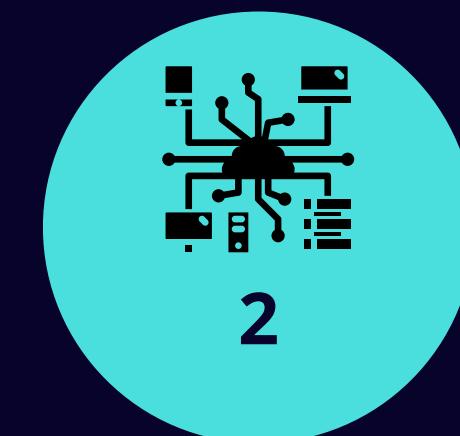


SECURE OPERATIONS CENTER (soc) ARCHITECTURE STRATEGY

DESIGNING AN ON-PREMISE
SOC NETWORK

PROJE SORULARI



650 uç noktadan oluşan bir şirkete SOC Hizmeti verilecektir.

Şirket Envanteri:

- 1- 650 uç nokta (PC, WS, Server)
- 2- 50 Web Server (www.)
- 3- 800 Çalışan
- 4- İki Network: Biri İnternete Kapalı, Biri Açık
- 5- Şirket, Cloud'a Çıkamaz

Soru 1: SOC yapılandırmasında hangi on-premise ürünler ve kategorileri tercih edersin? Hangi kategori ve ürünler arasında entegrasyon ve otomasyon olmalı ki insana bağımlılık azalmalı?

Soru 2: SOC Topoloji nasıl olmalı? Şirket 7/24 izleme talep ediyor. SOC topoloji ne anlam ifade ediyor?



PROJE: BÖRÜ

Yunan mitolojisindeki Kerberos'un nöbetçilik işlevine karşılık olarak; bu projede Türk mitolojisindeki BÖRÜ (Kurt) seçilmiştir.

BÖRÜ, sadece bir bekçi değil, aynı zamanda rehberlik (Threat Intelligence) ve sınırları koruma yeteneğini (SOC Capabilities) simgeler.

Projede kurulan yapı, aşağıdaki kritik görevleri üstlenmektedir:

1. 7/24 İzleme, Kontrol ve Otomasyon,
2. İzole Edilmiş Ağlar Arasındaki Güvenli İletişimi Kurma,
3. Tehditleri Tespit Etme, Sınıflandırma, Alarm Üretme ve Aksiyon Planını Otomatik Uygulama,
4. Şirketteki Veri Bütünlüğünü ve Varlıklarını Koruma.

BÖRÜ, bu işlevleri tek bir isimde birleştirmektedir.

BÖRÜ projesi siber tehditlere karşı otomatik bir refleks yaratır. Splunk SOAR çözümü ile birlikte BÖRÜ'nün anlık müdahale yeteneği; süreç bittikten sonra değil, eş zamanlı olarak, Trellix HX ve Magnet AXIOM gibi araçları saniyeler içinde harekete geçirir. Böylece, en kritik varlıkların güvenliği hep en ön plandadır.

STRATEJİ VE AMAÇ

Strateji: Merkezi Görünürlük ve Segment Edilmiş Ağ Yapısı

Amaç: 7/24 Görünürlük, Otomasyon ve Bilgi Güvenliği Regülasyonlarına Uygunluk

Değerli varlıkların belirlenmesi ve korunması için ihtiyaç duyulan sistemlere uygun çözümler kurgulanmıştır. Senaryonun amacına uygun olarak aşağıdaki konu başlıkları stratejiyi oluşturmuştur:

Ürün Alımı ve Ağdaki Yerleşimi: Hangi kayıtların ve verilerin alınacağına ve optimum izleme için sensörlerin nereye yerleştirileceğine karar verilmiştir.

Entegrasyon: Yeni tehditlerin hızlı bir şekilde tespit edilmesini sağlamak için tehdit istihbaratı entegrasyonu seçilmiştir.

Kural Oluşturma ve Normalleştirme: İlişkilendirme kurallarının geliştirilmesi, F/P azaltılması ve verilerin kolay anlaşılmasına yönelik normalleştirme gerekmektedir.

