

DAM Ekibi İçin Kılavuz: SQL Change Guard Bağlantılarını Tanıtma

Bu belge, veritabanı etkinlik izleme (DAM) ve SIEM yöneten ekip içindir. Amaç, SQL Change Guard'ın hedef veritabanlarındaki bağlantılarının "tanınmayan kaynak" diye alarm üretmemesi ve ürünün dışından gelen erişimin ayırt edilebilmesidir.

1. Ne yapılacak, kısaca

SQL Change Guard, onaylı değişiklikleri ve sorgu sonuçlarını hedef veritabanında çalıştırır. Bu bağlantılar iki makineden gelir: Worker makinesi ve API makinesi. DAM tarafında bu iki makinenin adresi, ürünün veritabanı hesabıyla birlikte izin listesine alınır.

Bu belgedeki adımlar tamamlandığında şu soru cevaplanabilir olur: "Bu oturum SQL Change Guard'ın işi mi, yoksa ürünün dışından mı geldi?"

2. Başlamadan önce kurum yetkilisinden alınacak bilgiler

- SQL Change Guard'a erişimi olan bir kullanıcı (Auditor, DbAdmin, ChangeManager ya da SystemManager rolü).
- İzlenen hedef veritabanı sunucularının listesi.
- Worker ve API'nin hangi makinede çalıştığı.

3. Adım adım

1. SQL Change Guard web arayüzüne girin. Raporlar menüsünde Access & Authorization grubundaki "Expected Access Principals" raporunu açın.
2. Tarih aralığını son 30 günü kapsayacak şekilde seçip raporu çalıştırın. Rapor, kayıtlı her hedef sunucu için bir satır verir. Hiç iş yapılmamış sunucu da listelenir (pencere sayısı 0).
3. Her sunucu satırından şu bilgileri alın: Sunucu adı (ServerName), Ürünün hesabı (ProductLogin), Görülen iş türleri (SeenRoles), Makine adları (SeenHosts), Hedefin gördüğü istemci adresleri (SeenClientAddresses). Birden fazla değer noktalı virgül ile ayrılır. Raporla parola yoktur.
4. DAM kuralına her sunucu için şu iki bilgiyi birlikte ekleyin: ürünün hesabı ve ürünün adresleri. Yalnız adres ya da yalnız hesap eklemeyin. İkisi birlikte tutuyorsa oturum ürünün işidir.
5. API makinesinin adresini ayrıca alın (aşağıda bölüm 4). Bu adres raporda görünmez.
6. Kuralı sınavın (aşağıda bölüm 6) ve sonucu kurum yetkilisine bildirin.

7. Kurum yetkilisi, SQL Change Guard'da Ayarlar > Parametreler > External Controls grubunda "DamAllowlistMaintained" deęerini "Yes" yapar. Kurum DAM kullanmıyorsa "NotUsed" seilir.

4. API makinesinin adresi nasıl ğrenilir

Rapor yalnız Worker'ın yrttę iřlerden trer. API makinesi nesne tanımlarını okur, kolon nizlemesi alır ve "baęlantıyı dene" iřlemini yapar. Bu baęlantılar deęiřiklik komutu alıřtırmaz ve rapora girmez. Adresi řyle ğrenin:

8. API makinesinde SQL Change Guard'da Ayarlar > Sunucular ekranından bir sunucu iin "baęlantıyı dene" iřlemini yapın.
9. Hedef sunucuda oturum adı "SQL Change Guard/Test" olan oturumu bulun. Sorgular blm 5'tedir. İstemci adresi stunu, API makinesinin hedefin gzndeki adresidir.

Makinenin kendi aę ayarındaki adresi deęil, hedef sunucunun grdę adres kullanılmalıdır. Aę adres evirisi (NAT), VPN ya da bulut hizmetinin n katmanı yznden ikisi farklı olabilir.

