

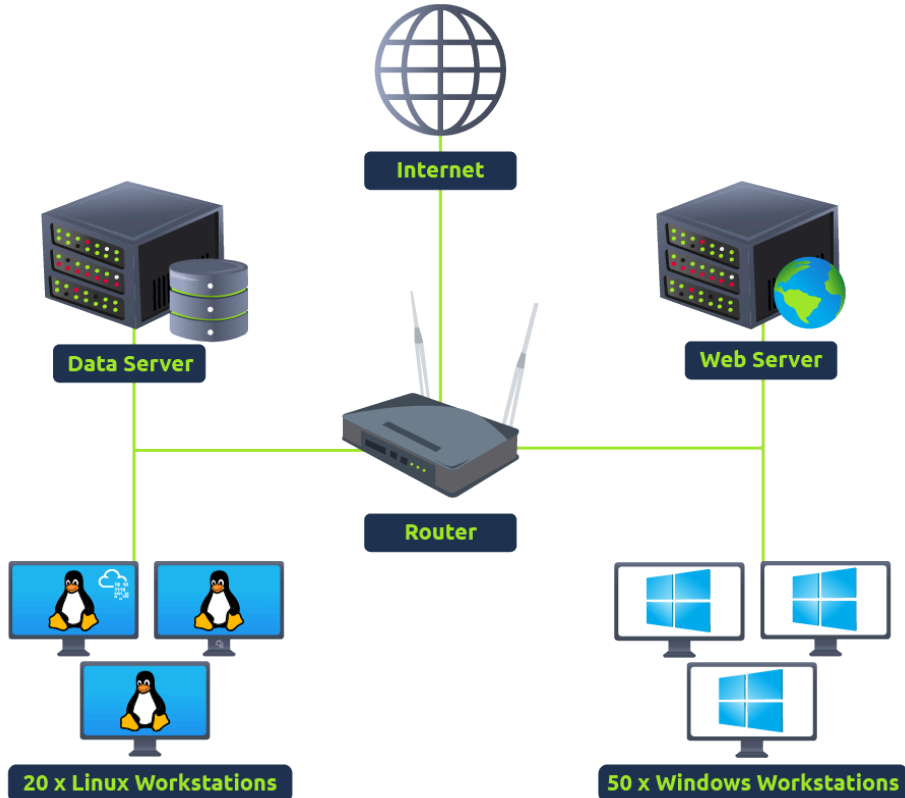
SIEM NEDİR? (Security Information and Event Management System)

SIEM, Güvenlik Bilgi ve Olay Yönetim Sistemi'nin kısaltmasıdır. Ağ üzerindeki çeşitli uç noktalardan/ağ cihazlarından veri toplayan, bunları merkezi bir yerde depolayan ve bunlar üzerinde ilişki kuran bir araçtır.

Bu yazıda aşağıdaki sorulara yanıt arayacak ve öğreneceğiz:

- ☐ Siem nedir ? Nasıl Çalışır?
- ☐ Siem e neden ihtiyaç duyulur?
- ☐ Ağ görünürlüğü nedir?
- ☐ Log Kaynakları nelerdir ve log alımı nasıl yapılır?
- ☐ SIEM'in sağladığı yetenekler nelerdir?

SIEM'in önemini anlatmadan önce, bir ağ içindeki tüm faaliyetlerin daha iyi görünürlüğü'nün neden kritik olduğunu anlayalım. Aşağıdaki görsel, birden fazla Linux/Windows tabanlı uç nokta, bir veri sunucusu ve bir web sitesinden oluşan basit bir ağın örneğini göstermektedir. Her bir bileşen bir diğeriyle haberleşir veya bir yönlendirici aracılığıyla internete erişir.



