KASPERSKY lab

Kaspersky Lab Destekli SOC

www.kaspersky.com.tr
#truecybersecurity

Kaspersky Lab destekli Güvenlik İşlemleri Merkezi

İşletmeler kendilerini korumanın daha iyi yollarını öğrenirken aynı anda suçlular da işletmelerin güvenlik duvarlarını yıkmak için daha karmaşık yöntemler geliştirir. Siber saldırıların sunduğu eşsiz fırsatların cazibesine kapılan ve sayıları her geçen gün artan tehdit aktörleri, fark edilmemiş güvenlik hatalarını arar ve hedef alır. Ortaya çıkan güvenlik sorunları ile mücadele etmek ve bu sorunlara hızlı bir yanıt ve çözüm bulmak için birçok şirket Güvenlik İşlemleri Merkezleri (SOC) kurmaktadır.

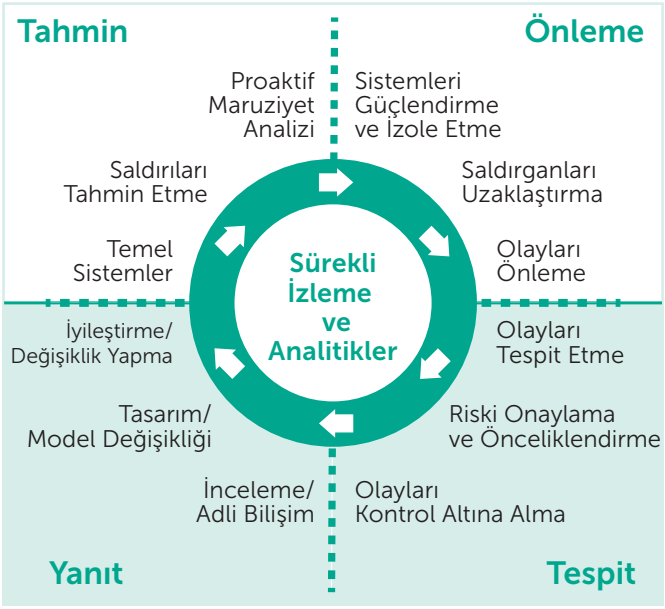
Yakın zamanda B2B International ("Global BT Güvenlik Riskleri Araştırması 2017"), 25 ülkeden 5274 işletmenin katıldığı bir araştırma yayınladı. Bu araştırmada 2016'ya kıyasla tüm saldırı türlerinde önemli bir artış olduğu tespit edildi:

- **Katılımcıların %49'u** (+%11) son 12 ayda virüsler ve kötü amaçlı **yazılımlarla ilgili ciddi sorunlar** yaşamış ve bunların sonucunda üretkenlik kaybı yaşamıştır.
- **Toplamda katılımcıların %49'ı ve kuruluşların %55'i veri kaybı/sızıntısı/ ifşası** yaşamıştır**.**
- Katılımcıların yaklaşık %40'ı bu sorunlar hakkında ciddi bir endişe duyduklarını belirtmiştir.
- **İşletmelerin %33'ü (+%16)** son 12 ayda birden fazla **DDoS saldırısına** maruz kalmıştır.
- İşletmelerin %23'ü son 12 ayda kripto kötü amaçlı yazılım olayından etkilenmiştir.
- Bir **saldırı yaşadığını bildiren işletme** oranı**, bu yıl büyük bir artış** göstererek **%77'ye ulaşmıştır**.
- En az bir veri ihlaline maruz kalan bir kuruluş için **ortalama finansal etki 992 bin USD'dir** (Bu miktar, ek şirket içi personel masraflarını, kredi derecelerindeki/sigorta primlerindeki zararı, kaybedilen işleri, marka hasarını düzeltmek için ek PR çalışmalarını ve dış danışmanların işe alınmasını kapsar).
- Koordineli çoklu vektör saldırıları, özellikle 1000'den fazla çalışanı olan işletmeler için ciddi bir sorundur. Bu tür bir saldırının finansal etkisi iki kat artarak 1,7 milyon USD'ye ulaşabilir.

SOC, tehditlerin sürekli izlenmesi ve analiz edilmesinin yanı sıra siber güvenlik olaylarının riskinin azaltılması ve önlenmesi için merkezi bir görev üstlenir

Gartner'ın Uyarlanabilir Güvenlik Mimarisi modeline göre SOC ekiplerinin mevcut tehdit ortamında başarılı bir şekilde mücadele etmeleri için aşağıdaki becerilere sahip olmaları gerekir:

- TAHMİN ETME
- TESPİT ETME
- ÖNLEME
- YANIT VERME



Gartner, Gelişmiş Saldırılara Karşı Koruma İçin Uyarlanabilir Güvenlik Mimarisi Tasarlama, Şubat 2014, Foundational Ocak 2016

"Güvenlik işlemleri merkezinin; bağlam bilinçli ve istihbarat temelli hale gelmesi için uyarlanabilir bir güvenlik mimarisi benimsenmeli ve merkez, istihbarat temel alınarak planlanmalıdır. Güvenlik liderleri modern tehditlerden korunmak için istihbarat temelli SOC'lerin araçları, süreçleri ve stratejileri nasıl kullandığını anlamalıdır."

Gartner, İstihbarat Temelli Güvenlik İşlemleri Merkezlerinin Beş Özelliği, Kasım 2015

Dört Temel Unsur

Sektör tarafından kabul edilen bir yaklaşımı devam ettirmek için açıkça tanımlanmış süreçlerin
ve ilgili teknolojilerin yanı sıra dört temel unsur kullanılmalıdır. Bu reklamlar:

