
GAZİ ÜNİVERSİTESİ
Gazi
1926

GÜVENLİK UYUMLULUĞU İÇİN WİNDOWS İŞLETİM SİSTEMİ SIKILAŞTIRMA KURALLARININ UYGULANMASI VE DENETİMİ

Hasan YALPI

YÜKSEK LİSANS TEZİ
BİLGİ GÜVENLİĞİ MÜHENDİSLİĞİ ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

HAZİRAN 2020

Hasan YALPI tarafından hazırlanan "GÜVENLİK UYUMLULUĞU İÇİN WİNDOWS İŞLETİM SİSTEMİ SIKILAŞTIRMA KURALLARININ UYGULANMASI VE DENETİMİ" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Bilgi Güvenliği Mühendisliği Ana Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Doç. Dr. Aysun COŞKUN

Bilgisayar Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi ……..……..

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

Başkan: Prof. Dr. Remzi YILDIRIM ...……

Bilgisayar Mühendisliği Ana Bilim Dalı, Yıldırım Beyazıt Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

...……

Üye: Prof. Dr. Yusuf SÖNMEZ

Elektrik ve Enerji Bölümü, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

Tez Savunma Tarihi: 30/06/2020

Jüri tarafından kabul edilen bu çalışmanın Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

……..…….

Prof. Dr. Sena YAŞYERLİ

Fen Bilimleri Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

……..
Hasan YALPI
30/06/2020

GÜVENLİK UYUMLULUĞU İÇİN WİNDOWS İŞLETİM SİSTEMİ SIKILAŞTIRMA KURALLARININ UYGULANMASI VE DENETİMİ

(Yüksek Lisans Tezi)

Hasan YALPI

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Haziran 2020

ÖZET

Kurum ve kuruluşlar çoğu zaman endüstriyel güvenlik standartlarına uyum sağlamaları için gerekli olan sıkılaştırma politikalarını uygulamakta zorluklarla karşılaşırlar. Ancak bu standartların sağlanamaması da kurum ve kuruluşları siber tehditlere karşı daha savunmasız hale getirebilir. Ayrıca güvenlik uyumluluğu standartlarının sağlanamaması durumunda denetçi kuruluşlar tarafından maddi yaptırımlar da uygulanabilmektedir. Bu çalışmada güvenlik uyumluluğu ile işletim sistemi sıkılaştırma standartları tanımlanmış ve işletim sistemi sıkılaştırma kurallarının nasıl uygulanacağı sonrasında da uygulanan sıkılaştırma kurallarının nasıl denetleneceğine yönelik bir çözüm modeli ortaya konulmuştur. Çözüm modelinin tasarlandığı test ortamı etki alanı yapısında olup 2 adet sunucu ve 2 adette istemci içerecek şekilde yapılandırılmıştır. Çalışma sonunda Microsoft firması tarafından önerilen sıkılaştırma standartlarına uyumlu sanal istemci imajı oluşturulmuş ve SCCM (System Center Configuration Manager) programına Powershell ve WQL (WMI Query Language) kodları kullanılarak bu standartları denetim yeteneği kazandırılmıştır. Bu sayede güvenlik uyumluluğu denetiminin merkezi ve otomatik bir şekilde yapılabilmesi sağlanmıştır. Denetimin yapılması sonrasında iki sanal istemci imajının karşılaştırması yapılarak elde edilen sonuçlar analiz edilmiştir.

Bilim Kodu : 92403
Anahtar Kelimeler : Güvenlik Uyumluluğu, İşletim Sistemi Sıkılaştırma, Güvenlik Standartları, Denetim, Otomasyon
Sayfa Adedi : 108
Danışman : Doç. Dr. Aysun COŞKUN

IMPLEMENTING AND AUDITING WINDOWS OPERATING SYSTEM HARDENING BASELINE FOR SECURITY COMPLIANCE

(M. Sc. Thesis)

Hasan YALPI

GAZİ UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

June 2020

ABSTRACT

Institutions and organizations often have difficulties in implementing the hardening policies required to comply with industrial security standards. However, failure to meet these standards may make institutions and organizations more vulnerable to cyber threats. In addition, if security compliance standards are not met, financial sanctions can be imposed by auditor organizations. In this study, security compliance and operating system hardening standards are defined and a solution model for how to control operating system hardening rules is presented. The test environment in which the solution model has been designed has a domain structure and is configured to include 2 servers and 2 clients. At the end of the study, a virtual client image compliant with the hardening standards recommended by Microsoft company has been created and SCCM (System Center Configuration Manager) program has gained the ability to control these standards by using Powershell and WQL (WMI Query Language) codes. In this way, it has been ensured that security compliance audit can be performed centrally and automatically. After the audit, the results have been analyzed by comparing two virtual client images.

Science Code : 92403

Key Words : Security Compliance, Operating System Hardening, Security Standarts, Auditing, Automation

Page Number : 108

Supervisor : Assoc. Prof. Dr.Aysun COŞKUN

TEŞEKKÜR

Bu tezin belirlenmesi ve hazırlanması sürecinde değerli katkı ve yönlendirmeleriyle her zaman desteğini çok yakından hissettiğim, önerilerinden faydalandığım danışman hocam Sayın Doç. Dr. Aysun ÇOŞKUN'a, Yüksek Lisans eğitimim süresince sabırla manevi desteğini esirgemeyen sevgili eşim Fulya YALPI'ya, biricik kızım Almira Rüya YALPI'ya, destekleriyle beni hiçbir zaman yalnız bırakmayan çok değerli aileme teşekkür ve şükranlarımı sunarım.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

RESİMLERİN LİSTESİ

Resim **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
ADMX	Administrative Template Xml
AS	Araştırma Sorusu
BSD	Berkeley Software Distribution
CERN	Conseil Européen pour la Recherche Nucléaire
CI	Configuration Item
CIS	Center for Internet Security
CNIL	Commission Nationale l'Informatique et des Libertés
DevOps	Development and Operations
DISA	The Defense Information Systems Agency
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
HKEY	Handle to Registry Key
HKCU	HKEY Current User
HKLM	HKEY Local Machine
HTTP	Hypertext Transfer Protocol
IE	Internet Explorer
ISO	International Organization for Standardization
JCB	Japan Credit Bureau
LAN	Local Area Network
LAPS	Local Admin Password Solution
MAPS	Microsoft Action Pack Subscription
MSFT	Microsoft
MS SCCM	Microsoft System Center Configuration Manager
NIST	National Institute of Standards
NSA	National Security Agency
NTLM	New Technology LAN Manager
OU	Organizational Unit

Kısaltmalar	Açıklamalar
PCI DSS	Payment Card Industry Data Security Standard
PSH	Powershell
RPC	Remote Procedure Call
RS	Redstone
SAM	Software Asset Management
SCM	Security Compliance Manager
SCT	Security Compliance Toolkit
SID	Security Identifier
SMB	Server Message Block
SSL	Secure Sockets Layer
STIG	Security Technical Implementation Guides
SYSVOL	System Volume
TDC	Tabular Data Control
UNC	Universal Naming Convention
USGCB	United States Government Configuration Baseline
WDAV	Windows Defender Antivirüs
WMI	Windows Management Instrumentation
WQL	WMI Query Language
XML	Extensible Markup Language

1. GİRİŞ

Günümüzde kurum ve kuruluşlar hizmetlerini giderek artan bir şekilde çevrimiçi vermeye başlamışlardır. Ancak hassas bilgiler barındıran bu sistemlerin kendilerini ve hizmet vereceği kişileri siber tehditlere karşı koruması için belirlenen güvenlik standartlarına uymaları hayati öneme sahiptir. Bu standartlar ürün ve sürüm bazlı değişiklik göstereceği gibi yıllar içerisinde de sürekli gelişim göstermektedirler.

Son yıllarda güvenlik uyumluluğu standartları ihlalleri sebebiyle şirketlere ağır yaptırımlar uygulanmakta ve şirketler bu uyumluluğu sağlamak adına büyük yatırımlar yapmaktadır. Fransız Veri Koruma Kurumu (Commission Nationale de l'Informatique et des Libertés [CNIL]) 2019 yılında Google şirketine, Avrupa Birliği Genel Veri Koruma Tüzüğü (General Data Protection Regulation [GDPR]) düzenlemelerini ihlal etmesi sebebiyle 57 milyon dolar ceza uygulamıştır [1].

Yapılan araştırmalar güvenlik ihlallerinin her geçen gün daha da arttığını ortaya koymaktadır. Aşağıda bazı veri ihlaline sebep olan siber saldırılar belirtilmiştir [2];

- Tarihteki en büyük veri ihlali 2013 yılında siber saldırganların Yahoo şirketine saldırması sonucu 3 milyar kullanıcı hesabının çalınmasıyla kayıtlara geçmiştir.
- 2014 yılı sonlarında ise Yahoo şirketine yapılan siber saldırıda 500 milyon hesap ele geçirilmiştir.
- Marriott Otellerine yapılan siber saldırılar sonucu son 4 yıla ait 500 milyon müşterinin verisi ele geçirilmiştir.

Bu araştırma sonuçları bile güvenliğin ne kadar önemli olduğunu ve belirlenen güvenlik standartlarının uygulanarak bu standartlarının denetiminin yapılmasının siber tehditleri minimize etmede hayati öneme sahip olduğunu göstermektedir.

Çalışma kapsamında incelenen Windows İşletim Sistemi ise halen dünyanın en çok kullanılan masaüstü işletim sistemi olmayı sürdürmektedir. Masaüstü işletim sistemleri sektör payları raporuna göre Windows işletim sistemleri %76,52 kullanım oranıyla dünyanın en çok kullanılan işletim sistemi olma özelliğini devam ettirmektedir [3]. Masaüstü işletim sistemleri kullanım oranları çizelgede verilmiştir.

Çizelge 1.1. İşletim sistemleri kullanım oranları [4]

İşletim Sistemi	Kullanım Oranı
Windows	%76,52
OS X	%18,99
Bilinmeyen	%1,75
Linux	%1,61
Chrome İşletim Sistemi	%1,12
FreeBSD (Berkeley Software Distribution)	%0

Bu tez çalışmasında, oluşturulacak bir Etki Alanı (Domain) ortamında Windows 10 (1803) İşletim Sistemi için Microsoft firması tarafından belirlenen işletim sistemi sıkılaştırma kuralları grup politikası vasıtasıyla uygulanarak, etki alanında bulunan ve dâhil edilecek tüm bilgisayarların sıkılaştırma standartlarına uygunluğu sağlanacaktır. Sadece bu sıkılaştırma kurallarının uygulanması tek başına yeterli olmayacağından bunun yanında denetlenebilirliğinin de sağlanmasına çalışılacaktır. Özetle işletim sistemi sıkılaştırma kurallarının uygulanması ve denetimini sağlayacak bir çözüm modeli oluşturulacaktır.

Kapsam

Bu tezde Windows İşletim Sistemi güvenlik sıkılaştırma standardı Windows 10 sürüm 1803 için oluşturulacaktır. Uygulanan sıkılaştırma kurallarının detayları EK-2'de ayrıca belirtilmiştir. Bu kurallar Microsoft firmasının sitesinde bulunan verilere dayanmaktadır [5].

Çözüm modelinde uygulanacak sıkılaştırma kurallarının kategorileri bölüm 3.4 'de açıklanmıştır. Model, Microsoft Hyper-V sanallaştırma platformu üzerinde test etki alanı kurularak ve bu etki alanında 1 adet etki alanı sunucusu (domain controller), 1 adet MS SCCM (Microsoft System Center Configuration Manager) sunucusu ve 2 adet Windows 10 (v1803) sanal istemci makinesi kurularak oluşturulmuştur. Etki Alanı kavramı, MS SCCM'in kurulum, yapılandırma ve çalışma prensibi, Grup Politikası Yönetim Konsolunun kullanımı vb. teknik hususlar tezin kapsamı dışında olduğu için

detaylandırılmamıştır. Tezde belirlenen standartların teknik olarak uygulanması ve denetimi üzerinde durulacaktır.

Problem

Kurum ve kuruluşların çoğunluğu işletim sistemlerini sıkılaştırma ve güvenli hale getirme süreçlerini sistem yöneticilerinin tecrübelerine ve kurum içi açıklık taraması sonuçlarına göre yapılandırmaktadır. Endüstriyel standartlar çoğu zaman uygulanmamaktadır.

Tripware şirketinin 2018 yılında oluşturduğu Siber Hijyen Durumu Raporuna (State of Cyber Hygiene Report) göre her 3 kuruluştan 2'si CIS ya da DISA gibi sıkılaştırma standartlarını kurumlarında uygulamamaktadır [6].

Ayrıca, kurum ve kuruluşlar belirlenen ve uygulanan bu güvenlik sıkılaştırma kurallarına ortamlarının uyumluluğunu düzenli olarak denetleyen ve olması gereken ile mevcut durumları arasında fark analizi yapan araçlara sahip değillerdir. Bu ihtiyaçlar genellikle otomatize olmayan yöntemlerle giderilmeye çalışılmakta ve bu da denetimi zorlaştırmaktadır.

Yine Tripware şirketinin Siber Hijyen Durumu Raporuna (State of Cyber Hygiene Report) göre kuruluşların yüzde 57'si (%57) ağlarına bağlanan cihazları tespit etmelerinin saatler, günler, aylar ya da daha uzun süre aldığını belirtmiştir [7].

Bu tezde esas olarak güvenlik uyumluluğunun sağlanmasına ve aşağıda belirtilen amaçların gerçekleştirilmesine odaklanılmıştır;

1. İşletim sistemi sıkılaştırma standardının Hyper-V sanallaştırma platformunda oluşturulacak test ortamı vasıtasıyla uygulandığı bir çözüm modeli oluşturmak,
2. Oluşturulan model üzerinde otomatik olarak standartları denetleyecek bir yapıyı inşa etmek,
3. İşletim sistemi sıkılaştırma kuralı uygulanan ve uygulanmayan iki farklı istemci imajı bazında denetim sonuçlarını raporlamak ve analiz etmek.

Tezdeki esas araştırma sorumuz "Kurum ve kuruluşlar güvenlik uyumluluğu için gereken sıkılaştırma kurallarına nasıl uyumlu hale getirilebilir?" olarak belirlenmiştir.

Bu sorunun cevaplanması için aşağıdaki araştırma sorularına cevap bulunacaktır.

AS1: Güvenlik uyumluluğu için mevcut endüstriyel güvenlik ve sıkılaştırma standartları nelerdir?

Endüstriyel olarak kabul gören güvenlik standartları PCI, HIPAA, ISO (27000 serisi), NIST (SP800 serisi) ve GDPR iken, sıkılaştırma standartları ise CIS, NSA, DISA STIGs ve Microsoft Sıkılaştırma standartlarıdır.

AS2: Güvenlik uyumluluğu için Windows işletim sistemi sıkılaştırma standardı nasıl uygulanabilir?

Microsoft firması tarafından belirlenen endüstriyel sıkılaştırma kurallarının Windows 10 (1803) istemci imajı için olan kısmı uygulanacaktır. Çözüm modeli için oluşturulan sanal platform üzerinde, EK-2'de belirtilen kurallar ile varsayılan grup politikaları karşılaştırılarak fark ve çakışma analiz yapılacaktır. Bu çalışma sonucu EK-1'de detaylandırılmıştır. Sonrasında ise sıkılaştırma kuralları için grup politikaları oluşturularak sıkılaştırma yapılacak istemci imajına uygulanması sağlanacaktır.

AS3: Güvenlik uyumluluğu için uygulanan sıkılaştırma standartları nasıl denetlenebilir?

Microsoft 2010 yılında yayınladığı ve güvenlik sıkılaştırma kuralları, politika karşılaştırma araçları vb. yetenekleri barındıran Security Compliance Manager (SCM) yazılımını yıllar içerisinde esnekliğini ve kullanım alanını kaybetmesi sebebiyle 15 Haziran 2017 tarihinde kullanımdan kaldırmıştır [8]. Her ne kadar mevcut yetenekleri Security Compliance Toolkit (SCT) aracında barındırsa da uygulanan sıkılaştırma kurallarının merkezi denetimi noktasında geçerli bir çözüm önerisi bulunmamaktadır. Oluşturulan çözüm modelinde MS SCCM merkezi, otomatize denetim aracı olarak yapılandırılacaktır. EK-2 'de uygulanan sıkılaştırma kurallarının 265 âdeti EK-3'te belirtilen powershell (PSH) kodu ile 4 âdeti de WMI Query Language (WQL) dili kullanılarak yapılandırma nesnelerine (configuration item [CI]) dönüştürülmüştür. EK-4'te dönüşüm işlemleri sonrası denetlenemeyen ayarlar sunulmuştur. Sonuç olarak MS SCCM yazılımına denetim yeteneği kazandırılacaktır.

AS4: Çözüm modelinin çalışabilirliği nasıl ölçülebilir?

Bu sorunun cevabının bulunabilmesi için sıkılaştırma uygulanan ve uygulanmayan istemci imajlarının denetim sonuçlarının analizi ve karşılaştırması gerekmektedir.

MS SCCM ile yapılan denetim sonuçlarına göre sıkılaştırma uygulanmayan imaj 269 sıkılaştırma standardı denetiminin hiçbirinde uyumluluk sağlayamamış, sıkılaştırma uygulanan tüm denetimleri uyumlu olarak tamamlamıştır. Detaylı raporlar EK-5'de bulunmaktadır.

Yöntem

Sorunun daha iyi anlaşılabilmesi maksadıyla veri ihlallerini içeren güvenlik raporları üzerine araştırmalar yapılmıştır. Bu rapor sonuçlarına göre güvenlik uyumluluğunun neden gerekli ve önemli olduğu anlaşılmaktadır. Ayrıca sıkılaştırma standartları üzerine de araştırmalar yapılmıştır.

Tez boyunca belirlenen araştırma soruları üzerine çalışılacaktır. İşletim Sistemi sıkılaştırması alanında mevcut çok fazla çalışma bulunmamaktadır. Kaynaklara genel olarak internet, akademik arama motorları, makaleler, web siteleri üzerinden ulaşılmaya çalışılmıştır.

Sıkılaştırma kurallarının tespiti açısından Microsoft firmasının endüstriyel sıkılaştırma standartlarını barındıran SCT aracından yararlanılmıştır. Bu araç Microsoft tarafından tavsiye edilen güvenlik yapılandırmalarına erişme, analiz ve test etme, düzenleme ve uygulama imkânı sunmaktadır [9].

Microsoft teknik dokümanı uyarınca oluşturulacak sanal test ortamında; sanal makinelerin oluşturulması, sıkılaştırmanın uygulanması ve denetimin sağlanmasına çalışılacaktır.

Tezin Yapısı

Araştırma sorularının cevaplanması maksadıyla tez aşağıda belirtilen şekilde yapılandırılmıştır;

1. Giriş: Tezin tanıtımı, kapsam ve yöntemin belirlenmesi ve son olarak problemin ortaya konularak araştırma sorularının oluşturulması

2. Genel Bilgiler: Tezin anlaşılması için gereken literatür taramasının yapılarak detaylandırılması
3. İşletim Sistemi Sıkılaştırma Standardının Uygulanması: Hazırlanan sanal ortamda çözüm modeli ortaya konulacaktır. Sıkılaştırma kurallarının belirlenerek varsayılan politikalarla karşılaştırılması ve sıkılaştırma yapılacak istemci imajına uygulanması da bu bölümde yapılacaktır. Bölüm içerisinde AS2'nin cevabı bulunmaya çalışılacaktır.
4. İşletim Sistemi Sıkılaştırma Standardının Denetimi: Microsoft firmasının sıkılaştırma politikalarını denetime yönelik bir çözüm önerisi bulunmamaktadır. Bu bölümde MS SCCM yazılımına bu yeteneğin kazandırılması ve denetimin sağlanması amaçlanmaktadır. Denetimin sağlanabilmesi adına uygulanan sıkılaştırma politikaları PSH ve WQL dilleri vasıtasıyla denetlenebilir nesnelere dönüştürülecek ve MS SCCM yazılıma dâhil edilecektir. Bölüm içerisinde AS3'ün cevabı bulunmaya çalışılacaktır.
5. Çözüm Modelinin Geçerlemesi: Çözüm modelinin çalışabilirliğini ortaya koyma adına güvenlik uyumluluğu denetim sonuçları, sıkılaştırma uygulanan ve uygulanmayan istemci imajları üzerindeki farklılıklar ortaya konularak analiz edilecektir. Bölüm içerisinde AS4'ün cevabı bulunmaya çalışılacaktır.
6. Sonuç ve Öneriler: Tezin genel özeti, araştırma sorularının cevaplanması ve kısıtlar belirtilecektir. Gelecekte yapılabilecek çalışmalara yönelik önerilerde bulunulacaktır.
7. EK-1 Politikaların Karşılaştırılma Sonuçları: Policy Analyzer aracı vasıtasıyla varsayılan ayarlarla oluşturulmuş etki alanının politikaları ile önerilen sıkılaştırma politikalarının karşılaştırma detayları bulunmaktadır.
8. EK-2 Uygulanan Sıkılaştırma Politikaları: Microsoft tarafından Windows 10 (1803) İS için önerilen sıkılaştırma politikaları ve ayrıntıları bulunmaktadır.
9. EK-3 Dönüşüm Kodu: Uygulanan sıkılaştırma grup politikalarının denetlenebilmesi için MS SCCM'e entegrasyonunu sağlayan PSH dönüşüm kodu bulunmaktadır.
10. EK-4 Denetlenemeyen Sıkılaştırma Politikaları: Dönüşüm sonrası denetlenemeyen standartlar ve ayrıntıları bulunmaktadır.
11. EK-5 Çözüm Modeli Denetim Raporları: Sıkılaştırma uygulanan ve uygulanmayan istemci imajlarının denetlenmesi sonrasında elde edilen detaylı rapor bulunmaktadır.

2. KAVRAMSAL ÇERÇEVE

Bu bölümde tez konusunun anlaşılabilmesi adına yapılan literatür çalışmaları sonuçları bulunmaktadır. İşletim sistemi sıkılaştırması kavramı açıklanacak ve güvenlik uyumluluğunun anlamı ve neden önemli olduğuna yönelik bilgi verilecektir. Ayrıca güvenlik ve sıkılaştırma standartları hakkında da bilgi verilecektir. Microsoft firmasının endüstriyel sıkılaştırma standardından da kısaca bahsedilecektir.

2.1. Güvenlik Uyumluluğu

Güvenlik uyumluluğu için literatürde farklı tanımlar bulunmaktadır. Lustig'e göre [8], "Düzenleyici uyumluluk, organizasyonların endüstri için gereken kanun, kural, standart, tanımlama ve düzenlemelere bağlı olmasıdır.".

Julisch ise [11], güvenlik uyumluluğunu "Bilgi teknolojisi sistemlerinde dışarıdan dayatılan fonksiyonel güvenlik gereksinimlerine uygunluk durumu" olarak ifade etmiştir.

Lustig [12], şirketlerin birtakım gereksinimleri karşılamaları gerektiğini aksi takdirde bazı olumsuz sonuçlarla karşılaşabileceklerini belirtmiş ve "Çoğu düzenleyici standartlar kişilerin ve şirketlerin verilerini korumak için bulunmaktadır" demiştir.

Birçok araştırma raporu veri ihlallerinin giderek arttığını ortaya koymaktadır. Tezin giriş bölümünde de örneklerini verilen bu ihlaller ancak güvenlik uyumluluğunun önemi anlaşılmasıyla azaltılabilir çünkü güvenlik uyumluluğu kurum ve kuruluşları daha fazla güvenli bir ortam oluşturmalarına yardım etmektedir.

2.2. İşletim Sistemi Sıkılaştırması

Bu bölümde işletim sistemi sıkılaştırması kavramı açıklanacaktır. Yapılan literatür taramalarında açıklayıcı tanımlara ulaşılmıştır.
Andress [13], işletim sistemi sıkılaştırmasını "İşletim sistemi sıkılaştırmasının ana amaçlarından biri işletim sisteminin saldırıya uğrayabileceği uygun alanları azaltmak" olarak tanımlamıştır.

Siik [14] ise sıkılaştırma kavramını “sistem saldırı yüzeyini azaltmak ve böylece güvenliği artırmak için sistem özelliklerini, programları veya bağlantı noktalarını kaldırmak veya devre dışı bırakmak” olarak tanımlamıştır.

İşletim sistemi sıkılaştırması güvenlik uyumluluğu gereksinimlerinin karşılanması içinde önemlidir. Endüstri tarafından kabul edilen birçok güvenlik standardı, işletim sistemi sıkılaştırma politikasının takip edilmesini istemekte ve denetçilerde bunun uygulandığını kontrol etmektedir.

Sistem sıkılaştırması kullanılan teknolojilerin yaşam döngüsü süresince gereklidir. Ayrıca sistem sıkılaştırmasının yapılması HIPAA ve PCI DSS güvenlik uyumluluğu standartları tarafından şart koşulmaktadır [15].

2.3. Güvelik Ve Sıkılaştırma Standartları

Kurum ve kuruluşları veri ihlallerine karşı korumak için dünya çapında kabul gören güvenlik uyumluluğu standartları bulunmaktadır.

PCI DSS, Ödeme Kartları Endüstrisi Veri Güvenliği Standartları olarak tanımlanabilir. Dünya genelinde kullanılan bu standart sayesinde, kart ödemelerinin güvenli bir şekilde yapılması, sahtecilik ve dolandırıcılık işlemlerine karşı etkin bir koruma sağlanmaktadır. Visa, Master Card, American Express ve JCB’nin yer aldığı PCI SSC adı verilen konsey tarafından kurulmuş olan bu sistem teknik ve operasyonel bir sistemdir [16].

Genel Veri Koruma Yönetmeliği (General Data Protection Regulation [GDPR]) Avrupa genelinde AB vatandaşlarının kişisel verilerini korumaya yönelik oluşturulmuş yönetmeliktir. 25 Mayıs 2018 tarihinden itibaren Avrupa Birliği'ne üye ülkelerde yürütmeliğe giren GDPR, Avrupa Birliği'ne üye ülkelerde büyük kurum ve kuruluşlarda var olan kişisel verilerin yönetmelikte belirtilen kurallar çerçevesinde güvenliğini sağlamayı konu edinmektedir. GDPR Avrupa birliği sınırları içerisindeki vatandaşlarının kişisel verilerini barındıran bütün işletmeleri kapsar. Şirketin konumu Avrupa birliği sınırları içerisinde bulunmasa dahi bu vatandaşların verilerini topladığı için yönetmelikten sorumlu tutulmaktadır [17].

Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (Health Insurance Portability and Accountability Act [HIPAA]), 1996 yılında kabul edilmiş olup bir standartlar bütünü olarak; dünya genelinde sağlık sektöründe referans bir güvenlik standardı olarak kullanılmaktadır. HIPAA, Sağlık Sistemini oluşturan sektörde, Gizlilik ve Güvenlik gerektiren, özel gerekliliklerin uygulanması ve raporlanması için kurallar tanımlar [18].

Yukarıda belirtilen standartları dışında Uluslararası Standartlar Örgütü (International Organization for Standardization [ISO]) 2700 ailesi standartları ve Ulusal Standartlar ve Teknoloji Enstitüsü Özel Yayını (National Institute of Standards and Technology Special Publication [NIST]) standartları gibi başka standartlarda bulunmaktadır [19].

Endüstriyel olarak kabul edilmiş sıkılaştırma standartları da bulunmaktadır. Bu standartlar aşağıda belirtilmiştir.

İnternet Güvenliği Merkezi (Center for Internet Security [CIS]) kâr amacı gütmeyen ve misyonu siber savunma için en iyi çözümleri tespit, geliştirme ve sürdürme olan bir kuruluştur. Siber güvenlik alanındaki uzmanlık ve dünya genelindeki bilişim uzmanlarının tecrübelerinden faydalanır [20].

Savunma Bilgi Sistemleri Ajansı (The Defense Information Systems Agency [DISA]), siber tehditleri azaltma ve sıkılaştırılmış sistemlerin oluşturulması için teknik yolları gösteren ve Güvenlik Teknik Uygulama Kılavuzları (Security Technical Implementation Guides [STIGs]) belgelerini sağlayan bir ajanstır. STIG'lar standartlarla uyumlu sistemlerin sıkılaştırılması için gereken tanımlamaları içeren rehberlerdir [21].

Aynı şekilde Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology [NIST]) ve Microsoft firmasının da işletim sistemi sıkılaştırmasına yönelik standartları bulunmaktadır.

Tez çalışmamızda ise Microsoft firması tarafından Windows 10 işletim sistemi için önerilen sıkılaştırma standartları kullanılmıştır.

2.4. Microsoft Sıkılaştırma Standardı

Microsoft, ürünlerinde aldığı güvenlik önlemlerine ek olarak, çeşitli sıkılaştırma standartları sağlayarak daha güvenli bir ortam oluşturulmasına olanak sağlamaktadır. Windows ve Windows Server işletim sistemleri güvenli olacak şekilde tasarlanmış olsa da birçok kuruluş güvenlik yapılandırmaları üzerinde daha ayrıntılı denetim istemektedir. Microsoft yöneticilerin kendi sıkılaştırma standartların oluşturması yerine, Microsoft'un geniş çapta bilinen ve iyi sınanmış endüstri kurallarının uygulanmasını önermektir. Bu şekilde esnekliğin artırılabileceğini ve maliyetlerin azaltılacağını belirtmiştir. Windows 10 için 3000 'den fazla grup politikası ayarı bulunmakta ve bunlara 1 800'den fazla Internet Explorer 11 ayarı da eklenirse sayı 4 800'e ulaşmaktadır. Eğer Microsoft tarafından önerilen ayarlar kullanılmaz ise bu 4 800 ayarın analizi ve etkilerinin belirlenmesi içinden çıkılmaz bir hal alabilir. Bu noktada en iyi yöntem önerilen standartların uygulanmasıdır [22].

Önerilen sıkılaştırma standartları Microsoft İndirme Merkezinden, SCT aracı indirilmek suretiyle elde edilmiştir. Bu araç Microsoft'un bütün ürünleri için sıkılaştırma standartlarını içerisinde barındırmaktadır [23].

Resim 2.1. SCT sıkılaştırma standardının seçilmesi [24]

2.4.1. Microsoft güvenlik çerçevesi

Geçmişte Windows 10 güvenlik yapılandırması faaliyeti her kullanıcının kendisinin yapması gereken bir iş olarak görülmekteydi. Bu anlayışın sonunda da birçok farklı

yapılandırma ortaya çıkmıştır. Standart sağlama noktasında Microsoft halen güvenlik, üretkenlik ve kullanıcının tecrübi faktörleri arasında denge sağlarken güvenlik yapılandırmalarının uygulanmasını basitleştiren bir yapıya geçmiştir.

