MAY CYBER TECHNOLOGY

scop SOC

ÖNEMLİ ÜRÜN ÖZELLİKLERİ

- SOC Süreçlerinin Merkezi Olarak Yönetilmesinin Sağlanması
- Merkezi Otomatik Keşif, Zafiyet Tarama, SIEM, Sistem İzleme ve Süreç Yönetim Altyapısı
- Siber İstihbarat Analiz Altyapısı ile Güvenlik Riski Taşıyabilecek Bağlantıların Tespit Edilmesi
- 500 TB+ Veri Üzerinde Gerçek Zamanlı Arama Yapabilme
- İstemci Yönetimi ile Bilinmeyen Uygulamaların Ağ Trafiğinin ve Kullanıcı Dosyalarına Erişiminin Engellenmesi

SOC KURULMASINDAKİ ZORLUKLAR

Entegrasyon Zorlukları
Etkin bir SOC, bileşenler arasında entegrasyon gerektirmektedir. Entegrasyonda yaşanan sorunlar, başarısızlığa veya maliyetin yükselmesine neden olmaktadır.

Veri İhlali Kaynakları Sayısında Artış
İnterneti kullanan hizmetlerin artması ve Kendi Cihazını Getir (BYOD), veri ihlallerine neden olan kaynakların sayısını önemli derecede artırmaktadır. Bu artış kurumların kritik verilere erişim izlemelerinde büyük zorluklar yaşamalarına neden olmaktadır.

Yüksek Boyutlarda Log Varlığı
Günümüzün rekabetçi ortamında BT altyapıları ile gittikçe daha fazla hizmet sağlanmaktadır. Bu değişime ek olarak olarak kullanıcıların söz konusu hizmetlere erişmek için kullandığı cihazların sayısı da artmaktadır. Bunun bir sonucu olarak da işlenmeyi ve analiz edilmeyi bekleyen denetim verisi sürekli artmaktadır.

Bilgi Körlüğü
Güvenlik ihlalleri tesadüfen veya düzenli denetimler sırasında fark edilmektedir. İhlalin kaynağındaki loglar silinebilmekte ve ihlalin etkisi bile bazen fark edilememektedir. Denetim verisinin analiz edilmesindeki yetersizlikler bilgi körlüğünün en önemli nedenlerinden bir tanesidir.

Kullanıcı Cihazlarının İzlenmesi
Kullanıcı cihazları bilgi erişim kaynaklarıdır. Bu cihazların yüksek miktarı ve dağınık yapısı denetlenmelerini zorlaştırmaktadır.

Kurumların bilgi teknolojilerine daha bağımlı hale gelmesiyle birlikte siber güvenliğin önemi sürekli olarak artmaktadır. Siber güvenlik altyapısının etkin yönetilebilmesi için güvenlik operasyon merkezleri önemli bir unsur haline gelmiş durumdadır. scopSOC, kurumların güvenlik operasyon merkezlerini etkin yönetebilmesi için bütünleşik bir platform sunmaktadır.

MODÜLLER

Süreç Otomasyon Katmanı

Varlık Tespiti | **Açıklık Tarayıcı** | **SmartAgent** | **İzleme**

Siber İstihbarat Ağı | **SIEM** | **Olay Yönetimi** | **Korelasyon**

SOC Kontrol Paneli / Entegrasyon Katmanı

YAPISAL ÖZELLİKLER

scopSOC, Güvenlik Operasyon Merkezleri yönetimi için geliştirilmiş; SIEM, istemci yönetimi, olay yönetimi, izleme, envanter analizi, zafiyet tarama ve siber istihbarat analizi sunan bütünleşik bir platformdur. scopSOC tüm güvenlik altyapısının merkezi olarak yönetilmesini sağlar.

SIEM

scopVISION, büyük veri teknolojisi kullanarak ajansız log toplama ve toplanan veriler üzerinde analitik işlemler yapılmasına imkan sağlar. Gelişmiş korelasyon yetenekleri ile güvenlik tehditlerinin tespit edilmesine katkı sağlar. Yüksek seviyede özelleştirme imkanı sunan kontrol paneli görselleştirmeleri Kibana tabanlıdır. Kendine özgü olarak tasarlanan veri analiz motoru ile toplanan bilgi standartlaştırılır ve etiketlenir.

