KASPERSKY lab

Kaspersky Siber Güvenlik Hizmetleri 2018

www.kaspersky.com
#truecybersecurity

Siber suç, artık sınır tanımıyor ve teknik özellikleri hızla gelişiyor. Saldırıların, sürekli olarak daha karmaşık hale geldiğini görüyoruz. Misyonumuz dünyayı her türlü siber tehditten korumaktır. Bu amaca ulaşmak ve interneti emniyetli ve güvenli hale getirmek için tehdit istihbaratlarının gerçek zamanlı olarak paylaşılması hayati önem taşır. Bilgilere zamanında ulaşmak, verilerin ve ağların etkili bir şekilde korunması için en temel unsurlardandır.

Eugene Kaspersky
Kaspersky Lab Yönetim Kurulu Başkanı ve CEO'su

Giriş

Her gün, farklı saklanma yöntemlerini ve farklı saldırı vektörlerini kullanan birçok siber tehdit ortaya çıkmaktadır.

Bunun için kapsamlı koruma sağlayan tek bir çözüm yoktur. Ancak büyük verinin önemli bir yer kapladığı dünyamızda tehlikelerin nereden geleceğini bilmek bu yeni tehditlerle mücadelenin büyük bir parçasını oluşturur.

Bir işletme yöneticisi olarak kurumunuzu günümüz tehditlerine karşı korumak ve gelecekte başınıza gelebilecek tehlikeleri tahmin etmek sizin görevinizdir. Bu, yalnızca bilinen tehditlere karşı akıllı işlemsel korumayı kapsamaz, üst düzey stratejik güvenlik istihbaratını da gerektirir. Çok az şirket bu düzeyde bir istihbaratı kurum içinde geliştirebilecek kaynaklara sahiptir.

Kaspersky Lab olarak işletmeye uzun vadeli bir kazanç getirmek için uzun ömürlü ilişkilere ihtiyaç olduğunu biliyoruz.

Kaspersky Lab, her zaman farklı kanallar aracılığıyla ekibinize güncel istihbaratlar sağlamaya hazır değerli bir iş ortağıdır. Çok çeşitli kanallar kullanmamız, güvenlik işlemleri merkezinizin (SOC)/BT güvenlik ekibinizin kurumunuzu her türlü çevrimiçi tehdide karşı koruması için tam donanımlı olmasını sağlar.

Kurumunuz Kaspersky Lab ürünlerini kullanmasa bile Kaspersky Lab Siber Güvenlik Hizmetleri'nden yararlanabilirsiniz.

Kaspersky Siber Güvenlik Hizmetleri

- **Kaspersky Tehdit İstihbarat Hizmetleri**
- **Kaspersky Tehdit Avlama Hizmetleri**
- **Kaspersky Güvenlik Eğitimi**
- **Kaspersky Olay Yanıt Hizmetleri**
- **Kaspersky Güvenlik Değerlendirme Hizmetleri**

Farklı bir güvenlik anlayışı

Dünya lideri Güvenlik İstihbaratı en temel yapı taşımızdır: Bu yapı taşı, yaptığımız her işi etkiler ve kötü amaçlı yazılımlara karşı piyasada bulunan en güçlü korumayı sağlar.

Teknoloji odaklı bir şirketiz: Başta CEO'muz Eugene Kaspersky olmak üzere en üst düzeyden en alt düzeydeki çalışanlara kadar şirketimizdeki herkes teknoloji odaklıdır.

Global Araştırma ve Analiz Ekibi'miz (GReAT) BT güvenliği uzmanlarından oluşan seçkin bir gruptur ve dünyadaki en tehlikeli kötü amaçlı tehditleri ve hedefli saldırıları ortaya çıkarma konusunda liderdir.

Dünyadaki en saygın güvenlik kuruluşları ve emniyet teşkilatlarının çoğu (INTERPOL, Europol, CERT ve Londra Polisi dahil olmak üzere) bizden etkin olarak yardım talep etmektedir.

Kaspersky Lab, temel teknolojilerinin tümünü kurum içinde geliştirir ve mükemmelleştirir. Bu nedenle ürünlerimiz ve istihbaratımız daha güvenilir ve etkilidir.

En saygın endüstri analiz şirketleri (Gartner, Forrester Research ve International Data Corporation (IDC) dahil olmak üzere) birçok önemli BT güvenliği kategorisinde
bizi Lider olarak seçmiştir.

130 OEM'den fazla şirket (Microsoft, Cisco, Blue Coat, Juniper Networks ve Alcatel Lucent dahil olmak üzere) kendi ürünlerinde ve hizmetlerinde bizim teknolojilerimizi kullanır.

Kaspersky Tehdit İstihbaratı Hizmetleri

Sürekli gelişen BT güvenlik tehditlerini takip etmek, analiz etmek, yorumlamak ve risklerini azaltmak çok büyük bir sorumluluktur. Tüm sektörlerden şirketler, BT güvenlik tehditlerini yönetmeye yardımcı olabilecek güncel ve ilgili verileri bulmak konusunda zorluk yaşamaktadır.

Kaspersky
Siber Güvenlik Hizmetleri

Kaspersky
Tehdit İstihbarat Hizmetleri

Tehdit Veri Akışları
APT İstihbarat Raporları
Özel Hazırlanmış Tehdit Raporları
Kaspersky Threat Lookup
Kaspersky Phishing Tracking
Kaspersky Botnet Tracking

Kaspersky
Tehdit Avlama Hizmetleri

Kaspersky
Güvenlik Eğitimi

Kaspersky
Olay Yanıt Hizmetleri

Kaspersky
Güvenlik Değerlendirme
Hizmetleri

Kaspersky Lab'in sağladığı Tehdit İstihbaratı Hizmetleri, bu tehditlerin riskini azaltmak için ihtiyaç duyduğunuz istihbarata erişmenizi sağlar. Bu istihbarat, dünya lideri araştırma ve analiz ekibimiz sayesinde edinilir.

Kaspersky Lab'in siber güvenliğin tüm yönleri hakkındaki bilgileri, deneyimi ve kapsamlı istihbaratı, şirketimizi INTERPOL ve CERT dahil olmak üzere dünyanın önde gelen emniyet teşkilatları için güvenilir bir iş ortağı haline getirmiştir. Bu istihbaratı anında kurumunuz için kullanmaya başlayabilirsiniz.

Kaspersky Lab Tehdit İstihbaratı Hizmetleri şunları kapsar:

- Tehdit Veri Akışları
- APT İstihbarat Raporları
- Özel Hazırlanmış Tehdit Raporları
- Kaspersky Threat Lookup
- Kaspersky Phishing Tracking
- Kaspersky Botnet Tracking

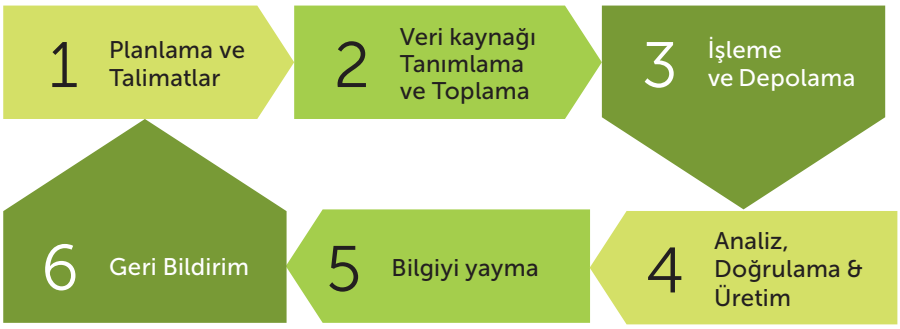
Tehdit Veri Akışları

Birinci sınıf güvenlik tedarikçileri ve şirketler, **üst düzey güvenlik çözümleri üretmek veya işletmelerini korumak** için başarısı zamanla kanıtlanmış ve güvenilir olan Kaspersky Tehdit Veri Akışını kullanır.

Siber saldırılar her gün gerçekleşir. Siber tehditler **savunma araçlarınızı saf dışı bırakmaya** çalışırken sıklık, karmaşıklık ve gizlenme açısından sürekli gelişmektedir. Saldırganlar, işinizi aksatmak ya da müşterilerinize zarar vermek için karmaşık izinsiz giriş **ölüm zincirleri**, saldırılar ve **Taktikler, Teknikler ve Prosedürler (TTP'ler) kullanır**.

Kaspersky Lab, **siber tehditlerle ilgili riskler ve sonuçlar hakkında işletmenize ve müşterilerinize bilgi vermek** için **sürekli olarak güncellenen** Tehdit Veri Akışı hizmeti sağlar. Bu sayede **tehdit risklerini daha etkili bir şekilde azaltmanıza** ve saldırı başlamadan önce onlara karşı **kendinizi savunmanıza** yardımcı olur.

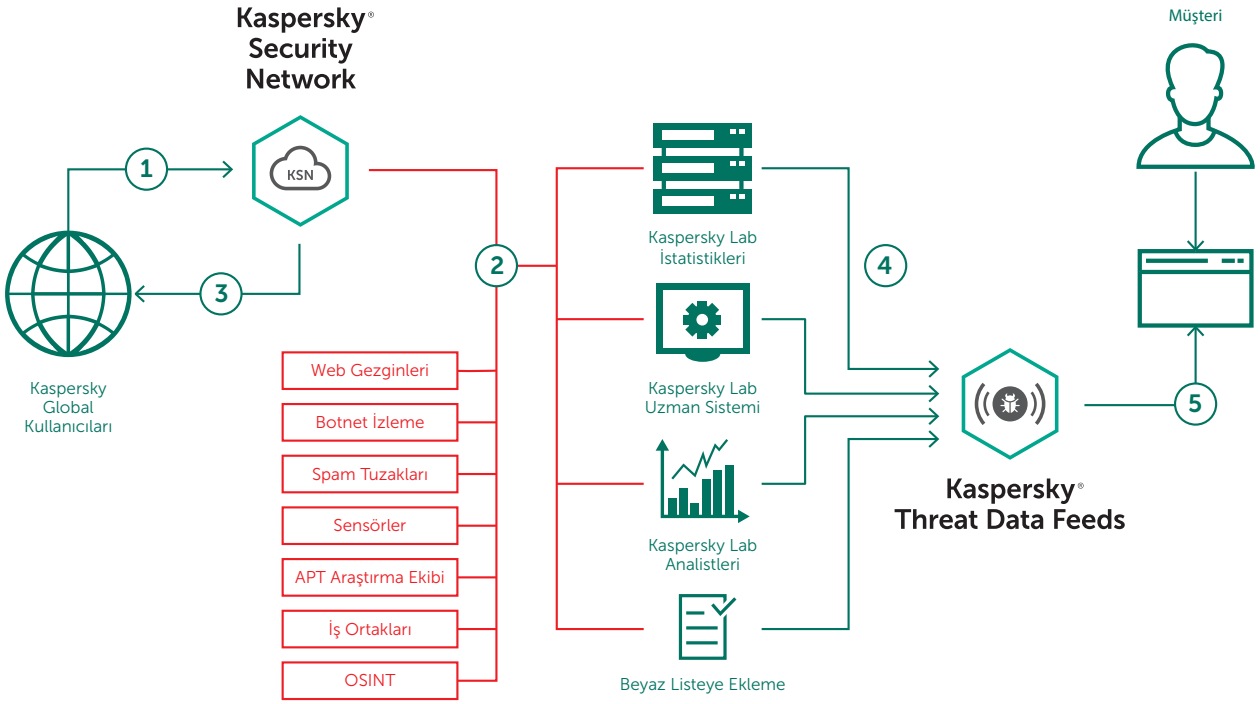
İstihbarat Döngüsü



Veri Akışları

Akışlar aşağıdaki setlerden oluşur:

- **IP Bilinirlik Akışı**: şüpheli ve kötü amaçlı bilgisayarları kapsayan IP adresleri seti;
- **Kötü Amaçlı ve Kimlik Avı URL Akışı**: kötü amaçlı ve kimlik avı amaçlı bağlantılar ve web sitelerini kapsar;
- **Botnet Komuta ve Kontrol (C&C) URL Akışı**: masaüstü botnet komuta ve kontrol sunucularını ve ilgili kötü amaçlı nesneleri kapsar;
- **Mobil Botnet Komuta Kontrol URL Akışı**: mobil botnet komuta ve kontrol sunucularını kapsar. Komuta ve Kontrol sunucuları ile iletişim kuran virüslü makineleri bulur;
- **Fidye Yazılımı URL Akışı**: fidye yazılımı nesnelerini barındıran veya bunlar tarafından erişilen bağlantıları kapsar
- **APT Risk Göstergesi Akışları** (APT İstihbarat Raporları çözümünün etkin kullanıcıları tarafından kullanılabilir): APT saldırıları düzenlemek için saldırganlar tarafından kullanılan kötü amaçlı etki alanlarını, sunucuları, kötü amaçlı IP adreslerini, kötü amaçlı dosyaları ve ilgili dosyalar ya da kötü amaçlı yazılım aileleri için YARA kurallarını kapsar
- **Kötü Amaçlı Karma Akışı**: en tehlikeli, yaygın ve yeni ortaya çıkan kötü amaçlı yazılımları kapsar;
- **Mobil Kötü Amaçlı Yazılım Akışı**: mobil Android ve iPhone platformlarına bulaşan kötü amaçlı nesnelerin tespitini destekler;
- **SMS Truva Atı Akışı**: saldırganların SMS mesajlarını çalmasını, silmesini ve onlara yanıt vermesini sağlamanın yanı sıra mobil kullanıcılar için fazla ücrete neden olan SMS Truva Atları'nın tespitini destekler;
- **Beyaz Liste Veri Akışı**: yasal yazılımlar hakkında sistematik bilgi sağlayarak üçüncü taraf çözümleri ve hizmetleri sunar.
- **Kaspersky Transforms for Maltego**: Maltego kullanıcıları için Kaspersky Lab Tehdit Veri Akışına erişim sağlayan dönüşüm setlerini içerir. Kaspersky Transforms for Maltego, Kaspersky Lab'den gelen veri akışına göre URL'leri, karmaları ve IP adreslerini kontrol etmenizi sağlar. Dönüşüm setleri, nesnenin kategorisini belirlemenin yanı sıra nesne hakkında eyleme geçirilebilir bağlam sağlar.



Kaspersky Tehdit Veri Akışı, gerçek dünyadan gerçek zamanlı olarak alınan ve tamamen denetlenmiş tehdit göstergesi verilerini içerir.

