabilir.

Dikkat Edilmesi Gereken Nokta: Full SQL Logging, depolama alanı ve performans planlaması gerektirir. Özellikle yüksek hacimli OLTP sistemlerinde hangi veritabanları ve hangi politikalar için etkinleştirileceği dikkatle belirlenmelidir.

5.10 Archive ve Export

Guardium ortamlarında denetim kayıtlarının yaşam döngüsü de en az toplanması kadar önemlidir.

Tipik süreç şu şekildedir:

Doğru yapılandırılmış bir arşivleme stratejisi;

- Yasal saklama gereksinimlerini karşılar,
- Collector disk kullanımını dengeler,

- Eski verilere gerektiğinde erişilebilmesini sağlar.

Gerçek projelerde arşivleme, dışa aktarma (export) ve temizleme (purge) süreçlerinin bir bütün olarak tasarlanması gerekir. Yanlış zamanlama veya eksik doğrulama, denetim sırasında ihtiyaç duyulan kayıtların erişilemez hâle gelmesine neden olabilir. Bu nedenle arşiv bütünlüğünün düzenli olarak test edilmesi ve geri yükleme senaryolarının doğrulanması önerilir.

Bölüm Sonu Değerlendirmesi

IBM Guardium mimarisi; Collector, Aggregator, Central Manager ve S-TAP gibi bileşenlerin birlikte çalışmasıyla yalnızca SQL trafiğini izleyen bir yapı değil, kurumsal ölçekte veri güvenliği ve denetim süreçlerini destekleyen bütünleşik bir platform sunar. Doğru boyutlandırma, merkezi politika yönetimi ve planlı arşiv stratejisi, çözümden maksimum faydanın elde edilmesinde kritik rol oynar.

---

6. Gerçek Zamanlı SQL İzleme ve Politika Yönetimi

6.1 Log Toplamak ile Güvenlik Sağlamak Aynı Şey Değildir

Birçok kurum, veritabanı güvenliğini yalnızca log toplamak olarak değerlendirme eğilimindedir. Oysa milyonlarca SQL kaydının tutulması, tek başına güvenliği artırmaz. Asıl değer; bu kayıtların **bağlamıyla birlikte analiz edilmesi**, riskli davranışların ayırt edilmesi ve güvenlik ekiplerinin gerçekten müdahale etmesi gereken olayların öne çıkarılmasıdır.

Basit bir örnek düşünelim:

```
SELECT *
FROM CUSTOMER;
```

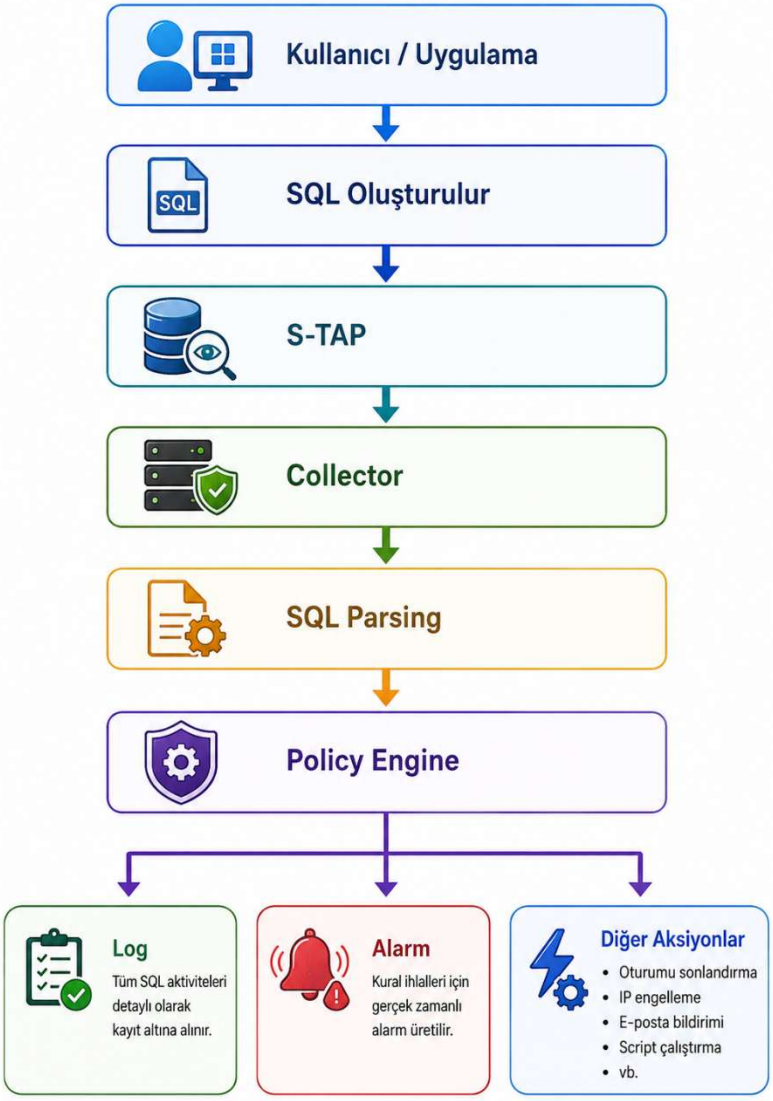
Bu sorgu tek başına zararlı değildir. Ancak aşağıdaki senaryolarda risk seviyesi değişir:

- Sorgu, normalde bu tabloya erişmeyen bir kullanıcı tarafından çalıştırılıyorsa,
- Mesai saatleri dışında gerçekleştiriliyorsa,
- Beklenenden çok daha fazla satır döndürüyorsa,
- Aynı kullanıcı kısa süre içinde benzer sorguları yüzlerce kez çalıştırıyorsa,
- Sonuçlar uygulama yerine doğrudan istemci oturumuna dönüyorsa.

Dolayısıyla aynı SQL ifadesi, bağlama göre düşük veya yüksek risk taşıyabilir. Politika tasarımının temel amacı da bu bağlamı değerlendirmektir.

6.2 SQL Yaşam Döngüsü

IBM Guardium, bir SQL isteğini yalnızca kaydetmekle kalmaz; onu çok aşamalı bir değerlendirme sürecinden geçirir.



Bu yaklaşım sayesinde her SQL ifadesi, önceden tanımlanmış güvenlik politikalarına göre değerlendirilir.

6.3 SQL Parsing Neden Önemlidir?

Veritabanı denetiminde en kritik aşamalardan biri SQL ifadelerinin doğru şekilde ayrıştırılmasıdır.

Örneğin aşağıdaki iki sorgu görünüşte benzerdir:

```
SELECT *
FROM EMPLOYEE;
```

```
SELECT *
FROM CREDIT_CARD;
```

Teknik olarak ikisi de SELECT komutudur. Ancak güvenlik açısından etkileri tamamen farklı olabilir.

İkinci sorgu, ödeme kartı verilerini içerdiği için PCI DSS kapsamına girebilir ve daha sıkı politikalara tabi tutulmalıdır. Bu nedenle yalnızca komut türünü değil, erişilen nesnenin hassasiyetini de dikkate almak gerekir.

6.4 Politika Tasarımının Temel Prensipleri

Başarılı bir Guardium ortamında politika sayısının fazla olması, güvenliğin yüksek olduğu anlamına gelmez.

Aksine, gereğinden fazla ve çakışan kurallar:

- Performans yükünü artırabilir,
- Alarm yorgunluğuna (Alert Fatigue) neden olabilir,
- Gerçek olayların gözden kaçmasına yol açabilir.

İyi bir politika tasarımı aşağıdaki ilkeleri benimser:

- Risk odaklı olmalıdır.
- Gereksiz tekrar içermemelidir.
- Yönetilebilir sayıda kural içermelidir.
- Kurumun iş süreçleriyle uyumlu olmalıdır.
- Düzenli olarak gözden geçirilmelidir.

6.5 Rule Set Yaklaşımı

Büyük ortamlarda tüm kuralları tek bir politika altında toplamak yerine mantıksal gruplara ayırmak daha sağlıklıdır.

Örnek bir yapı:

Bu yapı hem okunabilirliği artırır hem de bakım süreçlerini kolaylaştırır.

6.6 Alarm Üretirken Önceliklendirme

Her olay için aynı önemde alarm üretmek, SOC ekiplerinin iş yükünü gereksiz yere artırabilir.

Örnek bir sınıflandırma:

Bu yaklaşım sayesinde güvenlik ekipleri gerçekten müdahale edilmesi gereken olaylara odaklanabilir.

6.7 "Continue to Next" Kullanımı

Guardium'da bir kural eşleştiğinde, sonraki kuralların değerlendirilip değerlendirilmeyeceği tasarım açısından önemlidir.

Yanlış Kullanım Senaryosu:

Her kuralın sonunda "Continue to Next" seçeneğinin etkin bırakılması.

Sonuç:

- Aynı SQL için birden fazla alarm üretilebilir.
- Tek bir olay birçok farklı kural tarafından raporlanabilir.
- Alarm sayısı gereksiz şekilde artabilir.
- Analiz süresi uzayabilir.

Doğru Yaklaşım:

- Kurallar öncelik sırasına göre düzenlenmelidir.
- Gerektiğinde değerlendirme sonlandırılmalıdır.
- Bir olayın yalnızca ilgili politika kapsamında işlenmesi hedeflenmelidir.

Not: Gerçek projelerde gereksiz "Continue to Next" kullanımı, aynı olayın farklı kurallar tarafından tekrar tekrar değerlendirilmesine neden olabilir. Bu durum hem alarm hacmini artırabilir hem de politika bakımını zorlaştırabilir. Tasarım sırasında her kuralın akıştaki rolü dikkatle değerlendirilmelidir.

6.8 False Positive (Yanlış Pozitif) Yönetimi

Bir güvenlik çözümünün başarısı yalnızca kaç olay yakaladığıyla değil, ürettiği alarmların ne kadar anlamlı olduğuyla ölçülür.

Yanlış pozitifleri azaltmak için:

- Servis hesaplarını doğru sınıflandırın.
- Batch işlemlerini ayrı değerlendirin.
- Yedekleme süreçlerini hariç tutun.
- ETL kullanıcılarını tanımlayın.
- Bakım pencerelerini dikkate alın.

- Uygulama hesaplarını gruplandırın.

Bu sayede güvenlik ekipleri gereksiz alarmlarla vakit kaybetmez.

6.9 Performans ve Güvenlik Dengesi

Her SQL ifadesini aynı ayrıntıda incelemek her zaman gerekli değildir.

Örneğin:

- Kritik finans veritabanları için daha ayrıntılı denetim uygulanabilir.
- Test ortamlarında daha hafif politikalar tercih edilebilir.
- Full SQL Logging yalnızca belirli sistemlerde etkinleştirilebilir.

Bu yaklaşım hem performansı korur hem de kritik sistemlerde gerekli görünürlüğü sağlar.

6.10 Gerçek Hayattan Bir Senaryo

Bir kurumda İnsan Kaynakları veritabanında aşağıdaki politika tanımlanmıştır:

"PERSONEL_MAAS tablosuna yalnızca İK uygulaması ve yetkili İK yöneticileri erişebilir."

Bir gece saat 23:47'de aşağıdaki olay gerçekleşir:

- Kullanıcı: DBA_ADMIN
- İstemci: SQL Developer
- Kaynak IP: Yönetim ağı

- SQL: SELECT * FROM PERSONEL_MAAS

Bu olay tek başına kötü niyetli bir davranış olduğunu göstermez. Belki planlı bir bakım çalışması yapılmaktadır. Ancak politika sayesinde:

- Olay gerçek zamanlı olarak kaydedilir.
- Güvenlik ekibine uyarı gönderilir.
- Denetim izi korunur.
- Gerekirse ilgili ekipten açıklama istenebilir.

Bu örnek, DAM çözümlerinin temel amacını özetler: **Her erişimi engellemek değil, kritik erişimleri görünür ve denetlenebilir hâle getirmek.**

6.11 Politika Yönetiminde En İyi Uygulamalar

Başarılı bir Guardium ortamı için öneriler:

1. Önce kritik verileri belirleyin.
2. Kullanıcıları risk seviyesine göre sınıflandırın.
3. Politika sayısını mümkün olduğunca sade tutun.
4. Alarm seviyelerini standartlaştırın.
5. Düzenli politika gözden geçirme süreçleri oluşturun.
6. Test ve üretim ortamlarını ayrı değerlendirin.
7. Arşivleme ve raporlama stratejilerini birlikte planlayın.
8. Politikaların iş birimleriyle uyumunu doğrulayın.
9. SIEM entegrasyonunda olay zenginleştirmesi yapın.
10. Politika değişikliklerini değişiklik yönetimi sürecine dahil edin.

Bölüm Sonu Değerlendirmesi

IBM Guardium'un gerçek gücü, yalnızca SQL trafiğini kaydetmesinden değil; bu trafiği kurumun risk profiline göre değerlendirebilmesinden kaynaklanır. Başarılı bir politika tasarımı; doğru önceliklendirme, düşük yanlış pozitif oranı ve sürdürülebilir bakım süreçleri üzerine kurulmalıdır. Böylece güvenlik ekipleri milyonlarca kayıt arasında kaybolmak yerine gerçekten önemli olaylara odaklanabilir.

---

7. İç Tehditler ve Ayrıcalıklı Kullanıcı Denetimi

7.1 İç Tehdit (Insider Threat) Nedir?

Siber güvenlik denildiğinde çoğu zaman akla dış saldırganlar gelir. Ancak kurumların karşılaştığı risklerin önemli bir bölümü, **kurum içinde çalışan veya kurum sistemlerine yetkili erişimi bulunan kullanıcıların** faaliyetlerinden kaynaklanabilir.

İç tehdit kavramı yalnızca kötü niyetli çalışanları kapsamaz. Aşağıdaki kullanıcı grupları da belirli koşullarda iç tehdit kapsamına girebilir:

- Veritabanı yöneticileri (DBA)
- Sistem yöneticileri
- Uygulama yöneticileri
- Dış destek ekipleri
- Danışman firmalar
- Servis hesapları
- Otomasyon sistemleri
- Ele geçirilmiş kullanıcı hesapları

Dolayısıyla "iç tehdit", kişilerin niyetinden çok **erişim yetkisi ve oluşturabileceği risk** ile ilgilidir.

7.2 Ayrıcalıklı Hesaplar Neden Kritik?

Kurumsal ortamlarda bazı hesaplar diğerlerinden çok daha geniş yetkilere sahiptir.

Örneğin:

- SYS
- SYSTEM
- SA
- DB2INST1
- POSTGRES
- ROOT
- APP_ADMIN

Bu hesaplar;

- Kullanıcı oluşturabilir,
- Tablo silebilir,
- Yetki verebilir,
- Hassas verilere erişebilir,
- Logları değiştirebilir,
- Güvenlik ayarlarını güncelleyebilir.

Dolayısıyla bu hesapların faaliyetlerinin kayıt altına alınması yalnızca güvenlik açısından değil, yönetişim ve denetim açısından da kritik öneme sahiptir.

Önemli olan nokta şudur:

Ayrıcalıklı kullanıcıların izlenmesi, onlara duyulan güvensizlik anlamına gelmez. Bu yaklaşım; hesap verebilirliği, şeffaflığı ve kurumsal güvenliği güçlendiren bir kontrol mekanizmasıdır.

7.3 İç Tehdit Türleri

1. Kötü Niyetli Kullanıcı

Örnek:

İşten ayrılmadan önce müşteri listesini kopyalamak isteyen bir çalışan.

Olası belirtiler:

- Olağan dışı saatlerde erişim
- Büyük hacimli sorgular
- Export işlemleri
- USB veya harici aktarım hazırlıkları (ilgili çözümlerle birlikte değerlendirildiğinde)

---

2. İhmalkâr Kullanıcı

Örnek:

Yanlışlıkla aşağıdaki komutu çalıştıran bir DBA:

```
DELETE FROM CUSTOMER;
```

Kötü niyet yoktur; ancak sonuçları kritik olabilir.

---

3. Ele Geçirilmiş Hesap

Saldırganın bir DBA hesabını ele geçirdiğini düşünelim.

Veritabanına bağlanırken görülen bilgiler:

```
Kullanıcı : DBA_ADMIN
IP        : 10.10.5.20
Araç      : SQL Developer
```

Teknik olarak her şey normal görünmektedir.

Ancak aşağıdaki davranışlar dikkat çekebilir:

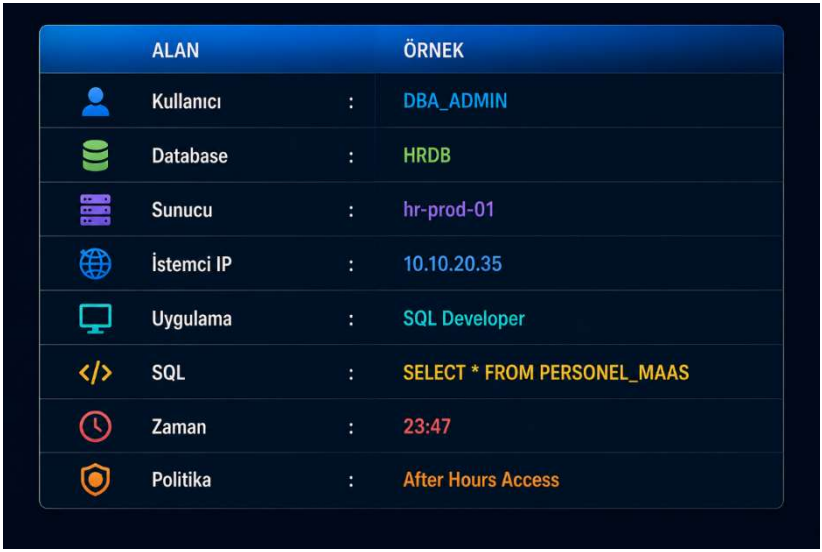
- Mesai dışı erişim
- Daha önce hiç erişilmeyen tabloların okunması
- Yoğun SELECT sorguları
- Yetki değişiklikleri
- Yeni kullanıcı oluşturulması

Bu nedenle **davranış analizi**, kimlik doğrulamadan sonra da önemini korur.

7.4 Ayrıcalıklı Kullanıcıların Denetlenmesi

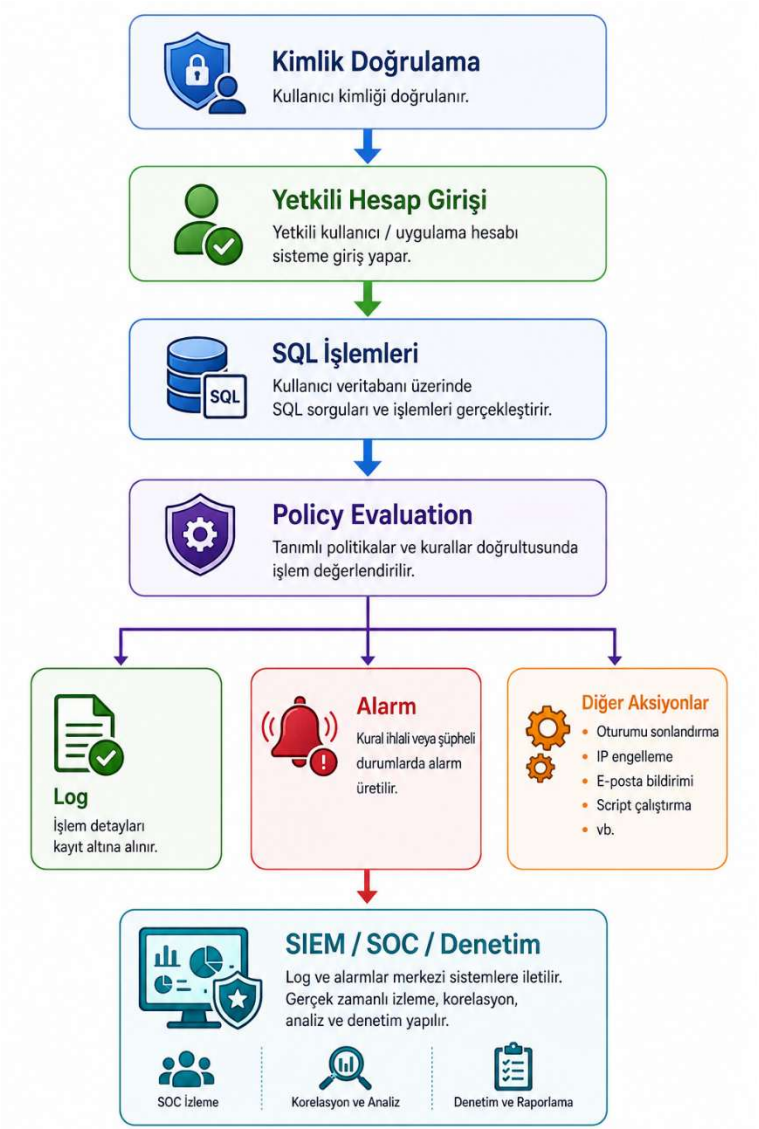
IBM Guardium, ayrıcalıklı kullanıcı faaliyetlerini ayrıntılı şekilde izleyebilir.

