EMA SECURITY

Tehdit İstihbaratı Hizmeti

AI-Powered Offensive Services

İletişim

www.emasecurity.com

info@emasecurity.com

Bostancı Mah, Ali Nihat Tarhan Cd, Kahraman Sk,
No:2/D:11, Hoffman Plaza, Kadıkoy/İstanbul

+90 (850) 244 49 26

Tehdit İstihbaratı Hizmeti

Hizmet Tanımı

Tehdit İstihbaratı Hizmeti (Threat Intelligence Service), organizasyonların siber tehditlere karşı proaktif savunma stratejileri geliştirmesine yardımcı olan kapsamlı bir güvenlik hizmetidir. Bu hizmet, tehdit aktörlerinin taktiklerini, tekniklerini ve prosedürlerini (TTP) analiz ederek, kurumlara yönelik mevcut ve potansiyel tehditleri belirlemeyi amaçlar.

Tehdit istihbaratı, saldırı vektörlerini, kötü amaçlı yazılım kampanyalarını, siber suç gruplarını ve hedeflenen saldırıları gerçek zamanlı olarak izleyerek organizasyonlara özel savunma mekanizmaları oluşturulmasını sağlar. Açık kaynak istihbaratı (OSINT), kapalı tehdit paylaşım ağları, darknet analizleri ve gelişmiş tehdit avcılığı (threat hunting) teknikleri kullanılarak siber tehdit ortamı sürekli olarak değerlendirilir.

Hizmet, taktiksel, operasyonel, stratejik ve teknik tehdit istihbaratı bileşenlerini kapsar. Taktiksel tehdit istihbaratı, güvenlik ekiplerinin tehditlere karşı anında tepki vermesini sağlarken, operasyonel istihbarat saldırganların motivasyonları ve yöntemleri hakkında bilgi sunar. Stratejik tehdit istihbaratı, yöneticilere siber güvenlik yatırımları ve risk yönetimi süreçleri hakkında içgörüler sağlarken, teknik istihbarat ise zararlı IP adresleri, kötü amaçlı yazılım imzaları ve tehdit göstergeleri (IoC) gibi veri odaklı analizler sunar.

Bu hizmet, MITRE ATT&CK, Diamond Model, Cyber Kill Chain, STIX/TAXII ve NIST Cybersecurity Framework gibi uluslararası standartlara uygun olarak gerçekleştirilir. Siber tehdit aktörlerinin faaliyetleri sürekli olarak takip edilerek, saldırı girişimlerine karşı erken uyarı sistemleri oluşturulur ve tehdit tespit süreçleri optimize edilir.

Tehdit İstihbaratı Hizmeti, finans, sağlık, kamu, telekomünikasyon ve kritik altyapı sektörleri başta olmak üzere her ölçekteki organizasyon için uygundur. Kurum içi güvenlik operasyon merkezleri (SOC), olay müdahale ekipleri ve güvenlik analistleri, bu hizmet sayesinde tehditleri daha etkin bir şekilde analiz edebilir ve önleyici tedbirler alabilir.

Siber tehditlerin giderek karmaşık hale geldiği günümüzde, Tehdit İstihbaratı Hizmeti, organizasyonların siber saldırılara karşı proaktif önlemler almasını sağlayarak güvenlik risklerini minimize eder, karar alma süreçlerini iyileştirir ve siber savunma yetkinliklerini güçlendirir.

Hizmete Ait Bileşenler

Tehdit Keşfi ve Analizi

Tehdit istihbaratı süreci, organizasyonun karşı karşıya olduğu mevcut ve potansiyel tehditleri belirlemekle başlar. Açık kaynak istihbaratı (OSINT), kapalı tehdit paylaşım ağları ve darknet analizleri kullanılarak tehdit aktörlerinin faaliyetleri incelenir.

Tehdit Göstergeleri (IoC) ve Davranışsal Analiz

Zararlı IP adresleri, alan adları, kötü amaçlı yazılım imzaları ve saldırı teknikleri gibi tehdit göstergeleri (Indicators of Compromise – IoC) belirlenerek anomali tespit sistemleriyle entegrasyonu sağlanır. Siber saldırganların taktikleri, teknikleri ve prosedürleri (TTP) analiz edilerek tehdit modelleme gerçekleştirilir.

