



Microsoft Defender ATP ile Uçtan Uca Güvenlik

Microsoft Defender ATP ile Uçtan Uca Güvenlik

İçindekiler

Yazar Hakkında	3
Giriş	4
Threat & Vulnerability Management	6
Security Recommendations	8
Software Inventory	9
Weaknesses	10
Attack Surface Reduction	11
Next Generation Protection	15
Behavior-base, heuristic and real-time antivirus protection	15
Cloud-delivered protection	16
Dedicated protection and product updates	17
Endpoint Detection & Response	18
Auto Investigation & Remediation	24
Advanced Hunting	26
Reports	30
Partners & API	31
MDATP Bitdefender GravityZone Entegrasyonu	31
MDATP Azure Sentinel Entegrasyonu	35
Settings	37
Windows Server 2008 R2 SP1, 2012 R2, 2016 Onboarding	37
Windows 10 Onboarding	41
System Center Configuration Manager SCEP Yapılandırması	46
AntiMalware Policy	49
Windows Defender Exploit Guard	66
Windows Defender ATP Policies	77
Windows Server 2016 Defender ATP Kurulumu	77
Group Policy ile Windows Defender Exploit Guard Yapılandırma	79
Attack Surface Reduction	79
Controlled Folder Access	81
Network Protection	84
Youtube Videoları	84
Faydalanılan Kaynaklar	85
SON SÖZ	86

Yazar Hakkında



Profesyonel iş hayatıma 2008 yılında başladım. 12 Yıllık dönem içerisinde teknikerlikten başlayarak bir çok farklı pozisyonda çalıştım. Dünyanın en büyük sigorta şirketleri arasında yer alan Allianz Türkiye’ de Kıdemli Sistem Uzmanı olarak çalıştıktan sonra beni heyecanlandıran bir teklif üzerine Dubai’ ye taşındım ve iş hayatıma Emirates NBD bankasında Kıdemli Sistem Mühendisi olarak devam etmekteyim. Profesyonel iş yaşantım dışında yönetim kadrosunda yer aldığım www.mshowto.org sitesinde gönüllü yazarlık yapmaktayım. 20+ konferansta konuşmacı olarak yer aldım. 150+ makale ve bu yazı serisi ile birlikte yedinci E-Kitabımı yazmanın mutluluğunu yaşamaktayım.

- ✓ CEH | Certified Ethical Hacker
- ✓ MCT | Microsoft Certified Trainer
- ✓ MVP | Cloud and Datacenter 2019-200
- ✓ MVP | Enterprise Mobility 2016-2017,2018-2019
- ✓ MCSE | Server Infrastructure
- ✓ MCSA | Server 2012
- ✓ MCPS | Microsoft Certified Professional
- ✓ Microsoft Specialist: Server Virtualization with Windows Server Hyper-V and System Center Specialist
- ✓ Tenable Certificate of Proficiency
- ✓ ICSI | CNSS Certified Network Security Specialist

Giriş

Merhabalar,

Yazım içerisinde Microsoft Defender ATP' yi MDATP olarak kısaltarak kullanacağım. Gartner raporuna baktığımız zaman MDATP' nin 2019 yılı endpoint protection sıralamasında lider olduğunu göreceksiniz. Merak edenler aşağıdaki linkten detaylıca inceleyebilirler.

<https://www.microsoft.com/security/blog/2019/08/23/gartner-names-microsoft-a-leader-in-2019-endpoint-protection-platforms-magic-quadrant/>

Kişisel olarak neden MDATP' yi kullanırım sorusunu kendime soracak olursam cevabım Microsoft kendi kernelini diğer 3rd parti vendor lardan daha iyi tanıyarak diyerek cevaplayabilirim.

Bu yazı serisinde de MDATP' yi bilgin doğrultusunda derinlemesine incelemeye çalışacağım. Bildiğiniz üzere Defender Windows Server 2016 ve Windows 10 işletim sisteminde varsayılan olarak bulunmaktadır. Yazı içerisinde bu bölüm daha yüzeysel işlenecektir. Yazı serimizin asıl amacı varsayılan olarak ATP ajanının gelmediği yapıları nasıl koruyabileceğimize değinmektir. Elbette <https://securitycenter.windows.com> paneli içerisindeki önemli noktalara yazım içerisinde yer vereceğim.