Microsoft ayrıca Windows 10 işletim sistemleri için basit ve anlaşılır puanlama esasına dayalı güvenlik skoru oluşturmuştur.

Çizelge 2.1. Güvenlik skor kartı [25]

Adı	**Tavsiye**	**Puan**
İşletim Sistemi Güncellemeleri	Son yayınlanan güncellemeleri yükle	**72**
Exploit Guard	Saldırı yüzeyi azaltma kurallarını aktive et	**33**
Exploit Guard	Kontrollü dosya erişimini aktive et	**32**
Anti virüs	Antivirüs raporlamayı düzenle	**19**
Credential Guard	Kimlik korumasını aktive et	**17**
Bitlocker	Sürücü uyumluluğunu sağla	**17**
Bitlocker	Destekleyen tüm sürücüleri şifrele	**8**
Windows Hello	Tüm kullanıcıların Hello kullanmasını sağla	**7**

Güvenlik yapılandırma çerçevesi ise Amerika Birleşik Devletleri Silahlı Kuvvetleri alarm seviyelerinden esinlenerek oluşturulan 5 seviyeli bir yapıdır. Ayrıntıları aşağıda belirtilen bu seviyelerin sayı numaraları azaldıkça sıkılaştırma seviyesi de artmaktadır [26].

Şekil 2.1. Beş seviyeli güvenlik mimarisi [27]

1. Kuruluş Güvenliği: Bu güvenlik seviyesi en az yapılandırmayı içermektedir. Bu seviyede yapılacak bir güvenlik yapılanmasının oluşturulması 30 gün içerisinde tamamlanabilir.
2. Kuruluş Yüksek Güvenliği: Bu güvenlik seviyesi kullanıcıların hassas veya gizli bilgiye eriştiği bilgisayarlar için tasarlanmıştır. Bu seviyedeki yapılandırmalar uygulamalar uyumluluğunu etkileyebileceği için denetle-yapılandır-uygula akışı içerisinde hareket edilmelidir. Bu seviyede yapılacak bir güvenlik yapılanmasının oluşturulması 90 gün içerisinde tamamlanabilir.
3. Kuruluş VIP Güvenliği: Bu güvenlik seviyesi yüksek risk grubunda olan kullanıcıların, güvenlik ekiplerinin kullandıkları bilgisayarlar için tasarlanmıştır. Organize ve desteklenen gelişmiş saldırgan gruplarının hedefi olan kurumlar bu yapılandırmayı kullanmalıdır. Bu seviyede uygulama noktasında zorluklarla karşılaşılabilir ve kurum çapında uygulama süresi 90 günü geçmektedir.
4. DevOps İş İstasyonu: Bu güvenlik seviyesi kimlik hırsızlığı saldırılarına maruz kalabilecek seviyede yüksek yönetici haklarına sahip geliştiriciler ve test faaliyeti icra eden kullanıcıların kullandığı bilgisayarlar için tasarlanmıştır.
5. Yönetici İş İstasyonu: Bu seviye ise yüksek seviyede yetkiye sahip yöneticilerin kullandıkları bilgisayarlar için oluşturulmuştur. Gelişim aşamasındadır.

Tez çalışmamızda kullandığımız Windows güvenlik kurallarının uygulanması 3'üncü seviye güvenlik sağlamaktadır.

2.4.2. Windows 10 sıkılaştırma standardı

Microsoft sıkılaştırma standartları her işletim sistemi için farklı yapılandırma ayarları sunmaktadır. Bu bölümde Windows 10 sürüm 1803 için önerdiği ayarlar incelenecektir.

Windows 10 sürüm 1803 için oluşturulan sıkılaştırma standartları 11 alt bölümden oluşmaktadır. Alt bölümlerin içeriği aşağıda detaylandırılmış olup içerikler Microsoft firmasının resmî sitesinde bulunan tablolar incelenerek elde edilmiştir [28];

1. Güvenlik Şablonu: Kendi içerisinde Oturum Açılması (3 adet ayar), Şifre Politikası (6 adet ayar), Güvenlik Opsiyonları (37 adet ayar) ve Kullanıcı Hak Tahsisleri (26 adet ayar) olmak üzere toplam **72 adet** sıkılaştırma ayarı barındırmaktadır. Tez çalışmamızda bu ayarların tamamı uygulanmıştır.

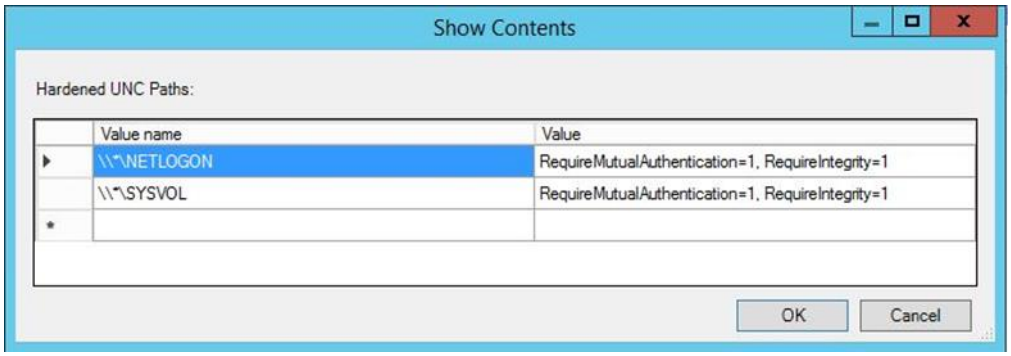
2. Gelişmiş Denetim Politikası: Kendi içerisinde Oturum Açılması (1 adet ayar), Hesap Yönetimi (2 adet ayar), Detaylı İzleme (2 adet ayar), Oturum Aç/Kapat (5 adet ayar), Nesne Erişimi (4 adet ayar), Politika Değişimi (4 adet ayar), Ayrıcalıklı Kullanım (1 adet ayar) ve Sistem (1 adet ayar) olmak üzere toplam *23 adet* sıkılaştırma ayarı barındırmaktadır. Tez çalışmamızda bu ayarların tamamı uygulanmıştır.
3. Windows Defender Güvenlik Duvarı: Kendi içerisinde Etki Alanı Profili (6 adet ayar), Özel Profil (6 adet ayar) ve Genel Profil (8 adet ayar) olmak üzere toplam *20 adet* sıkılaştırma ayarı barındırmaktadır. Tez çalışmamızda bu ayarların tamamı uygulanmıştır.
4. Bilgisayar: Kendi içerisinde Denetim Masası (2 adet ayar), Ağ (5 adet ayar), Sistem (17 adet ayar) ve Windows Bileşenleri (44 adet ayar) olmak üzere toplam *68 adet* sıkılaştırma ayarı barındırmaktadır. Tez çalışmamızda bu ayarların tamamı uygulanmıştır.
5. WDAV: Windows Bileşenleri (7 adet ayar) olmak üzere toplam *7 adet* sıkılaştırma ayarı barındırmaktadır. Tez çalışmamızda bu ayarların tamamı uygulanmıştır.
6. Kullanıcı: Kendi içerisinde Başlangıç Menüsü ve Görev Çubuğu (1 adet ayar) ve Windows Bileşenleri (1 adet ayar) olmak üzere toplam *2 adet* sıkılaştırma ayarı barındırmaktadır. Tez çalışmamızda bu ayarların tamamı uygulanmıştır.
7. IE Bilgisayar: Windows Bileşenleri (116 adet ayar) olmak üzere toplam *116 adet* sıkılaştırma ayarı barındırmaktadır. Tez çalışmamızda bu ayarların tamamı uygulanmıştır.
8. IE Kullanıcı: Windows Bileşenleri (1 adet ayar) olmak üzere toplam *1 adet* sıkılaştırma ayarı barındırmaktadır. Tez çalışmamızda bu ayarların tamamı uygulanmıştır.
9. LAPS: LAPS (1 adet ayar) olmak üzere toplam *1 adet* sıkılaştırma ayarı barındırmaktadır. Tez çalışmamızda bu ayarların tamamı uygulanmıştır.
10. Özel Ayarlar: Microsoft Güvenlik (11 adet ayar) olmak üzere toplam *11 adet* sıkılaştırma ayarı barındırmaktadır. Tez çalışmamızda bu ayarların tamamı uygulanmıştır.
11. Servisler: Servisler (4 adet ayar) olmak üzere toplam *4 adet* sıkılaştırma ayarı barındırmaktadır. Tez çalışmamızda bu ayarların tamamı uygulanmıştır.

2.4.3. Uygulama noktasında kritik sıkılaştırma ayarları

Tez çalışmamızda önerilen bütün sıkılaştırma ayarları uygulanmıştır. Ancak bazı ayarların uygulanması noktasında dikkatli olunması gerekmektedir.

Bu ayarlar aşağıda belirtilmiştir [29].

1. Sıkılaştırılmış UNC yolu (Hardened UNC path) Bu ayarın öncesi tüm UNC paylaşımları güvenilir olarak kabul edilmekteydi, bu ayar vasıtasıyla artık güvenilmeyen kaynaklardan çalıştırılabilecek kodların engellenmesi sağlanmıştır. Bu ayar grup politikası konsolunda aşağıdaki gibi görünmektedir.



Resim 2.2. Sıkılaştırılmış UNC yolu ayarları

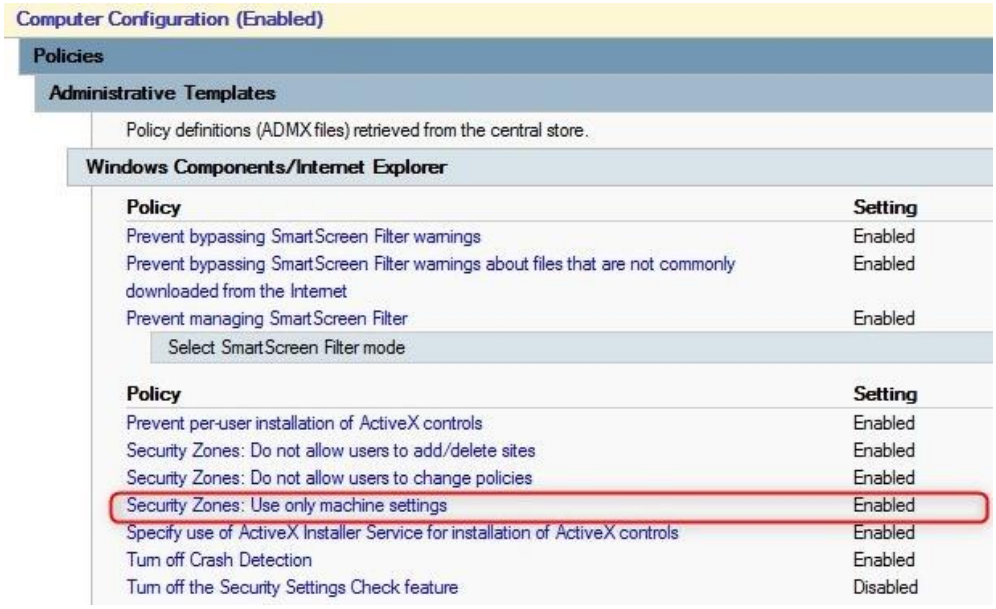
Bu ayarın uygulanması sonrasında bazı istemci bilgisayarlarında aşağıdaki hata alınabilmektedir.

The processing of Group Policy failed. Windows attempted to read the file \\yourdomain.fqdn\sysvol\yourdomain.fqdn\Policies\ {GPO GUID}\gpt.ini from a domain controller and was not successful.

Hata oluşması halinde de düzeltilmesi maksadıyla; *RequireMutualAuthentication=0, RequireIntegrity=0, RequirePrivacy=0* olacak şekilde yeniden değiştirilmesi gerekmektedir.

2. IE Bilgisayar Politika Ayarları

Eğer IE kullanıcı politikası, IE bilgisayar politikasından önce uygulanmakta ise sonradan uygulanan IE bilgisayar politikası önceki politikanın Güvenlik Bölgesi (Security Zone) ayarlarını değiştirmektedir.

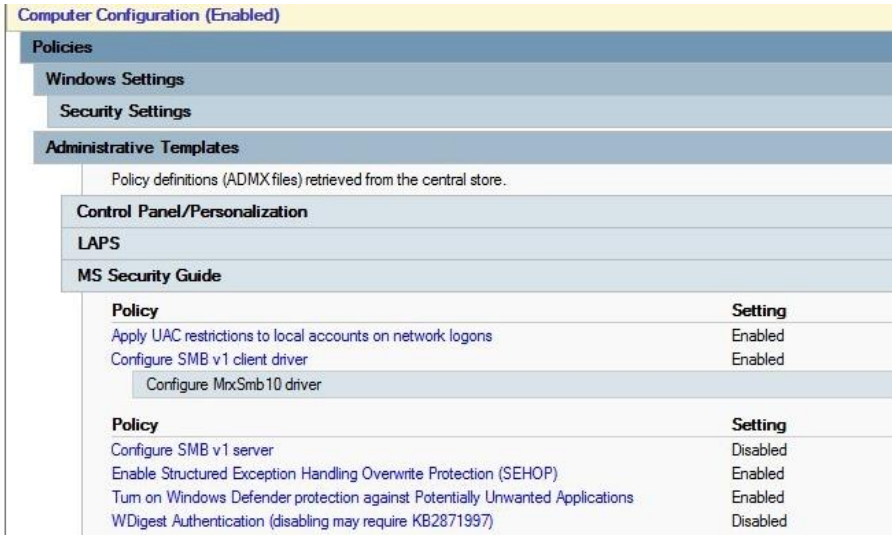


Resim 2.3. IE bilgisayar politika ayarları

Bu sorunun çözümü için ise IE Bilgisayar politikasının içerisine IE kullanıcı politikası ayarlarının dahil edilmesi gerekmektedir.

2. SMB Versiyon 1 Ayarları

Windows 10 versiyon 1709 ile SMB 1.0 varsayılan olarak kapatılmaktadır. WannaCry saldırısında en çok istismar edilen açık olan SMB 1.0'ın, aktif hale getirilmesi kesinlikle önerilmemektedir [30].



Resim 2.4. SMB versiyon 1'in kapatılma ayarı

2.5. Literatür Taraması

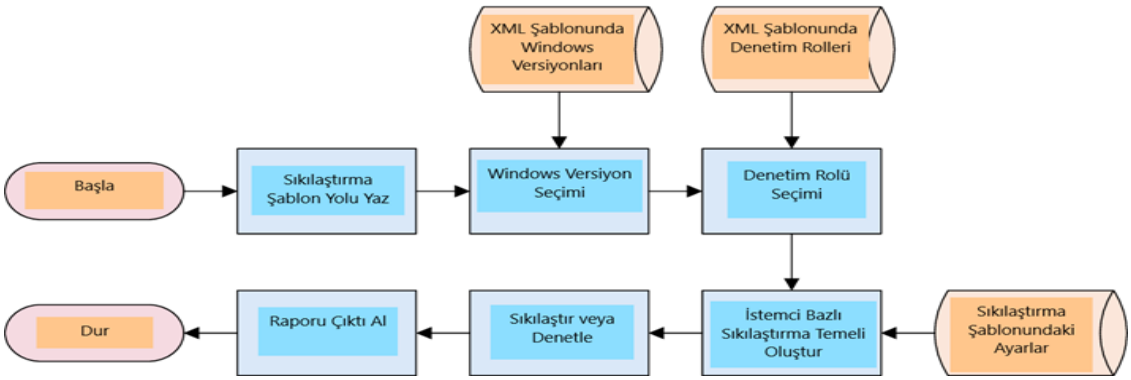
Güvenlik uyumluluğu ve işletim sıkılaştırması konularının önemine rağmen ülkemizde bu alanda yapılan bir araştırmaya rastlanılmamıştır. Dünyada ise kısıtlı olmakla birlikte birtakım araştırmalar tespit edilerek aşağıda özetlenmiştir.

Montesino ve Fenz [31], ISO 27001 ve NIST SP800-53 standartlarını esas alarak kaç tane güvenlik kontrolünün otomatize edilebileceğini analiz eden araştırmalarında mevcut araçlarla belirtilen standartlardaki güvenlik kontrollerinin yüzde 30 'unun (%30) otomatize edilebileceğini belirtmişlerdir. Araştırmalarında uygulama noktasında bir çözüm sunmamışlar ancak kullanılabilecek araçları ortaya koymuşlardır.

Jõgi [32], Linux işletim sistemleri için sıkılaştırma standardının oluşturulması, uygulanması ve denetimi üzerine çalıştığı tezinde DSA STIG for Red Hat Linux standardı kullanmış ve oluşturduğu denetim kodu vasıtasıyla 138 adet standardın 29 âdetinin (%21) sıkılaştırma yapılmayan imajda eksik olduğunu tespit etmiştir. Bu çalışmadaki en önemli kısıt denetim kodunun otomatik olarak tetiklenememesi ve tüm ortamın yüzdesel uyumluluk oranını ortaya çıkaran raporlama yeteneğinin olmamasıdır.

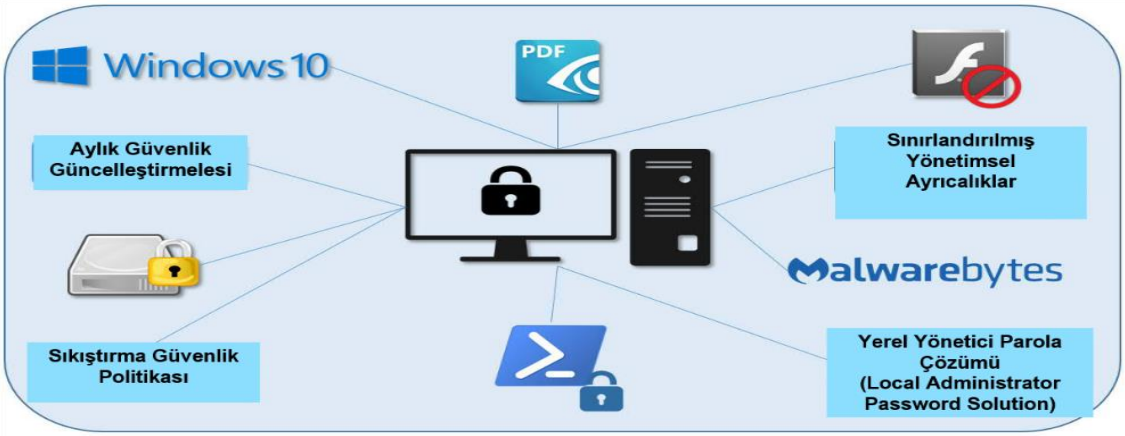
Siik [33] ise tezinde endüstriyel kontrol sistemlerinde işletim sistemi sıkılaştırmasının yönetimi üzerine çalışmalar yapmıştır. Bu çalışmada iki adet PSH kodu vasıtasıyla sıkılaştırmanın uygulanması ve denetimi üzerinde durulmuştur. Ancak oluşturulan kodların

tam fonksiyonel çalışmaması ve bazı servislerin (Xbox vb.) denetlenememesi gibi kısıtları bulunmaktadır. Çalışmasında ortaya koyduğu sıkılaştırma ve denetim akış şeması tez çalışmamızda da kullandığımız yöntemin belirlenmesinde fayda sağlamıştır.



Şekil 2.2. Sıkılaştırma ve denetim akış şeması [34]

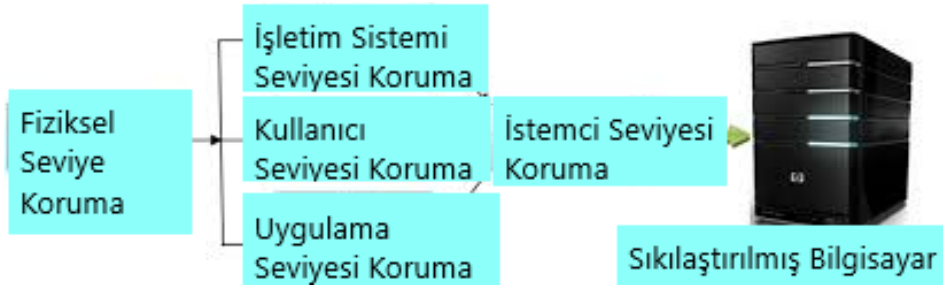
Zamora, Kwiatek, Bippus ve Elejalde [35] ise, CERN'de kullanılan 8 000'den fazla Windows işletim sistemine sahip bilgisayarın sıkılaştırılması üzerine yaptıkları çalışmada grup politikalarını kullanarak ve bazı uygulamaların kaldırılması suretiyle bir model oluşturmuşlardır. Adobe Reader uygulamasının 878 adet zafiyet içermesi sebebiyle onun yerine PDF X-Change adında (1 adet bilinen zafiyeti bulunmaktadır.) başka bir program kurmuşlardır. Grup politikaları vasıtasıyla Microsoft Office programlarının Macro özelliklerini pasif hale getirmişler ve internet tarayıcılara AdBlock Plus eklentisini eklemişlerdir. Windows Defender anti virüs yazılımının yanında Malwarebytes adında daha esnek bir virüs yazılımı kullanmaya başlamışlardır. Elde ettikleri yapılandırma görüntüsü aşağıdaki şekilde belirtilmiştir.



Şekil 2.3. CERN sıkılaştırma yapılandırması [36]

Yaptıkları bu çalışma sonrasında sıkılaştırma uygulanmış ve uygulanmamış bilgisayarlardaki anti virüs yazılımının ne kadar virüs tespit ettiğini analiz etmişlerdir. Sıkılaştırılmış bilgisayardaki tespit oranı yüzde 3,57 iken sıkılaştırma uygulanmayan bilgisayardaki virüs tespit oranı yüzde 6,37 olarak tespit edilmiştir ki bu sonuçlar bile başlı başına sıkılaştırmanım önemini açıkça ortaya koymaktadır.

Ibor ve Obidinnu [37] ise kritik verilere güvenli erişim için bir sistem sıkılaştırma mimarisi önerdikleri çalışmalarında istemci, uygulama, işletim sistemi, kullanıcı ve fiziksel katmanlar üzerinde koruyucu bir mekanizma oluşturmayı hedeflemişlerdir. İstemci seviyesinde, uygulama seviyesinde, işletim sistemi seviyesinde ve kullanıcı seviyesinde 4 farklı kategori oluşturmuş ve bu kategoriler için sıkılaştırmaya yönelik çözüm önerilerinde bulunmuşlardır. Aşağıdaki şekilde ortaya koydukları mimari çözüm gösterilmiştir.



Şekil 2.4. Sistem sıkılaştırma mimarisi [38]

Henttunen ise [39] çalışmasında, Amerika Birleşik Devletleri Hükümeti Yapılandırma Temeli (United States Government Configuration Baseline [USGCB]) güvenlik standartlarını baz alarak ve oluşturduğu sıkılaştırma kodlarını kullanarak otomatize bir şekilde sıkılaştırılmış işletim sistemi imajı elde etmeyi başarmıştır.

2.6. Özet

Bu bölümde güvenlik uyumluluğu ve işletim sistemi sıkılaştırması kavramlarının anlamı ve önemi anlatılmıştır. Ayrıca endüstri tarafından kabul gören DCI DSS, HIPAA, ISO, NIST güvenlik standartları ve CIS, NSA, NIST, DISA STIGs, Microsoft sıkılaştırma standartları özetlenmiştir. Uygulanan Microsoft sıkılaştırma kurallarından da kısaca bahsedilmiştir. Son olarak bu alanda yapılan çalışmalarda ortaya konulmuştur.

3. SIKILAŞTIRMA KURALLARININ UYGULANMASI

Bu bölümde Hyper-V sanallaştırma platformu üzerinde test etki alanı kurularak etki alanına alınan sanal istemci imajlarına grup politikaları vasıtasıyla sıkılaştırma kuralları uygulanacaktır. Sıkılaştırma kuralları Windows 10 (sürüm 1803) işletim sistemi temel alınarak uygulanacaktır. Bu bölüm içinde "Güvenlik uyumluluğu için Windows işletim sistemi sıkılaştırma kuralları nasıl uygulanabilir?" araştırma sorusuna cevap verilecektir.

3.1. Yaklaşım

AS2 'ye cevap bulmak amacıyla öncelikle sıkılaştırılmış işletim sisteminin amacı ve faydalarına değinilecektir. Uygulama süresince kullanacağımız araçlar ve kavramlar üzerine de bilgilendirme Kullanılan Araçlar Ve Önemli Kavramlar alt başlığı altında yapılacaktır. Sonrasında ise uygulanması planlanan sıkılaştırma kuralları belirlenecektir. Uygulanacak sıkılaştırma kuralları belirlendikten sonra test ortamı oluşturulacaktır. Test ortamında oluşturulacak istemci imajlarının birine sıkılaştırma kuralları uygulanırken diğeri varsayılan ayarlarda bırakılacaktır. Bu yaklaşım çözüm modelinin geçerlemesi ve farklılıkların ortaya konması adına önemlidir.

3.2. Sıkılaştırılmış İşletim Sistemi İmajının Faydaları

Windows İşletim Sistemleri varsayılan olarak her ne kadar güvenlik önlemleri alınarak üretilse de siber saldırıların hedefi olabilmekte ve açıklıklar barındırabilmektedir. Ortak Güvenlik Açığı ve Etkilenmeler (Common Vulnerabilities and Exposures [CVE]) indeksinin 2019 yılında en çok açıklık görülen 50 ürün listesinin ilk 5 sıralamasında işletim sistemleri bulunmakta ve Windows 10 işletim sistemi ise bu indekste 4'üncü sırada bulunmaktadır [40].

Çizelge 3.1. İşletim sistemleri açıklık raporu [41]

Sıra No	Ürün Adı	Üretici	Açıklık Sayısı
1	Android	Google	414
2	Debian Linux	Debian	360
3	Windows Server 2016	Microsoft	357
4	Windows 10	Microsoft	357

İşletim Sistemi sıkılaştırmasının yapılması ise siber saldırılara ve virüslere karşı önlem almamıza yardımcı olacaktır.

Yapılan bir araştırmaya göre CIS sıkılaştırma standardının ilk 5 kontrolünün kuruluşlarca uygulanması halinde siber saldırıların yüzde 85 (%85)'ini engellemek mümkün iken, 20 kontrolün tamamının uygulanması halinde ise saldırıların yüzde 97 (%97)'sinin engellenmesi mümkün olmaktadır [42].

Zamora ve arkadaşlarının Windows işletim sistemine sahip bilgisayarın sıkılaştırılması üzerine yaptıkları çalışmada, sıkılaştırılma uygulanan bilgisayarlarda daha az zararlı yazılım tespit edildiği ortaya koyulmuştur. Aşağıda elde ettikleri sonucu gösteren çizelge bulunmaktadır.

Çizelge 3.2. Tespit edilen zararlı yazılım yüzdeleri [43]

	Sıkılaştırma Uygulanmış Bilgisayarlar	Varsayılan Ayarlardaki Bilgisayarlar
Virüs Tespit Yüzdesi	%3,57	%6,37

Yukarıdaki çalışma sonuçları sıkılaştırmanın faydasını göstermesi açısından önemlidir.

3.3. Kullanılan Araçlar Ve Önemli Kavramlar

Tez içerisinde bahsedilen araç ve kavramların özet bilgileri aşağıda verilmiştir.

Etki Alanı (Domain); kullanıcı, bilgisayar, grup ve sunucu gibi birçok nesnenin bulunduğu merkezi yönetim ve güvenlik sağlayan bir yapılanmadır [44].

Grup Politikası; Microsoft Windows aktif dizinin kullanıcı ve bilgisayar hesaplarına ek denetimler ekleyen bir özelliğidir. Grup politikası, bilgi teknolojileri ortamlarında merkezi yönetimi ve işletim sistemlerini yapılandırmasını sağlar. Grup politikası, kullanıcının bilgisayarlarını sızma ve veri ihlallerine karşı korumanın başka bir yöntemidir [45].

Policy Analyzer (Politika Analiz) aracı; tekrarlayan grup politikalarını, grup politikaları arasındaki farklılıkları ortaya çıkaran ve politika ayarlarını karşılaştırmaya yarayan bir araçtır [46].

MS SCCM; Windows tabanlı bilgisayar ve sunucuların yönetilmesini sağlayan, işletim sistemi dağıtımı, uzaktan kontrol, yama yönetimi, uygulama yönetimi ve raporlama gibi özellikleri barındıran yazılım yönetim aracıdır [47].

Powershell (PSH); Microsoft'un Windows ve Windows Server (Sunucu) işletim sistemleri üzerindeki kontrol yetkinliğini arttırmak ve otomatikleştirilmiş işlevler hazırlamak amacıyla geliştirdiği otomatikleştirme platformu ve bir betik dilidir [48].

Hyper-V; Windows 10 Professional, Windows 10 Enterprise ve Windows Server işletim sistemleri ile yerleşik olarak gelen ve bu işletim sistemlerinin yüklü olduğu bir bilgisayarda birçok işletim sistemi kurmanıza ve çalıştırmanıza olanak sağlayan bir sanal makina/bilgisayar yazılımıdır [49].

Security Compliance Toolkit (Güvenlik Uyumluluğu Araç Takımı); Microsoft tarafından tavsiye edilen Windows ve diğer Microsoft ürünlerine ait güvenlik yapılandırma kurallarının indirilmesi, analizi, testi ve düzenlenmesini sağlayan araçlar bütünüdür [50].

Yapısal Birim (Organizational Unit [OU]); Microsoft Aktif Dizini içerisinde kullanıcı, bilgisayar ve grupları barındıran yapısal bir birimdir. Yönetimsel kolaylıklar ve grup politikalarının istenen birime uygulanabilmesi için oluşturulurlar [51].

WMI (Windows Management Instrumentation); Windows işletim sistemlerinde hemen hemen her nesnenin kontrol edilebilmesini sağlayan, işletim sistemindeki operasyonları ve yönetim işlevlerini gerçekleştirebilen bir teknolojidir. Tüm bu işleri bünyesindeki 900'e

yakın sınıf sayesinde gerçekleştirebilir. Bu sınıfların her birinde çeşitli amaçlara yönelik olarak hazırlanmış fonksiyonlar bulunmaktadır [52].

Yapılandırma Nesnesi (Configuration Item [CI]); genel olarak uyumluluğu değerlendirmek için kullanılan bir yapılandırma birimidir. Bir veya daha fazla öğe ve doğrulama ölçütleri içerebilir. Kayıt defteri, dosya sistemi, aktif dizin sorgusu, WQL sorgusu, WMI sorgusu ve komut dosyası gibi farklı öğe türleri kullanılarak bir CI oluşturulabilir [53].