Örneğin aşağıdaki bilgiler kaydedilebilir:



Bu bilgiler, olayın teknik bağlamını anlamaya yardımcı olur ve gerektiğinde denetim kanıtı olarak kullanılabilir.

7.5 Ayrıcalıklı Oturumların Yaşam Döngüsü



Bu akış, bir oturumun yalnızca başlangıcının değil, tüm yaşam döngüsünün izlenebilmesini sağlar.

7.6 Vendor ve Dış Destek Erişimleri

Birçok kurum, dış destek ekiplerine belirli zamanlarda veritabanı erişimi vermektedir.

Örneğin:

- ERP üreticisi
- Bankacılık uygulaması sağlayıcısı
- Danışman firma
- Destek mühendisi

Bu erişimler genellikle geçici olsa da yüksek yetkiler içerebilir.

İyi uygulamalar şunlardır:

- Erişim süresinin sınırlandırılması
- İş emri ile ilişkilendirme
- Faaliyetlerin kayıt altına alınması
- Kritik işlemler için alarm üretilmesi
- Oturum sonrasında raporlama

7.7 Break-Glass (Acil Durum) Hesapları

Bazı kurumlarda olağanüstü durumlar için kullanılan ortak veya acil durum hesapları bulunur.

Örneğin:

EMERGENCY_ADMIN

Bu hesaplar;

- Sistem arızalarında,
- Kritik bakım çalışmalarında,
- Felaket kurtarma süreçlerinde

Kullanılabilir.

Ancak bu hesapların kullanımı normal kullanıcı hesaplarından daha sıkı şekilde izlenmelidir.

Önerilen kontroller:

- Kullanım nedeni kayıt altına alınmalı.
- Erişim süresi sınırlandırılmalı.
- Çok faktörlü kimlik doğrulama uygulanmalı.
- Tüm SQL aktiviteleri ayrıntılı olarak denetlenmeli.
- Kullanım sonrasında gözden geçirme yapılmalı.

7.8 Davranış Temelli Yaklaşım

Her SELECT sorgusu şüpheli değildir.

Önemli olan davranışın bağlamıdır.

Örnek:

Bir İK yöneticisinin:

SELECT PERSONEL

Çalıştırması beklenen davranıştır.

Aynı sorgunun;

- Gece 03:00'te,
- Farklı bir ülkeden,
- Daha önce hiç kullanılmamış bir istemciden,

- Milyonlarca satır döndürecek şekilde

Çalıştırılması ise inceleme gerektiren bir durum olabilir.

Bu nedenle modern güvenlik yaklaşımları yalnızca "kim?" sorusunu değil, "nasıl?", "ne zaman?" ve "hangi kapsamda?" sorularını da değerlendirir.

7.9 Gerçek Hayattan Senaryo

Bir finans kuruluşunda gece saatlerinde aşağıdaki olay gerçekleşiyor:

```
Kullanıcı        : APP_SUPPORT
Kaynak IP        : 10.20.15.8
Uygulama         : SQL*Plus
Saat             : 02:18
İşlem            : SELECT
Tablo            : CREDIT_CARD
Okunan Kayıt     : 2.350.000
```

İlk bakışta kullanıcı yetkilidir.

Ancak güvenlik ekibi şu soruları sorar:

- Bu kullanıcı normalde bu tabloya erişiyor mu?
- Neden uygulama yerine SQL*Plus kullanıldı?
- İşlem planlı bir bakım kapsamında mı?
- Bu erişim değişiklik yönetimi kaydıyla ilişkili mi?
- Sonuçlar dışarı aktarıldı mı?

Bu örnek, görünürde "geçerli" olan bir işlemin bile bağlam içinde değerlendirilmesi gerektiğini gösterir.

7.10 Denetçilerin Sorduğu Sorular

Bir dış denetim sırasında aşağıdaki sorular sıkça gündeme gelir:

- Son bir yılda maaş verilerine kim erişti?
- DBA'lar mesai dışında hangi işlemleri yaptı?
- Yetkili kullanıcılar hangi DDL komutlarını çalıştırdı?
- Kritik tablolar üzerinde kim değişiklik yaptı?
- Vendor erişimleri kayıt altına alındı mı?
- Acil durum hesapları ne zaman kullanıldı?
- Hassas verilere erişimler raporlanabiliyor mu?

Bu sorulara hızlı ve doğrulanabilir yanıt verebilmek, yalnızca denetim sürecini kolaylaştırmaz; aynı zamanda kurumun yönetişim olgunluğunu da gösterir.

7.11 En İyi Uygulamalar

Ayrıcalıklı kullanıcı yönetiminde önerilen yaklaşım:

1. Ayrıcalıklı hesapları envanterleyin.
2. İş rollerine göre sınıflandırın.
3. Kritik tabloları belirleyin.
4. Risk bazlı politikalar oluşturun.
5. Mesai dışı erişimleri izleyin.
6. Vendor hesaplarını ayrı yönetin.

7. Acil durum hesaplarını sıkı denetleyin.
8. Düzenli erişim gözden geçirmeleri yapın.
9. SIEM ve PAM çözümleriyle entegrasyon sağlayın.
10. Denetim raporlarını periyodik olarak yönetime sunun.

Bölüm Sonu Değerlendirmesi

İç tehditler ve ayrıcalıklı kullanıcı faaliyetleri, modern veri güvenliğinin en kritik başlıklarından biridir. Bu risklerin yönetimi, kişilere duyulan güveni sorgulamak değil; kurumsal süreçlerin şeffaf, izlenebilir ve denetlenebilir olmasını sağlamaktır. IBM Guardium gibi DAM çözümleri, veritabanı üzerindeki faaliyetlere görünürlük kazandırarak güvenlik operasyonları ile denetim ekipleri arasında ortak bir gerçeklik zemini oluşturur.

---

8. Hassas Veri Keşfi ve Sınıflandırma (Data Discovery & Classification)

8.1 Kurumlar Gerçekten Neyi Koruduklarını Biliyor mu?

Bir kurumun veri güvenliği olgunluğunu değerlendirirken sorulması gereken ilk soru şudur:

"Kurum hangi verilerinin hassas olduğunu gerçekten biliyor mu?"

Bu soru ilk bakışta oldukça basit görünse de, büyük ölçekli kurumlarda cevap çoğu zaman net değildir.

Örneğin yüzlerce veritabanı bulunan bir finans kuruluşunda;

- Kaç adet müşteri tablosu vardır?
- Kredi kartı bilgileri hangi veritabanlarında bulunmaktadır?
- KVKK kapsamındaki kişisel veriler hangi kolonlarda tutulmaktadır?
- Test ortamlarında üretim verisi kullanılmakta mıdır?
- Kullanılmayan eski veritabanlarında hâlâ hassas bilgiler bulunuyor mudur?

Bu soruların cevaplarını manuel olarak bulmak neredeyse imkânsızdır.

İşte bu nedenle modern veri güvenliği yaklaşımı yalnızca erişimlerin izlenmesini değil, **korunacak verinin keşfedilmesini ve sınıflandırılmasını** da kapsar.

8.2 Veri Güvenliğinde En Büyük Problem

Çoğu kurumun düşündüğü problem:

"Veriye kim erişiyor?"

Gerçekte ise ilk problem şudur:

"Hangi veri gerçekten kritik?"

Bir tablo düşünelim.

```
CUSTOMER
```

İçinde;

```
ID
NAME
PHONE
EMAIL
ADDRESS
```

Bulunuyor.

Başka bir tablo:

```
PAYROLL
```

İçinde;

```
SALARY
BONUS
IBAN
TAX_NUMBER
```

Bulunuyor.

Her iki tablo da önemlidir.

Ancak risk seviyeleri aynı değildir.

8.3 Hassas Veri Nedir?

Kuruma göre değişmekle birlikte aşağıdaki bilgiler genellikle hassas veri olarak değerlendirilir.

Kimlik Bilgileri

- T.C. Kimlik Numarası
- Pasaport
- Ehliyet

Finansal Bilgiler

- Kredi Kartı
- CVV
- IBAN
- Hesap Numarası

Sağlık Bilgileri

- Tanılar
- Laboratuvar Sonuçları
- Reçeteler
- Sağlık Geçmişi

Ticari Sırlar

- Üretim reçeteleri

- Kaynak kodları
- Ar-Ge verileri
- Müşteri fiyat listeleri

Kişisel Veriler

KVKK kapsamında;

- Ad Soyad
- Telefon
- Adres
- IP
- Lokasyon
- E-posta

Gibi bilgiler de uygun bağlamda kişisel veri olarak değerlendirilebilir.

8.4 Data Discovery Süreci

IBM Guardium Data Discovery modülü, desteklenen veritabanlarında otomatik taramalar gerçekleştirerek hassas veri içerebilecek nesneleri belirlemeye yardımcı olur.

Temel süreç şu şekildedir:

Bu süreç sayesinde binlerce tablo tek tek incelenmeden önceliklendirme yapılabilir.

8.5 Pattern Matching

Birçok hassas veri belirli desenler (pattern) kullanılarak tespit edilebilir.

Örneğin:

```
TC_NO
IDENTITY_NO
SSN
CARD_NO
IBAN
EMAIL
PHONE
```

Veya kolon içeriği üzerinden;

```
16 haneli kart numarası
IBAN formatı
Mail adresi
Telefon formatı
UUID
Pasaport numarası
```

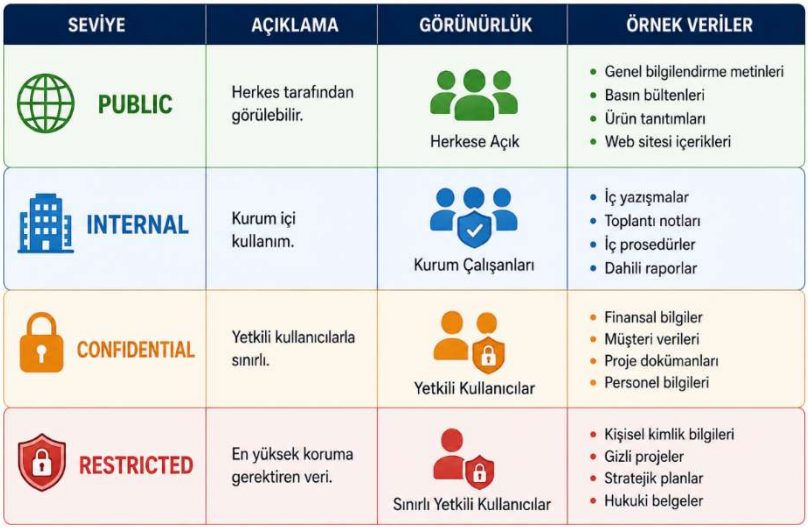
Gibi yapılar belirlenebilir.

Elbette sadece kolon adına bakmak yeterli değildir; içerik analizi ve kuruma özgü kurallar da önemlidir.

8.6 Sınıflandırma (Classification)

Keşfedilen verilerin aynı önemde değerlendirilmesi doğru değildir.

Örnek sınıflandırma:



Bu sınıflandırma daha sonra erişim politikalarının ve denetim kurallarının temelini oluşturur.

8.7 Risk Bazlı Yaklaşım

Aşağıdaki iki olay düşünelim.

Olay 1

SELECT

HR_EMPLOYEE

100 kayıt.

Olay 2

SELECT

CREDIT_CARD

5 milyon kayıt

Her ikisi de SELECT sorgusudur.

Ancak ikinci olay çok daha yüksek risk taşır.

Bu nedenle modern DAM çözümleri yalnızca SQL komutuna değil;

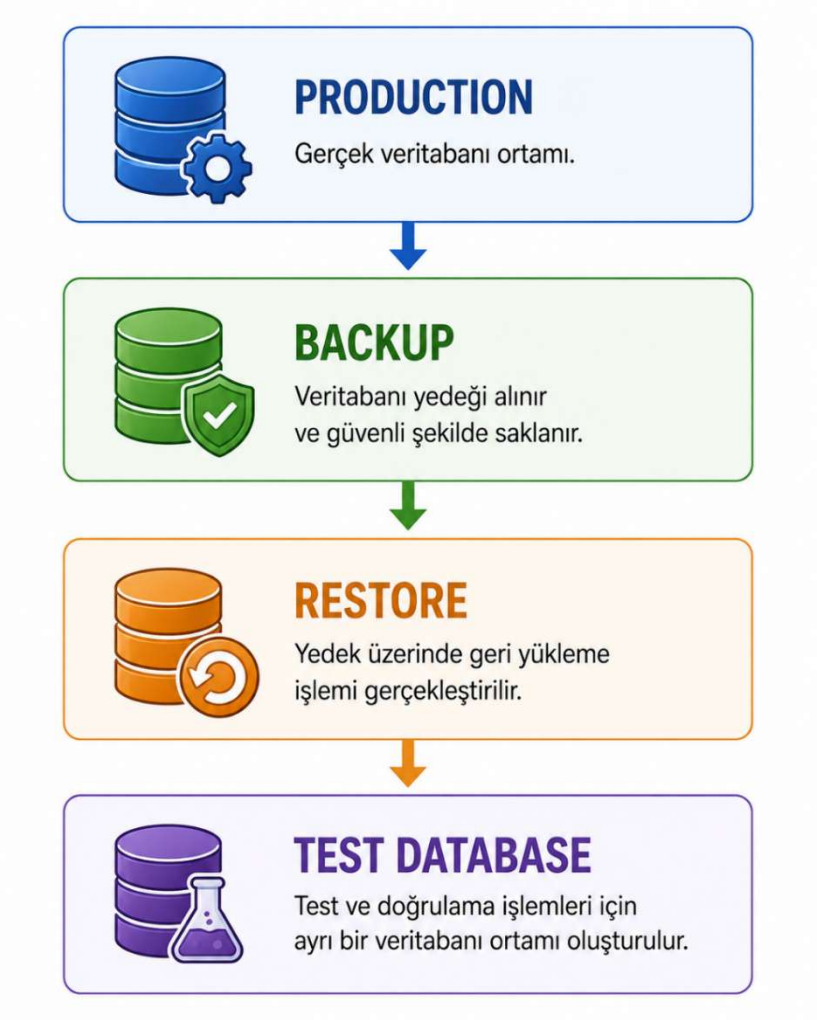
- Verinin hassasiyetine,
- Erişim hacmine,
- Kullanıcı rolüne,
- Zaman bilgisine,
- İstemci tipine

de bakarak değerlendirme yapar.

8.8 Test Ortamlarının Görünmeyen Riski

Gerçek projelerde sık karşılaşılan sorunlardan biri de üretim verilerinin test ortamlarına kopyalanmasıdır.

Örneğin;



Bu durumda;

- Gerçek müşteri bilgileri,
- Kredi kartları,
- Personel maaşları,

Test ortamına taşınmış olabilir.

Üstelik bu ortamlar çoğu zaman üretim kadar sıkı korunmaz.

Bu nedenle hassas veri keşfi yalnızca üretim sistemlerinde değil, geliştirme ve test ortamlarında da düzenli olarak yapılmalıdır.

8.9 Gerçek Hayattan Senaryo

Bir kurum, yalnızca üretim Oracle veritabanlarında kişisel veri bulunduğunu düşünmektedir.

Data Discovery çalışması sonucunda:

- 312 veritabanı taranır.
- 27 test veritabanında gerçek müşteri verileri bulunur.
- 9 eski sunucuda unutulmuş kredi kartı tabloları tespit edilir.
- Bir geliştirme ortamında yıllardır kullanılmayan personel maaş verileri keşfedilir.

Bu senaryoda sorun bir saldırı değildir. Sorun, kurumun hangi veriye sahip olduğunu tam olarak bilmemesidir.

8.10 IBM Guardium ile Veri Keşfinin Sağladığı Faydalar

Kurumlar için başlıca kazanımlar:

- Hassas verilerin merkezi olarak envanterlenmesi
- Risk bazlı politika oluşturulması
- Gereksiz veri kopyalarının tespiti
- Uyumluluk çalışmalarının hızlanması
- Denetim kapsamının doğru belirlenmesi

- Güvenlik yatırımlarının önceliklendirilmesi

8.11 En İyi Uygulamalar

- Veri keşfi tek seferlik bir çalışma olarak görülmemelidir.
- Yeni veritabanları düzenli olarak taranmalıdır.
- Veri sınıflandırması iş birimleriyle birlikte gözden geçirilmelidir.
- Test ortamlarında maskeleme veya anonimleştirme uygulanmalıdır.
- Kritik sınıflardaki verilere erişim için daha sıkı politikalar tanımlanmalıdır.
- Sınıflandırma sonuçları, DAM politikaları ve SIEM korelasyonlarıyla ilişkilendirilmelidir.

Bölüm Sonu Değerlendirmesi

Veri güvenliğinin ilk adımı, hangi verinin korunacağını bilmektir. Hassas veri keşfi ve sınıflandırma çalışmaları, yalnızca uyumluluk gerekliliklerini karşılamak için değil; kurumun güvenlik yatırımlarını doğru önceliklendirebilmesi için de kritik öneme sahiptir. IBM Guardium'un veri keşfi ve sınıflandırma yetenekleri, güvenlik ekiplerine bu görünürlüğü sağlayarak izleme ve politika süreçlerinin daha etkili hâle gelmesine katkıda bulunur.

---

9. Sürekli Denetim ve Regülasyon Uyumluluğu

9.1 Uyumluluk Bir Proje Değil, Süreçtir

Birçok kurum denetim yaklaşımını hâlâ belirli tarihlerde gerçekleştirilen faaliyetler olarak görmektedir.

Tipik bir senaryo:

Bu yaklaşım sürdürülebilir değildir.

Modern güvenlik anlayışında denetim;

- Sürekli,

- Otomatik,
- Ölçülebilir,
- İzlenebilir

Olmalıdır.

İşte bu yaklaşım **Continuous Compliance (Sürekli Uyumluluk)** olarak adlandırılır.

9.2 Continuous Compliance Nedir?

Continuous Compliance;

Güvenlik kontrollerinin yalnızca denetim öncesinde değil,

365 gün

24 saat

Çalışmasını ifade eder.

Örneğin;

Denetçi şu soruyu soruyor:

Son iki yılda maaş tablosuna kim erişti?

Eğer kurum yalnızca native loglara güveniyorsa;

- Loglar silinmiş olabilir,
- Farklı sistemlerde tutuluyor olabilir,
- Manuel rapor hazırlanması gerekebilir.

Continuous Compliance yaklaşımında ise bu bilgi standart raporlarla daha hızlı ve tutarlı şekilde sunulabilir.

9.3 Denetçilerin Beklentileri

Denetçiler çoğu zaman ürün ismi sormaz.

Onlar şu soruların cevaplarını ister.

Kim?

Veriye kim erişti?

Ne zaman?

Hangi tarihte?

Saat kaçta?

Nereden?

IP adresi

Sunucu

Uygulama

Ne yaptı?

