Proje Adı: Sophos EDR Yönetimi ve Güvenlik Operasyonları Projesi
Hazırlayan: Haydar Can Kotanoğlu
Tarih: 31 Mayıs 2025 (veya projenizi tamamladığınız tarih)

Giriş (Opsiyonel)

- 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` (veya benzeri isimdeki) yükleyici, Windows istemci sanal makinesine aktarıldı ve yönetici haklarıyla çalıştırılarak kurulum tamamlandı.
    - **Linux Sunucu Kurulumu (`[Linux Sunucu Adı/IP]`):**
        - "Installers" bölümünden Linux sunucusu için sunulan `wget` komutu (örneğin, `wget https://.../SophosInstall.sh` formatında) kopyalandı.
        - SSH ile Linux sunucusuna (`[Linux Sunucu Adı/IP]`) `oaklab` kullanıcısı ve sağlanan parola ile bağlanıldı.
        - Kopyalanan `wget` komutu Linux terminalinde çalıştırılarak `SophosInstall.sh` (veya benzeri) kurulum betiği sunucuya indirildi.
        - İndirilen betiğe `chmod +x SophosInstall.sh` komutu ile çalıştırma 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 (örn: 01 Ocak 2025 göstermesi) kaynaklandığı tespit edildi.
        - Sistem saati, öncelikle `sudo date -s "YYYY-MM-DD HH:MM:SS"` komutuyla (örn: `sudo date -s "2025-05-30 20:45:00"`) 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. Kurulum sırasında "Successfully registered with Sophos Central" mesajı gözlemlendi.
    - **Doğrulama:** Her iki cihazın da (Windows istemci `[Windows İstemci Adı/IP]` ve Linux sunucu `[Linux Sunucu Adı/IP]`) Sophos Central'daki "Computers" ve "Servers" listelerinde göründüğü, "Last Active" (Son Aktif) zamanlarının güncel olduğu ve "Health State" (Sağlık Durumu) durumlarının "Healthy" (Sağlıklı) veya yeşil simge ile belirtildiği doğrulandı.

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 `[Windows İstemci Adı/IP]` ile `[Linux Sunucu Adı/IP]` cihazlarına atamak.
- **Genel Yaklaşım:** Her bir güvenlik modülü için, öncelikle Sophos Central'da "Endpoint Protection > Policies" (Windows istemci için) veya "Server Protection > Policies" (Linux sunucu için) bölümlerine gidildi. "Add Policy" (Politika Ekle) seçeneğiyle yeni politikalar oluşturuldu. Bu politikalara, özelleştirildiklerini ve hangi cihaza/platforma ait olduklarını belirten özel isimler verildi (örn: `Ozel_TP_Calisan_HaydarCan`, `Ozel_WC_Sunucu_HaydarCan` vb.). Her politikanın "Settings" (Ayarlar) bölümünde, varsayılan ayarlardan farklı, daha sıkı veya projenin gereksinimlerine uygun yapılandırmalar tercih edildi. Son olarak, oluşturulan her özel politika ilgili cihaza (`[Windows İstemci Adı/IP]` veya `[Linux Sunucu Adı/IP]`) "Applies To" (Uygulandığı Yerler) veya benzeri bir bölümden atandı ve değişiklikler kaydedildi.
- **Uygulanan Modüller ve Detaylı Özelleştirmeler Özeti:**