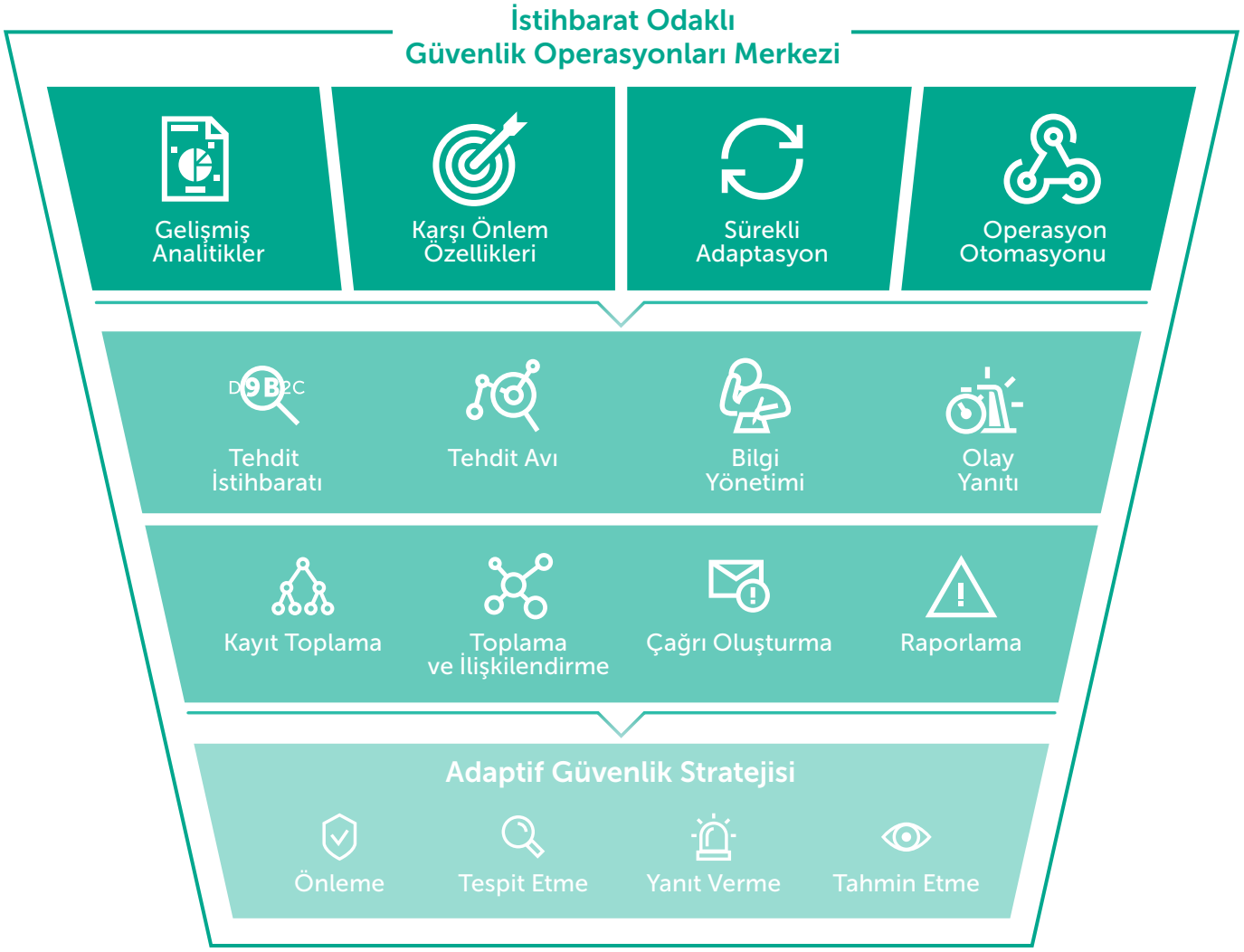
- **Bilgi yönetimi.** Gittikçe karmaşıklaşan saldırıları önlemek ve bunlara başarılı bir şekilde yanıt vermek için çalışanlar (SOC ekip üyeleri) adli bilişim, kötü amaçlı yazılım analizi ve olay yanıtı konusunda iyi eğitimli olmalıdır.

- **Birçok farklı kaynaktan (ne kadar çok olursa o kadar iyi olur) toplanan tehdit istihbaratı** yeni ortaya çıkan tehditlerin tespiti için büyük önem taşır:
  1. İç tehdit verileri
  2. Açık kaynak istihbaratı (OSINT)
  3. Sektördeki Bilgisayar Acil Durum Müdahale Ekipleri (CERT)
  4. Global kötü amaçlı yazılımlara karşı koruma yazılımı tedarikçileri

- **Koruma duvarı, IPS/IDS ve SIEM gibi geleneksel güvenlik sistemleri tarafından fark edilmeyen tehditleri proaktif bir şekilde aramak için tehdit avı**.

- **Zararı sınırlandırmak ve onarım masraflarını azaltmak için kullanılan bir olay yanıtı çerçevesi**.

Bu ögelerin hepsi aynı derecede önemlidir ve hepsiyle ayrı ayrı ilgilenilmesi gerekir.



Şekil 1:
SOC'un dört temel unsuru

Bilgi Yönetimi

SOC, büyük miktarda veriyi analiz etmek ve daha çok soruşturma gerektiren alanları belirlemek için yeterli bilgi ve uzmanlıktan oluşan bir kaynak havuzu sunmalıdır.

Kısıtlı bütçeler, SOC için gerekli yeterliliklere sahip personeller bulmayı zorlaştırır.

Şu anda piyasada iyi eğitimli siber güvenlik uzmanı sıkıntısı yaşanmakta ve bu durum işe alma ve çalıştırma maliyetlerini artırmaktadır.

Etkili bir SOC Ekibi Üyesi şu özelliklere sahip olmalıdır:

- Dağınık veri parçalarından entegre ve genel bir tablo oluşturmayı başarabilecek araştırmacı düşünce yapısı.
- Yüksek stres düzeylerine dayanma ve bu sırada sürekli olarak odaklanmayı başarabilme.
- Tercihen çok deneyimli olmanın yanı sıra BT ve siber güvenlik alanlarında iyi düzeyde genel bilgi.

SOC pozisyonlarını dışarıdan eleman almakla veya iç terfilerle doldurmayı düşünseniz de "kullanıma hazır" becerilere sahip ekip üyelerini bulmak kolay değildir. Yalnızca mevcut beceriler ve gereken beceriler arasındaki boşlukları kapatmak için değil aynı zamanda ekip üyelerinin sürekli değişen güvenlik teknolojileri ve hiç durmadan gelişen tehdit ortamıyla mücadele etmeleri için de sürekli eğitim gereklidir.

Olay yanıtı, adli bilişim ve kötü amaçlı yazılım analizi zorunlu becerilerdir.

Olay yanıtı ve adli bilişim	Kötü amaçlı yazılım analizi
• Olaya zamanında ve doğru şekilde yanıt verme • Kanıtları analiz etme (hdd imajları, bellek dökümleri, ağ etkinliği izleri) ve olay geçmişini ve mantığını yeniden oluşturma • Saldırının kaynaklarını ve ele geçirilmesi muhtemel olan diğer sistemleri ortaya çıkarma (mümkünse) • Benzer olayların yaşanmasını önlemek için olayın kök nedenini anlama	• Şüpheli yazılım numunesini ve özelliklerini anlama • Numunenin gerçekten kötü amaçlı yazılım olup olmadığını belirleme • Numunenin kurum içinde ele geçirilen sistemler üzerindeki olası etkilerinin belirlenmesi • Açığa çıkarılan kötü amaçlı yazılım davranışlarına dayalı kapsamlı bir onarım planı oluşturma

Kaspersky Lab şunları sunar: Siber Güvenlik Eğitim Hizmetleri

Kaspersky Lab'in siber güvenlik uzmanlığı (tehdit tespiti, kötü amaçlı yazılım analizi, tersine mühendislik ve adli bilişim dahil olmak üzere) 20 yıldan uzun bir süredir sürekli olarak gelişmekte ve ilerlemektedir. Uzmanlarımız, her gün karşılaştığımız 325,000 adet kötü amaçlı yazılım numunesinin oluşturduğu tehditlerle nasıl mücadele edileceğini bilir ve bu bilgi ve deneyimi günümüz siber dünyasının yeni tehlikeleriyle karşı karşıya kalan kurumlara nasıl sunabileceğini anlar.

Güvenlik Eğitimi Programı'mız, Kaspersky antivirüs laboratuvarlarının oluşturulmasına yardımcı olan ve geleceğin global uzmanlarına ilham veren ve onlara akıl hocalığı yapan güvenlik yetkilileri tarafından tasarlanmış ve geliştirilmiştir.

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

Eğitim kursları, genel ve gelişmiş sistem yönetimi ve programlama becerilerine sahip BT uzmanları için uygundur. Bu eğitimlerin tümü müşteri tesislerinde veya Kaspersky yerel ya da bölgesel ofislerinde sınıf içi şeklinde verilebilir.

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 istatistik analiz teknikleri (dize çözümlemesi, içeri aktarım 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 nesneyi 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		
• 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	• 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
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

Kullanılan araçlar zamanla değişse de temel çalışma yöntemleri ve bilgileri aynı kalır. Katılımcılar, sadece araç ve talimatlardan oluşan bir eğitim almaz aynı zamanda temel ilkeleri ve işlevleri de öğrenir. Tüm uygulamalı görevler, müşterinin gizliliği

ihlal edilmediği sürece gerçek vakalara dayalıdır.

