SİBERGÜVENLİK İLE İLGİLİ ÖNERİLER / EN İYİ UYGULAMALAR

Saldırılarda ve veri ihlallerinde eşi görülmemiş bir artışla birlikte mevcut tehdit ortamımızın görünümü , güvenlik dünyasının çevrelerindeki riskleri ve tehditleri azaltmak için sürekli inceleme ve benimseme sürecine ihtiyacı bulunmaktadır. Makine öğrenimi ve otomasyon gibi alanlardaki gelişmeler sayesinde güvenlik yanıt sistemleri artmaktadır. Siber suçlular ise teknolojik gelişmelerden kendi çıkarları için yararlanma konusunda oldukça beceriklidirler. İşletmelerin kendilerini saldırılara karşı korumak için doğru politikalara , süreçlere ve prosedürlere sahip olduklarından emin olmak için temellerini en iyi uygulamalarla kapsaması çok önemlidir. Ağ güvenliğinizi sağlamak ve verilerinizi korumak için her şirket tarafından söylenen öneriler ve en iyi uygulamalar hayata geçirilmelidir. Başarılı olmak çabalarınızın devam etmesiyle olacaktır. Düzenli olarak yöntemler değerlendirilmeli ve gerekirse koşullar değiştikçe değiştirilmelidir.

Ağı denetleyerek güvenlik kontrollerinin sorunsuz olduğundan emin olunuz. Güvenli ortamı sürdürmek bilgi gerektirir. Ağın net bir resmine sahip olmak BT grubu tarafından olmazsa olmazdır. Şirketin güvenlik duruşu önemlidir. Denetim tek seferlik bir iş olmamalı , daha ziyade tekrar eden bir süreç olmalıdır. BT çalışanları , denetim yoluyla şunları yapabilir ; Ele alınması gereken olası kusurları belirleyebilir. Yetersiz veya gereksiz tüm arka plan uygulamalarını tanımlayabilir ve kaldırılabilir. Güvenlik duvarının gücünü ve yapılandırmasının durumunu belirleyebilir. Ağa bağlı sunucuların , ekipmanın , yazılımın ve uygulamaların envanteri çıkartabilir. Güvenlik altyapısının genel etkinliğini doğrulayabilir. Sunucu yedeklemelerinin durumunu doğrulayabilir.

Güvenlik politikalarınızı gözden geçirip güncelliğinden emin olma ; Sağlam güvenlik duruşu sürdürmek için gerçekçi ve geçerli güvenlik politikanız olmalıdır. Kuruluşlar , mevcut iş operasyonlarını ve güvenlik ihtiyaçlarını karşılamaya devam ettiklerinden emin olmak için sık sık politikaları gözden geçirmeyi unuturlar. Kuruluşlar bu standartları hem BT personeline hem de son kullanıcılara çok sık iletmekte başarısız olmaktadır. BT uzmanları , değişiklikleri uygulamaya koyma ve yürütme konusunda resmi yönergeye sahip olmak gibi kuralları yeniden incelemek ve güncellemek için SANS Enstitüsü gibi kuruluşların referans materyallerini kullanabilir.

Verilerinizin yedeğini alarak kurtarma planı yapma ; İşletmeler , sorunun olup olmadığıyla değil , sistemlerine ne zaman saldırılacağı olduğu tehdit ortamında faaliyet göstermektedir. Bu nedenle , hem operasyonel açıdan kritik hem de son derece hassas verileri yedeklemek hayati önem taşımaktadır. Fidye yazılımı saldırıları her ölçekten işletmeyi etkileyerek daha tehlikeli hale geldikçe , kesinti süresini en aza indiren ve paradan tasarruf sağlayan kurtarma stratejisine sahip olmak kritik önem taşımaktadır.

Hassas bilgileri şifreleme yoluyla koruma ; Kuruluşun en değerli ve hassas verilerini korumanın bir yolu da veri şifrelemesidir. Veri kategorileri düzenli olarak gözden geçirilerek gerektiğinde şifreleme kullanılmalıdır. Zorunlu çalışanlar , hassas bilgilere uzak yerlerden erişerek faydalanabilir. Ek bir güvenlik düzeyi olarak VPN'ler kullanılabilir.

Kötü amaçlı yazılımdan koruma yazılımı güncellenmesi ; İşletmelerdeki en yaygın güvenlik açıklarından biri de güncel olmayan virüsten koruma veya kötü amaçlı yazılımdan koruma yazılımlarıdır. Aynı zamanda başa çıkmak için en basit olanlardan biridir. Koruma uzmanları , tüm cihazların en yeni güvenlik yazılımını çalıştırdığından emin olmak için kötü amaçlı yazılımdan koruma yazılımlarını düzenli olarak doğrulamalıdır.

İhtiyaçlarınıza ve kullanımınıza uygun erişim kontrollerini ayarlama ;

Çok faktörlü kimlik doğrulama ; Etkili erişim kontrolü , hangi kullanıcıların ve cihazların hangi kaynaklara erişimi olduğunu belirleyen politikaların oluşturulmasıyla başlar. Bilgiye kimin erişimi olduğunu kontrol etmek , erişim yönetim sistemlerinin ve ayrıcalıklı erişimin kullanılmasını gerektirmektedir.

Parola yönetimi ; Ağ güvenliği en iyi uygulamalarının da önemli bir yönüdür. Şifreler en az 10 karakter uzunluğunda olmalı ve düzenli olarak değiştirilmelidir. Parola yönetim yazılımı bu süreci kolaylaştırabilir. Bir diğer önemli teknoloji de yalnızca uygun kişinin uygun kaynağa erişimidir.

Bir güvenlik yönetişim yapısı kurularak iletilmelidir ; Uyumluluk her zaman güvenlik anlamına gelmese de , kendinizi tehditlerden nasıl koruyacağınız konusunda değerli bilgiler sağlayabilir. Uluslararası Standardizasyon Örgütü ile Ödeme Kartı Endüstrisi Güvenlik Standartları gibi düzenleyici kurumlar , örgüt oluşturmanın önemini vurgulamaktadır. Güvenliği sağlamaktan ve siber güvenlik olaylarına yanıt vermekten kimin sorumlu olduğunu tanımlar. Risk için bireysel sorumluluklar , yönetim , olay müdahalesi BT organizasyonları tarafından tanımlanmalıdır. Kuruluşlar , güvenlik açığı düzeltmelerine öncelik verebilir ve periyodik risk değerlendirmeleri yaparak hizmet dışı kalma süresinden tasarruf edebilir.

Son kullanıcıların eğitilmesi ; Kimlik avı saldırılarının birçok siber suçlunun tercih ettiği bir yöntem olduğu çağda , son kullanıcı farkındalığı çok önemlidir. Son kullanıcılar , normal iletişim gibi görünen saldırılara karşı savunmasızdır. Siber suçlular , profesyonel etkileşimleri yakından taklit etmek için e-posta ve diğer iletişim biçimlerini kullanma konusunda daha ustalaştıkça , bir personelin tehdide yenik düşme riski de artacaktır. Son kullanıcı eğitimi , çalışanları değişen tehdit ortamı ve ilgili kurumsal güvenlik politikaları hakkında bilgilendirmek için şirket kültürünün ayrılmaz bir parçası olan sürekli bir süreç olmalıdır.

En son haberlerin takip edilmesi ; Ağ güvenliğini sağlamanın en önemli gereksinimlerinden biri disiplini sürekli çaba olarak ele almaktır. Bu , tehdit ortamındaki gelişmelere ayak uydurmayı içermektedir. Güvenlik ve BT uzmanları , siber suçluların taktiklerini nasıl değiştirdiğinin farkında olmalıdır. Tehdit algılama ve azaltma gelişmeleri konusunda güncel kalmaları gerekir. Amaç , gelecekteki olayların olumsuz sonuçlarını azaltmak için önceki olaylardan öğrenilenleri kullanmak olmalıdır. Güvenlik altyapısı bakım sistemine sahip olunuz. BT işletmeleri , güvenliği , tüm sistemlerin ve kontrollerin çalışır durumda olduğundan emin olmak için düzenli kontroller gerektiren sürekli faaliyet olarak görmelidir. Firmalar altyapılarının güncel ve iyi çalışır durumda olduğunu garanti altına almak için protokoller oluşturmalıdır. Olay meydana geldiğinde , güvenlik sistemleri izlenerek değiştirilmelidir. BT kuruluşları , güvenlik politikaları ve uygulamalarında yapılan değişikliklerin onaylanmasına ve iletilmesine izin veren prosedürleri uygulamalıdır.

Veri güvenliği en iyi uygulamaları ; Veri güvenliği en iyi uygulamalarını bir işletmenin boyutuyla sınırlamak daha önce hiç işe yaramamıştır ve gelecekte de işe yaramayacaktır. Bilgisayar korsanları , işletmeleri ve müşterileri dolandırmak gibi açık hedefle tüketici verilerini toplamaktadır. Bilgisayar korsanlarının büyük şirketleri hedeflemeyi tercih ederken , aynı zamanda daha küçük firmalara da çekildikleri sır değildir. Etkili veri güvenliği önlemlerinin uygulanması esastır ;

Hassas verileri tanıyarak kategorilere ayırma ; Verilerinizi başarılı şekilde korumak için öncelikle ne tür verileriniz olduğunu anlamalısınız. Güvenlik ekibinizin veri havuzlarınızı taramasına ve sonuçlara göre raporlar üretmesine izin veriniz. Daha sonra verileri şirketiniz için önemine göre kategorilere ayırabilirler. Veriler oluşturulurken , değiştirilirken , işlenirken veya gönderilirken sınıflandırma güncellenebilir. İnsanları kategorizasyon derecelerini bilinçsiz kullanmaktan caydırmak için düzenlemeler yapmanız da faydalı olacaktır. Veri sınıflandırmasındaki yükseltmeler ve düşürmeler ayrıcalıklı kullanıcılarla sınırlandırılmalıdır.

Veri kullanımı için politikanızın olması ; Veri sınıflandırması yeterli değildir. Bunun yanında farklı erişim biçimlerini , veri erişimi için sınıflandırmaya dayalı kriterleri , verilere kimin erişimi olduğunu , uygun veri kullanımını neyin oluşturduğunu vb. açıklayan ilkeye ihtiyacınız olacaktır. Belirli alanlara kullanıcı erişimini kısıtlayarak bittiğinde bunları kapatabilirsiniz. Politika ihlalinin ciddi sonuçlara yol açabileceğini unutmayınız.

Hassas verilere kimlerin erişimi olduğuna dair kayıt tutma ; Uygun kullanıcıya uygun düzeyde erişim denetimi sağlamalısınız. Bilgi erişimini , sadece amaçlananları gerçekleştirmek için gereken ayrıcalıkların verilmesi gerektiğini belirten en az ayrıcalık ve bilinmesi gereken ilkesine dayalı olarak sınırlandırınız. Bu , verilerin sadece uygun kullanıcılar tarafından kullanılmasını sağlayacaktır.

