ADEO
CYBER SECURITY

2024
Tehdit Raporu

İÇİNDEKİLER

ADEO Hakkında

Şirketlerin ve kurumların siber güvenlik problemlerini tek başlarına çözemeyecekleri, yanlarına alacakları doğru bir müttefikle başarıya ulaşabilecekleri herkes tarafından kabul edilen bir gerçek. ADEO Cyber Security, bu anlayış çerçevesinde şirketlerin ve kurumların aktif siber savunma stratejilerini geliştirirken ihtiyaç duyacakları teknoloji, uzmanlık ve süreçlere ilişkin tüm başlıklarda hizmet vermek üzere 2008 yılında kuruldu.

ADEO, siber güvenlikte güvenilir bir müttefik olarak müşterileriyle aynı safta yer alıyor ve siber savunma hatlarını güçlendirecek stratejileri kurgulayarak hayata geçiriyor. Bunu yaparken maksimum verimliliği göz önünde bulunduran ADEO, derinlemesine uzmanlık gerektiren siber saldırı (ofansif), siber savunma (defansif), siber dayanıklılık yetenekleri ve teknoloji tedariği dahil olmak üzere 7x24 esasına dayalı kapsamlı siber güvenlik servisleri sunuyor.

ADEO, müşterilerinin altyapısını çok iyi bilen ve daha önce bu altyapılara yönelik siber saldırılara karşı pek çok kez müdahalede bulunmuş 180'in üzerinde çalışandan oluşan uzman kadrosuyla hizmet veriyor.

Pasif Değil Aktif

Saldırganlar artık zararlı kod kullanmaktan kaçınıyorlar. Tespit edilen saldırıların neredeyse %70'inde hiçbir zararlı kod kullanılmıyor. Bu nedenle yalnızca imza tabanlı pasif teknolojilerin ötesinde yüksek görünürlük sunan, siber güvenlik uzmanları tarafından aktif bir şekilde savunulan süreçlere geçilmesi gerekiyor.

Statik Değil Dinamik

Saldırganlar artık çok daha hızlı hareket ediyorlar. Bir sisteme ilk giriş aşamasından ele geçirme aşamasına kadar geçen süre ortalama bir buçuk saate indi.
Bu durum, siber istihbaratla beslenen dinamik tehdit avcılığına dayalı korunma yaklaşımının önemini artırıyor.

Kesintili Değil Sürekli

Siber saldırılar günün herhangi bir saatinde gerçekleşebiliyor. Hatta siber saldırganların, saldırıya karşı koyma riskini azaltmak için özellikle mesai dışı saatleri seçtikleri biliniyor. Bu yüzden siber savunma süreçlerinin 7x24 işletilmesi büyük önem taşıyor.

ADEO Yönetilen Tespit ve Müdahale (MDR) Servisi

Yönetilen Tespit ve Müdahale Hizmetleri (MDR), siber saldırıları mümkün olan en hızlı şekilde tespit etmek ve saldırıya hemen müdahale etmek için yürütülen çalışmalardır.

MDR, kuruluşunuz içinde tespit edilen tehditleri uzaktan izler, algılar ve yanıt verir. Bunun için hizmet sağlayıcı bir uç nokta tespit ve müdahale (EDR) aracı kullanır ve bu sayede uç noktadaki güvenlik olaylarına ilişkin gerekli görünürlük sağlanmış olur.

Gerekli görünürlük sağlandıktan sonra uç noktalardan elde edilen telemetri verileri merkez konsolda toplanır. Burada tehdit istihbarat verileri ve gelişmiş analitik yardımıyla hızlı şekilde şüpheli olayın tespiti yapılır ve müdahalesi gerçekleştirilir.

Bu araçlar MDR ekibi tarafından tespit edilen saldırıların;
- Yüksek oranda doğruluk payına sahip olmasına,
- İlgili siber olay öncesi ve sonrasında nelerin meydana geldiğinin detaylı şekilde görülebilmesine,
- Siber saldırıdan hemen sonra bu saldırıyı hızlıca önlemek için yapılacakların planlanmasına olanak sağlamaktadır.

Bu sayede hem bilinen hem de bilinmeyen siber saldırılara karşı kurumlar direnç kazanmaktadır.
MDR Analistleri gerçek zamanlı siber olay tespiti yapabilir ve tespit edilen bu siber saldırılar ile ilgili çok hızlı aksiyon alabilir.

Hızlı doğrulama ve aksiyon alma yetenekleri, gelişmiş siber saldırıların müdahalesinde çok ciddi önem taşımaktadır.

MDR; tehdit avı, izleme ve müdahale gerçekleştirmek için teknoloji ile insan uzmanlığını birleştiren bir **siber güvenlik** hizmetidir.

ADEO Yönetilen Tespit ve Müdahale (MDR) Servisi

EDR (Endpoint Detection and Response
Uç Nokta Tehdit Algılama ve Yanıt)

Uç noktalarda çalışan tüm işlemleri ve bunların yapmış olduğu aktiviteleri kayıt altına alarak, atomik indikatörlerin yanı sıra davranışsal indikatörlere göre tespit ve tehdit avcılığı imkanı sağlayan ve gerektiğinde şüpheli aktivitelere ait kanıtların toplanabildiği ya da şüpheli aktivitelere müdahale edebilen araçlardır.

XDR (Extended Detection and Response
Genişletilmiş Tespit ve Müdahale)

EDR araçlarına ek olarak başta network olmak üzere cloud, kimlik yönetimi, e-posta güvenliği gibi çeşitli kaynaklardan da kayıtlar analiz edebilen araçlardır.

ADEO 2024 Tehdit Raporu: 2024 Yılının Siber Güvenlik Analizi

Bu rapor, siber güvenlik alanındaki deneyimiyle sektörde öncü konumundaki ADEO'nun 2024 yılındaki verileri ele alarak hazırladığı kapsamlı bir analizin sonucudur.

Amacı, sektördeki güvenlik uzmanlarının, işletmelerin ve bireylerin, karşılaştığımız güvenlik tehditlerini anlamalarına yardımcı olmaktır.

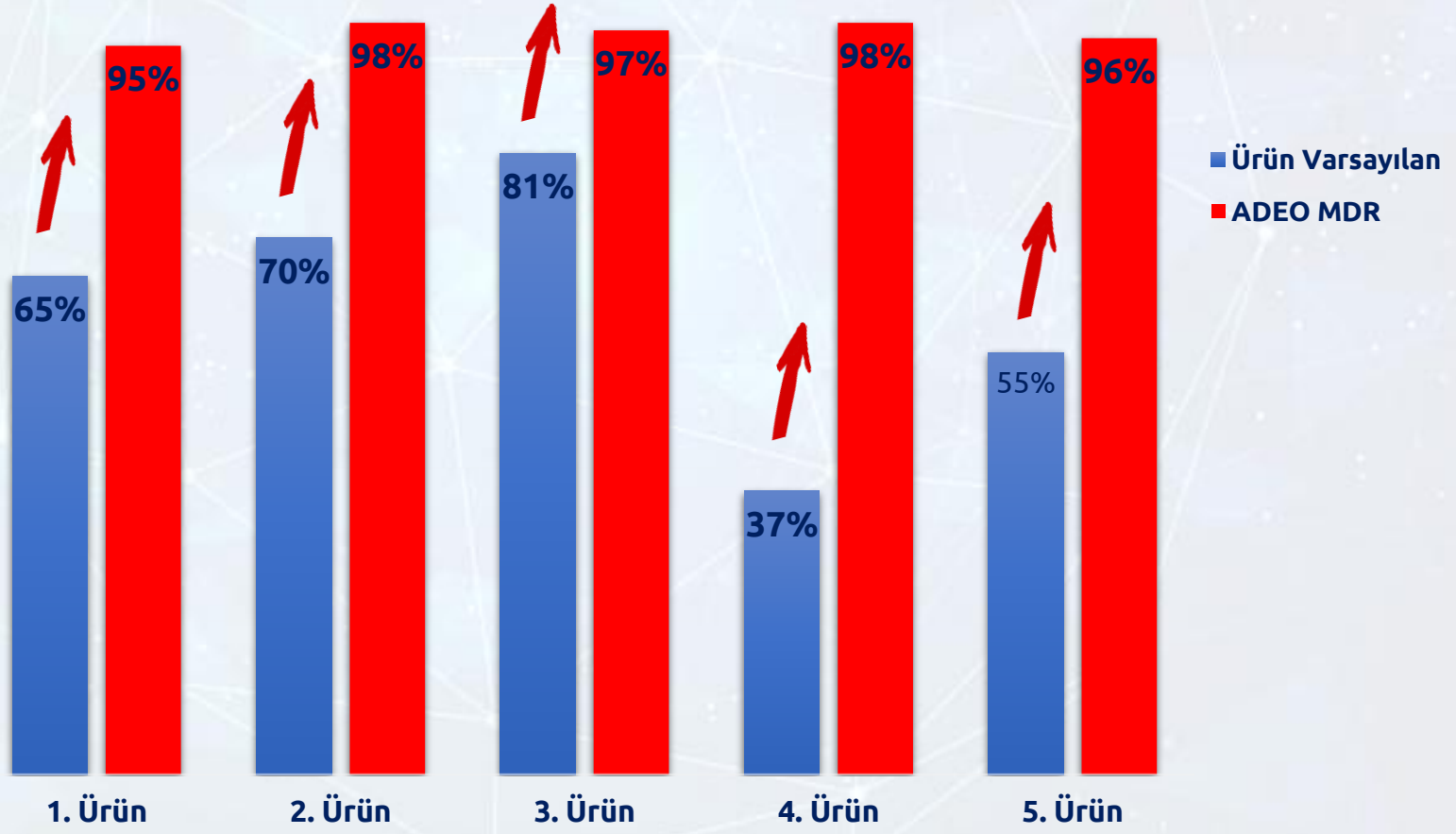
Raporda, önemli tehditlerin tespit edilmesi, bu tehditlerin nasıl ortaya çıktığı ve gelecekteki riskleri yönetmek için alınabilecek önlemler hakkında ayrıntılı bilgi sunulmaktadır.

ADEO 2024 Tehdit Raporu; kurumların ve bireylerin, siber güvenlik savunmalarını güçlendirme ve onları dijital varlıklarını korumaya yönelik bilinçlendirme ve bu hususta önlemler geliştirmelerine yardımcı olmak için, konusunda uzman bir ekip tarafından yapılan kapsamlı analizler doğrultusunda hazırlanmıştır.

2024 Yılında Neler Yaptık ?

Adeo MDR Ekibi özel olarak geliştirdiği kurallar sayesinde sistemlerini koruduğu müşterilerinin yatırım yaptığı EDR/XDR ürünlerinin tespit yeteneklerini **düzenli olarak arttırdı.**

İyileştirme çalışmaları yapılan EDR/XDR tespit mekanizmalarının, yapılandırma faaliyetleri ve sisteme eklenen kural çalışmaları sonrasında etkilerinin hangi oranda arttığı grafik ile sunulmuştur.



2024 Yılında **En Çok** Hedef Alınan Sektörler ve Bu Sektörlerdeki Toplam Vakalar

Holding
4 Saldırı

Havacılık
4 Saldırı

2024 Yılında **En Çok** Alarm Alınan Gün

ALARM; Siber saldırıları tespit etmek için kullanılan güvenlik araçlarına düşen uyarı mesajlarına denir.
Bu alarmlar kritiklik seviyelerine göre gruplandırılır.

27 Haziran

Alarm Sayısı 5969

Toplam Geliştirilen Kural Sayısı

Ocak 2024'te **5,000 olan tespit kuralı** sayısı yıl sonunda **5,500'e** çıkarıldı.

Ocak 2024'te **120,000** olan **IOC sayısı** yıl sonunda **175,000'e** çıkarıldı.

İçeriden ve dışarıdan sağlanan tehdit istihbaratı ile taranan **IOC sayısı: 175,000**

5500+

ADEO'nun tespit kurallarının olgunluk seviyesi, sürdürülebilir ve etkili bir güvenlik altyapısına olanak sağlıyor.

En Çok Kullanılan İlk Erişim Tekniği:

Saldırganın çeşitli zafiyetlerden faydalanarak sisteme ilk erişimi sağlayıp, hedeflerine ulaşarak diğer taktik ve teknikleri kullanmaya başlamasına **ilk erişim tekniği** denir.

Phishing

%64,28

MDR Ekibinin Günlük Rutini

İncelenen alarmların elde edilen verilere göre **%99.8**'i ADEO MDR ekibi tarafından müşteriye bildirilmeksizin analiz edildi ve kullanılan ürünün olgunluğuna göre gerekli **müdahale prosedürleri** uygulandı.

Bu sayede müşterilerimiz güvenli bir şekilde günlük iş akışlarına odaklanabilmektedirler.
Yapılan analizler ve alınan aksiyonlar raporlanır, belirli periyotlarda müşterilere iletilir.

ADEO MDR ekibi günde ortalama **5** kadar **yeni tespit kuralı** yazmaktadır. Buna ek olarak yanlış pozitif **(false positive)** olarak değerlendirilen kurallar özelinde ise **sıkılaştırma/iyileştirme** çalışmaları yapılır.

Alarmların **%0.02**'si teyit edildi ve
onay alındıktan sonra gerekli aksiyonlar uygulandı.

Tespit edilen **IP** ve **Domain**, **istihbarat servisleri** tarafında kontrol edilir ve
ağ içerisinde iletişimde olduğu makineler incelenerek **IP bloklama** işlemi yapılır.

Zararlı yazılım tespit edilmesi sonucunda aktiviteler **tehdit avcılığı** yaklaşımıyla incelenerek zararlı yazılım yayılan makineler **izole edilir** ve **gerekli aksiyonlar** alınır.

TRUE POSITIVE ALARM
Gerçek bir saldırı ya da istenmeyen/illegal davranış belirten alarmlardır.

FALSE POSITIVE ALARM
Yapılan analizler sonucunda gerçek bir saldırıya işaret etmediği belirlenen ya da hatalı yazılan kurallar doğrultusunda oluşan alarmlardır.

Yönetilen Tespit ve Müdahale Vaka Yönetim Aşamaları

VAKA

Tespit edilen gerçek bir alarmın analiz edilmesi sonucunda derinlemesine analiz ve olay müdahalesi süreçlerinin işletilmesini gerektiren saldırgan aktiviteleridir.

Saldırganların sıfırıncı gün (Zero-day) zafiyetlerini sömürmeleri ya da çalışanlara ait parola/kullanıcı adı bilgilerini ele geçirmeleri gibi bazı ilk erişim teknikleri sonrasında olay müdahale prosedürleri işletilmesi gerekmektedir.

ADEO MDR ekibi tarafından güvenliği ihlal edilmiş makinelerin araştırılması ve tespit edilmesi ile ilgili çalışmalar yürütülmektedir. **MDR tespit aşaması şüpheli aktivitenin sistemler üzerinde görülüp tanımlanmasını içerir.**

EDR, NDR, SOAR vb. güvenlik ürünlerinden ve MDR analistlerinin yetkinliklerinden faydalanılarak tespit edilen olası acil ve kritik anomali hareketlerin medyan tespit süresi **(Dwell Time) 5 dakika 55 saniye**'dir.

Çeşitli güvenlik ürünleri vasıtasıyla tespit edilen **şüpheli aktiviteler 7x24x365 gün ADEO MDR analistleri tarafından detaylı olarak incelenir.**

Müdahale aşaması, analiz sonucunda zararlı olarak tespit edilen aktivitelerin durdurulması, engellenmesi ve aktivitenin kurum içerisinde yayılmaması için alınan aksiyonlardır.

2024 yılı içerisinde ADEO MDR ekibinin acil ve kritik vakalara medyan müdahale süresi **15 dakika 41 saniye** olarak ölçülmüştür.

İyileştirme aşaması, tehdit oluşturan durumların ortadan kaldırılması, iyileştirilmesi ve tekrarlanmamasına yönelik önlemleri kapsamaktadır.

Gerçekleştirilen Müdahale Sayısı

14

VAKA YÖNETİM AŞAMALARI

GÜVENLİK İHLALİ TESPİT
ANALİZ
MÜDAHALE
İYİLEŞTİRME

Tespit ve Müdahale Süresi

Medyan (mean) Tespit Süresi
5dk 55s

Medyan (mean) Müdahale Süresi
15dk 41s

Yıllık Alarm Sayıları ve Seviyeleri

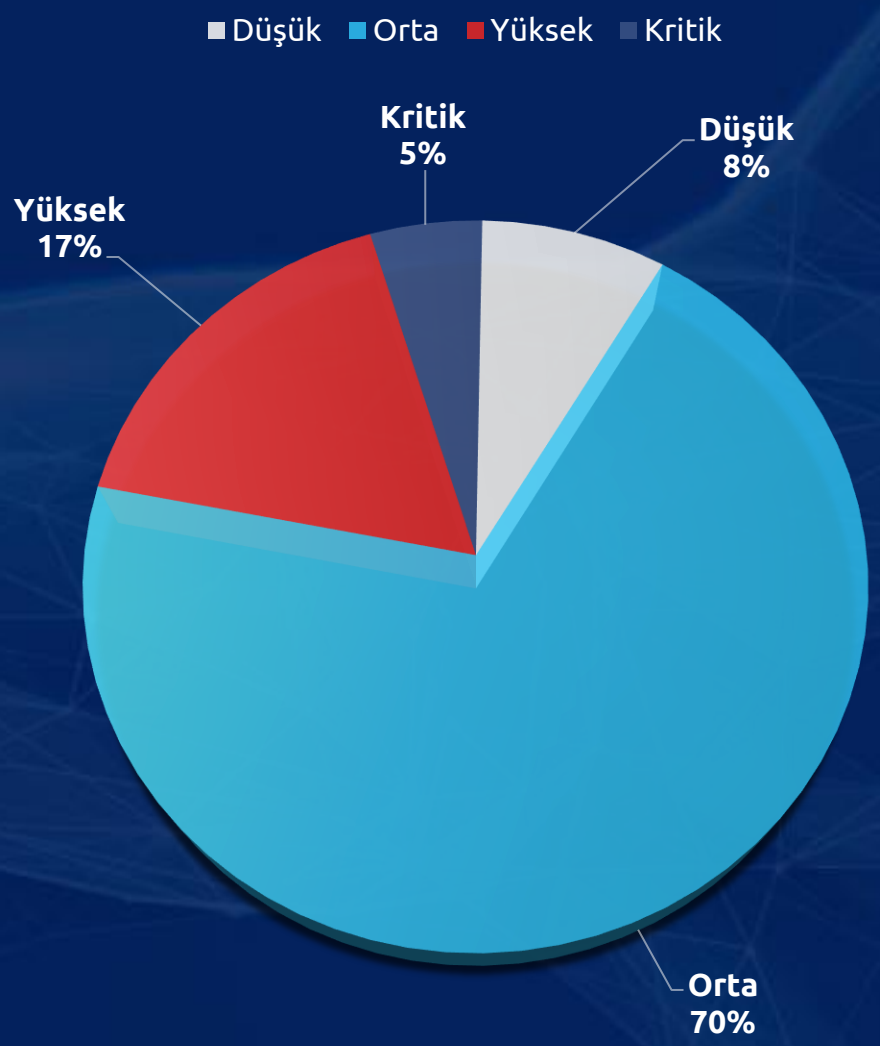
2023 yılında en yoğun gün alınan alarm sayısı **3886** iken, bu sayı **2024** yılının en yoğun gününde **5969** olarak raporlanmıştır.

