KASPERSKY lab

# Gelişmiş Tehdit Savunması ve Hedefli Saldırı Riskini Azaltma

Kaspersky Anti Targeted Attack çözümü

www.kaspersky.com
#truecybersecurity

# Gelişmiş tehditler ve hedefli saldırıların oluşturduğu risk artıyor

Şirketlerde güvenlik ihlalinin keşfedildiği günde ve bir hafta sonrasında başlatılan kurtarma çalışmaları %200 büyüdü*.

*2016 yılında Kaspersky Lab tarafından dünya çapında gerçekleştirilen Kaspersky Lab Kurumsal BT Güvenlik Riskleri Araştırması sonuçları

**Şirketlerin %15'i** hedefli saldırıya maruz kalmıştır ve
bu vakaların %53'ü hassas verilerin kaybedilmesiyle sonuçlanmıştır*.

*Kaspersky Global BT Güvenlik Riskleri Raporu 2015

Kendi piyasasında önemli bir yere sahip olan her büyük şirket potansiyel bir hedeftir. Bu, küçük şirketlerinde saldırılardan etkilenmeyeceği anlamına gelmez. Birçok vakada suçlular, küçük şirketleri daha büyük hedeflerine ulaşmak için güvenliği kolaylıkla kırılabilecek basamaklar olarak görür. Ancak piyasa liderleri için böyle bir saldırıya maruz kalma ihtimali önemli derecede artmaktadır. Artık bir saldırının "olup olmayacağını" değil "ne zaman" olacağını tartışmalıyız.

**Saldırıyı kimler düzenler?**

**Siber suçlular**: Verileri en yüksek fiyat veren kişiye satmayı veya yalnızca paranızı çalmayı amaçlarlar. Siber araçlarını genellikle kendileri geliştirir veya dark web'den satın alırlar.

**Rakip işletmeler**: Gizli verilerinizi ele geçirmeyi veya işinizi sabote etmeyi amaçlar. Genellikle siber paralı askerlerden (cyber-mercenaries) "hizmet satın alırlar".

**Siber paralı askerler**: siber casusluk konusunda
uzman olan bu kişiler kendi araçlarını geliştirir ve "hizmetlerini" en yüksek fiyat veren kişiye satarlar.

**Hacktivistler**: "Çoğunluğun" iyiliği için çalıştıklarını iddia eden bu yaratıcı grup karmaşık araçları kullanır ve ilgilerini çeken her türlü kurum için ciddi bir sorun teşkil eder

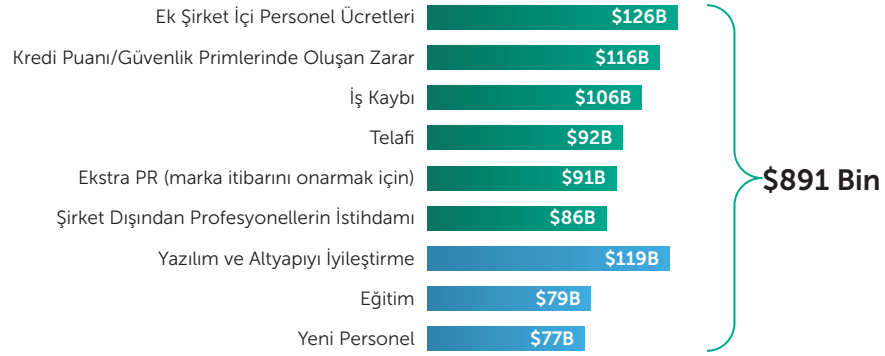
**Devlet kurumları**: Her ne kadar bu inkâr edilse de dünya genelinde devletlerin; bireyleri, grupları ve işletmeleri düzenli olarak takip ettikleri kabul edilmektedir. Bu grubun araçları son derece gelişmiş, pahalı ve tespit edilmesi zor olabilir.

## Kurumsal Tehdit Ortamı

Hedefli saldırılar ve Gelişmiş Kalıcı Tehditler (APT'ler) dahil olmak üzere gelişmiş tehditler, şirket sistemleri için en tehlikeli risklerden bazılarıdır. Ancak siber suçluların kullandığı tehditler ve teknikler hızla ilerlerken birçok kurum, günümüzün ve geleceğin tehditlerinden korunmak için geçmişteki güvenlik teknolojilerine ve çağ dışı bir zihniyete güvenmeye devam etmektedir.

Gelişmiş, özel hedefli tehditler haftalar, aylar hatta yıllar boyunca fark edilemeyebilir. Ancak bu sürede tehdit aktörleri yavaşça ve sessizce bilgi toplar ve seçtikleri hedef sistemin özgün güvenlik açıklarından yararlanmak için adım adım ilerler. Normal kötü amaçlı yazılımların aksine gelişmiş, hedefli tehditler saldırganlar tarafından etkin bir şekilde kontrol edilir ve yönetilir. Amaç, yalnızca kötü amaçlı yazılımın bulaştırılması değildir. Asıl hedef, şirketin güvenlik çevresinde varlığını sürdürmektir. Bu saldırılar, avları için beklemede kalmaya hazır olan saldırganların sabırlı ve genellikle son derece özenli araştırmalarının sonucudur.

### Tek bir tehditli saldırının neden olduğu ortalama kayıp tutarı:




## Güvenlik ihlallerinin başarılı olmasına neden olan iç ve dış etkenler

Hedefli saldırıların, BT altyapılarında başarılı bir şekilde ilerlemesine neden olan temel etkenler şunlardır:

- Önleme kabiliyetlerinde eksiklik ve mevcut çevre güvenliğiyle ilgili aşırı iyimser bakış açısı
- Çalışanların bilgi güvenliği riskleri hakkındaki farkındalığının düşük olması
- BT ortamında ve özellikle ağ yönlendirmesinde görünürlük açısından eksiklik
- Firmaya özel ve eski yazılım-işletim sistemleri
- Güvenlik ekiplerinin; kötü amaçlı yazılım araştırması, adli bilişim, olay yanıtı ve tehdit istihbaratı konusunda yeterince nitelikli olmaması

**Bu saldırılar nasıl bir risk oluşturur?**

**Tüm kurumlara yönelik riskler:**

- Yetkisiz finansal işlemler
- Kritik veri hırsızlığı veya hasarı
- Gizli süreçlerin manipülasyonu
- Rakipler Tarafından Zayıflatılma
- Şantajla para sızdırma
- Kimlik hırsızlığı

**Önemli endüstri sektörlerine yönelik riskler:**

**Finansal Hizmetler**

- Yetkisiz finansal işlemler
- Fiziksel nakit hırsızlığı için ATM saldırıları
- Kimlik hırsızlığı

**Devletler**

- Veri işleme
- Casusluk
- Çevrimiçi hizmetlerin kullanımının kısıtlanması
- Kimlik hırsızlığı
- Hacktivizm eylemleri

**Üretim ve İleri Teknoloji**

- Casusluk (teknik bilgiler)
- Kritik teknolojik süreçlerin gizliliğinin ihlâl edilmesi

**Telekomünikasyon**

- Telekom altyapısı kullanılarak kurumsal müşterilere saldırı
- Sosyal mühendislik için e-posta sunucularının manipüle edilmesi
- Faturalama kontrolü
- Web kaynaklarının kimlik avı amacıyla manipüle edilmesi
- DDoS saldırıları için ele geçirilen altyapının (cihazlar/nesnelerin interneti) kullanılması

**Enerji ve Kaynaklar**

- Hesaplama verileri ile manipülasyon
- Teknolojik ağlara fiziksel hasar verilerek yapılan saldırılar

**Kitle iletişim araçları**

- Hacktivizm
- Web sitesinin ele geçirilmesi (tahrif ve kimlik avı) ve saldırıları web site kullanıcılarına yayma