SOAR (Güvenlik Orkestrasyonu, Otomasyon ve Yanıt) kullanarak; SOC operasyonlarını kolaylaşırma, manuel müdahalelere olan bağımlılığı azaltma ve verimliliği artırmak amaçlanmıştır.

Otomasyon: Tehditlere hızlı yanıt vermek ve insan iş yükünü azaltmak için otomasyonun uygulanması (örneğin, SOAR kullanımı). Yanıtları otomatikleştirmek için kılavuzların ve manuel süreçleri yönlendirmek için dokümantasyonların (playbooks) oluşturulması gerekmektedir.

Mevcut Zorluk ve Geliştirilen Çözüm

Şirket İçi (On-Premise) SOC (Güvenlik Operasyonları Merkezi) mimarisi inşa etmek.

Temel Zorluk: Güvenli Yerel Ağ'daki (Secure Intranet) logları, hackerların External Network'den Güvenli Yerel Ağ'a geçmemesi için bir yol açmadan SOC'a nasıl ulaştırırız?

Çözüm: Tek Yönlü Ağ Mimarısına (Veri Diyonu - Data Diode konsepti) ihtiyaç duyulacaktır.

NOT: Veri Diyonu, ağ trafigini yalnızca iletmeye (transmit) izin veren, ancak geri almaya (receive) fiziksel olarak izin vermeyen bir cihazdır.



SEÇİLEN SOC NETWORK GÜVENLİK ÇÖZÜMLERİ

Kategori ve Ürünler; Tercih Edilme Nedenleri

No	Kategori	Ürün/Hizmet	Tercih Nedeni
1	DLP	Forcepoint DLP	"User Intent" tespitini anlamlandırmak için iyi bir çözüm olarak görülmektedir. Çevrimdışı (offline) sistemlerde ekran görüntülerindeki kritik/önemli verileri algılamak için güçlü OCR (Optik Karakter Tanıma) teknolojisine sahip olduğu belirtilmektedir.
2	EDR	Trellix Endpoint Security (HX)	Trellix HX yalnızca "zararlı yazılım" tespitinde değil, adli bilişim (forensic) yetenekleriyle de ön plana çıkmaktadır ve "Agent Handler" mekanizmasını kullanarak Air-Gapped ağına uygun çalışacaktır.
3	SOAR	Splunk SOAR (Phantom)	Splunk (SIEM) ile doğal olarak entegre çalışacaktır. Ayrık (disconnected) ortamlarda da ayrıntılı kontrol/alarm mekanizması oluşturmak için otomasyonda (playbook) güçlündür.
4	SIEM	Splunk Enterprise	Kurum içi (On-Premise) log analizinde pazar lideri (Gartner Magic Quadrant'a göre) konumundadır. Akış (flow) odaklı yaklaşımının aksine, "veri (data)" odaklı çalışmakta ve çevrimdışı ağ segmentinden gelen herhangi bir metin formatını otomatize olarak işleyebilmeyi sağlayacaktır.
5	Threat Intelligence	OpenCTI	Bilgi Grafiği (Knowledge Graph) olarak çalışır. Standart istihbarat beslemelerinin aksine, on-prem çalışan bir platformdur. Sadece zararlı IOC'leri listelemek yerine, aralarındaki ilişkileri eşler (örneğin, "XYZ IP'si, ABC sektörlerini hedefleyen APT28 tarafından kullanılıyor"). Birçok farklı TI sağlayıcıdan, PDF raporları, MISP bulguları gibi kaynakları kullanır ve veri almak için modüler bir Connector (bağlayıcı) mimariye sahiptir.
6	Breach and Attack Simulation	AttackIQ	İhlal Sonrası Aksiyon'un en önemli olduğu noktalara bağlı olarak çalışır (Post-Breach Mindset). Internet erişimi olmadan güvenlik kontrollerini test etmek için tasarlanmış özel Agent'lara sahiptir, bu da ağ segmentasyonunu doğrulamamıza yardımcı olacaktır.
7	CAASM (Asset Context)	OctoXLabs	Veri Tutarlılığı ve Eksiklik Kontrolü için önemli bir çözümdür. İzole ağ yaklaşımını destekleyecek şekilde kör noktaları (Shadow IT, EDR agent'i çökmüş sunucular) keşfedebilmek için kullanılır. OctoXLabs, Trellix ePO, OpenVAS ve Forcepoint'ten gelen veriyi varlık envanterinde birleştirir.

