KAIA-OR · KULLANIM ALANI ÖZETİ

Dijital risk ve siber tehdit istihbaratı

Kurumunuzun kullandığı yazılımları ilgilendiren siber olayları tesislerinizle aynı tabloda görün; çalışanlarınıza mesajlar ve bağlantılar için ikinci bir bakış sunun.

BELGE KİMLİĞİ	UCB-04-DIGITAL-RISK-AND-CYBER-THREAT-INTELLIGENCE
SÜRÜM	1.0
TARİH	3 Kasım 2026
HEDEF KİTLE	Ekiplerde, kurumsal şirketlerde ve kamu kurumlarında güvenlik ve bilgi teknolojileri sorumluları

Bir bakışta

Kimler için	Kendi geliştirmedikleri yazılımlara bağımlı olan ve çalışanları oltalama mesajları, şüpheli bağlantılar ve dosyalar alan kurumlar.
Sonuç	Yalnızca kullandığınız yazılımları ilgilendiren büyük ihlaller ve yeni istismar edilen güvenlik açıkları; her biri önem derecesi, güven düzeyi ve teyit durumuyla, tesislerinizi ilgilendiren fiziksel olayların yanında. Ayrıca çalışanlarınız için ikinci bir bakış.
Paket	KAIA-OR Ekip, Kurum veya Kamu

Zorluk

Güvenlik ve bilgi teknolojileri ekipleri okuyabileceklerinden çok daha fazla güvenlik açığı ve ihlal raporu alır. İşe yarayanlar, kurumlarının gerçekten kullandığı yazılımları ilgilendirenlerdir; onları bulmak da ilgilendirmeyen pek çok raporu okumayı gerektirir.

Bu arada kurumun her yerindeki çalışanlar oltalama mesajları, kötü amaçlı bağlantılar ve şüpheli dosyalar alır. Küçük ekiplerin danışabileceği güvenlik personeli yoktur; büyük ekipler ise çalışanlarının aldığı her mesajı inceleyemez.

Siber olaylar genellikle bir araçta, fiziksel olaylar başka bir araçta durur; bu yüzden bir ofisten sorumlu ekip bir fırtınayı bir yerde, o ofisin kullandığı yazılımdaki bir güvenlik açığını başka bir yerde görür ve ikisini birbirine bağlayan hiçbir şey yoktur.

© Kaia Technologies, Inc.

KAIA-OR ile neler değişir

Yazılımlarınızı ilgilendiren siber olaylar

Kullandığınız yazılımları ilgilendiren büyük ihlaller ve yeni istismar edilen güvenlik açıkları olay olarak görünür; her biri önem derecesi, güven düzeyi, kaynağı, teyit durumu ve eşleşme gerekçesiyle birlikte.

Fiziksel ve siber tek tabloda

Siber olaylar, tesislerinizi ilgilendiren tehlikeler, güvenlik olayları ve aksaklıklarla aynı ortak tabloda yer alır; böylece bir tesisten sorumlu kişiler ikisini birlikte görür.

Çalışanlarınız için ikinci bir bakış

Çalışanlar şüpheli bir mesajı yapıştırır ya da bir bağlantıyı açmadan kontrol eder. Neyin yolunda görünmediğini, kontrolün emin olamadığı durumları ve zaten güvendikleri bir kanaldan teyit etmek gibi önerilen bir sonraki adımı görürler. Kontroller uyarı işaretlerini İngilizce, Fransızca, Türkçe ve İbranice tanır.

Dosya ve casus yazılım risk göstergeleri

Dosyalar ve cihazlar için KAIA-OR, hüküm vermeden, daha dikkatli bakılmaya değer risk göstergelerini gösterir.

Kendi araçlarınıza

Olaylar API ve webhook'lar aracılığıyla ekibinizin zaten kullandığı araçlara aktarılır.

Denetleyebileceğiniz yanıtlar

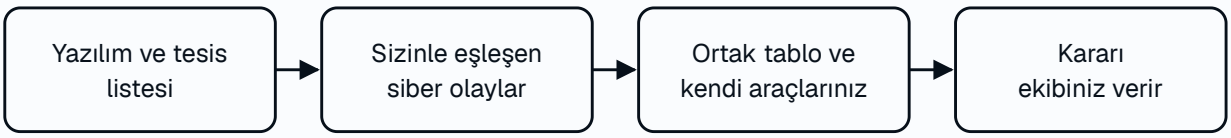
Bir olayın kullandığınız yazılımlar için ne anlama geldiğini Hey KAIA'ya sorun. Yanıtlar dayandıkları kanıtı belirtir ve bu kanıtla karşılaştırılır. Model çıktısı hiçbir yetki vermez; tarama araçları yalnızca sizin belirlediğiniz sınırlar içinde ve sizin yetkinizle harekete geçer.

