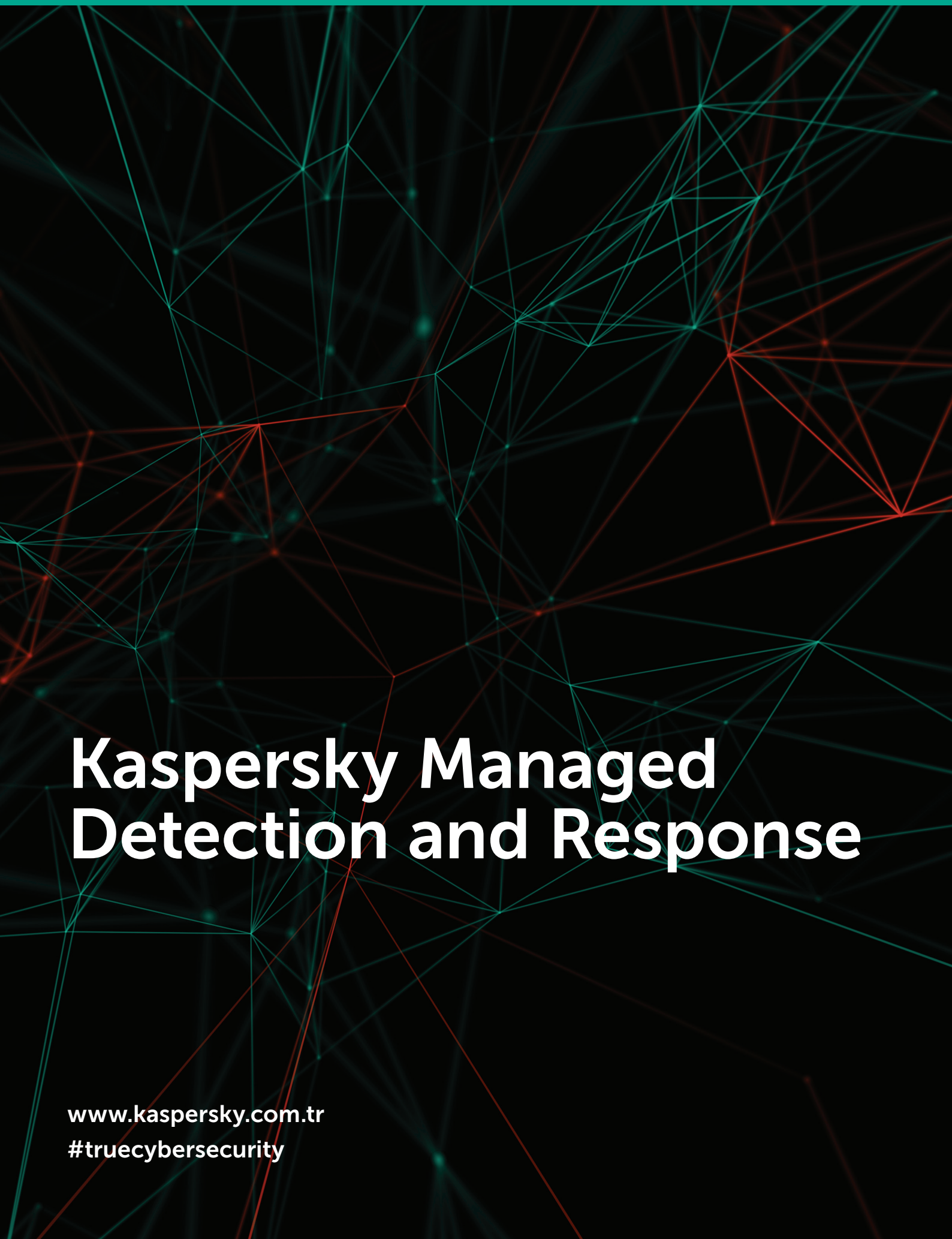
KASPERSKY lab



Kaspersky Managed Detection and Response

www.kaspersky.com.tr
#truecybersecurity

Kaspersky Managed Detection and Response

Problem Tanımı

Kurumsal süreçler geniş kapsamlı olarak otomasyona geçirildikçe işletmeler, bilgi teknolojilerine gitgide daha bağımlı hale gelir. Bu da, ana işletme süreçlerini aksatabilecek risklerin giderek BT alanına kayması demektir. Otomasyon araçlarını geliştirenler bunun farkındadır ve olası risklere cevap vermek amacıyla güvenilirlik, esneklik ve maliyet ile birlikte bir BT sistemin en önemli özelliklerinden biri olan BT güvenliğine gittikçe daha fazla yatırım yapmaktadır. Geçtiğimiz yıllarda yazılım ürünlerinin güvenliğinde çarpıcı gelişmeler yaşanmıştır. Neredeyse tüm küresel yazılım üreticileri artık güvenlik yapılandırmalarına ve ürünlerinin güvenli kullanımına dair belgeler yayınlarken, bilgi güvenliği pazarı farklı biçimlerde güvenlik sağlayacak tekliflerle dolup taşmaktadır.

Diğer yandan, bir şirketin işleri ne kadar BT'ye bağımlı ise şirketin bilgi sistemlerine sızma fikri de o kadar çekici hale gelir. Yazılım güvenlik düzeylerinde yukarıda bahsedilen artış, sızma saldırılarının başarılı olabilmesi için daha fazla kaynak gerekmesine sebep olmuştur.

Başarılı bir saldırı için gereken minimum maliyetin artması, saldırganların çoklu koruma katmanlarının üstesinden gelebilmek için hedef altyapıda uzun süreli varlık sağlama ve yatırımlarından maksimum geri dönüş elde etme mecburiyetiyle birleşince, hedefli saldırıların ortaya çıkmasına sebep olmuştur. Hedefli saldırılar dikkatle planlanır ve uygulanır; otomatik araçların