GNSAC Vigil

Dış Tehdit İstihbaratı ve Dijital Risk Koruması

Kimlik bilgisi maruziyetini, yeraltı faaliyetlerini, oltalama altyapısını, marka istismarını ve dışarıdan gözlemlenebilen teknoloji riskini kurumunuzun bağlamında inceleyin.

Mutabık kalınan kapsam, mimari ve güvenlik incelemesine tabi yönetilen SaaS ve on-premises dağıtım seçenekleri.

- **Kimlik bilgisi maruziyeti**
- **Yeraltı kaynakları**
- **Oltalama ve marka**
- **Dış maruziyet**

Dış sinyaller kurumsal bağlam gerektirir.

Güvenlik ekipleri kapsamlı iç telemetriye sahiptir. Vigil, müşteri sınırının ötesinde ortaya çıkabilen sinyaller için bir dış istihbarat katmanı ekler ve bunları yetkilendirilmiş kurumsal kapsamla ilişkilendirir.

1 Açığa çıkan kimlikler

Toplanan stealer log, birleşik liste ve ihlal verileri; inceleme gerektiren kurumsal kimlikler, parolalar, belirteçler veya oturum bağlamı içerebilir.

2 Yeraltı faaliyetleri

Seçili forumlar, pazarlar, hukuka uygun biçimde erişilebilen mesajlaşma toplulukları ve sızıntı siteleri; erişim teklifleri, veri satışı iddiaları veya ilgili aktör konuşmaları içerebilir.

3 Oltalama ve marka istismarı

Sertifika kayıtları, benzer alan adları, oltalama URL'leri ve sahte sayfalar; bir kurumu veya hizmetlerini taklit eden altyapıya ilişkin kanıt sağlayabilir.

4 Dış teknoloji ve üçüncü taraflar

İnternete açık varlıklar, gözlemlenen teknolojiler, zafiyet bağlamı ve tedarikçi referansları; iç envanterleri ve dönemsel güvence incelemelerini destekleyebilir.

SOC / SOME ile ilişkisi

Vigil mevcut güvenlik operasyonlarını tamamlar; bunların yerine geçmez. İç loglar ve olaylar müşteri SOC / SOME ekibinde kalır. Vigil, desteklenen inceleme ve entegrasyon iş akışları üzerinden dış bulguları ve mevcut kaynak bağlamını sunar.

Dış sinyalden incelenebilir bulguya.

Toplama hacmi tek başına sonuç değildir. Operasyon modeli; kaynak bağlamını korumak, müşteri tarafından onaylanan kapsamı uygulamak ve önceliklendirilmiş bulguları tekrarlanabilir bir inceleme sürecine taşımak üzere tasarlanmıştır.

1 Topla

Seçili dış kaynakları ve istihbarat akışlarını tanımlı hukuki, etik ve operasyonel kontroller altında topla.

2 Eşle

Gözlemlenen kayıtları yetkilendirilmiş alan adları, kimlikler, markalar, yöneticiler, tedarikçiler ve varlıklarla ilişkilendir.

3 Önceliklendir

Ön değerlendirmeyi desteklemek için güncellik, yetki seviyesi, oturum bağlamı, altyapı kanıtı ve müşteriyle ilgiyi kullan.

4 Sun

Bulguları mevcut zaman damgaları, kaynak bağlamı ve inceleme geçmişiyle göster; desteklenen entegrasyonlara yönlendir.

Operasyon ilkeleri

Yetkilendirilmiş kapsam

Müşteriye özel kontroller yalnızca izleme kapsamı ve yetki teyit edildikten sonra başlar.

İddiadan önce kanıt

Bulgular kaynaktan alınabilen bağlamı korur; işleme veya inceleme durumunu belirtir.

Analist incelemesi

Otomatik ilişkilendirme ön değerlendirmeyi destekler; doğrulama ve müdahale kararları müşteri ekiplerinin sorumluluğundadır.

Ölçülü kapsam

Kapsam ve uyarı zamanı; kaynak erişimine, toplama koşullarına, işleme durumuna ve yönlendirme kurallarına bağlıdır.

Tek inceleme iş akışında altı kabiliyet.

Her kabiliyet farklı bir dış risk alanına odaklanırken ortak izleme listelerini, ilişkilendirmeyi, kanıt incelemesini, vaka bağlamını ve raporlamayı kullanır.

1 Kimlik bilgisi istihbaratı

Toplanan stealer log, birleşik liste ve ihlal veri kümelerinde açığa çıkan kimlikleri; mevcut kaynak ve oturum bağlamıyla inceleyin.

2 Yeraltı kaynağı istihbaratı

Seçili yeraltı kaynaklarını ve hukuka uygun biçimde erişilebilen mesajlaşma topluluklarını kurumla ilgili referanslar için izleyin.

3 Oltalama ve marka koruması

Benzer alan adlarını, sertifika faaliyetini, oltalama altyapısını, sahte sayfaları ve mevcut kayıt veya barındırma kanıtını inceleyin.

4 Dış risk değerlendirmesi

Müşteri tarafından yetkilendirilmiş alan adlarında yapılandırılmış keşif ve istihbarat kontrolleri çalıştırın; öncelikli iyileştirme önerilerini inceleyin.

5 Tedarik zinciri ve VIP izleme

İlgili maruziyetleri ve üçüncü taraf referanslarını incelemek için tedarikçi, yönetici ve marka izleme listelerini kullanın.

6 Raporlama ve iş akışları

Tek bulgu kümesinden teknik ve yönetim çıktıları üretin; desteklenen uyarıları operasyon araçlarına yönlendirin.