ADEO'nun kural geliştirme ve iyileştirme çalışmaları sürekli olarak devam etmektedir.

Bu çalışmalar kapsamında 2025 yılı hedefi, Kritik ve yüksek seviyeli alarm sayılarının düşürülmesi ve gerçek pozitif alarm sayılarının artırılmasıdır.

Yıllık Alarm Sayıları ve Seviyeleri

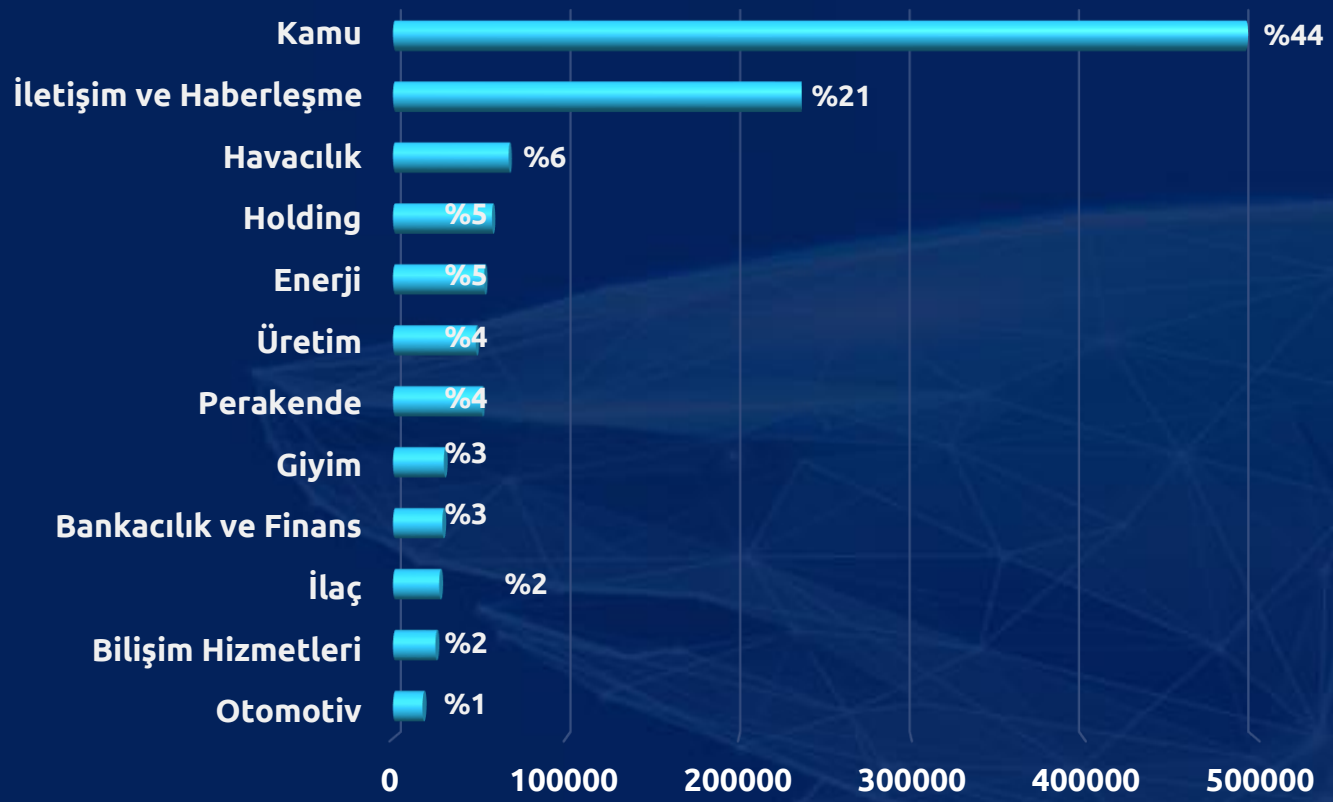
Sadece yüksek ve kritik seviyedeki alarmların medyan tespit süresi;
5 dakika 55 saniye,
medyan müdahale süresi ise
15 dakika 41 saniye
olarak ölçülmüştür.



TESPİT SÜRESİ
Saldırının gerçekleşmesi ile saldırının MDR ekibi tarafından görülüp saldırı olarak tanımlanması arasında geçen süreye denir.

MÜDAHALE SÜRESİ:
Saldırının gerçekleşmesi ile, ilgili saldırının MDR Ekibi tarafından görülüp tanımlanmasının ardından gerekli aksiyonun alındığı zaman aralığına denir.

Alarmların Sektörlere Göre Dağılımı



En Çok Alarm Gözlenen Sektörler:

HABERLEŞME

Telekomünikasyon ve internet hizmetleri, diğer tüm sektörlerin altyapısını destekleyen kritik sistemlerdir. Servis kesintileri büyük ölçekli etkilere yol açabilir ve özellikle DDoS saldırıları, veri sızıntıları ve yetkisiz erişim girişimleri bu sektörü hedef almaktadır. Ayrıca, kullanıcı verileri ve iletişim ağlarının korunması, ulusal güvenlik açısından da büyük önem taşımaktadır.

KAMU

Devlet kurumları, büyük miktarda hassas vatandaş verisi barındırır ve kritik altyapılara sahiptir. Bu da onları devlet destekli saldırılar, casusluk girişimleri ve fidye yazılımları için cazip bir hedef haline getirir. Ayrıca kamu sistemlerindeki eski teknolojiler ve geniş ağ yapıları, saldırganlar için ek fırsatlar sunar.

Bu nedenlerle, kamu ve iletişim sektörleri, siber saldırganların en çok odaklandığı alanlar arasında yer almakta ve sürekli olarak gelişen tehditlerle karşı karşıya kalmaktadır.

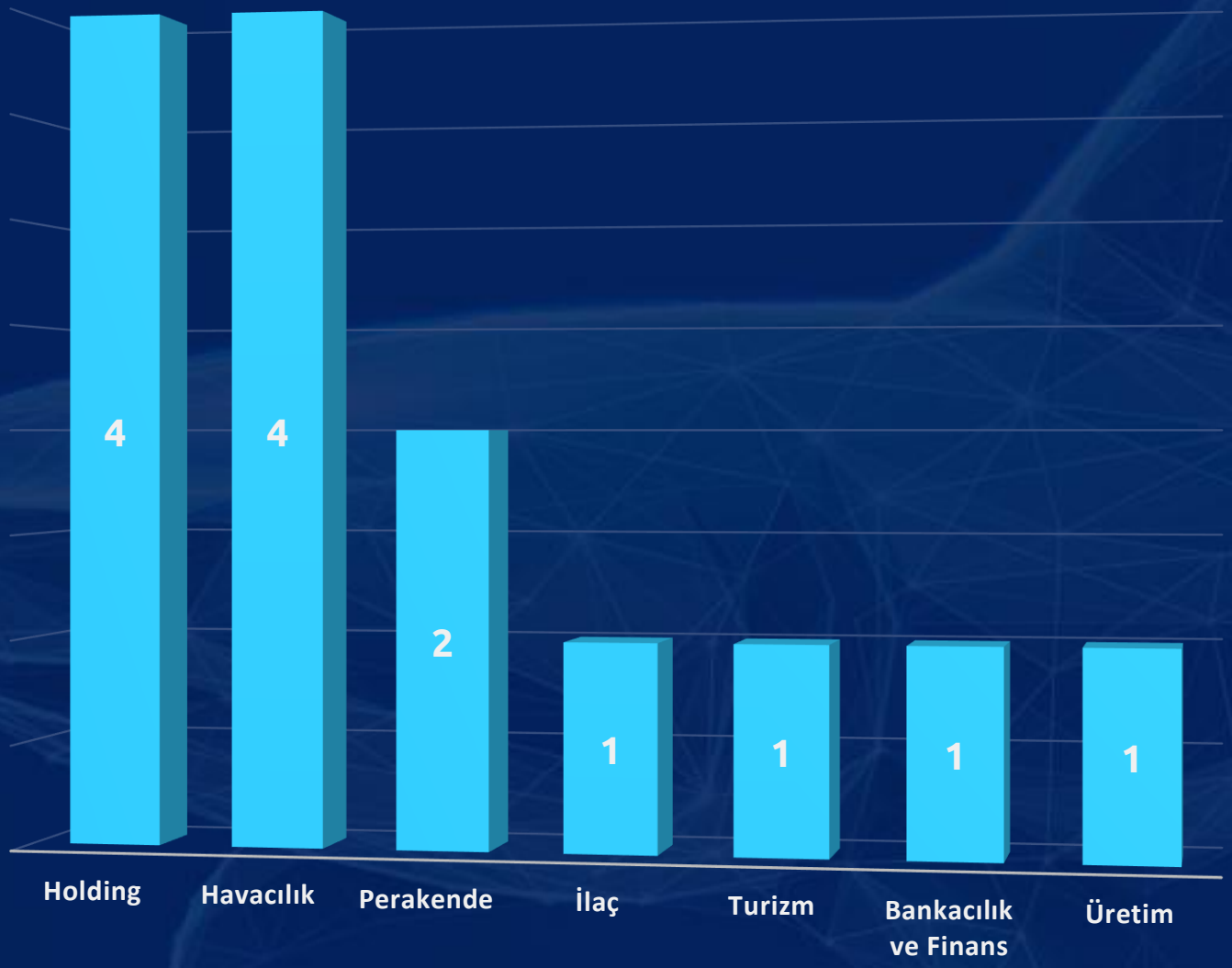
En Çok **Vaka** Gerçekleşen Sektörler

Neden Havacılık Sektörü &Holding?

Havacılık sektörü, kritik altyapıya sahip olması, yüksek değerli veriler işlemesi ve operasyonlarının kesintiye uğratılmasının büyük etkiler yaratması nedeniyle siber saldırganların hedefi olmuştur.

Holdingler ise geniş operasyon ağları, finansal kaynakları ve iştirakleri nedeniyle saldırganlar için cazip hedeflerdir.

Ayrıca, bu sektörlerde tedarik zinciri güvenliği zorlukları ve çalışanlar üzerinden yapılan saldırılar da riskleri artırmaktadır.



2024 Yılında Yaşanan Önemli Güvenlik Zafiyetleri & Sayılarla ADEO MDR Servisi Kural Çalışmaları

2024 yılında yayınlanan önemli **Top 20+** güvenlik açığı hakkında ADEO MDR olarak yazdığımız kurallar ve eklediğimiz IOC'lerin sayısı bir sonraki sayfada tabloda gösterilmiştir. Buradan da görüleceği üzere siber olayların sayısı her geçen gün artmaktadır.

Meydana gelen siber atakların detayına indiğimizde, bu atakların tespit edilme oranı önceki saldırıların tespit edilme oranına göre düşüktür. Ürünlerin kendi tespit yeteneklerine ek olarak, yeni çıkan saldırıların tespiti için proaktif güvenlik çözümlerine ihtiyaç bulunmaktadır.

"Yeni çıkan saldırıların tespiti için proaktif güvenlik çözümlerine ihtiyaç bulunmaktadır."

Bu noktada siber tehdit istihbaratı kaynaklarından yapılan düzenli araştırmalar sonucu elde edilen tehdit göstergelerinin bloklanması ve bu kaynaklardan elde edilen saldırıların analiz edilip ilgili saldırıların tespitine dair kuralların geliştirilmesi ve yazılan kuralların laboratuvar ortamlarımızda test edilmesi sonrasında ADEO kural veri tabanına eklenerek müşterilerimizin sistemleri üzerinde yaygınlaştırılması sağlanmaktadır.

Tehdit algılama ve istihbarat analistlerimiz yeni çıkan güvenlik açıkları hakkında düzenli olarak araştırmalar yapmaktadırlar. Zafiyetler teknik olarak incelenip laboratuvar ortamlarında test edildikten sonra tespit edilen IOC'ler ve gözlemlenen farklı paternler özelinde atak yüzeyinin görünürlüğünü artırmak için birden fazla kural seti geliştirilmektedir.

2024 Yılında Yaşanan Önemli Güvenlik Zafiyetleri & Sayılarla ADEO MDR Servisi Kural Çalışmaları

Güvenlik Açığı	Yazılan Kural Sayısı	Ürünlere Eklenen IOC Sayısı
AnyDesk Hacked - Signature	4	30
Lockbit Targeted Turkey in March	15	230
CVE-2024-3094 XZ Backdoor	2	63
CVE-2017-3506 Oracle WebLogic	-	87
CVE-2024-4577 PHP - CGI Argument Injection	-	116
CVE-2024-6387 RegreSSHion Vulnerability	5	34
APT40 Advisory by FBI	5	10
Void Banshee APT Exploits Microsoft Zero-Day in Spear-Phishing Attacks	3	11
China-linked APT17 Targets Italian Companies with 9002 RAT	2	8
FIN7Cybercrime Gang EDR Bypass	3	119
APT41 Has Arisen From the DUST	9	28
New ShadowRoot Ransomware Attacking Business Via Weaponized PDF's	5	22
Kematian Stealer	4	20
CROWDSTRIKE_BSOD_scams	1	355
BlankBot Banking Trojan	-	20
2018-0824 RCE Vulnerability exists in "Microsoft COM for Windows"	-	76
Palo Alto Networks PAN-OS CVE-2024-0012 and CVE-2024-9474	-	20
CVE-2024-47575 FortiManager Zero-Day Exploitation	-	5
CVE-2024-28986 SolarWinds Web Help Desk (WHD) Java Deserialization RCE	1	-
CVE-2024-38063 Windows TC/IPv6 RCE	1	-
CVE-2024-6409 Red Hat Enterprise Linux 9 OpenSSH	-	28
Brokewell Banking Trojan	-	32

2024 Yılında ADEO MDR Servisi Kural Çalışmaları

İlgili güvenlik zafiyetleri ve saldırıları hakkında geliştirilen kurallar ve MDR güvenlik analistleri yetkinlikleri ile düzenli periyotlarla müşterilerimizin sistemleri üzerinde tehdit avcılığı gerçekleştirilmektedir.

Potansiyel siber saldırıların gerçekleşmesi öncesinde ilgili zafiyetin veya saldırı göstergelerinin tespiti yapılmaktadır.

Yapılan tespit sonrasında, gereken önlem ve aksiyonlar alınarak, konu özelinde kuruma bilgilendirmeler yapılır.

Saldırı ile ilgili kurallar müşteri sistemlerine eklenerek, MDR güvenlik analistleri tarafından 7x24x365 gün boyunca izlenmektedir.

MDR raporlarıyla müşterilerimize tespit edilen bulguların detayları düzenli olarak paylaşılmaktadır.

"Saldırı ile ilgili kurallar müşteri sistemlerine eklenir ve müşteri sistemleri ADEO MDR güvenlik analistleri tarafından 7x24x365 gün boyunca izlenir."

Güvenlik analistleri tarafından izlenmekte olan müşteri sistemlerine kurallar eklendikten belli bir süre sonra ilgili zafiyetin istismar edilmesine dair alarmlar analistler tarafından tespit edilmektedir.

Yapılan incelemeler doğrultusunda siber atakların istismarı, geliştirilen kurallar ve IOC'ler aracılığı ile engellendikten sonra analistler tarafından zafiyete sebebiyet veren kök neden (root cause) araştırılmaktadır.

Analizler sonrasında elde edilen bulgu ve IOC verileri ile ADEO tehdit istihbarat kaynağı güncellenmektedir. Saldırılara ait elde edilmiş istihbarat veri setleri düzenli olarak müşterilerimizin sistemlerine eklenmektedir.

Böylelikle eklenen IOC ve istihbarat verileri ile tüm müşteri sistemleri üzerinde ilgili güvenlik açığının istismar edilmesinin önüne geçilmektedir.

2024 Yılında ADEO MDR Servisi Kural Çalışmaları

Saldırganların sistemlere nüfuz edip, kalıcılık sağlama sürelerinin dakikalara indiği bu günlerde, hedefli veya hedefsiz, bu tip tehditleri bertaraf edebilmek için en etkili yöntem; bilgili, becerili ve tecrübeli MDR analistlerinin çalıştığı bir MDR hizmetidir.

MDR hizmetinin de en temel işi, tehditleri en kısa sürede tespit etmek ve sonrasında hızlı ve doğru müdahale ile tehdidin etkisini en aza indirmektir.