Tehdit Kaynaklarının İzlenmesi ve Veri Toplama

Dark web forumları, tehdit istihbaratı platformları, fidye yazılım grupları ve siber suç organizasyonları düzenli olarak izlenerek tehdit trendleri hakkında bilgi toplanır. Siber saldırı girişimleri ve yeni tehdit vektörleri analiz edilerek erken uyarı sistemleri oluşturulur.

Sektörel ve Coğrafi Tehdit Değerlendirmesi

Belirli sektörlere (finans, sağlık, kamu, enerji vb.) ve bölgelere yönelik özel tehdit analizi gerçekleştirilerek organizasyonun risk profili oluşturulur. Sektörel tehdit istihbaratı, organizasyonun karşılaşabileceği spesifik tehditleri daha iyi anlamasını sağlar.

Zafiyet ve Saldırı Teknikleri Analizi

Güncel güvenlik açıkları (CVE'ler), istismar (exploit) kitleri ve zararlı yazılımlar analiz edilerek organizasyonun sistemlerine yönelik olası tehditler belirlenir. Siber saldırganların kullandığı en yeni saldırı teknikleri incelenerek proaktif savunma önlemleri geliştirilir.

Proaktif Tehdit Avcılığı (Threat Hunting)

Tehdit istihbaratı kapsamında, güvenlik ekipleri aktif tehdit avcılığı çalışmaları yürüterek sistemlerde gizlenen kötü niyetli aktiviteleri tespit eder. Anormal ağ trafiği, şüpheli erişimler ve zararlı yazılım etkinlikleri analiz edilerek erken müdahale sağlanır.

Olay Müdahale ve Tehdit Analizi

Gerçekleşen güvenlik olayları analiz edilerek saldırganların kimliği, amaçları ve kullandıkları yöntemler hakkında bilgi toplanır. Olay sonrası adli analiz (forensic analysis) yapılarak saldırı izleri takip edilir ve gelecekte benzer tehditlere karşı savunma mekanizmaları geliştirilir.

Tehdit İstihbaratı Entegrasyonu

Elde edilen tehdit istihbaratı, SIEM (Security Information and Event Management), EDR (Endpoint Detection and Response) ve XDR gibi güvenlik sistemlerine entegre edilerek otomatik tespit ve yanıt süreçleri güçlendirilir.

Raporlama ve Paylaşım

Tehdit istihbaratı bulguları düzenli olarak teknik ve yönetsel seviyede raporlanır. Özel sektör, kamu kuruluşları ve tehdit istihbaratı topluluklarıyla bilgi paylaşımı yapılarak kolektif savunma mekanizmaları oluşturulur.

Stratejik Tehdit Değerlendirmesi ve Karar Desteği

Üst yönetim ve güvenlik ekiplerine yönelik tehdit değerlendirme raporları sunularak siber güvenlik stratejilerinin şekillendirilmesine destek verilir. Risk bazlı güvenlik planlaması yapılarak uzun vadeli güvenlik önlemleri belirlenir.

Mevcut Durum Analizi

Tehdit istihbaratı hizmeti öncesinde, organizasyonun mevcut siber güvenlik durumu analiz edilir. Dijital varlıklar, ağ altyapısı, güvenlik politikaları ve tehdit algılama yetenekleri değerlendirilerek riskler belirlenir.

Açık kaynak istihbaratı (OSINT), dark web ve tehdit istihbaratı platformları üzerinden veri toplanarak organizasyona yönelik siber tehditler incelenir. Siber suç grupları, APT saldırıları, fidye yazılımları ve kimlik avı kampanyaları gibi tehdit unsurları analiz edilir.

Ayrıca, SIEM, EDR ve XDR gibi güvenlik sistemlerinin tehditleri izleme kapasitesi ve güvenlik ekiplerinin tehdit avcılığı yetkinliği değerlendirilir. Son olarak, organizasyonun ISO 27001, NIST CSF, GDPR, KVKK ve PCI DSS gibi regülasyonlara uyumu gözden geçirilerek tehdit istihbaratı stratejisi oluşturulur.