Tehdit istihbaratı ve tehdit avı

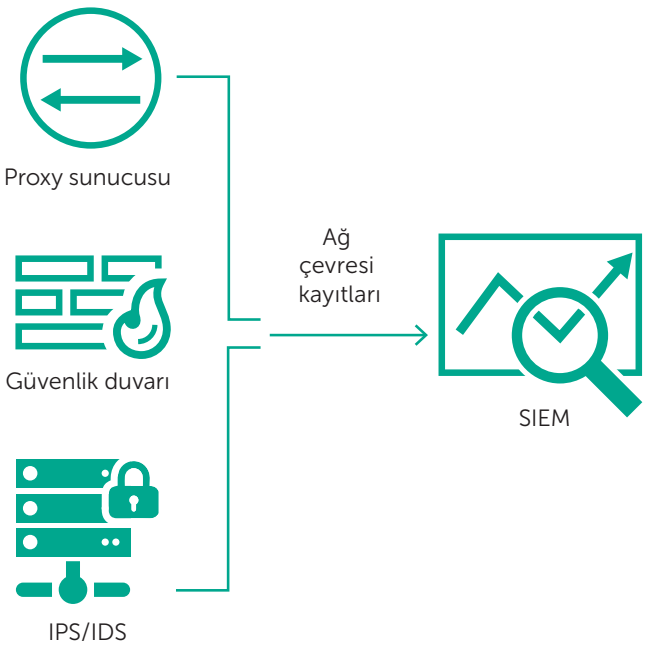
SOC genel olarak şu hizmetleri sunmak için geliştirilmiştir:

- Güvenlik cihazı yönetimi, çevre bakımı ve IPS/IDS, koruma duvarları ve proxy'ler gibi önleyici güvenlik teknolojileri.
- Güvenlik Bilgisi ve Olay Yönetimi sistemi (SIEM) aracılığıyla güvenlik olaylarını izleme.
- Olay adli bilişimi ve onarımı.
- Kurum içi gerekliliklere ve yönetmelik gerekliliklerine uyum (ör; PCI-DSS).

Birçok kurum artık kendi SOC ekiplerini oluşturarak daha çok tehdit görünürlüğü sağlamayı planlamaktadır. Ancak SOC merkezine sahip bazı kurumlar hala aynı sorunlara mücadele eder. Bu sorunun bazı nedenleri şunlardır:

- Kötü önceliklendirme nedeniyle gerçek tehditlerin her gün alınan ve analiz edilen binlerce güvenlik uyarısından dolayı gözden kaçması.
- İlgili tehdit aktörlerinin TTP'leri (Taktikler, Teknikler ve Prosedürler) tam olarak anlaşılmadan olay onarımı yapılması ve bu nedenle gelişmiş saldırıların fark edilememesi.
- İlgili tehdit verileri eksikliği nedeniyle hatalı negatifler.
- Keşfedilmemesine rağmen kurum içinde aktif olan tehditleri proaktif bir şekilde "avlamak" yerine reaktif olay yaklaşımı.
- Mevcut tehdit ortamıyla ilgili stratejik bir genel değerlendirme yapılmaması veya benzer şirketlerin karşılaştığı saldırılar ve kullanılabilir önlemler konusunda farkındalığın olmaması.
- Güvenlik ihlallerinin iş süreçleri için oluşturduğu risklerin teknik konularla ilgilenmeyen üst düzey yöneticilere anlatmanın zor olması nedeniyle belirli güvenlik teknolojileri alanına yeterli yatırım yapılmaması.

Bu noktalar göz önünde bulundurulduğunda güvenlik liderleri istihbarat temelli SOC yaklaşımını benimseme konusunda daha bilinçli hareket edecektir. SOC merkezinin etkili olabilmesi için tehdit ortamındaki hızlı değişikliklerle aynı doğrultuda ilerleyen yeni teknoloji ve kontrollere göre sürekli olarak kendini uyarlayabilmelidir.

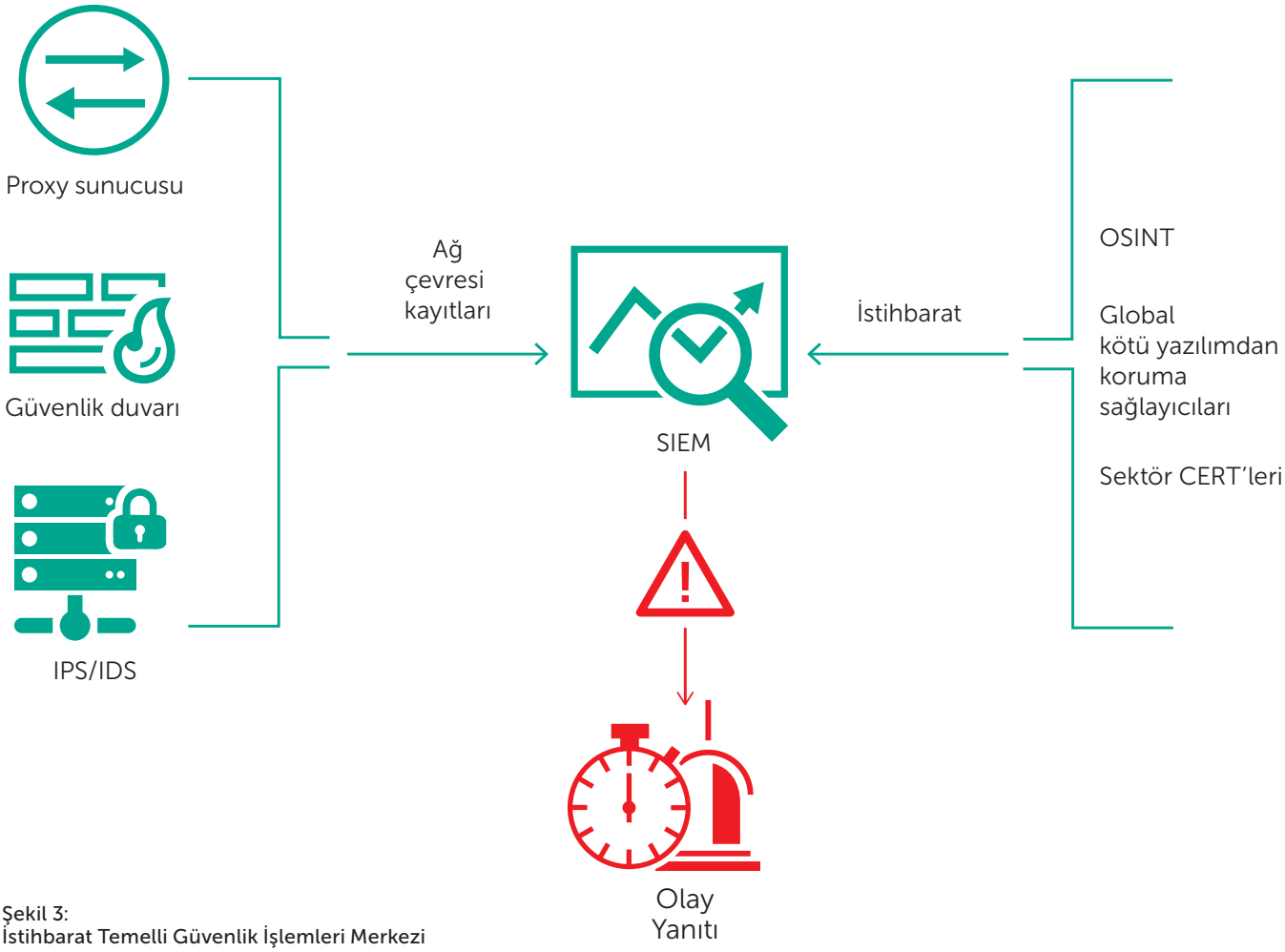


Şekil 2:
Geleneksel SOC

Gartner, Tehdit İstihbaratı'nı şu şekilde tanımlar: "Varlıklara karşı mevcut veya yeni ortaya çıkan bir tehdit veya zarar hakkında öznenin ilgili tehdit veya zarara karşı vereceği yanıtla ilgili kararları için kullanılabilecek bağlam, mekanizmalar, göstergeler, belirtiler ve eyleme geçirilebilir tavsiyeler dahil olmak üzere kanıta dayalı bilgiler."

