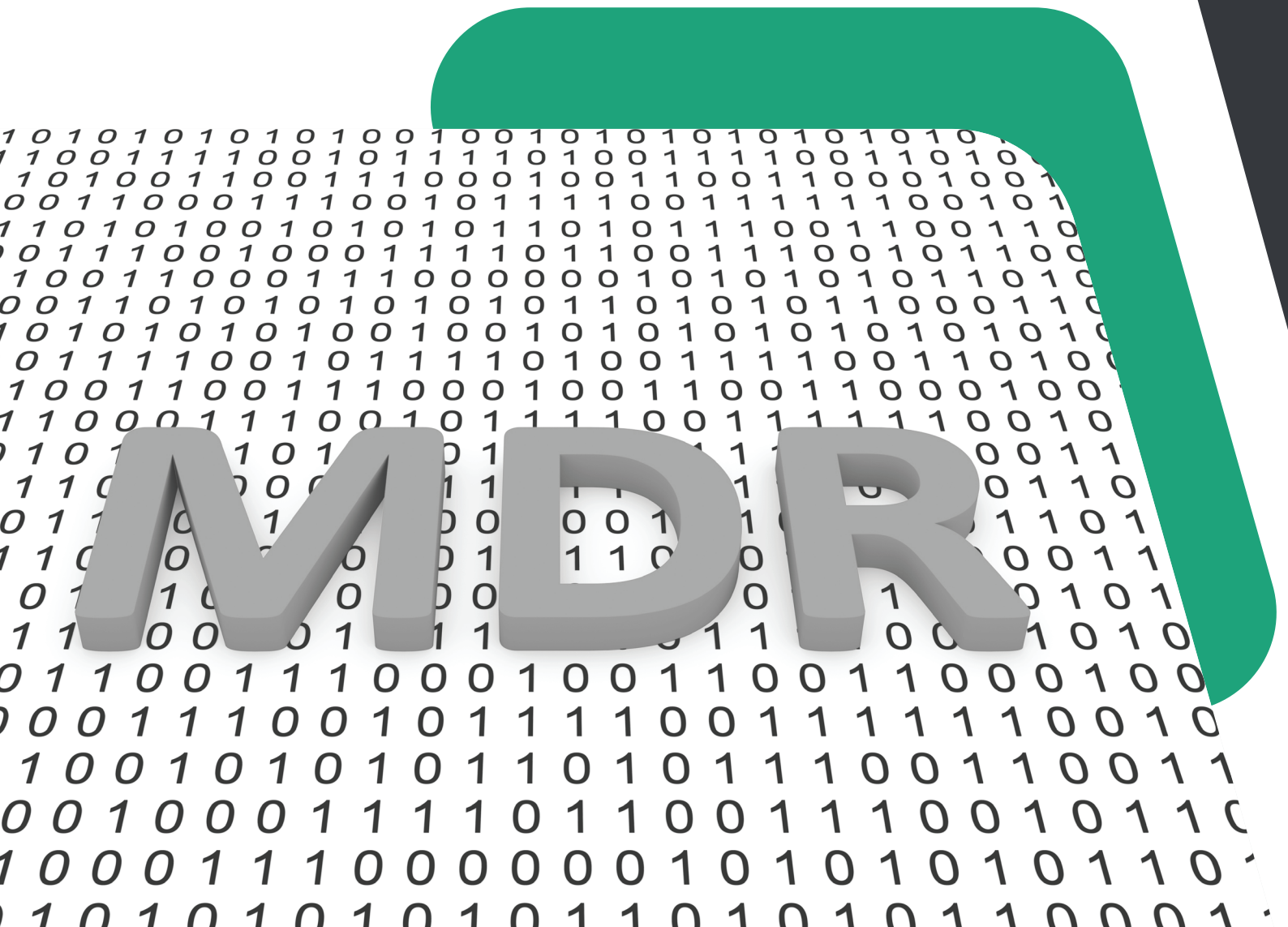
infinitum IT
Power of integrated Security