Bağlamsal Veriler

Veri Akışlarındaki her kayıt, **eyleme geçirilebilir bağlam** (tehdit adları, tarih damgası, coğrafi konum, virüslü web kaynaklarının çözülen IP adresleri, karmalar, popülerlik vb.) ile zenginleştirilmiştir. Bağlamsal veriler, verinin çeşitli kullanım alanlarını geçerli hale getirerek ve destekleyerek "büyük resmin" açığa çıkmasına yardımcı olur. Veriler bağlam içinde değerlendirildiğinde **kim, ne, nerede, ne zaman sorularını** daha kolay cevaplamak için kullanılabilir. Bu soruların cevapları düşmanlarınızı tanımlamanızı sağlayarak kurumunuzla ilgili zamanında kararlar almanıza ve harekete geçmenize **yardımcı olabilir.**

Hizmetin Öne Çıkan Özellikleri

- **Hatalı Pozitifler** ile kirlenen Veri Akışları değersizdir. Bu nedenle %100 incelenmiş verilerin sunulduğundan emin olmak için akış yayınlanmadan önce son derece kapsamlı testler ve filtreler uygulanır;
- Veri Akışları, dünya genelinden toplanan bulgular (213 ülkeden milyonlarca kullanıcıyı kapsayan Kaspersky Security Network İnternet trafiğinin önemli bir kısmı için görünürlük sağlar) temel alınarak gerçek zamanlı bir şekilde üretilir ve yüksek **tespit oranları** ve doğruluk sağlar;
- Tüm akışlar hataya son derece dayanıklı bir altyapı tarafından üretilir ve izlenir. Bu sayede **sürekli kullanılabilirlik** sağlanır;
- Veri Akışları kimlik avı, kötü amaçlı yazılım, açıklardan yararlanan yazılım, botnet komuta ve kontrol URL'leri ve diğer kötü amaçlı içerikleri barındırmak için kullanılan **URL'lerin anında tespit edilmesini** sağlar;
- **Her trafik türünde (web, e-posta, P2P, IM...) ve mobil platformlarda hedeflenen kötü amaçlı yazılımlar** da **anında tespit edilebilir** ve tanımlanabilir;
- **HTTPS** veya özel teslim mekanizmaları aracılığıyla basit ve hafif **dağıtım** formatları (**JSON, CSV, OpenIoC, STIX**), akışların güvenlik çözümlerine kolay entegrasyonunu sağlar;
- Tüm dünyadan **güvenlik analistleri**, **GReAT ekibimizden dünyaca ünlü güvenlik uzmanları** ve lider Ar-Ge ekipleri dahil olmak üzere yüzlerce uzman, bu akışların üretilmesine yardımcı olur. Güvenlikten sorumlu yöneticiler, en yüksek kalitedeki veriler kullanılarak üretilen kritik bilgileri ve uyarıları alır. Bu sayede gereksiz gösterge ve uyarı bombardımanına maruz kalma riski ortadan kalkar;
- **Uygulama kolaylığı**. Kaspersky Lab tarafından sağlanan tamamlayıcı belgeler, numuneler, özel teknik hesap yöneticisi ve teknik destek bir araya gelerek sorunsuz entegrasyon sağlar.

Toplama ve işleme

Veri Akışları birleşik, heterojen ve son derece güvenilir kaynaklardan toplanır. Bu kaynaklara; Kaspersky Security Network, kendi web gezginlerimiz, Botnet İzleme hizmeti (botnetlerin, hedeflerinin ve faaliyetlerinin 7 gün 24 saat 365 gün izlenmesi), spam tuzakları, araştırma ekipleri ve iş ortakları dahildir.

Daha sonra toplanan veriler gerçek zamanlı olarak denetlenir ve sadeleştirilir. Bu işlemler için istatistik kriterleri, Kaspersky Lab Uzman Sistemleri (koruma alanları, sezgisel motorlar, çoklu tarayıcılar, benzerlik araçları ve davranış profili oluşturma) analist doğrulaması ve beyaz liste onayı gibi birçok ön işleme tekniği kullanılır:

Avantajlar

- **SIEM'ler, Koruma Duvarları, IPS/IDS, Güvenlik Ara Sunucusu, DNS çözümleri ve APT'ye Karşı Koruma dahil olmak üzere sürekli olarak güncellenen Risk Göstergeleri (IOC'ler) ve siber saldırılar konusunda bilginin yanı sıra düşmanlarınızın niyeti, özellikleri ve hedeflerini daha iyi anlamanızı sağlayan eyleme geçirilebilir bağlam sayesinde ağ savunma çözümlerinizi güçlendirin**. Lider SIEM'ler (HP ArcSight, IBM QRadar, Splunk vb. dahil olmak üzere) tamamen desteklenir;
- **Çevreniz ve kenar ağı cihazları (yönlendiriciler, ağ geçitleri, UTM cihazları gibi) için kötü amaçlı yazılıma karşı koruma** geliştirin ve iyileştirin.
- **Olay yanıtınızı ve adli bilişim kabiliyetlerinizi geliştirir ve hızlandırır**: Güvenlik/Güvenlik İşlemleri Merkezi ekibinize hedefli tehditlerin arkasında yatan nedenleri anlamak için tehditler ve global veriler hakkında anlamlı bilgiler sunar. Ana bilgisayardaki ve ağdaki güvenlik olaylarını daha verimli ve etkili bir şekilde tanılar ve onaylar; olay yanıtı süresini en aza indirmek ve kritik sistemler ile veriler tehlikeye girmeden ölüm zincirini durdurmak için bilinmeyen tehditlere karşı iç sistemlerden gelen sinyalleri önceliklendirir;
- **Kurumsa abonelere tehdit istihbaratı sunar**. Yeni ortaya çıkan kötü amaçlı yazılımlar ve diğer kötü tehditler hakkında doğrudan bilgilerin kullanılmasını sağlar. **Savunma pozisyonunuzu saldırı başlamadan önce güçlendirir ve riskleri önler**;
- **Hedefli saldırıların riskini azaltmaya yardımcı olur**. Kurumunuzun karşılaştığı belirli tehditlere karşı mücadele için savunma stratejileri geliştirerek taktiksel ve stratejik tehdit istihbaratıyla güvenlik tutumunuzu geliştirir;
- **Ağlarınızda ve veri merkezlerinizde barındırılan kötü amaçlı içerikleri tespit etmek** için tehdit istihbaratı kullanır;
- **Virüslü makinelerden hassas varlıkların ve fikri mülkiyetin kurum dışına sızmasını önler**, virüslü varlıkları hızlı bir şekilde bulur, rekabet üstünlüğünün ve iş fırsatlarının kaybolmasını önler ve markanızın saygınlığını korur;
- Komuta ve kontrol protokolleri, IP adresleri, kötü amaçlı URL'ler veya dosya karmaları gibi tehdit göstergelerini derinlemesine araştırır, saldırıların önceliklendirilmesini sağlayan uzmanlar tarafından değerlendirilen tehdit bağlamı sağlar, BT giderleri ve kaynak ayrımı kararlarını iyileştirir ve **işletmeniz için en büyük riski oluşturan tehditlerin risklerinin azaltılmasına odaklanma konusunda sizi destekler**;
- Web içerik filtreleme ve istenmeyen posta/kimlik avı engelleme gibi **ürün ve hizmetleriniz tarafından sağlanan korumayı arttırmak** için uzmanlığımızı ve eyleme geçirilebilir bağlamsal istihbaratları kullanır;
- **MSSP olarak**, müşterilerinize üst düzey hizmet şeklinde sektör lideri tehdit istihbaratı sağlayarak işinizi büyütün. **CERT olarak**, siber tehdit tespit ve tanımlama becerilerinizi geliştirin ve artırın.

Kaspersky APT İstihbarat Raporları şunları sağlar:

- **Devam eden araştırma sırasında, basına sunulmadan önce en yeni tehditler hakkında teknik açıklamalara özel erişim**.
- **Halka açık olmayan APT'ler hakkında bilgiler**. Tüm üst düzey tehditler kamuya bildirilmez. Etkilenen kurbanlar, verilerin hassasiyeti, güvenlik açığı düzeltme sürecinin hassas tabiatı veya ilgili emniyet teşkilatı faaliyetleri nedeniyle bazı tehditler asla kamuya bildirilmez. Ancak bunların tamamı müşterilerimizle paylaşılır.
- **Ayrıntılı destek**: OpenIOC veya STIX dahil olmak üzere standart formatlarda kullanılabilir Risk Göstergeleri'nin (IOC) kapsamlı bir listesini içeren teknik veriler ve Yara kurallarımıza erişim imkânı.
- **APT saldırılarının sürekli izlenmesi.** Soruşturma sırasında eyleme geçirilebilir istihbarata erişim (APT dağıtımı, Risk Göstergeleri ve Komuta ve Kontrol altyapısı).
- **Farklı alıcılara uygun içerikler.** Her rapor, üst düzey yöneticilere yönelik özel bir özet ve ilgili APT'leri açıklayan anlaşılır bilgiler içerir. Yönetici özetinden sonra kötü amaçlı yazılım analistlerine, güvenlik mühendislerine, ağ güvenlik analistlerine ve APT araştırmacılarına ilgili tehditten daha iyi koruma sağlamak için eyleme geçirilebilir tavsiyeler sunarak APT'nin ayrıntılı bir teknik açıklamasının ve ilgili Risk Göstergeleri ile Yara kuralları sunulur.
- **Geçmişe yönelik analiz.** Abonelik döneminiz boyunca size sunulmuş olan özel raporlara erişim olanağı.
- **APT İstihbaratı Portalı.** Müşterilerimiz için sorunsuz bir kullanıcı deneyimine sahip APT İstihbarat Portalımız aracılığıyla en yeni Risk Göstergeleri dahil olmak üzere tüm raporlara erişilebilir. Ayrıca API kullanılabilir.

Not: Abone Sınırlaması

Bu hizmet tarafından sunulan bazı raporların içerdiği bilgileri hassasiyeti ve belirli nitelikleri nedeniyle bu hizmetin aboneliğini yalnızca güvenilir devletler ile kamu kuruluşları ve özel kuruluşlar için sınırlandırmak zorundayız.

APT İstihbarat Raporları

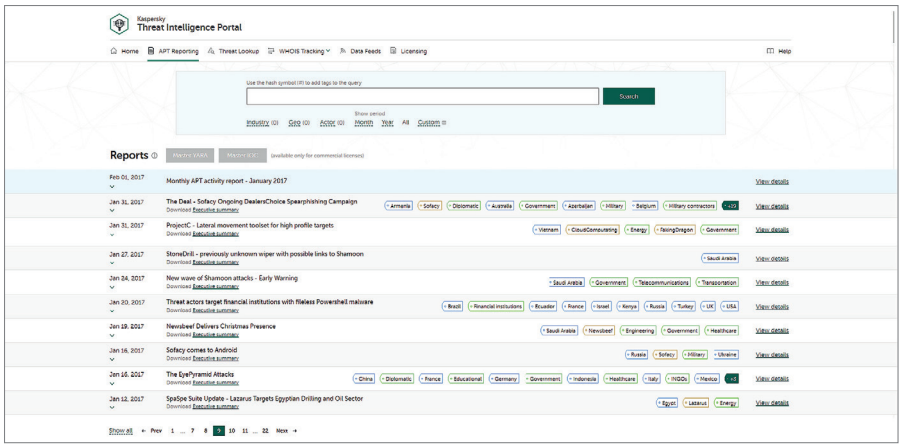
Kaspersky Lab'in sağladığı kapsamlı ve kullanışlı raporları kullanarak üst düzey siber casusluk saldırıları hakkındaki farkındalığınızı ve bilginizi arttırın.

Bu raporlarda sağlanan bilgilerden yararlanarak, yeni tehditlere ve güvenlik açıklarına hızlı bir şekilde yanıt verebilirsiniz. Bilinen vektörler aracılığıyla saldırıları engelleyebilir, gelişmiş saldırılardan kaynaklanan hasarı azaltabilir ve kendi güvenlik stratejinizi veya müşterilerinizin stratejisini geliştirebilirsiniz.

Kaspersky Lab, şimdiye kadarki en önemli APT saldırılarından bazılarını açığa çıkarmıştır. Ancak, Gelişmiş Kalıcı Tehditler ile ilgili tüm bulgular anında bildirilmez hatta bazıları hiçbir zaman halka duyurulmaz.

Kaspersky APT İstihbarat Raporları'nın abonesi olarak size devam eden soruşturmalarımız ve keşiflerimize benzersiz bir erişim olanağı sunarız. Bu raporlar, asla halka açıklanmayacak olan tehditler dahil olmak üzere açığa çıkmış tüm APT'ler hakkında çeşitli formatlarda sunulan tam teknik verileri içerir. 2016 yılında 100'den fazla rapor hazırladık!

Sektördeki en becerikli ve başarılı APT avcıları olan uzmanlarımız, siber suç çetelerinin taktiklerinde tespit ettikleri tüm değişimler hakkında sizi anında uyarır. Ayrıca Kaspersky Lab'in tam APT raporları veritabanına da erişim sağlayabilirsiniz. Bu veritabanı, kurumsal güvenlik savunma stratejiniz için daha güçlü bir araştırma ve analiz unsurudur.



Özel Hazırlanmış Tehdit Raporları

Müşteriye Özel Tehdit Raporlama

Kurumunuza yapılan saldırıyla mücadele etmek için en iyi yöntem nedir? Özellikle sizi hedef alan saldırganın elinde hangi bilgiler vardır ve hangi yol haritalarını takip eder? Saldırı zaten başladıysa tehlike altına girmiş olur musunuz?

Kaspersky Müşteriye Özel Tehdit Raporlama, bu soruları ve daha birçok soruyu sizin için cevaplar. Uzmanlarımız mevcut saldırı durumunuz hakkında kapsamlı bir şekilde parçaları bir araya getirirken kötüye kullanım için hazır zayıf noktaları tanımlar ve geçmişteki, şu andaki ve planlanan saldırıların kanıtlarını ortaya çıkarır.

Bu benzersiz bilgilere sahip olduğunuzda savunma stratejinizi siber suçluların birincil hedefi olarak işaretlenen alanlarda toplayabilirsiniz. İzinsiz giriş yapan saldırganları geri püskürtmek ve başarılı bir saldırının risklerini an aza indirmek için hızlıca ve hassasiyetle hareket edebilirsiniz.

Açık kaynak istihbaratımızı (OSINT), Kaspersky Lab uzman sistemlerinin ve veritabanlarının derin analizini ve yer altı siber suç şebekeleri hakkındaki bilgimizi kullanarak geliştirilen bu raporlar aşağıdaki alanları kapsar:

- **Tehdit vektörlerinin belirlenmesi**: ATM'ler, güvenlik kameraları ve mobil

teknolojileri kullanan diğer sistemler, çalışan sosyal ağ profilleri ve kişisel e-posta hesapları dahil olmak üzere ağınıza dışarıdan ulaşılabilen ve olası saldırı hedefleri olan önemli bileşenlerin belirlenmesi ve durum analizi.

- **Kötü amaçlı yazılım ve siber saldırı takip analizi**: Kurumunuzu hedef alan aktif ve pasif kötü amaçlı yazılım örnekleri, geçmişteki ve şu andaki botnet faaliyetleri ve her türlü ağ tabanlı faaliyetin tanımlanması, izlenmesi ve analizi.

