SİBER SALDIRILARIN TESPİTİNDE ETKİN SIEM KULLANIMI

Yazar: Cihat Işık
Baskı: 13 Şubat 2017

İÇİNDEKİLER

SIEM Nedir?

Daha önceleri SIM (Security Information Management) veya SEM (Security Event Management) olarak adlandırılan SIEM (Security Information Event Management), güvenlik olaylarını ve ihlallerini tek bir merkezden yönetmeyi sağlayan araçtır. Daha da açacak olursak, bir kurum ağındaki ağ ve güvenlik cihazları, işletim sistemleri, uygulamalar, sunucular, endpoint çözümleri vs gibi kritik cihazların logunun tek bir merkeze toplanması ve buradan yönetilmesidir.

SIEM Ne Yapar?

SIEM cihazı derinlemesine incelendiği zaman çok fazla modülden ve bileşenden oluşmaktadır. Bazı modüller veya özellikler ürün/marka bazlı değişebilmekte ve birbirinden farklı olmaktadır. Temel olarak her SIEM ürününde olması gereken özellikler ise aşağıdaki gibidir.

Log Toplama: En temel görev olarak, herhangi bir kaynağın loğunu kaynağın kendi formatında ya da istediği başka bir formatta alıp kendi üzerinde saklayabilir.

Birleştirme(Aggregation): Aynı logun birden fazla geldiği durumda, bu logu sayan fakat gösterim olarak tek bir logun altında gösteren özelliğidir.

Korelasyon: Birbirinden bağımsız loglar arasında ilişki kuran ve bunun sonuncunda aksiyon alma özelliğidir.

Aksiyon Alma: Cihaz üzerine toplanan loglardan raporların tasarlanması ya da yazılan kurallar neticesinde alarmlar oluşturulması.

Olay Sonrası Analiz (Incident Response): Olay sonrasında geriye doğru logların incelenebilmesi için logların arşivlenmesi.
Bir SIEM ürününün işleyişi aşağıdaki gibi bir görsel ile ifade edilebilir.

SIEM Ürün Seçimi

En kararsız kalınan konulardan birisi de SIEM konusunda ürün seçimidir. Burada seçim için birçok kriterin olması ve genel olarak başarısız geçen PoC süreçleri kurumlar tarafından genelde ikilem oluşturan durumlardır.

Ürün seçiminde en sık yapılan yanlışlardan biriside, başka bir müşterinin bir X siem ürününü almış olması ve ister istemez o kurumla rekabete girilerek aynı ürünün tercih edilmesidir. Burada kurumlar ile kıyasdan ziyade gerçek parametrelerle çalışmak en doğru ürünün seçilmesi konusunda en etkin yoldur. Yapılan araştırmalar neticesinde en popüler SIEM ürünleri, en temel özellikleri ile karşılaştırılmış ve belirli bir puan üzerinden değerlendirilmiştir. Çok yönlü bu inceleme sonucunda ise 2016 senesinde aşağıdaki gibi bir tablo ortaya çıkmıştır.

Capability	Log Rhythm	Splunk	McAfee Nitro	IBM QRadar	HP ArcSight
Real-time Security Monitoring	4.0	3.4	3.5	4.0	4.1
Threat Intelligence	3.5	3.5	3.7	4.0	4.0
Behavior Profiling	3.8	3.7	3.4	3.8	4.0
Data & End User Monitoring	4.1	3.5	3.7	3.5	3.5
Application Monitoring	3.6	3.7	4.0	4.0	3.8
Analytics	3.6	4.2	3.7	3.9	3.7
Log Management & Reporting	3.5	3.9	3.5	3.6	3.8
Deployment & Support Simplicity	4.0	3.1	3.5	4.0	3.3
Total (Weighted Score)	**30.1**	**29.0**	**29.0**	**30.8**	**30.2**

SIEM Product Comparison – 2016

Bu kıyaslamaya ek olarak, Gartner 2016 SIEM raporu ise yine SIEM alacak kurumlar için ayrıca bir değerlendirme kriteri olabilir. Bu raporda ise en popüler SIEM ürünlerinin 2016 yılına ait durumlarını gösteren aşağıdaki gibi grafiksel bir gösterim verilmiştir.