SEÇİLEN SOC NETWORK GÜVENLİK ÇÖZÜMLERİ

Kategori ve Ürünler; Tercih Edilme Nedenleri

No	Kategori	Ürün/Hizmet	Tercih Nedeni
8	Vulnerability Scanning	Rapid7 Nexpose	Güçlü bir on-premise zayıflık tarama aracıdır. Metasploit ile entegrasyonu sayesinde zayıflıkları otomatik olarak "doğrulamaya" (F/P'leri en azı indirmeye) imkan verir.
9	EASM	CyCognito	50 web sunucusunun dışarıya açık olduğu bir saldırının yüzeyinde; "saldırgan bakış açısı" ile tehditlere karşı hangi yapılandırmaların/teknolojilerin zayıflığı göründüğünü ya da atılı kıldığını tespit eder.
10	Incident Response	Magnet AXIOM Cyber	650 cihazın (endpoint) bulunduğu bir şirkette virüs taraması için fiziksel bilgisayarları kontrol etmek mümkün olmayacaktır. Magnet AXIOM Cyber, "Deep Forensics" özellikleri sayesinde detaylı aramalar yaparak; silinmiş dosyalar, registry değişiklikleri gibi gözden kaçırılan bulguları da anlaşılmış olacaktır.
11	Collaboration Platform	Intel471 (Titan)	SOC analistlerinin, belirli siber saldırıcıları (Ör; Türkiye'yi hedefleyen fidye yazılımı grupları) takip eden teknik kapasiteleri yüksek tehdit avıcılarıyla doğrudan iletişim kurmasına/şirket içi işbirliği yapmasına olanak tanır.
12	Load Balancing / Application Security	Imperva SecureSphere	Imperva; 50 web sunucusunun otomatize siber saldırılara (bot saldırısı) karşı güvenli kalabilmesi için uygulama ve veritabanı güvenliğine odaklanacaktır. Geliştirilmiş SQLi Payload'ları gibi zararlı istekleri keseciktir.
13	Anti-Virus	Symantec SES (Broadcom)	Önem seviyesi yüksek cihazların güvenliği için seçilmiştir. "(Lockdown)" modu sayesinde çevrimdışı ağdaki cihazlar (sunucular, WS ya da PC'ler) için de faydalı olacaktır.
14	DAST	OpenVAS	650 cihazın (endpoint) ve 50 web sunucusunun güvenliğini periyodik olarak test etebilmek için OpenVAS (Greenbone) kullanılacaktır. Lisans ücreti ödemeden DMZ ve Çevrimdışı ağda "Slave Scanners" konumlandırılmasına imkan verecektir. Splunk SOAR'ın taramaları proaktif olarak tetiklemesini sağlayacak Greenbone Management Protocol otomasyon sürecinde kullanılabilecektir.

CEVAP: 1

Soru 1: SOC yapılandırmasında hangi on-premise ürünler ve kategorileri tercih edersin? Hangi kategori ve ürünler arasında entegrasyon ve otomasyon olmalı ki insana bağımlılık azalmalı?

Tercih edilen ürünler/kategoriler entegrasyon ve otomasyon kurgularında insana bağımlılığı azaltabilmek için aşağıdaki amaçları kurgulamak ve soruları cevaplayabilmek için belirlenmiştir:

CAASM ile Zayıflı Cihaz Tespitinin Otomasyonu İçin Uygulanan Entegrasyon Örneği;

1. OctoXLabs → Splunk SOAR

- OctoXLabs sürekli olarak varlıkların aktifliğini sorgular. Ör;
 - "Rapid7 Nexpose tarafından taranmış ancak üzerinde Trellix EDR agent'ı olmayan, Kritik Zayıflı tüm sunucuları göster."
 - OctoXLabs bu "EDR Agent Yapılandırılmamış Sunucu" alarmını Splunk SOAR'a gönderir.

2. Splunk SOAR → Trellix ePO / Symantec SES

- SOAR, bu varlığın Trellix ePO'da mevcut olup olmadığını kontrol eder.
- Symantec'in veya Trellix'in local kurulum dosyalarından otomatik olarak yükleme komutunu tetikler.

