IDC Teknoloji Bülteni

Sponsor: **Kaspersky**

Yazarlar:

Mark Child

Yeşim Araç Öztürk

Ağustos 2020

Entegre Siber Güvenlik Zorlu Bir Ortamda Verimlilik ve Etkinlik Sağlıyor

Entegre Güvenlik Eksikliği Kurumları Riske Atıyor

IDC'nin gerçekleştirdiği araştırmaya göre, dünya genelindeki kurumların çoğu (%75'i), güvenlik ortamlarındaki entegrasyon eksikliği yüzünden güvenlik ekiplerinin vaktinin boşa harcandığını kabul ediyor.

Kurumlar halihazırda güvenlikle ilgili iki büyük zorlukla başa çıkmaya çalışıyor:

- Tehdit ve saldırı hacminin büyümesiyle kendini gösteren yoğun ve çok yönlü tehdit ortamı; dark web'de birçok araca ve veriye erişilebilmesiyle, hacimli saldırıların (DDoS gibi) daha sinsi saldırılarla birlikte kullanılmasıyla ve yüksek motivasyonlu siber suç çeteleri ile ulus devletlerden gelen sofistike saldırılar.
- Aynı zamanda profesyonel güvenlik uzmanları alanında küresel bir kaynak yetersizliğinden de söz edilebilir. IDC'nin Dünya Genelinde Teknoloji İşe Alım Etkisi Kılavuzu 2018H2, 2018'den 2023'e kadar %9,6'sı güvenlik uzmanı olan, özel BT becerilerine sahip 10,5 milyon tam zamanlı çalışana ihtiyaç duyulacağını ön görüyor. (ISC)[2] tarafından yayınlanan yeni bir çalışmaya göre, 2019 yılında dünya genelinde 4 milyondan fazla doldurulmamış güvenlik pozisyonu bulunuyordu. Aynı zamanda, IDC'nin 2020 CIO Anketi, kurumların %37'si için en büyük tehdidin güvenlik uzmanlığı eksikliği olduğunu ortaya koydu.

Güvenlik ekipleri, ellerindeki araçlarla verimli ve etkili bir şekilde çalışabilmelidir. Aksi takdirde kurumlar hem operasyonlarını, iş stratejilerini ve itibarlarını etkileyebilecek hem de ceza almalarına yol açabilecek siber saldırılara maruz kalabilir.

Tüm bu faktörler, güvenlik ekiplerinin ellerindeki araçlarla verimli ve etkili biçimde çalışabilmesini en önemli unsurlardan biri haline getiriyor. Aksi takdirde kurumlar, hem operasyonlarını, iş stratejilerini ve itibarlarını etkileyebilecek hem de ceza almalarına yol açabilecek ciddi ve artan siber saldırılara maruz kalabilir.

Buna karşın etkili güvenlik operasyonları ortaya koyabilmek, gelişmenin önündeki büyük engellerden biri olmaya devam ediyor. IDC Orta Doğu, Türkiye ve Afrika CIO Anketine göre, katılımcıların %13'ü, güvenlik programlarına en büyük tehdidi entegrasyon eksikliğinin oluşturduğunu belirtiyor. Güney Afrika'daki kurumların %28'i ve Türkiye'deki kurumların %20'si, güvenlik ürünleri arasındaki entegrasyon eksikliğinden kaynaklanan sorunlar yaşandığını ifade ediyor.

Manuel soruşturma ve analiz işlemleri ve güvenlik olayı önceliklendirmesi sırasında entegre olmayan sistemler arasında geçiş yapmak ciddi anlamda vakit kaybettirebilir. Bu nedenle, güvenlik portföyünün rasyonel ve entegre hale getirilmesi, harcanan adam/gün saat verimliliği ve olaylara müdahale süreleri açısından kuruma ciddi faydalar sağlayabilir. Daha yüksek entegrasyon, olay

müdahalesi süreçlerinin daha fazla otomatize edilmesine izin verdiği için, analistlerin farklı sistemlerden verileri birbiriyle ilişkilendirdikleri sırada ortaya çıkabilecek potansiyel hataları da azaltıyor. IDC'nin 2019 CIO BT Türkiye Anketi'ne göre kurumlar, BT güvenliği hizmetleri bütçelerinin %29'unu BT Güvenliği sistemi entegrasyonuna ayırıyor.

Kurum içinde kullanılan farklı araç ve çözümleri aynı anda yönetme yükünü çalışanların üzerinden almak, çalışanların derinlemesine olay analizi ve adli bilişim ya da daha ciddi vakaların araştırılması gibi daha yüksek değere sahip görevlere zaman ayırabilmesini sağlar. Otomasyonun artırılması aynı zamanda gündelik işleri yönetmekten kaynaklanan alarm yorgunluğunu ve analist yorgunluğunu da azaltır. Genel olarak, entegrasyon ve otomasyonla sağlanan gelişmiş verimlilik ve etkinlik, güvenlik ekibinin yalnızca gündelik operasyonları sürdürmesine değil, daha stratejik hareket etmesine de izin verir.