Endpoint Protection ürünlerini her zaman yüzüklerin efendisindeki bu savaş sahnesine benzetirim. Artık düşman son kalemize gelmiştir ve burayı da geçmesi gerekmektedir. Bu sebatte dolayı son kalemizi en iyi şekilde korumamız gerekmektedir. Umuyorum bu döküman biraz da olsa buna katkı sağlayacaktır.



Desteklenen İşletim Sistemleri

System Center Configuration Manager (SCCM) Current Branch (CB)

Microsoft Defender Antivirus (MDAV) (AV, EPP)

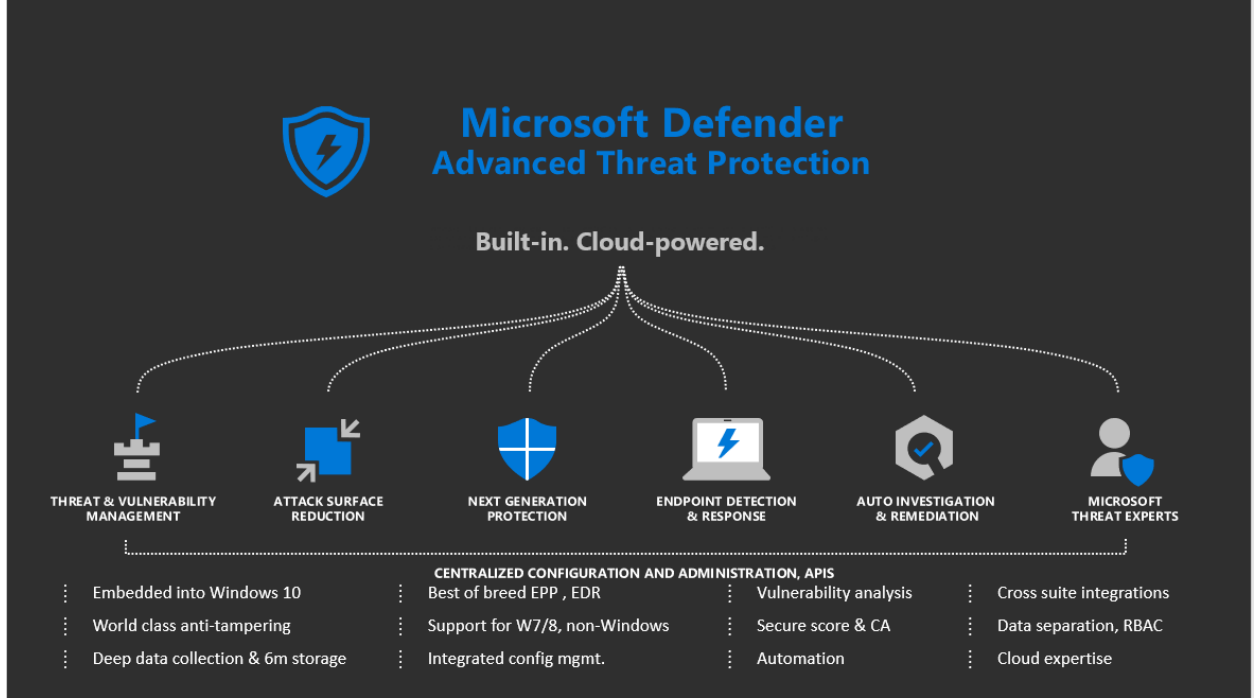
- Windows Server 2019
- Windows Server 2016
- Windows 10

System Center Endpoint Protection (SCEP) (AV, EPP)

- Windows Server 2012 R2
- Windows 8.1
- Windows Server 2012
- Windows 8
- Windows Server 2008 R2 SP1
- Windows 7 SP1
- Windows Server 2008 SP2

