Q Merhabalar. Tüm bu önerileriniz yapıldığında Websense in fatura ataklarına kesin çözüm olduğunu söyleyebilir misiniz? (Bilerek, isteyerek açılıp exe çalıştırılmadığını düşünerek) . İlaveten bu sunum ve çözüm önerileri için geç kalınmış bir bilgilendirme değil midir?

A Websense günümüz tehditlerine karşılık sürekli kendisini güncelleyen bir güvenlik anlayşına sahiptir, Eğer websense APX yani full olarak tüm modülleriyle ürünümüzü kullanıyorsanız bu ataklara karşı kurum çalışanlarınızı ve verilerinizi koruyabilirsiniz. Websense olarak düzenli olarak bu tarz etkinlikler yapmaya ve elimizden geldiğince sizlere bu tarz duyuruları yapmaya çalışıyoruz ancak webinar konusunda haklısınız bundan sonra daha aktif webinarlar düzenleyeceğiz.

Q ThreatScope ve Threat Analizer ürünleri cloud üzerinden çalışıyor, bunların on-site çalışacak şekilde gateway ürünlerine dahil edilmesi gibi bir çalışma var mıdır? Cloud çözümleri bazı regülasyonlardan dolayı bazı firmaların ihtiyaçlarına cevap veremiyebiliyor.

A Websense sadece Hibrid altyapısı aktif olduğunda ThreatScope modülü için Cloud altyapısını kullanabilir ancak Websense yılda 4 kez geliştirme yapar bu tarz bir çalışma olduğunu düşünüyoruz . Aslında cloud hizmeti veren 20 civarı datacenterimiz var , bunlardan bir tanesi Türkiye'de . Dolayısıyla Cloud anlamında regulasyon varsa elbette kurumun kararına saygı duymak zorundayız ancak Türkiye'de DC olması ve DC 'lerimizin ISO 27001 certified olması nedeniyle bu konuda endişenmenize gerek olmadığını belirtebilirim.

Q Usom a eklenen zararlı linklerin websense yapımızla senkronize olması için ne yapmamız gerekli?

A Herhangi bir şey yapmanıza gerek yok Websense Threat Seeker Intelligence Cloud tuzaklarımız bu bilgileri doğrudan alarak DB kategorilerinde double kontroller gerçekleştirmektedir.

Q Merhaba, Dashboard suspicious activity kısmında incidentler olması her zaman kontrol gerektirirmi ?

A Her zaman bu ekrana bakmanızı tavsiye ederim , bu ekran size Websense'in gerçek bir APT/ güvenlik altyapısına sahip olduğunu ispatlar. Ayrıca bu ekranda gördüğünüz aktiviteler içerisinde geçen kategoriler ilgili kişiler için kesinlikle izinli olmamalıdır.

Q HTTPS inspection kullanıyoruz. Lakin birçok devlet&kamu... vb. sitelerinde problem yaratıyor. Bunlar için *.gov, *.mil gibi uzantıları yazsak bile işe yaramıyor. Bu yüzden IP bazlı bypass kuralı yazıyoruz. HTTPS inspection'ı illaki kullanmalı mıyız? Eğer kullanmamız gerekiyorsa nasıl kullanmalıyız?

A HTTPS inspection günümüz tehditleri için olmazsa olmaz konulardan bir tanesi ve problem oluşturabileceği bir durum olmadığını belirtebilirim. Elbette bypass tanımları yapılabilir detaylı bilgi almak için iş ortağımız ya da bizimle irtibata geçebilirsiniz.

Q merhaba, websense log yapılandırması ve loglarının analizi konusunda da birkaç şey söyleyebilir misiniz fırsat bulursanız. teşekkür ederim.

A Websense çok detaylı bir raporlama altyapısına sahiptir bunun için SQL DB kullanır.

Q Sandboxing hizmetlerinden kastınız threatscope mudur?

A Evet isim olarak ThreatScope dediğimiz modül bu işi yapar , Sandbox sıfır gün ataklarına karşı güvenlik farkındalığının yukarı çekilmesine yardımcı olur.

Q Güvenilirlik açısından yeni çıkan bir atak metodu olduğunda websens databaselernin bunu farketme ve tepki verme süresinin resmi olarak bir değeri var mı?(orçun aktaş)

A Malesef statik davranmaktan yana değiliz , ACE güvenlik motorumuz dinamik olarak kodları , atakları ve sayfaları analiz etmesinden ötürü bunun bir süresi olmadığını belirtebilirim.