**Sağlık**

- Hasta bilgilerinin çalınması
- Teletıp ekipmanlarına saldırı

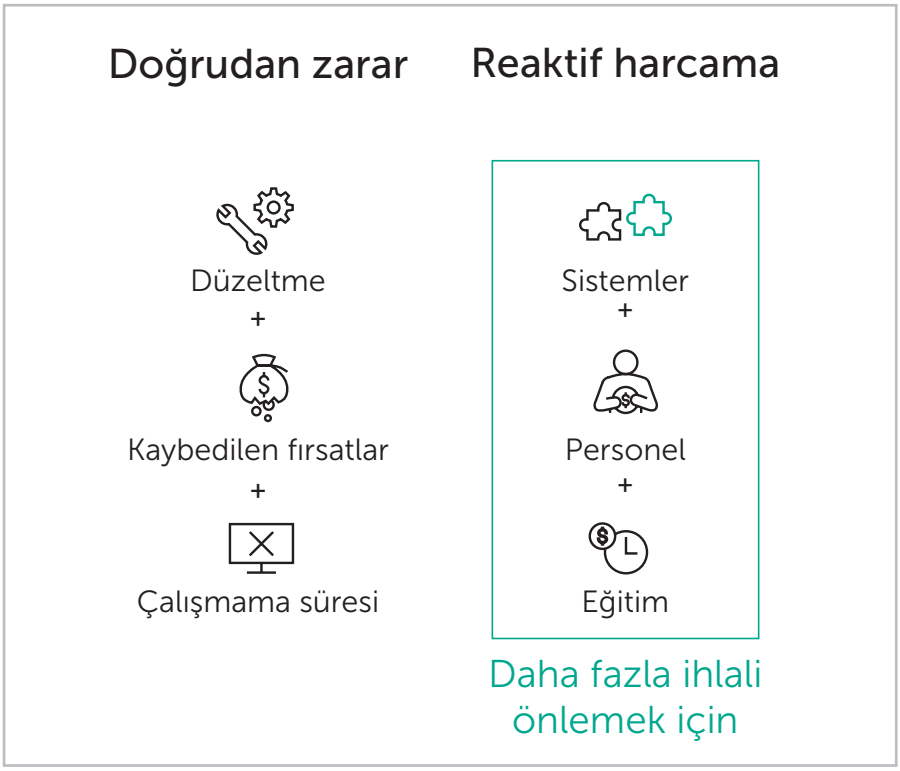
# Hedefli Saldırılar: Meslek Olarak Siber Suç

Hedefli saldırıların çoğu oldukça deneyimli siber suçlular tarafından yürütülür. Bu suçlular, saldırının her aşamasını geleneksel savunma sistemini atlatacak şekilde uyarlama, zayıflıklardan yararlanma ve para, gizli veriler vb. dahil olmak üzere çalabilecekleri değerli şeylerin miktarını arttırma konusunda uzmandır.

Geçmişte güvenlik saldırılarıyla ilgilenen zeki kişiler, dönüşüm geçirerek kariyerlerini siber suç mesleğinde devam ettirmeye başlamıştır. Herhangi bir şirketi hedef almalarının veya saldırmalarının tek nedeni maksimum kâr sağlamaktır. Bu kâr, henüz saldırı başlatılmadan önce ilgili maliyetler ve olası kazançlar temel alınarak hesaplanır. Amaç, tabii ki mümkün olduğunca ucuz araçlarla ön maliyetlerin azaltılması ve finansal açıdan maksimum sonuçların elde edilmesidir.

Hedefli saldırıların çoğu sosyal mühendislik ve özelleştirilmiş araçların birleşimini kullanır. Verimli bir hedefli saldırı başlatmanın maliyeti, toplam global saldırı sayısının orantılı bir şekilde artmasıyla ciddi anlamda azalmıştır.

Peki şirketinize benzer kurumlar hedefli saldırılara maruz kaldığında neler risk altındadır?



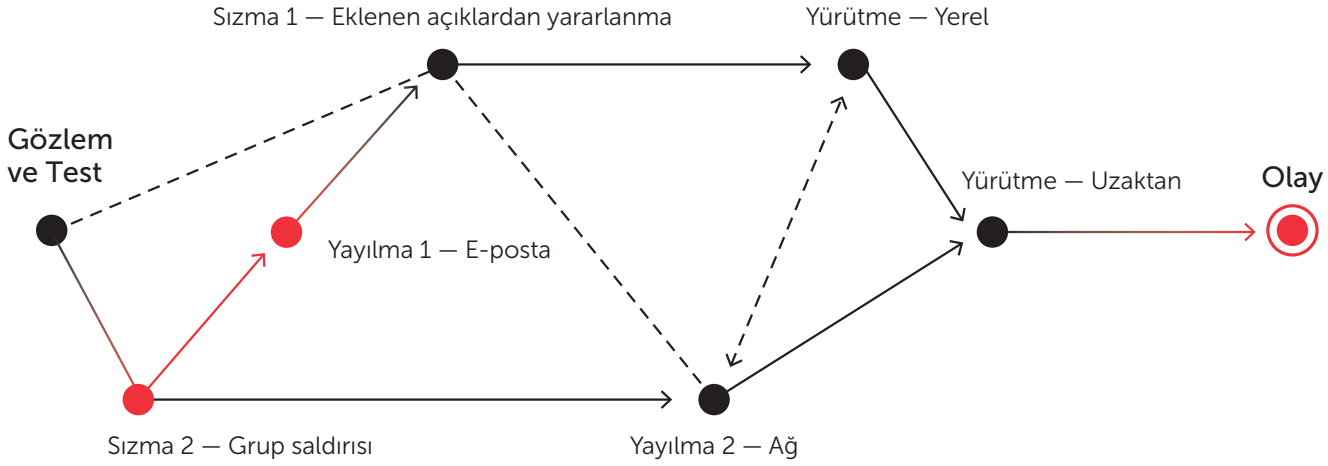

**Doğrudan finansal kayıplar.** Saldırganlar, kurum hesaplarına erişim sağlamak ve sahte işlemler yapmak için banka kimlik bilgilerini çalarak siber dolandırıcılık yapmaya çalışabilir.

**Önemli iş süreçlerinin aksaması.** Bazı saldırılar, sadece yan etki olarak, kritik iş süreçlerini olumsuz anlamda etkilerken veya yavaşlatırken bazı saldırılar da bu süreçleri sabote etmek için kasıtlı olarak başlatılır. Saldırı fark edilse bile hedef alınan işletme gerekli soruşturmaları yürütürken ve işlerini kurtarmaya çalışırken belirli bir süre daha aksama yaşanma ihtimali vardır. Bu sürede başka iş fırsatları kaçırılabilir.

**Temizleme maliyetleri.** Saldırıdan sonra daha önce bütçesini ayırmadığınız bir sürü harcamayla karşı karşıya kalabilirsiniz. Sistemleri ve süreçleri kurtarmak, hem sermaye harcamalarına hem de güvenlik ve sistem danışmanlarını işe almak gibi işlemsel maliyetlere sebep olabilir.

# Bir Hedefli Saldırının Anatomisi

Teoride, hedefli saldırının ölüm zinciri oldukça basit gibi görünür: Keşif ve Test, Sızma, Yayılma, Yürütme, Sonuç. Buradan şu sonuç çıkarılabilir: Çok aşamalı bir saldırının ilk aşamalarını otomatik olarak engellemek, saldırının kendisini önleyebilir.




Hedefli saldırılar, saldırganın geleneksel güvenlik teknolojileri tarafından fark edilmemesine yardımcı olarak güvenliği ihlâl eden ve kurbanın BT altyapısının yetkisiz kontrolünü saldırganın eline veren uzun vadeli bir süreçtir.

Bazı saldırılarda, son derece etkili ancak uygulaması maliyetli Gelişmiş Kalıcı Tehditler (APT'ler) kullanılmasına rağmen bazılarında gelişmiş kötü amaçlı yazılım veya sıfır gün açığı gibi tek bir teknik kullanılabilir.

