SIEM NEDİR AÇIK KAYNAK SIEM ÜRÜNLERİ

Bengü Çağla SARI

Adli Bilişim Mühendisliği, Teknoloji Fakültesi, Fırat Üniversitesi, Elazığ, Türkiye

ÖZET

İnternet teknolojilerinin kullanımının artması beraberinde birçok işlemi kolay bir şekilde yapılabilir hale getirdi. Bankalardan, çeşitli alışveriş sitelerinden, eğitim kurumlarından, devlet kurumlarından ve daha birçok alanlarda internet üzerinden işlemler hızlı yapılır hale geldi. Bu kolaylıklar bazen de kullanıcılardan kaynaklı zafiyetlerin oluşmasına neden oldu. Yetkisiz kullanıcılar tarafından yapılan siber saldırılardan ötürü maddi ve manevi kayıplar yaşandı. Yaşanan siber saldırıları tespit etmek ve önlemek için çeşitli araçlar kullanılmaya başlandı. Bunlardan birisi ise Siem'dir. Siem Security Information Event Management (Türkçe olarak Güvenlik Bilgileri ve Olay Yönetimi) kelimelerinin kısaltılmasıdır. Siem terimi 2005 yılında Mark Nicelett ve Amrit Williams of Gartner tarafından bulunmuştur. Siem ağ güvenlik cihazlarından bilgi toplama, analiz etme ve sunma ürün yeteneklerinden bazılarıdır. Bu çalışmada siem hakkında araştırma yapılmış olup çeşitli siem ürünleri incelenmiştir.

1.GİRİŞ

Siber saldırılarda bilişim teknolojileri sistemlerinde uygulamalardan ve donanımda herhangi bir boşluktan yararlanmaya çalışılır. Bu sebeple ağ güvenliğine yönelik tehditler hızla yayılmakta ve her geçen gün yenileri çıkmaktadır. Saldırıları önlemek ve bunlarla mücadele etmek için temel güvenlik yaklaşımlarından biri güvenlik olaylarını gerçek zamanlı olarak belirlemek ve olaylara yanıt vermektir. Güvenlik bilgileri ve olay yönetimi yazılımı (SIEM) güvenlik uyarılarını gerçek zamanlı olarak takip edilmesini sağlar.

Siem sistemlerin ürettiği log(günlük) kayıtlarını toplar, saklar ve analiz eder. Log kayıtları bilgisayar sisteminde belirli olaylar meydana geldiğinde otomatik olarak üretilen dosyalardır. Log dosyaları genellikle zaman damgalıdır. İşletim sistemlerinde veya yazılım uygulamalarında arka planda gerçekleşen her şeyi pratik olarak kaydeder. Log kayıtlarının yönetimine Log Management(Günlük Yönetimi) denir. Log Management bilgisayar tarafından oluşturulan büyük hacimli günlük verilerini oluşturmak, toplamak, ayrıştırmak için kullanılan tüm faaliyetleri ve süreçleri tanımlayan terimdir.

Siem Güvenlik Bilgileri Yönetimi(SIM) ve Güvenlik Olay Yönetimi(SEM) bir araya getirir. Sim bilgisayar günlüklerinden güvenlikle ilgili verileri toplama, izleme ve analiz etme uygulamasıdır. Sim güvenlik duvarları, Proxy sunucuları, izinsiz giriş tespit sistemleri ve anti-virüs yazılımı gibi güvenlik cihazlarından olay günlüğü verilerinin toplanmasını otomatikleştiren bir yazılımdır. Bu veriler daha sonra ilişkili ve basitleştirilmiş biçimlere çevrilir.

Sem olayların kaydedilmesini ve değerlendirilmesini sağlar ve güvenlik veya sistem yöneticilerinin bilgi güvenliği mimarisini, politikalarını ve prosedürlerini analiz etmesine, ayarlamasına ve yönetmesine yardımcı olur.

