IDC Teknoloji Bülteni

Sponsor: **Kaspersky**

Yazarlar:

Konstantin Rychkov

Yeşim Araç Öztürk

Ağustos 2020

Modern Güvenlik Operasyon Merkezlerinin (SOC) Mücadelesi

Güvenlik Operasyonlarının Gelişimi ve Güncel Durumu

Günümüzde güvenlik, her zamankinden daha fazla yeni parlak oyuncaklar satın almakla ilgili değil, aksine temel güvenlik ön koşullarını göz ardı etmeden genel iş önceliklerine katkıda bulunan süreçlerde verimlilik sağlamakla ilgilidir. Şu anda Orta Doğu, Türkiye ve Afrika bölgesindeki kurumların %17'si, 2020'de güvenlik operasyon merkezlerine yatırım yapmayı planlıyor. Körfez Arap Ülkeleri İşbirliği Konseyi'nde yer alan kurumların %69'u ise kendi güvenlik operasyon merkezlerine sahip. Bu merkezlerin %44'ü üçüncü taraflarca yönetilirken; %16'sı ise hibrit bir güvenlik operasyon merkezi yapısına sahiptir. Türkiye'deki kurumların %49'unun halihazırda farklı yapılarda da olsa bir güvenlik operasyon merkezi var; %21'i ise kurma aşamasında. Güney Afrika'daki kurumların %19'u ise 2020'de bir güvenlik operasyon merkezine yatırımı yapmayı planladıklarını belirtiyor. En gelişmiş kurumlar, kurum içi güvenlik operasyon merkezlerini BT yönetişimine entegre olacak şekilde ve geleceğin stratejik önceliklerine uygun biçimde kuruyor.

Yaklaşımdaki bu değişimin çok katmanlı yansımaları var:

- Eskiden güvenlik operasyon merkezlerinde ayrıcalıklı bir konuma sahip olan siber güvenlik otomasyon istihbaratı, müdahale ve yönetme teknolojileri, artık tespit ve müdahale teknolojileri ve hizmetleriyle rekabet halinde ve/veya bu teknolojiler tarafından kapsanıyor.
- Güvenlik operasyon merkezleri, NetOps, SecOps, DevOps ve kuruma katkıda bulunanların dahil olduğu ortak projeler haline geliyor.
- Kurumlarınçevresel sınırlarının genişlemesiyle oluşan alarm ve gürültü seli, aşağıdakilerin daha fazla kullanılmasına sebep oluyor:
    - Kurumların seçtiği hizmet sağlayıcıları veya güvenlik tedarikçilerinin sunduğu yönetilen güvenlik hizmetlerine (MSS) güvendiği durumlarda fonksiyonel dış kaynak kullanımı. Örnek vermek gerekirse, Birleşik Arap Emirlikleri'ndeki şirketlerin %57'den fazlası şu anda MSS kullanıyor ve gelecek birkaç yıl içerisinde daha fazla sayıda kurum MSS kullanmaya başlamayı düşünüyor. IDC Türkiye'nin güvenlik pazarı değerlendirme anketine göre Türkiye'deki kurumlar, güvenlik bütçelerinin %22'sini MSS'ye ayırdıklarını belirtiyor.
    - Ücret ödeme veya tehdit istihbaratı (TI) pratiği geliştirerek özel platformlara katılma yoluyla araştırma ve önceliklendirilmenin geliştirilmesi. Orta Doğu, Türkiye ve Afrika bölgesindeki kurumların %22'si, 2020'de tehdit istihbaratı kullanmayı

planlıyor. Dahası, Türkiye'de her iki CISO'dan biri MSSP'lerin sunduğu tehdit istihbaratı hizmetlerini kullandığını belirtiyor.

- Bütçe kısıtlamalarının yanı sıra, güvenlik ürünleri arasında entegrasyon/otomasyon eksikliği, Orta Doğu, Türkiye ve Afrika'daki kurumların %13'ü için güvenlik programlarına en büyük tehdidi oluşturuyor.
- Haziran 2020'de görüşülen CIO'ların %34'ü, 2020'de Orta Doğu, Türkiye ve Afrika bölgesindeki otomasyonu güçlendirmek için güvenlikte yapay zekaya (AI) ağırlık verip geliştirmeyi planladıklarını ifade etti. Aynı ankete göre, Türkiye'deki kurumların %37'si ile Birleşik Arap Emirlikleri'ndeki kurumların %36'sı güvenlik alanında yapay zeka kullanmayı planlarken, Güney Afrika'daki kurumların sadece %30'unun güvenlik odaklı yapay zeka yatırım planları bulunuyor.

Modern güvenlik operasyon merkezleri, verimli ve etkili olmalarına duyulan gereksinim ile birlikte çarpıcı bir şekilde gelişti.

