



Project Subject

Sophos EDR Projesi: Kurulum, Politika Yapilandırması ve Siber Güvenlik Operasyonları Raporu

Full Name

Haydar Can Kotanoglu

Project Duration

30.05.2025





Project Aims

Giriş

Projenin genel amacı, Sophos EDR çözümünün temel yönetim fonksiyonlarının öğrenilmesi, güvenlik politikalarının yapılandırılması ve temel siber güvenlik operasyonlarının (tehdit tespiti, müdahale, raporlama) pratik olarak uygulanmasıdır. Kapsam, belirlenen sanal makineler üzerinde ajan kurulumundan başlayarak, çok katmanlı güvenlik politikalarının oluşturulması, test edilmesi ve olay müdahale senaryolarının canlandırılmasını içermektedir.

Görev 1: Ajan Kurulumu

- **Amaç:** Belirlenen Windows istemci ([Windows İstemci Adı: Std/4, IP: 10.10.1.14]) ve Linux sunucu ([Linux Sunucu Adı: LnxSrv2, IP: 10.10.1.52]) sanal makinelerine Sophos ajan yazılımlarının Sophos Central üzerinden indirilerek kurulması ve merkezi yönetim konsolu ile iletişimlerinin doğrulanması.
- **Gerçekleştirilen Adımlar ve Gözlemler Özeti:**
 - Sophos Central (cloud.sophos.com) arayüzüne başarıyla giriş yapıldı.
 - Sophos Central'da "Protect Devices" (Cihazları Koru) veya "Installers" (Yükleyiciler) bölümüne gidilerek ajan yükleyicileri incelendi.
 - **Windows İstemci Kurulumu** ([Windows İstemci Adı/IP]):
 - "Download Complete Windows Installer" seçeneği kullanılarak Windows için tam yükleyici indirildi.
 - İndirilen SophosSetup.exe yükleyicisi, Windows istemci sanal makinesine aktarıldı ve yönetici haklarıyla çalıştırılarak kurulum sorunsuzca tamamlandı.
 - **Linux Sunucu Kurulumu** ([Linux Sunucu Adı/IP]):
 - "Installers" bölümünden Linux sunucusu için sunulan wget komutu kopyalandı.
 - SSH ile Linux sunucusuna ([Linux Sunucu Adı/IP]) oaklab kullanıcısı ve sağlanan parola ile bağlandı.
 - Kopyalanan wget komutu ile SophosInstall.sh kurulum betiği sunucuya indirildi.
 - chmod +x SophosInstall.sh komutu ile betiğe çalışma izni verildi.
 - sudo ./SophosInstall.sh komutu ile kurulum başlatılmaya çalışıldığında, **SSL sertifika geçerlilik hatası ("certificate is not yet valid")** ve Sophos Güncelleme Servisi'ne (SUS) bağlanamama sorunu ile karşılaşıldı. Bu sorunun, Linux sunucusunun sistem saatinin güncel olmamasından kaynaklandığı tespit edildi.
 - Sistem saati, sudo date -s "2025-05-30 20:45:00" komutuyla manuel olarak güncel tarihe ayarlandı.





- Ardından, otomatik zaman senkronizasyonu için sudo timedatectl set-ntp true komutu çalıştırıldı.
- Sistem saati düzeltildikten sonra sudo ./SophosInstall.sh komutu tekrar çalıştırılarak Sophos ajanı Linux sunucusuna başarıyla kuruldu ve "Successfully registered with Sophos Central" mesajı gözlemlendi.
- **Doğrulama:** Her iki cihazın da (Windows istemci ve Linux sunucu) Sophos Central'daki "Computers" ve "Servers" listelerinde göründüğü, "Last Active" zamanlarının güncel olduğu ve "Health State" (Sağlık Durumu) durumlarının "**Healthy**" (Sağlıklı) olduğu doğrulandı.

◆ **Önemli Not:** Linux sunucuda karşılaşılan SSL sertifika hatası, özellikle kapalı devre veya sanal ortamlarda sıkça rastlanan bir durumdur. Sistem saatinin doğru olması, güvenli (SSL/TLS) iletişim temel bir gerekliliğidir. Bu adım, problem çözme yeteneğini göstermesi açısından kritik bir gözlemdir.

