VERİ SAYFASI

One Identity Safeguard for Privileged Analytics

Ayrıcalıklı erişim ile ilgili güvenlik ihlallerini algılar ve önler

Avantajlar

- Kullanıcı etkinliğini izleyerek ve görselleştirerek BT sisteminizde neler olup bittiğini anlama imkânı sağlar
- Tuş darbesi dinamikleri ve fare hareketlerinin sabit analizi üzerinden sürekli kimlik doğrulama
- Makine öğrenmesiyle temel faaliyetten olağandışı sapmaları tespit eder
- Bağlamsal bilgiler ve kaydedilmiş oturumların riske dayalı önceliklendirilmesini içeren bir güvenlik olayının tespit edilme süresini kısaltır
- Güvenlik uyarılarının yarattığı gürültüyü azaltır, böylece gerçekten önemli olan şeye odaklanılabilir
- Potansiyel olarak zararlı faaliyetler hakkında bir uyarı verildiğinde herhangi bir bağlantıyı sonlandırarak güvenliği artırır

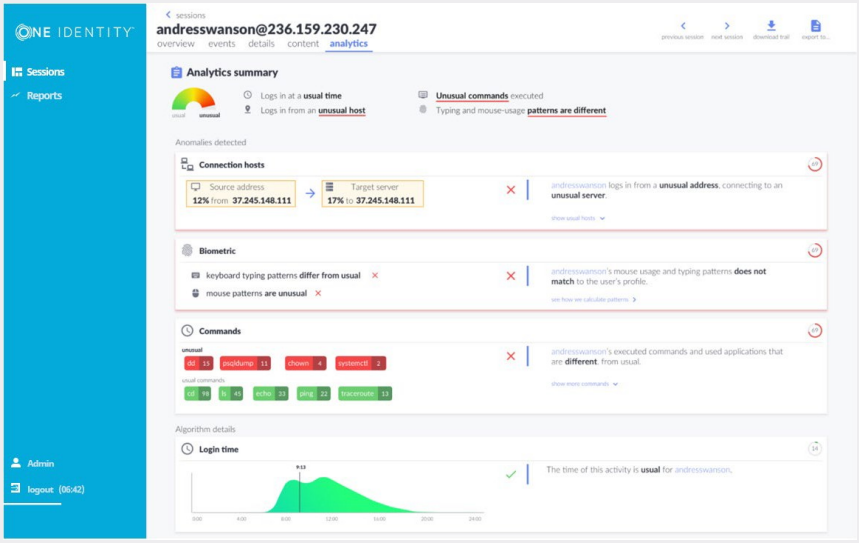
Genel Bakış

Bir BT güvenlik yöneticisi, şirketinin asla ayrıcalıklı bir hesap ihlali yaşamayacağını düşünmekten çok daha fazlasını yapmalıdır. Bugün, herhangi bir kurumun ihlali tespit etmesi ortalama olarak 206 gün sürer. Vakit nakittir ve risktir. Bu nedenle, ihlal ister ele geçirilmiş ayrıcalıklı bir hesaptan ister dolandırıcı bir yönetici tarafından yapılmış olsun, ne kadar uzun süre keşfedilmezse, içeri giren kişilerin verileri bulmaya ve çalmaya zamanı o kadar fazla olur. Aynı şekilde para cezaları ve ilave adli harcamalar da üst üste birikecek zamanı bulur.

Kuruluşlar zaman zaman güvenilir yöneticilerinden farklı kişilere ayrıcalıklı erişim sağlamak zorunda kalırlar. Dünyanın herhangi bir yerinden çalışan harici danışmanlardan dış kaynaklı yöneticileri sürece dahil etmek için genişlemek zorunda da kalabilirler. Peki ama kuruluşlar, ayrıcalıklı erişimi olan yöneticilerin onu kötü amaçlarla değil, iyi amaçlarla kullanacağından nasıl emin olabilirler?

“One Identity Safeguard for Privileged Analytics” ile en riskli kullanıcıların kim olduğunu bilinir, yeni iç ve dış tehditler sürekli gözetim altında tutulur ve olağandışı ayrıcalıklı davranışlar tespit edilebilir. Bu güçlü çözüm, kuruluşların ayrıcalıklı kullanıcılarını ve onların etkinliklerini tam olarak görmesini sağlar ve bir sorun varsa, derhal harekete geçilebilir ve veri ihlallerinin önlenmesi için iyi bir pozisyon alınabilir.

