SIEM Tanıtım

Güvenlik bilgileri ve olay yönetimi (SIEM), kuruluş içindeki verileri toplayan ve yorumlayan ve ardından olası tehditleri tespit eden bir güvenlik çözümüdür. SIEM sayesinde güvenlik tehditleri gerçek zamanlı olarak izlenebilir. Bu eğitimde genel olarak bir SIEM'in nasıl çalıştığını anlatacağız. Çok derine inmeden, SOC analistinin perde arkasında neler olduğunu anlaması için size yeterli bilgiyi sağlayacağız. Eğitimin sonunda, aşağıdaki konular hakkında genel bir anlayışa sahip olacaksınız:

SIEM nasıl çalışır?
SIEM günlükleri nasıl toplar?
Günlük depolama
uyarı oluşturma

SIEM Ürünleri

Piyasada birçok SIEM çözümü bulunmaktadır. Gartner 2021 raporuna göre en başarılı ticari SIEM çözümleri aşağıdaki görseldeki gibidir.

Source: Gartner (June 2021)

SIEM ve SOC Analisti

SIEM ile tespit edilen potansiyel tehditler, SOC analistleri tarafından incelenir

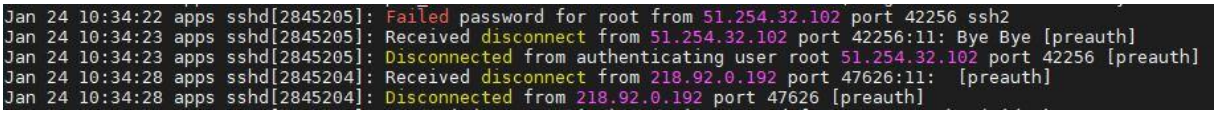
Günlük Toplama

Öncelikle SIEM çözümünün tehditleri algılaması için verilere ihtiyacımız var. Bu nedenle, günlük toplama işlemi SIEM mimarisinin en önemli parçalarından biridir, çünkü günlük SIEM'i olmadan hiçbir işe yaramaz.

Günlük ve Günlük Nedir?

Bilgi işlemde, bir günlük dosyası, bir işletim sisteminde veya diğer yazılım çalıştırmalarında meydana gelen olayları veya bir iletişim yazılımının farklı kullanıcıları arasındaki mesajları kaydeden bir dosyadır. Günlüğe kaydetme, günlük tutma eylemidir. En basit durumda, mesajlar tek bir günlük dosyasına yazılır.
tanım: wikipedia.org

Temel bir günlük, zaman, kaynak sistem ve bir mesaj içerir. Örneğin bir Ubuntu sunucusundaki "/var/log/auth.log" dosyasının içeriğine baktığımızda kaynak, saat ve mesaj bilgilerini görebiliriz.



Bu noktada amacımız çeşitli yerlerden (Hosts, Firewall, Server log, Proxy vb.) logları SIEM'e aktarmaktır. Böylece tüm verileri işleyebilir ve tehditleri merkezi bir noktada tespit edebiliriz. Günlükler genellikle aşağıdaki 2 yolla toplanır:

Log Agents
Agentless

Log Agents

Bu yöntemi uygulamak için bir günlük aracı yazılımı gereklidir. Aracılar genellikle ayrıştırma, günlük döndürme, arabelleğe alma, günlük bütünlüğü, şifreleme, dönüştürme özelliklerine sahiptir. Başka bir deyişle, bu aracı yazılım, topladığı günlükleri hedefe iletmeden önce işlem yapabilir.
Örneğin, agent yazılımı ile "username: LetsDefend; account: Administrator" olan bir logu 2 parçaya bölüp şu şekilde iletebiliriz:

mesaj1 = "kullanıcı adı: LetsDefend"
message2 = "hesap: Yönetici"

Yöntemin artıları

Geliştiriciler tarafından test edilmiş ve çalışan bir uygulamadır.

Otomatik ayrıştırma, şifreleme, günlük bütünlüğü vb. gibi birçok ek özelliğe sahiptir.

Yöntemin eksileri

Ek özellikler etkinleştirildikçe kaynak tüketimi artar. Bu da sistemin CPU, RAM gibi kaynaklarının artırılmasını gerektiriyor, dolayısıyla maliyet artıyor.