Görev 2: Özel Güvenlik Politikalarının Oluşturulması ve Atanması

- **Amaç:** Sophos EDR çözümünde bulunan tüm yönetilebilir güvenlik modülleri için, varsayılan (Base Policy) politikalar yerine, belirlenen güvenlik ihtiyaçlarına göre özelleştirilmiş politikalar oluşturmak ve bu politikaları ilgili cihazlara atamak.
- **Genel Yaklaşım:** Her güvenlik modülü için, ilgili "Policies" bölümüne gidildi ve "Add Policy" ile yeni politikalar oluşturuldu. Politikalara, ayırt edici özel isimler verildi (örn: *Ozel_TP_Calisan_HaydarCan*). Her politikanın "Settings" bölümünde varsayılan ayarlardan daha sıkı yapılandırmalar tercih edildi ve son olarak ilgili cihaza atandı.
- **Uygulanan Modüller ve Detaylı Özelleştirmeler Özeti:**
 - **Threat Protection (Tehdit Koruması):**
 - "Live Protection", "Deep Learning", Fidye Yazılımı Koruması (CryptoGuard) ve Exploit Önleme dahil tüm gelişmiş korumalar aktif edildi.
 - Düşük itibarlı dosyalara karşı eylem "**Block**" olarak ayarlandı.
 - Cihazların "kırmızı sağlık durumunda" otomatik olarak kendilerini izole etmelerine izin veren ayar (**Allow computers to isolate themselves on red health**) AÇIK yapıldı.
 - Haftada bir tam ve derin tarama yapacak şekilde zamanlanmış tarama etkinleştirildi.
 - **Web Control (Web Kontrolü):**
 - Riskli dosya indirmeleri ve uygunsuz web siteleri (kumar, yetişkin içerik vb.) engellendi.
 - Veri kaybı önleme ve olay loglama seçenekleri aktif edildi.
 - Spesifik olarak "**Gamble**" (**Kumar**) gibi kategoriler için eylem "**Block**" olarak ayarlandı.
 - **Application Control (Uygulama Kontrolü):**
 - **İstemci için:** P2P, oyunlar, onaylanmamış uzak erişim araçları gibi kategoriler engellendi.





- **Sunucu için:** Sunucunun ana göreviyle ilgisi olmayan neredeyse tüm uygulama kategorileri engellenerek çok daha kısıtlayıcı bir yaklaşım benimsendi.
- **Peripheral Control (Çevre Birimi Kontrolü):**
 - USB Depolama Cihazları için varsayılan eylem "**Block**" olarak ayarlandı. Bluetooth ve modemler gibi diğer riskli çevre birimleri de engellendi.
- **Data Loss Prevention (DLP - Veri Kaybı Önleme):**
 - "Credit Card Numbers" (Kredi Kartı Numaraları) içeren verilerin taşınabilir depolama aygıtlarına transferi "**Block**" olarak ayarlandı.
 - "Gizli Proje" gibi anahtar kelimeler içeren dosyaların web tarayıcıları üzerinden yüklenmesi için "**Warn user**" veya "**Block**" eylemi tanımlandı.
- **Update Management (Güncelleme Yönetimi):**
 - Güncellemelerin daha sık (örn: her 4 saatte bir) denetlenmesi için özel bir zamanlama ayarlandı.
- **Windows Firewall (Windows Güvenlik Duvarı):**
 - Sadece Windows istemci için uygulandı.
 - PUBLIC ve PRIVATE ağlar için varsayılan gelen bağlantılar "**Block All**" olarak ayarlandı. Bu değişiklik sonrası kesilen RDP bağlantısı, TCP 3389 portuna izin veren özel bir "Allow" kuralı eklenerek tekrar sağlandı.
- **Device Encryption (Cihaz Şifreleme):**
 - Sadece Windows istemci için uygulandı.
 - Tüm sabit disklerin şifrelenmesi ve başlangıçta kimlik doğrulaması gerektirmesi hedeflendi.

☞ **Önemli Not:** Politikaları doğrudan varsayılan (Base Policy) üzerinde değiştirmek yerine, bunları klonlayarak veya yeni özel politikalar oluşturarak çalışmak en iyi uygulamadır. Bu, test süreçlerini kolaylaştırır ve genel bir soruna yol açma riskini azaltır. Ayrıca, Windows Güvenlik Duvarı politikasında RDP erişiminin kesilmesi ve ardından kural eklenerek çözülmesi, politika değişikliklerinin anlık etkilerini ve doğru yapılandırmanın önemini gösteren mükemmel bir örnektir.