Bildiğimiz gibi, her ağ bileşeninin farklı günlükler üreten bir veya daha fazla günlük kaynağı olabilir. Ağ günlüğü kaynaklarımızı iki mantıksal parçaya bölebiliriz:

Ana Bilgisayar Merkezli Günlük Kaynakları	Ağ Merkezli Günlük Kaynakları
<p>Bunlar, ana bilgisayar içinde veya ana bilgisayarla ilgili olarak meydana gelen olayları yakalayan günlük kaynaklarıdır. Ana bilgisayar merkezli günlükler üreten bazı günlük kaynakları Windows Olay günlükleri, Sysmon, Osquery vb.'dir. Ana bilgisayar merkezli günlüklerin bazı örnekleri şunlardır:</p> <ul style="list-style-type: none">*Bir dosyaya erişen kullanıcı*Kimlik doğrulaması yapmaya çalışan kullanıcı*Bir işlem Yürütme Etkinliği*Bir kayıt defteri anahtarını veya değerini ekleyen/düzenleyen/silen işlem.*Powershell yürütme	<p>Ağ ile ilgili günlükler, ana bilgisayarlar birbirleriyle iletişim kurduğunda veya bir web sitesini ziyaret etmek için internete eriştiğinde oluşturulur. Bazı ağ tabanlı protokoller SSH, VPN, HTTP/s, FTP vb.'dir. Bu tür olayların örnekleri şunlardır:</p> <ul style="list-style-type: none">*SSH bağlantısı*FTP üzerinden erişilen bir dosya*Web trafiği*VPN üzerinden şirketin kaynaklarına erişen bir kullanıcı.*Ağ dosya paylaşımı Etkinliği

SIEM'in Önemi


Tüm bu cihazlar saniyede yüzlerce olay ürettiğinden, herhangi bir olaya karşı her cihazdaki imglogları tek tek incelemek sıkıcı bir iş olabilir.Bu, SIEM çözümünün yerinde olmasının avantajlarından biridir.

Sadece çeşitli kaynaklardan gerçek zamanlı günlükler almakla kalmaz, aynı zamanda olaylar arasında ilişki kurma, günlüklerde arama yapma, olayları araştırma ve derhal yanıt verme yeteneği de sağlar. SIEM tarafından sağlanan bazı temel özellikler şunlardır:

1. Gerçek zamanlı günlük alımı
2. Anormal aktivitelere karşı uyarı
3. 7/24 İzleme ve görünürlük
4. Erken tespit yoluyla en son tehditlere karşı koruma
5. Veri içgörüler ve görselleştirme
6. Geçmiş olayları araştırma yeteneği.

Günlük Kaynakları ve Günlük Toplama

Ağıdaki her cihaz, bir kullanıcının bir web sitesini ziyaret etmesi, SSH'ye bağlanması, iş istasyonunda oturum açması vb. gibi üzerinde bir etkinlik gerçekleştirildiğinde bir tür günlük oluşturur. Windows ve Linux olarak ikiye ayırdığımızda şu şekilde toparlayabiliriz:

Windows	Linux
<p>Windows, Olay Görüntüleyicisi yardımcı programı aracılığıyla görüntülenebilen her olayı kaydeder. Her günlük etkinliği türüne benzersiz bir kimlik atar ve analistin incelemesini ve takip etmesini kolaylaştırır.</p> <p>Windows ortamındaki olayları görüntülemek için arama çubuğuna Olay Görüntüleyicisi yazın; aşağıda gösterildiği gibi farklı günlüklerin depolandığı ve görüntülenebildiği araca yönlendirilirsiniz.</p> <p>Tüm Windows uç noktalarından gelen bu günlükler, izleme ve daha iyi görünürlük için SIEM çözümüne iletilir.</p> 	<p>Linux OS, olaylar, hatalar, uyarılar vb. gibi tüm ilgili günlükleri depolar. Bunlar daha sonra sürekli izleme için SIEM'e aktarılır. Linux'un günlükleri depoladığı yaygın konumlardan bazıları şunlardır:</p> <p>/var/log/httpd : HTTP İstek / Yanıt ve hata günlüklerini içerir.</p> <p>/var/log/cron : Cron işleriyle ilgili olaylar bu konumda saklanır.</p> <p>/var/log/auth.log ve /var/log/secure : Kimlik doğrulamayla ilgili günlükleri depolar.</p> <p>/var/log/kern : Bu dosya çekirdek ile ilgili olayları depolar.</p> <p>Herhangi bir olası web saldırısı girişimi için web sunucusuna gelen ve web sunucusundan çıkan tüm istekleri/yanıtları takip etmek önemlidir. Linux'ta, tüm apache ile ilgili günlükleri yazmak için yaygın konumlar /var/log/apache veya /var/log/httpd'dir.</p>