SELECT

UPDATE

DELETE

DROP

ALTER

Yetkisi var mıydı?

Normal davranış mıydı?

Kanıtı var mı?

Log mevcut mu?

Değiştirilebilir mi?

Rapor üretilebiliyor mu?

Bu sorulara güvenilir cevap verebilmek, denetim süreçlerini önemli ölçüde kolaylaştırır.

9.4 KVKK Perspektifinden IBM Guardium

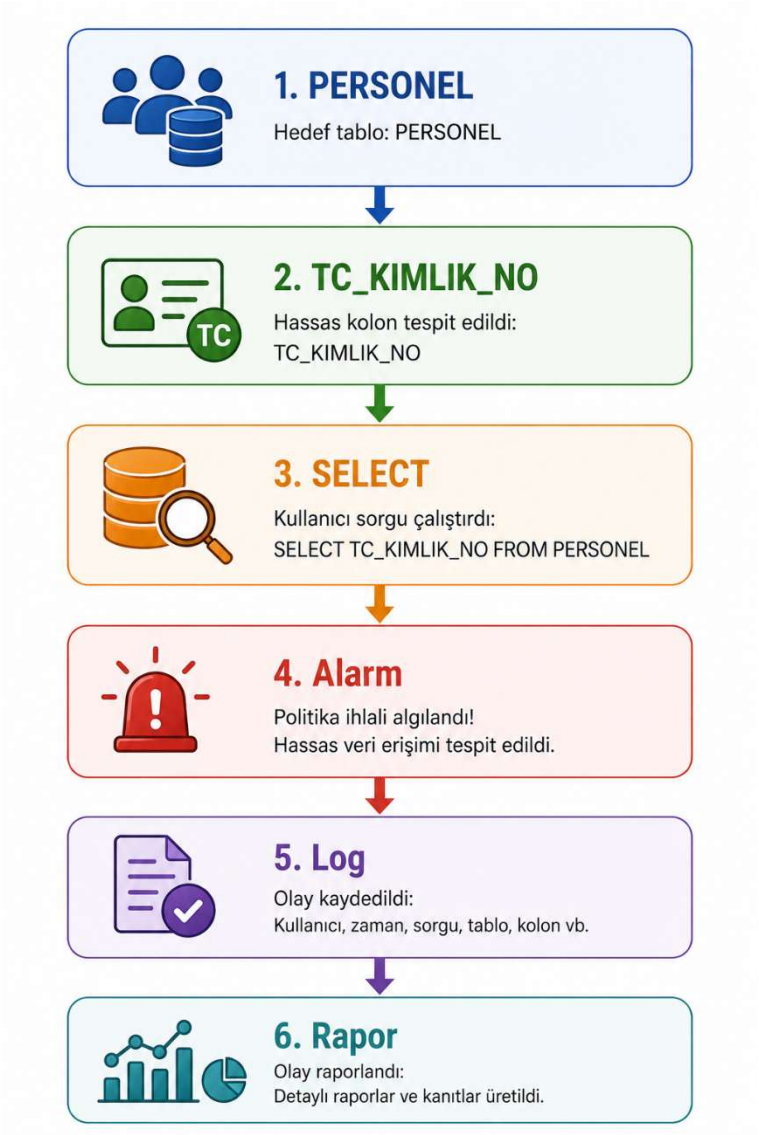
Türkiye'de kişisel verilerin korunmasına ilişkin yükümlülükler, kurumların kişisel verilerin güvenliğini sağlamasını ve uygun teknik ile idari tedbirleri almasını gerektirir.

IBM Guardium;

- Kişisel veri içeren tabloların belirlenmesine,
- Bu tablolara erişimlerin izlenmesine,
- Şüpheli erişimlerin raporlanmasına,
- Denetim kayıtlarının saklanmasına,

Katkı sağlayabilir.

Örnek senaryo:



Burada önemli olan nokta;

Guardium'un KVKK'nın tamamını karşılamadığı,

Ancak veri erişiminin izlenmesi ve kayıt altına alınması gibi teknik kontrolleri desteklediğidir.

9.5 PCI DSS 4.0 Perspektifi

PCI DSS;

Ödeme kartı bilgilerinin korunmasına yönelik uluslararası güvenlik standardıdır.

Özellikle aşağıdaki alanlarda detaylı denetim ister.

- Kim erişti?
- Yetkisi var mı?
- Log tutuluyor mu?
- Log değiştirilebiliyor mu?
- Ayrıcalıklı kullanıcılar izleniyor mu?

IBM Guardium özellikle aşağıdaki başlıklarda destek sağlayabilir:

- Kart verisi erişimlerinin izlenmesi
- Ayrıcalıklı kullanıcı faaliyetlerinin kaydı
- Denetim loglarının merkezi toplanması
- Gerçek zamanlı alarm üretimi
- Raporlama

Ancak PCI DSS uyumluluğu;

Ağ güvenliği,

Şifreleme,

Anahtar yönetimi,

Zafiyet yönetimi,

Kimlik doğrulama

gibi birçok farklı kontrolün birlikte uygulanmasını gerektirir.

9.6 ISO 27001 Perspektifi

ISO 27001;

Bir ürün standardı değil,

Bir **Bilgi Güvenliği Yönetim Sistemi (BGYS)** standardıdır.

IBM Guardium;

Özellikle aşağıdaki alanlarda destek sunabilir.

Log Yönetimi

Denetim kayıtları

Ayrıcalıklı Kullanıcı Yönetimi

Yetkili kullanıcı faaliyetlerinin izlenmesi

Olay Yönetimi

Alarm

İnceleme

Kanıt

Sürekli İzleme

Anormal erişimlerin belirlenmesi

Denetim

Hazır raporlar

9.7 NIST Cybersecurity Framework

NIST CSF;

Beş temel fonksiyon üzerine kuruludur.

FONKSİYON	GUARDIUM KATKISI
Identify	**Hassas veri keşfi ve envanter** Veritabanlarındaki hassas verileri otomatik olarak keşfeder, sınıflandırır ve envanterini çıkarır.
Protect	**Politika tabanlı erişim izleme** Tanımlı güvenlik politikaları ile kullanıcıların ve uygulamaların veri erişimlerini izler ve kontrol eder.
Detect	**Gerçek zamanlı SQL aktivite tespiti** SQL trafiğini gerçek zamanlı olarak analiz eder, şüpheli ve anormal aktiviteleri tespit eder.
Respond	**Alarm, SIEM entegrasyonu ve olay desteği** Alarm üretir, SIEM sistemlerine entegre olur ve olay yönetimi süreçlerinde destek sağlar.
Recover	**Arşiv kayıtlarıyla adli inceleme ve geri dönük analiz** Arşivlenen kayıtlar sayesinde geçmişe dönük inceleme yapılır, adli analiz ve raporlama imkanı sunar.

Bu tablo, Guardium'un NIST CSF'nin özellikle **Detect** ve **Respond** fonksiyonlarında önemli bir rol oynadığını gösterir.

9.8 DORA ve Finans Sektörü

Avrupa Birliği'nin **Digital Operational Resilience Act (DORA)** düzenlemesi, finans kuruluşlarının dijital operasyonel dayanıklılığını artırmayı amaçlar.

Veri tabanlı finansal işlemlerin yoğun olduğu ortamlarda:

- Kritik veri erişimlerinin izlenmesi,
- Olayların kayıt altına alınması,
- Güvenilir denetim izlerinin oluşturulması,

Operasyonel dayanıklılığın önemli bileşenlerindendir.

IBM Guardium, bu alanlarda kullanılabilecek teknik kontrollerden biri olarak konumlandırılabilir.

9.9 SWIFT CSP

Uluslararası ödeme sistemlerinde;

Ayrıcalıklı kullanıcıların izlenmesi,

Kritik sistem değişikliklerinin kayıt altına alınması,

Denetim izlerinin korunması

Önemlidir.

Guardium;

Özellikle ödeme sistemlerine ait veritabanlarının izlenmesi açısından değerli görünürlük sağlayabilir.

9.10 Denetim Süresinin Kısaltılması

Gerçek projelerde sık karşılaşılan durumlardan biri:

Bu süreç günler sürebilir.

Merkezi raporlama ve standart denetim çıktıları sayesinde aynı bilgi çok daha kısa sürede hazırlanabilir. Ancak bu kazanım; doğru

politika tasarımı, yeterli log saklama süresi ve düzenli raporlama süreçlerinin önceden planlanmış olmasına bağlıdır.

9.11 Gerçek Denetim Senaryosu

Bir denetçi aşağıdaki soruları yöneltiyor:

Son 12 ay içerisinde PERSONEL_MAAS tablosuna kimler erişti?

İyi yapılandırılmış bir DAM ortamında rapor şu bilgileri içerebilir:

- Kullanıcı adı
- Rol
- Tarih ve saat
- İstemci IP adresi
- Uygulama
- SQL komutu
- Politika sonucu
- Alarm durumu

Bu tür raporlar yalnızca denetimi kolaylaştırmakla kalmaz, olay incelemelerinde de güvenilir bir denetim izi sunar.

9.12 Uyumlulukta En Sık Yapılan Hatalar

Kurumlarda gözlemlenen yaygın eksiklikler:

- Logların çok kısa süre saklanması
- Tüm veritabanlarının aynı politika ile yönetilmesi
- Test ortamlarının kapsam dışında bırakılması

- Vendor erişimlerinin kayıt altına alınmaması
- Hassas veri sınıflandırmasının yapılmaması
- Alarm seviyelerinin tanımlanmaması
- Politika değişikliklerinin izlenmemesi
- Düzenli rapor üretiminin otomatikleştirilmemesi

Bölüm Sonu Değerlendirmesi

Regülasyonlara uyum, belirli bir tarihte tamamlanan bir proje değil; sürekli işletilmesi gereken bir yönetim sürecidir. IBM Guardium, veri erişimlerinin görünürlüğünü artırarak, denetim kayıtlarını merkezi olarak yöneterek ve politika ihlallerini raporlayarak bu süreci destekleyen önemli bir teknik kontrol katmanı sunar. Bununla birlikte, tam uyumluluk; süreçler, organizasyonel kontroller ve diğer güvenlik teknolojileriyle birlikte ele alınmalıdır.

---

10. IBM Guardium Best Practices ve Saha Deneyimleri

Not: Bu bölümde yer alan öneriler; IBM Guardium projelerinde yaygın olarak benimsenen mimari yaklaşımlar, üretici önerileri ve gerçek kurumsal projelerde edinilen deneyimlerin harmanlanmasıyla hazırlanmıştır. Her kurumun altyapısı, regülasyon yükümlülükleri ve risk profili farklı olduğundan, nihai tasarım bu ihtiyaçlara göre uyarlanmalıdır.

10.1 Başarılı Bir Guardium Projesi Nerede Başlar?

IBM Guardium projelerinde sık yapılan hatalardan biri, projeye doğrudan ürün kurulumu ile başlamaktır.

Oysa başarılı projeler aşağıdaki sırayı izler:

Kurulum, projenin başlangıcı değil; tasarım sürecinin bir çıktısıdır.

10.2 Collector Boyutlandırma (Sizing)

En kritik mimari karar Collector seçimidir.

Collector aşağıdaki yükleri taşır:

- SQL Parsing
- Policy Evaluation
- Alarm üretimi
- Full SQL Logging
- Archive işlemleri
- Export görevleri
- Yerel raporlama
- Sistem yönetimi

Bu nedenle yalnızca **veritabanı sayısına** bakılarak kapasite planlaması yapılmamalıdır.

Değerlendirilmesi gereken başlıca faktörler:

Guardium Performansını Etkileyen Faktörler

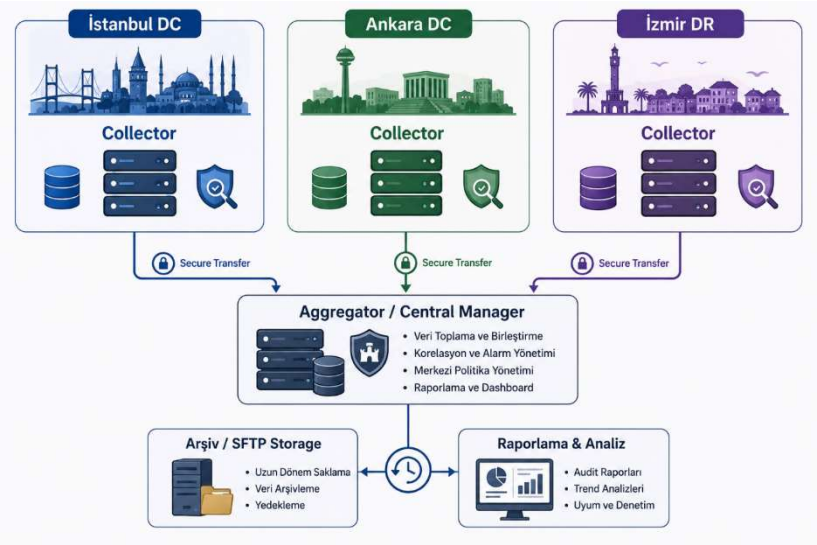
Faktör	Etkisi	Açıklama
Veritabanı sayısı	Orta	İzlenen veritabanı sayısı arttıkça izleme, raporlama ve yönetim yükü artar.
Saniyedeki SQL hacmi	Çok yüksek	SQL trafiği arttıkça Collector, işleme motoru, loglama ve disk I/O yükü ciddi şekilde artar.
Full SQL Logging kullanımı	Çok yüksek	Her SQL ifadesinin tam olarak kaydedilmesi, disk kullanımı ve sistem kaynaklarını önemli ölçüde artırır.
Aynı anda aktif bağlantı sayısı	Yüksek	Eşzamanlı bağlantı sayısı arttıkça oturum yönetimi, bellek kullanımı ve işlem yükü artar.
Alarm yoğunluğu	Orta	Alarm sayısının artması, işlem yükünü ve raporlama trafiğini artırabilir; ancak etkisi diğerlerine göre ortadır.
Saklama süresi	Disk ihtiyacını artırır	Verilerin daha uzun süre saklanması, disk kullanımını lineer olarak artırır ve yedekleme süresini uzatabilir.
Archive sıklığı	Depolama ve performansı etkiler	Daha sık archive, depolama alanı kullanımını optimize eder ancak sistem kaynaklarını kullanır. Daha seyrek archive, performansı artırır ancak disk ihtiyacını yükseltir.

Not: Az sayıda veritabanı bulunan ancak çok yüksek işlem hacmine sahip sistemler, çok sayıda fakat düşük trafikli veritabanlarından daha fazla Collector kaynağı tüketebilir.

10.3 Collector Yerleşimi

Yaygın kullanılan mimari yaklaşımlar:

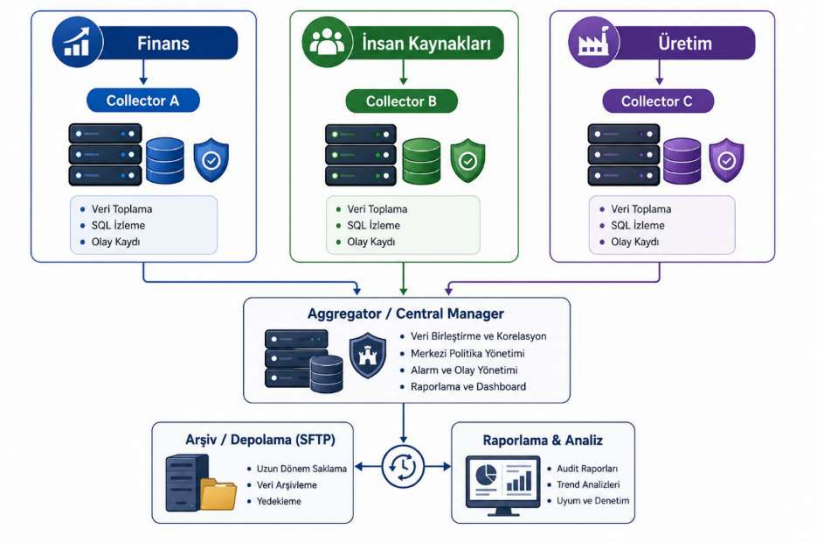
Model 1 – Bölgesel Collector



Avantajları:

- Ağ trafiği azalır.
- Yerel yönetim kolaylaşır.
- Bölgesel kesintilerden daha az etkilenir.

Model 2 – İş Birimine Göre Collector



Bu yaklaşım özellikle farklı veri hassasiyetine sahip iş birimlerinde faydalıdır.

10.4 Aggregator Tasarımı

Aggregator'ın amacı yalnızca veri depolamak değildir.

İyi bir Aggregator aşağıdaki görevleri üstlenir:

- Merkezi raporlama
- Denetim
- Trend analizi
- Arşiv yönetimi
- Kurumsal görünürlük

En iyi uygulama:

Ağır raporların Collector yerine Aggregator üzerinde çalıştırılması, veri toplama performansını olumlu yönde etkileyebilir.

10.5 Politika Sayısı Ne Kadar Olmalı?

En sık sorulan sorulardan biri:

"Kaç politika oluşturmalıyız?"

Doğru cevap:

Gerektiği kadar, ancak yönetilebilir sayıda.

Yanlış yaklaşım:

- 600 politika
- 900 kural
- Hepsi aktif

Sonuç:

- Karmaşık yapı
- Zor bakım
- Performans sorunları
- Alarm karmaşası

Daha iyi yaklaşım:

- Risk odaklı
- Basit
- Katmanlı
- Dokümante edilmiş politikalar

10.6 Full SQL Logging Her Yerde Açılmalı mı?

Hayır.

Bu, en yaygın yanlış inanışlardan biridir.

Avantajları:

- Ayrıntılı denetim izi
- Olay analizi
- Adli bilişim desteği

Dezavantajları:

- Daha fazla disk kullanımı
- Daha fazla arşiv ihtiyacı
- Daha fazla raporlama yükü
- Yönetim maliyeti

Öneri:

- Kritik sistemlerde etkinleştirin.
- Daha düşük riskli sistemlerde yalnızca gerekli politika eşleşmeleri için kullanmayı değerlendirin.
- Saklama süresini regülasyon ve operasyonel ihtiyaçlarla uyumlu planlayın.

10.7 Archive – Export – Purge Stratejisi

Kurumsal projelerde en fazla sorun yaşanan alanlardan biri budur.

Doğru yaşam döngüsü:

En kritik ilke:

Arşivlenen verinin güvenli şekilde saklandığı ve gerektiğinde geri yüklenebildiği doğrulanmadan temizleme (purge) işlemi planlanmamalıdır.

Bu yaklaşım, denetim ve olay inceleme süreçlerinde veri kaybı riskini azaltır.

10.8 SIEM Entegrasyonu

SIEM sistemine her olayı göndermek doğru yaklaşım değildir.

Örnek filtreleme:

Bu yaklaşım SIEM üzerindeki gereksiz yükü azaltabilir ve analiz kalitesini artırabilir.

10.9 S-TAP Yönetimi

S-TAP ajanları için öneriler:

- Versiyon uyumluluğunu düzenli kontrol edin.
- Güncellemeleri planlı bakım pencerelerinde yapın.
- Konfigürasyon değişikliklerini merkezi olarak yönetin.
- Ajan durumlarını düzenli izleyin.
- Desteklenmeyen işletim sistemi veya veritabanı sürümlerini envanterde işaretleyin.

10.10 Health Check Kültürü

Birçok kurum Guardium'u yalnızca sorun çıktığında kontrol eder.

Oysa düzenli sağlık kontrolleri, büyüyen sorunların erken fark edilmesini sağlar.