İŞLETMELER İÇİN MDR YÖNETİMİ REHBERİ

www.infinitumit.com.tr

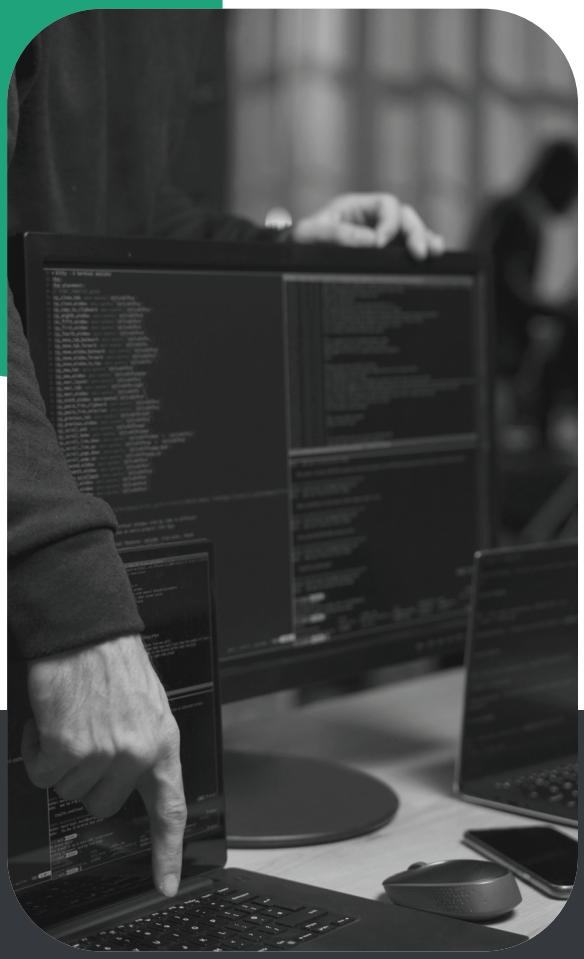
“İşletmeler İçin MDR Yönetimi Rehberi” ile sorularınızın cevaplarını keşfederek işletmenizi siber saldırılara karşı kontrol altına alabilir ve bir siber tehdide yanıt vermek için gereken süreyi azaltabilirsiniz.



İÇİNDEKİLER

GİRİŞ

Managed Detection and Response çok uzun süredir var olan bir hizmet olmasa da, sektör şimdiden yaklaşık 5 milyar dolarlık bir değere ulaşarak her yıl %18'in üzerinde bir büyüme göstermektedir. Yapılan araştırmalara göre, MDR sektörünün 2021 ila 2030 yılları arasında dört kattan fazla büyüyeceği ve işletmelerin %50'sinin 2025 yılına kadar MDR hizmetlerini kullanacağı tahmin edilmektedir.



Rakamlardan da anlaşılacağı gibi MDR hizmetindeki büyüme oranı ve talep oldukça şaşırtıcıdır.

Peki MDR hizmetlerine olan talebin bu kadar artmasını sağlayan faktörler nelerdir?

Aşağıdaki araştırma sonuçları ve açıklamalar doğrultusunda işletmelerin MDR hizmetlerine olan taleplerinin neden arttığını genel hatları ile açıklamaya çalışacağız.

> Yakın tarihli bir araştırmaya göre, bilgisayar korsanları her 39 saniyede bir potansiyel olarak yıkıcı bir siber saldırı başlatır ve işletmelerin %90'ından fazlası hızla gelişen siber saldırılara proaktif olarak yanıt vermek veya bunları hafifletmek için gerekli kaynaklara, altyapıya, becerilere ve bütçeye sahip değildir.

Ayrıca birçok işletme, güvenlik bütçelerini güvenlik duvarları, antivirüs ve diğer operasyonel güvenlik kontrolleri gibi önleyici tedbirlere yatırmaktadır. Ancak teknolojideki karmaşıklık ve siber tehditlerle ilgili saldırılar arttıkça, işletmeler zor yoldan da olsa hangi hizmetlere yatırım yapacağını öğrenmektedir.

Bu noktada MDR hizmetleri, siber tehditleri izleyip tespit ederek bu tehditlere anında yanıt verdiği için ön plana çıkmaktadır.

- Peki işletmeniz için neden Bir MDR hizmeti kullanmalısınız?
- Managed Detection and Response hizmetleri nelerdir?
- Managed Detection and Response hizmetinin işletmeler için avantajları nedir?
- MDR hizmeti işletmeler için hangi zorlukları çözebilir?
- MDR vs diğer güvenlik çözümleri

"İşletmeler İçin MDR Yönetimi Rehberi" ile tüm bu soruların ve daha fazlasının cevaplarını keşfederek işletmenizi siber saldırılara karşı kontrol altına alabilir ve bir siber tehdide yanıt vermek için gereken süreyi azaltabilirsiniz.

İŞLETMENİZ İÇİN **NEDEN BİR MDR HİZMETİ KULLANMALISINIZ?**

Her ölçekten işletmenin siber güvenlik tehditlerini algılamasına, araştırmasına ve bunlara yanıt vermesine olanak sağlayan bir siber güvenlik hizmeti olan Managed Detection and Response (MDR), işletmelere birçok avantaj sağlar.

Peki işletmeniz için neden bir MDR hizmeti kullanmalısınız?