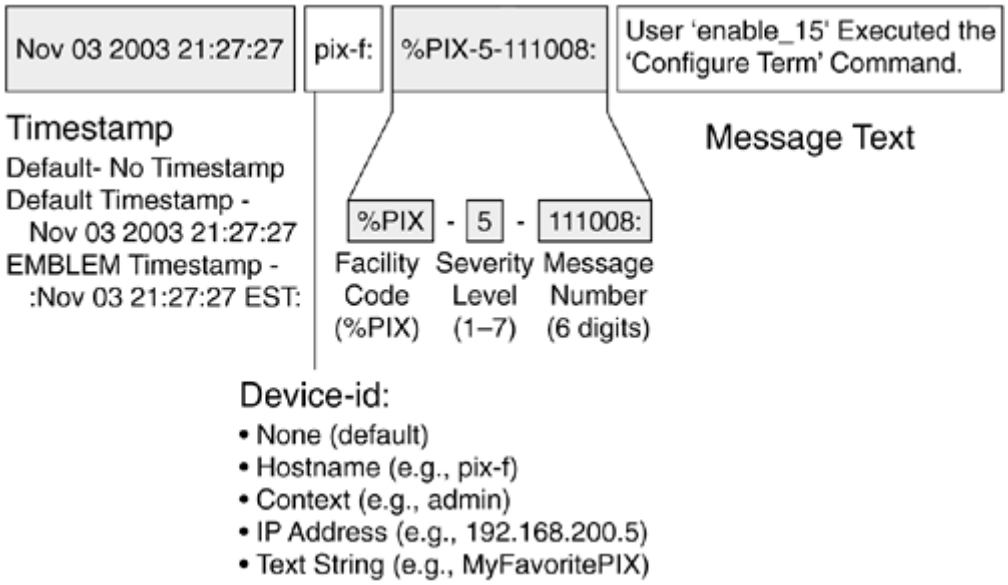
sistem günlüğü

Günlük aktarımları için çok popüler bir ağ protokolüdür. Hem UDP hem de TCP ile çalışabilir ve isteğe bağlı olarak TLS ile şifrelenebilir. Syslog'u destekleyen bazı cihazlar: Switch, Router, IDS, Firewall, Linux, Mac, Windows cihazları ek yazılımlarla syslog destekli hale gelebilir.

Günlük aracılarınızın Syslog ile günlükleri aktarmasını sağlayabilirsiniz. Bunun için öncelikle loglarınızı syslog formatında ayrıştırmanız gerekmektedir.

Sistem günlüğü Biçimi:

Zaman Damgası - Kaynak Cihaz - Tesis - Önem Derecesi - Mesaj Numarası - Mesaj Metni



Ayrıca Syslog UDP ile gönderilebilecek maksimum paket boyutu 1024 bayttır. TCP için 4096 bayttır.

3. Parti Temsilcileri

Çoğu SIEM ürününün kendi aracı yazılımı vardır. 3. taraf aracılar, destekledikleri özellikler nedeniyle syslog'dan daha fazla yeteneğe sahiptir. Bazı ajanlar:

Splunk: evrensel iletici
ArcSight: ArcSight Konnektörleri

Bu ajanların SIEM'e entegre edilmesi kolaydır ve ayrıştırma özelliklerine sahiptir.

Popüler açık kaynak aracıları:
Beats https://www.elastic.co/beats/
NXLog https://nxlog.co/

Agentless

Aracısız log gönderme işlemi bazen kurulum ve güncelleme maliyeti olmadığı için tercih edilmektedir. Genellikle loglar hedefe SSH veya WMI ile bağlanarak gönderilir.
Bu yöntem için günlük sunucusunun kullanıcı adı ve şifresi gereklidir, bu nedenle şifrenin çalınma riski vardır.
Ajan yönteminden daha kolay hazırlanır ve yönetilir. Ancak, sınırlı yetenekleri vardır ve kimlik bilgileri ağa sarılır.