Önerilen aylık kontroller:

Kontrol	Amaç
Disk kullanımı	Kapasite takibi
Archive durumu	Veri yaşam döngüsü
Export görevleri	Aktarım doğrulaması
Purge işlemleri	Disk optimizasyonu
S-TAP bağlantıları	İzleme sürekliliği
Policy hataları	Yanlış yapılandırmaların tespiti
Alerter servisi	Bildirim mekanizmalarının doğrulanması
Sistem kaynakları	CPU, RAM ve depolama eğilimleri

10.11 Denetim Öncesi Kontrol Listesi

Denetim başlamadan önce aşağıdaki soruların yanıtı hazır olmalıdır:

- Kritik veritabanlarının tamamı izleniyor mu?
- Hassas tablolar sınıflandırıldı mı?
- Ayrıcalıklı kullanıcı politikaları güncel mi?
- Arşivler doğrulandı mı?
- Rapor şablonları test edildi mi?
- Alarm seviyeleri gözden geçirildi mi?
- Son politika değişiklikleri kayıt altına alındı mı?
- SIEM entegrasyonu çalışıyor mu?
- Zaman senkronizasyonu (NTP) tüm appliance'larda doğru mu?

- Disk doluluk oranları kritik seviyede mi?

10.12 Gerçek Projelerde Karşılaşılan Yaygın Hatalar

Saha projelerinde sık rastlanan durumlar:

- Tüm olayların aynı önem derecesinde değerlendirilmesi
- Her politikada "Continue to Next" kullanımının varsayılan bırakılması
- Test ortamlarının izleme kapsamı dışında tutulması
- Gereğinden uzun veya kısa log saklama süreleri
- Arşivlerin geri yükleme testlerinin yapılmaması
- Full SQL Logging'in kapsamının plansız genişletilmesi
- Collector kapasitesinin yalnızca veritabanı sayısına göre planlanması
- SIEM'e gereksiz yüksek hacimde olay gönderilmesi
- Politika değişikliklerinin dokümante edilmemesi
- Health Check süreçlerinin düzenli işletilmemesi

Bölüm Sonu Değerlendirmesi

Başarılı bir IBM Guardium ortamı, yalnızca doğru kurulumla değil; doğru mimari tasarım, sürdürülebilir politika yönetimi, planlı kapasite yönetimi ve düzenli operasyonel kontrollerle mümkün olur. En iyi uygulamaların temel amacı, sistemi gereksiz karmaşıklıktan uzak tutarken güvenlik görünürlüğünü ve denetim kabiliyetini en üst düzeye çıkarmaktır.

---

11. Gerçek Saldırı Senaryoları ve IBM Guardium ile Tespit Süreçleri

Not: Bu bölümde yer alan senaryolar, gerçek olaylardan ilham alınarak hazırlanmış kurgusal örneklerdir. Amaç; IBM Guardium'un veri tabanı güvenliği süreçlerine nasıl katkı sağlayabileceğini göstermek, belirli bir kurum veya olayı temsil etmek değildir.

Senaryo 1

Mesai Dışı Ayrıcalıklı Kullanıcı Erişimi

Olay

Bir finans kuruluşunda gece 02:13'te aşağıdaki SQL sorgusu çalıştırılır.

```
SELECT *
FROM CUSTOMER_CREDIT_CARD;
```

Bağlantı bilgileri:

İlk Bakışta

Her şey normal görünmektedir.

✓ Kullanıcı yetkilidir.

✓ Veritabanına bağlanabilmektedir.

✓ SQL hatasız çalışmıştır.

Native log açısından problem görünmeyebilir.

Guardium Ne Görür?

Guardium yalnızca SQL'i değil;

- Erişim zamanını,
- Uygulamayı,
- İstemci bilgisini,
- Politika eşleşmesini,

- Erişilen tabloyu,
- Sorgu hacmini,

Birlikte değerlendirir.

Politika

```
IF

Sensitive Table

AND

After Working Hours

AND

Privileged User

THEN

Critical Alert
```

Sonuç

SOC ekibi olayı inceler.

Bakım kaydı bulunamaz.

DBA ile görüşülür.

Oturumun yetkisiz şekilde kullanıldığı anlaşılır.

Kazanım

Yetkili hesap kullanılmış olmasına rağmen,

bağlamsal analiz sayesinde olay erken fark edilmiştir.

Senaryo 2

Servis Hesabının Ele Geçirilmesi

Bir uygulama hesabı normalde yalnızca aşağıdaki tabloya erişmektedir.

CUSTOMER_SESSION

Bir gün aşağıdaki sorgular görülmeye başlanır.

```
SELECT *
FROM CREDIT_CARD;
```

```
SELECT *
FROM CUSTOMER_IBAN;
```

Politika

```
Application Account

↓

Sensitive Tables

↓

Alarm
```

Guardium Analizi

Guardium;

Kullanıcının geçmiş davranışını,

Eriştiği tabloları,

Uygulama bilgisini,

Zaman bilgisini

Karşılaştırır.

Servis hesabının alışılmadık nesnelere erişmeye başladığı görülür.

Olay Sonucu

Yapılan incelemede,

Uygulama sunucusunda çalışan bir web kabuğu (web shell) üzerinden servis hesabının kötüye kullanıldığı belirlenir.

Senaryo 3

Toplu Veri Dışa Aktarma Hazırlığı

Bir kullanıcı kısa süre içerisinde aşağıdaki işlemleri gerçekleştirir.

```
SELECT *

↓

5 milyon kayıt

↓
```

```
CSV Export

↓

Compression

↓

Harici transfer hazırlığı
```

Guardium

Aşağıdaki davranışları ilişkilendirir.

- Büyük hacimli SELECT
- Hassas tablo
- Export işlemi
- Mesai dışı erişim

Risk puanı yükseltilir.

SIEM Korelasyonu

SIEM tarafında;

VPN oturumu

-

USB aktivitesi

-

DLP uyarısı

-

Guardium alarmı

Bir araya getirilir.

Olay kritik seviyeye yükseltilir.

Senaryo 4

Yetki Yükseltme Girişimi

Aşağıdaki SQL çalıştırılır.

```
GRANT DBA TO USER_X;
```

Politika

```
GRANT

↓

Critical

↓

Immediate Alert
```

Alarm

Guardium;

SQL'i kaydeder.

Kullanıcıyı kaydeder.

IP adresini kaydeder.

İstemciyi kaydeder.

Politikayı ilişkilendirir.

SOC ekibi olaya anında müdahale eder.

Senaryo 5

Ransomware Öncesi Keşif Faaliyetleri

Bir saldırgan,

Veritabanına erişim sağladıktan sonra aşağıdaki sorguları çalıştırmaktadır.

```
SHOW TABLES;
```

```
SELECT *
FROM INFORMATION_SCHEMA.TABLES;
```

```
SELECT *
FROM DBA_USERS;
```

```
SELECT *
FROM DBA_TABLES;
```

MITRE ATT&CK

Bu davranışlar aşağıdaki tekniklerle ilişkilendirilebilir.

Guardium

Bu sorgular tek başına zararlı olmayabilir.

Ancak;

Aynı oturum içerisinde,

Yüksek sayıda metadata sorgusu,

Ardından hassas tablo erişimi,

Ardından DDL komutları görülüyorsa,

Risk puanı artırılabilir.

Senaryo 6

DROP TABLE Komutu

```
DROP TABLE CUSTOMER;
```

Bu olayın oluşması beklenmeyebilir.

Politika:

```
DROP

↓

Critical

↓

Immediate Alert
```

İsteğe bağlı olarak;

- SIEM bildirimi
- Ticket oluşturulması
- E-posta
- SMS
- SOAR entegrasyonu

Tetiklenebilir.

Senaryo 7

Vendor Hesabının Olağan Dışı Kullanımı

Vendor hesabı;

Hafta içi,

09:00–18:00

Arasında kullanılmaktadır.

Bir gece;

03:47

Bağlantı görülmektedir.

Politika

```
Vendor

AND

Outside Working Hours

↓

Alert
```

Yapılan incelemede;

Hesabın parolasının eski bir destek oturumundan sonra değiştirilmediği ortaya çıkar.

Senaryo 8

Test Ortamında Gerçek Müşteri Verisi

Guardium Data Discovery çalışması sonucunda;

TESTDB

İçerisinde

```
CUSTOMER
```

```
CREDIT_CARD

IBAN

TC_KIMLIK
```

Tabloları tespit edilir.

İnceleme sonucunda;

Üretim yedeğinin test ortamına anonimleştirme yapılmadan geri yüklendiği anlaşılır.

Bu durum,

Herhangi bir saldırı olmamasına rağmen, yüksek güvenlik riski oluşturur.

Senaryo 9

Denetim Sırasında İstenen Kanıt

Denetçi soruyor.

Son iki yılda PERSONEL_MAAS tablosuna kim erişti?

Guardium raporu:

- Kullanıcı
- Tarih
- Saat
- SQL
- Uygulama

- IP
- Politika
- Alarm

Dakikalar içerisinde hazırlanabilir.

Senaryo 10

Gerçek Değer Nerede?

IBM Guardium'un değeri;

```
SQL

↓

Context

↓

Risk

↓

Policy

↓

Alert

↓

Evidence
```

Zincirini kurabilmesidir.

Asıl değer;

Yalnızca SQL'i görmek değil,

SQL'in güvenlik açısından ne ifade ettiğini anlayabilmektir.

Bölüm Sonu Değerlendirmesi

Gerçek güvenlik olaylarında teknik kayıtlar tek başına yeterli değildir. Olayın bağlamı, erişilen verinin hassasiyeti, kullanıcının rolü, erişim zamanı ve diğer güvenlik sistemlerinden gelen bilgiler birlikte değerlendirildiğinde anlamlı bir risk resmi ortaya çıkar. IBM Guardium, bu bağlamsal görünürlüğü sağlayarak olay müdahale ekiplerinin daha hızlı karar almasına ve denetim ekiplerinin güvenilir kanıt üretmesine destek olur.

---

12. IBM Guardium Performans Optimizasyonu ve Kapasite Planlama

Önemli Not: Performans optimizasyonu, yalnızca daha hızlı rapor almak anlamına gelmez. Amaç; veri toplama, politika değerlendirme, alarm üretimi ve raporlama süreçlerinin güvenilir ve sürdürülebilir şekilde çalışmasını sağlamaktır.

12.1 Performansı Etkileyen Temel Faktörler

IBM Guardium performansı tek bir parametreye bağlı değildir. Aşağıdaki faktörlerin birleşimi sistem davranışını belirler.

Faktör	Etki Düzeyi	Açıklama
SQL işlem hacmi (TPS/QPS)	Çok Yüksek	Collector üzerindeki temel yük.
Full SQL Logging	Çok Yüksek	Disk ve CPU kullanımını artırabilir.
Politika sayısı	Yüksek	Her SQL için değerlendirme yapılır.
Policy karmaşıklığı	Yüksek	Çoklu koşullar işlem maliyetini artırabilir.
Archive işlemleri	Orta	Yoğun saatlerde planlanmamalıdır.
Export görevleri	Orta	Ağ ve disk kullanımı oluşturur.
Aynı anda çalışan raporlar	Yüksek	Özellikle Aggregator üzerinde etkili olur.
Disk I/O performansı	Çok Yüksek	Yavaş depolama genel sistemi etkiler.

12.2 En Büyük Yanlış Anlama

Birçok projede şu yaklaşım görülür:

"20 veritabanımız var, tek Collector yeter."

Oysa önemli olan veritabanı sayısı değil, **üretilen SQL hacmidir.**

Örnek:

Ortam	Veritabanı	Günlük SQL
ERP	2	250 milyon
CRM	35	18 milyon
Test	90	4 milyon

Bu örnekte en yüksek yük, en az veritabanına sahip ERP ortamındadır.

Tasarım ilkesi: Kapasite planlamasında işlem hacmi, eşzamanlı bağlantılar ve politika yoğunluğu birlikte değerlendirilmelidir.

12.3 CPU Kullanımını Artıran Unsurlar

Collector üzerinde CPU tüketimini artıran başlıca işlemler:

- SQL Parsing
- Policy Evaluation
- Regular Expression (Regex) kullanan politikalar
- Karmaşık koşullu Rule Set'ler
- Çok sayıda eşleşen politika
- Full SQL Logging

İyi Uygulama

- Gereksiz politikaları devre dışı bırakın.
- Aynı işi yapan kuralları birleştirin.
- Çok sık kullanılan tablolar için aşırı karmaşık koşullardan kaçının.
- Regex kullanımını yalnızca gerçekten gerekli durumlarda tercih edin.

12.4 Disk Planlaması

En hızlı dolan kaynak çoğu zaman disk alanıdır.

Disk tüketimini etkileyen başlıca unsurlar:

- Full SQL kayıtları
- Audit logları
- Arşiv dosyaları

- Geçici rapor çıktıları
- Sistem logları

Örnek yaklaşım:

Bu yaşam döngüsü düzenli izlenmezse disk doluluk oranı kritik seviyelere ulaşabilir.

12.5 Full SQL Logging Ne Zaman Kullanılmalı?

Full SQL Logging güçlü bir özelliktir; ancak her ortamda ve her işlem için etkinleştirilmesi doğru değildir.

Önerilen kullanım alanları:

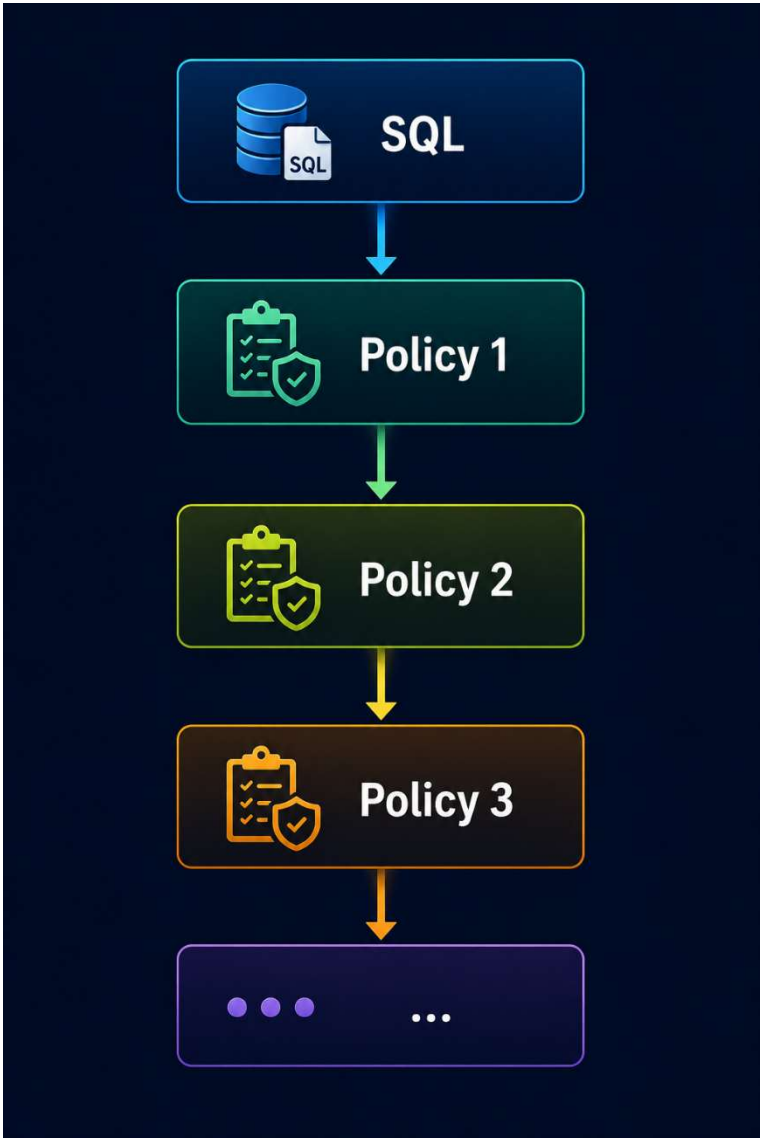
- Finans sistemleri
- Ödeme veritabanları
- İnsan Kaynakları
- Kritik müşteri verileri
- Regülasyon kapsamındaki sistemler

Daha dikkatli planlanması gereken alanlar:

- Çok yüksek hacimli OLTP sistemleri
- Geçici geliştirme ortamları
- Düşük riskli uygulamalar

12.6 Politika Performansı

Her SQL isteği aşağıdaki akıştan geçer:



Yüzlerce politika bulunan ortamlarda her ek değerlendirme, işlem maliyetini artırabilir.

Öneriler

- En sık eşleşen kuralları uygun sıraya yerleştirin.
- Nadir kullanılan kuralları ayrı Rule Set'lerde yönetin.
- Politika değişikliklerini test ortamında doğrulayın.
- Kullanılmayan veya eski politikaları periyodik olarak temizleyin.

12.7 Rapor Performansı

Kullanıcıların en sık şikâyet ettiği konulardan biri uzun süren raporlardır.

Başlıca nedenler:

- Çok geniş tarih aralıkları
- Aynı anda çalışan çok sayıda rapor
- Gereksiz sütunlar
- Filtre kullanılmaması
- Collector üzerinde ağır rapor çalıştırılması

En İyi Uygulama

- Operasyonel raporları mümkün olduğunca Aggregator üzerinden çalıştırın.
- Tarih aralıklarını ihtiyaca göre sınırlandırın.
- Hazır rapor şablonları oluşturun.
- Periyodik raporları zamanlayarak yoğun saatler dışında üretin.

12.8 Archive Performansı

Archive işlemleri sistem için kritik olmakla birlikte yoğun saatlerde çalıştırılması önerilmez.

Planlama yapılırken:

- İş yükünün düşük olduğu zaman dilimleri seçilmeli,
- Ağ bant genişliği dikkate alınmalı,
- Export işlemleriyle çakışmalar önlenmeli,
- Sonrasında doğrulama adımları uygulanmalıdır.

12.9 S-TAP Performansı

S-TAP ajanları hafif yapıda tasarlanmıştır; ancak yanlış yapılandırmalar gereksiz yük oluşturabilir.

Kontrol edilmesi önerilen noktalar:

- Desteklenen sürüm uyumluluğu
- Gereksiz izleme kapsamı
- Ağ bağlantı kalitesi
- Ajan sağlık durumu
- Merkezi konfigürasyon tutarlılığı

12.10 Kapasite Planlama Kontrol Listesi

Yeni bir Guardium kurulumu veya büyüyen bir ortam için aşağıdaki soruların yanıtlanması önerilir:

- Günlük ortalama SQL hacmi nedir?
- Eşzamanlı bağlantı sayısı kaçtır?
- Kaç veritabanı izlenecektir?
- Kaçı kritik sınıftadır?
- Full SQL Logging nerelerde kullanılacaktır?
- Veri ne kadar süre saklanacaktır?
- Günlük arşiv hacmi ne kadardır?
- Raporlama sıklığı nedir?
- SIEM'e hangi olaylar gönderilecektir?
- Gelecek 12–24 ay için büyüme beklentisi nedir?

12.11 Performans Sağlık Göstergeleri (KPI)

Operasyon ekiplerinin düzenli olarak takip edebileceği örnek göstergeler:

Bu göstergeler düzenli izlenerek kapasite sorunları büyümeden tespit edilebilir.

12.12 Gerçek Proje Deneyimlerinden Çıkarımlar

Farklı sektörlerde gerçekleştirilen Guardium projelerinde tekrar eden bazı gözlemler:

- En büyük darboğaz çoğu zaman işlemci değil, depolama performansıdır.
- Karmaşık politikalar, çok sayıda basit politikadan daha fazla kaynak tüketebilir.
- Full SQL Logging'in plansız genişletilmesi arşiv hacmini hızla artırabilir.
- Raporlama ihtiyaçları başlangıçta doğru analiz edilmezse Aggregator kapasitesi yetersiz kalabilir.

- Düzenli Health Check yapılmayan ortamlarda sorunlar genellikle kullanıcı şikâyetleriyle fark edilir.

Bölüm Sonu Değerlendirmesi

IBM Guardium performansı; donanım kapasitesi, politika tasarımı, veri yaşam döngüsü yönetimi ve operasyonel disiplinin birlikte ele alınmasıyla optimize edilebilir. Başarılı bir performans stratejisi, yalnızca mevcut yükü karşılamayı değil, kurumun büyüme planlarını da dikkate alan sürdürülebilir bir mimari oluşturmayı hedefler.