Modern Güvenlik Operasyon Merkezlerinin Karşılaştığı Zorluklar

Artan uyarı hacminin yanı sıra yetkin uzman açığı

Önceliklendirme ve sistem bakımı, kısıtlı kaynaklara sahip güvenlik ekiplerinin zamanını tüketiyor. Bu sorun, sektör için yeni bir durum değil; kurumların %37'sinden fazlası, gelişmiş tehditlere ilişkin güvenlik uzmanlığı eksikliğinin Orta Doğu ve Afrika'daki güvenlik programlarının karşılaştığı en büyük zorluk olarak öne çıktığını belirtiyor. Neredeyse her iki CIO'dan biri, Güney Afrika ve Türkiye'deki güvenlik programlarına en büyük tehdidin güvenlik uzmanlığı eksikliği olduğunu vurguluyor. BAE'deki kurumların %33'ü bu tehdidi ikinci sırada görüyor. Sızıntının keşfedilmesinden çözüme kadar geçen süreyi en aza indirmek için analistlerin zamanı, insan müdahalesine ihtiyaç duyan daha sofistike uyarılar üzerinde çalışmanın yanı sıra, proaktif bir şekilde tehditi araştırarak daha iyi kullanılabilir.

Aynı anda birçok panel yönetmenin zorluğu sürüyor

Tipik bir güvenlik operasyon merkezi 20 ya da daha fazla teknolojiden meydana gelen bir kombinasyon kullanabilir; anlaşılacağı üzere, bunların ayrı ayrı izlenmesi ve yönetilmesi zor olabilir. Önceliklendirmeyi iki ayrı kontrol panelinde gerçekleştirmek bile zorken, normalde Ağ, SIEM, TI ve daha fazlası devreye girdiği için üçün epeyce üzerinde sayılarla uğraşıyor oluruz.

Araçlar arasındaki entegrasyon eksikliği, çözüme yönelik çalışmaları karmaşık hale getirir. Genellikle uç nokta, ağ ve internet politikalarımız ayrıdır. Bunlara bir de buluttaki ve şirket içindeki dağıtım ortamları eklendiğinde iş daha da büyür.[1]

Yasalara ve mevzuata uygunluk

Mevzuata ilişkin büyük değişikliklerin 2016-2017'deki ilk aşamasından bu yana, güvenlik operasyonlarında mevzuata uymanın önemi son derece arttı. Mevzuata uyum, şu anda Orta Doğu, Türkiye ve Afrika'daki güvenlik liderleri için ilk 5 yatırım önceliği arasında yer alıyor ve kurumların %32'si mevzuata uyumla ilgili çözümlere yatırım yapmayı planlıyor. IDC'in Türkiye güvenlik pazarı değerlendirme anketine

[1] IDC Teknoloji Bülteni: Entegre Siber Güvenlik Zorlu Bir Ortamda Verimlilik ve Etkinlik Sağlıyor

göre kurumların %75'i, düzenlemeleri ve mevzuata uyumu 2020'deki stratejik güvenlik konularının başında görüyor.

Güvenlik sektörü bu yönde ciddi bir ilerleme kaydetmiş olsa da, yasalar ve güvenlik uyumluluğu henüz çözülememiş konular arasında yer almaya devam ediyor. Yalnızca denetimleri geçmeyi amaçlayan çok sayıda göstermelik uyum pratiğinin etkisini görmezden gelsek bile, çok uluslu şirketlerde farklı mevzuatların birbiriyle çelişmesi gibi sorunlar ortaya çıkmaya devam edecek. Dahası ise güvenlik operasyon merkezi ekibi için yönetilmesi gereken başka bir süreç, konsol ve/veya araç anlamına gelecek.

Bütçeler

Güvenlik operasyon merkezi araçlarında yatırımın geri dönüşünü (ROI) göstermek neredeyse imkansız, ancak kurumlar bütçe tahsisini belirlerken hala bu göstergeyi baz alıyor. CISSP-ISSMP resmi rehberinden aldığımız yatırımın geri dönüşü formülüne göre en zor olan kısım, güvenliğin sürdürülebilirliği için uygulanan önlemlerin parasal etkisini ölçebilmek olacaktır. Üstelik bu hala tepkisel (reaktif) bir güvenlik yaklaşımına dayanıyor.

Olumlu yanından bakarsak, güvenlik stratejisinin genel BT stratejisiyle hizalanması, CISO'nun bütçe artırımı için avantaj sağlayabilir. Pandemi sürecinde yaşanan son gelişmeler, güvenliğin kurumlara değer katan bir bileşen olduğunu kanıtladı. 2020'de Orta Doğu, Türkiye ve Afrika'daki dijital dönüşüm programlarına karşılık olarak CIO'lar, her saniye güvenlik yatırımlarını artırmayı bekliyor.

Bilgi aktarımı ve yetenek yönetimi

Güvenlik alanında yetenekli çalışanlar bulmanın bir problem olması şaşırtıcı değil, ancak şu anda özellikle iş rutinleriyle ilişkili sofistike kurumsal sistemler hakkında bilgi aktarımıyla ilgili de sorunlar yaşanıyor.

Kurum içerisinde yetenekli güvenlik personelleri bulup yetiştirmenin belirli bir maliyeti olmasının yanı sıra, birinci seviye bir analistin aynı şirkette çalışma süresi her geçen yıl azalıyor. Günümüzde bir analist, aynı şirkette ortalama olarak 27 ay çalışıyor ve bunun 4 ayı ise eğitimle geçiyor.

