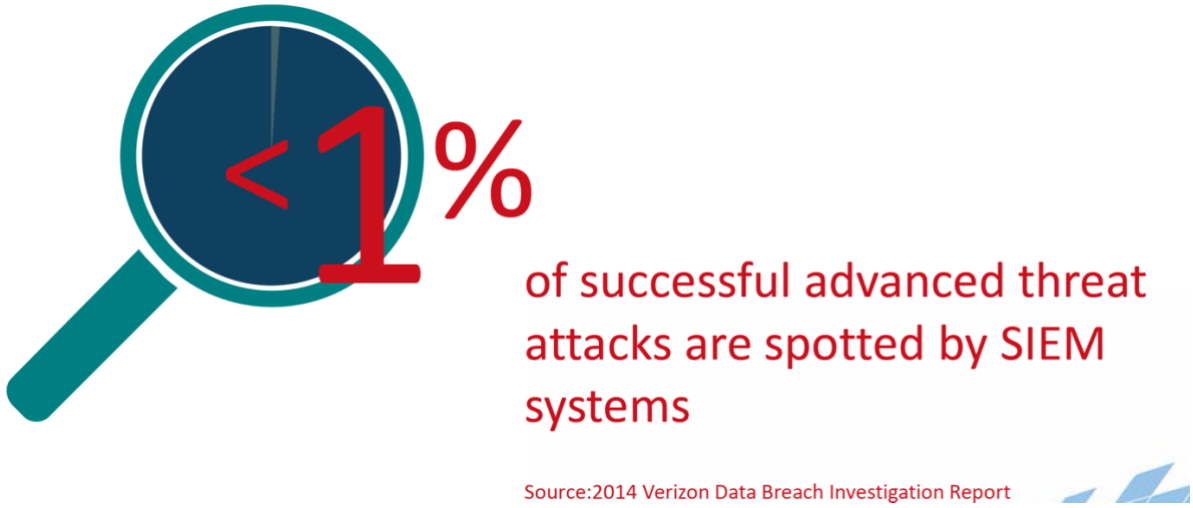
7 ADIMDA BAŞARILI LOG YÖNETİMİ / SIEM PROJESİ

Yazar: Huzeyfe Önal
Baskı: 2017

GİRİŞ

Günümüzde siber saldırıya uğrayan ve maddi, manevi zarara uğrayan kurumlarda yapılan kök sorun analizleri, bu kurumların siber saldırıları zamanında tespit edemediğini ve önlem alamadığını ortaya koymaktadır. Yaşanan kimi siber güvenlik ihlallerinin kurumları iflasın eşiğine getirdiği dahi gözlenmektedir. Dolayısıyla içinde bulunduğumuz bilişim çağında, bir kurumun siber tehditlere karşı koyabilmesi için siber saldırıları zamanında tespit edebilmek ve önlem alabilmek oldukça önemlidir.

Her yıl düzenli olarak veri sızıntıları ile ilgili rapor yayınlayan Verizon firmasının 2014 yılında ilginç bir istatistikle karşımıza çıkmıştır. Rapora göre halihazırda saldırıları merkezi olarak tespit etme amaçlı kullanılan SIEM (Security Information Event Management) yazılımları gelişmiş siber saldırıların %1'ini tespit edebilmektedir.



Kurumların siber saldırılar karşısındaki en temel eksikliği kurum siber altyapısına yeteri kadar hâkim olmamalarıdır. Yerel ağdan veya internet üzerinden gelecek bir saldırıyı önceden tespit etmek ve bu saldırı ile ilgili önlem alabilmek ancak tüm bilişim altyapısı üzerinde 360 derece alan hakimiyeti kurmakla mümkün olacaktır.

Bu yazıda kurumların sahip oldukları log yönetimi / siem çözümlerinin gerçek anlamda kuruma yönelik gerçekleştirilen siber saldırıları tespit edebilmesi ve anlık uyarabilmesi amacıyla yapılması gereken çalışmalar adım adım anlatılmaktadır.

Bu yazıdaki adımlar BGA olarak yaklaşık 3 yıldır *40'dan fazla* kurumda farklı SIEM çözümleri (IBM Qradar, HP Arcsight, Mcafee SIEM ve Splunk) ile başarıyla uygulanmıştır. Hizmet hakkında detaylı bilgi almak için siem@bga.com.tr adresine e-posta gönderebilirsiniz.

