**Veri Okyanusunda Güvenliği Sağlamak - ELK Stack'in Güvenlik Kalkanı Elastic Security**

Günümüzün dijital dünyasında kurumlar her saniye devasa boyutlarda veri üretir: sunucu logları, ağ trafiği, uygulama kayıtları, kullanıcı aktiviteleri ve daha nicesi. Bu veri okyanusunu anlamlandırmak ve yönetmek için **ELK Stack** (Elasticsearch, Logstash, Kibana) gibi güçlü araçlar kullanılır. Peki, bu devasa veri yığınını sadece operasyonel verimlilik için değil, aynı zamanda kurumumuzu siber tehditlere karşı korumak için nasıl kullanabiliriz? İşte bu sorunun cevabı **Elastic Security**'dir. Elastic Security, ELK Stack'i sıradan bir log yönetim platformundan, gelişmiş bir siber güvenlik operasyon merkezine dönüştüren güçlü bir çözümdür.

Bu yazıda, Elastic Security'nin ne olduğunu, neden modern siber savunmanın vazgeçilmez bir parçası haline geldiğini, nasıl kurulduğunu ve en önemlisi, bu aracı bir güvenlik uzmanı gibi etkili bir şekilde nasıl kullanabileceğinizi pratik örneklerle keşfedeceğiz.

**1. Elastic Security Nedir?**

**Elastic Security**, Elastic Stack üzerine inşa edilmiş, açık ve entegre bir güvenlik çözümüdür. Tek bir platformda iki ana siber güvenlik disiplinini birleştirir:

1. **SIEM (Security Information and Event Management - Güvenlik Bilgisi ve Olay Yönetimi):** Ağ cihazları, sunucular, bulut servisleri, güvenlik duvarları gibi farklı kaynaklardan gelen logları merkezi bir yerde toplar, analiz eder, ilişkilendirir (korelasyon) ve önceden tanımlanmış kurallara göre şüpheli aktiviteler için alarmlar üretir.
2. **EDR/XDR (Endpoint Detection and Response / Extended Detection and Response - Uç Nokta Tespiti ve Müdahalesi):** Sadece logları toplamakla kalmaz, aynı zamanda **Elastic Agent** aracılığıyla doğrudan uç noktalara (kullanıcı bilgisayarları, sunucular) yerleşir. Bu sayede, zararlı yazılımları (malware), fidye yazılımlarını (ransomware) ve karmaşık saldırıları daha başlamadan *engeller*, şüpheli süreçleri tespit eder ve analistlere olaylara anında müdahale etme yeteneği kazandırır.

Kısacası Elastic Security, veriyi toplama, tespit etme, analiz etme ve müdahale etme döngüsünün tamamını **Kibana** arayüzü üzerinden yönetmenizi sağlayan bütünleşik bir güvenlik platformudur.

**2. Neden Kullanılır?**

Elastic Security'nin popülerliği ve yaygın kullanımı birkaç temel avantajından kaynaklanmaktadır:

* **Merkezi Görünürlük:** Güvenlik ekiplerinin en büyük zorluklarından biri, farklı güvenlik araçlarından (antivirüs, güvenlik duvarı, vb.) gelen verileri bir araya getirmektir. Elastic Security, tüm bu verileri tek bir yerde toplayarak "tek bir pencereden" tüm altyapıyı izleme imkanı sunar.
* **Gelişmiş Tehdit Tespiti ve Önleme:** Yüzlerce yerleşik ve MITRE ATT&CK çerçevesiyle eşleştirilmiş tespit kuralı içerir. Bu kurallar, bilinen saldırı tekniklerini otomatik olarak algılar. Ayrıca, makine öğrenmesi yetenekleri sayesinde "normal" davranış kalıplarının dışındaki anormallikleri tespit ederek sıfır gün (zero-day) saldırılarını yakalama potansiyeli sunar. Uç noktada ise doğrudan önleme (prevention) yaparak saldırıyı durdurur.
* **Hızlı Soruşturma ve Tehdit Avcılığı (Threat Hunting):** Elasticsearch'ün inanılmaz hızı sayesinde, analistler saniyeler içinde terabaytlarca veri arasında arama yapabilir. **Timeline** gibi interaktif araçlar, bir saldırının adımlarını bir zaman çizelgesine dizerek olayın tüm hikayesini kolayca anlamayı sağlar.
* **Esneklik ve Ölçeklenebilirlik:** Hem küçük işletmelerin hem de devasa kurumsal ağların ihtiyaçlarına göre ölçeklenebilir. İstediğiniz her türlü veri kaynağını (custom loglar dahil) kolayca entegre etmenize olanak tanır.

**3. Nasıl Kurulum Yapılır?**

Elastic Security, ayrı bir ürün olarak kurulmaz; **Elastic Stack'i kurduğunuzda otomatik olarak gelen bir özelliktir.** Kurulum için iki ana yol bulunur:

**Yol 1: Elastic Cloud (En Kolay ve Tavsiye Edilen Yöntem)**  
Bu, Elastic firmasının sunduğu "hizmet olarak yazılım" (SaaS) modelidir.

