Bölüm A: Savunma Mimarisi ve Teknoloji Entegrasyonu

1. Ağ ve Çevre Güvenliği (Perimeter Layer)

Bir kurumun siber güvenlik mimarisi katmanlı olarak tasarlanmalıdır. Bunun temel nedeni, tek bir kontrol noktasının her saldırı türünü durdurmasının mümkün olmamasıdır. Bu nedenle savunma, saldırganın ilerleyebileceği her aşamada farklı kontrollerle desteklenir. Ağ ve çevre güvenliği, bu mimarinin ilk katmanını oluşturur.

Perimeter Layer – İlk Temas Noktası

Perimeter layer, kurum ağı ile internet arasındaki geçiş noktasını temsil eder. Bu katmanda amaç, saldırganı mümkün olduğunca erken aşamada karşılamak ve iç sistemlere ulaşmasını zorlaştırmaktır. Firewall ve IDS/IPS bu noktada birlikte çalışacak şekilde konumlandırılır.

Firewall, hangi trafiğin ağa girebileceğini belirleyen ilk kontrol mekanizmasıdır. Yetkisiz bağlantılar, izin verilmeyen portlar veya protokoller burada engellenir. Bu katman, saldırı yüzeyini küçültmek için oldukça kritiktir.

Bu noktada fark edilen önemli bir konu şudur: Firewall yalnızca tanımlı kurallara bakar. Trafik kurallara uygunsa, saldırı içerse bile geçmesine izin verebilir. Yeni başlayan biri için bu durum ilk başta kafa karıştırıcı olabilir.

IDS/IPS – Görünürlük ve Müdahale Katmanı

Firewall'dan geçen trafik tamamen güvenli kabul edilmez. Bu nedenle IDS ve IPS sistemleri devreye girer. Bu sistemler, trafiğin davranışını ve bilinen saldırı kalıplarını analiz eder.

IDS, trafiği engellemeden izler ve şüpheli durumları tespit eder. Buradaki temel amaç, güvenlik ekibine görünürlük (visibility) sağlamaktır. IDS'in her şüpheli durumda trafiği durdurmamasının nedeni, yanlış bir engellemenin iş sürekliliğini olumsuz etkileyebilmesidir.

IPS ise belirli saldırı türlerinde daha aktif davranarak müdahalede bulunabilir. Bu iki sistem birlikte kullanıldığında, biri uyarı üretirken diğeri gerektiğinde aksiyon alabilir.

Bu katmanda asıl amaç, her şeyi engellemek değil; neyin gerçekten tehlikeli olduğunu ayırt edebilmektir.

Internal Network Layer – NDR'in Konumlandığı Nokta

Gerçekçi saldırı senaryolarında, saldırganın perimeter güvenliğini aşabildiği varsayılır. Bu yaklaşım *assume breach* olarak adlandırılır. Bu noktadan sonra savunma, ağın iç kısmına taşınır.

NDR (Network Detection and Response), internal network layer'da konumlanır ve ağ içindeki east-west traffic'i izler. Buradaki temel fikir, sistemlerin normalde nasıl iletişim kurduğunu öğrenmek ve bu davranışın dışına çıkan durumları tespit etmektir.

Trafik şifreli (encrypted traffic) olsa bile; bağlantı sayısı, zamanlama ve yön gibi metaveriler analiz edilerek anormallikler yakalanabilir. Özellikle lateral movement denemeleri NDR için önemli bir göstergedir.

Yeni başlayan biri için burada fark edilen en önemli şey şudur: Saldırı her zaman dışarıdan gelmez. İçerideki anormal hareketleri fark edebilmek en az perimeter güvenliği kadar kritiktir.

Katmanlı Savunma Yaklaşımının Önemi

Bu mimaride her katman farklı bir riski hedef alır:

- Perimeter layer: Yetkisiz erişimi erken aşamada engeller
- IDS/IPS: Şüpheli trafik davranışlarını görünür hale getirir
- Internal network layer (NDR): Ağ içindeki anormal hareketleri tespit eder

Bu yaklaşım sayesinde savunma tek bir noktaya bağlı kalmaz. Yeni başlayan biri açısından bakıldığında, en önemli kazanım şudur: Güvenlik, tek bir ürünle değil; doğru konumlandırılmış katmanların birlikte çalışmasıyla sağlanır.