Kurumlar, daha etkili müdahale ve daha hızlı harekete geçme gibi avantajlar da elde eder. Farklı güvenlik araçları ve işlevleri arasında görüş ve tehdit istihbaratı paylaşımı, kurumun genel siber dayanıklılığını artırır.

Uç Nokta Güvenliği, Güvenlik Tutumunda Kilit Önem Taşıyor

Orta Doğu, Türkiye ve Afrika güvenlik pazarında en büyük payı %41,9'la uç nokta güvenlik yatırımları oluşturuyor. Uç nokta güvenliği pazarının, önümüzdeki beş yıl içerisinde yıllık %6,2'lik bileşik büyüme oranında büyümesi öngörülüyor.

Uç nokta cihazlar, özellikle yalnızca dijital dönüşüm sonucu değil, aynı zamanda COVID-19'un getirdiği evden çalışma zorunluğuyla ortaya çıkan çevre-sonrası dönemde, kurumsal ağlara erişmeye çalışan siber suçluların birincil hedefidir. Daha basitçe söylemek gerekirse IDC uç noktaları, çevre-sonrası dönemde korumada kilit birer kontrol noktası olarak görüyor.

Geleneksel imza tabanlı tespit yöntemleri, bazı eleştirilere rağmen geniş hacimli dosyaları taramak ve bilinen tehditleri engellemek için verimli bir yol sunar. Ancak imza tabanlı koruma tek başına işe yaramaz. İmzalı korumaların; eksiksiz koruma sağlamak için entegre bir uç nokra koruma platformu (EPP) içerisinde imzasız tespitle güçlendirilmesi gerekir: Yani ticari kötü amaçlı yazılımlara karşı imza tabanlı koruma ve tespitten kaçabilecek yeni, bilinmeyen ve karmaşık tehditlere karşı imzasız koruma sağlamak için gereklidir.

Koruma becerilerini artırarak gelişmiş tehditleri ve hedefli saldırıları tespit etmek amacıyla uç nokta tespit ve müdahale (EDR) çözümlerine de pazarda ilgi artıyor. EDR, profesyonel güvenlik uzmanlarını geçmiş log tabanlı ya da alarm tabanlı SIEM merkezli olmayan yeni bir adli bilişim araçlarıyla donattı. EDR, profesyonel güvenlik uzmanlarına bulunması zor kötü amaçlı yazılımları tespit edebilmeleri için birçok uzaktan ölçüm aracı sağladı.

Uç nokta koruması için entegre, çok katmanlı bir yaklaşım benimsemek, dayanıklı bir güvenlik programı oluşturmak için olmazsa olmazdır. Bu da EPP (reaktif), EDR (proaktif) ve tehdit istihbaratının (TI) (hem önleyici hem proaktif olabilir) sıkı sıkıya bağlı olmasını gerektirir. EPP için istisna, uç noktaları bağımsız bir çözüm olarak korumasıdır. Daha önce de belirttiğimiz gibi, EPP korur; EDR ise yalnızca uç nokta

aktiviteleriyle ve uzaktan ölçümle tespit edilemeyen kötü amaçlı girişimlere platformlar arası görünürlük, müdahale ve engelleme imkanı sağlayan artırılmış adli bilişim sunar. Eksiksiz bir güvenlik programı için her iki bileşen de önemlidir.

Tehdit istihbaratı, bir kurumun güvenlik tutumunu ciddi şekilde geliştirebilir. Önleyici açıdan bakarsak TI, uzun süredir bilinen tehditleri kara listeye almak için kullanılıyor. Daha proaktif bir açıdan ise TI verileri ve raporları, tehdit avlamayı sağlıyor; incelemeler sırasında daha kapsamlı bir bağlam sunuyor ve riski azaltmaya yardımcı olabiliyor. TI'ın sağladığı ekstra bağlam, uç nokta güvenliği açısından güvenlik kontrollerine rehberlik ederek çözümün etkinliğini artırabilir.

EDR'ın Dezavantajları

EPP'nin taşıdığı kritik rolü asla unutmayın. EDR çok büyük bir gelişmedir. Ancak yetersiz kaldığı iki önemli alan bulunuyor:

