Güvenlik Operasyon Merkezi Nedir?

Güvenlik operasyon merkezleri, kurum bilişim altyapısının güvenlik ihlallerine karşı 7 gün 24 saat izlendiği, olabilecek ihlallerin önceden değerlendirilip önlenmeye çalışıldığı, ihlal tespit edilmesi halinde ise olayın nedenini tespit etmeye ve olumsuz sonuçları en aza indirmeye yönelik operasyonların yürütüldüğü ve yönetildiği merkezdir.

Güvenlik Operasyon Merkezi Neden Gereklidir?

- Bilgi Sistem altyapısında kullanılan sistemlerin 7x24 izlenmesi ve analiz edilmesi
- Oluşan güvenlik ihlallerinin tespiti
- Tespit edilen güvenlik olaylarını önleyici tedbirlerin alınması
- Tespit edilen ihlallerin ilgili birimlere bildirilmesi
- İş sürekliliğinin (business continuity) sağlanması
- Detaylı Raporlama (Kullanılabilirlik, Performans, vb.)

Yukarıda belirtilen gereksinimler birçok kurum ve kuruluş için artık vazgeçilmez hale gelmiştir. Bu temel gereksinimleri karşılamak için Güvenlik Operasyon Merkezi kurulumu kaçınılmaz bir durumdur.

Güvenlik Operasyon Merkezinde Neler Olmalı?

Güvenlik Operasyon Merkezlerinin temel bileşeni SIEM sistemleridir. Ancak tek başına bir SIEM sistemi yeterli olmayacaktır. Bilişim altyapısını izlemek için bir Monitoring ürünü, oluşan olayları ilgili kişilere aktarmak için bir case managament sistemi de olmalıdır. Bunların yanısıra önleyici tedbirlerin alınması için ilgili ürünlerde işlem yapabilecek yetkili ve yetkin personel ihtiyacı da bulanmaktadır.

ScopSOC Nedir?

ScopSOC, MAY Siber Teknoloji A.Ş tarafından geliştirilmiş olan bir güvenlik operasyon yönetim yazılımıdır. Güvenlik Operasyon Merkezlerinin gereksinim ve ihtiyaçları göz önünde bulundurularak geliştirilmiştir.

ScopSOC; SIEM, istemci yönetimi, olay yönetimi, izleme, envanter analizi, zafiyet tarama, uç nokta bilgisayarları(istemci) yönetimi, siber istihbarat analizi ve güvenlik otomasyon çözümü sunan entegre bir platformdur. Tüm siber güvenlik yönetim gereksinimlerinin tek bir yazılımda birleştirilmesi çok önemli kazanımlar sağlamaktadır. Güvenlik analistlerinin ihtiyaç duydukları tüm güvenlik bilgisinin tek bir sistemde konsolide edilmesi etkinliğin önemli oranda arttırılmasını sağlamaktadır. ScopSOC bileşenleri ve temel özellikleri şunlardır:

ScopVision (SIEM)

Ajansız log toplama yeteneği ile toplanan veriler büyük veri platformuna aktarılır. Veriler büyük veri platformuna aktarılırken kendine özgü olarak tasarlanan veri analiz motoru ile toplanan bilgi standartlaştırılır, anlamlandırılır ve etiketlenir. Gerektiğinde istenmeyen veriler filtrelenebilir. Bu sayede toplanan veriler üzerinde gelişmiş analitik analizler yapılmasına imkân sağlanır. Gelişmiş korelasyon yetenekleri ile güvenlik tehditlerinin tespit edilmesini kolaylaştırır. Yüksek seviyede özelleştirme imkânı sunan kontrol paneli görselleştirmeleri Kibana tabanlıdır.

Log toplamak için RPC, WMI, SSH, Telnet, ODBC ve JDBC gibi protokoller desteklenmektedir. 300'den fazla farklı log çeşidi desteklenmektedir. Toplanan loglar üzerinde "full-text" arama yapılmaktadır.

