infinitum IT
Power of integrated Security

Yıkıcı Saldırılara Karşı Korunmak İçin Proaktif Hazırlık ve Güçlendirme

MANDIANT

İçindekiler Tablosu

GİRİŞ

Tehdit aktörleri, verileri yok etmek, kötü amaçlı faaliyet kanıtlarını ortadan kaldırmak veya sistemleri çalışamaz hale getirecek şekilde manipüle etmek için yıkıcı kötü amaçlı yazılımlardan yararlanır. Yıkıcı siber saldırılar, stratejik veya taktiksel hedeflere ulaşmak için güçlü bir araç olabilir. Saldırılar, kötü amaçlı yazılımları, silicileri(wipers) veya değiştirilmiş fidye yazılımlarını içerebilir.

Bu belge, kuruluşların bir ortamdaki yıkıcı saldırılara karşı korunmasına öncelik vermeleri için proaktif öneriler sağlamak amaçlı düzenlenmiştir. Öneriler, kuruluşları yalnızca yıkıcı saldırılardan değil, aynı zamanda bir tehdit aktörünün keşif gerçekleştirmeye, ayrıcalıkları artırmaya, yanlamasına hareket etmeye, erişimi sürdürmeye ve görevlerini gerçekleştirmeye çalıştığı olası olaylardan korumaya yardımcı olabilecek pratik ve ölçeklenebilir yöntemleri içerir. Öneriler, öncelikle şirket içi güvenlik güçlendirme ve savunmalara odaklanmıştır, ancak benzer kavramlar bulut tabanlı altyapıları da kapsayabilir.

Bu belgede özetlenen tavsiyeler, mevcut güvenlik araçlarına ek izleme işlevi görmesi içindir. Kuruluşlar, ek önleyici ve tespit edici önlemler olarak uç nokta ve ağ güvenliği araçlarından yararlanmalıdır. Bu araçlar, kötü niyetli faaliyetleri makul bir doğruluk derecesi ile tespit etmek için imzalar ve buluşsal yöntemler dahil olmak üzere geniş bir algılama yetenekleri yelpazesi kullanır. Bu belgede atıfta bulunulan özel algılama fırsatları, belirli tehdit aktörü davranışıyla ilişkilendirilir ve normal kalıplardan sapması ile tanımlanan anormal aktiviteyi tetiklemesi amaçlanır. Etkili izleme, bir kuruluşun benzersiz ortamının kapsamlı bir şekilde anlaşılmasına ve önceden belirlenmiş temel çizgilerin kullanımına bağlıdır.

Dışarıya Açık Varlıklar

Tanımlayın, Numaralandırın ve Güçlendirin

Dışarıya açık bir vektör aracılığıyla güvenlik açıklarından veya yanlış yapılandırmalardan yararlanan bir tehdit aktörüne karşı koruma sağlamak için kuruluşlar, dışarıdan erişilebilen uygulamaların ve kuruluş tarafından yönetilen hizmetlerin kapsamını belirlemelidir. Dışarıdan erişilebilen uygulamalar ve hizmetler, genellikle bilinen güvenlik açıklarından yararlanarak, ortak veya varsayılan kimlik bilgilerini kaba kuvvet kullanarak veya geçerli kimlik bilgilerini kullanarak kimlik doğrulama ile ilk erişim için tehdit aktörleri tarafından hedeflenir.

Dışarıya açık uygulamaları ve hizmetleri proaktif olarak belirlemek ve doğrulamak için dikkate alınması gereken hususlar şunlardır:

- Varlıkları ve ilgili güvenlik açıklarını (ör. Shodan, Tenable Nessus, Rapid7, Qualys) belirlemek için Mandiant Attack Surface Management'tan veya üçüncü taraf güvenlik açığı tarama teknolojisinden yararlanın.
- Kimlik doğrulama ve erişim için kullanılabilecek dışarıya açık vektörleri belirleme amacıyla odaklanmış bir güvenlik açığı değerlendirmesi veya sızma testi gerçekleştirin.
- Bir kuruluş tarafından dışarıya açık hizmetler için kullanılan ürünlerin bilinen güvenlik açıklarını azaltmak için yamalar veya güncellemeler gerektirip gerektirmediğini teknoloji satıcıları ile iletişim kurarak doğrulayın.

Tespit edilen güvenlik açıkları yalnızca yamalanmalı ve güçlendirilmemeli, aynı zamanda tanımlanan teknoloji platformları, şüpheli etkinlik veya teknoloji/cihaz değişikliklerine ilişkin kanıtların henüz oluşmadığından emin olmak için de gözden geçirilmelidir.

Çok Faktörlü Kimlik Doğrulamayı Zorlayın

Tek faktörlü kimlik doğrulamadan (SFA) yararlanan dışa açık varlıklar, kaba kuvvet saldırılarına, parola püskürtmeye veya geçerli (çalınmış) kimlik bilgileri kullanılarak yetkisiz uzaktan erişime karşı oldukça hassastır. Şu anda SFA'ya izin veren dışarıya açık uygulamalar ve hizmetler, çok faktörlü kimlik doğrulamayı (MFA) destekleyecek şekilde yapılandırılmalıdır. Ek olarak MFA, yalnızca şirket içi dışarıya açık yönetilen altyapıya erişim için değil, aynı zamanda bulut tabanlı kaynaklar için de doğrulamayı yapılandırırken, genellikle aşağıdaki yöntemler dikkate alınır (en güvenliden en az güvenliye doğru sıralanır):

• Fast Identity Online 2 (FIDO2) güvenlik anahtarı
• Yazılım/Donanım Açık Kimlik Doğrulama (OATH) belirteci
• Kimlik Doğrulayıcı Uygulaması (örneğin, Duo/Microsoft (MS) Kimlik Doğrulayıcı)
    o Parolasız oturum açma
    o Parola doğrulama
    o Anında bildirim (en az tercih edilen seçenek)
• Telefon görüşmesi
• Kısa Mesaj Servisi (SMS) doğrulaması
• E-posta tabanlı doğrulama

Spesifik MFA Yöntemlerinin Riskleri

PUSH BİLDİRİMLERİ

Bir kuruluş MFA için anında iletme bildirimlerinden yararlanıyorsa (örneğin, bir uygulama aracılığıyla kabul edilmesini veya bir mobil cihaza otomatik çağrı yapılmasını gerektiren bildirim), bir kullanıcı yanlışlıkla anında bildirimi kabul edebileceğinden, tehdit aktörleri bu tür MFA yapılandırmasını erişim girişimi için kullanabilir.

TELEFON/SMS DOĞRULAMA

Bir kuruluş MFA için telefon aramalarından veya SMS tabanlı doğrulamadan yararlanıyorsa, bu yöntemler şifrelenmez ve potansiyel olarak bir tehdit aktörü tarafından ele geçirilmeye açıktır. Bu yöntemler, bir tehdit aktörü, bir çalışanın telefon numarasını saldırgan kontrollü bir abone tanımlama modülü (SIM) kartına aktarabiliyorsa da savunmasızdır. Bu, MFA bildirimlerinin hedeflenen çalışan yerine tehdit aktörüne yönlendirilmesine neden olur.

E-POSTA TABANLI DOĞRULAMA

Bir kuruluş, erişimi doğrulamak veya MFA kodlarını almak için e-posta tabanlı doğrulamadan yararlanıyorsa ve bir tehdit aktörü, hedefinin e-postasına erişme yeteneğini zaten oluşturduysa, aktör, MFA sürecini doğrulamak ve tamamlamak için potansiyel olarak e-postaları da alabilir.

Bu MFA yöntemlerinden herhangi biri kullanılıyorsa aşağıdaki maddelere dikkat edilmelidir:

• Uzak kullanıcıları, aktif olarak oturum açmaya çalışmadıklarında bir oturum açma bildirimini asla kabul etmemeleri veya yanıtlamamaları için eğitmek.
• Güvenliği ihlal edilmiş bir hesabın göstergesi olabileceğinden, kullanıcıların şüpheli MFA bildirimlerini, bildirmeleri için bir yöntem oluşturmak.
• Kuruluş dışına e-posta mesajlarının otomatik iletilmesini önlemek için mesajlaşma politikalarının mevcut olduğundan emin olmak.

Dışa Yönelik Varlıklar ve MFA Girişimleri için Tespit Fırsatları

Kullanım Örneği	MITRE ID	Tanım
Brute Force	T1110 – Brute Force	Harici İnternet Protokolü adreslerinden (IP'ler) aşırı sayıda başarısız oturum açma ile tek bir doğru kullanıcı aranıyor. Bu risk, güçlü bir parola, MFA ve kilitleme politikası uygulanarak azaltılabilir.
Password Spray	T1110.003 – Password Spray	Genellikle benzer kaynak adreslerinden, başarısız oturumlara sahip çok sayıda hesap aranıyor.
Multiple Failed MFA Same User	T1110 – Brute Force T1078 – Valid Accounts	Aynı hesap için birden çok başarısız MFA koşulu aranıyor. Bu, daha önce güvenliği ihlal edilmiş bir kimlik bilgisinin göstergesi olabilir.

Multiple Failed MFA Same Source	T1110.003 – Password Spray T1078 – Valid Accounts	Aynı kaynaktan farklı kullanıcılar için birden çok başarısız MFA istemi aranıyor. Bu, güvenliği ihlal edilmiş birden çok kimlik bilgisinin ve erişim için MFA istemlerini/belirteçlerini "püskürtme" girişiminin göstergesi olabilir.
External Authentication from an Account with Elevated Privileges	T1078 – Valid Accounts	Ayrıcalıklı hesaplar, erişim için dahili olarak yönetilen ve güvenli ayrıcalıklı erişim iş istasyonlarını kullanmalı ve doğrudan harici (güvenilmeyen) bir kaynaktan erişilmemelidir.

Tablo 2: Dışa Yönelik Varlıklar ve MFA Girişimleri için Tespit Fırsatları

Kritik Varlık Korumaları

Etki Alanı Denetleyicisi ve Kritik Varlık Yedeklemeleri

Kuruluşlar, etki alanı denetleyicileri ve kritik varlıklar için yedeklerin mevcut olduğunu ve yetkisiz erişime veya değişikliğe karşı korunduğunu doğrulamalıdır. Yedekleme süreçleri ve prosedürleri sürekli olarak uygulamalıdır. Yedekler, hem ağ hem de kimlik segmentasyonunu içeren güvenli yerleşimler içinde korunmalı ve saklanmalıdır.

Bir kuruluşun Active Directory'si (AD) fidye yazılımı veya potansiyel olarak yıkıcı bir saldırı nedeniyle bozulursa veya kullanılamaz hale gelirse, Active Directory'yi etki alanı denetleyicisi yedeklerinden geri yüklemek, etki alanı hizmetlerini yeniden yapılandırmak için tek geçerli seçenek olabilir. Aşağıdaki etki alanı denetleyicisi kurtarma ve yeniden yapılandırma için bulunan uygulamaları, kuruluşlar proaktif olarak gözden geçirilmelidir:

• Etki alanı denetleyicilerinin ve SYSVOL paylaşımlarının bilinen iyi bir yedeği olduğunu doğrulayın (örn., bir etki alanı denetleyicisinden – backup C:\Windows\SYSVOL).

o Etki alanı denetleyicileri için bir sistem durumu yedeklemesi tercih edilir.
Not: Bir sistem durumu yedeklemesinin gerçekleşmesi için, Windows Server Yedekleme, bir etki alanı denetleyicisinde özellik olarak yüklenmelidir.

o Aşağıdaki komut, bir etki alanı denetleyicisinin sistem durumu yedeklemesini başlatmak için yükseltilmiş bir komut isteminden çalıştırılabilir.

```
wbadmin start systemstatebackup -backuptarget:<targetDrive>:
```

Şekil 1: Sistem Durumu Yedeklemesi Gerçekleştirme Komutu

o Aşağıdaki komut, bir SYSVOL yedeklemesi gerçekleştirmek için yükseltilmiş bir komut isteminden çalıştırılabilir (yönetim denetimi ve güvenlik günlüğü izinleri, yedeklemeyi gerçekleştiren hesap için de yapılandırılmalıdır).

```
robocopy c:\windows\sysvol c:\sysvol-backup /copyall /mir /b /r:0 /xd
```

Şekil 2: SYSVOL Yedekleme Gerçekleştirme Komutu

• Esnek tek ana işlem (FSMO) rollerine sahip etki alanı denetleyicilerini proaktif olarak tanımlayın, çünkü tam etki alanı geri yüklemesinin gerekli olması durumunda bu etki alanı denetleyicilerine kurtarma için öncelik verilmesi gerekir.

```
netdom query fsmo
```

Şekil 3: FSMO rollerini Barındıran Etki Alanı Denetleyicilerini Tanımlama Komutu

• Çevrimdışı yedeklemeler: Çevrimdışı etki alanı denetleyicisi yedeklerinin güvenli olduğundan ve çevrimiçi yedeklerden ayrı olarak depolandığından emin olun.

• Şifreleme: Yedekleme verileri hem aktarım sırasında (kablo üzerinden) hem de hareketsizken veya saha dışında depolama için yansıtıldığında şifrelenmelidir.

• DSRM Parola Doğrulama: Dizin Hizmetleri Geri Yükleme Modu (DSRM) parolasının her etki alanı denetleyicisi için bilinen bir değere ayarlandığından emin olun. Bu parola, yetkili veya yetkili olmayan bir etki alanı denetleyicisi geri yüklemesi gerçekleştirirken gereklidir.

• Yedekleme işlemleri için uyarıyı yapılandırın: Yedekleme ürünleri ve teknolojileri, yedekleme verilerinin kullanılabilirliği ve bütünlüğü için kritik olan işlemleri (örneğin, yedekleme verilerinin silinmesi, yedekleme meta verilerinin temizlenmesi, geri yükleme olayları, medya hataları) algılamak ve bunlara yönelik uyarı sağlamak üzere yapılandırılmalıdır.

• Rol tabanlı erişim kontrolünü (RBAC) uygula: Yedekleme ortamına ve veri yedeklemelerini yöneten uygulamalara erişim, saklanan verilere ve yapılandırma parametrelerine erişimi olan hesapların kapsamını kısıtlamak için RBAC'ı kullanmalıdır.

• Test etme ve doğrulama: Hem yetkili hem de yetkili olmayan etki alanı denetleyicisi geri yükleme süreçleri, düzenli olarak belgelenmeli ve test edilmelidir. Kritik varlıklar ve veriler için aynı test ve doğrulama süreçleri uygulanmalıdır.

İş Sürekliliği Planlaması

Kritik varlık kurtarma, genellikle bir kuruluşun İş Sürekliliği Planına (BCP) dahil edilen derinlemesine planlama ve hazırlık içeren bir süreçtir. Planlama ve kurtarma hazırlığı aşağıdaki temel yetkinlikleri içermelidir:

- Kritik iş operasyonlarına öncelik veren yedekleme, yük devretme ve geri yükleme görevleriyle uyumlu, önemli veriler ve destekleyici uygulamalar hakkında iyi tanımlanmış bir anlayış.
- Açıkça tanımlanmış varlık önceliklendirmesi ve kurtarma sıralaması.
- Kritik sistemler ve veriler için kapsamlı bir şekilde belgelenmiş kurtarma süreçleri.
- Kurtarma çabalarını desteklemek için eğitilmiş personel.
- Başarılı bir şekilde yürütülmesini sağlamak için kurtarma süreçlerinin doğrulanması.
- Verileri ve uygulama yedeklerini yönetmek ve doğrulamak için sorumluluğun net bir şekilde tanımlanması.
- Başlatma, sıklık, doğrulama ve test dahil çevrimiçi ve çevrimdışı veri yedekleme saklama ilkeleri (hem şirket içi hem de bulut tabanlı veriler için).
- Uygulama ve altyapı odaklı desteğe öncelik vermek için satıcılarla hizmet düzeyi anlaşmaları (SLA'lar) oluşturdu.

Süreklilik ve kurtarma planlaması zamanla güncelliğini yitirebilir ve süreçler genellikle ortam ve personel değişikliklerini yansıtacak şekilde yenilenmez. Değerlendirmelere, sürekli eğitime ve kurtarma doğrulama tatbikatlarına öncelik vermek, bir organizasyonun bir felaket durumuna daha iyi hazırlanmasını sağlayacaktır.

Yedeklemeler için Algılama Fırsatları

Kullanım Örneği	MITRE ID	Tanım
Volume Shadow Deletion	T1490 – Inhibit System Recovery	Bir tehdit aktörünün sistem kurtarmayı engellemek için birim gölge kopyalarını sileceği durumları aramak. Bu, komut satırı, PowerShell ve diğer yardımcı programlar kullanılarak gerçekleştirilebilir.
Unauthorized Access Attempt	T1078 – Valid Accounts	Veri yedeklemelerini yönetmek için kullanılan medyaya ve uygulamalara erişmeye çalışan yetkisiz kullanıcıları aramak.
Suspicious Usage of the DSRM Password	T1078 – Valid Accounts	Aşağıdakiler için etki alanı denetleyicilerinde güvenlik olay günlüklerini izleme: • Olay Kimliği 4794 - Dizin Hizmetleri Geri Yükleme Modu yönetici parolası belirlenmeye çalışıldı. Etki alanı denetleyicilerinde aşağıdaki kayıt defteri anahtarını izleme: HKLM\System\CurrentControlSet\Control\Lsa\DSRMAdminLogonBehavior Yukarıda belirtilen kayıt defteri anahtarının olası değerleri şunlardır: • 0 (varsayılan): DSRM Yönetici hesabı, yalnızca etki alanı denetleyicisi Dizin Hizmetleri Geri Yükleme Modunda yeniden başlatılırsa kullanılabilir. • 1: DSRM Yönetici hesabı, yerel Active Directory Etki Alanı Hizmetleri hizmeti durdurulursa, konsol tabanlı oturum açma için kullanılabilir. • 2: DSRM Yönetici hesabı, bir etki alanı denetleyicisini yeniden başlatmaya gerek kalmadan konsol veya ağ erişimi için kullanılabilir.