Süreçlere ilişkin dökümanların olmayışı ve prosedürlerdeki eksiklikler, güvenlik operasyon merkezi liderlerini ekipte her değişiklik olduğunda sıfırdan başlamaya zorluyor. Dolayısıyla analistlerin sürekli değişmesi, tüm güvenlik programının verimliliğini düşürüyor.

İnsansız teknolojinin operasyonlar üzerindeki etkisi

IDC'nin araştırmasına göre kurumların %22'si, rutin operasyonlara odaklanan operasyonel kaynakların güvenlik programlarını zayıflattığını söylüyor. "Büyük filtre" oluşturmak, temel sorunları çok daha hızlı çözerek gerçek problemleri önceliklendirmeye yardımcı olabilir.

Birinci seviyeden başlayabilir, daha fazla otomasyon ve yönetim ekledikçe güvenlik operasyon merkezlerimizin siber olgunluğunu artırabiliriz:

Kurum içi kaynakları kullanarak ve güvenlik operasyon merkezini yalnızca teknolojiyle güçlendirerek olgunluk eğrisinde ilerleme sağlamak pek çok kurum için uygun değildir. Bu nedenle, güvenlik fonksiyonlarının otomatik hale getirilmesi ve yönetilen güvenlik hizmetlerine sahip kurum içi güvenlik operasyon merkezlerinin geliştirilmesi hem kaçınılmaz hem de tavsiye edilen bir yaklaşımdır.

Şekil 1
Güvenlik Operasyonları İçin Olgunluk Eğrisi

Kaynak: IDC

Kurum içi kaynakları kullanarak ve güvenlik operasyon merkezini yalnızca teknolojiyle güçlendirerek olgunluk eğrisinde ilerleme sağlamak pek çok kurum için uygun değildir. Bu nedenle, güvenlik fonksiyonlarının otomatik hale getirilmesi ve yönetilen güvenlik hizmetlerine sahip kurum içi güvenlik operasyon merkezlerinin geliştirilmesi hem kaçınılmaz hem de tavsiye edilen bir yaklaşımdır.

Son zamanlarda güvenlik teknolojisi, bu konularda çalışanlara bu sorunu çözmelerine yardımcı olacak şekilde gelişim aşamalarında beklenenden öte bir sıçrama yaşadı. Otomasyon ve dış kaynak kullanımı, geleneksel *izleme, toplama, toplanan veriler arasında ilişki kurma, analiz etme, tespit etme ve bildirme* dizisini hızlandırıyor. Vaka yönetimi otomasyonu, iç görü ve aksiyon arasında operasyonel bağlantı kuruyor. Tehdit istihbaratı ise olay önceliklendirmeye ve olayların önünü almaya yardımcı olarak ekibin gayretlerini, verimliliği en üst düzeye çıkaracak şekilde yönlendiriyor.

Güvenlik Operasyon Merkezinizdeki Eksikleri Tamamlama

CISO'lar güvenlik operasyonları merkezlerinin karşılaştığı zorluklarının üstesinden gelebilmek için ekibin aşağıdakileri yapmasını sağlayacak kapsamlı bir çözüme ihtiyaç duyar:

- Otomasyonu oluşturan ve ardından bu bilgiyi özel olay müdahalesi senaryolarına aktararak uzun vadede benzer vakalarla mücadeleyi basitleştiren.
- Uzman ekiplerin tehdit istihbaratı bilgilerini kullanabilmesini sağlayan ve verimi en üst seviyeye taşıyan bir TI programı oluşturarak yönetim kademesine yatırım getirisini gösterebilen. Tehdit istihbaratının bu şekilde kullanımı pazarda uzun süredir savunuluyor.
- Olası saldırıları önlemeye yardımcı olmak için proaktif biçimde tehdit avlayan ve kurumun karşı karşıya olduğu tehditlere uygun tutum alma mekanizmaları ve defans oluşturan.

- Bilgisayar güvenliği olay müdahale ekibinin çağrı oluşturma, runbook otomasyonu, işbirliği kanalları, adli bilişim ve anahtar performans göstergeleri (KPI) takibi için ihtiyaç duyduğu tüm sistemlerle vaka yönetimi araçlarını entegre eden. Etkili bir güvenlik operasyon merkezi için müdahale aşamasında çeviklik olmazsa olmazdır.
- İnternetten, ağdan, uç noktadan, e-postadan ve ilave analizlerden gelen tüm bilgilerin birbiriyle ilişkilendirildiği ve soruşturma için saklandığı merkezi bir konsol kuran. Bu fonksiyon kuruma, gelişmiş bir saldırıyla karşı karşıya kaldığında güvenlik operasyon merkezi için hayati önem taşır.
- Güvenlik operasyon merkezi planı oluşturulmasının en başından itibaren güvenlik ve gizlilik kurallarını uygulayan ve risk odaklı yönetime odaklanan.
- Güvenlik operasyon merkezinin kurulmasından itibaren çalışanları elde tutmaya ve becerilerini geliştirmeye yönelik programlar oluşturan. Eğitim yalnızca ekibin temel bilgileri öğrenmesine değil, aynı zamanda etkili bir bilgi aktarım süreci sağlamaya da yardımcı olmalıdır. Çalışan değişiminin artırdığı güvenlik yeteneği eksiklikleri, en iyi yapılandırılmış güvenlik operasyon merkezi dönüşüm planlarını bile sekteye uğratabilir ve belirsiz süreler boyunca geciktirebilir.