Bölüm B: Teknik Sözlük ve Kavram Avı

1. Temel Yapıtaşları ve Ağ

Transistör & Bilgisayar

Transistörlerin 0 ve 1 şeklinde açılıp kapanması, bilgisayarın en temel karar mekanizmasını oluşturur ve bu basit mantık işlemleri bir araya gelerek işletim sistemlerinin çalışmasını mümkün kılar. Bu ilişki, yazılım seviyesinde gördüğümüz her şeyin donanımda çok temel elektriksel hareketlere dayandığını gösterir.

OSI vs TCP/IP

OSI modeli ağ iletişimini anlamak ve anlatmak için kullanılan teorik bir referans modelidir. TCP/IP ise gerçekten çalışan, internetin üzerinde kurulu olduğu ve pratikte kullanılan protokol yapısı olduğu için günümüz ağlarının temelini oluşturur.

Kriptografi

Kriptografi, verinin yetkisiz kişiler tarafından okunmasını engellemek için kullanılır. Aynı zamanda verinin değiştirilmediğini doğrulayarak veri bütünlüğünü (integrity) korumayı sağlar.

2. Saldırı Vektörleri (Offensive Terminology)

Sosyal Mühendislik & Phishing

Sosyal mühendislik, teknik sistemleri aşmak yerine insanın güvenini ve hatalarını hedef aldığı için genellikle daha kolaydır. Phishing sahte içeriklerle kullanıcıyı kandırmayı amaçlarken, e-mail spoofing teknik olarak e-postanın gönderici bilgisinin taklit edilmesiyle yapılır.

Malware & Ransomware

Malware, sisteme zarar vermek veya kontrol ele geçirmek amacıyla yazılmış tüm zararlı yazılımları kapsayan genel bir terimdir. Ransomware ise bu zararlı yazılımların, sistemi veya veriyi kilitleyip fidye talep eden özel bir türüdür.

Zero-Day (Sıfır Gün)

Zero-Day, henüz üreticisi tarafından bilinmeyen veya yaması çıkmamış bir güvenlik açığını ifade eder. Savunma tarafı için tehlikelidir çünkü ortada hazır bir koruma veya çözüm yoktur.

3. Savunma Mekanizmaları (Defensive Terminology)

Yama (Patch) Yönetimi

Patch'lerin zamanında uygulanmaması, bilinen güvenlik açıklarının sistemde açık kalmasına neden olur. Bu durum, saldırganların daha önce keşfedilmiş zafiyetleri kolayca kullanabilmesine yol açar.

Kimlik ve Erişim – 2FA

Parolalar tek başına yeterli değildir çünkü çalınabilir veya tahmin edilebilir. İki Faktörlü Kimlik Doğrulama (2FA), saldırganın sadece parolayı değil ikinci bir doğrulama unsurunu da ele geçirmesini gerektirdiği için güvenliği ciddi şekilde artırır.

VPN & SSL/TLS

VPN, internet üzerinde şifreli bir tünel oluşturarak veri trafiğini korur ancak kullanıcıyı tamamen görünmez yapmaz. SSL/TLS ise bu tünelin içinde, veri iletiminin güvenli şekilde şifrelenmesini sağlayan protokol katmanıdır.

4. Standartlar ve Süreçler

Zafiyet Taraması vs Pentest

Zafiyet taraması genellikle otomatik araçlarla bilinen açıkları tespit etmeyi amaçlar. Pentest ise bir saldırgan gibi düşünerek, bu açıkların gerçekten istismar edilip edilemeyeceğini manuel olarak test eder.

Regülasyonlar (ISO 27001, NIST, GDPR)

Bu standartlar doğrudan teknik araçlar değil, güvenliğin nasıl yönetilmesi gerektiğini tanımlayan birer çerçevedir. Bir mühendisin bunları bilmesi, yaptığı teknik işin kurumsal ve hukuki karşılığını anlayabilmesi için önemlidir.

Bölüm C: CTI ve İstihbarat Odaklı Vaka Analizi

Senaryo: SOC nöbetinde kritik sunucunun 45.128.232.67 IP'si ile şüpheli trafik ürettiği görülüyor.