Ancak hedefli saldırılar aslında son derece karmaşık olmasının yanı sıra ilerleme ve yürütme açısından doğrusal olmayan bir çizgide ilerler. Bu nedenle, otomatikleştirilmiş tespit özellikleri, sürekli izleme ve tehdit avı çok aşamalı bir savunma stratejisinin parçaları olarak mevcut olmalıdır.

Hedefli saldırı, güvenliği ihlal eden ve siber suçlunun doğrulama prosedürlerini atlatmasını ve BT altyapısıyla etkileşim kurarak geleneksel araçlar tarafından tespitinin önlenmesini sağlayan uzun bir süreçtir.

Sonuç olarak hedefli saldırı tek bir kötü amaçlı eylemden çok devam eden bir faaliyet, bir proje, yani bir süreçtir. Global saldırıları izleyerek edindiğimiz deneyimlerimize göre bu tür işlemler en az 100 gün sürer. Bu saldırı, devlet kurumları, piyasadaki büyük şirketler ve kritik altyapılar için yıllar boyunca da devam edebilir.

İkinci olarak bu süreç; belirli bir altyapıyı hedef alır, belirli güvenlik mekanizmalarının üstesinden gelecek şekilde tasarlanır ve başlangıç aşamasında çalışanların e-postası veya sosyal medya hesaplarını hedef almayı içerebilir. Bu, çok daha farklı amaçların peşinde olan saldırganların gönderdiği standart kötü amaçlı yazılım tabanlı, toplu e-postalardan oldukça farklıdır. Hedefli saldırı vakalarında, metodoloji ve zincir aşamaları belirli bir kurbanın etrafında şekillenir.

Üçüncü olarak bu operasyon, uzmanlardan oluşan, gelişmiş teknik araçlara sahip olan ve bazen uluslararası olarak çalışan organize bir grup veya ekibin yönetimindedir. Faaliyetlerinin, bir projeden ziyade çoklu saldırı operasyonlarına benzediği söylenebilir. Örneğin saldırganlar hedef kurumlar ve ağlar için "geçit" işlevi görebilecek olası çalışanların bir listesini çıkarır ve bu çalışanların çevrimiçi profillerini ve sosyal medya faaliyetlerini inceler. Bundan sonra, kurbanın iş bilgisayarı üzerinde kontrol sağlama görevi neredeyse tamamlanmış olur. Çalışanın bilgisayarı ele geçirildikten sonra saldırganlar suç faaliyetlerini yönlendirebilecekleri ağın kontrolünü ele geçirmeye çalışır.

# Kurumsal Güvenliğin Zorlukları

Karmaşık tehditler katlanarak artmaya devam ettikçe birçok şirket mevcut tehditlere karşı görünürlüğü ve korumayı bir üst düzeye taşıma umuduyla yeni teknolojiler ve hizmetler kullanmaya başlamıştır. Ancak çok yönlü yaklaşım ve stratejik planlama olmadan bu çabalar beklentileri karşılayamayabilir.

**Koruma Alanlarıyla İlgili Sorunlar**

Piyasadaki "hedefli saldırı tespit çözümlerinin" çoğu yalnızca tek bir bağımsız koruma alanından oluşur. Yeni ve gelişmiş tehdit bulma konusunda kayda değer bir başarıya sahip olmayan satıcılar bile koruma alanları vaat eder. Bu tür koruma alanları genellikle kötü amaçlı yazılıma karşı koruma motorunun bir uzantısı gibidir ve arkalarında ciddi bir tehdit istihbaratı da bulunmaz.

Kaspersky Lab'in gelişmiş koruma alanı ise entegre tespit kabiliyetlerimizin parçalarından biridir. Doğrudan şirket içindeki koruma alanı kompleksinde geliştirilen bu teknolojiyi on yıldan uzun bir süredir kullanıyoruz. Koruma alanının özellikleri, on yıllık tehdit analizinden toplanan istatistiklere göre geliştirilmiştir. Bu sayede, şu anda piyasada bulunan "sihirli çözümlere" göre daha gelişmiş ve hedefli saldırı odaklı bir çözüm sunar.

"Düzensiz" veya yapılandırılmamış güvenlik yatırımlarının hayal kırıcı sonuçları şunları içerir:

1. Koruma alanına, bağımsız teknolojilere, veya SOC (güvenlik işlemleri merkezi) oluşturmaya büyük yatırım yapılması, güvenlik açısından yeterli gelişmelerin elde edilmesini sağlamaz.

Güvenlik duvarı ve kötü amaçlı yazılıma karşı koruma yazılımları gibi çevre güvenliği teknikleri, daha fırsatçı bazı saldırılara dayanabilir. Ancak hedefli saldırılar bambaşka bir konudur.

Bazı satıcılar; koruma alanları, ağ anormalliği analizi veya uç nokta odaklı izleme gibi bağımsız ve ayrık ürünlerin farklı çeşitlerini kullanarak APT'lerle mücadele etmeyi denemiştir. Bu bağımsız araçların hepsi biraz koruma ve siber suçlu araçlarının engellenmesini sağlayabilmesine (ve sağlamasına) rağmen hedefli ve koordine bir saldırıyı açığa çıkarmak için kendi başlarına yeterli değillerdir.

Bunu başarmak için şirket altyapısının tüm düzeylerinde gerçekleşen birçok olayın tespit edilmesi gerekir. Daha sonra buradan elde edilen bilgiler, çok katmanlı bir analiz sistemi kullanılarak işlenir ve güvenilir bir kaynağın sağladığı gerçek zamanlı güvenlik istihbaratı ile yorumlanır. Diğer bir deyişle, yapabileceğiniz en iyi yatırım; ağ anormallikleri analizi, koruma alanı sağlama ve uç nokta olayları analizi gibi birçok teknolojinin en iyi özelliklerini bütünsel ve uçtan uca bir süreçte birleştiren bir yaklaşımdır.

2. Mevcut çözümler; SOC ekibinizin makul bir zaman dilimi içinde işleme, analiz etme, öncelik belirleme ve yanıt verme işlemlerini gerçekleştiremeyeceği kadar çok güvenlik olayı üretir.

3. Tehdit gelişmişliğinin şu andaki düzeyine uygun güvenlik becerilerinde eksiklik. Güvenlik uzmanları olay tespiti ve hızlı onarım (sanal makine şablonu (golden image), URL'leri/dosyaları kara listeye alma, bazı kurallar oluşturma) konusunda becerikli olabilir ancak genellikle yanıt sürecinin tam döngüsünü (risk düzeylerini nitelendirme, ilk analizleri gerçekleştirme, soruşturma, yayılımı sınırlandırma, adli bilişim) uygulayabilecek kadar nitelikli değillerdir

4. İşlemsel görünürlük eksikliği. Siber suçlular, hedefli saldırı sırasında, görünüşte herhangi bir sistem ihlali oluşturmamak için çalıntı kimlik bilgiler ve yasal yazılımlar kullanır. Bu sayede geleneksel güvenlik çözümlerinden kolaylıkla kurtulabilirler.

Saldırganlar, kötü amaçlı faaliyetlerini gizlemek amacıyla ellerinden geleni yaptıkları için şirketteki BT güvenlik ekibinin saldırıyı fark etmesi çok zor olabilir. Böylece saldırganlar, oldukça uzun bir süre boyunca hasar oluşturmaya devam edebilir.

Aslında kötü amaçlı yazılımlar güvenlik ihlallerinin yalnızca %40'ından sorumludur. Daha önce tehdit aktörlerinin, şirket sistemlerine erişim sağlamak için çok çeşitli teknikler kullandıklarını biliyoruz.
Kötü amaçlı yazılım kullanılsa bile bunların %70-90'ı bulundukları kuruma özgüdür (Verizon: Veri İhlali İnceleme Raporu).