Aşağıdaki listede işletmeniz için neden bir MDR hizmeti kullanmalısınız sorusunun cevabını bulacaksınız:

1. Üst Düzey Deneyim

MDR sağlayıcıları, siber tehditleri tespit etmek, araştırmak ve bunlara müdahale etmek üzere eğitilmiş bir siber güvenlik ekibine sahiptir. Bu ekipler, çok çeşitli siber saldırılarla başa çıkma konusunda üst düzey deneyime sahip oldukları için işletmenize en son tehditler ve siber saldırı teknikleri hakkında değerli bilgiler sağlar.

2. 7/24 İzleme

MDR hizmetleri, ağınızın ve sistemlerinizin sürekli olarak izlenmesini sağlayarak olası siber tehditlerin anında tespit edilmesini ve ele alınmasını sağlar. Bu özellikle finans veya sağlık hizmetleri gibi siber tehditlere karşı daha savunmasız sektörlerde faaliyet gösteren işletmeler için oldukça önemlidir.

3. Hızlı Yanıt

MDR hizmetleri, herhangi bir potansiyel tehdide hızlı yanıt vererek bir siber saldırıyı tespit etmek ve kontrol altına almak için gereken süreyi azaltır. Hızlı yanıt, bir siber olayın etkisini en aza indirmeye ve veri kaybı riskini azaltmaya yardımcı olur.

4. Uygun Maliyet

MDR hizmetleri, siber güvenlik duruşunuzu iyileştirmenin uygun maliyetli bir yoludur. Siber güvenliğinizi bir MDR sağlayıcısına devrederek, şirket içi bir güvenlik ekibi oluşturma ve pahalı güvenlik araç ve teknolojilerine yatırım yapma maliyetlerinden kurtulabilirsiniz.

5. Uyumluluk

MDR hizmetleri, gerekli güvenlik kontrollerini ve izleme yeteneklerini sağlayarak işletmelerin yasal uyumluluk gereksinimlerinin karşılanmasına yardımcı olur.

Managed Detection and Response Hizmetleri

Managed Detection and Response (MDR) hizmetleri, işletmelere siber tehditlere karşı kapsamlı izleme, tespit, soruşturma ve müdahale olanağı sağlayan siber güvenlik çözümleridir. MDR hizmetleri genellikle, bir işletmenin BT sistemlerinin sürekli izlenmesini ve yönetimini sağlamak için siber güvenlik uzmanları ekibi istihdam eden 3. taraf bir sağlayıcı aracılığıyla sağlanır.

MDR hizmetleri, ağ trafiğini, günlük verilerini ve güvenlik olaylarını gerçek zamanlı olarak izlemek için SIEM (Güvenlik Bilgileri ve Olay Yönetimi) sistemleri, gelişmiş analitik ve tehdit istihbaratı gibi gelişmiş güvenlik teknolojilerini kullanır. Amaç, güvenlik tehditlerini hızlı bir şekilde belirleyip bunlara yanıt vererek işletme üzerindeki etkiyi en aza indirmektir.

MDR hizmetleri genellikle, hizmet sağlayıcının olay soruşturması, kontrol altına alma ve düzeltme konusunda yardımcı olabileceği olay müdahale yeteneklerini içerir. Buna adli tıp analizi, kötü amaçlı yazılım temizleme ve sistem kurtarma dahildir.

MDR hizmetlerini kullanmanın avantajları arasında gelişmiş tehdit algılama, azaltılmış olay yanıt süreleri, 7/24 izleme, siber güvenlik uzmanlarına erişim ve maliyet etkinliği yer almaktadır. MDR hizmetleri özellikle kendi siber güvenlik operasyonlarını yönetecek kaynaklara veya uzmanlığa sahip olmayan küçük ve orta ölçekli işletmeler için faydalı olarak kabul edilmektedir.

Managed Detection and Response Hizmetinin İşletmeler için Avantajları

İşletmeler için Yönetilen Tespit ve Müdahale (MDR) hizmetlerini kullanmanın çeşitli avantajları vardır. Bu avantajlar aşağıdaki şekildedir:

1. Gelişmiş Tehdit Algılama

MDR hizmetleri, güvenlik tehditlerini gerçek zamanlı olarak algılamak ve bunlara yanıt vermek için SIEM, gelişmiş analitik ve tehdit istihbaratı gibi gelişmiş güvenlik teknolojilerinden yararlanmaktadır. Gelişmiş tehdit algılama, işletmelerin güvenliğine proaktif bir yaklaşım sağlar ve potansiyel tehditleri önemli bir hasara neden olmadan önce belirler.

2. 7/24 İzleme

MDR sağlayıcıları, 24 saat izleme ve koruma sağlar. Siber saldırılar her an gerçekleşebileceği için sağlanan bu sürekli koruma, siber tehditlere hızla yanıt vermek için çok önemlidir.