Verileri fiziksel olarak koruma ; İş istasyonlarınızı kullanılmadıklarında kapatarak ve hiçbir aygıtın fiziksel olarak tesislerinizden kaldırılmadığından emin olarak işe başlayabilirsiniz. Veri depolama sabit disklerinizi ve diğer kritik bileşenlerinizi koruyacaktır. Dolandırıcıların işletim sistemlerinize önyükleme yapmasını önlemek için BIOS parolası ayarlayınız. USB flash sürücüler , Bluetooth aygıtları , akıllı telefonlar , tabletler ve dizüstü bilgisayarların hepsinin halledilmesi gerekmektedir. Verilerinizi korumak için uç nokta güvenlik teknolojilerini kullanınız. Ağınızın uç noktaları sürekli saldırı altındadır. Bu sebeple , veri ihlallerini önlemek için güçlü uç nokta güvenlik altyapısı kurmak çok önemlidir. Şu adımları izleyerek başlayabilirsiniz ; Tüm sunuculara ve iş istasyonlarına antivirüs yazılımı yüklenmelidir. Düzenli taramalarla sisteminizin sağlığını ve fidye yazılımı gibi enfeksiyonları koruyunuz.

Casus yazılımdan koruma ; Casus yazılım , kullanıcının izni olmadan sık sık yüklenen bir tür zararlı bilgisayar yazılımıdır. Birinci amacı ; kullanıcı davranışı ve kişisel bilgiler hakkında veri toplamaktır. Casus yazılım önleme ve reklam yazılımı önleme programları , bunları kaldırmanıza veya engellemenize yardımcı olabilir.

Açılır pencere engelleyiciler ; Açılır pencereler , sisteme zarar vermekten başka görünür neden olmaksızın bilgisayarınızda çalışan istenmeyen programlardır. Açılır pencere engelleyicileri kullanarak kendinizi güvende tutunuz.

Güvenlik duvarları ; Güvenlik duvarları , verileriniz ve dolandırıcılar arasında engel görevi görerek veri güvenliği en iyi uygulamalarından biri olarak verilerinizi savunur. Dahili güvenlik duvarları kurularak ek güvenlik sağlanabilir. Siber güvenlik politikalarınızın listesini yapınız. Siber güvenlik söz konusu olduğunda , yüzyüze iletişim ve içgüdüler en iyi seçenekler değildir. Çalışanlarınıza ve paydaşlarınıza çevrimiçi eğitim , kontrol listeleri ve bilgiye özel bilgi aktarımı sağlamayı kolaylaştırmak için siber güvenlikle ilgili en iyi uygulamalarınızı , kurallarınızı ve protokollerinizi kapsamlı şekilde belgeleyiniz.

Risk tabanlı güvenlik yaklaşımı benimseyiniz. Kuruluşunuzun karşılaşabileceği tehditler ve bunların çalışan ile müşteri verilerini nasıl etkileyebileceği gibi en küçük noktalara dikkat ediniz. Kapsamlı risk değerlendirmesinin gerekli olduğu yerdir. Risk değerlendirmesinin yapmanızı sağladığı şeylerden bazıları şöyledir ; Varlıklarınızı ve konumlarını belirleyiniz. Mevcut durum siber güvenliğinizi belirleyiniz. Güvenlik yaklaşımınızı takip ediniz. Risk bazlı strateji kullanarak yönetmeliklere uyun ve şirketinizi olası sızıntılara ve ihlallere karşı koruyunuz. Birden çok faktörle kimlik doğrulaması yapınız. MFA , en gelişmiş ve kanıtlanmış veri güvenliği yöntemlerinden biridir. Bir hesabı doğrulamadan önce MFA , koruma derecesi ekler. Bilgisayar korsanı parolanıza sahip olsa bile , güvenlik belirteci , parmak izi , ses tanıma veya cep telefonu onayı gibi ikinci veya üçüncü doğrulama öğesi oluşturması gerekir.

Hizmet hesaplarını yönetmek ve güvence altına almak için en iyi uygulamalar ; Hizmet hesapları olarak bilinen insan dışı ayrıcalıklı hesaplar , otomatik hizmetler , sanal makine örnekleri ve diğer etkinlikleri gerçekleştirmek için kullanılır. Hizmet hesapları , belirli durumlarda etki alanı yönetici ayrıcalıklarına sahip ayrıcalıklı yerel veya etki alanı hesapları olabilir. Bu yüksek düzeyde erişim , birçok BT prosedürünün daha sorunsuz ilerlemesini sağlayarak çeşitli uygulamalarda ve işlemlerde tek hizmet hesabı kullanılabilir. Birbirleriyle bağlantılı olmaları ve kullanımlarının hayati gerekliliği , kontrol edilmelerini son derece zorlaştırmaktadır.

Hizmet hesaplarının bakımı ve korunmasına yönelik en iyi uygulamaları ile çözümleri ; Tüm hesapları tanımlayarak bunları merkezi yönetim altına alınız. Tüm hesap türlerinde ilk hedef , hepsinin merkezi olarak yönetilebilmesi için sürekli tanımlama ve kataloglama mekanizması uygulamaktır. PAM çözümleri , bir hizmet hesabının bulunduğu her siteyi bulabilir. Firmaların hesaba katılmayı ve risk azaltmayı hızlandırmasına yardımcı olur.

Yeni hesaplar için işe alım ve hesap yönetimi otomatikleştirilmesi ; BT altyapıları dinamik olduğundan otomatik keşif özellikleri zamandan tasarruf sağlayarak hiçbir hesabın yönetilmeyen kalmamasını sağlar. Hesapları otomatik olarak profillendirerek ve sınıflandırarak , yeni hizmet hesapları neredeyse anında kontrol altına alınarak insan yönetiminin karmaşıklığını ve riskini ortadan kaldırır. Bir sistemdeki tüm haklara tam görünürlük sağlar. Hizmet hesabı ayrıcalıklı kimlik bilgileri (parolalar , SSH anahtarları) merkezi olarak şifreli kimlik bilgileri kasasında saklanmalıdır. Kötüye kullanım tehlikesini azaltmak için bu kimlik bilgilerine erişim sınırlandırılmalı ve izlenmelidir.

Hizmet hesabı kimlik bilgilerinin tüm yerlere otomatik olarak yayılması ; Referans alındıkları yer , önleme sisteminin hayati bir yönüdür. Hizmet hesabı kimlik bilgileri değiştikçe arızalar ve kesinti süreleri değişecektir.

En Az Ayrıcalık İlkesini Kullanma ; İstenen görevleri yürütmek için gereken minimum ayrıcalıklarla hizmet hesapları oluşturmak en iyisidir. Uzaktan erişim , internet ve e-posta erişiminin yanı sıra uzaktan kontrol izinleri , normalde silinebilecek ek ayrıcalıklardan bazılarıdır.

ACL'ler , varlıklara kaynak atamak için kullanılır. Bu sürecin bir parçası olarak , hizmet hesabının erişiminin olduğu tüm kaynakları belirlemeli , bu erişimin uygun olup olmadığını değerlendirmeli ve en az ayrıcalığın uygulanmasını sağlamak için gerekli ayarlamaları yapmalısınız. En az ayrıcalığın bir parçası olarak , belirli bir kimliğe bağlı hizmet hesaplarının sayısını minimumda tutmaya çalışmalısınız.

Yol haritanız için önerilen teknolojiler ; Teknoloji sürekli büyüyor ve dijital dönüşümün , özellikle de siber güvenliğin bir adım önünde olmak , bir kuruluşun başarısı için her zamankinden daha fazla kritik önem taşımaktadır. Geçen yıl fidye yazılımı saldırılarında önemli artış görülmüştür ve işletmeler bunun bedelini ödemişlerdir. Gelecekte BT sistemlerini ve kurumsal ayarları daha iyi korumak için bu olaylardan alınacak çok dersler vardır fakat en önemli keşif , fidye yazılımlarının artık sektör ne olursa olsun her şirket için iş güvenliği riski olduğudur. Benimseme açısından yol haritanızda göz önünde bulundurmanız gereken teknolojiler şunlardır ;

Sıfır güven ağ erişimi " Zero Trust " ; Bilgisayar korsanları , fidye yazılımı saldırıları söz konusu olduğunda erişimi olmayan sistemleri şifreleyemezler. Bu riski iki teknolojiyi birleştirerek ele almak mümkün olacaktır ; sıfır güven ve yazılım tanımlı çevre. Sıfır güven ile birlikte kullanıldığında , yazılım tanımlı çevre , kullanıcının cihazının sürekli olarak numaralandırılmasının yanı sıra kullanıcının kimliğinin ve erişim düzeyinin doğrulanmasını sağlar. Uzak uç cihaz bağlantı noktası , kullanıcı cihazı gerekli standart için doğrulandıktan sonra ancak o zaman bu kullanıcıya sunulacaktır. Kullanıcılar ağ öğelerine sadece belirtilen kullanıcı erişilebilirlik düzeyinde erişebilir. Bu nedenle bu iki teknolojinin stratejik kullanımı şirket için gelişmiş güvenlik sağlayacaktır. Bu tür bir platform , bir kullanıcının güvenlik gereksinimlerini karşılamak için çeşitli şekillerde kurulabilir. Bu teknoloji , kullanıcıların görevlerini yerine getirmek için gereken seviyeye erişmelerini sağlar. Kullanıcı oturumu kapattığında veya zaman aşımına uğradığında bağlantı noktası kapatılarak hiçbir bağlantı noktası sorgulara yanıt vermeyeceğinden uzak uç sistemi artık tanımlanamazlar.

MDR / EDR / XDR ; Endpoint Detection and Response (EDR) , akıllı yeni nesil antivirüs yazılımıdır. Genişletilmiş Algılama ve Yanıt (XDR) , ortamınızda neler olup bittiğine dair size daha iyi resim sunmak için EDR verilerini ağ olaylarıyla birleştirir. EDR'ler size davranışsal verilerinizin daha iyi bir görünümünü verebilir. Bir kullanıcının verilere erişiminin olması , ona özenle davranacağını garanti etmez. EDR ve XDR programları , çevrede meydana gelen olayların görünürlüğünü ve korelasyonunu iyileştirerek tehdidin hızlı şekilde tanımlanabilmesi için gürültüyü en aza indirip bekleme süresini azaltır. Çoğu EDR sistemi kendi başına katma değerli veriler sağlayarak çevreye ilişkin derinlemesine bütünsel görünüm sağlamaz. MDR platformları , fidye yazılımlarına ve diğer kötü amaçlı yazılım türlerine karşı kritik savunma noktası haline gelmiştir.

Davranışsal analitik " Behavioral analytics " ; Bireylerin web siteleri , mobil uygulamalar , sistemler ve ağlarla nasıl etkileşime girdiğini anlamak için verileri inceler. Siber güvenlik alanındaki profesyoneller , potansiyel tehditleri ve zayıflıkları belirlemek için davranışsal analitik platformları kullanabilir. Model analizi , siber güvenlik tehditleri önerebilecek tuhaf olayları ve davranışları keşfetmeye yardımcı olabilir. Davranışsal analitik , bir cihazın olağandışı derecede önemli miktarda veri ürettiğini ortaya çıkarabilir. Bu , siber saldırının yakın olduğunu veya halihazırda devam ettiğini gösterebilir. Düzensiz bir sırayla meydana gelen olayların ve eylemlerin tuhaf zamanlaması , kötü niyetli faaliyetin diğer belirtileridir. Olası saldırıların erken tespiti ve gelecekteki saldırıları tahmin etme kapasitesi , davranışsal analitiğin iki avantajıdır. Davranış analitiği , işletmelerin algılama ve tepkiyi otomatikleştirmesine yardımcı olabilir.