1. Adım: Pasif İstihbarat Toplama (CTI)

1) Kimlik Tespiti (Country / Org / ASN)

- IP Bloğu (CIDR): 45.128.232.0/24 bloğu, BGP tarafında AS50053 ile ilişkilendiriliyor ve "Anton Levin / VDSKA-AS" gibi bir tanımla anılıyor.
  https://whois.ipip.net/cidr/45.128.232.0/24
  https://ipinfo.io/AS50053
  https://bgp.tools/as/50053
- Organizasyon / ASN İlişkisi: IPinfo'nun AS50053 sayfasında bu ASN altında "Individual Entrepreneur Anton Levin" gibi kayıtlar ve çeşitli IP blokları listeleniyor (hosting/leased altyapı izlenimi veriyor).
  https://ipinfo.io/AS50053

Yeni başlayan biri olarak burada çıkardığım yorum: "Ülke tek başına anlamlı değil; asıl kritik olan bu IP'nin hangi ASN/organizasyon altında toplandığı ve daha önce nasıl kullanıldığı." Çünkü saldırı altyapıları çoğu zaman "barındırma (hosting) / kiralık sunucu" tarafında hızlı değişebiliyor.

2) Sicil Kaydı (Ne ile ilişkilendirilmiş?)

- Pasif kaynaklarda (OSINT listeleri) 45.128.232.67 IP'si, SSH brute force yapan adreslerin listelerinde yer alıyor. Bu, IP'nin en azından geçmişte credential-guessing / password spraying benzeri davranışlarla aynı kümeye düştüğünü gösterir.

https://jamesbrine.com.au/vultrparis-ssh-bruteforce-ip-list-2024-01-06/?utm_source=chatgpt.com

https://jamesbrine.com.au/vultrwarsaw-ssh-bruteforce-ip-list-2024-07-03/?utm_source=chatgpt.com

https://jamesbrine.com.au/digitaloceanlondon-ssh-bruteforce-ip-list-2024-03-14/?utm_source=chatgpt.com

Burada küçük ama önemli fark: Bu tür listeler "kesin suçlu" demek değildir; ama SOC açısından risk skorunu yükseltir (özellikle kritik sunucu ile konuşuyorsa).

3) Zaman Çizelgesi (Yeni mi, eski mi?)

- Brute force listelerindeki örnek kayıtlar 2024 tarihli paylaşımlarda görünüyor (yani en azından geçmişte raporlanmış).
- Elimdeki pasif verilerle "son 24 saat" içinde güncel rapor var mı kesinleyemiyorum; bu yüzden bu IP'yi "geçmişte raporlanmış / potansiyel risk" sınıfında değerlendiriyorum.
  https://jamesbrine.com.au/vultrparis-ssh-bruteforce-ip-list-2024-01-06/?utm_source=chatgpt.com
  https://jamesbrine.com.au/vultrwarsaw-ssh-bruteforce-ip-list-2024-07-03/?utm_source=chatgpt.com

2. Adım: Terminoloji ve Yapılandırma (Applied Concepts)

IOC (Indicator of Compromise)

Bu senaryodaki IOC, tek başına "IP adresi" olmak zorunda değil; kritik sunucunun bu IP ile hangi port/protokolüzerinden konuştuğu, varsa URL/FQDN, hatta EDR tarafında process + hash bilgisi de IOC setine dahil edilebilir. Yani IOC bir paket gibidir: tek bir veri değil, olayı tanımlayan teknik izler bütünüdür.

Bu vakaya uygun IOC format örneği (teknik yazım):

- dst_ip: 45.128.232.67
- (Varsayımsal alanlar — loglardan doldurulur) dst_port: <port> , proto: <tcp/udp> , first_seen: <timestamp> , src_host: <critical-server>

Not: Port/timestamp gibi alanlar senin SIEM/SOC logundan gelir; ben burada formatı gösteriyorum.

CTI (Cyber Threat Intelligence) – Data'dan Intelligence'a

"Bu IP şu ülkede" demek sadece Data'dır. Bunu Intelligence yapan şey, bağlam (context) eklemektir: *Bizim kritik sunucumuz bu IP ile ne konuşuyor? Bu iletişim normal mi? Zamanlama/port/tekrar sayısı ne?*

Bu olayda bağlam şöyle kuruluyor: IP, AS50053 (Anton Levin / VDSKA-AS) gibi hosting benzeri bir ASN ile ilişkilendiriliyor ve ayrıca geçmiş OSINT kayıtlarında SSH brute force listelerinde görünüyor.