Siem teknolojisi, güvenlik uyarılarının gerçek zamanlı analizini sağlar. Siem çözümleri ağ yapılanmasındaki hatalar, olası güvenlik tehditleri için saldırı eylemleri, kritik ağ kaynakları belirleme, mevcut tehditlere uygun güvenlik politikası belirlemeyi sağlar. Siem tüm verileri koruma araçlarından toplayan, farklı kaynaklardan gelen birçok günlük biçimini anlayabilen sistemdir. Siem yazılımı olayları kurallar ve analiz motorlarıyla inceleme, küresel olarak toplanan iletişimi kullanarak gelişmiş tehditleri tespit etme, analiz etme ve arama yapmak için kullanılır. Siem çözümleri günlük girişlerini ve güvenlik sistemlerinden gelen olayları eyleme geçirebilme, bilgiye dönüştürme için kurallar ve istatiksel korelasyon kullanır. Siem güvenlik ekiplerinin tehditleri gerçek zamanlı olarak tespit etmesine, olay yanıtını yönetmesine, geçmiş güvenlik olaylarıyla ilgili adli soruşturma yapmasına ve uyumluluk amacıyla denetimler hazırlamasına yardımcı olur.

Siem ürünleri birçok cihazdan log toplayabilir. Toplanan loglarda inceleme yaparak saldırı olabilecek olayların tespit edilmesi ve belli durumlar sonunda alarm üretilmesine korelasyon denir. Önceden tanımlı veya güvenlik ekibi

tarafından oluşturulan korelasyonlar, her türlü saldırı senaryosuna uygun olarak düzenlenebilir ve olayların önemine göre alarm oluşturulur. Farklı cihazlardan toplanan logların tek bir veri formatı haline getirilmesine normalizasyon işlemi denir. Kural olarak tanımlanan olay veya olaylar dizisi Siem kuralını tetiklerse, sistem güvenlik personelini bilgilendirir.

1.1 SIEM ÇALIŞMA MEKANİZMASI

Siem yazılımı çeşitli cihazlardan logları toplar. Topladığı logları sistemde kullanmak için ortak bir formata dönüştürür. Log kayıtlarındaki olayları saldırı tipine göre belli sınıflara ayırır. Analiz ettiği olayları birbiriyle bağlantılı hale getirme ve detaylandırarak ilişkilendirme işlemini yapar. Olaylarda bulduğu güvenlik tehdidi ve problemleri yetkili kişilere bildirir. Toplanan verileri ve sonuçlarını güvenlik uzmanlarına izleme için panel oluşturur. Toplanan verilerin analiz aşamalarını ve sonuçlarını kapsayan rapor oluşturur.

2.SIEM ÜRÜNLERİ NELERDİR?

Siem ürünleri, uygulamalar ve ağ donanımı tarafından oluşturulan güvenlik uyarılarının gerçek zamanlı analizini ve raporlamayı, güvenli olayları analizini sağlayarak ağlara yönelik en son tehditleri tespit edebilme imkânı sağlar.

2.1 EN ÇOK KULLANILAN SIEM YAZILIMLARI

Source: Gartner (June 2021)

Şekil 1:Gartner 2021 Haziran Siem Magic Quadrant

1-**Exabeam**:

Yeni nesil bir Siem olan Exabeam Fusion, tehditlerin tespiti, araştırılması ve müdahalesi için kullanılan bulut tabanlı bir çözümdür. Fusion Siem ilgili tüm olayları toplar ve yasal olmayanları ayırt ederek diğer siem araçları tarafından göz ardı edilen tehditleri tespit eder. Fusion Siem otomatikleştirilmiş olay yanıtı sağlayan SOAR(güvenlik düzenleme ve otomasyon) çözümüyle entegre çalışır. Bu sayede tehditler gerçek zamanlı ve otomatik olarak ele alınır. Bulut tabanlı, günlük depolama, hızlı, kolay arama, kapsamlı uyumluluk raporlaması özelliği vardır.[3]

2-**IBM Qradar SIEM**:

Olayları gerçek zamanlı olarak görüntülemeyi sağlar. Tehditlerin algılanmasını ve önceliklendirilmesini kolaylaştıran mimari kullanır. Sınırlı raporlama , yüksek maliyet, zayıf ueba(kullanıcı ve varlık davranış analizi, kullanıcı ve kimliklerin modellerini öğrenip profil analizi yapar[4]) bu siem ürününün dezavantajlarıdır.