3. Splunk SOAR → OpenCTI

- SOAR, varlığın IP'sini OpenCTI'da sorgular.
- Eğer IP bilinen bir saldırgan tarafından kullanılıyorsa, OctoXLabs'taki risk puanı otomatik olarak yükseltilir.

Sonuç: İnsan eforu bu süreçte hiç yoktur. Agent yükleme ve temel güvenlik takibi tamamen otomatiktir.

Temel strateji, OctoXLabs'ın varlık ve güvenlik açığı bağlamını OpenCTI'dan gelen tehdit istihbaratıyla birleştirerek Splunk SOAR üzerinden Trellix ve Imperva'yı otonom olarak harekete geçirmektir.



NOT: Otomasyon örnekleri, kullanılan ürünlerle birlikte, Ağ Haritası ve Mimari bölümünde detaylandırılmıştır.

CEVAP: 1 / OTOMASYON İLE BAĞIMLILIK AZALTMA

Soru 1: SOC yapılandırmasında hangi on-premise ürünler ve kategorileri tercih edersin? Hangi kategori ve ürünler arasında entegrasyon ve otomasyon olmalı ki insana bağımlılık azalmalı?

Bu entegrasyonlar, alarm üretimi (Splunk), otomatik yanıt (Splunk SOAR) ve operasyonel eylemler (EDR/IR) arasındaki döngüyü tamamen otomatikleştirerek analistin sadece yüksek önem dereceli, karmaşık vakalara odaklanması sağlar.

İnsana (SOC Analystine) bağımlılığının azaltılması için SIEM (Splunk) ve SOAR, merkezi sinir sistemi görevi görmelidir.

Bu iki ana platform, aşağıdaki kilit güvenlik kategorileriyle çift yönlü entegrasyon kurarak Tier 1 görevlerini tamamen otomatikleştirebilir:

1- SOAR (Splunk SOAR) ve IR Platformu (Magnet AXIOM):

- SOAR tarafından tetiklenerek saldırıya uğramış uç noktaların (endpoints) anında izolasyonunu ve hızlı adli kanıt toplama işlemini otomatikleştirir.

2- Doğrulama (Splunk SOAR → OpenVAS)

- Splunk SOAR otomasyon adımı ekleyerek; OpenVAS'ı web sunucusunda zafiyet taraması başlatarak kullanır.
- Aynı otomasyon adımı AttackIQ'dan gelen bir testi çalıştırma/doğrulamak için de kurgulanabilir.

3- Tehdit İstihbaratı (OpenCTI):

- SIEM'e otomatik IOC aktarımı ve vaka zenginleştirme sağlayarak analistin manuel araştırma ihtiyacını ortadan kaldırır.

4- WAF (Imperva SecureSphere) ile Saldırı Tespiti:

- Imperva SecureSphere → Splunk SIEM akışında; web sunucularına yönelik bir SQL Injection saldırısını tespit eder ve saldırı loglarını Splunk'a gönderir.

CEVAP: 2

Soru 2: SOC Topoloji nasıl olmalı? Şirket 7/24 izleme talep ediyor. SOC topoloji ne anlam ifade ediyor?

SOC Topoloji Tanımı:

Sensörlerin, güvenlik çözümlerinin, log toplayıcılarının ve merkezi SIEM'in (Güvenlik Bilgisi ve Olay İzleme Sistemi) ağ segmentasyonundan negatif etkilenmeden (ödün vermeden) tam görünürlüğü sağlamak için farklı ağ bölgelerinde (DMZ, LAN, Air Gap) kurduğu iletişimini gösteren mimari haritadır.

Güvenlik kavramı yalnızca kullanılan araçlardan/çözümlerden oluşamaz; güvenlik, entegrasyon ile başlar.

SOC Topolojisinin Uygulanması:

1- Fiziksel Ağ Topolojisi

- **Zone A: DMZ (50 Websites):** Imperva SecureSphere WAF, OpenVAS Scanner ve Web sunucularını içerir. İnternete erişmektedir.
- **Zone B: Secure Intranet (Offline):** 650 Endpoints, OpenVAS Scanner, Splunk Forwarder, Trellix HX (EDR) Agent'larını içerir. İnternet erişimi yoktur.
- **Zone C: SOC Management Zone:** Splunk, Magnet AXIOM, OpenCTI, Trellix ePO ve Master Console gibi güvenlik araçlarını/kategorilerini içerir.