- **Threat Protection (Tehdit Koruması):**
  - Hem `[Windows İstemci Adı/IP]` hem de `[Linux Sunucu Adı/IP]` için ayrı özel politikalar oluşturuldu.
  - *Temel Özelleştirmeler:* "Live Protection" ve "Deep Learning" aktif edildi. "Real-time Scanning" (yerel dosyalar, ağ paylaşımları ve internet indirmeleri için) aktif edildi. Düşük itibarlı dosyalara karşı eylem "Prompt user" yerine **"Block"** olarak ayarlandı. Fidye yazılımı koruması (CryptoGuard), exploit önleme, PUA engelleme gibi tüm gelişmiş koruma katmanları aktif edildi. **"Monitor use of driver APIs"** AÇIK konuma getirildi. Cihazların "kırmızı sağlık durumunda" **otomatik olarak kendilerini izole etmelerine izin veren ayar (`Allow computers to isolate themselves on red health`)** AÇIK yapıldı. **Zamanlanmış taramalar (`Scheduled Scanning`)** etkinleştirildi, haftada bir tam ve **derin tarama (`Enable deep scanning`)** yapacak şekilde ayarlandı.
- **Web Control (Web Kontrolü):**
  - Hem `[Windows İstemci Adı/IP]` hem de `[Linux Sunucu Adı/IP]` için ayrı özel politikalar oluşturuldu.
  - *Temel Özelleştirmeler:* Ana "Web Control" anahtarı AÇIK yapıldı. **"Additional security options - Prevent users downloading potentially risky types of file"** AÇIK yapıldı. **"Acceptable web usage - Prevent users accessing adult and other potentially inappropriate web sites"** AÇIK yapıldı. **"Protect against data loss - Allow site categories that are associated with data sharing"** AÇIK yapıldı (bu ayarın altındaki kategorilerin ayrıca yönetilmesi gerektiği anlaşıldı). **"Log web control events"** AÇIK yapıldı ve en azından engellenen/uyarı verilen olayların loglanması sağlandı. "Control sites tagged in Website Management" bölümünden, özellikle "Gamble" (Kumar) gibi riskli ve uygunsuz web sitesi kategorileri için eylem **"Block"** olarak ayarlandı. `iddaa.com` gibi spesifik sitelerin engellenmesi için ya bu kategorilerin yeterliliği test edildi ya da global "Website Management" üzerinden özel engelleme listelerine eklenmesi gerektiği anlaşıldı. Sunucu politikası, istemciye göre daha kısıtlayıcı olacak şekilde (örneğin, daha fazla kategori engelleyerek veya sadece belirli IP/URL'lere izin vererek) yapılandırıldı veya istemciyle benzer temel engellemeler uygulandı.
- **Application Control (Uygulama Kontrolü):**
  - Hem `[Windows İstemci Adı/IP]` hem de `[Linux Sunucu Adı/IP]` için ayrı özel politikalar oluşturuldu.

        - *Temel Özelleştirmeler:* İstemci için P2P yazılımları, oyunlar, onaylanmamış uzak erişim araçları gibi istenmeyen veya verimliliği düşüren uygulama kategorileri "Block" olarak ayarlandı. Sunucu için çok daha kısıtlayıcı bir yaklaşımla, sunucunun ana göreviyle ilgisi olmayan birçok uygulama kategorisi (örn: oyunlar, sosyal medya istemcileri, gereksiz geliştirme araçları) engellendi.
    - **Peripheral Control (Çevre Birimi Kontrolü):**
        - Hem `[Windows İstemci Adı/IP]` hem de `[Linux Sunucu Adı/IP]` (Sophos Central'da Linux için bu modül mevcut ve yönetilebilir olduğu teyit edildi) için ayrı özel politikalar oluşturuldu.
        - *Temel Özelleştirmeler:* Ana "Peripheral Control" anahtarı AÇIK yapıldı. **USB Depolama Cihazları** için varsayılan eylem "Allow" yerine **"Block"** olarak ayarlandı. Bluetooth, modemler gibi diğer gereksiz veya riskli görülen çevre birimleri de engellendi. Sunucu için özellikle USB depolama cihazlarının engellenmesine odaklanıldı.
    - **Data Loss Prevention (DLP - Veri Kaybı Önleme):**
        - Hem `[Windows İstemci Adı/IP]` hem de `[Linux Sunucu Adı/IP]` (Sophos Central'da Linux için bu modül mevcut ve yönetilebilir olduğu teyit edildi) için ayrı özel politikalar oluşturuldu.
        - *Temel Özelleştirmeler:* Ana "Data Loss Prevention" anahtarı AÇIK yapıldı. En az bir veya iki özel DLP kuralı tanımlandı. Örnek olarak, Sophos'un önceden tanımlanmış "Credit Card Numbers" (Kredi Kartı Numaraları) içeriğini kullanan bir kural oluşturularak bu tür verilerin "Removable Storage Devices" (Taşınabilir Depolama Aygıtları) hedefine transferi **"Block"** olarak ayarlandı. Ayrıca, "Gizli Proje", "Şirket Sırrı" gibi anahtar kelimeler içeren dosyaların "Web Browsers (uploads)" (Web Tarayıcıları - yüklemeler) veya "Cloud Storage" (Bulut Depolama) gibi hedeflere aktarımı için **"Warn user"** veya **"Block"** eylemi tanımlandı.
    - **Update Management (Güncelleme Yönetimi):**
        - Hem `[Windows İstemci Adı/IP]` hem de `[Linux Sunucu Adı/IP]` için ayrı özel politikalar oluşturuldu.
        - *Temel Özelleştirmeler:* Güncellemelerin denetlenmesi ve indirilmesi için varsayılan zamanlamadan farklı, özel bir zamanlama (örn: her gün saat 14:00 veya her 4 saatte bir gibi daha sık bir aralık) ayarlandı. Güncelleme kaynağı "Sophos" olarak bırakıldı.
    - **Windows Firewall (Windows Güvenlik Duvarı):**