Gartner, Gartner Tehdit İstihbaratı'nı Nasıl Tanımlar, Şubat 2016

Çeşitli kaynaklardan toplanan bilgilerin (ör; Açık Kaynak İstihbaratı veya global kötü amaçlı yazılımlara karşı koruma tedarikçileri) kurum için tehdit verileriyle birleştirilmesi, saldırı tekniklerinin ve olası göstergelerin anlaşılmasını sağlar. Sonuç olarak bu yöntem, kurumların belirli kurumları hedef alan yaygın ve gelişmiş tehditlere karşı etkili savunma stratejileri geliştirmesini sağlar.



Şekil 3:
İstihbarat Temelli Güvenlik İşlemleri Merkezi

İstihbarat kaynakları dikkatli bir şekilde seçilmelidir. Kullanılan istihbaratın kalitesi ve bu istihbarat temel alınarak verilen kararların etkililiği birbirine doğrudan bağlıdır. Alakasız, yanlış ya da sektör ve işletme amaçlarınıza uygun olmayan istihbaratlara güvenirseniz veya tehdit bilgileri anında elde edilmediyse kurumunuzun karar alma sürecinin kalitesi ciddi anlamda düşebilir.

Bağlam olmadan sağlanan ham veriler, SOC ekiplerinin tam olarak etkili olması için gereken ilişkiyi kuramaz. Örneğin; bir URL'nin kötü amaçlı olduğunu bilmek aynı zamanda bu URL'nin güvenlik açıklarından yararlanan bir yazılım veya belirli bir tür kötü amaçlı yazılım barındırdığını bilmekten çok farklıdır. Bu ek istihbarat katmanı sayesinde, saldırıdan etkilenen bir makineyi incelen uzmanlarınız nelere bakmaları gerektiğini öğrenebilir.

Dış Tehdit İstihbaratı kaynaklarından neler beklenmelidir:

- Dünya geneline erişimi olan ve en geniş saldırı görünürlüğünü sağlayan istihbarat
- Yeni tehdit göstergelerini erken bulma konusunda iyi bir geçmişi olan tedarikçi
- Bağlam açısından zengin ve anında eyleme geçirilebilir istihbarat
- Mevcut güvenlik kontrollerine kolay entegrasyon sağlayan teslim formatları ve mekanizmaları

Tehdit avı görevi de günlük SOC işlemleri için önemli bir unsurdur. Tehdit avı yeni bir kavram değildir. Bilinmeyen ve gelişmiş tehditlerin tespiti, otomatik kurallar ve imza tabanlı tespit mekanizmaları yerine güvenlik analistlerinin titiz ve uygulamalı çabalarına dayanır.

Bu süreç; uç noktalar, ağlar, uygulanan güvenlik kontrolleri, doğrulama sistemleri vb.den elde edilen tüm verilerin toplanması ve bu verilere farklı tekniklerin (istatiksel analiz, makine öğrenimi ve görselleştirme gibi) uygulanmasını içerir. Bu prosesin amacı, olası güvenlik ihlali konusunda mevcut bir hipotezi doğrulamaktır. Tehdit avı teknolojilerinde analist, daha önce bahsedilen SIEM çözümleri, Açık Kaynak İstihbaratı, Tehdit İstihbaratı Platformları ve diğer veri kaynakları gibi kaynakları kullanabilir.

Tehdit avı analisti, dışarıdan alınan IOC'lere (Risk Göstergeleri) başvurur ve kurumun ana bilgisayarlarında bu yapıları bulmak için (IP adresleri, dosya karmaları, URL'ler şeklinde) özel araçlar kullanır. Güvenliğin ihlal edildiğine dair kesin bir belirti bulunduğunda olay yanıtı prosedürleri başlatılabilir.

Otomatikleştirilmiş önlemlerin tespit edemediği yapıları tanımlamak için büyük miktarlardaki verilerin arasında arama yapmak son derece nitelikli ve deneyimli uzmanların işidir.

Hizmetin öne çıkan özellikleri

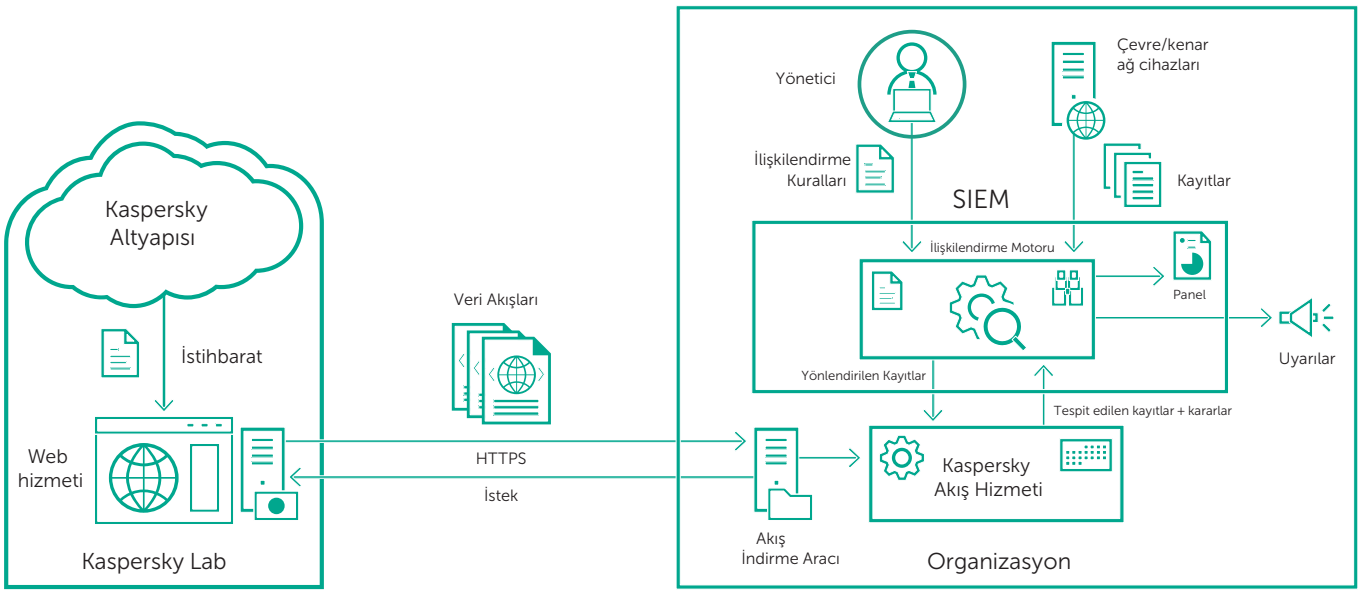
- Veri Akışları, dünya genelinden toplanan bulgular (200 ülkeden milyonlarca kullanıcıyı kapsayan Kaspersky Security Network İnternet trafiğinin önemli bir kısmı için görünürlük sağlar) temel alınarak gerçek zamanlı bir şekilde üretilir ve yüksek tespit oranları ve doğruluk sağlar.
- Veri Akışlarındaki 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 zamanında kararlar almanıza ve harekete geçmenize yardımcı olarak kuruluşunuzu korumanıza yardımcı olabilir.
- HTTPS veya özel teslim mekanizmaları aracılığıyla basit ve hafif dağıtım formatları (JSON, CSV, OpenIoC, STIX), akışların güvenlik çözümlerine kolay entegrasyonunu sağlar.
- Tehdit İstihbaratı, sürekli kullanılabilirlik ve tutarlı performans sağlayan ve hatalara son derece dayanıklı bir altyapı tarafından oluşturulur ve izlenir.
- HP ArcSight, IBM QRadar, Splunk ve daha birçok tedarikçiyle anında entegrasyon.