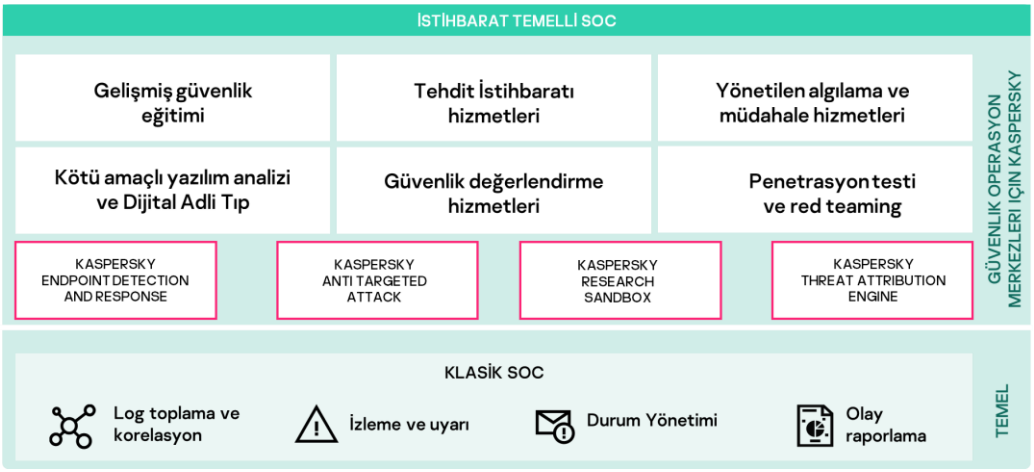
Yeni nesil güvenlik operasyon merkezlerini faaliyete geçirecek bir çözüm, süreçleri, insanları ve teknolojileri sürece dahil etmeli, ilgili rehberleri sunmalı, kapsamlı ve kullanıma hazır bir operasyonel çerçeveye sahip olmalı ve bir platform ya da yönetilen bir hizmet olarak sunulmalıdır. Bu gereksinimler fazla gibi görünse de, geleneksel güvenlik operasyon merkezlerini geliştirebilen ve geçiş yapılmasını sağlayan dönüştürücü hizmetler hali hazırda sunuluyor.

Güvenlik Operasyon Merkezi İçin Kaspersky Expert Framework ve Araç Seti

Güvenlik liderlerinin yeni nesil güvenlik operasyon merkezlerine geçişte karşılaştıkları problemlerin genişliği ve derinliği, tüm eksikleri giderecek ve her ortama uyum sağlayacak tek bir çözümü hayal etmeyi zorlaştırıyor. Açıkça söylemek gerekirse böyle bir çözüm henüz mevcut değil. Böyle bir çözümün, süreçleri, insanları ve teknolojileri sürece dahil etmesi, ilgili rehberleri sunması, kapsamlı ve kullanıma hazır bir operasyonel çerçeveye sahip olması ve bir platform ya da yönetilen bir hizmet olarak sunulması gerekir. Bununla birlikte, geleneksel güvenlik operasyon merkezlerini geliştiren ve siber olgunluk eğrisinde yükselmelerini sağlayan dönüştürücü hizmetler de sunuluyor.

Kaspersky Expert Framework, gelişmiş araçlardan oluşan geniş portföyünü özel hizmetler ve uzman desteğiyle bir araya getiriyor. Kaspersky'nin yaklaşımı, özünde hem süreçlerdeki hem de altta yatan teknolojideki sorunları ve gözden kaçanları tanımlamak; ardından bunları güvenlik operasyon merkezi dönüşümünü sağlayacak kapsamlı çözümler ve hizmetlerle ele almaya odaklanıyor. Anahtar bileşenlere ilişkin üst düzey bir genel bakış aşağıda Şekil 2'de verilmiştir:

Şekil 2
Güvenlik Operasyon Merkezi için Kaspersky



Kaynak: Kaspersky

Sunulan bu hizmetin merkezinde, üç kilit bileşenden oluşan tek bir teknolojik platform yer alıyor:

Kaspersky Anti Targeted Attack Platform (KATA),
Kaspersky Endpoint Detection and Response (KEDR) Expert sürümü,
Kaspersky Managed Detection and Response (MDR) Expert sürümü.

Expert çözümler, Optimum Framework dahilinde ana akım pazara yönelik sunulan hizmetlerin genişletilmiş sürümleridir. [2]

Expert Framework'ün güvenlik operasyon merkezlerine yönelik uzun bileşen listesi aşağıdakileri içeriyor:

Kaspersky TI ve CyberTrace Fusion aracı,
Kaspersky siber güvenlik eğitim programları,
Kurum genelinde ve sektöre özel güvenlik değerlendirme hizmetleri,
Vaka inceleme ve müdahale hizmetleri,
Profesyonel hizmetler (güvenlik operasyon merkezi danışmanlığı ve teknik destek gibi).