- **Üçüncü taraf saldırılar**: Özel olarak müşterilerinizi, iş ortaklarınızı ve abonelerinizi hedef alan ve daha sonra bu virüslü sistemlerle size saldırmak için kullanılacak olan tehditler ve botnet faaliyetlerine dair kanıtlar.

- **Bilgi sızıntısı**: Yeraltı çevrimiçi forumların ve toplulukların gizlice izlenmesi sayesinde hacker'ların sizi hedef alarak saldırı planlayıp planlamadığını veya kötü niyetli bir çalışanınızın bilgi satıp satmadığını öğreniriz.

- **Mevcut saldırı durumu**: ATP saldırıları uzun yıllar boyunca fark edilmeden devam edebilir. Altyapınızı etkileyen bir saldırı tespit ettiğimizde etkili bir şekilde onarım için tavsiyeler verebiliriz.

Hızlı Başlangıç - Kolay Kullanım - Kaynak Gerektirmez

Bu Kaspersky Lab hizmetini kullanmak için parametreler ve tercih edilen veri formatları bir kez seçildikten sonra herhangi ek bir altyapıya gerek yoktur.

Kaspersky Tailored Threat Reporting, ağ kaynaklarınız dahil olmak üzere kaynaklarınızın bütünlüğünü ve kullanılabilirliğini etkilemez.

Bu hizmet tek seferlik bir proje veya abonelikle düzenli bir şekilde (örneğin üç ayda bir) sağlanabilir.

Ülkeye Özel Tehdit Raporlama

Bir ülkenin siber güvenliği, o ülkenin tüm büyük kurum ve kuruluşlarını korumaktan geçer. Hükümet yetkililerine karşı gelişmiş kalıcı tehditlerin (APT) kullanılması ulusal güvenliği etkileyebilir. Üretim, telekomünikasyon, bankacılık ve diğer önemli sektörlere yapılan saldırılar da devlet düzeyinde finansal kayıplar, üretim kazaları, ağ iletişimlerinin engellenmesi ve halk arasında huzursuzluk gibi önemli hasarlar oluşturabilir.

Ülkenizi hedef alan kötü amaçlı yazılımlardaki ve hedefli saldırılardaki geçerli saldırı zemini ve geçerli trendler hakkında genel bir fikir sahibi olduğunuzda savunma stratejinizi, siber suçluların asıl hedefleri olarak belirtilen alanlarda toplayabilirsiniz. Bu sayede yetkisiz giriş yapan saldırganları püskürtmek ve başarılı saldırıların riskini azaltmak için hızlı ve kararlılıkla hareket edebilirsiniz.

Açık kaynak istihbaratından (OSINT) Kaspersky Lab uzman sistemlerinin ve veritabanlarının derin analizi ve yer altı siber suç şebekeleri hakkındaki bilgimize kadar çeşitli yöntemleri kullanarak geliştirilen bu Ülkeye Özgü Tehdit raporları aşağıdaki alanları kapsar:

- **Tehdit vektörlerinin belirlenmesi**: Savunmasız hükümet uygulamaları, telekomünikasyon ekipmanları, endüstriyel kontrol sistemlerine ait bileşenler (SCADA, PLC gibi) ve ATM'ler dahil olmak üzere ülkenin dışarıdan ulaşılabilen kritik BT kaynaklarının belirlenmesi ve durum analizi.

- **Kötü amaçlı yazılım ve siber saldırı takip analizi**: Benzersiz iç izleme kaynaklarımızdaki verilere dayalı olarak ülkenizi hedef alan APT saldırıları, aktif veya pasif kötü amaçlı yazılım örnekleri, geçmişteki veya gelecekteki botnet faaliyetleri ve diğer önemli tehditlerin tanımlanması ve analizi.

- **Bilgi sızıntıları**: yeraltı forumlarının ve çevrimiçi toplulukların gizlice izlenmesi sayesinde hacker'ların sizi hedef alan saldırılar planlayıp planlamadığını öğreniriz. Ayrıca saldırıya uğrayan kurum ve kuruluşlar için risk teşkil edebilecek ele geçirilen önemli hesapları da ortaya çıkarırız (örneğin Ashley Madison güvenlik ihlalinde, devlet kurumu çalışanlarına ait olan ve şantaj için kullanılabilecek hesaplar ele geçirilmişti).

Kaspersky Threat Intelligence Reporting çözümünün, denetlenen ağ kaynaklarının bütünlüğü ve kullanılabilirliği üzerinde herhangi bir etkisi yoktur. Bu hizmet, ağa müdahale etmeyen keşif yöntemlerine ve açık veya sınırlı erişime sahip kaynaklarda mevcut olan bilgilerin analizine dayalıdır.

Hizmetin sonunda, ayrıntılı teknik analiz sonuçları hakkında ek bilgilerin yanı sıra farklı devlet endüstrileri ve kurumları için önemli tehditlerin açıklamasını içeren bir rapor sunulur. Raporlar şifreli e-posta mesajları aracılığıyla iletilir.

Tehdit Arama

Hizmetin öne çıkan özellikleri

- **Güvenilir İstihbarat**: Kaspersky Threat Lookup çözümünün en önemli özelliklerin biri eyleme geçirilebilir bağlam ile zenginleştirilen tehdit istihbaratı verilerimizin güvenilirliğidir. Kaspersky Lab ürünleri, kötü amaçlı yazılımlara karşı koruma testlerinde alanın lideridir[1]. Bu sonuçlar, en yüksek tespit oranlarına ve neredeyse hiç hatalı pozitif oranına sahip olan güvenlik istihbaratımızın benzersiz kalitesini gösterir.
- **Tehdit Avı**: Saldırıların etkilerini ve sıklıklarını en aza indirmek için saldırıları önleme, tespit etme ve yanıt verme konusunda proaktif olun. Saldırıları takip edin ve mümkün olduğunca çabuk ortadan kaldırın. Tehdit ne kadar erken tespit edilirse o kadar az hasar oluşur, onarımlar o kadar hızlı gerçekleşir ve ağ işlemleri o kadar çabuk normale döner.
- **Koruma Alanı Analizi**:[2] Şüpheli nesneleri güvenli bir ortamda çalıştırarak bilinmeyen tehditleri tespit edin ve kolay okunabilen raporlar aracılığıyla tehdit davranışları ve yapaylıklarının tam etki alanını inceleyin.
- **Çok Çeşitli Dışa Aktarım Biçimleri**: IOC'leri (Risk Göstergeleri) ve eyleme geçirilebilir bağlamı; STIX, OpenIOC, JSON, Yara, Snort veya CSV gibi yaygın olarak kullanılan, daha düzenli ve makine tarafından okunur paylaşma formatlarında dışarı aktarın. Bu sayede tehdit istihbaratının tüm avantajlarından yararlanabilir, işlem akışını otomatikleştirebilir veya bu akışı SIEM gibi güvenlik kontrollerine entegre edebilirsiniz.
- **Kullanımı kolay Web Arabirimi veya RESTful API**: Bu hizmeti bir web arabirimi (web tarayıcısı) aracılığıyla manuel modda kullanabilir veya hizmete basit bir RESTful API ile erişim sağlayabilirsiniz.

Siber suç, artık sınır tanımamakta ve teknik özellikleri hızla gelişmektedir. Siber suçlular hedeflerini tehdit etmek için dark web kaynaklarını kullanmaya çalıştıkça saldırıların nasıl gittikçe daha karmaşık hale geldiğini görüyoruz. Savunma araçlarınızı saf dışı bırakmak için yeni saldırı girişimleri yapılırken siber tehditler sıklık, karmaşıklık ve gizlenme açısından sürekli gelişmektedir. Saldırganlar işlerinizi aksatmak, varlıklarınızı çalmak ve müşterilerinize zarar vermek için saldırılarında karmaşık ölüm zincirleri ve özel Taktik, Teknik ve Prosedürler (TTP'ler) kullanır.

Kaspersky Threat Lookup, siber tehditler ve ilişkileri hakkında Kaspersky Lab tarafından edinilen tüm bilgileri tek ve güçlü bir web hizmeti çatısında toplar. Amaç, güvenlik ekiplerine mümkün olduğu kadar çok veri sağlamak ve siber saldırılar kurumunuza zarar vermeden onları önlemektir. Bu platform; URL'ler, etki alanları, IP adresleri, dosya karmaları, tehdit adları, istatiksel/davranışsal veriler, WHOIS/DNS verileri, dosya özellikleri, coğrafi konum verileri, indirme zincirleri, zaman damgaları vb. hakkında en yeni ve ayrıntılı Tehdit İstihbaratını bulur. Sonuç olarak, yeni ve gelişmekte olan tehditlerin global görünürlüğü elde edilir. Bu sayede kurumunuzu koruyabilir ve olay yanıtınızı geliştirebilirsiniz.

Kaspersky Threat Lookup tarafından sağlanan tehdit istihbaratı, sürekli kullanılabilirlik ve tutarlı performans sağlayan ve hatalara son derece dayanıklı bir altyapı ile gerçek zamanlı olarak oluşturulur ve izlenir. Tüm dünyadan güvenlik analistleri, GReAT ekibimizden dünyaca ünlü güvenlik uzmanları ve lider Ar-Ge ekipleri dahil olmak üzere yüzlerce uzman, bu son derece değerli ve gerçek zamanlı
akışların üretilmesine yardımcı olur.

Temel Avantajlar

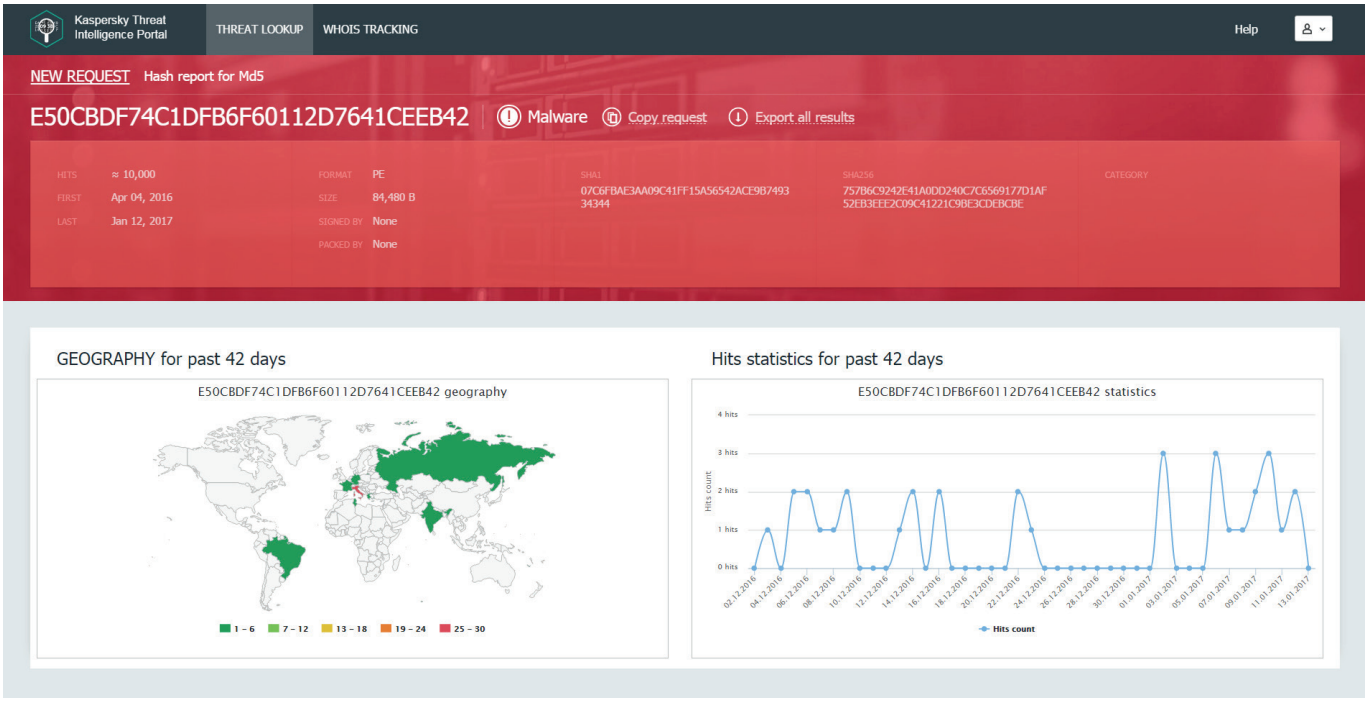
- **Olay yanıtınızı ve adli bilişim kabiliyetlerinizi geliştirir ve hızlandırır**: Güvenlik/Güvenlik İşlemleri Merkezi ekibinizin, hedefli tehditlerin arkasında yatan nedenleri anlaması için tehditler ve global veriler hakkında anlamlı bilgiler sunar. Ana bilgisayardaki ve ağdaki güvenlik olaylarını daha verimli ve etkili bir şekilde teşhis eder ve analiz eder; olay yanıtı süresini en aza indirmek ve kritik sistemler ve veriler tehlikeye girmeden ölüm zincirini durdurmak için bilinmeyen tehditlere karşı iç sistemlerden gelen sinyalleri önceliklendirir.

- **Tehdit göstergelerini derinlemesine araştırır**. IP adresleri, URL'ler, etki alanları veya dosya karmaları gibi tehdit göstergelerini son derece güvenilir tehdit bağlamıyla araştırır. Bu sayede saldırıları önceliklendirmenizi, personellere doğru görevlerin verilmesini ve işletmeniz için en büyük riski oluşturan tehditlere odaklanmanızı sağlar.

- **Hedefli saldırıların riskini azaltır**. Kurumunuzun, savunma stratejilerini geliştirerek taktiksel ve stratejik tehdit istihbaratıyla güvenlik altyapınızı geliştirir.

1 http://www.kaspersky.com/top3

2 Bu özelliğin, 2017'nin ilk yarısında piyasa sürülmesi planlanmaktadır.



Artık Şu İşlemleri Gerçekleştirebilirsiniz

- Web tabanlı ara birim veya RESTful API aracılığıyla tehdit göstergelerini arayabilirsiniz.
- Bir nesneye neden kötü amaçlı olarak davranıldığını anlayabilirsiniz.
- Fark edilen nesnenin yaygın mı yoksa özgün mü olduğunu kontrol edebilirsiniz.
- Yeni şüpheli nesneleri ortaya çıkarmak için sertifikalar, yaygın olarak kullanılan adlar, dosya yollar veya ilgili URL'ler dahil olmak üzere gelişmiş ayrıntıları inceleyebilirsiniz.

Bu özellikler yalnızca örnek olarak verilmiştir. İlgili ve granüler istihbarat verilerinden oluşan bu zengin ve sürekli kaynaktan yararlanmanın birçok yolu vardır.