Bir SIEM projesinin başarılı olarak sonuçlanması için ihtiyaç duyulan adımlar aşağıdaki gibidir:

1. Gereksinimlerin Tespiti, Kapsam Belirleme ve Proje Yönetimi
2. Log Kaynaklarının Belirlenmesi
3. Kaynaklardan Alınacak Logların Detay ve İçeriğinin Belirlenmesi
4. Log Anlamlandırma, Etiketleme ve Seviyelendirme Çalışması
5. Gelişmiş Korelasyon Kurallarının Oluşturulması
6. Siber Saldırı Simülasyon ve SOME Tatbikat Çalışması
7. Gerçek Zamanlı "Security Monitoring Dashboard" Tasarımı

Yazıya devam etmeden önce hatırlanması gereken en önemli konu, SIEM sistemlerinin **log üreten** değil, logları toplayan, anlamlandıran ve alarm üreten bileşen olduğudur. Çoğu kurum sadece SIEM kurarak yerel ağdaki anormalliklerden haberdar olacağını düşünmektedir, oysa SIEM, bir hesap makinesi gibidir, ona doğru rakam ve işlemi söylemezseniz sonuç beklediğiniz gibi çıkmaz.

Global pazarlar için bilişim sistemleri üzerine araştırma ve tavsiyelerde bulunan Gartner firması son iki yılda yayınladığı bir çok raporda SIEM ürünlerinin artık gelişmiş siber saldırılar

karşısında yetersiz kalacağını, SIEM yerine SOAPA(security operations and analytics platform architecture) kavramının daha fazla dikkate alınması gerektiğini yazmaktadır.

SOAPA konusunda BGA Blog'da Cihat IŞIK tarafından hazırlanmış Siber Saldırıların Tespitinde SIEM Ürünlerinin Yetersizliği ve Çözüm Önerileri yazısına göz atabilirsiniz.

SIEM Projeleri için Gerekli Adımlar

1.Adım: Gereksinimlerin Tespiti, Kapsam Belirleme ve Proje Yönetimi

Her kurumun log alma ihtiyacı konumuna ve ihtiyacına göre farklılıklar göstermektedir. Başarılı bir log/siem projesi için öncelikle kapsamın ve temel seviye ihtiyaçların belirlenmesi ve ardından bu gereksinimlere uygun ürün seçimiyle birlikte projenin başlatılması gerekmektedir.

Bu çalışma kapsamında aşağıdaki ana adımlar gerçekleştirilmektedir:

- Bilinen ticari ve açık kaynak kodlu LOG/SIEM ürünlerinin incelenmesi, POC adımları ve referans kontrollerinin gerçekleştirilmesi.
- Hangi log kaynaklarından hangi sıra ile logların toplanacağı vs gibi bilgiler de bu aşamada karar verilmelidir ve ona göre alınacak ürünün kapasitesi ve lisans durumu belirlenmelidir.
- Log/SIEM Projesi Taslak Takvimi

Bu çalışma adımı sonrasında kurumun ortamına uygun en ideal LOG/SIEM çözümüne karar verilerek ve Log Projesinin kapsamı belirlenerek çalışmalara başlanılmalıdır.

Hangi SIEM Ürününü Seçmeliyim?

Projenin başarısında en önemli bileşenlerden biri doğru ürünü seçmektedir. Doğru ürünü seçmek kadar önemli bir konu da ürün hakkında tecrübesi olan firma/danışman seçimidir. Yoksa dünyanın en iyi ürününü seçip kullanamayabilirsiniz.

Piyasadaki firmaların büyük çoğunluğu SIEM ürünlerini tercih ederken diğer firmaların neleri tercih ettiğini dikkate alarak karar vermektedir. Oysa her firmanın ihtiyaçları benzer olsa da farklıdır. SIEM ürünü seçimi için araştıracak zamanınız yoksa danışmanlık aldığınız firmadan belirlediğiniz 2-3 ürünün detaylı test edilmesi konusunda destek alabilirsiniz. Aşağıdaki örnek tablo BGA ekibinden İbrahim Akgül'ün piyasada bilinen ürünleri test ettiği çalışma sonrasında

çıkmıştır. Ürün alımı aşamasında olup ilgili çalışmanın detaylarını incelemek isteyenler some@bga.com.tr adresine e-posta göndererek bir kopyasını edinebilirler.