Tablo 3: Yedeklemeler için Algılama Fırsatları

BT ve OT Segmentasyonu

Kuruluşlar, kurumsal bilgi teknolojisi (BT) alanları, kimlikleri, ağları ve varlıkları ile operasyonel teknoloji (OT) süreçlerinin ve kontrolünün doğrudan desteklenmesinde kullanılanlar arasında hem fiziksel hem de mantıksal segmentasyon olmasını sağlamalıdır. Kuruluşlar, BT ve OT segmentasyonunu zorunlu kılarak, bir tehdit aktörünün, güvenliği ihlal edilmiş hesapları ve mevcut ağ erişim yollarını kullanarak kurumsal ortamlardan kritik görev OT varlıklarına dönme yeteneğini engelleyebilir.

OT ortamları, kurumsal kimlik ve kimlik doğrulamayı desteklemek için güvenilmeyen kimlik depolarından (örneğin, ayrılmış Active Directory etki alanları) yararlanmalıdır. **Bir kurumsal kimliğin veya varlığın tehlikeye atılması, bir tehdit aktörünün bir OT sürecini etkileme kabiliyetine sahip bir varlığa doğrudan erişim sağlama yeteneğiyle sonuçlanmamalıdır.**

BT ve OT için ayrı AD ormanlarının kullanılmasına ek olarak, segmentasyon ayrıca BT ve OT ortamlarında (yedekleme sunucuları, anti-virüs (AV), uç nokta algılama ve yanıt (EDR), atlama) ikili kullanımı olabilecek teknolojileri de içermelidir. OT segmentasyonu, kurumsal (BT) ortamında bir aksama olması durumunda, OT sürecinin kurumsal altyapı ile doğrudan bir bağımlılık (hesap, varlık, ağ yolu) olmadan güvenli bir şekilde bağımsız olarak çalışabileceği şekilde tasarlanmalıdır. Kolayca bölümlere ayrılamayan herhangi bir bağımlılık için kuruluşlar, BT (kurumsal) odaklı bir olayın kanıtı tespit edildiğinde OT ortamının etkin bir şekilde izole edilmesini sağlamak için potansiyel kısa vadeli süreçleri veya manuel kontrolleri belirlemelidir.

BT ve OT ortamlarını bölümlere ayırmak, Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) SP800-82 Rev 2: Endüstriyel Kontrol Sistemleri Güvenliği Kılavuzu (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf) gibi endüstri standartları tarafından önerilen en iyi uygulamadır.

Bu uygulama standartlarına göre BT ve OT ağlarını bölümlere ayırma işlemleri aşağıdakileri maddeleri içermelidir:

- Kurumsal (IT) ağından OT ağı içinde doğrudan erişilebilen bağlantı noktalarının, hizmetlerin ve protokollerin kapsamını kısıtlayarak OT saldırı yüzeyinin azaltılması.
- Kurumsaldan (BT) OT'ye gelen erişim, bölümlere ayrılmış bir OT, BT'den arındırılmış bölge (DMZ) içinde sonlandırılmalıdır. OT DMZ, ayrı bir kimlik doğrulama ve erişim düzeyi verilmesini gerektirmelidir (kurumsal BT alanında bulunan bir hesap veya uç noktadan yararlanmanın dışında).
- Açık güvenlik duvarı kuralları, hem kurumsal ortamdan gelen trafiği hem de OT ortamından giden trafiği kısıtlamalıdır.
- Güvenlik duvarları, yalnızca onaylanmış ve yetkilendirilmiş trafik akışlarına izin verilerek, varsayılan olarak reddetme ilkesi kullanılarak yapılandırılmalıdır. OT'yi destekleyen tüm varlıklar için çıkış (İnternet) trafik akışları da varsayılan olarak reddetme modelini izlemelidir.
- Kurumsal BT ve OT arasında kimlik (hesap) segmentasyonu uygulanmalıdır. Her iki ortamdaki bir hesap veya uç nokta, ilgili ortamın dışında atanmış herhangi bir izne veya erişim hakkına sahip olmamalıdır.
- OT ortamına uzaktan erişim, kurumsal BT ortamında atanmış uzaktan erişim izinlerine sahip benzer hesaplardan yararlanmamalıdır. OT varlıklarına ve kaynaklarına uzaktan erişim için ayrı kimlik bilgileri kullanan çok faktörlü kimlik doğrulama uygulanmalıdır.
- Güvenlik sistemleri için izolasyon ve güvenilirlik doğrulaması dahil olmak üzere manuel kontrol süreçlerinin eğitimi ve doğrulanması gerçekleştirilmelidir.

- OT altyapısını oluşturan sistemler ve cihazlar için yedeklemeler, programlama mantığı ve lojistik diyagramları depolamak için güvenli bölgele oluşturulmalıdır.
- OT cihazlarıyla ilişkili varsayılan kullanıcı adları ve parolalar her zaman varsayılan satıcı yapılandırmalarından değiştirilmelidir.

BT ve OT Segmentli Ortamlar için Algılama Fırsatları

Kullanım Durumu	MITRE ID	Tanım
Network Service Scanning	T1046 – Network Service Scanning	Bölümlere ayrılmış ortamlar arasında açık bağlantı noktalarını ve hizmetleri belirlemek için bir tehdit aktörünün dahili ağ keşfi gerçekleştirdiği örnekleri aramak.
Unauthorized Authentication Attempts Between Segmented Environments	T1078 – Valid Accounts	Başka bir ortamda oturum açmaya çalışan bir ortamla sınırlı hesaplar için başarısız oturum açmaları arama. Bu, ağlar arasında yanal hareket için kimlik bilgilerini yeniden kullanmaya çalışan tehdit aktörlerini tespit edebilir.

Tablo 4: BT ve OT Bölümlü Ortamlar için Algılama Fırsatları

Çıkış Kısıtlamaları

Seyrek olarak yeniden başlatılan sunucular ve varlıklar, komuta kontrol (C2) altyapısı için kalıcı işaretler oluşturmak üzere, arka kapılar oluşturmak için tehdit aktörleri tarafından yüksek oranda hedeflenir. Bir kuruluş, bu tür varlıklar için İnternet erişimini engelleyerek veya ciddi şekilde sınırlandırarak, bir tehdit aktörünün sunucuları tehlikeye atma, verileri çıkarma veya erişimi sürdürmek için çıkış iletişimlerinden yararlanan arka kapılar kurma riskini etkili bir şekilde azaltabilir.

Sunucuların, dahili ağ cihazlarının, kritik BT varlıklarının, OT varlıklarının ve saha cihazlarının harici siteler ve adreslerle (İnternet kaynakları) iletişim kurmaya çalışmaması için çıkış kısıtlamaları uygulanmalıdır. Varsayılan olarak reddet kavramı tüm sunucular, ağ cihazları ve kritik varlıklar (hem BT hem de OT dahil) için geçerli olmalı ve yalnızca izin verilenler listesindeki ve yetkili çıkış trafiği akışları açıkça tanımlanmış ve uygulanmış olmalıdır. Mümkün olduğunda, buna DNS tünelleme yoluyla iletişimi önlemek için izin verilenler listesine dahil edilmeyen özyinelemeli Etki Alanı Adı Sistemi (DNS) çözümlerinin engellenmesi de dahil edilmelidir.

Mümkünse, dış bağlantıları izlemek ve kötü niyetli etki alanlarına veya IP adreslerine olan bağlantıları engellemek için çıkış trafiği bir inceleme katmanı (proxy gibi) üzerinden yönlendirilmelidir. Kategorize edilmemiş ağ konumlarına (örneğin, yakın zamanda kaydedilmiş bir alan) bağlantılara izin verilmemelidir. İdeal olarak, DNS istekleri, kötü amaçlı etki alanlarına yapılan aramaları izlemek için harici bir hizmet (örneğin Cisco Umbrella, Infoblox DDI) aracılığıyla yönlendirilir.

Tehdit aktörleri genellikle, giden Sunucu İleti Bloğu (SMB) veya Web tabanlı Dağıtılmış Yazma ve Sürüm Oluşturma (WebDAV) iletişimlerine dayalı olarak kimlik bilgilerini (Yeni Teknoloji Yerel Alan Ağı (LAN) Yöneticisi (NTLM) karmaları dahil) toplamaya çalışır.

Kuruluşlar, ortamdaki herhangi bir uç noktadan izin verilen çıkış protokollerinin kapsamını gözden geçirmeli ve sınırlandırmalıdır. Hiper Metin Transfer Protokolü (HTTP) (İletim Kontrol Protokolü (TCP)/80) ve HTTP Güvenli (HTTPS) (TCP/443) çıkış iletişimleri büyük olasılıkla birçok kullanıcı tabanlı uç nokta için gerekli olsa da, harici sitelerin ve adreslerin kapsamı potansiyel olarak Web trafiği filtreleme teknolojilerine dayalı olarak sınırlıdır. İdeal olarak, kuruluşlar yalnızca önceden tanımlanmış bir izin verilenler listesine dayalı olarak çıkış protokollerine ve iletişimlerine izin vermelidir. Çıkış kısıtlamaları için yaygın yüksek riskli bağlantı noktaları şunları içerir:

- Dosya Aktarım Protokolü (FTP)
- Uzak Masaüstü Protokolü (RDP)
- Güvenli Kabuk (SSH)
- SMB
- Önemsiz Dosya Aktarım Protokolü (TFTP)
- WebDAV

Şüpheli Çıkış Trafiği Akışları için Tespit Olanakları

Kullanım Durumu	MITRE ID	Tanım
External Connection Attempt to a Known Malicious IP	TA0011 – Command and Control	Bilinen hatalı IP adreslerine yönelik denenen bağlantıları belirlemek için tehdit beslemelerinden yararlanın.
External Communications from Servers, Critical Assets, and Isolated Network Segments	TA0011 – Command and Control	Sunucular, kritik varlıklar, OT segmentleri ve saha cihazlarıyla ilişkili alt ağlardan ve adreslerden çıkış trafiği akışlarını arama.
Outbound Connections Attempted Over SMB	T1212 – Exploitation for Credential Access	Kimlik bilgileri karmalarını toplama girişimi olabileceğinden, SMB üzerinden harici bağlantı denemeleri aranıyor.

Sanallaştırma Altyapı Korumaları

Tehdit aktörleri genellikle keşif, yanal hareket, veri hırsızlığı ve potansiyel fidye yazılımı yerleştirme hedeflerinin bir parçası olarak sanallaştırma altyapısını (ör. VMware vCenter, Hyper-V) hedefler.

Sanallaştırılmış altyapının saldırı yüzeyini azaltmak için, VMware vCenter ve Hyper-V cihazları ve sunucuları için en iyi uygulama, yönetim arayüzlerine erişimi izole etmek ve kısıtlamak, esasen bu arayüzleri yalıtılmış sanal yerel alan ağları (VLAN'lar) ağ segmentleri içine yerleştirmektir. Burada bağlantıya yalnızca yönetim eylemlerinin başlatılabileceği özel alt ağlardan izin verilir.

VMware ESXi yönetim arabirimlerini korumak için, VMKernel ağ arabirim kartı (NIC), ana bilgisayarda çalışan sanal makinelere atanan aynı sanal ağa bağlı olmamalıdır. Ek olarak, ESXi sunucuları, yalnızca vCenter sunucularından konsol erişimine izin verecek şekilde kilitleme modunda yapılandırılabilir.

Kilitleme moduyla ilgili ek bilgi için https://kb.vmware.com/s/article/1008077 adresine bakın.

SSH protokolü (TCP/22), yönetim ve sorun giderme için bir fiziksel sanallaştırma sunucusuna veya aygıtına (vCenter) erişmek için ortak bir kanal sağlar. Tehdit aktörleri, yıkıcı saldırılar gerçekleştirmek üzere sanallaştırma altyapısına doğrudan erişim için genellikle SSH'den yararlanır. Yönetimsel arayüzlere erişimi kuşatmaya ek olarak, sanallaştırma altyapısına SSH erişimi devre dışı bırakılmalı ve yalnızca belirli kullanım durumları için etkinleştirilmelidir. SSH gerekliyse, bağlantıların nereden kaynaklanabileceğini sınırlamak için ağ ACL'leri kullanılmalıdır.

Kimlik segmentasyonu, sanallaştırma altyapısıyla ilişkili yönetim arabirimlerine erişilirken de yapılandırılmalıdır. Active Directory kimlik doğrulaması, fiziksel sanallaştırma yığınına doğrudan tümleşik erişim sağlıyorsa, geçerli bir Active Directory hesabını (sanallaştırma altyapısını yönetme izinleriyle) tehlikeye atan bir tehdit aktörü, verileri çalmak veya yıkıcı işlemler gerçekleştirmek için sanallaştırılmış sistemlere doğrudan erişmek için hesabı potansiyel olarak kullanabilir.

Sanallaştırılmış altyapıya yönelik kimlik doğrulama, güçlü parolalarla yapılandırılmış ve bir ortam içinde ek erişim için birlikte kullanılmayan özel ve benzersiz hesaplara dayanmalıdır. Ek olarak, sanallaştırma altyapısıyla ilişkili yönetim arayüzlerine erişim, yalnızca kritik altyapı bileşenlerine erişmek için kullanılan parolaların depolanmasını ve önbelleğe alınmasını engelleyen yalıtılmış ayrıcalıklı erişim iş istasyonlarından başlatılmalıdır.

VMWare vCenter (izolasyon için hedeflenmesi gereken) ile ilişkili yönetimsel bağlantı noktalarının listesi için https://kb.vmware.com/s/article/1008077 adresine bakın.

Hyper-V'nin güvenliğini sağlamaya yönelik en iyi uygulamaların listesi için https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/plan/plan-hyper-v-security-in-windows-server adresine bakın.

Sanallaştırma Altyapısına Erişim Tespit Olanakları

Kullanım Durumu	MITRE ID	Tanım
Unauthorized Access Attempt to Virtualized Infrastructure	T1078 – Valid Accounts	Yetkisiz hesaplar tarafından sanallaştırılmış altyapıya giriş denemeleri aranıyor.
Unauthorized SSH Connection Attempt	T1021.004 – Remote Services: SSH	Onaylanmış bir amaç için SSH etkinleştirilmediğinde veya belirli bir kaynak varlıktan beklenmediğinde bir SSH bağlantısının denendiği örnekler aranıyor.

Tablo 5: Sanallaştırma Altyapısı için Algılama Fırsatları

Şirket İçi Yanal Hareket Korumaları

Uç Nokta Güçlendirme

Windows Güvenlik Duvarı Yapılandırmaları

Şirket içi altyapıya ilk erişim sağlandıktan sonra, tehdit aktörleri erişim ve kalıcılığın kapsamını daha da genişletmeye çalışmak için yanal hareket yapacaktır. Windows uç noktalarına ortak yanal hareket teknikleri kullanılarak erişilmesini önlemek için, bir ortam içindeki uç noktalar arasında izin verilen iletişimin kapsamını kısıtlamak için bir Windows Güvenlik Duvarı ilkesi yapılandırılabilir. Bir Windows Güvenlik Duvarı ilkesi, bir Grup İlkesi Nesnesi (GPO) yapılandırmasının parçası olarak yerel veya merkezi olarak zorlanabilir.

En azından, iş istasyonundan iş istasyonuna ve iş istasyonlarından etki alanı olmayan denetleyicilere ve dosya dışı sunuculara engellenmesi gereken yanal hareket için kullanılan ortak bağlantı noktaları ve protokoller şunları içerir:

- SMB (TCP/445, TCP/135, TCP/139)
- Uzak Masaüstü Protokolü (TCP/3389)
- Windows Uzaktan Yönetim (WinRM)/Uzaktan PowerShell (TCP/80, TCP/5985, TCP/5986)
- Windows Yönetim Araçları (WMI) (Dağıtılmış Bileşen Nesne Modeli (DCOM) aracılığıyla atanan dinamik bağlantı noktası aralığı)

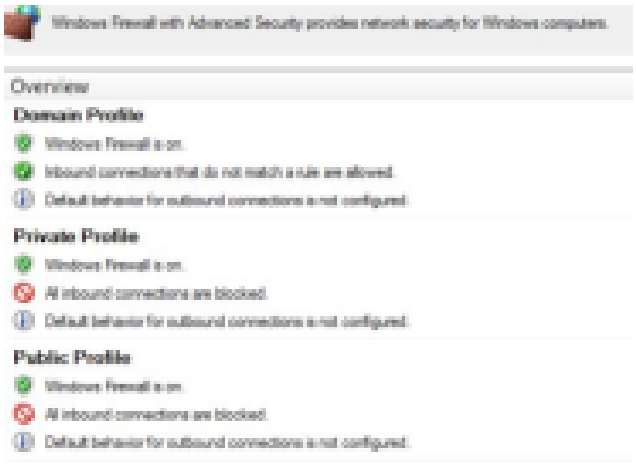
Bir GPO kullanarak (Şekil 5), Tablo 6'da listelenen ayarlar, Windows Güvenlik Duvarı'nın yönetilen bir ortamda uç noktalara gelen iletişimi kontrol etmesi için yapılandırılabilir. Başvurulan ayarlar, Özel ve Genel profiller için tüm gelen bağlantıları etkin bir şekilde engeller ve Etki Alanı profili için yalnızca önceden tanımlanmış bir engelleme kuralıyla eşleşmeyen bağlantılara izin verir.

Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security

Şekil 5: Windows Güvenlik Duvarı Kuralları Oluşturmak için GPO Yolu

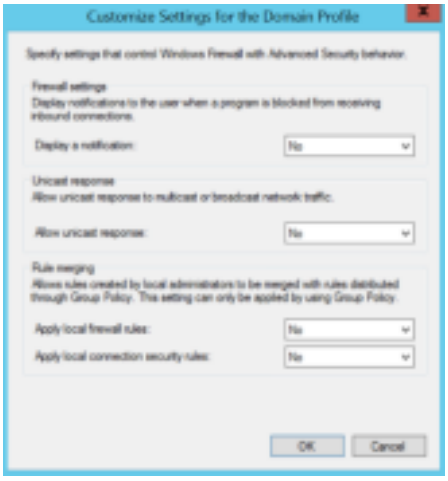
Profil Ayarları	Güvenlik Duvarı Durumu	Gelen Bağlantılar	Bırakılan Paketleri Günlüğe Kaydet	Başarılı Bağlantıları Günlüğe Kaydet	Günlük Dosya Yolu	Günlük Dosyası Maksimum Boyutu (KB)
Domain (Etki Alanı)	Açık	İzin ver	Evet	Evet	%systemroot%\system32\LogFiles\Firewall\pfirewall.log	4,096
Özel	Açık	Tüm Bağlantıları Engelle	Evet	Evet	%systemroot%\system32\LogFiles\Firewall\pfirewall.log	4,096
Açık	Açık	Tüm Bağlantıları Engelle	Evet	Evet	%systemroot%\system32\LogFiles\Firewall\pfirewall.log	4,096

Tablo 6: Windows Güvenlik Duvarı Önerilen Yapılandırma Durumu



Şekil 6: Windows Güvenlik Duvarı Öneri Yapılandırmaları

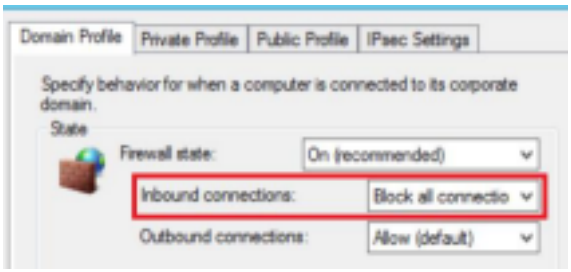
Ayrıca, yalnızca merkezi olarak yönetilen güvenlik duvarı kurallarının uygulandığından (ve bir tehdit aktörü tarafından geçersiz kılınamadığından) emin olmak için, "Yerel güvenlik duvarı kurallarını uygula" ve "Yerel bağlantı güvenlik kurallarını uygula" ayarları tüm profiller için "Hayır" olarak ayarlanabilir.



Şekil 7: Windows Güvenlik Duvarı Etki Alanı Profili Özelleştirilmiş Ayarları

Sistemleri hızlı bir şekilde kapsamak ve yalıtmak için, tüm bağlantıları engelleme (Şekil 8) merkezi Windows Güvenlik Duvarı ayarı, bir sisteme gelen bağlantıların kurulmasını engeller. Bu, iş istasyonlarında ve dizüstü bilgisayarlarda uygulanabilecek bir ayardır, ancak sunucular için zorunlu kılınırsa büyük olasılıkla operasyonları etkileyecektir, ancak bir ortamda aktif bir tehdit aktörünün yanal hareket gerçekleştirdiğine dair kanıt varsa, hızlı çözüm sağlamak için gerekli bir adım olabilir.

Not: Bu kontrol, etkin bir olayın parçası olarak kapsamayı kolaylaştırmak için geçici olarak kullanılıyorsa, olay kontrol altına alındıktan ve bir ortam içindeki sistemler arasında yeniden bağlantı kurmanın güvenli olduğu kabul edildikten sonra, Gelen Bağlantılar ayarı geri değiştirilebilir.



Şekil 8: Windows Güvenlik Duvarı - Tüm Bağlantıları Engelle Ayarları

Bir sınırlama olayı sırasında uç noktalar için tüm gelen bağlantıların engellenmesi veya en azından Etki Alanı profili yapılandırmaları pratik değilse, Tablo 7'de listelenen protokoller ya bir GPO kullanılarak ya da tabloda atıfta bulunulan komutlar aracılığıyla uygulanmalıdır.

Son kullanıcı uç noktalarına gelen bağlantı gerektirebilecek belirli uygulamalar için, yerel güvenlik duvarı ilkesi, bu tür cihazlara gelen bağlantıları başlatma yetkisine sahip kaynak sistemleri için belirli IP adresi istisnaları ile yapılandırılmalıdır.

Protocol/Port	Windows Firewall Rule	Command Line Enforcement
SMB o TCP/445, TCP/139, TCP/135	Predefined Rule Name: • File and Print Sharing	netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=no
Remote Desktop Protocol o TCP/3389	Predefined Rule Name: • Remote Desktop	netsh advfirewall firewall set rule group="Remote Desktop" new enable=no
WMI	Predefined Rule Name: • Windows Management Instrumentation (WMI)	netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=no
Windows Remote Management /PowerShell Remoting o TCP/80, TCP/5985, TCP/5986	Predefined Rule Name: • Windows Remote Management • Windows Remote Management (Compatibility) Port Rule: • TCP/5986	netsh advfirewall firewall set rule group="Windows Remote Management" new enable=no Via PowerShell: Disable-PSRemoting -Force

Tablo 7: Windows Güvenlik Duvarı Önerilen Engelleme Kuralları

Name	Group	Profile	Enabled	Action
Block WINRM SSL Port [5986] - Inbound		All	Yes	Block
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (SMB-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (Spooler Service -...	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (Spooler Service -...	File and Printer Sharing	All	Yes	Block
Remote Desktop - Shadow (TCP-In)	Remote Desktop	All	Yes	Block
Remote Desktop - User Mode (TCP-In)	Remote Desktop	All	Yes	Block
Remote Desktop - User Mode (UDP-In)	Remote Desktop	All	Yes	Block
Windows Management Instrumentation ...	Windows Management Instr...	All	Yes	Block
Windows Management Instrumentation ...	Windows Management Instr...	All	Yes	Block
Windows Management Instrumentation ...	Windows Management Instr...	All	Yes	Block
Windows Remote Management (HTTP-In)	Windows Remote Manage...	All	Yes	Block
Windows Remote Management (HTTP-In)	Windows Remote Manage...	All	Yes	Block
Windows Remote Management - Compa...	Windows Remote Manage...	All	Yes	Block

Şekil 9: Grup İlkesi aracılığıyla Windows Güvenlik Duvarı Tarafından Önerilen Kural Blokları

NTLM Kimlik Doğrulama Yapılandırmaları

Tehdit aktörleri genellikle giden SMB veya WebDAV iletişimlerine dayalı olarak kimlik bilgilerini (Windows NTLMv1 karmaları dahil) toplamaya çalışır. Kuruluşlar, Windows tabanlı uç noktalar için NTLM ayarlarını gözden geçirmeli ve NTLMv1 kimlik doğrulama isteklerini sağlamlaştırmak, devre dışı bırakmak veya kısıtlamak için çalışmalıdır.

NTLM kimlik doğrulamasını uzak sunucularla tamamen kısıtlamak için aşağıdaki GPO ayarlarından yararlanılabilir.

- Bilgisayar Yapılandırması > Windows Ayarları > Güvenlik Ayarları > Yerel İlkeler > Güvenlik Seçenekleri > Ağ Güvenliği: NTLM'yi Kısıtla: Uzak sunuculara giden NTLM trafiği
    - o Tümüne izin ver
    - o Tümünü denetle
    - o Tümünü reddet

Not: "Tümünü reddet" seçilirse, istemci bilgisayar NTLM kimlik doğrulamasını kullanarak uzak bir sunucuya kimlik doğrulaması yapamaz (kimlik bilgilerini gönderemez). "Tümünü reddet" olarak ayarlanmadan önce, kuruluşlar GPO ayarını "Tümünü denetle" zorlaması ile yapılandırmalıdır. Bu yapılandırma, denetim ve engelleme olayları, uç noktalarda (Applications and Services Log\Microsoft\Windows\NTLM) Operasyonel olay günlüğüne kaydedilecektir.

Kayıtlı herhangi bir NTLM kimlik doğrulama olayı gerekiyorsa, kuruluşlar NTLM kimlik doğrulamasını kullanmak için gerekli olan uzak sunucuların bir listesini tanımlamak için "Ağ güvenliği: NTLM'yi kısıtla: NTLM kimlik doğrulaması için uzak sunucu istisnaları ekle" ayarını yapılandırabilir.

SMB, WMI ve NTLM İletişimleri için Algılama Fırsatları

Kullanım Örneği	MITRE ID	Tanım
High Volume of SMB Connections	T1021.002 – SMB/Windows Admin Shares	Normal bir kalıbın dışında kalan SMB bağlantılarında keskin bir artış aranıyor.
Outbound Connection Attempted Over SMB	T1212 – Exploitation for Credential Access	Kimlik bilgileri karmalarını toplama girişimi olabileceğinden, SMB üzerinden harici bağlantı denemeleri aranıyor.
WMI Being Used to Call a Remote Service	T1047 – Windows Management Instrumentation	Yürütme için bir uzak hizmeti çağırmak için bir komut satırı veya PowerShell aracılığıyla kullanılan WMI aranıyor.

WMI Being Used for Ingress Tool Transfer	T1105 – Ingress Tool Transfer	Harici kaynakları indirmek için şüpheli WMI kullanımı aranıyor.
Forced NTLM Authentication Using SMB or WebDAV	T1187 – Forced Authentication	SMB veya WebDAV kullanarak olası NTLM kimlik doğrulama girişimleri aranıyor.

Tablo 8: SMB, WMI ve NTLM İletişimleri için Algılama Fırsatları

Uzak Masaüstü Protokolü Güçlendirme

Uzak Masaüstü Protokolü (RDP), tehdit aktörleri tarafından sistemlere uzaktan bağlanmak, çevreden yanal olarak daha geniş bir dahili sistem kapsamına geçmek ve kötü niyetli faaliyetler (veri hırsızlığı veya fidye yazılımı dağıtımı gibi) gerçekleştirmek için kullanılan yaygın bir yöntemdir. İnternete açık RDP'ye sahip dışa dönük sistemler yüksek bir risk oluşturur. Aktörler, bir kuruluşa ilk erişim elde etmek için bu vektörden yararlanabilir ve ardından misyon hedeflerini tamamlamak için kuruluşta yanal hareket gerçekleştirebilir.

Proaktif olarak, kuruluşlar, RDP (TCP/3389) ve internete açık diğer protokoller (SMB – TCP/445) ile sistemleri tanımlamak için genel IP adresi aralıklarını taramalıdır. En azından, RDP ve SMB, İnternet'e/İnternet'ten giriş ve çıkış erişimine doğrudan maruz bırakılmamalıdır. Operasyonel amaçlar için gerekirse, bu protokolleri kullanan sistemlerle arayüz oluşturabilecek kaynak IP adreslerini kısıtlamak için açık kontroller uygulanmalıdır.

Aşağıdaki güçlendirme, iyileştirme önerileri de uygulanmalıdır.

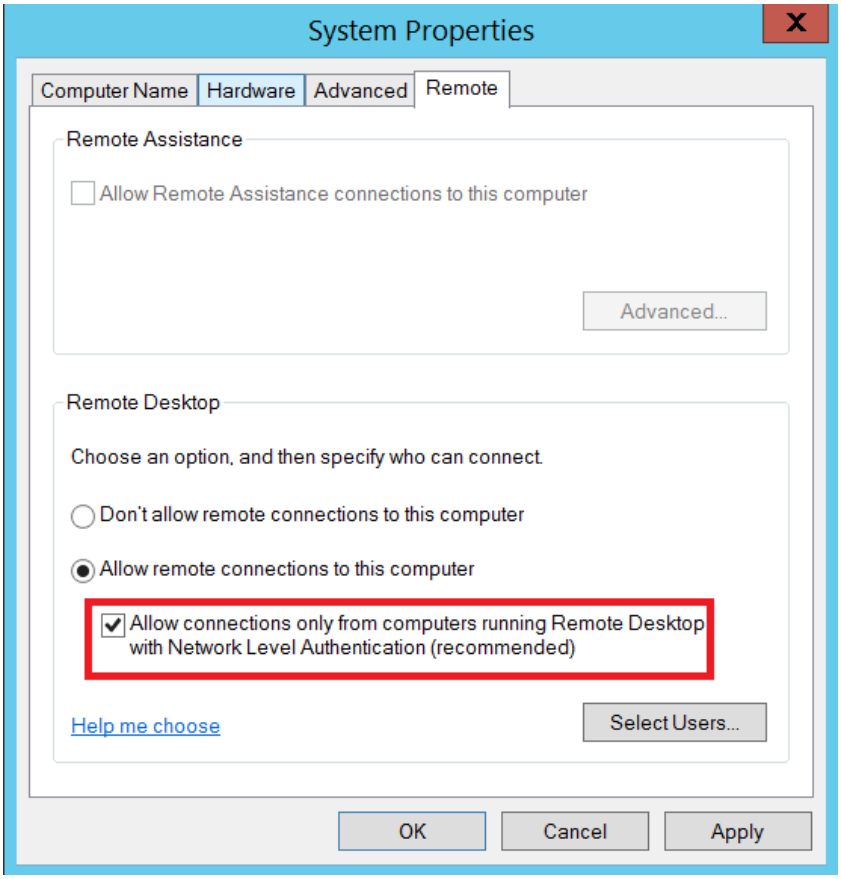
Çok Faktörlü Kimlik Doğrulamayı Zorla

Operasyonel amaçlar için dışa dönük RDP kullanılması gerekiyorsa, bu yöntem kullanılarak bağlanırken MFA zorunlu kılınmalıdır.

Bu, üçüncü taraf MFA teknolojisinin entegrasyonu yoluyla veya Uzaktan Kimlik Doğrulama Çevirmeli Kullanıcı Hizmeti (RADIUS) (https://docs.microsoft.com/en) kullanılarak bir Uzak Masaüstü Ağ Geçidi ve Azure Çok Faktörlü Kimlik Doğrulama Sunucusu kullanılarak gerçekleştirilebilir. (https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfaserver-nps-rdg)

Ağ Düzeyinde Kimlik Doğrulamadan Yararlanın

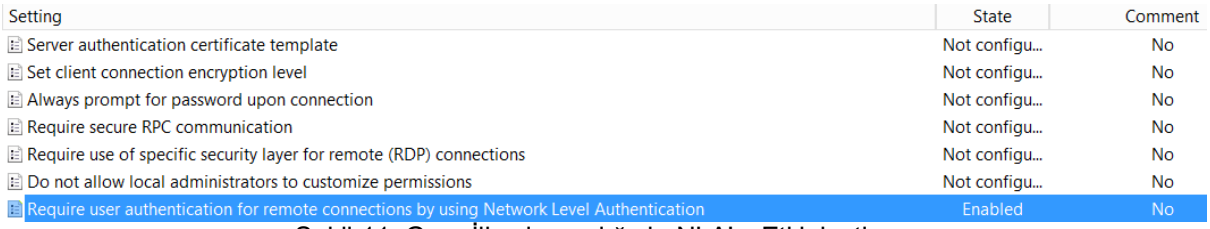
Dışarıya açık RDP sunucuları için, Ağ Düzeyinde Kimlik Doğrulama (NLA), bir bağlantı kurulmadan önce fazladan bir ön kimlik doğrulama katmanı sağlar. NLA, genellikle İnternet'e yönelik açık RDP sunucularını hedefleyen kaba kuvvet saldırılarına karşı koruma sağlamak için de yararlı olabilir. NLA, kullanıcı arabirimi (UI) (Şekil 10) veya Grup İlkesi (Şekil 11) aracılığıyla yapılandırılabilir.



Şekil 10: Kullanıcı Arabirimi aracılığıyla NLA'yı etkinleştirme

Bir GPO kullanarak, NLA ayarı şu şekilde yapılandırılabilir:

- Bilgisayar Yapılandırması > İlkeler > Yönetim Şablonları > Windows Bileşenleri > Uzak Masaüstü Hizmetleri > Uzak Masaüstü Oturum Ana Bilgisayarı > Güvenlik > Ağ Düzeyinde Kimlik Doğrulamayı kullanarak uzak bağlantılar için kullanıcı kimlik doğrulaması iste
    - Etkinleştirilmiş



Şekil 11: Grup İlkesi aracılığıyla NLA'yı Etkinleştirme

RDP için NLA'dan yararlanmayla ilgili bazı uyarılar:

- Uzak Masaüstü istemcisi v7.0 (veya üstü) kullanılmalıdır.
- NLA, başlatan sistemde kimlik doğrulama isteklerini iletmek için CredSSP'yi kullanır. CredSSP, kimlik bilgilerini başlatan sistemdeki Yerel Güvenlik Yetkilisi (LSA) belleğinde saklar ve bu kimlik bilgileri, bir kullanıcı sistemde oturumu kapattıktan sonra bile bellekte kalabilir. Bu, kaynak sistemdeki bellekteki kimlik bilgileri için potansiyel bir açığa çıkma riski sağlar.

