ADEO
CYBER SECURITY

2023 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 160'ın üzerinde çalışandan oluşan uzman kadrosuyla,

- Yönetilen Siber Güvenlik Hizmetleri
- Siber Dayanıklılık
- Yönetişim Risk ve Uyumluluk

alanlarında geniş bir yetkinlik yelpazesi ile hizmet veriyor.

ADEO Hakkında

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.

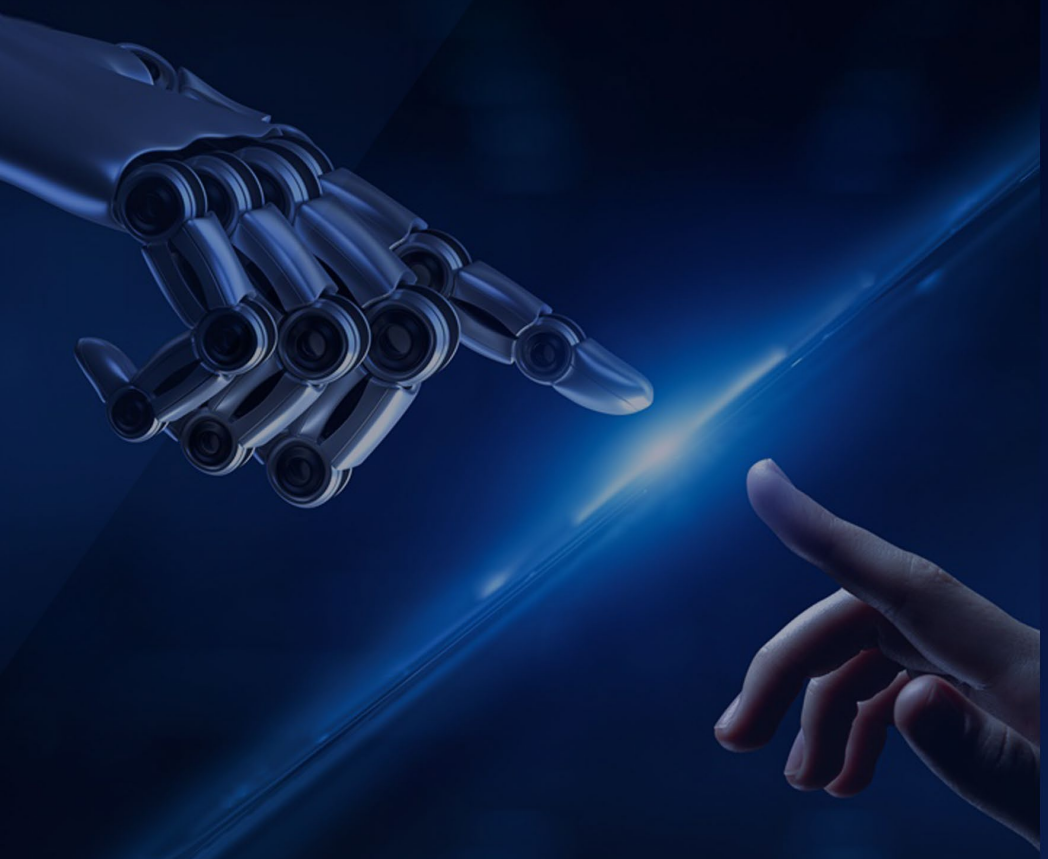
Statik Değil Dinamik

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



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

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.

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, atomic indikatörlerin yanı sıra davranışsal indikatörlere göre tespit ve tehdit avcılığı imkanı sağlayan ve gerektiğinde şüpheli aktivitelere ait kanıtların toplanabildiği ya da müdahale edilebildiği araçlardır.

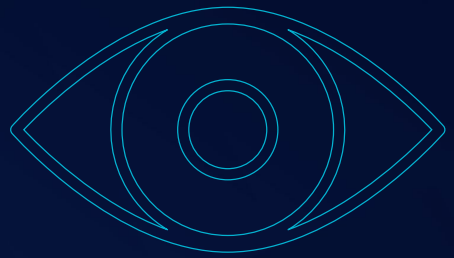
XDR (Extended Detection and Response/Genişletilmiş Tespit ve Müdahale)

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

ADEO 2023 Tehdit Raporu: 2023 Yılının Siber Güvenlik Analizi

Bu rapor, siber güvenlik alanındaki deneyimiyle sektörde öncü konumundaki ADEO'nun 2023 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, bunların nasıl ortaya çıktığı ve gelecekteki riskleri yönetmek için alınabilecek önlemler hakkında ayrıntılı bilgi sunulmaktadır.

ADEO 2023 Tehdit Raporu; kurumların ve bireylerin, siber güvenlik savunmalarını güçlendirme ve dijital varlıklarını korumaya yönelik bilinçlendirme ve önlemler geliştirmelerine yardımcı olmak için, konusunda uzman bir ekip tarafından yapılan kapsamlı analizler doğrultusunda hazırlanmıştır.

ADEO
CYBER SECURITY

2023 Yılında Neler Yaptık?

2023 İstatistikleri

En Çok Hedef Alınan Sektörler & Bu Sektörlerdeki Toplam Vakalar

Perakende
10 Saldırı

Havacılık
5 Saldırı

En Yoğun Gün

13 Haziran
Alarm Sayısı
3886

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

Toplam Geliştirilen Kural Sayısı 5000+

Ocak 2023'te **51,000** olan **IOC sayısı** yıl sonunda **120,000'e** çıkarıldı.

Ocak 2023'te **4,000 olan tespit kuralı** sayısı yıl sonunda **5,000'e** çıkarıldı.

İçeriden ve dışarıdan sağlanan tehdit istihbaratı ile taranan **IOC** sayısı: **120,000**

En Çok Kullanılan İlk Erişim Tekniği:

Exploit/Dışarıya Açık Zafiyetler

%39,28

İLK ERİŞİM TEKNİĞİ

Saldırgan, çeşitli zafiyetlerden faydalanarak sisteme ilk erişimi sağlayıp, hedeflerine ulaşarak diğer taktik ve teknikleri kullanmaya başlar.

MDR Ekibinin Günlük Rutini

İncelenen alarmların **%98**'i ADEO MDR ekibi tarafından müşteriye bildirilmeksizin analiz edilir ve kullanılan ürünün olgunluğuna göre gerekli **müdahale prosedürleri** uygulanır. 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 **10** kadar **yeni tespit kuralı** yazmaktadır. Buna ek olarak yanlış pozitif **(false positive)** olarak değerlendirilen kurallar özelinde ise **sıkılaştırma/iyileştirme** çalışmaları yapılır.

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.

Alarmların **%2**'si teyit edilir ve onay alındıktan sonra gerekli aksiyonlar uygulanır.

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.

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.

2023 yılında olay müdahalesi gerektiren ilk erişim tekniklerinin dağılımı **36.sayfada** belirtilmiştir.

28
Gerçekleştirilen Müdahale Sayısı

VAKA YÖNETİM AŞAMALARI

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) **11 dakika 19 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.

2023 yılı içerisinde ADEO MDR ekibinin acil ve kritik vakalara medyan müdahale süresi **27 dakika 31 saniye** olarak ölçülmüştür.

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

Yıllık Alarm Sayıları ve Seviyeleri

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

Bu çalışmalar kapsamında **2024 yılı hedefi,**

- Kritik ve yüksek seviyeli alarm sayılarının düşürülmesi ve
- Gerçek pozitif alarm sayılarının artırılmasıdır.

Tespit ve Müdahale Süresi

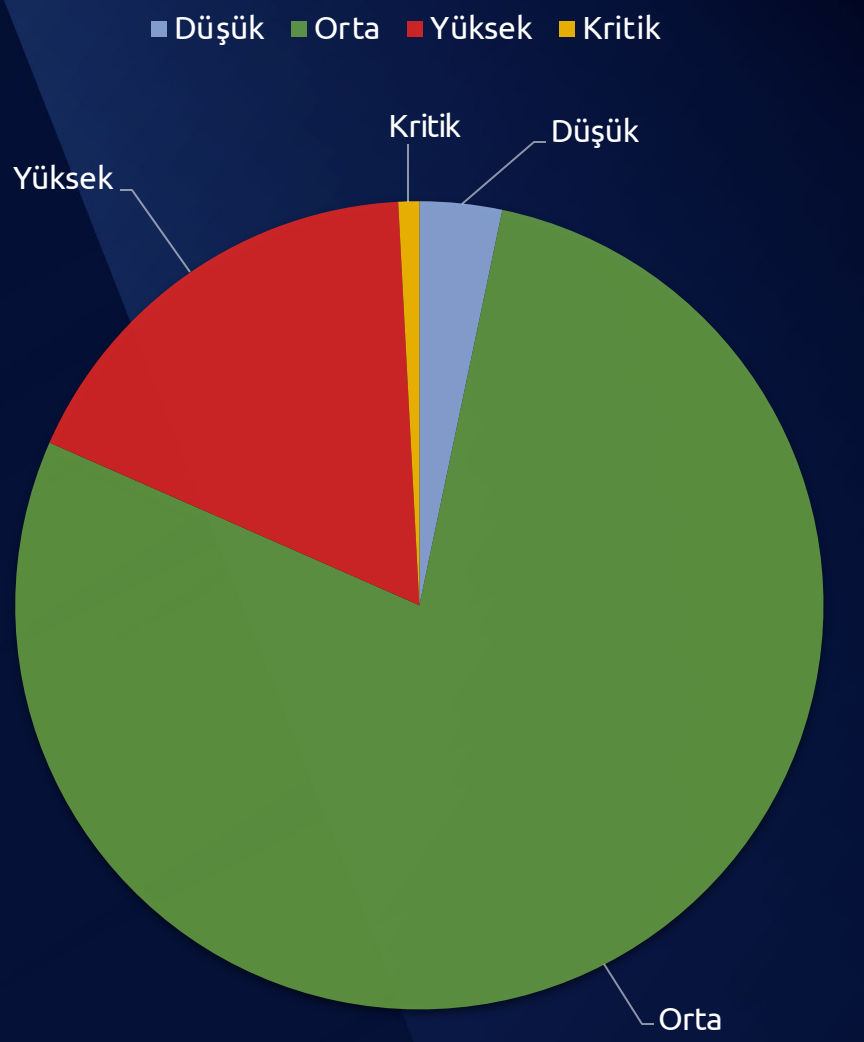
11dk 19s
Medyan (mean)
Tespit Süresi

27dk 31s
Medyan (mean)
Müdahale Süresi

2022 yılında en yoğun gün alınan alarm sayısı **652** iken, bu sayı 2023 yılının en yoğun gününde **3886** olarak raporlanmıştır.

Yıllık Alarm Sayıları ve Seviyeleri

Sadece yüksek ve kritik seviyedeki alarmların medyan tespit süresi **11 dakika 19 saniye**, medyan müdahale süresi ise **27 dakika 31 saniye** olarak ölçülmüştür.



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

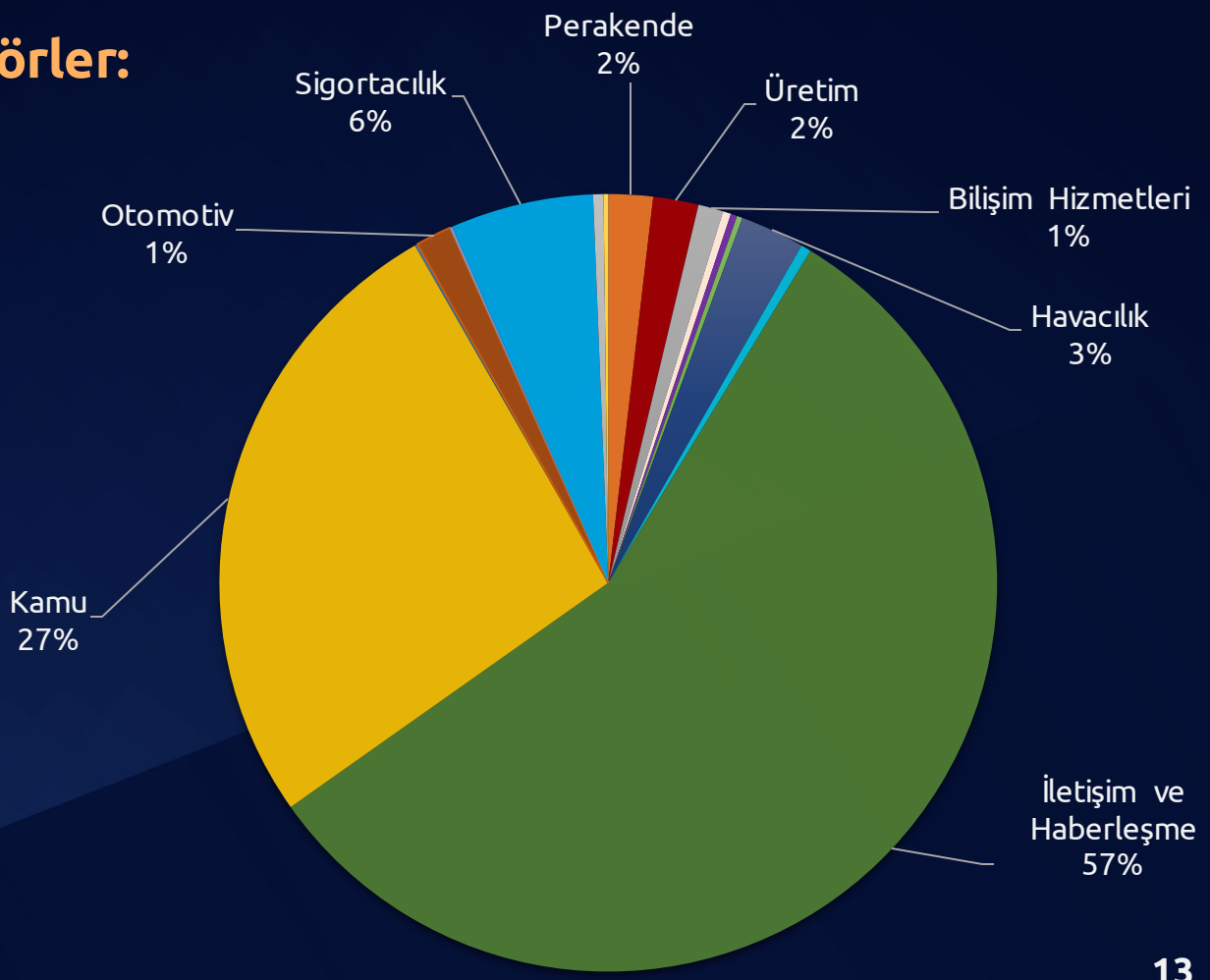
MÜDAHALE SÜRESİ:
Saldırının gerçekleşmesi ile, ilgili saldırının MDR Ekibi tarafından görülüp tanımlanmasının ardından gerekli aksiyonun alındığı zaman aralığına denir.