5. Hedefte oturumu grme sorguları

Baęlantılar řu adla aılır: SQL Change Guard/<Rol>/<Numara>. rnek: SQL Change Guard/Execute/123.

Rol	Ne zaman	Havuz	Pencere aar mı
Execute	Deęiřiklik talebi alıřırken	Kapalı	Evet
Query	Sorgu sonucu talebi, sunucu bařına	Kapalı	Evet
Release	Srm paketi, tek baęlantı kipi	Kapalı	Evet
Sandbox, SandboxRelease	İzole deneme	Kapalı	Evet
Health	Baęlantı saęlık kontrol (Worker)	Aık	Hayır
Preview, Definition, Test	nizleme, tanım okuma, baęlantı deneme	Aık	Hayır

Havuz aık olan roller (Health, Preview, Definition, Test) bořta bir oturumu bir sre aık tutar. Bu normal bir davranıřtır ve bu baęlantılar betik alıřtırmaz.

SQL Server:

```
SELECT es.session_id, es.program_name, es.host_name, es.login_name, c.client_net_address
```

```
FROM sys.dm_exec_sessions es
LEFT JOIN sys.dm_exec_connections c ON c.session_id = es.session_id
WHERE es.program_name LIKE N'SQL Change Guard%';
```

PostgreSQL:

```
SELECT pid, application_name, client_addr, username, state
FROM pg_stat_activity
WHERE application_name LIKE 'SQL Change Guard%';
```

Oracle:

```
SELECT sid, serial#, auidsid, username, machine, module, action, client_identifier
FROM v$session
WHERE module LIKE 'SQL Change Guard%' OR client_identifier LIKE 'SQL Change Guard%';
```

Aynı makinede çalışan bir kurulumda SQL Server adres yerine "<local machine>" yazabilir. Bu beklenen bir durumdur.

6. Kuralı doğrulama

SQL Change Guard her yürütmeye denetim kaydına bir "başladı" ve bir "bitti" olayı yazar. Bu olaylar SIEM'e de gider. Bir olayda şu alanlar bulunur: windowKind (iş türü), serverName, executionLogin (hesap), executorHost (makine), clientAddress (hedefin gördüğü adres), targetSessionId (oturum numarası), sessionApplicationName (oturum adı), executionStartedAt ve executionFinishedAt (UTC). Başlangıç olayında talebin ITSM kaydı da bulunur: changeTicket (örnek CHG0030001) ve acil talepte emergencyTicket (örnek INC0012345). Böylece DAM kaydındaki oturum, pencere üzerinden doğrudan ITSM kaydına bağlanır. Bitiş olayında windowId, başlangıç olayının numarasıdır ve sonuç windowOutcome alanındadır: executed, failed, cancelled, rolledBack ya da abandoned.

Sınama için:

10. Kurum yetkilisinden, hedef sunucuda küçük bir değişiklik talebi (örneğin bir test tablosuna bir satır ekleme) çalıştırmasını isteyin.
11. DAM kaydında o anda ürünün hesabıyla, ürünün adresinden gelen oturumu bulun.
12. Oturum numarasının ve zamanın SQL Change Guard'ın başlangıç ve bitiş olayıyla tuttuğunu kontrol edin.
13. Kural bu oturumu "ürünün işi" saymalı, alarm üretmemelidir.
14. Ürünün hesabıyla ama ürünün adresi dışında bir yerden aynı hesapla bir oturum açıldığında alarm üretildiğini de deneyin.

7. SIEM için yedi örnek kural

Aşağıdaki kurallar satıcıdan bağımsız yazılmıştır. Kendi SIEM ürününüzün diline çevrilir. Mantık şudur: hedef sunucudaki bir oturum, ürünün bir penceresinin içinde, ürünün hesabıyla, beklenen

adresten ve aynı oturum numarasıyla görünüyorsa eşleşmiştir. Eşleşmeyen oturum alarm adayıdır.