Siber Olgunluğa Sahip Güvenlik Operasyon Merkezlerine Yönelik Kaspersky Üssü Fonksiyonu

Yukarıda değindiğimiz gibi, Kaspersky'nin siber olgunluğa sahip müşterilere sunduğu hizmetler, ek fonksiyonlar içeriyor. KEDR Expert hizmeti, güvenlik operasyon merkezinin verimliliğini artırmak için inceleme otomasyonuna odaklanıyor. Güvenlik operasyon merkezi ekipleri, Optimum hizmetin sunduğu tüm fonksiyonlara ek olarak, MITRE ATT&CK haritalamasına sahip benzersiz IoA'lere, talep üzerine şüpheli örneklerin izole simülasyonlarda derin analizi için özelleştirilebilen güvenli alanlara ve incelemelere yönelik tehdit istihbaratına erişim sağlıyor.

[2] Bu framework burada daha ayrıntılı olarak anlatılmaktadır: http://media.kaspersky.com/en/business-security/enterprise/endpoint-detection-and-response-optimum-whitepaper.pdf

Expert Framework altındaki MDR hizmeti; 7/24 izleme, olay doğrulama ve geriye dönük tehdit avına yönelik genişletilmiş ham veri depolama dönemleriyle otomatik ve yönetilen tehdit avı imkanı sunuyor. Birinci seviye fonksiyonların dış kaynaklardan sağlanmasına izin veren bu hizmet, güvence ve doğrulama için Kaspersky'nin güvenlik operasyon merkezi uzmanlarıyla doğrudan iletişim kurabileceğiniz bir kanala da sahip. Tüm ham veriler ve tehdit istihbaratı, adli bilişim ve iç soruşturmalar için kullanılabiliyor. Buradaki amaç, zaman alan süreçlerin yükünden kurtulmak ve dış operasyonların tamamen geçici olmasını sağlamaktır.

MTTR (otomatik olay analizi sonucu otomatik alarm verilmesi ile Kaspersky uzmanları tarafından sorunun çözülmesi arasında geçen süre) ortalama 25 dakikadır.[3] Açıkçası bu ölçüt, özellikle de sızıntı sonrası bir iyileştirmeden bahsediliyorsa, sektörde saatlere, hatta günlere ve haftalara kadar uzayabiliyor. Hızlı, tempolu, ve modern güvenlik operasyon merkezi ortamlarında tepki süresinin dakikalarla ölçülmesi çok önemlidir.

Kaspersky'nin siber olgunluğa sahip güvenlik operasyon merkezlerine yönelik sunduğu en önemli bileşenlerden biri; ağ trafik analizi, uç nokta etkinliği izleme, birleşik görünürlük ve kontrol için operasyonları tek bir internet tabanlı konsolda merkezi hale getiren KATA platformudur. Platform; ağdan, e-postadan, internetten ve uç nokta uzaktan ölçümünden gelen meta verilerin toplanmasını, normalleştirilmesini, aralarında ilişki kurulmasını, depolanmasını ve incelenmesini otomatik hale getiriyor. 'RCA', adli bilişim, 'YARA' tespiti, 'IoC' temelli keşif, 'IoA' haritalama, tehdit avına yönelik sorgulama ve Kaspersky TI portalıyla entegrasyon ise yarı otomatik fonksiyonlar arasında yer alıyor.

KATA platformundaki keşif ve inceleme sonuçları, özelleştirilebilen politikalara ve eşiklere göre ağ geçidi düzeyinde otomatik müdahaleyi tetikliyor ve uygulamaya koyuyor. Hem KEDR hem de KATA ürünleri Syslog API'a sahip ve Syslog CEF ile çalışabilen tüm SIEM'leri ve SOAR'ları destekliyor. Bu fonksiyon "gürültüyü" önemli ölçüde azaltarak önemli güvenlik olaylarına odaklanmaya yardımcı oluyor. Önceden filtrelenen alarmlar, SIEM'in işlemlerini ve depolama ihtiyacını önemli ölçüde azalttığı için satın alma ve kullanım maliyetlerini de düşürüyor.

Kısacası, 'SOC Expert''in üç temel bileşeni, hem bilinen hem de yeni, 0-gün ve gelişmiş tehditlerin tespit edilmesi ve önlenmesine yönelik gelişmiş ve özelleştirilebilen araçlar sağlayabiliyor. Tamamı TI platformuyla bağlantılı olan bileşenler, eylemler ve soruşturmalar için bağlam sunuyor.

Kısacası, SOC Expert'in üç temel bileşeni, hem bilinen hem de yeni, 0-gün ve gelişmiş tehditlerin tespit edilmesi ve önlenmesine yönelik gelişmiş ve özelleştirilebilen araçlar sağlayabiliyor. Yönetilen bileşen, günlük izleme, önceliklendirme veya tek seferlik olay incelemeyle ilgili personel kısıtlamasını ortadan kaldırıyor. Talep üstüne eklenen bileşenler, derinlemesine hizmet ve fonksiyonlarıyla en sofistike vakalarda bile destek sağlayabiliyor. Tamamı TI platformuyla bağlantılı olan bileşenler, eylemler ve incelemeler için bağlam sunuyor.