Q Hangi kategorileri kesinlikle kapatmalıyız. security tmm. extended protecition tamam başka hangilerini önerirsiniz ?

A Bunun için ayrıca bir duyuru yapacağız.

Q Cloud Email Security kullanıyoruz. Ayrıca yapmamız gereken bir ayar varmıdır?

A Cloud Email Security bu tarz tehditler için çok yeterli olmayabilir çünkü atak temizmiş gibi görünen bir email ile başlıyor .

Q Kemal hocam zararlı urller genelde websense de newly registired web sited kategorisine giriyor . bu kategoriyi kapatırsak ne kadar etkili olur?

A Kesinlikle kapatalım , hiç bir şey olmaz.

Q w10 k da 10G port yokmuş , yeni model de düşünülüyor mu?

A V10K Appliance üzerinde 10G portu şu an düşünülmüyor çünkü bu cihaz üzerinde TPS değerlerini baz alıyoruz ve ayrıca tüm cihazlar 10G olmadığı için buna gerek olmadığını belirtebiliriz.

Q Bize bu etkinlikleri mail olarak bildirirmisiniz

A Bundan sonra ayda 1 kez bu tarz bir etkinlik yapmaya ve sizleri davet etmeye çalışacağız.

Q Usom tarafından yayınlanan linklerden efatura.ttnet-fatura.com'u websensete URL category de sorguladığımda unknown category cevabını alıyorum

A Eğer sayfa şu anda kullanımda değilse ki saldırganlar bu tarz atakları yaptıktan sonra sayfaları kapatıyor o yüzden unknow olması normaldir,çünkü Websense ACE dinamik bir güvenlik motorudur sayfa ayakta değilse bunun için kategorizasyon yapmaya gerek duymaz.

Q Bir eğitim kurumuyuz. Tabletli eğitim yapıyoruz. Tablet cihazlarımız android işletim sistemine sahip. MDM yazılımı olarak airwatch yazılımını kullanmaktayız. Tabletlerde web filter kullanmak istiyoruz. Bunun için websense demo key beklemekteyiz. Benim sorum airwatch ile websense i entegre ettiğimiz zaman websense te yapacağımız filitreleme tabletteki uygulamalarında içeriklerini denetleyebiliyor mu? yani uygulama çalışşın fakat kriterlere uymayan içerikler filitrelensin. Bu mümkün mü?

A Evet bu mümkün Airwatch ile doğrudan entegre olarak çalışabiliyoruz . Böylece cihazların üzerindeki uygulama ve web güvenliği Websense tarafından sağlanacaktır.

Q Email kuralını benimle paylaşabilirmisiniz?

A Bunun için doğrudan bizimle irtibata geçebilirsiniz.

Q websense anywhere ile sizce bu sıkıntıyla başedebilirmiyim ?

A SSL inspection , Hibrid altyapısı ve Web DLP gibi tüm modüllerimiz sağlıklı şekilde konfigüre edilirse evet .

Q orneğin soyle bir kota yapabilirmiyiz. youtube a 50 mb lik bantgenisliği ayırmak istiyoruz nasıl ayırırız

A Websense bir Band genişliği yönetim çözümü olmasa da sayfalar üzerinde zaman ve alınan gönderilen paket sınırı gibi kotalar koyabilirsiniz.

Q file type downloadda sadece executables seçilirse zip içindeki exelerde droplanır mı ?

A Evet ancak 7.8.3 ve sonrası için bunun mümkün olduğunu belirtebilirim.

Q ssl inspection aktif mi nasıl görebiliriz?

A Proxy üzerinden bunu kontrol edebilirsiniz detaylı bilgi için bu linki ziyaret edebilirsiniz. https://www.websense.com/assets/support/webinar/Presentation/Jan2013_WebinarSlides.pdf

Q merhaba, websense log yapılandırması ve loglarının analizi konusunda da birkaç şey söyleyebilir misiniz

Q Site içeriğindeki kodu kontrol edeiyor mu?

A Evet ACE güvenlik motoru 10000+ algoritma ile sayfaları analiz eder.