---

13. IBM Guardium High Availability (HA) ve Disaster Recovery (DR) Tasarım Rehberi

Önemli Not: IBM Guardium ortamlarında HA ve DR tasarımları, kurumun iş sürekliliği hedefleri, kabul edilebilir kesinti süresi (RTO), veri kaybı toleransı (RPO) ve altyapı mimarisi dikkate alınarak planlanmalıdır. Tek bir doğru mimari yoktur; doğru mimari kurumun ihtiyaçlarına göre şekillenir.

13.1 HA ve DR Aynı Şey Değildir

En sık karşılaşılan yanlışlardan biri şudur:

"İkinci bir Collector kurduk, artık felaket kurtarma altyapımız var."

Bu doğru değildir.

HA ve DR farklı amaçlara hizmet eder.

13.2 İş Sürekliliği Kavramları

HA ve DR planlamasında iki temel kavram vardır.

Recovery Time Objective (RTO)

Bir sistemin kesinti sonrasında kabul edilebilir en uzun süre içinde yeniden hizmet vermesi gerektiğini ifade eder.

Örnek:

RTO = 2 Saat

Bu durumda kurum, Guardium servisinin en geç iki saat içinde tekrar çalışır durumda olmasını hedeflemektedir.

Recovery Point Objective (RPO)

Kabul edilebilir veri kaybı miktarını ifade eder.

Örnek:

RPO = 15 Dakika

En kötü senaryoda son 15 dakikalık verinin kaybedilebilmesi kabul edilmektedir.

Bu hedefler; replikasyon, yedekleme ve arşiv stratejilerini doğrudan etkiler.

13.3 Temel Mimari

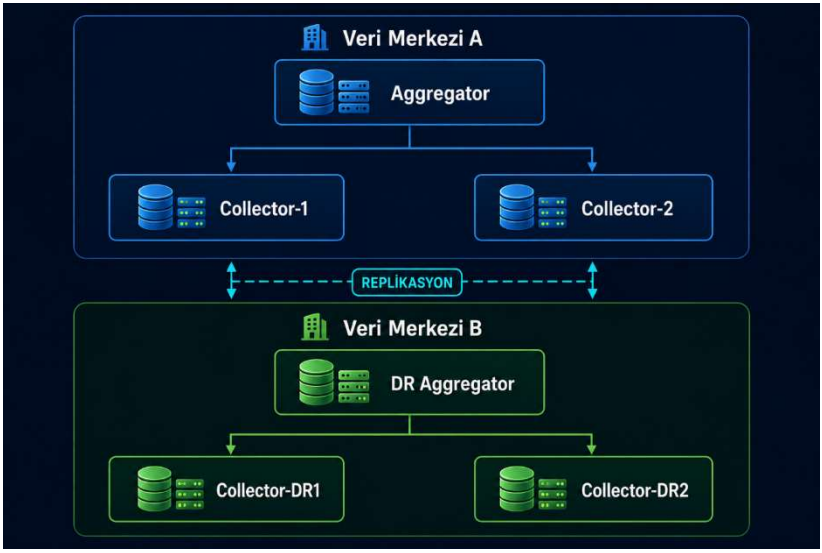
Küçük ve orta ölçekli kurumlarda yaygın mimari:

Avantajları:

- Merkezi raporlama
- Yönetim kolaylığı
- Ölçeklenebilir yapı

13.4 İki Veri Merkezi Mimarisi

Kurumsal yapılarda sık kullanılan yaklaşım:



Bu mimaride;

- Üretim ortamı birincil veri merkezinde,
- Felaket kurtarma ortamı ikinci veri merkezinde

bulunmaktadır.

13.5 Collector Yedekliliği

Collector'lar için dikkat edilmesi gereken temel konu:

Collector yalnızca bir cihaz değildir; üzerinde denetim kayıtları ve politika değerlendirme süreçleri çalışır.

Bu nedenle aşağıdaki riskler değerlendirilmelidir:

- Donanım arızası
- Disk arızası
- Ağ kesintisi

- İşletim sistemi problemi
- Sanallaştırma altyapısı sorunu

Yüksek erişilebilirlik tasarımında bu riskler için uygun önlemler planlanmalıdır.

13.6 Aggregator Neden Daha Kritik?

Collector geçici olarak devre dışı kaldığında etki belirli sistemlerle sınırlı olabilir.

Ancak Aggregator;

- Merkezi raporlama,
- Denetim,
- Tarihsel analiz,
- Yönetimsel görünürlük

Gibi işlevleri üstlendiği için daha geniş etkiye sahiptir.

Bu nedenle Aggregator'ın kapasitesi, yedekliliği ve yedekleme stratejisi ayrı bir tasarım konusu olarak ele alınmalıdır.

13.7 Ağ Tasarımı

HA mimarilerinde aşağıdaki noktalar göz önünde bulundurulmalıdır:

- Veri merkezleri arasındaki gecikme (latency)
- Bant genişliği

- Paket kaybı
- Güvenlik duvarı kuralları
- DNS ve isim çözümleme
- NTP senkronizasyonu

Özellikle zaman senkronizasyonu, olayların doğru sıralanabilmesi için kritik öneme sahiptir.

13.8 Yedekleme Stratejisi

Birçok kurum yalnızca sanal makine yedeği almanın yeterli olduğunu düşünmektedir.

Ancak aşağıdaki bileşenler ayrı ayrı değerlendirilmelidir:

- Guardium konfigürasyonu
- Politika tanımları
- Kullanıcı ve rol bilgileri
- Sertifikalar
- Arşiv dosyaları
- Dış depolama alanları

Yedeklerin düzenli olarak geri yükleme testlerinden geçirilmesi de iş sürekliliği planının önemli bir parçasıdır.

13.9 Felaket Senaryosu

Birinci veri merkezinde elektrik kesintisi yaşandığını düşünelim.

Bu sürecin ne kadar başarılı olduğu;

- Önceden hazırlanmış prosedürlere,
- Düzenli testlere,

- Ekip koordinasyonuna

Bağlıdır.

13.10 Felaket Kurtarma Testleri

Bir DR planı yalnızca dokümante edilmekle kalmamalıdır.

Belirli aralıklarla test edilmelidir.

Örnek kontrol listesi:

- Sistem beklenen sürede ayağa kalktı mı?
- Politikalar doğru çalışıyor mu?
- Raporlar üretilebiliyor mu?
- Arşiv verileri erişilebilir mi?
- SIEM entegrasyonu devam ediyor mu?
- Kullanıcı erişimleri doğrulandı mı?

13.11 Sık Yapılan Tasarım Hataları

Saha projelerinde sık karşılaşılan hatalar:

- HA ile DR'ın aynı çözüm olarak değerlendirilmesi
- İkinci veri merkezinde kapasitenin yetersiz planlanması
- DR ortamındaki yazılım sürümlerinin güncel tutulmaması
- Arşiv depolama alanının tek lokasyonda bırakılması
- NTP yapılandırmasının ihmal edilmesi
- Felaket kurtarma planlarının hiç test edilmemesi
- Yedeklerin geri yüklenebilirliğinin doğrulanmaması

13.12 En İyi Uygulamalar

- RTO ve RPO hedeflerini iş birimleriyle birlikte belirleyin.
- HA ve DR senaryolarını birbirinden bağımsız planlayın.
- Kritik bileşenler için kapasite fazlası bırakın.
- Yedekleme stratejisini düzenli olarak gözden geçirin.
- DR tatbikatlarını yılda en az bir kez gerçekleştirin.
- Zaman senkronizasyonunu tüm bileşenlerde doğrulayın.
- Dokümantasyonu güncel tutun.
- Değişiklik yönetimi süreçlerini DR planlarıyla uyumlu hale getirin.

Bölüm Sonu Değerlendirmesi

Yüksek erişilebilirlik ve felaket kurtarma, yalnızca teknik mimarinin değil; iş sürekliliği stratejisinin de temel unsurlarıdır. IBM Guardium ortamlarında doğru planlanmış HA ve DR tasarımı, güvenlik görünürlüğünün kesintisiz sürdürülmesine ve denetim kayıtlarının korunmasına katkı sağlar. Ancak bu hedeflere ulaşabilmek için mimari tasarımın düzenli testlerle desteklenmesi ve kurumun operasyonel süreçleriyle uyumlu olması gerekir.

14. IBM Guardium Health Check ve Operasyonel Olgunluk Rehberi

Amaç: Bu bölüm, IBM Guardium ortamlarının operasyonel olgunluğunu değerlendirmek için uygulanabilecek örnek bir kontrol çerçevesi sunar. Kontrol maddeleri kurumun mimarisine, sürümüne ve regülasyon gereksinimlerine göre uyarlanmalıdır.

14.1 Health Check Neden Yapılır?

Birçok kurum Health Check'i yalnızca bir problem yaşandığında gerçekleştirir.

Oysa düzenli sağlık kontrolleri aşağıdaki amaçlara hizmet eder:

- Yapılandırma hatalarının erken tespiti
- Performans sorunlarının büyümeden belirlenmesi
- Denetim hazırlığının korunması
- Kapasite planlamasına veri sağlanması
- Güncelleme öncesi risklerin görülmesi
- Operasyonel olgunluğun ölçülmesi

Health Check'in amacı arıza aramak değil, **riskleri erken görmek** olmalıdır.

14.2 Önerilen Kontrol Periyotları

14.3 Appliance Sağlık Kontrolleri

İlk kontrol katmanı appliance seviyesidir.

Kontrol Edilmesi Önerilen Başlıklar

- CPU kullanım eğilimleri
- Bellek kullanımı
- Disk doluluk oranı
- Swap kullanımı
- Dosya sistemi durumu
- Sistem zamanı
- NTP senkronizasyonu
- DNS çözümleme

- Ağ arayüzlerinin durumu
- Donanım uyarıları (fiziksel appliance'larda)

Amaç: Altyapı kaynaklı sorunların veri toplama süreçlerini etkilemesini önlemek.

14.4 Collector Sağlık Kontrolleri

Collector üzerinde düzenli doğrulanması önerilen noktalar:

- İzlenen veritabanlarının durumu
- Aktif bağlantılar
- SQL toplama sürekliliği
- Politika değerlendirme durumu
- Alarm üretimi
- Full SQL Logging kapsamı
- Yerel disk kullanımı
- Archive işlemlerinin başarısı
- Export görevleri
- Bekleyen (queued) işler

14.5 Aggregator Sağlık Kontrolleri

Aggregator için önerilen kontroller:

- Collector bağlantıları
- Veri akışının sürekliliği
- Rapor performansı

- Trend verileri
- Arşiv erişilebilirliği
- İndeks durumu
- Zamanlanmış görevler
- Raporlama başarısı

14.6 S-TAP Kontrolleri

Her S-TAP ajanı için aşağıdaki bilgiler düzenli olarak gözden geçirilmelidir:

Not: En sık karşılaşılan sorunlardan biri, ajanın kurulu olması ancak beklenen trafiğin Collector'a ulaşmamasıdır. Bu nedenle yalnızca "ajan çalışıyor" bilgisi yeterli değildir; veri akışının da doğrulanması gerekir.

14.7 Archive ve Export Kontrolleri

Veri yaşam döngüsü düzenli izlenmelidir.

Kontrol listesi:

- Son Archive başarılı mı?
- Son Export başarılı mı?
- Hedef depolama erişilebilir mi?
- Arşiv boyutları beklenen aralıkta mı?
- Beklenmeyen hata mesajları var mı?
- Geri yükleme testi yapıldı mı?

Bu kontroller, olası veri kaybı risklerini azaltmaya yardımcı olur.

14.8 Purge Kontrolleri

Purge işlemi yanlış yapılandırıldığında ciddi sonuçlar doğurabilir.

Kontrol edilmesi önerilen noktalar:

- Saklama süresi doğru tanımlandı mı?
- Archive tamamlanmadan Purge tetikleniyor mu?
- Export doğrulandı mı?
- Purge sonrası disk kullanımı beklenen seviyeye indi mi?
- Kritik veriler yanlışlıkla silinmedi mi?

14.9 Politika Sağlık Kontrolü

Politikalar zaman içinde karmaşıklaşabilir.

Kontrol edilmesi önerilen başlıklar:

- Kullanılmayan politikalar
- Çakışan kurallar
- Yinelenen koşullar
- Gereksiz "Continue to Next" kullanımı
- Yanlış alarm seviyeleri
- Dokümantasyonu eksik kurallar

Her politika için bir **iş gerekçesi (business justification)** bulunması iyi bir uygulamadır.

14.10 Alarm Mekanizmaları

Alarm üretmek tek başına yeterli değildir.

Kontrol edilmesi önerilen noktalar:

- Alarm gerçekten oluşuyor mu?
- Bildirim ilgili ekiplere ulaşıyor mu?
- SIEM entegrasyonu çalışıyor mu?
- Yanlış pozitif oranı kabul edilebilir seviyede mi?
- Alarm önceliklendirmesi doğru mu?

14.11 Raporlama Kontrolleri

Önerilen doğrulamalar:

- Kritik raporlar çalışıyor mu?
- Planlı rapor görevleri başarılı mı?
- Rapor süreleri normal mi?

- Eksik veri var mı?
- Filtreler güncel mi?

14.12 Güvenlik Sertleştirme (Hardening)

Örnek kontrol maddeleri:

- Varsayılan hesaplar gözden geçirildi mi?
- Gereksiz servisler devre dışı mı?
- Yönetim erişimleri sınırlandırıldı mı?
- SSH erişimi kurumsal politikaya uygun mu?
- Sertifikalar güncel mi?
- Yönetim arayüzü yalnızca yetkili ağlardan erişilebilir mi?

14.13 Operasyonel Olgunluk Modeli

Guardium ortamlarının olgunluk seviyesini değerlendirmek için örnek bir model:

Bu model, teknik yeterliliğin yanı sıra süreç olgunluğunu da değerlendirmeyi amaçlar.

14.14 Örnek Health Check Skor Kartı

Kategori	Ağırlık	Skor
Appliance Sağlığı	%15	14
Collector Yapısı	%20	18
Aggregator Yapısı	%15	13
Politika Yönetimi	%20	17
Archive / Export	%10	9
Alarm Mekanizması	%10	8
Güvenlik Sertleştirme	%10	9
Toplam	%100	88 / 100

Bu skor, teknik kararların yerini almaz; zaman içindeki gelişimi izlemek için kullanılabilecek örnek bir değerlendirme yöntemidir.

14.15 Health Check Sonrası Aksiyon Planı

Her bulgu aşağıdaki şekilde sınıflandırılabilir:

Bu yaklaşım, teknik bulguların somut aksiyonlara dönüştürülmesini kolaylaştırır.

Bölüm Sonu Değerlendirmesi

Başarılı bir IBM Guardium operasyonu, yalnızca sistemin çalışır durumda olmasıyla ölçülemez. Düzenli Health Check süreçleri; performans, güvenlik, denetim hazırlığı ve iş sürekliliği açısından ortamın sürekli değerlendirilmesini sağlar. Bu kontroller, olası sorunların erken tespit edilmesine ve operasyonel olgunluğun zaman içinde artırılmasına katkıda bulunur.

---

15. MITRE ATT&CK Perspektifinden IBM Guardium

15.1 MITRE ATT&CK Nedir?

MITRE ATT&CK, saldırganların gerçek dünyada kullandığı taktik ve teknikleri sistematik olarak sınıflandıran, dünya genelinde yaygın kabul gören bir bilgi tabanıdır.

Bir güvenlik ürünü açısından temel soru şudur:

"Saldırganın bu aşamadaki davranışını görebiliyor muyum?"

IBM Guardium açısından cevap, özellikle **veritabanı üzerinde gerçekleşen faaliyetler** için çoğu zaman "evet"tir.

15.2 Saldırı Zincirinde Guardium'un Konumu

Basitleştirilmiş bir saldırı akışı:

IBM Guardium özellikle şu aşamalarda yüksek görünürlük sağlayabilir:

- Veritabanına erişim

- SQL aktiviteleri
- Ayrıcalıklı kullanıcı işlemleri
- Hassas veri erişimi
- DDL değişiklikleri
- Veri dışa aktarma belirtileri

15.3 Taktik ve Teknik Eşleştirmesi

Aşağıdaki tablo, veritabanı odaklı bazı MITRE ATT&CK teknikleri ile Guardium'un sağlayabileceği görünürlüğe ilişkin örnek bir eşleştirmedir.

MITRE Tekniği	Örnek Davranış	Guardium Katkısı
T1087 – Account Discovery	Veritabanı kullanıcılarının listelenmesi	Hesap sorgularının izlenmesi
T1018 – Remote System Discovery	Metadata sorguları	Şema ve sistem sorgularının görünürlüğü
T1485 – Data Destruction	DROP TABLE, TRUNCATE	DDL komutlarının izlenmesi ve alarm üretimi
T1098 – Account Manipulation	GRANT, REVOKE, ALTER USER	Yetki değişikliklerinin kaydı
T1530 – Data from Cloud Storage Object	Bulut veritabanlarında hassas veri erişimi	Desteklenen platformlarda SQL aktivitesi görünürlüğü
T1005 – Data from Local System	Kritik tabloların okunması	Hassas tablo erişimlerinin izlenmesi

Not: Bu eşleştirmeler örnek niteliğindedir. Nihai görünürlük; veritabanı platformu, Guardium sürümü, politika tasarımı ve mimariye bağlı olarak değişebilir.

15.4 Discovery (Keşif) Aşaması

Bir saldırgan, veritabanına erişim sağladıktan sonra genellikle aşağıdaki soruların cevaplarını arar:

- Hangi tablolar var?
- Hangi kullanıcılar mevcut?
- Yetkiler neler?
- Hangi veriler daha değerli?

Örnek sorgular:

```
SELECT * FROM INFORMATION_SCHEMA.TABLES;
```

```
SELECT * FROM DBA_USERS;
```

```
SHOW TABLES;
```

Bu sorgular tek başına kötü niyet göstergesi olmayabilir.

Ancak;

- Olağan dışı zamanlarda,
- Beklenmeyen kullanıcılar tarafından,
- Yüksek hacimde

Çalıştırıldığında güvenlik ekipleri için anlamlı sinyaller oluşturabilir.

15.5 Credential Access Sonrası Davranış

Bir hesabın ele geçirildiğini düşünelim.

Kimlik doğrulama başarılıdır.

Artık saldırgan;

- Gerçek kullanıcı adıyla,
- Gerçek parola ile,

Bağlanmaktadır.

Bu noktada güvenlik açısından önemli olan:

"Bu kullanıcı normalde böyle davranıyor muydu?"

Davranış farklıysa;

- Alışılmadık tablo erişimleri,
- Farklı istemci araçları,
- Beklenmeyen IP adresleri,
- Sıra dışı sorgu hacmi

İncelenmeye değer hale gelir.

15.6 Collection

Saldırganın amacı çoğu zaman veri toplamaktır.

Örnek:

```
SELECT *
FROM CUSTOMER;
```

Tek bir sorgu zararsız görünebilir.

Ancak;

- Milyonlarca kayıt,
- Hassas veri,
- Kısa süre içinde tekrarlanan sorgular

Bir araya geldiğinde risk seviyesi değişebilir.

15.7 Exfiltration (Veri Dışa Aktarma)

MITRE ATT&CK'ta veri dışa aktarma, ayrı bir taktik olarak tanımlanır.

Guardium çoğu zaman doğrudan ağ üzerinden dosya aktarımını görmez.

Ancak aşağıdaki öncü davranışlara görünürlük sağlayabilir:

- Büyük hacimli SELECT işlemleri
- Kritik tablo erişimleri
- Export amaçlı sorgular
- Olağan dışı veri okuma desenleri

Bu bilgiler, DLP, SIEM veya SOAR platformlarından gelen diğer sinyallerle birlikte değerlendirildiğinde olayın daha net anlaşılmasına yardımcı olabilir.

