MAY CYBER TECHNOLOGY

>SCOP NET

ÜRÜN ÜSTÜNLÜKLERİ

• Altyapı Kontrolü.
Ağda yer alan cihazlar için kimlik doğrulaması yapılır ve yetkilendirme işlemi gerçekleştirilir.

• Kritik Sistemler İçin Tehdit Tespiti
Son kullanıcı makinelerinin ve ağın denetlenmesi ile kritik sistemleri hedefleyen tehditler belirlenir.

• Gerçek Zamanlı Analiz
Sistem Windows/MAC/Linux bilgisayarların ve ağ cihazlarının envanterini toplar ve bu bilginin analizini sağlar.

• Düşük Sahip Olma Maliyeti
Yetkisiz cihazların otomatik yönetilmesi sayesinde oluşabilecek iş yükü önlenir.

• Yönetilebilir BYOD (Bring Your Own Device/ Kendi Cihazını Getir) Stratejisi Oluşturma
BYOD bir çok kurum için ağ yönetimini zorlaştırmaktadır. scopNET ile BYOD stratejisi kolaylıkla uygulanabilir.

• Kolay Uygulama, Kolay Yönetim
scopNET ağ üzerinde herhangi bir değişiklik gerektirmeden, ağ altyapısı üzerinde birden fazla yöntem kullanarak tespit ve engelleme yapabilmektedir.

Denetlenmeyen veya yetkisiz cihazların kurumsal ağlara dahil olması önemli riskleri beraberinde getirmektedir. Bu cihazlar yetkisiz bilgi erişimlerine, bilgisayar ağlarının zarar görmesine ve önemli bilgilerin yetkisiz kişilerin eline geçmesine neden olabilmektedir. scopNET bilgisayar ağlarına yetkisiz erişimleri engelleyen, gelişmiş tehdit analizi ile zararlı yazılımları tespit edebilen ve 802.1x bağımlılığı olmayan bir çözümdür.

MODÜLLER

Süreç Otomasyon Katmanı

Ağ Taraması	Envanter Toplama	Tehdit Analizi	Uyumluluk Politikaları Kontrolü
Mobil Cihaz Yönetim Entegrasyonu	SIEM Entegrasyonu	Olay Yönetimi	Korelasyon

Entegrasyon Katmanı

YAPISAL ÖZELLİKLER

scopNET ağ erişimini yetkilendirmek için farklı yöntemler sunar. Sistem yönlendirici, anahtarlama cihazları ve güvenlik duvarları ile entegre edilebilir. ARP paket yönlendirme veya TCP Reset gibi yöntemler ile ağ cihazlarına bağımlı olmadan çalışabilir.

Son kullanıcı makinelerinde herhangi bir yazılım kurulum gereksinimi yoktur.
Tüm tehdit analizleri ve envanter toplama işlemleri ajansız yapılabilir. Kurumsal ağlarda az değişiklik gerektirmesi nedeniyle scopNET uygulaması kolay bir çözümdür.

Yeni bir cihaz ağa dahil olduğu zaman öncelikle sınıflandırma yapılır.
Cihazın sınıflandırılmasında Windows WMI, Windows RPC, SNMP ve SSH protokolleri kullanılır. Windows, Linux ve MAC işletim sistemleri desteklenmektedir.
Sistem üzerinden envanter bilgileri gerçek zamanlı olarak görüntülenebilmektedir.

Captive-Portal yapısı ile benzersiz bir son kullanıcı deneyimi sunulmaktadır.
Kısa mesaj servisi entegrasyonu ile misafir kullanıcısına kısıtlı ağ erişimi sağlanabilir.

scopNET, Mobil Cihaz Yönetimi çözümleri ile entegre edilebilir. Entegrasyon ile mobil cihazların daha iyi yönetilmesi sağlanır.

Gelişmiş tehdit analizi ile ağ içerisinde yer alan zararlı programlar tespit edilir.
Port tarama, zayıf şifre kullanımı ve güvenlik olay kayıtlarının analizi ile güvenlik riskleri tanımlanır.