yanı sıra, görevleri sızma testi ekiplerinin yaptığı işe benzeyen profesyonel saldırganların doğrudan ve derinlemesine müdahalesini de gerektirir. Bu profesyonel saldırganlarla mücadele etmek, bilgisayar saldırılarını tespit etmek ve önlemek için en son araçlarla donatılmış, en az onlar kadar nitelikli profesyonelleri gerektirir.

Profesyonel yayınlarda sık sık, hasar maliyetinin, korunan bilgi varlıklarının değerini aşması durumunda, bir kuruluşun güvenlik hedeflerine ulaşmış sayılacağı teorisi ileri sürülür. Ancak bu önerme, CIA ve NSA'in siber silahları hakkındaki son yayınlar ışığında ciddi anlamda yeniden ele alınmalıdır. Uygulamalar, siber silah geliştiricilerinin, buluşlarını pek de gizli tutmaya çalışmadıklarını göstermiştir. Bu durum, söz konusu buluşların çok daha mütevazı araştırma kaynaklarına sahip potansiyel tehdit unsurlarının eline geçebilme olasılığı olduğu anlamına gelir. İstihbarat servislerinin sahip olduğu kaynakların sınırsız olduğu düşünüldüğünde, bunlara ait buluşları kullanma olasılığının sızma maliyetlerini çarpıcı biçimde düşüreceği aşikardır. Böyle tehdit unsurlarıyla mücadele etmenin tek yolu, koruma için sistematik bir yaklaşım benimsemektir. Bu yaklaşım, tehdidi önlemek mümkün değilse, hızla tespit etmek; tespit etmek mümkün değilse, etkili bir karşılığa ve saldırıdan doğacak hasarı hafifletecek iyileştirme becerilerine sahip olmak gerektiğine işaret eder. Bu saldırıların çeşitli aşamalarda, çeşitli vektörler aracılığıyla, çeşitli ortamlarda, çok çeşitli taktikler, prosedürler ve teknolojiler kullanarak gerçekleştirilebileceği düşünüldüğünde bu korumanın önemi daha da artar.

