Use Case: Zararlı Yazılımların Tespit Edilmesi

Müşteri Gereksinimi

İmza tabanlı antivirüs teknolojilerinin, zararlı yazılımlara karşı savaşta birincil silah olarak verimliliğini yitirdiği iyi bilinmektedir. Algılama ve temizleme oranlarının son birkaç yıldır önemli ölçüde düştüğü görülmektedir. Zararlı yazılımlar parasal, kişisel, finansal veya ticari bilgileri hedeflemektedir. Diğer hedefler arasında kimlik hırsızlığı, siber savaş ve casusluk ya da belirli şirketleri hedef alan hizmet kesintileri sayılabilir.

Modern ticari zararlı yazılımları tespit etmek için, antivirüs araçlarının ağ trafiği analizi ve sistemlerin loglarının analizi ile takviye edilmesi gerekir. Buna ek olarak, antivirüs teknolojisinin tehdidi algıladığı ancak silemediği senaryolar yaşanmaktadır. Bu tür durumları tespit etmek ve vurgulamak için çoğu kuruluşun siber saldırılara karşı önemli oranda yeteneklerini geliştirmesi gerekmektedir.

Zararlı yazılımları nasıl tespit edebilir ve önleyebilirim?

Zararlı yazılımların tespit edilmesi zor ve karmaşıktır. Logsign SIEM oluşan zararlı yazılım indikatörlerini ve atak vektörlerini önceden tanımlı korelasyon kurallarını uygulayarak ve Siber Tehdit İstihbaratı (TI) servisi ile analiz ederek elde edilen verileri dashboardlar, alarmlar, raporlar oluşturularak IT yöneticileri ile paylaşmaktadır.

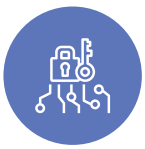
Logsign SIEM'in Zararlı Yazılım Tehditlerini Tespit Etmek ve Durdurmak İçin Kullandığı 5 Adım:

1- Siber Tehdit İstihbaratı (TI), Web Proxy, AD Auth, DNS server, IPS, Process events , Endpoint protection platform (EPP) kaynak logları kullanılarak Logsign SIEM korelasyon teknikleri ile zararlı yazılım tespit süreci başlatılır.

2- Korelasyon işlemleri ile davranış analizi yapılarak kullanıcı Attacker, Victim, Suspicious olarak etiketlenir.

3- Attacker tarafından kullanıcı tarafında başlatılan ilk aktivite sonrasında kaynaklardan gelen loglar ile davranış analizi yapılarak logların zenginleştirilmesi sağlanır. Attacker tarafından yapılan aktiviteler hem içeriden dışarı hem de dışarıdan içeri doğru yapıldığı esnada oluşan log aktiviteleri korelasyona tabi tutularak ilgili dashboard panellerde gösterimi sağlanır.

4- Sonuçlar ilgili BT yöneticileri ile paylaşılarak Mail- SMS şeklinde alarm mekanizmaları oluşturulur.



5- Zararlı yazılımın internet üzerindeki C&C sunucularına doğru oturum başlatması ile exploit sürecinin durdurulması için Logsign SIEM tarafından Palo Alto, Fortigate ve Checkpoint firewall üzerinde API paylaşımı ile ilgili deny kuralları yazılır.