5. Şirket içinde hangi uzmanlıkların işe alınması ve geliştirilmesi, hangi güvenlik görevleri için dış kaynak kullanılması ve nelerin otomatikleştirilmiş sistemlere bırakılması gerektiğini ayırt etmek zordur.

Güvenlik olaylarının ciddiyeti ve genel iş verimliliğine olası etkisi arttıkça güvenlik bölümünün karşılaştığı temel zorluklardan biri yeterli kalifiye uzman sayısına ve çeşitliliğine ulaşamamalarıdır. Tam verimli bir güvenlik stratejisi, sadece sürekli izleme ve tespit özellikleri değil aynı zamanda doğru adli bilişim işlemlerinin yerine getirilmesinin yanı sıra hızlı yanıt ve nitelikli onarım gerektirir.

Geleneksel SOC ekipleri bu görevin yalnızca tespit ve yanıt kısmına odaklanır. Otomatikleştirilmiş çözümlerin uygulanması, uzmanların olay yönetim sürecindeki diğer adımlara başlaması için zaman sağlar. Ancak çok az sayıda şirket, yüksek düzeyli görevlerin tümünü şirket içinde gerçekleştirmeye hazırlıklıdır. Bu noktadaki zorluk, genel sürecin hangi unsurlarının (yönetim, riskin nitelendirilmesi, önceliklendirme, hızlı kurtarma) şirket içi ekip tarafından, hangilerininse (kötü amaçlı yazılım araştırması, dijital adli bilişim, tehdit avı) dış uzmanlar tarafından daha etkili bir şekilde yürütülebileceğine karar vermektir.

# İstihbarata Dayalı Şirket Güvenlik İşlemleri Merkezi

Siber suçlular, yöntemlerini geleneksel savunma sistemlerinden kaçabilecek ve sistemde aylarca hatta yıllarca fark edilmeden gizlenebilecek şekilde uyarlamıştır. Artık şirket güvenlik sistemlerinin de istihbarat destekli ve çok katmanlı bir BT güvenliği yaklaşımı benimseyerek kendilerini uyarlama zamanı gelmiştir.

Yakın zamana kadar kötü amaçlı yazılım bulaşmasını veya şirket ağına yetkisiz erişimleri engelleyen yaygın güvenlik çözümlerini kullanarak şirket çevresinin korunması yeterliydi. Ancak günümüzde hedefli saldırıların artması nedeniyle bu basit yaklaşım artık yeterli olmamaktadır.

Güvenlik bölümünüzün yeni tehlikelere karşı koruma sağlamasını istiyorsanız tehdit istihbaratı ve çok katmanlı güvenlik çözümleri tarafından güçlendirilen geleneksel bir SOC ekibine dayalı ve güvenlik ihtiyaçları için çok yönlü ve son derece uyarlanabilir bir yaklaşıma ihtiyacınız olacaktır.


# Şirket güvenlik süreçlerini geliştirme

Bilgi Güvenliği Bölümü, genellikle karmaşık BT ortamlarında bulunan kritik bilgilerin ve iş süreçlerinin işlemsel ve teknik korumasından sorumludur. Bu görev, artan otomatik çözümlerin ve yazılım bileşenlerinin benimsenmesi ve elektronik belge yönetimine geçişi içerir.

Gelişmiş tehditler ve hedefli saldırıların çığ gibi büyümesi giderek daha çok çözümün üretilmesini sağlamıştır. Üretilen yapılandırılmamış verileri toplamak, saklamak ve işlemek ve çok düzeyli saldırıları tanımlamak ve önceliklendirmek için mevcut süreçler geliştirilmelidir. Bu süreçler arasında aşağıdakiler yer alır:

- tehditlerin manuel olarak önceliklendirilmesi ve olası bir hedefli saldırının göstergesi olabilecek etkenlerin değerlendirilmesi
- hedefli saldırılar hakkında toplanan bilgiler ve gelişmiş istatistik tehditleri;
- olayların tanımlanması ve olaylara yanıt verilmesi;
- ağ trafiğindeki ve e-posta eklerindeki şüpheli nesnelerin analizi
- korumalı altyapıdaki anormal/sıra dışı faaliyetlerin tespiti

Büyük şirketler, günümüzdeki gelişmiş tehditlere merkezi bilgi güvenliği sistemlerine geçiş yaparak, farklı Güvenlik çözümlerindeki verileri birleştirerek (otomatik veri toplama ve olayların korelasyonu - SIEM aracılığıyla) ve güvenlik izleme merkezlerinin (SOC, Güvenlik İşlemleri Merkezi) oluşturulmasıyla bu verilerin sunumunu bir araya getirerek yanıt verir. Ancak bu yaklaşımın hedefli saldırılar ve gelişmiş tehditler karşısında etkili olabilmesi için güvenlik sorunlarının kapsamlı bir şekilde anlaşılması ve siber tehdit analizi hakkında derin bir bilgiye sahip olunması gerekir.

# Çözümümüz

Kaspersky Lab, 2008 yılında özel bir gelişmiş tehdit laboratuvarı kuran ilk teknoloji şirketidir.

Bu sayede, diğer güvenlik satıcılarından daha çok gelişmiş ve hedefli tehdidi açığa çıkarmayı başardık. Haberlerde gördüğünüz yeni bir gelişmiş kalıcı tehdidin, Kaspersky Lab'e ait seçkin Global Araştırma ve Analiz Ekibi (GReAT) tarafından tespit edilmiş olma ihtimali oldukça yüksektir.

Hedefli saldırıları ve APT'leri tespit konusunda kıskanılacak bir başarıya sahip olan GReAT ekibimiz tehdit istihbaratı ile tanınır. Ekibimiz en gelişmiş saldırıların birçoğunu açığa çıkarma konusunda önemli görevler üstlenmiştir. Ekibimiz;

- Stuxnet
- RedOctober
- Flame
- Miniduke
- Epic Turla
- DarkHotel
- Duqu
- Carbanak
- Equation

ve daha birçok saldırının açığa çıkarılmasına yardımcı olmuştur.

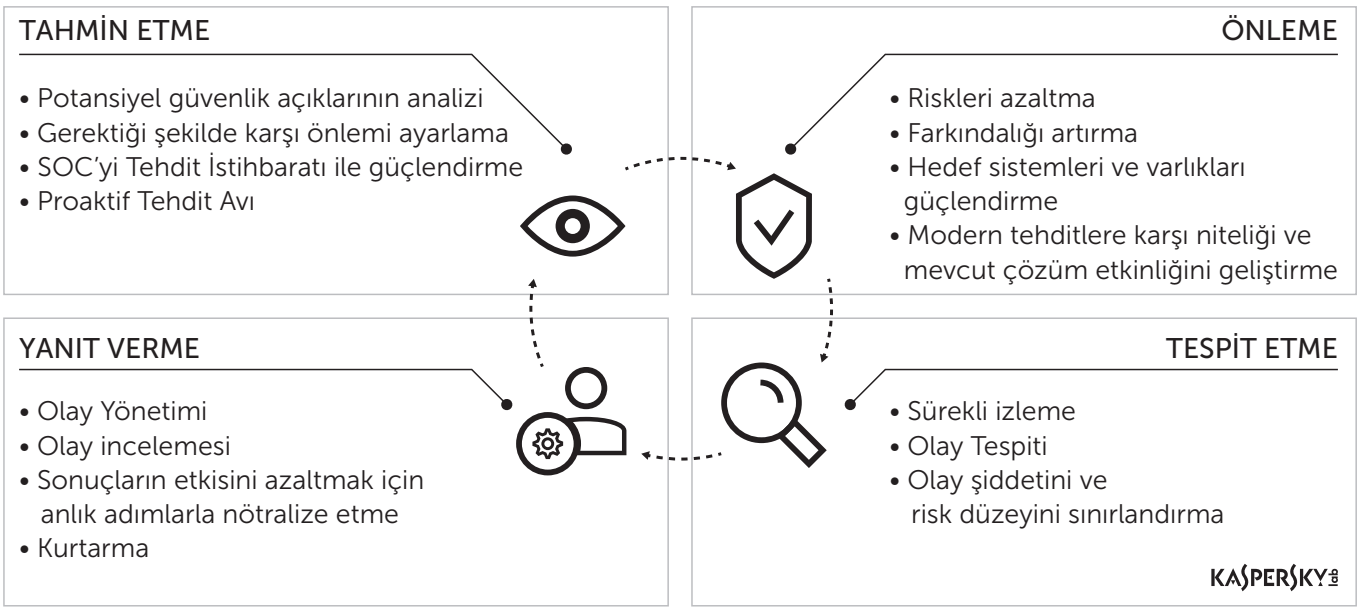
Kaspersky Lab olarak dünyadaki en gelişmiş bazı tehditlerin nasıl çalıştığını anlamamız sayesinde, tamamen entegre ve uyarlanabilir bir güvenlik yaklaşımı sunan stratejik bir teknoloji ve hizmet portföyü geliştirmeyi başardık. Uzmanlığımız, Kaspersky Lab'in bağımsız tehdit tespiti ve risk azaltma testlerinde diğer BT güvenliği şirketlerine göre daha çok birincilik almasını sağlamıştır. Hedefli saldırı konusundaki tespit uzmanlığımızı tek bir bağımsız çözümle birleştirdik. Bu çözüm, yirmi yıllık bir tehdit araştırması ve analizinden yola çıkarak üretilen gelişmiş ve başarısı kanıtlanmış teknolojilerin bir sonucudur.

