Bölüm 14

LOG YÖNETİMİ, SIEM VE SOAR

Nafiz ÜNLÜ[1]

GİRİŞ

Yakın tarihten bu yana dijitalleşen dünyada çözümlerin de dijitalleşmesi ile birlikte veriler, bilgisayar sistemleri içerisinde saklanmakta ve işlenmektedir. Verilerin büyük boyutlara ulaşması sonucunda ise uygulanan her işlemin izleri tutulmaya başlanmış ve bu izlerin takibi ise SIEM uygulaması ile birlikte kolay hale getirilmiştir. SIEM ile, log olarak adlandırılan (Miller, 2011) iz kayıtları anlamlı hale getirilmekte ve anlamlı hale getirilen veriler ile birlikte bilgi sistemlerindeki her hareketin takip edilmesi kolaylaştırılmaktadır. Hareketlerin içerisindeki anomalilerin tespit edilmesine yönelik korelasyon kuralları oluşturularak olayların tespit edilebilmesi ve bu tespitler sonucunda aksiyon alınabilmesi (active response) sağlanmaktadır (Akbaş, 2017). Bu tespitlerdeki en önemli faktörler ise olayların yanlış-gerçek (false-positive) olmaması ve gerçek veya gerçeğe yakın zamanlarda tespit edilerek hızlı bir şekilde aksiyon alınabilmesini sağlamaktır. Bu noktada Güvenlik düzenleme, otomasyon ve yanıt (SOAR) teknolojisi devreye girmektedir (Brooks, 2018). SOAR problemlerin hızlı koordine edilmesine ve tek bir platformda otomatik olarak çözülmesine yardımcı olur.

LOG YÖNETİMİ VE SIEM

Log yönetimi kapsamında loglar merkezi uygulamalar içerisinde toplanarak saklanmakta ve istatistiksel veriler ile gösterge haline getirilerek analiz işlemleri yapılabilmektedir. SIEM (Security Information and Event Management), bilgi güvenliği ve olay yönetimi kapsamında log yönetiminde olduğu gibi her çözümün ürettiği loglar ile beslenerek, logların anlamlı hale getirilmesini (Bayraktaroğlu, 2009), sınıflandırılarak anomalilerin tespit edilebilmesini ve oluşan anomaliler sonucunda aksiyon alınabilmesini sağlamaktadır (Arslan & Özbilgin, 2017).

[1] Dr. Öğr. Üyesi, İstanbul Teknik Üniversitesi, Bilişim Enstitüsü, nafiz.unlu@gmail.com

SIEM'İN GELİŞME SÜRECİ

1990'lı yıllarda Güvenlik Bilgi Yönetimi (SIM - Security Information Management) çözümleri ile birlikte log toplama işlemleri, Güvenlik Olay Yönetimleri (SEM - Security Event Management) çözümleri ile birlikte gerçek zamanlı görüntüleme ve korelasyon işlemleri gerçekleştirilmekteydi. 2000'li yıllara gelindiğinde, veriler büyümeye ve teknolojinin daha da gelişmesi ile birlikte Güvenlik Bilgi Yönetimleri'nin (SIM) ve Güvenlik Olay Yönetimleri'nin (SEM) ortak noktada birleştirilmesi ve sonrasında verilerin toplanması, işlenmesi, saklanması ve olay yönetimleri ile korelasyon işlemlerinin uygulanabileceği SIEM çözümü ortaya çıkmıştır. Teknolojinin daha da gelişmesi ile birlikte yapay zekâ ve makine öğrenme süreçleri SIEM'e dâhil edilerek yeni nesil (Next-Gen SIEM) SIEM çözümleri ortaya çıkarılmış ve yapay zekâ ve makine öğrenmesi ile daha uzun vadeli anomalilerin de tespit edilebilmesi sağlanmıştır (Şekil 1) (Podzins & Romanovs, 2019).

Şekil 1. SIEM Gelişim Süreci (Podzins & Romanovs, 2019).

LOG YAŞAM DÖNGÜSÜ

SIEM çözümlerinin bir log satırı ile uyguladığı döngü logların toplanması ve yönlendirilmesi (Collect) ile başlamaktadır. Logların toplanmasının ardından SIEM, ilgili logları hazırlanan ayrıştırıcılar yardımıyla ayrıştırıp (Parse) normalize etmekte ve bir log satırının farklı alanlar içerisinde anlamlı hale getirilmesini sağlamaktadır. Ayrıştırılan log satırları türlerine göre sınıflandırılmakta (Taxonomoy) ve ardından korelasyon (Correlate) işlemlerine tabi tutulup alarm oluşturulmaktadır (Hassanzadeh & Burkett, 2018). Oluşturulan alarmlar sonucunda alarm içeriğindeki bilgiler yardımıyla aksiyon (Active Response) alınabilmektedir (Şekil 2).