Örnek bir SIEM/Log Projesi Ürün POC Karşılaştırma Tablosu

	A ÜRÜNÜ	B ÜRÜNÜ	C ÜRÜNÜ	D ÜRÜNÜ	E ÜRÜNÜ
Log Yönetimi	9	9	9	4	6
Gerçek-Zamanlı İzleme	9	8	8	7	4
Olay Yönetimi	8	8	7	5	4
Raporlama	10	8	8	6	9
Kuruma Özel Log Kaynağı Tanımlama	9	9	8	6	7
Güvenlik Ürünleri ile Entegrasyon	8	10	8	5	6
Yönetim Kolaylığı	7	9	9	5	5
Performans	7	9	8	7	7
Destek	9	6	7	3	6
Referans	9	4	6	4	8
Teknik Değerlendirme	8	9	7	6	6
	93	89	85	58	68

Ürün tercihinde bulunurken eğer projenin amaçlarından biri siber saldırıları tespit amaçlı gelişmiş korelasyon kuralları yazmaksa mutlaka kendine ait korelasyon motoru olan bir ürün seçilmelidir. ÜRün demosu aşamasında mutlaka firmaya bir iki tane gelişmiş korelasyonu üründe nasıl yazacakları sorulmalı ve çıktısı incelenmelidir. Global piyasada 80'den fazla SIEM/Log ürünü bulunmaktadır, bunların büyük çoğunluğu logları merkeze toplamak ve alarm üretmek amaçlı kullanılmaktadır.

Başka bir kaynak olarak da Infosec Nirvana sitesindeki teknik karşılaştırmaları okuyabilirsiniz.

Açık kaynak kodlu yazılımlar tercih edilebilir mi?

Açık kaynak kodlu yazılımlar kullanarak logları merkeze toplayabilir, buradan temel alarmlar oluşturabilir ve sisteminizi saldırılara karşı izleyebilirsiniz. Piyasada çok fazla sayıda açık kaynak kodlu bileşen bulunmaktadır. Bunlardan size uyanını indirerek kullanabilirsiniz

Açık kaynak kodlu yazılımlar kullanılarak siber tehdit gözetleme sistemi kurulumu hakkında 2016 yılında Özgür Yazılım Günleri için hazırladığım sunuma aşağıdaki bağlantıdan ulaşabilirsiniz

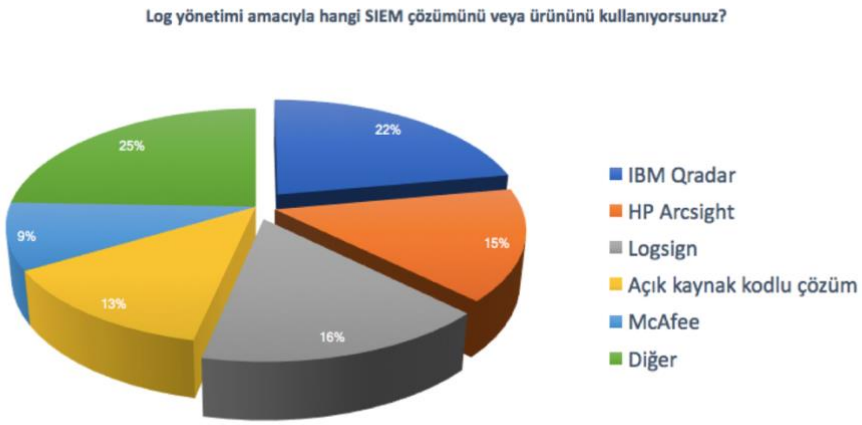
https://www.slideshare.net/bgasecurity/siber-tehdit-gzetleme-ve-siem-olarak-ak-kaynak-sistemlerin-kullanm

Yine buraya not düşmekte fayda var, açık kaynak kodlu çözümlerde ikili, üçlü çarpraz kurallar yazmak için gelişmiş bir korelasyon motoru bulunmamaktadır. Fakat bu konudaki tecrübelerime dayanarak şunu söyleyebilirim ki, bir firma log projesine başladıktan en erken bir sene sonra gelişmiş korelasyon kurallarını yazabilir hale gelmektedir.