Basit siber tehditlerin çoğu geleneksel, imza tabanlı ve sezgisel algoritmayla geliştirilen güvenlik ürünleri tarafından engellenebilirken günümüzün siber suçluları ve hacker'ları belirli kuruluşları hedef almak için gittikçe daha gelişmiş saldırılar kullanmaktadır. Gelişmiş Kalıcı Tehditler (APT'ler) dahil olmak üzere hedefli saldırılar, artık şirketlerin mücadele etmesi gereken en tehlikeli risklerden birisidir. Ancak siber suçluların ve hacker'ların kullandığı teknikler ve tehditler sürekli olarak gelişirken bazı şirketler güvenlik stratejilerini buna göre uyarlayamaz.

Tespit etmesi hatta bazen yok edilmesi bile zor olan hedefli saldırılar ve gelişmiş tehditler kapsamlı ve uyarlanabilir bir güvenlik stratejisi gerektirir. Gartner, Kaspersky Lab'in Uyarlanabilir Güvenlik Stratejisi'ni en uygulanabilir güvenlik mimarileri arasında göstermiştir. Yaklaşımımız dört önemli alanda etkinlik döngüsü sağlar: Önleme, Tespit Etme, Yanıtlama ve Tahmin Etme.

- Önleme: Gelişmiş tehdit ve hedefli saldırı riskini azaltır
- Tespit Etme: Hedefli bir saldırının göstergesi olabilecek faaliyetleri bulur
- Yanıt Verme: Güvenlik boşluklarını kapatır ve saldırıları araştırır
- Tahmin Etme: Yeni hedefli saldırıların nerede ve nasıl ortaya çıkabileceğini araştırır

Bu yaklaşım, temelde geleneksel önleme sistemlerinin tespit teknolojileri, tehdit analizleri, yanıt kabiliyeti ve önleyici güvenlik teknikleriyle birlikte çalışması gerektiğini öne sürer. Bu sayede şirketin karşılaştığı yeni zorluklara karşı sürekli olarak uyarlanabilen ve yanıt verebilen bir siber güvenlik sisteminin oluşması sağlanır.



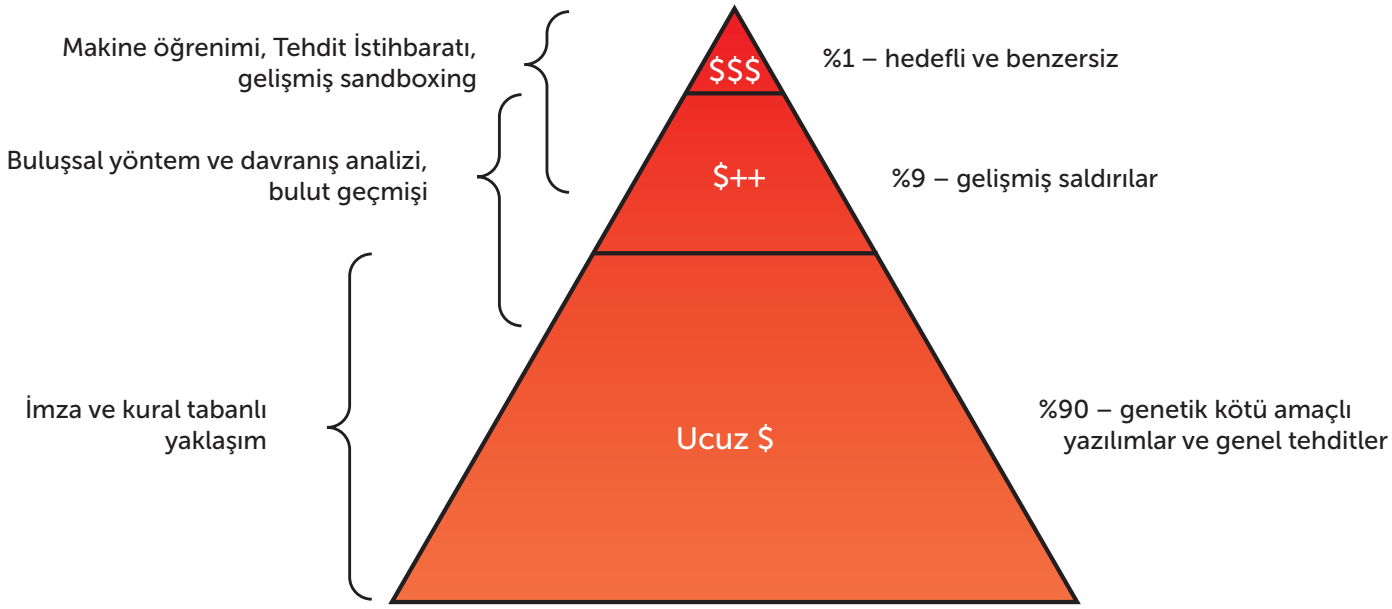
# Önleme: hedefli saldırı riskini azaltmak için ödüllü teknolojiler kullanılır

Önleme teknolojileri, hedefli saldırılar açısından gereksiz olayları, yaygın kötü amaçlı nesneleri ve olayla ilgisiz iletişimleri ayıklama konusunda büyük önem taşır.

Ancak hedefli güvenlik çözümleri ve güvenlik eğitiminin yanı sıra farkındalığı arttırarak kapsamlı sistemlerin güçlendirilmesi de değerlidir. Sistem güçlendirmesi, saldırganların kontrollü çevrenize girmek için harcaması gereken zamanı ve yatırımı arttırır ve sizi ucuz bir saldırı hedefi olmaktan çıkarır.

Önleme tabanlı güvenlik ürünleri; kötü amaçlı yazılımlar, ağ saldırıları ve veri sızıntıları gibi yaygın tehditlere karşı koruma sağlamak konusunda son derece etkili olabilir. Ancak bu teknolojiler bile bir işletmeyi hedefli saldırılara karşı korumak için yeterli değildir. Hedefli saldırı sırasında geleneksel, önleme tabanlı güvenlik teknolojileri bazı olayları fark edebilir ancak bu olayların işletmenizde ağır hasara yol açan ve uzun vadede de hasar oluşturmaya devam edecek olan çok daha tehlikeli ve karmaşık bir saldırının parçası olup olmadığını belirleyemez.