Figure 1. Magic Quadrant for Security Information and Event Management

Source: Gartner (August 2016)

Etkin SIEM Kullanımı

Günümüzde, birçok kamu kurumu ve özel şirkette bir tane SIEM ürünü bulunmaktadır. Bir SIEM Projesi yapmak, uzun bir PoC sürecinin yanı sıra kuruma özel konfigürasyon gerektirir. Her kurumun ihtiyacı ve sahip olduğu kaynaklar göz önüne bulundurulduğunda, herkesin ihtiyacı birbirinden farklılık gösterecektir. Böyle bir durumda ise kuruma özgü yapılandırılmaların yapılması, kuruma özgü kuralların yazılması ve bu doğrultuda alınacak aksiyonların belirlenmesi gerekmektedir.

En sık yapılan yanlışlardan başında yanlış ve eksik log entegrasyonu gelmektedir. Bir SIEM cihazını en etkili kullanmanın yolu, ürüne doğru ve anlamlı log almaktan geçer. Bunun için entegrasyon sürecinde kurum tarafından hangi logların hangi seviyede alınacağını bilmesi süreci kolaylaştıracaktır. Bütün loglar kontrolsüz bir şekilde alınacak olursa, SIEM ürününün log çöplüğüne dönüşmesi kaçınılmaz bir durumdur. Bunun için öncelikle bir envanter listesi çıkarılmalı ve kurumun sahip olduğu log kaynakları belirlenmelidir. Daha sonraki adımda ise hangi kaynakların saldırı tespitinde kullanılacağı hangilerinin incident response çalışmalarında kullanılacağı gruplandırılmalıdır.

Log entegrasyonu sürecinde logu alınan kaynakların gerçekten doğru logu gönderip göndermediği yapılan testler ile kontrol edilmelidir. Öyle ki size log gönderecek olan bir saldırı tespit sistemi, yapılan atak karşısında log oluşturmuyorsa gerekli imzaların kontrol edilmesi gerekecektir. Böylece yapılacak ataklar karşısında savunma ve tespit durumunuz net olarak ortaya çıkacaktır. Bir SIEM projesinde etkili bir kullanım için alınması gereken log kaynakları aşağıdaki gibi kategorize edilebilir.

- Anti-Virus/Anti-Spam
- Uygulama Sunucuları
- İstemci Tarafı Uygulama Güvenlik Yazılımları (Application Whitelisting)
- İçerik Filtreleme Sistemleri
- Veritabanı Güvenliği, Aktivite İzleme Sistemleri
- Ağ Tabanlı Saldırı Tespit ve Engelleme Sistemleri
- NETFlow / Network Trafik Analiz Sistemleri
- İşletim Sistemleri
- Ağ Yönlendirici Sistemler
- Ağ Altyapı Sistemleri (Switch, TAP, Bridge vs)
- Veritabanı Sistemleri

- Veri Sızıntı Tespit ve Engelleme Sistemleri
- Güvenlik Duvarı Sistemleri
- Host Tabanlı IPS ve Anormallik Tespit Sistemleri
- E-posta Filtreleme ve Spam
- E-posta Sunucu Sistemleri
- APT ve Zararlı Yazılım Tespit Sistemleri
- Ağ Tabanlı Davranışsal İzleme ve Uyarı Sistemleri
- Yük Dengeleme Sistemleri
- Ağ ve Sistem İzleme Sistemleri
- Sanallaştırma Altyapı ve Yönetim Sistemleri
- VPN Erişim ve Yönetim Sistemleri
- Zafiyet Tarama ve Değerlendirme Sistemleri
- Web Sunucu Yazılımları
- Web Application Firewall
- DDOS Sistemi
- Siber Tehdit İstihbaratı
- File Integrity Monitoring Çözümü

Gelişmiş Korelasyon Kurallarının Yazılması

Korelasyon kurallarının yazılması, bir SIEM ürünün asıl marifetini ortaya koyduğu kısımdır ve kullanıcı tarafından beklentinin en yüksek tutulduğu yerdir. Kural örneklerine geçmeden önce bazı kavramaları hatırlamakta fayda var.