Pratiği düşünürsek iyi destek aldığınız bir çalışan/danışman/firmanız varsa açık kaynak kodlu projeleri kullanarak gayet başarılı bir Siber Tehdit Gözetleme sistemi kurabilirsiniz. BGA olarak son 3 senede 37 farklı kuruma bu altyapıları başarıyla kurup çalıştırdığımızı gönül rahatlığıyla söyleyebilirim.

Türkiye'de Kullanılan Log Yönetimi / SIEM Çözümleri

Türkiye'de tercih edilen siem - log ürünleri ile ilgili BGA olarak yaptığımız anketin sonuçlarını inceleyebilirsiniz.



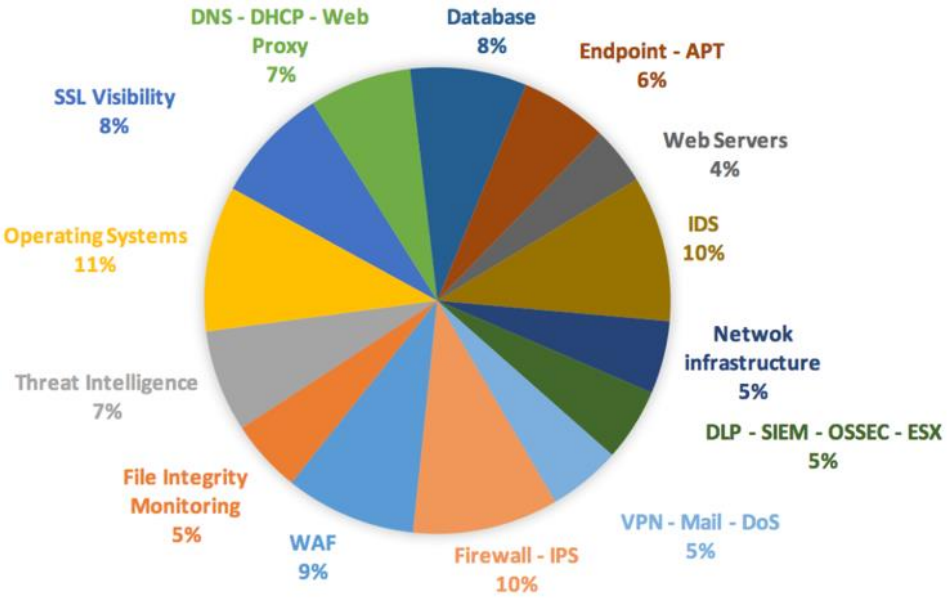
https://www.bgasecurity.com/2017/02/siem-urunleri-arastirma-anketi-sonuclari

2. Adım: Log Kaynaklarının Belirlenmesi

İlk adımda belirlenen kapsam ve gereksinimlere göre kurumdaki hangi IT sistemlerinden logların alınacağının belirlenmesi aşaması. Belirleme çalışmasında öncelikle kurumun uymakla yükümlü olduğu bir standart (PCI, ISO 27001) veya kanun ve yükümlülük (T.C. 5651, S.O.X vs) varsa önceliklendirme yapılmalıdır.

Genellikle orta ve büyük ölçekli kurumlarda log kaynaklarının tespiti ve önceliklendirmesi proje yönetimi aşamasında gerçekleştirilir. Bu aşamada belirleyeceğiniz kaynaklar proje sonrası ortaya çıkacak "Güvenlik Görselliğinizi" doğrudan etkileyecektir.

Aşağıda örnek bir projeden log kaynaklarının projenin başarısındaki oranları verilmiştir. Bu oranlar firmadan firmaya değişkenlik gösterebilmektedir.



Türkiye'de gerçekleştirdiğimiz 40 projeyi baz alarak Türkiye'de 300'den fazla ürünün kullanıldığını söyleyebiliriz. Her bir ürün kategorisi için kurumda neler kullanılıyor envanteri çıkartılarak loglarının alınması sağlanmalıdır. Bu çalışma projenin sonunda hangi korelasyon kurallarının yazılıp yazılamayacağı konusunda en önemli gösterge olacaktır. FIM (File Integrity Monitoring) yazılımına sahip olmayan bir kurumun bu konuyu ilgilendiren

korelasyon kurallarının eksik olacağı bu aşamada ortaya çıkacaktır. Projenin sonraki adımları buradaki ürünlerin sayısı ve çeşidine göre süre olarak değişkenlik gösterecektir.