2- Veri Akışı ("Unidirectional", Tek Yönlü Akış Metodu)

- **Problem/Zorluk:** Çevrimdışı Ağ'a (Offline Network) hackerları sokma riskine girmeden, o ağdaki logları nasıl görebiliriz?
- **Çözüm:** Tek Yönlü Ağ Geçidi (Unidirectional Gateway) mantığı (Veri Diyotu) kullanarak; Offline Network'ten → SOC Network'e doğru kesintisiz, tek yönlü akışı sağlamak.
 - Ör;
 - Uç noktalardaki UF'ler (Splunk Universal Forwarder (UF), logları sıkıştırır ve şifreler, ardından bu logları Offline Network'deki Splunk HF'e (Heavy Forwarder (HF) gönderir. HF ise bu veriyi sadece tek yönde (OUT) Splunk Indexer'a (SOC Network'deki) gönderir.
 - Firewall kuralı, bu log trafiği dışındaki başka hiçbir trafiğe izin vermez.

Air Gapped Network Tanımı:

Air Gap, yetkisiz erişimi ve veri ihlallerini önlemek amacıyla bir bilgisayar veya ağı diğer ağlardan fiziksel olarak izole etmeyi içerir.

Bu yöntem, güvenliği sağlanan ağ ile diğer güvensiz ağlar arasında kelimenin tam anlamıyla bir "hava boşluğu" yaratır.



SOC TOPOLOJİSİ VE AĞ MİMARİSİ

Strateji: "Anlayamadığımız veriyi izleyemeyiz."

Ağ topolojisi, kritik veri akışları ve güvenlik sınırlarına uygun oluşturulmuştur.

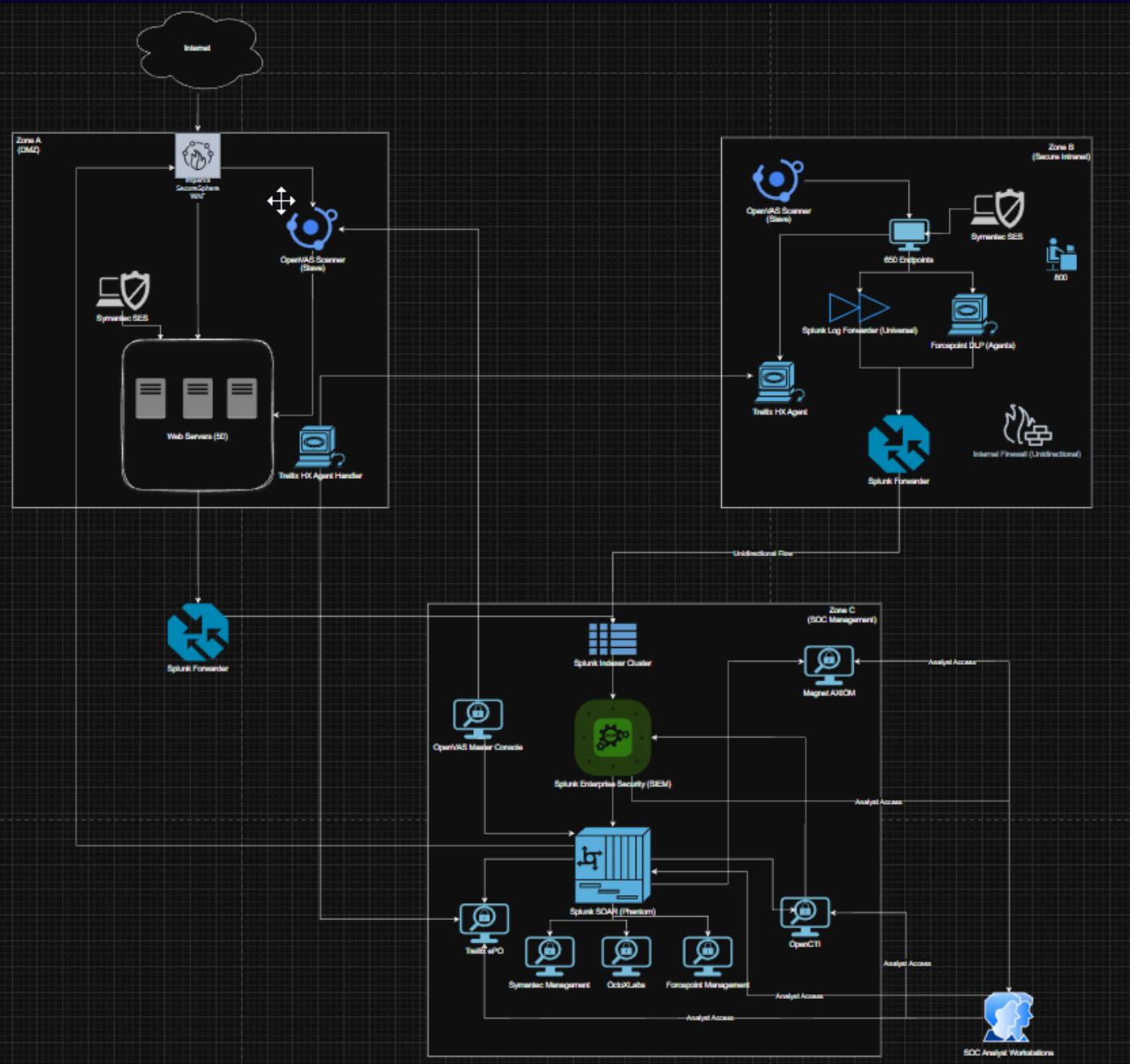
Verilerin şirkette nasıl hareket ettiği kurgulanarak; izleme/monitorleme noktalarının en etkili olacağı yerlerin belirlenmesinde önem arz etmiştir.