- EDR, aracı yönetmesi için bir insana ihtiyaç duyuyor. Profesyonel güvenlik uzmanlarının ise sayısı az, zamanları ise çok kıymetlidir. Bunun sonucunda EDR'a ve kullanılabilirliğine yönelik beklenti katlanarak artıyor. EDR araçlarının daha kolay kullanılabilmesi, uyarıların zararlı mı zararsız mı olduğuna dair hızlı karar verebilmesi ve profesyonel güvenlik uzmanlarının geleneksel yöntemlere kıyasla daha üst düzeyde performans gösterebilmesi için rehberlik sağlayabilmesi gerekiyor. Kısacası, profesyonel güvenlik uzmanlarını hem daha verimli hem de daha etkili hale getirmek için EDR araçlarının gelişmesi gerekiyor.
- EDR'ın ikinci zayıf noktası ise "fidye yazılımı etkisi"dir. Evet, "fidye yazılımı" diyerek durumu fazla basitleştirmiş olmak mümkün ancak kötü amaçlı yazılım saldırıları saniyeler, hatta saliseler içinde gerçekleşebiliyor. Asıl konu, sızıntı tespitinde sürenin öneminin dramatik bir biçimde artmasıdır. Manuel bir araç, dakikalar, saniyeler, hatta saliseler içinde gerçekleşen bir saldırıya yeterince hızlı biçimde müdahale edemeyeceği için fidye yazılımı tespitinde EDR'a güvenmek mantıklı değildir. Bir fidye yazılımı senaryosunda 200 ila 500 milisaniyelik bir gidiş-geliş süresi bile zarar verebileceği için, otomatik bulut tabanlı analiz kullanan çözümler bile yeterince hızlı sayılmaz. Bu nedenle, EDR ile belirlemeye çalıştığımız bazı vakalara müdahaleyi EPP'den beklemeliyiz.

Fidye yazılımları çağında EDR'ın EPP'ye değer katabilmesi için EDR araçlarının şunları yapabilmesi gerekir:

1. Yalnızca uç noktada uzaktan ölçüm yaparak tespit edilemeyen kötü amaçlı yazılımları bulabilmelidir.
2. EPP tarafından durdurulmadan önce kötü amaçlı yazılımın diğer güvenlik katmanlarından nasıl geçtiğini ortaya çıkaracak adli bilişim verileri sağlamalıdır.

Her iki kullanım senaryosu da benzer noktalara işaret eder: EDR'nin kullandığı veri, yalnızca uç noktadan gelmemelidir. Uzaktan ölçüm, ağdan, mesajlaşmalardan, internetten ve diğer güvenlik önlemlerinden sağlanmalıdır. Güvenlik sağlayıcıları bu genişlemeye "XDR" adını veriyor; burada "X", "katmanlar arası" olmayı temsil ediyor.

EDR, görüş alanını uç noktanın ilk sınırlarının ötesine genişlettiğinde değer yaratır. EDR'ın "kaderi", yalnızca uç nokta aktiviteleri ve uzaktan ölçümle tespit edilemeyen kötü amaçlı aktiviteleri durduran, platformlar arası görünürlük ve müdahale sağlayan bir araç olmaktır.

Örneğin, PowerShell betikleri her zaman kötü amaçlı değildir. Ancak, PowerShell, bir Word dosyasına gömülü bir makrodan başlatılıyorsa ve bu Word dosyası yeni gelen bir e-postada bulunuyorsa betiğin kötü amaçlı olma olasılığı yüksektir. Bu örnek, basit olmakla birlikte oldukça gerçekçidir. Müdahale ise bireysel uç noktayı tecrit etmenin ötesine geçer. Güvenlik analisti, benzer dosyalar olup olmadığını görmek için tüm e-posta hesaplarını tarayabilmeli, komuta ve kontrol (C&C) IP adresleriyle iletişimi engelleyebilmeli, güvenlik duvarı kurallarını güncelleyebilmeli ve şifre sıfırlamayı zorunlu tutabilmelidir. Hassas ortamlarda aynı e-postayı alan diğer bireyleri değerlendirmek, adli bilişim alanında özel bilgiler sağlayabilir.

EDR'ı değerlendirirken, EPP de aynı önemle ele alınmalıdır: EPP'den artan beklentiler, EPP'nin olası eksikliklerini telafi etmek için EDR kullanımının reddedilmesiyle sonuçlandı. Dolayısıyla EDR, ancak görüş alanını uç noktanın ilk sınırlarının ötesine genişlettiğinde değer yaratır. EDR'ın "kaderi", yalnızca uç nokta aktiviteleri ve uzaktan ölçümle tespit edilemeyen kötü amaçlı aktiviteleri durduran, platformlar arası görünürlük ve müdahale sağlayan bir araç olmaktır.

Aynı Çözüm Her Duruma Uymaz

Belirli bir düzeye kadar tüm şirketler tehditlere karşı koruma ve kurumun operasyon kabiliyetini güvence altına alma gibi belirli ihtiyaçlara sahip olsalar da, bir noktadan sonra ihtiyaçları ayrışır.

- Koruma ihtiyacı aynı kalmakla beraber, küçük veya orta ölçekli bir kurumun korumaya ayıracağı kaynaklar, çok uluslu bir kuruluşun kaynaklarıyla boy ölçüşemez.
- Güvenlik olgunluğu ciddi ölçüde farklılık gösterir.
- Kurum içerisindeki varlıklar da farklıdır ve bu varlıklar, risk tabanlı bir yaklaşım benimsenerek farklı şekilde ele alınmalıdır.