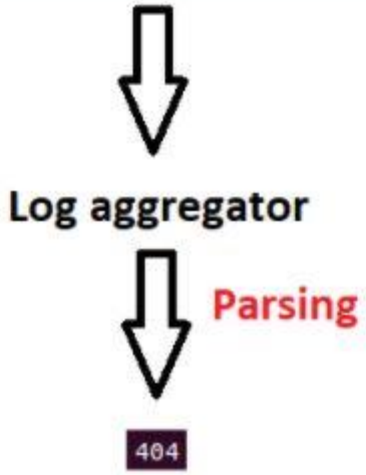
Manuel Koleksiyon

Bazen mevcut aracı yazılımlarla toplayamayacağınız günlükler olabilir. Örneğin, aracı ile bulut tabanlı bir uygulamanın günlüklerini okuyamıyorsanız, kendi komut dosyanızı yazmanız gerekebilir.

Özet
Gördüğünüz gibi, günlükleri toplamanın çeşitli yolları vardır. Bunlar ajanlar ve ajansızlardır. Piyasadaki acentelerin yeterli olmadığı durumlarda kendi scriptlerinizi yazmalısınız.

Oluşturulan günlüklerin gönderildiği ilk yer, günlük toplayıcıdır. Buraya gelen logları hedefe göndermeden önce düzenleyebiliriz. Örneğin bir web server loglarından sadece durum kodlarını almak istiyorsak gelen loglar arasında filtreleme yapabilir ve hedefe sadece istenilen kısımları gönderebiliriz.

```
192.168.131.23 - - [19/Apr/2020:11:33:23 -0700] "GET /read.php?id=1%27%20UNION%2
0ALL%20SELECT%20LOAD_FILE(%27/etc/passwd%27) HTTP/1.1" 404 208 "-" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0
.3987.163 Safari/537.36"
```



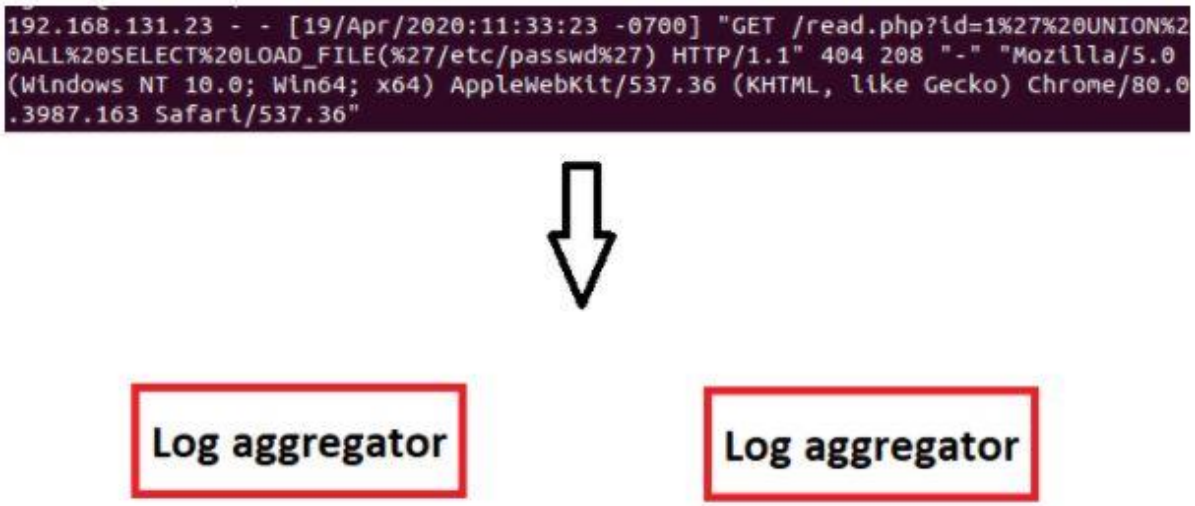
Toplayıcı EPS

EPS nedir?

EPS, saniye başına bir olaydır. Formül Olaylar/Süre saniyedir. Örneğin sistem 5 saniyede 1000 log alıyorsa EPS 1000/5 = 200 olur
. EPS değeri arttıkça kullanılması gereken toplayıcı ve depolama alanı da artar.