Alarmların Sektörlere Göre Dağılımı

En Çok Alarm Gözlenen Sektörler:

HABERLEŞME:
Çalışanların çoğunlukla sahada bulunduğu, dağıtık yapıda bir sektördür. Saldırılara bu dağıtık yapı sebebiyle maruz kalınmıştır.

KAMU:
2023 yılında yaşanan jeopolitik olaylar ve seçim gündemi nedeniyle kamu kurum ve kuruluşlarında alarm artışı gözlenmiştir.



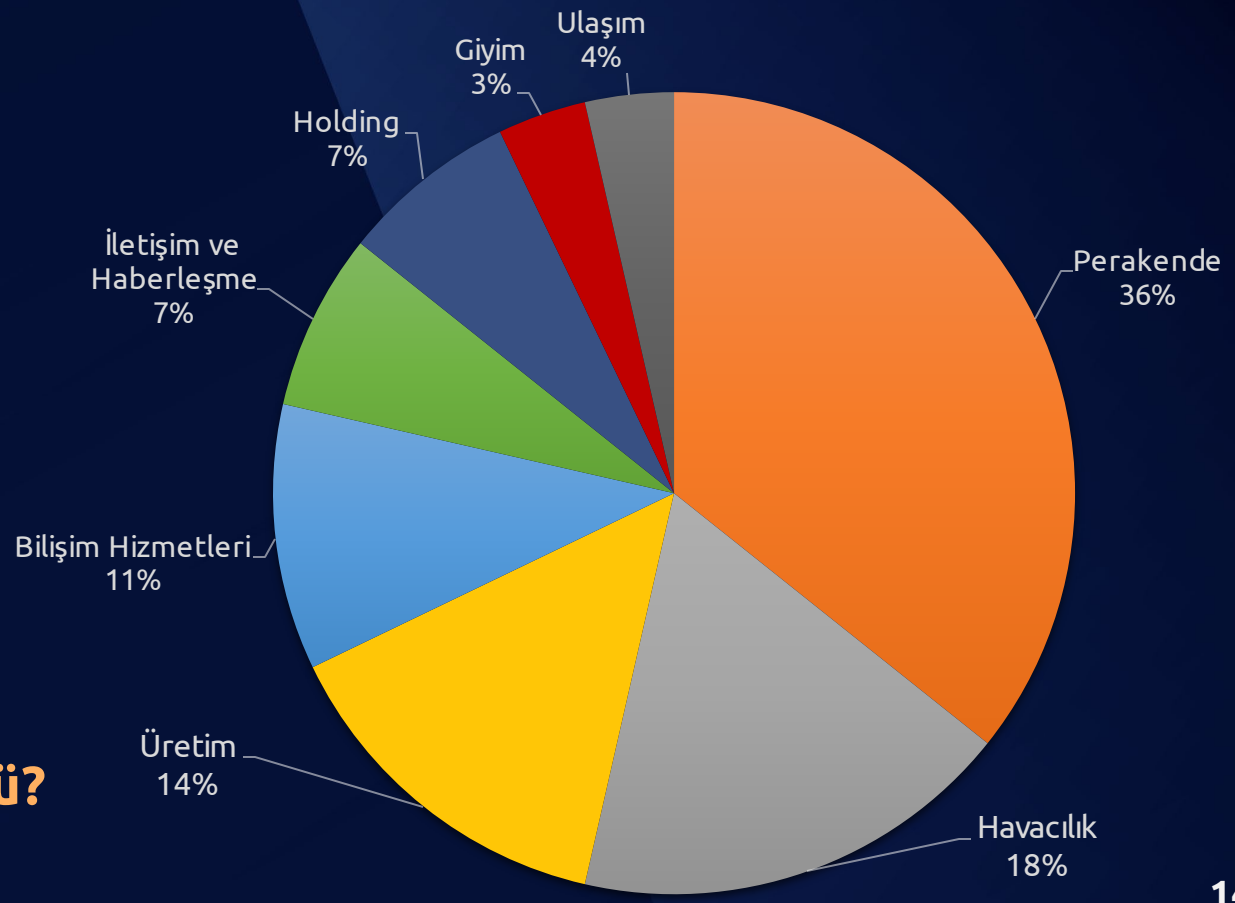
En Çok Vaka Gerçekleşen Sektörler

2023 yılında yaşanan ekonomik hareketlilik nedeniyle **perakende** sektöründe yer alan kurumlar çeşitli hacker gruplarının hedefi haline gelmiştir. Bununla birlikte **kurumların kendi iç dinamiklerini** test etmek amacıyla **kırmızı takım** faaliyetlerine önem verdiği görülmüştür. Perakende sektöründeki mağazacılık faaliyetleri gerek **iş sürekliliği** gerekse **saldırı yüzeyi** açısından özellikle dikkat edilmesi gereken bir unsurdur.

Mağaza sistemleri hem iş akışını doğrudan etkileyen nitelikte, hem de saldırıya açık ve göz ardı edilen sistemler olduğundan kurumların siber güvenliği için kritik önem arz etmektedir.

Bu sebeple perakende sektöründeki firmalar **7/24 izleme ve olay müdahalesi** konularına yatırım yaparak uçtan uca tüm sistemlerin güvenliğini sağlamalıdır.

Neden PERAKENDE Sektörü?



2023 Yılında Yaşanan Önemli Güvenlik Zafiyetleri & ADEO MDR Servisi Kural Çalışmaları

2023 yılında yayınlanan önemli **Top 15+** 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 istahbaratı 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.

2023 Yılında Yaşanan Önemli Güvenlik Zafiyetleri & Sayılarla ADEO MDR Servisi Kural Çalışmaları

Güvenlik Açığı	Yazılan Kural Sayısı	Ürünlere Eklenen IOC Sayısı
CVE-2023-22809 - Privilege Escalation Vulnerability	4	30
Possible KeePass [CVE-2023-24055] Exploitation Patterns (via powershell)	4	10
(CVE-2022-21894): Secure Boot Security Feature Bypass Vulnerability	8	50
Forta GoAnywhere Zero-Day	5	30
CVE-2023-23397 - Microsoft Outlook Privilege Escalation	15	20
3CXDesktopApp Supply Chain Attack	10	80
Rorschach - Ransomware via XDR Agent	3	4
CVE-2023-21554 - (QueueJumper) — Unauthorized Remote Code Execution	3	9
Novel Malware Persistence Within ESXi Hypervisors	8	31
MOVEit 0Day	10	70
Potential CVE-2023-36884 Exploitation Dropped File	3	13
Possible Outlook Reminder Persistence Attempt [CVE-2023-23397] (via powershell)	4	15
Credentials Harvest from Vulnerable CVE-2023-26258 Arcserve Unified Data Protection (UDP) [via register_event]	3	30
Exploiting Potential Barracuda ESG Zero-Day Vulnerability (CVE-2023-2868) Provides Persistence Through Scheduled Task (via file_event)	9	124
Possible PaperCut CVE-2023-27350 Exploitation Attempt (via cmdline)	4	17
Possible CVE-2023-21716 Microsoft Word Vulnerability Exploitation Patterns (via cmdline)	4	10
Amazon's AWS SSM agent can be used as post-exploitation RAT malware	8	10
New Collide+Power side-channel attack impacts almost all CPUs Vulnerabilities	8	5

2023 Yılında Yaşanan Önemli Güvenlik Zafiyetleri & 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.

2023 Yılında Yaşanan Önemli Güvenlik Zafiyetleri & Sayılarla 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 **90 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.

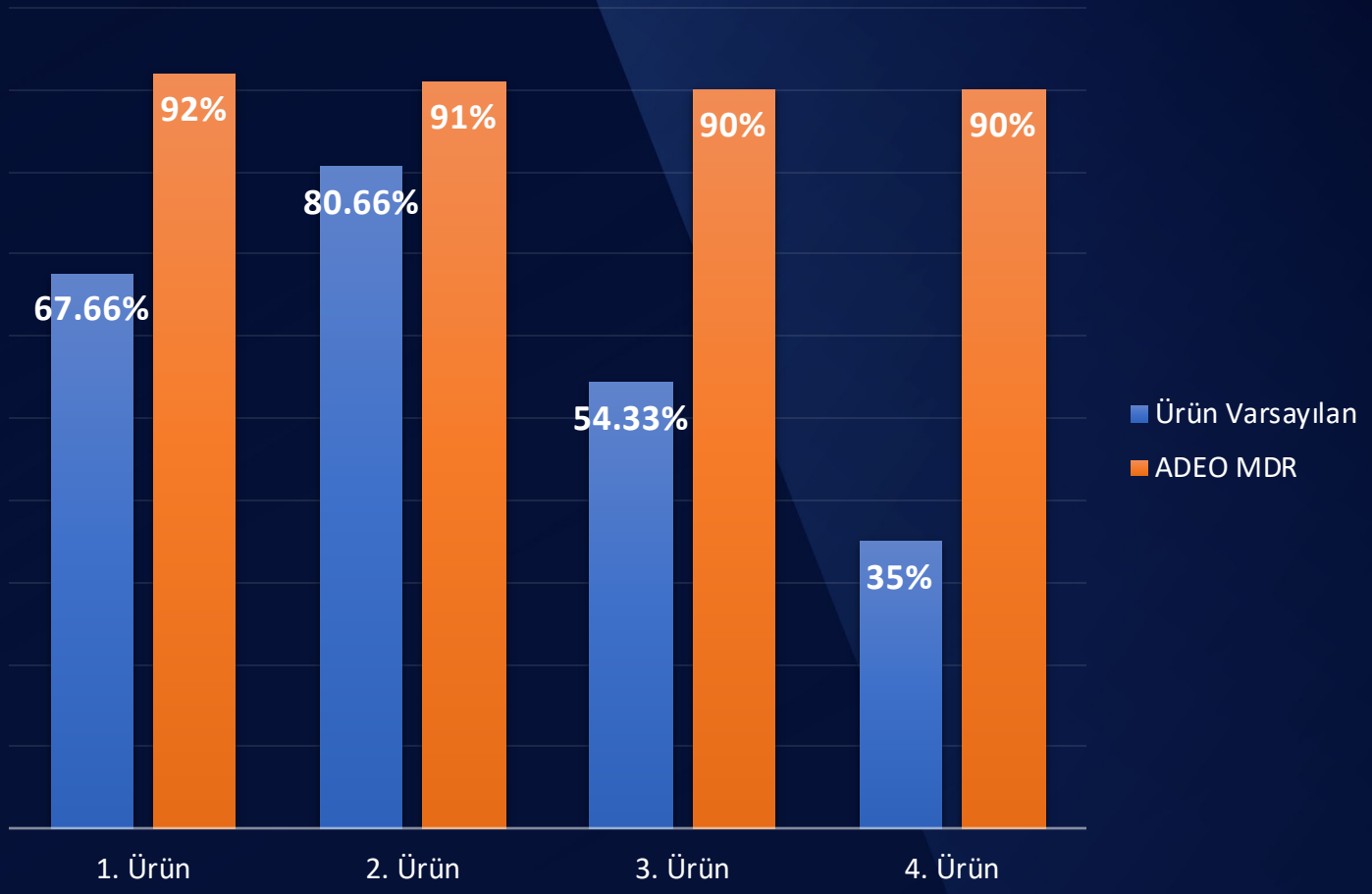
ADEO MDR ekibinin yapmış olduğu çalışmalar sonucunda elde edilen verilere bakıldığında, EDR/XDR tespit mekanizmalarının iyileştirilmesi gerektiği belirlenmiştir. EDR/XDR çözümlerinin kurum/kuruluş yapısına, karşılaşabileceği tehdit ve saldırılara göre iyileştirilmesi, güncel tutulması, en iyi yapılandırma 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 5 dakikanın altına inebilmektedir.

2023 Yılında Yaşanan Önemli Güvenlik Zafiyetleri & Sayılarla ADEO MDR Servisi Kural Çalışmaları

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



2023 Yılında Yaşanan Önemli Güvenlik Zafiyetleri & Sayılarla 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 korunduğunu bilmenin rahatlığıyla işlerine odaklanabiliyor.

Yıllara Göre Kural Sayısı Kıyaslamaları

2021 Kural Sayısı: 600'den 2.000'e

2022 Kural Sayısı: 2.000'den 4.000'e

2023 Kural Sayısı: 4.000'den 5.000'e

yükseldi.

Siber Güvenlikte Dev Adımlar

ADEO'nun Tespit Kurallarının Sayısı Katlanarak Artıyor!

ADEO olarak, siber güvenliğe yatırım yapmaya ve müşterilerimizi siber saldırılara karşı korumaya devam ediyoruz.
Bu kapsamda geliştirdiğimiz tespit (detection) kurallarının sayısını **son iki yılda üç katına çıkararak** büyük bir başarıya imza attık.

ADEO MDR Servisi Tespit Kuralı Sayıları ve Artışları

Geliştirilen Tespit Kuralları,

- TTP (Taktik, Teknik ve Prosedür) bazlı olarak MITRE ATT&CK çerçevesini kapsamakta ve takip etmektedir.
- Bu sayede, siber saldırıların en güncel yöntemlerine karşı da koruma sağlamaktadır.

Tespit kurallarındaki bu artış,

- Müşterilerimizin siber saldırılara karşı daha proaktif ve etkin bir şekilde korunmasını sağlamaktadır.
- Siber saldırıların tespit ve yanıt sürecinin daha hızlı ve verimli olmasına katkıda bulunmaktadır.
- Siber saldırıların neden olabileceği veri kaybı, finansal kayıp ve itibar zedelenmesi gibi riskleri en aza indirmektedir

2021
600 kural

2022
2000 kural

2023
4000 kural

2024
Ocak ayı itibarı ile
5000 kural

2023 Yılının En Sıcak Gündemi #TOP 6

En Yoğun Gün
13 Haziran

13 Haziran'da İncelenen Alarm Sayısı:
3886

Güncel zafiyetlere yönelik kurallar, global trendlerin kontrolü ve tehdit istihbaratlarının takip edilmesiyle hızlıca eklenmektedir.

2023 Yılının En Sıcak Gündemi
#TOP 1| Fortra GoAnywhere Managed File Transfer (MFT)

Fortra GoAnywhere Managed File Transfer (MFT) Nedir?