Strateji ve Yol Haritası Belirleme

Tehdit istihbaratı hizmeti kapsamında, organizasyonun ihtiyaçlarına uygun istihbarat stratejisi belirlenir. Öncelikle, tehdit aktörleri, sektör bazlı riskler ve organizasyonun dijital varlıkları analiz edilerek tehdit odaklı bir yaklaşım oluşturulur.

Tehdit veri kaynakları (OSINT, dark web, siber suç forumları, tehdit istihbaratı platformları) belirlenerek, otomatik ve manuel analizlerle istihbarat toplama süreçleri tanımlanır. Kritik varlıklar ve potansiyel saldırı vektörleri önceliklendirilerek, siber tehditlerin erken tespiti için proaktif güvenlik önlemleri geliştirilir.

Son olarak, sürekli izleme, tehdit avcılığı (threat hunting) ve olay müdahale süreçleri optimize edilerek organizasyona özel bir tehdit istihbaratı yol haritası oluşturulur.

Tehdit İstihbaratı Hizmeti Aşamaları

Tehdit istihbaratı süreci, öncelikle keşif aşamasıyla başlar. Bu aşamada, açık kaynak istihbaratı (OSINT), dark web taramaları ve tehdit istihbaratı platformları kullanılarak organizasyona yönelik tehditler hakkında bilgi toplanır.

Ardından, tehdit analizi gerçekleştirilerek zararlı aktörler, saldırı kampanyaları ve organizasyona yönelik spesifik riskler değerlendirilir. Toplanan veriler doğrulanarak tehdit seviyeleri belirlenir ve olası saldırı senaryoları analiz edilir.

İleri seviye tehdit avcılığı (threat hunting) teknikleriyle, organizasyon içindeki anormal aktiviteler tespit edilir ve olay müdahale ekipleri için önleyici aksiyon planları hazırlanır.

Son olarak, kapsamlı bir tehdit raporu hazırlanarak tespit edilen riskler, saldırı vektörleri ve önerilen güvenlik önlemleri sunulur. Tehdit istihbaratı döngüsünün sürekliliğini sağlamak amacıyla izleme ve güncelleme süreçleri düzenli olarak gerçekleştirilir.

Tehdit İstihbaratı Hizmeti Metodolojisi

Tehdit istihbaratı hizmeti, organizasyonların mevcut ve gelişen siber tehditlere karşı proaktif bir güvenlik stratejisi oluşturmasını sağlamak amacıyla, MITRE ATT&CK, Diamond Model, Cyber Kill Chain ve NIST gibi uluslararası güvenlik çerçeveleri temel alınarak yürütülür. İlk olarak, organizasyonun tehdit yüzeyi analiz edilir; dijital varlıklar, ağ altyapısı, açık kaynak verileri (OSINT) ve dark web üzerindeki potansiyel tehditler değerlendirilir. Bu aşamada, sektör bazlı tehdit grupları, APT (Advanced Persistent Threat) aktörleri, kötü amaçlı yazılım kampanyaları ve olası saldırı vektörleri belirlenerek istihbarat kapsamı oluşturulur.

Keşif sürecinde, pasif ve aktif veri toplama teknikleri kullanılarak zararlı aktörler, siber suç örgütleri ve devlet destekli tehditler incelenir. Sosyal mühendislik saldırıları, kimlik avı (phishing), tedarik zinciri saldırıları, zararlı yazılım dağıtım yöntemleri ve veri sızdırma girişimleri analiz edilir. Dark web, deep web ve kapalı forumlar üzerinden organizasyona yönelik tehditlerin varlığı araştırılarak sızdırılmış bilgiler, çalınan kimlik bilgileri ve güvenlik açıkları tespit edilir.

Tehdit istihbaratı sürecinin devamında, toplanan veriler korelasyon analizleri ile ilişkilendirilerek organizasyon üzerindeki etkisi değerlendirilir. Güvenlik olayları, tehdit raporları ve geçmiş saldırı vektörleri göz önünde bulundurularak olası saldırı senaryoları oluşturulur. Riskli alanlar belirlenerek, organizasyonun tehditlere karşı ne derece savunmasız olduğu ve saldırganların hangi yöntemleri kullanabileceği öngörülür.