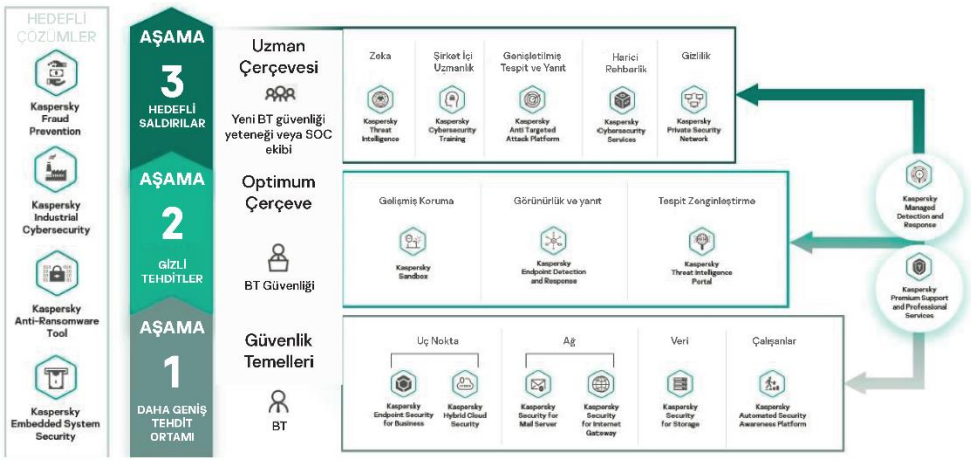
Güvenlik sağlayıcısı perspektifinden bakıldığında bu, çok çeşitli son kullanıcıların ihtiyaçlarını karşılayacak farklı düzeylerde koruma sağlayan, kapsamlı ve yapılandırılmış bir hizmet sunulması gerektiği anlamına gelir. Sunulan hizmetler:

- Heterojen bir altyapının güvenliğini sağlayabilecek yeterli kontrol ayrılığı sunabilmeli;
- Altyapıdaki ve operasyondaki genişleme veya dalgalanmalara göre ölçeklendirilebilmeli;
- Hibrit ortamlarda koruma sağlamalı;
- Altyapının ve süreçlerin tüm temel bileşenlerini kapsamalı (uç noktalar, ağ, mesajlaşma, internet, mobil, bulut ve operasyonel teknolojiler);
- Yukarıdakilerin hepsini sistemin veya kurum kaynaklarının üzerindeki yükü azaltarak yapmalı;
- Tüm bunlarla birlikte, birleşik ve entegre bir çözüm üzerinden yönetilebilmelidir.

Kaspersky'den Çok Katmanlı Bir Yaklaşım

Kaspersky'nin sunduğu hizmetlerin genişliği ve geniş bir yelpazede müşterilere uygun siber güvenlik çözümleri ve hizmetleri sunma deneyimi, hem ana akım pazarın hem de daha büyük, güvenlik açısından daha olgun müşterilerin ihtiyaçlarını karşılayabilecek entegre bir siber güvenlik yaklaşımı biçimlendirmesini sağladı.

Şekil 1
Kaspersky'nin Çok Aşamalı Siber Güvenlik Kavramsal Çerçevesi



Kaynak: Kaspersky

Security Foundations, Kaspersky'nin entegre güvenlik platformunun temelidir. Security Foundations, küçük büyük her türlü kurumun geniş çaplı tehdit ortamında kendisini koruyabilmek için ihtiyaç duyduğu temel unsurlardan meydana gelir. Üreticiye göre (dosyasız kötü amaçlı yazılımlar da dahil olmak üzere) bu tehditler, genel tehditlerin %90'ını oluşturuyor.

Örnek vermek gerekirse Kaspersky Security Foundations; Kaspersky Endpoint Security for Business (KESB), Kaspersky Secure Mail Gateway, Kaspersky Web Traffic Security ve Kaspersky Hybrid Cloud Security çözümlerini içeriyor. Bileşenlerin tamamı yukarıdaki Şekil 1'de görülebilir.

Kaspersky müşterileri, altyapılarının ve süreçlerinin güvenliğini sağlamak için hangi bileşenlere ve modüllere ihtiyaçları varsa bunları seçme olanağına sahip. Bütün modüller yerel entegrasyon avantajına sahip olduğu için müşteriler, ne kadar fazla kurulum yaparlarsa o kadar fazla avantajdan faydalanarak kurulumlarından hızla eksiksiz değer elde edebilir.

Security Foundations'ın en önemli avantajı, mümkün olan en yüksek sayıda tehditi (%90'ı) engellemeyi hedeflemesidir.

Bir sonraki tehdit kategorisi olan belirlenmesi zor tehditler, tüm tehditlerin yalnızca %9,9'unu oluşturur. Ancak bu karmaşık tehditler sıklıkla önleyici teknolojileri atlatabilir ve uzun vadede bir kuruma ciddi zararlar verebilir.