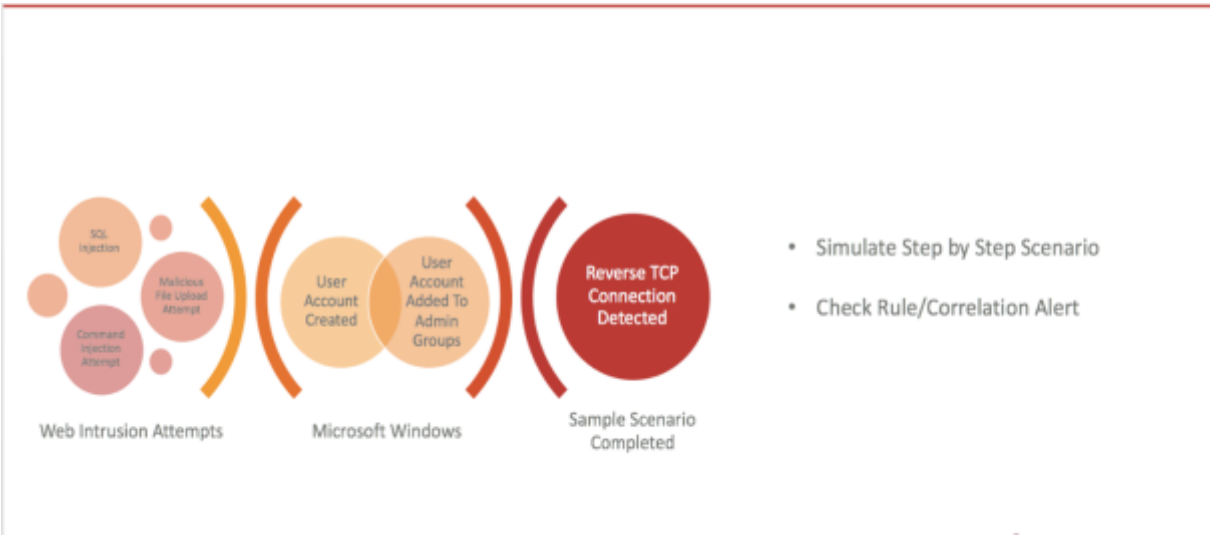
Log: Bilgisayar sistemlerinde, yapılan işlemlerin ya da bir işleyişin detaylarının tutulduğu kayıtlara denir. Bir kullanıcının bilgisayarda oturum açması ya da yeni bir kullanıcı oluşturulması örnek olarak verilebilir.

Threat: Saldırı vektörü ya da imzası içeren loga threat (tehdit) denir. SQL Injection atağı bir threat örneği olarak verilebilir.

Incident: Birden fazla threatin bir araya gelerek riskli bir durum oluşturarak güvenlik ihlali oluşturmasıdır. SQL Injeciton denemesi yapılan makineden reverse tcp bağlantısı denemesinin gelmesi ve o makineye kullanıcı eklenmesi buna bir örnek olarak verilebilir.

Bir SIEM ürününden en büyük beklenti ise yukarıda tanımı yapılan incident girişimlerinin tespit edilebilmesidir. Fakat yetersiz log kaynakları, saldırı tespit sistemlerinin yeterince sıkılaştırılmaması vs gibi nedenlerden dolayı bazen bu kadar efektif kullanılamamaktadır. Bunun için gerekli testler ile önce cihazlar sıkılaştırılmalı sonrasında ise gelişmiş kurallar yazılmalıdır.

Threatlerin bir araya gelerek oluşturduğu örnek bir senaryo aşağıdaki görselde ifade edilmiştir.



İstenilen seviyede bir kuralın yazılması için birden fazla kaynaktan log almak ve bunları korelasyona tabi tutmak gerekir. Örneğin aşağıdaki senaryoyu inceleyelim.