3.4. Sıkılaştırma Kurallarının Seçimi

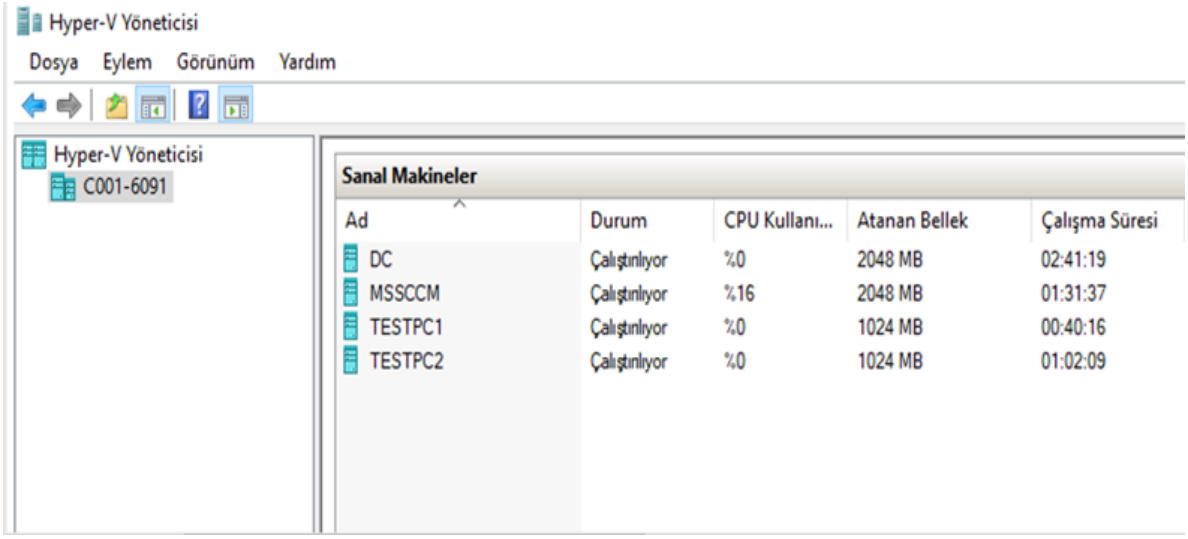
Uygulama safhasına geçmeden önce uygulanacak sıkılaştırma kurallarının ortaya konulması gerekmektedir. Uygulanacak sıkılaştırma kurallarının seçiminde Microsoft firması tarafından belirtilen sıkılaştırma kurallarından faydalanılmıştır. Bu kurallar her işletim sistemi sürümü için farklılık göstermekle birlikte, tez çalışmasında Windows 10 sürüm 1803 için olan politikalar kullanılmıştır. EK-2 ‘de ayrıntılarıyla belirtilen sıkılaştırma kuralları aşağıda belirtilen çizelgede alt kategorilere ayrılmıştır.

Çizelge 3.3. Uygulanan sıkılaştırma kuralları

Politika Adı
MSFT Internet Explorer 11- Bilgisayar (Computer)
MSFT Windows 10 RS4 - Bilgisayar (Computer)
MSFT Windows 10 RS4 - Bitlocker
MSFT Windows 10 ve Server 2016 - Defender Antivirüs
MSFT Windows 10 ve Server 2016 - Kimlik Denetimi (Credential Guard)
MSFT Windows 10 Xbox
MSFT Internet Explorer 11- Kullanıcı (User)
MSFT Windows 10 RS4 - Kullanıcı (User)

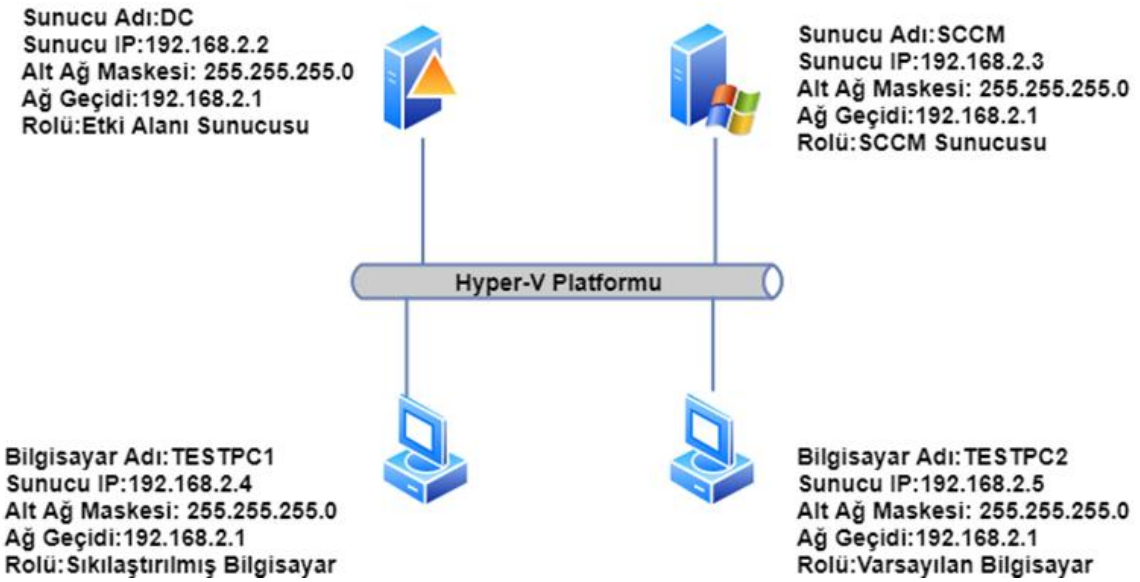
3.5. Test Ortamının Kurulması Ve Sıkılaştırma Kurallarının Uygulanması

Bu bölümde test ortamını Hyper-V sanallaştırma platformu üzerinde kurularak oluşturulacaktır. Sanallaştırma platformu üzerinde oluşturulan sunucu ve bilgisayarlar Resim 3.1’de belirtilmiştir.



Resim 3.1. Test sanallaştırma platformu

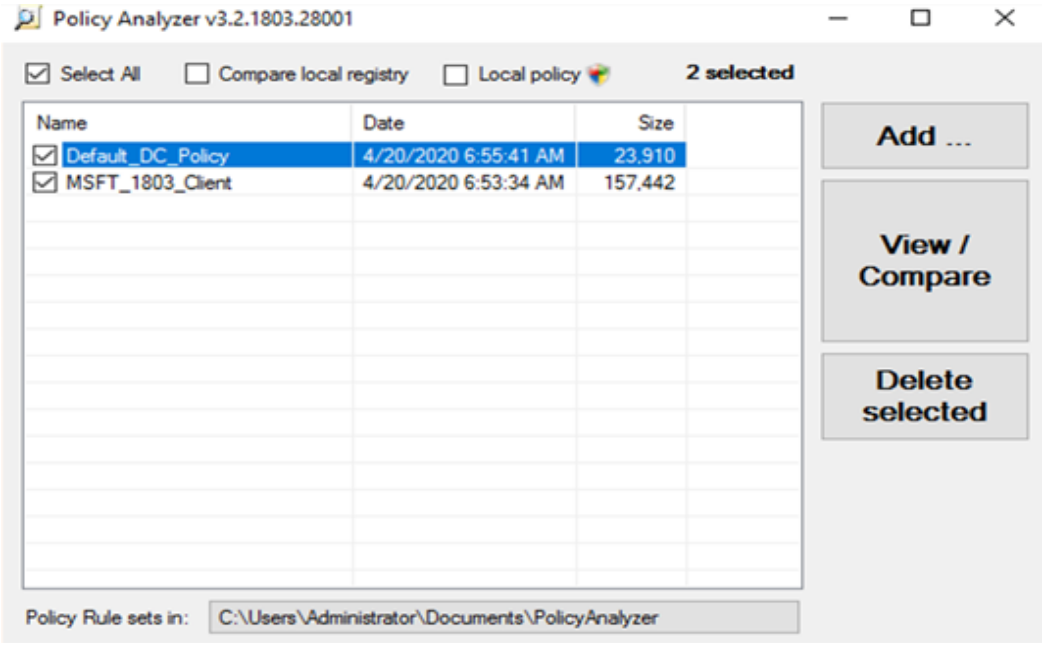
Sanallaştırma platformu üzerinde oluşturulan test etki alanı topolojisi ise sonraki sayfada belirtilmiştir.



Şekil 3.1. Test etki alanı topolojisi

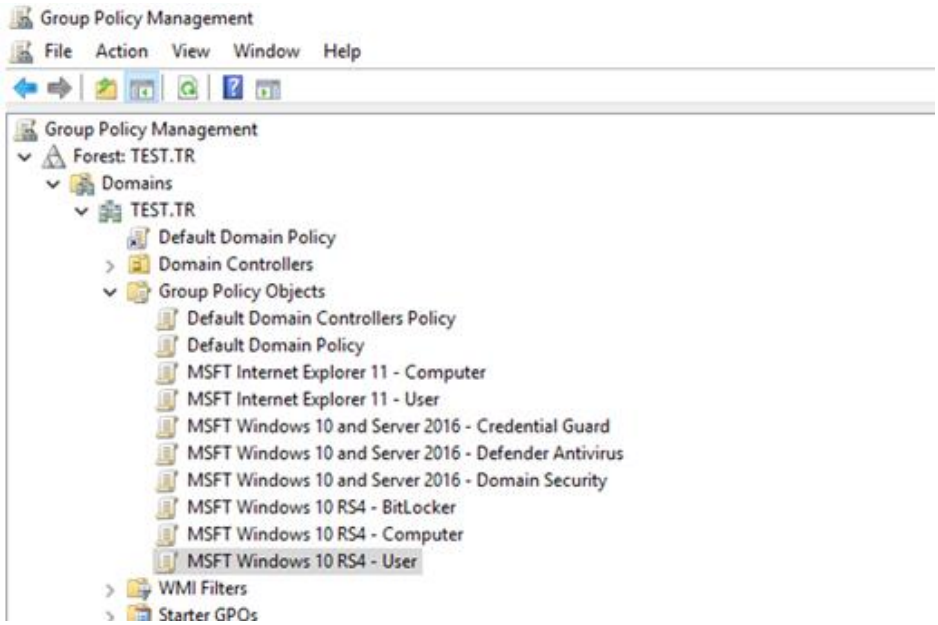
Sanallaştırma ortamının kurulmasından sonra Policy Analyzer (Politika Analiz) aracı ile varsayılan olarak gelen ve sıkılaştırma maksadıyla uygulanacak politikaların karşılaştırması yapılarak farklılıkları ortaya konulmuştur. Bunun amacı varsayılan olarak gelen politikaların gereksinimleri karşılamada ne kadar eksik olduğunu ortaya koymaktır. Yapılan analizler sonucunda *10 politika ayarının ortak bulunduğu ancak değerlerinin*

çakıştığı, 315 politika ayarının ise varsayılan olarak gelen politikalarda bulunmadığı ortaya çıkmıştır. Detaylı sonuçlar EK-1'de sunulmuştur.



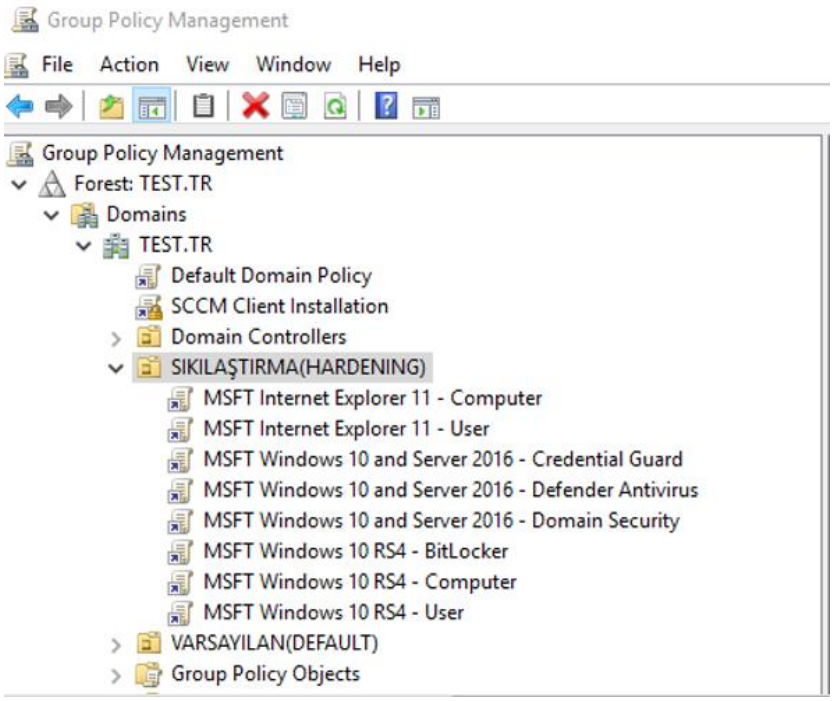
Resim 3.2. Policy Analyzer ile politika karşılaştırması

Sonrasında ise eksik politika ayarları tespit edilerek grup politikaları oluşturulmuş ve eksik ayarlar ilgili politikalara dâhil edilmiştir. Toplamda 8 adet politika oluşturulmuştur.



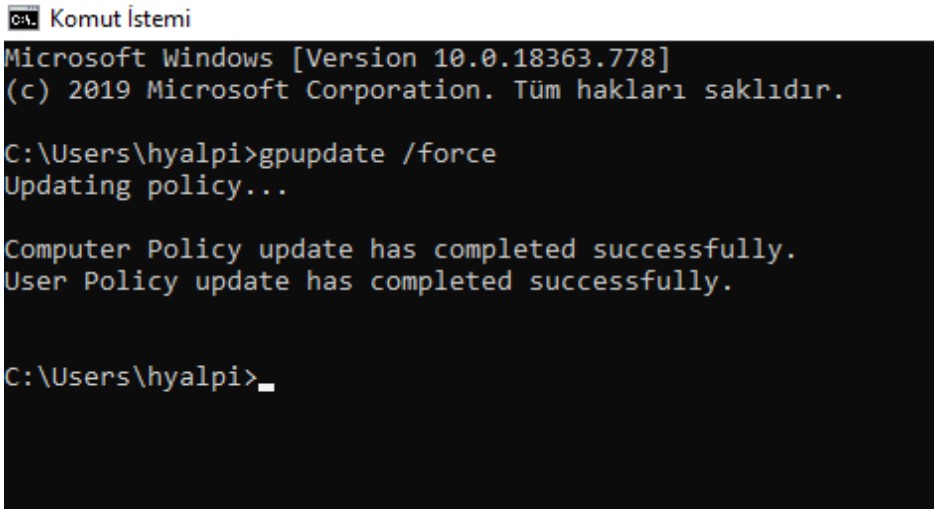
Resim 3.3. Sıkılaştırma politikalarının eklenmesi

Uygulanacak sıkılaştırma politikalarının oluşturulması sonrasında sıkılaştırma uygulanacak istemci bilgisayarı için (TESTPC1) SIKILAŞTIRMA OU'su oluşturulmuş bilgisayar bu OU'ya taşınarak sıkılaştırma politikaların SIKILAŞTIRMA OU'suna bağlanması işlemi yapılmıştır.

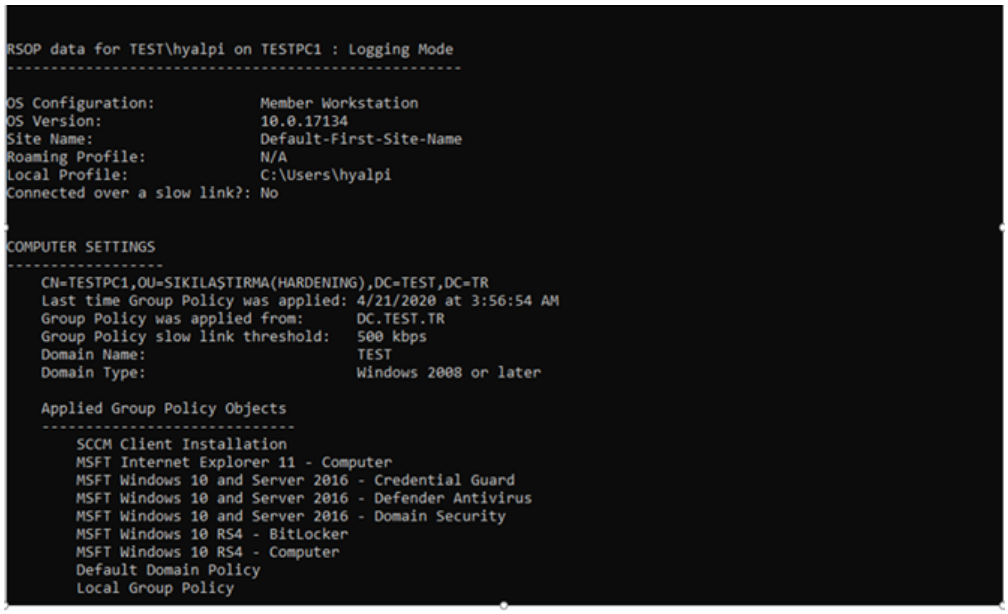


Resim 3.4. Sıkılaştırma OU'suna politikaların eklenmesi

Sıkılaştırma uygulanan TESTPC1 istemci bilgisayarı üzerinde belirtilen politikaların uygulandığını kontrol etmek maksadıyla ilgili bilgisayarın komut satırında *gpupdate /force* (Tüm politikaları güncelleme komutu) ve *gpresult /r* (Uygulanan politikaların gösterimini sağlayan komut) komutlarını yazılmış ve komutların sonuçları aşağıdaki resimlerde belirtilmiştir.



Resim 3.5. Gpupdate komutunun uygulanması



Resim 3.6. Gpresult komutunun uygulanması

Yapılan işlemler sonrasında sıkılaştırılmış istemci bilgisayarının (TESTPC1) oluşturulması faaliyeti tamamlanmıştır.

3.6. Özet

Bu bölümde işletim sistemi sıkılaştırmasının neden gerekli olduğuna değinilmiş, sonrasında da tez çalışmasında kullanılan ve çalışmanın anlaşılması adına bilinmesi gereken önemli kavramlar ve araçlar açıklanmıştır.

Çalışmada uygulanacak sıkılaştırma politikalarının seçiminde Microsoft firması tarafından belirtilen sıkılaştırma kurallarından faydalanılmıştır. Bu kurallar her işletim sistemi sürümü için farklılık göstermekle birlikte, tez çalışmasında Windows 10 sürüm 1803 için olan 8 adet politika kullanılmıştır.

Son olarakta çalışmanın yapıldığı test ortamı sanallaştırma platformu üzerinde oluşturularak TESTPC1 istemci imajına politikaların uygulanması sağlanmıştır. TESTPC1 istemcisi üzerinden de birtakım komutlar kullanılarak politikaların uygulandığının teyidi yapılmıştır.

4. SIKILAŞTIRMA KURALLARININ DENETİMİ

Bu bölümde uyumluluk denetimi konusunda yapılan çalışmalar incelenecek ve otomatize edilmiş denetimin öneminden bahsedilecektir. Sonrasında otomatize denetim için mevcut araçlar ve MS SCCM yazılımının seçilme sebebine değinilecektir. Son olarakta EK-3'te belirtilen PSH koduyla ve WQL komutlarıyla uygulanan sıkılaştırma politikalarının CI'lara dönüştürülmesi sağlanacak ve MS SCCM 'e denetim yeteneği kazandırılacaktır. MS SCCM'in denetleyemediği politika ayarları EK-4'te belirtilmiş olup özetle uygulanan 325 sıkılaştırma politikasının 269 âdeti (%82,76) denetlenebilmektedir.

4.1. Yaklaşım

3'üncü araştırma sorusuna yanıt bulmak ve çözüm modelimizin önemini ortaya koymak adına öncelikle otomatize ve merkezi güvenlik uyumluluğu denetiminin önemine *4.2.Otomatize Denetimin Önemi* kısmında bahsedeceğiz. Bu tezde amaç mevcut denetim araçlarının kullanılmasından öte kurum ve kuruluşlarda yama ve uygulama dağıtımı için kullanılan MS SCCM yazılımına bu yeteneğin kazandırılması olacaktır.

Teknik kısıtlamalar sebebiyle uygulanan 325 sıkılaştırmanın 269 âdeti denetlenebilir nesnelere dönüştürülmüştür. Kalan 56 adet ayarın denetlenebilir nesnelere dönüştürülememesinin sebebi bu ayarların bilgisayarın kayıt defterinde (registery) ve WMI veri tabanında tutulmamasıdır. Bu 56 ayar etki alanı sunucuları tarafında denetlenen parola politikası, güvenlik opsiyonları, kullanıcı hakları atamaları, hesap/oturum yönetimi ve detaylı izleme ile ilgili ayarlardır.

4.2. Otomatize Edilmiş Denetimin Önemi

Sıkılaştırma kurallarının oluşturulması ve uygulanması sağlansa da bunun denetiminin yapılması ve güvenlik bakış açısıyla uyumluluğunun kurum bazında merkezi olarak gözlemlenmesi gerekmektedir. Sadece sıkılaştırma kurallarının uygulanması başlı başına yeterli değildir.

Kurum ve kuruluşlar çoğu zaman uyumluluk denetimlerini evrak üzerinden ve çok fazla insan kaynağı tüketerek yaparlar. Ancak merkezi ve otomatize edilerek yapılan güvenlik uyumluluğu denetimi zaman ve kaynak tasarrufu sağlamanın yanında belirlenen yapılandırmalara uymayan sunucu ve bilgisayarların kolaylıkla tespitini kolaylaştırmaktadır.

Otomatize edilmiş güvenlik denetimi, organizasyonun sıkılaştırma standardı aleyhinde meydana gelebilecek değişikliklerin tespitini ve uyumsuzlukların ortadan kaldırılmasını kolaylaştıracaktır.

4.3. Otomatize Uyumluluk Denetim Araçları

Bu bölümde mevcut denetim araçlarından bazılarının karşılaştırma bilgisi verilecektir. Aşağıdaki çizelgede açık kaynak denetim yazılımlarının karşılaştırması yapılmaktadır.

Çizelge 4.1. Açık kaynak denetim araçlarının karşılaştırılması [54]

Yazılımn Adı	Destekleyen İşletim Sistemleri	İşletme Büyüklüğü	Denetim Yeteneği	Uyumluluk Yönetimi	Dosya Yönetimi	Risk Analizi	Akış Yönetimi
ADAudit Plus	Windows, Mac, Linux, Android	Küçük, Orta, Büyük	Evet	Evet	Evet	Evet	Evet
Open-Audit	Windows, Linux	Küçük	Evet	Hayır	Hayır	Evet	Hayır
Gensuite	Android	Küçük, Orta	Evet	Evet	Hayır	Evet	Evet
Qualityze	Web tabanlı	Küçük, Orta	Evet	Evet	Hayır	Evet	Evet
iAuditor	Windows, Mac, Android	Küçük, Orta	Evet	Evet	Hayır	Evet	Evet
AuditNet	Windows, Mac, Web tabanlı	Küçük, Orta	Evet	Evet	Hayır	Evet	Hayır

Çizelge incelendiğinde birçok denetim aracının bulunduğu ve yetenek açısından da neredeyse benzer yeteneklere sahip oldukları görülecektir. Ancak burada amaç denetim aracı olmayan bir yazılıma bu yeteneğin kazandırılmasıdır. Bu maksatla tez çalışmamızda uyumluluk denetim aracı olarak MS SCCM yazılımı kullanılmıştır. Bu yazılım yama yönetimi, uygulama dağıtımı ve envanter yönetimi maksatlı kullanılsa da sıkılaştırma politikalarının PSH ve WQL dilleri ile dönüştürülerek denetim nesneleri yaratılması ve böylece MS SCCM yazılımının uyumluluk denetimi yeteneğinin kazandırılması

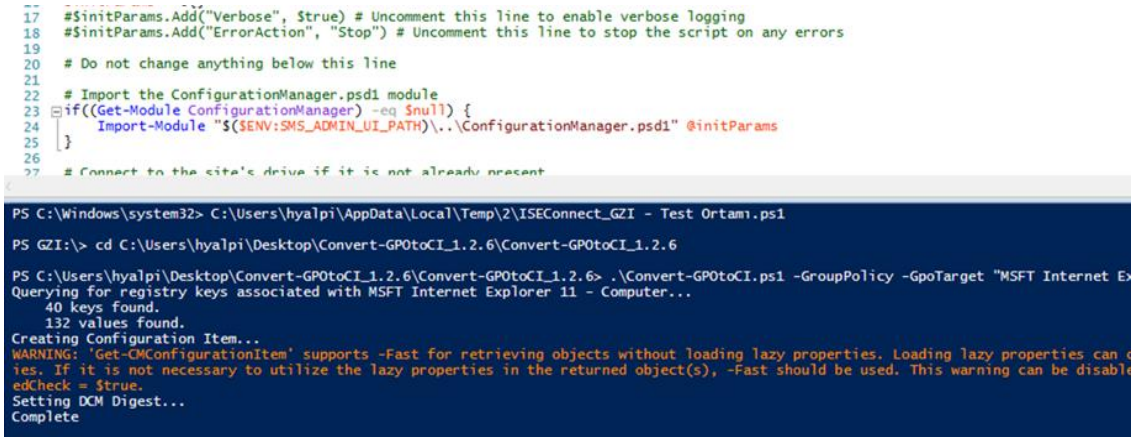
böylece MS SCCM yazılımının uyumluluk denetimi yeteneğinin kazandırılması sağlanmıştır. Uygulanan 325 sıkılaştırma ayarının 269 âdeti MS SCCM tarafından denetlenebilmektedir.

4.4. Sıkılaştırma Kurallarının Konfigürasyon Nesnelerine Dönüştürülmesi

Grup politikaları içerisinde kayıt defteri ayarlarını barındırırlar. Böylelikle uygulandıkları bilgisayar ve sunucuların kayıt defterlerini değiştirerek istenen ayarlara sahip olmaları sağlanır. EK-2'de tez çalışmasında uygulanan sıkılaştırma politikalarının ayarları ayrıntılarıyla belirtilmiştir. Bu politikaların CI'lara dönüştürülmesi maksadıyla PSH ve WQL dillerinden faydalanılmıştır.PSH dili vasıtasıyla politikaların içerisindeki kayıt defteri ayarları çekilerek bu kayıt defteri ayarlarının MS SCCM yazılımına aktarılması sağlanmıştır. Çalışmada kullanılan PSH kodu EK-3'te bulunmaktadır [55].

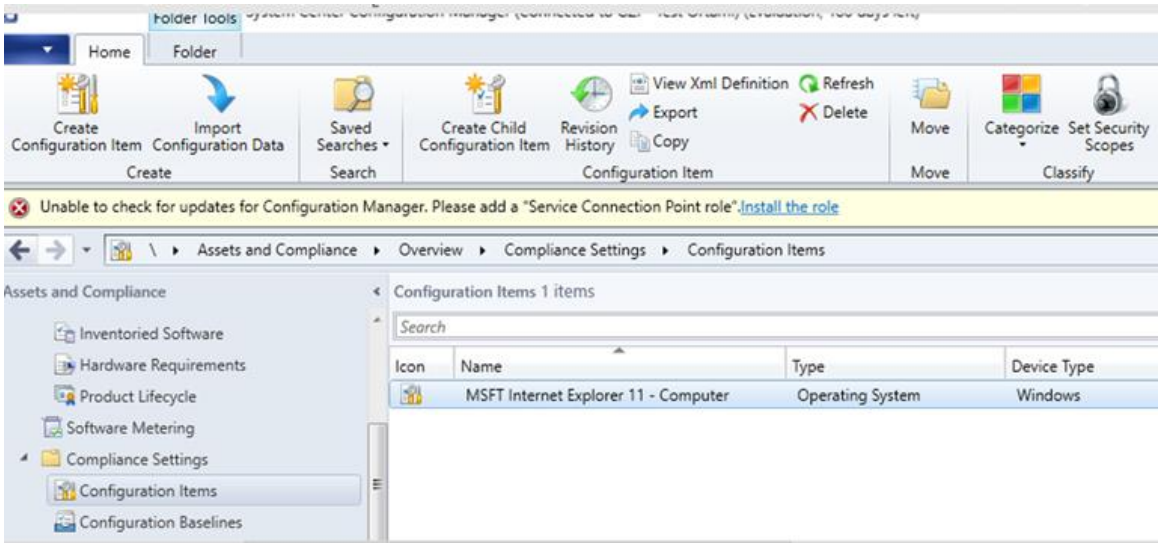
Yapılan dönüşüm işlemlerinde özellikle Xbox servislerinin denetimi noktasında PSH kodları yeterli olmamış bu noktada da WQL dili kullanarak CI'lar oluşturulmuştur. Yapılan dönüşüm işlemleri sonucunda denetlenemeyen ayarlar EK-4'te sunulmuştur.

Bu bölümde yapılan işlemler ortaya konulacaktır. Öncelikle sıkılaştırma politikaları PSH kodları vasıtasıyla dönüştürülmüştür. Dönüşüm işlemi SCCM sunucusunun PSH modülü kullanılması suretiyle ve *.\Convert-GPOtoCI.ps1 -GroupPolicy -GpoTarget "Politika Adı" -DomainTarget test.tr -SiteCode GZI -Severity Uyarı* komutuyla gerçekleştirilmiştir.



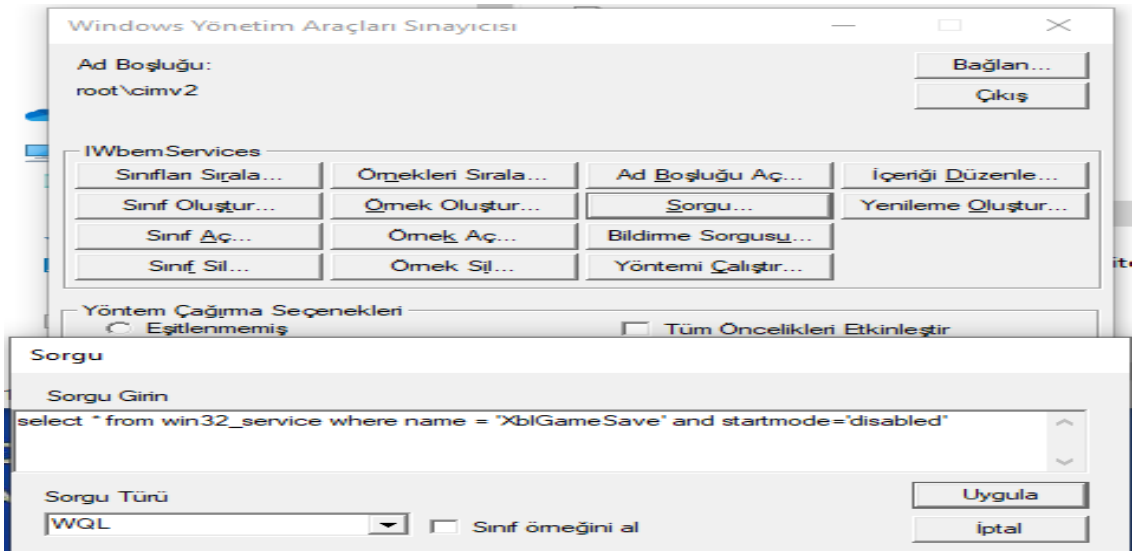
Resim 4.1. Politikaların PSH ile dönüşümü

PSH kodu vasıtasıyla dönüşüm işlemini her politika için gerçekleştirip sonrasında MS SCCM yönetim konsolunda denetim nesnelerinin oluşturulmasını sağlanmıştır. *MSFT Internet Explorer 11- Bilgisayar (Computer)* denetim nesnesinin konsol görüntüsü aşağıda gösterilmiştir.