[1] Ponemon’un 2017 Veri İhlali Maliyeti Çalışması



Riskli kullanıcıların ve davranışların kolayca belirlenmesi

Analiz özeti görüntülemeyle bir kullanıcının etkinliğinin olağandışı ve potansiyel olarak riskli olup olmadığını hızlı bir şekilde görür. Sıra dışı komutların, biyometrik aktivitenin ve bağlantı sunucularının bir özetini içerir.

Özellikler

Riskli kullanıcıların belirlenmesi

Privileged Analytics yüksek riskli hesapları tespit etmek için yetkilendirmeleri risk sınıflandırma kurallarına göre değerlendirir. Yetkilendirmelerdeki değişiklikler bir kullanıcının profilini yüksek riskli bir duruma getirdiğinde proaktif bildirimler gönderilir. Bu, birisi onları kötüye kullanmadan veya sömürmeden önce, gereksiz ya da faal olmayan yetkilendirmelerden kaynaklanan riski ortadan kaldırır.

Bilinmeyen tehditlerin gerçek zamanlı olarak tespit edilmesi

Kurallara dayalı güvenlik, yeni harici saldırı yöntemlerini veya kuruluşun içerisindeki kötü niyetli kişileri tespit edemez. “Safeguard for Privileged Analytics”, BT ortamında neler olup bittiğini daha iyi anlamak için kullanıcı aktivitesini gerçek zamanlı olarak izler ve görselleştirir. Önceden tanımlanmış korelasyon kuralları gerektirmez; sadece mevcut oturum verileriyle çalışır.

Örüntüsüz işlem

“Yanlış bilinen” davranışı saptamak için örüntüye dayalı eşleme kullanmak yerine - ki bu genellikle doğru değildir - "Safeguard for Privileged Analytics", BT ortamından toplanan verileri kullanır. “Normal” davranışın temelini oluşturur ve çeşitli makine öğrenme algoritmalarını kullanarak sapmaları tespit eder.

Ekran içeriği analizi

Ayrıcalıklı oturumların ekran içeriğini analiz ederek ve verilen komutları ve pencere başlıklarını anlayarak, "Safeguard for Privileged Analytics", ayrıcalıklı kullanıcıların düzenli olarak kullandıkları komutların ve uygulamaların temel davranış profilini zenginleştirebilir. Bu ayrıntılı analiz, tipik davranışların tanımlanmasını ve ayrıcalıklı kimlik hırsızlıklarının tespit edilmesini kolaylaştırır.

Davranışsal biyometri

Her kullanıcı, fareyi hareket ettirme veya yazı yazma gibi işlemleri gerçekleştirirken bile, kendine has davranış biçimleri sergiler. "Safeguard for Privileged Analytics" içine yerleştirilen algoritmalar, "Safeguard for Privileged Sessions" tarafından ele geçirilen bu davranış özelliklerini inceler. Tuş darbesi dinamikleri ve fare hareketi analizi yalnızca ihlallerin belirlenmesine yardımcı olmakla kalmaz, aynı zamanda sürekli bir biyometrik kimlik doğrulama işlevi görür.

Uyarı sesinin azaltılması

“Privileged Analytics”, kullanıcı olaylarını risk ve sapma seviyelerine göre kategorize ederek ve en şüpheli olayları vurgulayarak SIEM'ler tarafından oluşturulan uyarı sesini azaltır. Uyarılar SIEM'lere gönderilebilir veya güvenlik analistleri sezgisel kullanıcı ara yüzünde öncelikli olayların listesini görüntüleyerek en önemli olanlarına odaklanılmasını sağlayabilir.

Otomatik müdahale

Çoğu saldırı senaryosunda, yüksek etkiye sahip olaylar genellikle keşif aşamasından önce meydana gelir. Bu nedenle, bu aşamada tespit ve müdahale, zarar verici aktivitenin önlenmesi için kritik öneme sahiptir. "Safeguard for Privileged Sessions" ile sorunsuz entegrasyon, şüpheli bir olay gerçekleştiğinde veya kötü amaçlı davranış algılandığında otomatik oturumun sonlandırılmasını sağlar.

Profelis Hakkında

Profelis Bilişim ve Danışmanlık, kadrosunda bulunan sertifikalı mühendisleri ile One Identity bünyesindeki ürünlerinin desteğini ve danışmanlığını sunmaktadır. Detaylı bilgi için bizimle iletişime geçebilirsiniz.

Profelis Bilişim ve Danışmanlık Tic. ve San. A.Ş.
Vali Dr. Reşit Sokak No:6/1 Çankaya - Ankara
Telefon: +90 312 482 8021
Faks: +90 312 482 8040
bilgi@profelis.com.tr
www.profelis.com.tr