        - Sadece [Windows İstemci Adı/IP] için özel bir politika oluşturuldu, çünkü Sophos Central'da Linux sunucular için merkezi bir "Firewall" politika modülü mevcut değildi.
        - *Temel Özelleştirmeler:* "Monitor & Configure Network Profiles" seçeneği aktif edildi. **PUBLIC NETWORKS** ve **PRIVATE NETWORKS** için varsayılan gelen bağlantılar "Allow All" yerine **"Block All"** (Tümünü Engelle) olarak ayarlandı. Bu değişiklik yapıldığında Uzak Masaüstü (RDP) bağlantısının kesildiği gözlemlendi. Sorunu çözmek için, bu politikaya Uzak Masaüstü Bağlantısı (RDP) için özel bir "Allow" (İzin Ver) kuralı eklendi: **Action: Allow, Direction: Inbound, Protocol: TCP, Destination Port: 3389.** Bu kural eklendikten sonra RDP erişimi yeniden sağlandı.
    - **Device Encryption (Cihaz Şifreleme):**
        - Sadece [Windows İstemci Adı/IP] için özel bir politika oluşturuldu, çünkü Sophos Central'da Linux sunucular için bu modülün yönetimi mevcut değildi/uygulanamadı.
        - *Temel Özelleştirmeler:* "Device Encryption is on" AÇIK yapıldı. **"Encrypt boot volume only" KAPALI** bırakılarak tüm sabit disklerin şifrelenmesi hedeflendi. **"Require startup authentication" AÇIK** bırakıldı. **"Encrypt used space only" KAPALI** bırakılarak tüm diskin şifrelenmesi hedeflendi. Güvenli dosya paylaşımı için **"Enable right-click context menu" AÇIK** yapıldı. Şifrelemenin ciddi bir işlem olduğu ve kurtarma anahtarlarının önemi göz önünde bulundurularak ayarlar yapılandırıldı.

Görev 3: İnternet Erişiminin Kısıtlanmasının Test Edilmesi

- **Amaç:** [Windows İstemci Adı/IP] üzerinde uygulanan özel "Web Control" politikasının ([Oluşturulan Web Kontrol Politika Adı]) etkinliğini test etmek ve yapılandırılan kısıtlamaların beklendiği gibi çalışıp çalışmadığını doğrulamak.
- **Gerçekleştirilen Adımlar ve Gözlemler Özeti:**
    - [Windows İstemci Adı/IP] sanal makinesine Uzak Masaüstü ile bağlanıldı.
    - Bir web tarayıcısı (örn: Chrome, Edge) kullanılarak, "Web Control" politikasında "Block" (Engelle) olarak ayarlanan web sitesi kategorilerine (örneğin, "Gamble" (Kumar), "Social Networking" (Sosyal Ağlar), "Adult