Kaspersky Lab şunları sunar: Tehdit Veri Akışları

Kaspersky Lab, siber tehditlerle ilgili riskler ve sonuçlar hakkında SOC ekiplerinize bilgi vermek için sürekli olarak güncellenen Tehdit Veri Akışı hizmeti sağlar. Bu sayede tehdit risklerini daha etkili bir şekilde azaltmanız ve saldırı başlamadan önce onlara karşı kendinizi savunmanız için size yardımcı olur.

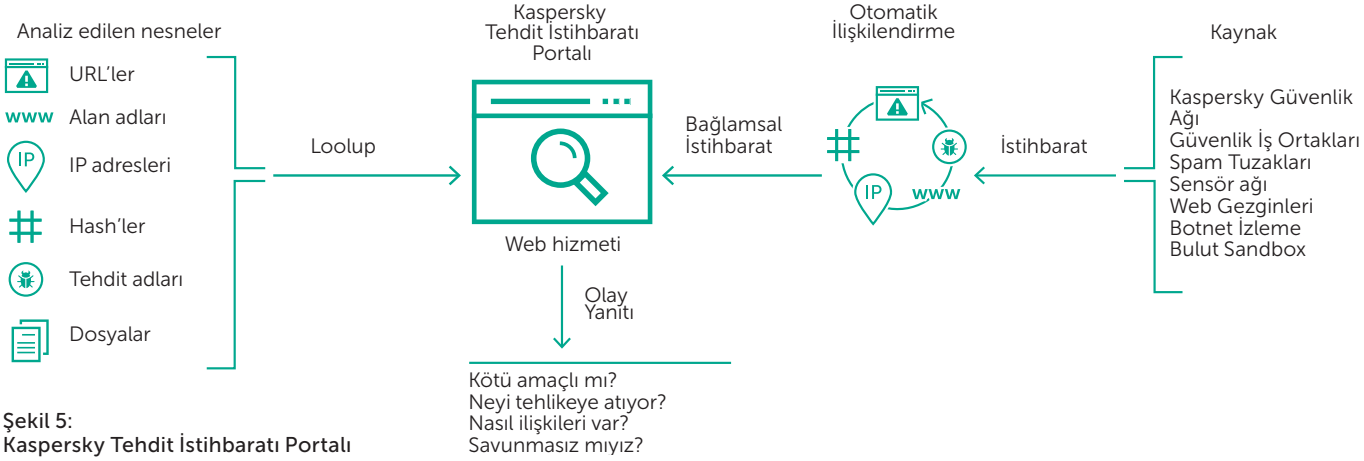
Akış açıklaması

- **IP Bilinirlik Akışı**: şüpheli ve kötü amaçlı bilgisayarları kapsayan IP adresleri seti.
- **Kötü Amaçlı URL'ler**: kötü amaçlı linkleri ve web sitelerini kapsayan URL seti. Maskelenmiş ve maskelenmemiş kayıtlar kullanılabilir.
- **Kimlik Avı URL'leri**: Kaspersky Lab tarafından kimlik avı siteleri olarak tanımlanmış URL seti. Maskelenmiş ve maskelenmemiş kayıtlar kullanılabilir.
- **Botnet Komuta ve Kontrol URL'leri:** botnet komuta ve kontrol (C&C) sunucuları ve ilgili kötü amaçlı nesneleri kapsayan URL seti.
- **Fidye Yazılımı URL Akışı**: fidye yazılımı nesnelerini barındıran veya bunlar tarafından erişilen bağlantıları kapsar.
- **APT Risk Göstergesi Akışları**: 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.
- **Beyaz Liste Veri Akışı**: yasal yazılımlar hakkında sistematik bilgi sağlayarak üçüncü taraf çözümleri ve hizmetleri sağlayan dosya karmaları seti.
- **Kötü Amaçlı Karma Akışı**: en tehlikeli, yaygın ve yeni ortaya çıkan kötü amaçlı yazılımları kapsar.
- **Mobil Kötü Amaçlı Karma Akışı**: mobil platformlara bulaşan kötü amaçlı nesneleri tespit etmeye yönelik dosya karması seti.
- **P-SMS Truva Atı Akışı**: mobil kullanıcılar için özel ücretlere neden olan ve saldırganın SMS mesajlarını çalmasını, silmesini ve bunlara cevap vermesini sağlayan SMS Truva Atları'nın tespiti için ilgili bağlamla birlikte Truva Atı karmaları seti.
- **Mobil Botnet Komuta ve Kontrol URL'leri**: Mobil botnet komuta ve kontrol sunucularını kapsayan bağlamlarıyla birlikte URL setleri.



Şekil 4: Tehdit Veri Akışları'nın SIEM ile entegrasyonu

Kaspersky Threat Intelligence Portal



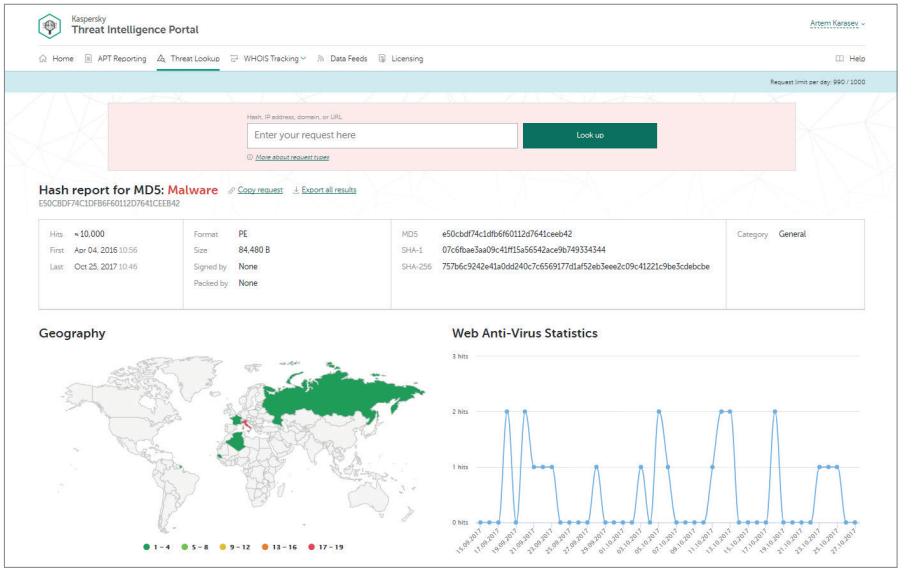
Şekil 5:
Kaspersky Tehdit İstihbaratı Portalı

Hizmetin öne çıkan özellikleri

- **Güvenilir İstihbarat**: Kaspersky Threat Intelligence Portal 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.
- **Korumalı Alan Analizi**: 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 İstihbaratı'nın 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.