Şekil 2. Log Yaşam Döngüsü

SIEM VE KORELASYON

SIEM çözümlerini, log yönetimi çözümlerinden ayıran en belirgin özellik korelasyon özelliğinin bulunması, diğer bir deyişle ilişkilendirme yapılabilmesidir. Bu özellik sayesinde, farklı olaylar arasında gerçek veya gerçeğe yakın zamanlarda ilişkilendirmeler yapılarak alarmlar oluşturulabilmekte ve bu olaylar sonucunda çözüme yönelik aksiyon alınabilmektedir. SIEM sunucularında toplanan loglar, normalize edilerek anlamlı hale getirilmekte ve sınıflandırma işlemi gerçekleştirilerek farklı olayların kategorize edilmesi sağlanmaktadır. Bu işlemlerin ardından, log içeriklerine ait alanlara şartlar girilerek korelasyon kuralları oluşturulabilmektedir. Senaryolara göre tek veya birden fazla kurallı, daha uzun vadeli süreçlerin takip edilmesi için aktif liste ve olayların oluşmasının ardından aksiyon alma işlemleri gerçekleştirilebilmektedir (Sekharan & Kandasamy, 2017).

Tek Kurallı Korelasyonlar

Bu kural türleri ile birlikte aynı çözüm veya log kaynakları üzerindeki olayların tespit edilmesine yönelik tek kurallı tanımlar yapılabilmekte ve bu tanımlar sonucunda olayların gerçekleşmesi ile alarm oluşturulmaktadır. Tek kurallı korelasyonlara aşağıdaki örnekler verilebilir:

- Mesai saati dışında güvenlik duvarı politikası değiştirilmesi (Firewall)
- SQL Injection tespit edilmesi (WAF)
- Zararlı bir dosya tespit edilmesi (Anti Virüs)

Birden Fazla Kurallı Korelasyonlar

Bu kural türleri ile birlikte aynı log kaynağı veya farklı log kaynakları arasında farklı alanlara yönelik şart veya şartlar girilerek ilişkilendirme yapılması ile alarm oluşturulması sağlanmaktadır. Birden fazla kurallı korelasyonlara aşağıdaki örnekler verilebilir:

- Port taraması sonrasında (Firewall), port taraması yapan IP/IP'ler X dakika içerisinde herhangi bir sisteme başarılı bir oturum açma girişiminde bulunması (Authentication)

- Aktif dizinde yerel bir kullanıcı oluşturulup (Active Directory), ilgili kullanıcının admin grubuna eklenmesi (Active Directory)

Aktif Liste Bazlı Korelasyonlar

Bu kural türleri ile birlikte loglardaki istenilen alanlara özgü olacak şekilde dinamik bir listenin tutulması ve bu dinamik listenin farklı kaynaklar üzerinde yeniden ilişkilendirilmesi sağlanmaktadır. Aktif liste bazlı korelasyonlara aşağıdaki örnekler verilebilir:

- Sanal makine yöneticisinin domainde oturum açmaması, ancak sanal makine üzerindeki makinenin kapatılması
- Son N saat içerisinde X MB upload trafiğinde bulunan kullanıcıların tespit edilmesi

Aksiyon Alma Bazlı Korelasyonlar

Tek kaynak veya farklı kaynaklarda yapılacak ilişkilendirme sonucunda log içeriğine göre veya logdan bağımsız bir şekilde karşı makinelerde aksiyon alınması sağlanmaktadır.

Aksiyon alma bazlı korelasyonlara aşağıdaki örnekler verilebilir:

- İç ağdaki kaynağın kara listedeki X farklı IP adresine Y defa veya kara listedeki A farklı URL adresine B defa erişim isteğinde bulunmasının ardından ilgili kaynağın güvenlik duvarından engellenmesi
- Dış ağdaki kaynağın N dakika içerisinde X farklı IP adresine RDP isteğinde bulunmasının ardından ilgili IP adresinin güvenlik duvarından engellenmesi
- Yetkili kullanıcı dışında dosya silme teşebbüsünün ardından domainden ilgili kullanıcının pasif edilmesi

KORELASYON TESPİT YÖNTEMLERİ

SIEM'de korelasyon kurallarının tespit edilmesine ve olayların gerçek veya gerçeğe yakın bir zamanda tespit edilmesine yönelik sorgu ve hafızada kullanım (in-memory) yöntemleri kullanılmaktadır.

Sorgu ile Alarm Tespiti

Korelasyon kurallarındaki şartların sorgu yöntemi ile kontrol edilmesi sürecinde, gelen loglar içerisinde ilişkilendirme yapılabilmesi için her gelen logda

girilen şartlar tek tek dosyadan okunarak veya API yardımıyla sorgu yapılarak kontrol edilebilmektedir. Çok yoğun olmayan sistemlerde veya çok yoğun olan ancak tek şartlı kuralların bulunduğu sistemlerde bu yöntem kullanılabilmektedir. Büyük verilerin işlendiği yoğun olan sistemlerde verinin artması ile birlikte birden fazla kurallı korelasyon tespitinde performans kaybı yaşanmaktadır. Bu kayıp ile birlikte alarmların gerçek veya gerçeğe yakın zamanda tespit edilebilmesi zorlaşmakta ve korelasyon özelliğinden verimli bir şekilde yararlanılamamaktadır.