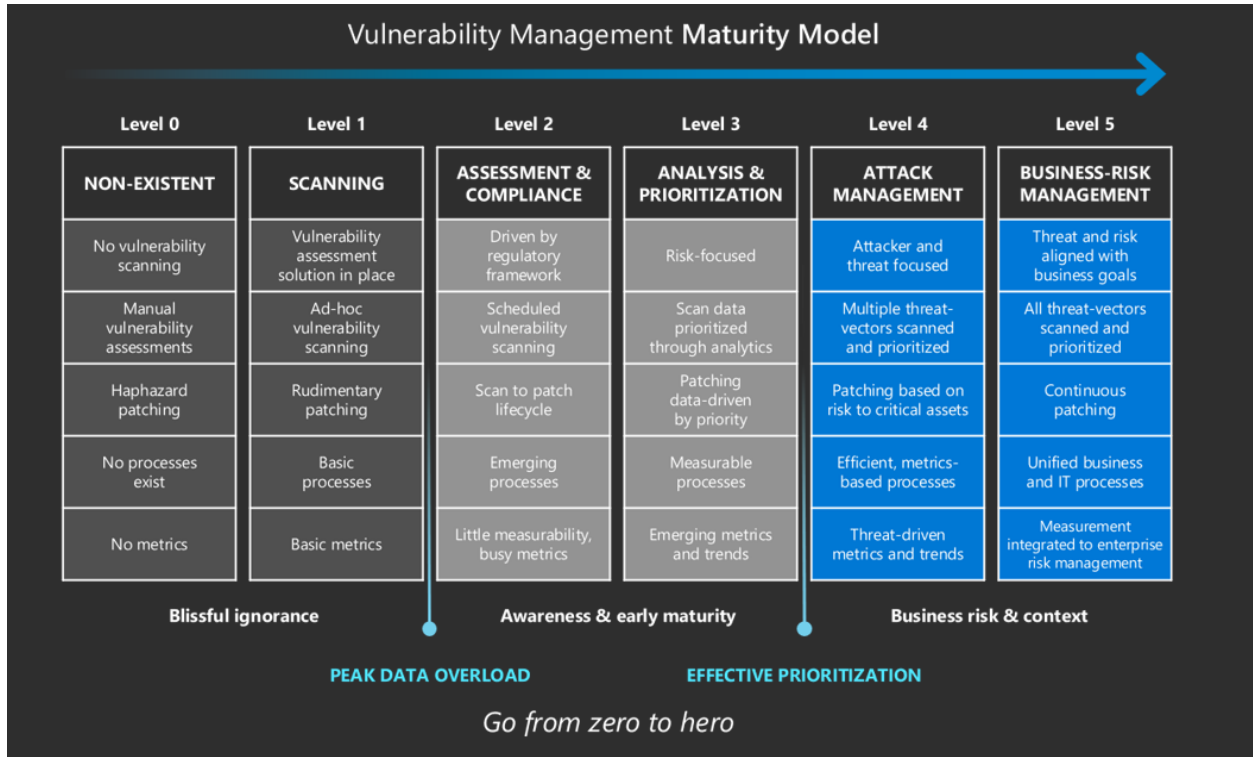
<https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/configs/supported-configurations>

Genel hatları ile ürün altı alt başlıktan oluşmaktadır ve yazım içerisinde herbirine ayrı başlıklar altında yer vereceğim.