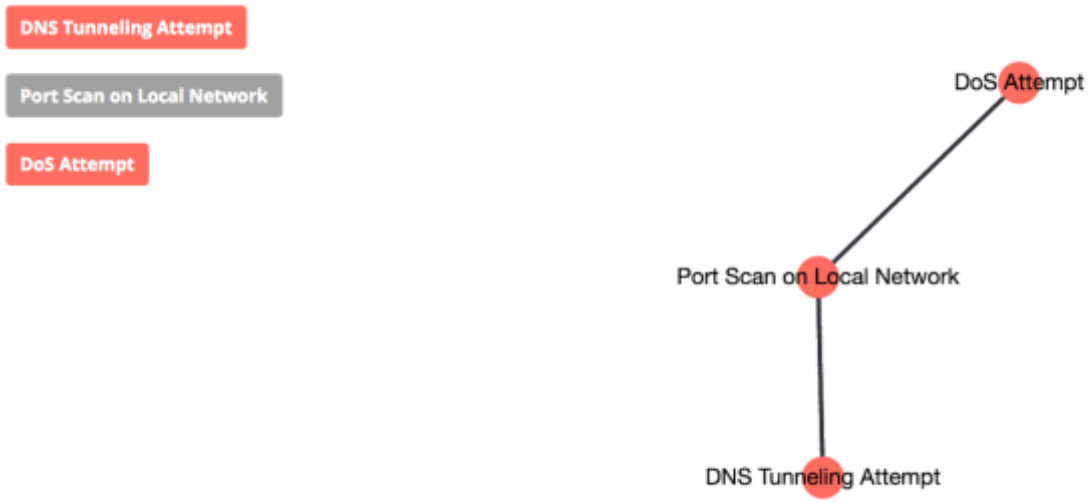
Kurum içindeki bir saldırgan öncelikle port taraması yaparak MsSQL makinelerini tespit etmektedir. Daha sonra ön tanımlı kullanıcı bilgisi ile sisteme giriş yaparak sistem üzerinde komut çalıştırmakta ve makineye atacağı bir casus yazılım ile makineden Shell elde ederek tespit ettiği Domain Admin token'ı ile kullanıcı ekleyip bunu Domain Admins grubuna eklemektedir.

Böyle bir senaryonun tespit edilebilmesi için birçok bileşene ihtiyaç duyulacaktır. Öncelikle bir IDS/IPS tarafından port taramanın tespit edilmesi ve sonrasında ise ön tanımlı DB kullanıcı bilgisi ile sisteme giriş yapıldığı bilgisi elde edilmelidir. Daha sonra makineye atılan casus yazılım antivirüs tarafından tespit edilemiyorsa File Integrity Monitoring tarafından tespit edilmelidir. Sorasında ise oluşturulan kullanıcı ve bu kullanıcının Domain Admin grubuna eklenmesine yönelik aktiviteyi tespit etmek için ise DC üzerinden gelen event loglara igtiyaç duyulacaktır. Senaryo bir bütün şeklinde korelasyon kuralı olarak yazıldı ise bu adımlardan herhangi birisinin tespit edilememesi bütün olarak senaryonun tespit edilmemesi anlamına gelecektir. O yüzden yazılan kurallarda tuning çalışması yapılmalı ve çalıştığı doğrulanmalıdır.

Kural çalışmasında örnek olarak aşağıdaki gibi örnek kurallar kullanılabilir.

- DNS Tunnel Activity Detected After Port Scanning
- User Account Created after Malicious File Detected
- Successfull Brute Force Attack Detected After Port Scan Activity
- Database Worm Detected After Malicious File Detected
- Botnet Trafik Detected after Same Malicious File Found on Different Sources
- Malicious (Backdoor) File Upload Attempt After Automated Scan Detected
- Same Malicious File Found on Multiple Sources After Spam Mail Activity

Yazılmış örnek bir kurala ait atak grafiği aşağıdaki gibi gösterilmiştir.



Ulusal Siber Olaylara Müdahale Merkezi (USOM)

Ulusal Siber Olaylara Müdahale Merkezi, (USOM, TR-CERT) Telekomünikasyon İletişim Başkanlığı'nın Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının 4.3 maddesi uyarınca oluşturulmasının planlanmasının ardından, 2014 yılında yine Türkiye Telekomünikasyon İletişim Başkanlığı tarafından kurulmuş olan, bilişim kuruluşudur.