Hafızada Kullanım (in-memory) ile Alarm Tespiti

Korelasyon kurallarındaki şartların hafızada kullanım (in-memory) yöntemi ile kontrol edilmesi sürecinde, gelen her bir log satırı işlendikten sonra aynı zamanda hafızaya yazılmaktadır. Hafızaya yazılan log satırları disklerden yapılan okumaya göre daha verimli sonuç vermekte ve tek kurallı veya birden fazla kurallı korelasyonlarda gerçek veya gerçeğe yakın bir şekilde tespit yapılarak alarm oluşturulabilmektedir. Ancak, verilerin çok daha büyük olduğu sistemlerde büyük hafıza değerlerine ihtiyaç duyulmaktadır. Sistemlerdeki hafıza miktarları arttırılarak ihtiyaç duyulan performansa erişilebilir ve gerçek veya gerçeğe yakın zamanda çok daha büyük verilerin bulunduğu sistemlerde de alarmların tespit edilmesi sağlanabilmektedir.

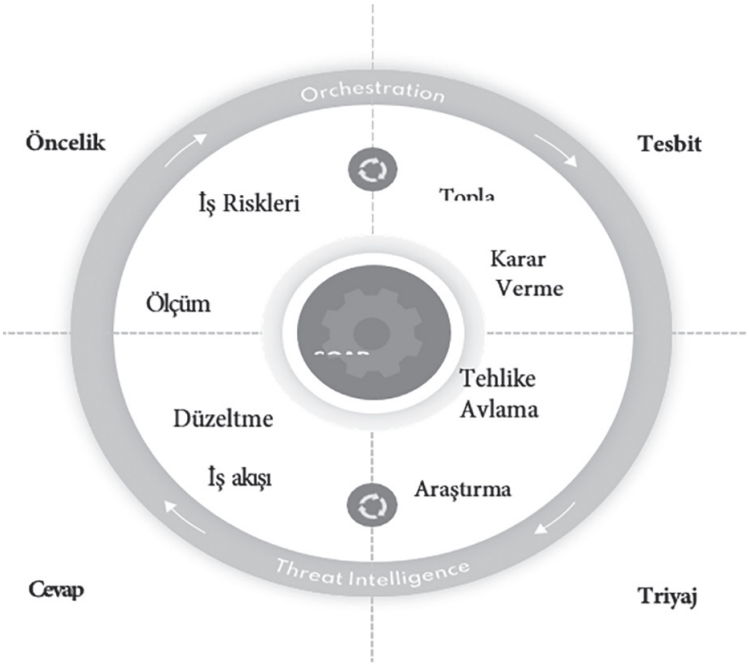
SOAR NEDİR?

Güvenlik düzenleme, otomasyon ve yanıt (SOAR) teknolojisi, çeşitli kişiler ve araçlar arasındaki görevlerin tek bir platformda koordine edilmesine, yürütülmesine ve otomatikleştirilmesine yardımcı olur (Şekil. 3) (Nugraha, 2021). Bu, kuruluşların yalnızca siber güvenlik saldırılarına hızlı bir şekilde yanıt vermelerine değil, aynı zamanda gelecekteki olayları gözlemlemelerine, anlamalarına ve önlemelerine, böylece genel güvenlik duruşlarını iyileştirmelerine olanak tanır (Gönüllü ve ark., 2022).

Gartner tarafından tanımlanan kapsamlı bir SOAR ürünü (Kavanagh ve ark., 2015) üç ana yazılım yeteneği altında çalışacak şekilde tasarlanmıştır:

- Tehdit ve güvenlik açığı yönetimi
- Güvenlik olayına müdahale ve
- Güvenlik operasyonları otomasyonu

Tehdit ve güvenlik açığı yönetimi (düzenleme), siber tehditleri değiştirmeye yardımcı olan teknolojileri kapsarken, güvenlik operasyonları otomasyonu (otomasyon), operasyonlar içinde otomasyon ve düzenlemeyi sağlayan teknolojilerle ilgilidir.



Şekil 3. SOAR İşlevi (Gönüllü ve ark., 2022)

SOAR'IN TEMEL ÖZELLİKLERİ

Otomasyon

Güvenlik otomasyonu, herhangi bir insan müdahalesi olmaksızın otomatikleştirilmiş önleme, tespit, araştırma, önceliklendirme ve müdahale süreçlerini ifade eder. Botlar ve playbook'ların yardımıyla ve ağdaki güvenlik ve güvenlik dışı cihazların kullanıma hazır entegrasyonları sayesinde iş akışlarını kolayca otomatikleştirebilirsiniz. Bu otomasyonlar, algılama ve yanıt verme ortalama süresini kısaltarak kuruluşun IR kapasitesini artırır.

SOAR, güvenlik personeli için işin çoğunu yapar, bu nedenle artık gelen her uyarıyı ayıklamak ve manuel olarak ele almak zorunda kalmazlar.

Güvenlik otomasyonu şunları yapabilir:

- Ortamınızdaki tehditleri tespit eder.
- Olayı araştırmak ve gerçek bir olay olup olmadığını tesbit etmek için güvenlik analistleri tarafından atılan adımları, talimatları ve karar verme iş akışını takip ederek olası tehditleri önceliklendirir.
- Olayla ilgili işlem yapılıp yapılmayacağını belirler.
- Sorunu listeler ve çözer.

Tüm bunlar, insan personelinin müdahalesi olmadan saniyeler içinde gerçekleşebilir. Daha önemli, katma değerli işlere odaklanabilmeleri için tekrarlayan, zaman alıcı eylemler güvenlik analistlerinin elinden alınır.