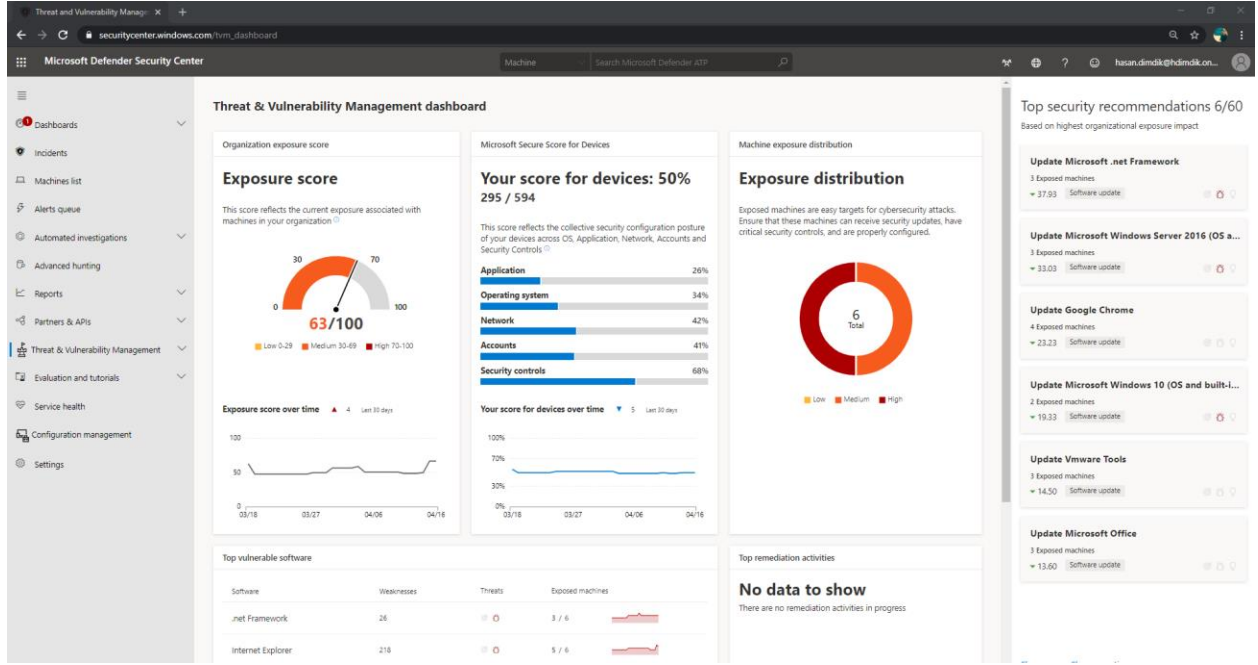


Threat & Vulnurability Management

Şirketler yapılarını her zaman daha iyileştirmeye çalışmaktadırlar. Endpoint Protection sadece yapımızı koruyan araçlardan bir tanesi. İlk olarak olgunluk seviyemizi belirlememiz ve şirket yapısına göre denge gözeterek iyileştirmelerimizi yapmamız gerekmektedir. Aşağıda örnek tabloda olgunluk seviyesi modelini görebilirsiniz.



Threat & Vulnerability Management içerisinde yapımızdaki zaafiyetleri tek bir panel içerisinde görebiliyoruz. Bu bize iyileştirmeye nereden başlamamız gerektiğine dair bilgi de vermektedir. Diğer bir ifadeyle zayıf halkanın neresi olduğunu hızlıca belirleyebiliyoruz.



Security Recommendations

Güvenlik tavsiyeleri içerisinde EDR teknolojisi ile taranıp bulunan zaafiyetleri tek çatı altında görüyoruz. Buradaki açıklıkları incelediğimizde sadece endpoint e yönelik zaafiyetler değil GPO ile yapabileceğimiz sıkılaştırmalar veya üçüncü parti yazılımlara ait tavsiyeleri de görüyoruz. Örneğin aşağıdaki ekran görüntüsünde Vmware tool ve Google Chrome' un güncellenmesi gerektiğine dair tavsiyelerde yer almaktadır.

Security recommendation	Weaknesses	Related component	Threats	Exposed machines
Update Microsoft .net Framework	26	Microsoft .net Framework	3 / 6	
Update Microsoft Windows Server 2016 (OS and built-in applications)	1328	Microsoft Windows Server 2016	3 / 3	
Update Google Chrome	24	Google Chrome	4 / 5	
Update Microsoft Windows 10 (OS and built-in applications)	72	Microsoft Windows 10	2 / 3	
Update VMware Tools	1	VMware Tools	3 / 3	
Update Microsoft Office	6	Microsoft Office	3 / 3	
Update VMware Workstation	11	VMware Workstation	1 / 1	
Update Intel Rapid Storage Technology	1	Intel Rapid Storage Technology	1 / 1	
Enable 'Local Security Authority (LSA) protection'	1	Operating system	6 / 6	
Set User Account Control (UAC) to automatically deny elevation requests	1	Operating system	6 / 6	
Disable 'Enumerate administrator accounts on elevation'	1	Operating system	6 / 6	
Disable SMBv1 client driver	1	Network	6 / 6	
Disable 'Always install with elevated privileges'	1	Operating system	6 / 6	
Disable 'Autoplay' for all drives	1	Operating system	6 / 6	
Set default behavior for 'AutoRun' to 'Enabled: Do not execute any autorun commands'	1	Operating system	6 / 6	