Kaspersky Threat Intelligence Portal, siber tehditler ve ilişkileri hakkında Kaspersky Lab tarafından edinilen tüm bilgileri tek ve güçlü bir web hizmeti çatısında toplar. Amaç, SOC ekiplerine mümkün olduğu kadar çok veri sağlamak ve siber saldırılar kurumunuza zarar vermeden onları önlemektir. Portal; URL'ler, etki alanları, IP adresleri, dosya karmaları, tehdit adları, istatistiksel veriler/davranış verileri, WHOIS/DNS verileri, dosya öznitelikleri, coğrafi konum verileri, indirme zincirleri ve zaman damgaları ile ilgili en yeni ve ayrıntılı Tehdit İstihbaratlarını sağlarken Bulut Korumalı Alan teknolojisi, bu bilgilerin analiz edilen örnek tarafından üretilen IOC'lerle ilişkilendirilmesini sağlar. Sonuç olarak, yeni ve gelişmekte olan tehditlerin global görünürlüğü elde edilir. Bu sayede kurumunuzu koruyabilir ve olay yanıtınızı geliştirebilirsiniz.

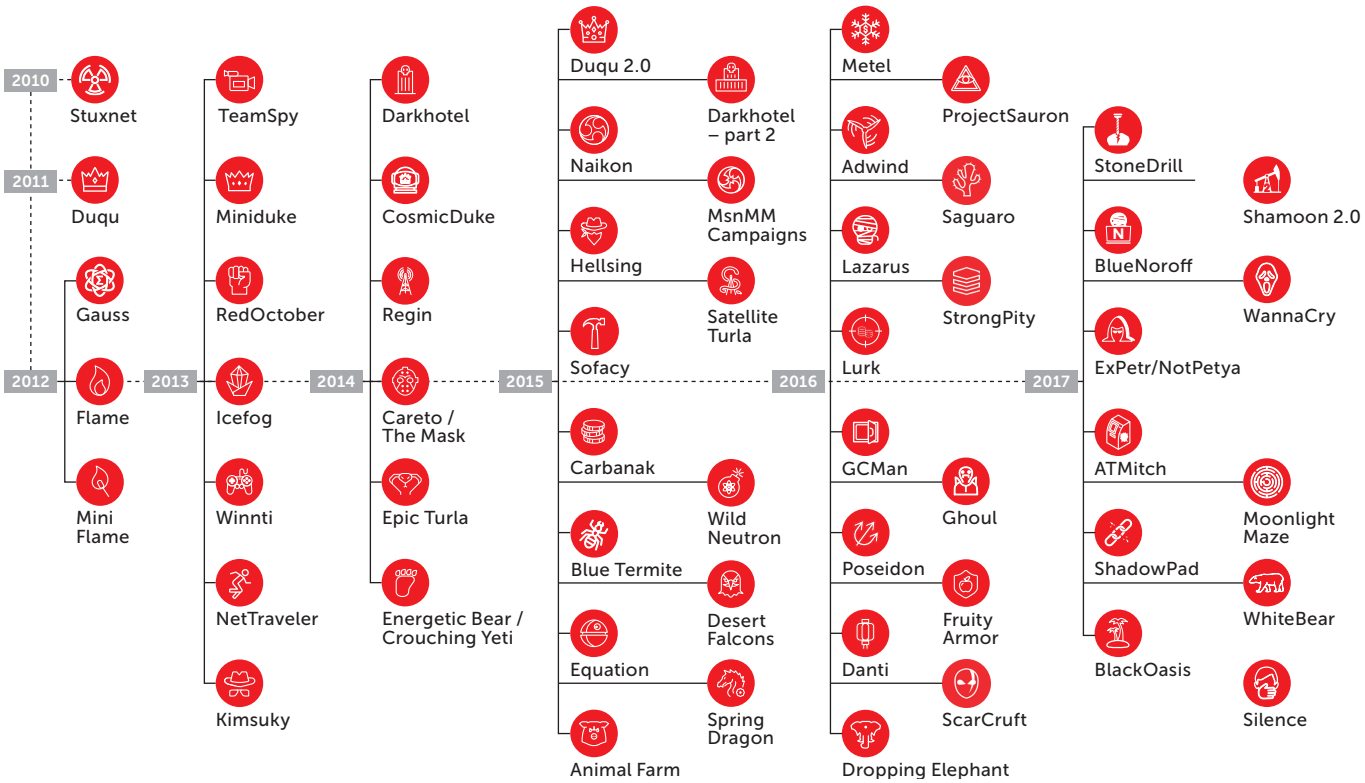
Kaspersky Threat Intelligence Portal tarafından sağlanan tehdit istihbaratı, sürekli kullanılabilirlik ve tutarlı performans sağlayan ve hatalara son derece dayanıklı bir altyapı ile gerçek zamanlı olarak oluşturulur ve izlenir. Tüm dünyadan güvenlik analistleri, GReAT ekibimizden dünyaca ünlü güvenlik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



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

APT İstihbarat Raporları

Gelişmiş Kalıcı Tehditler ile ilgili tüm bulgular anında bildirilmez hatta bazıları hiçbir zaman halka duyurulmaz. En yeni araştırmalarımızın yanı sıra APT'ler hakkında özel, kapsamlı ve eyleme geçirilebilir raporlarımızı ilk siz okuyun.



Şekil 6:
Kaspersky Lab tarafından bulunan APT'ler

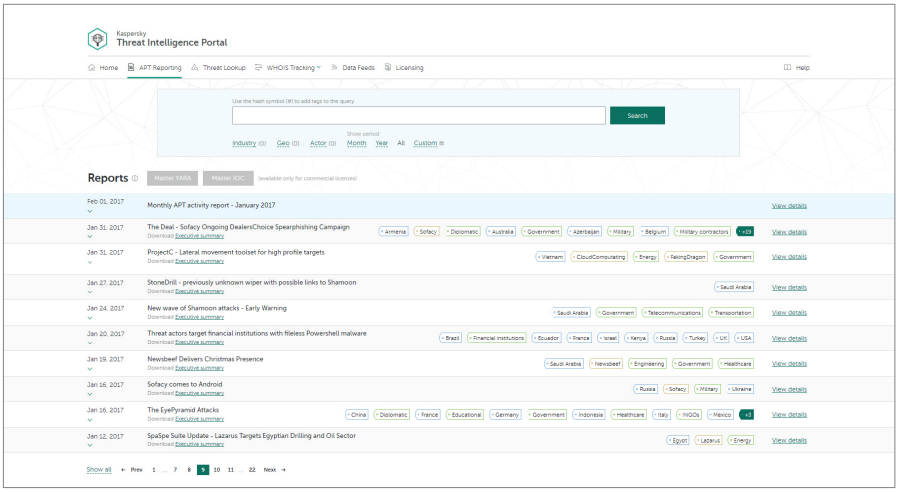
Hizmetin öne çıkan özellikleri

- Devam eden araştırma sırasında, basına sunulmadan önce en yeni tehditler hakkında teknik açıklamalara özel erişim. 2017 yılında 100'ün üzerinde APT raporu yayınlanmıştır.
- 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.
- OpenIOC formatında kullanılabilen Risk Göstergeleri'nin (IOC) kapsamlı bir listesini içeren ayrıntılı destek için 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).
- Geçmişe yönelik analiz: abonelik döneminiz boyunca size sunulmuş olan özel raporlara erişim olanağı.