ORKESTRASYON

Güvenlik Orkestrasyonu, etkin ve güçlü siber güvenlik operasyonları ve siber olaylara hatasız müdahale için güvenlik odaklı olsun ya da olmasın tüm araç, ekip ve süreçlerin birbirine bağlanması yöntemidir. Güvenlik düzenlemesi, insanların, süreçlerin ve teknolojinin uyumlu çalışmasıdır.

Güvenlik düzenlemesi, karmaşık bir altyapı genelinde birbirine bağlı bir dizi güvenlik eyleminin makine tabanlı koordinasyonudur. Ürünler ve iş akışları genelinde görevleri otomatikleştirirken tüm güvenlik araçlarınızın ve hatta güvenlikle ilgili olmayan araçların uyum içinde çalışmasını sağlar.

SOAR, olay araştırmasını, yanıtını ve nihayetinde çözümü koordine eder. Ek olarak, güvenlik analistlerinin birden fazla ekran ve sistemde gezinme ihtiyacını ortadan kaldırarak, her şeyi tek bir yerde derleyip tek bir gösterge panosunda görüntülüyor.

Güvenlik düzenlemesi şunları yapabilir:

- Güvenlik olaylarının birbiriyle olan bağlantısını sağlar. Bir güvenlik düzenleme aracı, daha derin bir öngörü sunmak için farklı kaynaklardan gelen verileri toplar. Bu şekilde, tüm ortamın kapsamlı bir görünümünü elde eder
- Daha derin, daha anlamlı araştırmalara izin verir. Güvenlik analistleri, uyarıları yönetmeyi durdurabilir ve bu olayların neden meydana geldiğini araştırmaya başlayabilir. Ek olarak, güvenlik düzenleme araçları genellikle son derece etkileşimli ve sezgisel panolar, grafikler ve zaman çizelgeleri sunar ve bu görseller araştırma sürecinde oldukça faydalı olabilir.

- İşbirliğini geliştirir. Farklı katmanlardaki analistler, yöneticiler, CTO ve C-suite yöneticileri, hukuk ekipleri ve İK dahil olmak üzere ek tarafların da belirli türde güvenlik olaylarıyla ilgilenmesi gerekebilir. Güvenlik düzenlemesi, gerekli tüm verileri herkesin parmaklarının ucuna getirerek işbirliğini, problem çözmeyi ve çözümü daha etkili hale getirebilir.

Sonuç olarak, orkestrasyon, savunmalarınızın entegrasyonunu artırarak güvenlik ekibinin karmaşık süreçleri otomatikleştirmesine ve güvenlik personelinin, süreçlerinizden ve araçlarınızdan aldığınız değeri en üst düzeye çıkarmasına olanak tanır.

OLAY MÜDAHALESİ

Güvenlik ekipleri günlerinin çoğunu olayları araştırmak ve bunlara yanıt vermekle geçirir. Bu, olay müdahale süreçlerinin standartlaştırılmasına veya olay müdahale kalitesinin artmasına izin vermez. Olay Müdahalesi, güvenlik olaylarınızın yaşam döngüsünü analizden sınırlamaya, ortadan kaldırmaya ve kurtarmaya kadar yönetmenize olanak tanır.

PLAYBOOK

Playbook askeri jargonda bir harekata veya operasyona ilişkin yapılacak faaliyet planlarının bir araya getirildiği kitapçığa verilen isimdir. Benzer şekilde spor müsabakalarında teknik direktörler veya oyun kurucular tarafından da kullanılan planlar bütününe de Playbook ismi veriliyor (Purujoki, 2020).

SOAR Playbook'lar, kontrol listelerinin titizliğini ve tekrarlanabilirliğini olay müdahalesine getirerek araştırmaların kalitesini iyileştirir. Tek bir cam bölmesinden müdahale eylemlerini düzenleyerek ve otomatikleştirerek olay müdahalesinin hızını artırırlar. SOAR Playbook lar, kopyala yapıştır, alt sekme ve döner sandalyeyi ortadan kaldırarak, SOC analistinin iş yükünden tekrarlayan ve manuel görevleri önemli ölçüde azaltır, stres seviyelerini azaltır ve onları daha üretken hale getirir.

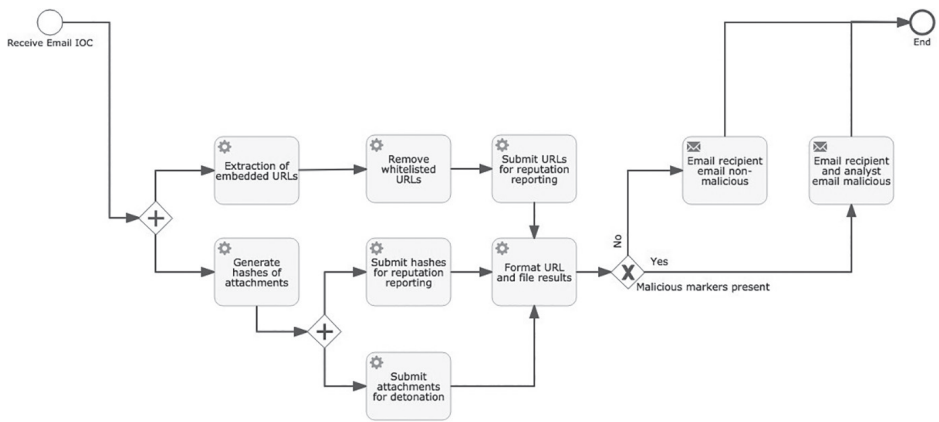
Playbook lar SOAR başarısı için çok önemlidir. Önceden oluşturulmuş veya özelleştirilmiş playbook, önceden tanımlanmış otomatik eylemlerdir. Karmaşık eylemleri tamamlamak için birden fazla SOAR playbook bağlanabilir. Örneğin, bir çalışan e-postasında kötü niyetli bir Tekdüzen Kaynak Konum Belirleyici (URL) bulunursa ve bir tarama sırasında tanımlanırsa, e-postayı engelleyen, çalışanı olası kimlik avı girişimi konusunda uyaran ve gönderenin adresi İnter-