Kuruluş, internet üzerinden kendileri ile iletişime geçen kullanıcılar, kolluk kuvvetleri, yerel ve uluslararası kuruluşlar, araştırma merkezlerinin yanı sıra özel sektör arasındaki siber güvenlik olaylarına müdahale ve koordinasyonun sağlanması amacıyla kurulmuştur. Bu kapsamda, kritik sektörlere yapılacak saldırıların önlenmesi, siber güvenlik olaylarının duyurulması, bu konuda ilgililerin uyarılması faaliyetlerini gerçekleştirir.

Ulusal Siber Olaylara Müdahale Merkezi altında SOME isimli ekipler bulunmaktadır. SOME'nin açılımı Siber Olaylara Müdahale Ekipleri'dir. USOM altında Kurumsal SOME ve Sektörel SOME adlarıyla kurulmuş iki ekip bulunur. Kurumsal SOME bakanlıklar, müstakil kamu kurumları ile bilgi işleme sahip diğer kamu kurumları ile koordinasyon içerisinde bulunur. Ayrıca Kurumsal SOME, sektörel bazda olan durumları kritik alt yapı işletmecileri (kamu veya özel) için de gerektiğinde koordinasyona geçebilir.

REFERANSLAR:

- http://infosecnirvana.com/siem-product-comparison-201/
- https://tr.wikipedia.org/wiki/Ulusal_Siber_Olaylara_M%C3%BCdahale_Merkezi

BGA Bilgi Güvenliği A.Ş. Hakkında

BGA Bilgi Güvenliği A.Ş. 2008 yılından bu yana siber güvenlik alanında faaliyet göstermektedir. Ülkemizdeki bilgi güvenliği sektörüne profesyonel anlamda destek olmak amacı ile kurulan BGA Bilgi Güvenliği, stratejik siber güvenlik danışmanlığı ve güvenlik eğitimleri konularında kurumlara hizmet vermektedir.

Uluslararası geçerliliğe sahip sertifikalı 50 kişilik teknik ekibi ile, faaliyetlerini Ankara ve İstanbul ve USA'da sürdüren BGA Bilgi Güvenliği'nin ilgi alanlarını "*Sızma Testleri, Güvenlik Denetimi, SOME, SOC Danışmanlığı, Açık Kaynak Siber Güvenlik Çözümleri, Büyük Veri Güvenlik Analizi ve Yeni Nesil Güvenlik Çözümleri*" oluşturmaktadır.

Gerçekleştirdiği başarılı danışmanlık projeleri ve eğitimlerle sektörde saygın bir yer edinen BGA Bilgi Güvenliği, kurulduğu günden bugüne alanında lider finans, enerji, telekom ve kamu kuruluşlarına 1.000'den fazla eğitim ve danışmanlık projeleri gerçekleştirmiştir.

BGA Bilgi Güvenliği, kurulduğu 2008 yılından beri ülkemizde bilgi güvenliği konusundaki bilgi ve paylaşımların artması amacı ile güvenlik e-posta listeleri oluşturulması, seminerler, güvenlik etkinlikleri düzenlenmesi, üniversite öğrencilerine kariyer ve bilgi sağlamak için siber güvenlik kampları düzenlenmesi ve sosyal sorumluluk projeleri gibi birçok konuda gönüllü faaliyetlerde bulunmuştur.

BGA Bilgi Güvenliği AKADEMİSİ Hakkında

BGA Bilgi Güvenliği A.Ş.'nin eğitim ve sosyal sorumluluk markası olarak çalışan Bilgi Güvenliği AKADEMİSİ, siber güvenlik konusunda ticari, gönüllü eğitimlerin düzenlenmesi ve siber güvenlik farkındalığını arttırıcı gönüllü faaliyetleri yürütülmesinden sorumludur. Bilgi Güvenliği AKADEMİSİ markasıyla bugüne kadar "Siber Güvenlik Kampları", "Siber Güvenlik Staj Okulu", "Siber Güvenlik Ar-Ge Destek Bursu" , "Ethical Hacking yarışmaları" ve "Siber Güvenlik Kütüphanesi" gibi birçok gönüllü faaliyetin destekleyici olmuştur.