XDR/EDR ürünleri, modern saldırı ve saldırganlar ile yaptığımız bu amansız kedi fare oyununda elimizdeki en güçlü silahlardır. Bu savaşta başarılı olunabilmesi için EDR/XDR ürünleri ile gerçekleştirilen tespit ve müdahale sürelerinin **20 dakikanın** altına inmesi gerekmektedir.

Her ne kadar günümüz EDR/XDR çözümleri siber tehdit ve saldırıları tespit etme konusunda gayet başarılı olsalar da, ne yazık ki yeterli değiller.

ADEO MDR ekibinin yapmış olduğu çalışmalar sonucunda elde edilen verilere bakıldığında, EDR/XDR tespit mekanizmalarının iyileştirilmesi gerektiği belirlenmiştir.

EDR/XDR çözümlerinin kurum/kuruluş yapısına, karşılaşabileceği tehdit ve saldırılara göre iyileştirilmesi, güncel tutulması, en iyi yapılandırma faaliyetlerinin gerçekleştirilmesi ve özellikle güncel tehditleri hedefleyen EDR/XDR kurallarının sistemlere eklenmesi yüksek önem arz etmektedir.

ADEO MDR kapsamında izlenen yüzbinlerce uç tarafından oluşan alarmların incelenmesi ile ve ADEO DFIR ekibinin müdahale ettiği yüzlerce siber güvenlik olayından topladığı taktik ve operasyonel siber tehdit istihbarat verisi kullanılarak oluşturulan EDR/XDR kuralları, bu tespit mekanizmalarının etkisini artırmaktadır.

Bu sayede ADEO MDR ve DFIR ekipleri, doğrudan sahadan alınan doğru ve kesin bilgiler ile oluşturulan EDR/XDR kuralları tespit seviyelerini gözle görülür oranda artırmakta ve tespit ve inceleme süreleri **6 dakikanın altına** inebilmektedir.

2024 Yılında ADEO MDR Servisi Kural Çalışmaları

Siber Güvenlikte Proaktif Yaklaşım: ADEO MDR Ekibi

Günümüzün dijital dünyasında siber güvenlik kritik önem taşımaktadır. Siber saldırılar her geçen gün artmakta ve daha karmaşık hale gelmektedir. Bu nedenle, siber tehditlere karşı proaktif bir yaklaşım benimsemek hayati önem taşımaktadır.

ADEO olarak, siber güvenliğe büyük önem veriyoruz. Müşterilerimizi siber saldırılara karşı korumak için MDR (Managed Detection and Response) hizmeti sunuyoruz. MDR ekibimiz, çıkan her zafiyeti yakından takip ediyor ve tespit edilemeyen ataklara karşı sürekli kural geliştiriyor.

Geliştirilen kurallar sayesinde, müşterilerimizi proaktif olarak koruyor ve sistemlerinin güncel kalmasını sağlıyoruz. Bu sayede, siber saldırıların neden olabileceği veri kaybı, finansal kayıp ve itibar zedelenmesi gibi riskleri en aza indiriyoruz.

ADEO MDR ekibinin proaktif yaklaşımının faydaları:

Daha hızlı tespit ve yanıt:
Ekibimiz, gelişmiş tehdit avı teknikleri ve yapay zeka kullanarak siber saldırıları daha hızlı tespit ediyor ve anında müdahale ediyor.

Daha iyi koruma:
Sürekli güncellenen kurallar sayesinde, müşterilerimiz en son siber tehditlere karşı korunmuş oluyor.

Azaltılmış risk:
Proaktif yaklaşımımız, siber saldırıların neden olabileceği riskleri en aza indiriyor.

Daha fazla huzur:
Müşterilerimiz, siber güvenliklerinin ADEO'nun uzman ekibi tarafından sağlandığını bilmenin rahatlığıyla işlerine odaklanabiliyor.

Kural Setinde Sürdürülebilir Büyüme ve Olgunlaşma Analizi: ADEO 2024 Perspektifi

Siber güvenlik altyapımızın kural seti gelişimini incelediğimizde, önceki yıllarda parabolik bir artış gözlemlenmiştir:

2021: 600'den 2.000'e (%233 artış)
2022: 2.000'den 4.000'e (%100 artış)
2023: 4.000'den 5.000'e (%25 artış)
2024: 5.000'den 5.500'e (%10 artış)

Bu yavaşlayan artış trendi aslında kural setimizin olgunlaşma sürecinin doğal bir sonucudur.

Başlangıçtaki hızlı büyüme, temel tehditleri kapsama ve geniş bir savunma yelpazesi oluşturma ihtiyacından kaynaklanıyordu.

2024'te gözlemlenen daha düşük artış oranı **(%10)** ise kural setimizin optimize edilmiş bir olgunluk seviyesine ulaştığının göstergesidir.

Bu yavaşlayan büyümenin arkasındaki temel nedenler:

- **Mevcut kuralların yüksek tespit (detection) oranı,**
- **MITRE ATT&CK çerçevesinin kapsamlı şekilde korunması,**
- **False positive oranlarının minimize edilmesi,**
- **Kural optimizasyonu ve iyileştirme çalışmalarının sonuç vermesi.**

Artık odak noktamız, kural sayısını artırmak yerine:

Mevcut kuralların etkinliğini optimize etmek,
Yeni tehdit vektörlerine özel, hedefli kurallar eklemek,
Kurallar arası korelasyonu güçlendirmek,
Tespit (Detection) kalitesini daha da yükseltmek.

Bu yaklaşım, siber güvenlik operasyonlarımızın verimliliğini maksimize ederken, gereksiz alarm yükünü minimize etmemizi sağlamaktadır.

Kural setimizin geldiği bu olgunluk seviyesi, daha sürdürülebilir ve etkili bir siber güvenlik altyapısı sunmamıza olanak tanımaktadır.

ADEO
CYBER SECURITY

2024 Yılının **En Sıcak** Gündemi **#TOP 5**

2024 Yılının En Sıcak Gündemi
#TOP 1| CVE-2024-3094 XZ Backdoor

XZ Nedir?

XZ, birçok Linux dağıtımında kullanılan genel amaçlı bir veri sıkıştırma formatıdır. Büyük dosyaları daha küçük boyutlara sıkıştırarak taşınabilirlik sağlar.

CVE-2024-3094 XZ Backdoor Zafiyeti Nedir Nasıl Çalışır?

Bu güvenlik açığı, XZ Utils'ın 5.6.0 ve 5.6.1 sürümlerini içeren çeşitli Linux dağıtımlarını etkilemiştir. Özellikle, Fedora 40 ve Rawhide, Debian'ın testing ve unstable sürümleri, OpenSUSE Tumbleweed ve Arch Linux gibi dağıtımlar bu durumdan etkilenmiştir.

Backdoor, XZ Utils'in derleme sırasında önceden oluşturulmuş bir nesne dosyasını (bad-3-corrupt_lzma2.xz) kullanarak liblzma kütüphanesindeki belirli işlevleri değiştirir. Backdoor, liblzma kütüphanesindeki işlevleri değiştirerek, bu kütüphaneyi kullanan uygulamaların davranışını manipüle eder.

Zafiyetin Bir Tehdit Aktörü Tarafından Kullanımı ve Etkileri:

CVE-2024-3094 zafiyeti, tehdit aktörlerinin manipüle edilmiş XZ Utils kütüphanesi üzerinden sistemlere arka kapı ekleyerek kalıcı erişim sağlamasına, güvenlik önlemlerini atlatmasına ve hassas verileri çalmasına olanak tanır. Bu zafiyet, tedarik zinciri saldırıları, APT kampanyaları ve zararlı yazılım yayılımı gibi geniş kapsamlı saldırı senaryolarında kullanılabilir. Manipüle edilen kütüphane, uygulama davranışlarını bozarak hizmet kesintilerine, veri manipülasyonuna ve sistem güvenliğinin zayıflamasına yol açabilir.

ADEO Olarak Oluşturduğumuz Özel Algılama Kuralları ve IoC'ler:

ADEO MDR Servisi **CVE-2024-3094 XZ Backdoor Zafiyeti** hakkında toplam **2 tespit kuralı ve 63 adet IOC'yi** müşteri ortamlarına aktarmıştır.

2024 Yılının En Sıcak Gündemi
#TOP 2| APT41 Has Arisen From the DUST

APT41 Has Arisen From the DUST:

APT41, gelişmiş bir tehdit aktörü (APT) olarak global çapta çeşitli sektörlere yönelik hedefli saldırılar gerçekleştiren bir siber casusluk grubudur. Grup, karmaşık araç setleri ve teknikler kullanarak uzun süreli ağ erişimi sağlayabilmekte ve hassas verileri çalabilmektedir. APT41, son dönemde aşağıdaki sektörlerde faaliyet gösteren kuruluşları hedef almıştır:

- Global taşımacılık ve lojistik sektörü
- Medya ve eğlence sektörü
- Teknoloji firmaları
- Otomotiv sektörü

Etkilenen bölgeler arasında İtalya, İspanya, Tayvan, Tayland, Türkiye ve Birleşik Krallık bulunmaktadır.

Tehdit Aktörünün Etkileri Nelerdir?

APT41 gibi gelişmiş bir tehdit aktörü, karmaşık araç setleri ve 0-day zafiyetlerini kullanarak hedef sistemlere sızabilir, hassas verileri çalabilir, uzun süreli kalıcılık sağlayabilir ve ağ içinde yanal hareket ederek diğer sistemleri ele geçirebilir. Bu saldırılar, veri ihlalleri, operasyonel kesintiler, finansal kayıplar, itibar zedelenmesi ve yasal yaptırımlar gibi ciddi sonuçlara yol açabilir.

ADEO Olarak Oluşturduğumuz Özel Algılama Kuralları ve IoC'ler:

ADEO MDR Servisi **APT41 Has Arisen From the DUST** hakkında toplam **9 tespit kuralı ve 28 adet IOC'yi** müşteri ortamlarına aktarmıştır.

2024 Yılının En Sıcak Gündemi
#TOP 3| CVE-2024-6387 RegreSSHion Zafiyeti

OpenSSH Nedir?

OpenSSH (Open Secure Shell), güvenli uzaktan bağlantılar ve veri aktarımı sağlayan açık kaynaklı bir araçtır. Güvenlik, esneklik ve kolay kullanım sağlamak amacıyla tasarlanan OpenSSH, genellikle Unix ve Linux sistemlerinde varsayılan olarak kullanılan bir protokoldür, ancak Windows dahil diğer platformlarda da kullanılabilir.

CVE-2024-6387 RegreSSHion Zafiyeti Nedir Nasıl Çalışır?

Bu zafiyet, OpenSSH'nin sinyal işleme mekanizmasındaki bir hatadan kaynaklanır. Sinyaller, işletim sistemleri tarafından process'lere belirli olayları bildirmek için kullanılır. OpenSSH, bu sinyalleri işlerken bir güvenlik açığına neden olan bir hata içerir. Bir istemci LoginGraceTime saniyeleri (varsayılan olarak 120, eski OpenSSH sürümlerinde 600) içinde kimlik doğrulaması yapmazsa, sshd'nin SIGALRM işleyicisi eş zamansız olarak çağrılır ve eş zamansız sinyal güvenli olmayan çeşitli işlevleri çağırır.

ADEO Olarak Oluşturduğumuz Özel Algılama Kuralları ve IoC'ler:

ADEO MDR Servisi **CVE-2024-6387 RegreSSHion Zafiyeti** hakkında toplam **5 tespit kuralı** ve **34 adet IOC 'yi** müşteri ortamlarına aktarmıştır.

2024 Yılının En Sıcak Gündemi

#TOP 4| CVE-2024-38063 Windows IPv6 TCP/IP RCE Zafiyeti

CVE-2024-38063 Windows IPv6 TCP/IP RCE Zafiyeti Nedir Nasıl Çalışır?

Windows'un özellikle IPv6 paketlerinin işlenmesi sırasında oluşan bir tam sayı taşması (integer underflow) hatasından kaynaklanır. Bu hata, saldırganların bellek taşmasına neden olarak sistem üzerinde rastgele kod çalıştırmasına imkan tanır.

Saldırı Vektörü:

Saldırganlar, hedef sisteme özel olarak hazırlanmış IPv6 paketleri göndererek bu zafiyeti istismar edebilirler. Bu saldırı, kullanıcı etkileşimi gerektirmeden gerçekleştirilebilir ve saldırganın hedef sistem üzerinde tam yetkiyle kod çalıştırmasına olanak tanır.

ADEO Olarak Oluşturduğumuz Özel Algılama Kuralları ve IoC'ler:

ADEO MDR Servisi **CVE-2024-38063 IPv6 TCP/IP RCE Zafiyeti** hakkında toplam **1 tespit kuralı** müşteri ortamlarına aktarılmıştır.

2024 Yılının En Sıcak Gündemi
#TOP 5|CVE-2024-49113 LDAPNightmare

LDAP Nedir?

LDAP (Lightweight Directory Access Protocol), ağ üzerindeki dizin hizmetlerine erişmek için kullanılan bir protokoldür. Özellikle kullanıcı bilgileri, gruplar ve diğer kaynaklar gibi bilgileri depolayan sistemlerde (örneğin, Active Directory) yaygın olarak kullanılır. LDAP, bilgileri hızlı ve verimli bir şekilde sorgulamak ve yönetmek için tasarlanmıştır.

CVE-2024-49113 LDAPNightmare Nedir?

CVE-2024-49113, Microsoft'un Windows işletim sistemindeki Basit Dizin Erişim Protokolü (LDAP) hizmetinde bulunan kritik bir hizmet dışı bırakma (DoS) güvenlik açığıdır. Bu açık, saldırganların özel hazırlanmış LDAP istekleri göndererek hedef sistemin çökmesine ve hizmet kesintilerine neden olmalarına olanak tanır.

Zafiyetin Etkileri:

Saldırı akışı, kurban sunucuya bir DCE/RPC isteği gönderilmesiyle başlar ve saldırgan özel olarak hazırlanmış bir Bağlantısız Hafif Dizin Erişim Protokolü (CLDAP) yönlendirme yanıt paketi gönderdiğinde Yerel Güvenlik Yetkilisi Alt Sistem Hizmetinin (LSASS) çökmesine ve yeniden başlatmaya zorlanmasına neden olur.

Bir Saldırgan Bu Güvenlik Açığından Nasıl Faydalanabilir?

Bu güvenlik açığından başarıyla yararlanan kimliği doğrulanmamış bir saldırgan, LDAP hizmeti bağlamında rastgele kod çalıştırma yeteneği kazanabilir. Ancak başarılı bir istismar, hangi bileşenin hedeflendiğine bağlıdır.

Bir LDAP sunucusu için bir etki alanı denetleyicisinden yararlanma bağlamında, saldırganın başarılı olabilmesi için hedefe özel olarak hazırlanmış RPC çağrıları göndererek saldırganın etki alanında bir arama yapılmasını tetiklemesi gerekir.

Bir LDAP istemci uygulamasından yararlanma bağlamında, saldırganın başarılı olabilmesi için kurbanı saldırganın etki alanı için bir etki alanı denetleyicisi araması yapmaya veya kötü niyetli bir LDAP sunucusuna bağlanmaya ikna etmesi veya kandırması gerekir. Ancak kimliği doğrulanmamış RPC çağrıları başarılı olmayacaktır.

ADEO Olarak Oluşturduğumuz Özel Algılama Kuralları ve IoC'ler:

ADEO MDR Servisi **CVE-2024-49113 LDAPNightmare Zafiyeti** hakkında toplam **2 tespit kuralı** müşteri ortamlarına aktarılmıştır.

Digital Forensics and Incident Response

ADEO Digital Forensics and Incident Response (DFIR) Servisi

Adli Bilişim, sayısal (dijital) verilerin delil toplama gereklerine uygun olarak elde edilme, muhafaza ve analiz süreçlerinin mahkemeye sunulma aşamasına kadar uygulanmasını kapsar.

Bu hizmet, bir siber olay sonrasında olayın sebebini ortaya çıkarmak adına sistemlerden sayısal delillerin toplanması, muhafaza edilmesi ve analiz edilmesi servisidir. Bu servis kapsamında toplanan sayısal deliller emanet zinciri prensibi göz önünde bulundurularak toplanmalı ve gerektiğinde adli makamlara sunulabilecek nitelikte olmalıdır.

Bu servis kapsamında toplanabilecek sayısal deliller ve bilgiler temelde şunlardan oluşur:

- **Siber saldırıdan etkilenen sistemlerin adli kopyaları**
- **Siber saldırıdan etkilenen sistemlerin hafıza imajları**
- **Siber saldırıdan etkilenen sistemler üzerinde yapılacak canlı incelemeyle elde edilecek uçucu veriler (çalışan uygulamalar, açık ağ bağlantıları vb.) veya olay müdahalesinde ihtiyaç duyulan diğer sayısal delil kaynakları (olay günlükleri, dosya sistemi kayıtları vb.)**
- **Siber olayın devam etmesi durumunda ağ üzerinden elde edilecek ham paket verisi veya ağ akış verileri**

Yukarıda listelenen delil türleri içinde bulunan ve siber olayların analizi sırasında başvurulan diğer delil türleri (örneğin işletim sistemi olay kayıtları, dosya sistemi kayıtları, ağ akış verileri vb.) bu servis kapsamında ihtiyaç duyulması halinde incelenir. İnceleme uluslararası kabul görmüş donanım ve yazılımların yer aldığı adli bilişim laboratuvarlarında ve yine uluslararası kabul görmüş sertifikalara sahip uzmanlar tarafından gerçekleştirilir.

ADEO DFIR ekibi, 2019 yılından itibaren; içerisinde finans, telekomünikasyon, kamu kurumu, enerji ve özel sektör olmak üzere **100'den** fazla kurum ve kuruluş için **400.000'den** fazla uç nokta üzerinde olay müdahalesi ve güvenlik ihlali tespiti gerçekleştirmiştir.