3-**Securonix**:

Securonix Siem analitik odaklı UEBA motoru kullanır. Güçlü davranış ve veri izleme özellikleri vardır.[5] Bu Siem ürününün dezavantajı olarak Soar sistemde dahil değildir.

4-**Splunk**:

Splunk Siem uygulama ve ağ izleme kullanım durumlarını ele alır. Gerçek zamanlı bilgi sağlar, kullanıcı arayüzü kullanımı kolaydır. Kullanıcıların davranışlarına göre analiz yapar. Gelişmiş tehditleri ve teknikleri tespit etmede sınırlı yetenekleri vardır. Soar ile birlikte kullanılırsa yetenekleri artırılabilir.

5-**Rapid7**:

Insight IDR, Rapid7'nin sunduğu bir bulut Siem çözümüdür. Veri toplama ve arama için bulut tabanlı sistem kullanır. Kötü amaçlı yazılım, kimlik avı gibi tehditleri önceden tespit edebilir. Saldırganın davranış analizi sağlar. Log kayıtlarını ortak bir alandan yönetimini sağlar. Kullanıcıların yapmış oldukları etkinlikleri temel alır. Uç noktaların güvenliği için Insight Agent kullanır.

6-**LogRhyhtm**:

Yapay zeka ve log korelasyonunu birlikte kullanarak analiz yapar. Güvenlik tehditlerini otomatik olarak algılayamaz manuel olarak eklenmesi gerekir.

7-**Microsoft Azure Sentinel**:

Microsoft tarafından geliştirilmiş olan siem, sahip olduğu cihazları tek panelde birleştirmek isteyen kullanıcılar için tercih sebebidir. Veriler sorunsuz şekilde eklenebilir. Microsoft sistemler için uygundur diğer sistemleri desteklemez. Soar gibi diğer ürünlerle entegre özelliği yoktur.

8-**McAfee Enterprise Security Manager**:

McAfee Enterprise Security Manager, gelişmiş tehdit algılaması gerçekleştirmeye, uyumlulukla ilgili olayı yönetmeye ve gerçek zamanlı rapor oluşturmayı sağlar. Acil durumlarda senaryo oluşturmak için yeni kaynaklar sağlar. Birden çok kaynakta ağ trafiği günlük kayıtlarını toplar. Kaydedilen günlüklerden sadece en temel ögeleri sistemde tutar bir olay olduğunda günlüklerin yeniden toplanması gerekebilir. Oluşabilecek yeni tehditlere karşı güncelleme işlemi yapar.

9-**LogPoint**:

Logpoint uygulama olay yönetimi ve uygulama güvenliğini artıran bir siemdir. Log kayıtlarına dayalı depolama, arama, filtreleme, hata izleme ve rapor oluşturmayı kolaylaştırır. Karmaşık bir arayüz sistemine sahiptir.

10-**Elastic Stack**:

ELK stack, Elasticsearch, Logstash ve Kibana ile çalışan bir log izleme ve log yönetimi aracıdır. Log kayıtlarını gerektiği gibi arama ve filtreleme işlemlerini yapar. Log kayıtlarının tek bir yerde depolanmasını ve gerçek zamanlı olarak oluşturulmasını sağlar. Kibana ile grafikler aracılığı istatiksel görselleştirme sağlar. Bilişim sistemlerinde oluşan sorunları erken tespit etmek için kullanılır.

2.2 AÇIK KAYNAK SIEM ÜRÜNLERİ

1-**AlienVault OSSIM**:

Ossim varlık keşfi, izinsiz giriş tespiti, siem olay korelasyonu, güvenlik açığı değerlendirmesi, davranışsal izleme işlemlerini tek bir platformda birleştirmiştir.