Yine de çok katmanlı ve önleme tabanlı teknolojiler, hedefli saldırılara karşı koruma sağlamak için yeni, proaktif yaklaşımın temel bir unsurunu oluşturur.




## Güvenlik teknolojileriyle farklı tehditlerin ele alınması

Hedefli saldırıların %80'i bir ek veya bağlantı içeren kötü amaçlı e-postalarla başlar.

Siber suçluların tercih ettiği sızma hedefleri arasında İK, çağrı merkezleri, üst düzey yöneticilerin asistanları ve işletmenin dışarıdan aldığı hizmetler vardır. Bu alanlar kurumun en hazırlıksız alanları olarak görülür.

Şirketler için "geleneksel" güvenlik çözümlerini kullanmaya devam etmek şu nedenlerden dolayı çok önemlidir:

1. Hedefli saldırılarla ilgili olmayan vakaların ve olayların filtrelenmesi ve otomatikleştirilmesi, gereksiz ayrıntılarla uğraşılmasını önler ve ilgili olayın ortaya çıkarılmasına yardımcı olur

2. BT altyapısını ucuz ve kolay uygulanabilen yöntemlere karşı güçlendirir (sosyal mühendislik, çıkarılabilir cihazlar, mobil cihazlar, kötü amaçlı yazılımlar ve kötü amaçlı e-postaların dağıtılması vb.). Aslında uygulanan kontrollerin yanı sıra çevre ve uç nokta güvenliğine yapılan tüm harcamalar siber suçluların ağınıza sızması için gereken çaba ve yatırım miktarını arttırmaya yardımcı olur.

Ancak, saldırgan yeterince motive olmuşsa veya başarılı bir saldırı gerçekleştirmek için üçüncü bir kişi tarafından tutulduysa yalnızca önleme tabanlı bir yaklaşım yeterli olmaz.

# Tespit: hasar oluşmadan önce çok vektörlü gelişmiş tehditler ortaya çıkarılır

**Kaspersky Anti Targeted Attack platformu şunları kapsar:**

- Çok katmanlı sensör mimarisi: "Bütünsel" bir görüş sağlar. Ağ, web, e-posta ve uç nokta sensörlerinin birleşimi sayesinde kurumsal BT altyapınızın her düzeyinde gelişmiş koruma sağlar
- Yeni tehditleri değerlendirmek için Gelişmiş Koruma Alanı
  : 10 yıllık sürekli gelişimin sonucu olan Gelişmiş Koruma Alanı, şüpheli nesnelerin güvenli bir şekilde çalıştırıldığı ve bu sayede davranışlarının gözlemlendiği izole ve sanal bir ortam sunar
- Güçlü analitik motorlar: Hızlı kararlar verilmesi ve daha az hatalı pozitif için kullanılır.
  Hedefli Saldırı Analiz Aracı'mız, ağ ve uç nokta sensörlerinden aldığı verileri değerlendirir ve güvenlik ekibiniz için hızlı bir şekilde tehdit tespit etme kararları oluşturur.

Saldırı ne kadar erken tespit edilirse finansal kayıplarınız ve kurumunuzun yaşayacağı aksama da o kadar az olur. Bu nedenle tespitin kalitesi ve etkililiği çok büyük önem taşır.

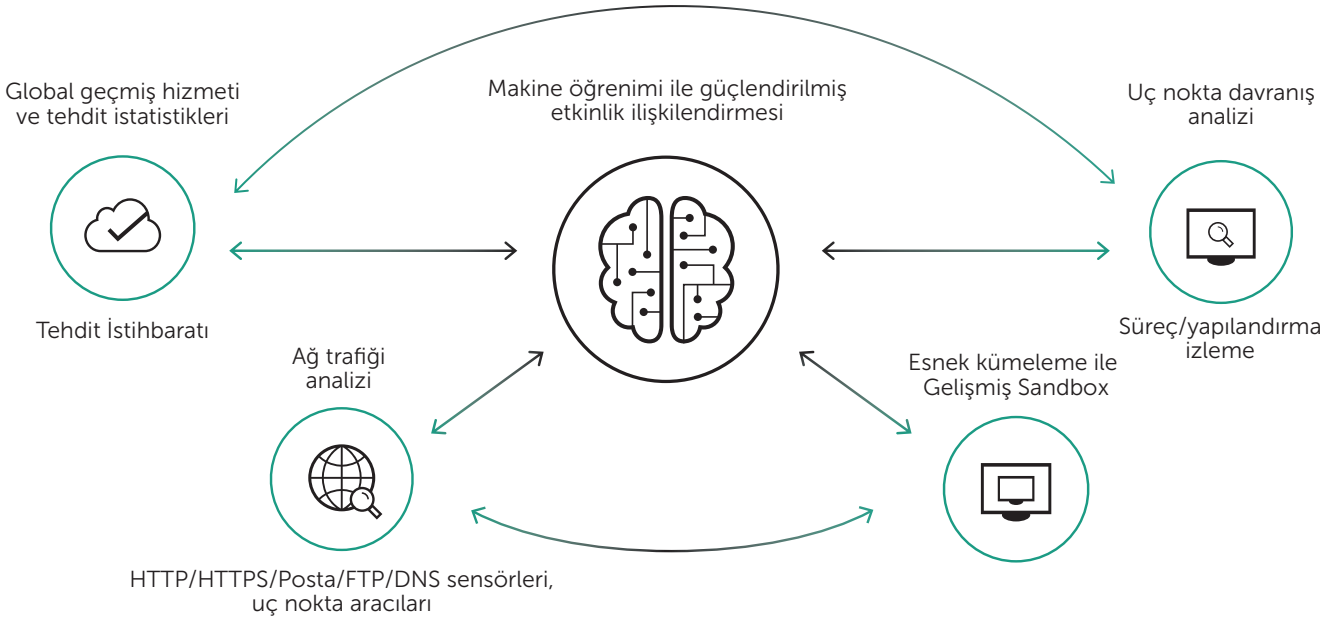
Hedefli saldırılar hem birleşik hem de karmaşık olduğu için bu saldırıları tespit etmek, gelişmiş ve hedefli saldırıların nasıl çalıştığıyla ilgili daha derin ve kullanışlı bilgiler gerektirir. Basit kötü amaçlı yazılıma karşı koruma çözümleri, bu tür saldırılara karşı koruma sağlayamaz. Bunun yerine, en güncel tehdit istihbaratı verilerine erişebilecek ve kurum ağınızın farklı düzeylerinde gerçekleşen şüpheli davranışları ayrıntılı şekilde analiz edebilecek tespit teknolojileri kullanmanız gerekir.

Hedefli saldırıları tespit etme becerisi, aşağıdakileri sunabilen bağlı çözümler ve hizmetlerden oluşur:

- Eğitim
- Hedefli Saldırıyı Ortaya Çıkarma uzmanlığı: tehlike belirtilerini bulmak için tek seferlik altyapı denetimi
- Özel çözüm: Kaspersky Anti Targeted Attack platformu
- Gerçek zamanlı tehdit değişimi ve yeni tehditler hakkındaki güncellemeler için Tehdit Veri Akışı
- Tehdit kaynaklarını ve yöntemlerini daha iyi anlamak için Özel Raporlar ve APT Raporları

Kaspersky Anti Targeted Attack Platform (KATA), geleneksel ve önleme odaklı güvenlik teknolojilerinden çok daha ötesinde tespit kabiliyetleri sağlayan yenilikçi bir çözümdür.

KATA, uyarlanabilir ve entegre şirket güvenliği yaklaşımın bir parçasıdır. Ağ trafiğinin gerçek zamanlı olarak izlenmesinin; nesneler için koruma alanı ve uç nokta davranış analizi ile birleşmesi sayesinde işletmenin BT altyapısında neler olduğu hakkında ayrıntılı bilgiler edinebilirsiniz. KATA; ağ, uç noktalar ve global tehdit ortamı dahil olmak üzere farklı katmanlardan gelen olayları ilişkilendirerek neredeyse "gerçek zamanlı" karmaşık tehdit tespiti işlemini gerçekleştirebilir ve geriye dönük soruşturma yapılmasını sağlar.