Fortra GoAnywhere MFT, kuruluşların dosya ve verilerini güvenli, otomatik ve izlenebilir bir şekilde aktarmalarını sağlayan bir yazılım çözümüdür. Platform, şifreleme ve kimlik doğrulama gibi güvenlik özellikleri sunar; otomatik dosya transferleri ve detaylı kayıt tutma gibi işlevler ile zamandan ve emekten tasarruf sağlar. UDP tabanlı ç özümü ile hızlı ve güvenilir dosya aktarımı sunan GoAnywhere MFT, MFTaaS seçeneği ile buluta da entegre edilebilir.

CVE-2023-0669– Fortra GoAnywhere Managed File Transfer (MFT) Remote Code Execution (RCE) Vulnerability Nedir?

Bu zafiyet 7.2 CVSS skoruna sahiptir ve severity değeri "High" olarak belirlenmiştir. Yayınlandığı tarih ise 6 Şubat (06.02.2023) 2023'tür.

28 Ocak 2023 ile 30 Ocak 2023 tarihleri arasında, yetkisiz bir tarafın belirli GoAnywhere müşterilerinin sistemlerine erişmek için zero-day uzaktan kod yürütme (RCE) güvenlik açığını kullandığı keşfedildi.

Yetkisiz tarafın bazı MFTaaS müşteri ortamlarında yetkisiz kullanıcı hesapları oluşturmak için CVE-2023-0669'u kullandığı ortaya çıktı.

Fortra (eski adıyla HelpSystems) GoAnywhere MFT'de, saldırgan tarafından kontrol edilen keyfi bir nesnenin serileştirilmesi nedeniyle Lisans Yanıtı Servlet'inde (License Response Servlet) kimlik doğrulama öncesi komut enjeksiyonu güvenlik açığı bulunmaktadır.

CVE-2023-0669– Fortra GoAnywhere Managed File Transfer (MFT) Remote Code Execution (RCE) Vulnerability Saldırısının Faaliyetleri Nelerdir?

Yetkisiz tarafın 28 Ocak 2023 ile 31 Ocak 2023 tarihleri arasında bazı MFTaaS müşteri ortamlarına "Netcat" ve "Errors.jsp" olmak üzere en fazla iki ek araç yüklemek için CVE-2023-0669 kullandığı tespit edildi.

Cl0p ransomware grubu 2023 yılındaki aktivitelerinde bu zafiyetten yararlanmıştır.

Özel oluşturduğumuz algılama kurallarını ne kadar süre ile güncelledik?

ADEO MDR Servisi olarak CVE-2023-0669 – Fortra GoAnywhere Managed File Transfer (MFT) Remote Code Execution (RCE) zafiyeti hakkındaki davranışları kendi laboratuvar ortamlarımızda canlandırıp, ilgili davranışların tespit edilebilmesi için farklı paternler kullandık.
Toplam **5 tespit kuralı ve 30 adet IOC**, tüm müşterilerimize **2 saat** içerisinde aktarılmıştır.

2023 Yılının En Sıcak Gündemi #TOP 2| PaperCut NG/MF

PaperCut NG/MF Nedir?

PaperCut NG/MF, kuruluşların baskı işlerini yönetmesine ve optimize etmesine yardımcı olan bir yazılımdır. (Print Management Software)

CVE-2023-27350 – PaperCut NG/MF Security Vulnerability Nedir?

20 Mart 2023 tarihinde, CVE-2023-27350 olarak adlandırılan kritik bir güvenlik açığı keşfedilmiştir. Bu zafiyet, 9.8'lik bir CVSS skoruna sahiptir ve "Critical" (Kritik) olarak derecelendirilmiştir. Bu, zafiyetin son derece tehlikeli olduğu ve acilen düzeltilmesi gerektiği anlamına gelir.

Zafiyet, saldırganların PaperCut MF/NG yazılımındaki kimlik doğrulamasını atlamasına ve SYSTEM ayrıcalıklarına sahip kod çalıştırmasına olanak tanır. Bu, saldırganların etkilenen sistemlerde tam kontrol elde etmesine, veri hırsızlığı veya fidye yazılımı saldırıları gerçekleştirmesine ve sistem bozulmasına yol açabilir. Cl0p Ransomware grubunun bu zafiyeti aktif olarak kullandığı bilinmektedir.

CVE-2023-27350 Zafiyetinin Etkileri Nelerdir?

Cl0p Ransomware grubu tarafından kullanılmıştır. SYSTEM haklarında kod çalıştırılacağı için zafiyetin etkisi daha büyük boyuta evrilmektedir.

Özel oluşturduğumuz algılama kurallarını ne kadar süre ile güncelledik?

ADEO MDR Servisi olarak CVE-2023-27350 - PaperCut NG/MF zafiyetinin davranışlarını kendi laboratuvar ortamlarımızda canlandırıp, ilgili davranışların tespit edilebilmesi için farklı paternler kullandık.
Toplam **4 tespit kuralı** ve **17 IOC**, tüm müşterilerimize **1,5** saat içerisinde aktarılmıştır.

2023 Yılının En Sıcak Gündemi
#TOP 3| Dark Power Ransomware

Dark Power Ransomware Grubu, ilk olarak Şubat 2023'te ortaya çıkan yeni bir fidye yazılımı grubudur. Kısa bir süre içinde Türkiye'yi de hedef alması ve NIM tarafından yazılan fidye yazılımı kullanması ile dikkat çekmeyi başarmıştır.

En Çok Etkilenen Ülkeler ve Sektörler?

Dark Power Ransomware grubunun birçok alanda faaliyet gösterdiği tespit edildi. Hedef aldığı bazı sektörleri; eğitim, sağlık ve imalat olarak sıralayabiliriz. Amerika Birleşik Devletleri, Peru, Türkiye, Fransa, İsrail, Mısır, Cezayir gibi bazı ülkelere Dark Power tarafından saldırılar yapıldığı tespit edildi.

Dark Power'ın 2023 Faaliyetleri?

Dark Power'ın sadece Şubat ayında 10 farklı organizyona saldırdığı tespit edildi. Özellikle saldırdıkları ülkelerin çeşitliliğinden küresel bir tehdit olduğunu söyleyebiliriz. Saldırılarda kullandıkları zararlılarını Nim ile yazmışlardır. Nim ransomware grupları arasında nispeten yeni yaygın olmaya başlayan bir çoklu platform (multi-platform) dilidir. Dosyaları şifrelerken ise Nimcrypto kütüphanesini kullanıyorlar. Şifrelenmiş dosyalarını "dark_power" uzantısını ile kaydediyorlar. Dark Power hacklediği kurumların ödeyeceği fidye tutarını 10.000$ değerinde XMR (Monero) olarak belirlemiştir. Fidye tutarı ödenmediği takdirde 72 saat içerisinde ele geçirdikleri verileri halka açık bir şekilde yayınlayacaklarını belirtiyorlar. Dark Power kullanıcılara saldırırken genelde oltalama saldırısı tekniğini kullanıyor.

Özel oluşturduğumuz algılama kurallarını ne kadar süre ile güncelledik?

ADEO MDR Servisi olarak Dark Power ransomware grubunun davranışlarını kendi laboratuvar ortamlarımızda canlandırıp, ilgili davranışların tespit edilebilmesi için farklı paternler kullandık. Toplam **2 tespit kuralı ve 27 IOC**, tüm müşterilerimize **2.5 saat** içerisinde aktarılmıştır.

2023 Yılının En Sıcak Gündemi
#TOP 4| CVE-2023-23397 - Outlook Vulnerability

CVE-2023-23397 - Outlook Vulnerability Nedir?

Zafiyet 9.8 CVSS skoruna sahiptir ve severity değeri "Critical" olarak belirlenmiştir. Yaylandığı tarih ise 14 Mart (14.03.2023) 2023'tür.

Microsoft Outlook'ta bulunan ve bir tehdit aktörünün, saldırgan tarafından kontrol edilen bir Sunucu İleti Bloğu (SMB) sunucusuna işaret eden Evrensel Adlandırma Kuralı (UNC) yolunu içeren özel bir PidLidReminderFileParameter özelliğine sahip bir ileti (.msg) dosyası oluşturmasına olanak tanıyan bir güvenlik açığıdır. PidLidReminderFileParameter, mesaj gönderenin toplantı bildirimleri gibi öğeler için özel bir bildirim sesi ayarlamasına olanak tanır.

Tehdit aktörü tarafından kontrol edilen SMB sunucusuna yapılan bağlantılar, hedeflenen kullanıcının Net-NTLMv2 hashlerini sızdıracaktır. Tehdit aktörü daha sonra bu hashleri kullanarak NTLMv2 kimlik doğrulamasını destekleyen diğer sunucularda kimlik doğrulaması gerçekleştirebilir veya açık metin kimlik bilgilerini (clear-text credentials) elde etmek için hashleri offline olarak kırmaya çalışabilir. Saldırganlar eğer SMB ile NTLMv2 hash değerine erişemezlerse webdav üzerinden bir bağlantı da sağlamaktadır.

Saldırı yalnızca hedeflenen kullanıcının mail almasını gerektirir. İstismarın tetiklenmesi için hiçbir kullanıcı etkileşimi gerekmez (zero-click).

CVE-2023-23397 Zafiyetinin Etkileri Nelerdir?

APT28 tarafından bu güvenlik açığı; hükümet, enerji ve ulaştırma sektöründeki Avrupa kuruluşlarını hedef almak için kullanıldı. Microsoft'u hedef alan APT28 grubu Rusya ile ilişkilendirilmektedir.

Dolayısıyla Microsoft Outlook (web outlook dışında) kullanılan clientlerde NTLMv2 hash bilgileri bu zafiyet vasıtasıyla tetiklenerek dışarı çıkarılabilir veya çıkarılmış olabilir. Bu dünya genelinde büyük bir etki yaratmıştır ve Polonya başta olmak üzere çeşitli devlet ve hükümet kurumlarında kullanılmıştır. Burada devletler arası siber savaşta koz olarak kullanılacak bir zafiyet olduğu varsayımında bulunabiliriz.

Özel oluşturduğumuz algılama kurallarını ne kadar süre ile güncelledik?

ADEO MDR Servisi olarak CVE-2023-23397 - Outlook Güvenlik açığı davranışlarını kendi laboratuvar ortamlarımızda canlandırıp, ilgili davranışların tespit edilebilmesi için farklı paternler kullandık.
Toplam **10 tespit kuralı ve 22 IOC,** tüm müşterilerimize **3 saat** içerisinde aktarılmıştır.

2023 Yılının En Sıcak Gündemi #TOP 5| MOVEit SQL Zafiyeti

MOVEit Uygulaması Nedir?

MOVEit Transfer (eski adıyla MOVEit DMZ veya MOVEit File Transfer), kullanıcılar için basit tarayıcı erişimi ile ortak bir paylaşılan klasör kullanarak kuruluşlar içinde ve arasında; sunucular, sistemler ve uygulamalar arasında ve ayrıca gruplar ve bireyler arasında dosya ve veri alışverişini destekler.

CVE-2023-34362 - MOVEit SQL Zafiyeti Nedir?

Zafiyet 9.8 CVSS skoruna sahiptir ve severity değeri "Critical" olarak belirlenmiştir.

Progress Software'ın MOVEit Transfer web uygulamasında kimliği doğrulanmamış (unauthenticated) bir saldırganın MOVEit Transfer'in veritabanına erişmesine izin verebilecek bir SQL enjeksiyonu güvenlik açığıdır. Kullanılan veritabanı motoruna (MySQL, Microsoft SQL Server veya Azure SQL) bağlı olarak, bir saldırgan veritabanının yapısı ve içeriği hakkında bilgi çıkarabilir ve veritabanı öğelerini değiştiren veya silen SQL sorgularını çalıştırabilir.

CVE-2023-34362 - MOVEit SQL Zafiyetinin Etkileri Nelerdir?

Cl0p Ransomware grubu tarafından kullanılmıştır. Cl0p Rusya bağlantılı bir fidye yazılım çetesidir. Birçok kuruluş tarafında SQL injection zafiyeti ransomware ile sonuçlanmıştır.

MOVEit saldırılarında kimler hedef alındı?

Clop, Rusya bağlantılı bir fidye yazılım çetesidir. ABD'deki federal kurumlara kimin sızdığı çok belli olmasa da Clop olarak bilinen fidye yazılımı çetesinin son haftalarda üniversiteler, bankalar ve büyük çok uluslu şirketler de dahil olmak üzere yüzlerce kuruluşa saldırmak için MOVEit yazılımındaki açıkları kullandığı ortaya çıkmıştı. İngiltere'nin iletişimden sorumlu düzenleyici kurumu Ofcom da MOVEit siber saldırılarında bazı gizli bilgilerinin ele geçirildiğini söyledi. Kurum yaptığı açıklamada, hackerların düzenlediği saldırılar sonucu şirketlerle ilgili bazı verilerin ve 412 Ofcom çalışanının kişisel bilgilerinin ihlal edildiğini doğruladı.

MOVEit güvenlik açığından yararlanılan ülkeler sıralandığında, bilinen ihlale uğramış yapıların %72.2'si ABD, %6.6'sı Almanya, %3.9'u ise Birleşik Krallık ve Kanada'da bulunduğu öğrenildi.

Özel oluşturduğumuz algılama kurallarını ne kadar süre ile güncelledik?

ADEO MDR Servisi olarak CVE-2023-34362 - MOVEit SQL Zafiyetinin davranışlarını kendi laboratuvar ortamlarımızda canlandırıp, ilgili davranışların tespit edilebilmesi için farklı paternler kullandık.
Toplam **10 tespit kuralı ve 70 IOC**, tüm müşterilerimize **3 saat** içerisinde aktarılmıştır.

2023 Yılının En Sıcak Gündemi
#TOP 6| Barracuda Email Security Gateway

Barracuda Email Security Gateway Nedir?

Barracuda ESG (E-mail Security Gateway), Barracuda Email Security Gateway, kurumları e-posta kaynaklı tehditlerden ve veri sızıntılarından korumak için gelen ve giden tüm e-posta trafiğini yöneten ve filtreleyen bir e-posta güvenlik ağ geçididir. Bu hizmetin birçok kuruluş tarafından kullanıldığı bilinmektedir.

CVE-2023-2868- Barracuda Email Security Gateway Vulnerability

Zafiyet 9.8 CVSS skoruna sahiptir ve severity değeri "Critical" olarak belirlenmiştir.