Ajansız log toplama altyapısını kullanarak, toplanan veri filtrelenir ve merkezileştirilir. RPC, WMI, SSH, Telnet, ODBC ve JDBC desteklenen protokollerden bazılarıdır. 300'den fazla farklı log çeşidi desteklenmektedir. Toplanan loglar üzerinde "full-text" arama yapılmaktadır. Biçim sınırlaması olmadan loglar toplanabilir. Ağ trafiğinin analizinde Netflow, Sflow ve Sniffing desteklenmektedir. Tek bir cihaz ile 15000 EPS performans sağlanmaktadır. 500 TB'den fazla log üzerinde arama saniyeler içerisinde yapılabilmektedir. Günde 1 TB üzerinde veri kolaylıkla indekslenebilmektedir.

Gelişmiş korelasyon özellikleri, güvenlik riskleri için gerçek zamanlı analiz imkanı sağlar.

MAY CYBER TECHNOLOGY

>scop SOC

scopSoc NEDEN FARKLIDIR?

• Klasik SIEM çözümleri ile karşılaştırıldığında scopSOC daha ölçeklenebilir bir yapı sunmaktadır. 500 TB'den fazla log verisi içerisinde gerçek zamanlı olarak arama yapılabilir.
• Akıllı istemci yönetimi ile entegre edilmiş olan SOC platformu MAY SİBER TEKNOLOJİ'ye özgüdür. Akıllı istemci yönetimi ile bilinmeyen uygulamaların yol açtığı ağ trafiği tespit edilebilmektedir.
• Dosya sistemi sürekli takip edilir. Bilinmeyen bir uygulama, kullanıcıya ait dokümanlardan birini sildiğinde, söz konusu program sonlandırılabilir. Böylelikle ransomware gibi zararlılara karşı önemli bir koruma sağlanır.

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

SOC YÖNETİM PANELİ

SOC Yönetim paneli varlıkları, logları ve uyarıları izlemek için merkezi bir ara yüz sunar. İzleme, otomatik keşif, zafiyet tarama ve SIEM modüllerinden gelen tüm bilgi tek bir noktada konsolide edilir. Esnek arama ve özelleştirmede Kibana'dan yararlanarak, yüksek derecede özelleştirilebilmiş görsel ekranlar oluşturulabilir.

AKILLI İSTEMCİ YÖNETİMİ

İstemcilerde kullanılan antivirüs veya saldırı engelleme sistemi gibi çözümler güvenlik ihlallerini ve veri sızıntılarını tespit etmede başarısız olabilmektedir. Akıllı istemci yönetimi Windows İşletim sistemleri için geliştirilmiş bir uygulamadır. Sistem işletim sistemi loglarını, USB ve yazıcı aktivitelerini kayıt altına alır ve envanter değişikliklerini izler. Aktif uygulamalar takip edilerek yetkilendirilmemiş olan bir uygulamanın ağ trafiği oluşturması veya kullanıcı dosyalarını değiştirmesi engellenir. Ransomware gibi zararlı yazılımlara karşı etkin koruma sağlanır.

İZLEME

Sunucularda ajan gerekmeksizin bütün kritik birleşenler izlenebilir. WMI, RPC, SSH, ICMP ve SNMP protokolleri desteklenmektedir. Sistemler üzerinde performans analizi yapılarak muhtemel ağ tıkanıklıklarının tespit edilmesi sağlanır. SLA seviyeleri takip edilir.

ENVANTER ANALİZİ & AÇIKLIK TARAMA

Otomatik taramada bulunan cihazlar sınıflandırılır. Entegre açıklık tarama yeteneği sayesinde bir bileşenin açıklıkları, envanteri, logları ve durumunun tek bir arayüz üzerinde takip edilmesi sağlanır. Toplanan bilgiler, SIEM tarafından tespit edilen güvenlik riskleri ile ilişkilendirilir. SIEM, envanter ve açıklıklara göre risk seviyesi hesaplanır ve takip edilir.

SİBER İSTİHBARAT AĞI

Siber istihbarat analizi ile zararlı yazılım, bir suç izi ve phishing siteleri sürekli olarak takip edilir. Toplanan bilgiler kurumların ağ trafikleri ile eşleştirilerek zararlı yazılım barındıran sitelere erişim tespit edilir.

OLAY YÖNETİMİ

SIEM tarafından tespit edilen kritik olaylar, zafiyetler, yeni varlık tespitleri veya zararlı sitelere erişimler açılan çağrılar ile takip edilir.