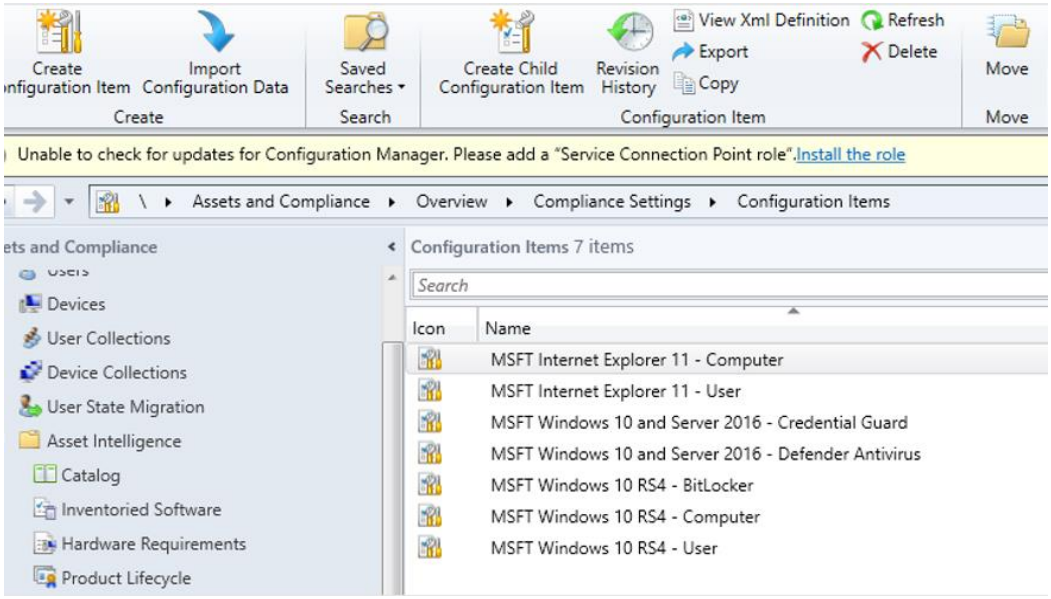
Resim 4.2. MS SCCM konsol görüntüsü

PSH kodu kullanılarak oluşturulan yapılandırma nesneleri Xbox servislerinin denetimi için gereken ayarları içermemektedir. Bu noktada WQL sorgu dilinden faydalanılmıştır. Örnek sorgu *Select * from Win32_service where name = <Servis Adı> and startmode =<Başlangıç Türü>* şeklindedir. Her bir Xbox servisi için gereken sorgular oluşturulmuştur.



Resim 4.3. WQL sorgularının oluşturulması

Bütün dönüşüm işleri tamamlandıktan sonra elde edilen MS SCCM Konsol görüntüsü aşağıdadır.

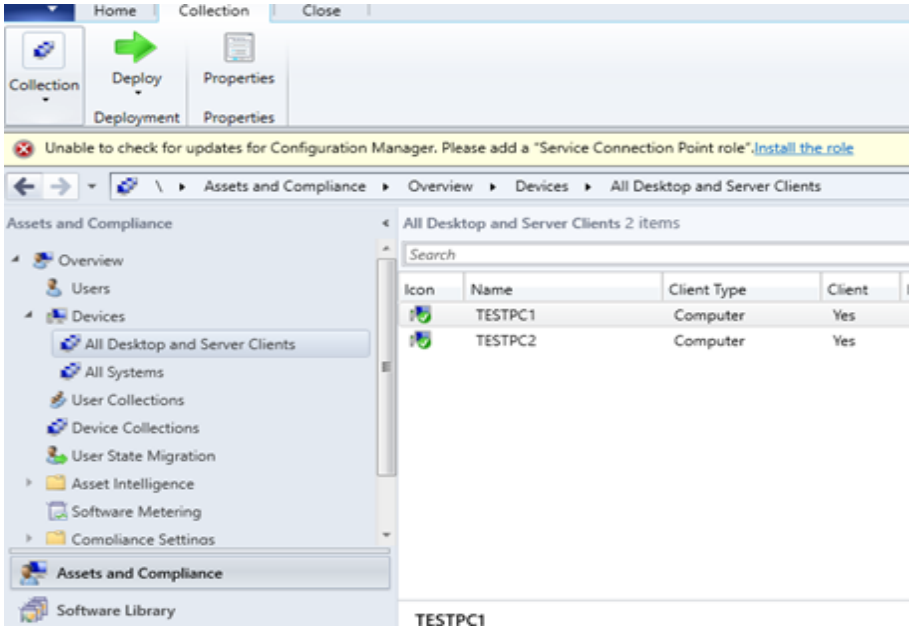


Resim 4.4. MS SCCM konsol görüntüsü

4.5. Güvenlik Uyumluluğu Denetim Testlerinin Yapılması

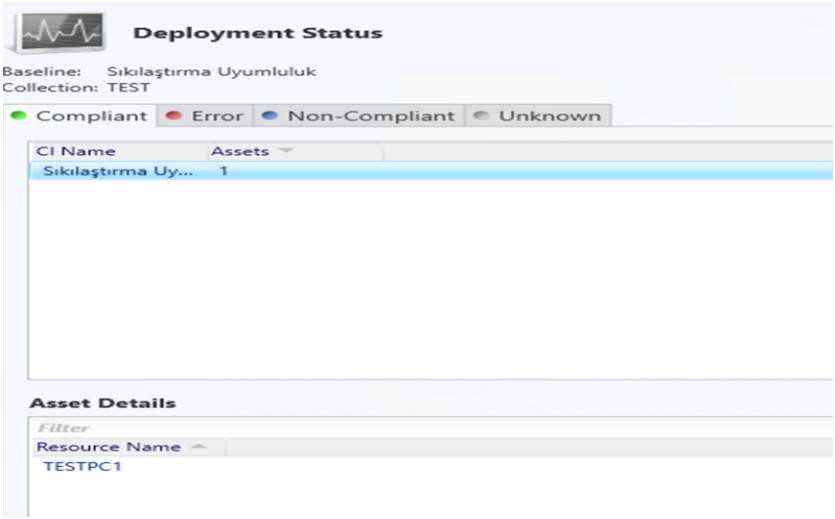
Önceki bölümde oluşturulan CI'ların denetim testlerinde kullanılması işlemi bu bölümde açıklanacaktır. Ayrıntılı denetim sonuçları 5'inci Bölümde ortaya konulacak olup detaylı sonuç raporları da EK-5'te bulunmaktadır.

Öncelikle sıkılaştırma uygulanan ve uygulanmayan istemci imajlarına MS SCCM ajanı kurularak, merkezi yönetim konsolunda aktif hale geldiğini kontrol etmemiz gerekmektedir. MS SCCM ajan kurulum faaliyeti grup politikaları vasıtasıyla yapılmakta olup bu tez kapsamında olmadığı için detaylandırılmamıştır.



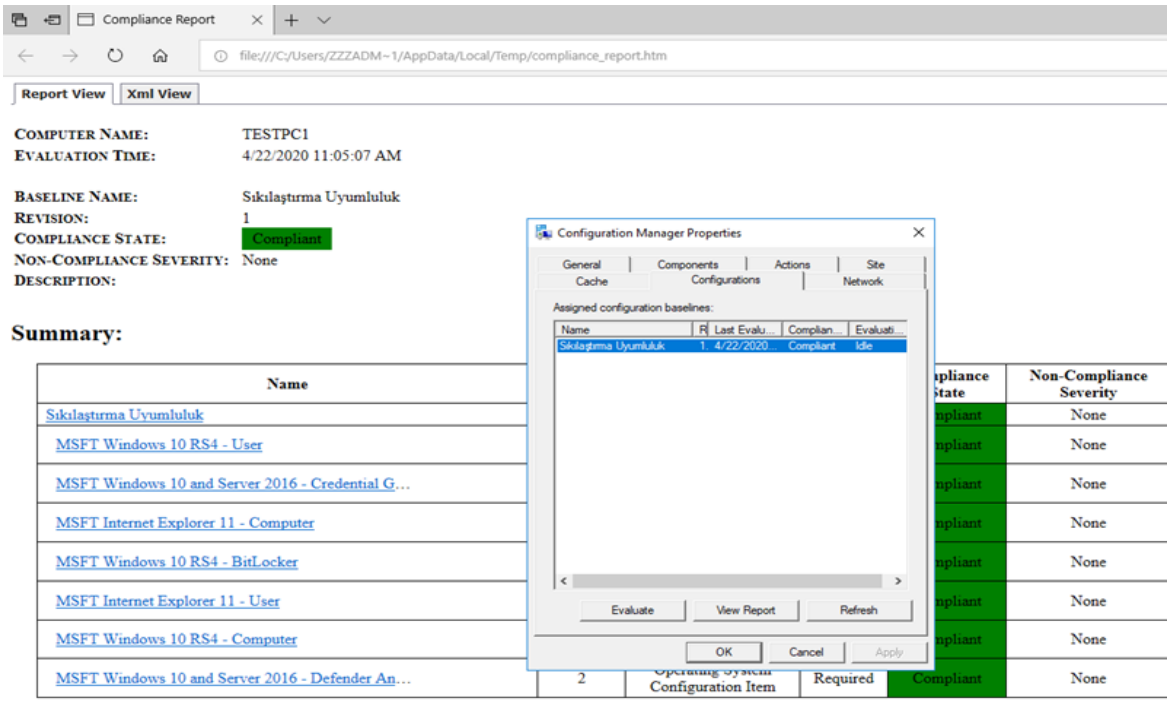
Resim 4.5. İstemci imajlarının konsol görüntüsü

Yukarıda da görüleceği üzere istemci imajları konsolda aktif hale gelmiştir. Sırada oluşturulan CI'ların iki imaja gönderilerek denetimin yapılması aşaması bulunmaktadır. Bu noktada denetim maksatlı oluşturulan CI'lar, *Sıkılaştırma Uyumluluk* adı altında toplanarak varsayılan ayarlarda bulunan ve sıkılaştırma uygulanan istemci imajlarına gönderilmiştir. Sonraki sayfada gönderim işlemi ardından merkezi sunucuya TESTPC1 (sıkılaştırma uygulanan imaj) isimli istemci imajının uyumlu olduğuna dair verinin ulaştığını gösteren konsol ekran görüntüsü bulunmaktadır.



Resim 4.6. Sıkılaştırma uyumluluğu denetiminin başlatılması

Sıkılaştırma uyumluluğu denetim ayarlarının ilgili bilgisayarlara ulaştığına yönelik sıkılaştırma uygulanan TESTPC1 isimli istemci imajı açılmış ve MS SCCM ajanı üzerinde bu denetim ayarının ulaştığı gözlemlenerek uyumluluk raporu elde edilmiştir. Özetle çözüm modelinin çalışır halde olduğu ortaya konulmuştur.



Resim 4.7. TESTPC1 üzerinde denetimin izlenmesi

4.6. Özet

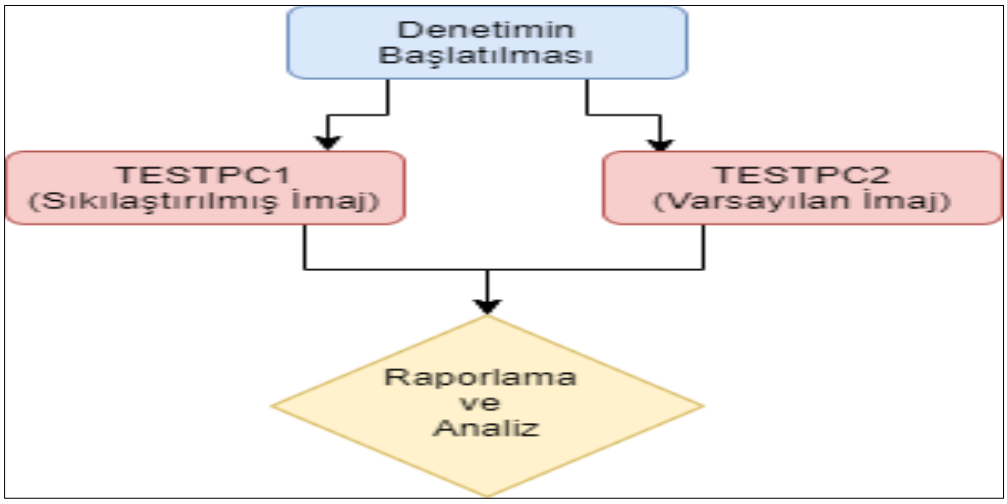
Bu bölümde otomatize denetimin öneminden bahsedilmiş ve güvenlik uyumluluğu için gereken denetim araçları hakkında bilgi verilmiştir. Hali hazırda kullanılan birçok denetim aracı bulunmakta ve genel olarak hepside benzer özellikler taşımaktadır. Ancak bu çalışmada amaç bu maksatla kullanılmayan MS SCCM yazılımına bu yeteneğin kazandırılmasıdır. Bu noktada sıkılaştırma için kullanılan grup politikalarının içerisinde barındırdığı kayıt defteri ayarları PSH kodlarıyla çıkartılmış ve 265 adet ayarın denetlenebilir hale gelmesi sağlanmıştır. Xbox servisleri ile ilgili ise WMI veritabanında servise ilişkin bulunan değerler WQL dili ile sorgulanmış ve 4 adet daha denetlenebilir nesne elde edilmiştir. Toplamda 325 adet sıkılaştırma politika ayarının 269 adeti denetlenebilmiştir. Bölüm sounda ise denetim, sıkılaştırma uygulanan TESTPC1 istemci imajı üzerinde uygulanarak, bu bilgisayar üzerinde bulunan ajan vastasıyla çalıştığının tespiti yapılmıştır.

5. ÇÖZÜM MODELİNİN GEÇERLEMESİ

Bu bölümde uyguladığımız çözüm modelimizin geçerlemesi yapılacaktır. Ayrıca geçerleme için kullandığımız yöntem ve ortamda tanımlanacaktır. Çözüm modelinin geçerlemesi adına sıkılaştırma uygulanmış ve uygulanmamış istemci imajlarının denetim sonuçları raporlanıp karşılaştırılacaktır.

5.1. Yöntem

Sanallaştırma platformu üzerinde oluşturulan iki adet sanal istemci imajını karşılaştırılacaktır. İstemcilerden birisi (TESTPC1) sıkılaştırma standartları uygulanmış imaja, diğeri ise (TESTPC2) varsayılan (sıkılaştırma uygulanmamış) imaja sahiptir. Geçerleme için bu iki sanal istemci imajının ne kadar sıkılaştırma standardına sahip oldukları denetlenecektir. Karşılaştırma MS SCCM yazılımı tarafından denetim yapılması suretiyle yapılacaktır. Test ortamı denetimi 1 saat aralıklarla olacak şekilde yapılandırılmıştır. Karşılaştırma sonuçları MS SCCM yazılımının raporlama özelliği vasıtasıyla elde edilecektir.



Şekil 5.1. Geçerleme yöntemi

5.2. Denetim Sonuçları

Sıkılaştırma uygulanmayan TESTPC2 isimli istemci imajının üzerinde 269 adet denetim yapılmış ve yapılan her bir denetimin ekran görüntüsü alınarak detaylı olarak EK-5'te

sunulmuştur. EK-5'te bulunan detaylı denetim sonuçlarının anlaşılması açısından örnek çizelge aşağıda sunulmuştur.

Çizelge 5.1. Detaylı denetim raporu açıklaması

Önem (Uyum veya uyumsuzluğu belirtir)	İfade (Olması gereken değeri belirtir)	Geçerli Değer (Mevcut değeri belirtir)	Örnek Kaynak (Kontrol edilen alanı belirtir)	Kural Tür (Denetlenen veri tipini belirtir)
Uyarı	Eşittir (Equals) 1	Boş (NULL)	Location = [Is64Bit=false]:HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4, Property = 1405	Değer

Aşağıdaki çizelgede ise varsayılan ayarlarla oluşturulmuş TESTPC2 istemci imajının genel denetim sonuçları gösterilmiştir.

Çizelge 5.2. TESTPC2 denetim raporu

Ad	Uyumluluk Durum	Uyumlu Değil Kurallar
Sıkılaştırma Uyumluluk	Uyumlu Değil	269
MSFT Windows 10 Xbox	Uyumlu Değil	4
MSFT Windows 10 RS4 - User	Uyumlu Değil	2
MSFT Windows 10 and Server 2016 - Credential Guard	Uyumlu Değil	4
MSFT Internet Explorer 11 - Computer	Uyumlu Değil	132
MSFT Windows 10 RS4 - BitLocker	Uyumlu Değil	17
MSFT Internet Explorer 11 - User	Uyumlu Değil	3
MSFT Windows 10 RS4 - Computer	Uyumlu Değil	91
MSFT Windows 10 and Server 2016 - Defender Antivirus	Uyumlu Değil	16

Sonuçlar incelenirse varsayılan ayarlarla oluşturulan istemci imajı 269 adet denetimin (268 adeti hiç bulunmamakta, 1 adeti ise eksik bulunmaktadır) hiçbirini sağlayamamıştır. Bu sonuçlar varsayılan olarak üretilen işletim sistemi imajlarının Microsoft tarafından güvenlik maksatlı önerilen hiçbir sıkılaştırma standardını sağlamadığını ortaya koymaktadır.

Bu noktada sıkılaştırma uygulanmış TESTPC1 istemci imajının denetleme sonuçlarını da ortaya koymak gerekir. Aşağıdaki çizelgede TESTPC1'in genel denetim raporu bulunmaktadır.

Çizelge 5.3. TESTPC1 denetim raporu

Adı	Uyumluluk Durmu	Uyumlu Olmayan Kurallar
Sıkılaştırma Uyumluluk	Uyumlu	0
MSFT Windows 10 Xbox Accessory Management Service	Uyumlu	0
MSFT Windows 10 RS4 - User	Uyumlu	0
MSFT Windows 10 and Server 2016 - Credential Guard	Uyumlu	0
MSFT Internet Explorer 11 - Computer	Uyumlu	0
MSFT Windows 10 RS4 - BitLocker	Uyumlu	0
MSFT Internet Explorer 11 - User	Uyumlu	0
MSFT Windows 10 RS4 - Computer	Uyumlu	0
MSFT Windows 10 and Server 2016 - Defender Antivirus	Uyumlu	0

Sonuçlar incelenirse sıkılaştırılmış istemci imajı 269 adet denetimin tamamını sağlamıştır. Bu sonuçlar sıkılaştırmanın önemini ve çözüm modelimizin çalıştığını ortaya koymaktadır.

Sıkılaştırma kurallarının uygulanması ve denetimi noktasında MS SCCM yazılımı raporlama yeteneği de sunmaktadır. Binlerce bilgisayar ve sunucunun olduğu bir ortamda yapılacak bu denetimin yöneticilere yüzdesel bir raporlama sunması denetim işlerini kolaylaştıracak ve ortamın yüzde kaçının sıkılaştırma standartlarıyla uyumlu olduğunu kolayca ortaya konulabilecektir. Test ortamımızda elde edilen rapor aşağıda belirtilmiştir. Rapor incelendiğinde test ortamımızın her bir sıkılaştırma standardına yüzdesel olarak ne kadar uyumlu olduğu görülebilecektir. Özetle çalışmada Microsoft endüstriyel sıkılaştırma standardına uyum oranı yüzde elli olarak belirlenmiştir.

Çizelge 5.4. Genel denetim raporu

Yapılandırma Temeli Adı	CI Adı	CI Tipi	Uyumluluk %	Uyumlu	Uyumlu Değil
Sıkılaştırma Uyumluluk	MSFT Windows 10 RS4 - BitLocker	OS	50	1	1
Sıkılaştırma Uyumluluk	MSFT Internet Explorer 11 - User	OS	50	1	1
Sıkılaştırma Uyumluluk	MSFT Windows 10 and Server 2016 - Defender Antivirus	OS	50	1	1
Sıkılaştırma Uyumluluk	MSFT Internet Explorer 11 - Computer	OS	50	1	1
Sıkılaştırma Uyumluluk	MSFT Windows 10 RS4 - User	OS	50	1	1
Sıkılaştırma Uyumluluk	MSFT Windows 10 and Server 2016 - Credential Guard	OS	50	1	1
Sıkılaştırma Uyumluluk	MSFT Windows 10 RS4 - Computer	OS	50	1	1
Sıkılaştırma Uyumluluk	MSFT Windows 10 Xbox	OS	50	1	1

5.3. Özet

Bu bölümde çözüm modelimizin geçerlemesini yapılmıştır. Sıkılaştırma denetimi sıkılaştırma uygulanmış ve uygulanmamış istemci imajları üzerinde yapılmış ve sıkılaştırma yapılan imajın tüm denetimleri sağladığı ancak varsayılan ayarlarla oluşturulan imajın hiçbir denetimi sağlayamadığı görülmüştür. Son olarak da test ortamının yüzdesel uyumluluk oranı ortaya çıkarılmıştır. Sıkılaştırma kurallarının denetimi noktasında önerilen modelin çalıştığı ve amaca hizmet ettiği görülmüştür.

6. SONUÇ VE ÖNERİLER

Bu tezde Microsoft firması tarafından önerilen sıkılaştırma kurallarına uyumlu Windows 10 (1803) sanal istemci imajının oluşturulması ve MS SCCM yazılımına bu sıkılaştırma ayarlarını denetim yeteneği kazandırılarak güvenlik uyumluluğu denetiminin yapılması sağlanmıştır.

Çalışmanın desteklenmesi için güvenlik uyumluluğu ve işletim sistemi sıkılaştırmasının önemine değinilmiş ve PCI DSS, HIPAA, ISO (27000), NIST(SP800) güvenlik standartları ile CIS, NSA, NIST, Microsoft sıkılaştırma standartları incelenmiştir.

Microsoft firmasının Windows 10 sürüm 1803 için belirlediği işletim sistemi sıkılaştırma kurallarının uygulanması için test ortamı oluşturulmuştur. Test ortamı Hyper-V sanallaştırma ortamı üzerinde oluşturulmuş ve kurumsal olması maksadıyla etki alanı yapısında 2 sunucu ve 2 adette istemci içerecek şekilde yapılandırılmıştır.

Sıkılaştırma kuralları belirlendikten sonra grup politikası vasıtasıyla TESTPC1 isimli istemciye sıkılaştırma uygulanmıştır. Sonra da bu uygulanan sıkılaştırma ayarları PSH ve WQL dilleriyle MS SCCM yazılımına CI olarak tanımlanmıştır. Böylece MS SCCM yazılımına denetim yeteneği kazandırılmıştır.

Son olarak çözüm modelinin geçerlemesi yapılmış ve denetim iki istemci üzerinde gerçekleştirilmiştir. Uygulanan 325 adet sıkılaştırma standardı ayarının 269 âdeti denetlenebilmiş ve sıkılaştırma uygulanan istemci tüm denetimleri geçerken uygulanmayan istemci tamamından kalmıştır.

Bu bölümde ise çalışmamızdaki kısıtlar belirtilecek ve araştırma soruları cevaplandırılacaktır. Son olarak da gelecekte yapılacak çalışmalara yönelik önerilerde bulunulacaktır.

6.1. Kısıtlar

Tez çalışması aşağıda belirtilen kısıtlamalar dâhilinde tamamlanmıştır.

1. Sıkılaştırma kurallarının belirlenmesinde Microsoft tarafından Windows 10 İşletim Sistemi sürüm 1803 için belirlenen standartlar kullanılmıştır.
2. Çözüm modelinde sıkılaştırma uygulanan sanal istemci imajı Windows 10 (1803) ‘dur. Diğer işletim sistemleri ve sürümler için uygulama ve sonuçlar farklılık gösterebilir.
3. Sıkılaştırma standartları tamamen uygulansa da denetim noktasında 269 adet ayar denetlenebilmiştir. Bunun sebebi ise kalan 56 ayarın bilgisayar üzerinde tutulmaması, etki alanı sunucu tarafından kontrol edilmesidir.
4. Sanallaştırma platformunun oluşturulduğu fiziksel bilgisayarın kaynakları sebebiyle test ortamında iki adet sunucu ve iki adet istemci oluşturulabilmiştir. Daha büyük bir ortama uygulanması halinde farklı sonuçlar elde edilebilir.
5. Gerçek ortamda bu çözüm modeli uygulanmadan önce test edilmesi gerekmektedir. Çalışmada belirtilmeyen sonuçlar elde edilmesi olasıdır.

6.2. Araştırma Sorularının Cevaplanması

Bu bölümde tezin başlangıcında ortaya konulan araştırma soruları cevaplandırılacaktır.

AS1: Güvenlik uyumluluğu için mevcut endüstriyel güvenlik ve sıkılaştırma standartları nelerdir?

Tez kapsamında PCI DSS, HIPAA, ISO (27000), NIST(SP800) güvenlik standartları ve CIS, NSA, NIST, DISA, Microsoft tarafından önerilen sıkılaştırma standartları incelenmiştir.

AS2: Güvenlik uyumluluğu için Windows işletim sistemi sıkılaştırma standardı nasıl uygulanabilir?

Hyper-V sanallaştırma platformu üzerinde etki alanı yapısında test ortamı oluşturulmuş ve Microsoft tarafından ilgili işletim sistemi ve sürüm için belirlenen sıkılaştırma standardı grup politikası vasıtasıyla uygulanmıştır. EK-2’de belirtilen grup politikası ayarlarının tamamı sıkılaştırması yapılan bilgisayara uygulanmıştır. Uygulama öncesi de Policy Analyzer aracı ile varsayılan grup politikaları ile sıkılaştırmada önerilen grup politika ayarlarının karşılaştırması yapılmıştır (EK-1). Uygulama sonrası sıkılaştırılması yapılan istemci üzerinde de sıkılaştırma ayarlarının uygulandığının teyidi yapılmıştır.

AS3: Güvenlik uyumluluğu için uygulanan sıkılaştırma standartları nasıl denetlenebilir?

İşletim Sistemi sıkılaştırma kurallarının denetlenebilmesi için sıkılaştırma standardı ayarları PSH ve WQL dilleri ile CI'lara dönüştürülmüş ve MS SCCM yazılımına dahil edilmiştir. PSH kodunun detayları EK-3'te bulunmaktadır. Dönüşüm işlemleri sonucu denetlenemeyen ayarlar ise EK-4'te ayrıntılarıyla bulunmaktadır. Denetimin otomatik ve belirlenen periyotlarda merkezi olarak yapılabilmesi sağlanmıştır.

AS4: Çözüm modelinin çalışılabilirliği nasıl ölçülebilir?

Bu araştırma sorusu aynı zamanda çözüm modelimizin geçerlemesinin yapılabilmesi maksadıyla cevaplanmıştır. MS SCCM raporlama sonuçlarına göre sıkılaştırma uygulanan istemci tüm denetimlerden geçmiş ancak uygulanmayan istemci hepsinden kalmıştır. Detaylı rapor sonuçları EK-5'te bulunmaktadır. Kısıtlı kaynak ve zaman sebebiyle sonuçlar sadece iki sanal istemci imajının karşılaştırılması vasıtasıyla elde edilmiştir.

6.3. Sonuç

Tez çalışmasının başlangıcında belirlenen bütün araştırma sonuçlarına cevap bulunmuştur. Kurum ve kuruluşlarda genellikle tam anlamıyla uygulanmayan sıkılaştırma kurallarının uygulanması yöntemi üzerine durulmuş ve Windows 10 (1803) işletim sistemi için Microsoft tarafından önerilen endüstriyel sıkılaştırma standartları temel alınmıştır. Belirlenen sıkılaştırma kurallarının uygulanması için test ortamı oluşturulmuş ve sonra da bu uygulanan kuralların denetimi noktasında birtakım dönüşümler yapılarak MS SCCM yazılımına denetim yeteneği kazandırılmıştır. Çözüm modelimizin çalıştığının geçerlemesi aşamasında sıkılaştırma uygulanan ve uygulanmayan istemci imajlarının denetimi yapılmış ve sonuçlar beklendiği şekilde elde edilmiştir. Sıkılaştırma yapılan istemci imajı tüm denetimleri geçerken varsayılan olarak üretilen imaj tüm denetimlerden kalmıştır. Varsayılan olarak üretilen imajların tavsiye edilen hiçbir sıkılaştırma ayarını içermediği tespit edilmiştir.

Veri ihlali üzerine yapılan araştırmalarda; güvenlik uyumluluğunun ve işletim sistemi sıkılaştırmasının riskleri azaltmada önemli olduğu sonucu elde edilmiştir. Tezde ortaya koyulan merkezi ve otomatize edilmiş uyumluluk denetimi çözümü kurumsal seviyede

bilgisayar ve sunucuların standartlara uyum seviyelerini ölçebilmekte ve yanlış yapılandırmaya sahip olanları raporlayabilmektedir.

Günümüzde kurum ve kuruluşlarda en çok kullanılan işletim sistemi olan Windows işletim sisteminin yine bir Microsoft ürünü olan MS SCCM ile uyumluluk denetiminin yapılması, diğer denetim araçlarına göre daha pratik ve maliyet etkin bir çözüm olarak ortaya çıkmaktadır.

6.4. Öneriler

Bu tezde ortaya konulan kısıtların gelecekte yapılacak çalışmalarda giderilmesi üzerine çalışılabilir. Ayrıca farklı güvenlik ve sıkılaştırma standartları da temel alınarak benzer çözüm modelleri geliştirilebilir. Farklı uyumluluk denetim araçlarının kullanılması sonucunda da değerli sonuçlar elde edilebilir.

KAYNAKLAR

1. İnternet: Dillet, R. (2019,21 Ocak) French data protection watchdog fines Google $57 million under the GDPR URL: https://techcrunch.com/2019/01/21/french-data-protection-watchdog-fines-google-57-million-under-the-gdpr/ Son Erişim Tarihi: 05 Nisan 2020.