3. Hızlı Olay Müdahalesi

MDR hizmetleri, servis sağlayıcının vaka soruşturması, kontrol altına alma ve iyileştirme konusunda yardımcı olabileceği olay müdahale yeteneklerini içerir. Hızlı olay müdahalesi, bir siber saldırının etkisini en aza indirmeye ve bir siber tehdide yanıt vermek için gereken süreyi azaltmaya yardımcı olur.

4. Üst Düzey Siber Güvenlik Uzmanlığından Yararlanma

MDR hizmetleri, deneyimli siber güvenlik uzmanlarına erişmenizi sağlayarak siber güvenlik becerileri açığının kapatılmasına yardımcı olur. Bu hem personel sayısını artırmadan hizmet alınmasına hem de müşterilerin ihtiyaç duydukları özel beceri setlerine erişim sağlar.

5. Uygun Maliyet

MDR hizmetleri, bir işletmenin siber güvenlik duruşunu iyileştirmenin uygun maliyetli bir yoludur. İşletmeler, siber güvenlik operasyonlarını bir MDR hizmet sağlayıcısına yaptırarak, kendi bünyesinde bir güvenlik ekibi oluşturma ve güvenlik teknolojilerine yatırım yapma maliyetlerinden kurtulur.

6. Uyumluluk

MDR sağlayıcıları genellikle yasal uyumluluk konusunda uzmanlığa sahiptir ve hizmetleri, geçerli yasa ve düzenlemelerin gerekliliklerini karşılayacak şekilde tasarlanmıştır.

7. Proaktif Yaklaşım

MDR, güvenlik açıklarını bir bilgisayar korsanı tarafından kullanılmadan önce belirleyip kapatarak siber saldırı riskini azaltmaya yardımcı olur.

Genel olarak MDR hizmetleri, işletmelere gelişmiş tehdit algılama, 7/24 izleme, hızlı olay müdahalesi, siber güvenlik uzmanlığından yararlanma, maliyet etkinliği ve mevzuat uyumluluğunu içeren kapsamlı bir siber güvenlik çözümü sağlar. Bu, işletmelerin siber olay risklerini azaltmasına, değerli verileri ve varlıkları korumasına ve operasyonlarının sürekliliğini sağlamasına yardımcı olur.

MDR Hizmeti İşletmeler için Hangi Zorlukları Çözülebilir?

Yönetilen Tespit ve Müdahale (MDR) hizmetleri, işletmelerin aşağıdakiler de dahil olmak üzere çeşitli siber güvenlik sorunlarının üstesinden gelmesine yardımcı olmaktadır:

1. Gelişmiş Siber Tehditler

Siber tehditler giderek daha karmaşık hale geldiği için geleneksel güvenlik çözümleri bu tehditlere karşı koruma için yeterli olmaz. MDR hizmetleri, gelişmiş tehditleri algılamak ve bunlara yanıt vermek için gelişmiş güvenlik teknolojilerinden ve tehdit istihbaratından yararlanarak siber olay riskini azaltır.

2. Sınırlı Kaynaklar

Küçük ve orta ölçekli işletmeler, kendi siber güvenlik operasyonlarını yönetecek kaynaklara veya uzmanlığa sahip olmayabilir. Bu noktada MDR hizmetleri, işletmelere şirket içi bir güvenlik ekibi oluşturmaya gerek kalmadan siber güvenlik uzmanlığına, 7/24 izleme ve olay müdahale yeteneklerine erişim sağlar.

3. Olaylara Hızlı Müdahale

Siber güvenlik olaylarının bir işletmenin operasyonları, itibarı ve finansal istikrarı üzerinde önemli bir etkisi vardır. Bu noktada MDR hizmetleri, işletmelerin tehditlere hızlı bir şekilde yanıt vermesini ve bir siber olayın etkisini en aza indirmesini sağlayan olay müdahale yetenekleri sunar.

4. Uyumluluk

MDR hizmetleri, gerekli güvenlik kontrollerini ve izleme yeteneklerini sağlayarak işletmelerin yasal uyumluluk gereksinimlerini karşılamasına yardımcı olur.

5. Maliyet

Siber güvenlik çözümleri maliyetli olduğu için küçük ve orta ölçekli işletmeler gerekli güvenlik teknolojilerini ve personel maliyetlerini karşılamakta zorlanabilir. MDR hizmetleri, işletmelerin siber güvenlik duruşlarını iyileştirmeleri için uygun maliyetli bir yol sunarak şirket içi bir güvenlik ekibi oluşturma ve güvenlik teknolojilerine yatırım yapma maliyetlerini azaltır.

MDR vs Diğer Güvenlik Çözümleri

Aşağıdaki güvenlik çözümlerinin tümü, kurumsal siber güvenlik duruşunuzun geliştirilmesinde önemli bir rol oynar. Fakat doğru çözümün seçilmesi, işletmenizin özel ihtiyaç ve gereksinimlerine bağlıdır.