Bu tehditlerle baş etmek, daha proaktif ve sofistike araçları gerektirir; bu araçlar da piramitin bir üst seviyesi olan Kaspersky Optimum Framework'de yer alıyor. Kaspersky Optimum Framework; Kaspersky EDR, Korumalı Alan ve Tehdit İstihbaratı Portalı çözümlerini içeriyor. Yukarıda görüldüğü gibi, müşteriler bileşenleri ayrı ayrı dağıtabilirler. Bununla birlikte üretici, KESB ve EDR Optimum (orta ölçekli müşterilere yönelik EDR tayini) gibi hazır paketler de sunuyor.

Security Foundations ve Optimum Framework dağıtan ya da benimseyen kurumlar, siber tehditlerin büyük çoğunluğuna karşı koruma sağlamış olur ve kendilerini güvenlik olgunluğu spektrumunun yüksek tarafına yakın görebilirler. Bununla birlikte, %0,1'lik hedefli saldırılar hala kapsam dışı kalmaktadır. İşletmeler, SOC ekiplerinin Kaspersky Expert Framework'ün sağladığı elit korumayla desteklenmesine de tam bu noktada ihtiyaçlar duyarlar.

Bu ileri çözümün kapsamlı değerlendirmesi, bu raporun kapsamı dışındadır. Bu tamamlayıcı yayında daha fazla ayrıntı mevcuttur.[1]

Bütün müşteriler, isterse güvenlik ihtiyaçlarına doğrudan hitap eden spesifik modülleri seçebilir, isterlerse de hazır paketlerden faydalanabilirler. Yukarıda belirtildiği gibi, yerel entegrasyonlar tüm bileşenlerin sorunsuzca birlikte çalışmasını sağlayarak güvenlik ekibine birleşik bir platformla çalışmanın avantajını getirir. Öte yandan Kaspersky'nin siber güvenlik sistemlerini kurumların stratejik olarak planlayabileceği bir siber olgunluk spektrumu olarak gördüğünü de unutmamak gerekiyor. Kurumlar bu sayede zaman içerisinde ilave, entegre bileşenler ve hizmetler ekleyerek güvenlik tutumlarını daha gelişmiş hale getirebilirler. En temel iki sınıflandırma, Optimum Framework ve Expert Framework'tür.

Ana Akım Pazar için Kaspersky Optimum Framework

Optimum Framework, kendilerini gelişmiş tehditlere karşı koruması gereken fakat kısıtlı BT güvenliği becerilerine sahip kurumları hedef alır. Optimum Framework'un ana bileşenleri; KESB, Kaspersky Güvenli Alanı ve EDR Optimum'dur. Bunların hepsi tek bir konsoldan yönetilerek sunucular ve sanal makineler de dahil olmak üzere tüm uç noktalar için güvenlik sağlar. Kaspersky, kombine KESB ve Güvenli Alan kurulumunun iki önemli avantajı olduğunu söylüyor: Birincisi, dinamik tehdit emülasyonu kullanan Güvenli Alan, "uç noktalar arası" olay müdahalesi senaryolarını otomatikleştirebiliyor. İkincisi, BT güvenliği ekibinin eyleme geçmesini gerektirmiyor; bu da, daha az güvenlik kaynağına sahip şirketler için özellikle önemlidir.

EDR Optimum, EPP'nin üzerine ekstra bir koruma katmanı ekliyor. Risk Göstergesi taraması, özelleştirilmiş tehdit göstergeleri oluşturma olanağı, saldırı yayılma yolu görselleştirmesi gibi kök neden analizi araçları ve bazı otomatik müdahaleler ile tehdit sınırlandırma becerileri içeriyor.

Sağlayıcı, Kaspersky EDR'dan tam olarak faydalanabilecek kurum içi kaynaklara sahip olmayan kurumlar için bir MDR Optimum hizmeti de sunuyor. Bu hizmet, bu müşterilere siber olgunluğa sahip bir bilgi güvenliği yetisi sağlıyor ve hızlı, kullanıma hazır bir hizmet aracılığıyla hızla dağıtılabiliyor. Kaspersky'nin MDR hizmeti, ekibin yönettiği güvenlik verisi toplama ve analizi, vaka sınıflandırma ve soruşturma, olay alarmları ve müdahale rehberliği ile hem uç noktaları hem de ağ