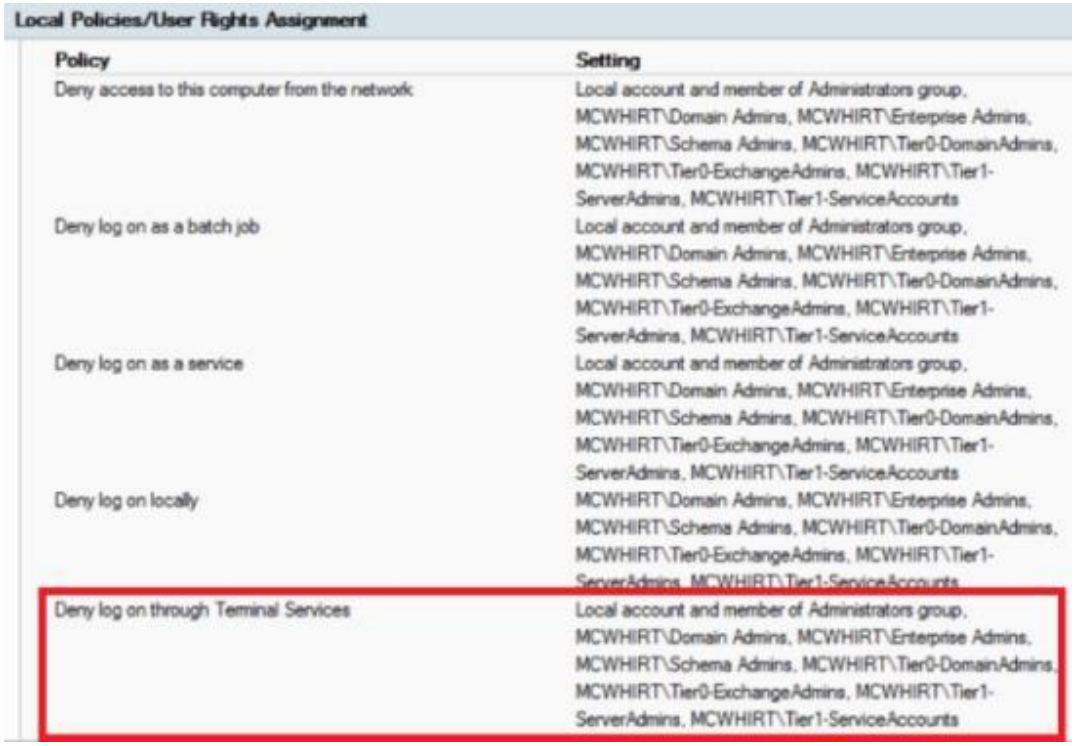
- RDP sunucusunda, RDP kullanarak uzaktan erişime izin verilen kullanıcılara, NLA zorunlu olduğunda bu bilgisayara ağdan eriş ayrıcalığı atanmalıdır. Bu ayrıcalık, genellikle kullanıcı hesaplarının yanal hareket tekniklerine karşı koruma sağlaması için açıkça reddedilir.

İdari Hesapların İnternete Açık Sistemlerinde RDP'den Yararlanmalarını Kısıtlayın

Dış dünyaya açık RDP sunucuları için, yüksek düzeyde ayrıcalıklı etki alanı ve yerel yönetim hesaplarının, RDP kullanan dışarıya açık sistemlerle kimlik doğrulama erişimine izin verilmemelidir (Şekil 12).

Bu, aşağıdaki yolla yapılandırılabilen Grup İlkesi kullanılarak uygulanabilir:

- Bilgisayar Yapılandırması > İlkeler > Windows Ayarları > Güvenlik Ayarları > Yerel İlkeler > Kullanıcı Hakları Ataması > Terminal Hizmetleri aracılığıyla oturum açmayı reddet



Local Policies/User Rights Assignment

Policy	Setting
Deny access to this computer from the network	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on as a batch job	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on as a service	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on locally	MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on through Terminal Services	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts

Şekil 12: Yüksek Ayrıcalıklı Etki Alanı ve Yerel Yönetim Hesaplarının RDP'den Yararlanmasını Kısıtlamak için Grup İlkesi Yapılandırması

Kullanım Örneği	MITRE ID	Tanım
RDP Kimlik Doğrulama Entegrasyonu	1110 – Brute Force T1078 – Valid Accounts T1021.001 – Remote Desktop Protocol	Mevcut kimlik doğrulama kuralları, RDP denemelerini içermelidir. Bu, aşağıdakiler için kullanım durumlarını içerir: • Kaba kuvvet • Parola Püskürtme • MFA Hataları, Tek Kullanıcı • MFA Hataları, Tek Kaynak • Yüksek Ayrıcalıklara Sahip Bir Hesaptan Harici Kimlik Doğrulama
RDP Üzerinden Anormal Bağlantı Denemeleri	T1078 – Valid Accounts T1021.001 – Remote Desktop Protocol	TCP/3389 gibi bilinen RDP bağlantı noktaları üzerinden anormal RDP bağlantı denemeleri aranıyor

Tablo 9: RDP Kullanımı için Algılama Fırsatları

İdari/Gizli Paylaşımları Devre Dışı Bırakma

Yanal hareket gerçekleştirmek için tehdit aktörleri, idari veya gizli ağ paylaşımlarını belirlemeye çalışabilir ve bunları bir ortamdaki uç noktalara uzaktan bağlanmak için kullanabilir. Koruyucu veya hızlı bir sınırlama önlemi olarak, kuruluşların varsayılan yönetimsel veya gizli paylaşımların uç noktalarda erişilebilir olmasını hızla devre dışı bırakması gerekebilir. Bu, aşağıdakilerden herhangi birini değiştirerek gerçekleştirilebilir:

Kayıt defteri, bir hizmeti durdurma veya MSS (Eski) Grup İlkesi şablonunu (https://www.microsoft.com/en-us/download/details.aspx?id=55319 kullanarak.

Uç noktalarda ortak yönetimsel ve gizli paylaşımlar şunları içerir:

- ADMIN$
- C$
- D$
- IPC$

Not: Özellikle etki alanı denetleyicileri dahil olmak üzere sunucularda yönetimsel ve gizli paylaşımların devre dışı bırakılması, etki alanı tabanlı bir ortamdaki sistemlerin çalışmasını ve işlevselliğini önemli ölçüde etkileyebilir.

Ayrıca, bir ortamda PsExec kullanılıyorsa, yönetici (ADMIN$) paylaşımının devre dışı bırakılması, bu aracın uç noktalarla uzaktan arabirim oluşturmak için kullanılma özelliğini kısıtlayabilir.

Kayıt Yöntemi (Registry Method**)**:

Kayıt defteri kullanılarak, uç noktalarda yönetimsel ve gizli paylaşımlar devre dışı bırakılabilir (Şekil 13 ve Şekil 14).

İş İstasyonu(Workstations):

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters DWORD Name = “AutoShareWks” Value = “0”

Şekil 13: İş İstasyonlarında Yönetim Paylaşımlarını Devre Dışı Bırakan Kayıt Değeri

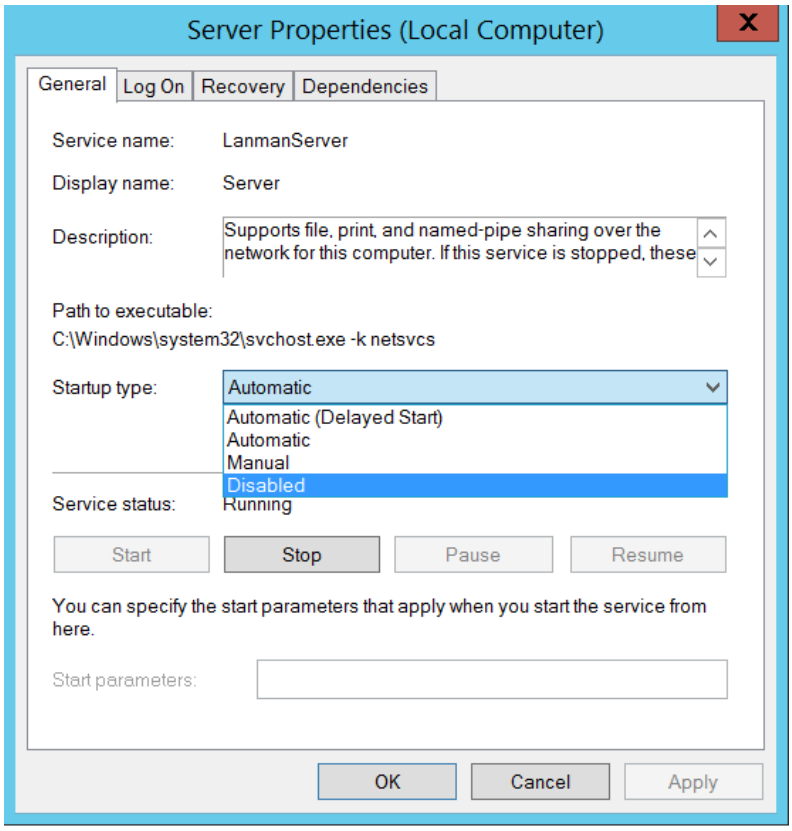
Sunucular(Servers):

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters DWORD Name = “AutoShareServer” Value = “0”

Şekil 14: Sunucularda Yönetim Paylaşımlarını Devre Dışı Bırakan Kayıt Değeri

Servis Yöntemi:

Bir uç noktada Sunucu hizmeti durdurulduğunda, uç noktada barındırılan tüm paylaşımlara erişim devre dışı bırakılacaktır.
(Şekil 15).



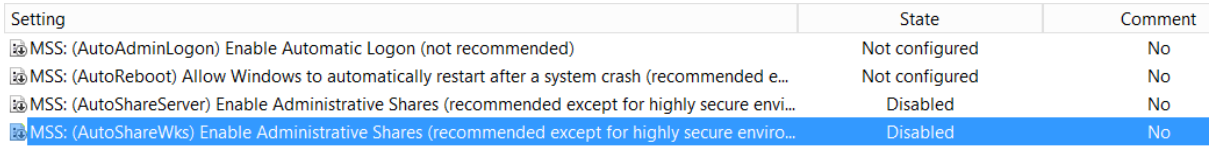
Şekil 15: Sunucu Hizmeti Özellikleri

Grup İlkesi Yöntemi:

MSS (Eski) Grup İlkesi şablonu kullanılarak, bir sunucuda veya sunucuda yönetimsel ve gizli paylaşımlar devre dışı bırakılabilir.

GPO ayarı aracılığıyla iş istasyonu (Şekil 16).

- Bilgisayar Yapılandırması > İlkeler > Yönetim Şablonları > MSS (Eski) > MSS (AutoShareServer)
  - Engelli
  -
- Bilgisayar Yapılandırması > İlkeler > Yönetim Şablonları > MSS (Eski) > MSS (AutoShareWks)
  - Engelli
  -



Şekil 16: MSS (Eski) Grup İlkesi Şablonu aracılığıyla Yönetimsel ve Gizli Paylaşımları Devre Dışı Bırakma

İdari veya Gizli Paylaşımlara Erişim Tespit Olanakları

Kullanım Örneği	MITRE ID	Tanım
Ağ Keşfi: Ağ Komutunun Şüpheli Kullanımı	T1049 - System Network Connections Discovery T1135 - Network Share Discovery	Bir ortamdaki dosya paylaşımları gibi sistemleri numaralandırmak için net komutunun şüpheli kullanımı aranıyor.

Tablo 10: İdari veya Gizli Paylaşımlara Erişim Tespit Olanakları

Windows Uzaktan Yönetimini Sağlamlaştırma

Tehdit aktörleri, bir ortamda yanal hareket etmek için Windows Uzaktan Yönetim'den (WinRM) yararlanabilir.

WinRM, tüm Windows Server işletim sistemlerinde varsayılan olarak etkindir (Windows Server 2012 ve sonrasından beri), ancak tüm istemci işletim sistemlerinde (Windows 7 ve Windows 10) ve daha eski sunucu platformlarında (Windows Server) devre dışı bırakıldı.
2008 R2).

PowerShell uzaktan iletişim (PS uzaktan iletişim), WinRM protokolünün üzerine inşa edilmiş yerel bir Windows uzaktan komut yürütme özelliğidir.

WinRM'nin devre dışı bırakıldığı Windows istemci (sunucu olmayan) işletim sistemi platformları şunları gösterir:

- WinRM dinleyicisi yapılandırılmamış
- Windows güvenlik duvarı istisnası yapılandırılmamış

Varsayılan olarak WinRM, Windows Güvenlik Duvarı kullanılarak devre dışı bırakılabilen veya WinRM kullanılarak uç noktalara bağlanmak için belirli bir IP adresi alt kümesinin yetkilendirilebileceği şekilde yapılandırılabilen TCP/5985 ve TCP/5986'yı kullanır.

WinRM ve PowerShell uzaktan iletişim, bir PowerShell komutu (Şekil 17) veya belirli GPO ayarları kullanılarak uç noktada açıkça devre dışı bırakılabilir.

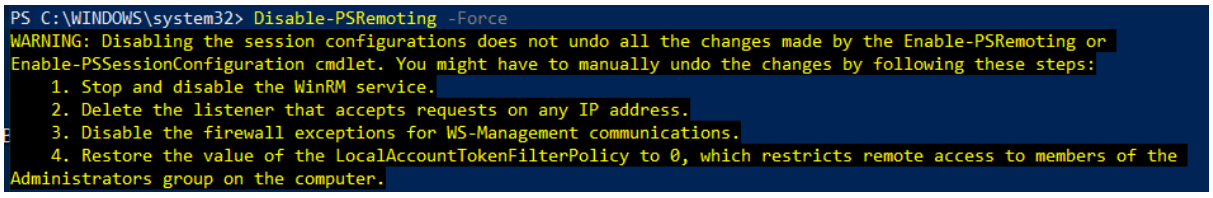
PowerShell:

```
Disable-PSRemoting -Force
```

Şekil 17: Bir Uç Noktada WinRM/PowerShell Uzaktan İletişimi Devre Dışı Bırakmak için PowerShell Komutu

Not: Disable-PSRemoting -Force'u çalıştırmak, yerel kullanıcıların yerel bilgisayarda veya uzak bilgisayarlara yönelik oturumlar için PowerShell oturumları oluşturmasını engellemez.

Komutu çalıştırdıktan sonra, Şekil 18'de kaydedilen mesaj görüntülenecektir. Bu adımlar ek sağlamlaştırma sağlar, ancak Disable-PSRemoting -Force komutunu çalıştırdıktan sonra, hedef uç noktaya yönelik PowerShell oturumları başarılı olmaz



Şekil 18: PSRemoting'i Devre Dışı Bıraktıktan Sonra Uyarı Mesajı

PowerShell aracılığıyla WinRM'yi devre dışı bırakmak için ek adımları uygulamak için (Şekil 19 - Şekil 22):

1. WinRM hizmetini durdurun ve devre dışı bırakın

```
Stop-Service WinRM -PassThruSet-Service WinRM -StartupType Disabled
```

Şekil 19: WinRM Hizmetini Durdurmak ve Devre Dışı Bırakmak için PowerShell Komutu

2. Herhangi bir IP adresindeki istekleri kabul eden dinleyiciyi devre dışı bırakın.

```
dir wsman:\localhost\listener

Remove-Item -Path WSMan:\Localhost\listener\
```

Şekil 20: Bir WSMan Dinleyicisini Silmek için PowerShell Komutları

3. WS-Management iletişimleri için güvenlik duvarı istisnalarını devre dışı bırakın.

```
Set-NetFirewallRule -DisplayName 'Windows Remote Management (HTTP-In)' -Enabled
False
```

Şekil 21: WinRM için Güvenlik Duvarı İstisnalarını Devre Dışı Bırakmak için PowerShell Komutu

4. LocalAccountTokenFilterPolicy'nin değerini, uzaktan erişimi kısıtlayan 0'a geri yükleyin.

```
Set-ItemProperty –Path HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system
- Name LocalAccountTokenFilterPolicy -Value 0
```

Şekil 22: LocalAccountTokenFilterPolicy için Kayıt Defteri Anahtarını Yapılandırmak için PowerShell Komutu

Grup ilkesi:

- Bilgisayar Yapılandırması > İlkeler > Yönetim Şablonları > Windows Bileşenleri > Windows Uzaktan Yönetimi (WinRM) > WinRM Hizmeti > WinRM aracılığıyla uzak sunucu yönetimine izin ver
  - Engelli

Bu ayar Devre Dışı olarak yapılandırılırsa, WinRM hizmeti, herhangi bir WinRM dinleyicisinin yapılandırılıp yapılandırılmadığından bağımsız olarak uzak bilgisayardan gelen isteklere yanıt vermez.

- Bilgisayar Yapılandırması > İlkeler > Yönetim Şablonları > Windows Bileşenleri > Windows Uzak Kabuğu > Uzak Kabuk Erişimine İzin Ver
  - Engelli

Bu ilke ayarı, komut dosyalarını yürütme ve desteklenen tüm kabuklara uzaktan erişim yapılandırmasını yönetecek.

WinRM Kullanımı için Tespit Olanakları

Kullanım Örneği	MITRE ID	Tanım
Unauthorized WinRM Execution Attempt	T1021.006 - Remote Services: Windows Remote Management	Bir sistemde WinRM için komut yürütme denemeleri aranıyor. WinRM devre dışı bırakıldı
Suspicious Process Creation Using WinRM	T1021.006 - Remote Services: Windows Remote Management	Yerleşik bir taban çizgisinden sapan WinRM kullanarak anormal süreç oluşturma olaylarını arama
Suspicious Process Creation Using WinRM	T1021.006 - Remote Services: Windows Remote Management	Kurulu bir taban çizgisinden sapan anormal bağlantıları belirlemek için TCP/5985 ve TCP/5986 gibi bilinen WinRM bağlantı noktaları üzerinden ağ etkinliğini arama.
Remote WMI Connection Using WinRM	T1021.006 - Remote Services: Windows Remote Management	WinRM kullanarak uzak WMI bağlantı denemeleri aranıyor.

Tablo 11: WinRM Kullanımı için Algılama Fırsatları

Ortak Yanal Hareket Araç ve Yöntemlerini Kısıtlama

Tablo 12, ortak uzaktan erişim araçlarına ve ortamlarda yanal hareket için kullanılan yöntemlere karşı mücadele etmek için kullanılabilecek güvenlik yapılandırmalarının birleştirilmiş bir özetini sağlar.