Dolayısıyla "kritik sunucu bu IP ile konuşuyor" bilgisi, saldırganın credential access / initial access denemesi olabileceği yönünde operasyonel anlam kazanır.

MISP (Malware Information Sharing Platform) – Paylaşımın değeri

Eğer bu IP'nin yeni bir Ransomware kampanyasında (ör. C2 / staging / brute force giriş noktası) kullanıldığını doğrulasaydık, bu IOC'yi MISP'e eklemek diğer kurumların mavi takım tarafında aynı IP'yi daha erken yakalamasına yardım ederdi. Özellikle "IP + davranış (TTP) + zaman aralığı + ilişkilendirilmiş artefact" birlikte paylaşıldığında, farklı SOC'lar kendi loglarında hızlı korelasyon yapabilir.

3. Adım: Karar ve Aksiyon (Actionable Intelligence)

Karar:

İzle (Monitor) + Koşullu Engelle (Conditional Block)

Gerekçe (teknik):

Bu IP, BGP/ASN bağlamında AS50053 (VDSKA-AS / Anton Levin) ile ilişkilendirilen bir altyapı altında görünüyor ve OSINT tarafında SSH brute force yapan IP listelerinde geçmişte yer almış.

Kritik sunucumuzun bu IP ile iletişim kurması normal bir iş ihtiyacına dayanmıyorsa (allowlist'te yoksa), bu durum yetkisiz erişim denemesi veya en azından recon/credential guessing şüphesi oluşturur. Bu nedenle ilk etapta bağlantıları SIEM'de "high attention" olarak izlemek, eş zamanlı olarak firewall tarafında kural bazlı kısıtlama (örn. sadece ilgili port / sadece belirli yön) uygulamak ve olayın doğrulanması halinde tam engelleme yapmak uygun olacaktır.

Sonuç:

Kritik sunucumuzun 45.128.232.67 IP'si ile şüpheli trafik ürettiği tespit edilmiştir. Pasif CTI incelemesinde bu IP'nin AS50053 (VDSKA-AS / Anton Levin) altyapısı ile ilişkilendiği ve OSINT kaynaklarında geçmişte SSH brute forceaktivitesi bulunan IP listelerinde yer aldığı görülmüştür. Bu nedenle iletişimin iş gerekçesi doğrulanana kadar olay Monitor statüsünde ele alınmış, ilgili log korelasyonları genişletilmiş ve doğrulama sonrası koşullu engelleme / tam engelleme aksiyonu için hazır plan oluşturulmuştur.

Bölüm D: Kriz Yönetimi ve Olay Müdahale Refleksleri

Siber güvenlikte gerçek sınav, her şey yolundayken değil; işler bozulduğunda verilir. Bu bölümde yaklaşımım, teknik aksiyonları süreç yönetimi ve doğru iletişim ile birlikte ele almak olurdu.

1. Senaryo: Fidye Yazılımı (Ransomware) Kıyameti

Finans departmanından bir kullanıcı, ekranında kırmızı bir kilit simgesi gördüğünü ve dosyalarının açılmadığını bildiriyor. Bu noktada bunun bir ransomware vakası olduğunu varsayarak hareket ederdim.

Acil Müdahale – İlk 3 Teknik Adım

1) Sistemi ağdan izole ederdim (kabloyu değil, ağı keserek).

İlk refleks "fişi çekmek" gibi görünse de bu, RAM'deki verilerin ve aktif sürecin kaybolmasına neden olabilir. Bunun yerine cihazın network bağlantısını keserek (VLAN izolasyonu / Wi-Fi kapatma) zararlının yayılmasını durdurmak daha kontrollü bir yaklaşımdır.

2) Olayın kapsamını belirlerdim.

Bu tek bir endpoint mi, yoksa başka sistemler de benzer davranış gösteriyor mu sorusuna hızlıca cevap arardım. Aynı hash, aynı uzantı veya aynı zaman aralığında başka alarmlar var mı diye EDR/SIEM tarafına bakardım.