Content" (Yetişkin İçerik)) ait çeşitli test web sitelerine (örn: `iddaa.com` ve diğerleri) erişim denemeleri yapıldı.
    - Bu denemeler sonucunda, Sophos tarafından sunulan ve sitenin ilgili politika gereği engellendiğini belirten bir **engelleme sayfası (block page)** tarayıcıda görüntülendiği gözlemlendi.
    - Eğer "Web Control" politikasında "Warn" (Uyar) eylemi ile yapılandırılmış kategoriler varsa, bu kategorilerdeki sitelere erişim denendiğinde, Sophos'un bir **uyarı sayfası (warning page)** gösterdiği ve kullanıcıya devam etme veya işlemi iptal etme seçeneği sunduğu gözlemlendi.
    - Politikada açıkça engellenmeyen veya uyarılmayan genel amaçlı ve güvenli web sitelerine (örneğin, haber siteleri, arama motorları) sorunsuz bir şekilde erişilebildiği teyit edildi.
    - Bu testler sonucunda, oluşturulan Web Kontrolü politikasının tanımlandığı şekilde çalıştığı ve internet erişimini başarılı bir şekilde kısıtladığı doğrulandı.

Görev 4: Zararlı Yazılım Testi (EICAR)

- **Amaç:** `[Windows İstemci Adı/IP]` üzerinde uygulanan özel "Threat Protection" politikasının (`[Oluşturulan Tehdit Koruma Politika Adı]`) ve Sophos EDR çözümünün, endüstri standardı EICAR test dosyasını kullanarak bilinen bir test zararlı yazılımını algılama, engelleme ve raporlama yeteneğini pratik olarak test etmek.
- **Gerçekleştirilen Adımlar ve Gözlemler Özeti:**
    - Test için Windows istemcisi `[Windows İstemci Adı/IP]` kullanıldı. Bu cihazda ilgili özel "Threat Protection" politikasının aktif olduğu teyit edildi.
    - Güvenlik yazılımlarını test etmek amacıyla kullanılan, zararsız ancak tüm antivirüs/EDR ürünleri tarafından "zararlı" olarak algılanan standart **EICAR test dosyası** kullanıldı.
    - EICAR test dosyası, `eicar.org` web sitesinden indirilerek veya standart 68 byte'lık EICAR test dizesi bir metin dosyasına (`eicar.com` veya `eicar.txt` olarak) kopyalanıp kaydedilerek `[Windows İstemci Adı/IP]` cihazına dahil edildi.
    - EICAR dosyası sisteme dahil edilir edilmez (örneğin, diske yazıldığı anda veya çalıştırılmaya çalışıldığında), `[Windows İstemci Adı/IP]` cihazındaki Sophos Endpoint Agent tarafından bir **anlık bildirim (toast notification)** ile EICAR dosyasının zararlı bir yazılım olarak algılandığı ve otomatik olarak engellendiği/karantinaya alındığı gözlemlendi. Dosyaya erişim engellendi veya dosya anında silindi/karantinaya taşındı.

- Sophos Central konsolunda, [Windows İstemci Adı/IP] cihazıyla ilgili olarak **"Alerts" (Uyarılar)** bölümünde yüksek öncelikli bir tehdit uyarısının oluştuğu ve **"Events" (Olaylar)** ile **"Detections" (Tespitler)** bölümlerinde EICAR tespitiyle ilgili detaylı bir olayın (tehdit adı: genellikle "EICAR-AV-Test", dosya yolu, tespit zamanı, alınan aksiyon: "Cleaned up" veya "Quarantined" gibi) kaydedildiği görüldü.
- Sophos EDR'ın EICAR test dosyasını başarıyla tespit ettiği, engellediği ve bu olayı merkezi konsola raporladığı doğrulandı.