Dostlarınızı ve düşmanlarınızı tanıyın. Kötü amaçlı olmadığı kanıtlanmış dosyaları, URL'leri ve IP adreslerini tanıyarak soruşturma hızınızı arttırın. Her saniyenin çok değerli olduğu bu süreçte güvenilir nesneleri analiz ederek zamanınızı kaybetmeyin.

Misyonumuz dünyayı her türlü siber tehditten korumaktır. Bu amaca ulaşmak ve interneti daha emniyetli ve güvenli bir yer haline getirmek için tehdit istihbaratlarının gerçek zamanlı olarak paylaşılması ve erişilebilmesi hayati önem taşır. Bilgilere zamanında ulaşmak, verilerinizin ve ağlarınızın etkili bir şekilde korunması için en temel unsurlardandır. Artık Kaspersky Threat Lookup ile istihbarat bilgilerine erişmek hiç olmadığı kadar verimli ve kolaydır.

Her Kaspersky Phishing Tracking bildirimi HTTPS aracılığıyla iletilir ve şunları kapsar:

- Kimlik avı URL'sinin ekran görüntüsü;
- Kimlik avı URL'sinin HTML kodu;
- Aşağıdaki alanları içeren JSON
- dosyası:
  - kimlik avı URL'si;
  - URL'nin hedef aldığı marka adı;
  - ilk kez görüldüğü tarihin damgası;
  - son görülme damgası;
  - kimlik avı URL'sinin popülerliği;
  - kimlik avı URL'sinden etkilenen kullanıcıların coğrafi konumu;
  - çalınan bilgi türü (kredi kartı bilgileri; banka, e-posta veya sosyal ağ kimlik bilgileri; kişisel bilgiler vb.);
  - saldırı türü (hesabı bloke etmek için tehdit; dosya indirme teklifi, kişisel bilgileri güncelleme talebi vb.);
  - kimlik avı URL'sinin çözülen IP adresleri;
  - WHOIS verileri;
  - ve daha birçok bilgi.

Kimlik Avı Takibi

Kimlik avı ve özellikle hedefli kimlik acı günümüzün en tehlikeli ve en etkili çevrimiçi dolandırıcılık yöntemlerinden biridir. Sahte web siteleri, kullanıcıların çevrimiçi kimliklerini ele geçirmek için oturum açma bilgilerini ve parolalarını çalar. Daha sonra saldırganlar kullanıcıların paralarını çalar veya ele geçirilen e-posta hesapları ve sosyal ağ platformları aracılığıyla istenmeyen e-postaları veya kötü amaçlı yazılımları yayar. Kimlik avı siber suç cephanesi için güçlü bir silahtır ve saldırıların sıklığı ve çeşitliliği artmaya devam etmektedir.

Bu saldırıya yalnızca finansal kuruluşlar uğramaz. Çevrimiçi satıcılar, İSS'ler ve devlet kurumları dahil olmak üzere herkes hedefli kimlik avının etkin saldırılarına maruz kalma riski taşır. Web sitenizin tüm kurumsal marka özelliklerine sahip kusursuz kopyaları veya doğrudan yöneticinizin adıyla gelen mesajlar, kullanıcıları gizli bilgileri vermeleri konusunda kolaylıkla ikna edebilir. Kullanıcılar hem kendilerine zarar verir hem de kurumlarında olası büyük bir hasara yol açabilir.

Başarılı tek bir kimlik avı saldırısının, kurum üzerinde çok büyük etkisi olabilir. Doğrudan zararların yanı sıra ele geçirilen web sitelerini ve hesapları temizleme gibi dolaylı masraflar da ortaya çıkar. Ayrıca saygınlığınıza zarar gelmesi durumuyla da karşılaşabilirsiniz. Müşterilerinizin çevrimiçi hizmetlerinize olan güvenlerinin zedelenmesi, müşterileri kaybetmenize ve gelecek yıllarda güvenilirlik konusunda sorun yaşamanıza neden olabilir. Siber suç, artık sınır tanımamaktadır ve teknik özellikleri hızla gelişmektedir. Siber suçlular hedeflerini tehdit etmek için dark web kaynaklarını kullanmaya başladıkça saldırıların nasıl gittikçe daha karmaşık hale geldiğini görüyoruz. Savunma araçlarınızı saf dışı bırakmak için yeni saldırı girişimleri yapılırken siber tehditler sıklık, karmaşıklık ve gizlenme açısından sürekli gelişmektedir. Saldırganlar işlerinizi aksatmak, varlıklarınızı çalmak ve müşterilerinize zarar vermek için saldırılarında karmaşık ölüm zincirleri ve özel Taktik, Teknik ve Prosedürler (TTP'ler) kullanır.

Çözümümüz - Kaspersky Phishing Tracking Service

Bu hizmet, markanızı hedef alan kimlik avı sitelerini takip eder ve bulunduğunda gerçek zamanlı olarak sizi uyarır. Kullanıcılarınızdan kimlik bilgilerini hassas bilgileri, finansal bilgileri ve kişisel bilgileri çalan kötü amaçlı yazılımlar ve kimlik avı URL'leri dahil olmak üzere doğrudan işletmenizle alakalı kimlik avı veya dolandırıcılık faaliyetleri hakkında ilgili, doğru veya ayrıntılı raporlar hazırlar. Ayrıca bu hizmeti kullanarak kimlik avı siteleri için belirli üst düzey etki alanlarını hatta bölgeleri izleyebilirsiniz

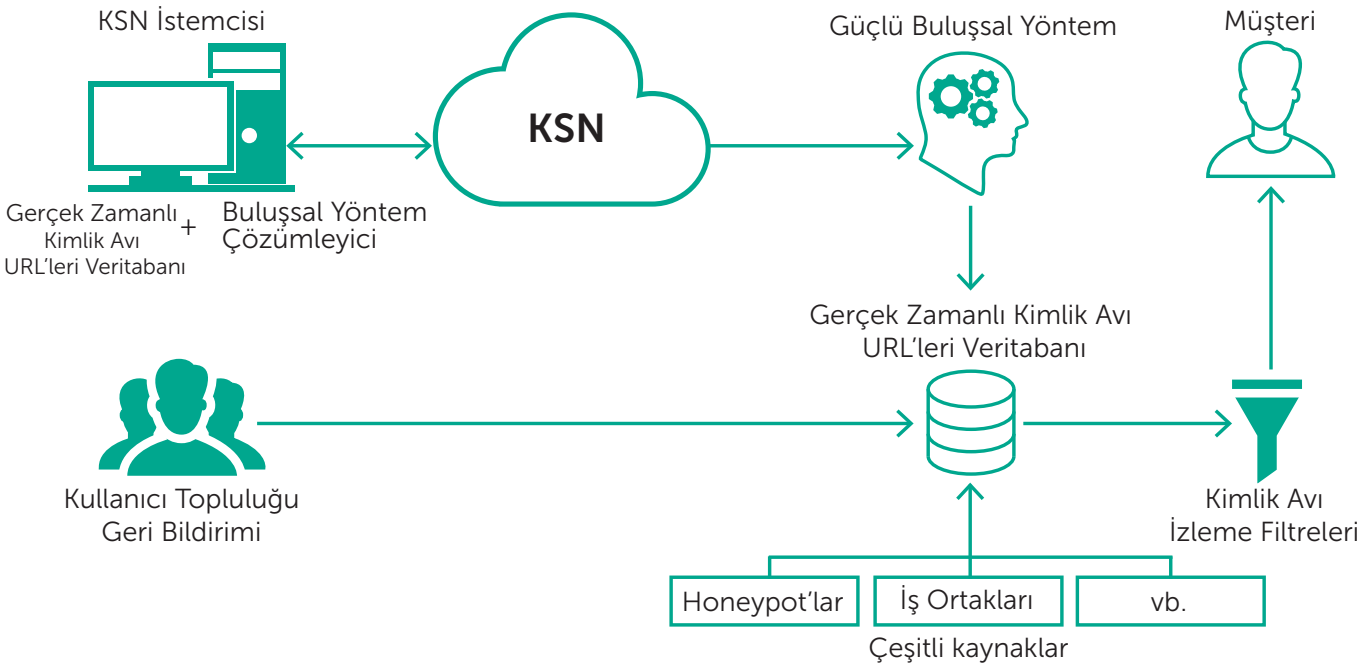
Markalarınıza, şirket adınıza veya ticari markalarınıza karşı onaylanan kimlik avı saldırıları hakkında sürekli olarak e-posta bildirimleri gönderilir. Her bildirim, gittikçe karmaşık hale gelen kimlik avı saldırıları hakkında derin bir araştırma, yüksek doğruluk derecesi ve güvenilir bilgi sunar. Bu sayede dinamik olarak üretilen kimlik avı salgınlarının yanı sıra kimlik avı etki alanları ve URL'lerine hızlı bir şekilde tepki verebilirsiniz. Kimlik avı sitelerini içeren bir listenin yanı sıra her türlü kimlik avı saldırısına karşı anında belirli önlemleri alabileceğin ek istihbarat bilgileri sunulur.

Bu güncel ve profesyonel olarak onaylanmış istihbarat bilgileri sayesinde, dolandırıcılığa karşı proaktif bir tutum alarak kurumunuz ve müşterileriniz ile ilgili kimlik avı faaliyetlerinin etkisini azaltmak için hızlı ve hassas bir şekilde hareket edebilirsiniz.

İstihbarat kaynakları

Kaspersky Phishing Tracking; güçlü sezgisel motorlar, e-posta sanal sunucuları, web gezginleri, Kaspersky Security Network (KSN), istenmeyen posta tuzakları, araştırma ekipleri ve kötü amaçlı nesneler hakkında son 2 yıldır topladığımız veriler dahil olmak üzere heterojen ve son derece güvenilir istihbarat kaynaklarından gelen verileri birleştirir. Daha sonra toplanan veriler gerçek zamanlı olarak denetlenir ve sadeleştirilir. Bu işlemler için istatistik kriterleri, Kaspersky Lab Uzman Sistemleri

(koruma alanları, sezgisel motorlar, benzerlik araçları ve davranış profili oluşturma) içerik analisti doğrulaması ve beyaz liste onaylama araçları gibi birçok ön işleme tekniği kullanılır.
Kaspersky Security Network çözümünün dünya çapındaki kapsama alanı ile Kaspersky Lab tespit teknolojileri ve test ve filtrelerden oluşan bir setin birleşmesi,



neredeyse hiç hatalı pozitif olmadan her türlü kimlik avı saldırısı ve tehdidinin maksimum tespitini sağlar. Bu başarı, sürekli olarak bağımsız testlerle de kanıtlanmaktadır.

Kimlik Avı Saldırıları Hakkında Erken Uyarı

Kaspersky Phishing Tracking hizmetine abone olmak size saldırganlar karşısında avantaj sağlar. Devam eden veya planlanan ve markalarınızı, çevrimiçi hizmetlerinizi ve müşterilerinizi hedef alan kimlik avı saldırıları hakkında erken uyarı almak, kaynaklarınızı korumanıza ve riskleri daha pragmatik, daha doğru ve daha uygun maliyetle azaltmanıza yardımcı olur.

Saldırganların Önüne Geçin

Bu hizmet, gelişmiş saldırıların planlandığını veya başladığını belirten kötü amaçlı faaliyetler hakkında düzenli raporların yanı sıra gerçek zamanlı olarak kritik bilgiler paylaşır. Artık saldırganlar değil siz bir adım öne geçerek onları gözetleyebilirsiniz.

Kullanıcı Deneyimini Geliştirme

Hedefli kimlik avı saldırganlarınızı öğrendikten ve anladıktan sonra, eskimiş yazılımların yasaklanmasından SMS tabanlı doğrulamaya kadar farklı tekniklerle uygun koruma stratejinizi planlayabilirsiniz. Tüm bu önlemler, çevrimiçi müşterilerinizin daha korumalı ve güvenli hissetmelerini sağlar.

Etkiyi En Aza İndirme

Kimlik avı web sitelerinin URL'lerini bilmek, siteleri barındıran ISS'lerin uyarılabileceği anlamına gelir. Bu sayede, site tarafından edinilen kişisel bilgileri daha fazla yayılması önlenir ve saldırılar durdurulur.

Daha İyi Bilgilendirme

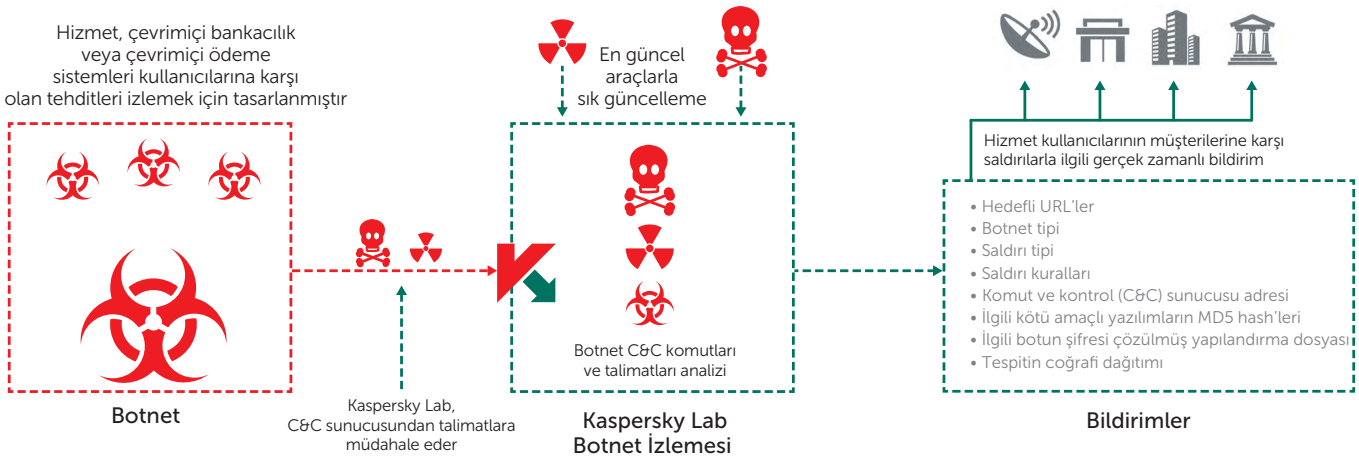
Hiç "hatalı pozitif" veya zaman kaybettirici veriler içermeyen bu ilgili, doğru ve ayrıntılı bilgi akışı, sizi bilgilendirmeye ve şu andaki ve gelecekteki güvenlik stratejinizi geliştirmeye yardımcı olur. İşletmeniz artık çevrimiçi dolandırıcılığa karşı proaktif ve bilinçli bir tutum sergileyebilir.

AV comparatives Approved 2016 Anti-Phishing

* Talep edilmesi halinde AV karşılaştırmalı test raporlarına erişilebilir.

Botnet Takibi

Müşterileriniz ve saygınlığınızı tehdit eden botnetleri bulmak için uzman izleme ve bildirim hizmetleri.



