

Transistör Nedir? Nasıl Çalışır?

Bilgisayar Nedir? Nasıl Çalışır?

OSI Referans Modeli Nedir?

TCP/IP Modeli Nedir?-

İki Faktörlü Kimlik Doğrulama Nedir?

Güvenlik Güncellemeleri Neden Önemlidir?

Sosyal Mühendislik Nedir?

Phishing Nedir?

Malware Nedir?

Ransomware nedir?

Güvenlik Açığı Nedir?

Firewall Ne İşe Yarar?

Kriptografi Nedir?

Ağ Zafiyet Taraması hakkında bildiklerin neler?

Zero-Day Saldırısı Nedir?

Patch Nedir?

VPN (Sanal Özel Ağ) Nedir?

EDR/XDR/Antivirüs Programları Ne İşe Yarar?

SSL/TLS Ne İşe Yarar?

ISO 27001, NIST, GDPR gibi güvenlik standartları nedir ne işe yarar?

E-mail Spoofing Nedir Süreç Nasıl İşler?

CTI Nedir?

Sorumluluğundaki bir makinenin 45.128.232.67 ip adresi ile trafik oluşturduğu tespit edildi. Ip adresi hakkında CTI kaynaklarını kullanarak hakkında pasif bilgi topla ve topladığın bilgiler sonrası nasıl bir aksiyon alırsın bunu açıklamamı istiyorum. Ip ile etkileşime geçme. Sadece CTI kaynaklarını kullanarak ip adresini incele.

**Güvenlik Duvarları (Firewall) Nedir ve Nasıl Çalışır?**

- Güvenlik duvarlarının temel işlevleri ve yapılandırma süreci hakkında bilgi ver.

**İzinsiz Giriş Tespiti ve Önleme Sistemleri (IDS/IPS) Arasındaki Fark Nedir?**

- IDS ve IPS'nin nasıl çalıştığını ve aralarındaki temel farkları açıkla.

**Saldırı Tespit Sistemleri (HIDS ve NIDS) Arasındaki Farklar Nelerdir?**

- Host-based IDS (HIDS) ve Network-based IDS (NIDS) arasındaki farkları ve kullanım senaryolarını anlat.

**Sızma Testi Nedir ve Mavi Takım İçin Önemi Nedir?**

- Sızma testi süreçlerini ve sonuçlarının mavi takım için nasıl değerlendirildiğini açıkla.

**Güvenlik Bilgisi ve Olay Yönetimi (SIEM) Sistemleri Nedir?**

- SIEM sistemlerinin nasıl çalıştığını ve mavi takım tarafından nasıl kullanıldığını açıkla.

**Bir Fidye Yazılımı Saldırısı Durumunda İlk Adımların Ne Olurdu?**

- Fidye yazılımı saldırısını tespit edildiğinde izlenecek adımları açıkla.

**Bir Güvenlik İhlali Durumunda Olay Müdahale Sürecini Anlat.**

- Olay müdahale sürecinde hangi adımları takip edeceğinizi ve neden bu adımları atacağınızı anlat.

**Phishing Saldırısını Nasıl Tespit Edersin ve Önlemler Alırsın?**

- Phishing saldırılarını tespit etme yöntemlerinizi ve alınacak önlemleri açıkla.

**Mavi Takımın Ana Sorumlulukları Nelerdir?**

- Mavi takımın siber güvenlikteki rolü ve sorumluluklarını anlat.

**Güvenlik Protokollerı ve Standartları Hakkında Bilgin Nedir?**

- ISO 27001, NIST ve diğer önemli güvenlik protokollerinin hakkında bilgi ver.

**Siber Tehdit İstihbaratı (CTI) Nedir ve Mavi Takım İçin Önemi Nedir?**

- CTI'nin ne olduğunu ve mavi takım için nasıl kullanıldığını açıkla.

**Ekip İçinde Etkili İletişim Kurma Yöntemleriniz Nelerdir?**

- Ekip çalışmasında nasıl etkili iletişim kurduğunu ve bunu nasıl sağladığınızı anlat.

**Stresli ve Acil Durumlarda Nasıl Tepki Verirsiniz?**

- Stres yönetimi ve acil durumlarda nasıl tepki verdığınızı açıkla.

**Sürekli Değişen Siber Tehditlere Karşı Nasıl Güncel Kalırsınız?**

- Kendinizi sürekli değişen siber güvenlik tehditlerine karşı nasıl güncel tuttuğunuza anlat.

**Aşağıdaki Terimleri açıklamanı istiyorum;**

EDR

NDR

XDR

MDR

SOC

SIEM

SOAR

IOC

MISP