2. İnternet: 7 Hidden Benefits of IT Security Compliance for Your Business.URL: https://www.cherwell.com/library/blog/it-security-compliance/ Son Erişim Tarihi: 10 Mart 2020.

3. İnternet: Operating systems market share of desktop PCs 2013-2020, by month.URL: https://www.statista.com/statistics/218089/global-market-share-of-windows-7/ Son Erişim Tarihi: 15 Mart 2020.

4. İnternet: Operating systems market share of desktop PCs 2013-2020, by month.URL: https://www.statista.com/statistics/218089/global-market-share-of-windows-7/ Son Erişim Tarihi: 15 Mart 2020.

5. İnternet: Microsoft Download Center.URL: https://www.microsoft.com/en-us/download/details.aspx?id=55319 Son Erişim Tarihi:16 Mart 2020.

6. İnternet: Tripwire State of Cyber Hygiene Report.URL: https://www.tripwire.com/-/media/tripwiredotcom/files/research/tripwire_dimensional_research_state_of_cyber_hygiene.pdf?rev=71e588867934484aac0c8bc3d5dbe3a7 Son Erişim Tarihi:3 Mayıs 2020.

7. İnternet: Tripwire State of Cyber Hygiene Report.URL: https://www.tripwire.com/-/media/tripwiredotcom/files/research/tripwire_dimensional_research_state_of_cyber_hygiene.pdf?rev=71e588867934484aac0c8bc3d5dbe3a7 Son Erişim Tarihi:4 Mayıs 2020.

8. İnternet: Security Compliance Manager (SCM) retired; new tools and procedures.URL: https://techcommunity.microsoft.com/t5/microsoft-security-baselines/security-compliance-manager-scm-retired-new-tools-and-procedures/ba-p/701059 Son Erişim Tarihi:20 Mart 2020.

9. İnternet: Microsoft Security Compliance Toolkit 1.0.URL: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10 Son Erişim Tarihi: 20 Mart 2020.

10. Lustig, M. (2015). *Compliance at Speed.* Sebastopol, California: O'Reilly Media, Inc.

11. Julisch, K. (2009). Security Compliance: The Next Frontier in Security esearch. *Proceedings of the 2008 workshop on New security paradigms*, p71-74. Rüschlikon, Switzerland.

12. Lustig, M. (2015). *Compliance at Speed.* Sebastopol, California: O'Reilly Media, Inc.

13. Andress, J. (2014). *The Basics of Information Security (Second Edition).* Waltham: Syngress.

14. Siik, P. (2017). Management of Operating System Hardening in Industrial Control Systems, Yüksek Lisans Tezi, Tampere Teknoloji Üniversitesi, Tampere, 40-43.

15. İnternet: System Hardening.URL: Son Erişim https://www.beyondtrust.com/resources/glossary/systems-hardening Tarihi: 21 Mart 2020.

16. İnternet: PCI-DSS Nedir? URL: https://blog.codevist.com/eec28e285d53 Son Erişim Tarihi: 22 Mart 2020.

17. İnternet:Gdpr Nedir? URL: https://www.beyaz.net/tr/guvenlik/makaleler/gdpr_nedir.html Son Erişim Tarihi: 23Mart 2020.

18. İnternet: HIPAA Nedir? URL: https://www.homederma.com/hipaa.php Son Erişim Tarihi: 23 Mart 2020.

19. İnternet: Information Security Compliance: Which regulations relate to me? URL: https://www.tcdi.com/information-security-compliance-which-regulations/ Son Erişim Tarihi: 25Mart 2020.

20. İnternet: Center for Internet Security (CIS) Benchmarks URL: https://docs.microsoft.com/tr-tr/microsoft-365/compliance/offering-cis-benchmark?view=o365-worldwide Son Erişim Tarihi: 01 Mart 2020.

21. İnternet: The Defense Information Systems Agency (DISA) nedir? URL: https://docs.vmware.com/en/VMwarevSphere/6.7/com.vmware.vsphere.security.doc/GUID-9478D24D-A29D-4C0D-A069-647667C6F853.html Son Erişim Tarihi: 01 Nisan 2020.

22. İnternet: Windows security baselines URL: https://docs.microsoft.com/tr-tr/windows/security/threat-protection/windows-security-baselines Son Erişim Tarihi: 23 Nisan 2020.

23. İnternet: Microsoft Download Center URL:https://www.microsoft.com/en-us/download/details.aspx?id=55319 Son Erişim Tarihi: 23 Nisan 2020.

24. İnternet: Microsoft Download Center URL:https://www.microsoft.com/en-us/download/details.aspx?id=55319 Son Erişim Tarihi: 23 Nisan 2020.

25. İnternet: Introducing the security configuration framework: A prioritized guide to hardening Windows 10 URL: https://www.microsoft.com/security/blog/2019/04/11/introducing-the-security-configuration-framework-a-prioritized-guide-to-hardening-windows-10/ Son Erişim Tarihi: 25 Nisan 2020.

26. İnternet: Introducing the security configuration framework: A prioritized guide to hardening Windows 10 URL: https://www.microsoft.com/security/blog/2019/04/11/introducing-the-security-configuration-framework-a-prioritized-guide-to-hardening-windows-10/ Son Erişim Tarihi: 25 Nisan 2020.

27. İnternet: Introducing the security configuration framework: A prioritized guide to hardening Windows 10 URL: https://www.microsoft.com/security/blog/2019/04/11/introducing-the-security-configuration-framework-a-prioritized-guide-to-hardening-windows-10/ Son Erişim Tarihi: 25 Nisan 2020.

28. İnternet: Microsoft Download Center URL:https://www.microsoft.com/en-us/download/details.aspx?id=55319 Son Erişim Tarihi: 23 Nisan 2020.

29. İnternet: How to use the Windows 10 Security Baseline URL: https://www.systemcenterdudes.com/how-to-use-the-windows-10-security-baseline/ Son Erişim Tarihi: 23 Nisan 2020.

30. İnternet: Microsoft Offers More Advice on Disabling Windows SMB 1 URL: https://redmondmag.com/articles/2017/05/18/more-advice-on-disabling-windows-smb-1.aspx Son Erişim Tarihi: 2 Nisan 2020.

31. Montesino, R., Fenz, S. (2011). Information Security Automation: How Far Can We Go?, Sixth International Conference on Availability, Reliability and Security, Vienna, 2011, pp. 280-285

32. Jõgi, M. (2017). Establishing, Implementing and Auditing Linux Operating System Hardening Standard for Security Compliance, Yüksek Lisans Tezi, Tartu Üniversitesi Bilgisayar Bilimleri Enstitüsü, Tartu, 43-44.

33. Siik, P. (2017). Management of Operating System Hardening in Industrial Control Systems, Yüksek Lisans Tezi, Tampere Teknoloji Üniversitesi, Tampere, 31-43.

34. Siik, P. (2017). Management of Operating System Hardening in Industrial Control Systems, Yüksek Lisans Tezi, Tampere Teknoloji Üniversitesi, Tampere, 40-43.

35. Zamora, P., Kwiatek, M., Bippus, V., Elejalde, E. (2019). Increasing Windows security by hardening PC configurations. EPJ Web of Conferences. 214. 08019. 10.1051/epjconf/201921408019, 4-5.

36. Zamora, P., Kwiatek, M., Bippus, V., Elejalde, E. (2019). Increasing Windows security by hardening PC configurations. EPJ Web of Conferences. 214. 08019. 10.1051/epjconf/201921408019, 4.

37. Ibor, A. E., Obidinnu, J. N. (2015). "System Hardening Architecture for Safer Access to Critical Business Data Business Data", Nigerian Journal of Technology Vol. 34 No. 4, October 2015, pp. 788 – 792.

38. Ibor, A. E., Obidinnu, J. N. (2015). "System Hardening Architecture for Safer Access to Critical Business Data Business Data", Nigerian Journal of Technology Vol. 34 No. 4, October 2015, pp. 788 – 792.

39. Henttunen, K. (2018). Automated Hardening and Testing Centos Linux 7, Lisans Bitirme Tezi, Turku Teknoloji Üniversitesi Uygulamalı Bilimler, Turku.

40. İnternet: Cve details, Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2019.URL: https://www.cvedetails.com/top-50-products.php?year=2019 Son Erişim Tarihi: 11 Nisan 2020.

41. İnternet: Cve details, Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2019.URL: https://www.cvedetails.com/top-50-products.php?year=2019 Son Erişim Tarihi: 11 Nisan 2020.

42. İnternet: Lapena, R. (2018, 9 Ağustos). Two-Thirds of Organizations Don't Use Hardening Benchmarks to Establish a Secure Baseline, Report Reveals.URL: https://www.tripwire.com/state-of-security/security-data-protection/security-hardening/organizations-hardening-benchmarks-secure-baseline/ Son Erişim Tarihi: 03 Nisan 2020.

43. Zamora, P., Kwiatek, M., Bippus, V., Elejalde, E. (2019). Increasing Windows security by hardening PC configurations. EPJ Web of Conferences. 214. 08019. 10.1051/epjconf/201921408019, 5-6.

44. İnternet: Active Directory domain URL: https://searchwindowsserver.techtarget.com/definition/Active-Directory-domain-AD-domain Son Erişim Tarihi: 23 Nisan 2020.

45. İnternet: Grup İlkesi Nedir ve Neden Önemlidir? URL: https://aktifdizin.com/grup-ilkesi-nedir-ve-neden-onemlidir/ Son Erişim Tarihi: 05 Nisan 2020.

46. İnternet: Microsoft Security Compliance Toolkit 1.0 URL: https://docs.microsoft.com/tr-tr/windows/security/threat-protection/security-compliance-toolkit-10 Son Erişim Tarihi: 06 Nisan 2020.

47. İnternet: SCCM URL: https://www.computerhope.com/jargon/s/sccm.htm Son Erişim Tarihi: 20 Nisan 2020.

48. İnternet: Windows PowerShell Nedir? PowerShell Komutları ve PowerShell ile Neler Yapılabilir? URL: https://wmaraci.com/nedir/windows-powershell Son Erişim Tarihi: 3 Nisan 2020.

49. İnternet: Windows 10'da Hyper-V Nasıl Yüklenir? URL: https://teknodestek.com.tr/windows-10da-hyper-v-nasil-yuklenir-resimli-anlatim/ Son Erişim Tarihi: 7 Nisan 2020.

50. İnternet: Microsoft Download Center URL:https://www.microsoft.com/en-us/download/details.aspx?id=55319 Son Erişim Tarihi: 18 Nisan 2020.

51. İnternet: organizational unit URL:https://searchwindowsserver.techtarget.com/definition/organizational-unit-OU Son Erişim Tarihi: 18 Nisan 2020.

52. İnternet: WMI Nedir? Sorgu ve Test Araçları Nelerdir? URL: https://www.mshowto.org/wmi-nedir-sorgu-ve-test-araclari-nelerdir.html Son Erişim Tarihi: 18 Nisan 2020.

53. İnternet: Winstanley, P. (2018,14 Kasım) Custom Configuration Items: Maybe the Most Underrated Tool in Your ConfigMgr Kit URL: https://insights.adaptiva.com/2018/custom-configuration-items-configmgr-kit/ Son Erişim Tarihi: 18 Nisan 2020.

54. İnternet: The Best 7 Free and Open Source Audit Software Solutions URL: https://www.goodfirms.co/blog/best-free-open-source-audit-software-solutions Son Erişim Tarihi: 1 Mayıs 2020.

55. İnternet: Convert-GPOtoCI URL: https://github.com/SamMRoberts/Convert-GPOtoCI Son Erişim Tarihi: 8 Nisan 2020

EKLER

EK-1. Politikaların karşılaştırılma sonuçları

Çizelge 1.1.Çakışan grup politika ayarları

Politika Grubu veya Kayıt Defteri Anahtarı	**Politika Ayarı**	**Varsayılan Politika**	**Sıkılaştırma Politikası**
Ayrıcalık Hakları	Dosya ve dizinleri yedekle (SeBackupPrivilege)	*S-1-5-32-544,*S-1-5-32-549,*S-1-5-32-551	*S-1-5-32-544
Ayrıcalık Hakları	Yetkilendirme için bilgisayar ve kullanıcı hesaplarına güvenilmesini sağla (SeEnableDelegationPrivilege)	*S-1-5-32-544	
Ayrıcalık Hakları	Yerel olarak oturum açmaya izin ver (SeInteractiveLogonRight)	*S-1-5-32-544,*S-1-5-32-548,*S-1-5-32-549, *S-1-5-32-550,*S-1-5-32-551,*S-1-5-9	*S-1-5-32-544,*S-1-5-32-545
Ayrıcalık Hakları	Aygıt sürücülerini yükle ve kaldır (SeLoadDriverPrivilege)	*S-1-5-32-544,*S-1-5-32-550	*S-1-5-32-544
Ayrıcalık Hakları	Bu bilgisayara ağdan erişin (SeNetworkLogonRight)	*S-1-1-0,*S-1-5-11,*S-1-5-32-544, *S-1-5-32-554,*S-1-5-9	*S-1-5-32-544,*S-1-5-32-555
Ayrıcalık Hakları	Uzak bir sistemden kapanmayı zorla (SeRemoteShutdownPrivilege)	*S-1-5-32-544,*S-1-5-32-549	*S-1-5-32-544
Ayrıcalık Hakları	Dosyaları ve dizinleri geri yükle (SeRestorePrivilege)	*S-1-5-32-544,*S-1-5-32-549,*S-1-5-32-551	*S-1-5-32-544
Sistem Erişimi	Başarısız oturum açma denemesi sayısı (LockoutBadCount)	0	10
Sistem Erişimi	Maksimum parola yenileme süresi (MaximumPasswordAge)	42	60
Sistem Erişimi	En Az Parola Uzunluğu (MinimumPasswordLenght)	7	14

Çizelge 1.2.Güvenlik tanımlayıcıları

Güvenlik tanımlayıcısı (Security Identifier [SID])	**Adı**
S-1-5-32-544	Yöneticiler (Administrators)
S-1-5-32-549	Sunucu Operatörleri (Server Operators)
S-1-5-32-551	Yedekleme Operatörleri (Backup Operators)
S-1-5-32-548	Hesap Operatörleri (Account Operators)
S-1-5-32-550	Yazdırma Operatörleri (Print Operators)
S-1-5-9	Kurumsal Alan Adı Denetleyicileri (Enterprise Domain Controllers)
S-1-5-32-545	Kullanıcılar (Users)
S-1-1-0	Herkes (Everyone)
S-1-5-11	Kimliği Doğrulanmış Kullanıcılar (Authenticated Users)
S-1-5-32-555	Yerleşik \ Uzak Masaüstü Kullanıcıları (Builtin\Remote Desktop Users)

EK-2. Uygulanan sıkılaştırma politikaları

Çizelge 2.1. MSFT Internet Explorer 11- bilgisayar (computer)

Bilgisayar Yapılandırması (Etkin)	
İlkeler	
Yönetim Şablonları	
Windows Bileşenleri/Internet Explorer	
İlke	**Ayar**
ActiveX denetimlerinin kullanıcı başına yüklenmesini engelle	Etkin
ActiveX denetimlerinin yüklenmesinde ActiveX Yükleyici Hizmeti'nin kullanımını belirt	Etkin
Güvenlik Ayarlarını Denetleme özelliğini kapat	Devre Dışı
Güvenlik Bölgeleri: Kullanıcıların ilke değiştirmesine izin verme	Etkin
Güvenlik Bölgeleri: Kullanıcıların site eklemesine/silmesine izin verme	Etkin
Güvenlik Bölgeleri: Yalnızca makine ayarlarını kullan	Etkin
İnternet'ten sıklıkla indirilmeyen dosyalar hakkındaki SmartScreen Filtresi uyarılarının atlanmasını engelle	Etkin
Kilitlenme Algılamasını Kapat	Etkin
SmartScreen Filtresi uyarılarını atlamayı engelle	Etkin
SmartScreen Filtresi'nin yönetimini engelle	Etkin
SmartScreen Filtresi modunu seç	Açık
Windows Bileşenleri/Internet Explorer/Güvenlik Özellikleri	
İlke	**Ayar**
SSL 3.0'a (Internet Explorer) geri dönüşe izin ver	Etkin
Güvenli olmayan geri dönüşe şunun için izin ver:	Site Yok
Windows Bileşenleri/Internet Explorer/Güvenlik Özellikleri/ ActiveX Yüklemesini Kısıtla	
İlke	**Ayar**
Internet Explorer İşlemleri	Etkin
İlke	**Ayar**
Internet Explorer İşlemleri	Etkin
İlke	**Ayar**
Internet Explorer İşlemleri	Etkin
İlke	**Ayar**
Internet Explorer İşlemleri	Etkin
İlke	**Ayar**
Internet Explorer için tarihi geçmiş ActiveX denetimlerinin engellenmesini kapat	Devre Dışı
Internet Explorer'daki tarihi geçmiş ActiveX denetimleri için "Bu kez çalıştır"ı kaldır	Etkin

EK-2. (devam) Uygulanan sıkılaştırma politikaları

Çizelge 2.1. (devam) MSFT Internet Explorer 11 – bilgisayar (computer)

Windows Bileşenleri/Internet Explorer/Güvenlik Özellikleri	
İlke	**Ayar**
Internet Explorer İşlemleri	Etkin
Windows Bileşenleri/Internet Explorer/Güvenlik Özellikleri/Mime Algılaması Güvenlik Özelliği	
İlke	**Ayar**
Internet Explorer İşlemleri	Etkin
Windows Bileşenleri/Internet Explorer/Güvenlik Özellikleri /MK Protokolü Güvenlik Kısıtlaması	
İlke	**Ayar**
Internet Explorer İşlemleri	Etkin
Windows Bileşenleri/Internet Explorer/Güvenlik Özellikleri/Tutarlı Mime İşleme	
İlke	**Ayar**
Internet Explorer İşlemleri	Etkin
Windows Bileşenleri/Internet Explorer/Internet Denetim Masası	
İlke	**Ayar**
Sertifika hatalarını yok saymayı engelle	Etkin
Windows Bileşenleri/Internet Explorer/Internet Denetim Masası/Gelişmiş Sayfa	
İlke	**Ayar**
Geliştirilmiş Korumalı Mod etkinleştirildiğinde ActiveX denetimlerinin Korumalı Mod'da çalıştırılmasına izin verme	Etkin
Geliştirilmiş Korumalı Modu'nu kapat	Etkin
İmza geçersiz olsa bile yazılımın çalıştırılmasına veya yüklenmesine izin ver	Devre Dışı
Karşıdan yüklenen programların imzalarını denetle	Etkin
Sunucu sertifikalarının geçerliliğini denetle	Etkin
Şifreleme desteğini kapat	Etkin
Güvenli Protokol bileşimleri	TLS 1.1 ve TLS 1.2 kullan
İlke	**Ayar**
Windows'un 64 bit sürümlerinde Gelişmiş Korumalı Mod çalışırken 64 bit sekme işlemlerini aç	Etkin
Windows Bileşenleri/Internet Explorer/Internet Denetim Masası/Güvenlik Sayfası	
İlke	**Ayar**
Eşleşmeyen sertifika adresi uyarısını aç	Etkin
İntranet Siteleri: Tüm ağ yollarını (UNC) içer	Devre Dışı

EK-2. (devam) Uygulanan sıkılaştırma politikaları

Çizelge 2.1. (devam) MSFT Internet Explorer 11 – bilgisayar (computer)

Windows Bileşenleri/Internet Explorer/Internet Denetim Masası /Güvenlik Sayfası/Güvenilen Siteler Bölgesi	
İlke	**Ayar**
ActiveX denetimlerine karşı kötü amaçlı yazılımdan koruma programlarını çalıştırma	Etkin
ActiveX denetimlerine karşı kötü amaçlı yazılımdan koruma programlarını çalıştırma	Devre Dışı Bırak
İlke	**Ayar**
Güvenli olarak işaretlenmemiş ActiveX denetimlerini başlat ve komut dizilerinde kullan	Etkin
Güvenli olarak işaretlenmemiş ActiveX denetimlerini başlat ve komut dizilerinde kullan	Devre Dışı Bırak
İlke	**Ayar**
Java izinleri	Etkin
Java izinleri	Yüksek güvenilirlik
Windows Bileşenleri/Internet Explorer/Internet Denetim Masası/Güvenlik Sayfası/Internet Bölgesi	
İlke	**Ayar**
.NET Çerçevesi'ne bağlı Authenticode ile imzalanan bileşenleri çalıştır	Etkin
.NET Çerçevesi'ne bağlı Authenticode ile imzalanan bileşenleri çalıştır	Devre Dışı Bırak
İlke	**Ayar**
.NET Çerçevesi'ne bağlı Authenticode ile imzalanmamış bileşenleri çalıştır	Etkin
.NET Çerçevesi'ne bağlı Authenticode ile imzalanmamış bileşenleri çalıştır	Devre Dışı Bırak
İlke	**Ayar**
ActiveX denetimlerine karşı kötü amaçlı yazılımdan koruma programlarını çalıştırma	Etkin
ActiveX denetimlerine karşı kötü amaçlı yazılımdan koruma programlarını çalıştırma	Devre Dışı Bırak
İlke	**Ayar**
Açılır Pencere Engelleyicisi Kullan	Etkin
Açılır Pencere Engelleyicisi Kullan	Etkinleştir
İlke	**Ayar**
Betik yoluyla durum çubuğu güncelleştirmelerine izin ver	Etkin
Komut dosyasıyla durum çubuğu güncelleştirmeleri	Devre Dışı Bırak
İlke	**Ayar**
Boyut ve konum kısıtlamaları olmadan komut dosyası ile başlatılan pencerelere izin ver	Etkin
Boyut ve konum kısıtlamaları olmadan komut dosyası ile başlatılan pencerelere izin ver	Devre Dışı Bırak
İlke	**Ayar**
Dosyaların sürüklenip bırakılmasına veya kopyalanıp yapıştırılmasına izin ver	Etkin
Dosyaların sürüklenip bırakılmasına veya kopyalanıp yapıştırılmasına izin ver	Devre Dışı Bırak
İlke	**Ayar**
Etki alanları arasında veri kaynaklarına erişim	Etkin

EK-2. (devam) Uygulanan sıkılaştırma politikaları

Çizelge 2.1. (devam) MSFT Internet Explorer 11 – bilgisayar (computer)

Dosyaların sürüklenip bırakılmasına veya kopyalanıp yapıştırılmasına izin ver	Devre Dışı Bırak
İlke	**Ayar**
Etki alanları arasında veri kaynaklarına erişim	Etkin
Etki alanları arasında veri kaynaklarına erişim	Devre Dışı Bırak
İlke	**Ayar**
Farklı etki alanlarındaki pencerelerde ve çerçevelerde gezin	Etkin
Farklı etki alanlarındaki pencerelerde ve çerçevelerde gezin	Devre Dışı Bırak
İlke	**Ayar**
Güvenli olarak işaretlenmemiş ActiveX denetimlerini başlat ve komut dizilerinde kullan	Etkin
Güvenli olarak işaretlenmemiş ActiveX denetimlerini başlat ve komut dizilerinde kullan	Devre Dışı Bırak
İlke	**Ayar**
Güvenli olmayabilecek dosyalar için güvenlik uyarısı göster	Etkin
Programlar ve güvenli olmayan dosyaları açma	Sor
İlke	**Ayar**
Internet Explorer WebBrowser denetimlerine betikle erişilmesine izin ver	Etkin
Internet Explorer Web tarayıcı denetimi	Devre Dışı Bırak
İlke	**Ayar**
İmzalı ActiveX denetimlerini karşıdan yükle	Etkin
İmzalı ActiveX denetimlerini karşıdan yükle	Devre Dışı Bırak
İlke	**Ayar**
İmzasız ActiveX denetimlerini karşıdan yükle	Etkin
İmzasız ActiveX denetimlerini karşıdan yükle	Devre Dışı Bırak
İlke	**Ayar**
Java izinleri	Etkin
Java izinleri	Java'yı devre dışı bırak
İlke	**Ayar**
Karşıdan dosya yüklemesinin otomatik olarak sorulması	Etkin
Karşıdan dosya yüklemesinin otomatik olarak sorulması	Devre Dışı Bırak
İlke	**Ayar**
Kod parçacıklarına izin ver	Etkin
Kod Parçacıkları	Devre Dışı Bırak
İlke	**Ayar**
Korumalı Modu'nu kapat	Etkin
Koruma Modu	Etkinleştir
İlke	**Ayar**
Kullanıcı bilgisi saklama	Etkin
Kullanıcı bilgisi saklama	Devre Dışı Bırak
İlke	**Ayar**
Kullanıcı dosyaları sunucuya yüklerken yerel dizin yolunu ekle	Etkin
Dosyaları bir sunucuya karşıya yüklerken yerel dizin yolunu ekle	Devre Dışı Bırak

EK-2. (devam) Uygulanan sıkılaştırma politikaları

Çizelge 2.1. (devam) MSFT Internet Explorer 11 – bilgisayar (computer)

İlke	**Ayar**
Oturum açma seçenekleri	Etkin
Oturum açma seçenekleri	Kullanıcı adını ve parolayı sor
İlke	**Ayar**
Panodan komut dosyası aracılığıyla kesme, kopyalama ve yapıştırma işlemlerine izin ver	Etkin
Komut dizisi ile yapıştırma işlemine izin ver	Devre Dışı Bırak
İlke	**Ayar**
Pencereler arasında farklı etki alanlarından içerik sürüklemeyi etkinleştir	Etkin
Pencereler arasında farklı etki alanlarından içerik sürüklemeyi etkinleştir	Devre Dışı Bırak
İlke	**Ayar**
Pencerenin içinde farklı etki alanlarından içerik sürüklemeyi etkinleştir	Etkin
Pencerenin içinde farklı etki alanlarından içerik sürüklemeyi etkinleştir	Devre Dışı Bırak
İlke	**Ayar**
Siteler Arası Betik Filtresi'ni aç	Etkin
Siteler Arası Komut Dizisi (XSS) Filtresi'ni aç	Etkinleştir
İlke	**Ayar**
SmartScreen Filtresi taramasını aç	Etkin
SmartScreen Filtresi Kullan	Etkinleştir
İlke	**Ayar**
Uygulamaları ve dosyaları bir IFRAME içinde açma	Etkin
Uygulamaları ve dosyaları bir IFRAME içinde açma	Devre Dışı Bırak
İlke	**Ayar**
Web siteleri, daha az kısıtlanmış Web içerik bölgelerinde yeni pencereler açabilir	Etkin
Web siteleri, daha az kısıtlanmış Web içerik bölgelerinde yeni pencereler açabilir	Devre Dışı Bırak
İlke	**Ayar**
XAML dosyalarını yüklemeye izin ver	Etkin
XAML Dosyaları	Devre Dışı Bırak
İlke	**Ayar**
Yalnızca onaylanmış etki alanlarının TDC ActiveX denetimini kullanmasına izin ver	Etkin
Yalnızca onaylanmış etki alanlarının TDC ActiveX denetimini kullanmasına izin ver	Etkinleştir

EK-2. (devam) Uygulanan sıkılaştırma politikaları

Çizelge 2.1. (devam) MSFT Internet Explorer 11 – bilgisayar (computer)

İlke	**Ayar**
Yalnızca onaylı etki alanlarının sormadan ActiveX denetimleri kullanmasına izin ver	Etkin
Yalnızca onaylı etki alanlarının uyarmadan ActiveX denetimleri kullanmasına izin ver	Etkinleştir
İlke	**Ayar**
ActiveX denetimlerine karşı kötü amaçlı yazılımdan koruma programlarını çalıştırma	Etkin
ActiveX denetimlerine karşı kötü amaçlı yazılımdan koruma programlarını çalıştırma	Devre Dışı Bırak
İlke	**Ayar**
Güvenli olarak işaretlenmemiş ActiveX denetimlerini başlat ve komut dizilerinde kullan	Etkin
Güvenli olarak işaretlenmemiş ActiveX denetimlerini başlat ve komut dizilerinde kullan	Devre Dışı Bırak
İlke	**Ayar**
Java izinleri	Etkin
Java izinleri	Yüksek güvenilirlik
Windows Bileşenleri/Internet Explorer/Internet Denetim Masası /Güvenlik Sayfası/Kilitlenmiş Güvenilen Siteler Bölgesi	
İlke	**Ayar**
Java izinleri	Etkin
Java izinleri	Java'yı devre dışı bırak
Windows Bileşenleri/Internet Explorer/Internet Denetim Masası/Güvenlik Sayfası/Kilitlenmiş Internet Bölgesi	
İlke	**Ayar**
SmartScreen Filtresi taramasını aç	Etkin
SmartScreen Filtresi Kullan	Etkinleştir
Windows Bileşenleri/Internet Explorer/Internet Denetim Masası/Güvenlik Sayfası/Kilitlenmiş İntranet Bölgesi	
İlke	**Ayar**
Java izinleri	Etkin
Java izinleri	Java'yı devre dışı bırak
Windows Bileşenleri/Internet Explorer/Internet Denetim Masası/Güvenlik Sayfası/Kilitlenmiş Yasak Siteler Bölgesi	
İlke	**Ayar**
Java izinleri	Etkin
Java izinleri	Java'yı devre dışı bırak
İlke	**Ayar**
SmartScreen Filtresi taramasını aç	Etkin
SmartScreen Filtresi Kullan	Etkinleştir

EK-2. (devam) Uygulanan sıkılaştırma politikaları

Çizelge 2.1. (devam) MSFT Internet Explorer 11 – bilgisayar (computer)

Windows Bileşenleri/Internet Explorer/Internet Denetim Masası/Güvenlik Sayfası/Kilitli Yerel Makine Bölgesi	
İlke	**Ayar**
Java izinleri	Etkin
Java izinleri	Java'yı devre dışı bırak
Windows Bileşenleri/Internet Explorer/Internet Denetim Masası/Güvenlik Sayfası/Yasak Siteler Bölgesi	
İlke	**Ayar**
.NET Çerçevesi'ne bağlı Authenticode ile imzalanan bileşenleri çalıştır	Etkin
.NET Çerçevesi'ne bağlı Authenticode ile imzalanan bileşenleri çalıştır	Devre Dışı Bırak
İlke	**Ayar**
.NET Çerçevesi'ne bağlı Authenticode ile imzalanmamış bileşenleri çalıştır	Etkin
.NET Çerçevesi'ne bağlı Authenticode ile imzalanmamış bileşenleri çalıştır	Devre Dışı Bırak
İlke	**Ayar**
Active komut dizilerine izin ver	Etkin
Active komut dizilerine izin ver	Devre Dışı Bırak
İlke	**Ayar**
ActiveX denetimlerine karşı kötü amaçlı yazılımdan koruma programlarını çalıştırma	Etkin
ActiveX denetimlerine karşı kötü amaçlı yazılımdan koruma programlarını çalıştırma	Devre Dışı Bırak
İlke	**Ayar**
ActiveX denetimlerini ve eklentilerini çalıştır	Etkin
ActiveX denetimlerini ve eklentilerini çalıştır	Devre Dışı Bırak
İlke	**Ayar**
Açılır Pencere Engelleyicisi Kullan	Etkin
Açılır Pencere Engelleyicisi Kullan	Etkinleştir
İlke	**Ayar**
Betik yoluyla durum çubuğu güncelleştirmelerine izin ver	Etkin
Komut dosyasıyla durum çubuğu güncelleştirmeleri	Devre Dışı Bırak
İlke	**Ayar**
Boyut ve konum kısıtlamaları olmadan komut dosyası ile başlatılan pencerelere izin ver	Etkin
Boyut ve konum kısıtlamaları olmadan komut dosyası ile başlatılan pencerelere izin ver	Devre Dışı Bırak
İlke	**Ayar**
Çalıştırılması güvenli ActiveX denetimlerini komut dizilerinde kullan	Etkin
Çalıştırılması güvenli ActiveX denetimlerini komut dizilerinde kullan	Devre Dışı Bırak