Görev 3: İnternet Erişiminin Kısıtlanmasının Test Edilmesi

- **Amaç:** Windows istemcisi üzerinde uygulanan özel "Web Control" politikasının etkinliğini test etmek.
- **Gerçekleştirilen Adımlar ve Gözlemler Özeti:**
 - Windows istemci üzerinde, politikada "**Block**" olarak ayarlanan "Gamble" (Kumar) gibi kategorilere ait sitelere (örn: iddaa.com) erişim denendi.
 - Erişim denemesi sonucunda, tarayıcıda Sophos tarafından sunulan ve sitenin politika gereği engellendiğini belirten bir **engelme sayfası (block page)** görüntülendi.
 - "**Warn**" olarak ayarlanan kategorilerdeki sitelere erişimde ise kullanıcıya devam etme seçeneği sunan bir uyarı sayfası gösterdi.





- Politikada engellenmeyen genel sitelere sorunsuz eriştiği teyit edildi. Test, politikanın başarıyla çalıştığını doğruladı.

Görev 4: Zararlı Yazılım Testi (EICAR)

- Amaç:** "Threat Protection" politikasının, endüstri standartı EICAR test dosyasını algılama, engelleme ve raporlama yeteneğini test etmek.
- Gerçekleştirilen Adımlar ve Gözlemler Özeti:**
 - Zararsız bir test dosyası olan EICAR, eicar.org sitesinden indirilerek veya metin dosyasına içeriği kopyalanarak Windows istemcisine dahil edildi.
 - Dosya diske yazıldığı anda, Sophos Endpoint Agent anlık bir bildirimle (**toast notification**) tehiddi algıladı ve otomatik olarak **engelledi/karantinaya aldı**.
 - Sophos Central konsolunda, ilgili cihaza ait "Alerts" bölümünde yüksek öncelikli bir EICAR-AV-Test uyarısı oluştu.
 - "Events" ve "Detections" bölümlerinde, tehdidin adı, dosya yolu ve alınan aksiyon ("Cleaned up" veya "Quarantined") gibi detayların kaydedildiği görüldü.
 - Test, Sophos EDR'in gerçek zamanlı koruma ve raporlama yeteneklerinin başarılı olduğunu kanıtladı.

 **Önemli Not:** EICAR testi, bir güvenlik ürününün en temel algılama katmanının çalışıp çalışmadığını kontrol etmek için hızlı ve güvenli bir yöntemdir. Gerçek bir üretim ortamında bu testi yapmadan önce ilgili güvenlik ekiplerini bilgilendirmek, yanlış alarmların ve gereksiz panik durumlarının önüne geçmek için profesyonel bir yaklaşımdır.

Görev 5: Cihaz İzolasyonu ve Canlı Soru

- Amaç:** Bir tehdit sonrası, şüpheli cihazı ağdan izole etmek ve "Live Discover" (Canlı Soru) özelliği ile cihaz üzerinde adli bilişim incelemesi yapmak.
- Gerçekleştirilen Adımlar ve Gözlemler Özeti:**
 - EICAR tespiti yapılan Windows istemcisi, Sophos Central arayüzünden "**Isolate**" (İzole Et) seçeneği kullanılarak ağdan izole edildi.
 - Cihazın durumu kısa sürede "**Isolated**" olarak güncellendi.
 - "Threat Analysis Center" altındaki "**Live Discover**" bölümüne gidildi.
 - İzole edilmiş cihaz hedef seçilerek, Sophos'un hazır SQL tabanlı sorgu kütüphanesinden aşağıdaki gibi sorgular çalıştırıldı:
 - Running Processes (Çalışan İşlemler)
 - Sophos Detections on Endpoint (Uç Noktadaki Sophos Tespitleri)
 - Recent Network Connections (Son Ağ Bağlantıları)
 - Recently Created Files (Son Oluşturulan Dosyalar)
 - EICAR zararsız olduğu için anormal ek bulgulara rastlanmadı, ancak bu sorgular, gerçek bir olay anında sistemde neler olup bittiğini anlama, tehdidin yayılmasını kontrol etme ve adli analiz yapma yeteneğini pratik olarak gösterdi.





- İnceleme sonrası, cihazın izolasyonu "Remove from Isolation" seçeneği ile kaldırıldı.

❖ **Önemli Not:** Cihaz izolasyonu, bir fidye yazılımı veya solucan saldırısı durumunda tehdidin yanal hareketle diğer sistemlere yayılmasını önlemek için kullanılabilecek en etkili müdahale yöntemlerinden biridir. "Live Discover" ise sadece olay müdahalesi için değil, aynı zamanda proaktif **tehdit avcılığı (threat hunting)** için de güçlü bir araçtır.