Araç/Taktik	Güvenlik Yapılandırmalarını Azaltma (Hedef Uç Noktalar)
PsExec (-u anahtarı olmadan, geçerli oturum açmış kullanıcı hesabını kullanarak) -u anahtarından yararlanılmazsa, kimlik doğrulama, kaynak uç noktanın geçerli oturum açmış kullanıcısı için Kerberos veya NTLM'yi kullanır ve hedef uç noktada Tip 3 (ağ) oturum açması olarak kaydolur. PsExec üst düzey işlevsellik: • SMB (TCP/445) aracılığıyla uzak bir uç noktada gizli ADMIN$ paylaşımına (C:\Windows klasörüyle eşleme) bağlanır. • PSExecsvc hizmetini başlatmak ve uzak bir uç noktada adlandırılmış bir kanal etkinleştirmek için Hizmet Denetim Yöneticisi'ni (SCM) kullanır. • Konsol için giriş/çıkış yeniden yönlendirmesi, oluşturulan adlandırılmış kanal aracılığıyla gerçekleştirilir.	**Seçenek 1:** GPO yapılandırması: • Bilgisayar Yapılandırması > İlkeler > Windows Ayarları > Güvenlik Ayarları > Yerel İlkeler > Kullanıcı Hakları Ataması o Bu bilgisayara ağdan erişimi engelle **Seçenek 2:** Windows Güvenlik Duvarı kuralı: `netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=no` *Şekil 23: Yerel Windows Güvenlik Duvarı Kuralı Kullanan Bir Uç Nokta için Gelen Dosya ve Yazdırma Paylaşımını (SMB) Devre Dışı Bırakmak için PowerShell Komutu* **Seçenek 3:** Disable administrative and hidden shares.
PsExec (Alternatif Kimlik Bilgileri ile, -u anahtarı aracılığıyla) -u anahtarından yararlanılırsa, kimlik doğrulama, sağlanan alternatif kimlik bilgilerini kullanır ve hedef uç noktasında bir Tip 3 (ağ) ve Tip 2 (etkileşimli) oturum açma olarak kaydedilir.	**Seçenek 1:** GPO yapılandırması: • Bilgisayar Yapılandırması > İlkeler > Windows Ayarları > Güvenlik Ayarları > Yerel İlkeler > Kullanıcı Hakları Ataması o Bu bilgisayara ağdan erişimi engelle oYerel olarak oturum açmayı reddet **Seçenek 2:** Windows Güvenlik Duvarı kuralı: `netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=no`

	Şekil 24: Gelen Dosyayı Devre Dışı Bırakmak için PowerShell Komutu ve Yerel Windows Güvenlik Duvarı Kuralı Kullanan Bir Uç Nokta için Yazdırma Paylaşımı (SMB)
Uzak Masaüstü Protokolü (RDP)	**Seçenek 1:** GPO yapılandırması: • Bilgisayar Yapılandırması > İlkeler > Windows Ayarları > Güvenlik Ayarları > Yerel İlkeler > Kullanıcı Hakları Ataması o Terminal Hizmetleri aracılığıyla oturum açmayı reddet **Seçenek 2:** Windows Güvenlik Duvarı kuralı: netsh advfirewall firewall set rule group="Remote Desktop" new enable=no Şekil 25: Yerel bir Windows Güvenlik Duvarı Kuralı Kullanarak Bir Uç Nokta için Gelen Uzak Masaüstü'nü (RDP) Devre Dışı Bırakmaya Yönelik PowerShell Komutu

Tablo 12: Ortak Yanal Hareket Araçları/Yöntemleri ve Güvenlik Kontrollerini Azaltma

Ortak Yanal Hareket Araçları ve Yöntemleri için Tespit Olanakları

Kullanım Örneği	MITRE ID	Tanım
Anomalous PsExec Usage	T1569.002 – System Services: Service Execution T1021.002 – Remote Services: SMB/Windows Admin Shares T1570 – Lateral Tool Transfer	PsExec'in devre dışı bırakıldığı veya normal etkinlikten saptığı sistemlerde PsExec'in çalıştırılmaya çalışılması aranıyor.

Process Creation Event Involving a COM Object by Different User	T1021.003 – Remote Services: Distributed Component Object Model T1078 – Valid Accounts	Şu anda sistemde oturum açmış kullanıcı olmayan bir hesap tarafından başlatılan COM nesneleri de dahil olmak üzere süreç oluşturma olaylarını arama.
High Volume of DCOM Related Activity	T1021.003 – Remote Services: Distributed Component Object Model	DCOM ile ilgili aktivite hacminde bir artış aranıyor.
Third-Party Remote Access Applications	T1219 – Remote Access Software	Üçüncü taraf uzaktan erişim uygulamalarının anormal kullanımı aranıyor. Bu tür bir etkinlik, bir tehdit aktörünün alternatif bir iletişim kanalı olarak veya uzaktan etkileşimli oturumlar oluşturmak için üçüncü taraf uzaktan erişim uygulamalarını kullanmaya çalıştığını gösterebilir.

Tablo 13: Ortak Yanal Hareket Araçları ve Yöntemleri için Tespit Olanakları

Ek Uç Nokta Güçlendirme

Uç noktalarda çağrılan kötü amaçlı ikili dosyalara, kötü amaçlı yazılımlara ve şifreleyicilere karşı korunmaya yardımcı olmak için ek güvenlik güçlendirme teknolojileri ve denetimleri dikkate alınmalıdır. Windows tabanlı uç noktalar için değerlendirilmek üzere ek güvenlik denetimlerinin örnekleri aşağıda verilmiştir.

Windows Defender Uygulama Kontrolü

Windows Defender Uygulama Denetimi, kullanıcıların uç noktalarda hangi uygulamaları ve dosyaları çalıştırabileceğini denetlemek için kilitleme ve denetim mekanizmaları sağlayan Active Directory içindeki bir dizi doğal yapılandırma ayarıdır. Bu işlevle, GPO'lar içinde aşağıdaki kural türleri yapılandırılabilir:

- Yayıncı kuralları: Dijital imzalara ve diğerlerine dayalı olarak dosyaların yürütülmesine izin vermek veya bunları kısıtlamak için kullanılabilir.
- Yol kuralları: Belirli bir yerde bulunan dosyalara dayalı olarak dosya yürütmeye veya erişime izin vermek veya kısıtlamak için kullanılabilir.
- Dosya karma kuralları: Bir dosyanın karma değerine dayalı olarak dosya yürütmesine izin vermek veya dosya yürütmeyi kısıtlamak için kullanılabilir.

Windows Defender Uygulama Denetimi ile ilgili ek bilgiler için https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview adresine bakın.

Microsoft Defender Saldırı Yüzeyi Azaltma

Microsoft Defender Saldırı Yüzeyi Azaltma (ASR) kuralları, aşağıdakiler dahil çeşitli tehditlere karşı korunmaya yardımcı olabilir:

- Dosyaları indirmeye veya çalıştırmaya çalışan yürütülebilir dosyaları ve komut dosyalarını başlatan bir tehdit aktörü.
- Gizlenmiş veya şüpheli komut dosyaları çalıştıran bir tehdit aktörü.
- Yerel Güvenlik Otoritesi Alt Sistem Hizmeti ile arayüz oluşturan kimlik bilgisi hırsızlığı araçlarını çağıran bir tehdit aktörü (LSASS).
- PsExec veya WMI komutlarını çağıran bir tehdit aktörü.
- Uygulamaların genellikle standartlaştırılmış etkinliğin bir parçası olarak başlatmadığı davranışları normalleştirme ve engelleme.
- E-posta istemcilerinden ve Web postasından (kimlik avı) yürütülebilir içeriğin engellenmesi.

ASR, Windows E3 veya üzeri bir lisans gerektirir. Windows E5 lisansı, ASR için gelişmiş yönetim yetenekleri sağlar.

Microsoft Defender Saldırı Yüzey Azaltma işleviyle ilgili ek bilgi için https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction adresine bakın.

Kontrollü Klasör Erişimi

Kontrollü klasör erişimi, verilerin fidye yazılımı tarafından şifrelenmesini önlemeye yardımcı olabilir. Windows 10 sürüm 1709+ ve Windows Server 2019+ ile başlayarak, Windows Defender Antivirus içinde kontrollü klasör erişimi tanıtıldı
(Windows Defender Exploit Guard'ın bir parçası olarak).

Kontrollü klasör erişimi etkinleştirildiğinde, uygulamalar ve yürütülebilir dosyalar, bir uygulamanın kötü amaçlı veya güvenli olup olmadığını belirleyen Windows Defender Antivirus tarafından değerlendirilir. Bir uygulamanın kötü amaçlı veya şüpheli olduğu belirlenirse, korumalı bir klasördeki herhangi bir dosyada değişiklik yapması engellenir.

Etkinleştirildiğinde, kontrollü klasör erişimi bir dizi sistem klasörüne ve aşağıdakiler dahil varsayılan konumlara uygulanacaktır:

- Documents
  - C:\users\<username>\Documents
  - C:\users\Public\Documents
- Pictures
  - C:\users\<username>\Pictures
  - C:\users\Public\Pictures
- Videos
  - C:\users\<username>\Videos
  - C:\users\Public\Videos
- Music
  - C:\users\<username>\Music

- C:\users\Public\Music
- Desktop
  - C:\users\<username>\Desktop
  - C:\users\Public\Desktop
- Favorites
  - C:\users\<username>\Favorites

Windows Güvenlik uygulaması, Grup İlkesi, PowerShell veya mobil cihaz yönetimi (MDM) yapılandırma hizmeti sağlayıcıları (CSP'ler) kullanılarak ek klasörler eklenebilir. Ek olarak, uygulamalar korumalı klasörlere erişim için izin verilenler listesine alınabilir.

Not: Kontrollü klasör erişiminin tam olarak çalışması için Windows Defender'ın Gerçek Zamanlı Koruma ayarı etkinleştirilmelidir.

Kontrollü klasör erişimiyle ilgili ek bilgi için https://docs.microsoft.com/en-us/microsoft 365/security/defender-endpoint/enable-controll-folders adresine başvurun.

Dış Müdahale Koruması

Tehdit aktörleri genellikle uç noktalarda güvenlik özelliklerini devre dışı bırakmaya çalışır. Windows'ta (Microsoft Defender for Endpoint aracılığıyla) veya üçüncü taraf AV/EDR platformlarına entegre edilmiş kurcalama koruması, güvenlik araçlarının bir tehdit aktörü tarafından değiştirilmesini veya durdurulmasını önlemeye yardımcı olabilir.

Kuruluşlar, uç noktalara dağıtılan güvenlik teknolojilerinin yapılandırmasını gözden geçirmeli ve yetkisiz değişikliklere karşı koruma sağlamak için kurcalamaya karşı korumanın etkinleştirilip etkinleştirilmediğini (veya sağlanıp sağlanamadığını) doğrulamalıdır. Bir kez uygulandıktan sonra, kuruluşlar kurcalamaya karşı korumayı test etmeli ve doğrulamalıdır.

Windows Defender for Endpoint için ek bilgiler için https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/prevent-changes-to-security-settings-with-tamper-protection adresine başvurun.

Dış Müdahale Koruma Olayları için Tespit Olanakları

Kullanım Örneği	MITRE ID	Tanım
Threat Actor Attempting to Disable Security Tooling on an Endpoint	T1562.001 - Disable or Modify Tools	Durdurulan güvenlik araçlarına/hizmetlerine ilişkin süreçlerin veya komut satırı argümanlarının kanıtını izleme.

Tablo 14: Dış Müdahale Koruma Olayları için Algılama Olanakları

Kimlik Bilgileri ve Hesap Korumaları

Ayrıcalıklı Hesap ve Grupların Belirlenmesi

Tehdit aktörleri, keşif çabalarının bir parçası olarak ayrıcalıklı hesapların belirlenmesine öncelik verecek. Tehdit aktörleri belirlendikten sonra, yanal hareket, kalıcılık ve görevin yerine getirilmesi için bu hesaplar için kimlik bilgilerini almaya çalışacaktır.

Kuruluşlar, Active Directory içindeki yüksek ayrıcalık düzeyine sahip hesapların ve grupların kapsamını belirlemeye ve gözden geçirmeye proaktif olarak odaklanmalıdır. Yüksek bir ayrıcalık düzeyi aşağıdaki kriterlere göre belirlenebilir:

- Varsayılan etki alanına üyelik atanan ve Exchange tabanlı ayrıcalıklı hesaplar veya iç içe gruplar
  gruplar (Şekil 29).
- AdminSDHolder tarafından korunan güvenlik gruplarına üyelik atanan hesaplar veya iç içe gruplar.
- Ayrıcalıklı hesapları, grupları veya uç noktaları barındıran kuruluş birimleri (OU'lar) için hesaplara veya gruplara izinler atanmıştır.
- Doğrudan etki alanının kökünde veya izinlerin alt nesneler tarafından devralındığı kuruluş birimleri için belirli genişletilmiş hak izinleri atanan hesaplar veya gruplar. Örnek şunları içerir:
    - o DS-Replication-Get-Changes-All
    - o Administer Exchange Information Store
    - o View Exchange Information Store Status
    - o Create-Inbound-Forest-Trust
    - o Migrate-SID-History
    - o Reanimate-Tombstones
    - o View Exchange Information Store Status
    - o User-Force-Change-Password
- GPO'ları değiştirmek veya bağlamak için hesaplara veya gruplara izinler atanmıştır.
- Etki alanı denetleyicilerinde veya Katman 0 uç noktalarında açık izinler atanan hesaplar veya gruplar.
- Dizin hizmeti çoğaltma izinlerine atanan hesaplar veya gruplar.
- Bir sistemde tüm uç noktalarda (veya geniş kapsamlı kritik varlıklarda) yerel yönetim erişimine sahip hesaplar veya gruplar

Varsayılan etki alanı tabanlı ayrıcalıklı gruplara üyelik sağlanan veya tarafından korunan hesapları belirlemek için
AdminSDHolder, aşağıdaki PowerShell cmdlet'leri bir etki alanı denetleyicisinden çalıştırılabilir.

```
get-ADGroupMember -Identity "Domain Admins" -Recursive | export-csv -path <output directory>\DomainAdmins.csv -NoTypeInformation

get-ADGroupMember -Identity "Enterprise Admins" -Recursive | export-csv -path <output directory>\EnterpriseAdmins.csv -NoTypeInformation

get-ADGroupMember -Identity "Schema Admins" -Recursive | export-csv -path <output directory>\SchemaAdmins.csv -NoTypeInformation

get-ADGroupMember -Identity "Administrators" -Recursive | export-csv -path <output directory>\Administrators.csv -NoTypeInformation

get-ADGroupMember -Identity "Account Operators" -Recursive | export-csv -path <output directory>\AccountOperators.csv -NoTypeInformation

get-ADGroupMember -Identity "Backup Operators" -Recursive | export-csv -path <output directory>\BackupOperators.csv -NoTypeInformation

get-ADGroupMember -Identity "Cert Publishers" -Recursive | export-csv -path <output directory>\CertPublishers.csv -NoTypeInformation

get-ADGroupMember -Identity "Print Operators" -Recursive | export-csv -path <output directory>\PrintOperators.csv -NoTypeInformation

get-ADGroupMember -Identity "Server Operators" -Recursive | export-csv -path <output directory>\ServerOperators.csv -NoTypeInformation

get-ADGroupMember -Identity "DNSAdmins" -Recursive | export-csv -path <output directory>\DNSAdmins.csv -NoTypeInformation

get-ADGroupMember -Identity "DNSAdmins" -Recursive | export-csv -path <output directory>\DNSAdmins.csv -NoTypeInformation

get-ADGroupMember -Identity "Group Policy Creator Owners" -Recursive | export-csv -path <output directory>\Group-Policy-Creator-Owners.csv -NoTypeInformation

get-ADGroupMember -Identity "Exchange Trusted Subsystem" -Recursive | export-csv -path <output directory>\Exchange-Trusted-Subsystem.csv -NoTypeInformation

get-ADGroupMember -Identity "Exchange Windows Permissions" -Recursive | export-csv -path <output directory>\Exchange-Windows-Permissions.csv -NoTypeInformation

get-ADGroupMember -Identity "Exchange Recipient Administrators" -Recursive | export-csv -path <output directory>\Exchange-Recipient-Admins.csv -NoTypeInformation

get-ADUser -Filter {(AdminCount -eq 1) -And (Enabled -eq $True)} | Select-Object Name, DistinguishedName | export-csv -path <output directory>\AdminSDHolder_Enabled.csv
```

Şekil 29: Etki Alanı ve Exchange Tabanlı Ayrıcalıklı Hesapları Tanımlama Komutları

Ek güvenlik gruplarına üyelik verilen ayrıcalıklı hesaplar, bir tehdit aktörüne, hesapların oturum açma veya sistemlere uzaktan erişim iznine sahip olduğu uç noktalara dayalı olarak etki alanı yönetimi düzeyinde izinlere giden potansiyel bir yol sağlayabilir.

İdeal olarak, bir etki alanı içinde yüksek ayrıcalıklı erişime sahip yalnızca küçük bir hesap kapsamı sağlanmalıdır.

Yüksek ayrıcalıklı izinler günlük kullanım için kullanılmamalı, iş istasyonlarında, dizüstü bilgisayarlarda veya ortak sunucularda etkileşimli veya uzaktan oturum açmak için kullanılmamalı veya etki alanı olmayan denetleyici (Katman 0) varlıklarında işlevler gerçekleştirmek için kullanılmamalıdır.

Ayrıcalıklı hesaplara erişimi kısıtlamaya yönelik ek öneriler için Ayrıcalıklı Hesapta Oturum Açma bölümüne bakın.