EK-2. (devam) Uygulanan sıkılaştırma politikaları

Çizelge 2.1. (devam) MSFT Internet Explorer 11 – bilgisayar (computer)

İlke	**Ayar**
Dosya yüklemeye izin ver	Etkin
Dosya yüklemeye izin ver	Devre Dışı Bırak
İlke	**Ayar**
Dosyaların sürüklenip bırakılmasına veya kopyalanıp yapıştırılmasına izin ver	Etkin
Dosyaların sürüklenip bırakılmasına veya kopyalanıp yapıştırılmasına izin ver	Devre Dışı Bırak
İlke	**Ayar**
Etki alanları arasında veri kaynaklarına erişim	Etkin
Etki alanları arasında veri kaynaklarına erişim	Devre Dışı Bırak
İlke	**Ayar**
Farklı etki alanlarındaki pencerelerde ve çerçevelerde gezin	Etkin
Farklı etki alanlarındaki pencerelerde ve çerçevelerde gezin	Devre Dışı Bırak
İlke	**Ayar**
Güvenli olarak işaretlenmemiş ActiveX denetimlerini başlat ve komut dizilerinde kullan	Etkin
Güvenli olarak işaretlenmemiş ActiveX denetimlerini başlat ve komut dizilerinde kullan	Devre Dışı Bırak
İlke	**Ayar**
Güvenli olmayabilecek dosyalar için güvenlik uyarısı göster	Etkin
Programlar ve güvenli olmayan dosyaları açma	Devre Dışı Bırak
İlke	**Ayar**
Internet Explorer WebBrowser denetimlerine betikle erişilmesine izin ver	Etkin
Internet Explorer Web tarayıcı denetimi	Devre Dışı Bırak
İlke	**Ayar**
İkili ve komut dosyası davranışlarına izin ver	Etkin
İkili ve Komut Dosyası Davranışlarına İzin Ver	Devre Dışı Bırak
İlke	**Ayar**
İmzalı ActiveX denetimlerini karşıdan yükle	Etkin
İmzalı ActiveX denetimlerini karşıdan yükle	Devre Dışı Bırak
İlke	**Ayar**
İmzasız ActiveX denetimlerini karşıdan yükle	Etkin
İmzasız ActiveX denetimlerini karşıdan yükle	Devre Dışı Bırak
İlke	**Ayar**
Java izinleri	Etkin
Java izinleri	Java'yı devre dışı bırak

EK-2. (devam) Uygulanan sıkılaştırma politikaları

Çizelge 2.1. (devam) MSFT Internet Explorer 11 – bilgisayar (computer)

İlke	**Ayar**
Java programcıklarının çalıştırılması	Etkin
Java programcıklarının çalıştırılması	Devre Dışı Bırak
İlke	**Ayar**
Karşıdan dosya yüklemesinin otomatik olarak sorulması	Etkin
Karşıdan dosya yüklemesinin otomatik olarak sorulması	Devre Dışı Bırak
İlke	**Ayar**
Kod parçacıklarına izin ver	Etkin
Kod Parçacıkları	Devre Dışı Bırak
İlke	**Ayar**
Korumalı Modu'nu kapat	Etkin
Koruma Modu	Etkinleştir
İlke	**Ayar**
Kullanıcı bilgisi saklama	Etkin
Kullanıcı bilgisi saklama	Devre Dışı Bırak
İlke	**Ayar**
Kullanıcı dosyaları sunucuya yüklerken yerel dizin yolunu ekle	Etkin
Dosyaları bir sunucuya karşıya yüklerken yerel dizin yolunu ekle	Devre Dışı Bırak
İlke	**Ayar**
META REFRESH'e izin ver	Etkin
META REFRESH'e izin ver	Devre Dışı Bırak
İlke	**Ayar**
Oturum açma seçenekleri	Etkin
Oturum açma seçenekleri	Adsız oturum açma
İlke	**Ayar**
Panodan komut dosyası aracılığıyla kesme, kopyalama ve yapıştırma işlemlerine izin ver	Etkin
Komut dizisi ile yapıştırma işlemine izin ver	Devre Dışı Bırak
İlke	**Ayar**
Pencereler arasında farklı etki alanlarından içerik sürüklemeyi etkinleştir	Etkin
Pencereler arasında farklı etki alanlarından içerik sürüklemeyi etkinleştir	Devre Dışı Bırak
İlke	**Ayar**
Pencerenin içinde farklı etki alanlarından içerik sürüklemeyi etkinleştir	Etkin
Pencerenin içinde farklı etki alanlarından içerik sürüklemeyi etkinleştir	Devre Dışı Bırak
İlke	**Ayar**
Siteler Arası Betik Filtresi'ni aç	Etkin
Siteler Arası Komut Dizisi (XSS) Filtresi'ni aç	Etkinleştir

EK-2. (devam) Uygulanan sıkılaştırma politikaları

Çizelge 2.1. (devam) MSFT Internet Explorer 11 – bilgisayar (computer)

İlke	**Ayar**
SmartScreen Filtresi taramasını aç	Etkin
SmartScreen Filtresi Kullan	Etkinleştir
İlke	**Ayar**
Uygulamaları ve dosyaları bir IFRAME içinde açma	Etkin
Uygulamaları ve dosyaları bir IFRAME içinde açma	Devre Dışı Bırak
İlke	**Ayar**
Web siteleri, daha az kısıtlanmış Web içerik bölgelerinde yeni pencereler açabilir	Etkin
Web siteleri, daha az kısıtlanmış Web içerik bölgelerinde yeni pencereler açabilir	Devre Dışı Bırak
İlke	**Ayar**
XAML dosyalarını yüklemeye izin ver	Etkin
XAML Dosyaları	Devre Dışı Bırak
İlke	**Ayar**
Yalnızca onaylanmış etki alanlarının TDC ActiveX denetimini kullanmasına izin ver	Etkin
Yalnızca onaylanmış etki alanlarının TDC ActiveX denetimini kullanmasına izin ver	Etkinleştir
İlke	**Ayar**
Yalnızca onaylı etki alanlarının sormadan ActiveX denetimleri kullanmasına izin ver	Etkin
Yalnızca onaylı etki alanlarının uyarmadan ActiveX denetimleri kullanmasına izin ver	Etkinleştir
Windows Bileşenleri/Internet Explorer/Internet Denetim Masası/Güvenlik Sayfası/Yerel Makine Bölgesi	
İlke	**Ayar**
ActiveX denetimlerine karşı kötü amaçlı yazılımdan koruma programlarını çalıştırma	Etkin
ActiveX denetimlerine karşı kötü amaçlı yazılımdan koruma programlarını çalıştırma	Devre Dışı Bırak
İlke	**Ayar**
Java izinleri	Etkin
Java izinleri	Java'yı devre dışı bırak
Ek Kayıt Defteri Ayarları	
Bazı ayarların görünen adları bulunamıyor.	
Ayar	**Durum**
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\140C	3
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\140C	3
Kullanıcı Yapılandırması (Devre Dışı)	
Ayar tanımlanmadı.	

EK-2. (devam) Uygulanan sıkılaştırma politikaları

Çizelge 2.2. MSFT Internet Explorer 11 – kullanıcı (user)

Bilgisayar Yapılandırması (Devre Dışı)	
Ayar tanımlanmadı.	
Kullanıcı Yapılandırması (Etkin)	
İlkeler	
Yönetim Şablonları	
İlke tanımları (ADMX dosyaları) yerel bilgisayardan alındı.	
Windows Bileşenleri/Internet Explorer	
İlke	**Ayar**
Formlarda kullanıcı adlarını ve parolaların otomatik tamamlanmasını aç	Devre Dışı

Çizelge 2.3. MSFT Windows 10 – kimlik denetimi (credential guard)

Bilgisayar Yapılandırması (Etkin)	
İlkeler	
Yönetim Şablonları	
İlke tanımları (ADMX dosyaları) yerel bilgisayardan alındı.	
Sistem/Cihaz Koruyucu	
İlke	**Ayar**
Sanallaştırma Tabanlı Güvenlik'i aç	Etkin
Platform Güvenlik Düzeyi seç:	Güvenli Önyükleme ve DMA Koruması
Kod Bütünlüğü için Sanallaştırma Tabanlı Koruma:	UEFI kilidi ile etkin
Credential Guard Yapılandırması:	UEFI kilidi ile etkin
Kullanıcı Yapılandırması (Devre Dışı)	
Ayar tanımlanmadı.	

Çizelge 2.4. MSFT Windows 10 RS4 – kullanıcı (user)

Bilgisayar Yapılandırması (Devre Dışı)	
Ayar tanımlanmadı.	
Kullanıcı Yapılandırması (Etkin)	
İlkeler	
Yönetim Şablonları	
İlke tanımları (ADMX dosyaları) yerel bilgisayardan alındı.	
Başlat Menüsü ve Görev Çubuğu/Bildirimler	
İlke	**Ayar**
Kilit ekranında bildirimleri kapat	Etkin
Windows Bileşenleri/Bulut İçeriği	
İlke	**Ayar**
Windows spot ışığında üçüncü taraf içeriği önermeyin	Etkin

EK-2. (devam) Uygulanan sıkılaştırma politikaları

Çizelge 2.5. MSFT Windows 10 - Defender Antivirus

Bilgisayar Yapılandırması (Etkin)	
İlkeler	
Yönetim Şablonları	
İlke tanımları (ADMX dosyaları) yerel bilgisayardan alındı.	
Windows Bileşenleri/Endpoint Protection/Gerçek Zamanlı Koruma	
İlke	**Ayar**
Davranış izlemeyi aç	Etkin
Windows Bileşenleri/Endpoint Protection/MAPS	
İlke	**Ayar**
Daha fazla analiz gerektiğinde dosya örnekleri gönder	Etkin
Daha fazla analiz gerektiğinde dosya örnekleri gönder	
İlke	**Ayar**
Microsoft MAPS'a katıl	Etkin
Microsoft MAPS'a katıl	Gelişmiş MAPS
Windows Bileşenleri/Endpoint Protection/Tarama	
İlke	**Ayar**
Çıkarılabilir sürücüleri tara	Etkin
E-posta taramasını aç	Etkin
Ek Kayıt Defteri Ayarları	
Ayar	**Durum**
Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\ExploitGuard_ASR_Rules	1
Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules\3b576869-a4ec-4529-8536-b80a7769e899	1
Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules\5beb7efe-fd9a-4556-801d-275e5ffc04cc	1
Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules\75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84	1
Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules\92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B	1
Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules\9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2	1
Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules\b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4	1
Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules\be9ba2d9-53ea-4cdc-84e5-9b1eeee46550	1
Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules\d3e037e1-3eb8-44c8-a917-57927947596d	1
Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules\d4f940ab-401b-4efc-aadc-ad5f3c50688a	1
Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\Network Protection\EnableNetworkProtection	1
Kullanıcı Yapılandırması (Devre Dışı)	
Ayar tanımlanmadı.	

EK-2. (devam) Uygulanan sıkılaştırma politikaları

Çizelge 2.6. MSFT Windows 10 RS4 – BitLocker

Bilgisayar Yapılandırması (Etkin)	
İlkeler	
Yönetim Şablonları	
İlke tanımları (ADMX dosyaları) yerel bilgisayardan alındı.	
Sistem/Aygıt Yükleme/Aygıt Yükleme Kısıtlamaları	
İlke	**Ayar**
Bu aygıt kimliklerinden herhangi biriyle eşleşen aygıtların yüklenmesini engelle	Etkin
Bu Aygıt Kimliklerinden herhangi biriyle eşleşen aygıtların yüklenmesini engelle:	Etkin
PCI\CC_0C0A	Etkin
Ayrıca zaten yüklü olan eşleşen aygıtlara da uygulayın.	Etkin
İlke	**Ayar**
Bu aygıt kurulum sınıflarıyla eşleşen sürücüleri kullanan aygıtların yüklenmesini engelle	Etkin
Sistem/Güç Yönetimi/Uyku Ayarları	
İlke	**Ayar**
Uyku modundayken bekleme durumlarına (S1-S3) izin ver (pil devredeyken)	Devre Dışı
Uyku modundayken bekleme durumlarına (S1-S3) izin ver (prize takılıyken)	Devre Dışı
Windows Bileşenleri/BitLocker Drive Encryption	
İlke	**Ayar**
Sürücü şifreleme yöntemini ve şifreleme gücünü seçin (Windows 10 [Sürüm 1511] ve sonraki sürümler)	Etkin
İşletim sistemi sürücüleri için şifreleme yöntemini seçin:	XTS-AES 256-bit
Sabit veri sürücüleri için şifreleme yöntemini seçin:	XTS-AES 256-bit
Çıkarılabilir veri sürücüleri için şifreleme yöntemini seçin:	AES-CBC 256-bit
Windows Bileşenleri/BitLocker Drive Encryption/Çıkarılabilir Veri Sürücüleri	
İlke	**Ayar**
BitLocker ile korunmayan çıkarılabilir sürücülere yazma erişimi verme	Etkin
Başka bir kuruluşta yapılandırılmış aygıtlara yazma izni verme	Devre Dışı
Windows Bileşenleri/BitLocker Drive Encryption/İşletim Sistemi Sürücüleri	
İlke	**Ayar**
Başlangıç için gelişkin PIN'lere izin ver	Etkin
Bütünlük doğrulaması için Güvenli Önyükleme'ye izin ver	Etkin
En kısa PIN uzunluğunu başlangıç için yapılandır	Etkin
En az karakter sayısı:	7
Ek Kayıt Defteri Ayarları	
Ayar	**Durum**
SOFTWARE\Policies\Microsoft\FVE\DisableExternalDMAUnderLock	1
Kullanıcı Yapılandırması (Devre Dışı)	
Ayar tanımlanmadı.	

EK-2. (devam) Uygulanan sıkılaştırma politikaları

Çizelge 2.7. MSFT Windows 10 - etki alanı güvenliği (domain security)

Bilgisayar Yapılandırması (Etkin)	
İlkeler	
Windows Ayarları	
Güvenlik Ayarları	
Hesap İlkeleri/Parola İlkesi	
İlke	**Ayar**
En az parola uzunluğu	14 karakter
En kısa parola uzunluğu	1 gün
Parola geçerlilik süresi üst sınırı	60 gün
Parola geçmişini zorla	24 parola anımsanır
Parolalar karmaşıklık gereksinimlerine uymalıdır	Etkin
Parolaları, ters çevrilebilir şifreleme kullanarak depola	Devre Dışı
Hesap İlkeleri/Hesap Kilitleme İlkesi	
İlke	**Ayar**
Hesap kilitleme eşik değeri	10 geçersiz oturum açma denemesi
Hesap kilitleme süresi	15 dakika
Şu süreden sonra Hesap kilitleme sayacını sıfırla	15 dakika
Kullanıcı Yapılandırması (Devre Dışı)	
Ayar tanımlanmadı.	

EK-2. (devam) Uygulanan sıkılaştırma politikaları

Çizelge 2.8. MSFT Windows 10 RS4 – bilgisayar (computer)

Bilgisayar Yapılandırması (Etkin)	
İlkeler	
Windows Ayarları	
Güvenlik Ayarları	
Yerel İlkeler/Kullanıcı Hakları Ataması	
İlke	**Ayar**
Aygıt sürücüleri yükle ve kaldır	BUILTIN\Administrators
Belirteç nesnesi oluştur	
Birim bakım görevleri gerçekleştir	BUILTIN\Administrators
Bu bilgisayara ağ üzerinden eriş	BUILTIN\Administrators, BUILTIN\Remote Desktop Users
Bu bilgisayara ağ üzerinden erişime izin verme	BUILTIN\Guests, NT AUTHORITY\Yerel hesap
Denetimi ve güvenlik günlüğünü yönet	BUILTIN\Administrators
Disk belleği dosyası oluştur	BUILTIN\Administrators
Dosya ve dizinleri geri yükle	BUILTIN\Administrators
Dosya ve dizinleri yedekle	BUILTIN\Administrators
Dosyaların veya diğer nesnelerin sahipliğini al	BUILTIN\Administrators
Genel nesneler oluştur	BUILTIN\Administrators, NT AUTHORITY\SERVICE, NT AUTHORITY\Local Service, NT AUTHORITY\NETWORK SERVICE
Kimlik doğrulamasından sonra istemcinin özelliklerini al	BUILTIN\Administrators, NT AUTHORITY\SERVICE, NT AUTHORITY\Local Service, NT AUTHORITY\NETWORK SERVICE
Programların hatalarını ayıkla	BUILTIN\Administrators
Sayfaları bellekte kilitle	
Simgesel bağlantılar oluştur	BUILTIN\Administrators
Tek işlem profili oluştur	BUILTIN\Administrators
Terminal Hizmetleri üzerinden oturum açmayı reddet	BUILTIN\Guests, NT AUTHORITY\Yerel hesap
Uzak sistemden kapatmayı zorla	BUILTIN\Administrators
Üretici yazılımı ortam değerlerini değiştir	BUILTIN\Administrators
Yerel olarak oturum açmayı kabul et	BUILTIN\Administrators, BUILTIN\Users
Yerel olarak oturum açmayı reddet	BUILTIN\Guests
Zamanlama önceliğini artır	BUILTIN\Administrators
Yerel İlkeler/Güvenlik Seçenekleri	
Ağ Erişimi	
İlke	**Ayar**
Ağ erişimi: Adlandırılmış Kanallar ve Paylaşım'lara anonim erişimi kısıtla	Etkin
Ağ erişimi: Anonim SID/Ad çevirisine izin ver	Devre Dışı

EK-2. (devam) Uygulanan sıkılaştırma politikaları

Çizelge 2.8. (devam) MSFT Windows 10 RS4 – bilgisayar (computer)

Ağ erişimi: SAM hesaplarının anonim numaralandırmasına izin verme	Etkin
Ağ erişimi: SAM hesaplarının ve paylaşımlarının anonim numaralandırmasına izin verme	Etkin
Ağ Güvenliği	
İlke	**Ayar**
Ağ güvenliği: LAN Manager kimlik doğrulama düzeyi	Yalnızca NTLMv2 yanıtı gönder. LM ve NTLM'yi reddet
Ağ güvenliği: LDAP istemcisi imza gereksinimleri	İmzalama için anlaş
Ağ güvenliği: NTLM SSP tabanlı (güvenli RPC dahil) istemciler için en düşük oturum güvenliği	Etkin
NTLMv2 oturum güvenliği gerektir	Etkin
128 bit şifreleme gerektir	Etkin
Ağ güvenliği: NTLM SSP tabanlı (güvenli RPC dahil) sunucular için en düşük oturum güvenliği	Etkin
NTLMv2 oturum güvenliği gerektir	Etkin
128 bit şifreleme gerektir	Etkin
Ağ güvenliği: Sonraki parola değişiminde LAN Manager karma değerini depolama	Etkin
Etkileşimli Oturum Açma	
İlke	**Ayar**
Etkileşimli oturum açma: Akıllı kart çıkarma davranışı	İş İstasyonunu Kilitle
Hesaplar	
İlke	**Ayar**
Hesaplar: Konuk hesabı durumu	Devre Dışı
Hesaplar: Yerel hesabın boş parola kullanmasını yalnızca konsol oturumuyla sınırla	Etkin
Hesaplar: Yönetici hesap durumu	Devre Dışı
Kullanıcı Hesabı Denetimi	
İlke	**Ayar**
Kullanıcı Hesabı Denetimi: Dosya ve kayıt defteri yazma hatalarını kullanıcı konumlarında sanallaştır	Etkin
Kullanıcı Hesabı Denetimi: Standart kullanıcılar için yükseltme isteminin davranışı	Yükseltme isteklerini otomatik olarak reddet
Kullanıcı Hesabı Denetimi: Tüm yöneticileri Yönetici Onay Modu'nda çalıştır	Etkin
Kullanıcı Hesabı Denetimi: Uygulama yüklemelerini algıla ve yükseltme isteminde bulun	Etkin
Kullanıcı Hesabı Denetimi: Yalnızca güvenilir konumlara yüklenmiş UIAccess uygulamalarını yükselt	Etkin
Kullanıcı Hesabı Denetimi: Yerleşik Yönetici hesabı için Yönetici Onay Modu	Etkin
Kullanıcı Hesabı Denetimi: Yönetici Onay Modu'ndaki yöneticiler için yükseltme isteminin davranışı	Güvenli masaüstünde izin isteminde bulun

EK-2. (devam) Uygulanan sıkılaştırma politikaları

Çizelge 2.8. (devam) MSFT Windows 10 RS4 – bilgisayar (computer)

Microsoft Ağ İstemcisi	
İlke	**Ayar**
Microsoft ağ istemcisi: İletişimleri dijital olarak imzala (her zaman)	Etkin
Microsoft ağ istemcisi: Üçüncü taraf SMB sunucularına şifrelenmemiş parola gönder	Devre Dışı
Sistem Nesneleri	
İlke	**Ayar**
Sistem nesneleri: İç sistem nesnelerinin (Simgesel Bağlantılar gibi) varsayılan izinlerini güçlendir	Etkin
Diğer	
İlke	**Ayar**
Ağ erişimi: SAM için uzaktan arama yapmalarına izin verilen istemcileri kısıtla	"O:BAG:BAD:(A;;RC;;;BA)"
Ağ güvenliği: Çevrimiçi kimlikleri kullanmak için bu bilgisayarda PKU2U kimlik doğrulama isteklerine izin ver.	Devre Dışı
Ağ güvenliği: LocalSystem NULL oturum geri dönüşüne izin ver	Devre Dışı
Denetim: Denetim ilkesi kategori ayarlarını geçersiz kılmak için denetim ilkesi alt kategori ayarlarını zorla (Windows Vista veya daha sonraki sürümü)	Etkin
Etki alanı üyesi: En uzun hesap parolası yaşı	30 gün
Etki alanı üyesi: Güçlü (Windows 2000 veya daha sonraki) oturum anahtarı gerektir	Etkin
Etki alanı üyesi: Güvenli kanal verisini dijital olarak imzala (uygun olduğunda)	Etkin
Etki alanı üyesi: Güvenli kanal verisini dijital olarak şifrele (uygun olduğunda)	Etkin
Etki alanı üyesi: Güvenli kanal verisini dijital olarak şifrele veya imzala (her zaman)	Etkin
Etki alanı üyesi: Makine hesabı parola değişikliklerini devreden çıkar	Devre Dışı
Etkileşimli oturum açma: Makinede etkinlik yapılmama süresi sınırı	900 saniye
Microsoft ağ sunucusu: İletişimleri dijital olarak imzala (her zaman)	Etkin
Sistem Hizmetleri	
xbgm (Başlangıç Modu: Devre Dışı)	
Xbox Live Kimlik Doğrulama Yöneticisi (Başlangıç Modu: Devre Dışı)	
Xbox Live Oyun Kaydetme (Başlangıç Modu: Devre Dışı)	
XboxGipSvc (Başlangıç Modu: Devre Dışı)	
XboxNetApiSvc (Başlangıç Modu: Devre Dışı)	

EK-2. (devam) Uygulanan sıkılaştırma politikaları

Çizelge 2.8. (devam) MSFT Windows 10 RS4 – bilgisayar (computer)

Gelişmiş Güvenliğe Sahip Windows Güvenlik Duvarı	
Etki Alanı Profili Ayarları	
İlke	**Ayar**
Güvenlik duvarı durumu	Açık
Gelen bağlantılar	Engelle
Giden bağlantılar	İzin Ver
Yerel güvenlik duvarı kuralları uygula	Yapılandırılmadı
Yerel bağlantı güvenliği kuralları uygula	Yapılandırılmadı
Bildirimleri görüntüle	Hayır
Tek noktaya yayın yanıtlarına izin ver	Yapılandırılmadı
Bırakılan paketleri günlüğe kaydet	Evet
Başarılı bağlantıları günlüğe kaydet	Evet
Günlük dosyası yolu	Yapılandırılmadı
Günlük dosyası en büyük boyutu (KB)	16384
Özel Profil Ayarları	
İlke	**Ayar**
Güvenlik duvarı durumu	Açık
Gelen bağlantılar	Engelle
Giden bağlantılar	İzin Ver
Yerel güvenlik duvarı kuralları uygula	Yapılandırılmadı
Yerel bağlantı güvenliği kuralları uygula	Yapılandırılmadı
Bildirimleri görüntüle	Hayır
Tek noktaya yayın yanıtlarına izin ver	Yapılandırılmadı
Bırakılan paketleri günlüğe kaydet	Evet
Başarılı bağlantıları günlüğe kaydet	Evet
Günlük dosyası yolu	Yapılandırılmadı
Günlük dosyası en büyük boyutu (KB)	16384
Ortak Profil Ayarları	
İlke	**Ayar**
Güvenlik duvarı durumu	Açık
Gelen bağlantılar	Engelle
Giden bağlantılar	İzin Ver
Yerel güvenlik duvarı kuralları uygula	Hayır
Yerel bağlantı güvenliği kuralları uygula	Hayır
Bildirimleri görüntüle	Hayır
Tek noktaya yayın yanıtlarına izin ver	Yapılandırılmadı
Bırakılan paketleri günlüğe kaydet	Evet
Başarılı bağlantıları günlüğe kaydet	Evet
Günlük dosyası yolu	Yapılandırılmadı
Günlük dosyası en büyük boyutu (KB)	16384

EK-2. (devam) Uygulanan sıkılaştırma politikaları

Çizelge 2.8. (devam) MSFT Windows 10 RS4 – bilgisayar (computer)

Hesap Oturumu Açma	
İlke	**Ayar**
Kimlik Bilgisi Doğrulamayı Denetle	Başarı, Hata
Hesap Yönetimi	
İlke	**Ayar**
Güvenlik Grubu Yönetimini Denetle	Başarı
Kullanıcı Hesabı Yönetimini Denetle	Başarı, Hata
Ayrıntılı İzleme	
İlke	**Ayar**
PNP Etkinliği Denetleme	Başarı
İşlem Oluşturmayı Denetle	Başarı
Oturum Açma/Kapatma	
İlke	**Ayar**
Hesap Kilitlemeyi Denetle	Hata
Denetim Grubu Üyeliği	Başarı
Oturum Açı Denetle	Başarı, Hata
Diğer Oturum Açma/Kapatma Olaylarını Denetle	Başarı, Hata
Özel Oturum Açmayı Denetle	Başarı
Nesne Erişimi	
İlke	**Ayar**
Ayrıntılı Dosya Paylaşımını Denetle	Hata
Dosya Paylaşımını Denetle	Başarı, Hata
Diğer Nesne Erişim Olaylarını Denetle	Başarı, Hata
Çıkarılabilir Depolama Birimini Denetle	Başarı, Hata
İlke Değişimi	
İlke	**Ayar**
İlke Değişimini Denetle	Başarı
Kimlik Doğrulama İlkesi Değişikliğini Denetle	Başarı
MPSSVC Kural Düzeyi İlke Değişikliğini Denetle	Başarı, Hata
Diğer İlke Değişikliği Olaylarını Denetle	Hata
Ayrıcalık Kullanımı	
İlke	**Ayar**
Hassas Ayrıcalık Kullanımını Denetle	Başarı, Hata

EK-2. (devam) Uygulanan sıkılaştırma politikaları

Çizelge 2.8. (devam) MSFT Windows 10 RS4 – bilgisayar (computer)

Sistem	
İlke	**Ayar**
Diğer Sistem Olaylarını Denetle	Başarı, Hata
Güvenlik Durumu Değişikliğini Denetle	Başarı
Güvenlik Sistemi Uzantısını Denetle	Başarı
Sistem Bütünlüğünü Denetle	Başarı, Hata
Yönetim Şablonları	
İlke tanımları (ADMX dosyaları) yerel bilgisayardan alındı.	
Ağ/Ağ Bağlantıları	
İlke	**Ayar**
DNS etki alanı ağında Internet Bağlantısı Paylaşımı'nın kullanılmasını engelle	Etkin
Ağ/Ağ Bağlantıları/Windows Güvenlik Duvarı/Etki Alanı Profili	
İlke	**Ayar**
Windows Güvenlik Duvarı: Bildirimleri yasakla	Etkin
Windows Güvenlik Duvarı: Günlük tutmaya izin ver	Etkin
Bırakılan paketleri günlüğe kaydet	Etkin
Başarılı bağlantıları günlüğe kaydet	Etkin
Günlük dosyası yolu ve adı:	
Boyut sınırı (KB):	16384
İlke	**Ayar**
Windows Güvenlik Duvarı: Tüm ağ bağlantılarını koru	Etkin
Ağ/Ağ Sağlayıcısı	
İlke	**Ayar**
Sağlamlaştırılmış UNC Yolları	Etkin
*\SYSVOL	RequireMutualAuthentication=1,RequireIntegrity=1
*\NETLOGON	RequireMutualAuthentication=1,RequireIntegrity=1
Ağ/Lanman İş İstasyonu	
İlke	**Ayar**
Güvenli olmayan konuk oturum açma işlemlerini etkinleştir	Devre Dışı
Ağ/Windows Bağlantı Yöneticisi	
İlke	**Ayar**
Etki alanı kimlik doğrulamalı ağa bağlandığında etki alansız bağlantıyı yasaklayın	Etkin
Ağ/WLAN Hizmeti/WLAN Ayarları	
İlke	**Ayar**
Windows'un, önerilen açık etkin noktalara, kişiler tarafından paylaşılan ağlara ve ücretli hizmetler sunan etkin noktalara otomatik olarak bağlanmasına izin ver	Devre Dışı

EK-2. (devam) Uygulanan sıkılaştırma politikaları

Çizelge 2.8. (devam) MSFT Windows 10 RS4 – bilgisayar (computer)