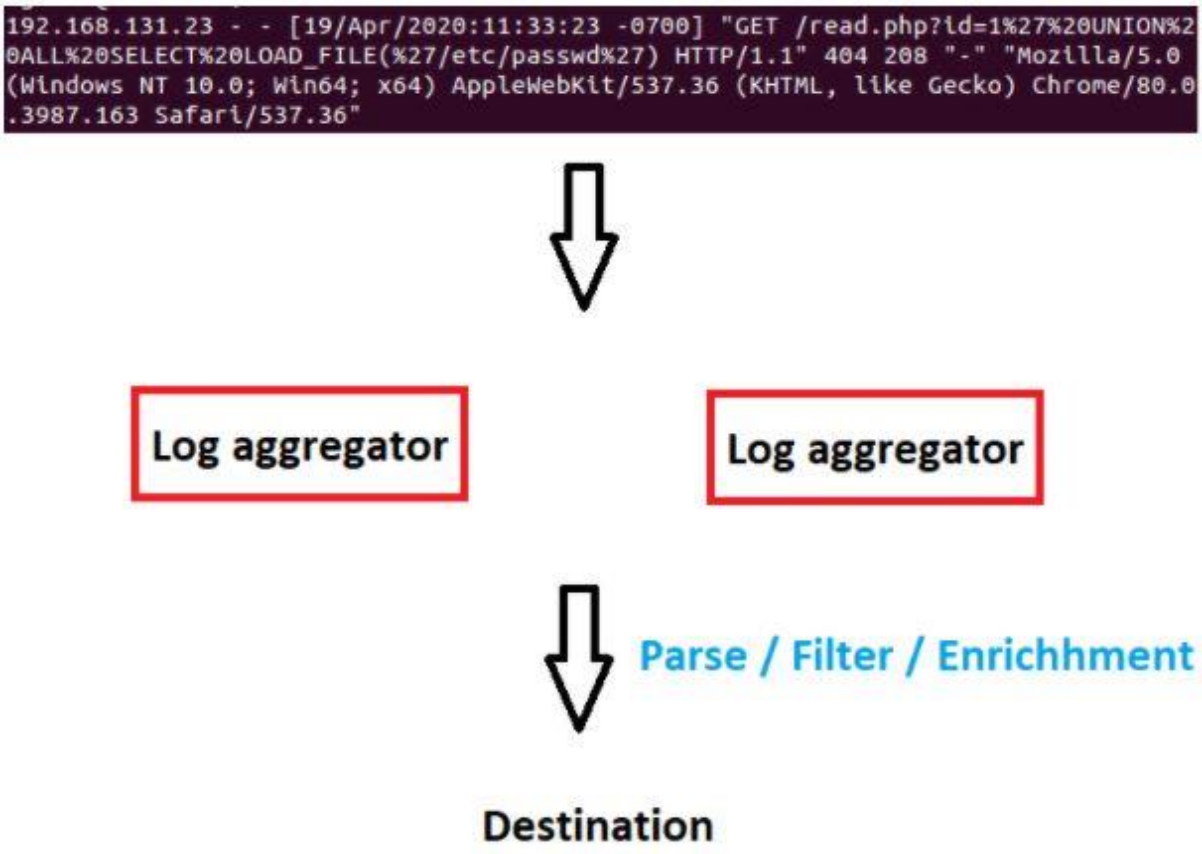
Toplayıcıyı Ölçeklendirme

Gelen günlüklerin her seferinde aynı toplayıcıyı yüklememesi için birden fazla toplayıcı eklenebilir. Ve sıralı veya rastgele seçim sağlanabilir.



Günlük Toplayıcı Süreci

Toplayıcıya gelen log işlenir ve ardından hedefe yönlendirilir. Bu süreç ayrıştırma, filtreleme ve zenginleştirme olabilir.



Günlük Değişiklik

Bazı durumlarda, gelen günlüğü düzenlemeniz gerekir. Örneğin, topladığınız günlüklerin çoğu tarih bilgisi gg-aa-yyyy biçiminde gelirken, aa-gg-yyyy olarak tek bir kaynaktan geliyorsa, o günlüğü dönüştürmek istersiniz. Başka bir örnek, UTC + 2 gelen zaman bilgisini UTC + 1'e dönüştürmeniz gerekebilir.