Görev 6: Log ve Rapor Hazırlama Süreçlerinin Tanımlanması

- Amaç:** Sophos Central'in "Logs & Reports" modülünü kullanarak tipik günlük ve haftalık güvenlik raporlarının nasıl hazırlanabileceğini tarif etmek.
- Gerçekleştirilen Adımlar ve Gözlemler Özeti:**
 - Mevcut Log Türleri:** "Events", "Alerts", "Threat Detections", "Web Control Events" ve "Audit Logs" gibi tüm log kaynakları incelendi ve bunların filtrelenenebilir yapısı gözlemlendi.
 - Önceden Tanımlanmış Raporlar:** "Executive Summary", "Threat Report", "Web Usage Report" gibi şablonların özelleştirilebilir, dışa aktarılabilir ve zamanlanabilir olduğu görüldü.
 - Günlük Rapor Hazırlama Süreci (Tarif):**
 - Odak:** Son 24 saatteki kritik uyarılar, yeni tehditler, önemli politika ihlalleri ve sağlık durumu "kötü" olan cihazlar.
 - Yöntem:** "Alerts" ve ilgili modüllerin olay loglarının son 24 saatte göre filtrelenerek incelemesi.
 - Haftalık Rapor Hazırlama Süreci (Tarif):**
 - Odak:** Son 7 günlük genel tehdit trendleri, en çok ihlal edilen politikalar, genel cihaz sağlığı ve önemli olayların özeti.
 - Yöntem:** "Executive Summary" ve "Threat Report" şablonlarının "Last 7 Days" için çalıştırılması ve haftalık trendlerin analiz edilmesi.

❖ **Önemli Not:** Raporlama, yapılan teknik işlerin görünürüğünü artırmak ve güvenlik duruşunu nicel verilerle kanıtlamak için hayatı öneme sahiptir. Raporları hedef kitleye göre (yönetim için özet, teknik ekip için detaylı) özelleştirmek, iletişim etkinliğini artırır.

Sonuç Proje boyunca Sophos EDR çözümünün kurulumu, çok katmanlı güvenlik politikalarının (Tehdit Koruması, Web Kontrolü, Uygulama Kontrolü, Çevre Birimi Kontrolü, Veri Kaybı Önleme, Güncellemeye Yönetimi, Güvenlik Duvarı, Cihaz Şifreleme) oluşturulması ve atanması, tehdit simülasyonu (EICAR), olay müdahale adımları (izolasyon, Live Query) ve raporlama yetenekleri pratik olarak deneyimlenmiştir. Sophos Central'in merkezi yönetim kolaylığı, kapsamlı güvenlik özellikleri ve olaylara müdahale esnekliği başarılı bir şekilde gözlemlenmiştir. Bu proje, modern bir EDR çözümünün temel operasyonel süreçleri hakkında önemli bilgiler ve değerli pratik beceriler kazandırmıştır. Bu çalışma, siber güvenlik altyapısının güçlendirilmesi için sağlam bir temel oluşturmaktadır.





Disclosures

Açıklamalar ve Sınırlamalar

Bu bölümde projenin bağlamını ve sınırlarını belirtmek için aşağıdaki maddeleri kullanabilirsiniz:

- Kontrollü Ortam Beyanı:** Bu proje kapsamındaki tüm kurulum, yapılandırma ve test işlemleri, canlı (production) sistemlerden tamamen izole edilmiş, kontrollü bir sanal laboratuvar ortamında gerçekleştirilmiştir.
- Amaç ve Kapsam:** Çalışmanın temel amacı, Sophos EDR çözümünün yeteneklerini öğrenmek ve temel operasyonel süreçleri pratik olarak uygulamaktır. Bu rapor, bir eğitim ve değerlendirme çalışmasını temsil etmektedir.
- Simülasyon Vurgusu:** Zararlı yazılım (EICAR) ve olay müdahale (cihaz izolasyonu, canlı sorgu) testleri, gerçek bir siber saldırısı değil, kontrollü ve güvenli bir simülasyonu içermektedir. EICAR dosyası, gerçek bir tehdit unsuru değildir.
- Politika Yapılandırması:** Oluşturulan güvenlik politikaları, ürünün özelliklerini test etme amacıyla yapılandırılmış olup, en iyi uygulama (best practice) niteliğinde genel geçer kurallar olmayabilir. Gerçek bir kurum ortamında uygulanacak politikaların, o kurumun özel ihtiyaçları ve risk analizleri doğrultusunda dikkatlice özelleştirilmesi gerekmektedir.
- Veri Kullanımı:** Testler sırasında hiçbir gerçek, hassas veya kişisel veri kullanılmamıştır. Veri Kaybı Önleme (DLP) gibi modüllerde kullanılan veriler, test amaçlı oluşturulmuş sentetik verilerdir.

Participant

Haydar Can Kotanoglu

Training Institution

Oak Academy