15.8 Yetki Yükseltme

Örnek komutlar:

```
GRANT DBA TO USER_X;
```

```
ALTER USER USER_X IDENTIFIED BY ...
```

```
CREATE USER ...
```

Bu işlemler;

- Değişiklik yönetimi,
- Bakım çalışmaları

Kapsamında beklenen faaliyetler olabilir.

Ancak plan dışı gerçekleşmeleri durumunda yüksek öncelikli inceleme gerektirebilir.

15.9 Savunmadan Kaçınma (Defense Evasion)

Saldırganlar bazen iz bırakmamaya çalışabilir.

Örneğin:

- Geçici tabloların kullanılması
- Yetkili uygulama hesaplarının tercih edilmesi
- Bakım saatlerinde işlem yapılması

Bu tekniklerin tespiti yalnızca Guardium'a değil, bütünleşik güvenlik mimarisine bağlıdır. Guardium ise SQL aktivitelerine ilişkin denetim izi sağlayarak olay analizine katkıda bulunur.

15.10 SIEM Korelasyonu

Tek başına aşağıdaki olaylar düşük önemde olabilir:

- Gece bağlantısı
- Büyük SELECT
- Yeni IP adresi

Ancak birlikte değerlendirildiğinde:

Yüksek riskli bir senaryo oluşabilir.

Bu nedenle Guardium çıktılarının SIEM platformlarıyla ilişkilendirilmesi, olay müdahalesine önemli katkı sağlayabilir.

15.11 Purple Team Çalışmaları

MITRE ATT&CK yalnızca savunma ekipleri için değil;

- Red Team
- Blue Team
- Purple Team

Çalışmaları için de ortak bir dil sunar.

Guardium politikaları;

- Hangi SQL davranışlarının izleneceği,
- Hangi işlemlerde alarm üretileceği,
- Hangi erişimlerin raporlanacağı

Gibi konularda Purple Team egzersizlerini destekleyebilir.

15.12 Örnek ATT&CK Kapsam Analizi

ATT&CK Taktiği	Guardium Katkı Düzeyi	
Initial Access	Düşük	Veritabanına ilk erişim yöntemlerini izleyemez.
Execution	Düşük	İşletim sistemi komutlarını izleyemez.
Persistence	Orta	Kullanıcı/hesap değişikliklerini ve yetkilendirme kalıcılıklarını izler.
Privilege Escalation	Yüksek	Yetki yükseltme ve kritik yetki değişikliklerini izler.
Defense Evasion	Orta	Anormal sorgu desenleri ve şüpheli aktiviteleri tespit eder.
Credential Access	Düşük	Kimlik bilgisi ele geçirme aktivitelerini doğrudan izleyemez.
Discovery	Yüksek	Metadata sorguları ve sistem keşif aktivitelerini izler.
Collection	Çok Yüksek	Hassas veriye erişim ve toplama aktivitelerini detaylı izler.
Exfiltration	Orta	Veri sızıntısının öncü göstergelerini (ani artış, büyük hacim) izler.
Impact	Yüksek	DDL komutları ve kritik değişikliklerin görünürlüğünü sağlar.

Bu tablo, Guardium'un en güçlü olduğu alanların **Discovery**, **Collection**, **Privilege Escalation** ve **Impact** ile ilişkili veritabanı aktiviteleri olduğunu göstermektedir.

Bölüm Sonu Değerlendirmesi

MITRE ATT&CK çerçevesi, saldırgan davranışlarını anlamak için güçlü bir referans sunar. IBM Guardium ise bu çerçevenin özellikle veritabanı katmanında gerçekleşen tekniklerine görünürlük kazandırarak güvenlik operasyonlarına katkı sağlar. Guardium'un sağladığı SQL aktivite kayıtları, hassas veri erişim bilgileri ve politika ihlali kayıtları; SIEM, SOAR ve diğer güvenlik kontrolleriyle birlikte değerlendirildiğinde daha kapsamlı bir tehdit görünürlüğü elde edilmesine yardımcı olur.

---

16. Denetçi Soru Bankası ve IBM Guardium ile Kanıt Üretimi

Önemli Not: Aşağıdaki sorular; KVKK, PCI DSS, ISO/IEC 27001, finans sektörü denetimleri ve kurumsal iç denetimlerde karşılaşılabilecek örnek sorulardır. Kurumun faaliyet alanına göre ek gereksinimler bulunabilir.

16.1 Denetçiler Aslında Ne Arar?

Denetçiler çoğu zaman ürün ismine odaklanmaz.

Onlar aşağıdaki dört soruya cevap arar:

IBM Guardium'un en büyük katkılarından biri, veri tabanı aktivitelerine ilişkin güvenilir ve merkezi bir denetim izi oluşturabilmesidir.

16.2 Kullanıcı Erişimleri

Soru

Son altı ay içerisinde PERSONEL tablosuna kimler erişti?

Beklenen kanıt:

- Kullanıcı adı
- Tarih
- Saat
- İstemci IP adresi
- Uygulama
- SQL komutu
- Politika sonucu

Soru

Maaş bilgilerine mesai saatleri dışında erişim oldu mu?

Beklenen kanıt:

- Erişim zamanı
- Kullanıcı rolü
- İstemci bilgisi
- Alarm kaydı (varsa)

Soru

DBA hesapları hangi tablolar üzerinde işlem yaptı?

Beklenen kanıt:

- Ayrıcalıklı kullanıcı listesi
- İşlem türü (SELECT, UPDATE, DELETE, DDL)
- Hedef nesne

- Zaman bilgisi

16.3 Ayrıcalıklı Kullanıcılar

Soru

SYS veya SYSTEM hesabı son üç ayda hangi işlemleri gerçekleştirdi?

İncelenebilecek örnek alanlar:

Soru

CREATE USER komutunu kim çalıştırdı?

Örnek sorgulanan işlemler:

CREATE USER

ALTER USER

GRANT

REVOKE

16.4 Hassas Veri Erişimi

Soru

Kredi kartı bilgilerine kim erişti?

Beklenen bilgiler:

- Kullanıcı
- Tablo
- Tarih
- Saat
- Uygulama
- Politika

Soru

KVKK kapsamındaki kişisel verilere erişimler kayıt altına alınıyor mu?

Beklenen yaklaşım:

- Hassas veri sınıflandırması
- Erişim kayıtları
- Alarm politikaları
- Raporlama

16.5 DDL İşlemleri

Soru

Son bir yılda hangi tablolar silindi?

İlgili SQL örnekleri:

DROP TABLE

TRUNCATE TABLE

ALTER TABLE

Soru

Kim tablo yapısını değiştirdi?

Beklenen kayıtlar:

- Kullanıcı
- SQL
- Tarih
- Nesne
- İstemci

16.6 Olağan Dışı Davranışlar

Soru

Mesai saatleri dışında gerçekleşen kritik erişimler nelerdir?

Örnek filtreler:

- Saat
- Rol

- Hassas tablo
- Alarm seviyesi

Soru

Bir kullanıcı normal davranışının dışında işlem yaptı mı?

İnceleme kriterleri:

- Yeni istemci
- Yeni IP
- Farklı uygulama
- Olağan dışı sorgu hacmi
- Hassas veri erişimi

16.7 Vendor Erişimleri

Soru

Dış destek firmaları hangi tarihlerde sisteme erişti?

Beklenen bilgiler:

- Vendor hesabı
- Erişim süresi
- İşlem türü
- Değişiklik kayıtları
- İlişkili bakım talebi (varsa)

16.8 Servis Hesapları

Soru

Servis hesapları hangi tabloları okuyor?

Beklenen analiz:

- Uygulama hesabı
- SQL hacmi
- Hassas veri erişimi
- Olağan dışı sorgular

16.9 Alarm Yönetimi

Soru

Üretilen alarmlar inceleniyor mu?

Beklenen kanıt:

- Alarm geçmişi
- Öncelik
- İnceleme notları
- Kapatma bilgisi
- İlişkili olay numarası (varsa)

16.10 Arşiv Yönetimi

Soru

Eski loglara erişebiliyor musunuz?

Beklenen bilgiler:

- Saklama süresi
- Archive durumu
- Export doğrulaması
- Geri yükleme testi sonuçları

Soru

İki yıl önceki bir olayı gösterebilir misiniz?

Bu soru yalnızca log saklama değil, arşiv yönetiminin de doğruluğunu test eder.

16.11 Yetki Yönetimi

Soru

Guardium üzerinde yönetici yetkisi kimlerde var?

İncelenmesi önerilen başlıklar:

- Kullanıcılar
- Roller
- Son giriş zamanı
- Atanan yetkiler

Soru

Eski çalışanların hesapları kaldırıldı mı?

Beklenen yaklaşım:

- Kimlik yaşam döngüsü süreçleriyle uyum
- Periyodik hesap gözden geçirmeleri

16.12 Denetim Senaryosu

Gerçekçi bir örnek:

Denetçi aşağıdaki soruyu soruyor.

14 Mart tarihinde PERSONEL_MAAS tablosuna erişen tüm kullanıcıları gösterebilir misiniz?

Teknik ekip aşağıdaki bilgileri hazırlıyor:

- Kullanıcı adı
- Tarih ve saat
- SQL komutu
- İstemci IP
- Uygulama
- Politika sonucu
- Alarm durumu

Denetçi ikinci soruyu soruyor.

Bu erişimlerden hangileri mesai saatleri dışında gerçekleşti?

İyi yapılandırılmış raporlar sayesinde aynı veri kümesi farklı filtrelerle yeniden değerlendirilebilir.

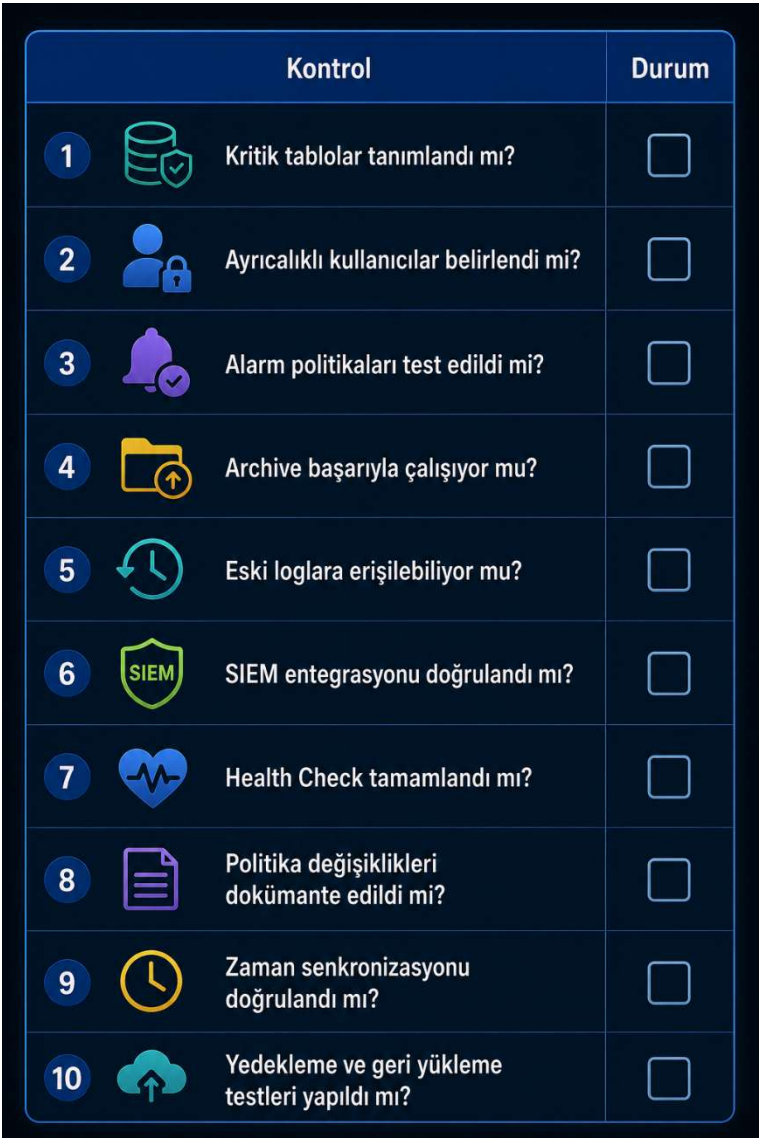
16.13 Kanıt Kalitesi

Denetimlerde yalnızca logun bulunması yeterli değildir.

Kanıtın şu özelliklere sahip olması beklenir:

16.14 Denetim Hazırlık Kontrol Listesi

Denetim öncesinde aşağıdaki sorulara "Evet" cevabı verilebilmelidir:


Kontrol
Durum
1
Kritik tablolar tanımlandı mı?
2
Ayrıcalıklı kullanıcılar belirlendi mi?
3
Alarm politikaları test edildi mi?
4
Archive başarıyla çalışıyor mu?
5
Eski loglara erişilebiliyor mu?
6
SIEM
SIEM entegrasyonu doğrulandı mı?
7
Health Check tamamlandı mı?
8
Politika değişiklikleri dokümante edildi mi?
9
Zaman senkronizasyonu doğrulandı mı?
10
Yedekleme ve geri yükleme testleri yapıldı mı?

Bölüm Sonu Değerlendirmesi

Başarılı bir denetim, yalnızca doğru teknolojilere sahip olmakla değil; bu teknolojilerden elde edilen bilgilerin güvenilir, anlaşılır ve doğrulanabilir şekilde sunulabilmesiyle mümkündür. IBM Guardium, veri tabanı aktivitelerine ilişkin merkezi kayıt ve raporlama yetenekleriyle denetim süreçlerini destekler. Ancak güçlü bir denetim hazırlığı için politika tasarımı, veri saklama stratejisi ve düzenli operasyonel kontrollerin de aynı derecede önemli olduğu unutulmamalıdır.

---

17. IBM Guardium Politika Tasarım Rehberi (Policy Design Guide)

Önemli Not: Bu bölümde yer alan politika örnekleri referans amaçlıdır. Her kurumun veri sınıflandırması, iş süreçleri ve risk iştahı farklı olduğundan, politikalar üretim ortamına alınmadan önce test edilmelidir.

17.1 Başarılı Bir Politika Nasıl Tasarlanır?

Birçok Guardium projesinde yüzlerce politika yazılır.

Ancak çok sayıda politika yazmak her zaman iyi bir güvenlik anlamına gelmez.

Başarılı bir politika aşağıdaki özelliklere sahip olmalıdır:

✓ İş ihtiyacını karşılamalı

✓ Yanlış pozitif üretmemeli

✓ Performansı olumsuz etkilememeli

✓ Anlaşılabilir olmalı

✓ Dokümante edilmiş olmalı

17.2 Politika Yaşam Döngüsü

Bir politika "yazıldı ve bitti" yaklaşımıyla ele alınmamalıdır. İş süreçleri değiştikçe politikaların da güncellenmesi gerekir.

17.3 Politika Şablonu

Bu makale boyunca tüm politika örnekleri aşağıdaki formatta sunulacaktır.

Politika 1

DBA Mesai Dışı Erişim

Amaç

Ayrıcalıklı kullanıcıların çalışma saatleri dışındaki erişimlerini görünür kılmak.

Risk

Ele geçirilmiş yönetici hesapları veya yetkisiz bakım faaliyetleri.

Tetikleme

```
Role = DBA
```

```
AND

Time = Outside Business Hours
```

Alarm

Yüksek

Önerilen Aksiyon

- Alarm üret
- SIEM'e gönder
- Olay kaydı oluştur

Yanlış Pozitif

Planlı bakım çalışmaları.

Politika 2

Hassas Veri Erişimi

Amaç

Kredi kartı, IBAN, TC Kimlik No, maaş gibi hassas verilerin erişimlerini izlemek.

Kapsam

- CUSTOMER
- PERSONNEL
- PAYMENT
- CREDIT_CARD

Alarm

Yüksek

Önerilen Aksiyon

- Alarm
- Haftalık rapor
- Denetim kaydı

Politika 3

DROP TABLE İzleme

Amaç

Veri kaybına neden olabilecek DDL işlemlerini izlemek.

SQL

```
DROP TABLE
```

Alarm

Kritik

Aksiyon

- Anında Alarm
- SIEM
- SOAR
- E-posta

Politika 4

CREATE USER

Risk

Yetkisiz kullanıcı oluşturulması.

SQL

```
CREATE USER
```

Alarm

Kritik

Politika 5

ALTER USER

Amaç

Parola değişikliklerini ve kullanıcı yapılandırmalarını izlemek.

SQL

```
ALTER USER
```

Alarm

Yüksek

Politika 6

GRANT Yetki Takibi

SQL

```
GRANT
```

Alarm

Kritik

Politika 7

REVOKE İşlemleri

Amaç:

Yetki kaldırma işlemlerinin izlenmesi.

SQL

```
REVOKE
```

Alarm:

Orta

Politika 8

Büyük Veri Okuma

Koşul

```
Rows Returned

>

100.000
```

Alarm

Yüksek

Yanlış Pozitif

Raporlama uygulamaları.

Politika 9

Service Account Abuse

Koşul

```
Application Account
```

```
↓

Sensitive Tables
```

Alarm

Yüksek

Politika 10

Vendor Access

Koşul

```
Vendor

AND

Weekend
```

Alarm

Orta

Politika 11

SQL Developer Kullanımı

Kurumsal uygulama yerine SQL Developer, DBeaver, TOAD gibi istemciler üzerinden yapılan erişimleri görünür kılmak.

Risk

Doğrudan veritabanı erişimi.

Politika 12

Export Hazırlığı

Koşullar

- Büyük SELECT
- Hassas veri
- Aynı oturum

↓

Alarm

Politika 13

Metadata Enumeration

SQL

```
INFORMATION_SCHEMA

veya

DBA_TABLES
```

↓

Orta Alarm

Politika 14

Çok Sayıda Başarısız Giriş

Koşul

```
5 dakika
```

```
↓

10 başarısız giriş
```

↓
Alarm

Politika 15

Test Ortamında Gerçek Veri

```
Data Discovery

↓

Sensitive Data

↓

TEST Database
```

↓
Alarm

Politika 16

Kritik Tablo Güncellemesi

SQL

```
UPDATE CUSTOMER
```

↓
Yüksek Alarm

Politika 17

Maaş Bilgileri

```
SELECT

↓

PERSONNEL_SALARY
```

↓
Alarm

Politika 18

Toplu DELETE

SQL

```
DELETE

Rows

>

10.000
```

↓
Kritik

Politika 19

TRUNCATE TABLE

SQL

```
TRUNCATE
```

↓

Kritik

Politika 20

Olağan Dışı İstemci

Koşul

```
DBA

↓

Unknown Client
```

↓

Alarm

17.4 Politika Önceliklendirme Matrisi

Her politika aynı öneme sahip değildir. Kaynakların etkin kullanımı için önceliklendirme yapılmalıdır.

17.5 Yanlış Pozitif Yönetimi

Başarılı bir politika yalnızca olay üretmez; gereksiz alarmları da azaltır.

Yanlış pozitifleri azaltmak için:

- Bakım pencerelerini hariç tutun.
- Yetkili servis hesaplarını tanımlayın.
- İş birimleriyle kritik tabloları doğrulayın.
- Aynı alarmı farklı kurallarla tekrar üretmeyin.
- Politika etkinliğini düzenli olarak gözden geçirin.

17.6 Politika Dokümantasyonu

Her politika için aşağıdaki bilgilerin kayıt altına alınması önerilir:

- İş sahibi (Business Owner)
- Teknik sorumlu
- Oluşturulma tarihi
- Son güncelleme tarihi
- Değişiklik geçmişi
- İlgili regülasyon (KVKK, PCI DSS, ISO 27001 vb.)
- Test sonuçları

Bu yaklaşım, denetimlerde politikaların neden oluşturulduğunu ve nasıl yönetildiğini göstermeye yardımcı olur.