Ağ trafiğinin analizinde Netflow, Sflow ve Sniffing desteklenmektedir. 500 TB'den fazla log üzerinde arama saniyeler içerisinde yapılabilmektedir. Günde 1 TB üzerinde veri kolaylıkla depolanabilmektedir.

Gelişmiş korelasyon özellikleri, güvenlik riskleri için gerçek zamanlı tespit, uyarı ve aksiyon imkânı sunar.

ScopMon (Envanter Yönetimi)

ScopMon bileşeni, Bilgi Sistem varlıklarını otomatik olarak keşfeder ve sınıflandırır. Bu işlem için izlenecek bileşenlere herhangi bir yazılım kurulum ihtiyacı bulunmamaktadır. Tamamen ajansız bir yapı ile keşif ve izleme işlemlerini yapabilir. Keşif ve sınıflandırma sonrası varlık envanterini oluşturur. Oluşturulan varlık envanterindeki bileşenlerin durumlarını izler. Belirlenen periyotlarda varlıkların zafiyet analizlerini yapar. İzleme modülü ile performansı etkileyen saldırı ve arıza gibi durumlara ışık tutar. Varlıklar ve olaylar otomatik olarak ilişkilendirilir.

Bilgi Sistem altyapısındaki sunucu ve ağ bileşenlerinin izlenmesi ajansız olarak yapılabilmektedir.

İzlenen bileşenler için periyodik olarak zafiyet taramaları yapılabilmektedir.

Apache, Icmp, PerformanceCounter, Snmp, SnmpTrap, SnmpUtilization, Ssh, Web, Wmi seçenekleri ile sunucu ve ağ bileşenlerinin izlenmesi yapılabilmektedir.

SIEM, envanter ve açıklıklara göre risk seviyesi hesaplanır ve takip edilir.

Merkezi Olay Yönetimi (EventEngine)

Event Engine bileşeni, tüm sistem genelinde meydana gelen olayları merkezileştirir ve sınıflandırır. Güvenlik uzmanlarına, olayları metodolojik olarak değerlendirme imkânı sunar.

- Her şey bir olay
- Merkezi eylem ve olay yönetimi
- Otomatik eylemler
- 3rd party ürünlerle entegrasyon
    - Güvenlik açığı tespit edilen bilgisayarın güvenlik duvarındaki engelleme listesine eklenmesi
    - Olay kayıtlarına göre otomatik posta ve yeni olaylar
- Tanımlanmış kurallar için çoklu eylemler
- Bilinen tüm sistem verilerinin kullanımı (Assets, Monitoring, Vuln, Logs ..)

ScopDESK (Case Managament)

ScopDesk bileşeni, tüm sistem genelinde aksiyon alınması gereken tüm işlemlerle ilgili süreçlerin otomatize edilmesi için kullanılır. Alarm ve uyarılar sonrası yapılması gereken işlemleri yapması gereken birim ya da kişilere otomatik olarak yönlendirir.

- Olay/sorun/değişiklik yönetimi ve varlık takibi gibi SOC yapılarındaki süreçlerin takibi yapılabilmektedir.
- SOC ortamında yer alan analistlere gerekli problemlerin otomatik olarak açılması sağlanarak, olay yönetim takibi yapılabilmektedir.

Automatic Response

Automatic Response bileşeni, sistemde yer alan güvenlik duvarı, saldırı engelleme sistemi, Ağ Erişim Kontrol Sistemi gibi siber güvenlik bileşenleri ile entegre olarak sistem tarafından tespit edilen tehditlere karşı önleyici tedbirlerin otomatik olarak alınmasını sağlar. Bu sayede yetkili ve yetkin personel ihtiyacını büyük ölçüde minimize eder.