Ağ topolojisini oluştururken aşağıdaki soruların cevaplarına odaklanılmıştır:

- En hassas veriler nereye akıyor?
- Kritik ağ tıkanıklıkları nelerdir?
- Trafik, ağ segmentleri arasında nasıl hareket ediyor?
- Performansı etkilemeden ürünler nereye yerleştirilmeli?

Diyagramda İfade Edilen Önemli Noktalar:

- **Segmentasyon Çooook Önemli:** "Network Separation" açıkça uygulanmıştır.
- **Veri Diyoti Prensibi:** Çevrimdışı ağır logları dışa aktarmaması için uygulanmıştır.
- **Kontrollü Çift Yönlü Veri Akışı:** Relay Servers, Air-Gapped bir ağda EDR ve IR için "smart compromise" noktalarıdır.
- **Merkezi Görünürlük:** Tüm veriler Splunk SIEM'e aktarılmaktadır (funnels into).
- **Otomatik Yanıt:** Splunk Phantom, alarmları çeşitli araçlar arasında düzenler (orchestration).
- **Doğrulama (Validation):** OctoXLabs, CyCognito ve Trellix gibi araçlar, sadece reaktif (tepki veren) değil, proaktif çalışma ve çıktı verir.



https://drive.google.com/file/d/1w-Exk208JJ7k2nol9PGqlvgfC3NH69iC/view?usp=drive_link

SOC TOPOLOJİSİ: İNTERNETE AÇIK İSTEKLER

User Request >> Imperva SecureSphere WAF >> 50 Web Servers

Log Üretilmesi ve İşlenmesi:

- **Imperva SecureSphere WAF:** WAF loglarını (SQL injection, XSS, zararlı bot istekleri gibi güvenlik olayları) ve Yük Dengeleyici loglarını (trafik dağıtımları, health-checks) üretir. Bu loglar DMZ'deki Splunk Heavy Forwarder (HF)'a yönlendirilir ve güvenli bir şekilde (Splunk Indexer Cluster aracılığıyla) SOC Network'deki Splunk'a iletir.
- **Web Sunucuları:** Web sunucusu loglarını (örneğin, Apache/Nginx erişim/hata logları), İşletim Sistemi (OS) loglarını ve EDR/AV loglarını (Trellix HX/Symantec SES) aynı DMZ'deki Splunk Heavy Forwarder'a (HF) gönderir.

Otomasyon Örneği: F5 ASM bir web saldırısı (örneğin, belirli bir SQLi Payload'u) tespit ederse:

1. F5 ASM, QRadar'a bir alarm gönderir.
2. QRadar bir ihlal (offense) oluşturur.
3. XSOAR, F5'in engelleme listesini (blocklist) otomatik olarak günceller.
4. SOC ekibi bilgilendirilir.