Tüm olay müdahale süreci uluslararası alanda kabul görmüş olay müdahale planları dahilinde gerçekleştirilmektedir.

Müdahale yapılan tüm vakalarda saldırgan grup tarafından kullanılan;

- Taktikler
- Teknikler
- Araçlar

tespit edilir ve detaylı bir şekilde analiz edilerek raporlanır.

Olay Müdahalesi sonucunda;

- İlgili saldırgan grubun erişimi etkilenen kurumdan kesilmiş ve engellenir.
- Alınması gereken kısa vadeli ve uzun vadeli aksiyon planı etkilenen kurumla paylaşılır.

ADEO Digital Forensics and Incident Response (DFIR) Servisi

2024 Yılında Müdahale Edilen Vakaların Sektörlere Göre Dağılımı

Vakalar Sırasında Görülen Temel Durumlar

Command Injection:
Sistemin komut satırına kullanıcı girdileri üzerinden kötü niyetli komutlar enjekte edilerek, saldırganın yetkisiz işlemler yapmasına olanak tanınır. Bu açık genellikle güvenli olmayan girdi kontrolünden kaynaklanır.

Credential Stealing/Accessing Admin Panel of Website:
Kullanıcı adı ve şifrelerin çalınmasıyla web sitelerinin yönetim panellerine yetkisiz erişim sağlanır. Saldırılar genelde keylogger, phishing ya da brute force yöntemleriyle gerçekleştirilir.

Permission Change:
Sistem ya da dosya izinlerinin değiştirilmesi, hassas verilere yetkisiz erişime yol açabilir. Çoğunlukla zayıf kullanıcı politikalarından veya insider tehditlerden kaynaklanır.

Miner:
Sistem kaynaklarının kötüye kullanılarak kripto para madenciliği yapılması. Özellikle yüksek işlem gücüne sahip sunucular hedeflenir ve sistem performansını ciddi şekilde düşürür.

Phishing:
Kurbanları kandırarak kimlik bilgilerini çalmak veya zararlı yazılımları bulaştırmak amacıyla sahte e-postalar veya web siteleri kullanılır. İnsan faktörünü hedef alan popüler bir saldırı tekniğidir.

RCE (Remote Code Execution):
Bir saldırganın uzaktan komut veya kod çalıştırmasını sağlayan kritik bir güvenlik açığıdır. Genelde kötü yapılandırılmış uygulamalardan veya eski yazılımlardan kaynaklanır.

Ransomware:
Kurbanın dosyalarını şifreleyerek, erişim sağlamak için fidye talep eden zararlı yazılım türüdür. Çoğunlukla phishing saldırıları veya güvenlik açıkları üzerinden yayılır.

SQL Injection:
Veritabanı sorgularına kötü amaçlı SQL komutlarının eklenmesiyle, saldırganların veri çekmesine veya manipüle etmesine olanak tanır. Zayıf giriş kontrolü en büyük etkendir.

USB Malware:
Fiziksel USB cihazları kullanılarak sistemlere zararlı yazılımlar yüklenir. Özellikle offline sistemleri hedef almak için yaygın olarak kullanılır.

Unauthorized Access:
Yetkisi olmayan kişilerin hassas belgelere erişim sağlaması. Genellikle zayıf erişim kontrolü veya insider tehditlerden kaynaklanır.

Karşılaşılan Vakalarda Saldırganlar Tarafından Kullanılan Taktik ve Teknikler:

Obfuscation:
Saldırganların, tespit edilme sürecinden ve güvenlik ürünlerinin alarm üretmesinden kaçınmak için kullandığı karmaşıklaştırma ve kafa karıştırma taktik ve teknikleridir. Saldırganlar, verileri kodlayabilir ve/veya gereksiz kod blokları ekleyerek zararlı yazılımları analiz eden kişilerin kafasını karıştırmayı hedefler.

Insider:
Saldırganların saldırıya uğrayan kurum bünyesinde çalışıyor olması veya saldırganların kurum bünyesinde çalışan kimseler ile anlaşarak kurum içerisindeki verileri sızdırması durumudur.

Vulnerability Exploitation:
Güncel güvenlik açıklarının ve 0day (sıfırıncı gün) adı verilen güvenlik açıklarının sömürülmesi durumuna denir. Güvenlik ürünlerinin kullanılmaması, ürünlerin düzenli olarak güncellenmemesi bu duruma sebep doğurur.

Lateral Movement:
Saldırganların SMB, LDAP, WMI gibi protokolleri kullanarak ele geçirdiği sistem üzerinden ortam içerisindeki diğer sistemlere yayılması olayıdır.

Discovery:
Saldırganların cihazlara saldırı öncesinde veya ortamda yayılabilmek için yaptıkları keşif işlemlerine denir. Hedef sistemleri tanımlamak, saldırılacak kişileri belirlemek gibi aşamalar içermektedir.

Persistence:
Saldırganların ele geçirdiği sistem üzerinde kalıcı hale gelebilmek için kullandıkları metotlara denir. Saldırganlar, Windows servisleri, zamanlanmış görevler gibi yapılar üzerine kurulmayı hedefleyebilir.

Karşılaşılan Vakalarda Saldırganlar Tarafından Kullanılan Taktik ve Teknikler:

Saldırganların 2024 Yılında En Çok Kullandığı İlk Erişim Metotları:

Credential Leak:
Saldırganların, daha önce sızdırılan kullanıcı verilerini kullanarak sisteme erişim sağlaması olayıdır.

CVE-2023-46604:
CVE-2023-46604, Apache ActiveMQ'nun OpenWire protokolünde bulunan bir deserialization açığıdır. Bu açık, ActiveMQ'nun çalıştığı sunucuda kod çalıştırmak için bir saldırgan tarafından istismar edilebilir.

CVE-2024-21887 ve CVE-2023-46805:
CVE-2023-46805, bir saldırganın kimlik doğrulama kontrollerini atlatmasına olanak tanıyan bir kimlik doğrulama atlama güvenlik açığıdır. CVE-2024-21887, bir saldırganın kimliği doğrulanmış bir yönetici gibi davranmasına ve özel olarak hazırlanmış rastgele komutlar aracılığıyla uzaktan kod yürütme (RCE) elde etmesine izin veren bir komut enjeksiyonu güvenlik açığıdır. Saldırganlar bu iki güvenlik açığını birleştirerek kimliği doğrulanmamış kod yürütme elde edebilir, bu da veri sızıntısı (kullanıcı kimlik bilgileri ve yapılandırma verileri dahil), yapılandırma değişiklikleri, dosya değiştirme, webshell dağıtımı ve daha fazlasına yol açabilir.

SQL Injection:
SQL Enjeksiyonu (SQLi), kötü niyetli SQL ifadelerinin yürütülmesini mümkün kılan bir enjeksiyon saldırısı türüdür. Bu ifadeler bir web uygulamasının arkasındaki bir veritabanı sunucusunu kontrol eder. Saldırganlar, uygulama güvenlik önlemlerini atlamak için SQL Enjeksiyonu güvenlik açıklarını kullanabilir.

Spear Phishing:
Spear Phishing, belirli bir kişiyi, grubu veya kuruluşu hedef alan bir oltalama saldırısı türüdür. Bu kişiselleştirilmiş dolandırıcılıklar, kurbanları hassas verileri ifşa etmeleri, kötü amaçlı yazılım indirmeleri veya bir saldırgana para göndermeleri için kandırır.

Insider:
Saldırganların saldırıya uğrayan kurum bünyesinde çalışıyor olması veya saldırganların kurum bünyesinde çalışan kimseler ile anlaşarak kurum içerisindeki verileri sızdırması durumudur.

Karşılaşılan Vakalarda Saldırganlar Tarafından Kullanılan Taktik ve Teknikler:

Saldırganların Para Kazanma Metotları:

Ransomware
Saldırganların sunucu içerisindeki kritik verileri şifreleyip, verilerin kurtarılması için şantaj yapması saldırısıdır.

Miner
Saldırganların sunucu kaynaklarını BTC, ETH, XMR gibi para birimlerini kazmak için sömürdüğü saldırıdır.

Data Theft
Saldırganların sunucu üzerinden çaldığı verileri çalıp, underground forumlarda satılığa çıkarması olayıdır.

Blackmailing
Saldırganların, kurum sahiplerine hizmetlerini keseceğine dair tehdit ve şantaj yaparak para talep etmesi olayıdır.

2024 Yılında En Çok Karşılaşılan APT Grupları:

ADEO DFIR ekibi tarafından 2024 yılında yapılan çalışmalarda çeşitli APT grupları ile karşılaşılmıştır. Bu APT gruplarının genel motivasyonunun ransomware (fidye yazılımı) saldırısı gerçekleştirmek olduğu tespit edilmiştir.

İlgili APT grupları listedeki gibidir:

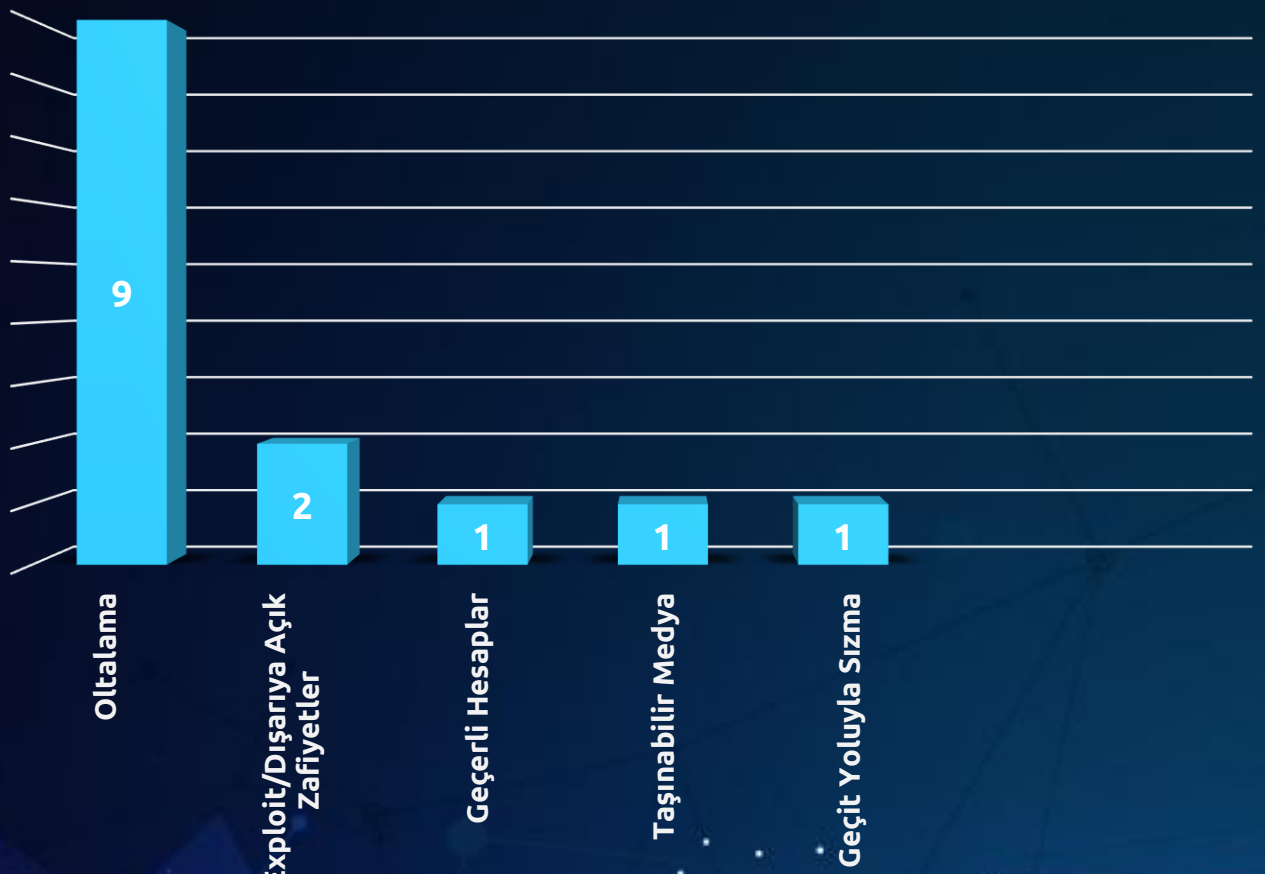
- Lockbit Ransomware
- Conti Ransomware
- SeXi APT Inc Ransomware
- Mimic (N3ww4v3)
- Phalcon Ransomware

APT grupları tarafından 2024 yılı içerisinde en çok hedef alınan sektörler:

- Bankacılık ve Finans
- Üretim
- Bilişim Hizmetleri
- Eğitim
- Sağlık
- Turizm
- Havacılık
- Vakıf

ADEO MDR Servisi
Taktikler, Teknikler ve Tespit Kurallarımız

En Çok Kullanılan İlk Erişim Teknikleri



Bir saldırganın ortamda yer edinebilmesi **ilk erişim (initial access)** ile başlar.

Güvenliği ihlal edilmiş hesapların kimlik bilgileri, çeşitli tekniklerle ele geçirilerek ağ içindeki sistemlerde farklı kaynaklara uygulanan erişim denetimlerini atlamak için kullanılabilir.

Saldırgan ilk erişimin ardından hedeflere ulaşmak için diğer taktik ve tekniklere geçiş yapabilir. Dolayısıyla **ilk erişimin engellenmesi sistemin güvenliği açısından önem arz etmektedir.**

Saldırı Tespit Kurallarımız

Siber Güvenlikte Zirve: ADEO'nun %96'lık Başarısı!

Siber saldırılar her geçen gün artmakta ve daha karmaşık hale gelmektedir. Bu nedenle günümüzde siber güvenliğe yatırım yapmak ve proaktif bir şekilde korunmak her zamankinden daha önemli hale geliyor.

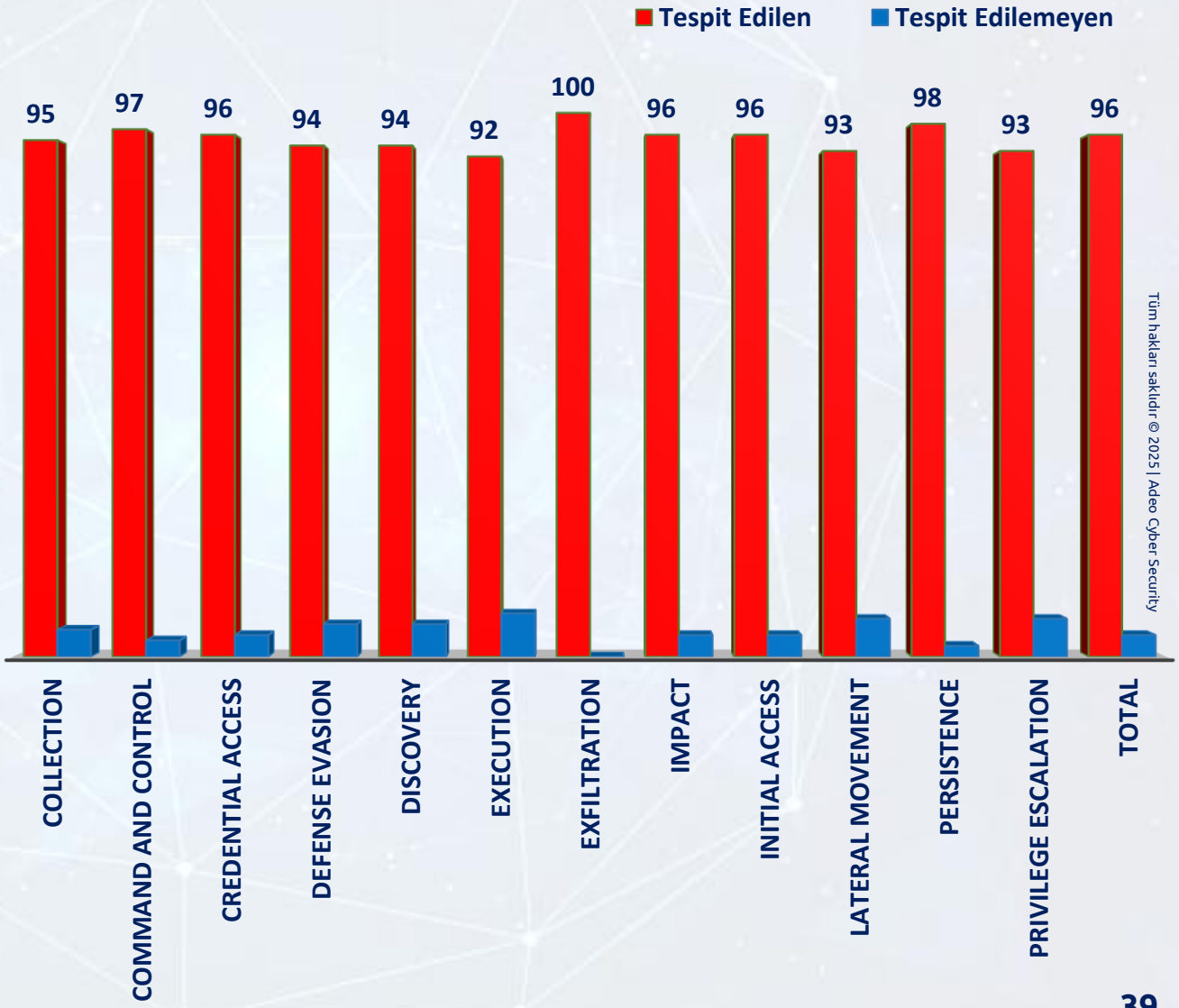
ADEO olarak, siber güvenlik yaklaşımlarımızda müşterilerimizi siber saldırılara karşı korumak için;

- En son teknolojiyi,
- Konusunda en yetkin uzman analistlerin deneyimleriyle kullanıyoruz.