Q Web Security Modülü category filter file type kısmında compressed files seçilmeden executables seçeneği seçilir ise zipli dosyalar içindeki exeler blocklanır mı? Ben bunu sadece web dlp inbound rules içinde yapabiliyoruz diye biliyorum.

A Evet ancak 7.8.3 ve sonrası için bunun mümkün olduğunu belirtebilirim ayrıca SSL tabanlı bir sayfa ise SSL inspection yapılması gerektiğini hatırlatmak isterim.

Q Category filter file type kısmında threats türü dosyaları blockladığımızda tam olarak hangi tip dosyaları blocklamış oluyoruz? False-positive olma riski nedir?

A Detaylı olarak bilgi almak için bu linki ziyaret edebilirsiniz . https://www.websense.com/content/support/library/web/v80/triton_web_help/ft_extensions.aspx

Q DLP modülündede email içindeki urlleri inceleyen policynin tam olarak içeriği nedir? (Email_Corp_Drops)

A Talep etmeniz durumunda bunu sizinle paylaşabiliriz , bizimle irtibata geçebilirsiniz.

Q Cloud hizmetine sizinde bahsettiğiniz gibi finans sektöründe sıcak bakılmıyor. Threatscope için appliance çıkarılması ile ilgili belirli bir tarih var mıdır?

A ThreatScope bir Cloud çözümü değil öncelikle bunu belirtmek isterim sadece Cloud destekli bir sandboxing çözümüdür, Sandbox olmadan hali hazırda oldukça güçlü bir güvenlik altyapısına sahibiz özellikle SSL tabanlı ataklar söz konusu olduğunda elimizi güçlendiren bir altyapımız var. Sorduğunuz soru için ürün geliştirmeleri konusunda kesin bir tarih vermek istemem , böyle bir çalışma olduğunu biliyorum.

Q Email security tarafında websense tarafındaki en büyük şikayetimiz email içinde url scanning işleminden tam olarak istediğimizi alamıyoruz. (bütün kategoriler açık olmasına rağmen) Bu konuda önerileriniz nelerdir.

A Email security içerisindeki URL kontrolleri statik database kontrolleri gerçekleştirir yani URL 'in arkasındaki kodlar zararlı mı değilmi bakmaz . Hibrid kullanım söz konusu olursa sahneye ACE güvenlik motoru çıkar ve güvenlik noktasında ciddi derece bir artış olur. Email tarafında bunun için tavsiyem email dlp politikalarının kullanılmasıdır.

Q USOMdan bugün düşen zararlı link: btinternet.islamhood.net bunu sorgulayabilir miyiz ?

A Sorguladığımda zararlı olarak algılandığını görüyorum. Sayfa ayakta görünmüyor ancak malicious kategoride olduğunu ilgili linki ziyaret ederek görebilirsiniz . http://csi.websense.com/Report/21c4ba01-a14c-4962-956c-a47500c89990

Q Remote filtering kullanıyoruz. dışarda iken kullanıcı ssl inspection yapabiliyor mu remote filtering ya da ne yapılmalı ?

A SSl inspection için Remote filtering yerine Hibrid filtering kullanılması gerekmektedir.

Q Exception tanımlıyorum izin verdiğim halde kategoriden dolayı block yapmaya devam ediyor ?

A Bunun için ilgili iş ortağımızla ya da bizimle irtibata geçerseniz sorunun nereden kaynaklandığı konusunda size yardımcı olabiliriz.

Q File types kısmında threatsi aktif hale getirmek false positivee yol açabilir mi ?

A Eğer bir dosyadan vbs download etmek isterseniz evet olabilir , yine de detaylı bilgi almak için bu linki ziyaret edebilirsiniz . https://www.websense.com/content/support/library/web/v80/triton_web_help/ft_extensions.aspx

Q Custom-Encrypted Uploads görüyorum dashboardda kesinlikle illegal bir şey mi var demek ?

A Bazen yanlış alarmlar olabilir bunun nedeni ilgili sayfanın bilgisayar üzerinden bilgi çekmeye çalışması yada web sayfasının kodlamasıyla alakalı olabilir . Yine de incelenmesi gereken bir durum olduğunu belirtebilirim. Çünkü saldırganlar çoğu zaman ele geçirdikleri bilgisayarlar üzerindeki verileri özel yöntemlerle şifreleyerek kendilerine ait olan sunuculara doğru upload etmektedir.