Güvenlik Operasyon Merkezi Programlarına Değer Katan Bileşenler

KATA, KEDR ve MDR ileri düzeydeki soruşturmaları ve müdahale süreçlerini otomatik hale getirmek ve yönetmek için tasarlanmıştır. Yine de güvenlik operasyon merkezlerinin henüz yalnızca teknolojiyle kapatılamayan eksikleri bulunur. Bu sebeple Kaspersky Expert Framework, güvenlik kurulumundaki bazı hataları tanımlayıp zararlarını en aza indirecek bir dizi hizmet ve destekleyici araç içeriyor.

[3] http://securelist.com/managed-detection-and-response-analytics-report/94076/

Güvenlik operasyon merkezi dönüşümü, açık bir yol haritası ve sürekli uygulama doğrulaması gerektiren karmaşık bir süreçtir. Güvenlik değerlendirmeleri, anlık görüntüye dayalı olmalarına rağmen güvenlik programı ve teknoloji araçları içerisindeki büyük sorunları ve tutarsızlıkları su yüzüne çıkarabilir. Sızma testi, red team uygulaması ve yazılım güvenliği değerlendirmelerinin bulguları, değişim planının kilit unsurlarıdır ve hem ilerlemeyi ölçebilir hem de karşılaştırmalı analiz sunabilir.

Uzman rehberliği, teknik destek ve danışmanlık hizmetleri; sektördeki en iyi uygulamaları organizasyonel kurum hedefleriyle uyumlu hale getirecek şekilde özelleştiren bir güvenlik operasyon merkezi kurmaya yardımcı olabilir. Etkili planlama, maliyeti düşürür; riske dayalı mimari kararlar almaya yardımcı olur ve kurum hissedarlarına güvenliğin yatırımın geri dönüşünü gösterme imkanı tanır.

Daha önce de birkaç defa belirttiğimiz gibi, personel, her boyutta güvenlik operasyon merkezi için esas mesele ve en önemli varlıktır. Modern güvenlik operasyonları inşa etmek için analistlerin eğitimi ve becerilerinin artırılması stratejide önceliklendirilmelidir. Kaspersky bu sebeple güvenlik operasyon merkezleri için Expert Framework çözümüne eğitimi de dahil etmiştir ve LoB'ler için güvenlik farkındalığının temellerinden olay müdahalesine, kötü amaçlı yazılım analizine ve üçüncü seviye analistler için tehdit avına kadar çok farklı düzeylerde personele yönelik derslere sahiptir.

İşletmedeki güvenlik durumunun gerçekçi ve eleştirel değerlendirmesinden doğan, güvenlik operasyonları için sektördeki en iyi uygulamaları benimseyen, eğitimli personel tarafından etkinliği artırılan ve teknik destekle desteklenen bir dönüşüm haritasıyla modern bir güvenlik operasyon merkezi oluşturmaya doğru bir yolculuğa çıkabiliriz.

Güvenlik Operasyon Merkezini Tehdit İstihbaratıyla Güçlendirmek

Modern güvenlik operasyon merkezleri, zamanında bilinçli kararlar vermek için teknolojiye ve süreçlere olduğu kadar, bağlama oturtulmuş iç görülere de ihtiyaç duyar. Expert Framework'ün bağımsız bileşenleri amaca yönelik çözümler olarak da değerli olabilir; ancak, bu bileşenleri teknoloji entegrasyonu olmadan kullanmak için ortak bir enformasyon düzlemine ihtiyacınız olacaktır.

Kaspersky'nin değer katan temel bileşenlerinden sonuncusu ise TI platformudur. En ilgili ve en etkili IoC'leri sınıflandırmaya ve öne çıkarmaya yardımcı olmak için kurumsal tehdit profili ile tehdit veri akışları karşılaştırılıyor. Kaspersky'nin tehdit veri akışları (bunlarla kısıtlı olmamakla birlikte) şunları içeriyor: Tehdit türlerine (fidye, kimlik avı, vb.) ve hedeflenen ortamlara (IoT, mobil, vb.) göre ayrılan URL'ler, IP itibarı, APT IoC'leri, pasif DNS çözümlemeleri, FQDN'ler, güvenlik açıkları ve CVE'ler, C&C botnet'leri ve MD5 karmaları. Tehdit istihbaratı, savunucuları tehditler hakkında güncel tutmak için aynı zamanda ATP araştırmalarından yöntemler, teknikler ve taktikler de içeriyor.

Expert güvenlik operasyon merkezi hizmetinde KEDR ve KATA, tarama makineleri için IoC içe aktarmayı destekliyor. Çözümler, tehdit istihbaratını üçüncü taraf sağlayıcılardan, iş ortaklarından ve OSINT'den alan Kaspersky Security Network (bulut bilgi üssü) ile yerel olarak entegredir. Kaspersky TI portalı, nesneleri veri akışlarında aramaya ve eşleştirmeye olanak sağlıyor; ardından da IR ekiplerini

uyarıyor. Son olarak da CyberTrace (TI füzyon ve analiz aracı), SIEM'e yönlendirmek veya kayıtlar arasında ilişki kurmak üzere tüm formatlardaki veri akışlarını birleştirmeye yardımcı oluyor (özel iç akışlar da dahil olmak üzere JSON, STIX, XML ve CSV formatları).