Bu noktada InfinitumIT, her ölçekteki işletmeye uygun olan siber güvenlik hizmetleri sunar ve işletmenizi doğru çözümle en iyi şekilde eşleştirerek işletmenizin ihtiyaçlarını öğrenerek işe başlar.

1. Managed Security Service Provider (MSSP)

EDR, işletmenizin uç noktalarındaki tehditleri tespit etmenize ve bunlara yanıt vermenize yardımcı olur. İster tesisinizdeki bir masaüstü bilgisayar, ister veri merkezinizdeki bir depolama denetleyicisi veya uzak bir konumdan kullanılan bir dizüstü bilgisayarı olsun, uç nokta işletmenizin ağına bağlanan herhangi bir cihazdır.

2. Managed Detection and Response (MDR)

MDR, tehditleri algılamak ve bunlara yanıt vermek için süreçleri, insanları ve teknolojiyi birleştiren, yönetilen bir güvenlik hizmetidir. Sadece uç noktaları değil, ağları ve bulut ortamlarını da herhangi bir potansiyel tehdit için izlemek üzere insan bilgisini, analitiği ve tehdit istihbaratını kullanır.

MDR çözümleri, güvenlik operasyonlarını şirket içinde yönetecek kaynaklara veya uzmanlığa sahip olmayan her büyüklükteki işletme için ideal bir çözümdür. Bu çözümler, işletmelere ortamlarını 7/24 izleyebilecek bir siber güvenlik uzmanları ekibi sağlar. Bu sayede HIPAA veya GDPR gibi herhangi bir düzenleyici standarda uyması gereken işletmeler, uyumluluk gereksinimlerini karşılamak için sağlanan uzmanlıktan büyük ölçüde yararlanır.

3. Security Information and Event Management (SIEM)

SIEM çözümleri, ağ cihazlarından, sunuculardan, uygulamalardan ve işletmenizin sahip olabileceği diğer kaynaklardan alınan günlük verilerini merkezileştirmeye odaklanır. Olası olayları belirlemek için korelasyon kurallarını kullanan SIEM çözümleri, daha sonra güvenlik ekiplerini herhangi bir şüpheli etkinlik konusunda uyarır. Bu çözümler ayrıca güvenlik ekiplerinin verilerdeki kalıpları anlamasına ve eğilimleri belirlemesine yardımcı olur. SIEM çözümleri, işletmenin güvenliğine ilişkin daha kapsamlı bir görünüm sağlamak için EDR ve XDR ile birlikte çalışacak şekilde entegre edilebilir.

SIEM çözümleri, verileri merkezileştiren birden fazla uç nokta, uygulama ve sunucu içeren karmaşık bir BT altyapısına sahip işletmeler için idealdir. Sağlık, finans ve bankacılık gibi hassas verileri yöneten tüm sektörler, gerçek zamanlı izleme ve tehdit tespiti sağlayan bir SIEM çözümünden yararlanabilir.

4. Endpoint Detection and Response (EDR)

EDR, uygulandığında uç noktalardaki güvenlik tehditlerini algılayan ve bunlara yanıt veren bir siber güvenlik çözümüdür. Uç noktalar dizüstü bilgisayarlar, mobil cihazlar, tabletler ve sunucular olabilir. EDR çözümleri, belirlenen tehditlere hızlı yanıt vererek tehditleri gerçek zamanlı olarak algılamak ve bunlara yanıt vermek üzere yapılandırılmıştır. Uç nokta etkinliğini izler ve şüpheli davranış belirtileri için veri toplar. EDR çözümleri, gerekli olan uç nokta etkinliğine yüksek düzeyde görünürlük sağlama eğilimindedir.

EDR çözümleri, özellikle birden fazla dizüstü bilgisayar, masaüstü bilgisayar, sunucu ve mobil cihaza sahip büyük işletmeler gibi korunması gereken çok sayıda uç noktaya sahip işletmeler için yararlıdır.

5. Extended Detection and Response (XDR)

EDR'nin en iyi özelliklerini bir araya getiren XDR çözümü, birden fazla güvenlik aracını ve veri kaynağını entegre ederek daha kapsamlı tehdit algılama ve müdahale yetenekleri sağlar. Bu çözüm, analitiği ve tehdit istihbaratını birleştirir ve tehditleri gerçek zamanlı olarak daha iyi algılamak ve bunlara yanıt vermek için otomasyon sağlar. Bir XDR çözümünün avantajlarından biri, birden çok kaynaktan gelen verileri entegre ederek diğer güvenlik çözümlerinin gözden kaçırabileceği karmaşık saldırıları belirleyebilmesidir.

XDR çözümleri, özellikle finans, sağlık ve kamu gibi yüksek düzeyde düzenlemeye tabi sektörler için avantajlıdır. Özellikle bu sektörler, en katı yasal gerekliliklerden bazılarına sahiptir ve XDR çözümleri, işletmenizin güvenliğine ilişkin en eksiksiz genel bakışı sunar.