Denetim Masası/Kişiselleştirme	
İlke	**Ayar**
Kilit ekranı kamerasının etkinleştirilmesini engelle	Etkin
Kilit ekranı slayt gösterisinin etkinleştirilmesini engelle	Etkin
İlke	**Ayar**
Önyükleme Başlatma Sürücüsü Başlatma İlkesi	Etkin
Başlatılabilecek önyükleme başlatma sürücülerini seçin:	İyi, bilinmeyen ve kötü ancak kritik
Sistem/Grup İlkesi	
İlke	**Ayar**
Kayıt defteri ilkesi işlemini yapılandır	Etkin
Dönemsel arka plan işleme sırasında uygulama	Devre Dışı
Grup İlkesi nesneleri değişmemişse bile işle	Etkin
Sistem/Güç Yönetimi/Uyku Ayarları	
İlke	**Ayar**
Bilgisayar uyandığında parola iste (pil devredeyken)	Etkin
Bilgisayar uyandığında parola iste (prize takılıyken)	Etkin
Sistem/İnternet İletişim Yönetimi/İnternet İletişimi ayarları	
İlke	**Ayar**
HTTP üzerinde yazdırmayı kapat	Etkin
HTTP üzerinde yazıcı sürücülerini karşıdan yüklemeyi kapat	Etkin
Web Yayımı ve çevrimiçi sipariş sihirbazları için Internet'ten yüklemeyi kapat	Etkin
Sistem/Oturum Açma	
İlke	**Ayar**
Etki alanına katılan bilgisayarlarda yerel kullanıcıları numaralandır	Devre Dışı
PIN ile kolay oturum açmayı etkinleştir	Devre Dışı
Sistem/Uzaktan Yardım	
İlke	**Ayar**
İstenen Uzaktan Yardımı Yapılandır	Devre Dışı
Sistem/Uzaktan Yordam Çağrısı	
İlke	**Ayar**
Kimliği Doğrulanmamış RPC istemcilerini kısıtla	Etkin
Uygulanacak RPC Çalıştırma Zamanı Kimliği Doğrulanmamış İstemci Kısıtlaması:	Kimliği Doğrulanan

EK-2. (devam) Uygulanan sıkılaştırma politikaları

Çizelge 2.8. (devam) MSFT Windows 10 RS4 – bilgisayar (computer)

Windows Bileşenleri/Ara	
İlke	**Ayar**
Şifrelenmiş dosyaların dizinini oluşturmaya izin ver	Devre Dışı
Windows Bileşenleri/Biyometri/Yüz Özellikleri	
İlke	**Ayar**
Kullanılabilir olduğunda gelişmiş kimlik sahtekârlığına karşı korumayı kullan	Etkin
Windows Bileşenleri/Bulut İçeriği	
İlke	**Ayar**
Microsoft tüketici deneyimlerini devre dışı bırak	Etkin
Windows Bileşenleri/Dosya Gezgini	
İlke	**Ayar**
Bozulma durumunda yığın sonlandırmayı kapat	Devre Dışı
Internet Explorer için Veri Yürütme Engellemesini kapat	Devre Dışı
Windows SmartScreen'ı Yapılandır	Etkin
Windows Bileşenleri/Kimlik Bilgileri Kullanıcı Arabirimi	
İlke	**Ayar**
Yükseltme işleminde yönetici hesaplarını numaralandır	Devre Dışı
Windows Bileşenleri/Olay Günlüğü Hizmeti/Güvenlik	
İlke	**Ayar**
Günlük dosyası boyut üst sınırını belirt (KB)	Etkin
En Fazla Günlük Boyutu (KB)	196608
Windows Bileşenleri/Olay Günlüğü Hizmeti/Sistem	
İlke	**Ayar**
Günlük dosyası boyut üst sınırını belirt (KB)	Etkin
En Fazla Günlük Boyutu (KB)	32768
Windows Bileşenleri/Olay Günlüğü Hizmeti/Uygulama	
İlke	**Ayar**
Günlük dosyası boyut üst sınırını belirt (KB)	Etkin
En Fazla Günlük Boyutu (KB)	32768
Windows Bileşenleri/Otomatik Kullan İlkeleri	
İlke	**Ayar**
Birim olmayan aygıtlar için Otomatik Kullan'a izin verme	Etkin
Otomatik Çalıştırma için varsayılan davranışı ayarlar.	Etkin
Varsayılan Otomatik Çalıştırma Davranışı	Otomatik çalıştırma komutlarını yürütme
İlke	**Ayar**
Otomatik Kullan özelliğini kapat	Etkin
Otomatik Çalıştır'ı kapat:	Tüm sürücüler
Windows Bileşenleri/RSS Özet Akışları	
İlke	**Ayar**
Eklerin indirilmesini engelle	Etkin

EK-2. (devam) Uygulanan sıkılaştırma politikaları

Çizelge 2.8. (devam) MSFT Windows 10 RS4 – bilgisayar (computer)

Windows Bileşenleri/Uygulama çalışma zamanı	
İlke	**Ayar**
Microsoft hesaplarının isteğe bağlı olmasına izin ver	Etkin
Windows Bileşenleri/Uzak Masaüstü Hizmetleri/Uzak Masaüstü Bağlantısı İstemcisi	
İlke	**Ayar**
Parolaların kaydedilmesine izin verme	Etkin
Windows Bileşenleri/Uzak Masaüstü Hizmetleri/Uzak Masaüstü Oturumu Ana Bilgisayarı/Cihaz ve Kaynak Yeniden Yönlendirmesi	
İlke	**Ayar**
Sürücü yeniden yönlendirmesine izin verme	Etkin
Windows Bileşenleri/Uzak Masaüstü Hizmetleri/Uzak Masaüstü Oturumu Ana Bilgisayarı/Güvenlik	
İlke	**Ayar**
Bağlantı sağlandığında her zaman parola sor	Etkin
Güvenli RPC iletişimi iste	Etkin
İstemci bağlantısı güvenlik düzeyini ayarla	Etkin
Şifreleme Düzeyi	Yüksek Düzey
Windows Bileşenleri/Windows Ink Çalışma Alanı	
İlke	**Ayar**
Windows Ink Çalışma Alanı'na İzin Ver	Etkin
Aşağıdaki eylemlerden birini seç	
Windows Bileşenleri/Windows Installer	
İlke	**Ayar**
Her zaman yükseltilmiş ayrıcalıklarla yükle	Devre Dışı
Yüklemeler üzerinde kullanıcı denetimine izin ver	Devre Dışı
Windows Bileşenleri/Windows Oturum Açma Seçenekleri	
İlke	**Ayar**
Sistem tarafından gerçekleştirilen bir yeniden başlatma işleminden sonra otomatik olarak en son etkileşimde bulunan kullanıcının oturumunu aç	Devre Dışı
Windows Bileşenleri/Windows PowerShell	
İlke	**Ayar**
Turn on PowerShell Script Block Logging	Etkin
Log script block invocation start / stop events:	Devre Dışı
Windows Bileşenleri/Windows Uzaktan Yönetim (WinRM)/WinRM Hizmeti	
İlke	**Ayar**
Şifresiz trafiğe izin ver	Devre Dışı
Temel kimlik doğrulamasına izin ver	Devre Dışı
WinRM'nin RunAs kimlik bilgilerini depolamasına izin verme	Etkin

EK-2. (devam) Uygulanan sıkılaştırma politikaları

Çizelge 2.8. (devam) MSFT Windows 10 RS4 – bilgisayar (computer)

İlke	**Ayar**
Özet Kimlik Doğrulamasına izin verme	Etkin
Şifresiz trafiğe izin ver	Devre Dışı
Temel kimlik doğrulamasına izin ver	Devre Dışı
Ek Kayıt Defteri Ayarları	
Ayar	**Durum**
Software\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy	0
Software\Policies\Microsoft Services\AdmPwd\AdmPwdEnabled	1
Software\Policies\Microsoft\MicrosoftEdge\Main\FormSuggest Passwords	no
Software\Policies\Microsoft\MicrosoftEdge\PhishingFilter\EnabledV9	1
Software\Policies\Microsoft\MicrosoftEdge\PhishingFilter\PreventOverride	1
Software\Policies\Microsoft\MicrosoftEdge\PhishingFilter\PreventOverrideAppRepUnknown	1
Software\Policies\Microsoft\Windows Defender Security Center\App and Browser protection\DisallowExploitProtectionOverride	1
Software\Policies\Microsoft\Windows Defender\MpEngine\MpEnablePus	1
Software\Policies\Microsoft\Windows\CredentialsDelegation\AllowProtectedCreds	1
Software\Policies\Microsoft\Windows\GameDVR\AllowGameDVR	0
Software\Policies\Microsoft\Windows\System\ShellSmartScreenLevel	Block
SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential	0
SYSTEM\CurrentControlSet\Control\Session Manager\kernel\DisableExceptionChainValidation	0
SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\SMB1	0
SYSTEM\CurrentControlSet\Services\MrxSmb10\Start	4
SYSTEM\CurrentControlSet\Services\Netbt\Parameters\NoNameReleaseOnDemand	1
SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting	2
SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect	0
SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\DisableIPSourceRouting	2
Kullanıcı Yapılandırması (Devre Dışı)	
Ayar tanımlanmadı.	

EK-3. Dönüşüm kodu

```
[CmdletBinding(DefaultParameterSetName = "GpoMode")]
Param(
 [Parameter(
4                ParameterSetName = "GpoMode",
5                Mandatory=$true)]
6                [string]$GpoTarget,    # Name of GPO
7        [Parameter(
8                Mandatory=$true)]
9                [string]$DomainTarget,    # Domain name
10       [Parameter(
11               Mandatory=$true)]
12               [string]$SiteCode,    # ConfigMgr site code
13       [Parameter(
14               Mandatory=$false)]
15               [switch]$ExportOnly,     # Switch to disable the creation of CIs and only
export to a CAB file
16       [Parameter(
17               Mandatory=$false)]
18               [switch]$Remediate,    # Set remediate non-compliant settings
19       [Parameter(
20        Mandatory=$false)]
21        [ValidateSet('None', 'Informational', 'Warning', 'Critical')]
22               [string]$Severity='Informational',    # Rule severity
23       [Parameter(
24        ParameterSetName = "RsopMode",
25               Mandatory=$false)]
26               [switch]$ResultantSetOfPolicy,     # Uses Resultant Set of Policy instead of
specific GPO for values
27       [Parameter(
28               ParameterSetName = "GpoMode",
29               Mandatory = $false)]
30               [switch]$GroupPolicy,    #  Uses a single GPO for values
31       [Parameter(
32        ParameterSetName = "RsopMode",
33               Mandatory=$true)]
34               [string]$ComputerName,    # Computer name to be used for RSOP
35       [Parameter(
36        ParameterSetName = "RsopMode",
37               Mandatory=$false)]
38               [switch]$LocalPolicy,     # Switch to enable capturing local group policy
when using RSOP mode
39       [Parameter(
40               Mandatory=$false)]
41               [switch]$Log    # Switch to enable logging all registry keys and their GPOs
to a file
42 )
43
```

EK-3. (devam) Dönüşüm kodu

```
# Constants
$MAX_NAME_LENGTH= 255

$scriptPath = Split-Path -Parent $MyInvocation.MyCommand.Definition
$scriptDir = Split-Path -Parent $scriptPath
$startingDrive = (Get-Location).Drive.Name + ":"
$Global:ouPath = $null

if (($GroupPolicy -eq $false) -and ($ResultantSetOfPolicy -eq $false))
{
    $GroupPolicy = $true
}

<#
    Utilizes native GroupPolicy module to query for registry keys assocaited with a given Group Policy
#>
function Get-GPOKeys
{
  param(
    [string]$PolicyName,    # Name of group policy
    [string]$Domain    # Domain name
  )

    If ((Get-Module).Name -contains 'GroupPolicy')
    {
        Write-Verbose "GroupPolicy module already imported."
    }
    Else
    {
        Try
        {
            Import-Module GroupPolicy        # Imports native GroupPolicy PowerShell module
        }
        Catch [Exception]
        {
            Write-Host "Error trying to import GroupPolicy module." -ForegroundColor Red
            Write-Host "Script will exit." -ForegroundColor Red
            pause
            Exit
        }
    }
```

EK-3. (devam) Dönüşüm kodu

```
86    Write-Host "Querying for registry keys associated with $PolicyName..."
87
88          $gpoKeys  =  @("HKLM\Software",  "HKLM\System",  "HKCU\Software",
"HKCU\System")   # Sets registry hives to extract from Group Policy
89    $values = @()
90    $keyList = @()
91    $newKeyList = @()
92    $keyCount = 0
93    $prevCount = 0
94    $countUp = $true
95
96      # While key count does not increment up
97    while ($countUp)
98    {
99          $prevCount = $keyCount
100          $newKeyList = @()
101          foreach ($gpoKey in $gpoKeys)
102          {
103             try
104             {
105                    $newKeys = (Get-GPRegistryValue -Name $PolicyName -Domain
$Domain -Key $gpoKey -ErrorAction Stop).FullKeyPath    # Gets registry keys
106             } catch [Exception]
107             {
108                                  If  ($_.Exception.Message  -notlike  "*The  following
Group Policy registry setting was not found:*")
109                                  {
110                                        Write-Host       $_.Exception.Message       -
ForegroundColor Red
111                                        Break
112                                  }
113             }
114                              # For each key in list of registry keys
115             foreach ($nKey in $newKeys)
116             {
117                                  # If key is not already in list
118                if ($keyList -notcontains $nKey)
119                {
120                   #Write-Verbose $nKey
121                   $keyList += $nKey
122                   $keyCount++
123                }
124                if ($newKeyList -notcontains $nKey)
125                {
126                   $newKeyList += $nKey
```

EK-3. (devam) Dönüşüm kodu

```
127                 }
128             }
129         }
130         [array]$gpoKeys = $newKeyList
131                     # If previous key count equals current key count.  (No new keys found; end of list)
132         if ($prevCount -eq $keyCount)
133         {
134             $countUp = $false
135         }
136     }
137
138     If ($newKeys -ne $null)
139     {
140             foreach ($key in $keyList)
141             {
142                     $values += Get-GPRegistryValue -Name $PolicyName -Domain $Domain -Key $key -ErrorAction SilentlyContinue | select FullKeyPath, ValueName, Value, Type | Where-Object {($_.Value -ne $null) -and ($_.Value.Length -gt 0)}
143             }
144             if ($Log)
145             {
146                     foreach ($value in $values)
147                     {
148                             Write-Log -RegistryKey $value -GPOName $PolicyName
149                     }
150             }
151     }
152

153     $valueCount = $values.Count
154

155     Write-Host "`t$keyCount keys found."
156     Write-Host "`t$valueCount values found."
157

158     $values
159 }
160

161 <#
162     Utilizes the ConfigurationManager PowerShell module to create Configuration Item settings based on registry keys
163 #>
164 function New-SCCMConfigurationItemSetting
165 {
```

EK-3. (devam) Dönüşüm kodu

```
167   Param(
168     [Parameter(
169       Mandatory=$true)]
170       [string]$DisplayName,
171     [Parameter(
172       Mandatory=$false)]
173       [string]$Description = "",
174     [Parameter(
175       Mandatory=$true)]
176     [ValidateSet('Int64', 'Double', 'String', 'DateTime', 'Version', 'StringArray')]
177       [string]$DataType,
178     [Parameter(
179       Mandatory=$true)]
180             [ValidateSet('HKEY_CLASSES_ROOT',  'HKEY_CURRENT_USER',
'HKEY_LOCAL_MACHINE', 'HKEY_USERS')]
181       [string]$Hive,
182     [Parameter(
183       Mandatory=$true)]
184       [bool]$Is64Bit,
185     [Parameter(
186       Mandatory=$true)]
187       [string]$Key,
188     [Parameter(
189       Mandatory=$true)]
190       [string]$ValueName,
191     [Parameter(
192       Mandatory=$true)]
193       [string]$LogicalName
194   )
195

196    If ($DisplayName.Length -gt $MAX_NAME_LENGTH)
197    {
198           $DisplayName = $DisplayName.Substring(0,$MAX_NAME_LENGTH)
199    }
200

201   Write-Verbose "`tCreating setting $DisplayName..."
202

203   $templatePath = "$scriptPath\xmlTemplates"
204

205   $settingXml = [xml](Get-Content $templatePath\setting.xml)
206   $settingXml.SimpleSetting.LogicalName = $LogicalName
207   $settingXml.SimpleSetting.DataType = $DataType
208   $settingXml.SimpleSetting.Annotation.DisplayName.Text = $DisplayName
209   $settingXml.SimpleSetting.Annotation.Description.Text = $Description
```

EK-3. (devam) Dönüşüm kodu

```
210     $settingXml.SimpleSetting.RegistryDiscoverySource.Hive = $Hive
211                             $settingXml.SimpleSetting.RegistryDiscoverySource.Is64Bit      =
$Is64Bit.ToString().ToLower()
212     $settingXml.SimpleSetting.RegistryDiscoverySource.Key = $Key
213     $settingXml.SimpleSetting.RegistryDiscoverySource.ValueName = $ValueName
214
215     $settingXml.Save("c:\users\public\test1.xml")
216     $settingXml
217 }
218
219 <#
220     Utilizes the ConfigurationManager PowerShell module to create Configuration
Item rules for previously created CI settings
221 #>
222 function New-SCCMConfigurationItemRule
223 {
224     [CmdletBinding()]
225     Param(
226         [Parameter(
227             Mandatory=$true)]
228             [string]$DisplayName,
229         [Parameter(
230             Mandatory=$false)]
231             [string]$Description = "",
232         [Parameter(
233             Mandatory=$true)]
234         [ValidateSet('None', 'Informational', 'Warning', 'Critical')]
235             [string]$Severity,
236         [Parameter(
237             Mandatory=$true)]
238                 [ValidateSet('Equals', 'NotEquals', 'GreaterThan', 'LessThan', 'Between',
'GreaterEquals', 'LessEquals', 'BeginsWith', `
239             'NotBeginsWith', 'EndsWith', 'NotEndsWith', 'Contains', 'NotContains', 'AllOf',
'OneOf', 'NoneOf')]
240             [string]$Operator,
241         [Parameter(
242             Mandatory=$true)]
243                 [ValidateSet('Registry', 'IisMetabase', 'WqlQuery', 'Script', 'XPathQuery',
'ADQuery', 'File', 'Folder', 'RegistryKey', 'Assembly')]
244             [string]$SettingSourceType,
245         [Parameter(
246             Mandatory=$true)]
247                 [ValidateSet('String', 'Boolean', 'DateTime', 'Double', 'Int64', 'Version',
'FileSystemAccessControl', 'RegistryAccessControl', `
```

EK-3. (devamı) Dönüşüm kodu

```
248                                     'FileSystemAttribute', 'StringArray', 'Int64Array',
'FileSystemAccessControlArray',                                 'RegistryAccessControlArray',
'FileSystemAttributeArray')]
249             [string]$DataType,
250         [Parameter(
251             Mandatory=$true)]
252         [ValidateSet('Value', 'Count')]
253             [string]$Method,
254         [Parameter(
255             Mandatory=$true)]
256             [bool]$Changeable,
257         [Parameter(
258             Mandatory=$true)]
259             $Value,
260         [Parameter(
261             Mandatory=$true)]
262                 [ValidateSet('String', 'Boolean', 'DateTime', 'Double', 'Int64', 'Version',
'FileSystemAccessControl', 'RegistryAccessControl', `
263                                     'FileSystemAttribute', 'StringArray', 'Int64Array',
'FileSystemAccessControlArray',                                 'RegistryAccessControlArray',
'FileSystemAttributeArray')]
264             [string]$ValueDataType,
265         [Parameter(
266             Mandatory=$true)]
267             [string]$AuthoringScope,
268         [Parameter(
269             Mandatory=$true)]
270             [string]$SettingLogicalName,
271         [Parameter(
272             Mandatory=$true)]
273             [string]$LogicalName
274     )
275
276     If ($DisplayName.Length -gt $MAX_NAME_LENGTH)
277     {
278             $DisplayName = $DisplayName.Substring(0,$MAX_NAME_LENGTH)
279     }
280
281     Write-Verbose "`tCreating rule $DisplayName..."
282
283     $templatePath = "$scriptPath\xmlTemplates"
284     $id = "Rule_$([guid]::NewGuid())"
285     $resourceID = "ID-$([guid]::NewGuid())"
286     #$logicalName = "OperatingSystem_$([guid]::NewGuid())"
287
```

EK-3. (devam) Dönüşüm kodu

```
288     if ($DataType -eq "StringArray")
289     {
290         $ruleXml = [xml](Get-Content $templatePath\ruleSA.xml)
291     }
292     else
293     {
294         $ruleXml = [xml](Get-Content $templatePath\rule.xml)
295     }
296
297     $ruleXml.Rule.Id = $id
298     $ruleXml.Rule.Severity = $Severity
299     $ruleXml.Rule.Annotation.DisplayName.Text = $DisplayName
300     $ruleXml.Rule.Annotation.Description.Text = $Description
301     $ruleXml.Rule.Expression.Operator = $Operator
302             $ruleXml.Rule.Expression.Operands.SettingReference.AuthoringScopeId =
$AuthoringScope
303                 $ruleXml.Rule.Expression.Operands.SettingReference.LogicalName =
$LogicalName
304         $ruleXml.Rule.Expression.Operands.SettingReference.SettingLogicalName =
$SettingLogicalName
305             $ruleXml.Rule.Expression.Operands.SettingReference.SettingSourceType =
$SettingSourceType
306                     $ruleXml.Rule.Expression.Operands.SettingReference.DataType =
$ValueDataType
307     $ruleXml.Rule.Expression.Operands.SettingReference.Method = $Method
308                 $ruleXml.Rule.Expression.Operands.SettingReference.Changeable =
$Changeable.ToString().ToLower()
309
310     # If registry value type is StringArray
311     if ($DataType -eq "StringArray")
312     {
313                     $ruleXml.Rule.Expression.Operands.ConstantValueList.DataType =
"StringArray"
314         $valueIndex = 0
315         # For each value in array of values
316         foreach ($v in $Value)
317         {
318             # if not first value in array add new nodes; else just set the one value
319             if ($valueIndex -gt 0)
320             {
321                 # if only one index do not specifiy index to copy; else specify the index to
copy
322                 if ($valueIndex -le 1)
323                 {
324                                                                 $newNode =
$ruleXml.Rule.Expression.Operands.ConstantValueList.ConstantValue.Clone()
325                 }
```

EK-3. (devam) Dönüşüm kodu

```
326             else
327             {
328                                                                 $newNode    =
$ruleXml.Rule.Expression.Operands.ConstantValueList.ConstantValue[0].Clone()
329             }
330
$ruleXml.Rule.Expression.Operands.ConstantValueList.AppendChild($newNode)
331
$ruleXml.Rule.Expression.Operands.ConstantValueList.ConstantValue[$valueIndex].Data
Type = "String"
332
$ruleXml.Rule.Expression.Operands.ConstantValueList.ConstantValue[$valueIndex].Valu
e = $v
333
334         }
335         else
336         {
337
$ruleXml.Rule.Expression.Operands.ConstantValueList.ConstantValue.DataType          =
"String"
338
$ruleXml.Rule.Expression.Operands.ConstantValueList.ConstantValue.Value = $v
339         }
340         $valueIndex++
341       }
342    }
343    else
344    {
345                         $ruleXml.Rule.Expression.Operands.ConstantValue.DataType    =
$ValueDataType
346       $ruleXml.Rule.Expression.Operands.ConstantValue.Value = $Value
347    }
348    $ruleXml
349 }
350

351 <#
352    Utilizes the ConfigurationManager PowerShell module to create Configuration
Items based on previously created settings and rules
353 #>
354 function New-SCCMConfigurationItems
355 {
356    [CmdletBinding()]
357    Param(
358       [Parameter(
359          Mandatory=$true)]
360          [string]$Name,
```

EK-3. (devam) Dönüşüm kodu

```
361         [Parameter(
362             Mandatory=$false)]
363             [string]$Description="",
364         [Parameter(
365             Mandatory=$true)]
366                     [ValidateSet('MacOS', 'MobileDevice', 'None', 'WindowsApplication',
'WindowsOS')]
367         [string]$CreationType,
368         [Parameter(
369             Mandatory=$true)]
370             [array]$RegistryKeys,
371                 [Parameter(
372             Mandatory=$false)]
373         [ValidateSet('None', 'Informational', 'Warning', 'Critical')]
374                 [string]$Severity='Informational'    # Rule severity
375     )
376
377     If ((Get-Module).Name -contains 'ConfigurationManager')
378     {
379             Write-Verbose "ConfigurationManager module already loaded."
380     }
381     Else
382     {
383             Try
384             {
385                     Import-Module                                    "$(Split-Path
$env:SMS_ADMIN_UI_PATH)\ConfigurationManager"          #   Imports   ConfigMgr
PowerShell module
386             }
387             Catch [Exception]
388             {
389                     Write-Host "Error trying to import ConfigurationManager module."
-ForegroundColor Red
390                     Write-Host "Script will exit." -ForegroundColor Red
391                     pause
392                     Exit
393             }
394     }
395

396     If ($Name.Length -gt $MAX_NAME_LENGTH)
397     {
398             $Name = $Name.Substring(0,$MAX_NAME_LENGTH)
399     }
400

401     Write-Host "Creating Configuration Item..."
```

EK-3. (devam) Dönüşüm kodu

```
402

403     Set-Location "$SiteCode`:"
404

405     $origName = $Name
406     #$tmpFileCi = [System.IO.Path]::GetTempFileName()
407      # If ResultantSetOfPolicy option is used use the OU path to name the CI xml
408      if ($ResultantSetOfPolicy)
409      {
410                $ouNoSpace = $Global:ouPath.Replace(" ", "_")
411                $ouNoSpace = $ouNoSpace.Replace("/", "_")
412                $ciFile = "$scriptPath\$ouNoSpace.xml"
413      }
414      # If ResultantSetOfPolicy option is not used use the GPO nane to name the CI xml
415      else
416      {
417                $gpoNoSpace = $GpoTarget.Replace(" ", "_")
418                $ciFile = "$scriptPath\$gpoNoSpace.xml"
419      }
420

421
422     for ($i = 1; $i -le 99; $i++)
423     {
424        $testCI = Get-CMConfigurationItem -Name $Name -Fast
425        if ($testCI -eq $null)
426        {
427           break
428        }
429        else
430        {
431           $Name = $origName + " ($i)"
432        }
433     }
434

435          $ci = New-CMConfigurationItem -Name $Name -Description $Description -
CreationType $CreationType
436                                                                  $ciXml =
[xml]($ci.SDMPackageXML.Replace('<RootComplexSetting/></Settings>',
'<RootComplexSetting><SimpleSetting></SimpleSetting></RootComplexSetting></Setti
ngs><Rules><Rule></Rule></Rules>'))
437

438     $ciXml.Save($ciFile)
439
```

EK-3. (devam) Dönüşüm kodu

```
440     foreach ($Key in $RegistryKeys)
441     {
442         $len = ($Key.FullKeyPath.Split("\")).Length
443         $keyName = ($Key.FullKeyPath.Split("\"))[$len - 1]
444         $valueName = $Key.ValueName
445         $value = $Key.Value
446         $value = $value -replace "[^\u0030-\u0039\u0041-\u005A\u0061-\u007A]\Z", ""
447         $type = $Key.Type
448         $dName = $keyName + " - " + $valueName
449         $hive = ($Key.FullKeyPath.Split("\"))[0]
450         $subKey = ($Key.FullKeyPath).Replace("$hive\","")
451         $logicalNameS = "RegSetting_$([guid]::NewGuid())"
452                                                                 $ruleLogName          =
$ciXml.DesiredConfigurationDigest.OperatingSystem.LogicalName
453                                                                 $authScope            =
$ciXml.DesiredConfigurationDigest.OperatingSystem.AuthoringScopeId
454
455             if ($Key.Type -eq "Binary")
456             {
457                     continue
458             }
459             if ($Key.Type -eq "ExpandString")
460         {
461             $dataType = "String"
462         } elseif ($Key.Type -eq "MultiString")
463         {
464             $dataType = "StringArray"
465         } elseif ($Key.Type -eq "DWord")
466         {
467             $dataType = "Int64"
468         } else
469         {
470             $dataType = $Key.Type
471         }
472
473         if ($value.Length -gt 0)
474         {
475             $settingXml = New-SCCMConfigurationItemSetting -DisplayName $dName -
Description ("$keyName - $valueName") -DataType $dataType -Hive $hive -Is64Bit
$false `
476                 -Key $subKey -ValueName $valueName -LogicalName $logicalNameS
477
478             if ($dataType -eq "StringArray")
479             {
480                 $operator = "AllOf"
481             }
482             else
483             {
```

EK-3. (devam) Dönüşüm kodu

```
484             $operator = "Equals"
485         }
486
487          $ruleXml = New-SCCMConfigurationItemRule -DisplayName ("$valueName - $value - $type") -Description "" -Severity $Severity -Operator $operator -SettingSourceType Registry -DataType $dataType -Method Value -Changeable $Remediate `
488                 -Value $value -ValueDataType $dataType -AuthoringScope $authScope -SettingLogicalName $logicalNameS -LogicalName $ruleLogName
489
490         # If array returned search arrary for XmlDocument
491         if ($ruleXml.count -gt 1)
492         {
493             for ($i = 0; $i -lt ($ruleXml.Count); $i++)
494             {
495                 if ($ruleXml[$i].GetType().ToString() -eq "System.Xml.XmlDocument")
496                 {
497                     $ruleXml = $ruleXml[$i]
498                     continue
499                 }
500             }
501         }
502         $importS = $ciXml.ImportNode($settingXml.SimpleSetting, $true)
503
$ciXml.DesiredConfigurationDigest.OperatingSystem.Settings.RootComplexSetting.AppendChild($importS) | Out-Null
504         $importR = $ciXml.ImportNode($ruleXml.Rule, $true)
505
506
$ciXml.DesiredConfigurationDigest.OperatingSystem.Rules.AppendChild($importR)       | Out-Null
507         $ciXml = [xml] $ciXml.OuterXml.Replace(" xmlns=`"`"", "")
508         $ciXml.Save($ciFile)
509       }
510    }
511
512    If ($ExportOnly)
513    {
514             Write-Host "Deleting Empty Configuration Item..."
515             Remove-CMConfigurationItem -Id $ci.CI_ID -Force
516             Write-Host "Creating CAB File..."
517             if ($ResultantSetOfPolicy)
518             {
519                     Export-CAB -Name $Global:ouPath -Path $ciFile
520             }
521             else
522             {
```