GÜNLÜK ALIMI

Tüm bu günlükler çok sayıda bilgi sağlar ve güvenlik sorunlarının belirlenmesine yardımcı olabilir. Her SIEM çözümünün günlükleri almanın kendine özgü bir yolu vardır. Bu SIEM çözümleri tarafından kullanılan bazı yaygın yöntemler aşağıda açıklanmıştır:


- 1) Agent / Forwarder-** Aracı/Yönlendirici: Bu SIEM çözümleri, Uç Noktaya yüklenen bir aracı (Splunk tarafından yönlendirici) adı verilen hafif bir araç sağlar. Tüm önemli günlükleri yakalamak ve bunları SIEM sunucusuna göndermek üzere yapılandırılmıştır.
- 2) Syslog:** Syslog, web sunucuları, veritabanları vb. gibi çeşitli sistemlerden veri toplamak ve gerçek zamanlı verileri merkezi hedefe göndermek için yaygın olarak kullanılan bir protokoldür.
- 3) Manuel Yükleme:** Splunk, ELK vb. gibi bazı SIEM çözümleri, kullanıcıların hızlı analiz için çevrimdışı verileri almasına izin verir. Veri alındıktan sonra normalleştirilir ve analiz için kullanılabilir hale getirilir.
- 4) Port Yönlendirme:** SIEM çözümleri ayrıca belirli bir portu dinleyecek şekilde yapılandırılabilir ve ardından uç noktalar verileri dinleme portundaki SIEM örneğine iletebilir.

Splunk'un günlük toplama için çeşitli yöntemler sağlamasına dair bir örnek aşağıda gösterilmektedir:


Or get data in with the following methods



Upload
files from my computer
Local log files
Local structured files (e.g. CSV)
[Tutorial for adding data](#)



Monitor
files and ports on this Splunk platform instance
Files - HTTP - WMI - TCP/UDP - Scripts
Modular inputs for external data sources



Forward
data from a Splunk forwarder
Files - TCP/UDP - Scripts

NEDEN SIEM ?

SIEM, tehditleri tespit etmek için toplanan veriler üzerinde korelasyon sağlamak amacıyla kullanılır. Bir tehdit algılandığında veya belirli bir eşik aşıldığında bir uyarı verilir. Bu uyarı, analistlerin soruşturmaya dayalı olarak uygun eylemlerde bulunmasını sağlar.

SIEM, Siber Güvenlik alanında önemli bir rol oynar ve en son tehditleri zamanında tespit etmeye ve korumaya yardımcı olur. Ağ altyapısında neler olup bittiğine dair iyi bir görünürlük sağlar.

SIEM YETENEKLERİ

SIEM, aşağıda gösterildiği gibi bir Güvenlik Operasyon Merkezi (SOC) ekosisteminin önemli bir bileşenidir. SIEM, günlükleri toplayarak ve herhangi bir olayın/akışın kuralda belirlenen koşulla eşleşip eşleşmediğini veya belirli bir eşiği geçip geçmediğini inceleyerek başlar. SIEM'in bazı yaygın yetenekleri şunlardır:

- Farklı günlük kaynaklarından gelen olaylar arasında korelasyon.
- Hem Ana Bilgisayar merkezli hem de Ağ merkezli etkinliklerde görünürlük sağlama.
- Analistlerin en son tehditleri ve zamanında yanıtları araştırmasına izin verin.
- Yerinde olan kurallar tarafından tespit edilmeyen tehditleri arayın.



SOC Analisti Sorumlulukları

SOC Analistleri, ağ içinde neler olup bittiğine dair daha iyi bir görünürlüğe sahip olmak için SIEM çözümlerini kullanır. Sorumluluklarından bazıları şunlardır:

- İzleme ve Araştırma.
- Yanlış pozitifleri belirleme.
- Gürültüye veya yanlış pozitiflere neden olan Kuralları ayarlama.
- Raporlama ve Uyumluluk.
- Ağ görünürlüğündeki kör noktaları belirleme ve bunları kapatma.