Gördükleriniz

Öğe	Ne gösterir
Siber olay	Kategori, önem derecesi, zaman aralığı, güven düzeyi, kaynak ve teyit durumu, ilgilendirdiği yazılım ve eşleşme gerekçesi.
Ortak tablo	Tesislerinizi ilgilendiren fiziksel olayların yanında siber olaylar.
Mesaj veya bağlantı kontrolü	Tanınan uyarı işaretleri ve önerilen bir sonraki adım; bağlantı açılmadan kalır.
Dosya veya casus yazılım kontrolü	Hüküm içermeyen, daha dikkatli bakılmaya değer risk göstergeleri.

© Kaia Technologies, Inc.

Nasıl çalışır



Listelediğiniz yazılımlarla eşleştirilen siber olaylar, tesislerinizle aynı tabloda.

1. Bir güvenlik sorumlusu kurumun kullandığı başlıca yazılımları listeler ve ofisleri tesis olarak ekler.
2. Yeni istismar edilen bir güvenlik açığı bu ürünlerden birini ilgilendirdiğinde ortak tabloda bir olay olarak, önem derecesi, güven düzeyi, teyit durumu ve eşleşme gerekçesiyle birlikte görünür.
3. Pakete bağlı olarak olay, API ve webhook'lar aracılığıyla ekibin kendi araçlarına da aktarılır; böylece bu tür işlerle zaten ilgilenen kişilere ulaşır.
4. Bir çalışan emin olmadığı bir bağlantı içeren bir mesaj aldığında mesajı yapıştırır. Bağlantı açılmadan kalır; çalışan neyin yolunda görünmediğini ve önerilen bir sonraki adımı görür.
5. Güvenlik sorumlusu güvenlik açığının kurum için ne anlama geldiğini Hey KAIA'ya sorar. Yanıt dayandığı kanıtı belirtir; ne yapılacağına dair karar ekipte kalır.

© Kaia Technologies, Inc.

Gizlilik ve denetim

- Her kişinin kontrol ettiği mesajlar ve bağlantılar kendi cihazında kalır.
- Roller kişileri değil, üyeliği yönetir. Üyelik, başka bir üyenin mesajlarına, cihazlarına, konumuna veya kayıtlı yerlerine asla erişim hakkı vermez.
- Bu üyelik sınırları ve kurumlar arasındaki yalıtım uygulama katmanında sağlanır.
- Siz önce kabul etmedikçe hiçbir şey bulut tabanlı bir yapay zekâ hizmetine gitmez. Kamu kurumlarında bulut tabanlı yapay zekâ başlangıçta kapalıdır.

Dürüst sınırlar

- KAIA-OR bir virüsten koruma yazılımı değildir. Bilgi verir; sistemlerinizde kendiliğinden hiçbir şeyi değiştirmez, kaldırmaz veya yamamaz.
- Dosya ve casus yazılım sonuçları hüküm değil, risk göstergesidir. KAIA-OR bir dosya, bağlantı veya cihaz için “tehlike yok” sonucu vermez.
- Siber olaylar listelediğiniz yazılımlarla eşleştirilir. Kapsam, resmî ve yetkili kaynakların yayımladıklarına bağlıdır; teyit edilemeyen raporlar teyit edilmemiş olarak etiketlenir.

Paketler ve ilgili kullanım alanları

Dijital risk Ekip, Kurum ve Kamu paketlerinin bir parçasıdır. API erişimi pakete bağlıdır; KAIA-OR web sitesindeki Paketler sayfasına bakın. KAIA-OR; iOS, iPadOS, macOS, Android telefonlar, Android TV, Windows ve web’de İngilizce, Fransızca (Kanada), Türkçe ve İbranice çalışır. Tek hesap her platformda aynı özellikler ve aynı gizlilik kurallarıyla çalışır.

İlgili kullanım alanları

- Dolandırıcılık ve oltalama kontrolleri
- Tedarik zinciri
- Finansal hizmetler

© Kaia Technologies, Inc.

Erken erişim talep edin

> Üyelik davetle verilir. KAIA-OR web sitesinden erken erişim talep edin ve Ekip, Kurum veya Kamu paketini seçin. Kurumsal şirketlerdeki ve kamu kurumlarındaki ekipler, KAIA-OR web sitesindeki “Bize ulaşın” seçeneğini de kullanabilir.

© Kaia Technologies, Inc.

UCB-04-DIGITAL-RISK-AND-CYBER-THREAT-INTELLIGENCE · Sürüm 1.0 · 3 Kasım 2026

Bir yeteneğin sunulup sunulmadığı pakete ve kuruluma bağlıdır. Yetenekler, KAIA-OR’un taahhüt edilen ürün kapsamı olarak açıklanmıştır.