Görev 5: Cihaz İzolasyonu ve Canlı Sorgu

- **Amaç:** Bir tehdit tespitinden sonra (Görev 4'teki EICAR tespiti), tehdidin bulaştığı varsayılan [Windows İstemci Adı/IP] cihazını Sophos Central üzerinden ağdan izole ederek potansiyel yayılımını engellemek, izolasyon durumunu gözlemlemek ve ardından Sophos EDR'ın "Live Discover" (Canlı Sorgu) özelliği ile cihaz üzerinde detaylı adli bilişim (forensic) incelemesi yapmak.
- **Gerçekleştirilen Adımlar ve Gözlemler Özeti:**
  - EICAR "zararlı yazılımının" tespit edildiği Windows istemcisi [Windows İstemci Adı/IP], Sophos Central arayüzünde "Alerts" (Uyarılar) bölümünden veya doğrudan "Computers" (Bilgisayarlar) listesinden bulundu.
  - Cihaz seçildikten sonra sunulan eylemler arasından **"Isolate" (İzole Et)** veya **"Network Isolate" (Ağı İzole Et)** seçeneği kullanılarak cihazın ağ bağlantıları (Sophos Central ile olan yönetimsel iletişim hariç) kesildi.
  - Sophos Central'da, [Windows İstemci Adı/IP] cihazının durumunun kısa bir süre içinde "Isolated" (İzole Edildi) olarak güncellendiği ve bu durumun bir etiket veya simge ile belirtildiği doğrulandı.
  - EICAR test dosyası bağlamında "kötü amaçlı yazılımın etkileri", Sophos EDR'ın otomatik engelleme/karantinaya alma işlemi, ardından yapılan manuel izolasyon ve sonrasında gerçekleştirilen Live Query ile araştırma adımları olarak değerlendirildi.
  - Sophos Central'daki **"Threat Analysis Center" (Tehdit Analiz Merkezi)** altında bulunan **"Live Discover" (Canlı Sorgu)** bölümüne gidildi.
  - "Live Discover" arayüzünde, izole edilmiş olan [Windows İstemci Adı/IP] cihazı sorgu için hedef olarak seçildi.
  - Cihaz üzerinde tehdit analizi, sistem durumu tespiti ve genel adli bilişim incelemesi amacıyla Sophos'un sorgu kütüphanesinde bulunan çeşitli önceden tanımlanmış SQL tabanlı sorgular çalıştırıldı. Çalıştırılan örnek sorgular şunlardır:

        - **`Running Processes` (Çalışan İşlemler):** Sistemdeki aktif prosesleri listelemek ve anormal bir durum olup olmadığını kontrol etmek.
        - **`Sophos Detections on Endpoint` (Uç Noktadaki Sophos Tespitleri):** Cihazda Sophos tarafından yapılan tüm tespitleri, özellikle EICAR olayını doğrulamak için listelemek.
        - **`File access for a specific file` (Belirli bir dosya için dosya erişimi):** EICAR dosyasının oluşturulma/erişilme aktivitelerini (varsa) incelemek.
        - **`Recent Network Connections (last hour)` (Son Saatlik Ağ Bağlantıları):** Cihazın izolasyon öncesindeki ağ aktivitelerini incelemek.
        - **`Recently Created Files (last hour)` (Son Saatte Oluşturulan Dosyalar):** Şüpheli yeni dosya oluşumlarını kontrol etmek.
    - Bu sorguların amacı, bir tehdit durumunda sistemde neler olup bittiğini anlamak, tehdidin yayılıp yayılmadığını, sistemde başka zararlı aktiviteler olup olmadığını tespit etmek ve genel bir adli analiz yapmaktı. EICAR zararsız olduğu için bu sorgularda önemli ek anormal bulgulara rastlanmadı, ancak "Live Discover" özelliğinin güçlü sorgulama ve veri toplama yetenekleri deneyimlendi.
    - Canlı Sorgularla yapılan inceleme tamamlandıktan sonra, EICAR tehdidi zaten Sophos tarafından temizlenmiş olduğu ve cihazın güvenli olduğu değerlendirilerek, cihazın ağa geri dahil edilmesi için izolasyonun kaldırılması (Sophos Central'dan "Remove from Isolation" seçeneği ile) işlemi gerçekleştirildi veya bu işlemin nasıl yapılacağı not edildi.