net Protokolünü (IP) engelleme listeleri oluşturan bir playbook oluşturulabilir.. SOAR araçları, gerekirse güvenlik ekipleri tarafından takip eden soruşturma eylemlerini de tetikleyebilir. Kimlik avı örneği açısından, takip, benzer e-postalar için diğer çalışanların gelen kutularını aramayı ve bulunursa bu e-postaları ve IP adreslerini engellemeyi içerebilir.

SOAR PLAYBOOK'LARINA NEDEN İHTİYAÇ DUYULUR?

SOAR Playbook, güvenlik ekiplerinin zaman alan süreçleri hızlandırmasını ve düzenlemesini sağlar. Güvenlik araçlarını entegre etme ve sorunsuz özelleştirilebilir iş akışları oluşturma yetenekleriyle donatılmış bu Playbook'lar, güvenlik ekiplerinin sıradan ve tekrarlayan görevleri otomatikleştirmesine olanak tanırken, insan analistlerini insan zekasına ve karar vermeye bağlı daha önemli görevler için serbest bırakır. Günümüzde modern güvenlik taktikleri, son derece kritik güvenlik durumları için insan karar verme sürecini otomasyonla entegre etmelerini sağlayan "tutulabilir" özelliklerle birlikte gelir. Bu sayede genel güvenlik operasyonlarında önemli üretkenlik kazanımlarının ortaya çıkması ve zaman tasarrufunun maksimum seviyeye çıkması ile güvenlik ekipleri konforlu bir çalışmaya geçme imkânını yakalamış olurlar.

Burada önemli olan bir başka nokta da bir çok planın bir arada olması ve bu planların zaman zaman birbirinin devamı bazen de birbirinin alternatifi olarak bir araya getirilmesidir. Bu planlar genellikle birbirine bağlı olayların sonuçlarına göre uygulanacak şekilde hazırlanır (Singh, 2020). Aşağıda bir örnek (Şekil 4) playbook görüyoruz. Bu temel yapıyı açıklar.



Şekil 4. IOC İçeren Mail İnceleme Süreci (Singh, 2020)

SOAR'daki playbook'ların temel yapı taşı aslında iş akışlarıdır (workflow). Playbook'lar iş akışlarından veya diğer playbook'lardan oluşur. Bazıları sadece SIEM ile tespit edilen bir kullanıcının Microsoft AD'de yapmış olduğu oturum açma hareketlerini sorgulayıp, listelemesini sağlayan tek aşamalı işlerken, gelen tüm epostalar içerisindeki dosya ve url'leri sorgulayıp temiz olanları geçirmesini, geri kalanları IoC olarak ekleyip diğer ürünler ile taramasını yapıp sonuçların listelenmesini sağlayan ve onlarca aşamadan oluşan işler de olabilir.

Kurumların veya şirketlerin Güvenlik ile ilgili SOAR çözümleri (Orkestrasyon, Otomasyon ve Müdahale), Güvenlik takımlarının kritik ve BT süreçlerini güvenlik bakış açısıyla performanslarının artırılmasına ileri seviyede yardımcı olmaktadır.

Bu performans başarısı, SOAR çözümlerinin temel bir yeteneği olan playbooklar yardımıyla elde edilir. Playbook'lar bugün son kullanıcılar tarafından SOAR'ların alınmasına neden olan en önemli içeriktir.

SOAR'ı bir kuruluşun Siber Güvenlik Operasyonları Merkezine alarak kurmak, görevleri otomatikleştirerek, birden çok güvenlik cihazından gelen uyarıları koordine ederek ve olay müdahalesi için playbook sağlayarak genel güvenlik verimliliğini ve etkinliğini artırabilir. SOAR çözümleri, herhangi bir manuel müdahale olmaksızın farklı türden tehditlere yanıtları otomatikleştirmek için çeşitli playbooklardan yararlanmaktadır (Purujoki, 2020).

SOAR playbooklarını kullanan SGOM ekipleri, aşağıdaki görevleri yapabilirler:

- Uyarıları yönetebilir,
- Farklı olay türleri için otomatik yanıtlar oluşturabilir ve sorunları daha etkili ve tutarlı bir şekilde hızla çözebilir,
- Bu playbooklar ayrıca otomatik olay incelemesini yapabilirler,
- Tehdit istihbaratını çeşitlendirmeyi, kötü niyetli risk göstergelerinin (IOC'ler) engellenmesi gibi olay eylemlerini SIEM, Firewall, Threat Intelligence Platformlar üzerinde, gerçekleştirebilir ve aksiyonu kendiliğinden alabilir.