MAY CYBER TECHNOLOGY

SCOP NET

ÖNEMLİ ÜRÜN ÖZELLİKLERİ

- Ağ cihazları & 802.1X bağımsız mimari yapı
- Windows/MAC/Linux işletim sistemi platformları için ajansız çalışabilme
- Yetkisiz erişimler için farklı engelleme yöntemleri kullanabilme
- Kontrollü erişim için otomatik kullanıcı kaydı
- Uzak şube entegrasyonu için ek donanım/yazılım bağımsız mimari
- Entegre tehdit izleme yapısı

TEHDİT ANALİZİ

- Ağ Portu Kullanan Uygulamaların Sınıflandırılması
- Ağ Trafiği Oluşturan Uygulamaların Sınıflandırılması
- Bant Genişliği Kullanım Analizi
- Ağ Trafiği Analitiği
- Port Tarama Tespiti
- Yetkisiz Kullanıcı Adı/Şifre Kullanımı
- Zayıf SNMP Şifrelerinin Tespiti
- Zayıf Windows Şifrelerinin Tespiti
- Zararlı Program Analizi

Ankara
ODTÜ Teknokent, Mustafa Kemal Mah.
Dumlupınar Bulvarı, 280/G Kat: 2, 06530
Çankaya - Ankara / Türkiye
+90 312 227 05 09
+90 312 227 05 75
info@maysiber.com

İstanbul
Maslak No/1 Plaza
Eski Büyükdere Caddesi No: 1
Kat: 17, 34485
Maslak - İstanbul / Türkiye
+90 212 283 00 46
+90 212 283 00 47
info@maysiber.com

GENEL ÖZELLİKLER

- Ajansız mimari
- Bir bilgisayarın ağ erişimi önlemek için farklı yöntemler kullanabilme:
  - ARP Zehirlenmesi
  - Switch Port Kapatabilme
  - Switch Port VLAN Değiştirebilme
  - ACL Yönetimi
  - TCP Reset Gönderimi
- WMI veya uzaktan kütük erişimi ile herhangi bir bilgiyi güvenlik doğrulaması için kullanabilme:
- Merkezi yönetim ve dağıtım
- Dağıtık mimari desteği
- Web tabanlı arayüz
- Detaylı raporlama
- Misafir yönetimi için Captive-Portal
- Entegre SIEM altyapısı
- Cihaz sınıflandırılması için detaylı ağ tarama

AĞ ERİŞİM KONTROLÜNDEKİ ZORLUKLAR

Ziyaretçi Erişimi Organizasyona çeşitli nedenlerle gelen ziyaretçilerin yetkilendirilmeleri ve kontrollü olarak kurumsal ağa dahil edilmeleri önemli bir sorundur. Bu erişim talebi; internet erişimi, destek için gelen bir yüklenici firma personeli veya ayrıcalıklı bir ziyaretçi tarafından olabilir.

Artan Mobil Cihaz Kullanımı Çalışanların kendi mobil cihazını kurumsal ağda kullanma oranının artması kurumların ortak sorunudur. Her geçen gün daha fazla kullanıcı mobil cihazları ile kurumsal kaynaklara erişmek istemektedir.

Kritik Sistemleri Hedefleyen Tehditler Kritik sistemlere yapılan saldırılarda iç ağ kullanımı artmaktadır. İç ağ içerisindeki farklı erişim gereksinimleri nedeniyle saldırılardan sistemleri korumak çok daha zordur.

Uyumluluk Gereksinimleri BT güvenliği ile ilgili her standart doğru yetki seviyelerinin verilmesini ve etkin bir denetim altyapısının kurulmasını hedeflemektedir. Erişim kontrolü, karmaşık ve dağıtık ağlar için büyük bir sorundur.

Heterojen & Dağıtık Ağ Altyapısı Kablosuz ağların ve uç noktaların artmasıyla, NAC çözümlerinin kullanımında önemli sorunlar yaşanmaktadır. Geleneksel NAC çözümleri 802.1x desteği gerektirir ve ağ yöneticilerine ağdaki değişiklikler nedeniyle iş yükü oluşturur. Bu nedenle birçok kurum NAC uygulamasını sadece merkez ofislerinde devreye almaktadır.