ScopClient (İstemci Yönetimi)

İstemcilerde kullanılan Antivirüs veya saldırı engelleme sistemi gibi çözümler güvenlik ihlallerini ve veri sızıntılarını tespit etmekte yetersiz kalabilmektedir. Akıllı istemci yönetimi Windows İşletim sistemleri için geliştirilmiş bir uygulamadır. Bu uygulama ile işletim sistemi logları, USB ve yazıcı aktiviteleri kayıt altına alınır ve envanter bilgileri izlenebilir. Aktif uygulamalar takip edilerek yetkilendirilmemiş olan bir uygulamanın ağ trafiği oluşturması veya kullanıcı dosyalarını değiştirmesi engellenir. Ransomware gibi zararlı yazılımlara karşı etkin koruma sağlanır.

Neden ScopSOC?

- May Siber tarafından tamamen Türkiye'de geliştirilmiştir. Tüm kodları May Siber yazılım mühendisleri tarafından yazılmış, hiçbir kaynaktan tek bir satır kod alınmamıştır.
- Herhangi bir donanım bağımlılığı yoktur, tüm sunucu sistemleri ve sanallaştırma platformlarına uyumludur. Sınırsız genişleme desteği mevcuttur.
- İhtiyacınız olduğunda ihtiyacınız kadar genişletilebilir.
- Scop Platformunda yer alan, diğer Scop bileşen ve ürünlerini ekleyerek çözümün kapsamı genişletilebilir.
- Güvenlik Operasyon Merkezi (SOC) ihtiyaçları (İzleme, Olay Yönetimi, Uzaktan Komut Çalıştırma) dahilinde geliştirilmiş ve tüm ihtiyaçların tek bir platform üzerinde karşılanabilmesini sağlamaktadır.
- Scop Platformu aracılığıyla diğer Scop ürünleriyle sorunsuz ve gelişmiş entegrasyon desteğine sahiptir.
- Müşteriler için doğrudan yerinde ya da uzaktan destek hizmeti istek ve ihtiyaçlar dahilinde sunulmaktadır.
- Müşteriler tarafından talep edilen ve onaylanan özellik taleplerinin yıllar değil aylar içinde geliştirilip, kullanıma sunulabilmesi mümkündür.
- Ağ güvenliğinin en zayıf halkası son kullanıcı bilgisayarları için geliştirilmiş Scop Client yazılımı ile benzersiz Dosya/Ağ Etkinliği Takibi yapılabilmektedir.
- Tamamen ajansız log toplama desteği ile log kaynakları üzerine ilave bir yazılım kurulumu yapılmadan tüm olay kayıtlarının uzaktan toplanabilmesi mümkündür.

- Gerektiğinde ya da istenildiğinde log toplamak için log kaynakları üzerine ajan kurulumu yapılabilmektedir.

ScopVision Kullanımı Sonrası Kazanımlar;

- Merkezi olay motoru ile aşağıdaki örnek tiplerdeki olaylar için aksiyon alınabilmesi, Log politikalarından kaynaklı olay, Log toplama kesintileri, Korelasyon olayları, Yeni varlık tespiti, Yeni zafiyet tespiti, Sistem izleme olayları (Örneğin: İşlemcinin kritik seviyede kullanılması, bir servisin durması vb)
- Oluşan olayların otomatik varlık eşleşmesi yöntemi ile varlıklarla ilişkilendirilmesi
- Varlık yönetimi ara yüzü üzerinden hangi varlıkta hangi olayın oluştuğu bilgisine ulaşılabilmesi,
- Merkezi kimlik doğrulama altyapısı ile ayrı ayrı kullanıcılar yerine tüm sistemde tek kullanıcının işlem yapabilmesi,
- Kapsamlı yetkilendirme ile hangi kullanıcının hangi bileşenlerde hangi işlemi yapabileceğinin rol bazlı belirlenmesi,
- Güvenlik cihazları ile entegrasyon,
- Veri yetkilendirmesi ile kullanıcıların eriştikleri bileşenlerde görebileceği verinin kısıtlanması.