Barracuda Email Security Gateway (ESG) ürününde bulunan bir uzaktan kod yürütme (RCE) zafiyetidir. Barracuda zero-day güvenlik açığı, CVE-2023-2868 kimliği ve 9.8 kritik CVSS puanı ile 19 Mayıs 2023'te resmi olarak açıklandı.

Bu zafiyet, ".tar" dosyalarının işlenmesinde kullanılan işlemin yeterince temizlenmemesi nedeniyle ortaya çıkmaktadır. Zafiyet, kullanıcı tarafından sağlanan ".tar" dosyasının içeriğindeki dosya adlarının doğrulanmasının eksik olmasından kaynaklanmaktadır. Saldırgan, bu dosya adlarını belirli bir şekilde biçimlendirerek, Email Security Gateway ürününün yetkileriyle Perl'in "qx" operatörü aracılığıyla uzaktan bir sistem komutu yürütmeyi başarabilir.

Bu da, "Perl'ün qx{} rutini aracılığıyla bir sistem komutu olarak çalıştırılan bir değişkeni aracılığıyla etkin bir şekilde temizlenmemiş ve filtrelenmemiş kullanıcı kontrollü girdi" anlamına gelir.

Barracuda ESG Zero-day Saldırısının Faaliyetleri Nelerdir?

Yapılan analizlere göre, bu güvenlik açığının ilk kez sömürülme tarihi 10 Ekim 2022 olarak belirlendi. Bu saldırı, Çin destekli APT grubu UNC4841 tarafından gerçekleştirildi. (3) Avrustralya Başkent Bölgesi Hükümetinin bu saldırıdan etkilendiği belirtildi. Ayrıca Barracuda'nın yaptığı açıklamaya göre dünya çapında cihazların %5'I etkilendi.

Özel oluşturduğumuz algılama kurallarını ne kadar süre ile güncelledik?

ADEO MDR Servisi olarak CVE-2023-2868 - Barracuda Email Security Gateway Zafiyetinin davranışlarını kendi laboratuvar ortamlarımızda canlandırıp, ilgili davranışların tespit edilebilmesi için farklı paternler kullandık. Toplam **9 tespit kuralı** ve **124 IOC**, tüm müşterilerimize **2.5 saat** içerisinde aktarılmıştır.

ADEO
CYBER SECURITY

DFIR

ADEO 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

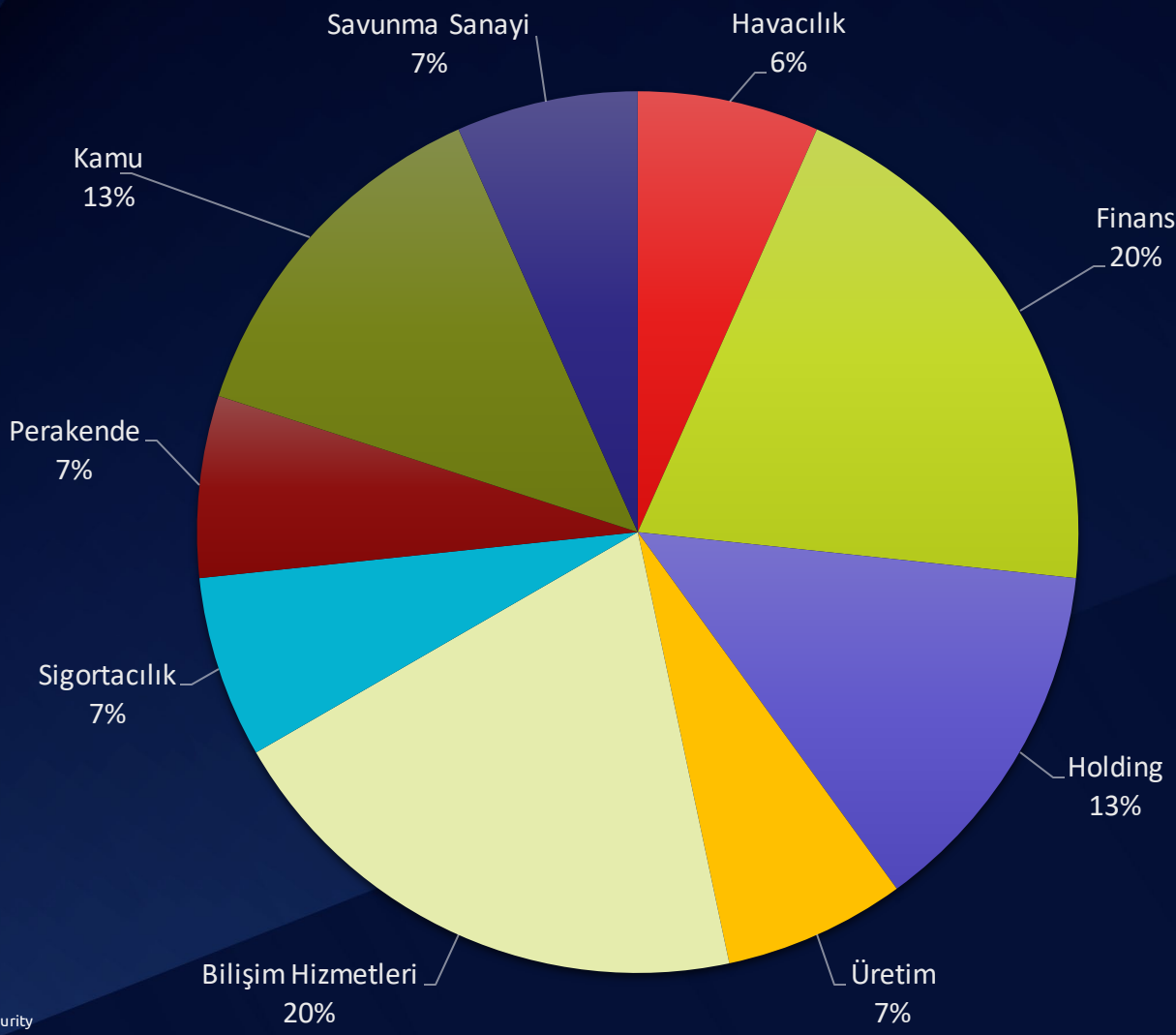
tespit edilir ve detaylı bir şekilde analiz edilerek raporlanır.

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 DFIR Servisi

2023 Yılında Müdahale Edilen Vakaların Sektörlere Göre Dağılımı:



Vakalar Sırasında Görülen Temel Durumlar

Ransomware (Fidye Yazılımları):

Mevcut hedef kişi veya kurumlara karşı saldırganlar tarafından tehdit ve şantaj amaçlı Encryption aktiviteleri yapıldığı görülmüştür. İlk erişimi elde eden (Vulnerability Exploitation, Phishing vb.) saldırganlar keşif araçları (Nmap, theHarvester vb) kullandıktan sonra ağ içinde yayılarak (Credential Dumping-Mimikatz) olabildiğince çok cihaz üzerinde veri kaçırma (Data Exfiltration) ve veri şifreleme (Data Encryption) işlemini gerçekleştir ve kurumdan fidye talep ettikleri bir e-posta ile isteklerini bildirirler.

- File and System Encryption (Dosya ve Sistem Kilitleme)
- Ransom Demands (Fidye Talepleri)

Cyber Espionage (Siber Casusluk):

Saldırgan gruplar tarafından herhangi bir şifreleme aktivitesi/ fidye talebi olmaksızın gerçekleştirilen veri kaçırma işlemleri ile karşılaşılmıştır. Doğrudan finansal kazanca dönüştürülmeyen bu gibi aktiviteler "Cyber Espionage" başlığı altında toplanabilir.

- Information Gathering (Bilgi Toplama)
- Targeted Data Theft (Hedefe Özgü Veri Çalma)

E-mail Phishing (E-posta Oltalaması):

Siber saldırganlar tarafından özellikle ilk erişimi elde etme (Initial Access) ve e-posta manipülasyonu (E-mail Tampering) için tercih edilen bir siber saldırı tekniğidir.

Alt başlıklar:

- Data Encryption (Veri Şifreleme)
- Data Exfiltration (Veri Sızdırma)
- Data Corruption/Loss (Veri Bozulması/Kaybı)
- Crypto Miners (Kripto Madenciler)
- Intrusion (İstilacılık)

Info Stealer Malware (Bilgi Çalan Kötü Amaçlı Yazılımlar):

Saldırılar sırasında hedefe yönelik bilgi çalma aktiviteleri gerçekleştirildiği görülmüştür. Bu aktiviteler esnasında kullanılan zararlı yazılımlar "Info Stealer Malware" başlığı altında toplanabilir.

- Personal Identifiable Information (PII) (Kişisel Tanımlanabilir Bilgiler)
- Financial Information (Finansal Bilgiler)
- Credit Card Information etc. (Kredi Kartı Bilgileri vb.)

Karşılaşılan Vakalarda Saldırganlar Tarafından Kullanılan Taktik ve Teknikler:

Obfuscation:

Tespit(detection) araçlarından kaçınmak ve analiz sürecini yavaşlatmak için bir Anti-Forensics yöntemi olarak Obfuscation, karşılaştığımız vakalarda saldırganlar tarafından sıklıkla tercih edilmiştir.

- Veri Kodlama/Şifreleme
- Gereksiz Kod Ekleme

Spear Phishing:

Doğrudan spesifik bir hedefe yönelik saldırılarda uygulanan metodolojidir.

- E-posta üzerinden
- Hedefe Özel Saldırılar

Vulnerability Exploitation (Zafiyet Sömürüsü):

Özellikle güncel patch'lerin takip edilmediği sistem ve uygulamalarda yer alan açığın saldırganlar tarafından amaca yönelik kullanımıdır. Keşfedilen zafiyetlerin yayınlandığı bazı platformları (NVD, MITRE vb.) saldırganlar da takip etmekte ve saldırıları esnasında bu platformlardaki bilgilerden yararlanarak önlemi alınmamış/güncel olmayan hedef sistem/uygulama üzerinde kötü amaçlı aktivitelerini gerçekleştirmektedirler.

Karşılaşılan Vakalarda Saldırganlar Tarafından Kullanılan Taktik ve Teknikler:

Genellikle Uzaktan Kod Çalıştırma (RCE) Zafiyetleri

Spray&Pray:

- Zafiyet Sömürüsü Kapsamında
- Yayma ve Umma Yaklaşımı

Lateral Movement (Yanal Hareket):

- Kimlik Bilgisi Çalma
- Sistemler Arası Hareket

Discovery (Keşif):

- Ağ Taraması vb.
- Hedef Sistemlerin Tanımlanması

Persistence (Kalıcılık):

- Arka Kapılar
- Kayıt Defteri Değişiklikleri
- Zamanlanmış Görevler vb.

Saldırganların Para Kazanma Metotları

- Ransomware (Doğrudan fidye talebi)
- Crypto Miners (Kaynakların kripto para kazanımı için kullanımı)
- Data Theft and Sale (Verilerin çalınması ve satılması)
- Carding (Kart bilgilerinin çalınıp nakite dönüştürülmesi)
- Blackmailing [Tehdit ve şantaj (DDOS Attack vb.)]

Karşılaşılan İlk Erişim (Initial Access) Metotları

- External Remote Services/Exploit Public-Facing Application
- Phishing
- Malware
  - Reverse/Bind ShellCrypto Miners (Kaynakların kripto para kazanımı için kullanımı)
  - Remote Control Tools (Ammyy Admin, Anydesk vb.)

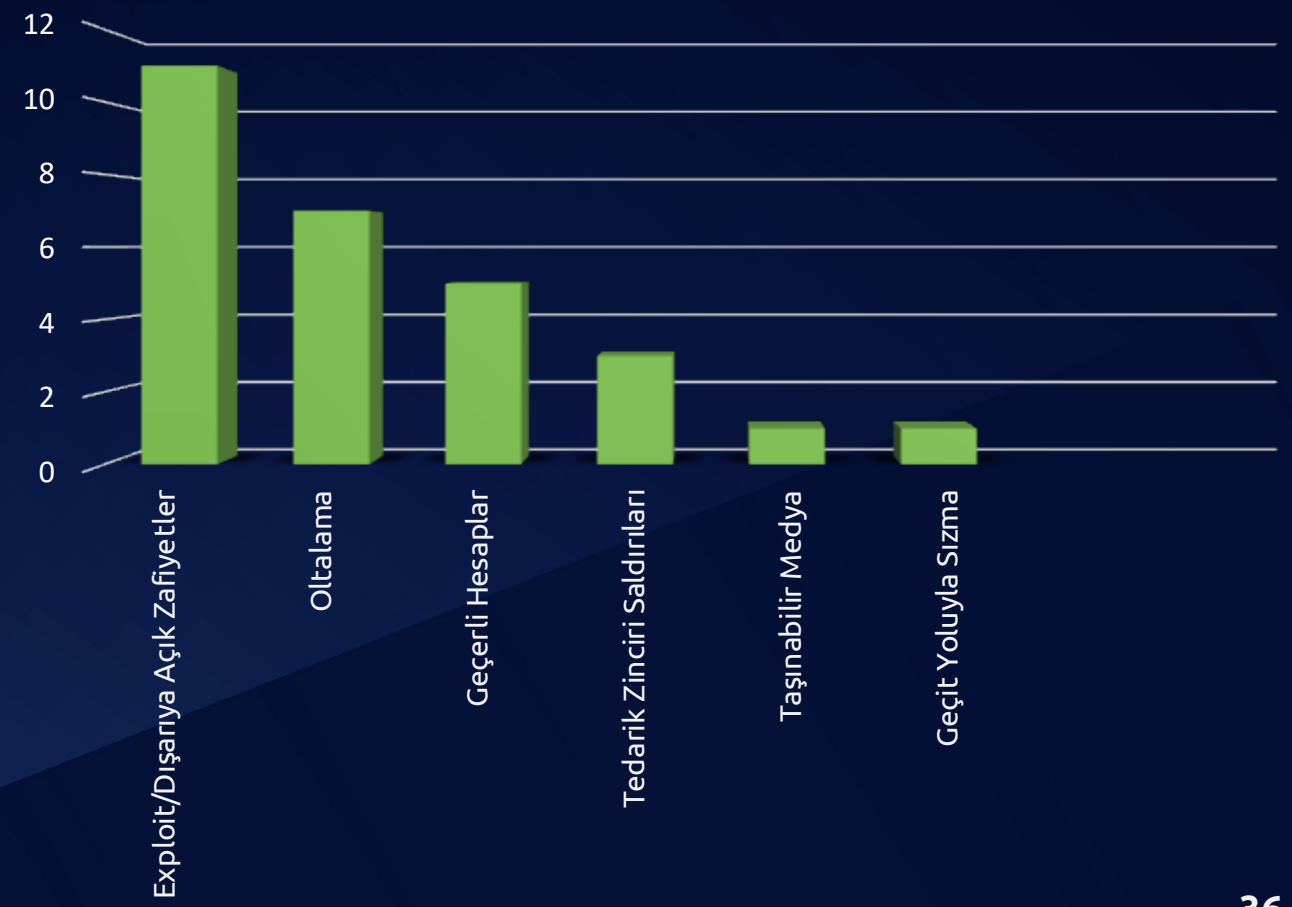
En Çok Kullanılan İlk Erişim Teknikleri

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.