2-**SIEM MONSTER**:

Birçok açık kaynak ürünlerini bir merkezde bir araya getirir, gerçek zamanlı tehdit incelemesi yaparak kullanıcıları saldırılara karşı korur. UEBA insan temelli davranışlara göre yanlış tahminleri en aza indirmeye çalışır. Siber saldırılara karşı derin öğrenme yöntemlerini kullanılır. Oluşabilecek saldırılara otomatik yanıt vermeyi sağlar.

3-**WAZUH**:

Wazuh tehdit algılama, log kayıtlarının bütününü izleme, uyumluluğunu sağlama ve olay yönetimi aracı olarak kullanılır. Sisteme yapılan izinsiz girişleri algılama, tehditleri belirleme, log kayıtlarındaki anormallikleri belirler. Log kayıtlarını toplar, indeksler ve analiz eder. Sistemdeki güvenlik açıklarını tespit eder. Bulut sistemlerin güvenliğini sağlar. Oluşabilecek saldırılara karşı olay müdahalesi yapar.

4-**ELK (ELASTIC STACK)**:

ELK Stack Elasticsearch, Logstash ve Kibana açık kaynaklı ürünlerden oluşur. ElasticSearch log kayıtlarından toplanan verilerin analizi ve arama işlemlerini yapmayı sağlayan bir arama motorudur.

Logstash toplanan verilerin indekslenip, işlendiği ve anlamlı hale getirildiği araçtır.

Kibana anlamlı hale gelen verilerinin görselleştirilip analizinin yapıldığı araçtır.

Beast Family toplanan logların işlenmesi gerekenleri logstash'e işlenmesine ihtiyaç duyulmayan kısmını elasticsearch'e yönlendirerek logların kibana üzerinde görünmesini sağlar.

5-**OSSEC**:

Ossec ana bilgisayar tabanlı bir saldırı tespit sistemidir. Günlük analizi, dosya bütünlüğü izleme, Windows kayıt defteri izleme, zararlı yazılım algılama, gerçek zamanlı uyarı sistemi Ossec yazılımın görevlerindendir.

6-**SNORT**:

Snort IP ağlarında gerçek zamanlı ağ trafiği analizinde saldırı tespit ve önleme sistemidir. Ağ tabanlı sistemler ağ üzerinde tüm trafiği tarar. Ağ akışları üzerinde gerçek zamanlı analiz yapar, sonuçları günlüğe kaydeder.

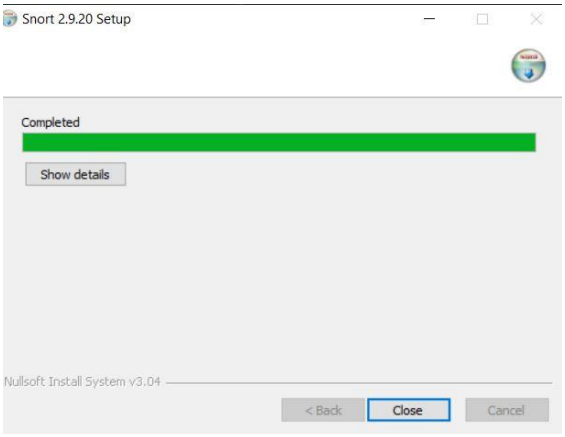
7-**MOZDEF**:

MozDef(The Mozilla Defense Platform) Mozilla tarafından geliştirilmiş ve Elasticsearch üzerinde bulunan açık kaynaklı yazılımdır. Çeşitli sistemlerden olayları ve günlükleri toplama, depolama ve yönetimini sağlar. Olayları ve günlüklerde arama yapar, anormal olay tespitinde uyarı oluşturur.