EDR vs. XDR vs. MDR

	EDR	MDR	XDR
YETENEKLER	Antivirüs çözümlerini ve diğer önleyici teknikleri atlatan tehditler için uç noktaları izler.	EDR ile aynı yeteneklerin yanı sıra tehditleri izlemek, azaltmak, ortadan kaldırmak ve düzeltmek için 7/24 yönetilen hizmetler sağlar.	EDR ile aynı yeteneklerin yanı sıra tehditleri izlemek, azaltmak, ortadan kaldırmak ve düzeltmek için 7/24 yönetilen hizmetler sağlar.
BİLEŞENLER	Gerçek zamanlı uç nokta izleme Davranış analizi (IOC'ler ve IOA'lar) Tehdit veri tabanı ve grafik oluşturma Ağ koruması Düzeltme önerileri	EDR yetenekleri + 7/24 yönetilen hizmetler: Yönetilen soruşturma hizmetleri Yönetilen iyileştirme Tehditlerin ve uyarıların önceliklendirilmesi Yönetilen hizmet ve şirket içi ekipler için merkezi iletişim ve koordinasyon merkezi	EDR yetenekleri +: Otonom analiz, müdahale ve tehdit avı Bulut tabanlı alım Otomatik inceleme ve puanlama Domain'ler arası korelasyon İşlem yapılabilir tehdit özetleri Gelişmiş algılama, olay yanıtı ve tehdit avı

	EDR	MDR	XDR
YÖNTEMLER, ARAÇLAR VE TEKNOLOJİLER	Yazılım tabanlı EDR çözümü	Uç nokta koruma platformu (EPP)	Ağ analizi ve görünürlük (NAV) Yeni nesil güvenlik duvarı E-posta güvenliği Kimlik ve erişim yönetimi (IAM) Cloud workload protection platform (CWPP) Bulut erişimi güvenliği aracısı (CASB) Veri kaybı önleme (DLP)
TEHDİT GÖRÜNÜRLÜĞÜ	Endpoints	Endpoints	Tüm uç noktalar, kullanıcılar, ağ varlıkları, bulut iş yükleri, e-posta, veriler ve diğer varlıklar
KORUMA	EDR araçları, her siber güvenlik stratejisinin temel bir bileşeni ve tüm gelişmiş siber çözümlerin ve yeteneklerin temelidir.	MDR, tehdit avı, tehdit istihbaratı ve yönetilen yanıt gibi proaktif güvenlik eylemleri gerçekleştirmek için bir EDR çözümünün gerçek zamanlı izleme ve yanıt verme yeteneklerini, deneyimli siber güvenlik uzmanlarıyla birleştirir.	XDR, işletmeyi riske atan siloları ve boşlukları ortadan kaldırmak için ağ mimarisi genelinde araç ve sistemlerin EDR ve sağlam entegrasyonu yoluyla en yüksek düzeyde koruma sağlar.

İŞLETMENİZ İÇİN **MDR SAĞLAYICINIZI NASIL SEÇMELİSİNİZ?**

İşletmeniz için doğru bir Managed Detection and Response (MDR) sağlayıcısını seçmek, dikkatlice değerlendirilmesi gereken önemli bir karardır. Bir MDR sağlayıcısı seçerken dikkate alınması gereken bazı faktörler aşağıdakileri içermektedir:

1. Uzmanlık

Sektörünüzde iyi bir deneyime ve işletmenizin karşılaşabileceği belirli siber güvenlik tehditleri ile başa çıkma konusunda uzmanlığı sahip olan bir MDR sağlayıcısı arayın. Siber güvenlik ekiplerinin nitelik ve sertifikalarını sorun ve siber güvenlik olaylarını yönetme konusundaki deneyimlerini inceleyin.

2. Teknoloji

MDR sağlayıcısının SIEM, tehdit istihbaratı ve gelişmiş analitik gibi gelişmiş güvenlik teknolojilerini kullandığından emin olun. Teknolojilerin mevcut güvenlik altyapınızla nasıl bütünleştiğini ve veri gizliliği ile güvenliğini nasıl sağladıklarını araştırın.

3. Hizmet Düzeyi Sözleşmeleri (SLA'lar)

Yanıt sürelerini, olay işleme süreçlerini ve çözüm sürelerini özetleyen ve açık SLA'lar sunan bir MDR sağlayıcısı seçin. SLA'ların iş ihtiyaçlarınızla ve beklentilerinizle uyumlu olduğundan emin olun.

4. Maliyet

MDR hizmetlerinin maliyeti, hizmet düzeyine ve sağlanan teknolojiye bağlı olarak değişiklik gösterir. Bu noktada bütçenize ve siber güvenlik gereksinimlerinize uygun ve maliyetli bir çözüm sunan bir MDR sağlayıcısı seçtiğinizden emin olun.