Bölüm Sonu Değerlendirmesi

Etkili bir IBM Guardium politikası, yalnızca belirli SQL ifadelerini izlemekten ibaret değildir. Kullanıcının rolü, erişim zamanı, veri sınıfı, istemci uygulaması ve iş bağlamı birlikte değerlendirildiğinde daha anlamlı güvenlik çıktıları elde edilir. Düzenli gözden geçirilen ve iş ihtiyaçlarıyla uyumlu politikalar, hem güvenlik operasyonlarının etkinliğini artırır hem de denetim süreçlerini destekler.

---

18. IBM Guardium Troubleshooting Guide

Sık Karşılaşılan Problemler ve Çözüm Yaklaşımları

18.1 Sorun Giderme Yaklaşımı

IBM Guardium ortamlarında bir problem görüldüğünde doğrudan log dosyalarına geçmek yerine sistematik bir yaklaşım izlenmelidir.

Önerilen akış:

Problem 1

Collector'a Trafik Gelmiyor

Belirti

- Yeni SQL kayıtları oluşmuyor.
- Dashboard'da trafik görünmüyor.
- Alarm üretimi duruyor.

Olası Nedenler

- S-TAP bağlantısı kesilmiş.
- Ağ iletişim problemi.
- Güvenlik duvarı değişikliği.
- Veritabanı yeniden başlatılmış ancak ajan yeniden bağlanamamış.
- İzleme kapsamı yanlış yapılandırılmış.

Kontrol Listesi

- S-TAP aktif mi?
- Collector erişilebilir mi?
- Ağ bağlantısı çalışıyor mu?
- Son trafik zamanı nedir?
- İlgili veritabanı hâlâ izleniyor mu?

Problem 2

Alarm Üretilmiyor

Belirti

Politika tanımlı olmasına rağmen alarm oluşmuyor.

Kontrol Edilecek Noktalar

- Politika etkin mi?
- Rule Set doğru sırada mı?

- İlgili nesne politika kapsamına dahil mi?
- Alarm seviyesi doğru tanımlandı mı?
- İstisna (exception) kuralları alarmı engelliyor mu?
- Bakım penceresi veya zaman filtresi var mı?

Not

Çok sayıda politika bulunan ortamlarda, kural sıralaması beklenmeyen davranışlara neden olabilir. Politika akışının test ortamında doğrulanması önerilir.

Problem 3

Archive Başarısız

Belirti

Planlı Archive görevi tamamlanmıyor.

Kontrol Listesi

- Disk alanı yeterli mi?
- Hedef depolama erişilebilir mi?
- Kimlik doğrulama bilgileri güncel mi?
- Ağ bağlantısı kesintisiz mi?
- Zamanlanmış görev çakışması var mı?

Öneri

Archive işlemi tamamlanmadan Purge sürecinin başlamaması sağlanmalıdır.

Problem 4

Export Başarısız

Muhtemel Sebepler

- SFTP sunucusu erişilemiyor.
- Kullanıcı yetkileri değişmiş.
- Depolama alanı dolu.
- Ağ kesintisi.
- Kimlik doğrulama problemi.

Doğrulama

- Hedef dizine dosya yazılabiliyor mu?
- Export logları hata içeriyor mu?
- Son başarılı Export ne zaman gerçekleşti?

Problem 5

Purge Beklenenden Fazla Veri Sildi

Muhtemel Nedenler

- Saklama süresi yanlış tanımlandı.
- Archive doğrulanmadan Purge çalıştı.
- Yanlış tarih filtresi kullanıldı.

Önleyici Yaklaşım

- Purge öncesinde Archive ve Export başarıyla tamamlanmış olmalıdır.
- Geri yükleme testleri düzenli yapılmalıdır.

Problem 6

Rapor Çok Yavaş Çalışıyor

Muhtemel Sebepler

- Çok geniş tarih aralığı
- Gereksiz sütunlar
- Aynı anda çalışan çok sayıda rapor
- Disk I/O darboğazı
- Arşivlenmemiş büyük veri hacmi

İyileştirme Önerileri

- Tarih aralığını daraltın.
- Uygun filtreler kullanın.
- Operasyonel raporları mümkün olduğunca Aggregator üzerinden çalıştırın.
- Yoğun raporları mesai dışı zamanlayın.

Problem 7

Full SQL Görünmüyor

Belirti

Oturum (Session) kayıtları mevcut ancak Full SQL içeriği eksik.

Kontrol Edilecek Noktalar

- Full SQL Logging ilgili politika veya veri kaynağı için etkin mi?
- Saklama süresi dolmuş olabilir mi?
- Arşivden geri yüklenen veri tam mı?
- İlgili tarih aralığında yalnızca özet kayıtlar mı saklandı?

Saha Deneyimi

Bazı durumlarda oturum kayıtlarının mevcut olmasına rağmen Full SQL verilerinin farklı saklama veya arşivleme süreçlerinden

etkilenmesi nedeniyle görünmediği gözlemlenebilir. Bu tür senaryolarda arşiv doğrulaması, ilgili görev günlükleri ve üretici desteğiyle birlikte değerlendirme yapılması önerilir.

Problem 8

Collector – Aggregator Veri Akışı Yok

Belirti

Collector veri topluyor ancak Aggregator'da görünmüyor.

Kontrol Edilecek Noktalar

- Export görevleri başarılı mı?
- Import süreçleri çalışıyor mu?
- Ağ bağlantısı aktif mi?
- Zaman senkronizasyonu doğru mu?
- İlgili görev loglarında hata var mı?

Problem 9

S-TAP Bağlı Görünüyor Ama Trafik Yok

Olası Sebepler

- Yanlış Inspection Engine yapılandırması
- Yanlış port izleme
- Desteklenmeyen bağlantı yöntemi
- Veritabanı tarafında değişiklik

Kontrol

- Son trafik zamanı
- Trafik hacmi

- Yapılandırma değişiklik geçmişi
- Test sorguları ile doğrulama

Problem 10

GIM Agent Dağıtımı Başarısız

Kontrol Edilecek Noktalar

- SSH erişimi
- İşletim sistemi uyumluluğu
- Kullanıcı yetkileri
- Disk alanı
- Ağ bağlantısı

Problem 11

SIEM'e Alarm Gitmiyor

Kontrol

- Alarm gerçekten oluşuyor mu?
- Syslog yapılandırması doğru mu?
- Ağ üzerinden bağlantı sağlanabiliyor mu?
- Güvenlik duvarı izinleri uygun mu?
- SIEM tarafında alım kuralları doğru yapılandırılmış mı?

Problem 12

Upgrade Sonrası Beklenmeyen Davranış

Kontrol

- Desteklenen yükseltme yolu izlendi mi?
- Tüm bileşenler aynı sürüme yükseltildi mi?
- Politikalar doğrulandı mı?
- Sertifikalar ve entegrasyonlar kontrol edildi mi?
- S-TAP sürümleri uyumlu mu?

Problem 13

Disk Sürekli Doluyor

Kontrol

- Archive düzenli çalışıyor mu?
- Purge tamamlanıyor mu?
- Full SQL Logging kapsamı gereğinden geniş mi?
- Beklenmeyen log artışı var mı?

İyileştirme

- Saklama politikasını gözden geçirin.
- Veri büyüme trendini izleyin.
- Kapasite planlamasını güncelleyin.

Problem 14

Çok Fazla Yanlış Pozitif Alarm

Muhtemel Sebepler

- Politika kapsamı çok geniş.
- Kritik olmayan tablolar izleniyor.
- Bakım hesapları hariç tutulmamış.

- Eşik değerleri uygun belirlenmemiş.

Öneri

Politikaları iş birimleriyle birlikte periyodik olarak gözden geçirin ve gereksiz alarmları azaltacak istisna kurallarını dikkatli şekilde uygulayın.

Problem 15

Performans Beklenenden Düşük

Kontrol Listesi

- CPU kullanımı
- Bellek kullanımı
- Disk gecikmesi (I/O)
- Ağ gecikmesi
- Politika sayısı
- Full SQL Logging kapsamı
- Aynı anda çalışan görevler

18.2 Sorun Önceliklendirme Matrisi

18.3 Sorun Giderme İçin Kanıt Toplama

IBM Support veya kurum içi ikinci seviye ekiplerle çalışırken aşağıdaki bilgilerin hazırlanması önerilir:

- Guardium sürümü ve yama seviyesi
- Etkilenen bileşen (Collector, Aggregator vb.)
- Sorunun ilk görüldüğü tarih ve saat
- İlgili görev günlükleri (Archive, Export, Import)
- Politika veya yapılandırma değişiklik geçmişi
- Ekran görüntüleri ve hata mesajları
- Sorunun tekrar üretilebildiği adımlar (varsa)
- Gerekli must_gather log çıktıları

Bu bilgiler, olayın daha hızlı analiz edilmesine yardımcı olur.

Bölüm Sonu Değerlendirmesi

Sorun giderme süreçlerinde en önemli unsur, sistematik ilerlemektir. Belirtileri doğru tanımlamak, ilgili bileşeni izole etmek ve doğrulanabilir kanıtlarla ilerlemek; gereksiz müdahaleleri azaltır ve çözüm süresini kısaltır. IBM Guardium ortamlarında düzenli Health Check, kapasite planlaması ve değişiklik yönetimi süreçleri, birçok operasyonel problemin ortaya çıkmasını önleyebilir.

---

19. IBM Guardium Upgrade ve Migration Rehberi

19.1 Neden Düzenli Upgrade Yapılmalı?

Bazı kurumlarda "çalışıyorsa dokunmayalım" yaklaşımı tercih edilir.

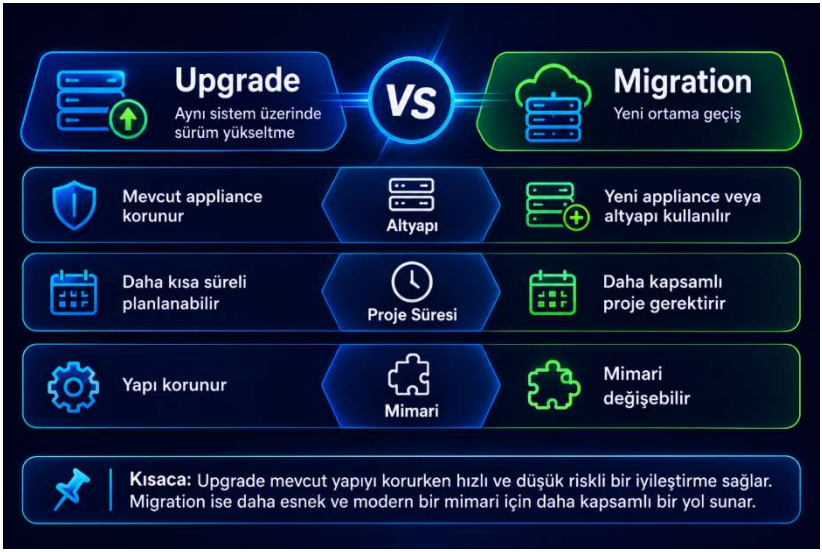
Ancak uzun süre güncellenmeyen sistemler aşağıdaki riskleri beraberinde getirir:

- Destek süresinin sona ermesi (End of Support)
- Güvenlik açıklarının giderilememesi
- Yeni veritabanı sürümlerinin desteklenmemesi
- Yeni işletim sistemi sürümleriyle uyumluluk sorunları
- Performans iyileştirmelerinden yararlanamama
- Yeni raporlama ve politika özelliklerini kullanamama

Upgrade yalnızca yeni özellikler için değil, sürdürülebilir operasyon için de önemlidir.

19.2 Upgrade mi Migration mı?

Bu iki kavram sıkça karıştırılır.



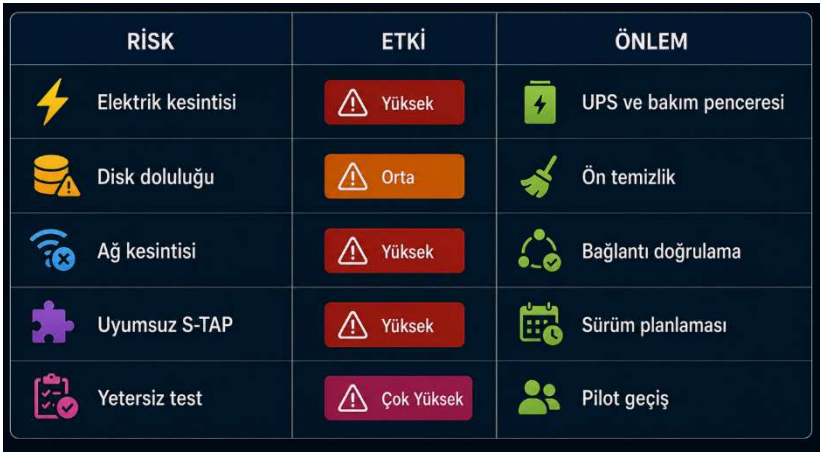
19.3 Upgrade Öncesi Kontrol Listesi

Yükseltme başlamadan önce aşağıdaki kontrollerin yapılması önerilir:

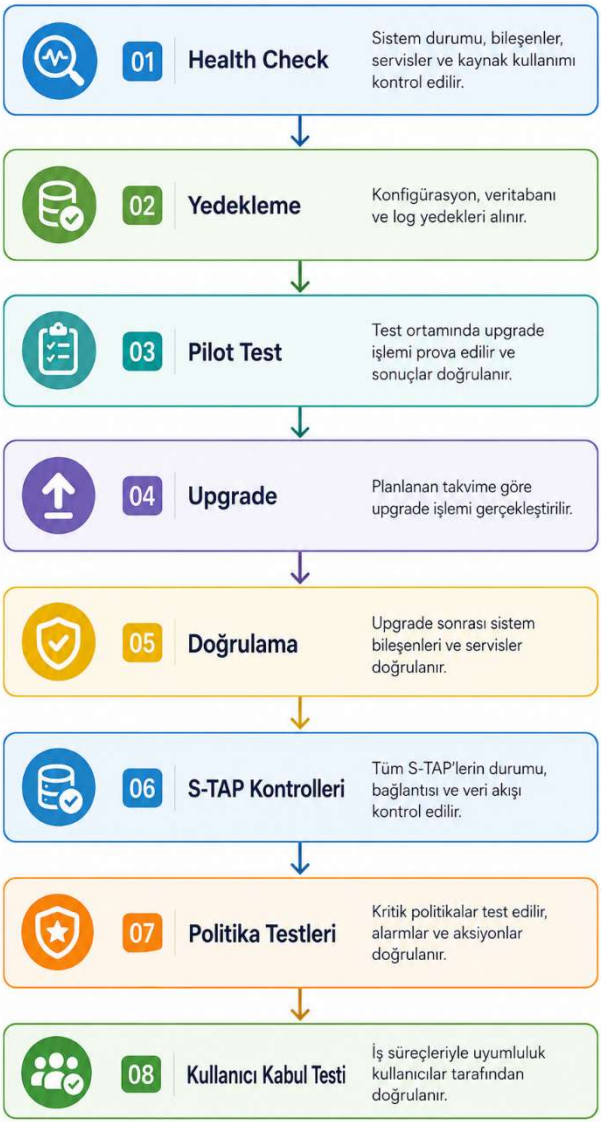
	Kontrol	Durum
1	Desteklenen upgrade yolu doğrulandı	☐
2	Güncel yedek alındı	☐
3	Archive görevleri tamamlandı	☐
4	Kritik raporlar test edildi	☐
5	Boş disk alanı yeterli	☐
6	Lisans bilgileri doğrulandı	☐
7	Health Check tamamlandı	☐
8	Geri dönüş planı hazırlandı	☐

19.4 Risk Analizi

Her upgrade öncesinde aşağıdaki riskler değerlendirilmelidir.



19.5 Önerilen Upgrade Süreci



19.6 Collector Upgrade

Collector yükseltmesi sırasında doğrulanması önerilen başlıklar:

- SQL trafiği devam ediyor mu?
- Politikalar çalışıyor mu?
- Alarmlar oluşuyor mu?
- Archive görevleri başarılı mı?
- Export görevleri çalışıyor mu?
- Disk kullanımı normal mi?

19.7 Aggregator Upgrade

Aggregator yükseltmesi sonrasında:

- Collector bağlantıları
- Raporlar
- Dashboard
- Trend analizleri
- SIEM entegrasyonu
- Kullanıcı rolleri

Tekrar doğrulanmalıdır.

19.8 S-TAP Upgrade

En kritik bileşenlerden biridir.

Kontrol edilmesi önerilen noktalar:

- Desteklenen sürüm

- İşletim sistemi uyumluluğu
- Veritabanı sürümü
- Ağ bağlantısı
- Trafik doğrulaması

Pilot sistemlerde test edilmeden geniş ölçekli dağıtım yapılmaması önerilir.

19.9 Migration Planlaması

Migration projelerinde aşağıdaki bileşenler birlikte değerlendirilmelidir:

- Collector
- Aggregator
- Central Manager (varsa)
- Archive sunucuları
- SFTP altyapısı
- SIEM entegrasyonu
- SMTP yapılandırması
- Sertifikalar
- DNS kayıtları

19.10 Archive Migration

En sık gözden kaçan konulardan biri arşiv altyapısıdır.

Kontrol edilmesi önerilen başlıklar:

- Eski arşivlere erişim
- Dizin yapılarının korunması
- Kimlik doğrulama bilgileri
- Depolama kapasitesi
- Geri yükleme testleri

Migration tamamlandıktan sonra eski arşivlerden örnek veri geri yüklenerek doğrulama yapılması iyi bir uygulamadır.

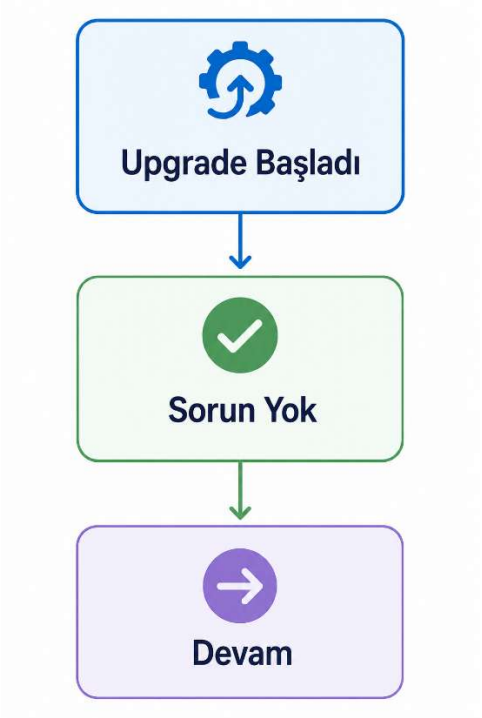
19.11 Upgrade Sonrası Doğrulama

Yükseltme tamamlandıktan sonra aşağıdaki testler yapılmalıdır:

19.12 Rollback Planı

Her yükseltme projesinde geri dönüş planı bulunmalıdır.

Örnek karar noktaları:



veya

Rollback kararı için teknik ve iş birimi temsilcilerinin önceden mutabık kaldığı kriterler belirlenmelidir.

19.13 Sık Yapılan Hatalar

Saha projelerinde tekrar eden bazı hatalar:

- Güncel yedek almadan upgrade başlamak
- Desteklenmeyen sürüm geçişi planlamak
- S-TAP sürümlerini unutmamak yerine gözden kaçırmak
- Bakım penceresini kısa planlamak

- Archive ve Export görevlerini doğrulamamak
- Rollback planı hazırlamamak
- Değişiklik sonrası kullanıcı kabul testlerini atlamak

19.14 Başarı Kriterleri

Bir upgrade projesi aşağıdaki koşullar sağlandığında başarılı kabul edilebilir:

- Planlanan süre içinde tamamlandı.
- Veri kaybı yaşanmadı.
- SQL trafiği kesintisiz izleniyor.
- Tüm politikalar beklenen şekilde çalışıyor.
- Alarm mekanizmaları doğrulandı.
- Raporlama fonksiyonları test edildi.
- SIEM ve diğer entegrasyonlar yeniden doğrulandı.
- Kullanıcı kabul testleri tamamlandı.