Kullanım Alanları/Hizmet Avantajları

- Çevrimiçi kullanıcılarınızı hedef alan botnetlerle ilgili tehditler hakkında proaktif uyarılar almak, her zaman saldırganlardan bir adım önde olmanızı sağlar
- Çevrimiçi müşterilerinizi hedef alan Komuta ve Kontrol sunucusu URL'lerinden oluşan bir listeye sahip olmak, CERT'lere veya emniyet teşkilatlarına talep göndererek bu URL'leri engellemenizi sağlar
- Saldırının yapısını anlayarak çevrimiçi bankacılık/ödeme noktalarınızın güvenliğini arttırabilirsiniz
- Bu saldırılarda kullanılan sosyal mühendislik tehlikelerini fark etmeleri ve bunlardan kaçınmaları için çevrimiçi müşterilerinizi bilgilendirebilirsiniz

Gerçek zamanlı olarak sunulan bilgilerle harekete geçin:

Bu hizmet, Kaspersky Lab tarafından izlenen botnetlerdeki anahtar kelimeleri takip ederek eşleşen marka adlarıyla ilgili istihbarat bilgilerini içeren kişisel bildirimlere abone olma imkânı sunar. Bildirimler HTML veya JSON formatında e-posta veya RSS aracılığıyla iletilebilir. Bildirimler aşağıdaki bilgileri içerir:

- **Hedeflenen URL'ler**: Bot kötü amaçlı yazılımı, kullanıcı hedeflenen kurumun URL'sine erişim sağlayana kadar beklemek ve daha sonra saldırmak için tasarlanmıştır.
- **Botnet türü**: Siber suçlunun, müşterilerinizin işlemlerinin tehlikeye sokmak için tam olarak hangi kötü amaçlı yazılım tehdidini kullandığını anlayabilirsiniz. Bu yazılımlara örnek olarak Zeus, SpyEye ve Citadel verilebilir.
- **Saldırı türü**: Saldırganların kötü amaçlı yazılımı ne için kullandığını öğrenin (örneğin, web verileri ekleme, ekran kaydırma, video çekme veya kimlik avı URL'lerini iletme vb.).
- **Saldırı kuralları**: HTML talepleri (GET / POST) gibi hangi web kodu ekleme kurallarının kullanıldığını, eklemeden önce web sayfasının verilerini ve eklemeden sonra web sayfasının verilerini öğrenin.
- **Komuta ve Kontrol (C&C) sunucu adresleri**: Tehdidi daha hızlı yok etmek için suç işlenmesine neden olan sunucunun internet servis sağlayıcısını bilgilendirmenizi sağlar.
- **İlgili kötü amaçlı yazılımın MD5 karmaları**: Kaspersky Lab kötü amaçlı yazılım doğrulaması için kullanılan karma toplamını sunar.
- **İlgili botun şifresi çözülen yapılandırma dosyası**: Hedeflenen URL'lerin tam listesine ulaşmanızı sağlar.
- **Tespitin coğrafi dağılım (ilk 10 ülke)**: Dünya genelinden ilgili kötü amaçlı yazılım hakkındaki istatiksel veriler.

Kaspersky Tehdit Avlama Hizmetleri

Tüm sektörlerdeki güvenlik ekipleri, sürekli olarak gelişen siber tehditlere karşı kapsamlı koruma sağlamaya yönelik sistemler üretmek için çok çalışır. Ancak bu sistemlerin çoğu güvenlik olaylarına "uyarı" tabanlı bir yaklaşımla bakar. Yani yalnızca olay gerçekleştikten sonra tepki verilir. Son araştırmalara göre, güvenlik olaylarının büyük bir kısmı tespit bile edilemez. Bu tehditler radardan saklanarak, işletmelerin güvende olduğu yanılgısına kapılmalarını sağlar. Sonuç olarak gittikçe daha çok kurum, henüz tespit edilmeyen ancak altyapılarında gizlenen tehditleri proaktif olarak avlama gereğini anlamaya başlamıştır. Kaspersky Tehdit Avlama Hizmetleri, son derece nitelikli ve deneyimli güvenlik uzmanları tarafından yürütülen tehdit avlama tekniklerini kullanarak kurumun içinde gizlenen gelişmiş tehditlerin ortaya çıkarılmasına yardımcı olur.

Kaspersky
Siber Güvenlik Hizmetleri

- **Kaspersky Tehdit İstihbarat Hizmetleri**
- **Kaspersky Tehdit Avlama Hizmetleri**
  Kaspersky Managed Protection
  Targeted Attack Discovery
- **Kaspersky Güvenlik Eğitimi**
- **Kaspersky Olay Yanıt Hizmetleri**
- **Kaspersky Güvenlik Değerlendirme Hizmetleri**

Kaspersky Managed Protection

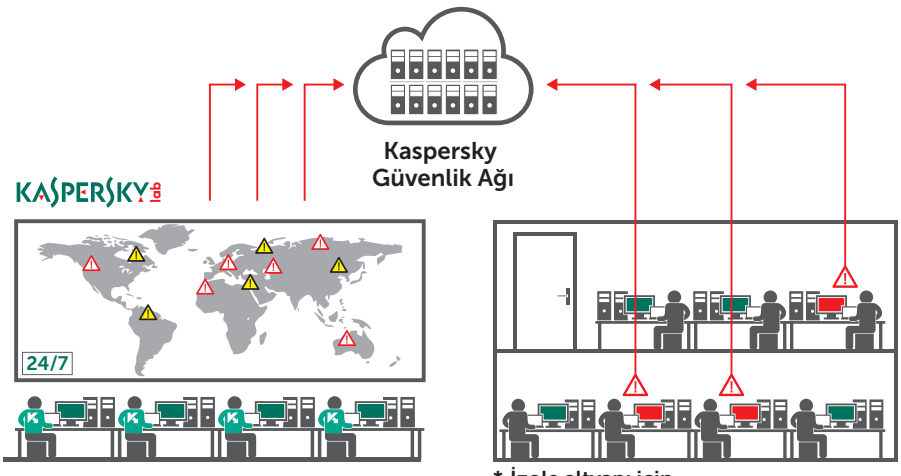
Kaspersky Managed Protection hizmeti, Kaspersky Endpoint Security ve Kaspersky Anti Targeted Attack Platform kullanıcılarına kurumlarındaki hedefli saldırıları tespit etmek ve önlemek için gelişmiş teknik önlemlerden oluşan benzersiz bir birleşim kullanarak tam yönetimli bir hizmet sunar. Bu hizmet, Kaspersky Lab uzmanlarının sürekli gözetimini ve siber tehdit verilerinin sürekli analizini içerir. Bu sayede, kritik bilgi sistemlerini hedef alan eski ve yeni siber casusluk ve siber suç saldırılarının gerçek zamanlı tespiti sağlanır.

Hizmetin öne çıkan özellikleri

- Hedefli saldırılara ve kötü amaçlı yazılımlara karşı sürekli yüksek düzeyde koruma sağlar. Kaspersky Lab uzmanları, uzmanlık becerilerini ve tehdit istihbaratını kullanarak 7/24 izleme ve destek hizmeti sunar.
- Kötü amaçlı yazılımların kullanılmadığı, daha önce bilinmeyen araçları içeren ve sıfır gün açıklarından yararlanan yazılımların bulunduğu saldırıların zamanında ve doğru şekilde tespit edilmesi sağlanır.
- Otomatik antivirüs veritabanıyla tespit edilen tehditlere karşı anında koruma sağlanır.
- Tehdit aktörleri tarafından kurumunuza karşı kullanılan yöntem ve teknolojileri içeren olayların ve tehdit avlamanın geçmişe dönük analizi.
- Entegre yaklaşım: Kaspersky Lab portföyü, hedefli saldırılara karşı uygulamanız gereken teknoloji ve hizmetlerin tam döngüsünü içerir: Hazırlık - Tespit - Soruşturma - Veri Analizi - Otomatik Koruma.

Hizmetin avantajları

- Daha hızlı ve etkili risk azaltma ve onarım sağlayan hızlı ve etkili tespit sağlanır.
- Her türlü şüpheli faaliyetin net olarak anında tanımlanması ve sınıflandırılması sayesinde zaman kaybettirici hatalı pozitifler olmaz.
- Genel güvenlik maliyetleri azaltılır. Şirket içinde ihtiyaç duyabileceğini kurum içi uzmanlarını işe almanıza veya eğitmenize gerek kalmaz.
- En karmaşık ve yenilikçi kötü amaçlı yazılım kullanmayan tehditlere karşı bile sürekli olarak korunduğunuzu bilmenin rahatlığını yaşayabilirsiniz.
- Saldırganlar, motivasyonları, yöntemleri, araçları ve oluşturabilecekleri potansiyel hasarlar hakkında bilgi edinebilirsiniz. Bu sayede bilinçli ve etkili bir güvenlik stratejisi geliştirmeniz desteklenir.



Hizmetle ilgili ayrıntılar

Kaspersky Targeted Attack Discovery aşağıdaki faaliyetleri gerçekleştirebilir:

Tehdit istihbaratı toplama ve analiz. Amaç, saldırı yüzeyinin zamanında bir anlık görüntü elde etmek. Siber suç ve siber saldırı tehditleri ve saldırıları potansiyel olarak veya aktif olarak varlıklarınızı hedefliyor. Kaspersky Lab izleme sistemlerinin yanı sıra yeraltı dolandırıcılık şebekeleri dahil olmak üzere iç ve dış istihbarat kaynaklarından faydalanırız. Bu istihbarat bilgilerini analiz etmek altyapınızdaki zayıf noktalar, siber suçluların ilgi duyduğu alanlar veya ele geçirilen hesaplar gibi bilgilere ulaşmamızı sağlar.

Yerinde veri toplama ve erken olay yanıtı. Kendi laboratuvarlarımızdan yürütülen tehdit istihbaratı faaliyetlerinin yanı sıra Kaspersky Lab uzmanları ağ ve sistem yapılarını ve kullanılabilir SIEM bilgilerini toplar. Ayrıca anında harekete geçebilmek için en kritik güvenlik hatalarını ortaya çıkarmak amacıyla kısa bir güvenlik açığı değerlendirmesi de yapabiliriz. Olay zaten gerçekleşmişse soruşturma için delil toplarız. Bu aşamada size kısa vadeli onarım adımları için ara tavsiyelerde bulunuruz.

Veri analizi. Toplanan ağ ve sistem yapıları, sisteminizde tam olarak ne olduğunu anlamak için Kaspersky Lab'in Risk Göstergeleri bilgi tabanı, Komuta ve Kontrol kara listeleri, korumalı alan teknolojisi vb. araçları kullanılarak laboratuvarda analiz edilir. Bu aşamada yeni kötü amaçlı yazılımlar fark edilirse bu yazılımları anında tespit edebilmeniz için gereken tavsiye ve araçları (ör. YARA kuralları) size sunarız. Bu süre boyunca sizinle sürekli iletişim içinde olarak uygun olduğu takdirde sistemleriniz üzerinde uzaktan çalışırız.

Rapor hazırlama. Son olarak hedefli saldırı keşif sonuçlarımızı ve onarım faaliyetleri için önerilerimizi içeren resmi raporumuzu hazırlarız.

Targeted Attack Discovery

Kaspersky Lab uzmanları, işletme varlıklarınızın gerçek güvenliğini sağlamak için proaktif Targeted Attack Discovery hizmetini sunar.

Targeted Attack Discovery sonuçları, ağınızda geçerli siber suç ve siber casusluk faaliyetlerini tanımlamanızı, bu olayların arkasındaki nedenleri veya olası kaynakları anlamanızı ve gelecekte benzer saldırılardan kaçınmak için etkili risk azaltma planları oluşturmanızı sağlar. Sektörünüze yöneltilen saldırılar hakkında endişeliyseniz, kendi sistemlerinizde olası şüpheli davranışlar fark ettiyseniz veya kurumunuz düzenli önleyici denetimlerin faydalı olduğunu düşünüyorsa Kaspersky Targeted Attack Discovery hizmetleri sizin için aşağıdaki soruları cevaplamaya hazırdır:

- Şu anda saldırı altında mısınız? Bu saldırı kim tarafından ve nasıl düzenleniyor?
- Saldırı sistemlerinizi nasıl etkiliyor? Bu konuda neler yapabilirsiniz?
- Gelecekteki saldırılardan nasıl korunabilirsiniz?

Bu hizmet nasıl çalışır?

Dünya çapında tanınan bağımsız uzmanlarımız ağınızda devam eden olayları, gelişmiş kalıcı tehditleri (APT'ler), siber suç ve siber casusluk faaliyetlerini ortaya çıkarır, tanımlar ve analiz eder. Bu da kötü amaçlı faaliyetleri açığa çıkarmanıza, olayların olası kaynaklarını anlamanıza ve en etkili onarım eylemlerini planlamanıza yardımcı olur.

Bu işlemleri aşağıdakiler yaparak gerçekleştiririz:

- Kurumunuza özel tehdit manzarasını anlamak için istihbarat kaynaklarını analiz etme
- Olası risk belirtilerini açığa çıkarmak için BT altyapınızda ve verilerinizde (günlük dosyaları gibi) derinlemesine taramalar yapma
- Herhangi şüpheli bir faaliyetin olup olmadığını anlamak için giden ağ bağlantılarınızı analiz etme
- Saldırının olası kaynaklarını ve ele geçirilmesi muhtemel olan diğer sistemleri ortaya çıkarma

Sonuçlar

Sonuçlarımız şunları içeren ayrıntılı bir rapor şeklinde sunulur:

Tüm keşiflerimiz: ağınızda risk belirtilerinin olduğu veya olmadığına dair teyit

Derinlemesine analiz: toplanan tehdit istihbarat verileri ve ortaya çıkarılan Risk Göstergeleri'nin (IOC'ler) analizi.

Ayrıntılı açıklamalar: yararlanılan güvenlik açıklamaları, olası saldırı kaynakları ve etkilenen ağ bileşenlerine dair açıklamalar.

Onarım tavsiyeleri: ortaya çıkan olayın sonuçlarının etkisini en aza indirmek ve kaynaklarınızı gelecekteki benzeri saldırılardan korumak için önerilen adımlar.

Ek hizmetler

Ayrıca uzmanlarımızdan olayın belirtilerini analiz etmelerini, belirli sistemler için derin dijital analiz yapmalarını, kötü amaçlı yazılım ikilisini (varsa) tanımlamalarını ve kötü amaçlı yazılım analizi gerçekleştirmelerini isteyebilirsiniz. Bu isteğe bağlı hizmetler, daha çok onarım tavsiyesiyle ayrı raporlar halinde sunulur.

Ayrıca ağınıza kalıcı olarak veya "kavram kanıtlama" çalışması şeklinde **Kaspersky Anti Targeted Attack (KATA) Platform** çözümünü uygulayabiliriz. Bu platform, hedefli saldırıları hızlıca tespit etmek ve yanıt vermek için en son teknolojileri ve global analizleri birleştirerek sisteminizdeki saldırı yaşam döngüsünün tüm aşamalarında saldırıyla mücadele eder.