K1 ila K7 kuralları değişiklik komutlarına bakar. Okuma için ayrı üç kural vardır (R1 ila R3, aşağıda) ve yalnız ürünün hesabıyla yapılan okumaları (SELECT) kapsar. Kurumdaki diğer hesapların okuma izlemesi kurumun kendi politikasıdır. Health, Preview, Definition ve Test bağlantıları değişiklik komutu çalıştırmaz ve pencere açmaz.

Ön koşullar:

- İzin listesi: ürünün hesabı ve adresleri "Expected Access Principals" raporundan, API makinesinin adresi elle, kurumun diğer hesapları kurumdan.
- SIEM gönderim eşiği (SiemMinSeverity) Notice ya da altında olmalı ve Denetim (Audit) akışı açık olmalı. Pencere olayları Notice ciddiyetindedir.
- DAM, veritabanı sunucusu, ürünün makineleri ve SIEM aynı saat kaynağını kullanmalı.
- Pencere tablosu: SIEM, başlangıç olaylarını olay numarasıyla (windowId) bir tabloya yazar. Bitiş olayı gelince aynı satırı kapatır. Kurallar bu tabloya bakar.
- "Olay yok" diyen kurallar (K2 ve K5) olayın kendi zamanına (occurredAt) bakmalı ve birkaç dakika gecikmeli değerlendirilmelidir. Toplayıcı kesintisinde olaylar birikir, varış zamanına bakmak alarm yağmuru üretir.

No	Kural	Mantık	Ne yakalar
K1	İzinsiz hesapla değişiklik	Üretim sunucusunda değişiklik komutu ve hesap izin listesinde yok	Doğrudan erişim, paylaşılan hesap
K2	Pencere yokken ürün hesabı	Ürün hesabıyla değişiklik komutu ve o sunucuda o an açık pencere yok	Ürün parolasının başka yerde kullanılması
K3	Yabancı adresten ürün	Ürün hesabıyla ya da ürün adıyla oturum ve istemci adresi ürünün adres listesinde yok	Ad, makine adı ve hesap taklidi
K4	Talep numarası uyuşmazlığı	Oturum adındaki numara, o sunucuda o an açık pencerenin numarasından (talep ya da paket) farklı	Başka talebin adıyla çalışma
K5	Kapanmayan pencere	Başlangıç var, belirli süre içinde aynı windowId ile bitiş yok. Süre, çökme kurtarma eşiği (varsayılan 120 dakika) ile en uzun sorgu zaman aşımının (MaxQueryTimeout, varsayılan 3600 saniye) toplamından büyük olmalı. Önerilen: 4 saat	Worker'ın dönmediği çökme, takılan iş
K6	Gözden geçirilmeyen acil değişiklik	ChangeRequest.Executed olayında isEmergency doğru ve 24 saat içinde ChangeRequest.EmergencyReviewed yok	Kapanmayan acil iş

K7	Pencere içinde başka oturum	Açık pencere içinde, ürün hesabıyla, pencerenin targetSessionId değerinden farklı oturumdan değişiklik komutu	Pencere sürerken hesabı ikinci oturumdan kullanan
-----------	-----------------------------	---	---

Okuma kuralları (sorgu sonucu talepleri): sorgu sonucu talebi her hedef sunucuda ayrı bir Query penceresi açar. Okuma hedefte bir işlem içinde yapılır ve commit edilmeden geri alınır; pencere olayları bu okumalar için de yazılır.