Ayrıcalıklı Hesaplar, Gruplar ve GPO Değişiklikleri için Algılama Fırsatları

Kullanım Örneği	MITRE ID	Tanım
Interactive or Remote Logon of a Highly Privileged Account to an Unauthorized System	T1078 – Valid Accounts	Oturum açma araması, Tier 0 katmanının dışında bulunan sistemlerde kimlik doğrulaması yapan yüksek ayrıcalıklı hesaplarla ilişkilendirilmeye çalışılır.
Privileged Account and Group Discovery	T1069 – Permission Groups Discovery Groups Discovery T1078 – Valid Accounts	Bir kullanıcının ayrıcalıklı hesapları ve grupları numaralandırmaya çalıştığı komut satırı olaylarını arama.
Account Added to Highly Privileged Group	T1078 – Valid Accounts T1098 – Account Manipulation	Hesapların yüksek ayrıcalıklı gruplara ne zaman eklendiğini belirleme. Bu, normal aktivitenin bir parçası olarak gerçekleşebilse de, seyrek olmalı ve belirli hesaplarla sınırlı olmalıdır.
Modification of Group Policy Objects	T1484.001 – Domain Policy Modification: Group Policy Modification	Grup ilkesi nesnelerinin (GPO'lar) ne zaman oluşturulduğunu veya değiştirildiğini belirleme. GPO'lar ayrıca son değişiklik zaman damgalarını belirlemek için dışa aktarılabilir ve gözden geçirilebilir.

		get-gpo -all | export-csv -path “c:\temp\gpo-listing all.csv” –NoTypeInformation Şekil 30: GPO Oluşturma ve Değiştirme Zaman Damgalarını Dışa Aktarmak ve İncelemek için PowerShell cmdlet'i

Tablo 15: Ayrıcalıklı Hesaplar, Gruplar ve GPO Değişiklikleri için Tespit Fırsatları

Ayrıcalıklı ve Hizmet Hesabı Korumaları

SPN ile Yapılandırılan Bilgisayar Dışı Hesapları Tanımlayın ve İnceleyin

Hizmet asıl adlarına (SPN'ler) sahip hesaplar, genellikle ayrıcalık yükseltme için tehdit aktörleri tarafından hedeflenir. Kerberos kullanarak, herhangi bir etki alanı kullanıcısı, bir SPN ile yapılandırılmış herhangi bir hesap için bir etki alanı denetleyicisinden bir Kerberos hizmet bileti (TGS) talep edebilir. Bilgisayar olmayan hesaplar muhtemelen tahmin edilebilir (rastgele olmayan) şifrelerle yapılandırılmıştır.

Etki alanı işlev düzeyi veya ana bilgisayarın Windows sürümü ne olursa olsun, bilgisayar dışı bir hesap altında kayıtlı SPN'ler, Gelişmiş Şifreleme Standardı (AES) yerine eski RC4-HMAC şifreleme paketini kullanır. RC4-HMAC şifreleme türünün şifrelenmesi ve şifresinin çözülmesi için kullanılan anahtar, hesabın şifresinin kırılması yoluyla elde edilebilecek bir NTLM karma sürümünü temsil eder.

Kuruluşlar, bir SPN ile yapılandırılmış bilgisayar dışı hesapları belirlemek için Active Directory'yi incelemelidir. Kayıtlı SPN'lerle ilişkilendirilen bilgisayar dışı hesaplar büyük olasılıkla hizmet hesaplarıdır ve bir tehdit aktörünün (yönetici ayrıcalıkları olmadan) hesap için düz metin parolasını türetmesi (kırması) için bir yöntem sağlar (Kerberoasting). Bir SPN ile yapılandırılmış bilgisayar dışı hesapları belirlemek için Şekil 31'de belirtilen PowerShell cmdlet'i bir etki alanı denetleyicisinden çalıştırılabilir.

```
Get-ADUser -Filter {(ServicePrincipalName -like "*")} | Select Object

name,samaccountname,sid,enabled,DistinguishedName
```

Şekil 31: Bir SPN ile Yapılandırılan Bilgisayar Dışı Hesapları Tanımlamak için PowerShell cmdlet'i

Mümkün olduğunda, kuruluşlar, yapılandırılmış SPN'lere sahip bilgisayar dışı hesapların kaydını silmelidir. SPN'lerin gerekli olduğu durumlarda, kuruluşlar Kerberoasting saldırılarıyla ilişkili riski azaltmalıdır. SPN'li hesaplar, güçlü, benzersiz parolalarla (ör. minimum 25+ karakter) yapılandırılmalıdır.

Ayrıca, her hesabın amaçlanan işlev için gereken minimum ayrıcalıklara sahip olmasını sağlamak için, bu hesapların ayrıcalıkları gözden geçirilmeli ve azaltılmalıdır.

SPN'li hesaplar, bu belgede ayrıntılı olarak açıklanan proaktif sağlamlaştırma önlemleri kapsamında düşünülmelidir.

Not: SPN'ler asla normal etkileşimli kullanıcı hesaplarıyla ilişkilendirilmemelidir.

SPN ile Yapılandırılan Bilgisayar Dışı Hesaplar için Algılama Fırsatları

Kullanım Örneği	MITRE ID	Tanım
Potential Kerberoasting Attempt Using RC4	T1558.003 – Steal or Forge Kerberos Tickets: Kerberoasting	İndirgenmiş RC4 şifrelemesi kullanarak bir Kerberos isteği aranıyor.

Tablo 16: Bir SPN ile Yapılandırılan Bilgisayar Dışı Hesaplar için Algılama Fırsatları

Ayrıcalıklı Hesap Oturum Açma Kısıtlamaları

Ayrıcalıklı ve hizmet hesapları kimlik bilgileri, yatay hareket ve kalıcılık sağlamak için yaygın olarak kullanılır.

Bir ortamda ayrıcalıklı erişime sahip herhangi bir hesap için, hesaplar standart iş istasyonlarında ve dizüstü bilgisayarlarda değil, bunun yerine kısıtlı ve korumalı VLAN'larda ve katmanlarda bulunan belirlenmiş sistemlerden (örneğin ayrıcalıklı erişimli iş istasyonları (PAW'ler)) kullanılmalıdır. Adanmış ayrıcalıklı hesaplar, her bir katman için tanımlanmalı ve hesapların yalnızca belirlenen katman içinde kullanılabileceğini zorunlu kılan kontroller bulunmalıdır.

Ayrıcalıklı hesaplar için erişim kapsamını kısıtlama önerileri, Microsoft'un ayrıcalıklı erişimin güvence altına alınmasına yönelik kılavuzuna dayanmaktadır. Ek bilgi için referans:

- https://docs.microsoft.com/en-us/security/compass/privileged-access-access-model
- https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/authentication-policies-and-authentication-policy-silos

Kullanıcı Hakları Atamaları

Proaktif bir güçlendirme veya hızlı sınırlama önlemi olarak, ayrıcalıklı AD erişimine sahip tüm hesapların standart iş istasyonlarına, dizüstü bilgisayarlara ve ortak erişim sunucularına (ör. sanallaştırılmış masaüstü altyapısı) giriş yapmasını (uzaktan veya yerel olarak) engellemeyi düşünün.

Aşağıdaki şekilde başvurulan ayarlar, GPO'larda tanımlanan kullanıcı hakları atamaları kullanılarak şu yol aracılığıyla yapılandırılabilir:

• Bilgisayar Yapılandırması > İlkeler > Windows Ayarları > Güvenlik Ayarları > Yerel İlkeler > Kullanıcı Hakları Atama Etki alanı tabanlı ayrıcalıklı erişimle yetkilendirilen hesapların, aşağıdaki ayarlar bağlamında (kullanılarak yapılandırılabilir) standart iş istasyonlarına ve dizüstü bilgisayar sistemlerine erişimi açıkça reddedilmelidir.
Şekil 32'de gösterilene benzer GPO ayarları

• *Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment*

Etki alanı tabanlı ayrıcalıklı erişimle yetkilendirilen hesapların, aşağıdaki ayarlar bağlamında (Şekil 32'de gösterilene benzer GPO ayarları kullanılarak yapılandırılabilir) standart iş istasyonlarına ve dizüstü bilgisayar sistemlerine erişimi açıkça reddedilmelidir.

• Ağdan bu bilgisayara erişimi engelleyin (ayrıca S-1-5-114: NT AUTHORITY\Local hesabı ve Administrators grubunun üyesini içerir) (SeDenyNetworkLogonRight)

• Toplu iş olarak oturum açmayı reddet (SeDenyBatchLogonRight)

• Hizmet olarak oturum açmayı reddet (SeDenyServiceLogonRight)

• Yerel olarak oturum açmayı reddet (SeDenyInteractiveLogonRight)

• Terminal Hizmetleri aracılığıyla oturum açmayı reddet (SeDenyRemoteInteractiveLogonRight)

Local Policies/User Rights Assignment

Policy	Setting
Deny access to this computer from the network	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on as a batch job	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on as a service	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on locally	MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on through Terminal Services	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts

Şekil 32: GPO Ayarlarını Kullanan Standart Bir İş İstasyonu için Ayrıcalıklı Hesap Erişim Kısıtlamaları

Örneği Ek olarak, aşağıdaki kullanıcı hakları atamalarına sahip hesapların kapsamını azaltarak ayrıcalık yükselmesine ve olası veri hırsızlığına karşı koruma sağlamak için GPO'lar kullanılarak izinler uç noktalarda kısıtlanabilir:

- Hata ayıklama programları (SeDebugPrivilege)
- Dosyaları ve dizinleri yedekleyin (SeBackupPrivilege)
- Dosyaları ve dizinleri geri yükleyin (SeRestorePrivilege)
- Dosyaların veya diğer nesnelerin sahipliğini alın (SeTakeOwnershipPrivilege)

Kullanım Örneği	MITRE ID	Tanım
Attempted Logon of a Privileged Account from a Nonprivileged Access Workstation	T1078 – Valid Accounts	Oturum açma araması, Katman 0 katmanının dışında bulunan sistemlerde kimlik doğrulaması yapan yüksek ayrıcalıklı hesaplarla ilişkilendirilmeye çalışır.

Tablo 17: Ayrıcalıklı Hesap Oturum Açmaları için Algılama Olanakları Hizmet Hesabı Oturum Açma Kısıtlamaları

Kuruluşlar ayrıca, hesapların etkileşimli, uzak masaüstü ve mümkünse ağ tabanlı oturum açma işlemleri için kullanılma yeteneğini kısıtlamak için etki alanı tabanlı hizmet hesaplarının güvenliğini artırmayı düşünmelidir.

Hizmet hesapları için önerilen minimum oturum açma sağlamlaştırması (etkileşimli veya uzaktan oturum açma amaçları için hizmet hesabının gerekli olmadığı uç noktalarda):

• Bilgisayar Yapılandırması > İlkeler > Windows Ayarları > Güvenlik Ayarları > Yerel İlkeler > Kullanıcı Hakları Ataması

- o Yerel olarak oturum açmayı reddet (SeDenyInteractiveLogonRight)
- oTerminal Hizmetleri aracılığıyla oturum açmayı reddet (SeDenyRemoteInteractiveLogonRight)

Hizmet hesapları için ek önerilen oturum açma sağlamlaştırması (ağ tabanlı oturum açma amaçları için hizmet hesaplarının gerekli olmadığı uç noktalarda):

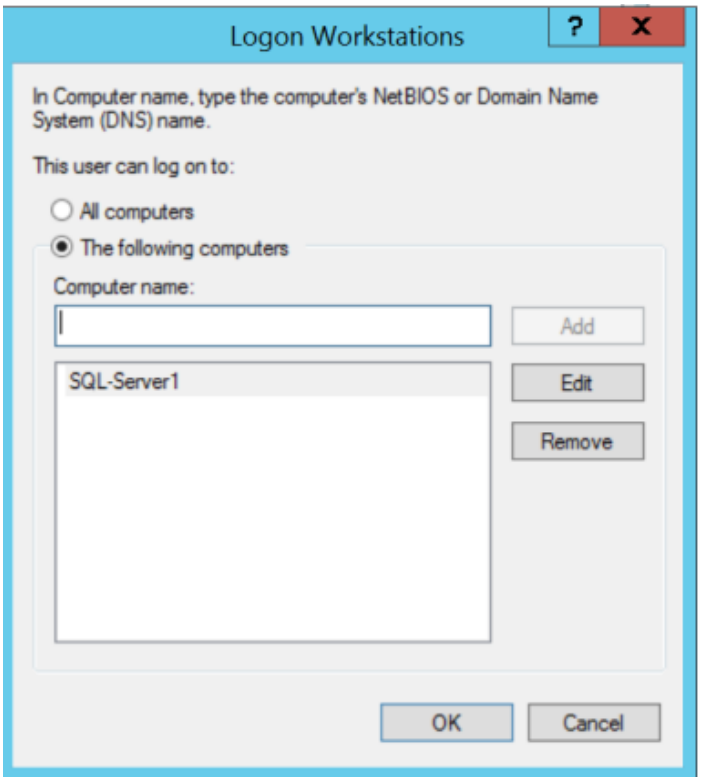
• Bilgisayar Yapılandırması > İlkeler > Windows Ayarları > Güvenlik Ayarları > Yerel İlkeler > Kullanıcı Hakları Ataması

- o Bu bilgisayara ağdan erişimi engelle (SeDenyNetworkLogonRight)

Bir hizmet hesabının belirli bir hizmeti çalıştırmak için yalnızca tek bir uç noktada kullanılması gerekiyorsa, hizmet hesabı, hesabın yalnızca önceden tanımlanmış bir uç nokta listesinde kullanımına izin verecek şekilde daha da kısıtlanabilir (Şekil 33).

• Active Directory Kullanıcıları ve Bilgisayarları > Hesabı seçin
- o Hesap sekmesi

▪ Oturum Aç düğmesi > Erişim için uygun bilgisayar kapsamını seçin



Şekil 33: Bir Hesabın Belirli Uç Noktalarda Oturum Açmasını Kısıtlama Seçeneği

Hizmet Hesabı Oturum Açmaları için Algılama Fırsatları

Kullanım Örneği	MITRE ID	Tanım
Anomalous Logon from a Service Account	T1078 – Valid Accounts	Yeni (beklenmedik) bir uç noktada bir hizmet hesabı için oturum açma denemeleri aranıyor. Bu, hizmet hesaplarının beklenen (onaylanmış) sistemlere temellendirilmesini gerektirecektir.

Tablo 18: Hizmet Hesabı Oturum Açmaları için Algılama Fırsatları

Yönetilen/Grup Tarafından Yönetilen Hizmet Hesapları

Statik hizmet hesaplarına sahip kuruluşlar, hizmet hesaplarını yönetilen hizmet hesapları (MSA'lar) veya grup yönetilen hizmet hesapları (gMSA'lar) olarak taşımanın fizibilitesini incelemelidir.

MSA'lar ilk olarak Windows Server 2008 R2 Active Directory şemasıyla (etki alanı-işlev düzeyi) tanıtıldı. Belirli uç noktalarda çalışan hizmetler ile ilişkili özel hizmet hesapları için otomatik parola yönetimi (30 günlük rotasyon) sağlar.

• Standart MSA: Hesap tek bir uç nokta ile ilişkilendirilir ve hesabın karmaşık parolası otomatik olarak yönetilir ve önceden tanımlanmış bir sıklıkta değiştirilir (varsayılan olarak 30 gün). Bir MSA yalnızca tek bir bilgisayar hesabıyla ilişkilendirilebilirken, aynı uç noktadaki birden çok hizmet MSA'dan yararlanabilir.

• Grup tarafından yönetilen hizmet hesabı (gMSA): İlk olarak Windows Server 2012 ile tanıtıldı ve MSA'lara çok benzer, ancak birden çok uç noktada tek bir gMSA'nın kullanılmasına izin verir.

MSA'lar ve gMSA'ların ortak kullanımları:

• Zamanlanmış Görevler
• İnternet Bilgi Servisleri (IIS) uygulama havuzları
• Yapılandırılmış Sorgu Dili (SQL) hizmetleri (SQL 2012 ve sonrası) – Express sürümleri MSA'lar tarafından desteklenmez.
• Microsoft Exchange hizmetleri
• Ağ Yük Dengeleme (kümeleme) – yalnızca gMSA'lar
• MSA'ları destekleyen üçüncü taraf uygulamalar
• Standart MSA: Hesap tek bir uç nokta ile tamamlanır ve hesabın karmaşık parolası otomatik olarak yönetilir sizin için bir sıkışıklıkta 30 gün olarak. Bir MSA yalnızca tek bir bilgisayar hesabıyla gösterilebilirken, aynı uç noktadaki çok sayıda hizmet MSA'dan planlayabilirsiniz.
• Grup tarafından sunulan hizmet seçeneği (gMSA): İlk olarak Windows Server 2012 ile tanıtıldı ve MSA'lara çok benzer, ancak çok uç nokta tek bir gMSA'nın kullanımına izin verir.

MSA'lar ve gMSA'ların kullanımları:

• Zamanlanmış Görevler
• İnternet Bilgi Servisleri (IIS) uygulama havuzları
• Yapılandırılmış Sorgu Dili (SQL) hizmetleri (SQL 2012 ve sonrası) – destek MSA'lar tarafından desteklenmez.
• Microsoft Exchange Hizmetleri
• Ağ Yük Dengeleme (kümeleme) – yalnızca gMSA'lar
• Çocuklar tarafından uygulanan MSA'ları

Yönetilen/Grup Tarafından Yönetilen Hizmet Hesapları için Algılama Fırsatları

Kullanım Örneği	MITRE ID	Tanım
Group Membership Addition	T1069 – Permission Groups Discovery T1098 – Account Manipulation	MSA'ları/gMSA'ları ve ilişkili olanları arama PrincipalsAllowedToRetrieveManagedPassword veya PrincipalsAllowedToDelegateToHesap izinleri; MSA/gMSA'dan kötü amaçlı amaçlar için yararlanma yeteneği sağlayabilir. MSA'lar/gMSA'lar ve ilişkili nitelikler için sorgulama için örnek keşif komutları: get-adserviceaccount get-adserviceaccount -filter {name -eq 'accountname'} -prop * | select Name, MemberOf, PrincipalsAllowedToDelegageToAccount, PrincipalsAllowedToRetrieveManagedPassword Figure 34: Example Reconnaissance Commands for Querying for MSAs/gMSAs

Tablo 19: Yönetilen/Grup Tarafından Yönetilen Hizmet Hesapları için Algılama Fırsatları

Korunan Kullanıcılar Güvenlik Grubu

Bir kuruluş, ayrıcalıklı hesaplar için Korumalı Kullanıcılar güvenlik grubundan yararlanarak, diskteki veya bellekteki ayrıcalıklı hesaplar için kimlik bilgilerini uç noktalardan alan bir tehdit aktörü veya kötü amaçlı yazılım varyantı tarafından çeşitli maruz kalma faktörlerini ve yaygın yararlanma yöntemlerini en aza indirebilir.