Kaspersky Güvenlik Eğitimi

Siber güvenlik eğitimi, sürekli gelişen tehditlerin günden güne artmasıyla karşı karşıya kalan şirketler için en önemli araçlardandır. BT Güvenlik personeli, etkili kurumsal tehdit yönetiminin ve risk azaltma stratejilerinin önemli bir bileşenini oluşturan gelişmiş teknikler konusunda becerili olmalıdır.

Kaspersky
Siber Güvenlik Hizmetleri

- **Kaspersky Tehdit İstihbarat Hizmetleri**
- **Kaspersky Tehdit Avlama Hizmetleri**
- **Kaspersky Güvenlik Eğitimi**
  - Adli Bilişim
  - Kötü Amaçlı Yazılım Analizi ve Tersine Mühendislik
  - İleri Adli Bilişim
  - Gelişmiş Kötü Amaçlı Yazılım Analizi ve Tersine Mühendislik
  - Olay Yanıtı
  - Yara
  - KATA Yönetimi
  - KATA Güvenlik Analizi
- **Kaspersky Olay Yanıt Hizmetleri**
- **Kaspersky Güvenlik Değerlendirme Hizmetleri**

Bu kurslar, siber güvenlik konuları ve teknikleri konusunda geniş bir müfredat ve başlangıç seviyesinden uzman seviyesine kadar farklı değerlendirme yöntemleri sunar. Tüm bu eğitimler, müşteri tesislerinde veya Kaspersky yerel ya da bölgesel ofislerinde sınıf içi şeklinde verilebilir.

Kurslar, hem teorik dersleri hem de uygulamalı "laboratuvarlar" derslerini içerecek şekilde tasarlanmıştır. Tamamlanan her kurstan sonra katılımcılar, bilgilerini değerlendirmek için bir değerlendirme testi tamamlaya davet edilir.

Hizmetin Avantajları

Adli Bilişim ve İleri Düzey Adli Bilişim

Kurum içindeki adli bilişim ve olay yanıtı ekiplerinizin uzmanlıkları arttırılır. Kurslar, saldırı zaman dilimlerini ve kaynaklarını geri getirmek için dijital siber suç kanıtlarını arama ve farklı türlerdeki verileri analiz etme konusundaki pratik becerileri geliştirerek ve ilerleterek deneyim boşluğunu kapatmak için tasarlanmıştır. Kurs tamamlandıktan sonra öğrenciler bilgisayar olaylarını başarılı bir şekilde soruşturabilir ve işletmenin güvenlik seviyesini arttırabilir.

Kötü Amaçlı Yazılım Analizi ve Tersine Mühendislik ve Gelişmiş Kötü Amaçlı Yazılım Analizi ve Tersine Mühendislik

Tersine mühendislik eğitimi, olay yanıtı ekiplerine kötü amaçlı saldırıların soruşturulması konusunda yardımcı olmak için tasarlanmıştır. Bu kurs, BT departmanı çalışanları ve sistem yöneticilerine yöneliktir. Öğrenciler kötü amaçlı yazılımları analiz etmeyi, IOC'leri (Risk Göstergeleri) toplamayı, virüslü makinelerde tespit edilen kötü amaçlı yazılımlar için imza yazmayı ve virüslü/şifreli dosyaları ve belgeleri kurtarmayı öğrenir.

Olay Yanıtı

Kurslar, şirket içindeki ekibinizi olay yanıt sürecinin tüm aşamalarından geçirmek için yönlendirir ve başarılı olay onarımı için gereken kapsamlı bilgilerle donatır.

Yara

Katılımcılara, en etkili Yara kurallarını yazmayı, onları nasıl test edeceklerini ve başka hiçbir aracın bulamadığı tehditleri bulacak şekilde nasıl geliştireceklerini öğretir.

KATA Yönetimi

KATA Yönetim Eğitimi, tehdit tespit etkililiğini optimize etmek için çözümü planlama, yükleme ve yapılandırmak için gereken tüm teknik bilgileri verir.

KATA Güvenlik Analizi

Bu eğitim, gerçek tehdit senaryolarına bağlı bir grup uygulamalı alıştırmadan oluşur. Katılımcılara KATA uyarılarını güvenli bir şekilde izlemek, yorumlamak ve yanıtlamak için gereken bilgiyi sağlar.

Uygulamalı Deneyim

Lider güvenlik tedarikçisi Kaspersky Lab'in sunduğu bu eğitimde katılımcılar global uzmanlarımızla birlikte çalışma ve öğrenme fırsatı yakalar. Siber suç tespiti ve önleme konusunda "cephede" mücadele eden bu uzmanlar kendi deneyimleriyle katılımcılara ilham kaynağı olur.

Program Açıklaması

Konular	Süre	Kazanılan beceriler
Adli Bilişim		
• Adli Bilişime Giriş • Canlı yanıt ve kanıt toplama • Windows kayıt iç ögeleri • Windows yapı analizi • Tarayıcı adli bilişimi • E-posta analizi	5 gün	• Adli Bilişim laboratuvarı oluşturma • Dijital kanıt toplama ve kanıtlarla uygun şekilde ilgilenme • Olayı yeniden oluşturma ve zaman damgaları kullanma • Windows İşletim Sistemindeki yapıtlara dayalı olarak yetkisiz erişim izlerini bulma • Tarayıcı ve e-posta geçmişini bulma ve analiz etme • Adli bilişim araçlarını ve gereçlerini uygulayabilme
Kötü Amaçlı Yazılım Analizi ve Tersine Mühendislik		
• Kötü Amaçlı Yazılım Analizi ve Tersine Mühendislik amaçları ve teknikleri • Windows iç ögeleri, yürütülebilir dosyalar, x86 birleştirme • Temel statik analiz teknikleri (dizileri ayıklama, içe aktarma analizi, • Bir bakışta PE girdi noktaları, otomatik paket açma vb.) • Temel dinamik analiz teknikleri (hata ayıklama, izleme araçları, trafik engelleme vb.) • .NET, Visual Basic, Win64 dosyaları analizi • Komut dosyası analizi ve PE olmayan analiz teknikleri (Batch files; Autoit; Python; JScript; JavaScript; VBS)	5 gün	• Kötü amaçlı yazılım analizi için güvenli ortam oluşturma: koruma alanı ve tüm gerekli araçların uygulanması • Windows program yürütme ilkelerini anlama • Paketi açma, hataları ayıklama ve kötü amaçlı nesneleri analiz etme, işlevlerini tanımlama • Komut dosyası kötü amaçlı yazılım analizi ile kötü amaçlı siteleri tespit etme • Hızlı kötü amaçlı yazılım analizi gerçekleştirme
İleri Adli Bilişim		
• Windows için Kapsamlı Adli İnceleme • Veri kurtarma • Ağ ve bulut adli incelemesi • Bellek adli incelemesi • Zaman çizelgesi analizi • Gerçek hayattan hedefli saldırılarla adli bilişim uygulaması	5 gün	• Derin dosya sistem analizi gerçekleştirme • Silinen dosyaları geri kurtarabilme • Ağ trafiğini analiz edebilme • Dökümlerden kötü amaçlı yazılımları bulabilme • Olay zaman çizelgesini yeniden oluşturabilme
Gelişmiş Kötü Amaçlı Yazılım Analizi ve Tersine Mühendislik		
• Kötü Amaçlı Yazılım Analizi ve Tersine Mühendislik amaçları ve teknikleri • Gelişmiş statik analiz teknikleri (shellcode'u statik olarak analiz eme, PE üst bilgisini ayrıştırma, TEB, PEB, farklı karma algoritmalarına göre yükleme fonksiyonları) • Gelişmiş dinamik analiz teknikleri (PE yapısı, manuel ve gelişmiş paket açma, tüm yürütülebilir dosyaları şifreli bir biçimde depolayan kötü amaçlı paketleyicilerin paketini açma) • APT için tersine mühendislik (kimlik avından başlayarak mümkün olduğunca derin konulara kadar bir APT saldırı senaryosunu kapsar) • Protokol analizi (şifreli Komuta ve Kontrol iletişim protokolünü analiz etme ve trafiği deşifre etme) • Rootkit ve Bootkit analizi (Ida ve VMWare kullanarak önyükleme kesiminin hatalarını ayıklama, 2 sanal makine kullanarak çekirdek hatalarını ayıklama, Rootkit numunelerini analiz etme)	5 gün	• Tersine mühendislik konusunda en iyi uygulamaları öğrenirken aynı anda tersine mühendisliğe (gizlenme, hata ayıklamaya karşı koruma) karşı hileleri fark edebilme • Rootkit/Bootkit tahlili için gelişmiş kötü amaçlı yazılımı uygulayabilme • Farklı dosya türlerine ve Windows'a yönelik olmayan kötü amaçlı yazılımlara gömülü açıklardan yararlanan yazılım shellcode'unu ve analiz edebilme

Program Açıklaması

Konular	Süre	Kazanılan beceriler
Olay Yanıtı		
• Olay Yanıtına Giriş • Tespit ve ön analiz • Dijital analiz • Tespit kurallarını oluşturma (YARA, Snort, Bro)	5 gün	• APT'leri diğer tehditlerden ayırt etme • Çeşitli saldırgan tekniklerini ve hedefli saldırı anatomisini anlama • Belirli izleme ve tespit yöntemlerini uygulama • Olay yanıtı iş akışını takip etme • Olay kronolojisi ve mantığını yeniden oluşturma • Tespit kuralları oluşturma ve raporlama
Yara		
• Yara söz dizimine kısa giriş • Hızlı ve etkili kuralları oluşturmak için ipuçları ve tüyolar • Yara oluşturucu • Hatalı pozitif sonuçlar için Yara kurallarını test etme • VT'de yeni tespit edilmemiş numuneleri avlama • Etkili tehdit avlama için dış modülleri kullanma • Anormallik araması • Gerçek hayattan birçok (!) örnek • Yara becerilerini geliştirmek için bazı örnekler	2 gün	• Etkili Yara kuralları oluşturma • Yara kurallarını test etme • Yara kurallarını başka hiçbir aracın bulamadığı tehditleri bulacak şekilde geliştirme
KATA Yönetimi		
• Yaygın Çözüm Dağıtım Senaryoları ve Sunucu Konumları • Boyutlandırmayla İlgili Hususlar • Lisanslama Modeli • Korumalı Alan Sunucusu • Merkezi Düğüm • Sensör • Altyapı ile Entegrasyon • Uç Nokta Sensörü Kurulum • Lisans Ekleme ve Veritabanlarını Güncelleme • Çözümü Çalıştırma Algoritması	1 gün	• Müşteri ortamına yönelik uygulama planını tasarlama • Tüm KATA bileşenlerini yükleme ve kurma • Çözümü koruma ve izleme
KATA Güvenlik Analizi		
• KATA uyarılarını yorumlama • Tespit ve analiz teknolojileri açıklaması • Puanlama ve risk motorları açıklaması	1 gün	• Puanlamanın nasıl çalıştığını ve motorlar tarafından nasıl kullanıldığını anlama • KATA uyarılarını güvenli bir şekilde izleme, yorumlama ve yanıtlama

Kaspersky Olay Yanıt Hizmetleri

BT ve güvenlik uzmanlarınız, her ağ bileşeninin hem saldırganlara karşı güvenli hem de gerçek kullanıcılara karşı tamamen kullanılabilir olması için çok çalışır. Ancak yine de tek bir güvenlik açığı, bilgi sistemlerinizin kontrolünü ele geçirmeye çalışan her türü siber suçluya açık bir kapı bırakabilir. Hiç kimse bundan muaf değildir. Güvenlik kontrolleriniz ne kadar güçlü olursa olsun saldırıya maruz kalabilirsiniz.

Bilgi güvenlik olaylarını önlemek, her geçen gün zorlaşmaktadır. Bir saldırıyı, güvenlik çevrenize girmeden önce durdurmak her zaman için mümkün olmasa da ortaya çıkan hasarı sınırlamak ve saldırının yayılmasını önlemek kesinlikle bizim elimizdedir.

Kaspersky
Siber Güvenlik Hizmetleri

- **Kaspersky**
  Tehdit İstihbarat Hizmetleri
- **Kaspersky**
  Tehdit Avlama Hizmetleri
- **Kaspersky**
  Güvenlik Eğitimi
- **Kaspersky**
  Olay Yanıt Hizmetleri

  Olay Yanıtı
  Kötü Amaçlı Yazılım Analizi
  Adli Bilişim
- **Kaspersky**
  Güvenlik Değerlendirme
  Hizmetleri

Olay Yanıtı'nın genel amacı bir güvenlik ihlâlinin veya BT ortamınıza yapılan bir saldırının etkilerini azaltmaktır. Bu hizmet, kanıtların yerinde toplanmasından ek risk göstergelerinin tanımlanmasına, onarım planı hazırlanmasına ve tehdidi kurumunuzdan tamamen kaldırmaya kadar tüm olay soruşturma döngüsünü kapsar.

Bu işlemleri aşağıdakiler yaparak gerçekleştiririz:

- Ele geçirilen kaynakların tanımlanması.
- Tehdidin izole edilmesi.
- Saldırının yayılmasının durdurulması.
- Kanıtların bulunması ve toplanması.
- Kanıtların analiz edilmesi ve olay kronolojisinin ve mantığının yeniden oluşturulması.
- Saldırıda kullanılan kötü amaçlı yazılımın analizi (kötü amaçlı yazılım bulunduysa).
- Saldırının kaynaklarının ve ele geçirilmesi muhtemel olan diğer sistemlerin ortaya çıkarılması (mümkünse).
- Olası risk göstergelerini ortaya çıkarmak için BT altyapınızda araç destekli taramaların gerçekleştirilmesi.
- Şüpheli şeyleri (olası komuta ve kontrol sunucuları gibi) tespit etmek için ağınız ve dış kaynaklar arasında giden bağlantıların analizi.
- Tehdidin ortadan kaldırılması.
- Yapabileceğiniz ek düzeltme eylemlerinin önerilmesi.

Kendi olay yanıtı ekibinizin olup olmamasına bağlı olarak uzmanlarımızdan tüm soruşturma döngüsünü tamamlamayı, yalnızca ele geçirilen makinelerin tanımlanmasını, izole edilmesini ve tehdidin yayılmasını önlemeyi ya da Kötü Amaçlı Yazılım Analizi veya Adli Bilişim işlemlerini gerçekleştirmelerini isteyebilirsiniz.

Kaspersky Lab'in Olay Yanıtı Hizmetleri, son derece deneyimli siber saldırı tespiti analistleri ve araştırmacıları tarafından yürütülür. Global uzmanlığımız sayesinde güvenlik olayınızın çözümü için Adli Bilişim ve Kötü Amaçlı Yazılım Analizi kullanılabilir.