Blok Zinciri ; Verileri güvenli şekilde bloklar halinde tutan veri tabanı biçimidir. Blokları bağlamak için kriptografi kullanır. Bilgi blok zincirinde toplanabilir fakat değiştirilemez veyahut kaldırılamazlar. Siber güvenlik uzmanları , sistemleri veya cihazları güvence altına almak , tek tip güvenlik süreçleri geliştirmek ve veritabanı korsanlığını neredeyse imkansız hale getirmek için blok zinciri kullanabilir. Daha iyi kullanıcı gizliliği , insan hatasını azaltarak şeffaflığı artırdı ve üçüncü taraf doğrulama ihtiyacını ortadan kaldırarak maliyet tasarrufu , blockchain'in tüm avantajlarını ortaya çıkarmıştır. Verileri tek bir yerde depolamanın güvenlik sorunu da blok zinciri tarafından ele alınmaktadır. Bunun yerine , veriler ağlar arasında dağıtılarak bilgisayar korsanlarına karşı daha az savunmasız olan merkezi olmayan sistem oluşturulur. Blok zincirinin maliyeti ve verimsizliği , teknolojinin dezavantajlarından ikisidir.

Bulut şifreleme ; Bulut hizmetleri , kuruluşların verimliliği artırarak daha iyi uzaktan hizmetler sunmasını ve paradan tasarruf etmesini sağlar. Bulutta veri depolama ise veri güvenliği risklerini artırabilir. Veriler buluta gönderilmeden önce , bulut şifreleme teknolojisi onu okunamayan koda dönüştürür. Bulut şifrelemeyi tamamlamak için siber güvenlik uzmanları matematiksel yöntem kullanır. Kodun kilidi yalnızca yetkili kullanıcılar tarafından şifreleme anahtarı kullanılarak açılabilir ve verilerin bir kez daha okunmasına izin verilir. Yetkisiz saldırganların neden olduğu veri ihlalleri , bu kısıtlı erişimle daha az olasıdır. Uzmanlara göre bulut şifreleme , verilerin güvenliğini sağlamanın harika bir yoludur. Şifreleme kullanılıyorsa yetkisiz kullanıcılar buluttaki verilere erişemezler. Bulut şifreleme , işletmelerin devlet gereksinimlerine uymasına yardımcı olurken aynı zamanda müşterilerin bulut hizmetlerine olan güvenini artırır.

Bağlama duyarlı güvenlik " Context-aware security " ; Bağlama duyarlı güvenlik , kuruluşların daha iyi gerçek zamanlı güvenlik kararları almasına yardımcı olan siber güvenlik teknolojisidir. Geleneksel siber güvenlik sistemleri , evet / hayır soruları sorarak sisteme mi yoksa verilere mi erişim izni verip vermeyeceğini belirler. Bu kolay işlem sonucunda bazı geçerli kullanıcılar reddedilebilir ve bu da üretkenliği azaltır. Bağlama duyarlı güvenlik , yetkili kullanıcının erişiminin reddedilme olasılığını en aza indirir. Bağlama duyarlı güvenlik , evet / hayır yanıtlarına bağlı kalmak yerine , kullanıcının meşruluğunu zaman , konum ve URL itibarı gibi çeşitli destekleyici veri noktalarını kullanarak değerlendirir. Bağlama duyarlı güvenlik , veri erişimini hızlandırarak meşru kullanıcıların işlerini kolaylaştırır. Öte yandan , son kullanıcı gizlilik hususları bir sorun teşkil etmektedir.

Savunmaya yönelik yapay zeka ; Savunmaya yönelik yapay zeka (AI) , siber saldırıları tespit etmek ve önlemek için siber güvenlik uzmanları tarafından kullanılabilir. Standart siber güvenlik çözümleri , düşmanca yapay zeka ve düşmanca makine öğrenimi gibi teknolojileri tespit etmekte zorlanarak bilgili siber suçlular bunlardan yararlanır. Deep fake , sahte fotoğraflar , kişiler ve videolar , hiç olmamış veya var olmayan kişileri veya şeyleri etkili şekilde tasvir ettikleri için saldırgan AI örnekleridir. Kötü niyetli aktörler , makinelere hatalı veriler sağlayarak , onların arızalanmasına neden olmak için düşmanca makine öğrenimini kullanabilir. Savunma amaçlı yapay zeka , siber güvenlik uzmanları tarafından saldırgan yapay zekanın bir sistemin veya ağın nasıl çalıştığını izlemesini , test etmesini ve öğrenmesini belirlemek , önlemek için kullanılabilir. Savunma amaçlı yapay zeka , algoritmaları güçlendirerek kırılmasını zorlaştırabilir. Araştırmacılar , daha sıkı güvenlik açığı testleri gerçekleştirmek için makine öğrenimi algoritmalarını kullanabilir.

Sıfır güven ; Uygulamalara ve verilere izin verilmeden veya erişim sağlanmadan önce , kuruluşun ağının içindeki veya dışındaki tüm kullanıcılar , güvenlik yapılandırması ve duruşu için doğrulanmalı , yetkilendirilmeli ve sürekli olarak değerlendirilmelidir. Sıfır Güven , tipik ağ ucu olmadığını varsayar ; ağlar yerel , bulut tabanlı veya ikisinin bir karışımı olabilir ve kaynaklar ve çalışanlar herhangi bir yerde bulunabilir. Günümüzün modern dijital dönüşümü için Zero Trust , altyapıyı ve verileri korumaya yönelik çerçevedir. Uzak çalışanları , hibrit bulut ayarlarını ve fidye yazılımı saldırıları gibi günümüzün kurumsal endişelerini karşılayan türünün tek ürünüdür. Birçok tedarikçi Sıfır Güven'i kendi başına tanımlamaya çalışsa da , Sıfır Güven'i işinizle uyumlu hale getirmenize yardımcı olabilecek saygın kuruluşlardan çeşitli standartlar vardır.

Sıfır güven ve NIST 800-27 ; NIST 800-207 , mevcut satıcılardan en tarafsız , kapsamlı standarttır. Sadece devlet kurumları için değil tüm şirketler için geçerlidir. Forrester's ZTX ve Gartner's CARTA gibi kuruluşların diğer özellikleri de dahildir. NIST standardı şunları sağlar ;günümüz saldırılara karşı uyumluluk ve koruma. işletmelerin bulut öncelikli , her yerden çalışma paradigması vardır.

Sıfır güven ilkeleri ; Sıfır güven güvenliğini uygulamak oldukça basittir. Sıfır Güven üç ana ilkeye dayanmaktadır ; Her kullanıcıyı doğrulayınız. Her cihazı doğrulayınız. Erişimi akıllıca sınırlayınız.

Her kullanıcıyı doğrulama ; Tek oturum açma gibi sadece tek bir kimlik doğrulama mekanizmasına dayanan işletmeler sıklıkla hata yapar. Kullanıcılar bir şeyi her kullanmak veya bir şeye erişmek istediklerinde şifre yazmak zorunda kalmazlar. Tek oturum açma (SSO) ile yönetmeleri gereken şifre sayısı azalır. Peki ya bu kimlik bilgilerinden biri çalınırsa veya biri masasından ayrılırken bilgisayarını kilitlemeyi unutursa? SSO , bu durumda güvenlik açığı oluşturur. Bu sorunu önlemek için TOA , MFA gibi diğer teknolojilerle eşleştirilmelidir.

MFA , yeniden yönlendirme döngüleri veya fiziksel anahtarlarla uğraşma fikirleri uyandırabilirken , teknoloji son yıllarda çarpıcı şekilde gelişmiştir. SSO ile eşleştirildiğinde , bir kuruluşun ağını çevreleyen güvenli ağ oluşturur. Ama yeterince güvenli değildir. Sonunda , güvenlik ve son kullanıcı memnuniyeti arasında denge kurmalısınız.

Her cihazı doğrulama ; Günümüzde neredeyse herkesin akıllı telefonunda şifresi vardır. Fakat parolaların yapbozun yalnızca bir parçası olduğunu unutmayınız. Gerçek güvenliği elde etmek için cihazların ayrıca uyarlanabilir MFA'ya sahip olması gerekir. MFA destekli şifreler bir miktar cihaz kontrolü ile birleştirildiğinde , ilgili kurallar kurulup yerinde kilitlendiğinde ve cihazın içeriği (nerede kullanıldığı , hangi tarayıcıya sahip olduğu vb.) her zaman bilinir.

Erişimi akıllıca sınırlama ; Bir kuruluşun kaynaklarını kimin kullandığını anlamak , Sıfır Güven'in son yönüdür. Kime erişim sağlıyoruz? Sorusuna cevaptır. Görevlerini tamamlamak için hangi kaynaklara ihtiyaç duyuyorlar ve bunu nasıl ele alıyoruz? Bu kullanıcıların en baştan üretken olduklarından , ihtiyaç duydukları hesaplara erişimlerinin olduğundan , cihazlarının ihtiyaç duydukları istemcilerle yapılandırıldığından emin olunuz. İş değiştirdiklerinde erişimleri de değişir ve ayrıldıklarında ayrıcalıkları otomatik olarak geri alınır. En önemlisi , API'ler ve uygulamalarda oturum açan kullanıcılar için erişim kararlarının gecikmeden alınabilmesi için tüm bu özelliklerin birbirine bağlı olması ve gerçek zamanlı olarak birlikte çalışması gerekir.

Sıfır güven benimseme yolu ; Sıfır güven yolculuğuna çıkarken atılması gerektiğine inandığımız bazı önemli adımlar şöyledir ;

Sıfır güven terimini tanımlayınız ; İdeal başlangıç noktası , ekibinizin bir araya gelerek sıfır güven kavramı üzerinde anlaşmaya varmasıdır. Politika hedeflerini tanımlayarak bunlara ulaşmak için yol haritası oluşturunuz. Mevcut çevre koruma teknolojisinin terk edilmesi gerektiği anlamına gelmez. Bununla birlikte , önemli varlıklarınızı korumak söz konusu olduğunda , kutunun dışına çıkıp organizasyonel düzenlemeler yapmaya istekli olmak anlamına gelir.

Kullanıcı deneyimini tanıyınız ; Stratejinizi oluştururken sıfır güven yaklaşımının kullanıcı deneyiminiz üzerindeki etkisini düşününüz. Asla güvenmemeyi ve her zaman onaylamayı vurgulayan sıfır güven yaklaşımı , kullanıcıların sistemleriniz ve verilerinizle etkileşimini değiştirebilir. Kullanıcılarınızın kim olduğunu , hangi uygulamaları kullandıklarını , uygulamalarınıza nasıl bağlandıklarını ve bu erişimi korumak için uyguladığınız güvenlik kontrollerini anlamalısınız. Kullanıcı deneyimini değiştirmeden önce , gelecekte nasıl görüneceğini bildiğinizden emin olunuz. Tüm uygulamalarınızda ve tüm kullanıcılara tutarlı şekilde sıfır güvenin uygulanmasını nasıl sağlayacağınızı düşününüz.