%96'lık tespit(detection) oranıyla sunduğumuz servis hizmeti bu konudaki uzmanlığımızın somut verilerinden biri olarak 2024 raporunda yerini alıyor.

2024 yılında gerçekleşen **2592 adet aksiyon** sonrasında, **12 MITRE ATT&CK TTP değeri** referans alındığında, ortalama **%96 tespit(detection) oranına** sahip olduğumuz görülüyor.

Son 4 yıldır, MITRE ATT&CK TTP sayısı artmasına rağmen, aktif kural geliştirme çalışmalarımız sayesinde bu oran **%96** seviyesinin üzerinde kalmaya devam ediyor.



1.Veri Toplama (Collection)

Tespit (detection) araçlarından kaçınmak ve analiz sürecini yavaşlatmak için bir Anti-Forensics yöntemi olarak saldırgan, amacına uygun verileri toplamaya çalışır.

Bu taktik, saldırganın amacına hizmet eden verileri toplamak için kullandığı tekniklerden oluşur.

Genellikle hedef alınan kaynaklar arasında çeşitli sürücü tipleri, tarayıcılar, ses ve video dosyaları ve e-postalar bulunur.

Ekran görüntüsü alma, klavye girişi takip etme yaygın yöntemler arasındadır.

Veri Toplama (Collection) taktiği kullanılarak yapılan saldırıların %95'i ADEO MDR Servisi tarafından tespit edilebilmektedir.

Bu ve benzeri saldırıların tespiti için **EDR teknolojisine ek olarak**, veri kaybı önleme sistemlerinin uygulanması önerilir. Saldırı riski, etkisi ve derecesinin azaltılması gibi kontrolleri planlamak ve politikaların sürekliliğinin sağlanması gibi çalışmalar için ek veri sızıntısı engelleme sistemi olan **DLP** teknolojisi kullanılması tavsiye edilir.

Sıkıştırılmış veya şifrelenmiş dosyaların sızdırılma teşebbüslerini engellemek ve **kullanıcı davranış analizlerini (UBA)** yapabilmek için **XDR, NDR, Firewall, DLP** vb. teknolojilerin kullanılması tavsiye edilir.

Kullanıcı farkındalığının artırılması için düzenli periyotlarda **farkındalık eğitimlerinin** organize edilmesi önem arz etmektedir.

Kullanılan sistem imajlarının ve **yazılımlarının güncel tutulması** tavsiye edilir.

Exchange ortamında, yöneticilerin kötü amaçlı olabilecek otomatik iletme, indirme ve açma gibi etkinliklerini engellemek için **Exchange** kurallarının sıkılaştırılması gerekmektedir.

Dışarıdan erişime açık e-posta sunucuları için **çok faktörlü kimlik doğrulamasının (MFA)** kullanılması saldırıları büyük oranda azaltacaktır.

%95

2.Komuta ve Kontrol (Command And Control)

Saldırgan kontrolü ele geçirmek için güvenliği ihlal edilmiş sistemlerle iletişim kurmayı dener. Bunu yaparken tespit edilmekten kaçınmak için genellikle normal, beklenen trafiği taklit etmeye çalışır.

Komuta ve Kontrol (C&C), saldırganların kendi kontrolleri altındaki sistemlerle bir hedef network aracılığı ile iletişim kurduğu tekniklerden oluşur.

Saldırganın komuta ve kontrol taktiğini oluşturmasının, saldırı altındaki network'ün yapısına ve savunmasına bağlı olarak çeşitlilik gösteren birçok yolu vardır.

Komuta ve Kontrol (Command and Control) taktiği kullanılarak yapılan saldırıların %97'si ADEO MDR Servisi tarafından tespit edilebilmektedir.

Bilinen kötü veya şüpheli etki alanlarına (Domain) giden/gelen **web trafiğinin** izlenmesi gerekmektedir.

DNS isteklerinin; bilinmeyen, güvenilmeyen veya bilinen kötü etki alanlarına ve kaynaklara **firewall üzerinden filtrelenmesi** tavsiye edilir.

Bu ve benzeri saldırıların tespiti için EDR'a ek olarak **Firewall, NDR, IDS/IPS**; kullanıcı davranışı analizleri için **UBA** tabanlı ürünlerin kullanılması tavsiye edilir.

Network'te oluşan **trafiğin izlenmesi** ve içeriden dışarıya giden ve dışarıdan gelen **IP'lerin istihbarat servisleriyle sürekli olarak kontrol edilmesi** gerekmektedir.

Sisteme yüklenebilen uygulamaların onay mekanizmasından geçmesi ve izin verilen uygulamalar listesinde **(White List)** olması zorunlu kılınmalıdır. Bilgisayar sisteminiz herhangi bir uygulamanın çalıştırılmasına veya yüklenmesine izin vermemelidir. Bilinmeyen kaynaklardan uygulamaların **yüklenmesini engelleyerek,** C2 kanalları oluşturmak için kullanılan **kötü amaçlı yazılımların sisteminize yüklenmesini önleyebilirsiniz.**

%97

3.Kimlik Bilgileri Erişimi (Credential Access)

Saldırgan bu taktik ile hesap adlarını ve parolalarını çalmayı dener.

Kimlik bilgilerini almak için kullanılan yaygın teknikler arasında keylogging ve kimlik bilgisi dökümü (Credential Dumping) bulunur.

Meşru kimlik bilgilerinin kullanılması, saldırganların sisteme erişmesini sağlayabilir, tespit edilmelerini zorlaştırabilir ve hedeflerine kolay ulaşmalarına yardımcı olacak daha fazla hesap oluşturmalarına olanak sağlar.

Kimlik Bilgileri Erişimi (Credential Access) taktiği kullanılarak yapılan saldırıların %96'sı ADEO MDR Servisi tarafından tespit edilebilmektedir.

WAF, kuruluşlar tarafından web sistemlerini sıfırıncı gün istismarlarına, uzaktan komut çalıştırmaya, diğer bilinen ve bilinmeyen tehdit ve güvenlik açıklarına karşı koruma sağlayan yaygın **bir güvenlik kontrolü olup**, **kurum içinde konumlandırılması** önem arz etmektedir

Parolaların farklı platformlarda kullanılmaması, parolanın **en fazla 1 veya 3 aylık periyotlarda** değiştirilmesi ve özel karakter barındırmasına dikkat edilmesi gerekmektedir. **Gereksiz/fazla yetkilendirmeden kaçınılması**, personel işten çıktıktan sonra mevcut hesaplarının kapatılması önem arz etmektedir. **Dosya paylaşımları** yalnızca gerekli kullanıcılara erişimi olan **belirli dizinler ile sınırlandırılmalıdır.**

Kritik kaynaklara erişim izinlerine sahip kullanıcıların hesaplarının güvenli bir şekilde yönetilmesi **için Ayrıcalıklı Erişim Yönetimi – Privileged Access Management (PAM)** ürünlerinin kurum içinde konumlandırılması tavsiye edilir.

Başta VPN ve E-posta erişimleri olmak üzere, mümkün olan bütün girişlerde **MFA aktif edilmesi** önem arz etmektedir.

VLAN kullanılarak departmanların birbirinden izole edilmesi ile olası tehlikelerin en aza indirilmesi konusu önem arz etmektedir. Başta Domain Controller sunucuları olmak üzere **kimlik bilgilerinin barındırıldığı** uygulamaların **güvenlik güncellemelerinin** düzenli periyotlarda yapılması tavsiye edilir.

%96

4.Savunmayı Atlatma (Defense Evasion)

Saldırgan tespit edilmekten kaçınmaya çalışır.

Savunmayı Atlatma, saldırganların yarattıkları tehlike boyunca tespit edilmekten kaçınmak için kullandıkları tekniklerden oluşur.

Savunmayı Atlatma için kullanılan teknikler arasında güvenlik yazılımının kaldırılması/devre dışı bırakılması veya veri ve komut dosyalarının gizlenmesi/şifrelenmesi yer alır.

Saldırganlar ayrıca kötü amaçlı yazılımlarını gizlemek ve maskelemek için güvenilir süreçleri kötüye kullanır.

Savunmayı Atlatma (Defense Evasion) taktiği kullanılarak yapılan saldırıların %94'ü ADEO MDR Servisi tarafından tespit edilebilmektedir.

PowerShell ve **Command Prompt** komut satırı uygulamaları aracılığı ile yapılan aktivitelerin analiz edilebilmesi için ilgili uygulamaların loglarının merkezi bir noktada kaydedilmesi/arşivlenmesi önerilir. Hizmet engelleme saldırılarından **(DoS / DDoS)** korunmak ve atak türlerini minimize etmek için **Load Balance** (Yük Dengeleme), **DDoS Protection**, ürünlerinin kurum içinde konumlandırılması tavsiye edilir.

Kullanıcı **ayrıcalıklarının sınırlandırılması** önerilir. Yalnızca yetkili kullanıcılar hizmet değişiklikleri yapabilecek şekilde sınırlanmalıdır. Dosya indirme dizinleri ve geçici dosya (Temporary Files) dizinleri gibi kullanıcı dizinlerinden **yürütmenin engellenmesi** önerilir.

Saldırganlar, kötü amaçlı kodu gizlemek için derlenmiş **HTML dosyalarını (.chm)** kötüye kullanabilir. CHM dosyaları genellikle Microsoft HTML yardım sisteminin bir parçası olarak dağıtılır. CHM dosyaları **VBA, JScript, Java ve ActiveX** gibi çeşitli içeriklerin sıkıştırılmış derlemeleridir. **Application whitelist** yazılımları ile bu tarz yaygın kullanılmayan **script uzantılarının** çalıştırılması **engellenebilir ya da tespit edilebilir**.

Kurum içinde **ihtiyaç duyulmayan uygulamaların** güvenlik açığı verebilecek özelliklerinin **devre dışı bırakılması/kaldırılması** önerilir.

E-posta yolu ile yapılan **oltalama saldırılarının** önlenmesi için **Sandbox** türevi teknolojilerin ve **Email Security Gateway** ürünlerinin konumlandırılması, kullanılan **uygulama envanterlerinin** düzenli periyotlarda **güvenlik güncelleştirmelerinin yapılması** önem arz etmektedir.

%94

5.Keşif (Discovery)

Saldırgan hedefini tanımaya, keşfetmeye çalışır.

Keşif, saldırganın sistem ve dahili network hakkında bilgi edinmek için kullanabileceği tekniklerden oluşur. Bu teknikler, saldırganın nasıl hareket edeceğine karar vermeden önce çevreyi gözlemlemesine ve planına yön vermesine yardımcı olur ve saldırgana ayrıca neyi kontrol edebileceği ve giriş noktalarının çevresinde neler olabileceği konusunda fikir verir, fayda sağlar.

Keşif (Discovery) taktiği kullanılarak yapılan saldırıların %94'ü ADEO MDR Servisi tarafından tespit edilebilmektedir.

Kurumlarda var olan ortam (**Active Directory, Firewall, Network Segmentasyon** ve varsa diğer güvenlik cihazlarının yardımı ile) ihtiyaca uygun şekilde sıkılaştırılarak, **atak yüzeyi daraltılmalıdır**. Ortamlar üzerinde çalışan **Audit** ve **Log seviyelerinin sıkılaştırılması ve olgunlaştırılması** tavsiye edilir.

Keşif ve olası sömürü riskini önlemek için varlık envanterlerinin belirli periyotlarda incelenmesi, **gereksiz bağlantı noktalarının, hizmetlerin ve servislerin kapalı** olduğundan emin olunması gerekmektedir.

Uzaktan hizmet taramalarını algılamak ve önlemek için **IPS/IDS teknolojilerinin** kullanılması tavsiye edilir.

Birçok önemli bilgi, Windows Yönetim Araçları ve PowerShell gibi Windows sistem yönetim araçları aracılığıyla da edinilebilir. Sistem ve ağ bilgilerini toplamak için gerçekleştirilebilecek bu tarz eylemleri tespit edebilmek için **Windows event logları** yapılandırılmalı ve merkezi olarak toplanmalıdır.

Varlık envanterinde olan uygulamaların **güvenlik güncelleştirmeleri** düzenli periyotlarda kontrol edilmelidir.

Kullanıcı hesap yönetimi sağlanmalı, **minimum ayrıcalık ilkesi** uygulanmalıdır.

%94

6. Yürütme (Execution)

Yürütme, yerel veya uzak bir sistemde saldırganın kontrolündeki kodun çalıştırılmasını sağlayan tekniklerden oluşur.

Kötü amaçlı kod çalıştıran teknikler, bir network'ü keşfetmek veya veri çalmak gibi daha geniş hedeflere ulaşmak için genellikle diğer tüm taktiklerdeki tekniklerle eşleştirilir. Örneğin bir saldırgan, uzaktan sistem keşfi yapan bir Powershell betiğini çalıştırmak için bir uzaktan erişim aracı kullanabilir.

Yürütme (Execution) taktiği kullanılarak yapılan saldırıların %92'si ADEO MDR Servisi tarafından tespit edilebilmektedir.

Kullanıcı, kötü amaçlı bir dosyayı veya bağlantıyı açarak kötü amaçlı kod yürütmek için sosyal mühendislik saldırısına maruz kalabilir. Bu tür saldırıları önlemek için son kullanıcı tarafındaki e-posta ya da internet tarayıcı **uygulamalarının denetiminin ve güncellemesinin düzenli periyotlarda yapılması gerekmektedir.**

Saldırganların **RCE zafiyetinden yararlanmalarını** engellemek ya da tespit etmek için **NGFW** veya **NDR** ürünleri ile ağ trafiği üzerindeki görünürlük artırılmalıdır.

Kurumlarda var olan ortam **(Active Directory, Firewall, Network Segmentasyon ve varsa diğer güvenlik cihazlarının yardımıyla)** ihtiyaca uygun şekilde sıkılaştırılarak, **atak yüzeyi daraltılmalıdır**. Ortamlar üzerinde çalışan **Audit** ve **Log seviyelerinin** sıkılaştırılması, olgunlaştırılması ve **SIEM** teknolojilerinin kullanılması tavsiye edilir.

Dışarıya açık sunucularda bulunabilecek bir **RCE zafiyeti** saldırganın kolaylıkla kurum ağına girmesini sağlayacaktır. **Zero Trust** güvenlik stratejisi ile dışarıya açık sunuculardan içeriye ya da diğer sunuculara **yapılan erişimler, ağ erişim kontrolü (NAC) araçları ile sınırlandırılmalı ve takip edilmelidir.**

%92

7.Veri Kaçırma (Exfiltration)

Veri Kaçırma, saldırganların ağınızdan veri çalmak için kullandığı tekniklerden oluşur. Saldırganlar verileri topladıklarında tespit edilmekten kaçınmak için onları sıkıştırma ve şifrelemeyi içerebilecek biçimde paketler.

Hedef bir ağdan veri elde etme teknikleri, tipik olarak, verinin kendi komuta ve kontrol kanalı veya alternatif bir kanal üzerinden aktarılmasını içerir. Ayrıca aktarıma boyut sınırları da koyulabilir.

Verilerin ağdan ayrılabilmesi için tasarlanmış bir çıkış noktasından geçmesi gerektiğinden, tipik olarak C2 algılaması için yararlı olan imza tabanlı virüsten koruma özelliklerine sahip, **yeni nesil bir güvenlik duvarı (NGFW)** veya trafik protokollerini görebilen ağa izinsiz giriş önleme sistemi **(IPS) sızıntıyı tespit etmeye ve önlemeye yardımcı olabilir.**

DLP, kullanıcı tarafından hassas verilere yetkisiz olarak erişimi ve bu verilerin kullanımını izler. Verilerin dışarı çıkmasını önlediği için kullanılması tavsiye edilir.

Saldırganlar, **USB üzerinden** zararlı kodu çalıştırarak, ağ üzerinden yayılırlar. Bazı durumlarda bir kullanıcı tarafından tanıtılan bir **USB aygıtı aracılığıyla veri kaçırma** gerçekleşebilir. USB aygıtı, son veri kaçırma noktası olarak veya başka şekilde bağlantısız sistemler arasında geçiş yapmak için kullanılabilir. Bunun önüne geçebilmek için **farkındalığın düşük olduğu yerlerde usb portlarının devre dışı bırakılması önerilir.**

Saldırgan, verileri tek parça göndermek yerine **dosyaları parçalayarak gönderebilir**. Bu şekilde minimum yükleme boyutunu aşmadan verinin iletimini sağlar. Saldırıyı önlemek için **network trafiğinin sürekli olarak izlenmesi** önerilir.

Veri Kaçırma (Exfiltration) taktiği kullanılarak yapılan saldırıların %100'ü ADEO MDR Servisi tarafından tespit edilebilmektedir.

%100

8.Etki (Impact)

Saldırgan, sistemlerinizi ve verilerinizi manipüle etmeyi, kesmeyi veya yok etmeyi dener.

Etki, saldırganların iş ve operasyonel süreçleri manipüle ederek kullanılabilirliği bozmak ve bütünlüğü tehlikeye atmak için kullandığı tekniklerden oluşur.

Etki için kullanılan teknikler verileri yok etme veya bozmayı içerebilir. Bazı durumlarda iş süreçleri iyi görünebilir, sorunsuz durur ancak saldırganın hedeflerine fayda sağlayacak şekilde değiştirilmiş olabilir.

Bu teknikler saldırganlar tarafından nihai hedeflerine ulaşmak veya bir gizlilik ihlalini örtmek için kullanılabilir.

Etki (Impact) taktiği kullanılarak yapılan saldırıların %96'sı ADEO MDR Servisi tarafından tespit edilebilmektedir.