Kötü Amaçlı Yazılım Analizi

Kötü Amaçlı Yazılım Analizi, kurumunuzu hedef alan belirli kötü amaçlı yazılım dosyalarının davranışlarını ve amaçlarını tam olarak anlamanızı sağlayabilir. Kaspersky Lab'in uzmanları, sağladığınız kötü amaçlı yazılım örneği üstünde kapsamlı bir analiz gerçekleştirir ve aşağıdakileri içeren ayrıntılı bir rapor hazırlar:

- **Numunenin özellikleri:** Numunenin kısa bir açıklaması ve kötü amaçlı yazılım sınıflandırmasıyla ilgili karar.

- **Ayrıntılı kötü amaçlı yazılım açıklaması:** IOC'ler dahil olmak üzere kötü amaçlı yazılım numunenizin fonksiyonları, tehdit davranışları ve amaçlarının kapsamlı bir analizi, yazılımın faaliyetlerini önlemek için gereken bilgileri sağlar.

- **Düzeltme senaryosu:** Bu rapor, bu tür tehditlere karşı kurumunuzun güvenliğini sağlamak için adımlar önerir.

Adli Bilişim

Araştırma sırasında herhangi bir kötü amaçlı yazılım tespit edildiyse Adli Bilişim süreci yukarıda bahsedilen kötü amaçlı yazılım analizini içerebilir. Kaspersky Lab uzmanları, tam olarak ne olduğunu anlamak için HDD görüntüleri, bellek dökümleri ve ağ izleri dahil olmak üzere farklı kanıtları bir araya getirir. Sonuç olarak olayın ayrıntılı bir açıklaması elde edilir. Siz, müşteri olarak kanıtları toplama ve olayın bir özetini sağlamak işlemleriyle süreci başlatırsınız. Kaspersky Lab uzmanları; onarım adımlarını içeren ayrıntılı bir rapor sunmak için kötü amaçlı yazılım ikilisini (varsa) tanımlayarak ve kötü amaçlı yazılım analizini gerçekleştirerek olay belirtilerini analiz eder.

İletim seçenekleri

Kaspersky Lab'in Olay Yanıt Hizmetleri aşağıdaki şekillerde kullanılabilir:

- Abonelik ile
- Tek bir olaya yanıt vermek için

Her iki seçenekte uzmanlarımızın olayı çözmek için harcadığı zamana bağlıdır. Bu konu, sözleşme imzalanmadan önce görüşülür. Çalışmamızı istediğiniz saat sayısını belirtebilirsiniz ya da olaya ve bireysel gereksinimlerinize bağlı olarak uzmanlarımızın tavsiyelerine uyabilirsiniz.

Kaspersky Güvenlik Değerlendirme Hizmetleri

Kaspersky Lab Güvenlik Değerlendirme Hizmetleri, kurum içi uzmanlarımızın sunduğu bir hizmettir. Bu uzmanlarımızın birçoğu kendi alanlarında dünya çapında tanınan otoritelerdir. Bilgileri ve deneyimleri güvenlik istihbaratında dünya lideri olmamızın en temel nedenlerindendir.

Hiçbir BT altyapısı birbirine benzemediği ve en güçlü siber tehditler belirli bir kurumun belirli güvenlik açıklarından yararlanmak amacıyla özel olarak hazırlandığı için uzmanlık hizmetlerimizde özel olarak hazırlanır. İlerleyen sayfalarda açıklanacak olan hizmetler profesyonel araç takımımızın yalnızca bir parçasını oluşturur. Sizinle çalışırken bu hizmetlerin bazılarını veya tümünü, kısmen veya tamamen, uygulayabiliriz.

Öncelikli amacımız, uzman danışmanlarımız riskleri değerlendirmeniz, güvenliğinizi güçlendirmeniz ve gelecekteki tehditlere karşı riskleri azaltmanız konusunda size yardımcı olurken sizinle birebir olarak çalışmaktır.

Güvenlik Değerlendirme Hizmetleri şunları içerir:

- Sızma testi
- Uygulama güvenliği Değerlendirmesi
- ATM/POS Güvenlik Değerlendirmesi
- Telekomünikasyon Ağları Güvenlik Değerlendirmesi

Kaspersky Siber Güvenlik Hizmetleri

Kaspersky Tehdit İstihbarat Hizmetleri

Kaspersky Tehdit Avlama Hizmetleri

Kaspersky Güvenlik Eğitimi

Kaspersky Olay Yanıt Hizmetleri

Kaspersky Güvenlik Değerlendirme Hizmetleri

Sızma Testi
Uygulama Güvenliği Değerlendirmesi
ATM/POS Güvenlik Değerlendirmesi
Telekomünikasyon Ağları Güvenlik Değerlendirmesi

Sızma Testi

BT altyapısının olası siber saldırılara karşı güvende olmasını sağlamak tüm kurumlar için sürekli devam eden bir mücadeledir. Ancak binlerce çalışana, yüzlerce bilgi sistemine ve dünya genelinde birçok iş yerine sahip büyük şirketler için bu mücadele çok daha zorlayıcıdır.

Sızma testi, kötü amaçlı bir aktörün önemli sistemlerde yüksek ayrıcalıklar elde etmek için ağınızdaki güvenlik kontrollerini atlatmaya çalıştığı olası bir saldırı senaryosunun uygulamalı gösterimidir.

Kaspersky Lab'in Sızma Testi, güvenlik açıklarını ortaya çıkararak farklı saldırı biçimlerinin olası sonuçlarını analiz ederek, mevcut güvenlik önlemlerinizin etkililiğini değerlendirerek ve onarımla ilgili önlemler ve iyileştirmeler önererek altyapınızdaki güvenlik hatalarını daha iyi anlamanızı sağlar.

Kaspersky Lab'in Sızma Testi size ve kurumunuza şu konularda yardımcı olur:

- **Ağınızdaki en zayıf noktaları belirleyin**. Bu sayede gelecekteki riskleri azaltmak için dikkatinizi ve bütçenizi toplamanız gereken alanlar konusunda daha bilinçli kararlar alabilirsiniz.
- **Siber saldırıların neden olduğu finansal, işlemsel ve saygınlık açısından kayıpları önleyin.** Güvenlik açıklarını proaktif bir şekilde tespit ederek ve düzelterek bu saldırıların gerçekleşmesini tamamen önleyin.
- **Resmi, sektörel ve kurumsal standartlara uyum sağlayın**. Bu tür bir güvenlik değerlendirmesi gerektiren standartlara uyum sağlayın (örneğin, Ödeme Kartı Sektörü Veri Güvenliği Standartları (PCI DSS)).

Sızma testi sonuçları

Bu hizmet, kritik ağ bileşenlerine yetkisiz erişim sağlamak amacıyla yararlanılabilecek güvenlik eksikliklerini ortaya çıkarmak için tasarlanmıştır. Bu güvenlik eksiklikleri şunları içerebilir:

- Savunmasız ağ mimarisi, yetersiz ağ koruması
- Ağ trafiğinin engellenmesine ve yeniden yönlendirilmesine neden olabilecek güvenlik açıkları
- Farklı hizmetlerdeki yetersiz doğrulama ve yetkilendirme
- Zayıf kullanıcı kimlik bilgileri
- Aşırı kullanıcı ayrıcalıkları dahil olmak üzere yapılandırma hataları
- Uygulama kodundaki hatalardan kaynaklanan güvenlik açıkları (kod enjeksiyonu, dizin gezinimi, müşteri tarafı güvenlik açıkları vb.)
- Yeni güvenlik güncellemelerine sahip olmayan eskimiş donanımların ve yazılım sürümlerinin kullanılmasına dayalı güvenlik açıkları
- Bilgilerin ifşa edilmesi

Sonuçlar; test sonuçlarının genel hatlarını içeren ve saldırı vektörlerini gösteren bir yönetici özetinin yanı sıra test süreci, sonuçları, ortaya çıkarılan güvenlik açıkları ve onarım için önerileri içeren bir nihai rapor olarak sunulur. Ayrıca gerektiği takdirde teknik ekibiniz veya üst düzey yöneticileriniz için videolar ve sunumlar hazırlanabilir.

Hizmetin kapsamı ve seçenekler

İhtiyaçlarınıza ve BT altyapınıza bağlı olarak aşağıdaki hizmetlerden herhangi birini veya tümünü kullanmayı tercih edebilirsiniz:

- **Dışarıdan sızma testi:** Sisteminiz hakkında hiçbir ön bilgisi olmayan bir "saldırganın" internet üzerinden düzenlediği saldırı sonucu yapılan güvenlik değerlendirmesi.

- **İçeriden sızma testi:** Ofisinize yalnızca fiziksel erişimi olan bir ziyaretçi veya sınırlı sistem erişimi olan sözleşmeli bir çalışan gibi içeriden bir saldırgana dayalı senaryolar.

- **Sosyal mühendislik testi:** Kimlik avı, e-postalarla sahte kötü amaçlı bağlantılar gönderilmesi ve şüpheli ekler gibi sosyal mühendislik saldırılarını taklit ederek personelinizin arasında güvenlik farkındalığı değerlendirmesi.

- **Kablosuz ağ güvenliği değerlendirmesi:** Uzmanlarımız şirketinizi ziyaret ederek WiFi güvenlik kontrollerinizi analiz eder.

BT altyapınızın istediğiniz kısmını sızma testinin kapsamına alabilirsiniz. Ancak tüm ağı veya en büyük bölümlerini bu testte değerlendirmenizi öneririz. Çünkü uzmanlarımız olası bir saldırganla aynı koşullar altında çalıştığında her zaman daha yararlı sonuçlar elde edilir.

Kaspersky Lab'in sızma testlerine yaklaşımı hakkında

Sızma testleri, gerçek hacker saldırılarını taklit etmesine rağmen bu testler son derece sıkı bir şekilde kontrol edilir. Testler, Kaspersky Lab güvenlik uzmanları tarafından sistemlerinizin gizliliğine, bütünlüğüne ve kullanılabilirliğine dikkat edilerek ve aşağıdakiler dahil olmak üzere uluslararası standartlara ve en iyi uygulamalara uygun olarak gerçekleştirilir:

- Sızma Testi Uygulama Standardı (PTES)
- NIST Özel Yayınları 800-115 Bilgi Güvenliği Testi ve Değerlendirmesi için Teknik Kılavuz
- Açık Kaynak Güvenlik Testi Metodolojisi El Kitabı (OSSTMM)
- Bilgi Sistemleri Güvenlik Değerlendirmesi Çerçevesi (ISSAF)
- Web Uygulama Güvenliği Konsorsiyumu (WASC) Tehdit Sınıflandırması
- Açık Web Uygulamaları Güvenlik Projesi (OWASP) Test Kılavuzu
- Yaygın Güvenlik Açıkları Puanlama Sistemi (CVSS)

Proje ekip üyeleri, alan hakkında kapsamlı, güncel ve kullanışlı bilgilere sahip deneyimli uzmanladır. Bu uzmanlar Oracle, Google, Apple, Microsoft, Facebook, PayPal, Siemens ve SAP dahil olmak üzere endüstri liderlerine güvenlik danışmanlığı yapan saygın kişilerdir.

İletim seçenekleri

Güvenlik değerlendirmesinin türüne, sistemlerinizdeki ayrıntılar ve çalışma pratiklerine bağlı olarak güvenlik değerlendirmesi hizmetleri uzaktan veya yerinde yapılabilir. Birçok hizmet uzaktan gerçekleştirilebilir, hatta içeriden sızma testi bile VPN erişimiyle gerçekleştirilebilir. Ancak bazı hizmetlerin (kablosuz ağ güvenliği değerlendirmesi gibi) şirket içinde sunulması gerekir.

Uygulama Güvenliği Değerlendirmesi

İster kurumsal uygulamalarınızı şirket içinde üretin isterseniz üçüncü bir taraftan satın alın, tek bir kodlama hatasının sizi saldırılara açık bırakacak bir güvenlik açığı oluşturduğunu unutmayın. Böyle bir güvenlik açığı yüzünden ciddi anlamda finansal ve saygınlık açısından zarara uğrayabilirsiniz. Bir uygulamanın yaşam döngüsü boyunca yazılım güncellemeleri veya güvenli olmayan bileşen yapılandırması aracılığıyla uygulamada yeni güvenlik açıklıkları oluşabilir veya

yeni saldırı yöntemleri gelişebilir.

Kaspersky Lab'in Uygulama Güvenlik Değerlendirmesi, büyük bulut tabanlı çözümler, ERP sistemleri, çevrimiçi bankacılık ve diğer özel işletme uygulamaları gibi her türlü uygulamanın yanı sıra farklı platformlarda (iOS, Android ve diğerleri) yer alan mobil ve gömülü uygulamalardaki güvenlik açıklarını ortaya çıkarın.

Uzmanlarımız, pratik bilgiler ile deneyimler ve uluslararası en iyi uygulamaları birleştirerek kurumunuzu aşağıdaki tehditlere karşı savunmasız hale getirebilecek güvenlik kusurlarını tespit eder:

- Gizli bilgileri çekmek
- Verilere ve sistemlere sızmak ve bunları değiştirmek
- Hizmeti engelleme saldırıları başlatmak
- Dolandırıcılık faaliyetleri gerçekleştirmek

Tavsiyelerimize uyduğunuz takdirde uygulamalarda ortaya çıkarılan güvenlik açıkları düzeltilebilir ve bu tür saldırılar önlenebilir.

Hizmetin avantajları

Kaspersky Lab Uygulama Güvenliği Değerlendirme Hizmetleri, uygulama sahiplerine ve geliştiricilerine şu konularda yardımcı olur:

- **Finansal, işlemsel ve saygınlık açısından kayıpları önleyin**. Uygulamalara karşı düzenlenen saldırılarda kullanılan güvenlik açıklarını proaktif bir şekilde tespit eder ve düzeltir

- **Onarım masraflarından tasarruf edin**. Henüz geliştirilme veya test etme sürecinde olan uygulamalardaki güvenlik açıklarını takip eder ve uygulamalar kullanıcı ortamına ulaşmadan düzeltilir. Aksi takdirde onları onarmak önemli karmaşıklıklara ve masraflara neden olabilir.

- **Güvenli bir yazılım geliştirme yaşam döngüsünü (S-SDLC) destekler**. Güvenli uygulamaları oluşturmayı ve korumayı taahhüt eder.

- **PCI DSS veya HIPAA gibi uygulama güvenliğini kapsayan devlet, endüstri ve şirket kurumsal standartlarına uyum sağlar**

Hizmetin kapsamı ve seçenekler

Değerlendirilen uygulamalar, gömülü ve mobil uygulamalar dahil olmak üzere standart veya bulut tabanlı resmi web sitelerini ve işletme uygulamalarını kapsar.