Doğru mimariyi seçme ; Sıfır güven modeli oluşturmak için tek bir teknik veya teknoloji yoktur. En temel düzeyde , sıfır güven , uygulamalarınıza yalnızca güvenli şekilde yetkilendirilmiş kullanıcıların ve cihazların erişimini garanti etmekle ilgilidir. Ağda nerede olduğunuz , kimliğinizin ne kadar iyi doğrulandığı ve cihazınızın ne kadar güvenilir olduğu önemli değildir. Sıfır güven modeli oluşturmanın birbiriyle rekabet eden üç yolu vardır ; mikro segmentasyon , yazılım tanımlı çevreler (SDP) ve sıfır güven proksileridir. Mikrosegmentasyon yıllardır şu veya bu şekilde olmuştur ve tüm ağ varlıklarını , kullanıcıları , uygulamaları , veri depolarını ve diğer öğeleri mantıksal kategorilerde gruplandırmayı gerektirir. Gruplar , yaygın olarak VLAN kullanan yerleşim bölgelerine bölünmüştür ve güvenlik duvarı , aralarında trafik polisi görevi görür. Bazı insanlar yanlışlıkla sıfır güvenin ağ segmentasyonu ile ilgili olduğuna inanır fakat durum böyle değildir.

Sıkı kullanıcı ve cihaz doğrulama prosedürlerini uygulama ; Sıfır güven , her uygulamanın , uç noktanın , altyapının ve kullanıcının güvenliğinin nasıl sağlandığının tamamen elden geçirilmesini gerektirir. Sıfır güven ve geleneksel güvenlik arasındaki temel fark , zorlama mekanizmalarının ağ çevresinden hedef sistem ve uygulamaya aktarılmasıdır. Bir kullanıcının kurumsal kaynağa güvenilir veya güvenilmeyen ağ üzerinden erişip erişmediğine göre güvenlik önlemleri almak yerine , asıl odak noktası , kullanıcının kimliğini doğrulamak ve cihazını onaylamaktır. Kullanıcı tarafında , sağlanması gereken erişim düzeyini belirlemek için MFA ve ek doğrulama aşamalarının kullanılmasını gerektirir. Kullanıcı türü (son kullanıcı , ayrıcalıklı kullanıcı , dış kaynaklı BT , iş ortağı veya müşteri) veya erişilen kaynak ne olursa olsun , sıfır güven ilkeleri kullanılmalıdır.

Zorluklarla yüzleşmeye hazır olma ; Özellikle büyük işletmelerde sıfır güven çerçevesi oluşturmak için gereken çabanın boyutunu ve kapsamını hafife almayınız. Ağın neresinde olursanız olun , programlara yalnızca kimliği doğrulanmış ve yetkilendirilmiş erişime izin veren modele geçmek kolay değildir. Sıfır güven , uygulamayı korumadan önce kullanıcı kimliğinin korunmasını içerir. Bunu yapmanın en iyi yolu , içten dışa bağlantı , kesin erişim , kimseye güvenmeme şifrelemesi vb. sağlamaktır. Ağın ve uç noktaların artık önemli olmadığı anlamına gelir. Önemli olan , kullandıkları cihazdan veya nerede olduklarından bağımsız olarak insanların güvende olmalarıdır. Kullanıcının kimliğini korursak , kullandıkları uygulamaları anlarsak ve uygulamaları yeterince güvenli hale getirirsek , uç nokta cihazları ve ağları önemsiz hale gelir.

SD-WAN ; SD-WAN , yazılım tanımlı ağ (SDN) kavramlarını kullanarak ağ trafiğini geniş alan ağı (WAN) arasında dağıtan teknolojidir. SD-WAN , şubeler ve veri merkezi siteleri arasındaki uygulama trafiği için en verimli yönlendirmeyi bulmak için ilkeleri kullanır. Merkezi kontrolör , SD-WAN'ları yöneterek tüm bağlı cihazlara politika bilgisi gönderir. Yazılım , BT personelinin sıfır temaslı veya düşük temaslı provizyon ile ağ uç cihazlarını uzaktan programlamasına olanak tanıyarak ağ mühendislerinin şube ofislerinde manuel olarak yönlendirici kurma gereksinimini azaltır veya ortadan kaldırır. Çok Protokollü Etiket Anahtarlama (MPLS) , internet geniş bant , fiber , kablosuz veya Uzun Vadeli Evrim (LTE) gibi temel özel veya genel WAN bağlantılarını soyutlayarak , çoğu SD-WAN teknolojisi , aktarımdan bağımsız sanal yer paylaşımı üretir. SD-WAN teknolojisi , ağ kontrolünü merkezileştirir ve bu kanallar üzerinden çevik , gerçek zamanlı uygulama trafiği yönetimini mümkün kılarak işletmelerin mevcut WAN hatlarını korumasını sağlar.

SD-WAN güvenliği ; SD-WAN güvenliği büyük ölçüde segmentasyona dayanır. İşletmeler bu stratejiyi kullanarak ağ trafiğini izole edebilir , önceliklendirebilir ve atayabilir. Tanıdık olmayan bir cihazdan gelen trafik ağa bağlanmaya çalışırsa , BT önce onu güvenlik duvarı üzerinden yönlendirmek için ağ ilkeleri ayarlayabilir. Her zaman belirli bir bağlantıya gitmek için yüksek öncelikli trafiğe de öncelik verilebilir. Ağ trafiğinin kimliğini doğrulamak için çoğu SD-WAN hizmeti , İnternet Protokolü Güvenliği'ni (Ipsec) içerir. Uygulama trafiğini izlemek , ilkeleri belirlemek ve cihazlar ile siteleri yapılandırmak için SD-WAN hizmetleri ağ yönetim konsolu veya arabirimi gerektirir. Bu arayüz ayrıca uçtan uca ağ görünürlüğüne yardımcı olur. Birçok SD-WAN üreticisi , hizmetlerini SD-WAN ile entegre etmek için güvenlik firmalarıyla da işbirliği yapmaktadır.

SD-WAN ile hızlı kazançlar ; SD-WAN teknolojisi , işletmelere çeşitli avantajlar sağlar ; WAN optimizasyon tekniklerini , her uygulamanın ihtiyaçlarını karşılamak için trafiği dinamik olarak değiştirme esnekliğiyle birleştirerek geliştirilmiş uygulama performansı verir. Otomatik yük devretme , biri başarısız olursa veya kalabalıklaşırsa trafik otomatik olarak başka bağlantıya yönlendirilir. Sonuç olarak , uygulama performansı ve gecikme süresi daha da iyileştirilmiştir. Daha düşük maliyetli genel internet bağlantıları aracılığıyla daha düşük öncelikli , daha az hassas verileri ileterek , IP üzerinden ses (VoIP) gibi görev açısından kritik veya gecikmeye duyarlı uygulama trafiği için özel hatlar ayırarak , maliyetli kiralık MPLS devrelerine daha az güven oluşur. SD esnekliği WAN'lar , aşırı tedarik ihtiyacını ortadan kaldırarak genel WAN maliyetlerini düşürür. Site dağıtımları , ayarları ve işlemlerinin tümü otomatikleştirilmiştir.

Siber güvenlik stratejisinde SD-WAN'ın rolü ; SD-WAN , geleneksel ağ teknolojisine yeni güvenlik özellikleri ekleyerek ağ trafiğini kontrol etmeyi ve korumayı kolaylaştırır. BT yöneticileri için veri ihlalleri ve güvenlik riskleri en önemli konulardır. Kalifiye güvenlik personeli bulmak her zamankinden daha zordur. İşletmeler güvenlik stratejilerini geliştirmek için basit çözümler arıyorlar. Bir olasılık , SD-WAN kullanmaktır. SD-WAN'ın yeni güvenlik avantajları sağladığı ve tüm ekosistemde önemli bir rol oynadığı birkaç alanı bulunmaktadır ; VPN endişeleri artık bir sorun değildir. Bir şirket interneti bir yol olarak kullandığında SD-WAN'ın güvenlik üzerinde doğrudan etkisi vardır. Şirketler , interneti bir yedek veya hatta büyük bir taşıma yöntemi olarak kullanırken SD-WAN ortaya çıkmadan önce trafiklerinin güvenli geçişini sağlamak için bir VPN veya DMVPN oluşturacak idi. Bu , ilki artan sayıda VPN'yi yönetme ihtiyacı olan çeşitli zorluklar doğurur.

Bu VPN'leri oluşturabilmek için kurumun veri merkezlerinde güvenlik duvarlarına ve uzak konumlarda VPN cihazına veya güvenlik duvarına ihtiyacı vardır. Her site , internete bağlı kalmak için gereken çabaya bağlıdır. Yük devretme bu yöntemle bir zorluktur. Şirketler , bu arada birkaç tuşa basmak zorunda kalmadan fiber tabanlı geçiş modundan diğerine zahmetsizce geçemezler. Sorunsuz yük devretme zor ve maliyetlidir. SD-WAN , VPN sorunlarını azaltır. VPN'ler , SD-WAN'lı güvenlik duvarları gerektirmezler. VPN'lerinizi kurmanız veya trafiğinizi şifrelemeniz gerekmeyecektir. Her SD-WAN çözümü , sizin için her şeyi yöneten denetleyiciye sahiptir. Cihazı taktığınız anda , yazılım tanımlı gelişmiş motorun tüm siteler arasında tüm bu IPsec tünellerini oluşturduğu anlamına gelir.

Güvenlik trafiği azaltılmalıdır ; Tüm siteden siteye trafik şifrelenir. Bu nedenle SD-WAN'ın güvenlik stratejisini etkileyen bir diğer önemli yararı ; güvenlik parametrelerinden geçmesi gereken trafik miktarını azaltmasıdır. Güvenliği kontrol etmek artık biraz daha kolaydır. Birçok işletme siteden siteye iletişim için VPN kullandığında , güvenlik duvarlarından veya güvenlik ayak izini artıran başka şifreleme biçiminden geçmeleri gerekir. Güvenliği daha zor ve pahalı hale getirir. SD-WAN kullanarak oyunun kuralları değişmiştir.

SD-WAN yerleşik güvenlikle birlikte gelir ; Belirli güvenlik özelliklerinin doğrudan SD-WAN platformu üzerinden uygulanabilmesi , gerçek güvenlik platformundaki maliyetleri ve karmaşıklığı azaltabilmesi , SD-WAN'ın güvenlik stratejisini değiştirdiği üçüncü alandır. Silverpeak SD-WAN teklifi güvenlik içerdiğinden Silverpeak cihazları güvenliğin çoğunu sizin için halleder. Bunun üzerine ikinci güvenlik duvarı kurmanız gerekmeyecektir. Fiziksel güvenlik duvarı gereksinimini ortadan kaldıran Versa'nın SD-WAN'ı ile güvenlik duvarını sanallaştırabilirsiniz. SD-WAN , yalnızca temel koruma gerektiren siteler için bazı yerleşik güvenlik özellikleri sağlar. Belirli web sitelerine erişimi etkinleştirebilir ve kısıtlayabilir , trafiği belirli web sitelerine sınırlayabilir. SD-WAN dağıtımı , çeşitli sitelerde güvenlik ihtiyacını azaltabilir veya genişletebilir.