SOAR PLAYBOOK USE CASE'LER

Tehdit istihbaratı otomasyonu: Tehdit istihbaratı çeşitlendirme, farklıi bir olay veya tehdit soruşturma sürecinin önemli bir tarafını oluşturur. Bu çeşitlendirme süreci, false positive olarak ifade edilen yanlış tetiklenen olayları ortadan kal-

dırır ve diğer güvenlik operasyonları için eyleme geçirilebilir olarak istihbarat toplamaktadır. SOAR playbookları, dış ve iç istihbarat kaynaklarından IOC'leri otomatik olarak alır, normalleştirir ve toplanan IOC'leri zenginleştirir. çeşitlendirme sürecinin ardından playbooklar, bilgiyi otomatik olarak puanlayabilir ve sonraki yanıt adımlarına öncelik verebilir (Singh, 2020).

Otomatik olay müdahale: Gelişmiş tehdit bağlamsallaştırma, analiz ve SOAR playbookları ile SGOM ekipleri, tüm güvenlik tehditlerine ve olaylarına entelektüel yanıtlar verebilir. SOAR playbookları, güvenlik ekiplerinin tehditleri makine hızında tespit etmek, analiz etmek, çeşitlendirmek ve bunlara yanıt vermek için otomasyonun etkinliğinden, hızından ve gücünden yararlanmasına olanak verir. SOAR playbooklar ayrıca Firewall, EDR, SIEM ve diğer araçlarda tehdit göstergelerini (IOC'ler) engellemek için de kullanılabilir.

Güvenlik açığı yönetimi: SOAR playbooklar, SGOM ekiplerinin yamaları otomatik olarak uygulayarak veya planlayarak güvenlik açıklarına hızla anında yanıt vermesine olanak tanır. SOAR playbooklar, SGOM ekiplerinin tüm mevcut güvenlik açıklarından haberdar olmalarını ve uygun risk azaltma önlemlerini almak için her güvenlik açığının potansiyel riskini başarıyla değerlendirmelerini sağlamak için de kullanılabilir. Takımlara bilgi sağlamanın yanı sıra, SOAR playbooklar bir veri tabanını, varlık bilgileri için aktif dizinleri veya güvenlik açıkları hakkında ek bilgi toplamak için olaylar için EDR araçlarını sorgulamak için kullanılabilir.

Gelişmiş tehdit avcılığı: Sürekli ortaya çıkan yeni güvenlik açıkları ve saldırılarla, tehdit avcılığı yalnızca bir zorluk değil, bir öncelik haline geliyor. SOAR playbookları kullanan güvenlik ekipleri, şüpheli alanları, kötü amaçlı yazılımları ve diğer göstergeleri belirlemek için tehdit avlama süreçlerini otomatikleştirebilir, avlanma sürecini hızlandırabilir ve kritik zorlukların üstesinden gelmek için kendilerini serbest bırakabilir. SOAR playbooklar yardımıyla, SGOM ekipleri uyarı yorgunluğunun ötesine geçerek olayların oluşup karşılaşılma anından önce yanıt verebilir.

Phishing mail incelemeleri: Phishing, veri ihlalleri için en önemli saldırı vektörlerinden biri olmuştur. SOAR playbooklarıyla, SGOM ekiplerinin hassas bilgiler için her URL'yi, eki veya şüpheli talebi manuel olarak araştırması gerekmez.

SOAR playbookları kullanılarak otomatikleştirilebilir ve güvenlik ekiplerinin kötü amaçlı içeriği azaltmaya odaklanmasına ve çalışanları kimlik avı uygulamaları konusunda eğitmesine olanak tanımaktadır.

SOAR'A NEDEN İHTİYAÇ DUYULUR?

SOAR platformu, güvenlik ekiplerinin manuel müdahale olmaksızın güvenlik operasyonlarını kendi başlarına yürütmesini sağlar. Güvenlik operasyonlarında otomasyonun kapsamı bir operasyondan diğerine farklılık göstermektedir. Bazen manuel bir iş akışıyla tek bir otomatik adım olabilir veya güvenlik personelinin incelemeden sonra onaylamasını gerektiren otomatik bir iş akışı olabilir. SOAR platformları, güvenlik ekiplerinin bir olay müdahale süreci sırasında çeşitli düzeylerde otomasyon uygulamasına olanak tanır. Güvenlik olarak operasyonlar resmileşir ve olgunlaşır, otomasyonun kapsamı daha sonra artar. Otomasyon olmadan, bir güvenlik ekibi uyarılarla bireysel olarak ilgilenir. Bu, belirli uyarıların daha önce bir süre bekleyeceği anlamına gelir. Bu bekleme süresi nedeniyle kritik uyarılar kaçırılırsa, bir kuruluş olumlu bir şekilde sonuçlanmayabilir (Hafiz & Soewito, 2022).

İşte burada SOAR, güvenlik ekibinin daha önemli işlere odaklanabilmesi için tekrarlayan, sıradan eylemlerin çoğunu hafifleterek büyük bir fark yaratabilir.

Ek olarak, bir SOAR aracı veri toplayabilir ve analistlerin olayları değerlendirmesini ve bunları düzeltmek için doğru eylemleri gerçekleştirmesini kolaylaştıran öneriler sunabilir.