1. cloud.elastic.co adresine gidin ve bir hesap oluşturun.
2. Birkaç tıklama ile yeni bir "deployment" (küme) başlatın.
3. Elasticsearch, Kibana ve diğer bileşenler sizin için otomatik olarak kurulur ve yapılandırılır.
4. Kibana arayüzüne giriş yaptığınızda, sol menüdeki "Security" bölümü kullanıma hazırdır.

**Yol 2: Kendi Sunucularınıza Kurulum (On-Premise)**  
Daha fazla kontrol isteyen kullanıcılar için bu yöntem tercih edilir.

1. **Elasticsearch'ü Kurun:** Verilerinizin depolanacağı ve indeksleneceği veritabanını kurun.
2. **Kibana'yı Kurun:** Elasticsearch'teki verileri görselleştireceğiniz ve yöneteceğiniz arayüzü kurun.
3. **Elastic Agent'ı Entegre Edin:** Bu en kritik adımdır. Veri toplamak ve uç noktaları korumak istediğiniz tüm sunuculara ve kullanıcı bilgisayarlarına **Elastic Agent**'ı kurmanız gerekir. Agent kurulumu ve yönetimi, Kibana içerisindeki **Fleet** arayüzu üzerinden merkezi olarak yapılır. Fleet, binlerce ajanı tek bir yerden yönetmenizi, onlara politika atamanızı (örn: "Bu sunucularda ransomware korumasını aç ve sistem loglarını topla") sağlar.

Kurulumun özü, veriyi kaynaklarından (uç noktalar, ağ cihazları) alıp Elasticsearch'e göndermekten ibarettir. Veri akmaya başladığı anda Elastic Security uygulaması anlamlı hale gelir.

**4. Kullanım Parametreleri (Temel Bileşenler ve Ayarlar)**

Elastic Security, komut satırı parametrelerinden ziyade, Kibana arayüzü üzerinden yönetilen modüler bir yapıya sahiptir. En önemli "parametreleri" yani bileşenleri şunlardır:

* **Detection Rules (Tespit Kuralları):** Güvenlik çözümünün beynidir. Gelen verilere karşı sürekli çalışan sorgulardır. Örneğin, "Tek bir IP'den 5 dakika içinde 20'den fazla başarısız giriş denemesi" gibi bir kural tanımlanabilir. Elastic, yüzlerce hazır kural sunar ve siz de kendi özel kurallarınızı yazabilirsiniz.
* **Alerts (Alarmlar):** Bir tespit kuralı tetiklendiğinde oluşan kayıtlardır. Analistler bu alarmları inceler.
* **Cases (Vakalar):** Bir alarmın önemli olduğuna karar verildiğinde, daha derinlemesine bir soruşturma için "Vaka"ya dönüştürülür. Vaka yönetimi, soruşturma adımlarını, bulguları ve yorumları tek bir yerde toplamayı sağlar.
* **Timeline (Zaman Çizelgesi):** İnteraktif soruşturma aracıdır. Bir alarmı veya şüpheli bir olayı (IP adresi, kullanıcı adı vb.) zaman çizelgesine sürükleyip bırakarak ilgili tüm olayları kronolojik sırada görebilirsiniz.
* **Host ve Network Analizi:** Uç noktalar ve ağ trafiği ile ilgili tüm verileri detaylı olarak inceleyebileceğiniz özel sayfalardır.
* **Agent Policies (Ajan Politikaları):** Fleet üzerinden yönetilen bu politikalar, uç noktalardaki Elastic Agent'ların ne yapacağını belirler. Örneğin, "Malware koruması aktif olsun mu?", "Hangi log dosyaları toplansın?", "Network trafiği izlensin mi?" gibi ayarlar bu politikalarla yapılır.

**5. Bu Aracı Etkili Kullanmanın 5 Örneği ve Açıklamaları**

**Örnek 1: Fidye Yazılımı (Ransomware) Saldırısını Engelleme**

* **Senaryo:** Bir çalışan, oltalama (phishing) e-postasındaki zararlı bir eki açar. Ek, bilgisayardaki dosyaları şifrelemeye çalışan bir fidye yazılımı içerir.
* **Elastic Security Nasıl Çalışır?**
  1. Çalışanın bilgisayarında kurulu olan **Elastic Agent**, aktif **Malware/Ransomware koruması** politikası ile çalışmaktadır.
  2. Agent, dosyaları hızla değiştirmeye çalışan, bilinen fidye yazılımı imzalarına sahip veya şüpheli davranışlar sergileyen (örn: gölge kopyaları silme) süreci anında tespit eder.
  3. Saldırıyı daha başlamadan **engeller**, zararlı süreci sonlandırır ve dosyayı karantinaya alır.
  4. Kibana'daki Security paneline "Malware Prevention Alert" (Zararlı Yazılım Engelleme Alarmı) düşer. Analist, hangi kullanıcıda, hangi dosyanın ve ne zaman engellendiğini anında görür.