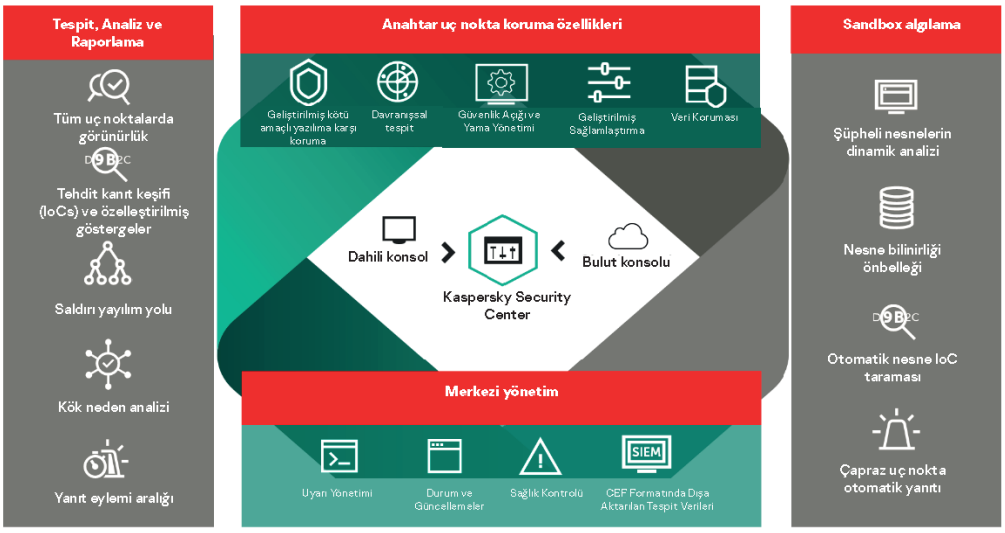
[1] IDC Teknoloji Bülteni: Modern Güvenlik Operasyon Merkezlerinin (SOC) Mücadelesi

güvenliğini kapsıyor. Şirket, müdahale ile ilgili olarak müşterilerinin ihtiyaçlarına uyacak esnek bir yaklaşım sunuyor: "Müdahale etmeme" seçeneği, müdahaleyi tamamen müşteriye bırakıyor; bir sonraki seviyede Kaspersky ekibi müdahale ile ilgili önerilerde bulunuyor; "eksiksiz hizmet" seçeneğinde ise olay müdahalesi tamamen Kaspersky ekibi tarafından gerçekleştiriliyor.

Aşağıda yer alan Şekil 2'de Kaspersky EPP, Sandbox ve EDR Optimum hizmetlerinin anahtar unsurlarının bir özetini görebilirsiniz:

Şekil 2

Kaspersky Optimum Framework Araçları ve Yetenekleri



Kaynak: Kaspersky

BT Güvenliği Alanında Olgunlaşmış Müşteriler İçin Kaspersky Expert Framework

Kaspersky Expert Framework, siber olgunluğa erişmiş bir BT ekibi tutumu, oturmuş güvenlik ekipleri ve kaynakları olan kurumları hedefler. Expert Framework en geniş anlamda hedefli saldırılara ve APT'lere karşı uç nokta, ağ, e-posta internet koruması dahil tüm güvenlik fonksiyonlarının merkezi olarak yönetilebildiği tek bir konsol sunar. İzleme, görselleştirme, bildirim ve raporlamayı; gelişmiş tehdit algılamasını; derinlemesine araştırmayı, tehdit avını ve olay müdahalesini kapsar. Optimum Framework'de olduğu gibi, şirket içi araçları ve yeterlilikleri tamamlayan bir MDR hizmeti sunulur; bu çerçevede bu hizmet MDR Expert olarak adlandırılır. Beklendiği üzere MDR Expert; bir Kaspersky Güvenlik Operasyonları Merkezi analistine erişim, genişletilmiş ham veri depolama, Kaspersky Tehdit İstihbaratı Portalı'ndan seçilen özelliklere erişim ve özelleştirilmiş müdahale senaryoları gibi özelliklerle birlikte çok daha geniş bir hizmet sunar. [2]

Herkes için Tespit ve Müdahale: EDR ve MDR

Geçtiğimiz birkaç yıl içerisinde Orta Doğu, Türkiye ve Afrika pazarında EDR araçları ve MDR hizmetleri kullanımında bir artış görüldü. EDR araçları tehdit avına, adli bilişim analizine, anormallik tespitine ve olay müdahalesine olanak sağlıyor. Türkiye

[2] Expert Framework'e kapsamlı bir genel bakış, bu belgenin kapsamı dışındadır, ancak daha ayrıntılı bilgi IDC Teknoloji Bülteni: Modern Güvenlik Operasyon Merkezlerinin (SOC) Mücadelesinde bulunabilir.

güvenlik pazarı değerlendirmesine göre, Türkiye'deki kurumların %91'i güvenlik operasyon merkezi hizmetlerini güvenlik izleme ve tespit amacıyla kullanıyor. Bu kurumların %68'i, güvenlik operasyon merkezilerinin olay müdahalesi becerilerinden faydalanıyor. Türkiye'de tehdit istihbaratı kullanan kurumların oranı ise %61'dir. Bu kurumlar EDR ve MDR hizmetlerine yatırım yapmayı gitgide daha fazla düşünüyor.