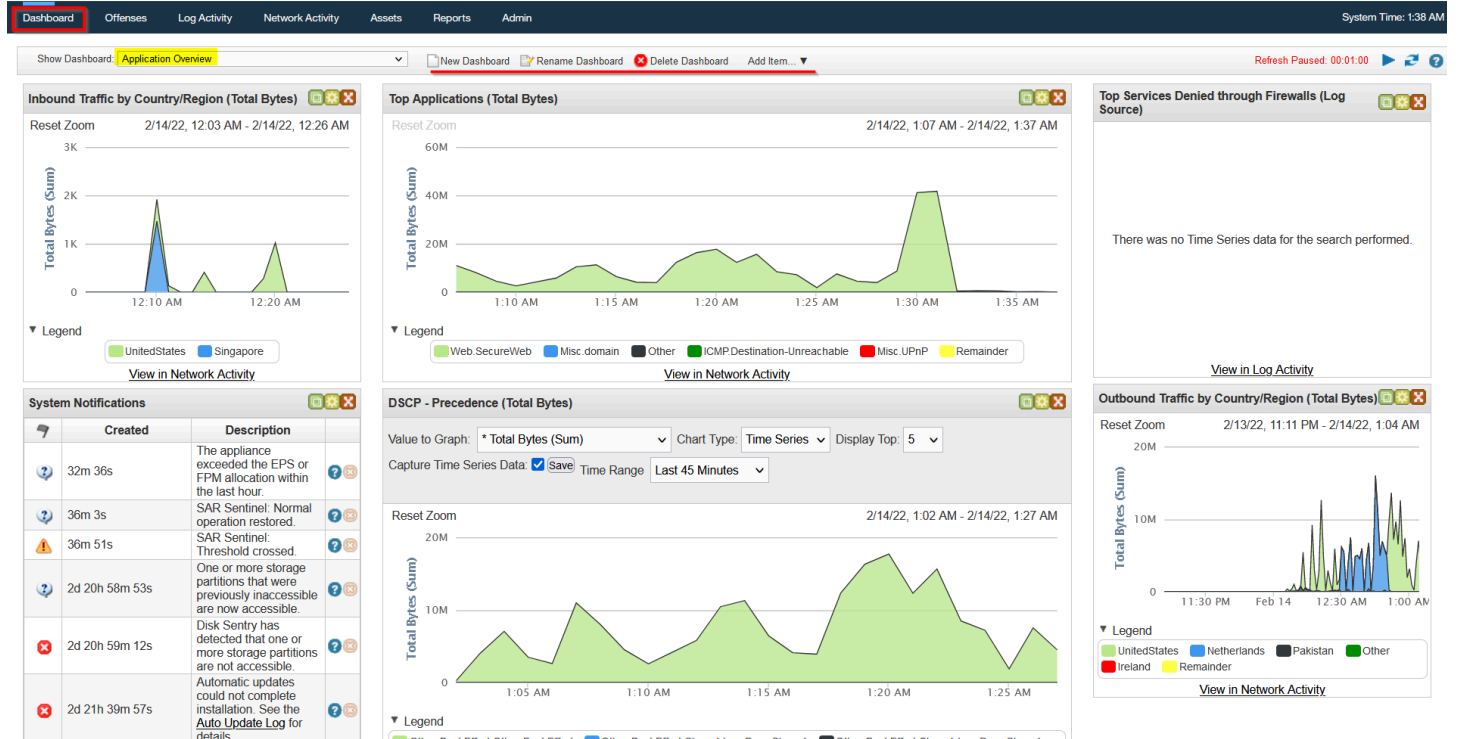
GÜNLÜK VE UYARI ANALİZİ

SIEM aracı, araçlar, port yönlendirme vb. aracılığıyla tüm güvenlikle ilgili günlükleri alır. Günlükler alındıktan sonra, SIEM analistler tarafından kurallarda belirlenen koşulların yardımıyla günlüklerde istenmeyen davranış veya şüpheli örüntü arar. Koşul karşılanırsa, bir kural tetiklenir ve olay araştırılır.