Microsoft Windows 8.1 ve Microsoft Windows Server 2012 R2 (ve üzeri) ile başlayarak, bir ortamda kimlik bilgilerinin açıklanmasını yönetmek için Korumalı Kullanıcılar güvenlik grubu tanıtıldı. Bu grubun üyeleri, aşağıdakiler dahil olmak üzere, hesaplara otomatik olarak uygulanan belirli korumalara sahiptir:

• Kerberos bileti verme bileti (TGT), normal 10 saatlik varsayılan ayar yerine dört saat sonra sona erer.
• Yalnızca Kerberos kimlik doğrulaması kullanıldığından (bir hesap için NTLM kimlik doğrulaması devre dışı bırakılır) LSASS'de bir hesap için NTLM karması depolanmaz.
• Önbelleğe alınmış kimlik bilgileri engellenir. Hesabın kimliğini doğrulamak için bir etki alanı denetleyicisi mevcut olmalıdır.
• WDigest kimlik doğrulaması, bir uç noktanın uygulanan ilke ayarlarından bağımsız olarak bir hesap için devre dışı bırakılır.
• DES ve RC4, Kerberos ön kimlik doğrulaması için kullanılamaz (Sunucu 2012 R2 veya üstü); bunun yerine, AES şifrelemeli Kerberos uygulanacaktır.
• Hesaplar, sınırlandırılmış veya sınırlandırılmamış yetkilendirme için kullanılamaz (Active Directory Kullanıcıları ve Bilgisayarları'nda Hesap hassastır ve devredilemez ayarının uygulanmasına eşdeğerdir).

Korumalı Kullanıcılar güvenlik grubunun üyeleri için başarılı (Olay Kimlikleri 303, 304) veya başarısız (Olay Kimlikleri 100, 104) oturum açma olayları, aşağıdaki olay günlüklerindeki etki alanı denetleyicilerine kaydedilebilir:

•%SystemRoot%\System32\Winevt\Logs\Microsoft-Windows Authentication%4ProtectedUserSuccesses-DomainController.evtx

•%SystemRoot%\System32\Winevt\Logs\Microsoft-Windows Authentication%4ProtectedUserFailures-DomainController.evtx

Olay günlükleri varsayılan olarak devre dışıdır ve her etki alanı denetleyicisinde etkinleştirilmelidir. Bir etki alanı denetleyicisinde Korumalı Kullanıcılar güvenlik grubu için olay günlüklerini etkinleştirmek için Şekil 35'te atıfta bulunulan PowerShell cmdlet'lerinden yararlanılabilir.

```
$log1 = New-Object
System.Diagnostics.Eventing.Reader.EventLogConfiguration Microsoft-
Windows-Authentication/ProtectedUserSuccesses-DomainController

$log1.IsEnabled=$true
$log1.SaveChanges()

$log2 = New-Object
System.Diagnostics.Eventing.Reader.EventLogConfiguration Microsoft-
Windows-Authentication/ProtectedUserFailures-DomainController
$log2.IsEnabled=$true
$log2.SaveChanges()
```

Şekil 35: Etki Alanı Denetleyicilerinde Korunan Kullanıcılar Güvenlik Grubu için Olay Günlüğünü Etkinleştirmeye yönelik PowerShell cmdlet'leri

Not: Kimlik doğrulama başarısız olacağından, hizmet hesapları (MSA'lar dahil) Korumalı Kullanıcılar güvenlik grubuna eklenmemelidir.

Korumalı Kullanıcılar güvenlik grubu kullanılamıyorsa, en azından ayrıcalıklı hesaplar, Active Directory'de Hesap Hassas ve Temsil Edilemez bayrağıyla yapılandırılarak yetkilendirmeye karşı korunmalıdır.

Korunan Kullanıcılar Güvenlik Grubu için Algılama Fırsatları

Kullanım Örneği	MITRE ID	Tanım
Removal of Account from Protected User Group	T1098 – Account Manipulation	Korumalı Kullanıcılar grubundan kaldırılmış bir hesap aranıyor.
Attempted Logon of an Account in the Protected User Group from a Nonprivileged Access Workstation	T1078 – Valid Accounts	Ayrıcalıklı olmayan kullanıcıların iş istasyonlarından kimlik doğrulaması yapan Korumalı Kullanıcılar grubundaki hesaplardan oturum açma girişimleri aranıyor.

Tablo 20: Korunan Kullanıcılar Güvenlik Grubu için Algılama Fırsatları

Açık Metin Parola Korumaları

Ayrıcalıklı hesaplar için erişimi kısıtlamaya ek olarak, uç noktalarda bellekte kimlik bilgilerinin ve belirteçlerin açığa çıkmasını en aza indiren denetimler uygulanmalıdır. Eski Windows sürümlerinde, öncelikle WDigest kimlik doğrulamasını desteklemek için açık metin parolaları bellekte (LSASS) depolanır. WDigest, varsayılan olarak devre dışı bırakılmadığı tüm Windows uç noktalarında açıkça devre dışı bırakılmalıdır. Varsayılan olarak, WDigest kimlik doğrulaması Windows 8.1+ ve Windows Server 2012 R2+'da devre dışıdır.

Windows 7 ve Windows Server 2008 R2'den başlayarak, KB2871997 yüklendikten sonra, WDigest kimlik doğrulaması, kayıt defteri değiştirilerek veya Microsoft Güvenlik Uyumluluk Araç Seti'nden Microsoft Güvenlik Kılavuzu GPO şablonu kullanılarak yapılandırılabilir. (https://www.microsoft.com/en-us/download/details.aspx?id=55319)

Kayıt Yöntemi (Registry Method):

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\U
seLogonCredential REG_DWORD = “0”
```

Şekil 36: WDigest Kimlik Doğrulamasını Devre Dışı Bırakmak için Kayıt Defteri Anahtarı ve Değeri

Açıkça yapılandırılması gereken başka bir kayıt defteri ayarı, Windows 8.1 ve sonraki sürümlerin davranışını taklit ederek oturumu kapatan kullanıcıların belleğindeki kimlik bilgilerini 30 saniye sonra temizleyen TokenLeakDetectDelaySecs ayarıdır. (Şekil 37).

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\TokenLeakDetectDelaySe
cs REG_DWORD = "30"
```

Şekil 37: TokenLeakDetectDelaySecs Ayarını Zorlamak için Kayıt Defteri Anahtarı ve Değeri

Grup İlkesi Yöntemi:

Microsoft Güvenlik Kılavuzu Grup İlkesi şablonu kullanılarak, WDigest kimlik doğrulaması bir GPO ayarı aracılığıyla devre dışı bırakılabilir (Şekil 38).

• Bilgisayar Yapılandırması > İlkeler > Yönetim Şablonları > MS Güvenlik Kılavuzu > WDigest Kimlik Doğrulaması
  o Engelli

Setting	State	Comment
Configure SMB v1 server	Not configured	No
Configure SMB v1 client driver	Not configured	No
Configure SMB v1 client (extra setting needed for pre-Win8.1/2012R2)	Not configured	No
Extended Protection for LDAP Authentication (Domain Controllers only)	Not configured	No
Turn on Windows Defender protection against Potentially Unwanted Applications (DEPRECATED)	Not configured	No
Enable Structured Exception Handling Overwrite Protection (SEHOP)	Not configured	No
Apply UAC restrictions to local accounts on network logons	Not configured	No
WDigest Authentication (disabling may require KB2871997)	Disabled	No
Lsass.exe audit mode	Not configured	No
LSA Protection	Not configured	No
Remove "Run As Different User" from context menus	Not configured	No
Block Flash activation in Office documents	Not configured	No

Şekil 38: MS Güvenlik Kılavuzu Grup İlkesi Şablonu aracılığıyla WDigest Kimlik Doğrulamasını Devre Dışı Bırakma

Ek olarak, bir kuruluş, Şekil 39'da atıfta bulunulan kayıt defteri anahtarlarında İzin Ver* ayarlarının belirtilmediğini doğrulamalıdır, çünkü bu yapılandırma tspkgs/CredSSP sağlayıcılarının açık metin parolalarını bellekte saklamasına izin verir.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Credssp
\PolicyDefaults

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Creden
tialsDelegation
```

Şekil 39: Açık Metin Parola Depolamasını Sağlamlaştırmaya Yönelik Ek Kayıt Anahtarları

Grup İlkesi Yeniden İşleme

Tehdit aktörleri, kayıt defterini doğrudan değiştirerek uç noktalarda WDigest kimlik doğrulamasını manuel olarak etkinleştirebilir (UseLogonCredential 1 değerine yapılandırılır). WDigest kimlik doğrulamasının varsayılan olarak otomatik olarak devre dışı bırakıldığı uç noktalarda bile, yapılandırılmış (beklenen) ayarlar için otomatik olarak otomatik grup ilkesi yeniden işlemeyi zorunlu kılacak, aşağıda belirtilen GPO ayarlarının uygulanması önerilir.

• Bilgisayar Yapılandırması > İlkeler > Yönetim Şablonları > Sistem > Grup İlkesi > Güvenlik ilkesi işlemeyi yapılandır
  o Etkin - Grup İlkesi nesneleri değişmemiş olsa bile işle

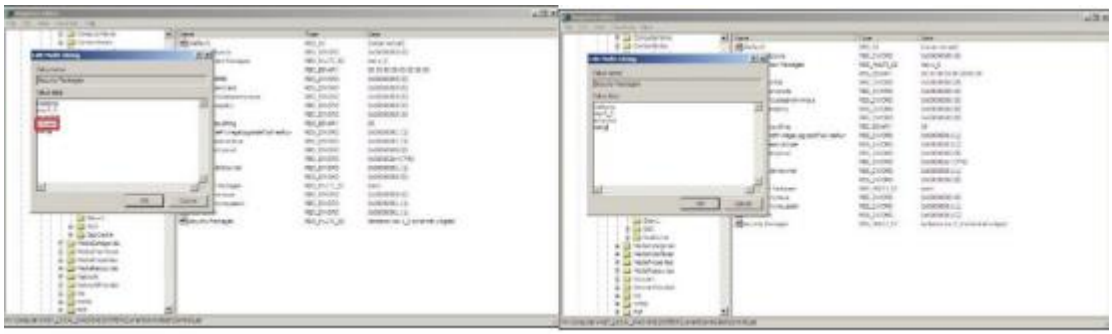
• Bilgisayar Yapılandırması > İlkeler > Yönetim Şablonları > Sistem > Grup İlkesi > Kayıt ilkesi işlemeyi yapılandır.
    o Etkin - Grup İlkesi nesneleri değişmemiş olsa bile işle

Not: Varsayılan olarak, Grup İlkesi ayarları yalnızca gerçek Grup İlkesi varsayılan yenileme aralığından önce değiştirilmişse yeniden işlenir ve yeniden uygulanır.

KB2871997, Windows XP, Windows Server 2003 ve Windows Server 2008 için geçerli olmadığından, sistem yeniden başlatılmadan önce bu platformlarda WDigest kimlik doğrulamasını devre dışı bırakmak için, WDigest'in kayıt defterindeki LSA güvenlik paketleri listesinden kaldırılması gerekir (Şekil 40). ve Şekil 41).

```
HKLM\System\CurrentControlSet\Control\Lsa\Security Packages
```

Şekil 40: LSA Güvenlik Paketlerini Değiştirmek için Kayıt Defteri Anahtarı



Şekil 41: Sağlayıcı Listesinden WDigest Kimlik Doğrulamasının Kaldırılmasından Önce ve Sonra LSA Güvenlik Paketi Kayıt Defteri Anahtarı

WDigest Kimlik Doğrulama Koşulları için Algılama Fırsatları

Kullanım Örneği	MITRE ID	Tanım
Enable WDigest Authentication	T1112-Modify Registry	Windows Kayıt Defterinde etkinleştirilmiş WDigest kanıtı aranıyor. HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential REG_DWORD = “1” Şekil 42: WDigest Windows Kayıt Defteri Değişikliği

Tablo 21: WDigest Kimlik Doğrulama Koşulları için Algılama Fırsatları

Bir tehdit aktörü bir uç noktada yerel yönetim erişimi elde edebiliyorsa, daha önce bir uç noktaya erişen hesaplar için parolalara (WDigest devre dışı bırakılmış olsa bile) erişilebilir.

Bu taktik genellikle tehdit aktörleri tarafından, uç noktalarda elde edilen yönetimsel erişim yoluyla bellekte (Mimikatz güvenlik destek sağlayıcısı (SSP) modülünü kullanarak) yerleşik açık metin kimlik bilgilerini elde etmek için kullanılır. Windows Defender Credential Guard'ı kullanmak, NLTM parola karmalarını, Kerberos bilet verme biletlerini ve bellekte depolanan kimlik bilgilerini koruyarak, hash-pass veya pass-the-bilet tarzı bir saldırının etkisini ve kapsamını en aza indirmeye yardımcı olabilir.

Windows Defender Credential Guard, Microsoft'un Windows 10 ve Windows Server 2016 ile sunduğu bir özelliktir.

Bu teknoloji, LSA sırlarını güvenlikten izole etmek için hem donanım hem de sanallaştırma tabanlı güvenliğin bir kombinasyonunu kullanır.

Windows Defender Credential Guard'ı yapılandırma ve test etmeyle ilgili ek ayrıntılar için bkz. https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage.

RDP Kullanırken Kimlik Bilgisi Korumaları

RDP için Kısıtlı Yönetici Modu

RDP için Kısıtlı Yönetici Modu, Uzaktan Kumanda işlemini gerçekleştiren personele atanan tüm son kullanıcı sistemleri için etkinleştirilebilir.

Bu özellik, RDP kullanılarak erişildiğinde bir hedef uç noktasındaki yönetici kimlik bilgilerinin bellek içi gösterimini sınırlayabilir.

Kısıtlı yönetici RDP'sinden yararlanmak için Şekil 43'te başvurulan komut çağrılabilir.

```
mstsc.exe /RestrictedAdmin
```

Şekil 43: Kısıtlı Yönetici RDP'sini Çağırma Komutu

Bir RDP bağlantısı Kısıtlı Yönetici Modu özelliğini kullandığında, kimlik doğrulama hesabı hedef uç noktada bir yöneticiyse, kullanıcı hesabının kimlik bilgileri bellekte depolanmaz; bunun yerine, kullanıcının hesabı, hedef makine hesabı olarak görünür (domain\destination-computer$).

RDP için Kısıtlı Yönetici Modundan yararlanmak için, hedef uç noktaya ek olarak başlangıç uç noktasında ayarların zorunlu kılınması gerekir.

Kaynak Uç Nokta (İstemci Modu - Windows 7 ve Windows Server 2008 R2 ve üzeri):

RestrictedAdmin özelliği kullanılarak uzak masaüstü oturumunu başlatan kaynak uç noktaya bir GPO ayarı uygulanmalıdır.

- Bilgisayar Yapılandırması > İlkeler > Yönetim Şablonları > Sistem > Kimlik Bilgileri Temsilcisi > Uzak sunuculara kimlik yetki devrini kısıtla
    - Kısıtlı Yönetici Gerektir > Etkin olarak ayarlayın
        - Aşağıdaki Kısıtlı Modu kullanın > Gerekli Kısıtlı Yönetici

Bu GPO ayarının yapılandırılması, Şekil 44'te belirtilen kayıt defteri anahtarlarının bir uç noktada yapılandırılmasına neden olacaktır.

```
HKLM\Software\Policies\Microsoft\Windows\CredentialsDelegation\Res
trictedRemoteAdministration
0 = Disabled
1 = Enabled

HKLM\Software\Policies\Microsoft\Windows\CredentialsDelegation\Res
trictedRemoteAdministr ationType

1 = Require Restricted Admin
2 = Require Remote Credential Guard
3 = Restrict Credential Delegation
```

Şekil 44: Kısıtlı Yönetici Modu Gerektiren Kayıt Defteri Ayarları

Hedef Uç Nokta (Sunucu Modu - Windows 8.1 ve Windows Server 2012 R2 ve üstü):

Bir kayıt defteri ayarının yapılandırılması gerekecektir (Şekil 45):

```
HKLM\System\CurrentControlSet\Control\Lsa\DisableRestrictedAdmin
0 = Enabled
1 = Disabled
```

Şekil 45: RestrictedAdmin RDP'yi Etkinleştirme veya Devre Dışı Bırakma için Kayıt Defteri Ayarı

Önerilen: Kısıtlı Yönetici Modunu etkinleştirmek için kayıt defteri değerini 0 olarak ayarlayın.

Restricted Admin RDP ile, yapılandırılması gereken başka bir ayar DisableRestrictedAdminOutboundCreds kayıt defteri anahtarıdır (Şekil 46).

