MAY CYBER TECHNOLOGY

>SCOP VISION

ÜRÜN AVANTAJLARI

• Bütünleşik Altyapı Kontrolü
scopVISION son kullanıcı bilgisayarlarını, sunucuları, uygulamaları ve veri tabanlarını izlemek için tam bir denetim platformu sağlar.

• Kritik Sistemler Üzerindeki Tehditlerin Tespiti Güvenlik riskleri anlık olarak tespit edilir. Gelişmiş korelasyon yeteneği sayesinde toplanan bilgiler üzerinden gerçekleşebilecek anomaliler tespit edilir.

• Ağınızdaki Tüm Aktivitelerin İzlenmesi
Sistem USB ve Printer ile ilgili tüm hareketleri, envanter değişikliklerini ve tüm log kayıtlarını izler. Toplanan bilgiler ihtiyaç planlamasının daha iyi yapılmasını ve bu sayede organizasyon ağı içerisindeki bilgi akışının görünebilirliğini sağlar.

• Düşük Operasyonel Maliyet
Günlük log toplama, envanter, USB/Printer hareketlerinin takibi ve korelasyon gibi özellikler için birden fazla ürünün kullanılması gerekir. scopVISION bu ve daha fazla özelliği tek çatı altında uygun maliyetle sunmaktadır.

• Uygulama ve Yönetme Kolaylığı
Ajansız log toplayabilme yeteneği, python script desteği ve Lucene tabanlı Big Data platformu sayesinde scopVISION alt yapısı kolaylıkla uygulanır ve yönetilir.

scopVISION entegre bir güvenlik ve bilgi yönetimi platformudur. Log yönetimi, korelasyon, envanter yönetimi, yazıcı takibi, USB izleme, USB yetkilendirme, parola yönetimi ve uygulama denetim modüllerine sahip olan scopVISION, Elastic tabanlı Big Data platformu ile toplanan bilgiler üzerinde görülmemiş analiz yetenekleri sunmaktadır.

GÜVENLİK VE OLAY YÖNETİMİ ZORLUKLARI

Bilgi güvenliği ihlalleri sürekli artmaktadır. İnternet üzerinden kullanılan hizmetlerin artması ve kullanıcıların kendi cihazlarını kurumlara getirme eğilimleri (Bring Your Own Device) bilgi güvenliği risklerini artırmaktadır.

Toplanan bilgisayar kayıtlarının hacmi beklenenden daha büyük bir hızla artmaktadır. Kurumların teknoloji altyapılarının büyüklüğü, bu altyapılar üzerinden sunulan hizmetlerin çeşitliliği ve bu hizmetlerden yararlanan kullanıcı sayıları bu artışın en önemli nedenidir.

Güvenlik ihlalleri genellikle düzenli denetimler sırasında veya tesadüfen tespit edilir. Geç tespitin en önemli nedenlerinden bir tanesi verilerin analiz edilmesindeki yetersizliklerdir.

Son kullanıcı hataları bilgi sızıntılarının yaşanmasındaki en önemli nedenlerden bir tanesidir. Son kullanıcıların sistemlerde yaptıkları işlemlerin denetlenememesi son kullanıcı kaynaklı risklerin tespitini zorlaştırmaktadır.

Dağınık ve karmaşık teknoloji altyapısına sahip kurumlarda denetim gereksinimlerinin karşılanması büyük zorluklar içerir.

YAPISAL ÖZELLİKLER

Elastic tabanlı büyük veri platformu veri toplama ve analiz için kullanılır. Ajansız log toplama altyapısı ile toplanan veriler filltrelenir ve merkezileştirilir. Gelişmiş korelasyon özellikleri ile güvenlik riskleri gerçek zamanlı tespit edilir.

Son kullanıcı makinelerinin denetimi için Windows tabanlı bir uygulama kullanıcı bilgisayarlarına kurulmaktadır. İlgili uygulama Active Directory üzerinden politikalar ile veya IP aralığının taranması ile tespit edilerek bilgisayarlara kurulur.

Uygulama yüklendikten sonra, uygulamanın durumu merkezi olarak izlenir. Bir sorun oluşursa veya bir makinede uygulama kaldırılırsa güvenlik yöneticilerine uyarı gönderilir. Envanter analiz modülü sayesinde yazılım yüklemeleri/kaldırılmalar, bilgisayarlarda çalışan programlar ve birçok benzer bilgi izlenebilir. Gerekli herhangi bir envanter WMI protokolü kullanılarak alınabilir.

scopVISION ayrıca USB diskleri ve yazıcıları denetleyebilir. USB diskler yetkilendirilebilir. scopVISION bu yeteneklerine ilave olarak yerel kullanıcı hesabı şifresini yönetebilir.

Tüm kurallar merkezi olarak yapılandırılır. Alarmlar merkezi olarak yönetilir.

MAY CYBER TECHNOLOGY

SCOP VISION

Son Kullanıcı Makinelerinin Denetimi

- Log Yönetimi
- USB Yönetimi
- Yazıcı Yönetimi
- Ağ Paylaşımlarının İzlenmesi
- Envanter Analizi
- Veri Sızıntı Analizi
- Ağ Trafik Analizi
- Yetkisiz Dosya Erişim Kontrolü

GENEL ÖZELLİKLER

- Veri analizi için Elastic Tabanlı Büyük Veri Platformu
- Tek bir cihazla 15.000 EPS log toplama
- 200+ farklı uygulama ve işletim sisteminden log toplayabilme
- Ajanlı veya ajansız log toplayabilme
- Gelişmiş korelasyon
- Gerçek zamanlı sistemlere yetkisiz erişim tespiti (log silme işlemleri, log ayarlarının değiştirilmesi, başarısız oturum açma denemeleri vs.)
- Envanter yönetimi. Envanter değişikliklerine göre alarm üretilmesi
- Yerel yönetici hesapları ve parolalarının yönetimi
- Dosyaların çıkarılabilir disklere kopyalanmasının takip edilebilmesi
- Merkezi kurulum
- Yazılımın kaldırılması veya uygulamanın durması nedeniyle oluşan problemlerin otomatik tespit edilmesi
- Toplanan tüm veriler üzerinden rapor oluşturma ve analiz yeteneği
- Web tabanlı arayüz

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