Görev 6: Log ve Rapor Hazırlama Süreçlerinin Tanımlanması

- **Amaç:** Sophos Central'ın "Logs & Reports" (Loglar ve Raporlar) modülünü etkin bir şekilde kullanarak, bir güvenlik operasyon merkezinin (SOC) veya güvenlik yöneticisinin ihtiyaç duyacağı tipik günlük ve haftalık güvenlik raporlarının nasıl hazırlanabileceğini anlamak, bu süreçleri tarif etmek ve önemli raporlama metriklerini belirlemek.
- **Gerçekleştirilen Adımlar ve Gözlemler Özeti:**
    - Sophos Central'daki **"Logs & Reports"** ana bölümüne erişilerek genel arayüz, log kaynakları ve raporlama seçenekleri incelendi.
    - Mevcut **Log Türleri** incelendi: Bunlar arasında "Genel Olaylar (Events)", "Uyarılar (Alerts)", "Tehdit Tespit Logları (Threat Detections)", "Web Kontrolü Olayları (Web Control Events)", "Uygulama Kontrolü Olayları

(Application Control Events)", "Çevre Birimi Kontrolü Olayları (Peripheral Control Events)", "Veri Kaybı Önleme Olayları (DLP Events)" ve "Denetim Logları (Audit Logs)" gibi önemli log kaynakları bulunduğu görüldü. Bu logların tarih, cihaz, kullanıcı, olay türü gibi çeşitli kriterlere göre filtrelenebildiği gözlemlendi.

- Sophos Central tarafından sunulan **Önceden Tanımlanmış Rapor Şablonları** incelendi. Bu şablonlar arasında "Yönetici Özeti (Executive Summary)", "Tehdit Raporu (Threat Report)", "Web Kullanım Raporu (Web Usage Report)", "Cihazların Güvenlik Durumu (Endpoint Health Status Report)" gibi çeşitli kullanışlı raporların bulunduğu ve bu raporların zaman aralığı, cihaz/kullanıcı filtreleri gibi parametrelerle özelleştirilebildiği, ayrıca PDF/CSV formatlarında dışa aktarılabildiği veya zamanlanarak otomatik gönderilebildiği görüldü.
- **Günlük Rapor Hazırlama Süreci:**
  - **Odak Noktaları:** Son 24 saat içinde meydana gelen kritik ve yüksek öncelikli uyarılar, yeni tehdit tespitleri (zararlı yazılım, fidye yazılımı, PUA), önemli politika ihlalleri (sık engellenen web siteleri/kategoriler, uygulamalar, USB erişimleri, DLP olayları) ve sağlık durumu "kötü" olan veya dikkat gerektiren cihazlar olarak belirlendi.
  - **Hazırlama Yöntemi:** "Alerts" bölümü son 24 saate göre filtrelenerek, "Threats" raporu "Last 24 Hours" için çalıştırılarak ve Web Control, Application Control, DLP gibi modüllerin olay logları son 24 saat için incelenerek ilgili verilerin toplanacağı ve özetleneceği bir süreç tarif edildi.
- **Haftalık Rapor Hazırlama Süreci:**
  - **Odak Noktaları:** Son 7 günlük genel tehdit trendleri (en çok karşılaşılan tehdit türleri, en çok etkilenen cihazlar/kullanıcılar), politika uyum durumu (en çok ihlal edilen politikalar, en çok engellenen web kategorileri/uygulamalar), genel cihaz sağlık ve güncelleme durumu, önemli güvenlik olaylarının özeti olarak belirlendi.
  - **Hazırlama Yöntemi:** Sophos Central'daki "Executive Summary" veya "Threat Report" gibi haftalık özet sunabilecek rapor şablonlarının "Last 7 Days" için çalıştırılacağı, ayrıca spesifik modül raporlarından (Web Usage, Application Usage vb.) haftalık trendlerin çıkarılacağı bir süreç tarif edildi.
- Bu raporların, güvenlik duruşunun sürekli izlenmesi, iyileştirme alanlarının belirlenmesi ve yönetim bilgilendirmesi için kritik öneme sahip olduğu sonucuna varıldı.

Sonuç (Opsiyonel)

- Proje boyunca Sophos EDR çözümünün kurulumu, çok katmanlı güvenlik politikalarının (Tehdit Koruması, Web Kontrolü, Uygulama Kontrolü, Çevre Birimi Kontrolü, Veri Kaybı Önleme, Güncelleme 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'ın merkezi yönetim kolaylığı ve kapsamlı güvenlik özellikleri gözlemlenmiştir. Bu proje, modern bir EDR çözümünün temel operasyonel süreçleri hakkında önemli bilgiler ve pratik beceriler kazandırmıştır.