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. 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.

Pratik bir açıdan bakıldığında Risk Göstergeleri SOC uzmanları için raporun en eyleme geçirebilir kısmını oluşturur. Bu yapısal bilgiler, daha sonra bulaşma belirtileri için altyapınızı kontrol etmenize yardımcı olacak belirli otomatik araçlarla birlikte kullanım için sunulur.

Tüm raporlara web arayüzü veya RESTful API aracılığıyla ulaşılabilir.



Şekil 7:
APT İstihbarat Raporları

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 (müşteriye özgü raporlar için) ve tercih edilen veri formatları bir kez seçildikten sonra herhangi ek bir altyapıya gerek yoktur.

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

Ülkeye Özel Tehdit Raporlama

Bir ülkenin siber güvenliği, o ülkenin tüm büyük kurum ve kuruşlarını korumaktan geçer. Hükumet 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 hükumet 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.

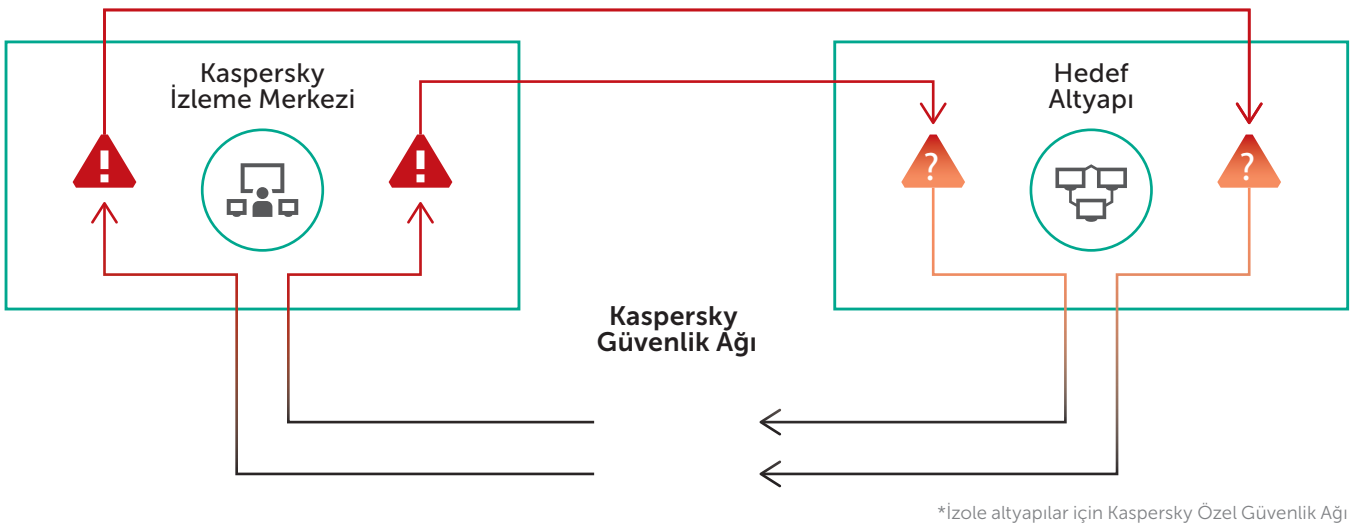
Hizmetin sonunda, ayrıntılı teknik analiz sonuçları hakkında ek bilgilerin yanı sıra farklı devlet endüstrileri ve kurumları için önemli tehditlerin açıklamasını içeren bir rapor sunulur. Raporlar şifreli e-posta mesajları aracılığıyla iletilir.

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

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 avantajları



*İzole altyapılar için Kaspersky Özel Güvenlik Ağı

Şekil 8:
Kaspersky Managed Protection

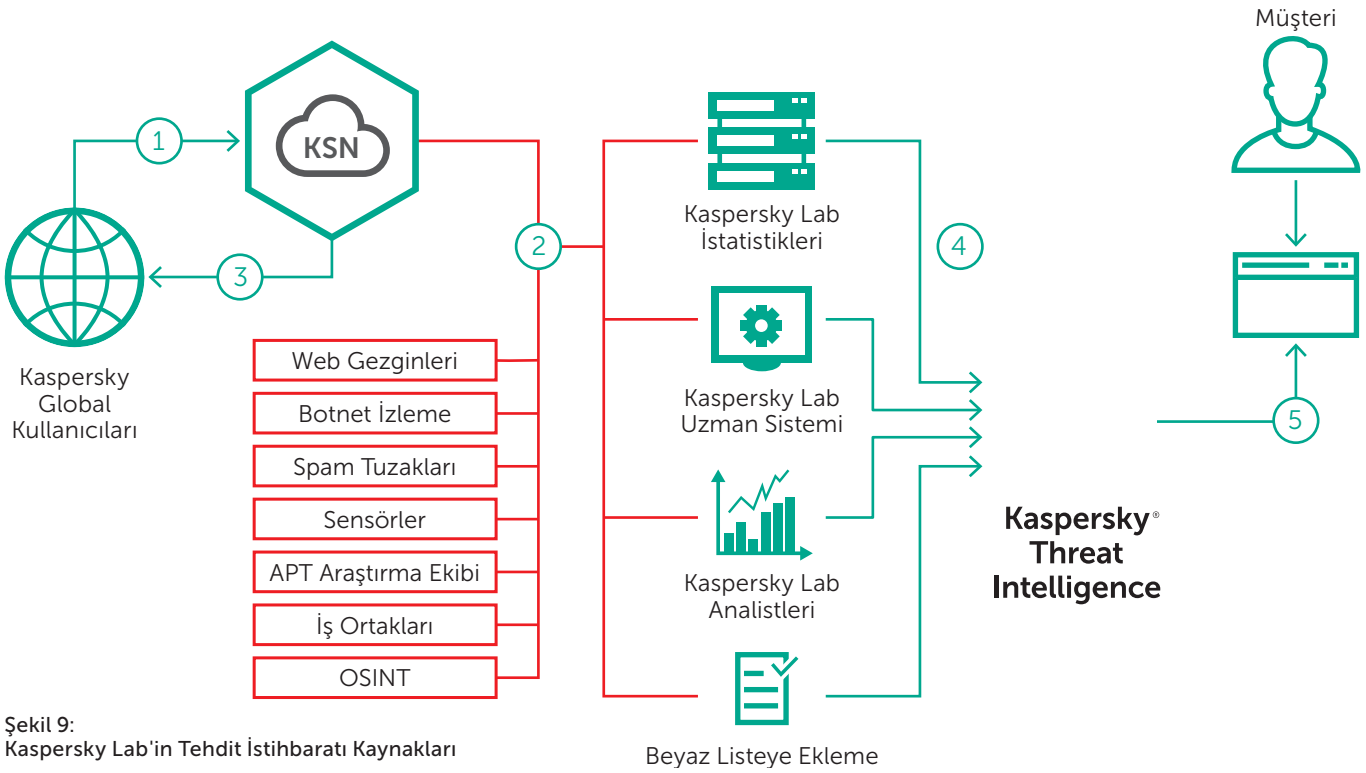
Hizmetin öne çıkan özellikleri

- 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.
- 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.

