FORCEPOINT

Bilgi Formu

FORCEPOINT UEBA

Bilgi Güvenliği

FİKRİ MÜLKİYET HAKLARINIZI KORUYUN, GİZLİLİĞİ İHLAL EDİLMİŞ HESAPLARI TESPİT EDİN VE İÇ TEHDİT RİSKİNİ AZALTIN

Forcepoint Kullanıcı ve Öğe Davranışı Analizleri (UEBA), güvenlik ekiplerinin işletme bünyesindeki yüksek riskli davranışları proaktif olarak izlemesini mümkün kılar. Güvenlik analizleri platformumuz kötü niyetli, gizliliği ihlal edilmiş ve ihmalkar kullanıcıları belirlemek için yapısal ve yapısal olmayan verileri birleştirerek benzersiz bir bağlam sağlar. Gizliliği ihlal edilmiş hesaplar, kurumsal casusluk, fikri mülkiyet hırsızlığı ve sahtekarlık gibi kritik sorunlar ortaya çıkarılır.

GÜVENLİK İÇİN NEDEN FORCEPOINT UEBA?

Müşterilerimiz, kurum bünyesindeki insan davranışlarının bağlamını öğrenme konusunda bize güvenmektedir. Güvenlik analistlerinin kurum için en önemli olan sorunları çözmesine yardımcı olan yapılandırılabilir analizleri yalnızca Forcepoint UEBA sunar. Güvenlik ekiplerinin:

- Şirket içinden saldırıları tespit etmek için harcadığı zamanı azaltmaya,
- Güvenlik ekiplerinin çok yoğun olduğu esnada gerekli uyarıları gün yüzüne çıkarmalarına,
- SIEM ve sahip olduğunuz diğer araçlardan farklı olarak iç faaliyetler konusunda granüler yaklaşım sergilemelerine
- Olay müdahalesi ve ihlal sonrası adli sürece yönelik soruşturma verimliliğini artırmaya yardımcı olur.

PLATFORMUN TEMELLERİ

Forcepoint UEBA, sadece anormal faaliyet uyarıları değil aynı zamanda yüksek riskli davranışlar ve kişilerle ilgili bilgi sağlar. Forcepoint UEBA insanlar, veriler, cihazlar ve uygulamalar arasındaki etkileşimleri değerlendirerek güvenlik ekipleri için zaman dilimlerinin önceliğini belirler. Yazılımımız dört temel üzerine kurulmuştur:

Zengin Bağlam › Farklı veri kaynaklarını tek bir rapor şeklinde birleştirir; SIEM, uç nokta ve çalışan girdilerinin yanı sıra niyeti deşifre etmeye yönelik haberleşme içeriğini bir araya getirir.

Davranış Analizleri › Karmaşık saldırıları daha iyi tespit etmek için değişim, ve anormal faaliyete odaklanan farklı türlerde davranışa ve içeriğe dayalı analizler uygular.

Arama ve Keşif › Sürekli izleme ve derin soruşturmalar için, bağlam açısından zengin bir kullanıcı arayüzü yoluyla güçlü adli arama ve keşif araçları içerir.

Sezgisel İş Akışı › Kurum verimliliğini düzenlemek için kullanıcı davranışı iş akışı ve mevcut müşteri bilgileri mimarisini tamamen kapsayan proaktif raporlama sunar.

Başlıca Kullanım Durumları

- **Öncelikli Faaliyetler**
- **İçerik Bilinçli DLP**
- **Gizliliği İhlal Edilmiş Hesap Tespiti**
- **Veri Keşfi**
- **Ayrıcalıklı Kullanıcı Suistimali**
- **Güvenlik Analizleri**

GÜVENLİK ANALİZLERİNİ YENİDEN TANIMLAMA

İçerik Odaklı Görünürlük › Forcepoint UEBA yapısal olmayan, içerik açısından zengin veri akışları ile yapısal verileri birleştirerek çalışan faaliyetleri, davranışları ve ilişkileri konusunda benzersiz görünürlük sağlar. Analitik modellerimiz, birimler ve olayların tüm veri akışları genelinde birden fazla mercek kullanılarak puanlanmasını ve önceliklendirilmesini sağlar; bu da güvenlik ekiplerinin daha önce sahip olmadığı bir olanaktır. Ayrıca, iç soruşturmaları büyük ölçüde destekleyen güçlü bir adli platform ve durum farkındalığı sunmak için Aktif Dizin, SIEM, EDR'ler ve kilit veri kaynaklarının entegrasyonu sağlanmaktadır.