"İlk erişimin engellenmesi sistemin güvenliği açısından büyük önem arz etmektedir."



ADEO CYBER SECURITY

ADEO MDR Servisi

Taktikler, Teknikler ve Tespit Kurallarımız

Saldırı Tespit Kurallarımız

Siber Güvenlikte Zirve: ADEO'nun %94'lük 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.

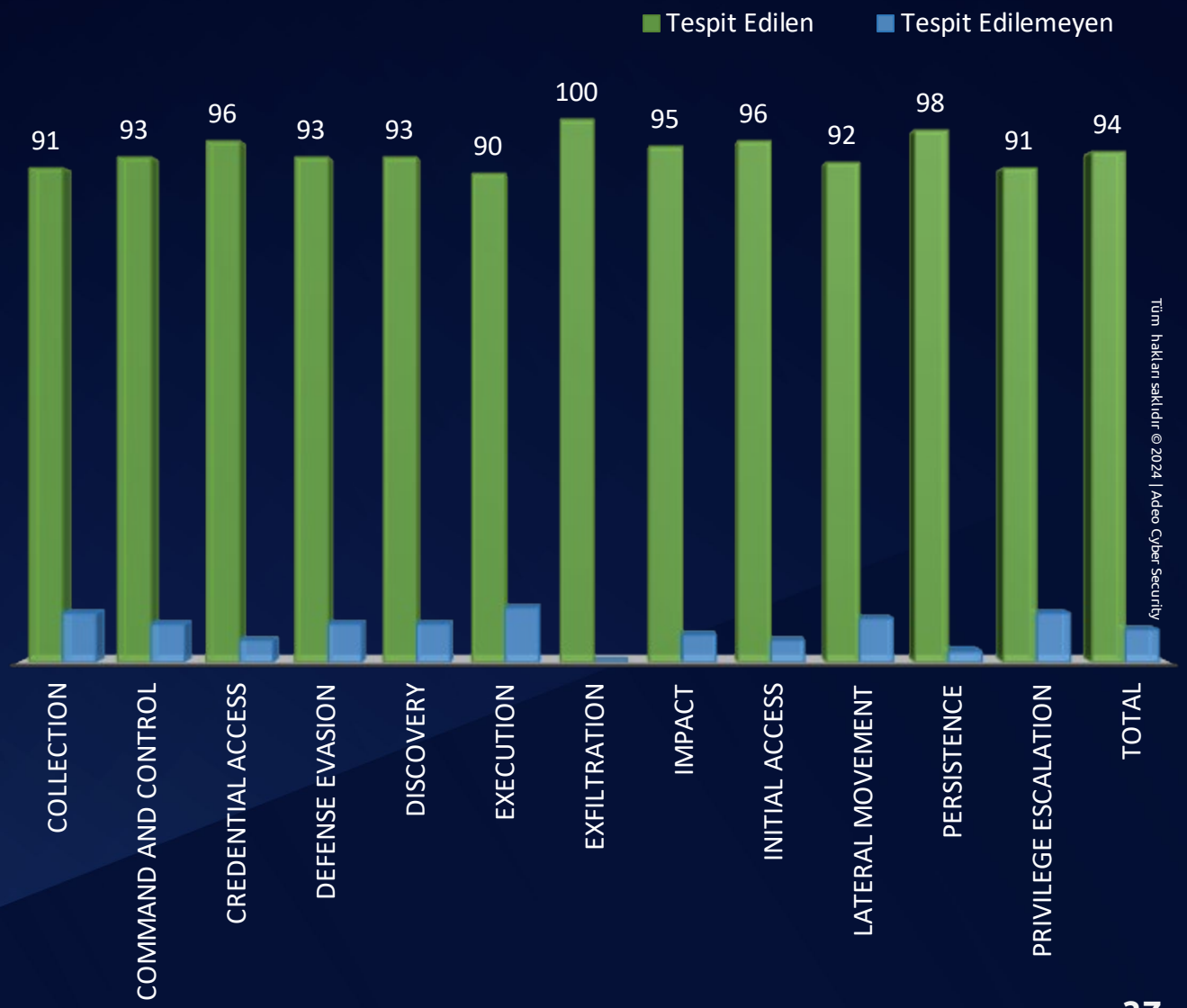
ADEO olarak, siber güvenlik yaklaşımlarımızda müşterilerimizi siber saldırılara karşı korumak için;

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

%94'lük tespit(detection) oranıyla sunduğumuz servis hizmeti bu konudaki uzmanlığımızın somut verilerinden biri olarak 2023 raporunda yerini alıyor.

2023 yılında gerçekleşen **11.507 adet saldırı** tekniği sonrasında, **12 MITRE ATT&CK TTP değeri** referans alındığında, ortalama **%94 tespit(detection) oranına** sahip olduğumuz görülüyor.

Son 3 yıldır, MITRE ATT&CK TTP sayısı artmasına rağmen, aktif kural geliştirme çalışmalarımız sayesinde bu oran **%94+** seviyesinin üzerinde kalmaya devam ediyor.



Taktikler

1.Veri Toplama (Collection)

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

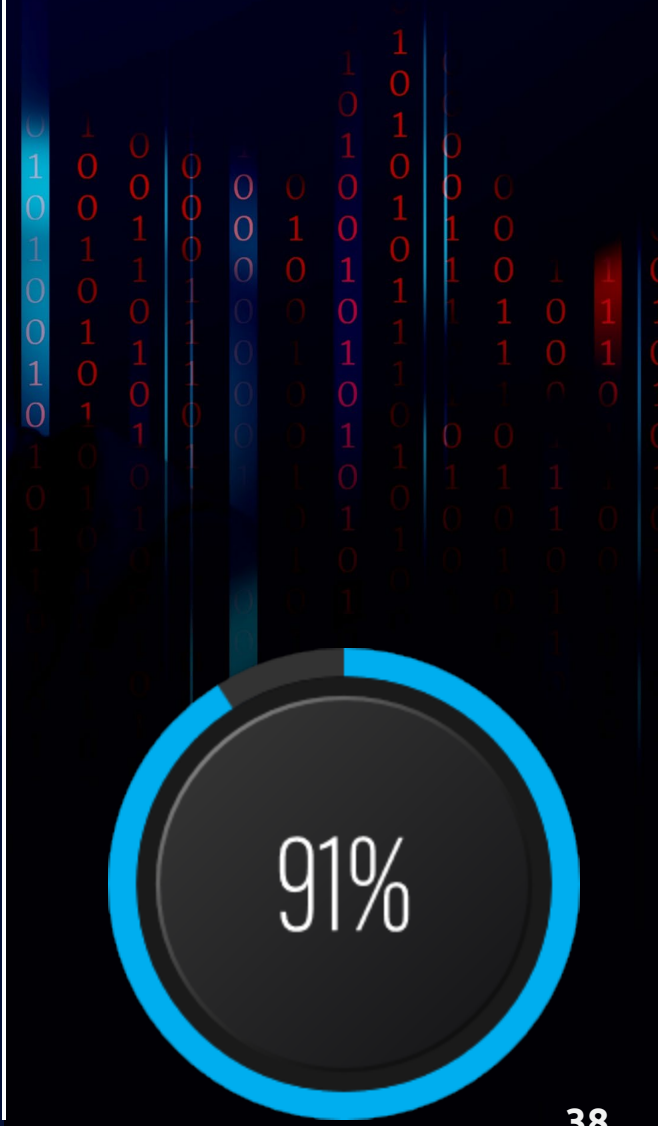
Bu taktik, saldırganın amacına hizmet eden verileri toplamak için kullandığı tekniklerden oluşur.

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 **%91'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.



Taktikler

2.Komuta ve Kontrol (Command And Control)

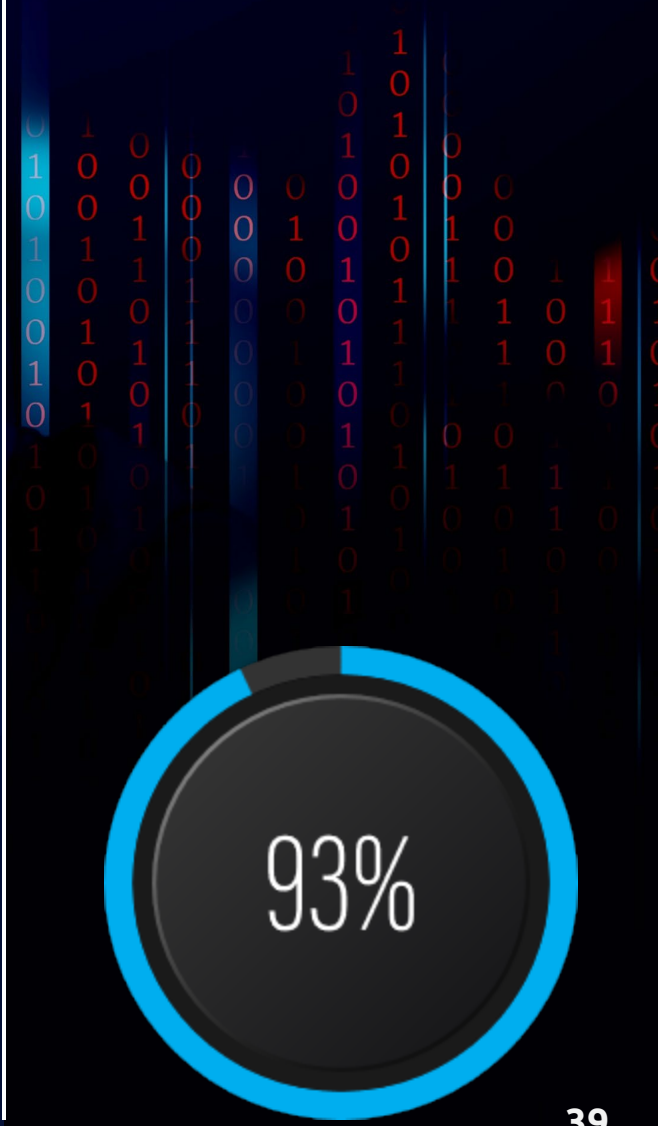
Saldırgan kontrolü ele geçirmek için güvenliği ihlal edilmiş sistemlerle iletişim kurmayı dener. Bunu yaparken tespit edilmekten kaçınmak için genellikle normal, beklenen trafiği taklit etmeye çalışır.

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 **%93'ü** 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.**



Taktikler

3.Kimlik Bilgileri Erişimi (Credential Access)

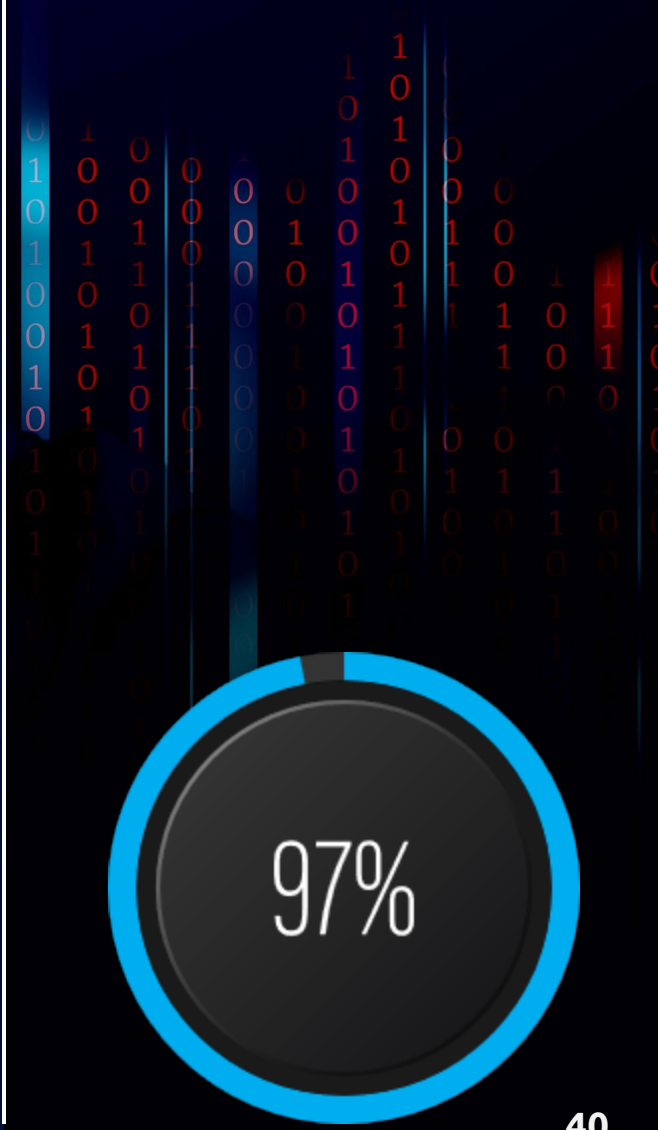
Saldırgan bu taktik ile hesap adlarını ve parolalarını çalmayı dener.

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 **%97'si** 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.



Taktikler

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 **%93'ü** ADEO MDR Servisi tarafından tespit edilebilmektedir.