Secure Service Edge'e (SSE) ; Gartner'a göre Security Service Edge (SSE) , web sitelerine , SaaS uygulamalarına ve özel uygulamalara güvenli erişim sağlayan bir dizi entegre bulut merkezli güvenlik özelliğidir. SSE'ye bağlı güvenlik özelliklerinden bazıları şöyledir ; Sıfır Güven Ağ Erişimi (Zero Trust Network Access - ZTNA) , Güvenli Web ağ geçidi (Secured Web gateway - WSG) , Hizmet Olarak Güvenlik Duvarı (Firewall as a Services - FwaaS) , Bulut Güvenliği Erişim Aracısı (Cloud Security Access Broker - CASB).

Kapsamlı SSE çözümü , kuruluşlara , uygulamalara , verilere, araçlara ve diğer kurumsal kaynaklara çalışanlara , güvenilir ortaklara ve yüklenicilere güvenli uzaktan erişim sağlamak , açık olduklarında davranışları izleyerek ihtiyaç duydukları eksiksiz güvenlik teknolojileri setini sağlar. ağ. Uzak ve mobil kullanıcıların yanı sıra eriştikleri veri ve uygulamaların güvenliğini sağlamak , hibrit iş gücü büyüdükçe daha önemli hale gelecektir. SSE , yükselen endüstriyel trend olarak uzaktan çalışma , bulut bilişim , güvenli uç bilgi işlem ve dijital dönüşüm gibi temel organizasyonel zorlukları ele almaktadır. Kuruluşların verileri , SaaS , IaaS hizmetinin yanı sıra diğer bulut uygulamalarını benimsedikleri için şirket içi veri merkezlerinin dışına dağıtılır. Bulut uygulamalarına ve verilerine herhangi bir bağlantı kullanarak herhangi bir yerden erişen mobil ve uzak kullanıcılar giderek artan sayıda kullanıcıdır.

Tipik ağ güvenliği önlemleriyle , şu nedenlerden dolayı bulut uygulamalarının ve mobil kullanıcıların güvenliğini sağlamak zordur ; Daha eski teknolojiler veri merkezine bağlıdır. Bu sebeple kullanıcı bulut uygulaması etkileşimlerini izleyemezler. Kullanıcı trafiğini inceleme için veri merkezine göndermek için tipik VPN kullanmak her şeyi yavaşlatır. Geleneksel veri merkezi yaklaşımları , yönetim ve donanım bakımı nedeniyle maliyetlidir. Yama eksikliği nedeniyle VPN'lerden yararlanmak kolaydır. Daha da kötüsü , günümüzün veri merkezi güvenlik yığınları , karmaşık , entegre edilmesi zor nokta ürün koleksiyonlarına dönüşmüştür. Bu karmaşıklık , ayrı güvenlik çözümleri arasında boşluklara yol açarak karmaşık tehditler veya fidye yazılımı saldırıları tehlikesini artırır.

SSE'nin temel işlevleri ; SSE çözümünün dört temel güvenlik özelliği şöyledir ;

Sıfır Güven Ağ Erişimi (ZTNA) ; Erişim denetimi düzenlemelerine dayalı olarak uygulamalara ve hizmetlere güvenli uzaktan erişim sağlayan bir grup teknolojiyi ifade etmektedir. Bir LAN'a tam erişim sunan VPN'lerin aksine , ZTNA çözümleri varsayılan olarak reddederek yalnızca kullanıcının açıkça talep ettiği hizmetlere erişime izin verir. Eksiksiz SSE stratejisi söz konusu olduğunda , ZTNA , çok katmanlı denetim ve uygulama ile çok katmanlı , uzaktan erişimli güvenlik yöntemi sunar.

Güvenli Web Ağ Geçidi (SWG) ; Kurumsal kabul edilebilir kullanım ilkelerini belirlemeye ve uygulamaya ek olarak kullanıcıları web tabanlı tehditlerden korur. Kullanıcılar doğrudan web sitesine bağlanmak yerine , onları gerekli web sitesine bağlayan , URL filtreleme , çevrimiçi görünürlük , kötü amaçlı içerik denetimi , web erişim kontrolleri , diğer güvenlik önlemleri gibi hizmetler sağlayan SWG'ye bağlanır. Kullanıcılar şirket VPN'inden çıkarıldığında , SWG'ler , kullanıcılara güvenli internet erişimi sağladıklarından , kapsamlı SSE stratejisinin çok önemli bir yönüdür. ASWG'ler kuruluşların şunları yapmasına izin verir ; Uygun olmayanlara erişimi engellemek için kabul edilebilir kullanım politikaları kullanabilirsiniz. Güvenlik politikalarını daha sıkı hale getirebilirsiniz. Daha güvenli erişim sağlayabiliriniz. Yasa dışı veri aktarımının önlenmesine yardımcı olur.

Bulut Erişimi Güvenlik Aracısı (CASB) ; Kuruluşların verilerini çok sayıda SaaS uygulamasında ve bulut ortamları , şirket içi veri merkezleri veyahut mobil çalışanlar arasında geçiş halindeyken bulmalarına yardımcı olur. CASB , kuruluşun güvenlik , yönetişim ve uyumluluk düzenlemelerini uygulayarak yetkili kullanıcıların bulut hizmetlerine erişmesine ve bunları kullanmasına izin verirken , kuruluşların verilerini çeşitli konumlarda etkili ve güvenilir şekilde korumalarına olanak tanır. Geleneksel CASB'ler ve entegre CASB'ler , mevcut iki tür CASB'dir. İşletmelerin SaaS genişlemesine ayak uydurmalarına yardımcı olmak için verimli SSE yaklaşımı , entegre CASB'yi kullanmaktadır. Entegre CASB , hem mevcut hem de yeni SaaS uygulamalarında tüm SaaS risklerini tespit ederek kontrol etmek için hat içi güvenlik mekanizması kullanır. SaaS uygulamalarını hassas veriler , kötü amaçlı yazılımlar ve politika ihlalleri için gerçek zamanlı olarak kontrol edebilen , üçüncü taraf araçları kullanmadan uyumluluğu sağlayan ve saldırıları önleyen API tabanlı güvenlik mekanizması sunar.

Hizmet Olarak Güvenlik Duvarı (FwaaS) ; Bulut tabanlı verileri ve uygulamaları korumak için FwaaS , güvenlik duvarlarının bir şirketin bulut mimarisinin parçası olarak sağlanmasına olanak tanır. FWaaS yetenekleri , kuruluşların yerinde veri merkezleri , şubeler , mobil kullanıcılar ve bulut altyapısı gibi farklı kaynaklardan gelen trafiği toplamasını sağlamak için SSE stratejisinde kullanılır. Fiziksel cihazlara ihtiyaç duymadan tam ağ görünürlüğü ve yönetimi sağlarken , politikaların tüm konumlar ve kullanıcılar arasında tutarlı , güvenli şekilde uygulanmasını sağlar. SSE'nin , birleşik bulut merkezli platform aracılığıyla sağlanan geleneksel kurulum SSE'ye göre avantajları , işletmelerin geleneksel ağ güvenliği sorunlarından kurtulmasına olanak tanır. SSE birkaç önemli avantaj sunar ;

Daha etkili risk azaltma ; SSE , bir ağa bağlanmadan siber güvenliğin sağlanmasına izin verir. Güvenlik , nerede olurlarsa olsunlar kullanıcıdan uygulamaya bağlantıyı izleyebilen bulut platformu aracılığıyla sağlanır. Tüm güvenlik hizmetlerini birleşik şekilde sunarak , nokta ürünler arasındaki boşluklar ortadan kaldırıldığı için risk azaltılır. SSE , nerede olduklarına bakılmaksızın tüm kanallardaki kullanıcıların ve verilerin görünürlüğünü artırır. SSE , insan BT yönetimiyle ilişkili olağan gecikme süresi olmadan bulut genelinde güvenlik güncellemelerini zorunlu kılar.

Sıfır güven ile erişim ; Kullanıcı , cihaz , uygulama ve içerik olmak üzere dört faktöre dayanan sağlam sıfır güven ilkesiyle , SSE platformları (SASE ile birlikte) , kullanıcılardan buluta veya özel uygulamalara en az ayrıcalıklı erişim sunmalıdır. Erişime , kullanıcının doğal güvenilirliğine değil , kimlik ve politikaya dayalı olarak izin verilmelidir. Kullanıcılar hiçbir zaman ağa yerleştirilmez. Bu sebeple iş düzenlemelerini kullanarak kullanıcıları ve uygulamaları internet üzerinden güvenli şekilde bağlamak daha güvenli uzaktan deneyim sunar. Bu arada tehditler yanlamasına hareket edemez ve uygulamalar SSE platformunun arkasında güvendedir. Uygulamalar internete açık değildir. Bu nedenle tespit edilemezler. Bu da saldırı yüzeyini azaltarak güvenliği artırır ve iş riskini azaltır.

Kullanıcı memnuniyeti ; Gartner'a göre SSE , dünya çapındaki veri merkezi ağı boyunca tam olarak dağıtılmalıdır. SSE platformlarını IaaS altyapılarında barındıran şirketlerin aksine , en iyi SSE mimarileri , her veri merkezinde inceleme için amaca yöneliktir.

TLS / SSL şifre çözme ve incelemeyi içeren içerik incelemesi , son kullanıcının SSE bulutuna bağlandığı yerde gerçekleşir. Böylece dağıtılmış tasarım performansı artırarak gecikmeyi en aza indirir. SSE platformu genelinde eşleme ile birlikte , mobil kullanıcılarınız için en iyi deneyimi sağlar. Yavaş VPN'leri kullanmak zorunda değiller ve genel ile özel bulutlardaki uygulamalara erişim hızlı ve sorunsuzdur.

Konsolidasyonun faydaları ; Tüm önemli güvenlik hizmetlerinizi birleştirerek paradan ve zamandan tasarruf edebilirsiniz. SSE , SWG , CASB , ZTNA , bulut güvenlik duvarı (FwaaS) , bulut korumalı alanı , bulut DLP , CSPM ve CBI dahil olmak üzere tek bir platformda çeşitli güvenlik hizmetleri sağlayabilir. Tüm bu hizmetlere hemen ihtiyacınız yoksa , şirketiniz büyüdükçe bunlardan herhangi birini kolayca ekleyebilirsiniz. Tüm koruma tek bir politika altında toplanarak , kullanıcılarınızın ve verilerinizin tüm kanallarda tutarlı bir şekilde korunmasını sağlar.