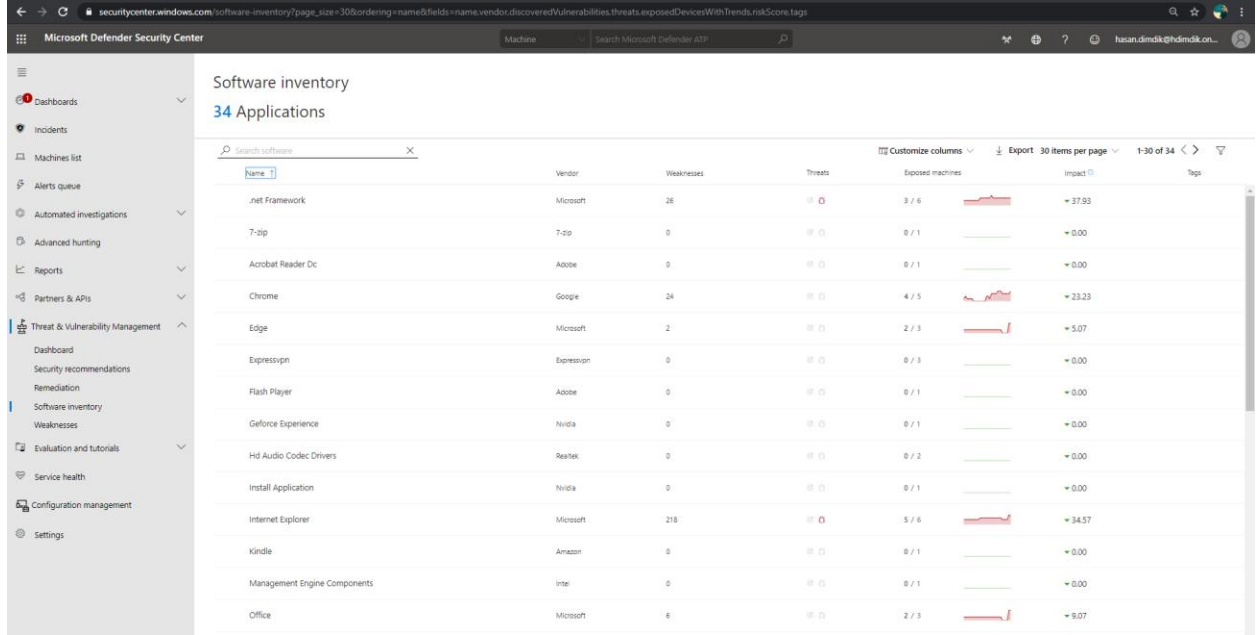
Güvenlik tavsiyelerini endpoint özelinde de raporlayabiliyoruz.

Security recommendation	Weaknesses	Related component	Threats	Status
Update Google Chrome	1	Google Chrome		Active
Update Microsoft .net Framework	26	Microsoft .net Framework		Active
Update Microsoft Windows Server 2016 (OS and built-in applications)	1328	Microsoft Windows Server 2016		Active
Update VMware Tools	1	VMware Tools		Active
Disable 'Allow running plugins that are outdated'	1	Application (Google Chrome)		Active
Disable 'Continue running background apps when Google Chrome is closed'	1	Application (Google Chrome)		Active
Block webpages from automatically running Flash plugins	1	Application (Google Chrome)		Active
Disable 'Password Manager'	1	Application (Google Chrome)		Active
Enable 'Block third party cookies'	1	Application (Google Chrome)		Active
Enable 'Local Security Authority (LSA) protection'	1	Operating system		Active
Set User Account Control (UAC) to automatically deny elevation requests	1	Operating system		Active
Disable 'Enumerate administrator accounts on elevation'	1	Operating system		Active
Disable Microsoft Defender Firewall notifications when programs are blocked for Domain profile	1	Security controls (Firewall)		Active
Disable Microsoft Defender Firewall notifications when programs are blocked for Private profile	1	Security controls (Firewall)		Active
Disable Microsoft Defender Firewall notifications when programs are blocked for Public profile	1	Security controls (Firewall)		Active
Disable merging of local Microsoft Defender Firewall rules with group policy firewall rules for the Public profile	1	Security controls (Firewall)		Active
Disable merging of local Microsoft Defender Firewall connection rules with group policy firewall rules for the Public profile	1	Security controls (Firewall)		Active

Software Inventory

Şirketlerdeki en büyük sorunlardan bir tanesi kurum içerisinde yüklü olan uygulamaların bilinmiyor olması, diğer bir deyişle uygulama envanterine hakim olunamaması. Software inventory adından da anlaşıldığı gibi bu sorunumuzu çözmektedir. Elbette burdaki öncelikli amaç hangi uygulama

ne kadar yapımızda açıklığa sebep oluyor bulmaktır.(Expose cümlesini türkçeye çevirdiğimizde açığa çıkarmak, maruz bırakmak veya teşhir etmek anlamlarına gelmektedir.)