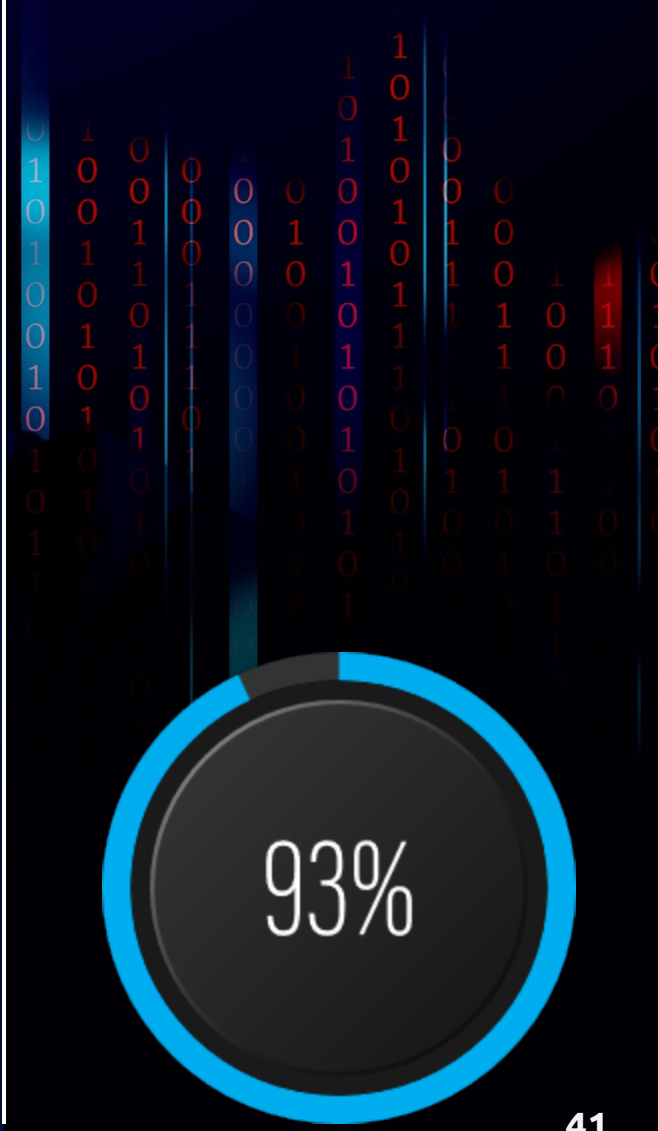
- **PowerShell** ve **Command Prompt** komut satırı uygulamaları aracılığı ile yapılan aktivitelerin analiz edilebilmesi için ilgili uygulamaların loglarının merkezi bir noktada kaydedilmesi/arşivlenmesi önerilir. Hizmet engelleme saldırılarından **(DoS / DDoS)** korunmak ve atak türlerini minimize etmek 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.



Taktikler

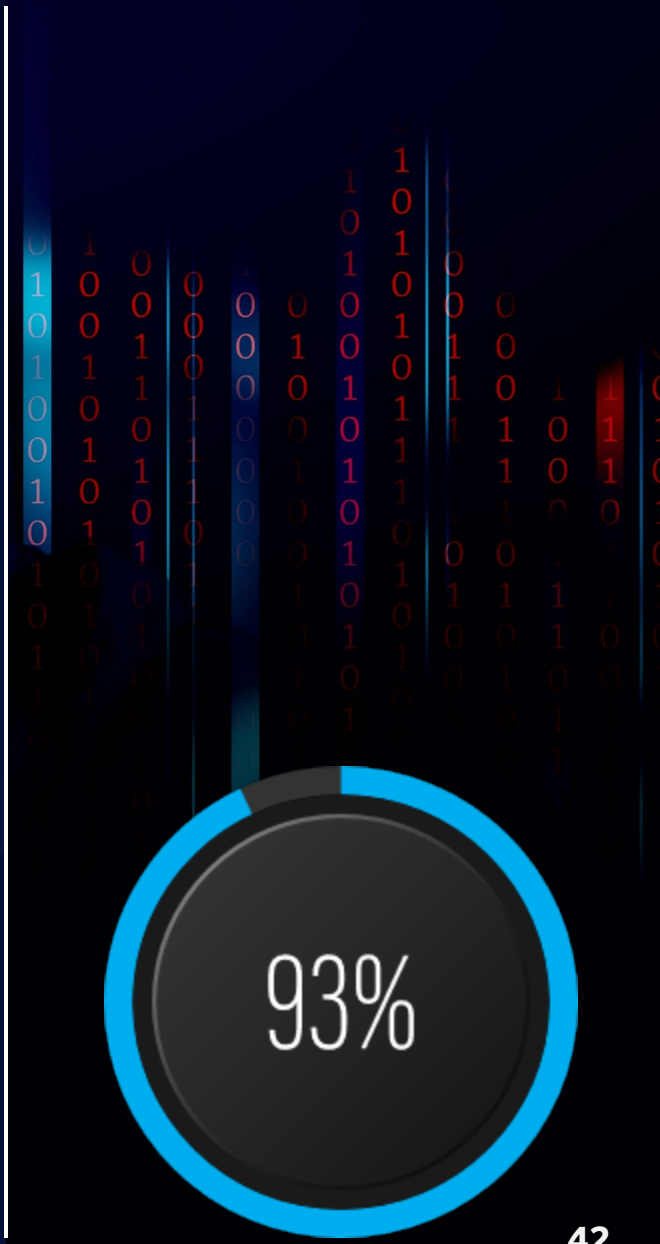
5.Keşif (Discovery)

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 **%93'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.



Taktikler

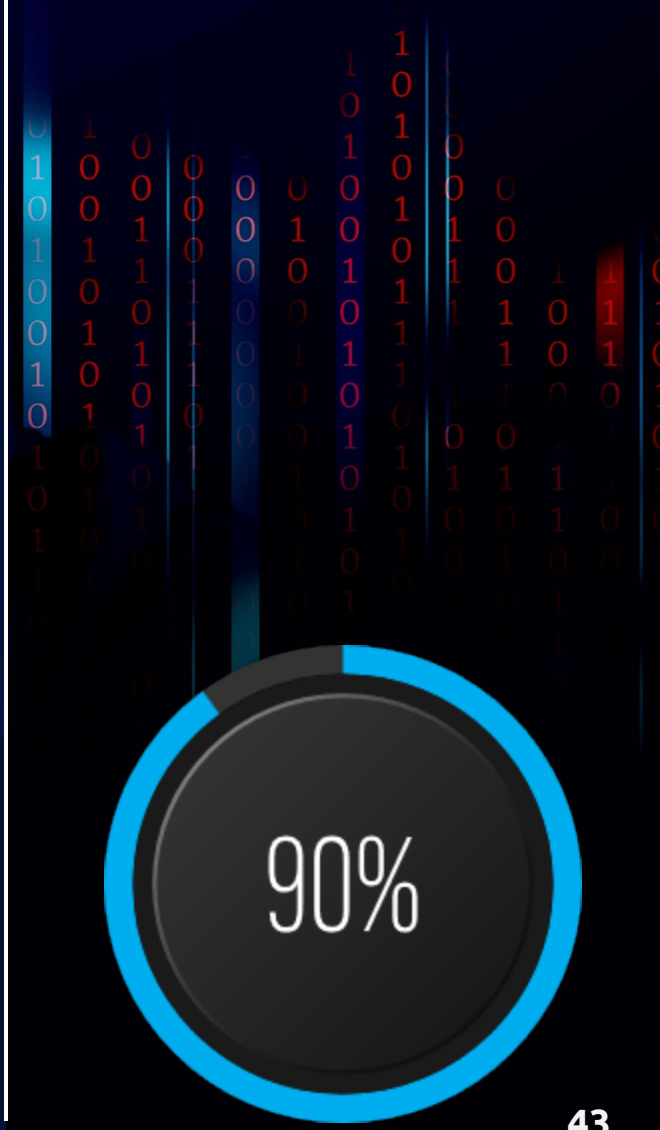
6. Yürütme (Execution)

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 **%90'ı** 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.**



Taktikler

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.

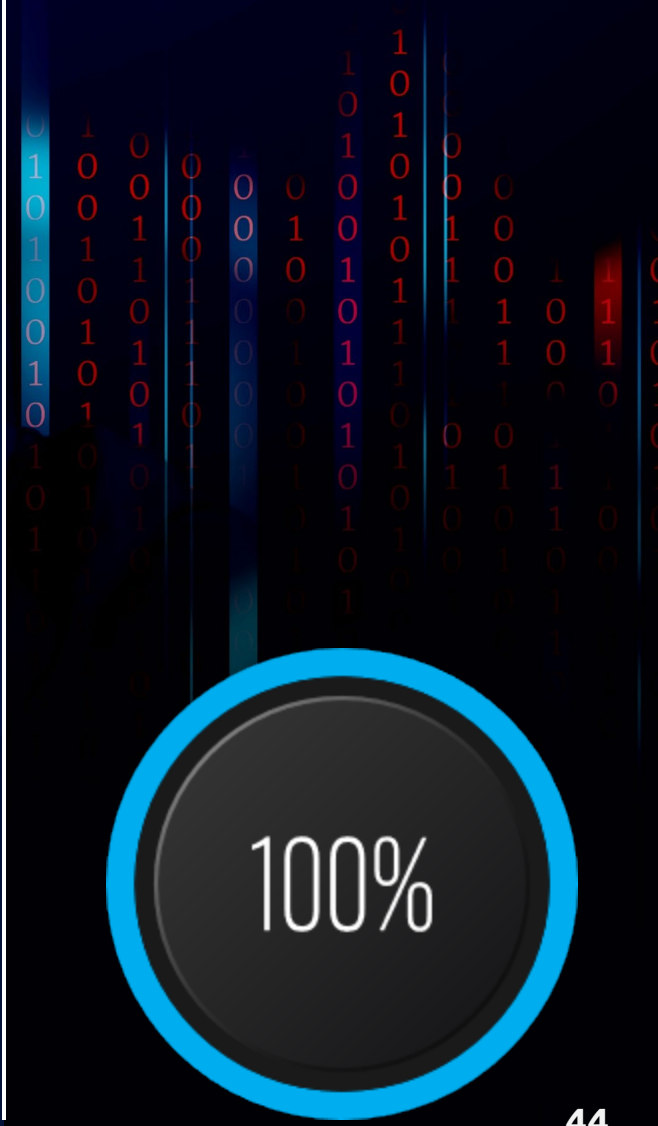
Veri Kaçırma (Exfiltration) taktiği kullanılarak yapılan saldırıların **%100'ü** ADEO MDR Servisi tarafından tespit edilebilmektedir.

- 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.



Taktikler

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.

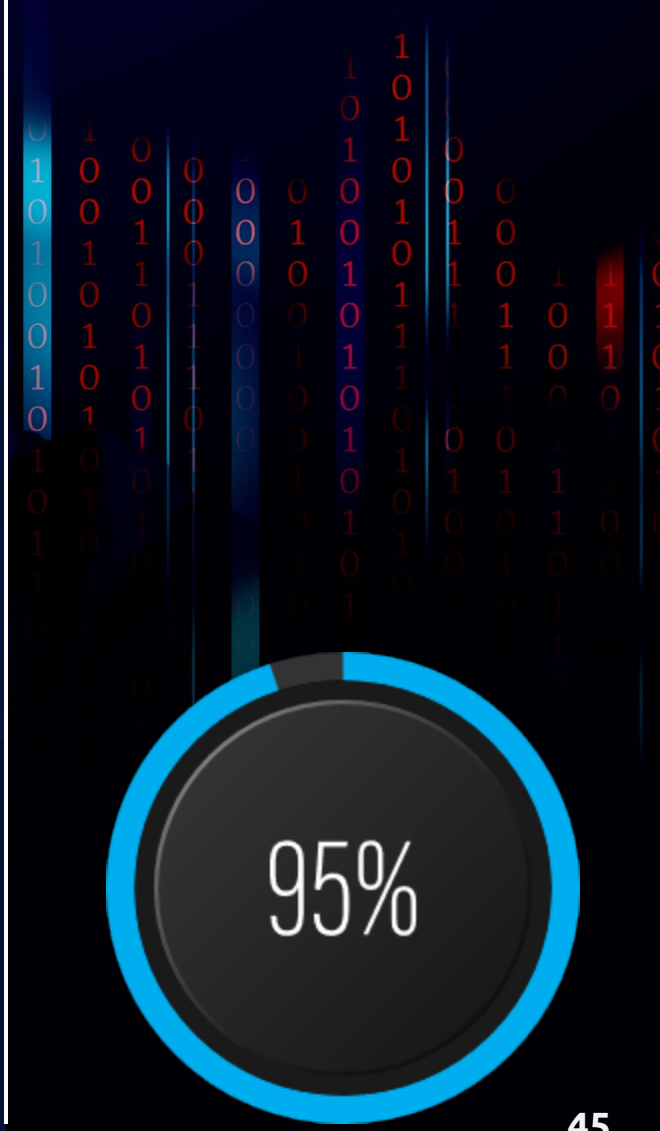
Etki (Impact) taktiği kullanılarak yapılan saldırıların **%95'i** ADEO MDR Servisi tarafından tespit edilebilmektedir.

- **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.



Taktikler

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.

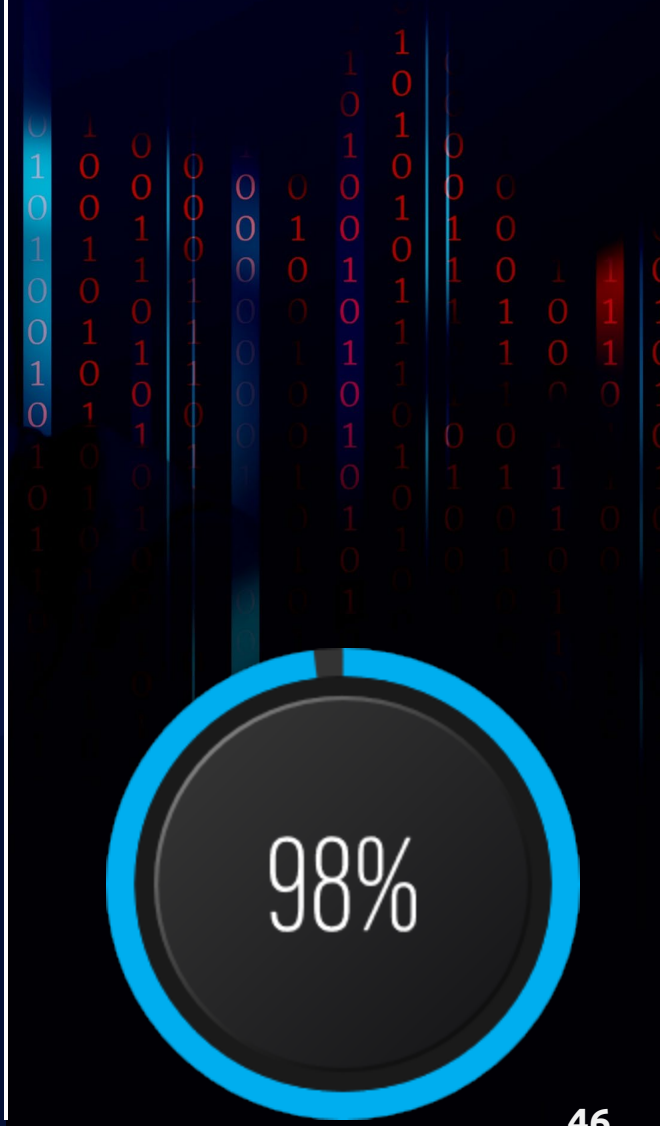
Kalıcılık (Persistence) taktiği kullanılarak yapılan saldırıların **%98'i** ADEO MDR Servisi tarafından tespit edilebilmektedir.

