ATP ENDPOINT

Nedir?

- Yazılım appliance'ıdır.
- SEP'ten vakaları korele etmektedir.
- Endpoint Taramalarını başlatır.
- İyileştirme görevlerini başlatır. (Dosyaları kaldır ya da blokla gibi)
- Cynic'ten gelen dosyaları onaylar.
- Ek ajana gerek duymaz.

Faydalar

- Yeni bir tehdit oluştuğunda, doğrulamadan önce active olup olmadığını anlarsınız.-> Araştırmaya daha az vakit harcarsınız.
- ATP leri daha hızlı tanımlayabilirsiniz ve ek olarak saldırı karşılama ile etkilerini sınırlandırabilirsiz.
- SEP in özelliklerini mi genişletmek istiyorsunuz? Makinanızı karantina altına alabilir, dosyaları silebilir veya ayıklayabilir.

Ne gerekmektedir?

Tam EDR (Endpoint Detection and Response) kapasitesi 12.1 RU6 ve SEP 12.1 RU 5 desteklenmektedir. Fakat müşterinin bilgisayarından dosyaları silemez ya da Cynic için onaylayamaz.

CYNIC

Şüpheli dosyaları otomatik olarak veya ihtiyaca göre, fiziksel ve sanal çevrelerde Symantec Global Zeka Ağı ve machine learning kombinasyonu aracılığı ile tespit eder. Herzaman güncel olan zeka ağı, direk erişim ile ihtiyacınız olan dosyaları size dakikalar içerisinde verir, işlem saatlerce sürmez. Dosyalar çapında, geniş bir ofis dökümanları yelpazesi sunar.(PDF, Java, gibi)

ATP EMAIL

Nedir?

- Yazılım appliance'ıdır.
- ES.cloud vakalarını korele etmektedir.
- Daha detaylı raporlama sağlayabilmekredir.
- Kötü URL uzantılarını saptar ve Cynic'e dosyaları onaylar.
- Ek ajana gerek duymaz.

Faydalar

- Kurumunuzu ve kritik datanızı hedefli saldırılardan korumak için tanımlamalar yapar.
- Gerçek zamanlı kararlarda, bilinmeyen dosyaları önceden otomatik olarak bulur.
- Detaylı risk bilgisini SIEMe aktarır ve risk haritası çıkarmaya yardımcıdır.

Ne gerekmektedir?

Müşterilerin bu ürünü satın alabilmesi için, herhangi bir Email Security.cloud ürününe (Email Protect Email Safeguard veya Email & Web Safeguard)sahip olmaları gerekir.

SYNAPSE

Altuçlar, ağlar, ve e-maillller etrafındaki vakaları korele eder ve tüm veriyi Symantec Global Zeka Ağı ile birleştirir. Aynı zamanda tek Nokta kontolü sağlar ve saldırı aktivitelerini yönetir.Tüm bu saldırıların önceliklendirilmesini sağlar böylelikle zamandan tasarruf edebilirsiniz. Güvenlik analistleriniz daha az vaka inceler.

ATP NETWORK

Nedir?

- Yazılım ya da donanım appliance'ıdır.
- Herşeyin repütasyon kontrolünü yapar. *GIN ile indirilen tüm dosyalarda.
- Güç avantajı vardır.
- Ağ içerisindeki hedefleri tanımlar.
- Cynic'e dosyaları onaylar.
- Yeni saldırı kaynaklarına karşı görünürlük sağlar.

Faydalar

- Daha fazla öngörü için Symantec Global Zeka Ağından gelen dosyaları değerlendirir.
- Değerli hedeflerin görünürlüğü üzerinde ağınızdaki etkilenen müşterileri tespit eder.
- Gerçek zamanlı kararlarda, bilinmeyen dosyaları önceden otomatik olarak bulur.

Ne gerekmektedir?

Müşterinizin ihtiyacının sanal app ya da donanımsal olup olmadığından emin değil misiniz? ATP ölçekledirme ve mimarisindeki ihtiyaçlar için datasheeti inceleyiniz.

VANTAGE

Ağdan gelen şüpheli trafiği tanımlar ve etkilenen ve kötü yazılımların control serverları ile konuşan makineleri ağın içinde konumlandırmada yardımcı olur.

ATP SUITE

Nedir?

- Mevcut SYMC yatırımlarını güçlendirir.
- Anahtar control noktalarını korele eder.
- Vakaları tanımlar ve önceliklendirir.
- (EDR) Altuç Tespit ve Savunma Sistemi.
- Tek tıkla vakaların hızlandırılması.
- Host sandbox detonasyonu
- Ajansız çalışır.

Faydalar

Tüm bunların ötesinde, kurumun tüm tüm altuçlarında, ağında ve emaillerinde saldırı geçmişinin özelleştirilmiş ve tek bir noktadan korelasyonlar aracılığı ile ve ajan eklentisine gerek olmaksınızın görünümünü sağlayın.

Ne gerektirmektedir?

Her bileşen için özel bir teknoloji mimarisi,

Donanımsal ya da sanal appliance, *beklenen ağ trafiğine göre dizayn edilmiş.

ATP: Ağ için.

Symantec

Lisanslama

- ATP Endpoint – kullanıcı başı
- ATP Email – kullanıcı başı
- ATP Network – kullanıcı başı
- Kombinasyon / Suite – kullanıcı başı
- Yıllık Üyelik - min. 1 yıl

Rakipler

- Bit9 + Carbon Black
- PaloAlto
- FireEye
- Proofpoint
- TrendMicro Deep Discovery
- Cisco Source Fire
- McAfee Advanced Threat Defence

SAVO da karşılaştırma kartları mevcuttur.

platin Bilişim Teknolojileri