5. Uyumluluk

İşletmeniz sağlık veya finans gibi yasal düzenlemelere tabi bir sektörde faaliyet gösteriyorsa, MDR sağlayıcısının yasal uyumluluk gereksinimlerini karşılayacağından emin olun.

6. Müşteri Desteği

7/24 müşteri desteği ve özel bir hesap yöneticisi sunan bir MDR sağlayıcısı arayın. Bu noktada mükemmel müşteri hizmeti ve desteği sağlama konusunda kanıtlanmış bir geçmiş performansa sahip olan bir sağlayıcı seçtiğinizden emin olun.

7. Referanslar

Seçeceğiniz MDR sağlayıcısının hizmetlerini kullanmış olan diğer işletmelerden referans isteyin, çevrimiçi incelemeleri kontrol edin ve hizmet sağlayıcının siber güvenlik olaylarını yönetme konusundaki deneyimlerini gösteren vaka çalışmalarını inceleyin.

İşletmeniz için doğru MDR sağlayıcısını seçerken; uzmanlık, teknoloji, SLA'lar, maliyet, uyumluluk, müşteri desteği ve referanslar dahil olmak üzere çeşitli faktörlerin dikkatle değerlendirilmesi gerekmektedir. İş ihtiyaçlarınıza ve siber güvenlik gereksinimlerinize uygun bir MDR sağlayıcısı seçerek sistemlerinizin ve verilerinizin siber tehditlere karşı korunmasını sağlayabilirsiniz.

MDR İşletmeniz için Uygun Bir Çözüm Mü?

Yönetilen Tespit ve Müdahale (MDR) işletmeniz için doğru çözüm olup olmadığı, özel siber güvenlik ihtiyaçlarınıza ve kaynaklarınıza bağlıdır.

Fakat özellikle şirket içi bir güvenlik operasyonları merkezi (SOC) oluşturacak ve yönetecek kaynaklara sahip olmayan her büyüklükteki işletmeye fayda sağlamaktadır.

Ayrıca işletmeniz, finans veya sağlık gibi yüksek düzeyde düzenlemeye tabi bir sektörde faaliyet gösteriyorsa veya hassas müşteri verilerini yönetiyorsa, yasal uyumluluk gereksinimlerini karşılamak ve verilerinizi siber tehditlerden korumak için mutlaka bir MDR hizmetine ihtiyacınız olacaktır.

MDR hizmetleri, işletmeler için 7/24 izleme, tehdit algılama ve müdahale, olay yönetimi ve deneyimli siber güvenlik uzmanlarından yararlanma dahil olmak üzere çeşitli avantajlar sağlar. Bu hizmetler, siber tehditleri gerçek zamanlı olarak belirlemenize ve bunlara yanıt vermenize, veri ihlali riskinizi azaltmanıza ve bir siber saldırının işletmeniz üzerindeki etkisini en aza indirmenize yardımcı olmaktadır.

Bu noktada MDR'nin işletmeniz için doğru çözüm olup olmadığını belirlemek için mevcut siber güvenlik yetenek ve kaynaklarınızı değerlendirmeniz gerekmektedir. Siber güvenlik risklerini şirket içinde yönetecek uzmanlığa veya kaynaklara sahip değilseniz veya işletmeniz yüksek riskli bir sektörde faaliyet gösteriyorsa, MDR sizin için doğru çözüm olacaktır.

MDR'ın Geleceği Nasıl Şekilenecek?

Managed Detection and Response (MDR), hızla gelişen ve gelişmekte olan bir alandır. MDR, makine öğrenimi, yapay zeka ve otomasyon gibi ileri teknolojilerden ve insan deneyiminden yararlanarak işletmelere siber tehditleri tespit etme ve bunlara yanıt verme yeteneği sağlayan bir hizmettir.

MDR'nin geleceği muhtemelen aşağıdaki eğilimler tarafından şekillenecektir.

1. Diğer siber güvenlik hizmetleriyle entegrasyon

MDR daha popüler hale geldikçe, güvenlik açığı yönetimi, tehdit istihbaratı ve güvenlik bilgileri ve olay yönetimi (SIEM) çözümleri gibi diğer siber güvenlik hizmetleriyle entegre olacaktır.

2. Bulut tabanlı MDR hizmetlerinin benimsenmesi

Daha fazla işletme BT altyapılarını buluta taşıdıkça, MDR hizmetlerinin bu değişikliğe uyum sağlaması gerekecektir. Bulut tabanlı MDR hizmetleri daha yaygın hale gelecek ve işletmelerin bulut bilişimin ölçeklenebilirliği ve esnekliğinden faydalanmasını sağlayacaktır.