EDR araçlarının analitik becerileri, güvenlik analistlerinin sinsi veya gözden kaçabilen tehditleri tespit etmesine yardımcı olarak tespit yüzeyini EPP paketlerinin sunduğu hizmetin ötesine genişletiyor. Orta Doğu, Türkiye ve Afrika'da bulunan kurumlar, uç nokta koruma yapılarını tamamlamak ve geliştirmek için EDR'a yatırım yapmış durumda, ancak bu araçlardan faydalanabilmek için kurumda sırf bu araçlardan sorumlu analistlerin çalışması gerekiyor. IDC CIO Anketi'ne göre Orta Doğu, Türkiye ve Afrika bölgesinde bulunan kurumların %37'si 2020'de uç nokta güvenlik ve tespit teknolojilerine yatırım yapmayı planlıyor. Türkiye'deki kurumların %67'si uç nokta güvenlik ve tespit teknolojilerine öncelik veriyor. Güney Afrika ve BAE'de uç nokta güvenliği yatırımı planlayan kurumların oranı ise sırasıyla %42 ve %17'dir. Bu durum, Orta Doğu, Türkiye ve Afrika'da en varlıklı kurumların dışında kalan tüm kurumları (veya varlıkları, aktiviteleri ya da mevzuat yükümlülükleri en sıkı güvenlik önlemlerini alması gereken kurumlar) etkileyen güvenlik uzmanı azlığına dikkat çekiyor.

Bu da, EDR araçlarının müşteri adına yönetilen güvenlik hizmetleri sağlayıcısı (MSSP) tarafından yönetildiği MDR hizmetlerine talep uyandıran bir pazar yarattı. Hem (Kaspersky gibi) güvenlik çözümleri tarafından hem de hizmet tarafından oyuncuları barındıran bu segment hızla büyüdü. MDR sağlayıcılarının çoğu, tüm müşteri gruplarının ihtiyaçlarını karşılayabilmek için farklı düzeylerde özel destek, raporlama, tehdit avcılığı ve olay müdahalesi sunan kademeli hizmetler veriyor. Orta Doğu, Türkiye ve Afrika bölgesindeki tüm kurumlar, kendi kendilerine EDR yürütecek kaynaklara sahip olmadığı için bu hizmetler, pazardaki bir ihtiyacı karşılıyor. Dolayısıyla IDC, 2020'nin geri kalanında ve sonrasında da talepte artış görmeye devam etmeyi bekliyor.

Zorluklar

Kaspersky, kapsamlı ve karmaşık bir portföy geliştirerek uç nokta güvenliği ve güvenlik entegrasyonu konusunda her türlü kuruma rehberlik edebilecek ayrıntılı bir çerçeve ortaya koydu. Bununla birlikte üretici, bu vizyonu hayata geçirirken bazı zorluklarla da karşılaşacak.

MDR pazarı Orta Doğu, Türkiye ve Afrika'da istikrarlı biçimde büyüyor ve pazardan pay alan oyuncuların sayısı artıyor. Bu oyuncular, hem güçlü EDR çözümü sağlayıcılarından hem de sağlayıcılara şüpheyle yaklaşan, üstün becerili ve deneyimli güvenlik analistlerine sahip MSSP'lerden oluşuyor. Bu alanda herhangi bir sağlayıcının kendini diğerlerinden ayrıştırması oldukça zorlu bir durum ve müşterilerin ödedikleri hizmetin karşılığını aldığını hissetmelerini sağlamak için hizmet sağlayıcının yeterli kaynak yatırımı yapmasını gerektiriyor. Elbette denemeden anlamak mümkün değil; başarının temel ölçütü, şirketin herhangi bir sızıntı yaşamamasıdır. Öte yandan, CISO'nun da yönetim kurulunu hizmete yaptıkları yatırımın geri döndüğüne ikna etmesi gerekebilir. Dolayısıyla, Kaspersky'nin MDR müşterilerine ihtiyaç duydukları ölçütleri sağlamaya hazır olması önemlidir.

Kaspersky'nin kademeli yaklaşımı ve Optimum Framework göz önünde bulundurulduğunda sağlayıcı, güvenlik tutumlarını geliştirmek üzere stratejik bir yaklaşım benimsemek isteyen orta ölçekli şirketlere yardım etmeye hazır

durumdadır. Bununla birlikte, pazarın yüksek tarafında, oturmuş müşteri portföylerine sahip köklü kurumsal güvenlik oyuncularıyla karşı karşıya gelecek. Kaspersky'nin platformunun en büyük avantajlarından biri, (Security Foundation düzeyinden entegre siber güvenlik düzeyine kadar) çok sayıda modül ve bileşeninin yerel entegrasyonu ve daha fazla modül kurulumundan elde edilen toplam faydadır. Öte yandan, kurulum ne kadar kapsamlı olursa o kadar eski ürünün değiştirilmesi gerekecektir.