Günlük Zenginleştirme

Toplanan logların verimini artırmak ve zamandan tasarruf etmek için zenginleştirme yapılabilir. Örnek zenginleştirmeler:

coğrafi konum
DNS
Ekle Kaldır

coğrafi konum

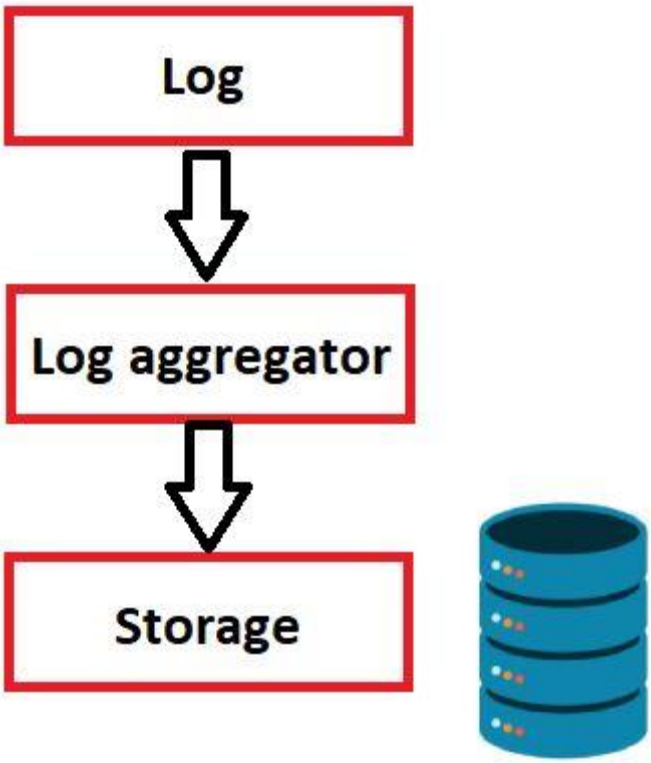
Belirtilen IP adresinin coğrafi konumu bulunabilir ve günlüğe eklenebilir. Böylece logu görüntüleyen kişi zamandan tasarruf sağlar. Ayrıca konum tabanlı davranışı analiz etmenize olanak tanır.

DNS

DNS sorguları ile domainin IP adresi bulunabilir veya ters DNS yapılarak IP adresi bulunabilir.

Günlük Depolama

Önceki yazılarımızda loglar ve log toplayıcılardan bahsetmiştik. Bir sonraki adım, gelen günlükleri saklamaktır.



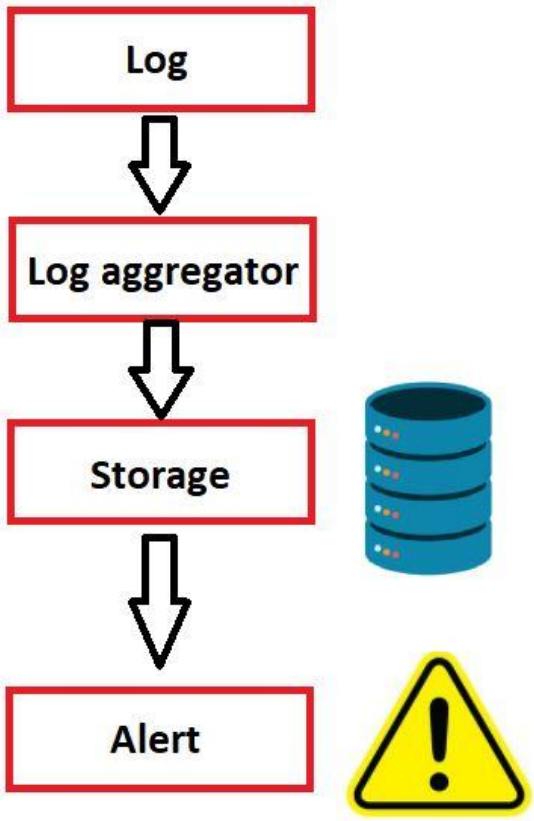
SIEM yapılarında yapılan yaygın hatalardan biri de depolama boyutuna odaklanmaktır. Bu verilere erişim hızı kadar yüksek boyutlu depolama da önemlidir. Örneğin WAF, Firewall, Proxy vb. tüm logları topladığımızı varsayalım ve bu loglarda arama yapmanın 15 dakika sürdüğünü düşünelim. Verilere ulaşmanın bu kadar zor olduğu bir durumda çalışmalar çok verimli olmayacaktır. Bu nedenle depolamada veri erişim hızı da göz önünde bulundurulmalıdır.