İhtiyaçlarınıza ve uygulamanın özelliklerine uygun hale getirilebilen hizmetler şunları içerebilir:

- **Kara kutu testi**: dış saldırgan taklit edilir

- **Gri kutu testi**: çeşitli profillere sahip geçerli kullanıcılar taklit edilir

- **Beyaz kutu testi**: kaynak kodlar dahil olmak üzere uygulamaya tam erişim analizi; bu yaklaşım güvenlik açığı sayısının ortaya çıkartılması açısından en etkili yöntemdir

- **Uygulama koruma duvarı etkililiği değerlendirmesi**: güvenlik açıklarını bulmak ve açıklardan yararlanan yazılımların engellenip engellemediğini doğrulamak için uygulamalar, koruma duvarı koruması etkinken ve devre dışıyken test edilir

Kaspersky Lab'in Uygulama Güvenliği Değerlendirmesine Yaklaşımı Hakkında

Uygulamaların güvenlik değerlendirmeleri Kaspersky Lab'in güvenlik uzmanları tarafından hem manuel olarak hem de otomatik araçlar kullanılarak

Sonuçlar

Kaspersky Lab Uygulama Güvenliği Değerlendirme hizmetleri tarafından tanımlanabilecek güvenlik açıkları şunları içerir:

- Çok faktörlü doğrulama dahil olmak üzere doğrulama ve yetkilendirme konusundaki kusurlar
- Kod enjeksiyonu (SQL Enjeksiyonu, İşletim Sistemi Komutları vb.)
- Dolandırıcılığa neden olan mantıksal güvenlik açıkları
- Müşteri tarafı güvenlik açıkları (Çapraz Site Komut Çalıştırma, Çapraz Site İstek Sahteciliği, vb.)
- Zayıf şifreleme kullanımı
- Müşteri tarafı iletişimlerinde güvenlik açıkları
- Ödeme sistemlerinde PAN maskeleme eksikliği gibi veri depolamanın ve aktarımının güvenli olmaması
- Oturum saldırılarına yol açanlar dahil olmak üzere yapılandırma kusurları
- Hassas bilgilerin ifşa edilmesi
- WASC Tehdit Sınıflandırması v2.0 ve OWASP İlk 10 gibi projelerde listelenen tehditlere yol açan diğer web uygulaması güvenlik açıkları.

Sonuçlar; yönetimle ilgili noktaları vurgulayan bir yönetici özetinin yanı sıra değerlendirme süreçleri, sonuçları, ortaya çıkan güvenlik açıkları ve onarım için önerileri içeren bir nihai rapor olarak sunulur. Ayrıca gerektiği takdirde teknik ekibiniz veya üst düzey yöneticileriniz için videolar ve sunumlar hazırlanabilir.

gerçekleştirilir. Bu test sırasında sistemlerinizin gizliliğine, bütünlüğüne ve kullanılabilirliğine dikkat edilir ve aşağıdaki uluslararası standartlar ile en iyi uygulamalara uyum sağlanır:

- Web Uygulama Güvenliği Konsorsiyumu (WASC) Tehdit Sınıflandırması
- Açık Web Uygulamaları Güvenlik Projesi (OWASP) Test Kılavuzu
- OWASP Mobil Güvenlik Test Kılavuzu
- Kurumunuzun sektörüne ve konumuna göre diğer standartlar

Proje ekip üyeleri farklı platformlar, programlama dilleri, çerçeveler, güvenlik açıkları ve saldırı yöntemleri dahil olmak üzere alanlarında kapsamlı ve kullanışlı bilgilere sahip deneyimli uzmanlardır. Uzmanlarımız, önemli uluslararası konferanslarda sunumlar yapmakta ve Oracle, Google, Apple, Facebook ve PayPal dahil olmak üzere büyük uygulama ve bulut hizmetleri tedarikçilerine güvenlik danışmanlığı hizmeti vermektedir.

İletim seçenekleri

Güvenlik değerlendirme hizmetleri; hizmet kapsamındaki sistemlerin özelliklerine, güvenlik değerlendirme hizmetinin türüne ve çalışma koşulları gerekliliklerinize bağlı olarak uzaktan veya şirket içinde sağlanabilir. Bu hizmetlerin birçoğu uzaktan yürütülebilir.

ATM/POS Güvenlik Değerlendirmesi

ATM'ler ve POS'lar artık ATM hırsızlığı veya kart kopyalama gibi fiziksel saldırılara karşı savunmasız değildir. Bankalar ve ATM/POS tedarikçileri tarafından uygulanan önlemler geliştikçe bu cihazlara karşı düzenlenen saldırılarda gelişmekte ve hızlanmaktadır. Hacker'lar ATM/POS altyapı mimarilerindeki ve uygulamalarındaki güvenlik açıklarından yararlanır ve ATM/POS cihazlarına özel olarak kötü amaçlı yazılımlar geliştirir. Kaspersky Lab ATM/POS Güvenlik Değerlendirmesi hizmetleri, ATM/POS cihazlarındaki güvenlik kusurlarını fark etmenizi ve sistemlerinizin ele geçirilme riskini azaltmanızı sağlar.

ATM/POS Güvenlik Değerlendirmesi, ATM ve/veya POS cihazlarınızın kapsamlı bir analizini kapsar. Bu analiz yetkisiz nakit çekme, yetkisiz finansal işlemler gerçekleştirme, müşterilerinizin ödeme kartı verilerini çalma ve hizmet engelleme saldırıları başlatma gibi faaliyetler için saldırganlar tarafından kullanılan güvenlik açıklarını tanımlamak amacıyla tasarlanmıştır. Bu hizmet, ATM/POS altyapılarında farklı saldırı türleriyle kötüye kullanılabilecek güvenlik açıklarını ortaya çıkarır, kötüye kullanımın olası sonuçlarını vurgular, mevcut güvenlik önlemlerinizin etkililiğini değerlendirir ve tespit edilen kusurlar düzeltmek ve güvenliğinizi geliştirmek için daha çok önlem planlamanıza yardımcı olur.

Hizmetin avantajları

Kaspersky Lab tarafından sağlanan ATM/POS Güvenlik Değerlendirmesi satıcılara ve finansal kuruluşlara şu konularda yardımcı olur:

- **Güvenlik açıklarını anlayın.** Çözüm, ATM/POS cihazlarındaki açıkları anlayabilir ve ilgili güvenlik işlemlerinizi buna göre geliştirebilirsiniz

- **Finansal, işlemsel ve saygınlık açısından kayıpları önleyin**. Saldırganların yararlanabileceği güvenlik açıklarını proaktif bir şekilde tespit ederek ve düzelterek saldırının neden olduğu kayıpları önleyin.

- **Resmi, sektörel ve kurumsal standartlara uyum sağlayın**. Güvenlik değerlendirmesi gerçekleştirmeyi zorunlu kılan standartlara uyum sağlayın (örneğin, Ödeme Kartı Sektörü Veri Güvenliği Standartları (PCI DSS)).

ATM/POS Güvenlik Değerlendirmesi Sonuçları

ATM/POS Güvenlik Değerlendirmesi hizmeti, aşağıdakiler dahil olmak üzere çeşitli güvenlik açıklarını tanımlayabilir:

- Ağ mimarisinde güvenlik açıkları ve yetersiz ağ koruması.
- Saldırganın kiosk modundan çıkmasını ve işletim sistemine yetkisiz erişim sağlamasına izin veren güvenlik açıkları.
- Üçüncü taraf yazılımlarında olası saldırganların güvenlik kontrollerini aşmasını sağlayan güvenlik açıkları.
- Aktarılan verilerin engellenmesini ve değiştirilmesine neden olan cihaz iletişimi güvenlik açıkları dahil olmak üzere yetersiz girdi ve çıktı cihazı koruması (kart okuyucu, para verme ünitesi vb.).
- Uygulama kodundaki hatalardan veya eski donanım ve yazılım sürümleri kullanmaktan kaynaklanan güvenlik açıkları (arabellek aşımı, kod enjeksiyonları vb.)
- Bilgilerin ifşa edilmesi.

Değerlendirme tamamlandıktan sonra test süreçleri, sonuçlar, güvenlik açıkları ve tavsiyeler dahil olmak üzere ayrıntılı teknik bilgileri içeren bir rapor sunulur. Rapor ayrıca test sonuçlarına dayalı çıkarımların vurgulandığı ve çeşitli saldırı vektörlerinin açıklandığı bir yönetici özeti içerir. Ayrıca gerektiği takdirde teknik ekibiniz veya üst düzey yöneticileriniz için saldırı göster-imleriyle ilgili videolar ve sunumlar da hazırlanabilir.

Hizmet kapsamı

Bu hizmet, test ortamında fuzzing ve saldırı gösterimleri dahil olmak üzere kapsamlı bir ATM/POS analizini içerir. Bu değerlendirme, tek bir ATM/POS cihazında veya cihazlardan oluşan bir ağda gerçekleştirilebilir. Değerlendirme için kurumunuzda en çok kullanılan ATM/POS cihazı türünü veya tipik yapılandırmaları konusunda en kritik olan cihazları (örneğin önceden bir saldırıya maruz kalmış cihazlar) seçmenizi öneririz.

Kaspersky Lab'in ATM/POS Güvenlik Değerlendirmesine Yaklaşımı Hakkında

Analiz sırasında uzmanlarımız yalnızca hataları ve eski yazılım sürümlerindeki güvenlik açıklarını bulmaya ve tanımlamaya odaklanmaz. Ancak bileşen seviyesinde yeni (0 gün) açıklarını tanımlama amaçlı güvenlik araştırmaları yaparak ATM/POS cihazlarınız tarafından gerçekleştirilen işlemlerin arkasındaki mantığı derinlemesine analiz ederler. Bir saldırganın kullanabileceği güvenlik açıkları tespit edersek (örneğin yetkisiz nakit çekmeden kaynaklanan açıklar) uzmanlarımız özel olarak üretilmiş otomasyon araçlarını ve cihazlarını kullanarak olası saldırı senaryolarını gösterebilir.

Bir ATM/POS Güvenlik Değerlendirmesi aracılığıyla gerçek bir hacker'ın saldırı yöntemi taklit edilerek savunma stratejilerinizin etkililiği ve tamamen güvende ve saldırılamaz olup olmadığı değerlendirilir. Bu hizmet, sistemlerinizin gizliliği, bütünlüğü ve kullanılabilirliğine özel bir önem veren ve uluslararası kanunlar ile en iyi uygulamalara göre hareket eden deneyimli Kaspersky Lab uzmanları tarafından gerçekleştirilir. Bir müşterimizin ATM/POS cihazında yeni bir açık fark edersek tedarikçiyi bilgilendirerek ve açığı onarmak için danışmanlık hizmeti sunarak sorumlu bir şekilde bildirim ilkelerini izleyeceğimizi taahhüt ederiz.

Kaspersky Lab, ATM/POS Güvenlik Değerlendirmesi hizmetlerini aşağıdaki uluslararası standartlar ve en iyi uygulamalara göre sağlar:

- Ödeme Kartı Endüstri Standartları
  - Veri Güvenliği Standardı
  - Ödeme Uygulaması Veri Güvenliği Standardı
  - PIN İşlem Güvenliği
- Açık Kaynak Güvenlik Testi Metodolojisi El Kitabı (OSSTMM)
- Bilgi Sistemleri Güvenlik Değerlendirmesi Çerçevesi (ISSAF)
- Yaygın Güvenlik Açıkları Puanlama Sistemi (CVSS)
- Gerekli olduğu takdirde belirli işletme modellerine ve coğrafi konuma dayalı diğer standartlar uygulanabilir.

Proje ekip üyeleri, alan hakkında kapsamlı bilgiye sahip olan ve sürekli olarak becerilerini geliştiren son derece deneyimli uzmanlardır. Düzenli olarak ATM/POS satıcılarına güvenlik danışmanlığı sağlar ve ATM/POS güvenlik araştırmalarımızın sonuçlarını önemli bilgi güvenliği konferanslarında (Black Hat gibi) sunarlar.

Telekomünikasyon Ağları Güvenlik Değerlendirmesi

Hizmetlere Genel Bakış

Bir telekomünikasyon şirketinin BT güvenliği, çeşitli fonksiyonlara ve teknolojilere dayanan birbirine bağlı ağlardan oluşur. Bu ağlar genellikle yönetim unsurlarını içeren bir kurumsal ağ ve abonelerine geniş bantlı İnternet Erişimi, özel yüksek hızlı gövde kanalları, barındırma ve bulut hizmetleri sağlayan bir çekirdek radyo ağları (GSM/UMTS/LTE) içerir. Bu altyapının her parçası işletme için kritiktir ve finansal, işlemsel ve saygınlık açısından risklerin en aza indirilmesi için hacker saldırılarına karşı çok iyi korunmalıdır. Kaspersky Lab'in telekomünikasyon ağları için sunduğu hizmetler, sistemlerinizdeki güvenlik açıklarını fark ederek ve yeni kontrollerle bu açıkları kaldırarak ya da etkilerini onararak bu riskleri azaltmanızı sağlar.

Kaspersky Lab, telekomünikasyon ağları için aşağıdaki güvenlik hizmetlerini sunar:

- BT Altyapısı Sızma Testi
- BT Altyapısı Yapılandırma Güvenliği Değerlendirmesi
- GSM/UMTS/LTE Ağları için Güvenlik Değerlendirmesi
- Uygulama Güvenlik Değerlendirmesi (çeşitli hizmetler sağlayan uygulamalar için: IP-TV, istemci self-servis portalları vb.)
- VoIP Güvenlik Değerlendirmesi
- Telekomünikasyon Ekipmanları Güvenlik Değerlendirmesi

Hizmetin Sonuçları

Her güvenlik değerlendirmesinin sonunda, güvenlik kontrollerinizin etkililiği hakkında çıkarımların yanı sıra telekomünikasyon ağlarınızdaki güvenlik hatalarıyla ilgili teknik ve üst düzey görüşleri alabilirsiniz. Bu sonuçlar ağınızın güvenliğini arttırmak ve bilgi güvenliği tehditleriyle ilgili finansal, işlemsel ve saygınlık açısından riskleri azaltabilirsiniz.

Rapor aşağıdaki bilgileri içerir:

- Telekomünikasyon ağlarınızın mevcut güvenlik düzeyi hakkında üst düzey çıkarımlar
- Hizmet metodolojisinin ve sürecinin açıklanması.
- Önem düzeyi, kullanım karmaşıklığı, savunmasız sistemin olası etkileri ve güvenlik açığı olduğuna dair kanıtlar (varsa) dahil olmak üzere tespit edilen güvenlik açıklarının ayrıntılı açıklamaları.
- Yapılandırmadaki değişiklikler, güncellemeler, kaynak kodları değiştirme veya güvenlik açığının kapatılamadığı yerlerde telafi edici kontroller uygulama gibi güvenlik açığı kapatma konusunda öneriler

Kaspersky Lab
Enterprise Cybersecurity:**www.kaspersky.com.tr/enterprise**
Siber Tehdit Haberleri: **www.securelist.com**
BT Güvenliğiyle İlgili Haberler: **business.kaspersky.com.tr/**

#truecybersecurity
#HuMachine

www.kaspersky.com.tr