- **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.



10.Yetki Yükseltme (Privilege Escalation)

Yetki Yükseltme, saldırganın bir sistem veya ağ üzerinde daha üst düzeyizinler 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 **%91'i** ADEO MDR Servisi tarafından tespit edilebilmektedir.

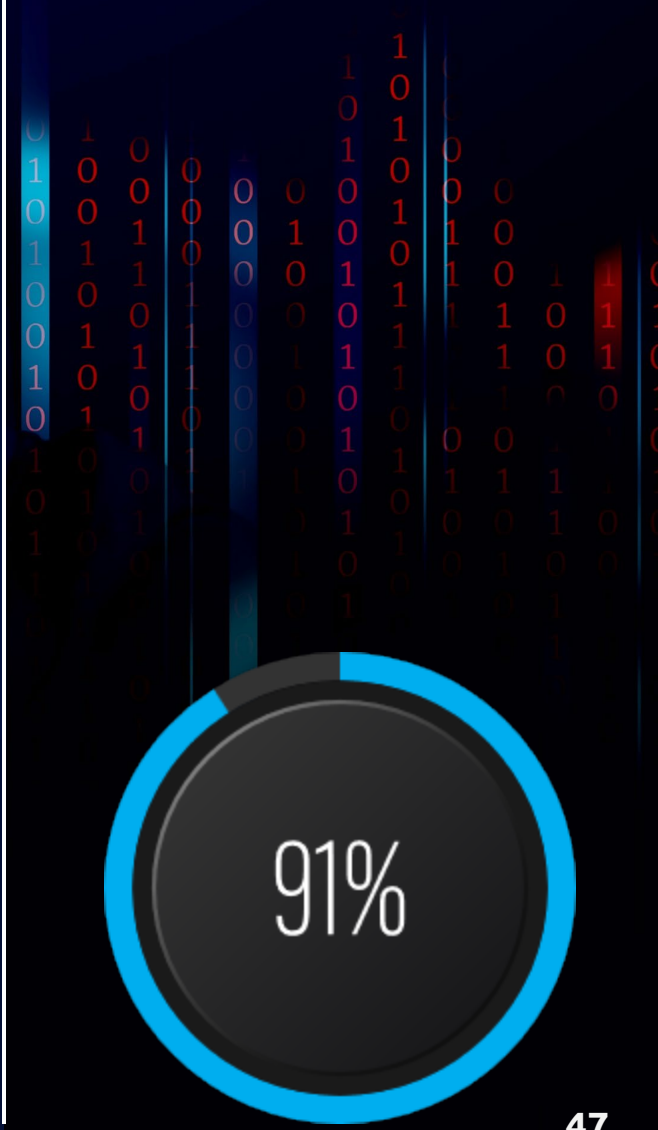
- **Active Directory (AD) veya LDAP** gibi dizin sunucularından gelen logların yapılandırılması gerekmektedir. Kullanıcı hak yükseltme veya yeni kullanıcı oluşturma olaylarının takip edilmesi gerekmektedir. **Yetkili kullanıcı** hesap adlarının, yetkilerinin bir **listesinin oluşturulması** gerekmektedir. **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.**



Taktikler

11.İlk Erişim (Initial Access)

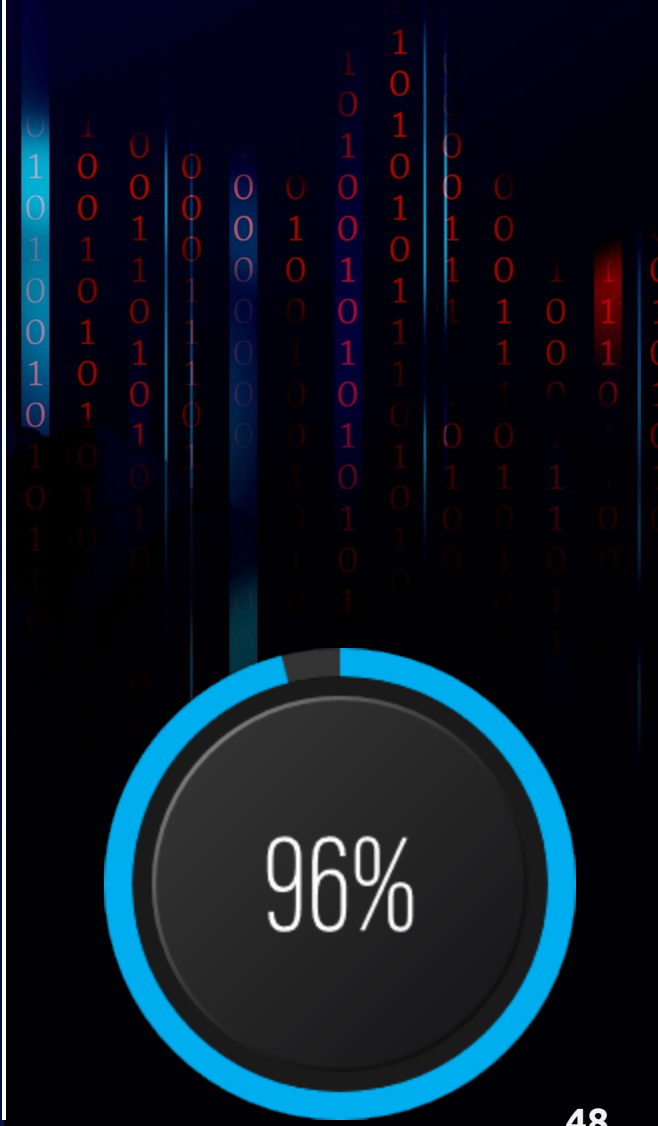
İlk Erişim, saldırganın hedef ağ içerisinde birincil dayanağını elde etmesine yarayan çeşitli giriş vektörlerinin kullanıldığı tekniklerden oluşur.

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.**



Taktikler

12.Yanal Hareket (Lateral Movement)

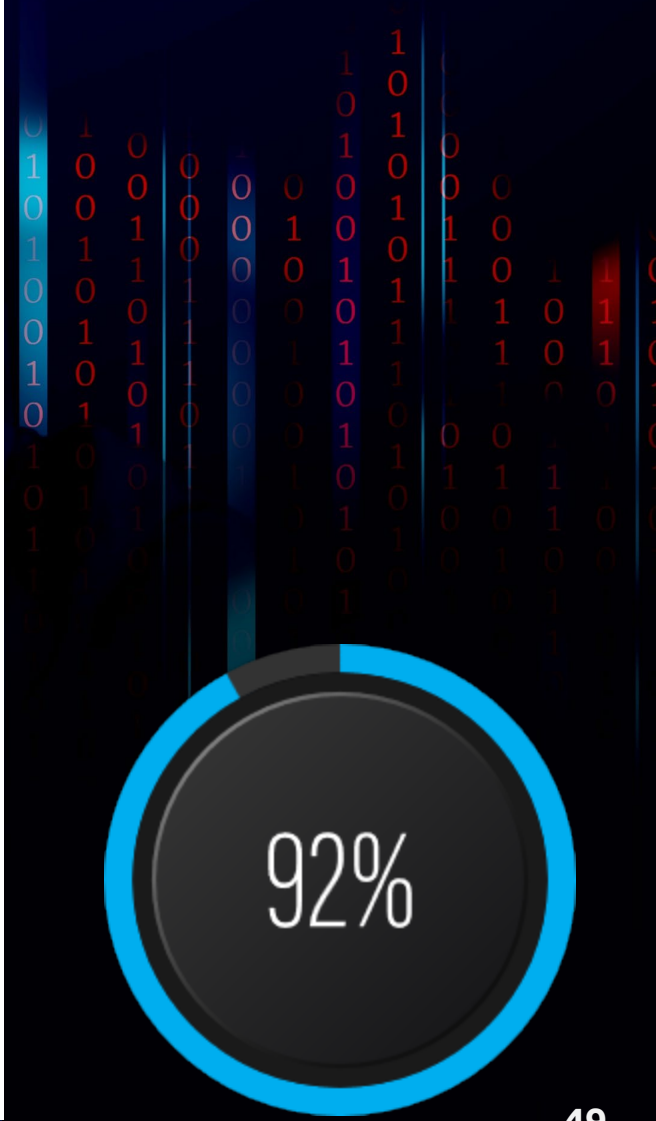
Yanal Hareket, saldırganların bir ağdaki uzak sistemlere girmek ve onları kontrol etmek için kullandığı tekniklerden oluşur. Gerçek hedeflerini takip etmek, genellikle hedeflerini bulmak için ağı keşfetmeyi ve ardından ona erişim sağlamayı gerektirir.

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 **%92'si** 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.**



İşletim Sistemlerine Göre Kural Dağılımı

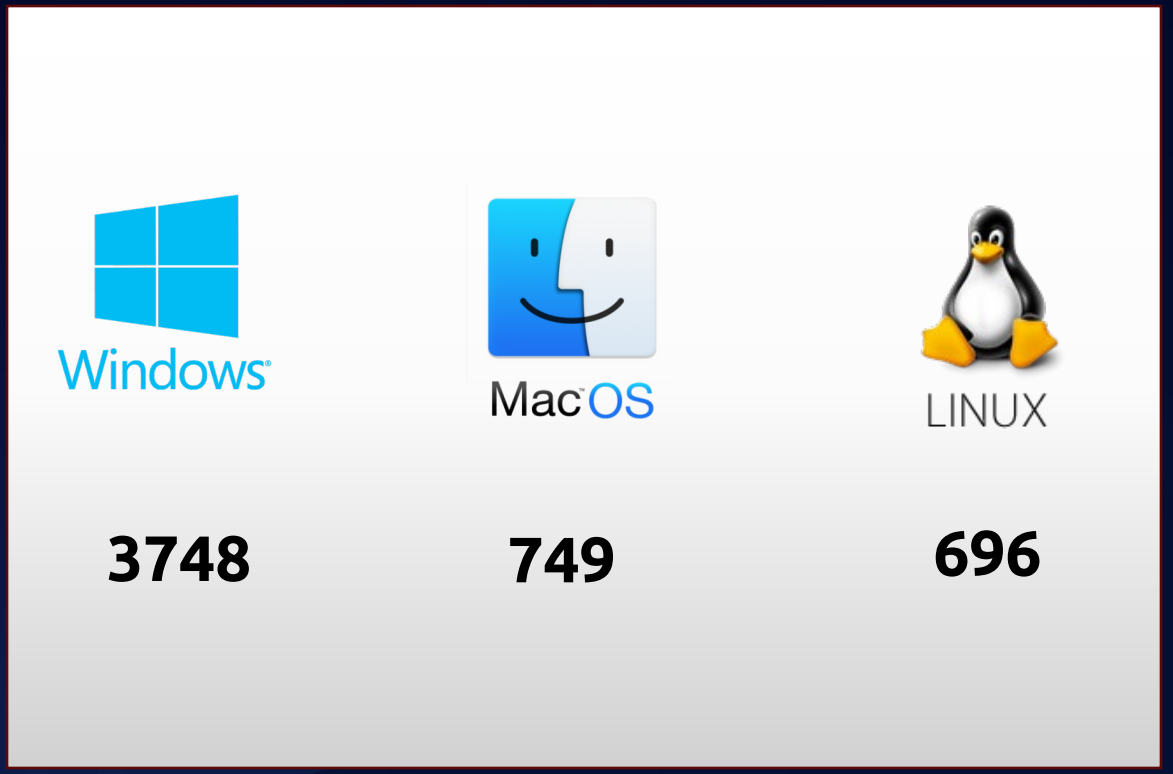
ADEO MDR Servisi olarak Windows, Linux, MacOS işletim sistemi ve türevleri (WindowsServer, Workstation, Centos, Unix, Debian, Ubuntu tabanlı vb.) özelinde toplam **5000+** tespit kuralımız mevcuttur.

Geliştirilen tespit kurallarının dağılımı; **Windows işletim sisteminde 3748, Linux'ta 749 ve MacOS'ta ise 696 kural** şeklindedir.

Geliştirdiğimiz tespit kuralları MITREATT&CK® Framework'teki Linux, MacOs, Windows tabanlı tüm işletim sistemleri için oluşturulan Taktik, Teknik, Prosedürlerin(TTP*) ortalama **%94'ünü** kapsamaktadır.

Bu sayede tüm müşterilerimize 3 işletim sistemi ve türevleri için **%94'ün** üzerinde tespit oranıyla destek verebilmekteyiz.

"Tüm müşterilerimize 3 işletim sistemi ve türevleri için %94'ün üzerinde tespit oranıyla destek vermekteyiz."



TTP

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

ADEO
CYBER SECURITY

2024 Yılı Siber Güvenlik Trendleri ve Tahminleri

2024 Yılı Siber Güvenlik Trendleri ve Tahminleri:
Halil Öztürkci:

2024 yılına girerken, teknolojinin baş döndürücü bir hızla ilerlediği, dijital dönüşümün her sektörü derinden etkilediği bir dönemden geçiyoruz. Pandemi sonrası normalleşme sürecinde, uzaktan çalışma modellerinin kalıcı hale gelmesi ve bulut tabanlı çözümlere artan talep, siber güvenliğin önemini daha da artırıyor.

Siber suçluların da bu değişen koşullara ayak uydurduğunu, saldırı yöntemlerini sürekli geliştirdiklerini görüyoruz. Yapay zeka, makine öğrenimi, otomasyon gibi teknolojiler siber güvenlik alanında hem fırsat hem de tehdit oluşturuyor. Veri gizliliği ve uyumluluk konusundaki düzenlemeler ise tüm dünyada hız kazanıyor.