Kaspersky Tehdit İstihbaratı kaynakları hakkında daha fazla bilgi

Tehdit İstihbaratı birleşik, heterojen ve son derece güvenilir kaynaklardan toplanır. Bu kaynaklara; Kaspersky Security Network (KSN), kendi web gezginlerimiz, Botnet İzleme hizmetimiz (botnetlerin, hedeflerinin ve faaliyetlerinin 7 gün 24 saat 365 gün izlenmesi), spam tuzakları, araştırma ekipleri, iş ortakları ve Kaspersky Lab tarafından 20 yıldan uzun bir süredir toplanan kötü amaçlı nesnelerle ilgili geçmişe ait diğer veriler dahildir. 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) analist doğrulaması ve beyaz liste onayı gibi birçok ön işleme tekniği kullanılır.

Uygun becerilere ve eğitime sahip Çalışanlar ve güvenilir kaynaklardan toplanan ve mevcut güvenlik kontrollerine uygulanan Tehdit İstihbaratı ile birlikte artık Olay Yanıtı'nızı düşünmeye başlayabilirsiniz.



Şekil 9:
Kaspersky Lab'in Tehdit İstihbaratı Kaynakları

Olay yanıtı çerçevesi

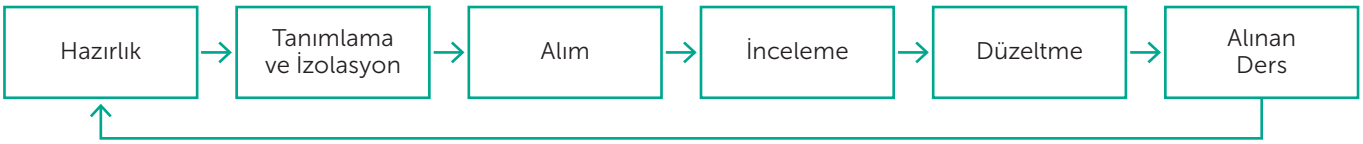
Adli bilişim ve olay yanıtı, kısa süre içinde veya anında önemli iç kaynaklar arasında görev paylaşımı yapılmasını gerektirir. Siber tehditlerle mücadele konusunda kapsamlı pratik deneyimlere sahip olan bilgili uzmanlar, kötü amaçlı etkinliği tanımlama, izole etme ve engelleme konusunda çok hızlı hareket etmelidir. Sonuçların ve onarım masraflarının en aza indirilmesi için hız, hayati önem taşır.

Bu kadar kısa süre içinde bu düzeyde bir uzmanlıkla hareket etmek, iyi yapılandırılmış SOC Ekipleri için bile zorlayıcı olabilir. Çok az şirket, hareket halindeki gelişmiş bir saldırıyı durdurabilecek kurum içi kaynağa sahiptir. Ayrıca, ilgili APT aktörlerinin kullandığı belirli yaklaşımlar ve taktikler konusunda SOC Ekibi'nin yeterli uzman bilgisine sahip olmadığı devlet destekli karmaşık tehditler veya APT'ler gibi vakalarla karşılaşılabilir.

Bu gibi durumlarda hızlı ve bilinçli bir yanıt verebilmek için hazır olan üçüncü taraf Olay Yanıtı tedarikçisi veya danışmanı ile birlikte çalışmak daha uygun maliyetli ve verimli olabilir.

Kapsamlı bir Olay Yanıtı Çerçevesi aşağıdakileri içermelidir:

- **Olayın Tanımlanması**
  İlk olay analizi ve etkilenen sistemlerin izole edilmesi
- **Kanıt toplama**
  Gerekli kanıtların toplanması için olayın türüne bağlı olarak farklı kaynakların incelenmesi gerekir
- **Adli Bilişim Analizi (gerekirse)**
  Bu aşamada olayla ilgili ayrıntılı bir tablo oluşturulabilir
- **Kötü Amaçlı Yazılım Analizi (gerekirse)**
  İlgili kötü amaçlı yazılımların özellikleri anlaşılabilir
- **Onarım Planı**
  Hem sorunun kök nedenini hem de kötü amaçlı kodun tüm izlerini ortadan kaldırmak için bir plan geliştirilir
- **Alınan dersler**
  Benzer olayları önlemek için mevcut güvenlik kontrollerinin incelenmesi ve güncellenmesi



Olay yanıt sistemi

Şekil 10:
Olay Yanıtı Çerçevesi

Kaspersky Lab şunları sunar: Olay Yanıtı Hizmetleri

Olay Yanıtı Hizmetleri, kanıtların yerinde toplanmasından ek risk göstergelerinin tanımlanmasına, onarım planı hazırlanmasına ve tehdidi kurumunuzdan tamamen kaldırmaya kadar tüm olay soruşturma döngüsünü kapsayan özel bir hizmettir. Kaspersky Lab'in soruşturmaları, son derece deneyimli Siber Saldırı Tespit Analistleri ve Araştırmacıları tarafından yürütülür. Global uzmanlığımız sayesinde güvenlik olayınızın çözümü için Adli Bilişim ve Kötü Amaçlı Yazılım Analizi kullanılabilir.

Bu hizmet sırasında aşağıdaki hedeflere ulaşılır:

- 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.
- Uygulayabileceğiniz onarım 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.

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. Müşteri, ne kadar çalışma saati gerektiğini düşünüyorsa o kadar saat ekleyebilir veya uzmanlarımızın her vaka için özel olarak tasarladığı tavsiyelere uyabilir.

Neden Kaspersky Lab?

Çünkü şu özelliklere sahibiz:

- Interpol ve Bilgisayar Acil Durum Müdahale Ekipleri gibi global emniyet teşkilatları ile iş ortaklıkları
- Dünya genelinde gerçek zamanlı olarak milyonlarca siber tehdidi izlediğimiz bulut tabanlı araçlar
- Her türlü internet tehdidini analiz edebilen ve anlayabilen global ekipler

Çünkü şu özelliklere sahibiz:

- Dünyanın en büyük Tehdit İstihbaratı ve teknoloji liderliğine odaklanmış bağımsız güvenlik yazılımı şirketiyiz
- Diğer tüm satıcılara kıyasla daha çok bağımsız kötü amaçlı yazılım tespiti testinde tartışmasız liderlik kazandık
- Gartner, Forrester ve IDC tarafından Lider seçildik.

Kaspersky Lab Hakkında

Kaspersky Lab, dünyada uç nokta koruma çözümü tedarik eden en büyük özel şirkettir. Şirket, uç nokta kullanıcıları için güvenlik çözümleri sağlayan en büyük dört şirketin arasında yer alır. Kaspersky Lab, 19 yıllık tarihi boyunca BT güvenliği sektöründe her zaman yenilikçi bir şirket olmuştur ve büyük şirketler, SMB'ler ve tüketiciler için etkili dijital güvenlik çözümleri sağlamaktadır. Holding şirketi Birleşik Krallık'ta tescilli olan Kaspersky Lab, dünya genelinde yaklaşık 200 ülke ve bölgede faaliyet göstermekte ve dünya çapında 350 milyondan fazla kullanıcı için koruma sağlamaktadır.

Uyarı.

Bu belge, halka açık değildir ve yalnızca tanıtım amaçlıdır.

Hizmetlerin kapsamı, belirli coğrafi bölgelerde kullanılabilirliğine göre değişiklik gösterebilir. Bu belgede tanımlanan bazı hizmetler, Kaspersky Lab ile ek anlaşma gerektirir.

Daha fazla bilgi için lütfen Kaspersky Lab'in bölge temsilcisine başvurun veya taleplerinizi şu adrese gönderin: intelligence@kaspersky.com.

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

© 2017 AO Kaspersky Lab. Tüm hakları saklıdır. Tescilli ticari markalar ve hizmet markaları ilgili sahiplerinin mülkiyetindedir.