Yapılandırılabilir Analizler › Geleneksel kara kutu UBA araçları çoğu zaman farklı sistemlerde analiz edilen, sabit analiz yapılandırmasına sahip yapısal veri kaynakları ile sınırlıdır. Bunun tersine Forcepoint UEBA, güvenlik ekiplerinin gelişen güvenlik kullanım durumlarını ele almasını ve tüm veri kümeleri genelinde gelişmiş arama dahil gerçek zamanlı ad hoc analiz gerçekleştirmesini sağlayan güçlü analitik kabiliyetler sunar. Analizlerimiz ek programlamaya gerek olmadan düzenlenebildiği için, güvenlik tehditlerine karşı daha hızlı müdahale mümkündür.

Ölçek › Esas olarak ölçeklendirme için altyapımızı hazır. Büyük miktarlarda veriye anında erişimi sağlayan ElasticSearch yalnızca Forcepoint UEBA tarafından kullanılmaktadır. Platformumuz hem yapısal hem de yapısal olmayan verileri sorunsuz biçimde depolar ve yatay olarak ölçeklendirir. Forcepoint UEBA ayrıca değişen seviyelerde erişim ve idari kontroller sunar, dolayısıyla işletmeniz için herhangi bir kurulum türün için teknolojimize güvenebilirsiniz.