3. Artan otomasyon kullanımı

MDR hizmetleri, siber tehditleri algılamak ve bunlara yanıt vermek için giderek daha fazla otomasyona güvenecektir. Otomasyon, yanıt sürelerinin kısaltılmasına, doğruluğun artırılmasına ve güvenlik analistlerinin daha karmaşık görevlere odaklanmasına yardımcı olacaktır.

4. Gelişmiş tehdit algılama yetenekleri

MDR hizmetleri, makine öğrenimi ve yapay zeka gibi ileri teknolojilerden yararlanarak tehdit algılama yeteneklerini geliştirmeye devam edecektir. Bu teknolojiler, aksi takdirde fark edilmeyecek tehditlerin tespit edilmesine yardımcı olacaktır.

5. Tehdit avcılığının proaktif olarak ele alınması

MDR hizmetleri, tehditlerin tespit edilmesini beklemek yerine aktif olarak aramayı içeren proaktif tehdit avcılığına giderek daha fazla odaklanacaktır. Bu, işletmelerin bilgisayar korsanlarının bir adım önünde olmalarına ve hasar oluşmasını önlemelerine yardımcı olacaktır.

Genel olarak, MDR'nin geleceği muhtemelen siber güvenlik tehditlerinin sürekli gelişimi ve ileri teknolojilerin artan şekilde benimsenmesi ile şekillenecektir. İşletmeler giderek daha karmaşık tehditlerle karşı karşıya kalmaya devam ettikçe, MDR hizmetlerinin çağın ilerisinde kalabilmek için uyum sağlaması ve yenilik yapması gerekecektir.

InfinitumIT ile MDR

InfinitumIT, diğer MDR hizmet sağlayıcılara göre önemli avantajlara sahip tam Yönetilen Tespit ve Müdahale çözümü sunar. MDR çözümümüz, endüstri standardı algılama ve yanıt vermenin ötesine geçer ve tehditleri ortadan kaldırma ve önleme sürecinin tamamına daha sofistike ve entegre bir yaklaşım sağlar.

01 Uçtan uca eksiksiz hizmet

Özel SOC ekibimiz, ağınızın ve uç noktaların 7/24 izlenmesini sağlayarak şirket içi kaynaklarınızı temel faaliyetlerinize odaklanması için serbest bırakır ve yönetim yükünü azaltır.

02 Gelişmiş tehdit algılama

Siber tehdit konusundaki uzmanlığımız ve tehdit istihbaratı kullanımımız, gelişmiş kötü amaçlı yazılımlar, istismarlar ve gizli komut dosyası tabanlı saldırılar da dahil olmak üzere tüm ana vektörlerdeki gelişmiş saldırıları proaktif olarak ortaya çıkarmamıza ve ihlalleri durdurmamıza olanak tanıyarak işletmenize üst düzey güvenlik sağlar.

03 Etkili tehdit tespiti ve müdahalesi

Yapay zeka destekli tehdit istihbaratı, otomatik sistemlerden elde edilen hızlı yanıt ve özel güvenlik uzmanlarından oluşan ekibi ile sürekli gelişen siber güvenlik ortamına ayak uyduran InfinitumIT, tehdit algılama ve yanıta yönelik eksiksiz bir yönetilen yaklaşım sunar.

04 360 derece tehdit görünürlüğü

Çözümlerimiz, işletme ağının içindeki ve dışındaki siber tehditlerin 360 derece görünümünü sağlar. Şirket içinde, bulutta ve hibrit ortamlarda sağlanan tam tehdit görünürlüğü, güvenlik uzmanlarından oluşan ekibimiz tarafından izlenir.

05 Özel çözümler

InfinitumIT, ihtiyaçlarınız için doğru teknolojileri seçebilmeniz ve kendi teknoloji çözümlerinizle entegre edebilmeniz için özel MDR çözümleri oluşturmanıza olanak tanır.

06 Raporlama ve uyum

InfinitumIT, hem haftalık hem de aylık hizmet raporlarının yanı sıra düzenli teknik servis incelemeler ve uygunluk raporları sağlar.

07 7/24 izleme

Analistlerimiz ağınızı ve uç noktalarınızı 7/24 izler. Bu sayede işletmeniz herhangi bir tehditle karşılaştığında, anında yanıt vermeye hazır hale getirilir.

InfinitumIT MDR hizmetinin işletmenize nasıl yardımcı olabileceği hakkında daha fazla bilgi edinmek isterseniz, hemen bir InfinitumIT uzmanıyla iletişime geçin.

infinitum IT
Power of integrated Security

İşletmenizin MDR Hizmetine mi İhtiyacı Var ?

Siber Güvenlik Uzmanlarımızla Görüşün

Sizi Arayalım

www.infinitumit.com.tr

infinitumitlabs