Gölge Analist Raporu

Bölüm A – Savunma Mimarisi ve Teknoloji Entegrasyonu

1. Ağ ve Çevre Güvenliği (Sınır Hattı)

Kuruma yönelik saldırılar genellikle ilk olarak ağ sınırında karşılanır. Firewall bu noktada **kimlerin içeri girip giremeyeceğine karar veren kapı görevlisi** gibidir. IP, port ve protokol bazlı kurallar ile bilinen kötü trafiği doğrudan engeller. Ancak Firewall, trafiğin **niyetini** her zaman anlayamaz.

Bu noktada IDS/IPS devreye girer. IDS, kapıdan geçenleri durdurmaz ama **şüpheli davranışı tespit edip alarm üretir**. IPS ise bu alarmları aksiyona çevirerek trafiği kesebilir. Bu ayrım kritiktir çünkü her şüpheli davranış anında engellenirse, iş sürekliliği zarar görebilir.

Firewall'ın atlatıldığı veya şifreli trafiğin kullanıldığı senaryolarda **NDR** önem kazanır. NDR, paketin içeriğine değil **ağ içi davranışlara** bakar. Normalde muhasebe sunucusunun bağlanmadığı bir segmentle iletişim kurması gibi anormallikler, saldırganın yanal hareket (lateral movement) yaptığını gösterebilir.

Bölüm B – Teknik Sözlük ve Kavram Avı

- **a)** Transistörlerin 0-1 mantığı, işlemcilerin talimatları çalıştırmasını sağlar; işletim sistemleri bu donanım gerçekliği üzerinde soyutlama katmanı oluşturur.
- **b)** OSI tcp ip nin nasıl çalıştığını anlatır.Osi bizim işleri anlamamız için görselleştirilmiş gibi düşünebiliriz.
- **c)** Insan beşerdir şaşar.bilgisayar için aksidr ya 1 ya 0 her şey nettir.

- **D)**Malware halk dilinde virüstür.Ransomware ise bir virüs türüdür.Bilgisayardaki tüm dosyaları şifreleyerek sizden para talep eder.
- **E)**Henüz kimsenin bilmediği daha yeni ortaya cıkmış demektir
- **F)** Güncellemeler sürekli sistemi dinamik tutar.win xp üzerinde deney yapıp açıklar bulmak daha kolaydır çünkü daha eskidir,tekonolojiler eskidir,bu sayede açıklar daha fazla ve rahat bulunur.Ama sürekli güncellenen sistemde biri farketmeden aççıklar yazılım geliştirme ekipleri tarafından bile farkedilip olası bir zero dayı önleyebilir.

- **G)** Parola ele geçirilse bile ikinci faktör saldırganın ilerlemesini engeller.
- **H)** VPN görünmezlik değil, şifreli bir tünel sağlar; TLS bu tünelin içindeki iletişimi korur.

Bölüm C – CTI ve Vaka Analizi

Pasif İstihbarat

```
a)sicil kaydı:brüte force

b)eski bir tehdit
```

Bölüm D – Kriz Yönetimi

1. Ransomware

- **Sistemi ağdan izole etmek en dopru karardır.virüsün nerden geldiği belli değil ve bunun yayılmasını engellemek için biran önce aksyon alınmalı.**

2. Phishing

- **Kaynaığı içeri mi dışarı mı bilinmediğii için gateway üzerinde kural yazarım.Eposta detayı ise headerda belli olur**

3. Süreç ve İletişim

Nist kurallarını izlerim ve haberdar etmek için kısa ve öz şekilde yönetimi bilgilendiririm.