Çıktılar

Bulgu kayıtları, teknik raporlar, yönetim özetleri, göstergeler ve desteklenen API / iş akışı entegrasyonları. Kesin çıktılar seçilen lisansa ve mutabık kalınan kapsama bağlıdır.

Belgelenmiş kontrollere sahip dağıtım seçenekleri.

Dağıtım, bağlantı ve veri akışları müşteri güvenlik incelemesinin parçası olarak değerlendirilmelidir. Seçilen model, ilgili sipariş formunda ve teknik tasarımda tanımlanır.

1 On-premises

Vigil, müşteri kontrolündeki sanallaştırma ortamına OVF / OVA cihazı olarak kurulabilir. İzlenen varlıklar, bulgular ve kullanıcı faaliyetleri bu ortamda müşteriye özel izole veri tabanında tutulur. Gerekli bağlantı ve istihbarat senkronizasyonu güvenlik incelemesi için belgelenir.

2 Yönetilen SaaS

Vigil uygun durumlarda yönetilen SaaS hizmeti olarak sunulabilir. Veri konumu, saklama, erişim, bağlantı ve destek gereksinimleri ticari ve güvenlik kapsam çalışmasında belirlenir.

İncelemeye sunulan kontrol seti

- İki faktörlü kimlik doğrulama ve rol tabanlı erişim kontrolü
- Denetlenebilir kullanıcı faaliyeti ve inceleme geçmişi
- Seçilen dağıtım modeline uygun müşteri izolasyonu
- Mimari, bağlantı ve veri akışı dokümantasyonu
- Lisans kapsamında desteklenen REST API, webhook ve operasyon entegrasyonları
- İlgili sözleşmede tanımlanan destek ve eskalasyon düzenlemeleri

Veri yönetişimi yaklaşımı

Bu kontroller veri yönetişimi, tedarikçi güvence ve denetim süreçlerini destekleyebilir. Mevzuata uyum; her kurumun uygulamasına, politikalarına, işleme faaliyetlerine ve hukuki yükümlülüklerine bağlıdır.

Operasyonel kullanıma kontrollü geçiş.

Devreye alma; müşteri ortamı, yetkilendirilmiş izleme listeleri, entegrasyonlar, uyarı öncelikleri ve operasyon sorumluluklarına göre kapsamlandırılır. Süre; altyapı hazırlığına, onaylara ve karmaşıklığa bağlıdır.

1 Kapsamı ve yetkiyi teyit et

Alan adlarını, kimlikleri, markaları, yöneticileri, tedarikçileri, kaynak gereksinimlerini ve izin verilen değerlendirme faaliyetlerini kesinleştir.

2 Mimariyi incele

Dağıtım modelini, veri konumunu, bağlantıyı, erişim kontrollerini, saklamayı ve güvenlik inceleme kanıtını belirle.

3 Kur ve yapılandır

Hizmeti kur veya devreye al; rolleri oluştur, izleme listelerini aktar ve toplama ile eşleştirme kurallarını yapılandır.

4 Ayarla ve entegre et

Önem ve yönlendirme kurallarını belirle, temsili bulguları incele ve desteklenen SIEM, SOAR, vaka veya iş birliği araçlarını bağla.

5 Operasyona devret

Sorumlulukları, eskalasyon yollarını, raporlama sıklığını, eğitimi ve kabul kriterlerini teyit et.

Alıcının teyit etmesi gerekenler

- Hangi kaynaklar ve bölgeler gereksinimlerimizle ilgili?
- Her bulgu için hangi kanıt saklanıyor?
- Seçilen dağıtımda hangi veri içeri giriyor veya dışarı çıkıyor?
- Lisansımıza hangi entegrasyonlar ve API işlevleri dahil?
- Sözleşmede hangi destek saatleri, yanıt hedefleri ve eskalasyon yolları var?
- Kapsam, hatalı pozitif yönetimi ve operasyonel sonuçlar nasıl ölçülecek?

Vigil'i kendi ortamınıza göre değerlendirin.

Odaklı ürün oturumu; mevcut arayüzü, temsili kanıtı, inceleme iş akışını, dağıtım seçeneklerini, desteklenen entegrasyonları ve kurumunuzla ilgili ticari kapsamı göstermelidir.

1 Ürün incelemesi

Mevcut modülleri ve temsili uyarı, inceleme ve raporlama iş akışlarını değerlendirin.

2 Metodoloji incelemesi

Kaynak bağlamını, eşleştirme mantığını, önceliklendirme etkenlerini ve mevcut kanıtın sınırlarını inceleyin.

3 Teknik inceleme

Dağıtım, bağlantı, erişim kontrolü, veri konumu, saklama ve desteklenen entegrasyonları görüşün.

4 Ticari kapsam

İzlenen unsurları, kullanıcıları, taramaları, raporları, API erişimini, desteği ve müşteriye özel çalışmaları teklif ile sipariş formunda kesinleştirin.

Önemli sınırlama

Hiçbir siber güvenlik platformu her tehdidin, maruziyetin veya olayın tespit ya da önlenmesini garanti edemez. Ürün kapsamı ve zamanlama; sözleşmedeki kapsama, kaynak erişimine, işleme durumuna, seçilen dağıtıma ve yapılandırılmış yönlendirme kurallarına bağlıdır.

Ürün oturumu talep edin

Müşteri alan adına yönelik değerlendirmeler yalnızca kapsam ve yetkilendirme teyit edildikten sonra gerçekleştirilir.

sales@gnsac.com.tr
support@gnsac.com.tr
+90 216 706 40 65
https://gnsac.com.tr