Temel olarak aşağıdaki log kaynaklarından log toplanmaktadır:

İşletim Sistemleri

- Windows 2008, Windows 2012, Windows XP, 7 ve 8 , Red hat Linux, Suse Linux, IBM AIX, HP UIX

Veritabanı Sistemler

- Oracle, MSsql, Sybase, Firebird

Sanallaştırma Sistemleri

- Vmware, Microsoft, Citrix

Güvenlik Cihazları

- Güvenlik Duvarı, Web Uygulama Güvenlik Duvarı, Saldırı Tespit ve Engelleme Sistemi, DLP, NAC, MDM, Anormallik Tespit Sistemi, DDoS Engelleme ve Tespit Sistemi, İçerik Filtreleme, Antivirüs, Antispam, APT Sistemleri Logları, Netflow, VPN Bağlantı Logları

Ağ Sistemleri

- Switch, Router, Kablosuz Ağ AP, DNS , E-posta ve SMTP, VOIP Sistemleri, DHCP, FTP, SFTP Logları

Web Sunucu Uygulama Logları

- Bilinen uygulama logları, Çağrı Merkezi Logları, Web Mail

3. Adım: Kaynaklardan Alınacak Logların Detay ve İçeriğinin Belirlenmesi

Log kaynaklarının belirlenmesinden sonra hangi log kaynağından ne tip bir log toplanacağı da aynı derecede önem arzetmektedir. Gereğinden fazla log toplayarak sistemin çalışmaması da gerektiği kadar log toplamayarak saldırı analizinde logların yetersiz kalması da sık karşılaşılan durumlardır.

Bu adımda belirlenen kapsam dahilinde hangi sistemlerden hangi tip logların hangi detayda alınacağının belirlendiği ve uygulamaya geçildiği aşamadır.

Örnek verecek olursak Microsoft Windows 2008 ile birlikte gelen toplamda açılabilecek 346 tane security audit politikası vardır ve bunların ***ön tanımlı olarak sadece %30****'u açık gelmektedir.*

Bazı durumlarda kullanılan IT sistemi istenilen türde log üretmemektedir. Bu gibi durumlarda alternatif çözümler üretilerek ilgili log parçalarının toplanması sağlanacaktır.

Windows işletim sistemlerinde guvenlik loglarının nasıl açılacağı konusunda BGA Blog'daki *"Windows Loglama Altyapısında Belirli Event ID Açma/Kapama İşlemleri" konulu yazı* incelenebilir.

4. Adım: Log Anlamlandırma, Etiketleme ve Seviyelendirme Çalışması

Log kaynakları ve hangi tip logların toplanacağı belirlendikten sonraki ilk aşama toplanan logların basit seviye korelasyonudur. Bu aşamada gelen logların kurum için seviyelendirmesi ve etiketlenmesi gerçekleştirilecektir. Log etiketleme ve anlamlandırma IT sistemlerinin ürettiği spesifik kayıtların standart bir güvenlik uzmanının anlayacağı hale getirilmesidir.

Örnek verilecek olursa güvenlik duvarının ürettiği "big icmp packet" uyarısı yerine "Ping of death saldırısı" şeklinde logun üretilmesini sağlamak gibi.