SSE için seçim kriterleri ; Size hızlı , ölçeklenebilir güvenlik ve sorunsuz sıfır güven kullanıcı deneyimi sağlayan SSE platformu arayınız. Şunları yapabilen platforma ihtiyacınız olacak ;

Hızlı kullanıcı ve bulut uygulaması deneyimi için özel olarak tasarlanmış olması ; Hızlı ve güvenli erişim için geniş veri merkezi ayak izine küresel olarak dağılmış bulutta yerel mimari gerekir. Denetim odaklı SSE platformları , gerçek zamanlı içerik denetiminin taleplerini karşılamak üzere tasarlanmayan IaaS bulutlarında barındırılan SSE platformlarına göre avantaja sahiptir. Her bir veri merkezi bir inceleme düğümü olarak hizmet verdiğinde , nerede olurlarsa olsunlar güvenlik her zaman hızlı ve kullanıcıya yakındır. Bulut uygulaması deneyiminin optimal olmasını sağlamak için hızlı ve güçlü eşleme sunan SSE satıcılarını arayınız.

Sıfır güven mimarisi sıfırdan inşa edilmesi ; Erişim kontrolü kimliğe dayalı olmalı ve ağınıza asla insan eklememelisiniz. Tüm kişiler , cihazlar , IoT , bulut uygulamaları ve iş yükleri genelinde sıfır güven erişimini destekleyen sağlayıcıları arayınız. Geniş küresel veri merkezi ayak izine sahip satıcı , kullanıcılarınızın VPN gerekliliği olmadan her zaman hızlı bağlantıya sahip olmasını sağlayacaktır. Ölçeklenebilirlik , uzak kullanıcı üretkenliği için kritik öneme sahiptir. Satıcınızın SSE'ye yönelik ZTNA çözümü , büyük küresel dağıtımlarda bir geçmişe sahip olmalıdır.

Ölçeklenebilir hat içi proksi inceleme özelliği ; Cihazdan ve bulut uygulamasından gelen her iki bağlantı da proksi incelemesi ile sonlandırılır. İkisi arasında oturmak , tam SSL denetimine izin vererek bağlantıların geçmesini önlemektedir. Geleneksel geçiş güvenlik duvarları , bu düzeyde koruma ve denetleme ile rekabet edemez. İçerik sunabilen ve global TLS / SSL Denetimi yapabilen SSE sistemlerine odaklanınız. Sıralı inceleme tipik olarak kritik görev trafiğinde gerçekleştirilir. Ölçeklenebilirlik endişelerinin önemli bir etkisi olabilir. Seçtiğiniz SSE satıcısının sağlam hizmet düzeyi anlaşmalarına (SLA) ve büyük çok uluslu şirketler için hat içi trafiği değerlendirme geçmişine sahip olduğundan emin olunuz.

Daha fazla yenilik yoluyla SSE büyümesini artırma ; Ek güvenlik özellikleri ve hizmetleri , daha fazla işletme tek bir platform olarak benimsediği için SSE platformunun geleceğe dönük olmasını sağlayacaktır. BT'nin kullanıcı-bulut-uygulama ilişkisindeki bağlantı sorunlarını anında keşfetmesine yardımcı olan dijital deneyim izleme , SSE'ye taşınan bir işlevdir. SASE mimarisi tarafından açıklandığı gibi ağ hizmeti konsolidasyonu , SSE platformu olarak kritik öneme sahiptir. SD WAN bağlantısını , yerel şube ofis bağlantısını ve çoklu bulut bağlantısını içermektedir. SSE inovasyonunu da destekleyen SASE hizmet sağlayıcılarına odaklanarak kuruluşunuzun bulut ekosistemi geliştikçe , karmaşıklık eklemeden geliştirme için yer sağlayabilirsiniz.

AI ve ML'nin benimsenmesi ; İşletmeler için saldırı yüzeyi çok büyüktür ve daha da büyüyecektir. Riski etkin şekilde ölçmek için şirketinizin büyüklüğüne bağlı olarak zamanla değişen yüz milyarlarca sinyal incelenmelidir. Siber güvenlik duruşunu analiz etmek ve iyileştirmek artık insan ölçeğinde görev değildir. Bu benzeri görülmemiş zorluğun sonucu olarak , yapay zeka (AI) tabanlı siber güvenlik araçları , bilgi güvenliği ekiplerine ihlal riskini azaltmada ve güvenlik duruşlarını daha verimli , etkili şekilde iyileştirmede yardımcı olmak için gelişmiştir. Yapay zeka ve makine öğrenimi (ML) , milyonlarca olayı hızlı şekilde analiz edebildikleri ve sıfırıncı gün güvenlik açıklarından yararlanan kötü amaçlı yazılımlardan kimlik avı saldırısına veya kötü amaçlı yazılımlara yol açabilecek riskli davranışları tespit etmeye kadar çok çeşitli tehditleri tanımlayabildikleri için bilgi güvenliğinde kritik teknolojiler haline gelmiştir. Algoritmalar , mevcut yeni saldırı türlerini tespit etmek için önceki saldırılardan öğrenerek zamanla daha iyi hale gelir. Kullanıcı , varlık ve ağ profilleri , davranış geçmişleri kullanılarak oluşturulur ve AI'nın yerleşik normlardan sapmaları algılamasına , bunlara yanıt vermesine olanak tanır. Yapay zeka siber güvenliği , makine öğreniminin yardımıyla çok da uzak olmayan gelecekte güçlü araç olmaya hazırlanıyor. Diğer sektörlerde olduğu gibi güvenlik sektöründe de insan etkileşimi uzun süredir gerekli ve vazgeçilmez olmuştur. Siber güvenlikte insan katılımı hala çok önemli olsa da , teknoloji bazı görevlerde yavaş yavaş bizden daha iyi hale gelmektedir. Teknolojideki her ilerlemeyle , insan işlerini verimli şekilde tamamlamaya biraz daha yaklaşıyoruz. Bu gelişmelerin merkezinde çeşitli araştırma konuları yer almaktadır ; AI , bilgisayarlara insan zihniyle aynı düzeyde yanıt vermeyi amaçlar. Makine öğrenimi ve derin öğrenme gibi diğer birçok disiplin , bazıları bu çatı terimi altındadır. ML , mevcut davranış kalıplarını analiz ederek geçmiş verilere ve sonuçlara dayalı kararlar verir. Bazı ayarlamalar için hala insanlara ihtiyaç bulunmaktadır. Bugüne kadar , makine öğrenimi en alakalı AI siber güvenlik disiplinidir. Derin öğrenme (DL) , önceki kalıplara dayalı kararlar alması fakat iyileştirmeler yapması bakımından makine öğrenimine benzer. Bu aynı zamanda ML'nin gelişmiş versiyonu olarak da bilinir.

AI ve ML'nin siber güvenlik alanındaki etkisi ; Yapay zeka ve siber güvenlik , hayal edebileceğimizden çok daha yakın zamanda oyunun kurallarını değiştiren teknolojiler olarak bizleri karşıladı. Gelecekte yavaş gelişmelerle uğraşmak zorunda kalabiliriz. Makine öğrenimi ve yapay zekanın olası güvenlik sonuçlarını araştırırken , mevcut siber güvenlik sorunlu noktalarını bağlamsallaştırmak çok önemlidir. Uzun süredir hafife aldığımız birçok süreç ve unsur , AI teknolojileri kullanılarak ele alınabilir ;

İnsan kaynaklı yapılandırma hatası ; Siber güvenlik kusurlarının büyük bir bölümünü insan hatası oluşturur. Kurulumda yer alan devasa BT ekipleriyle bile , doğru sistem yapılandırmasının yönetilmesi son derece zor olabilir. Bilgisayar güvenliği , sürekli yenilik nedeniyle her zamankinden daha katmanlı hale gelmiştir. Duyarlı araçlar , ağ sistemleri değiştirilirken , yükseltilirken ve güncellenirken ortaya çıkan sorunları belirlemede ve çözmede ekiplere yardımcı olabilir. Bulut bilişim ve diğer çağdaş internet altyapısının daha eski yerel çerçevelerin üzerine nasıl katmanlanabileceğini düşününüz. BT personelinin , onları güvende tutmak için kurumsal sistemlerde birlikte çalışabilirliği sürdürmesi gerekecektir. Ekipler , sonsuz güncellemeleri rutin günlük destek çalışmalarıyla birleştirdikçe , yapılandırma güvenliğini değerlendirmeye yönelik manuel teknikler , bunların tükenmesine neden olur. Ekipler , akıllı , uyarlanabilir otomasyon kullanarak yeni keşfedilen zorluklar hakkında anında rehberlik alabilir. Nasıl devam edecekleri konusunda tavsiye alabilirler veya ayarları uygun şekilde otomatik olarak değiştiren mekanizmalara sahip olabilirler.

Tekrarlanan faaliyetler insan verimliliğini artırır ; Siber güvenlik sektöründeki bir diğer konu da insan verimliliğidir. Dinamik bir ortamda , hiçbir manuel yöntem her seferinde mükemmel şekilde yeniden üretilemez. En çok zaman alan süreçlerden biri de bir kuruluşun birçok uç nokta makinesinin her birini ayrı ayrı kurmaktır. BT ekipleri , ilk kurulumdan sonra , uzaktan yükseltmelerle düzeltilemeyen yanlış yapılandırmaları veya eski ayarları düzeltmek için sık sık aynı iş istasyonlarına döner. Personel buna yanıt vermekle görevlendirildiğinde , tehlikenin kapsamı hızla değişebilir. Yapay zeka ve makine öğrenimine dayalı sistem , insan odağının öngörülemeyen engellerle yavaşladığı yerlerde minimum gecikmeyle hareket edebilir.

Tehdit uyarısının tükenmesi ; Düzgün şekilde ele alınmazsa , tehdit uyarı yorgunluğu , kuruluşlar için başka bir zayıflık haline gelebilir. Yukarıda bahsedilen güvenlik katmanları daha karmaşık ve kapsamlı hale geldikçe saldırı yüzeyleri büyümektedir. Pek çok güvenlik sistemi , bilinen çeşitli sorunlara yanıt olarak sadece refleksif alarmlardan oluşan bombardıman yaymak üzere programlanmıştır.

Ekipleri olası kararları sıralamak ve bu bireysel ipuçlarının bir sonucu olarak harekete geçmek için bırakılır. Muazzam miktarda uyarı , bu derece karar vermeyi stresli hale getirir. Karar yorgunluğu , nihayetinde siber güvenlik çalışanları için sık görülen bir durum haline gelmektedir. Bu riskleri ve güvenlik açıklarını ele almak için proaktif adımlar atmak tercih edilirken , birçok ekip bunu yapmak için zaman ve kaynaktan yoksundur.

Bazen takımlar , en acil sorunları ilk önce ele almayı seçerek ikinci hedeflerin bir kenara atılmasına izin vermelidir. AI , BT ekiplerinin bu tehlikelerin çoğunu etkili ve pratik şekilde yönetmesine yardımcı olabilir. Otomatik etiketleme , bu tehditlerin her biriyle başa çıkmayı çok daha kolay hale getirebilir. Makine öğrenimi yönteminin kendisi de bazı endişelerinizi giderebilir.