Toplanan istihbarat verileri doğrultusunda, organizasyonun güvenlik duruşunu güçlendirmek için teknik ve stratejik iyileştirme önerileri sunulur. Olay müdahale süreçleri, tehdit avı (threat hunting) yöntemleri, SIEM entegrasyonları, anomali tespiti ve sürekli izleme mekanizmaları geliştirilerek tehdit istihbaratının operasyonel hale getirilmesi sağlanır.

Son olarak, tehdit istihbaratı hizmeti düzenli olarak güncellenerek, yeni tehdit trendleri, gelişen saldırı teknikleri ve organizasyona özgü risk faktörleri değerlendirilir. Bu sayede, organizasyonun siber tehditlere karşı proaktif önlemler alması, saldırı yüzeyini minimize etmesi ve uzun vadede güvenlik duruşunu sürekli iyileştirmesi sağlanır.

Raporlama ve İyileştirme

Tehdit istihbaratı hizmeti kapsamında, tespit edilen siber tehditler, saldırı kampanyaları ve güvenlik açıkları detaylı şekilde raporlanır. Bulgular; tehdit aktörleri, saldırı vektörleri, veri sızıntıları, zararlı yazılım analizleri ve istihbarat kaynakları açısından değerlendirilir. Tespit edilen tehditler, risk seviyelerine göre sınıflandırılarak organizasyon için önceliklendirilmiş düzeltici ve önleyici aksiyon planları sunulur.

Olay sonrası analiz sürecinde, organizasyonun güvenlik önlemlerinin tehditlere nasıl tepki verdiği incelenir ve savunma mekanizmalarının etkinliği değerlendirilir. Erişim kontrolleri, güvenlik izleme sistemleri (SIEM, SOAR), tehdit avı (Threat Hunting) süreçleri ve saldırı tespit sistemleri (IDS/IPS) gözden geçirilerek gerekli iyileştirmeler önerilir.

Sıkça Sorulan Sorular (SSS)

Tehdit istihbaratı hizmeti neden önemlidir?

Bu hizmet, organizasyonların potansiyel saldırıları önceden belirlemesine, siber tehdit aktörlerini tanımasına ve güvenlik stratejilerini proaktif bir şekilde geliştirmesine yardımcı olur.

Tehdit istihbaratı nasıl toplanır?

İstihbarat, açık kaynaklar (OSINT), dark web analizleri, zararlı yazılım verileri, saldırı kampanyaları ve güvenlik araştırmalarından elde edilen bilgilerin analiziyle toplanır.

Tehdit istihbaratı türleri nelerdir?

Taktiksel, operasyonel, stratejik ve teknik tehdit istihbaratı olmak üzere dört ana kategoriye ayrılır. Her biri farklı seviyelerde güvenlik kararlarını destekler.

Bu hizmet kimler için uygundur?

Finans, sağlık, kamu, enerji ve teknoloji sektörleri gibi kritik altyapıya sahip organizasyonlar için tehdit istihbaratı hizmeti büyük önem taşır.

Tehdit istihbaratı ile sızma testi arasındaki fark nedir?

Sızma testi mevcut güvenlik açıklarını belirlemeye odaklanırken, tehdit istihbaratı olası tehditleri tespit ederek önleyici güvenlik önlemleri alınmasını sağlar.

Tehdit istihbaratı hizmeti regülasyonlara uyum sağlar mı?

Evet, ISO 27001, NIST, GDPR, KVKK ve diğer sektörel uyumluluk çerçevelerine uygun olarak tehdit istihbaratı raporları sağlanabilir.

Tehdit istihbaratı ile fidye yazılım saldırıları önlenebilir mi?

Evet, fidye yazılım gruplarının kullandığı teknikler, saldırı vektörleri ve hedefleme yöntemleri analiz edilerek organizasyonların erken önlem alması sağlanır.

Tehdit istihbaratı platformları ile entegrasyon sağlanabilir mi?

Evet, SIEM, SOAR, IDS/IPS gibi güvenlik sistemleriyle entegrasyon sağlanarak tehdit istihbaratının otomatik olarak işlenmesi mümkündür.

Dark web tehdit istihbaratı nedir?

Dark web üzerindeki tehdit aktörleri, çalınmış veriler, zararlı yazılım satışları ve saldırı planları hakkında bilgi toplanarak organizasyonların önceden önlem alması sağlanır.