SOC TOPOLOJİSİ: ONLINE ENDPOINT

Endpoint Activity (Network Users/Servers - DMZ/ONLINE)

Endpoints (DMZ/Online Segmentindeki PC'ler, Sunucular):

- Trellix HX Ajanları:** Tüm süreç aktivitelerini, dosya değişikliklerini, ağ bağlantılarını 7/24 izler.
- Symantec SES Ajanları:** Zararlı yazılımdan koruma (anti-malware) ve bilgisayarlarla izinsiz girişleri önlemeyi (host intrusion prevention) sağlar.
- Forcepoint DLP Ajanları:** Veri hareketini (USB, e-posta, ağ paylaşımı) izler.
- OpenVAS Scanner:** Uç noktalardaki zayıfları taramalarını periyodik olarak gerçekleştirir, bulgularını Splunk Log Forwarder aracılığıyla ileterir ve SOAR Playbook'larına otomatize girdi sağlar.

Log İşlenmesi:

- Uç Nokta/Sunucu:** Splunk Universal Forwarder (UF), yerel sistemdeki tüm Trellix, Symantec ve Forcepoint log dosyalarını okur.
- Toplama:** UF, bu verileri şifreli kanallar üzerinden DMZ'de bulunan Splunk Heavy Forwarder (HF)'a gönderir.
- İşleme:** DMZ'deki HF, logları filtreler ve toplar (logların ham halini değil, özetlenmiş halini göndermek için).
- SOC Network'e İletim:** HF, veriyi Splunk Indexer Cluster'a (SOC Network'e) gönderir.
- Korelasyon:** Splunk Indexer, bu logları işler ve Splunk Enterprise Security (SIEM), gelen veriyi OpenCTI'daki tehdit istihbarat verileri ile detaylandırarak alarmlar (Offense) oluşturur.

Otomasyon Örneği (Forcepoint DLP Agent): Kritik Seviyeli ve Hassas Veri (PII) Ağ Paylaşımına Kopyalama Girişiminin Tespit Edilmesi:

- Log, Splunk SIEM'de "DLP İhlali" olarak işlenir.
- Splunk SOAR, ihlalin yapıldığı üç nokta IP'sini alır ve OpenCTI'da sorular: "Bu kullanıcı daha önce hangi kötü amaçlı IP'lerle iletişim kurmuş?"
- SOAR, Trellix ePO'ya API isteği göndererek üç noktayı ağdan izole eder (Isolate Host).
- SOAR, Magnet AXIOM Cyber'a komut vererek olayla ilgili anlık RAM dump ve disk imajı alma görevini başlatır.

SOC TOPOLOJİSİ: OFFLINE (INTERNAL) ZONE

Endpoint Activity (Secure Internal Network - OFFLINE)

Bu segment, Air-Gapped yapı nedeniyle en kritik kısımdır. DMZ/ONLINE ağdaki gibi doğrudan çift yönlü iletişim kurulmayacaktır.

Endpoints (Internal Segmentindeki PC'ler, Sunucular):

- Splunk Universal Forwarder (UF):** Uç noktadaki tüm logları (OS, EDR, DLP) şifreler ve sıkıştırır.
- Trellix HX:** Sunucularda veya kullanıcı makinelerinde process activity, dosya erişimi ve komut satırı erişim logları kontrol edilir.
- Forcepoint DLP Agent:** Ağ Paylaşımı, fiziksel medya (USB) veya baskı yoluyla hassas veri (KVKK/PII) sızdırmaya yönelik girişimleri tespit eder.
 - İnternete kapalı olduğu için odak nokta fiziksel ve iç ağ kanallarıdır.
- Trellix Agent Handler (AH) / Relay Server:** SOC Network'den gelen karantina (isolate) gibi kritik komutları, Offline ajanlarının dışarıdan çekebilmesi (pull) için bekleten köprü görevi görür.