3) Delil bütünlüğünü korurdum.

Disk imajı veya en azından ilgili logların overwrite olmaması için sistem üzerinde gereksiz işlem yapmazdım. Amaç “hemen düzeltmek” değil, önce ne olduğunu anlamak olurdu.

Yeni başlayan biri olarak burada öğrendiğim kritik nokta şu:

Yanlış bir hızlı hareket, saldırının kendisinden daha fazla zarar verebilir.

Analiz – Zararlı Sisteme Nasıl Girdi?

Bu sorunun cevabını bulmak için farklı log kaynaklarını birlikte incelerdim:

- Email Gateway / Mail Logs: Şüpheli bir attachment veya link var mı?
- EDR Logs: Şifreleme işlemini başlatan process, parent process nedir?
- Authentication Logs: Olaydan önce şüpheli bir login veya yetki artışı olmuş mu?
- Proxy / Web Logs: Bilinen malicious bir URL ile iletişim kurulmuş mu?

Amaç tek bir loga bakmak değil, zaman çizelgesi (timeline) oluşturmaktır.

2. Senaryo: Oltalama (Phishing) Dedektifliği

CEO’dan gelmiş gibi görünen “Acil Fatura Ödemesi” konulu bir e-posta inceleniyor.

Teknik İnceleme – Sahte Olduğunu Nasıl Kanıtlarım?

Ben olsaydım aşağıdaki teknik parametrelere bakardım:

- Email Header: From, Return-Path ve Received alanları tutarlı mı?
- Gönderici IP: CEO’nun normalde mail attığı IP/ASN ile uyuşuyor mu?
- SPF / DKIM / DMARC: Domain spoofing var mı?
- URL Yapısı: Link varsa gerçek domain mi yoksa benzer yazılmış (typosquatting) bir alan adı mı?

Bu inceleme, “bana sahte gibi geldi” değil, teknik olarak sahtedir diyebilmek içindir.

Önlem – Diğer Kullanıcılara Gitmesini Nasıl Engellerim?

Bu saldırının yayılmasını önlemek için:

- Email Gateway üzerinde:
    - Gönderici domain/IP için block veya quarantine kuralı
    - Benzer subject veya URL pattern'ı için filtre
- Gerekirse Firewall / DNS tarafında:
    - İlgili malicious domain'ler için deny kuralı

Buradaki amaç sadece bu maili değil, aynı kampanyanın devamını engellemektir.

3. Süreç ve İletişim – "Mavi Takım" Ruhu

Standartlar – Hangi Çerçeveye Dayanırım?

Olay müdahale sürecimi,

NIST Incident Response Lifecycle yaklaşımına dayandırırdım:

Hazırlık → Tespit → Sınırlama → Temizleme → Kurtarma

ISO 27001 gibi standartlar ise bu sürecin kurum içinde sürdürülebilir ve denetlenebilir olmasını sağlar. (Burada amaç belge almak değil, düzenli refleks kazanmaktır.)

Kriz İletişimi – Panik Yönetimi

Saldırı devam ederken iletişim en az teknik aksiyon kadar kritiktir.

Ben olsaydım:

- Yönetimi kısa, net ve teknik doğruluğu olan güncellemelerle bilgilendirirdim
- "Bilmiyoruz" dediğim yerde tahmin yapmazdım
- Ekip içinde suçlayıcı değil, çözüm odaklı bir dil kullanırdım

Örnek yaklaşım:

"Şu an yayılma kontrol altında, kök neden analizi devam ediyor. X saat içinde bir sonraki güncellemeyi paylaşacağız."

Bu yaklaşım paniği değil, güveni yönetir.

4. Vizyon: Güncel Kalma Sanatı

Tehditler sürekli değiştiği için ben kendimi güncel tutmak adına şu kaynakları takip ederdim:

1) CVE / NVD Database – Yeni zafiyetleri ve etkilenen ürünleri görmek için

2) The Hacker News / BleepingComputer – Güncel saldırı kampanyalarını takip etmek için

3) Twitter (X) – Güvenlik Araştırmacıları – Zero-day ve aktif exploit paylaşımlarını erken görmek için

Yeni başlayan biri için fark ettiğim şey şu:

Güncel kalmak bir yetenek değil, bir alışkanlıktır.