Tehdit istihbaratını kullanabilmek ve uygulayabilmek, yalnızca TI sahibi olmaktan daha önemlidir. Eskiden güvenlik ekipleri yalnızca istihbarat toplardı ve süreç entegrasyonu olmadığı için bütün bu istihbarat rafta kalmaya mahkumdu. Eyleme dökülebilen ve kuruma/endüstriye özel istihbarat, operasyonların entegre bir parçası olmalı ve soruşturmalara katılmalıdır.

Zorluklar ve Geleceğe Bakış

Güvenlik operasyon merkezlerine yönelik Kaspersky Expert Framework ve araç seti; insan, süreç ve teknoloji açısından güvenlik operasyonlarındaki eksikleri tamamlamayı hedefleyen oldukça ayrıntılı ve özelleştirilmiş bir hizmettir. Seçilen yaklaşım, güvenlik operasyon merkezi analistlerinin becerilerini artırmak, yetenekli ve bilgili personeli şirket bünyesinde tutmak/eğitmek ve güvenlik fonksiyonlarını zenginleştirmek için hizmet ve teknolojiyi benzersiz biçimde bir araya getiriyor. Bununla birlikte tüm çözümler gibi bu hizmetin de bazı kısıtlamaları var.

Bileşenlerin bu kadar sofistike olması, güvenlik operasyon merkezinin üstün becerilere sahip çalışanları olmasını gerektiriyor. Kaspersky Expert Framework, birçok bileşenin halihazırda yerinde olduğu ve ayrıntılı bir yönetim çerçevesi altında işleyen siber olgunluğa sahip ortamlar için uygundur. 'Expert' hizmetin bağımsız bileşenleri, çok az değişiklikle olgun ortamlara uyum sağlayabilir; ancak sistemin tamamı, süreçlerin yeniden yapılandırılmasını ve mevcut araçların (özellikle de özelleştirilmiş araçların) entegrasyonunu gerektirebilir. PoC sırasında gereksinimlerin ayrıntılı biçimde değerlendirilmesini tavsiye ediyoruz. Değerlendirme hizmetleri belli bir ölçüye kadar bu analizi destekleyebilir, fakat kararı yine de güvenlik operasyon merkezi yöneticisine ve CISO'ya bırakır.

Tüm paketin uygulanmasının maliyeti, özellikle uç birim lisanslı ürünlerin Kaspersky çözümleriyle değiştirilmesi gereken durumlarda bazı kurumlar için yüksek fiyatlı kalabilir. Bu tür projelerde yatırımın geri dönüşünün değerlendirmesi ilk adımlardan biri olmalıdır. Alternatif olarak bileşenler ayrı ayrı satın alınabilir fakat bu durumda da şirket içi envanterle entegrasyonun maliyeti kontrol edilmelidir.

Kaspersky Expert Framework'ün merkezinde yatan teknoloji, tüm siber sahadaki tehditlerle savaşmaya uygundur. KEDR ve KATA'in işlevselliği ve etkiliği, sektördeki uzmanlarca ve pratikte kullananlarca yüksek puanlandırıldı, ancak burada da bazı kısıtlamalar var. KATA'nın trafik verimliliği makine kurulumu tarafından kısıtlanıyor ve performansı sürdürmek için veri akışı işleme tasarımı ve mimarisi üzerinde çalışmak gerekiyor. KEDR ise hafif ve Kaspersky'ye ait olmayan EPP araçlarıyla birlikte çalışabiliyor; ancak dağıtmak için ayrı bir KEDR sunucusuna ve yüklemeyi, güncellemeleri, kaldırmayı ve aracı yönetim senaryolarını yönetmek için Kaspersky Security Console (KSC) sunucusuna ihtiyacınız var. Bazı uygulamalarda şüpheli nesnelerin KEDR'den güvenli alana otomatik olarak iletilmesi mümkün değil ve doğrulama gerektiriyor.

Kaspersky'nin Expert Framework ve araç seti, SOC'ler için yalnızca olgun SOC'lerin güvenlik operasyonlarının verimliliğini ve güvenlik seviyesini en üst düzeye çıkarmasına yardımcı olmak amacını taşıyan benzersiz bir çözümdür. Geliştikçe, böyle bir framework modern SOC'nin temeli haline gelebilir.

Mimari açıdan bakıldığında hem KEDR hem de KATA fiziksel makinelerde ve sanal sunucularda çalışabiliyor; bazı kısıtlı fonksiyonları tercih edilen genel bulutta da dağıtılabiliyor. Şu anda EDR bileşeninin en büyük eksiği, aracıların dağıtılabildiği işletim sistemi: Şimdilik yalnızca Windows cihazlar destekleniyor. Ürün geliştirme planları Linux ve MacOS desteğini de içeriyor fakat 2021'de piyasaya sürülmeleri öngörülüyor.