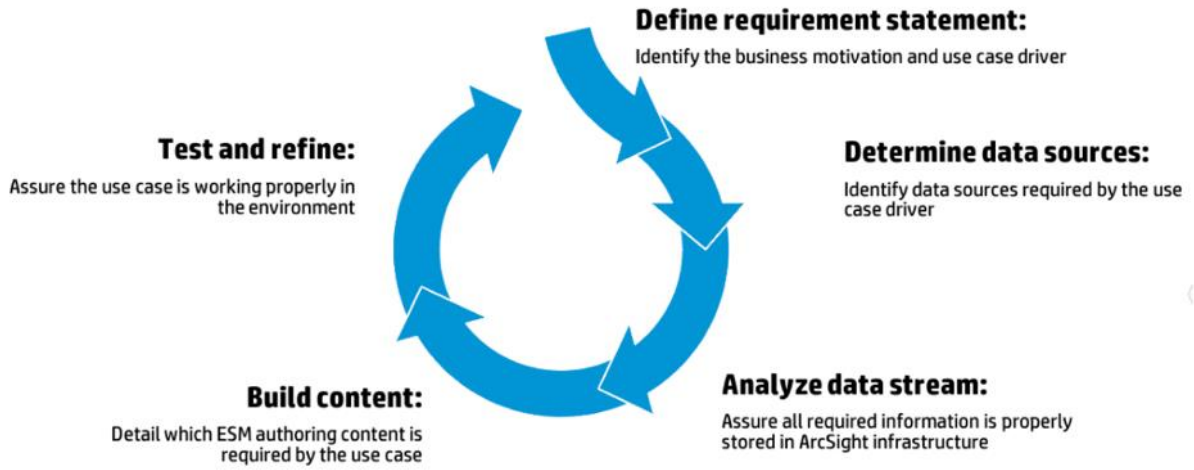
Aynı zamanda bu adımda daha önce üretilen loglar arasındaki false positive'lerin elenmesi de vardır.

5. Adım: Gelişmiş Korelasyon Kurallarının Oluşturulması

Toplanan logların gerçek manada değer ifade edebilmesi için kurum ortamına özel korelasyon kurallarının tanımlanması ve destek alınan firmayla iş birliği içinde kullanılan SIEM çözümüne aktarılması gerekmektedir. Bu adımda kurumla birlikte ihtiyaç duyulabilecek korelasyon kuralları tanımlanarak sisteme giriş yapılacaktır.

Gelişmiş korelasyon kurallarının yazımı için en sağlıklı yöntem kurumua yönelik gerçekleşebilecek siber saldırılar düşünülerek tehdit ağacı oluşturmak ve bu ağacın dallarının her biri için uygun use-case'ler tanımlamak.

Use-case tanımlama için genellikle Cyber kill Chain kullanılmaktadır. HP'nin aşağıda 5 adımlık gösterilmiş Use-case tanımlama metodolojisi SIEM projeleri için önerilmektedir.



Örnek bir Senaryo ve use-case tanımlamaları

Senaryo No	**1**
Zorluk/Yaygınlık	4/5 - 2/5
Senaryo Başlığı	Login Paneli Parola Tahmini /Bruteforce(Yatay/Dikey) Sisteme Arka Kapı(Shell) Yükleme Senaryosu
Kategori	Internet-Web
Amaç ve Detay	Internet'e açık DMZ alanında bulunan açık kaynak kodlu CMS yazılımı(veya kurumsal uygulama) login panelinde kullanıcı adı ve parola tahmin edilerek sisteme php/aspx tabanlı antivirüsler tarafından tanınmayan arka kapı (web shell) yüklenmiş ve bu shell üzerinden sisteme yine antivirüsler tarafından tanınmayacak kalıcı arka kapı yüklenmiştir. Sisteme yüklenen arka kapı kullanılarak aşağıdaki işlemler gerçekleştirilecektir: • Arka kapı yazılımı kullanılarak işletim sisteminde (Linux) root haklarına sahip olmak için çeşitli exploitler indirilmiştir. • Arka kapı yazılımı yüklenerek işletim sisteminde doğrudan Administrator haklarıyla (Windows) komut çalıştırılmıştır. • Sistemlerde hak yükseltme denenmiştir ve başarılı/başarısız olunmuştur.
Sonuç ve İyileştirme	• DMZ'den Internet'e yönelik trafiğin incelenmesi ve sıkı politikalarla erişimin kısıtlanmış olması • Windows/Linux sistemlerde yeni bir port açıldığında merkezi log sistemine uyarı gitmesi • Linux/Windows sistemlerde **web dizinine** yeni eklenen bir dosyanın uzantısı asp, php ise merkezi log sistemine uyarı gitmesi • Linux/Windows sunucularda politika sıkılaştırılması, yetki kısıtlaması • Upload edilen dosyalar içinde belirli imzaların aranması (bilinen shell dosyaları için) **Sistem**; • başarılı ve başarısız brute force denemelerini ayırt edebilmeli ve başarısız brute force denemelerini seviyesi düşük olarak işaretleyebilmeli. • Yatay ve dikey brute force denemelerini tespit edebilmeli • Brute force denemelerini sadece kaynak IP ve threshold değerleriyle değil, hedef IP ve eşik değerleri ile de hesaplayabilmeli. • Web uygulamasının kurulu olduğu dizinler FIM sistemleri