Fidye yazılımı, sistem ve ağ kaynaklarına **erişimi kesmek** için hedef sistemlerdeki veya bir ağda bulunan çok sayıda sistemdeki verileri şifreleyebilir. Saldırıları önlemek için **felaket senaryoları hazırlanarak yedekler alınması** ve bu yedeklerin saldırganlar tarafından erişilmez hale getirilmesi önerilmektedir.

DDoS saldırısında; saldırıya uğrayan kaynağın, birden çok makineden gelen isteğe maruz kalmasıyla kapasiteyi aşarak yanıt vermemesi ile hizmet engelleme saldırısı başarıyla sonuçlanır. **DDOS önlemek için** trafiği filtreleyerek **İçerik Dağıtım Ağları (CDN)** veya **DoS** azaltma konusunda uzmanlaşmış sağlayıcılar tarafından sağlanan **DDoS önleme hizmeti alınması** önerilmektedir.

Veri Manipülasyonu: Saldırganlar, farklı sonuçlar ile faaliyetlerini gizleyerek verileri ekleyebilir, silebilir. Bu şekilde rakibinin verilerini manipüle ederek bir iş sürecini, organizasyonel anlayışı veya karar vermeyi etkilemeye çalışabilir. Oluşabilecek maddi kayıpları önlemek için **veriyi şifreleme, saklama yöntemi ve DLP** çözümlerinin kullanılması önerilir.

Man in the middle saldırısı ağda iki bağlantı arasındaki iletişimin dinlenmesi ile çeşitli verilerin ele geçirilmesi veya iletişimi dinleyip yanıltıcı bir iletişim oluşturarak verinin manipüle edilmesi şeklinde gerçekleşen bir saldırı yöntemidir. **MitM** saldırı türlerini önlemek için **SSH, IPSec protokollerinin, HTTPS destekli sitelerin kullanılması**, **public** ortamlarda paylaşılan şifresiz **WIFI ağlarına bağlanmamaya** dikkat edilmesi önemlidir.

%96

9.Kalıcılık (Persistence)

Kalıcılık, saldırganın sistem erişiminin sürekliliğini sağlamayı hedefleyen tekniklerden oluşur.

Kalıcılık için kullanılan teknikler, meşru kodu değiştirme/ele geçirme veya başlangıç kodu ekleme gibi sistemlerde yerlerini korumalarına izin veren tüm erişim, eylem ve yapılandırma değişikliklerini içerir.

Kalıcılık (Persistence) taktiği kullanılarak yapılan saldırıların %98'i ADEO MDR Servisi tarafından tespit edilebilmektedir.

NDR, tüm bağlantı ve protokollerde size şeffaflık sağlar. Bağlantıları, akışları, paketleri ve meta verileri gerçek zamanlı olarak analiz etmek için trafiği derinlemesine tarar ve geriye dönük analiz yapar. **Algılanan bir tehdidin çözüm süresini en aza indirmek için** entegre bir **network algılama ve müdahale** çözümü kullanılması tavsiye edilir.

Önleme: Haftalık olarak ağda olan tüm cihazlar için **zararlı yazılım taraması** yaptırılması önem arz etmektedir. Ayrıca belirli aralıklarla **güvenlik ihlali analiz ve değerlendirme (Compromise Assessment)** çalışması yapılmalıdır.

Saldırganlar çeşitli zafiyetler barındıran varlıklarda **uzaktan komut çalıştırarak**, sistemlerde **sistem kapatma/yeniden başlatma** işlemi yaparak verilerin bozulmasına, e-ticaret ve hastane gibi ortam ve yerlerde maddi zararlara ve can kayıplarına sebebiyet verebilir. Bu ve benzeri atak türlerinin önlenebilmesi için **Extended Detection and Response (XDR), Firewall, Backup (yedekleme)** teknolojilerinin kullanılması tavsiye edilir.

Korsan/Cracklenmiş program, oyun, işletim sistemi gibi yüklemeler sisteminizi ciddi saldırıların hedefi yapabilir. Kurumların fidye, veri ihlali, arka kapı gibi saldırılara maruz bırakılmasına yol açabilir. Bu ve benzeri saldırılar genellikle **kullanıcı farkındalığının az olmasından** kaynaklanır. Bu sebeple çalışanlara düzenli periyotlarda **temel güvenlik eğitimlerinin** verilmesi tavsiye edilir.

%98

10.Yetki Yükseltme (Privilege Escalation)

Yetki Yükseltme, saldırganın bir sistem veya ağ üzerinde daha üst düzey izinler elde etmek için kullandığı tekniklerden oluşur. Saldırganlar genellikle ayrıcalıksız erişime sahip bir ağa girip keşif yapabilir ancak hedeflerini takip edebilmek için artırılmış izinlere ihtiyaç duyar. Yaygın yaklaşımlar, sistem zayıflıklarından, yanlış yapılandırmalardan ve güvenlik açıklarından yararlanmaktır.

Yükseltilmiş erişim örnekleri şunları içerir; Sistem/ Kök seviyesi (Root Level) Domain yöneticisi (Domain Administrator),Yerel yönetici (Local Administrator) Yönetici benzeri erişime sahip kullanıcı hesabı (admin-like access), Belirli bir sisteme erişimi olan veya belirli bir işlevi yerine getiren kullanıcı hesapları

Bir saldırganın varlığını sürdürmesine izin veren işletim sistemi özellikleri yükseltilmiş bir bağlamda yürütülebildiğinden, bu teknikler genellikle “Persistence (Kalıcılık)” taktiği ile örtüşür.

Yetki Yükseltme (Privilege Escalation) taktiği kullanılarak yapılan saldırıların %93’ü ADEO MDR Servisi tarafından tespit edilebilmektedir.

Active Directory (AD) veya LDAP gibi dizin sunucularından gelen logların yapılandırılması gerekmektedir. Kullanıcı hak yükseltme veya yeni kullanıcı oluşturma olaylarının takip edilmesi gerekmektedir. **Yetkili kullanıcı** hesap adlarının, yetkilerinin bir **listesinin oluşturulması** gerekmektedir. **Kimlik tabanlı güvenlik (Identity-based Security)** ürünleri kullanılarak yetki yükseltme saldırıları ya da yetkili kullanıcılara yönelik saldırılar tespit edilebilir.

Ayrıcalıklı erişim haklarının uygun aralıklarla (ayda en az 1 kez) gözden geçirilmesi ve **ayrıcalıklı izinler** atamasının **düzenli olarak** gözden geçirilmesi gerekmektedir. Dosyalara ve veri tabanlarına olan (yerel sistem erişimi dahil) tüm **ayrıcalıklı kullanım erişimlerinin izlenmesi** gerekmektedir. Kritik ayrıcalıklı kullanıcı değişikliklerinin alarm mekanizmalarının Mail-SMS oluşturularak ilgili **BT yöneticileri ile anlık olarak paylaşılması gerekmektedir**.

Kullanıcıların **kötü amaçlı** dosyaları yürütmek için yerleştirebileceği yerleri azaltmak adına **dizin erişim denetiminin ayarlandığından** emin olun. Tüm yürütülebilir dosyalarda **yazma korumalı** dizinlere yerleştirilmesi tavsiye edilir.

Güvenlik açıklarını saldırganlar bu zafiyetlerden faydalanmadan tespit etmek önem taşımaktadır. **Güvenlik açığı tarama araçları** ile yapılan etkili bir tarama işlemi; sistemdeki **yanlış yapılanmaları, zayıf parolaları ve Web Sunucusu Güvenliği’ndeki zayıflıkları** ortaya çıkarır.

Etkili güvenlik açığı taraması ile kuruluşlar, tehdit vektörlerini uzak tutmak için ek güvenlik katmanlarını **güncelleyebilir, yamalayabilir veya dağıtabilir.**

%93

11.İlk Erişim (Initial Access)

İlk Erişim, saldırganın hedef ağ içerisinde birincil dayanağını elde etmesine yarayan çeşitli giriş vektörlerinin kullanıldığı tekniklerden oluşur.

Bir erişim elde etmek için kullanılan bu teknikler, hedeflenen kimlik avı ve dışarıya açık web sunucularındaki zayıflıklardan yararlanmayı içerir.

İlk Erişim yoluyla kazanılan erişimler, geçerli hesaplar ve harici uzak hizmetlerin kullanımı gibi sürekli erişime izin verebilir veya değişen parolalar nedeniyle sınırlı kullanım olabilir.

İlk Erişim (Initial Access) taktiği kullanılarak yapılan saldırıların %96'sı ADEO MDR Servisi tarafından tespit edilebilmektedir.

Kullanıcıların parola belirlerken sosyal ağlarda ve diğer platformlardaki parolalarını kullanmamaları, parolaların değiştirilme aralığının **1 ile 3 ay arasında** olması, özel karakter içermesi ve **minimum 14 karakter** zorunluluğu getirilmesi gerekmektedir.

Hesap yetkilendirme yapılması sırasında gereksiz yetki verilmesinden kaçınılmalıdır. **İşten çıkan personelin hesaplarının kapatılması** önemlidir.

E-posta içindeki **URL incelemesi** (kısaltılmış bağlantıların genişletilmesi dahil), bilinen kötü amaçlı sitelere giden bağlantıların algılanabilmesine yardımcı olabilir. **Sandbox** çözümleri bu bağlantıları algılamak ve kötü amaçlı davranışları belirlemek için otomatik olarak bu sitelere erişim sağlayarak veya bir kullanıcı bağlantıyı ziyaret ederse içeriği beklemek ve yakalamak için kullanılabilir.

Kimlik doğrulama loglarını toplanması ve normal çalışma saatleri dışında olağan dışı/yetkisiz erişimlerin tespit edilmesi gerekmektedir.

Kullanılan uygulama varlık envanterlerinin (web tarayıcıları, bileşenler, eklentiler, ofis ve medya vb.) **düzenli periyotlarda güncelleştirilmesi** önem arz etmektedir.

Tehdit istihbaratı kaynakları tarafından kötü amaçlı olarak sınıflandırılan ağ trafiklerinin **engellenmesi, uyarı oluşturulması sağlanmalıdır**

%96

12.Yanal Hareket (Lateral Movement)

Yanal Hareket, saldırganların bir ağdaki uzak sistemlere girmek ve onları kontrol etmek için kullandığı tekniklerden oluşur. Gerçek hedeflerini takip etmek, genellikle hedeflerini bulmak için ağı keşfetmeyi ve ardından ona erişim sağlamayı gerektirir.

Hedeflerine ulaşmak için, genellikle birden fazla sistem ve hesap arasında geçiş yapmayı içerir.

Saldırganlar, yanal hareketi gerçekleştirmek için kendi uzaktan erişim araçlarını kurabilir veya daha gizli olabilecek yerel ağ ve işletim sistemi araçlarıyla meşru kimlik bilgilerini kullanabilir.

Yanal Hareket (Lateral Movement) taktiği kullanılarak yapılan saldırıların %93'ü ADEO MDR Servisi tarafından tespit edilebilmektedir.

Yanal hareket teknikleri ağ ortamına ve nasıl kullanıldığına bağlı olarak meşru olabilir. **Uzaktan oturum açmadan (RDP)** sonra oluşan erişilen dosyalar ya da gerçekleşen aktiviteler gibi faktörler, bu hareket ile ilgili şüpheli veya kötü amaçlı davranışlara işaret edebilir. Normalde birden çok sisteme nispeten kısa bir süre içinde erişemeyecekleri sistemlerde **oturum açmış kullanıcı hesaplarının izlenmesi önerilir.**

VLAN network ağlarını birbirinden **izole** ederek saldırıların ağda yayılmasına ve veri ihlallerinin önüne geçmektedir.

VPN ile erişilen sistemlerin ya da hizmetlerin sınırlandırılması VPN hesaplarının ele geçmesi durumunda içeride yayılımı minimum düzeyde tutacaktır.

WinRM kullanımı sistem ekipleri tarafından yaygın değilse devre dışı bırakılmalıdır. Eğer yaygın olarak kullanılıyorsa **Windows event logları** yapılandırılmalı ve merkezi olarak **SIEM** üzerinde toplanmalıdır.

Yazılan kurallar ile toplanan bu loglar üzerinden şüpheli erişimler tespit edilmelidir.

SSH kullanımı, ağ ortamına ve nasıl kullanıldığına bağlı olarak meşru olabilir. Uzaktan oturum açmadan sonra oluşan aktiviteler gibi diğer faktörler, **şüpheli veya kötü amaçlı davranışlara** işaret edebilir. Normalde birden çok sisteme nispeten kısa bir süre içinde erişemeyecekleri sistemlerde oturum açmış **kullanıcı hesaplarını izlemek gerekmektedir.**

%93

İşletim Sistemlerine Göre Kural Dağılımı

ADEO MDR Servisi olarak Windows, Linux, MacOS işletim sistemi ve türevleri (WindowsServer, Workstation, Centos, Unix, Debian, Ubuntu tabanlı vb.) özelinde toplam **5500+** tespit kuralımız mevcuttur.

Geliştirilen tespit kurallarının dağılımı; **Windows işletim sisteminde 4808, MacOS'ta 755 ve Linux'ta ise 717 kural** şeklindedir.

Geliştirdiğimiz tespit kuralları MITREATT&CK® Framework'teki Linux, MacOs, Windows tabanlı tüm işletim sistemleri için oluşturulan Taktik, Teknik, Prosedürlerin(TTP*) ortalama **%96'sını** kapsamaktadır.

TTP
Bir tehdit aktörünün işleyişini açıklamak/tanımlamakta kullanılan Teknik, Taktik ve Prosedürler başlıklarının kısaltmasıdır.
TTP'ler belirli bir tehdit aktörünün profilini çıkarmak için kullanılmaktadır.

Tüm müşterilerimize 3 işletim sistemi ve türevleri için %96'nın üzerinde tespit oranıyla destek vermekteyiz.

Windows

4808

MacOS

755

LINUX

717

2025 Yılı Siber Güvenlik Trendleri ve Tahminleri

2025 Yılı Siber Güvenlik Trendleri ve Tahminleri:

1. Yapay Zeka: Tehdit ve Savunmanın Yeni Cephesi

Yapay zeka, 2025'te siber güvenliğin merkezinde konumlanıyor. Kuruluşların %66'sı AI'ın siber güvenlik üzerinde büyük etki yaratacağını öngörürken, %47'si üretken yapay zeka kaynaklı tehditlerden ciddi endişe duyuyor. Tehdit aktörleri, AI ile güçlendirilmiş kötü amaçlı yazılımlar üreterek antivirüs çözümlerini atlatma ve deepfake teknolojisiyle sosyal mühendislik saldırıları gerçekleştirme kapasitelerini artırıyor. Aynı zamanda savunma tarafında AI, otonom tehdit tespiti ve hızlı müdahale için kritik araçlar sunarak SOC ekiplerinin etkinliğini yükseltiyor.

Savunma stratejileri açısından yapay zeka, anormallikleri tespit etme, uyarıları önceliklendirme ve rutin görevleri otomatize etme konusunda önemli avantajlar sağlıyor. Ancak bu teknolojinin kullanımı veri zehirleme gibi karşı saldırılara açık olduğundan, AI sistemlerinin güvenliğini sağlamak ve kararlarını izlemek giderek önem kazanıyor.

2. Fidye Yazılımı ve Tedarik Zinciri: Değişen Saldırı Vektörleri

Fidye yazılımı saldırıları 2025'te evrim geçirerek "çifte şantaj" taktiğiyle veri şifreleme ve sızdırma tehdidini birleştiriyor. Küresel maliyeti 30 milyar dolara ulaşması beklenen bu tehdit, özellikle sağlık, eğitim ve kamu hizmetleri gibi kesinti toleransı düşük sektörleri hedef alıyor. Tedarik zinciri saldırıları da önemli bir tehdit vektörü olarak öne çıkıyor; büyük şirketlerin %54'ü tedarik zinciri bağımlılıklarını siber dirençlerinin önündeki en büyük engel olarak görüyor.

Saldırganlar, doğrudan hedeflemesi zor olan organizasyonlara ulaşmak için daha zayıf tedarikçileri basamak olarak kullanıyor. "Güncelleme zehirleme" ve tedarikçi hesaplarının ele geçirilmesi yoluyla gerçekleştirilen bu saldırılar, tek bir yazılım kütüphanesine yerleştirilen zararlı kodun binlerce uygulamayı etkileyebilmesi potansiyeliyle ciddi risk oluşturuyor.

2025 Yılı Siber Güvenlik Trendleri ve Tahminleri:

3. IoT ve Operasyonel Teknoloji Güvenliği

IoT cihazlarına yönelik saldırıların son bir yılda %400 artış göstermesi, bu alanın artan önemini vurguluyor. IoT trafiğinin %98'inin şifresiz iletilmesi ve cihazların çoğunda güncel olmayan işletim sistemlerinin kullanılması, özellikle üretim, enerji ve sağlık sektörlerinde büyük risk yaratıyor. Botnet oluşturmak için ele geçirilen IoT cihazları, büyük ölçekli DDoS saldırıları için kullanılabiliyor.

Operasyonel teknoloji (OT) sistemleri, kritik altyapının parçası olarak ulusal güvenlik endişesi haline geliyor. 2025'te daha fazla ülke, enerji şebekeleri, su dağıtım sistemleri ve üretim tesisleri için özel siber güvenlik standartları uygulayacak. AB'nin Siber Dayanıklılık Yasası gibi düzenlemeler, IoT cihaz üreticilerine asgari güvenlik gereklilikleri getirmeye hazırlanıyor.

4. Kurumsal Savunma Stratejileri ve Teknolojiler

Zero Trust mimarisi, 2025'te şirketlerin savunma stratejilerinin temelini oluşturuyor. Büyük işletmelerin %60'ının bu güvenlik çerçevesini benimsemesi beklenirken, kimlik ve erişim yönetimini merkeze alan yaklaşımlar, her erişim talebini sürekli doğrulayarak yetkisiz yatay hareketleri sınırlandırıyor. Siber dayanıklılık kavramı da öne çıkıyor; kurumlar sadece saldırıları önlemeye değil, saldırı gerçekleştiğinde hızla toparlanma stratejilerine odaklanıyor.