Piyasadaki popüler depolama teknolojilerine (Örnek: mysql) baktığımızda veri ekleme, düzenleme ve silme odaklı olduğunu görüyoruz. Ancak bizim odak noktamız verileri indekslemek, saklanan günlüğü daha sonra düzenlemeyi düşünmüyoruz. Amacımız verilere en hızlı şekilde ulaşmaktır. Bunun için WORM (bir kez yaz çok oku) tabanlı teknolojilerin SIEM'de kullanılması daha uygundur.

Solucan hakkında daha fazla bilgi bir kez çok okuyun:
https://en.wikipedia.org/wiki/Write_once_read_many

uyarı

Bu noktaya kadar günlükleri topladık, işledik ve depoladık. Şimdi elimizdeki verileri kullanarak anormal davranışları tespit edip uyarılar oluşturmamız gerekiyor.



Uyarıların zamanında ortaya çıkması, arama hızımıza bağlı olarak değişir. Bugün oluşturulan bir günlük için 2 gün sonra uyarı oluşturmak yerine hemen uyarı oluşturmak istiyoruz. Bu nedenle bir önceki yazımızda da belirttiğimiz gibi uygun bir depolama ortamı oluşturulmalıdır.

SIEM için oluşturacağımız alarmlar genellikle şüpheli olacaktır ve araştırılması gerekmektedir. Bu, uyarının optimize edilmesi ve çok sayıda tetiklenmemesi gerektiği anlamına gelir (istisnai durumlar hariç).

Bir uyarı oluşturmanın bazı yolları şunlardır:

Saklanan verileri arayarak
Log çekerken alarm oluşturma

Oluşturulabilecek örnek uyarılar:

Global yöneticiye yeni kullanıcı eklendi
15 Giriş aynı IP adresiyle 3 dakika içinde başarısız oldu

Bir kalite uyarısı oluşturabilmek için elinizdeki verileri anlamanız gerekir. Daha iyi günlük aramaları yapmak için bazı teknikler kara listeye alma, beyaz listeye alma ve uzun kuyruk analizidir.

kara liste

İstenmeyen durumları yakalamak için kullanılabilir. Örneğin yasaklanmış işlem adlarını (Örnek: mimikatz.exe) toplayıp bir listeye yazabiliriz. Daha sonra bu listedeki bir işlem loglarda gözükürse uyarı oluşturabiliriz. Benzer şekilde, yasaklı bir IP listesi oluşturan ve bu listeye erişen bir cihaz olduğunda bir uyarı oluşturulabilir.

Yönetilmesi ve uygulanması kolaydır, ancak atlanması çok kolaydır. Örneğin, mimikatz.exe yerine mimikatz2.exe adı kullanılırsa herhangi bir uyarı oluşmaz.

beyaz liste

Kara listeden farklı olarak istenilen durumlar için kullanılır. Örneğin, normal iletişime sahip IP adreslerinin bir listesi tutulabilir. Bu liste dışında bir adresle iletişim kurulursa uyarı oluşturabiliriz. Bu yöntem oldukça etkilidir ancak yönetilmesi zordur. Listenin sürekli güncellenmesi gerekiyor.

Uzun Kuyruk Log Analizi

Bu yöntem, sürekli olarak meydana gelen davranışların normal olduğunu varsayar. Başka bir deyişle, bir cihazda sürekli olarak "Event ID 4624 Bir hesap başarıyla oturum açıldı" günlüğü oluşuyorsa, bu yöntemle bunu normal kabul etmeli ve en az oluşan günlüklere şüpheyle yaklaşmalıyız.