	tarafından anlık kontrol edilmeli ve dosya değişiklikleri alarm üretmeli. • Aynı IP adresinden hem başarılı dosya upload hem de başarılı bruteforce alarmı geldğinde seviyeyi yükseltebilmeli. • Ele geçirilen sistem üzerinden internete doğru http/https/dns paketleri oluştuğunda bunları tespit edebilmeli, eğer Firewall tarafında tüm paketler drop oluyorsa bunu bildirmeli. • Linux işletim sistemi üzerinde açılan root oturumları (Exploit başarılı olursa priv. esc. yakalanması için) loglanmalı.
Kurulacak Sistemler	Wordpress, BgaBank
Log Kaynakları	Web sunucu logları , POST istekleri için WAF veya IPS logları, İşletim sistemi dosya bütünlük değişiklik logları, işletim sistemi dosya upload logları.
Önerilen Çözümler	WAF, IPS, FIM(File Integrity Monitoring), File Auditing
Başarı Ölçüm Kriterl	• WAF, IPS ya da benzeri bir sistem brute force saldırılarını engelleyebilyor mu (HTTP HTML Authentication) • Dosya upload işlemleri WAF, IPS tarafından yakalanabiliyor mu • Brute force yapan IP adresleri üzerinden belirli zaman içinde gelebilecek diğer saldırılar korele ediliyor mu?

6. Adım: Siber Saldırı Simülasyon ve SOME Tatbikat Çalışması

Kurulan bir SIEM/Log sisteminin gerçek saldırılar karşısında ne kadar efektif olduğunu ölçmenin en kolay yanı kurum ortamına sanal bir saldırı simülasyonu gerçekleştirmek ve bu esnada siem sistemini izlemektir. Aksi halde yazılan ve doğru zamanda çalışıp alarm üreteceği düşünülen korelasyon kurallarının sizi yolda bırakma ihtimali %100'dür. Korelasyon kuralları yazıldıktan sonra mutlaka farklı senaryolarla tetiklenerek hatalı/eksik durumlar giderilmeli ve doğru zamanda doğru alarm üreteceğinden emin olunmalıdır.

BGA olarak SIEM Korelasyon projelerinde kullanmak üzere yaklaşık 75 adet Siber Saldırı Senaryosu kullanmaktayız, bu senaryolar hazırlanırken son 3 yıl içerisinde Türkiye ve dünya üzerinde büyük kurumlara gerçekleştirilmiş siber saldırılar ve BGA tarafından gerçekleştirilmiş sızma testi sonuçları incelenmiş, bunlar içinde Türkiye'deki kurum ve kuruluşların altyapıları düşünülerek olabildiğince gerçekci olmasına özen gösterilmiştir.

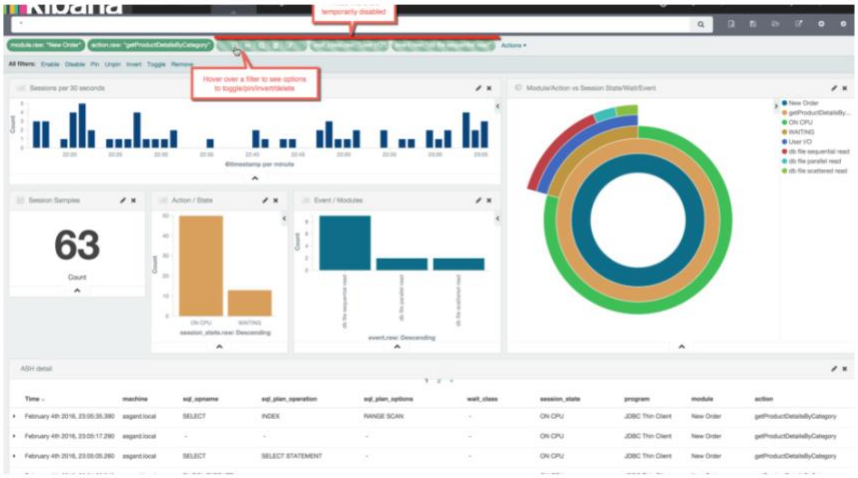
Tatbikat çalışmalarında kolaylık olması açısından Saldırı Simüasyon yazılımları (Örnek: Picus) kullanabilirsiniz.