Genel olarak SOAR aşağıdaki nedenlerle güvenlik çözümlerinin ana halkasını oluşturur;

- Tekrarlayan, basit ama zaman alan görevleri otomatize etmek
- Olay tespit ve müdahale sürelerini kısaltmak
- Güvenlik uzmanlarının verimliliğini arttırmak
- Tehdit yaşam döngüsünü uçtan uca kontrol altına almak

SIEM İLE SOAR ARASINDAKİ FARKLAR NELERDİR? SOAR, SIEM İLE NASIL UYUM SAĞLAR?

Bilgi Yönetimleri'nin (SIM) ve Güvenlik Olay Yönetimleri'nin (SEM) ortak noktada birleştirilmesi ve sonrasında verilerin toplanması, işlenmesi, saklanması ve olay yönetimleri ile korelasyon işlemlerinin uygulanabileceği SIEM ve Güvenlik düzenleme, otomasyon ve yanıt (SOAR) teknolojisi, bir güvenlik operasyon merkezinin (SOC) ayrılmaz araçlarıdır ve olay yönetimi ve müdahalesine yardımcı olurlar. SIEM, tehditleri tespit etmek için birden fazla kaynaktan gelen günlükleri analiz etmeyi içerirken, SOAR, birkaç bilgi parçasını düzenlemek ve

yanıtı otomatikleştirmekle ilgilidir. Bu iki yaklaşım arasındaki farkları anlamak ve yorumlamak çok önemlidir çünkü her ikisi de bir güvenlik analistine yardımcı olmak için gereklidir.

SOAR ÇÖZÜMÜ VE SIEM İLE ENTEGRASYONU

SIEM ve SOAR (güvenlik düzenlemesi, otomasyonu ve yanıtı) genellikle birleştirilir çünkü yetenekleri birbirini tamamlar. Her iki teknoloji de büyük güvenlik operasyonları (SecOps) ekipleri tarafından SOC'lerini geliştirmek için kullanılır.

- Olay keşfinden çözüme kadar geçen süreyi azaltma
- Güvenlik olaylarını belirlemek için uyarı ve raporlama verilerini kullanır.
- Analistlerin bir olayı daha fazla araştırması için gereken verileri kullanır
- Verileri sorgulamaya ve keşfetmeye dayanan proaktif olay müdahalesi ve tehdit avlama konusunda analistlere yardımcı olur.
- Güvenlik olaylarından kaynaklanan risklerin en aza indirilmesini sağlar.
- Yanıt süreçlerinin kolay görselleştirilmesine izin verir.
- Belirli tehditlere otomatik olarak yanıt verilmesini sağlayan önceden tanımlanmış playbook'lar otomatik olarak başlatılabilir (Nugraha, 2021).
- SOC operasyonlarının genel etkinliğini ve verimliliğini artırır.
- Mevcut güvenlik teknolojileri için yatırım getirisini artırır.

SIEM araçlarını bir SOAR çözümüyle entegre etmek, güvenlik ekiplerinin etkili bir şekilde yanıt verebileceği daha güvenilir ve anlamlı uyarılar üretmek, verimli ve duyarlı bir güvenlik çözümü oluşturmak için her birinin gücünü birleştirir.

SOAR VE SIEM İN BİRLİKTE ÇALIŞMASI

Güvenlikte olay müdahalede, SIEM aracından alınan bilgiler ile aşağıdaki listelendiği gibi genel özelliklerdir;

Koleksiyon: olaylar çeşitli protokoller kullanılarak alınır (González-Granadillo ve ark, 2021).

Ayrıştırma: Olaylar bölünür ve alanlara girilir.

Zenginleştirme: Olaylara bağlamsal bilgiler eklenir.

İndeksleme: Olaylar veritabanında saklanır.

Korelasyon: Benzer olaylar birbirine bağlanır ve analiz edilir.

Doğrulama: Olay ayrıntıları birden çok kaynakta kontrol edilir.

Yanıt: Bir tehdide karşı koymak için işlem yapılır.

SONUÇ

Son yıllarda teknolojinin gelişmesi ve verilerin dijital ortamlarda işlenmesi sebebiyle SIEM'e olan ihtiyaç da giderek artmaktadır. İnsan gözlemi ile tespit edilemeyen büyük verilerin bulunduğu sistemlerdeki olayların, SIEM ile erken tespit edilebilmesine ve tespit sonrasında çözüme yönelik işlemlerin uygulanabilmesi konusunda kolaylık sağlanmaktadır. Ancak, günümüzdeki bazı saldırılar kısa vadeli olmamakla birlikte uzun vadeli gerçekleşmektedir. Çok daha uzun süreçte uygulanan saldırıların yakalanabilmesi adına yeni nesil SIEM çözümleri ile olaylardaki anomalilerin tespit edilebilmesi bu kapsamda önemli bir husus olarak karşımıza çıkmaktadır.

Bugün teknolojinin gelişen ve karmaşık yüzü siber tehditler nedeniyle, SIEM ortamları, SGOM analistlerine ağır iş yükleri ve yorgunluk yüklemektedir. SGOM analistleri güvenli çalışmak ve yüklerini azaltmak ve iş yoğunluğunu düşürmek adına ayrıca güvenlik otomasyonu sağlamak adına SOAR sistemleri ortaya çıkmıştır. SOAR sistemleri, siber tehdit algılama, azaltma ve SGOM analistlerini güçlendirmek üzere tasarlanmıştır.