EK-3. (devam) Dönüşüm kodu

```
523                     Export-CAB -Name $GpoTarget -Path $ciFile
524             }
525     }
526     Else
527     {
528             Write-Host "Setting DCM Digest..."
529             Set-CMConfigurationItem   -DesiredConfigurationDigestPath   $ciFile   -Id
$ci.CI_ID
530             Remove-Item -Path $ciFile -Force
531     }
532 }
533
534 function Export-CAB
535 {
536     Param(
537             [string]$Name,
538             [string]$Path
539     )
540
541     $fileName = $Name.Replace(" ", "_")
542     $fileName = $fileName.Replace("/", "_")
543     $ddfFile = Join-Path -Path $scriptPath -ChildPath temp.ddf
544

545     $ddfHeader =@"
546 ;*** MakeCAB Directive file
547 ;
548 .OPTION EXPLICIT
549 .Set CabinetNameTemplate=$fileName.cab
550 .set DiskDirectory1=$scriptPath
551 .Set MaxDiskSize=CDROM
552 .Set Cabinet=on
553 .Set Compress=on
554 "$Path"
555 "@
556
557     $ddfHeader | Out-File -filepath $ddfFile -force -encoding ASCII
558     makecab /f $ddfFile | Out-Null
559

560     #Remove temporary files
561     Remove-Item ($scriptPath + '\temp.ddf') -ErrorAction SilentlyContinue
562     Remove-Item ($scriptPath + '\setup.inf') -ErrorAction SilentlyContinue
563     Remove-Item ($scriptPath + '\setup.rpt') -ErrorAction SilentlyContinue
564     Remove-Item ($scriptPath + '\' + $fileName + '.xml') -ErrorAction SilentlyContinue
565 }
566
```

EK-3. (devam) Dönüşüm kodu

```
function Get-RSOP
{
    [CmdletBinding()]
    Param(
            [Parameter(
                    Mandatory=$true)]
            [string]$ComputerName
    )

    $tmpXmlFile = [System.IO.Path]::GetTempFileName()    # Creates temp file for rsop results

    try
    {
            Write-Host "Processing Resultant Set of Policy for $ComputerName"
            Get-GPResultantSetOfPolicy -Computer $ComputerName -ReportType xml -Path $tmpXmlFile
    }
    catch [Exception]
    {
            Write-Host "Unable to process Resultant Set of Policy" -ForegroundColor Red
            Pause
            Exit
    }

    $rsop = [xml](Get-Content -Path $tmpXmlFile)
    $domainName = $rsop.Rsop.ComputerResults.Domain
    $rsopKeys = @()

    # Loop through all applied GPOs starting with the last applied
    for ($x = $rsop.Rsop.ComputerResults.Gpo.Name.Count; $x -ge 1; $x--)
    {
            $rsopTemp = @()
            # Get GPO name
            $gpoResults = ($rsop.Rsop.ComputerResults.Gpo | Where-Object {($_.Link.AppliedOrder -eq $x) -and ($_.Name -ne "Local Group Policy")} | select Name).Name
            If ($gpoResults -ne $null)
            {
                    # If name is not null gets registry keys for that GPO and assign to temp value
                    $rsopTemp = Get-GPOKeys -PolicyName $gpoResults -Domain $domainName
                    if ($Global:ouPath -eq $null)
```

EK-3. (devam) Dönüşüm kodu

```
605                     {
606                             $Global:ouPath                                  =
($rsop.Rsop.ComputerResults.SearchedSom | Where-Object {$_.Order -eq $x} | select
Path).path
607                     }
608             }
609             # foreach registry key value in gpo results
610             foreach ($key in $rsopTemp)
611             {
612                     # if a value is not already stored with that FullKeyPath and
ValueName store that value
613                     if ((($rsopKeys | Where-Object {($_.FullKeyPath -eq
$key.FullKeyPath) -and ($_.ValueName -eq $key.ValueName)}) -eq $null)
614                     {
615                             $rsopKeys += $key
616                     }
617             }
618     }
619

620     Remove-Item -Path $tmpXmlFile -Force   # Deletes temp file
621

622     $rsopKeys
623 }
624

625 function Write-Log
626 {
627     [CmdletBinding()]
628     Param(
629             [Parameter(
630                     Mandatory=$true)]
631                     [array]$RegistryKey,
632             [Parameter(
633                     Mandatory=$true)]
634                     [string]$GPOName
635     )
636

637     [string]$logPath = 'gpo_registry_discovery_' + (Get-Date -Format MMddyyyy) +
'.log'
638     [string]$outString = $GPOName + "`t" + $RegistryKey.FullKeyPath + "`t" +
$RegistryKey.ValueName + "`t" + $RegistryKey.Value + "`t" + $RegistryKey.Type
639     Out-File -FilePath .\$logPath -InputObject $outString -Force -Append
640 }
641
```

EK-3. (devam) Dönüşüm kodu

```
function WriteXmlToScreen ([xml]$xml)
{
    $StringWriter = New-Object System.IO.StringWriter;
    $XmlWriter = New-Object System.Xml.XmlTextWriter $StringWriter;
    $XmlWriter.Formatting = "indented";
    $xml.WriteTo($XmlWriter);
    $XmlWriter.Flush();
    $StringWriter.Flush();
    Write-Output $StringWriter.ToString();
}


if ($GroupPolicy)
{
     $gpo = Get-GPOKeys -PolicyName $GpoTarget -Domain $DomainTarget
}
# If ResultantSetOfPolicy option is used remove the first index of the array that contains RSOP information
if ($ResultantSetOfPolicy)
{
    $gpo = Get-RSOP -ComputerName $ComputerName
    if ($gpo[0].RsopMode -ne $null)
    {
            $gpo = $gpo[1..($gpo.Length - 1)]
    }
}


If ($gpo -ne $null)
{
    # If ResultantSetOfPolicy option is used use the OU path to name the CI
    if ($ResultantSetOfPolicy -eq $true)
    {
            $ciName = $Global:ouPath
    }
    # If ResultantSetOfPolicy option is not used use the target GPO to name the CI
    elseif ($GroupPolicy -eq $true)
    {
            $ciName = $GpoTarget
    }


    New-SCCMConfigurationItems -Name $ciName -Description "This is a GPO compliance settings that was automatically created via PowerShell." -CreationType "WindowsOS" -Severity $Severity -RegistryKeys $gpo


    Set-Location $startingDrive
```

EK-3. (devam) Dönüşüm kodu

```
684     Write-Host "Complete"
685 }
686 Else
687 {
688     Write-Host "** ERROR! The script will terminate. **" -ForegroundColor Red
689 }
```

EK-4. Denetlenemeyen sıkılaştırma politikaları

Çizelge 4.1. Denetlenemeyen politika ayarları

Politika Yolu	MS Kuralı (Baseline)	Kayıt Defteri (Registry) Bilgisi
Hesap Açma	15	Hesap Açma Politikası güvenlik ayarları kayıt defteri anahtarı değildir
Hesap Açma	10	Hesap Açma Politikası güvenlik ayarları kayıt defteri anahtarı değildir
Hesap Açma	15	Hesap Açma Politikası güvenlik ayarları kayıt defteri anahtarı değildir
Parola Politikası	24	Parola Politikası güvenlik ayarları kayıt defteri anahtarı değildir
Parola Politikası	60	Parola Politikası güvenlik ayarları kayıt defteri anahtarı değildir
Parola Politikası	1	Parola Politikası güvenlik ayarları kayıt defteri anahtarı değildir
Parola Politikası	14	Parola Politikası güvenlik ayarları kayıt defteri anahtarı değildir
Parola Politikası	Etkin	Parola Politikası güvenlik ayarları kayıt defteri anahtarı değildir
Parola Politikası	Etkin Değil	Parola Politikası güvenlik ayarları kayıt defteri anahtarı değildir
Güvenlik Opsiyonları	Etkin Değil	Kayıt defteri anahtarı değildir
Güvenlik Opsiyonları	Etkin Değil	Kayıt defteri anahtarı değildir
Güvenlik Opsiyonları	Etkin Değil	Kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Boş	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Yöneticiler; Uzak masaüstü kullanıcıları	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Boş	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Yöneticiler; Users	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Yöneticiler	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Yöneticiler	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Boş	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Yöneticiler; yerel servisi; ağ servisi; servisi	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Boş	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir

EK-4. (devam) Denetlenemeyen sıkılaştırma politikaları

Çizelge 4.1. (devam) Denetlenemeyen politika ayarları

Politika Yolu	MS Kuralı (Baseline)	Kayıt Defteri (Registry) Bilgisi
Kullanıcı Hakları Atamaları	Yöneticiler	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Yöneticiler	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Misafirler, NT AUTHORITY\yerel hesap	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Misafirler	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Misafirler, NT AUTHORITY\yerel hesap	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Boş	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Yöneticiler	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Yöneticiler, servisi, yerel servisi, ağ servisi	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Yöneticiler	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Yöneticiler	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Boş	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Yöneticiler	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Yöneticiler	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Yöneticiler	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Yöneticiler	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Yöneticiler	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Kullanıcı Hakları Atamaları	Yöneticiler	Kullanıcı hakları güvenlik ayarları kayıt defteri anahtarı değildir
Hesap Oturum Açma	Kimlik Geçerlemesini Denetle	Başarı ve Başarısızlık
Hesap Yönetimi	Güvenlik Grup Yönetimini Denetle	Başarı
Hesap Yönetimi	Kullanıcı Hesap Yönetimini Denetle	Başarı ve Başarısızlık

EK-4. (devam) Denetlenemeyen sıkılaştırma politikaları

Çizelge 4.1. (devam) Denetlenemeyen politika ayarları

Politika Yolu	MS Kuralı (Baseline)	Kayıt Defteri (Registry) Bilgisi
Detaylı İzleme	PNP Aktivitesini Denetle	Başarı
Detaylı İzleme	İşlem Yaratma Denetmi	Başarı
Oturum açma / kapatma	Hesap Açma Denetimi	Başarısızlık
Oturum açma / kapatma	Grup Üyeliği Denetimi	Başarı
Oturum açma / kapatma	Oturum Açma Denetimi	Başarı ve Başarısızlık

EK-5. Çözüm modeli denetim raporları

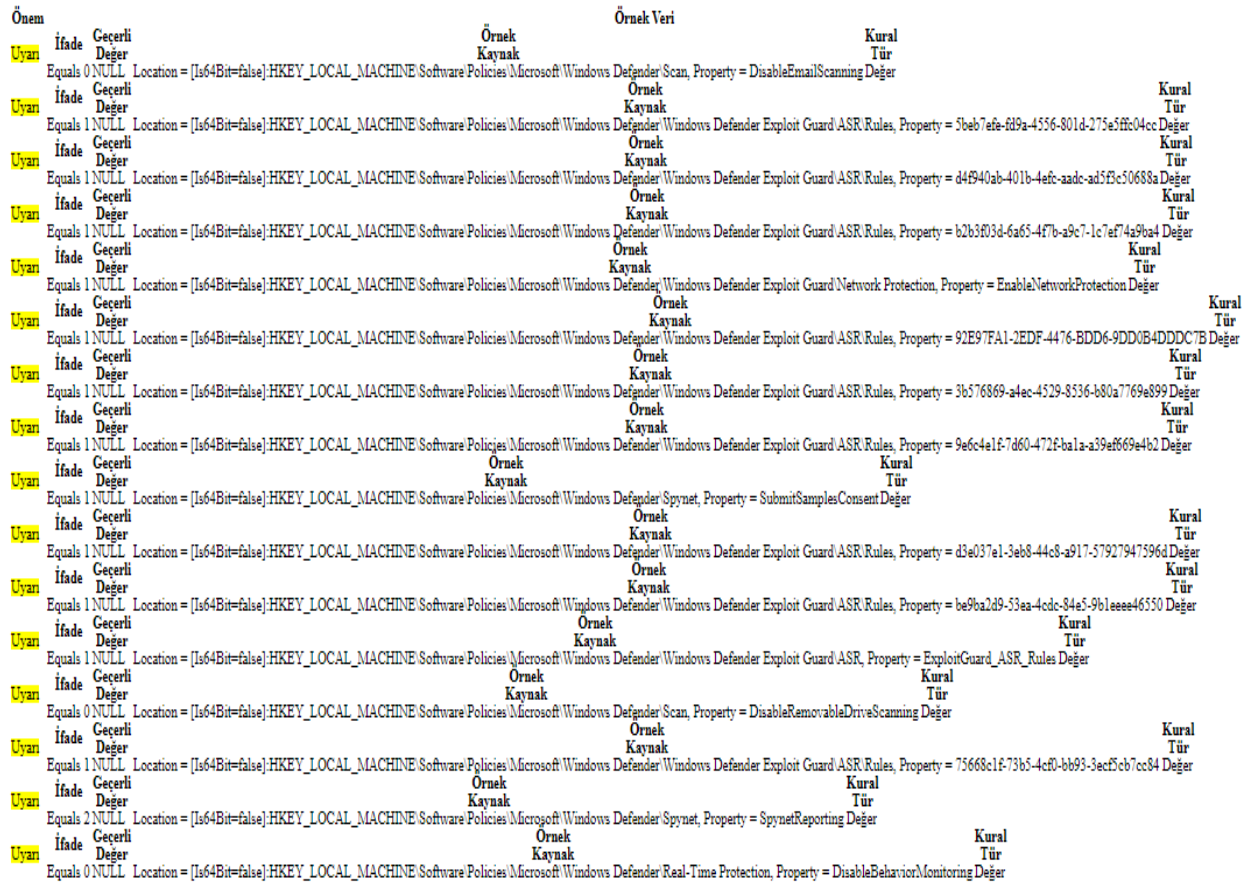
Çizelge 5.1. TESTPC1 denetim sonuç raporu

Adı	Uyumluluk Durmu	Uyumlu Olmayan Kurallar
Sıkılaştırma Uyumluluk	Uyumlu	0
MSFT Windows 10 Xbox Accessory Management Service	Uyumlu	0
MSFT Windows 10 RS4 - User	Uyumlu	0
MSFT Windows 10 and Server 2016 - Credential Guard	Uyumlu	0
MSFT Internet Explorer 11 - Computer	Uyumlu	0
MSFT Windows 10 RS4 - BitLocker	Uyumlu	0
MSFT Internet Explorer 11 - User	Uyumlu	0
MSFT Windows 10 RS4 - Computer	Uyumlu	0
MSFT Windows 10 and Server 2016 - Defender Antivirus	Uyumlu	0

Çizelge 5.2. TESTPC2 denetim sonuç raporu

Ad	Uyumluluk Durum	Uyumlu Değil Kurallar
Sıkılaştırma Uyumluluk	Uyumlu Değil	269
MSFT Windows 10 Xbox	Uyumlu Değil	4
MSFT Windows 10 RS4 - User	Uyumlu Değil	2
MSFT Windows 10 and Server 2016 - Credential Guard	Uyumlu Değil	4
MSFT Internet Explorer 11 - Computer	Uyumlu Değil	132
MSFT Windows 10 RS4 - BitLocker	Uyumlu Değil	17
MSFT Internet Explorer 11 - User	Uyumlu Değil	3
MSFT Windows 10 RS4 - Computer	Uyumlu Değil	91
MSFT Windows 10 and Server 2016 - Defender Antivirus	Uyumlu Değil	16

EK-5. (devam) Çözüm modeli denetim raporları



Önem		Örnek Veri					
Uyarı	İfade	Geçerli Değer	Örnek Kaynak	Kural Tür			
	Equals 0	NULL	Location = [Is64Bit=false]:HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Scan, Property = DisableEmailScanning	Değer			
Uyarı	İfade	Geçerli Değer	Örnek Kaynak	Kural Tür			
	Equals 1	NULL	Location = [Is64Bit=false]:HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules, Property = 5beb7efe-fd9a-4556-801d-275e5ffc04cc	Değer			
Uyarı	İfade	Geçerli Değer	Örnek Kaynak	Kural Tür			
	Equals 1	NULL	Location = [Is64Bit=false]:HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules, Property = d4f940ab-401b-4efc-aadc-ad5f3c50688a	Değer			
Uyarı	İfade	Geçerli Değer	Örnek Kaynak	Kural Tür			
	Equals 1	NULL	Location = [Is64Bit=false]:HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules, Property = b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4	Değer			
Uyarı	İfade	Geçerli Değer	Örnek Kaynak	Kural Tür			
	Equals 1	NULL	Location = [Is64Bit=false]:HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\Network Protection, Property = EnableNetworkProtection	Değer			
Uyarı	İfade	Geçerli Değer	Örnek Kaynak	Kural Tür			
	Equals 1	NULL	Location = [Is64Bit=false]:HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules, Property = 92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B	Değer			
Uyarı	İfade	Geçerli Değer	Örnek Kaynak	Kural Tür			
	Equals 1	NULL	Location = [Is64Bit=false]:HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules, Property = 3b576869-a4ec-4529-8536-b80a7769e899	Değer			
Uyarı	İfade	Geçerli Değer	Örnek Kaynak	Kural Tür			
	Equals 1	NULL	Location = [Is64Bit=false]:HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules, Property = 9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2	Değer			
Uyarı	İfade	Geçerli Değer	Örnek Kaynak	Kural Tür			
	Equals 1	NULL	Location = [Is64Bit=false]:HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Spynet, Property = SubmitSamplesConsent	Değer			
Uyarı	İfade	Geçerli Değer	Örnek Kaynak	Kural Tür			
	Equals 1	NULL	Location = [Is64Bit=false]:HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules, Property = d3e037e1-3eb8-44c8-a917-57927947596d	Değer			
Uyarı	İfade	Geçerli Değer	Örnek Kaynak	Kural Tür			
	Equals 1	NULL	Location = [Is64Bit=false]:HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules, Property = be9ba2d9-53ea-4cdc-84e5-9b1eeee46550	Değer			
Uyarı	İfade	Geçerli Değer	Örnek Kaynak	Kural Tür			
	Equals 1	NULL	Location = [Is64Bit=false]:HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR, Property = ExploitGuard_ASR_Rules	Değer			
Uyarı	İfade	Geçerli Değer	Örnek Kaynak	Kural Tür			
	Equals 0	NULL	Location = [Is64Bit=false]:HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Scan, Property = DisableRemovableDriveScanning	Değer			
Uyarı	İfade	Geçerli Değer	Örnek Kaynak	Kural Tür			
	Equals 1	NULL	Location = [Is64Bit=false]:HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules, Property = 75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84	Değer			
Uyarı	İfade	Geçerli Değer	Örnek Kaynak	Kural Tür			
	Equals 2	NULL	Location = [Is64Bit=false]:HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Spynet, Property = SpynetReporting	Değer			
Uyarı	İfade	Geçerli Değer	Örnek Kaynak	Kural Tür			
	Equals 0	NULL	Location = [Is64Bit=false]:HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Real-Time Protection, Property = DisableBehaviorMonitoring	Değer			

Resim 5.1. TESTPC2 MSFT Windows 10 Defender Antivirus denetimi

EK-5. (devam) Çözüm modeli denetim raporları

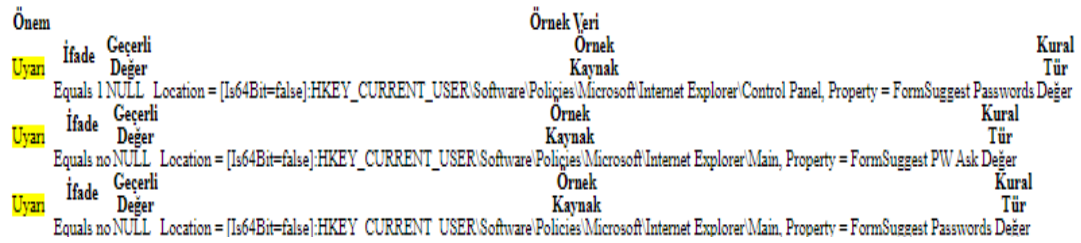
Resim 5.2.TESTPC2 MSFT Windows 10 RS4 – bilgisayar denetimi

EK-5. (devam) Çözüm modeli denetim raporları

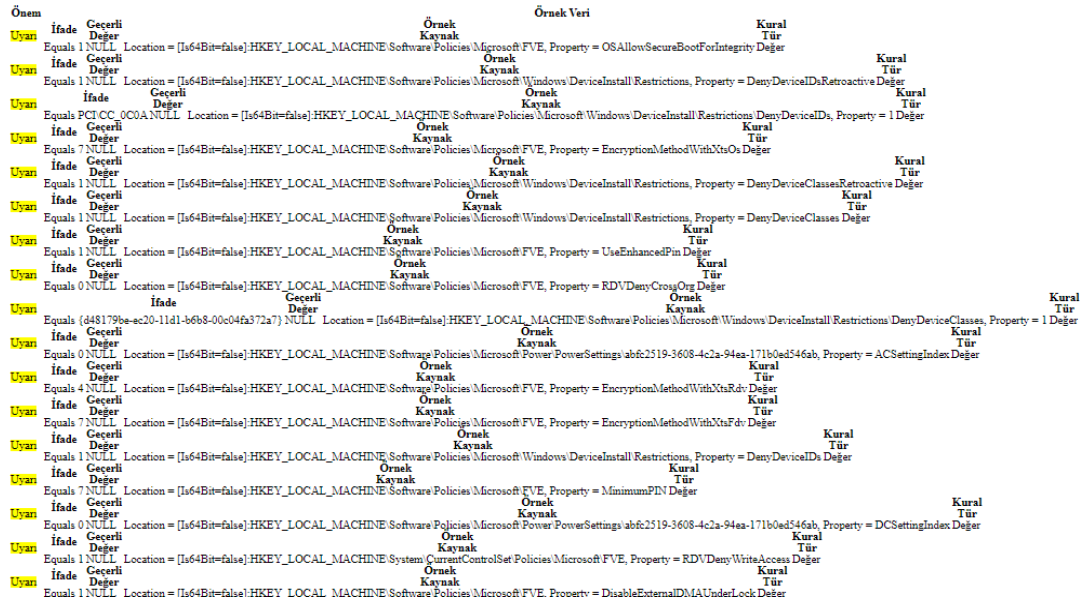
Resim 5.2. (devam) TESTPC2 MSFT Windows 10 RS4 – bilgisayar denetimi

EK-5. (devam) Çözüm modeli denetim raporları

Resim 5.2. (devam) TESTPC2 MSFT Windows 10 RS4 – bilgisayar denetimi



Resim 5.3. TESTPC2 MSFT Internet Explorer 11 – kullanıcı denetimi

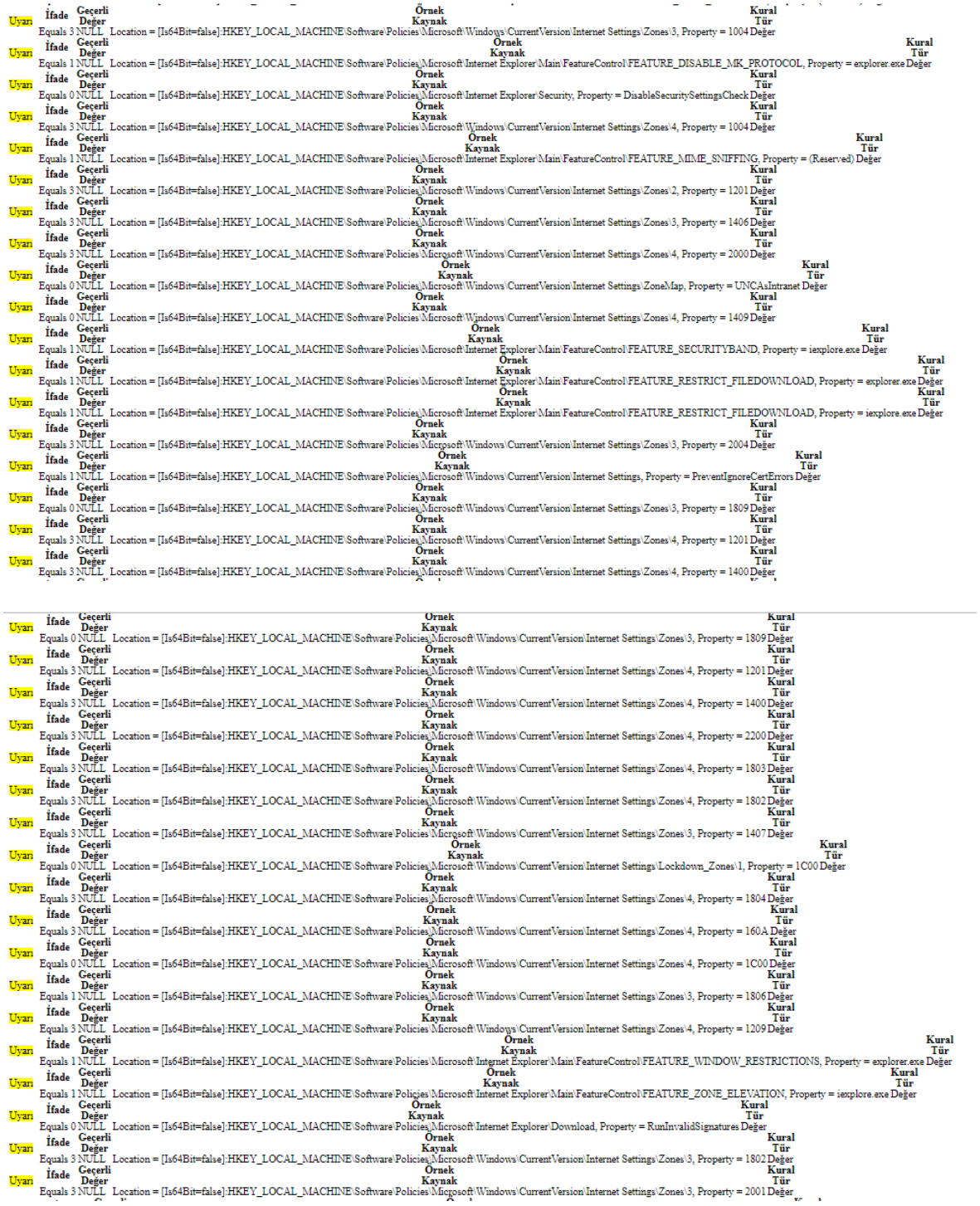


Resim 5.4. TESCTPC2 MSFT Windows 10 RS4 – BitLocker denetimi

EK-5. (devam) Çözüm modeli denetim raporları

Resim 5.5.TESTPC2 MSFT Internet Explorer 11 –bilgisayar denetimi

EK-5. (devam) Çözüm modeli denetim raporları



Resim 5.5. (devam) TESTPC2 MSFT Internet Explorer 11 –bilgisayar denetimi

EK-5. (devam) Çözüm modeli denetim raporları

Resim 5.5. (devam) TESTPC2 MSFT Internet Explorer 11 –bilgisayar denetimi

EK-5. (devam) Çözüm modeli denetim raporları

Resim 5.5. (devam) TESTPC2 MSFT Internet Explorer 11 –bilgisayar denetimi

EK-5. (devam) Çözüm modeli denetim raporları

Önem	Örnek Veri				
	İfade	Geçerli Değer	Örnek Kaynak	Kural Tür	
Uyarı	Equals 3	NULL	Location = [Is64Bit=false]:HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\DeviceGuard, Property = RequirePlatformSecurityFeatures	Değer	
	İfade	Geçerli Değer	Örnek Kaynak	Kural Tür	
Uyarı	Equals 1	NULL	Location = [Is64Bit=false]:HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\DeviceGuard, Property = LsaCfgFlags	Değer	
	İfade	Geçerli Değer	Örnek Kaynak	Kural Tür	
Uyarı	Equals 1	0	Location = [Is64Bit=false]:HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\DeviceGuard, Property = EnableVirtualizationBasedSecurity	Değer	
	İfade	Geçerli Değer	Örnek Kaynak		Kural Tür
Uyarı	Equals 1	NULL	Location = [Is64Bit=false]:HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\DeviceGuard, Property = HypervisorEnforcedCodeIntegrity		Değer

Resim 5.6. TESTPC2 MSFT Windows 10 kimlik denetimi

Ayar Ad	Ayar Tür	Ayar Açıklama	Kural Adı	Kural Açıklaması	Önem	Örnek Veri			
						İfade	Geçerli Değer	Örnek Kaynak	Kural Tür
Xbox Live Ağ Hizmeti	Wql Sorgusu		Xbox Live Ağ Hizmeti		Uyarı	NotEquals 0	0		Var Olan
Xbox Live Kimlik Doğrulama Yöneticisi	Wql Sorgusu		Xbox Live Kimlik Doğrulama Yöneticisi		Uyarı	NotEquals 0	0		Var Olan
Xbox Accessory Management Service	Wql Sorgusu		Xbox		Uyarı	NotEquals 0	0		Var Olan
Xbox Live Oyun Kaydetme	Wql Sorgusu		Xbox Live Oyun Kaydetme		Uyarı	NotEquals 0	0		Var Olan

Resim 5.7. TESTPC2 MSFT Windows 10 Xbox denetimi

Önem				
	İfade	Geçerli Değer	Örnek Kaynak	Kural Tür
Uyarı	Equals 1	NULL	Location = [Is64Bit=false]:HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CloudContent, Property = DisableThirdPartySuggestions	Değer
	İfade	Geçerli Değer	Örnek Kaynak	Kural Tür
Uyarı	Equals 1	NULL	Location = [Is64Bit=false]:HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\PushNotifications, Property = NoToastApplicationNotificationOnLockScreen	Değer

Resim 5.8. TESTPC2 MSFT Windows 10 RS4 – kullanıcı denetimi

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: YALPI, Hasan
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 01.01.1987, Tefenni
Medeni hali	: Evli
Telefon	: 0 (533) 485 23 15
E-mail	: hasan.yalpi@gazi.edu.tr

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Yüksek Lisans	Gazi Üniversitesi / Bilgi Güvenliği Mühendisliği	Devam ediyor
Lisans	Anadolu Üniversitesi / Uluslararası İlişkiler	2016
Lisans	Kara Harp Okulu / Elektronik Mühendisliği	2009
Lise	Işıklar Askeri Lisesi	2005

İş Deneyimi

Yıl	Yer	Görev
2018-Halen	Kara Kuvvetleri Karargâhı	Sistem Yöneticisi
2009-2018	Kara Kuvvetleri Komutanlığı	Birlik Komutanlığı

Yabancı Dil

İngilizce

Yayınlar

1. Coşkun, A., Yalpı, H. (2020, 10 Mayıs). İşletim Sistemi Sıkılaştırma Standartlarının Uygulanması ve Denetimi. Balkan 2. Uluslararası Uygulamalı Bilimler Kongresi, Edirne.

Hobiler

Yüzme, Koşu

GAZİ GELECEKTİR..