Bölüm Sonu Değerlendirmesi

Başarılı bir IBM Guardium upgrade veya migration projesi, yalnızca teknik adımların uygulanmasıyla değil; risk yönetimi, test süreçleri ve geri dönüş planlamasıyla birlikte değerlendirilmelidir. Düzenli bakım, desteklenen sürümlerin kullanılması ve kapsamlı doğrulama testleri, uzun vadeli operasyonel süreklilik açısından kritik öneme sahiptir.

---

20. IBM Guardium ve Regülasyon Uyumluluğu

KVKK • PCI DSS 4.0 • ISO/IEC 27001:2022 • NIST CSF 2.0

20.1 Regülasyonlarda Ortak Beklentiler

Farklı regülasyonlar farklı terminolojiler kullansa da ortak beklentiler büyük ölçüde benzerdir.

IBM Guardium, bu alanların önemli bir bölümünde görünürlük ve kayıt üretme yeteneği sunabilir.

20.2 KVKK Perspektifi

KVKK'nın temel amacı kişisel verilerin hukuka uygun işlenmesi ve korunmasıdır.

IBM Guardium aşağıdaki alanlarda katkı sağlayabilir:

Örnek Denetim Sorusu

Son bir yıl içinde PERSONEL tablosuna kimler erişti?

Bu tür talepler, uygun şekilde yapılandırılmış raporlarla desteklenebilir.

20.3 PCI DSS 4.0

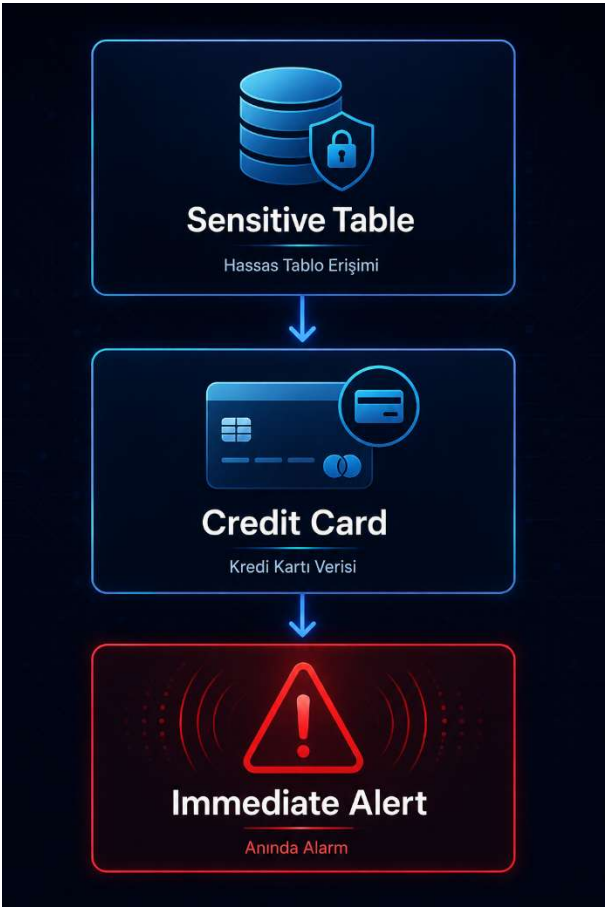
Ödeme kartı verilerini işleyen kurumlar için en önemli gereksinimlerden biri erişimlerin izlenebilir olmasıdır.

IBM Guardium aşağıdaki başlıklarda katkı sağlayabilir:

- Kredi kartı tablolarının izlenmesi

- Ayrıcalıklı kullanıcı aktiviteleri
- Yetki değişiklikleri
- Alarm üretimi
- Denetim kayıtları

Örnek Politika



20.4 ISO/IEC 27001:2022

ISO/IEC 27001 bir yönetim sistemi standardıdır.

Guardium;

Özellikle aşağıdaki teknik kontrollerin uygulanmasına destek olabilir:

- Loglama
- İzleme
- Ayrıcalıklı erişim
- Olay yönetimi
- Denetim kanıtı

Ancak standardın süreç, politika, risk yönetimi ve organizasyonel gereksinimleri farklı kontroller de gerektirir.

20.5 NIST Cybersecurity Framework 2.0

NIST CSF fonksiyonları ile örnek ilişkilendirme:

20.6 Denetim Kanıtları

Bir denetçi aşağıdaki kanıtları talep edebilir:

- Son 12 aylık DBA aktiviteleri
- DROP TABLE işlemleri
- CREATE USER kayıtları
- Maaş verilerine erişimler
- Mesai dışı erişimler
- Kritik alarm geçmişi
- Politika değişiklik kayıtları

IBM Guardium, bu taleplerin önemli bir kısmı için teknik kayıt sağlayabilir.

20.7 Veri Saklama Politikası

Regülasyonlar farklı süreler öngörebilir.

Bu nedenle aşağıdaki konular kurum tarafından belirlenmelidir:

- Saklama süresi
- Arşiv stratejisi
- Geri yükleme prosedürleri
- Purge politikası
- Kanıt bütünlüğü

Bu süreler; yasal gereklilikler, sektör düzenlemeleri ve kurum politikaları doğrultusunda tanımlanmalıdır.

20.8 Politika ve Regülasyon İlişkisi

Bu eşleştirmeler, politika tasarımının denetim gereksinimleriyle ilişkilendirilmesine yardımcı olur.

20.9 Yönetici Gösterge Paneli (Executive Dashboard)

CISO ve üst yönetim için örnek metrikler:

Bu göstergeler teknik ayrıntılardan çok yönetsel karar desteği sağlamayı amaçlar.

20.10 Regülasyonlara Hazırlık İçin Yol Haritası

Bu döngü, sürekli iyileştirme yaklaşımının temelini oluşturur.

20.11 Guardium'un Sınırları

IBM Guardium güçlü bir Database Activity Monitoring çözümüdür; ancak aşağıdaki görevleri tek başına yerine getirmesi beklenmemelidir:

- Kimlik yönetimi (IAM)
- Son kullanıcı cihaz güvenliği (EDR)
- Ağ trafiği analizi (NDR)
- Veri kaybını önleme (DLP)
- Güvenlik bilgi ve olay yönetimi (SIEM)
- Güvenlik orkestrasyonu (SOAR)

En yüksek fayda, Guardium'un bu çözümlerle entegre çalıştığı bütünleşik güvenlik mimarilerinde elde edilir.

20.12 Kurumsal Olgunluk Modeli

IBM Guardium kullanan kurumlar için örnek olgunluk modeli:

Bölüm Sonu Değerlendirmesi

Regülasyonlara uyum, yalnızca teknolojik çözümlerle sağlanabilecek bir hedef değildir. Başarılı bir uyum programı; süreçler, yönetişim, eğitim, risk yönetimi ve teknik kontrollerin birlikte çalışmasını gerektirir. IBM Guardium, veri tabanı katmanındaki görünürlüğü, denetim kayıtları ve politika tabanlı izleme yetenekleriyle bu ekosistemin önemli bileşenlerinden biri olabilir.

---

21. Veri Güvenliğinin Geleceği

Yapay Zekâ Çağında Database Activity Monitoring'in Evrimi

21.1 Yeni Bir Dönemin Başlangıcı

Son yirmi yılda kurumların en değerli varlığı fiziksel altyapıdan dijital verilere doğru kaymıştır.

Artık saldırganların temel hedefi çoğu zaman işletim sistemleri değil; doğrudan **verinin kendisidir**.

Bu değişimle birlikte güvenlik yaklaşımı da dönüşmektedir:

Geçmiş yaklaşım

Yeni yaklaşım

Bu dönüşüm, veri güvenliği çözümlerinin de yalnızca kayıt tutan sistemler olmaktan çıkıp daha akıllı analiz yetenekleri kazanmasını gerektirmektedir.

21.2 Yapay Zekâ Destekli Saldırılar

Üretken yapay zekâ araçlarının yaygınlaşması, saldırganların çalışma yöntemlerini de değiştirmektedir.

Örnek eğilimler:

- Daha ikna edici kimlik avı içerikleri
- Otomatik kod üretimi
- Çok daha hızlı zafiyet araştırmaları
- Sosyal mühendislik senaryolarının ölçeklenmesi
- Komut ve sorguların dinamik olarak oluşturulması

Bu durum, güvenlik ekiplerinin yalnızca imza tabanlı yaklaşımlarla yetinmesini zorlaştırmaktadır.

21.3 Veritabanları Neden Daha Kritik Hale Geliyor?

Bulut, mobil uygulamalar ve yapay zekâ sistemleri büyüdükçe veritabanlarının taşıdığı kritik veri miktarı da artmaktadır.

Özellikle:

- Müşteri bilgileri
- Sağlık verileri
- Finansal kayıtlar
- Kimlik bilgileri
- Yapay zekâ modellerini besleyen veri kümeleri

Kurumların en değerli varlıkları arasında yer almaktadır.

Bu nedenle saldırganlar için nihai hedef çoğu zaman veritabanlarıdır.

21.4 Zero Trust ve Veri Katmanı

Zero Trust yaklaşımı artık yalnızca ağ erişimini değil, veri erişimini de kapsamaktadır.

Temel prensip:

"Hiçbir kullanıcıya veya uygulamaya varsayılan olarak güvenme; her erişimi doğrula."

Bu yaklaşım kapsamında:

- Kim erişiyor?
- Nereden erişiyor?
- Ne zaman erişiyor?
- Hangi veriye erişiyor?
- Bu davranış normal mi?

Sorularına sürekli cevap aranır.

IBM Guardium gibi çözümler, veritabanı katmanındaki görünürlüğü artırarak bu yaklaşımı destekleyebilir.

21.5 Davranış Analitiği (UEBA)

Geleneksel güvenlik ürünleri çoğu zaman "ne oldu?" sorusuna cevap verir.

Davranış analitiği ise şu soruyu sorar:

"Bu kullanıcı normal davranışının dışında mı hareket ediyor?"

Örnek göstergeler:

- İlk kez farklı bir ülkeden bağlantı
- Gece saatlerinde yüksek hacimli sorgular
- Alışılmadık istemci uygulamaları
- Beklenmedik tablo erişimleri

Bu tür analizler, özellikle içeriden gelen tehditlerin tespitinde değerli olabilir.

21.6 Yapay Zekâ Destekli Güvenlik Operasyonları

Gelecekte güvenlik operasyon merkezlerinde (SOC) yapay zekâ destekli yardımcı sistemlerin daha fazla kullanılması beklenmektedir.

Örneğin:

- Alarm önceliklendirme
- Olay özetleme
- İlk analiz raporlarının hazırlanması
- Korelasyon önerileri
- Benzer olayların eşleştirilmesi

Bu tür sistemler, analistlerin karar verme sürecini hızlandırabilir; ancak nihai değerlendirme ve aksiyon yine insan uzmanlar tarafından verilmelidir.

21.7 Çoklu Bulut (Multi-Cloud) Ortamları

Kurumlar artık tek bir veri merkezinde çalışmıyor.

Yaygın mimariler:

- Şirket içi veritabanları
- Genel bulut hizmetleri
- Özel bulut
- Hibrit mimariler

Bu çeşitlilik, görünürlüğün ve politika yönetiminin merkezi şekilde ele alınmasını daha önemli hâle getiriyor.

21.8 Otonom Güvenlik Yaklaşımı

Gelecekte bazı güvenlik süreçlerinin otomatik olarak yürütülmesi beklenmektedir.

Örneğin:

Bu tür otomasyonlar müdahale süresini azaltabilir. Ancak otomatik aksiyonların yanlış pozitif üretme riski göz önünde bulundurularak dikkatli tasarlanması gerekir.

21.9 Kuantum Bilişim ve Veri Güvenliği

Kuantum bilişim, uzun vadede kriptografik yöntemleri etkileyebilecek bir teknoloji olarak değerlendirilmektedir.

Bugün için veritabanı güvenliği üzerindeki doğrudan etkisi sınırlı olsa da;

- Uzun süre saklanacak hassas veriler,
- Kriptografik anahtar yönetimi,
- Gelecekteki şifreleme standartları

Kurumların stratejik planlamasında yer almaya başlamıştır.

21.10 Geleceğin Database Activity Monitoring Çözümleri

Önümüzdeki yıllarda DAM çözümlerinde şu eğilimlerin öne çıkması beklenmektedir:

- Yapay zekâ destekli anomali tespiti
- Risk puanlaması
- Davranış tabanlı alarm üretimi
- Bulut yerel mimarilerle entegrasyon
- Daha kapsamlı API entegrasyonları
- Otomatik politika önerileri
- Gelişmiş görselleştirme ve analitik

Bu gelişmeler, operasyon ekiplerinin daha hızlı ve daha bağlamsal kararlar almasına yardımcı olabilir.

21.11 Kurumlara Stratejik Öneriler

Veri güvenliği yatırımlarını planlayan kurumlar için öneriler:

1. Veriyi sınıflandırmadan güvenlik projesine başlamayın.
2. Kritik veritabanlarını önceliklendirin.
3. Politika sayısını değil, etkinliğini ölçün.
4. Düzenli Health Check süreçleri oluşturun.
5. Arşiv ve geri yükleme testlerini ihmal etmeyin.
6. Guardium'u SIEM, SOAR ve kimlik yönetimi çözümleriyle entegre değerlendirin.
7. Yapay zekâ destekli araçları analistlerin yerine değil, onları desteklemek için kullanın.
8. Güvenlik metriklerini yönetim seviyesinde düzenli olarak raporlayın.
9. Bulut ve hibrit mimariler için veri görünürlüğünü koruyun.
10. Sürekli iyileştirme yaklaşımını benimseyin.

21.12 Sonuç

Veri güvenliği artık yalnızca bilgi işlem ekiplerinin teknik bir konusu değildir. Kurumların itibarı, yasal yükümlülükleri, müşteri güveni ve operasyonel sürekliliği doğrudan verinin korunmasına bağlıdır.

IBM Guardium gibi Database Activity Monitoring çözümleri, veritabanı katmanında görünürlük sağlayarak bu hedefe katkıda bulunur. Bununla birlikte, etkili bir veri güvenliği programı; doğru süreçler, eğitimli ekipler, düzenli denetimler ve diğer güvenlik kontrolleriyle birlikte ele alınmalıdır.

Önümüzdeki yıllarda yapay zekâ, otomasyon ve davranış analitiği güvenlik operasyonlarının ayrılmaz bir parçası hâline gelecektir. Bu dönüşüme hazırlıklı olan kurumlar, yalnızca tehditlere daha hızlı yanıt vermekle kalmayacak; aynı zamanda veri güvenliğini stratejik bir rekabet avantajına dönüştürebilecektir.

Kaynakça

IBM Dokümantasyonu

1. IBM. *IBM Guardium Documentation*. IBM Documentation Portal.
2. IBM. *IBM Guardium Data Protection Knowledge Center*.
3. IBM. *IBM Security Guardium Data Protection Administration Guide*.
4. IBM. *IBM Security Guardium Data Protection Installation Guide*.
5. IBM. *IBM Security Guardium Data Protection Configuration Guide*.
6. IBM. *IBM Security Guardium Data Protection CLI Reference*.
7. IBM. *IBM Security Guardium Best Practices Guide*.
8. IBM. *IBM Guardium Vulnerability Assessment User Guide*.
9. IBM. *IBM Guardium Data Discovery and Classification Guide*.
10. IBM. *IBM Security Guardium Release Notes*.
11. IBM. *IBM Security Guardium Fix Central Release Documentation*.
12. IBM. *IBM Guardium Performance and Scalability Best Practices*.
13. IBM. *IBM Security Support Documentation*.
14. IBM. *IBM Guardium Technical Notes*.
15. IBM. *IBM Redbooks – Security and Data Protection*.

IBM Redbooks

16. IBM Redbooks. *Security Intelligence with IBM Security Solutions*.
17. IBM Redbooks. *IBM Security Solutions Architecture*.
18. IBM Redbooks. *Enterprise Security Architecture Using IBM Technologies*.
19. IBM Redbooks. *Cloud Security with IBM Solutions*.
20. IBM Redbooks. *Data Protection Best Practices*.

NIST Yayınları

21. National Institute of Standards and Technology (NIST). *Cybersecurity Framework (CSF) 2.0*.
22. NIST Special Publication 800-53 Rev. 5. *Security and Privacy Controls for Information Systems and Organizations*.
23. NIST Special Publication 800-61 Rev. 2. *Computer Security Incident Handling Guide*.
24. NIST Special Publication 800-137. *Information Security Continuous Monitoring (ISCM)*.
25. NIST Special Publication 800-207. *Zero Trust Architecture*.
26. NIST Special Publication 800-92. *Guide to Computer Security Log Management*.

MITRE

27. MITRE Corporation. *MITRE ATT&CK Framework*.
28. MITRE. *ATT&CK for Enterprise*.
29. MITRE. *ATT&CK Evaluations*.
30. MITRE. *D3FEND Knowledge Graph*.

PCI Security Standards Council

31. PCI Security Standards Council. *PCI DSS Version 4.0*.
32. PCI Security Standards Council. *PCI DSS Quick Reference Guide*.
33. PCI Security Standards Council. *Information Supplements and Guidance Documents*.

ISO Standartları

34. ISO/IEC 27001:2022. *Information Security Management Systems – Requirements*.
35. ISO/IEC 27002:2022. *Information Security Controls*.
36. ISO/IEC 27005. *Information Security Risk Management*.
37. ISO/IEC 27701. *Privacy Information Management*.
38. ISO/IEC 27035. *Information Security Incident Management*.

Türkiye'deki Düzenlemeler

39. T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. *Bilgi ve İletişim Güvenliği Rehberi*.
40. Kişisel Verileri Koruma Kurumu (KVKK). *6698 Sayılı Kişisel Verilerin Korunması Kanunu*.
41. Kişisel Verileri Koruma Kurumu. *Kişisel Veri Güvenliği Rehberi*.
42. Bankacılık Düzenleme ve Denetleme Kurumu (BDDK). Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Yönetmeliği.

43. MASAK mevzuatı ve ilgili rehber dokümanları (gerektiğinde ilgili sürümler esas alınmalıdır).

CIS

44. Center for Internet Security. *CIS Critical Security Controls v8*.
45. CIS Benchmarks.

OWASP

46. OWASP Foundation. *OWASP Top 10*.
47. OWASP Foundation. *Application Security Verification Standard (ASVS)*.
48. OWASP Foundation. *Database Security Cheat Sheet*.

ENISA

49. European Union Agency for Cybersecurity (ENISA). *Threat Landscape Reports*.
50. ENISA. *Guidelines for Incident Reporting*.

Gartner ve Sektör Araştırmaları

51. Gartner. Veri güvenliği ve güvenlik operasyonları alanındaki ilgili araştırma raporları.
52. IDC. Veri güvenliği ve veri koruma teknolojileri üzerine sektör analizleri.
53. Forrester Research. Güvenlik operasyonları ve veri güvenliği raporları.

Akademik Kaynaklar

54. Stallings, W. *Network Security Essentials*.
55. Stallings, W. *Cryptography and Network Security*.
56. Bishop, M. *Computer Security: Art and Science*.
57. Anderson, R. *Security Engineering*.
58. Ross, S. *Database Systems Concepts*.
59. Silberschatz, A., Korth, H. F., & Sudarshan, S. *Database System Concepts*.

Olay Müdahalesi ve Adli Bilişim

60. Casey, E. *Digital Evidence and Computer Crime*.
61. Carrier, B. *File System Forensic Analysis*.
62. Mandia, K., Prosise, C., & Pepe, M. *Incident Response and Computer Forensics*.

Güvenlik Organizasyonları

63. ISACA. *COBIT 2019 Framework*.
64. ISACA. *CISA Review Manual*.
65. (ISC)². *Official CISSP Common Body of Knowledge (CBK)*.
66. SANS Institute. Güvenlik farkındalığı, olay müdahalesi ve log yönetimi üzerine teknik makaleler.
67. Cloud Security Alliance (CSA). Bulut veri güvenliği ve yönetişim rehberleri.