Aynı zamanda SIEM verilerinin analizi, işlenmesi gelecek tehditlerin bertaraf edilmesi için SOAR çalışmasına ihtiyaç vardır. Otomatik olarak SOAR'a gelen veriler herhangi bir insan müdahalesi olmaksızın otomatikleştirilmiş önleme, tespit, araştırma, önceliklendirme ve müdahale süreçlerinden geçerek gerekli tedbirler alınarak tehlike yok edilir.

Birçok devlet kurumu, özel sektör Siber dünyada güvenliklerini sağlamak için log yönetimi gibi daha az gelişmiş teknolojileri sıkça kullanmaktadır. Bazıları ise bu loğları toplayarak SIEM'e entegre eder ve güvenliklerini SIEM üzerinden alırlar ve buna göre değişik güvenlik ürünleri üzerinden olaylara karşı eylem geliştirirler. SOAR teknolojisi ise bunların tamamını başka bir teknolojiye ihtiyaç duymadan tek başına yapar. Yakın zamanda birçok kurum ve kuruluş hala SOAR'a geçmeyi başaramamış olsalar dahi gelecekte tüm Siber Güvenlik saldırılarına karşı SOAR ile tedbir alacaklar ve bu ise SOAR'ın gelişimini hızlandıracaktır.

Ancak bu, SOAR çözümlerinin genellikle SIEM çözümlerinden yararlandığı gerçeğini ihmal eder. Sonuçta, SIEM kritik günlükleri ve uyarı bilgilerini

toplar. Bununla birlikte SIEM olmasaydı, SOAR, kurumsal ağlara ilişkin hayati bir içgörü kaynağını kaybedecekti. Ayrıca SOAR, entegrasyon yoluyla çalışır ve SIEM'i uç nokta güvenliği ve kimlik yönetimi gibi diğer kritik siber güvenlik çözümlerine bağlar.

Bununla birlikte, SOAR'ın bir gün SIEM yeteneklerini kendi tekliflerine dâhil edip etmeyeceği belirsizliğini koruyor. Elbette, talepler değiştikçe yeni pazarlara dönüşmek için modern siber güvenlik çözümlerinin modelini takip ediyor. Siber güvenlik personeli krizi derinleştikçe otomasyonun önemi kesinlikle önemlidir.

KAYNAKLAR

Akbaş, E. (2017). *Bilgi güvenliği ve log yönetimi sistemlerinin analizi.* http://www. academia. edu/9203287/Bilgi_G% C3% BCvenli% C4% 9Fi _ve_Log_Y% C3% B6netimi_Sistemlerinin_Analizi) (Erişim Tarihi: Ekim 2017).

Arslan, I., & Ozbilgin, I. G. , (2017). *Virtualization and security: examination of a virtualization platform structure*. 2017 International Conference on Computer Science and Engineering (UBMK) (pp.221-226). Antalya, Turkey

Bayraktaroğlu, E. (2009). *Bilgi sistemlerinde log yönetimi ve logların değerlendirilmesi.* Doktora Tezi, Fen Bilimleri Enstitüsü. Bahçeşehir Üniversitesi.

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): analysis, trends and usage in critical infrastructures. *Sensors*, 21(14), 4759.

Gönüllü M.A., Benzer, R., Tüfekçi, A. (2022). Bölüm 1: güvenlik orkestrasyon, otomasyon ve olaylara müdahale (SOAR) Benzer, R. (Ed.): *Yönetim Bilişim Sistemleri & Siber Güvenlik.* Akademisyen Kitabevi, Ankara.

Hafiz, M. & Soewito, B. (2022). Information security systems design using SIEM, SOAR and Honeypot. *Jurnal Pendidikan Tambusai*, 6(2), 15527-15541.

Hassanzadeh, A. & Burkett, R. (2018). SAMIIT: Spiral attack model in IIoT mapping security alerts to attack life cycle phases. *In 5th International Symposium for ICS & SCADA Cyber Security Research,* (pp. 11-20). University of Hamburg, Germany.

Kavanagh, K. M., Rochford, O., & Bussa, T. (2015). *Magic quadrant for security information and event management*. Gartner Group Research Note.

Miller, D. R. (2011). *Security information and event management (SIEM) implementation*. McGraw-Hill Higher Education.

Nugraha, I. (2021). A review on the role of modern SOC in cybersecurity operations. *Int. J. Current Sci. Res. Rev.* 4(5), 408-414.

Nugraha, I. P. E. D. (2021). A review on the role of modern SOC in cybersecurity operations. *Int. J. Current Sci. Res. Rev*., 4(5), 408-414.

Purujoki, J. (2020). SOAR *Playbook implementation-incident deduplication and its effects.* Thesis. JAMK University of Applied Sciences.

Resmi Gazete (2007). *İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun*. Alıntı http://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm adresinden ulaşılmıştır

Sekharan, S. S. & Kandasamy, K. (2017, March). Profiling SIEM tools and correlation engines for security analytics. *In 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 22-23 March 2017, Chennai, India, (pp. 717-721). IEEE.

Singh, K. (2020). *Application of SIEM/UEBA/SOAR/SOC (Cyber SUSS) Concepts on MSCS 6560 computer lab*. Doctoral dissertation, Marquette University.