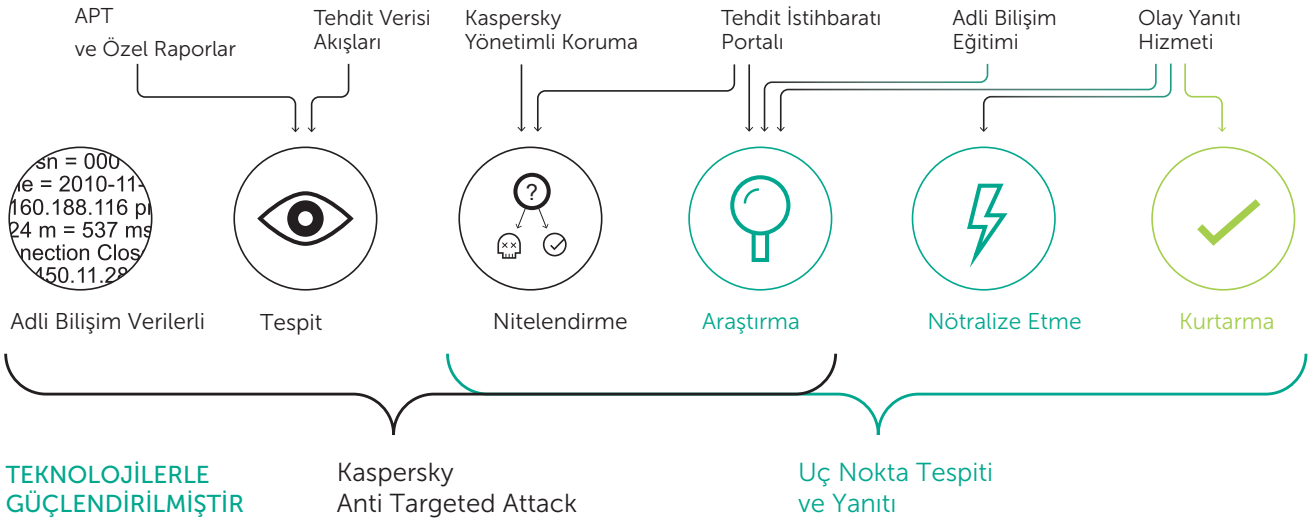


# Yanıt: saldırılardan sonra kurtarma işlemleri için işletmelere yardımcı olur

Daha yüksek tespit oranı mücadelenin yalnızca bir parçasını oluşturur. Kurumunuza zarar verebilecek "canlı" tehditlere hızlı bir şekilde yanıt vermek için gereken araçlara ve uzmanlığa sahip değilseniz en iyi tespit teknolojileri bile işinize yaramaz

Saldırıyı tespit ettikten sonra aşağıdaki konularda size yardımcı olmaları için gereken beceri ve deneyime sahip, tanınmış güvenlik uzmanlarına ulaşabilmek önemlidir:

- Hasarı değerlendirme ve giderme
- Çalışmalarınızı hızlıca kurtarma
- Olay Soruşturma sürecinden sonra eyleme geçirebilir istihbaratlar sağlama
- Aynı saldırı senaryolarının tekrarlanmasını önlemek için tedbirler planlama




Kaspersky Anti Targeted Attack Platform, işletmenizin saldırı altında olduğunu algıladığı anda uzmanlarımız da saldırıyı analiz etmenize yardımcı olabilir. Olay Yanıt Hizmetimiz şunları kapsar:

- Olay değerlendirmesi. Olayın ilk analizi: bu hizmet, işletmenizin uğradığı zararı en aza indirmenize yardımcı olmak için hızlı bir şekilde sunulur (analiz işletmenizin içinde veya uzaktan gerçekleştirilebilir)
- Delil toplama. Bu hizmet kapsamında sabit disk sürücüsü görüntüleri, bellek dökümleri, ağ izleri ve olaya ilişkin diğer bilgiler toplanır
- Adli bilişim analizi. Şunlar hakkında bilgi edinmek için ayrıntılı bir analiz yapılır:
  - Saldırılan sistem
  - Saldırıyı düzenleyenler
  - İşletmenizin saldırıya uğradığı zaman aralığı
  - Saldırının kaynağı
  - İşletmenize saldırılmasının nedeni
  - Saldırının uygulanma şekli
- Kötü amaçlı yazılım analizi. Saldırının parçası olarak kullanılan kötü amaçlı yazılımın ayrıntılı analizi.
- Onarım planı. Kötü amaçlı yazılımın ağınıza daha fazla yayılmasını önlemek ve bir kaldırma planı oluşturmak konusunda işletmenize yardımcı olmak için ayrıntılı bir plan oluşturulur.
- Soruşturma raporu. Olay soruşturması veya onarımı hakkında bilgiler içeren ayrıntılı bir rapor hazırlanır.

Kendi güvenlik ekibiniz olay yanıtı görevlerinin birçoğunu gerçekleştirebiliyorsa aşağıdaki hizmetlerimizden de yararlanabilirsiniz:

- Kötü Amaçlı Yazılım Analizi Hizmeti: Ekibinizin izole hale getirdiği kötü amaçlı yazılımı ayrıntılı bir analize tabi tutar.
- Dijital Adli Bilişim Hizmeti: Ekibiniz tarafından toplanan dijital delilleri ve olayın etkilerini analiz eder.

# Tahmin: gelecekteki tehditlere karşı daha çok koruma sağlanır

Sürekli gelişen tehdit ortamı, güvenlik stratejinizin de yeni zorluklarla mücadele için sürekli olarak gelişmesini gerektirir.

Güvenlik "tek seferlik bir faaliyet" değildir. Aşağıdaki etkenlerin hiç durmadan değerlendirilmesini gerektiren bir devamlı bir süreçtir:

- En yeni tehditler
- BT güvenliğinizin verimliliği

Bunları yaptığınız takdirde, işletmeniz yeni risklere ve değişen taleplere uyum sağlayabilir.

Size global tehdit ortamı hakkında güncel bilgiler sağlamanın yanı sıra sistemlerinizi ve mevcut savunma mekanizmalarınızı test etmenize yardımcı olacak uzmanlara ulaşabilmeniz, kurumunuzun yeni güvenlik tehditlerine uyum sağlamasına ve ayak uydurmasına yardımcı olur.

Global güvenlik uzmanlarımız, yıllar içinde gelişmiş ve tehditli saldırıların nasıl çalıştığıyla ilgili birçok bilgi toplamıştır. Aynı zamanda sürekli olarak yeni saldırı tekniklerini analiz etmeye de devam etmekteyiz. Çok çalışarak kazandığımız bu uzmanlık sayesinde yeni saldırı yöntemlerini tahmin edebilir ve onlarla mücadele etmeniz için hazırlanmanıza yardımcı olabiliriz.