Kaspersky; kademeli yaklaşımıyla (Şekil 2); Security Foundations, Optimum Framework ve Expert Framework içinde yer alan çok sayıda ayrı bileşen ve hizmetle; ikili EDR ve MDR seviyeleriyle ve normal EDR, otomatik EDR ve MDR ile ilgili daha fazla seçenekle karmaşık bir hizmet sunuyor. Sağlayıcı, müşterilerine ve potansiyel müşterilerine ihtiyaçlarını karşılayacak optimum çözüm kombinasyonunu belirleyebileceği mesajını net bir şekilde verebilmelidir.

Geleceğe Bakış

Kapsamlı ve yoğun tehditlerle karşı karşıya kalan, kısıtlı ekiplerle ve ayrı ayrı parçalardan oluşan güvenlik altyapısıyla güvenlik operasyonlarını yönetmekte zorlanan şirketler, entegre ve birleşik siber güvenlik çözümlerine ihtiyaç duyuyor. Kaspersky'nin sunduğu siber güvenlik çözümlerinin geniş yelpazesi, hem ana akım pazarın hem de daha büyük, güvenlik açısından daha olgun müşterilerin ihtiyaçlarını karşılayabilecek entegre bir siber güvenlik yaklaşımı biçimlendirmesini sağlıyor.

Kaspersky'nin sunduğu siber güvenlik çözümlerinin geniş yelpazesi, hem ana akım pazarın hem de daha büyük, güvenlik açısından daha olgun müşterilerin ihtiyaçlarını karşılayabilecek entegre bir siber güvenlik yaklaşımı biçimlendirmesini sağladı.

Kaspersky bilinen, bilinmeyen ve gelişmiş tehditlere karşı koruma sağlayan ürünleriyle bağımsız testlerde düzenli olarak yüksek puanlar alıyor. Ayrıca düzenli olarak yayınladığı güvenlik araştırmaları da oldukça saygın kabul ediliyor. Üretici, yaklaşımını ve çerçevesini belirlediği bir vizyona sahip; bundan sonraki görevi, bu vizyonu pazara anlatmak ve müşterilerine siber güvenliklerini geliştirme yolculuklarında yol göstermektir.

Değişen tehditlerle birlikte kurumlarında değişmesi, güvenlik tutumlarını güçlendirmek üzere kapsamlı çözümleri ve hizmetleri değerlendirmesi gerekiyor. Orta Doğu, Türkiye ve Afrika bölgesinde yer alan ve sağlam bir güvenlik programı oluşturmaya ihtiyaç duyan kurumlar, uç nokta güvenliğine entegre edilebilen çok katmanlı bir yaklaşım benimsemeyi gitgide daha fazla düşünüyor; gelişmiş saldırı vektörlerinin ve hedefli saldırıların artık geleneksel antivirüs yöntemleriyle çözülemeyeceğini her geçen gün daha iyi anlıyorlar. Buna bağlı olarak Orta Doğu, Türkiye ve Afrika pazarında EDR araçları ve MDR hizmetleri gitgide daha fazla benimseniyor. EDR ve MDR benimsenmesinin arkasında yatan en büyük motivasyonlar, koruma becerilerini artırmak, gelişmiş tehditleri ve hedefli saldırıları tespit etme gereksinimidir.

Güney Afrika, Suudi Arabistan ve Türkiye'deki kurumlar, MDR hizmetlerinden ziyade EDR hizmetlerine daha fazla talep gösteriyor. Orta Doğu, Türkiye ve Afrika bölgesinde şimdilik Güvenlik Operasyon Merkezi hizmeti müşterileri, MDR hizmetlerine daha fazla değerlendiriyor. Daha önce değindiğimiz artan farkındalık ve diğer motivasyonlar da bölgede MDR hizmetlerinin benimsenmesini hızlandırmaya başladı. Kurumların varlıklarını siber saldırılardan korumak büyük bir zorluk olmaya devam ettikçe tespit ve müdahale ürün ve hizmetlerinin kullanımı da artmaya devam edecek.

IDC Hakkında

International Data Corporation (IDC), bilgi teknolojileri, telekomünikasyon ve tüketici teknolojisi pazarlarına yönelik pazar istihbaratı, danışmanlık hizmetleri ve etkinliklerinde üst düzey bir küresel tedarikçi konumundadır. IDC, BT profesyonellerinin, yöneticilerin ve yatırım topluluklarının teknoloji satın alımlarını ve iş stratejilerini kanıtlara dayalı bir şekilde yapabilmelerini sağlamaktadır. 1.100'den fazla IDC analisti 110'dan fazla ülkede teknoloji ve endüstri fırsatları hakkında küresel, bölgesel ve yerel uzmanlık hizmetleri sunmaktadır. Son 54 yıldır IDC, müşterilerinin kilit iş hedeflerine ulaşabilmelerine yardımcı olmak için stratejik iç görüler sunmaktadır. IDC, dünyanın lider teknoloji medyası, araştırma ve etkinlik şirketi olan IDG'nin bağlı şirketidir.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, Birleşik Krallık
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

IDC #EUR246748220