```
HKLM\System\CurrentControlSet\Control\Lsa\DisableRestrictedAdminOutboundCreds
0 = default value (doesn't exist) - Admin Outbound Creds are Enabled
1 = Admin Outbound Creds are Disabled
```

Şekil 46: Yönetici Giden Kimlik Bilgilerini Devre Dışı Bırakmak için Kayıt Defteri Ayarı

Önerilen: Yönetici giden kimlik bilgilerini devre dışı bırakmak için kayıt defteri değerini 1 olarak ayarlayın.

Not: Bu ayar 0 olarak ayarlandığında, tüm giden kimlik doğrulama istekleri, bir kullanıcının Kısıtlı Yönetici Modu'nu kullanarak bağlandığı sistem (domain\destination-computer$) olarak görünür.

Bunu 1'e ayarlamak, bir kullanıcının RDP için Kısıtlı Yönetici Modu'nu kullanarak bağlandığı bir sistemden gidenin kimliğini doğrulamaya çalışırken herhangi bir aşağı akış ağ kaynağında kimlik doğrulama özelliğini devre dışı bırakır.

RDP için Kısıtlı Yönetici Modu ile ilgili ek bilgi için, referans:

• https://support.microsoft.com/kb/2973351

• https://blogs.technet.microsoft.com/kfalde/2013/08/14/restricted-admin-mode-for-rdp-in-windows-8-1-2012-r2/

RDP için Kısıtlı Yönetici Modu için Algılama Fırsatları

Kullanım Örneği	MITRE ID	Tanım
Disable Restricted Admin Mode for RDP	T1112 – Modify Registry	Windows Kayıt Defteri'nde RDP için Kısıtlı Yönetici Modunu devre dışı bırakan bir hesap aranıyor. HKLM\System\CurrentControlSet\Control\Lsa\DisableRestrictedAdmin REG_DWORD = "1" Şekil 47: Bir Hedef Uç Noktada Windows Kayıt Defterinde Devre Dışı Bırakılan RDP için Kısıtlı Yönetici Modu

Disable Require Restricted Admin	T1484.001 –Domain Policy Modification: Group Policy Modification	Bir GPO yapılandırmasında Kısıtlı Yönetici Gerektir seçeneğinin devre dışı bırakılması aranıyor. Computer Configuration > Policies > Administrative Templates > System > Credential Delegation > Restrict delegation of credentials to remote servers“Require Restricted Admin” > set to Disabled olarak ayarlayın Şekil 48: Bir GPO'da Kısıtlı Yöneticinin Devre Dışı Bırakılmasını Gerektirin

Tablo 22: RDP için Kısıtlı Yönetici Modu için Algılama Fırsatları

Windows Defender Uzaktan Kimlik Bilgisi Koruması

Windows 10 ve Windows Server 2016 uç noktaları, bağlantı için uzak masaüstü kullanıldığında hedef uç noktalarda bellekte ayrıcalıklı hesapların açığa çıkmasını azaltmak için Windows Defender Remote Credential Guard'dan yararlanılabilir. Remote Credential Guard ile tüm kimlik bilgileri istemcide (başlangıç sistemi) kalır ve doğrudan hedef uç noktasına maruz kalmaz. Bunun yerine, hedef uç nokta gerektiğinde kaynaktan hizmet biletleri talep eder.

Bir kullanıcı, Remote Credential Guard'ın etkin olduğu bir uç noktada RDP aracılığıyla oturum açtığında, bellekteki SSP'lerin hiçbiri hesabın düz metin parolasını veya parola karmasını saklamaz. Hedef sunucudan etkileşimli (ve çoklu oturum açma (SSO)) deneyimlerine izin vermek için Kerberos biletlerinin bellekte kaldığını unutmayın.

Uzak Masaüstü istemcisi (başlangıç noktası) ana bilgisayarı:

• Kimlik bilgilerini sağlayabilmek için en az Windows 10 (v1703) çalıştırıyor olmalıdır.
• Kullanıcının oturum açmış kimlik bilgilerini kullanmak için en az Windows 10 (v1607) veya Windows Server 2016 çalıştırıyor olmalıdır
• Bu, kullanıcının hesabının hem istemcide (başlangıç) hem de uzak (hedef) uç noktada oturum açabilmesini gerektirir.
• Uzak Masaüstü Klasik Windows uygulamasını çalıştırıyor olmalıdır.
• Uzak Masaüstü Evrensel Windows Platformu uygulaması, Windows Defender Uzaktan Kimlik Bilgisi Korumasını desteklemez.
• Uzak ana bilgisayara bağlanmak için Kerberos kimlik doğrulaması kullanılmalıdır.

Not: İstemci bir etki alanı denetleyicisine bağlanamazsa, RDP NTLM'ye geri dönmeye çalışır. Windows Defender Uzaktan Kimlik Bilgisi Koruması, kimlik bilgilerini riske maruz bırakacağından NTLM'nin geri dönüşüne izin vermez.

Uzak Masaüstü uzak (hedef) ana bilgisayarı:

• En az Windows 10 (v1607) veya Windows Server 2016 çalıştırıyor olmalıdır.
• Kısıtlı Yönetici bağlantılarına izin vermelidir.
• İstemcinin etki alanı kullanıcısının Uzak Masaüstü bağlantılarına erişmesine izin vermelidir.
• Dışa aktarılamayan kimlik bilgilerinin yetkilendirilmesine izin vermelidir.

Bir GPO yapılandırması kullanarak istemci (başlangıç) ana bilgisayarında Remote Credential Guard'ı etkinleştirmek için:

• Bilgisayar Yapılandırması > Yönetim Şablonları > Sistem > Kimlik Bilgileri Temsilciliği > Kimlik bilgilerinin uzak sunuculara devredilmesini kısıtla

o Kısıtlı Yönetici modu veya Windows Defender Remote Credential Guard'ı zorunlu kılmak için Windows Defender Remote Credential Guard'ı Tercih Et'i seçin.

▪ Bu yapılandırmada Remote Credential Guard tercih edilir, ancak Remote Credential Guard kullanılamadığında Kısıtlı Yönetici Modu (destekleniyorsa) kullanılır.
▪ Uzak Kimlik Bilgisi Koruması veya RDP için Kısıtlı Yönetici Modu, Uzak Masaüstü sunucusuna kimlik bilgilerini düz metin olarak göndermez.

o Remote Credential Guard'ı zorunlu kılmak için, Require Windows Defender Remote Credential Guard'ı seçin.

▪ Bu yapılandırmada, Uzak Masaüstü bağlantısı yalnızca uzak bilgisayar Uzak Kimlik Bilgileri Koruması gereksinimlerini karşılıyorsa başarılı olur.

Uzak (hedef) ana bilgisayarda Remote Credential Guard'ı etkinleştirmek için (Şekil 49):

```
HKLM\System\CurrentControlSet\Control\Lsa
Registry Entry: DisableRestrictedAdmin
Value: 0

reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v DisableRestrictedAdmin /d 0
/t
REG_DWORD
```

Şekil 49: Uzak (Hedef) Ana Bilgisayarda Uzaktan Kimlik Bilgisi Korumasını Etkinleştirmek için Kayıt Defteri Anahtarı ve Komut Seçenekleri

Remote Credential Guard'dan yararlanmak için Şekil 50'de belirtilen komutu kullanın.

```
mstsc.exe /remoteguard
```

Şekil 50: Uzaktan Kimlik Bilgisi Korumasından Yararlanma Komutu

Windows Defender Remote Credential Guard için Algılama Fırsatları

Kullanım Örneği	MITRE ID	Tanım
Disable Remote Credential Guard	T1112 – Modify Registry	Windows Kayıt Defterinde Remote Credential Guard'ı devre dışı bırakan bir hesap aranıyor. HKLM\System\CurrentControlSet\Control\Lsa Registry Entry: DisableRestrictedAdmin Value: 1 Şekil 51: Bir Hedef Uç Noktada Windows Kayıt Defterinde Uzak Kimlik Bilgisi Korumasının Devre Dışı Bırakılması

Disable Require Remote Credential Guard	T1484.001 – Domain Policy Modification: Group Policy Modification	Bir GPO yapılandırmasında Uzaktan Kimlik Bilgisi Koruması Gerektir seçeneğinin devre dışı bırakılması aranıyor. Computer Configuration > Administrative Templates > System > Credentials Delegation > Restrict delegation of credentials to remote servers Şekil 52: Bir GPO'da Uzak Kimlik Bilgisi Korumasının Devre Dışı Bırakılması

Şekil 52: Bir GPO'da Uzak Kimlik Bilgisi Korumasının Devre Dışı Bırakılması

Yerel Hesapların Uzaktan Kullanımını Kısıtla

Uç noktalarda bulunan yerel hesaplar, genellikle tehdit aktörleri tarafından bir ortamda yanal olarak hareket etmek için kullanılan ortak bir yoldur. Bu taktik, özellikle yerleşik yerel yönetici hesabının parolası birden çok uç noktada aynı değere yapılandırıldığında etkilidir.

Yerel hesapların yanal hareket için kullanılmasının etkisini azaltmak için kuruluşlar, hem yerel yönetici hesaplarının uzak bağlantılar kurma yeteneğini sınırlamayı hem de ortam genelinde yerel yönetici hesapları için benzersiz ve rastgele parolalar oluşturmayı düşünmelidir.

KB2871997 (https://support.microsoft.com/en-us/help/2871997/microsoft-security-advisory-update-to-improve-credentials-protection-a) yanal hareket için yerel hesapların kullanımını kısıtlamak için GPO ayarlarında kullanılabilen iki iyi bilinen SID'yi tanıttı.

• S-1-5-113: NT AUTHORITY\Local account
• S-1-5-114: NT AUTHORITY\Local account and member of Administrators group

Özellikle, yerel hesap BUILTIN\Administrators grubunun bir üyesiyse, SID S-1-5-114: NT AUTHORITY\Local hesabı ve Administrators grubunun üyesi bir hesabın erişim belirtecine eklenir. **Bu, herhangi bir yerel yönetim hesabı için kimlik bilgilerini kullanarak yayılan bir tehdit aktörünün (veya fidye yazılımı varyantının) durdurulmasına yardımcı olmak için kullanılabilecek en faydalı SID'dir.**

Not: SID S-1-5-114 için: NT AUTHORITY\Yerel hesap ve Yöneticiler grubunun üyesi, Yük Devretme Kümelemesi kullanılıyorsa, bu özellik, küme düğümü yönetimi için yönetimsel olmayan bir yerel hesaptan (CLUSR) yararlanmalıdır. Bu hesap, kümenin parçası olan bir uç noktada yerel Yöneticiler grubunun bir üyesiyse, ağ oturum açma izinlerinin engellenmesi küme hizmetlerinin başarısız olmasına neden olabilir. Dikkatli olun ve bu yapılandırmayı Failover Clustering'in kullanıldığı sunucularda kapsamlı bir şekilde test edin.

Adım 1 – Seçenek 1: S-1-5-114 SID

Yerel yönetim hesaplarının yanal hareket için kullanılmasını azaltmak için, aşağıdaki ayarlarda SID S-1-5-114: NT AUTHORITY\Local hesabı ve Yöneticiler grubunun üyesini kullanın:

• Bilgisayar Yapılandırması > İlkeler > Windows Ayarları > Güvenlik Ayarları > Yerel İlkeler > Kullanıcı Hakları Ataması

- o Bu bilgisayara ağdan erişimi engelle (SeDenyNetworkLogonRight)
- o Toplu iş olarak oturum açmayı reddet (SeDenyBatchLogonRight)
- o Hizmet olarak oturum açmayı reddet (SeDenyServiceLogonRight)
- oTerminal Hizmetleri aracılığıyla oturum açmayı reddet (SeDenyRemoteInteractiveLogonRight)
- o Hata ayıklama programları (SeDebugPrivilege: Ayrıcalık yükseltme ve işlem ekleme girişimi için kullanılan izin

Adım 1 – Seçenek 2: UAC Token Filtreleme

GPO ayarları aracılığıyla uygulanabilen ek bir kontrol, bir ağ oturumu sırasında uzaktan yönetim ve bağlantı için yerel hesapların kullanımına ilişkindir. İzinlerin (daha önce atıfta bulunulan) tam kapsamı kısa bir zaman diliminde uygulanamazsa, ağ tabanlı oturum açmalar için yerel hesaplara Kullanıcı Hesabı Denetimi (UAC) belirteç filtreleme yöntemini uygulamayı düşünün.

Bir GPO ayarı aracılığıyla bu yapılandırmadan yararlanmak için:

1. MS Security Guide ADMX dosyasını kullanmak için Security Compliance Toolkit'i (https://www.microsoft.com/en-us/download/details.aspx?id=55319) indirin.
2. İndirildikten sonra, SecGuide.admx ve SecGuide.adml dosyaları,
Sırasıyla \Windows\PolicyDefinitions ve \Windows\PolicyDefinitions\en-US dizinlerine kopyalanmalıdır.
3. Etki alanı için merkezi bir GPO deposu yapılandırılmışsa, PolicyDefinitions klasörünü C:\Windows\SYSVOL\sysvol\<domain>\Policies klasörüne kopyalayın.

GPO ayarı:

• Bilgisayar Yapılandırması > İlkeler > Yönetim Şablonları > MS Güvenlik Kılavuzu > Ağ oturum açmalarında yerel hesaplara UAC kısıtlamaları uygulayın.

- o Etkin

Etkinleştirildiğinde, kayıt defteri değeri (Şekil 53) her uç noktada yapılandırılacaktır:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
LocalAccountTokenFilterPolicy

REG_DWORD = “0” (Enabled)
```

Şekil 53: Yerel Hesaplar için UAC Kısıtlamalarını Etkinleştirmeye İlişkin Kayıt Defteri Anahtarı ve Değeri

0'a ayarlandığında, yüksek bütünlüklü erişim belirteçleriyle uzak bağlantılar yalnızca düz metin kullanılarak mümkündür.

FilterAdministratorToken seçeneği, RID 500 yerel yöneticisi için Yönetici Onay modunu (1) etkinleştirebilir veya (0) (varsayılan) devre dışı bırakabilir. Etkinleştirildiğinde, RID 500 yerel yönetici hesabı için erişim belirteci filtrelenir ve bu nedenle bu hesap için UAC uygulanır (sonuçta bu hesaptan uç noktalar arasında yanal hareket için yararlanma girişimlerini durdurabilir).

GPO ayarı:

• Bilgisayar Yapılandırması > İlkeler > Windows Ayarları > Güvenlik Ayarları > Yerel İlkeler > Güvenlik Seçenekleri >Kullanıcı Hesabı Denetimi: Yerleşik Yönetici hesabı için Yönetici Onay Modu

Etkinleştirildiğinde, kayıt defteri değeri (Şekil 54) her uç noktada yapılandırılacaktır:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
FilterAdministratorToken

REG_DWORD = “1” (Enabled)
```

Şekil 54: Yerel Yönetim Hesapları için Yönetici Onay Modu Gerektiren Kayıt Defteri Anahtarı ve Değeri

Not: Ayrıca, Kullanıcı Hesabı Denetimi: Tüm yöneticileri Yönetici Onay Modunda çalıştır (EnableLUA seçeneği) için varsayılan ayarın Etkin'den (Şekil 55'te gösterildiği gibi varsayılan) Devre Dışı olarak değiştirilmediğinden emin olmak ihtiyatlıdır. Bu ayar devre dışı bırakılırsa, tüm UAC ilkeleri de devre dışı bırakılır. Bu ayar devre dışı bırakıldığında, yerel yöneticiler grubunun bir üyesi olan herhangi bir yerel hesapla düz metin kimlik bilgileri veya parola karmaları kullanarak ayrıcalıklı uzaktan kimlik doğrulama gerçekleştirmek mümkündür.

GPO ayarı:

• Bilgisayar Yapılandırması > İlkeler > Yönetim Şablonları > MS Güvenlik Kılavuzu > Kullanıcı Hesabı Denetimi: Tüm yöneticileri Yönetici Onay Modunda çalıştırın
    o Etkin

Etkinleştirildiğinde, kayıt defteri değeri (Şekil 55) her uç noktada yapılandırılacaktır. Bu varsayılan ayardır.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\
EnableLUA

REG_DWORD = “1” (Enabled)
```

Şekil 55: Tüm Yerel Yönetim Hesapları için Yönetici Onay Modu Gerektiren Kayıt Defteri Anahtarı ve Değeri

UAC erişim belirteci filtreleme, bir uç noktada yerel Yöneticiler grubundaki hiçbir etki alanı hesabını etkilemez.

2. Adım: LAPS

Bir kuruluş, uç noktalara erişmek için uzaktan kimlik doğrulamasından yerel yönetici hesaplarının kullanımını engellemenin yanı sıra, yerleşik yerel yönetici hesabı için parola rastgeleleştirmeyi zorunlu kılacak bir stratejiyi de uyumlu hale getirmelidir. Birçok kuruluş için bu görevi gerçekleştirmenin en kolay yolu, Microsoft'un Yerel Yönetici Parola Çözümlerini (LAPS) dağıtmak ve bunlardan yararlanmaktır.

LAPS ile ilgili ek bilgi için https://www.microsoft.com/en-us/download/details.aspx?id=46899 adresine bakın.

Yerel Hesaplar için Tespit Olanakları

Kullanım Örneği	MITRE ID	Tanım
Attempted Remote Logon of Local Account	T1078.003 - Valid Accounts: Local Accounts	Bir uç noktada yerel hesaplar için uzaktan oturum açma girişimleri aranıyor.

Tablo 24: Yerel Hesaplar için Tespit Olanakları

Çözüm

Fidye yazılımları da dahil olmak üzere yıkıcı saldırılar, kuruluşlar için ciddi bir tehdit oluşturuyor. Bu teknik inceleme, tehdit aktörleri tarafından ilk erişim, keşif, ayrıcalık yükseltme ve görev hedefleri için kullanılan yaygın tekniklere karşı koruma konusunda pratik rehberlik sağlar.

Bu teknik inceleme, her taktik için kapsamlı bir savunma kılavuzu olarak görülmemelidir, ancak kuruluşların bu tür saldırılara hazırlanmaları için değerli bir kaynak olarak hizmet edebilir.

Kuruluşların potansiyel olarak yıkıcı tehdit aktörlerine ve saldırılarına hazırlamasına, ortadan kaldırmasına ve sistemlerini daha güvenli hale getirmesine yardımcı olacak yöntemlere dayanmaktadır.

infinitum IT
Power of integrated Security

Yıkıcı Saldırılara Karşı Korunmak İçin Proaktif Hazırlık ve Güçlendirme

MANDIANT