Bunlara ek olarak, BT altyapınızı "güçlendirmeniz" için özel hizmetler de sunabiliriz:

- Sızma Testi Hizmetleri: Mevcut güvenlik önlemlerinizin etkililiğini değerlendirmenize yardımcı olur
- Uygulama Güvenliği Değerlendirme Hizmetleri: Siber suçlular bulmadan önce yazılım açıklarınızı bulmaya yardımcı olur
- Gelişmiş Siber Güvenlik Eğitimi: Kendi uzmanlarınızı eğitmenize ve kendi Güvenlik İşlemleri Merkezi'nizi oluşturmanıza yardımcı olur
- İstihbarat Raporları ve Özelleştirilmiş Tehdit Raporları: Günümüzün sürekli değişen tehdit ortamı hakkında en güncel bilgilere ulaşmanızı sağlar
- Tehdit Arama Portalı: Kötü amaçlı yazılım araştırmacılarınızı Güçlendirmek için Kaspersky Lab istihbarat global veri tabanına erişim imkânı sunar

Gartner, Kaspersky Uyarlanabilir Güvenlik Stratejisi'ni en uygulanabilir güvenlik mimarileri arasında göstermiştir. Kaspersky Lab yaklaşımı şu dört alanda faaliyet döngüleri sağlamayı içerir: Önleme, Tespit Etme, Yanıtlama ve Tahmin Etme. Bu yaklaşım, temelde geleneksel önleme sistemlerinin tespit teknolojileri, tehdit analizleri, yanıt kabiliyeti ve önleyici güvenlik teknikleriyle bağlantılı bir şekilde çalışmasını önerir. Bu sayede şirketin karşılaştığı yeni zorluklara karşı sürekli olarak uyarlanabilen ve yanıt verebilen bir siber güvenlik sisteminin oluşması sağlanır.

Kaspersky Lab'in Gelişmiş Güvenlik Stratejisi'ni benimsemek şunları sağlar:

1. Tepkisel güvenlik modelinden risk yönetimi tabanlı proaktif modele geçiş, sürekli izleme, daha ayrıntılı olay raporu ve tehdit avlama kabiliyeti

2. Faaliyet planlarınız güvenlik süreçlerinin günlük olarak daha düzenli bir şekilde ilerlemesini sağlar. Ayrıca gelişmiş tehditleri, saldırının her aşamasında önleyen ve tespit eden çok katmanlı savunma modeli aracılığıyla güvenlik verimliliği arttırılır.

3. Entegre edilen platform, uyarılara tehdit istihbaratı tabanlı bağlam ve önceliklendirme sağlayarak birçok güvenlik ekibini yoran güvenlik uyarılarını azaltır. Aynı zamanda tehdit bilgilerini ve kapsamlı uzman görüşlerini paylaşır ve güvenlik istihbaratı hizmeti sunar.

4. Bu ortam, güvenlik analistlerine saldırının tüm aşamalarında birleşik bir görünürlük sağlar. Bu sayede, tehditler işletmeyi etkilemeden önce sorunsuz tehdit analizinin yanı sıra bilinen ve bilinmeyen tehditlerin soruşturulmasına imkân sağlanır.

5. APT ve tehdit istihbaratı portalları aracılığıyla paylaşılan Global Tehdit İstihbaratı, rakiplerinizin amaçları ve niyetleriyle ilgili benzersiz, proaktif bilgiler edinmenizi sağlar. Böylece bu bilgilerden yola çıkarak ilkelerinizi ve güvenlik yatırımlarınızı önceliklendirebilirsiniz.

# Kaspersky Lab Teknolojileri'nde uzmanlık dünyası

Kaspersky Lab ürünlerinin verimliliği, bağımsız testlerin sonuçlarıyla düzenli olarak kanıtlanır. Şirket, 2016 yılında, en iyi 3 güvenlik çözümü üreticisi sıralamasında birinciliği elde etmiştir. Birçok ülkede saygın değerlendirme kurumları tarafından düzenlenen 78 farklı testin sonuçlarına göre, Kaspersky Lab çözümleri bu testlerin %90'ınında ilk üçe girerken 55 kez birinci olmayı başarmıştır. Bu test sonuçları, Kaspersky Lab'in sektördeki en iyi korumayı sağladığına dair inkâr edilemez bir kanıt sunar.


# Gelişmiş tehditlere karşı başarısını kanıtlamış çözümler

Kaspersky Anti-Targeted Attack Platform, 2017 yılında ICSA Lab testlerine katıldı.

585 saldırı ve 519 temiz dosyadan oluşan son test 37 gün sürdü. KATA bu testte mükemmel sonuçlar elde etti:

- Mükemmel tespit oranı: %100 (HİÇBİR numune atlanmadı)
- Mümkün olan en düşük hatalı pozitif oranı: %0
- "Sertifikalı" statüsünü almaya hak kazandı

Aşağıda, ICSA tarafından 7 Temmuz tarihinde yayınlanan sonuç raporundan bazı alıntıları bulabilirsiniz:

- "Kaspersky'nin çözümü bu test döngüsünde önemli bir başarılı elde etmiştir"
- "Kaspersky Lab KATA platformu, test sırasında karşılaştığı tehditlerin %100.0'ünü tespit etmiştir. Bu oran, sertifika için gereken yüzdeden oldukça yüksektir."
- "Kaspersky Lab'in KATA platformu, yaklaşık olarak 600 yeni ve az bilinen tehdide karşı mükemmel bir tehdit tespiti verimliliği göstermiştir."
- "Tehdit ne kadar yeni veya eski de olsa, Kaspersky KATA platformu tüm yeni ve az bilinen kötü amaçlı tehditleri tespit etmiştir."
- "Kaspersky KATA platformu test döngüsü sırasında sıfır hatalı pozitifle mükemmel bir sonuca ulaşmıştır."
- "Kaspersky Lab'in KATA gelişmiş tehditlere karşı savunma çözümü, tüm test vakalarını başarıyla tamamlayarak ICSA Labs Gelişmiş Tehditlere Karşı Savunma Sertifikasını almaya hak kazanmıştır. Bu test döngüsünün başarıyla tamamlanması, Kaspersky Lab'in ICSA Labs ATD sertifikası test kriterlerini art arda 3. kez karşıladığı çeyreği gösterir."

NOT: ICSA test metodolojisi dinamiktir ve her üç ayda değişir. Test, gerçek hayata dayalı bir ortamın ve saldırı yöntemlerinin sürekli olarak gelişen bir simülasyonudur. Güvenlik düzeyi ölçümü, yalnızca belirli bir anı değil birçok saldırı altında sürekli çalışılan uzun (30 günden daha fazla) bir zaman dilimini kapsar. Böylece test çözümün kullanıcı bakış açısından yeterliliğini ve verimliliğini ölçmeyi amaçlar.

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

# Vizyoner ve kapsamlı yaklaşım

Radicati Group, uzun yıllardır APT Koruma Çözümleri Piyasası'nın bağımsız bir analizini yapmaktadır. Bu analiz sonucunda En Üst Düzeydekiler (Top Players), Öncüler (Trail Blazers), Uzmanlar (Specialists) ve Gelişmiş Firmalar (Mature Players) kategorilerindeki şirketlerin belirlenmesi amaçlanmıştır. Yeni yayınlanan piyasa analizi sonuçlarına göre Kaspersky Lab'in hedefli saldırılar ve gelişmiş tehditlere karşı mücadele yaklaşımı mükemmel olarak değerlendirilmiştir.

KATA, 2017 yılında Uzmanlar kategorisinden Öncüler kategorisindeki lider konumuna yükselmiştir.

Öncü konumundaki satıcılar, çözümlerinin bazı alanlarında gelişmiş ve türünün en iyisi teknolojiler sunarken En Üst Düzeydekiler kategorisine girmek için gerekli tüm özelliklere ve işlevselliğe sahip olamayabilir. Ancak yine de Öncü kategorisindeki şirketler, yeni teknoloji ve modelleri ile piyasayı "etkileme" potansiyeline sahiptir. Öncüler, zamanla En Üst Düzeydekiler kategorisine girme ihtimali en yüksek olan şirketlerdir.

«Kaspersky Anti Targeted Attack Platform; ilk bulaşma, komuta ve kontrol iletişimi, yanal hareketler ve veri sızıntısı olmak üzere hedefli bir saldırının tüm katmanlarında gelişmiş tehdit ve hedefli saldırı tespiti sağlar».

Kaspersky Lab
Kurumsal Güvenlik: **www.kaspersky.com/enterprise**
Siber Tehdit Haberleri: **www.securelist.com**
BT Güvenliğiyle İlgili Haberler: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

**www.kaspersky.com**