Elastic SIEM Lab Oluşturma Rehberi



Siber güvenlik dünyasında, SIEM (Security Information and Event Management) sistemleri kurumların güvenlik tehditlerine karşı daha hazırlıklı olmalarını sağlayan kritik araçlardır. SIEM sayesinde güvenlik olayları toplanır, analiz edilir ve anlamlandırılır. Bu rehberde, kendi SIEM lab ortamınızı oluşturmanın adımlarını paylaşacağım. Bu ortam, temel seviyede güvenlik olaylarının nasıl toplanıp analiz edileceğini öğrenmek isteyenler için harika bir başlangıç olacaktır.

SIEM Nedir ve Neden Önemlidir?

SIEM, güvenlik verilerini toplama, analiz etme ve bu verilerden anlamlı sonuçlar çıkarma amacıyla kullanılan bir teknolojidir. SIEM araçları sayesinde güvenlik olayları hızlıca tespit edilebilir ve kurumlar tehditlere karşı daha hızlı reaksiyon gösterebilir. Özellikle siber güvenlik alanında kariyer yapmak isteyenler için SIEM lab ortamı kurmak, teorik bilgiyi pratiğe dökmek açısından büyük bir fırsattır.

SIEM Lab İçin Gerekenler

Bir SIEM lab ortamı kurarken ihtiyacınız olan temel gereksinimleri şöyle sıralayabiliriz:

• VirtualBox veya VMware: Sanal makineler kullanarak lab ortamı oluşturmak için gereklidir.

- **Elastic SIEM**: Logların toplanması, analizi ve görselleştirilmesi için kullanılacak SIEM platformudur.
- Linux OS: Güvenlik olaylarını toplayacak ve Elastic SIEM'in çalışacağı işletim sistemi olarak tercihen Kali Linux önerilir.



Elastic SIEM'in Kurulumu

Elastic Stack, logları toplamak ve analiz etmek için oldukça popüler bir araçtır.

Görevler:

- Ücretsiz bir Elastic hesabı oluşturun.
- Kali VM'i kurun.
- Logları toplamak ve SIEM'e iletmek için Linux VM üzerinde Elastic Agent'ı yapılandırın.
- Kali VM üzerinde güvenlik olayları oluşturun.
- Elastic SIEM'de güvenlik olaylarını bulmak için sorgu yapın.
- Güvenlik olaylarını görselleştirmek için bir Dashboard oluşturun.
- Güvenlik olayları için uyarılar oluşturun.

Host Linux Sunucusunda Elastic Agent'ı Yükleyin, Yapılandırın ve Yönetin

- 1. Elastic Defender Agent entegrasyonunu aratın ve ekleyin.
- 2. Sayfadaki talimatları takip ederek devam edin.

Oluşturulan Sanal Makinede Güvenlik Olayları Oluşturma

- 1. **Nmap** gibi ağ keşfi için ücretsiz ve açık kaynaklı bir araç kullanın.
- Nmap, portları taramak, hedefte çalışan işletim sistemi ve yazılımı belirlemek için kullanılabilir.
- Ağ hakkında bilgi toplamak için kullanılır.

Nmap komutunu çalıştırın:

- sudo nmap <vm-ip>
- IP adresini bulmak için "ifconfig" komutunu kullanabilirsiniz.
- Alternatif olarak, nmap -p- localhost komutunu çalıştırın.
- Birkaç Nmap komutu çalıştırarak çeşitli güvenlik olaylarını gözlemleyin:

sudo nmap -sS localhost

- **TCP SYN taraması**: Stealth Scan (diğer adıyla "yarı açık" tarama) olarak da bilinir. SYN paketi gönderir, yanıt bekler ve yanıt alınırsa bağlantıyı kapatır.
- Bu tarama daha hızlıdır ve tam TCP el sıkışmasını tamamlamadığı için güvenlik duvarları veya saldırı tespit sistemleri tarafından daha az tespit edilir.

nmap -p- localhost

- Varsayılan olarak, Nmap yalnızca en yaygın 1000 portu tarar. -p- ile tüm TCP portları hedeflenir.
- Bu seçenek, kapsamlı taramalar için faydalı olabilir ancak ağdaki açık portların sayısına bağlı olarak çok daha uzun sürebilir.

nmap -sT localhost

- **TCP Connect Scan**: Tam bir TCP Bağlantı Taramasıdır. Hedef makineyle tam bir üç yönlü el sıkışma gerçekleştirir ve TCP bağlantısını tamamen kurar.
- Eğer bağlantı başarılı olursa, portun açık olduğunu gösterir. Aksi takdirde kapalı veya filtrelenmiştir.
- Kullanımı daha kolaydır ve kök yetkisi gerektirmez, ancak daha yavaş ve tespit edilmesi daha kolaydır çünkü portla tamamen bağlantı kurması gerekir.

3. Nmap, birkaç port bulacaktır.



Elastic SIEM'de Güvenlik Olaylarını Sorgulama

- 1. Bağlantı kurulduktan sonra verilerimizi SIEM Lab'imize iletmiş olacağız.
- 2. Artık SIEM üzerinde logları sorgulamaya ve analiz etmeye başlayabiliriz.
- 3. Elastic Cloud'da **Observability** sayfasına gidin ve **Logs** \rightarrow **Stream** seçeneğini seçin.
- 4. Sunucumuzdan gelen çok sayıda log göreceksiniz. Nmap taramaları ile ilgili tüm logları bulmak için bir sorgu girin, örneğin:
- event.action: "nmap_scan" veya process.args: "sudo"

Her olayın yanındaki üç noktaya tıklayarak log detaylarını rahatlıkla görüntüleyebilirsiniz.

	iss.args: nmap		0	
Customize Highlights				
Nov 3, 2024	event.dataset	Message		
Showing entries t	rom Nov 3, 18:52:55			
18:52:55.069	endpoint.events.process	Endpoint process event		
18:52:55.070	endpoint.events.process	Endpoint process event		
18:52:55.070	endpoint.events.process	Endpoint process event		
18:52:55.072	endpoint.events.process	Endpoint process event		
18:52:55.072	endpoint.events.process	Endpoint process event		
18:52:55.072	endpoint.events.process	Endpoint process event		0.10
18:52:55.072	endpoint.events.process	Endpoint process event		
18:52:55.072	endpoint.events.process	Endpoint process event		
18:52:55.072	endpoint.events.process	Endpoint process event		

6. Olayları Görselleştirmek için Bir Dashboard Oluşturma

- 1. Analytics bölümüne gidin ve Dashboards sekmesine tıklayın.
- 2. **Dashboard** oluştururken yatay ekseni @timestamp, dikey ekseni ise count olarak ayarlayın.
- 3. Dashboard'u kaydedin ve tamamlayın.



Kurallarımız Bir Olayı Tespit Ettiğinde Bildirim Almak için Uyarı Oluşturmak

- 1. Security bölümüne gidin ve Alerts seçeneğini seçin.
- 2. Yeni bir kural oluşturmak için Custom Query seçeneğini seçin.
- 3. Nmap ile çalıştığımız için, buna göre bir uyarı oluşturacağız.
- 4. process.name: "nmap" veya event.action: "nmap_scan" adlı sorguyu girin ve diğer bölümleri varsayılan ayarlarda bırakın.
- 5. Actions bölümünde, tetiklendiğinde bildirim almak istediğiniz işlemi seçin.

Son olarak, tüm işlemler tamamlandı. Bu uyarıları görüntüleyebilir ve yönetebilirsiniz. Farklı uyarılar ekleyerek kendinizi test etmeyi unutmayın.