Log İşlenmesi (Tek Yönlü Veri Akışı):

- Uç Nokta/Sunucu: Splunk Universal Forwarder (UF), tüm logları (Trellix, Forcepoint, OS) toplar.
- UF, bu logları Offline Network sınırlarında yer alan Splunk Heavy Forwarder (HF)'a şifreli bir tünel üzerinden ileter.
- Splunk HF (Veri Diyotu mantığıyla çalışan yazılım katmanı), aldığı logları işledikten sonra, tek yönde (OUTBOUND), SOC Network'deki Splunk Indexer Cluster'a gönderir.

Kritik Kural: Sadece HF'den Indexer'a doğru trafik açılmalıdır, spesifik bir port ve protokol ile kısıtlanmalıdır. SOC Network'den Offline Network'e bu kanaldan veri geçisi fiziksel olarak engellenmiştir.

- Splunk Indexer'lar logları alır ve Splunk Enterprise Security (SIEM) motoru, Offline Network'den gelen logları diğer ağlardaki ve istihbarattaki verilerle korele eder.

SOC TOPOLOJİSİ: ÜRÜN TERCİHLERİNİN DETAYI

Security Tool/Category Flows (Within SOC Management Network)

Rapid7 Nexpose:

- Kurum içi zafiyetlerin tespit edilmesi ve önceliklendirilmesi için konumlandırılmıştır.
- Master Console SOC Network'de bulunur ve DMZ/Internal ağlardaki Slave Scanner'ları yönetir.
- Örnek otomasyon akışı:
 - Nexpose taramayı bitirir, tespit raporunu (XML/CSV) Splunk SIEM'e gönderir.
 - Splunk SOAR, zafiyeti alır ve OctoXLabs'da sorgular:
 - "Bu varlık kritik mi?" Eğer kritikse, SOAR bu zafiyetin bilinen bir saldırgan tarafından kullanılıp kullanılmadığını OpenCTI'a da sorgular.
 - Kritik ve zafiyet sömürülebilir ise (Exploitable), IT ekibine önceliği yüksek bir alarm açar.

CyCognito (EASM):

- Dışarıya açık atak yüzeyini (50 Web Sunucusu ve ilgili IP'ler) saldırgan bakış açısıyla haritalandırır.
- Cloud Connection zorunlu olduğu için, SOC'da bulunan Splunk'un güvenli bir API tüneli ile CyCognito platformundan veri çekmesi gerekecektir.
- Örnek otomasyon akışı:
 - CyCognito yaptığı haritalama sonucunda; yeni, test amaçlı ya da unutulmuş (shadow) bir varlık/servisi keşfedecektir.
 - Keşfedilen bulgular Splunk'a API ile çekilir.
 - Splunk SOAR, keşfedilen varlığı/servisi OpenVAS Master Console üzerinden hedef alarak zafiyet taraması başlatır.
 - Trellix ePO'ya da komut vererek bu yeni varlığın ağ segmentasyonunu kontrol eder.

Intel471 - Titan (Collaboration):

- Gelişmiş ve sofistikte araçlara/yöntemlere sahip, siber tehdit aktörlerine ait istihbaratı verileri SOC Network'e aktarmak için kullanılır.
- Örnek otomasyon akışı:
 - Intel471 portalını kullanan bir SOC analist, şirketi hedef alan yeni bir zararlı yazılım kampanyası (ransomware) hakkında bilgi edinir.
 - Güncel ve doğru IoC'leri OpenCTI'a bir API aracılığı ile yükler (STIX formatında).
 - OpenCTI'a yeni istihbarat girer girmez, Splunk SOAR bir Playbook tetikler:
 - IoC'leri alır ve otomatik olarak Imperva WAF'ta engelleme kuralı (blocklist) oluşturur.
 - Zararlı yazılımlara ait Hash değerlerini Trellix ePO'ya ileterek tüm uç noktalarda tarama başlatır.

KAYNAKLAR

<https://riversafe.co.uk/wp-content/uploads/How-to-Build-a-SOC-a-Guide-for-Effective-Security-Operations.pdf>
<https://ine.com/blog/soc-design-integrating-network-monitoring-from-day-one>
<https://www.fortinet.com/fr/resources/cyberglossary/what-is-air-gap0>
<https://www.gartner.com/reviews/market/external-attack-surface-management>
<https://learn.microsoft.com/en-us/answers/questions/2239077/best-load-balancer-option-for-container-apps-with>

TEŞEKKÜRLER