Dashboards(Gösterge Panelleri) : Gösterge panelleri herhangi bir SIEM'in en önemli bileşenleridir. Bu analizlerin özeti, birden fazla gösterge panelinin yardımıyla eyleme dönüştürülebilir içgörüler şeklinde sunulur. Her SIEM çözümü bazı varsayılan panolarla gelir ve özel Pano oluşturma seçeneği sunar. Bir panoda bulunabilecek bilgilerin bazıları şunlardır:

- **Alert –Uyarı**
- **Highlights–Öne Çıkanlar**
- **System Notification–Sistem Bildirimi**
- **Health Alert–Sağlık Uyarısı**
- **List of Failed Login Attempts–Başarısız Giriş Girişimlerinin Listesi**
- **Events Ingested Count–Yutulan Olay**
- **Rules triggered–Sayısı Tetiklenen Kurallar**
- **Top Domains Visited–Ziyaret Edilen En İyi Alan Adları**

Qradar SIEM'deki Varsayılan gösterge panelinin bir örneği aşağıda gösterilmektedir:



Korelasyon Kuralları

Korelasyon kuralları tehditlerin zamanında tespit edilmesinde önemli bir rol oynar ve analistlerin zamanında harekete geçmesini sağlar. Korelasyon kuralları, tetiklenmek üzere ayarlanmış mantıksal ifadelerdir.

Korelasyon kurallarına birkaç örnek şunlardır:

1. Bir Kullanıcı 10 saniyede 5 başarısız Giriş Denemesi alırsa– Birden Fazla Başarısız Giriş Denemesi için bir uyarı oluşturun – **Multiple Failed Login Attempts**
2. Birden fazla başarısız oturum açma girişiminden sonra oturum açma başarılı olursa – Bir uyarı oluşturun – **Successful Login After multiple Login Attempts**
3. Bir kullanıcı USB taktığında her seferinde uyarı verecek bir kural ayarlandı (USB'nin şirket politikası gereği kısıtlanmış olması durumunda kullanışlıdır)
4. Giden trafik > 25 MB ise – Olası Veri Sızdırma Girişimine karşı bir uyarı oluşturun (Genellikle şirket politikasına bağlıdır)

Bir korelasyon kuralı nasıl oluşturulur?

Kuralın nasıl çalıştığını açıklamak için aşağıdaki Eventlog kullanım durumlarını göz önünde bulundurun:

Kullanım Örneği 1: Rakipler, izlerini yok etmek için genellikle istismar sonrası aşamada kayıtları kaldırmayı tercih ederler.	Kullanım Örneği 2: Saldırganlar, istismar/ayrıcalık yükseltme aşamasından sonra whoami gibi komutları kullanır.
 Bir kullanıcı olay günlüklerini kaldırmaya veya temizlemeye çalıştığında her seferinde benzersiz bir Olay Kimliği 104 kaydedilir. Bu aktiviteye dayalı bir kural oluşturmak için koşulu şu şekilde ayarlayabiliriz: Rule– Kural: Log kaynağı WinEventLog ise ve EventID 104 ise – Bir uyarıyı tetikle – <u>Event Log Cleared</u>	 Aşağıdaki Alanlar kurala dahil edilmesinde yardımcı olacaktır. Rule–Kural: Eğer Log Kaynağı WinEventLog ise ve EventCode 4688 ise ve NewProcessName whoami içeriyorsa, o zaman bir UYARI tetikleyin– <u>WHOAMI komutu Yürütme TESPİT EDİLDİ</u>

UYARI ARAŞTIRMASI

SIEM'i izlerken analistler zamanlarının çoğunu, ağa ilişkin çeşitli önemli ayrıntıları çok özet bir şekilde gösteren gösterge panellerinde geçirirler. Bir uyarı tetiklendiğinde, uyarıyla ilişkili olaylar/akışlar incelenir ve hangi koşulların karşılandığı görmek için kural kontrol edilir.

Analist, soruşturmaya dayanarak bunun Doğru veya Yanlış pozitif olup olmadığını belirler. Analizden sonra

gerçekleştirilen eylemlerden bazıları şunlardır:

- Uyarı Yanlış Alarmdır. Benzer Yanlış pozitiflerin tekrar oluşmasını önlemek için kuralın ayarlanması gerekebilir.
- Uyarı Gerçek Pozitif. Daha fazla araştırma yapın.
- Etkinlik hakkında bilgi almak için varlık sahibiyle iletişime geçin.
- Şüpheli etkinlik doğrulandı. Enfekte olmuş ana bilgisayarı izole edin.
- Şüpheli IP'yi engelleyin.