**Örnek 2: "Password Spraying" Saldırısını Tespit Etme**

* **Senaryo:** Bir saldırgan, dış ağdan kurumun Active Directory (AD) sunucusuna karşı, sık kullanılan birkaç parolayı (örn: "MevsimYil2023", "Password123") yüzlerce farklı kullanıcı adı ile dener.
* **Elastic Security Nasıl Çalışır?**
  1. AD sunucusuna kurulan Elastic Agent, Windows güvenlik loglarını (Olay ID 4625 - Başarısız Oturum Açma) toplar ve Elasticsearch'e gönderir.
  2. Elastic Security'nin yerleşik tespit kurallarından biri olan **"Multiple Logon Failures from a single source"** (Tek bir kaynaktan çoklu oturum açma hatası) kuralı tetiklenir.
  3. Güvenlik analistinin ekranına bir alarm düşer. Alarmda, saldırganın IP adresi, denediği kullanıcı hesapları ve deneme sayısı gibi kritik bilgiler yer alır. Analist, bu IP adresini güvenlik duvarından anında engelleyerek saldırıyı durdurabilir.

**Örnek 3: Tehdit Avcılığı ile "Living Off the Land" Tekniğini Keşfetme**

* **Senaryo:** Bir saldırgan, sisteme sızdıktan sonra antivirüsleri atlatmak için Windows'un kendi meşru aracı olan **PowerShell**'i kullanarak ağda yatayda ilerlemeye çalışır. Bu aktivite standart bir kuralı tetiklemeyebilir.
* **Elastic Security Nasıl Çalışır?**
  1. Güvenlik analisti proaktif bir avcılık (threat hunting) yapmak ister.
  2. Kibana'da **Timeline** veya **Discover** sekmesini açar ve tüm uç noktalardaki süreç verileri içinde basit bir sorgu çalıştırır: process.name: "powershell.exe".
  3. Çıkan sonuçları daha da daraltır: Şüpheli görünen, uzun ve şifrelenmiş (-enc) komutlar içeren, ağ bağlantısı başlatan (net.webclient) veya sistemde normalde görülmeyen PowerShell kullanımlarını arar.
  4. Bu sayede, alarm üretmeyen ancak son derece şüpheli olan bu aktiviteyi manuel olarak tespit ederek gizli saldırganı ortaya çıkarabilir.

**Örnek 4: Şüpheli Veri Sızdırmayı Tespit Etme**

* **Senaryo:** İçeriden bir tehdit veya ele geçirilmiş bir hesap, büyük miktarda veriyi kurum dışındaki bir bulut depolama servisine (örn: Dropbox, Mega) yüklemeye çalışır.
* **Elastic Security Nasıl Çalışır?**
  1. Elastic Security, ağ trafiği verilerini (Netflow, Packetbeat vb.) analiz etmektedir.
  2. Analist, network.bytes\_out (giden byte miktarı) metriğini izleyen bir kural veya dashboard oluşturur.
  3. Bir kullanıcının iş saatleri dışında veya normalin çok üzerinde bir veri çıkışı (egress) yaptığını fark eder.
  4. Aynı zaman diliminde o kullanıcının uç nokta verilerini incelediğinde, bu trafiğin şüpheli bir süreç tarafından başlatıldığını görerek veri sızıntısını tespit eder ve müdahale eder.

**Örnek 5: Bulut Güvenliği İhlalini Soruşturma**

* **Senaryo:** Bir geliştiricinin AWS erişim anahtarları (access keys) sızdırılır ve saldırgan bu anahtarları kullanarak yeni bir IAM kullanıcısı oluşturur.
* **Elastic Security Nasıl Çalışır?**
  1. Elastic, AWS CloudTrail loglarını toplayacak şekilde yapılandırılmıştır.
  2. Yerleşik **"Unusual IAM User Created"** (Alışılmadık IAM Kullanıcısı Oluşturuldu) kuralı, normalde bu tür bir işlem yapmayan bir kullanıcı tarafından yeni bir yönetici hesabı oluşturulduğunu tespit eder ve alarm üretir.
  3. Analist, alarmı **Timeline**'a sürükler. Aynı anda, bu işlemi yapan kaynak IP'nin geldiği ülkeyi, kullanıcının diğer aktivitelerini ve olayın öncesinde/sonrasında ne olduğunu tek bir ekranda görerek olayın tam resmini çizer.

**Sonuç**

Elastic Security, sadece logları depolayan bir sistem olmanın çok ötesine geçerek, ELK Stack'i tam teşekküllü bir siber savunma platformuna dönüştürür. SIEM'in geniş kapsamlı görünürlüğü ile EDR/XDR'ın derinlemesine tespit ve önleme gücünü birleştiren bu çözüm, güvenlik ekiplerine modern tehditlere karşı daha hızlı, daha akıllı ve daha etkili bir şekilde yanıt verme yeteneği kazandırır. Günümüzün karmaşık siber tehdit ortamında, veriyi güvenliğin merkezine koyan Elastic Security gibi platformlar, artık bir seçenek değil, bir zorunluluk haline gelmiştir.