KATA'de yer alan gelişmiş internet ve e-posta analizi özelliğinin en iyi Kaspersky ürünleriyle birlikte çalıştığı bildiriliyor. Heterojen ortamlardaki dağıtımlar, meta verilerin analizi için haritalamak üzere tam paket entegrasyonu gerektirecek.

Kaspersky'nin tehdit istihbaratı paketi de KATA gibi özel bir sunucu gerektiriyor. Kayıtları birbiriyle ilişkilendirme, SIEM'e doğru ve SIEM'den geri iletim gerektirebilir; bu da fazladan ağ ayak izi üretiyor. CyberTrace'in yeni sürümünün 2021'de piyasaya çıkması planlanıyor; bu sürüm, bu sorunları kısmen çözebilir.

Daha geniş açıdan baktığımızda, Kaspersky Expert hizmeti derin bir teknoloji bilgisi gerektiriyor ve "herkese uygun" basit bir çözüm değil. Kullanıma hazır beceriler, entegrasyonlar ve özelleştirme esnekliği bu ürünü modern bir güvenlik operasyon merkezi için çok değerli bir bileşen haline getiriyor olabilir, ancak uzman hizmetler olmadıkça bu paketten maksimum şekilde faydalanmak kolay bir iş değil. Karmaşık yapısı ve bileşenlerin sayısı, sağlayıcının net vizyonunu ve profesyonel desteğini gerektiriyor. Bu hizmet, dağıtımın uygulanmasını basitleştirmek için ideal olarak referans bir mimari ve kullanım senaryosu portalı ile birlikte sunulmalıdır.

Son olarak, Kaspersky Expert Framework ve güvenlik operasyon merkezi araç kiti, yeni özellikler ve entegrasyonlar eklenerek sürekli gelişen benzersiz bir hizmet. Başlıca amacı, siber olgunluğa sahip güvenlik operasyon merkezlerinin operasyon verimliliğini ve kuruma sağladığı koruma düzeyini en üst seviyeye çıkarmak. Böyle bir sistem MDR ve insan merkezli hizmetlerle geliştikçe modern güvenlik operasyon merkezi dönüşümünde bir mihenk taşı olabilir.

Son yıllarda mobilite, bulut, nesnelerin interneti (IoT), yapay zeka gibi yeni teknolojilerin benimsenmesiyle birlikte siber güvenlik ortamı oldukça değişti. Bu durum Orta Doğu, Türkiye ve Afrika bölgesindeki kurumların tehdit yüzeyini genişlettiği için kurumlar artan sayıda sofistike siber saldırılara maruz kalıyor. Gölge BT de saldırı yüzeyini önemli ölçüde etkiliyor. IDC CIO anketine göre, BAE'deki kurumların %41'i, kurumlarının ağına, verilerine ve internet güvenliklerine en büyük tehlikeyi gölge BT'nin oluşturduğunu ifade ediyor. Güney Afrika'daki kurumların %33'ü gölge BT'yi en büyük ikinci tehdit olarak görürken Türkiye'deki kurumların yalnızca %17'si "gölge BT"yi başta gelen bir tehdit olarak sınıflandırıyor. Bunun yanı sıra, veri esnekliği ve gizlilik yasaları; Orta Doğu, Türkiye ve Afrika bölgesindeki bazı ülkelerde bulut teknolojisinin benimsenmesinde görülen artış; deneyimli güvenlik kaynaklarının eksikliği ve maliyet optimizasyonu, güvenlik operasyon merkezi yatırımlarının arkasındaki önemli itici güçler olmaya devam ediyor.

Suudi Arabistan ve Katar siber saldırıları tanımlamak ve müdahale etmek için çoğunlukla üçüncü bir tarafın uzaktan yönettiği güvenlik operasyon merkezlerine odaklanırken özellikle BAE ve Türkiye'deki telekomünikasyon ve finans kurumları kendi güvenlik operasyon merkezlerini işletmeyi tercih ediyor. Sahra Altı Afrika'da bazı bankalar, devlet kurumları ve perakende kurumları da kendi bünyelerinde

güvenlik operasyon merkezleri kurmuş durumda. Bununla birlikte, özellikle Güney Afrika'daki büyük kurumların başka hizmetlerle birlikte paket halinde sunulan güvenlik operasyon merkezi hizmetlerine talebi her geçen yıl artıyor. Bu güvenlik operasyon merkezleri genel olarak log korelasyonu, izleme ve olay raporlama gibi geleneksel özelliklere sahip fakat kurumlar, EDR, MDR hizmetleri ve entegre tehdit istihbaratı çözümlerine artan bir ilgi gösteriyor.

Orta Doğu, Türkiye ve Afrika bölgesindeki güvenlik operasyon merkezleri siber olgunluk eğrisinde geliştikçe, pazarda SOC ekiplerinde yer alan yetenekli yeni ve eski çalışanların eğitimi de dahil olmak üzere, gelişmiş güvenlik operasyon merkezi çözüm ve hizmetlerinin benimsenmesinde artış yaşanacak. Güvenlik operasyon merkezlerinin artan siber olgunluğu, kurumların SOC alanındaki eksiklerini gidermeyi ve güvenlik yaklaşımlarını güçlendirmeyi hedefleme motivasyonlarının devam etmesini sağlayacak.

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 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.