7. Adım: Gerçek Zamanlı Security Dashboard Tasarımı - Log Görselleştirme

Genellikle log / siem sistemleri gün boyu tespit ettiği anormallikleri kaydedip e-posta ya da benzeri sekilde yöneticilere gönderir fakat ortalama EPS değerlerinin 2000-3000 civarında ve üzerinde olduğu ortamlarda genellikle körlük oluşmaktadır.

Bu aşamada tek bir ekranda SIEM/Log çözümün topladığı ve yorumladığı logların anlaşılabilir şekilde gösterileceği SOC (Security Operation Center) ekranının tasarlanması ve devreye alınması gerçekleştirilecektir. Bu ekranın amacı kurum sistemlerine yönelik bir siber saldırının veya sistemler üzerindeki anormalliklerin anlık olarak tespit edilmesi ve aksiyon alınmasına yardımcı olunmasıdır.

Örnek Dashboard Tasarımları (Kibana Kullanılmıştır)



BGA Bilgi Güvenliği A.Ş. Hakkında

BGA Bilgi Güvenliği A.Ş. 2008 yılından bu yana siber güvenlik alanında faaliyet göstermektedir. Ülkemizdeki bilgi güvenliği sektörüne profesyonel anlamda destek olmak amacı ile kurulan BGA Bilgi Güvenliği, stratejik siber güvenlik danışmanlığı ve güvenlik eğitimleri konularında kurumlara hizmet vermektedir.

Uluslararası geçerliliğe sahip sertifikalı 50 kişilik teknik ekibi ile, faaliyetlerini Ankara ve İstanbul ve USA'da sürdüren BGA Bilgi Güvenliği'nin ilgi alanlarını "*Sızma Testleri, Güvenlik Denetimi, SOME, SOC Danışmanlığı, Açık Kaynak Siber Güvenlik Çözümleri, Büyük Veri Güvenlik Analizi ve Yeni Nesil Güvenlik Çözümleri*" oluşturmaktadır.

Gerçekleştirdiği başarılı danışmanlık projeleri ve eğitimlerle sektörde saygın bir yer edinen BGA Bilgi Güvenliği, kurulduğu günden bugüne alanında lider finans, enerji, telekom ve kamu kuruluşlarına 1.000'den fazla eğitim ve danışmanlık projeleri gerçekleştirmiştir.

BGA Bilgi Güvenliği, kurulduğu 2008 yılından beri ülkemizde bilgi güvenliği konusundaki bilgi ve paylaşımların artması amacı ile güvenlik e-posta listeleri oluşturulması, seminerler, güvenlik etkinlikleri düzenlenmesi, üniversite öğrencilerine kariyer ve bilgi sağlamak için siber güvenlik kampları düzenlenmesi ve sosyal sorumluluk projeleri gibi birçok konuda gönüllü faaliyetlerde bulunmuştur.

BGA Bilgi Güvenliği AKADEMİSİ Hakkında

BGA Bilgi Güvenliği A.Ş.'nin eğitim ve sosyal sorumluluk markası olarak çalışan Bilgi Güvenliği AKADEMİSİ, siber güvenlik konusunda ticari, gönüllü eğitimlerin düzenlenmesi ve siber güvenlik farkındalığını arttırıcı gönüllü faaliyetleri yürütülmesinden sorumludur. Bilgi Güvenliği AKADEMİSİ markasıyla bugüne kadar "Siber Güvenlik Kampları", "Siber Güvenlik Staj Okulu", "Siber Güvenlik Ar-Ge Destek Bursu", "Ethical Hacking yarışmaları" ve "Siber Güvenlik Kütüphanesi" gibi birçok gönüllü faaliyetin destekleyici olmuştur.