



CereAI XDR platformu: Raporlama ve analiz yetenekleri

CereAI XDR, güvenlik tehditlerini etkili bir şekilde yönetmek ve bunlara yanıt vermek için gereken içgörülerle güvenlik ekiplerini güçlendirmek üzere tasarlanmış güçlü raporlama ve analiz yetenekleri sunar. Platform tarafından sağlanan temel raporlama ve analiz özelliklerinden bazıları şunlardır:

Gerçek Zamanlı Kontrol Panelleri

CereAI XDR, kuruluşunuzun güvenlik durumuna bir bakışta genel bakış sağlayan sezgisel, gerçek zamanlı kontrol panelleri içerir. Bu kontrol panelleri, tehdit algılamaları, sistem sağlığı ve kullanıcı etkinlikleri gibi temel ölçümleri ve göstergeleri görüntüleyerek güvenlik ekiplerinin mevcut güvenlik durumunu hızlı bir şekilde değerlendirmesine ve acil müdahale gerektiren alanları belirlemesine olanak tanır.

Detaylı Olay Raporları

Platform, tespit edilen tehditlerin niteliğini, kapsamını ve etkisini ayrıntılarıyla anlatan kapsamlı olay raporları oluşturur. Bu raporlar, tehdidin kaynağı, etkilenen sistemler ve sorunu azaltmak için atılan adımlar gibi bilgileri içerir. Bu ayrıntılı belgeler, olay sonrası analize ve güvenlik politikaları ile müdahale stratejilerinin geliştirilmesine yardımcı olur.

Özelleştirilebilir Uyarılar

CereAI XDR'nin uyarı sistemi son derece özelleştirilebilir ve güvenlik ekiplerinin uyarı oluşturmak için belirli kriterleri tanımlamasına olanak tanır. Uyarılar; şiddet, tehdit türü ve etkilenen sistemler gibi çeşitli faktörlere göre yapılandırılabilir. Bu, daha az önemli olaylardan kaynaklanan gürültüyü en aza indirirken, güvenlik ekiplerinin kritik sorunlardan anında haberdar olmasını sağlar.

Geçmiş Veri Analizi

Platform, geçmiş verileri saklayarak güvenlik ekiplerinin geçmiş olayların ve eğilimlerin derinlemesine analizini yapmasına olanak tanır. Bu tarihsel perspektif, tekrar eden sorunları belirlemek, uzun vadeli kalıpları anlamak ve gelecekteki tehditleri tahmin etmek için çok önemlidir. Ayrıca geçmiş olayların ve yanıtların net bir kaydını sağlayarak uyumluluk raporlamasına ve denetimine yardımcı olur.

Gelişmiş Arama ve Korelasyon

CereAI XDR, güvenlik ekiplerinin ilgili bilgileri bulmak için büyük miktarlardaki günlük verilerini hızlı bir şekilde incelemesine olanak tanıyan güçlü arama ve korelasyon yetenekleri sunar. Platform, farklı kaynaklardan gelen olayları ilişkilendirerek, koordineli bir saldırıyı veya kalıcı tehdidi gösterebilecek gizli ilişkileri ve kalıpları ortaya çıkarabilir.



Kapsamlı Raporlama

Platform, güvenlik operasyonlarının çeşitli yönlerini kapsayan çok çeşitli önceden oluşturulmuş ve özelleştirilebilir raporlar sunar. Bu raporlar otomatik olarak çalışacak şekilde planlanabilir ve ihtiyaca göre uyarlanabilir.

Teknik ekiplerden yönetici liderliğe kadar farklı paydaşların özel ihtiyaçlarını karşılayın. Raporlar tehdit etkinliğinin, uyumluluk durumunun, sistem performansının ve daha fazlasının özetlerini içerebilir.

Tehdit İstihbaratı Entegrasyonu

CereAI XDR, küresel tehdit istihbaratını analitiğine entegre ederek raporlamasının doğruluğunu ve alaka düzeyini artırır. Platform, harici tehdit akışlarından gelen verileri birleştirerek tespit edilen tehditlere ilişkin bağlam sağlayabilir ve güvenlik ekiplerinin daha geniş tehdit ortamını ve düşmanlar tarafından kullanılan belirli taktikleri, teknikleri ve prosedürleri (TTP'ler) anlamalarına yardımcı olabilir.

Kullanıcı Davranışı Analizi

Platform, anormallikleri ve potansiyel içeriden gelen tehditleri tespit etmek için kullanıcı etkinliklerini izleyen ve analiz eden kullanıcı davranışı analitiği (UBA) yeteneklerini içerir. CereAI XDR, normal davranışın temel çizgilerini oluşturarak, kötü niyetli niyet veya güvenliği ihlal edilmiş hesaplara işaret edebilecek sapmaları tespit edebilir.

Uyumluluk ve Denetim Raporlaması

CereAI XDR uyumluluk ve denetim raporları oluşturma sürecini basitleştirir. GDPR, HIPAA ve PCI-DSS gibi çeşitli düzenleyici çerçevelerin gereksinimlerini karşılayan raporlar oluşturmak için şablonlar ve araçlar sağlar. Bu, kuruluşların düzenleyici standartlara bağlılıklarını gösterebilmelerini ve güçlü bir uyumluluk duruşunu sürdürebilmelerini sağlar.

Görselleştirme Araçları

Platform, güvenlik ekiplerinin karmaşık verileri çizelgeler, grafikler ve diğer görsel yardımlar aracılığıyla yorumlamasına yardımcı olan gelişmiş görselleştirme araçlarını içerir. Bu araçlar eğilimleri tanımlamayı, anormallikleri tespit etmeyi ve bulguları teknik olmayan paydaşlara etkili bir şekilde iletmeyi kolaylaştırır.

Özetle CereAI XDR'nin raporlama ve analiz yetenekleri, güvenlik ekiplerine güvenlik tehditlerini etkili bir şekilde izlemek, analiz etmek ve bunlara yanıt vermek için ihtiyaç duydukları araçları sağlar. Gerçek zamanlı kontrol panelleri ve ayrıntılı olay raporlarından gelişmiş arama ve korelasyon özelliklerine kadar platform, karar almayı geliştiren ve genel güvenlik duruşunu iyileştiren kapsamlı bilgiler sunar.