Konsolidasyon eğilimi güçleniyor; kurumlar çok sayıda farklı güvenlik aracı yerine entegre platformlara yöneliyor. SOAR (Security Orchestration, Automation and Response) sistemleri ve yapay zeka destekli tehdit avcılığı pratikleri yaygınlaşırken, kuantum hesaplama tehdidine karşı post-kuantum kriptografi hazırlıkları başlıyor. Yönetim kurulları daha fazla siber güvenlik okuryazarlığı gösteriyor ve CISO'ların yaklaşık yarısı artık doğrudan CEO'ya raporlama yapıyor.

2025 Yılı Siber Güvenlik Trendleri ve Tahminleri:

5. Düzenleyici Ortam ve Küresel İşbirliği

2025'te siber güvenlik regülasyonları küresel ölçekte daha da güçlenecek. ABD'de halka açık şirketlerin önemli siber olayları 4 iş günü içinde kamuya bildirmesini şart koşan SEC düzenlemesi, AB'de daha geniş sektör yelpazesine siber güvenlik önlemleri ve olay bildirimi zorunluluğu getiren NIS2 Direktifi, yapay zeka sistemlerini risk seviyelerine göre sınıflandıran AI Act gibi düzenlemeler şirketlere yeni yükümlülükler getiriyor.

Düzenlemelerin ülkeler arasında farklılık göstermesi uluslararası şirketleri zorluyor; siber liderlerin %76'sı bu dağınık yapının uyum sağlamayı karmaşıklaştırdığını belirtiyor. Buna rağmen kamu-özel sektör iş birliği modelleri ve bölgesel inisiyatifler güçleniyor. NATO siber tatbikatları, ASEAN'ın çalışmaları ve bölgesel CERT ağları gibi yapılar bilgi paylaşımı sağlıyor. Dünya Ekonomik Forumu, dijital dünyanın ancak kamunun ve özel sektörün sıkı iş birliğiyle güvenli kalabileceğini vurguluyor.

Öneriler

- **Yapay Zekayı Benimseme ve Kontrol Etme:** Kurumlar, yapay zeka tabanlı güvenlik çözümlerini denemekten çekinmemeli, ancak bunları bir panzehir olarak görmeyip doğru alanlarda uygulamalı. Örneğin, AI tabanlı anomali tespit araçları ağ güvenliğinde çok faydalı olabilir, fakat çıktıları her zaman bir uzman tarafından doğrulanmalı.
- **Temel Siber Hijyenin Sağlanması:** Parola politikaları, çok faktörlü kimlik doğrulama, sistem ve uygulamaların düzenli yamalanması, yedekleme ve ağ segmentasyonu gibi temel önlemler gerçekleşecek birçok saldırıyı önleyebilecek güçte.
- **Olay Müdahale Planlarının Güncellenmesi:** Bir saldırı anında kimin ne yapacağını önceden belirleyen, iletişim akışlarını tanımlayan ve düzenli olarak test edilen olay müdahale (incident response) planları hayati önem taşıyor. 2025'te yaşanacak olası bir siber sladırıya en hazırlıklı şekilde karşılık vermek için olay müdahale planlarınızın güncel ve bütün ekipler ve paydaşlarınız tarafından biliniyor ve takip ediliyor olduğundan emin olun.

2025 Yılı Siber Güvenlik Trendleri ve Tahminleri:

Öneriler

- **Proaktif ve İstihbarat Odaklı Yaklaşım:** Saldırıların kaçınılmaz olabileceği gerçeğinden hareketle, kurumlar "ne zaman?" sorusuna odaklanmalı ve sürekli tetikte olmalı. Tehdit istihbarat servislerinden faydalanarak güncel saldırı tekniklerini ve hedef alınan sektörleri takip etmek artık eskisinden çok daha kritik bir öneme sahip olacak.
- **İnsan Faktörüne Yatırım:** Teknoloji kadar, onu yöneten ve kullanan insanların eğitimi ve farkındalığının da kritik önem taşıdığı herkesin malumu. Oltalama simülasyonları, düzenli güvenlik eğitimleri ve özelikle üst yönetim için siber kriz yönetimi konularından yapacağınız çalıştaylar ile siber dayanıklılığınızı arttırın.

2025 yılı siber güvenlikte zorlu bir yıl olsa da, aynı zamanda yenilik ve dönüşümün de yılı olacak. Saldırganlar her zamankinden daha karmaşık ve hızlı olabilir, ancak unutmayın, savunma tarafı da kendi üzerine düşeni yaptığı müddetçe korkmaya hiç gerek yok.

Global Stratejiden Sorumlu Başkan Yardımcısı
Halil Öztürkci

Yapay Zeka Çağında Siber Güvenlik Stratejileri

Yapay Zeka Çağında Siber Güvenlik Stratejileri:

Kurumsal Direncin İnşası

Bilişim teknolojilerinin yaygınlaşması ve dijital dönüşümün hız kazanmasıyla birlikte, siber güvenlik olgusu, modern kurumların karşı karşıya kaldığı en kritik stratejik zorluklardan biri haline gelmiştir. Geleneksel tehdit vektörlerinin ötesine geçerek, yapay zeka (YZ) destekli saldırılar, gelişmiş kalıcı tehditler (APT'ler), tedarik zinciri zafiyetleri ve derin öğrenme tabanlı manipülasyonlar gibi sofistike unsurlar, dijital ekosistemimizin kırılganlığını derinleştirmektedir. Bu bağlamda, kurumların ve organizasyonların salt taktiksel savunma mekanizmalarına odaklanmak yerine, uzun vadeli bir stratejik vizyon çerçevesinde siber güvenlik yaklaşımlarının yeniden yapılandırılmaları bir zorunluluk arz etmektedir. Bu makalede, 2025 ve ötesi için siber güvenlik stratejilerinin temel bileşenleri akademik bir perspektifle analiz edilecek ve kurumsal direncin inşası için kapsamlı bir plan ele alınacaktır.

Siber Güvenliğin Stratejik İmperatifi: Çok Katmanlı Risk Yönetimi

Günümüzde siber tehditler, yalnızca bilgi teknolojileri (BT) departmanlarının sorumluluğunda olan teknik bir sorun olmaktan çıkmış, kurumsal sürdürülebilirlik, itibar yönetimi, finansal istikrar ve hatta ulusal güvenlik gibi geniş bir yelpazede stratejik etkiler yaratan bir risk faktörü haline gelmiştir. Siber saldırılar, operasyonel aksaklıklara, veri ihlallerine, fikri mülkiyetin kaybına ve yasal yaptırımlara yol açarak kurumların temel işleyişini ve uzun vadeli hedeflerini ciddi şekilde tehdit edebilmektedir. Bu nedenle, siber güvenliğin, kurumsal risk yönetimi çerçevesinin ayrılmaz bir parçası olarak ele alınması ve üst yönetim düzeyinde stratejik bir öncelik olarak konumlandırılması gerekmektedir.

Taktiksel Savunmadan Stratejik Dirence: Bütünleşik Bir Çerçeve

Etkili bir siber güvenlik stratejisi, reaktif önlemlerin ötesine geçerek, proaktif savunma, erken tespit, hızlı müdahale ve etkili iyileştirme süreçlerini içeren bütünleşik bir çerçeve üzerine inşa edilmelidir. Bu bağlamda, "stratejik direnç" kavramı ön plana çıkmaktadır. Stratejik direnç, bir kurumun siber saldırılara karşı yalnızca savunma yapmakla kalmayıp, aynı zamanda bu saldırılardan sonra iş sürekliliğini sağlayabilme, operasyonlarını en kısa sürede yeniden başlatabilme ve uzun vadede rekabet avantajını koruyabilme yeteneğini ifade etmektedir. Bu amaca ulaşmak için, kurumların kapsalı bir siber güvenlik stratejisi geliştirmesi ve bu stratejiyi tüm iş süreçlerine entegre etmesi gerekmektedir.

Yapay Zeka Çağında Siber Güvenlik Stratejileri:

Gelişmiş Kalıcı Tehditler (APT'ler) ve Devlet Destekli Aktörler: Karmaşık Tehdit Ortamı

Stratejik siber saldırıların en önemli bileşenlerinden biri, gelişmiş kalıcı tehditler (APT'ler) ve devlet destekli aktörlerdir. Bu tür saldırılar, genellikle yüksek düzeyde teknik uzmanlık, sabır ve kaynak gerektirir. Amaç, sisteme gizlice sızmak, uzun süre boyunca varlığını sürdürmek ve hassas bilgilere erişmektir. 2024 yılında ortaya çıkan XZ Utils saldırısı, bu tür tehditlerin ne kadar karmaşık ve gizli olabileceğine dair çarpıcı bir örnek teşkil etmektedir.

Açık kaynak bir yazılım bileşenine yapılan bu sofistike saldırı, küresel çapta birçok sistemi etkileme potansiyeline sahipti ve devlet destekli bir aktör tarafından gerçekleştirildiği tahmin edilmektedir. Bu olay, kurumların yalnızca dış tehditlere değil, aynı zamanda tedarik zincirlerindeki ve açık kaynak projelerindeki potansiyel zafiyetlere karşı da teyakkuzda olmaları gerektiğini açıkça göstermektedir.

Proaktif Tehdit İstihbarat Stratejisinin Formülasyonu

Etkili bir siber güvenlik stratejisinin temelini, proaktif bir tehdit istihbarati yaklaşımı olusturur. Bu yaklaşım, yalnızca bilinen tehditlerin ve saldırı yöntemlerinin takibini değil, aynı zamanda potansiyel saldırganların motivasyonlarını, hedeflerini ve taktiklerini anlamayı da içerir.
Gelişmiş tehdit istihbaratı platformlar, dark web analizleri, sektördeki bilgi paylaşım ağları ve akademik araştırmalar, bu bağlamda önemli bilgi kaynaklarıdır. Kurumlar, bu kaynaklardan elde ettikleri bilgileri analiz ederek, kendi özel tehdit ortamlarını daha iyi anlayabilir ve savunma mekanizmalarını buna göre şekillendirebilirler. Tehdit istihbaratının stratejik karar alma süreçlerine entegre edilmesi, uzun vadeli güvenlik planlarının oluşturulmasında kritik bir rol oynar.

Sistemsel Zafiyetlerin Ele Alınması: Açık Kaynak Yazılım Örneği

Açık kaynak yazılımların (AKY) yaygın kullanımı, beraberinde önemli güvenlik risklerini de getirmektedir. AKY projelerindeki güvenlik açıkları, kötü niyetli aktörler tarafından genis çaplı saldırılar için istismar edilebilmektedir. Bu durum, kurumların AKY kullanımına yönelik stratejik bir yaklaşım benimsemelerini zorunlu kılmaktadır.

Bu yaklaşım, AKY bileşenlerinin envanterinin çıkarılması, güvenlik açığı taramalarının düzenli olarak yapılması, yama yönetim süreçlerinin etkinleştirilmesi ve güvenilir AKY kaynaklarının tercih edilmesi gibi unsurları içermelidir. Ayrıca, AKY projelerine güvenlik katkısı sağlamak ve toplulukla is birliği yapmak da uzun vadede güvenliği artırmaya yönelik stratejik bir adım olabilir.

Yapay Zeka Çağında Siber Güvenlik Stratejileri:

Siber Suç Olarak Hizmet (CaaS) Ekosistemi: Stratejik Bir Meydan Okuma

Siber suçun hizmet olarak sunulması (CaaS) modeli, siber saldırıların ölçeğini ve karmaşıklığını önemli ölçüde artırmıştır. Saldırganlar, fidye yazılımı operasyonlarından oltalama kampanyalarna kadar çesitli siber suç faaliyetlerini, uzmanlaşmış gruplardan hizmet olarak satın alabilmektedirler.

Bu durum, kurumların çok katmanlı bir savunma stratejisi geliştirmelerini ve olay müdahale yeteneklerini güçlendirmelerini gerektirmektedir. Stratejik düzeyde, bu tür tehditlere karşı ulusal ve uluslararası iş birliğinin artırılması, siber suçluların yakalanması ve cezalandırılması açısından kritik öneme sahiptir.

Yasal Düzenlemelerin Stratejik Etkileri: NIS2 ve Ötesi

Siber güvenlik alanındaki yasal düzenlemeler, kurumların stratejik kararlarını önemli ölçüde etkilemektedir. Avrupa Birliği'nin NIS2 Direktifi gibi düzenlemeler, kritik sektörlerde faaliyet gösteren kuruluşlara yönelik siber güvenlik standartlarını ve uyumluluk gereksinimlerini belirlemektedir.

Bu tür düzenlemelere uyum sağlamak, kurumların yalnızca yasal yükümlülüklerini yerine getirmelerini değil, aynı zamanda siber dirençlerini artırmalarını ve paydaşlarının güvenini kazanmalarını da sağlar. Stratejik düzeyde, kurumların bu tür düzenlemeleri yakından takip etmeleri, uyum süreçlerini planlamaları ve gerekli yatırımları yapmaları gerekmektedir.

Soyut Varlıkların Korunması: Dijital Çağda Marka Güvenliği

Marka güvenliği, günümüzde kurumların en değerli soyut varlıklarından biridir. Siber saldırılar ve dijital dolandırıcılık faaliyetleri, marka itibarını ciddi şekilde zedeleyebilir ve müşteri güvenini sarsabilir. Bu nedenle, marka güvenliğini korumak, kurumların stratejik öncelikleri arasında yer almalıdır.

Bu bağlamda, alan adı yönetimi, marka izleme sistemleri, sosyal medya güvenliği ve müşteri bilinçlendirme gibi önlemlerin alınmasi kritik önem taşımaktadır. Stratejik düzeyde, marka güvenliği, kurumsal iletişim ve pazarlama stratejileriyle entegre edilmelidir.

Yapay Zeka Çağında Siber Güvenlik Stratejileri:

Geleceğe Yönelik Siber Güvenlik Statejisinin Temel Stratejik Unsurları

Gelişen tehdit ortamına karşı uzun vadeli bir siber güvenlik stratejisi oluşturmak için aşağıdaki temel stratejik unsurlara odaklanmak gerekmektedir:

- **Sıfır Güven (Zero-Trust) Mimarisi**

Geleneksel çevre güvenliği modelinin yetersiz kaldığı günümüzde, sıfır güven mimarisi, tüm kullanıcıların ve cihazların kimliğinin doğrulanmasını ve yetkilendirilmesini temel alan daha güvenli bir yaklaşım sunmaktadır. Bu mimarinin stratejik olarak benimsenmesi, iç ve dış tehditlere karşı direnci artırabilir.

- **Güvenli Tasarım (Security by Design) Prensibi:**

Yazılım ve sistemlerin geliştirilmesinin erken aşamalarından itibaren güvenlik gereksinimlerinin dikkate alınması, potansiyel güvenlik açıklarının maliyetli hale gelmeden tespit edilmesini ve giderilmesini sağlar. Bu prensibin stratejik olarak benimsenmesi, uzun vadede daha güvenli sistemlerin ortaya çıkmasına katkıda bulunur.

- **Sürekli İyileştirme ve Adaptasyon**

Siber tehdit ortamı sürekli olarak değiştiği için, siber güvenlik stratejilerinin de dinamik ve adaptif olması gerekmektedir. Düzenli olarak güvenlik kontrollerinin yapılması, tehdit istihbaratının güncel tutulması ve stratejilerin yeni tehditlere göre ayarlanması, sürekli iyileştirme prensibinin temelini oluşturur.

Güvenlik Odaklı Bir Kültürün Geliştirilmesi: Stratejik Savunmada İnsan Faktörü

Siber güvenlik stratejisinin başarısında, insan faktörü kritik bir rol oynamaktadır. Çalışanların siber güvenlik konusunda bilgilendirilmesi ve eğitilmesi, kurumun genel güvenlik duruşunu önemli ölçüde etkileyebilir. Stratejik düzeyde, kurumların güvenlik odaklı bir kültür oluşturmaya yönelik uzun vadeli bir plan geliştirmeleri gerekmektedir. Bu plan, düzenli farkındalık eğitimlerini, oltalama simülasyonlarını ve güvenlik politikalarına uyumu teşvik eden bir ortamı içermelidir.

Sonuç: Yapay Zeka Destekli Tehditler Çağında Stratejik Çeviklik

2025 ve ötesi, yapay zeka destekli siber tehditlerin daha da yaygınlaşacağı ve sofistike hale geldiği bir dönem olacaktır. Bu zorlu ortamda başarılı olmak için kurumların, geleneksel savunma yaklaşımlarını geride bırakarak, stratejik çeviklik, proaktif tehdit istihbaratı, sıfır güven mimarisi, güvenli tasarım prensipleri ve güvenlik odaklı bir kültür gibi unsurları içeren kapsamlı bir siber güvenlik stratejisi benimsemeleri gerekmektedir.

Unutulmamalıdır ki, siber güvenlik sadece bir teknoloji yatırımı değil, aynı zamanda kurumsal sürdürülebilirliğin ve uzun vadeli başarının temelini oluşturan stratejik bir zorunluluktur. Bu nedenle, kurumların siber güvenlik konusuna gereken önemi vermeleri ve sürekli olarak gelişen tehdit ortamına karşı hazırlıklı olmaları hayati önem taşımaktadır.

Melih Özhan
Chief Strategy Officer

Öneriler

Öneriler #TOP5

1

Olası bir saldırının önüne geçilmesi için kurumların MSSP veya MDR hizmeti ile 7x24x365 gün izlenmesi gerekmektedir.

2

İki faktörlü doğrulama MFA aktif edilmesi, gereksiz yetki verilmesinden kaçınılması, farkındalığın düşük olduğu yerlerde önleyici önlemlerin alınması önemlidir.