No	Kural	Mantık	Ne yakalar
R1	Pencere yokken ürün hesabıyla okuma	Ürünün hesabıyla SELECT ve o sunucuda o an açık pencere yok (ad pencere açmayan bir ürün rolü değilse)	Ürünün parolasıyla veri okuma
R2	Pencere içinde başka oturumdan okuma	Açık Query penceresi sürerken ürünün hesabıyla farklı oturumdan SELECT	Pencere sürerken hesabı ikinci oturumdan kullanan
R3	Sorgu penceresi var, DAM okuma kaydı yok	Query penceresi executed ile kapandı ve DAM o aralıkta hiç SELECT görmedi	DAM'in okuma izleme boşluğu

Health, Preview, Definition ve Test bağlantıları da okuma yapar ama pencere açmaz. Bunlara R1 alarmı vermemek için "ürünün hesabı, ürünün adresi ve bu rol adlarından biri" izin kuralı yazılır. Ad taklit edilebildiği için bu izin yalnız ürünün (API ve Worker) adreslerinden gelen okumalara verilmelidir. Denetçi için okuma kanıtı ürünün kendisinde de vardır: Query Result Activity, Masking Activity ve Data Access and Export Log raporları ile denetim dosyasının sorgu sonucu bölümü.

Doğrulanamayan pencere: başlangıç olayında targetSessionId ya da clientAddress boşsa (oturum bilgisi okunamadıysa) K3 ve K7 o pencere için değerlendirilemez. Bunu ayrı bir bilgi satırı olarak gösterin.

Sınır: Ürünün hesabını kullanabilecek kişiler API makinesinin yöneticisi, Worker makinesinin yöneticisi ve Worker erişim anahtarını ele geçiren kişidir. Pencerenin dışında değişiklik yaparsa K2, başka adresten bağlanırsa K3, pencerenin içinde başka oturumdan yaparsa K7 yakalar. Ürünün kendi sürecine girip komutu ürünün oturumundan gönderen kişiyi hiçbir kural yakalamaz. Bu yüzden API ve Worker makinelerinin erişimi ayrıca izlenmelidir.

8. Dikkat edilmesi gereken kurallar

- Uygulama adı bir etikettir. İstemci bunu kendisi söyler, biri aynı adı kendi bağlantısına verebilir. Adı tek başına kanıt saymayın. Hesap, hedefin gördüğü adres, oturum numarası ve olayın zaman aralığı birlikte aranmalıdır.
- Ürünün SQL hesabı yalnız bu ürüne ait olmalıdır: kişisel kullanıma verilmez, parolası kasadadır, başka bir uygulamada kullanılmaz. Hesap ortaksa ürünün işi ile diğer işler ayırt edilemez. Kurum yetkilisi bunu "TargetAccountDedicated" beyanıyla kaydeder.
- Hesap adında "token", "secret" ya da "password" kelimeleri geçmemelidir. SIEM'e giderken bu tür değerler maskelenir.
- Bulut ya da vekil/yük dengeleyici arkasındaki bir veritabanında hedefin gördüğü adres, ürünün makinesinin gerçek adresi yerine ara katmanın adresi olabilir. Bu durumda adresi tek başına kanıt saymayın. Hesap, oturum numarası ve zaman aralığı yine kullanılabilir.
- SIEM'e giden pencere olayları "Notice" ciddiyetindedir. SIEM tarafında gönderim eşiği Notice'in üstündeyse ya da Denetim akışı kapalıysa bu olaylar gelmez. Kurum yetkilisi bunu Yönetişim Kurulum Kontrolü ekranından görür.
- Bir pencerenin bitiş olayı yazılamazsa ya da süreç çökerse, o pencere sonradan "abandoned" ile kapatılır. Gerçek sonuç talep kaydındadır.
- Oracle kullanan kurumlarda targetAuditSessionId alanı CEF biçiminde taşınmaz; JSON, RFC 5424 ya da LEEF biçimi önerilir. CEF'te bilete cs3 (changeTicket), olay kaydı flexString1 (emergencyTicket), paketin talep listesi flexString2 (requestIds) alanındadır.

9. Adresler değişirse

Worker ya da API başka bir makineye taşınırsa, ağ yapısı değişirse ya da veritabanı farklı bir ağa alınırsa izin listesi güncellenmelidir. Yeni adresleri her seferinde yukarıdaki rapordan alın, tahmin etmeyin.