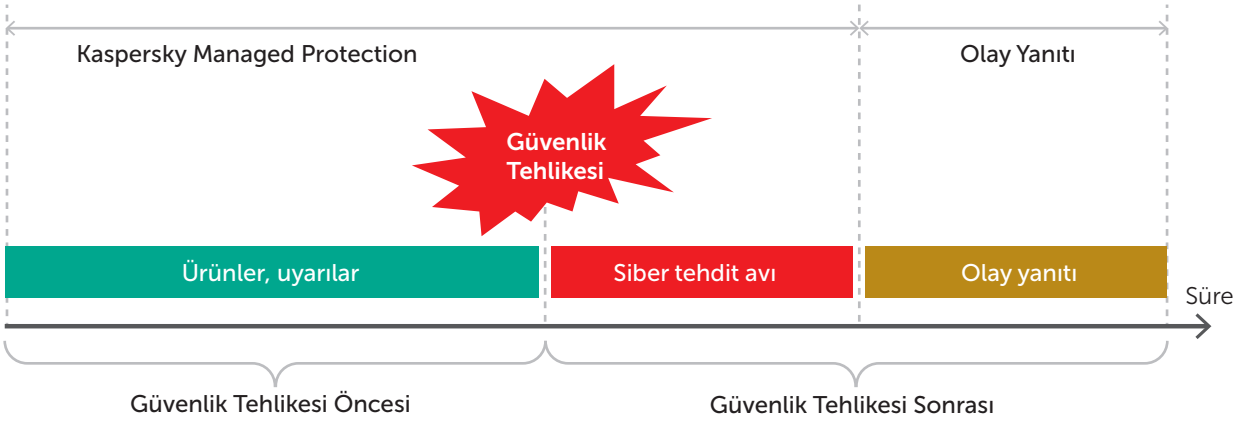
Kaspersky Managed Protection and Incident Response

Kaspersky Lab, 20 yılı aşkın süredir bilgisayar saldırılarını araştırmakta ve önlemektedir. Büyük veri ve makine öğrenimi üzerine yapılan son araştırmalar dahil, yıllar içerisinde geliştirdiğimiz tehdit tespiti ve önleme teknolojilerimiz sayesinde, Kaspersky Lab güvenlik ürünlerinin otomatik modda tespit edilebilen ve etkisiz hale getirilebilen tüm saldırıları durdurabileceğini güvenle söyleyebiliriz.

Öte yandan, hedefli saldırılar, kurbanların kullandığı koruma araçlarını dikkate aldığı ve saldırılar buna yönelik olarak geliştirildiği için otomatik tespit ve önleme sistemlerini atlatabilir. Bu tür saldırılar çoğunlukla yazılım kullanmadan gerçekleştirilir ve saldırganların eylemleri, BT ya da bilgi güvenliği çalışanlarının eylemlerinden güçlükle ayırt edilebilir. Günümüz saldırılarında kullanılan tekniklerden bazıları şunlardır:

- adli bilişimi engelleyecek araçların kullanımı, örneğin, delilleri sabit disk üzerinden güvenle silmek ya da saldırıyı yalnızca bir bilgisayarın belleği içerisinde gerçekleştirmek;
- BT ve bilgi güvenliği departmanlarının rutin olarak kullandığı, yasal araçların kullanımı;
- önceki adıma dair izlerin güvenle silindiği çok aşamalı saldırılar;
- profesyonel bir ekip tarafından gerçekleştirilen interaktif çalışma (sızma testi sırasında kullanılana benzer şekilde).

Bu tür bir saldırı ancak hedef varlık hasar aldığında tespit edilebilir; çünkü, ancak o zaman kötü amaçlı etkinliğe işaret eden şüpheli hareket tespit edilebilir. İlk güvenlik ihlali gerçekleştikten sonra, saldırıları tespit etmek için siber tehdit avlama adı verilen bir yaklaşım kullanılır. Bu yaklaşımın kilit unsuru, karar almanın son aşamasına profesyonel bir analistin de katılmasıdır. Olay analizi zincirinde bir insanın bulunması, otomatik tehdit tespit mantığının zayıflıklarını telafi etmeye yardımcı olur. Ayrıca sızma testine benzer saldırılarda saldıran tarafta bir insan bulunması durumunda, bu insan otomatik teknolojileri atlatmak konusunda şüphesiz daha avantajlı konumdadır. Bu yüzden, böyle saldırılara karşı koymanın tek yolu, analist bir insanın varlığıdır. Ne otomatik tehdit tespit ve önleme araçları ne de siber tehdit avlama tek başına tüm modern tehditlerle başa çıkabilir. Ancak hasar öncesinde geleneksel tespit ve önleme araçlarının aktif olması ve hasar sonrasında otomatik araçlar tarafından fark edilmeyen yeni tehditlerin tekrar tekrar aranması sürecinin bir birleşimi, etkili olabilir.