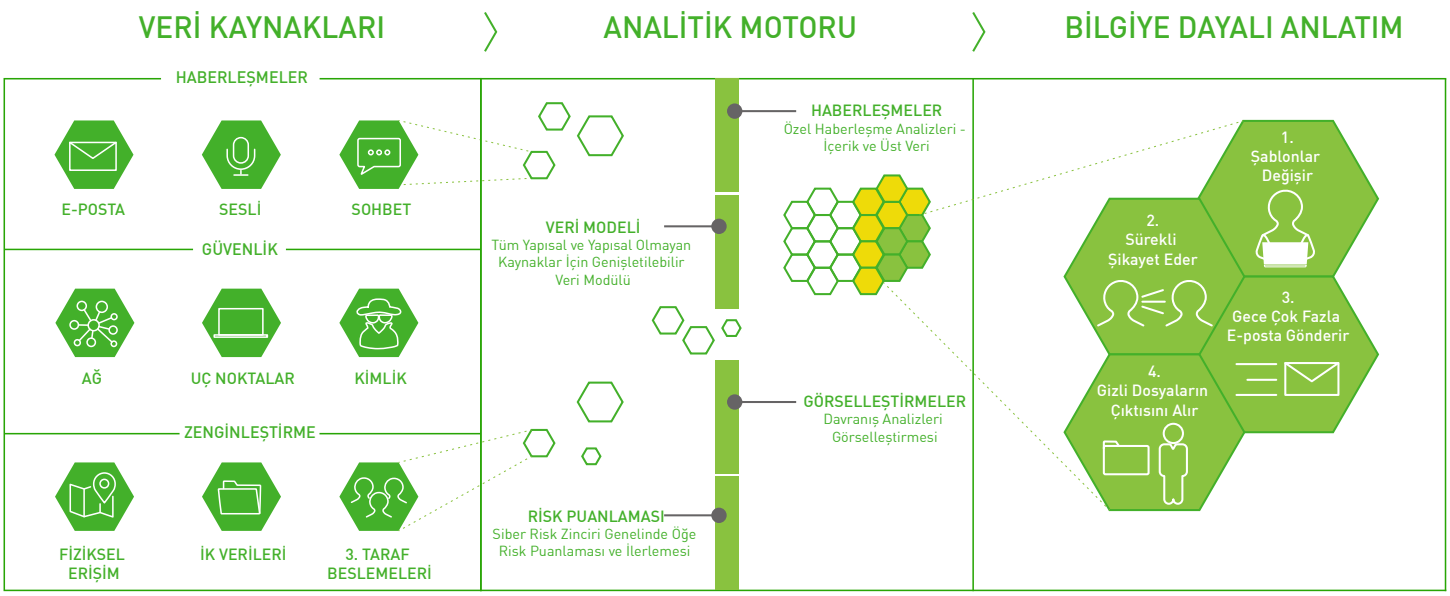
Kabiliyetler

- **Göreve Dayalı Panolar ve İş Akışları** Uyumlu olmayan faaliyetlerin sezgisel kullanıcı arayüzü vasıtasıyla hızlıca gözden geçirilmesini sağlar, böylece analistler ve yöneticiler anında soruşturma, inceleme, eskale etme ve önlem alma imkanı bulabilir.
- **Sağlam Veri Hakları** Hem iç kontroller hem de dış odaklı veri gizliliği sorunlarının gerektirdiği karmaşık veri hakları için tam destek.
- **Genişletilebilir Platform** Yapılandırılabilir analizler, gösterge panelleri ve iş akışı güvenlik kullanım durumlarını destekler ve her türlü risk kullanım durumuna genişletme imkanı sunar. Geniş bir profesyonel hizmet taahhüdü olmadan gelişmiş veri bilimi modelleri sunar.
- **Esnek Kullanım Seçenekleri** Forcepoint UEBA'yı şirket içinde, sanal özel bulut ortamında ve hatta bir Forcepoint UEBA aracı vasıtasıyla hemen kullanın.

Gelişmiş Analitik

- **Davranış Analizleri** Duygu ve içerik analizini kullanarak çalışanların mevcut veya potansiyel yasa dışı, istenmeyen veya uyumsuz faaliyetlerini işaret edebilecek davranış değişikliklerini belirleyin.
- **Akıllı Önceliklendirme** İçerik ve üst veri kalıplarının analizine bağlı olarak ilgili olayları ve uyarıları önceliklendirin.
- **Doğal Dil İşleme (NLP)** Akıllı NLP uygulaması, her dilde karmaşık veri sözlükleri ve sorumluluk retlerini ve zincir e-postalardan alınan metinleri tanıyan metin tanıma teknolojisi yoluyla yanlış pozitif sonuçların sayısını büyük ölçüde azaltın.
- **Görselleştirmeler** Bir analistin çıkarım yapma kabiliyetlerini ortaya çıkarmak ve ilgili faaliyetler çerçevesinde maksimum içeriksunmak için özel olarak geliştirilmiş görselleştirmeler. Çalışan eylemleri ile ilgili kim, ne, ne zaman ve nasıl sorularına hemen cevap bulun.
- **İçerik Sınıflandırması** Forcepoint UEBA'nın içerik sınıflandırma motorunu kullanarak DLP kullanımlarını güçlendirin ve istenmeyen posta, 3. parti e-posta, vb. gibi alakasız haberleşmeleri belirleyin ve filtreleyin.

İLETİŞİM
www.forcepoint.com/contact


VERİ KAYNAKLARI
ANALİTİK MOTORU
BİLGİYE DAYALI ANLATIM
HABERLEŞMELER
E-POSTA
SESLİ
SOHBET
GÜVENLİK
AĞ
UÇ NOKTALAR
KİMLİK
ZENGİNLEŞTİRME
FİZİKSEL ERİŞİM
İK VERİLERİ
3. TARAF BESLEMELERİ
VERİ MODELİ
Tüm Yapısal ve Yapısal Olmayan Kaynaklar İçin Genişletilebilir Veri Modülü
RİSK PUANLAMASI
Siber Risk Zinciri Genelinde Öğe Risk Puanlaması ve İlerlemesi
HABERLEŞMELER
Özel Haberleşme Analizleri - İçerik ve Üst Veri
GÖRSELLEŞTİRMELER
Davranış Analizleri Görselleştirmesi
1. Şablonlar Değişir
2. Sürekli Şikayet Eder
3. Gece Çok Fazla E-posta Gönderir
4. Gizli Dosyaların Çıktısını Alır