3

Tespit yeteneklerinin artırılması ve bunun için öncellikle görünürlüğün artırılması; ilgili atakları tespit edecek kuralların ve korelasyonların sürekli olarak güncellenmesi gerekmektedir.

4

Olası siber olaylara karşın hep güncel bir aksiyon planının oluşturulması ve belli periyotlarla simülasyonların tekrar edilerek farkındalığın ve hazırlıkların güncel tutulması gerekmektedir.

5

Varlık envanterlerinin belirli periyotlarda incelenmesi ve dışarıya açık olan servislerin kontrollerinin sağlanması gerekmektedir.

Öneriler

IT ve OT sistemlerinin tamamını kapsayan görünürlük ve sıkılaştırmaların eksiksiz takip edilmesi önemlidir.

Otomatize ürün ve yazılımların, sistemlerin satın alınmasından ziyade insan temelli servislerin veya siber güvenlik ekiplerindeki insanlara yatırımın artırılması gerekmektedir.

Kırmızı Takım (Red Team) ve Sızma (Penetrasyon) Testi aktivitelerinin düzenli periyotlarda uzman ekiplerce gerçekleştirilmesi sağlanmalıdır.

Saldırıların büyük bir çoğunluğunun yeni çıkan zafiyetlerden kaynaklandığı göz önünde bulundurulmalıdır. Buradan hareketle "Vulnerability Management" (Zafiyet Yönetimi) prosedürlerinin sürekli olarak uygulanması ve bunların sıkı bir şekilde takip edilmesi önem arz etmektedir.

Oltalama (Phishing) saldırılarına karşı çalışanlara belirli periyotlarda farkındalık eğitimlerinin uygulamalı olarak verilmesi, insan kaynaklı saldırıların önüne geçme noktasında faydalı olmaktadır.

Siber güvenlik ekiplerinin olgunluk seviyesinin ölçülmesine yönelik Mor Takım (Purple Team) aksiyonlarının, uzman ekiplerce alınması sağlanmalıdır.

Kurumlarda var olan ortam (Active Directory, Firewall, Network Segmentasyon ve varsa diğer güvenlik cihazlarının) ihtiyaca uygun şekilde sıkılaştırılarak, atak yüzeyi daraltılmalıdır.

ADEO Cyber Security 2023 yılından beri ChatGPT başta olmak üzere **birçok AI modelini** kullanmaktadır.

Yapay Zeka ve Siber Güvenlik: Geleceğin Savunma Stratejisi

Günümüzün hızla dijitalleşen dünyasında, siber güvenlik artık kurumlar için hayati bir öneme sahip. Teknolojinin sürekli gelişmesiyle birlikte, siber saldırılar da giderek sofistike hale geliyor. İşte bu noktada, yapay zeka (AI) teknolojileri, siber güvenlik uzmanlarının elindeki en güçlü savunma mekanizmalarından biri haline geldi.

Siber güvenlik firması olarak biz ADEO'da geleneksel yöntemlerin ötesine geçerek yapay zeka ve makine öğrenme teknolojilerini aktif olarak kullanmaktayız. Bu teknolojiler, hassas verilerin korunmasında ve saldırıların tespit edilip önlenmesinde bizlere yardım etmekte ve farklı bakış açıları kazanmamızda rol oynamaktadır.

Yapay Zeka ve Siber Güvenlikte Faaliyet Alanlarımız: Savunma Kalkanları ve Otomasyona Geçiş

Faaliyet alanlarımız, hem müşterilerimiz hem de kendi şirketimiz için gelişmiş savunma stratejileri oluşturarak güvenliği artırma odaklıdır. Bu yaklaşımı saldırgan bakış açılarını daha iyi analiz edebilmek ve kural optimizasyonlarımız için kullanırken aynı zamanda ADEO olarak insan gücünü daha verimli kullanabilmek adına da birçok işimizi AI destekli otomasyon teknolojisi ile birleştiriyoruz.

Gelecek yıllarda ADEO olarak alarm analizi, kural yazma, güncel haber alma gibi birçok konuda yapay zekayı aktif olarak, %70'in üzerinde bir oranla kullanmayı planlamaktayız.

Yapay zeka teknolojilerinin siber güvenlik alanında geleceğin güvenliğini şekillendireceğini hatırlatmak isteriz. Sürekli olarak veri analizi yapabilen, öğrenen ve kendini geliştiren yapay zeka sistemleri, siber saldırıların önlenmesinde ve zararlarının minimalize edilmesinde kritik bir rol oynayacaktır.

ADEO olarak, hizmet verdiğimiz kurumlara da, hayati önem taşıyacak olan bu yeni teknolojiye de hazırız. Siber güvenliğin günümüzün dijital dünyasında ne kadar önemli olduğunu biliyoruz ve bu alanda yapay zeka gibi en son teknolojileri kullanarak müşterilerimize en iyi hizmeti sunuyoruz.

Ürün Ailesinin Yeni Üyeleri

Splunk SIEM ile Akıllı Güvenlik ve Hızlı Tehdit Tespiti

Splunk SIEM, gelişmiş veri analitiği ve yapay zeka desteğiyle güvenlik tehditlerini hızlıca tespit eder. Gerçek zamanlı analizler ve güçlü korelasyon motoru ile siber saldırılara karşı güçlü bir koruma sağlar. Güvenlik verilerinizi merkezi bir platformda toplar, kolayca izler ve raporlar.

Cequence ile API Güvenliği ve Bot Yönetimi

Cequence, API keşfi, güvenliği ve bot yönetimi alanlarında güçlü çözümler sunar. Yapay zeka destekli tehdit algılama, gerçek zamanlı API izleme ve gelişmiş dolandırıcılık önleme ile dijital varlıklarınızı korur. API'lerinizin güvenliğini sağlar, düzenleyici uyumu destekler ve organizasyonların karşılaşabileceği riskleri azaltır. Esnek dağıtım seçenekleri ile her sektöre uygun çözümler sunar.

Wallarm ile API ve Web Uygulamalarınız Daha Güvenli

Wallarm ile gerçek zamanlı koruma ve otomatik güvenlik testleriyle, OWASP Top 10 bot saldırıları ve L7 DDoS tehditlerine karşı güvenliği üst seviyeye taşıyın.

IBM QRadar ile Proaktif Güvenlik ve Tehdit Tespiti

IBM QRadar, gelişmiş korelasyon motoru ve yapay zeka desteği ile güvenlik tehditlerini hızlıca tespit eder. Gerçek zamanlı analiz ve otomatize edilmiş özellikleriyle, siber saldırılara karşı güçlü bir koruma sağlar. Merkezi veri toplama ve görselleştirme araçları ile güvenlik durumunuzu kolayca izleyebilirsiniz.

Ürün Ailesinin Yeni Üyeleri

SecHard ile Zero Trust ve Gelişmiş Güvenlik Çözümleri

SecHard, AI destekli tehdit algılama, adli bilişim ve güvenlik analitiği ile dijital riskleri hızlıca tespit ve nötralize eder. Gerçek zamanlı tehdit izleme ve risk değerlendirmesi ile organizasyonlarınızı proaktif şekilde korur. Zero Trust yaklaşımını benimseyerek, tüm varlıklarınızın güvenliğini sağlar

SECHARD
Complete Zero Trust

Brandefense ile Dijital Risk Koruması ve Proaktif Tehdit Yönetimi

Brandefense, AI destekli dijital risk koruması ve siber tehdit izleme çözümleri sunar. Gerçek zamanlı tehdit izleme, marka koruma ve siber saldırılara karşı önleyici güvenlik hizmetleri sağlar. Platform, webin derin, yüzey ve karanlık katmanlarında riskleri tespit eder, önceliklendirir ve organizasyonları potansiyel tehditlere karşı korur.

BRANDEFENSE
CYBER THREAT INTELLIGENCE

Soteryan AI Destekli Gelişmiş Tehdit İstihbaratı ile Proaktif Çözüm

Soteryan, siber güvenlik alanındaki lider kuruluşlara yönelik gelişmiş tehdit istihbaratı ve güvenlik çözümleri sunar. AI destekli tehdit avcılığıyla dijital riskleri etkili bir şekilde nötralize eder; böylece organizasyonlarınızın güvenliğini güçlendirir. Gerçek zamanlı tehdit izleme, kapsamlı veri analitiği ve önceliklendirilmiş tehdit raporlaması ile potansiyel saldırılara karşı hızlı müdahale sağlanır. Ayrıca, milyarlarca aktif enfekte kaydını izleyerek küresel tehditlerin yerelleştirilmiş analizini yapar ve her an değişen siber riskleri proaktif bir şekilde bildirir. Soteryan, adli bilişim, güvenlik analitiği ve risk değerlendirmeleri ile kuruluşların güvenlik seviyelerini artırarak onları siber tehditlerden korur.

Soteryan

Forestall ile Gelişmiş Active Directory Güvenliği ve Tehdit Yönetimi

Forestall, Active Directory güvenliği için kapsamlı çözümler sunar. FSProtect, miskonfigürasyonları ve gizli saldırı yollarını tespit ederken, FSDetect sürekli izleme ve tehdit algılama sağlar. Ayrıca, Borabay, ofis belgelerindeki kötü amaçlı makroları ve RTF açıklarını analiz ederek verilerinizi güvence altına alır. Forestall, güçlü tehdit tespiti ve hızlı çözüm odaklı yaklaşımlarla, organizasyonlarınızı gelişmiş tehditlere karşı korur.

FORESTALL

Ürün Ailesinin Yeni Üyeleri

OctoXLabs ile Gelişmiş Varlık Yönetimi ve Güvenlik İzleme

OctoXLabs, Cyber Asset Attack Surface Management (CAASM) platformu ile tüm siber varlıklarınızı merkezi bir noktadan yönetmenizi sağlar. API entegrasyonları ile varlık keşfi, güvenlik açıklarını tespit etme ve risk haritalaması yaparak güvenlik seviyenizi artırır. Ayrıca, uygulama envanteri ve lisans yönetimi ile işletmenizin siber güvenlik süreçlerini optimize eder.

Phishy ile Hızlı ve Etkili Olay Yanıtı

Phishy, e-posta güvenliği için gelişmiş olay yanıtı çözümleri sunar. Şüpheli e-postaları hızlıca tespit eder ve analiz eder; tehditlerin gerçekliğini veya sahte olup/olmadığını belirler.
E-postaları derinlemesine inceler ve tehditler tek tıklama ile şirket genelinde izole edilir. Ayrıca, otomatik e-posta kaldırma özelliği ile ağı güvenli tutar.

Hizmet Ağımız

ADEO ve Türkiye’de İlkler

ADEO Cyber Security 'nin ayrıcalıklı siber güvenlik hizmetlerini www.adeosecurity.com web sitemiz üzerinden inceleyebilirsiniz.

MSSP Alert Top 250 2024 List via the link below.

ADEO ve Türkiye'de İlkler

Microsoft MISA Üyesi

İlk Microsoft MISA Üyesi (2022)

Microsoft MSSP İş Ortağı

İlk Microsoft MSSP İş Ortağı (2022)
(Bölgede 2. ve Dünyada ise 8. konumdadır.)

ADEO, Türkiye'nin Microsoft Intelligent Security Association'a (MISA) üye olarak kabul edilen ilk ve tek Siber Güvenlik firmasıdır.

MXDR

İlk Microsoft MISA, MXDR İş Ortağı, (2024)
(CEMA bölgesinde bu yetkinliğe sahip 109 firma içinde 1. konumdadır)

Microsoft onaylı Yönetilen Genişletilmiş Tespit ve Müdahale (MXDR) hizmeti, ekibinizin bir uzantısı gibi çalışan ve uzman kaynaklara günün her saati ulaşabilmenizi sağlayan bütünsel bir güvenlik hizmetidir. Ortamınızın izlenmesi ve acil müdahale gerektiren olayların zamanında önceliklendirilmesi, sağlıklı bir güvenlik duruşunun sürdürülmesi için kritik öneme sahiptir. Geleneksel güvenlik modellerinden farklı olarak MXDR, veri toplama, korelasyon, sürekli tehdit avcılığı ve olay müdahalesini tek bir yönetilen hizmette birleştirir. Özünde, kurumları siber tehditlere karşı korumak için teknoloji ve insan uzmanlığını birleştiren bütünsel bir güvenlik çözümüdür.

Member of
Microsoft Intelligent Security Association

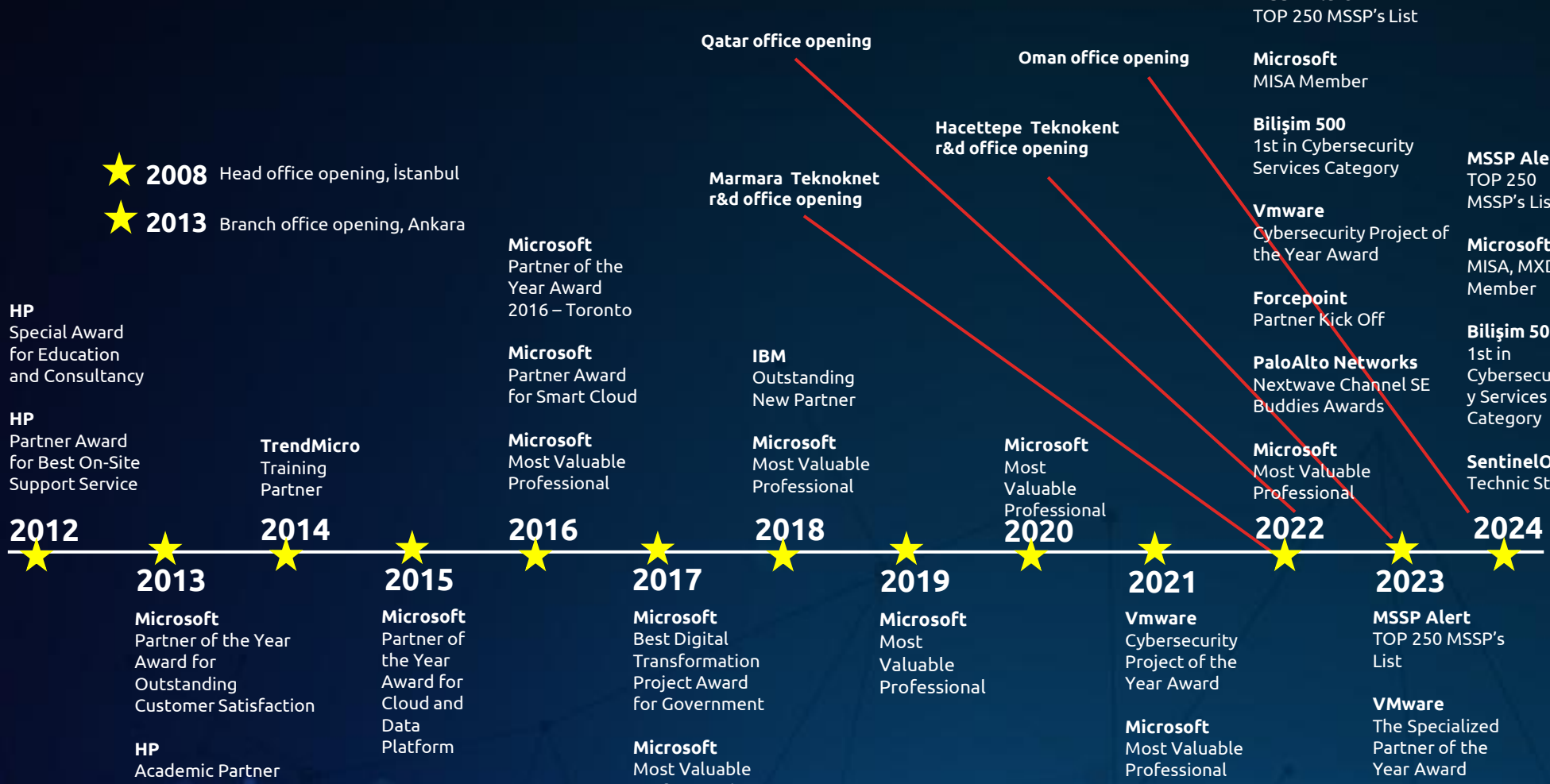
Microsoft Security

Microsoft Verified
Managed XDR Solution

ADEO ve Türkiye’de İlkler

- The First Digital Forensics Lab in Turkey, 2015
- Member of Turkey Cyber Security Cluster, 2018
- The First Carbon Black MSSP Partner in Turkey, 2019
- The First MDR Service Provider in Turkey, 2020
- The First Palo Alto Networks, MSSP Partner in Turkey, 2020
- (is also one of the 11 companies in the world with this competence.)
- The First Microsoft MSSP Partner in Turkey, 2021
- (ranks 2nd in the region, and 8th in the world.)
- The First Microsoft, MISA Member in Turkey, 2022
- MSSP Alert, TOP 250 MSSP’s List, 2022 & 2023 & 2024
- 2022 - ADEO Cyber Security has achieved significant success by being recognized and listed among the top 250 Managed Security Services Providers (#MSSPs) globally, as compiled by MSSP Alert.
- 2023 - Adeo Cyber Security, a powerhouse in managed security services, just soared 47 spots in this year's Top 250 MSSP rankings.
- 2024 - Adeo Cyber Security, a powerhouse in managed security services, just soared 24 spots in this year's Top 250 MSSP rankings
- The First ADTR Service Provider in Turkey, 2023
- The First APTR Service Provider in Turkey, 2023
- The First Microsoft MISA, MXDR Member in Turkey, 2024
- (is also 1st of the 109 companies in the CEMA region with this competence.)
- Bilişim 500 1st in Cybersecurity Services Category 2023 & 2024
- SentinelOne Technic Star 2024

ADEO'nun Başarıları



ADEO CYBER SECURITY

www.adeosecurity.com

 ADEO Cyber Security Services

 @adeocomtr

 ADEOcomtr

 @adeocomtr

 @adeocomtr