Tehdide yanıt verme süresi ; Siber güvenlik ekibinin etkinliğini belirlemek için en önemli göstergelerden biridir. Kötü amaçlı saldırılar , kullanımdan dağıtıma hızla geçme konusunda bir üne sahiptir. Geçmişteki tehdit aktörleri , saldırı başlatmadan önce haftalarca ağ izinlerinde gezinmek ve birden fazla ağda güvenliği devre dışı bırakmak zorunda idi. Bilinen saldırı türlerinde bile insan tepkisi yavaş olabilir. Birçok ekip başarılı saldırılara yanıt vermek için saldırı girişimlerini önlemekten daha fazla zaman harcamıştır. Keşfedilmemiş saldırılar ise kendi risklerini oluşturur. Makine öğrenimi destekli güvenlik sayesinde bir saldırıdan elde edilen veriler hızla sıralanabilir ve analize hazır hale getirilebilir. İşleme ve karar vermeyi kolaylaştırmak için siber güvenlik ekiplerine daha basit raporlar sunabilir. Bu tür bir koruma , raporlamaya ek olarak daha fazla hasarı sınırlamak ve gelecekteki saldırıları önlemek için öneriler sağlayabilir.

Yeni tehditleri belirleme ve tahmin etme ; Siber saldırı tepki sürelerini etkileyen diğer husus da yeni tehditlerin belirlenmesi ve tahmin edilmesidir. Mevcut tehditler , gecikme süresine sahiptir. Bilinmeyen saldırı türleri , taktikleri ve araçları , bir ekibin tepki vermesinin çok uzun sürmesine neden olabilir. Veri hırsızlığı gibi daha kötü , daha sinsi tehlikeler uzun süre fark edilmeyebilir. Ağ savunma çabaları , her zaman sıfırıncı gün açıklarından yararlanmayla sonuçlanan sürekli saldırı gelişimiyle ilgilenir. Çoğu siber saldırı sıfırdan oluşturulmaz. Makine öğrenimi , sıklıkla önceki saldırıların davranışları , çerçeveleri ve kaynak kodları üzerine kurulduğundan , çalışmak için önceden var olan bir yola sahiptir. Bir saldırının tanınmasına yardımcı olmak için ML tabanlı programlama , mevcut tehlike ile önceden keşfedilen tehditler arasındaki ortak noktaların vurgulanmasına yardımcı olabilir. Uyarlanabilir güvenlik mekanizmalarının önemini vurgulayarak , insanların hemen yapamayacakları bir şeydir. Makine öğrenimi , ekiplerin yeni riskleri tahmin etmesini kolaylaştırabilir ve daha fazla tehdit farkındalığı nedeniyle gecikme süresini azaltabilir.

Personel kapasitesi ; Dünya çapında BT ve siber güvenlik kuruluşlarını etkileyen zorluklardan biridir. Bir kuruluş için mevcut nitelikli uzmanların sayısı , taleplerine bağlı olarak sınırlı olabilir. İnsan yardımı almanın bir kuruluşun parasının önemli bir bölümünü tüketebilmesi önemli bir noktadır. İşçileri desteklemek , onları sadece günlük emekleri için ödüllendirmeyi değil , aynı zamanda devam eden eğitim ve sertifikasyon ihtiyaçları konusunda onlara yardımcı olmayı da gerektirir. Siber güvenlik pratisyeni olarak güncel kalmak zordur. Personel ve onları desteklemek için daha küçük bir ekiple , yapay zeka tabanlı güvenlik sistemleri liderliği alabilir. Bu iş gücünün en yeni yapay zeka ve makine öğrenimi konularında güncel kalması gerekecek olsa da , daha az personel ihtiyacı maliyet ve zaman tasarrufu sağlayacaktır.

Uyarlanabilirlik ; Ana hatlarıyla belirtilen diğer noktalar kadar belirgin endişe kaynağı değildir fakat bir kuruluşun güvenlik yeteneklerini önemli ölçüde değiştirebilir. Ekipler , beceri setlerini özel ihtiyaçlarınıza göre uyarlayamayabilir. Çalışanlarınız belirli yöntemler , araçlar ve süreçler konusunda eğitimli değilse , sonuç olarak ekibinizin etkinliği zarar görebilir. İnsan temelli ekiplerde , yeni güvenlik politikalarının uygulanması gibi görünüşte temel görevler bile uzun zaman alabilir. İnsanlar bir şeyleri hemen yapmanın yeni yöntemlerini biranda öğrenemez ve bunu yapmak için zaman tanımalıyız. Uygun şekilde eğitilmiş algoritmalar , uygun veri kümeleri kullanılarak özel olarak size özel bir çözüme dönüştürülebilir.

Makine öğrenimi için vakaları kullanma ; Siber güvenlikte makine öğreniminin önemini göstermek için şu örnekleri göz önünde bulundurunuz ;

Veri gizliliği sınıflandırmalarına uygunluk ; Son birkaç yılda şirketinizi gizlilik yasası ihlallerinden korumak kesinlikle büyük sorumluluk haline gelmiştir. Kaliforniya Tüketici Koruma Yasası (CCPA) gibi diğer yasal öneriler , Genel Veri Koruma Yönetmeliği'ne (GDPR) yanıt olarak ortaya çıkmıştır. Bu eylemler , müşterilerinizden ve kullanıcılarınızdan edindiğiniz verileri yönetmenizi gerektirir ve genelde bu verilerin istek üzerine silinmek üzere erişilebilir olması gerektiği anlamına gelir. Bu yasalara uyulmaması , şirketinizin itibarına zarar vermenin yanı sıra önemli para cezalarına da neden olabilir. Tanımlayıcı kullanıcı verilerini anonimleştirilmiş veya tanımlanamayan verilerden ayırmaya veri sınıflandırması yardımcı olabilir. Özellikle büyük veya eski şirketlerde yararlı olan büyük miktarda eski ve yeni veriyi ayırmaya çalışırken zamandan ve emekten tasarruf etmenizi sağlar.

Kullanıcı davranışı için güvenlik profilleri ; Güvenlik , kullanıcı davranışına bağlı olarak ağ personeli üzerinde bireysel profiller oluşturarak kuruluşunuzu karşılayacak şekilde özel olarak yapılabilir. Bu model , kullanıcı davranışının uç noktalarına dayanarak , yetkisiz kullanıcının nasıl görünebileceğini tahmin edebilir. Klavye vuruşları tehdit modeli oluşturmak için kullanılabilir. ML güvenliği , potansiyel olarak yetkisiz kullanıcı davranışının olası sonuçlarının ana hatlarına dayalı olarak açıkta kalan saldırı yüzeylerini azaltmak için önerilen çözümler sağlayabilir.

Sistem performansı için güvenlik profilleri ; Bilgisayarınız sağlıklı olduğunda , tıpkı kullanıcı davranışı profili konsepti gibi tüm performansının özel tanılama profili oluşturulabilir. İşlemci ve bellek kullanımı , aşırı internet veri kullanımı gibi özelliklerin izlenmesi , dolandırıcılık faaliyetini ortaya çıkarabilir. Ancak bazı kullanıcılar , video konferans sırasında veya büyük medya dosyalarını indirirken olduğu gibi , günlük olarak çok büyük miktarda veri kullanabilir. Tıpkı kullanıcı davranışı yönergeleri gibi genel olarak nasıl göründüğünü öğrenerek bir sistemin temel performansının nasıl görünmemesi gerektiğini belirleyebilir.

Bot yasağı kullanıcının davranışına bağlıdır ; Bot etkinliği , bir web sitesinin gelen bant genişliğini tüketebilir. Özellikle özel e-ticaret mağazaları olan ve fiziksel tesisleri olmayanlar gibi sadece çevrimiçi trafiğe güvenen işletmeler için geçerlidir. Gerçek kullanıcılar , trafik ve gelir kaybıyla sonuçlanan yavaş deneyim yaşayabilir. ML güvenlik teknolojileri , sanal özel ağlar gibi onları anonimleştirmek için kullanılan araçlardan bağımsız olarak , etkinliklerini tanımlayarak botların ağını kısıtlayabilir. Düşman taraflar üzerindeki davranışsal veri noktaları , makine öğrenimi güvenlik aracının bu davranış etrafında tahmin modelleri oluşturmasına ve gelecekte aynı davranışı göstermesi için yeni web adreslerini engellemesine yardımcı olabilir.

Dijital Adli Tıp ve Olay Müdahalesi (DFIR) ; Yenilikçi düşünce ve yeni bakış açısı gerektiren sürekli gelişen bir alandır. Modern siber güvenlik sorunlarının artan karmaşıklığını yönetmek için dijital araştırma hizmetlerini olay müdahale deneyimiyle birleştirmek çok önemlidir. Siber saldırılar , davalar veya diğer dijital soruşturmalarla ilgili tanımlama , araştırma , içerme , düzeltme , tanıklık etme , dijital adli tıp ve olay müdahalesi gerektiren siber güvenlik dallarıdır.

DFIR hizmetlerinin iki temel bileşeni ; Dijital adli tıp , kullanıcı davranışı ve sistem verilerini içeren dijital kanıtları toplayan , analiz eden ve sunan adli bilim alanıdır. Dijital adli tıp , bilgisayar sisteminde , ağ cihazlarında , telefonlarda veya tabletlerde neler olup bittiğiyle ilgili gerçekleri ortaya çıkarmak için davalarda , düzenleyici soruşturmalarda , şirket içi soruşturmalarda , suç faaliyetlerinde ve diğer tür dijital soruşturmalarda yaygın olarak kullanılır. Olay Müdahalesi , dijital adli tıpa benzer ve verileri toplayıp analiz ederek bilgisayar sistemlerini araştırır. Güvenlik sorununa yanıt verme bağlamında açıkça yapılır. Bu nedenle soruşturma kritik olsa da , sınırlama ve kurtarma gibi diğer eylemler birbirine karşı dikkatlice değerlendirilir.

DFIR'nin siber güvenlikteki önemi ; Kurtarma , siber güvenlik saldırısından etkilenen firmalar için büyük öncelik olup saldırının nasıl ve neden yapıldığını anlamak da kritik öneme sahiptir. DFIR , uzun ve karmaşık adli süreç yoluyla bu daha derin anlayışı sağlar. DFIR uzmanları , onlara kimin saldırdığını , nasıl içeri girdiğini , saldırganların sistemlerini ihlal etmek için yaptıkları eylemleri ve güvenlik açıklarını kapatmak için neler yapabileceklerini bulmak için büyük miktarda veri toplayarak inceler. Bu bilgiler sıklıkla , kimliği tespit edilen faillere karşı yasal davanın geliştirilmesine yardımcı olmak için kullanılır. Veriler , araştırmacıların dijital kanıtları keşfetmelerine ve korumalarına yardımcı olan dijital adli prosedür yoluyla toplanır.

DFIR ile ilgili en iyi uygulamalar ; Tehditlere karşı savunmasız olan işletmeler, hızlı bir şekilde yanıt vermelerini sağladığı için sağlam bir DFIR hizmetinden yararlanabilir. Kapsamlı bir siber olay anlayışına sahip yetenekli ekiplerin saldırılara hızlı ve verimli bir şekilde yanıt vereceğini garanti eder.