3.SNORT KURULUMU

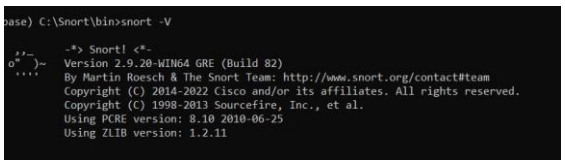
Snort, gerçek zamanlı ağ trafiği analizi ve veri paketi günlüğünü sağlayan açık kaynaklı saldırı tespit sistemi(IDS) ve saldırı önleme sistemidir(IPS). Sistemde olabilecek kötü amaçlı etkinlikleri tespit etmek için belirli kurallara göre inceleme yapar. Siber güvenlik uzmanları tarafından snort ile hizmet reddi(dos) ve ddos, arabellek taşmalarını ve gizli bağlantı noktalarını tespit eder.

Snort kurulumu için öncelikle setup dosyası kurulur.(“ https://www.snort.org/downloads/#rule-downloads”) Snort yazılımının çalışması için Npcap uygulaması kurulması gerekir. Npcap Windows için paket yakalama ve gönderme kitaplığıdır.



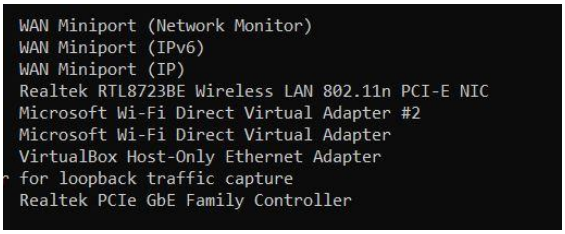
Şekil 2 : Snort setup kurulumu

Snort yazılımının versiyon bilgisi öğrenilir.



Şekil 3: Snort versiyon bilgisi öğrenme

Cmd ekranında snort –W yazılarak incelenen cihaza ait bağlı olan ve önceden bağlanmış olan kablosuz arayüz kartlarını gösterir.



Şekil 4: Snort kablosuz arayüz kartları

4. ÖRNEK SIEM KURALLARI

Warn if the servers the connection times out(Sunucular bağlantı zaman aşımına uğrarsa uyar.)

Warn if it logs into the server with an unregistered IP address(Sunucuya kayıtsız bir IP adresiyle giriş yaparsa uyar.)

Warn if the user makes three incorrect entries into the same machine within an hour(Kullanıcı bir saat içinde aynı makineye üç yanlış giriş yaparsa uyar.)

Warn if logging on to the server and machine after working hours(Çalışma saatlerinden sonra sunucuya ve makineye giriş yapılırsa uyar.)

Warn if there is a message in the Mail asking for password(Postada şifre isteyen bir mesaj varsa uyar)

KAYNAKÇA

[1] IBM. “What is SIEM” https://www.ibm.com/topics/siem

[2]Beyaz.Net. “Loglama ve Siem Nedir” https://www.beyaz.net/tr/guvenlik/makaleler/loglama_ve_siem_nedir.html

[3]Exabeam. “Best Siem Solutions” https://www.exabeam.com/explainers/siem/siem-solutions/

[4] Hakan Uzuner. “UEBA” https://www.hakanuzuner.com/user-and-entity-behavior-analytics-ueba/

[5]DataVersity. “What is SIEM and Why is it So İmportant” https://www.dataversity.net/what-is-siem-and-why-is-it-so-important/

[6] LOGIQ.AI. “Best Open Source SIEM Tools” https://www.logiq.ai/best-open-source-siem-tools/

[7] DevOps.Com .“5 Open Source Siem Tools Worth Checking Out” https://devops.com/5-open-source-siem-tools-worth-checking-out/

[8] logit.io. “The top 14 Free and Open Source Siem Tools For 2022” https://logit.io/blog/post/the-top-14-free-and-open-source-siem-tools-for-2021

[9] Kostrecova, E. and Binova H. , Security Information and Event Management Volume:4, Issue:2, February 2015

[10] Kotenko I. , Chechulin A. and Novikova E. , Attack Modelling and Security Evaluation for Security Information and Event Management, 40634.pdf

[11] Akbaş E. Log Correlation SIEM Rule Examples and Correlation Engine Performance Data, July 2016