Bu dinamik ortamda, kurumlara ve bireylere düşen, siber tehditlere karşı daima tetikte olmak, proaktif bir yaklaşım benimsemek ve en iyi uygulamaları hayata geçirmektir. Gelin şimdi, 2024 yılında siber güvenlik gündemini meşgul edeceğini düşündüğümüz başlıca trendlere ve tahminlere birlikte göz atalım:

Yapay Zeka Destekli Siber Güvenlik ve Saldırılar

2024 yılında, yapay zeka (AI) teknolojisinin siber güvenlik alanında çok daha etkin bir şekilde kullanılmasını bekliyoruz. Tehdit algılama, anomali tespiti, güvenlik olaylarına müdahale gibi konularda AI tabanlı çözümler yaygınlaşacak. Öte yandan, yapay zekanın siber suçluların eline geçmesi de büyük bir risk oluşturuyor. Deep fake içerikler, chatbot üzerinden sosyal mühendislik, otomatikleştirilmiş saldırılar gibi yöntemlerle siber suçlular da yapay zekayı kendi amaçları doğrultusunda kullanabilir. Bu nedenle, yapay zeka destekli savunma mekanizmaları geliştirmek ve bu alanda yetkin uzmanlar yetiştirmek büyük önem kazanacak

Bilgi Operasyonlarına (Information Operations) Karşı Mücadele

Bilgi operasyonları ve dezenformasyon kampanyaları son yıllarda giderek artıyor. Özellikle kritik seçim dönemlerinde, siber uzayda yürütülen propaganda faaliyetleri, yanlış bilgilerin yayılması, halkın manipüle edilmesi gibi girişimler yoğunlaşıyor. 2024 yılında da çeşitli ülkelerde yapılacak seçimler öncesinde ve sonrasında bu tür operasyonların artmasını bekliyoruz. Sosyal medya platformları, hükümetler, sivil toplum kuruluşları ve elbette siber güvenlik şirketleri, dezenformasyonla mücadelede iş birliği içinde hareket etmeli. Doğrulama mekanizmalarının geliştirilmesi, şeffaflığın artırılması ve kullanıcıların medya okuryazarlığının yükseltilmesi bu mücadelenin anahtarları olacak.

2024 Yılı Siber Güvenlik Trendleri ve Tahminleri

Fidye Yazılımların Evrimi

Fidye yazılım saldırıları, kurumların korkulu rüyası olmaya devam ediyor. Saldırganlar, sadece verileri şifrelemekle kalmıyor, kurbanı kamuoyu önünde ifşa etmekle tehdit ederek daha yüksek fidyeler talep ediyor. 2024'te fidye yazılımların daha da karmaşık hale gelmesini, saldırganların yeni taktikler geliştirmesini öngörüyoruz. Örneğin, yapay zeka tabanlı fidye yazılımların ortaya çıkması, deep fake teknolojisiyle kurumların itibarını zedeleme girişimleri, ileri düzey şifreleme yöntemlerinin kullanılması gibi gelişmeleri görebiliriz. Bu tehditle mücadele için yedekleme ve olay müdahale süreçlerinin iyileştirilmesi, güvenlik farkındalığının artırılması, saldırı yüzeyinin daraltılması gibi önlemler kritik önem taşıyor.

Veri Gizliliği Alanında Yeni Düzenlemeler ve Uyumluluk

Kişisel verilerin korunması, 2024 yılında da gündemdeki yerini koruyacak. Avrupa Birliği'nin GDPR'ı, dünya çapında pek çok ülkenin benzer veri koruma yasaları çıkarmasına öncülük etti. Gelecek yıl, daha fazla ülkenin kapsamlı veri gizliliği düzenlemelerini hayata geçirmesini bekliyoruz. Bu düzenlemelerin ışığında, kurumların uyumluluk çabalarını artırması, veri yönetimi süreçlerini iyileştirmesi gerekecek. Müşteri güvenini ve itibarını korumak isteyen şirketlerin, veri etiği ilkelerini benimsemesi de önem kazanacak.

Zero Trust ve Kimlik Yönetimi

Artan siber tehditler ve hibrit çalışma modelleri, geleneksel güvenlik yaklaşımlarının yetersiz kaldığını ortaya koydu. Zero Trust (Sıfır Güven) prensibine dayalı mimariler, 2024 yılında hızla yaygınlaşacak. "Asla güvenme, her zaman doğrula" ilkesine dayanan bu model, ağdaki her kullanıcı, cihaz ve uygulamanın sürekli olarak doğrulanmasını gerektiriyor. Böylece, bir saldırganın ağa sızması durumunda bile hasar sınırlandırılabiliyor. Ancak Zero Trust modelinin başarısı, sağlam bir kimlik ve erişim yönetimi altyapısına bağlı. Bu nedenle, çok faktörlü kimlik doğrulama, biyometrik teknolojiler, risk tabanlı kimlik doğrulama gibi gelişmiş yöntemler ön plana çıkacak.

2024 Yılı Siber Güvenlik Trendleri ve Tahminleri

Tedarik Zinciri Saldırıları ve Üçüncü Taraf Risk Yönetimi

Kurumlar, dijital ekosistemin bir parçası haline geldikçe, tedarik zincirlerindeki zayıf halkalar siber suçluların hedefi oluyor. Solarwinds ve Kaseya olayları, tedarik zincirinin bir parçası olan yazılımlara ve hizmetlere yönelik saldırıların ne kadar yıkıcı olabileceğini gösterdi. 2024 yılında, tedarik zinciri saldırılarının artarak devam edeceğini öngörüyoruz. Bu saldırılar, sadece doğrudan hedef alınan kurumu değil, o kurumla iş yapan tüm paydaşları da etkileyebilir. Bu nedenle, üçüncü taraf risk yönetimi hayati önem kazanıyor. Tedarikçi ve iş ortaklarının siber güvenlik olgunluk seviyelerinin düzenli olarak değerlendirilmesi, sözleşmelerde güvenlik gereksinimlerinin net bir şekilde tanımlanması, güvenlik açıklarına karşı proaktif önlemler alınması gerekiyor.

OT ve IoT Güvenliği

Operasyonel teknoloji (OT) sistemleri ve Nesnelerin İnterneti (IoT) cihazları, siber suçluların radarına giderek daha fazla giriyor. Fabrikalar, enerji santralleri, akıllı şehir altyapıları gibi kritik sektörlerde kullanılan bu sistemler, geleneksel BT güvenlik önlemlerinden yoksun olabiliyor. Üstelik, pek çok IoT cihazı güncel olmayan yazılımlar, varsayılan parolalar, zayıf şifreleme gibi güvenlik açıkları barındırıyor. 2024 yılında, OT ve IoT sistemlerine yönelik saldırıların artmasını, bu alanda yeni düzenlemeler ve standartlar geliştirilmesini bekliyoruz. Ayrıca, uç nokta güvenliği, ağ segmentasyonu, güvenli uzaktan erişim gibi çözümlere talep artacak.

Siber tehditlerin sürekli değiştiği ve geliştiği bir ortamda, siber güvenliğin sadece teknoloji sorunu değil, aynı zamanda bir insan ve süreç meselesi olduğunu unutmamak gerekiyor. 2024 yılında başarılı olmak isteyen kurumların, tüm çalışanların siber farkındalığını artırması, siber güvenliği iş süreçlerine entegre etmesi ve üst yönetimin sahiplenmesini sağlaması şart.

Unutmayalım ki siber güvenlik, hepimizin ortak sorumluluğu. Birlikte çalışarak, içinde bulunduğumuz dijital dönüşüm çağında siber riskleri en aza indirebilir, yeni teknolojilerin sunduğu fırsatlardan güvenle yararlanabiliriz.

"Siber güvenli bir gelecek dileğiyle, Halil Öztürkci"

2024 Yılı Siber Güvenlik Trendleri ve Tahminleri:

ChatGPT Ne Diyor?

Siber güvenlik tehditleri hızla gelişiyor ve çeşitleniyor, ancak bazı olası saldırı türleri şunlar olabilir:

Ransomware Saldırıları:

Bu saldırılar, bilgisayar sistemlerini veya dosyaları kilitleyip fidye talep eden kötü amaçlı yazılımları içerir. Özellikle büyük kuruluşlar, sağlık kurumları ve kamu kurumları hedef alınabilir.

Bulut Tabanlı Saldırılar:

Kurumların bulut hizmetlerine olan bağımlılığı arttıkça, bulut tabanlı saldırılar da artabilir. Bu, kötü amaçlı yazılımların veya veri sızıntılarının bulut altyapısını hedef aldığı saldırıları içerebilir.

İnternet of Things (IoT) Saldırıları:

IoT cihazlarının yaygınlaşmasıyla, bu cihazlar üzerinden gerçekleştirilen saldırılar da artabilir. Örneğin, güvenlik kameraları, termostatlar ve akıllı ev cihazları gibi IoT cihazları, bir ağdaki zayıf noktalar olabilir.

Yapay Zeka Destekli Saldırılar:

Yapay zeka ve makine öğrenimi, siber saldırganlar tarafından daha sofistike ve öngörülemez saldırılar gerçekleştirmek için kullanılabilir. Bu, daha hızlı ve daha etkili saldırılar anlamına gelebilir.

Büyük Veri İhlalleri:

Büyük kuruluşların ve kurumların büyük veri depolama ve analiz sistemleri, kötü niyetli kişiler için değerli hedefler olabilir. Bu tür ihlaller, milyonlarca kişinin kişisel verilerinin sızdırılmasına veya çalınmasına neden olabilir.

Devlet Destekli Siber Saldırılar:

Ülkeler arasındaki jeopolitik gerilimler, devlet destekli siber saldırıların artmasına neden olabilir. Bu tür saldırılar, devlet kurumları, altyapılar veya stratejik endüstrileri hedef alabilir.

Bu sadece birkaç örnek, ancak siber güvenlik alanında sürekli olarak ortaya çıkan yeni tehditler ve saldırı türleri vardır. Bu nedenle, kuruluşların güvenlik önlemlerini sürekli olarak güncellemesi ve iyileştirmesi önemlidir.

"Önemli olan, siber güvenlik önlemlerini almayı ve çevrimiçi faaliyetleriniz sırasında dikkatli olmayı sürdürmektir."

2024 Yılı Siber Güvenlik Trendleri ve Tahminleri:

Gemini Ne Diyor?

Siber güvenlik tehditleri hızla gelişiyor ve çeşitleniyor, ancak bazı olası saldırı türleri şunlar olabilir:

Beklenen Tehditler:

- Yapay zeka ve makine öğrenimi tabanlı saldırılar
- Uç nokta saldırıları
- Bulut güvenliği riskleri
- Siber casusluk
- Sosyal mühendislik saldırıları
- IoT saldırıları
- Kritik altyapılara saldırılar
- Yıkıcı hacktivizm
- Olimpiyat temalı sahtekarlıklar
- Yönetilen hizmet sağlayıcılara yönelik saldırılar

Korunma Yolları:

- Yapay zeka ve makine öğrenimi destekli güvenlik yazılımları
- Bilinçli kullanıcı olma
- Güncel kalmak
- Yedeklilik
- Siber güvenlik eğitimi
- Veri koruma ve gizlilik politikaları

Önemli Noktalar:

- Siber saldırılar her geçen gün daha karmaşık ve tehlikeli hale geliyor.
- Siber güvenliğe yatırım yapmak ve güncel kalmak her zamankinden daha önemli.
- Bireylerin ve kuruluşların siber güvenlik risklerine karşı bilinçli davranması gerekiyor.

Öneriler #TOP 5

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.

Yapay Zeka ve Siber Güvenlik

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.

ADEO olarak 2023 yılından itibaren ChatGPT başta olmak üzere **birçok AI modelini** kullanmaktayız.

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 sunmaya çalışıyoruz.

Ürün Ailesinin Yeni Üyeleri

"Picus ile Güncel Saldırılara Hazırlıklı Olun."

2023 yılında ürün ailesine katılan Picus, MDR ekiplerinin siber saldırılara karşı proaktif olmalarını sağlayarak, gerçekçi saldırı simülasyonları, siber güvenlik açıklarını ve zafiyetlerini belirleme, farkındalık ve bilgi birikimini artırma, eğitim ve tatbikat imkanı ile pratik deneyim kazandırma ve raporlama ve analiz ile savunma stratejilerini optimize etme gibi birçok avantaj sunar. Bu sayede Picus, MDR ekiplerinin siber güvenlik dayanıklılığını önemli ölçüde geliştirmelerine ve siber saldırılara karşı daha güçlü hale gelmelerine yardımcı olur.

**2023 yılında çalışmalarımızda yaptığımız testlerde Picus ürünü kullanılmıştır. Bu iş birliği için teşekkürlerimizi sunarız.*

"SentinelOne ile Yeni Nesil Gelişmiş Uç birim Koruma"

ADEO MDR ekibi Yapay zeka destekli SentinelONE ile siber tehditleri otomatik olarak tespit ederek koruma sağlar.
SentinelOne tespit edilen olaylara hızlı müdahale edilmesini kolaylaştırarak sistemlerinizin güvende kalmasını sağlar.

"Threatzone ile Zararlı Yazılımları Keşfedin, Yakalayın ve Analiz Edin."

Threatzone bilgisayarlardaki dosyaların zararlı etkinlikleri izole bir ortamda görmenizi sağlayan bir zararlı yazılım analiz platformudur.
ADEO MDR ekibi Threat Zone Sandbox kullanarak dosyaları izole bir ortamda detaylı analiz ederek kompleks saldırıları tespit eder ve zararlı bulaşma riskini ortadan kaldırarak, hızlı ve güvenli analiz yapılmasını sağlar.

"Cyberthint ile Doğru ve İsabetli İstihbarat"

ADEO MDR ekibi Cyberthint ile siber tehditler ve saldırganlar ile ilgili detaylı ve isabetli verilere hızlı bir şekilde ulaşır. Bu sayede saldırıyı hızla tespit ettikten sonra zaman kaybetmeden müdahale ederek proaktif korumayı sağlar.

Hizmet Ağımız

ADEO ve Türkiye'de İlkler

Top 250 MSSPs Listesi'ndeyiz

ADEO Cyber Security, MSSP Alert tarafından hazırlanan dünyadaki "En iyi 250 MSSP Listesi"nde yer alan "**ilk ve tek Türk Siber Güvenlik firması**" olarak büyük bir başarıya imza attı ve 2023 yılında sıralamadaki derecesini 47 sıra yukarı taşıdı.

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.

ADEO ve Türkiye'de İlkler

- İlk Dijital Forensics Laboratuvarı, 2015
- Siber Güvenlik Kümelenmesi Üyeliği, 2018
- İlk Carbon Black MSSP Partner, 2019
- İlk MDR Servisleri İş Ortağı, 2020
- İlk Palo Alto Networks, MSSP İş Ortağı, 2020 (Adeo, Dünyada bu yetkinliğe sahip 11 iş ortağı arasındadır.)
- İlk ADTR Servis Sağlayıcı, 2023
- İlk APTR Servis Sağlayıcı, 2023

ADEO
CYBER SECURITY

ADEO Cyber Security Services

@adeocomtr

ADEOcomtr

@adeocomtr

@adeocomtr

www.adeo.com.tr