Kaspersky Managed Protection (KMP), birden fazla otomatik tespit teknolojisini profesyonel analistlerin becerileriyle destekleyerek en son siber tehdit avlama yaklaşımlarını kullanır ve Kaspersky Lab ürünlerinin genel tehdit tespit kalitesini arttırır. KMP'nin en önemli avantajı, aşağıdaki gibi otomatik tespit ve önleme araçlarının gözden kaçırabileceği saldırıları tespit etmesidir:

- ürünlerin otomatik modda tespit edemediği yeni kötü amaçlı yazılımların tespiti; • eylemleri, otomatik mantık tespit eşiğinin altında olan, tekrarlı saldırıların tespiti;
- kötü amaçlı yazılım kullanılmadan yapılan saldırıların tespiti;
- eylemleri, yalnızca RAM bellekte gerçekleştirilen dosyasız kötü amaçlı yazılımların tespiti;
- profesyonel saldırganlar tarafından gerçekleştirilen sızma testi benzeri saldırıların tespiti.

KMP, tehdit tespitinin yanında aşağıdaki faydaları da sunar:

- saldırganların incelemeyi engelleyecek teknikler (güvenli silme araçları, çoklu aşamalar, vb.) kullanması durumunda saldırı aşamaları dizisini yeniden oluşturabilme;
- saldırılar müşterilerin BT altyapı analizlerinin bir parçası olarak tespit edildiği için müşterilere %100 uygunluk;
- teknik olarak uygulanabilir durumlarda, Kaspersky Lab önleme ürünlerinin yanında (Kaspersky Endpoint Security, Kaspersky Security for Mail Gateway, vb.) gerçek zamanlı koruma ve ardından işlemin etkili olduğundan emin olmak için gerçekleştirilen denetim özelliği sunulabilir.

Bununla birlikte, bütün saldırılar yalnızca otomatik bir koruma aracına etkisiz hale getirme bileşenlerin eklenmesiyle durdurulamayabilir: Saldırgan tespit edildiğini anlarsa, araçlarını ve taktiklerini değiştirecek, bir analist tarafından siber tehdit avlama çerçevesinde tekrar tespit edilene kadar gözden kaybolacaktır. Bu döngüyü tekrar edip durmak elbette problemi çözmenin etkili bir yolu değildir. Dolayısıyla bu noktada devreye, yeni kötü amaçlı yazılım örneklerini ve adli bilişimi içeren ilave Olay Yanıtlama hizmeti girer.

Olay Yanıtlama hizmetinin bir parçası olarak, her bir güvenlik olayı derinlemesine analiz edilir. Bu sayede yeni ve daha etkili saldırıyla başa çıkma prosedürleri geliştirilir ve gelecekte benzeri saldırıları engelleyecek önlemler alınır.

KMP ve Olay Yanıtlama hizmetleri birbirini tamamlar; çünkü olay inceleme prosedürleri sayesinde, koruma hizmetinin otomatik tespitiyle sağlanandan daha etkili bir karşılık belirlenebilir. Aynı zamanda, tüm incelemeler, olayların Kaspersky Managed Protection çerçevesi içerisinde analiz edilmesiyle ortaya konabilecek bulgulara ihtiyaç duyar.

Aralarındaki yakın ilişkiye ve entegrasyonun faydalarına rağmen, Kaspersky Managed Protection ve Olay Yanıtlama, Kaspersky Lab hizmetleri portföyünde iki ayrı hizmet olarak uygulanır. Böylelikle müşteriye hangisinin ihtiyaçlarına daha uygun olacağını seçme esnekliği sunulur.

Hedefli Saldırıları Araştırma Konusunda Benzersiz Bir Deneyim

Kaspersky Lab, dünya çapında Duqu, Project Sauron, Lambert, Equation ve daha birçok gelişmiş hedefli saldırıyı tespit eden ve bu saldırılara karşı koruma araçları sağlayan uzmanları sayesinde etkili hedefli saldırı araştırmalarında başarılı bir geçmişe sahiptir. En ünlü kötü amaçlı saldırıların kronolojisi için:
https://apt.securelist.com/#!/threats/.

www.kaspersky.com.tr

#truecybersecurity