Dijital adli tıp için en iyi uygulamalar ; Hızlı ve kapsamlı reaksiyon , DFIR'nin etkinliği için kritik öneme sahiptir. Dijital adli tıp ekipleri , bir soruna hızlı ve etkili şekilde yanıt verebilmek için bol miktarda bilgiye ve gerekli DFIR araçlarına ve uygulamalarına sahip olmalıdır. Dijital adli tıp uzmanlığının , bir olayın nedenini belirleme ve kapsamı ile etkisini kesin olarak belirleme becerisi de dahil olmak üzere çeşitli avantajları vardır. Doğru araştırma araçlarının kullanılması , bir saldırıya veya istenmeyen ifşaya neden olan güvenlik açıklarının hızla keşfedilmesini sağlayacaktır

Olay müdahalesinde en iyi uygulamalar ; Olay müdahale hizmetleri , acil duruma gerçek zamanlı olarak yanıt vermek üzere tasarlanmıştır. İtibar zararını , mali kaybı ve iş kesintisini önlemek için en iyi IR uygulamaları , hazırlık ve planlama ile hızlı , doğru ve güvenilir azaltma ve müdahaleyi içermektedir. Birlikte kullanıldığında , dijital adli tıp ve olay müdahalesi en iyi uygulamaları , sorunların temel nedenini bulmayı , erişilebilir tüm kanıtları / verileri uygun şekilde tanımlamayı ve almayı ve şirketinizin güvenlik duruşunun gelecek için güçlendirilmesini sağlamak için sürekli destek sağlamayı içermektedir.

Açık kaynaklı teknoloji yığını seçerken dikkate alınması gereken önemli noktalar ; Açık kaynaklı yazılım , dünya çapında ilgi görmektedir. Yazılım geliştirme sürecinin her aşamasında kullanılmaktadır. Dünya çapındaki işletmelerde yaygın şekilde benimsenerek buluta geçerken giderek daha görünür hale gelmektedir. Bir sorunu çözmemiz gerektiğinde ihtiyaçlarımızı karşılıyor gibi görünen en yakın yazılım kitaplığına veya programa ulaşmak çok basittir. Fakat her birimizin karşılaştığı önemli bir sorun , erişilebilir sayısız seçenek arasından hangi açık kaynaklı yazılımın kullanılacağına karar vermektir. Açık kaynaklı araç seçmek söz konusu olduğunda , çoğumuz metodik yaklaşım benimsemeyiz ve bu da yazılım geliştirme yaşam döngüsünün sonraki aşamalarında sorunlara yol açmaktadır. Ürünümüze sorunlu açık kaynaklı bileşen eklemek , gelecekte bir takım sorunlara yol açabileceğinden ve belki de maliyeti artırabileceğinden , hangi açık kaynaklı yazılımın kullanılacağına karar verirken kullanmak için bazı ortak kriterlere ihtiyacımız vardır.

Gereksinimin karşılanması ; Açık kaynaklı yazılım seçerken göz önünde bulundurulması gereken en önemli faktörlerden biri de yazılım ürünleri geliştirme standartlarımızı karşılayıp karşılamadığıdır. Aynı şeyi yapan birçok açık kaynaklı yazılım bulunmaktadır. Birini diğerlerinden ayıran nokta sunduğu ek yeteneklerdir. Çoğumuz , yalnızca sunduğu ek özelliklerin / eklentilerin sayısına bağlı olarak açık kaynaklı proje seçme hatasına düşüyoruz ve bu tür özellikler genelde gereksinimlerimizi bile karşılamıyor. Tüm gereksinimlerimizi karşılayan daha az popülerlik ve daha az temel özellik / eklenti içeren açık kaynaklı çözüm , popüler olan ve yüzlerce özelliğe sahip olan ancak ihtiyaçlarımızı karşılamayan bir çözümden her zaman daha iyi bir seçim olacaktır.

Yetenek Seti ; Tüm ihtiyaçlarımızı karşılayan ve birçok işlevsellik katan açık kaynaklı yazılımlar olabilir. Onu kullanmak için gerekli becerilere sahip değilizdir. Yazılım seçimi , ek eğitim gerektirebilir ve bu da açık kaynaklı yazılım kullanma amacını ortadan kaldırır. Her zaman mevcut beceri seti tarafından kullanılabilen ve sürdürülebilen açık kaynaklı yazılımları seçmeliyiz. Yeni beceri seti öğrenmek tüm gereksinimleri karşılıyorsa ve gelecekte proje maliyetlerini düşürme açısından gerçekten değerliyse , biri devam edebilir ve bunu yapabilir.

Toplum ; Açık kaynaklı proje için en değerli kaynaklardan biri de kullanıcı topluluğudur. Canlı bir topluluk , projeyi ilerletmek için her zaman faydalıdır. Ürünü kullanan ve bildirilen sorunlar ile özellik istekleri hakkında kullanıcı sorularını yanıtlamak gibi bir şekilde etkileşimde bulunan kişile r, kullanıcı topluluğunu oluşturur. İyi açık kaynaklı yazılım projesinde her zaman kod gönderen , hataları bulan ve diğer kullanıcılara yardım eden geliştiriciler veya aktif kullanıcılardan oluşan topluluk bulunur. Test ve kalite girdisinin çoğu topluluk tarafından yapılır. Topluluk , açık kaynaklı yazılımın kalitesini ve güvenilirliğini test etmek için kullanılabilir. Kriz durumunda , topluluk ne kadar büyük olursa , destek o kadar iyi olur. Güçlü bir topluluğa sahip yazılımları seçmek , gelecekte hataları çözerken takılırsanız her zaman işe yarayacaktır.

Destek ; OSS seçmeden önce her zaman sunulan yardımı göz önünde bulundurunuz. Mükemmel müşteri hizmetiyle birlikte gelen yazılımlar her zaman tercih edilir. Seçtiğiniz açık kaynaklı yazılımın arkasında güçlü topluluk olduğundan daima emin olunuz. Kullanıcıların kurulum veya diğer sorunlarla ilgili sorularına yanıt alabilecekleri aktif herkese açık grupları veya forumları arayınız. Güçlü topluluk , gelecekte ortaya çıkabilecek sorunları çözmenize her zaman yardımcı olacaktır. Zaman zaman ücretli destek de verilmektedir. Üçüncü taraf ücretli desteğin mevcudiyeti , yüksek kaliteli yazılımın göstergelerinden biridir. Topluluğun yardımıyla çözemeyeceğiniz kritik bir şeye takılırsanız bu kullanışlı olacaktır. Hem ücretli hem de topluluk desteği sunan OSS seçmek her zaman iyi bir fikirdir.

Belgeler ; Popüler ve yüksek kaliteli açık kaynaklı çözümler her zaman yeterli belgelere sahiptir. Topluluğun kalitesinin ve desteğinin iyi bir işaretidir. İki farklı kategoriye ayrılabilir. Kullanıcı belgeleri bir örnektir. Genel olarak sistemin nasıl kullanılacağını açıklar. Kullanıcı belgelerinde , farklı kullanıcı düzeyleri ve haklarıyla ilişkili birkaç katman vardır. Yönetici rolü uygulamalarının ayrı belgeleri olabilir. İhtiyaçlarımız sağlanan belgelerle karşılanmalıdır. Geliştirici belgeleri ise kodun nasıl ekleneceğini ve değiştirileceğini açıklar. Gelecekte kodumuzu güncellemeyi planlıyorsak , bu belgeler gerçekten yardımcı olacaktır.

Güvenlik ; Güvenlik artık tüm aşamalarda yazılım geliştirme yaşam döngüsünün kritik bir bileşenidir. OSS'nin çoğunluğunun kaynak kodu halka açıktır. Bu nedenle kusurları ortaya çıkarmak her zaman kolaydır. Geliştirici , kodu inceleyerek ve bunları düzeltmek için çalışarak koddaki kusurları ortaya çıkarabilir. Bir geliştiricinin keşfedilen güvenlik açıklarına nasıl yanıt vereceği tamamen onlara bağlıdır. Yazılım güvenlik açıklarını ararken şu web sitelerinden yararlanabilirsiniz. (1 – 2) Bir yazılımın web sitesini ziyaret ederek ve sürüm notlarını okuyarak güvenlik açısından ne kadar tehlikeli olduğunu belirleyebiliriz.

Lisanslama ; Açık Kaynak Yazılımın (OSS) her parçası , uymamız gereken bir lisansla birlikte gelir. Copyleft en bilinenlerden biridir. GNU GPL gibi Copyleft lisansları , kullanıcıları kaynak kodunun tamamından ve ürünün tüm kodunu değiştirme ile dağıtma haklarından vazgeçmeye zorlar. Lisans her zaman yazılımın kullanım amacına uygun olmalıdır. Programı bir şekilde değiştirmeyi ve yeniden dağıtmayı planlıyorsanız fakat kaynak kodunu dağıtmak istemiyorsanız , copyleft lisansı yerine copyleft olmayan lisans seçiniz. Kısacası yazılımı seçmeden önce daima lisansa bakınız.

Çözüm ; Şirketler önümüzdeki yıllarda siber güvenliği ciddiye almalı ve buna yeterli kaynak ayırmalıdır. Siber güvenlik ve ağ güvenliği tavsiyelerini ve en iyi uygulamaları takip etmek , başlamak için iyi bir yerdir. Her büyüklükteki şirket , ağ ve cihaz güvenliğini izleyerek güvenlik açıklarının hızla düzeltilmesini sağlamak için siber güvenlik ekiplerine , kurum içi uzmanlara veya en azından danışmanlara ihtiyaç duymaktadır. En iyi uygulamala r, proje yönetimi ve denetim işlevleri gibi görevleri başarılı ve hızlı şekilde yerine getirmek için kurumsal dünyada kullanılan bir dizi etik yönergedir. En iyi uygulamalar , endüstri kıyaslamaları olarak kullanılabilir ve işletmeler , isterlerse en iyi uygulamalarını diğer işletmelerle paylaşabilir veya tartışabilir. Son yıllarda yapay zeka , insan bilgi güvenliği ekiplerinin çalışmalarını tamamlamak için gerekli bir araç olarak ortaya çıkmıştır. İnsanlar artık dinamik kurumsal saldırı yüzeyini yeterince koruyamıyor. AI , siber güvenlik uzmanları tarafından ihlal riskini azaltmak ve güvenlik duruşunu iyileştirmek için kullanılabilecek çok ihtiyaç duyulan analiz ve tehdit tanımlaması sağlamaktadır. Güvenlik alanında , AI , riski tanımlayabilir ve öncelik sırasına koyarak ağdaki kötü amaçlı yazılımları gerçek zamanlı olarak tespit ederek olay müdahalesine öncülük edip ihlalleri oluşmadan önce tespit edebilir. AI , siber güvenlik ekiplerinin bilgimizi genişleten , yaşamlarımızı zenginleştiren ve siber güvenliği , parçalarının toplamından daha büyük görünen şekilde yönlendiren güçlü insan-makine ortaklıkları kurmasını sağlar.