Name	Vendor	Weaknesses	Threats	Exposed machines	Impact	Tags
.NET Framework	Microsoft	26	0	3 / 6	37.93	
7-zip	7-zip	0	0	0 / 1	0.00	
Acrobat Reader DC	Adobe	0	0	0 / 1	0.00	
Chrome	Google	24	0	4 / 5	23.23	
Edge	Microsoft	2	0	2 / 3	5.07	
Expression	Expression	0	0	0 / 3	0.00	
Flash Player	Adobe	0	0	0 / 1	0.00	
Geforce Experience	Nvidia	0	0	0 / 1	0.00	
Hd Audio Codec Drivers	Realtek	0	0	0 / 2	0.00	
Install Application	Nvidia	0	0	0 / 1	0.00	
Internet Explorer	Microsoft	218	0	5 / 6	34.57	
Kindle	Amazon	0	0	0 / 1	0.00	
Management Engine Components	Intel	0	0	0 / 1	0.00	
Office	Microsoft	6	0	2 / 3	9.07	

Weaknesses

Bildiğiniz üzere bir açıklık CVE olarak değerlendirildiğinde alenen artık zaafiyetin ne olduğu herkes tarafından biliniyor demektir. Bu durumda bırakın Black hat Hacker' ları Script Kiddie lerin bile hedefi olabileceğiniz anlamına gelmektedir. Bu bölümde detaylıca ilgili zaafiyetleri raporlayıp iyileştirmelere başlayabilirsiniz.

The screenshot displays the Microsoft Defender Security Center interface. The left sidebar contains navigation options: Dashboards, Incidents, Machines list, Alerts queue, Automated investigations, Advanced hunting, Reports, Partners & APIs, Threat & Vulnerability Management (selected), Dashboard, Security recommendations, Remediation, Software inventory, Weaknesses, Evaluation and tutorials, Service health, Configuration management, and Settings. The main content area is titled 'Weaknesses' and shows a list of 129k vulnerabilities. The table columns are Name, Severity, CVSS, Related Software, Age, and Published on. The first row is selected, showing CVE-2020-1014 with a High severity and a CVSS score of 7.8. The right sidebar provides details for CVE-2020-1014, including a vulnerability description, details (CVE-ID, CVSS, Updated on, Related Software), threat insights, and exploit kits.

Name	Severity	CVSS	Related Software	Age	Published on
CVE-2020-1014	High	7.8	Windows Server 2008 (+13 more)	3 days	4/14/20
CVE-2020-1011	High	7.8	Windows Server 2008 (+12 more)	3 days	4/14/20
CVE-2020-0964	High	8.0	Windows Server 2008 (+13 more)	3 days	4/14/20
CVE-2020-0821	Medium	5.5	Windows Server 2008 (+12 more)	3 days	4/14/20
CVE-2020-0955	Medium	5.5	Windows Server 2008 (+13 more)	3 days	4/14/20
CVE-2020-1009	High	7.8	Windows Server 2008 (+13 more)	3 days	4/14/20
CVE-2020-0968	High	7.5	Internet Explorer	3 days	4/14/20
CVE-2020-0958	High	7.0	Windows Server 2008 (+13 more)	3 days	4/14/20
CVE-2020-0889	Medium	6.7	Windows Server 2008 (+13 more)	3 days	4/14/20
CVE-2020-0907	High	7.8	Windows Server 2008 (+13 more)	3 days	4/14/20
CVE-2020-0952	Medium	5.5	Windows Server 2008 (+13 more)	3 days	4/14/20
CVE-2020-0936	High	7.1	Windows Rtl 8.1 (+10 more)	3 days	4/14/20
CVE-2020-0940	High	7.0	Windows Server 2008 (+13 more)	3 days	4/14/20
CVE-2020-0987	Medium	5.5	Windows Server 2008 (+13 more)	3 days	4/14/20
CVE-2020-0953	High	7.8	Windows Server 2008 (+13 more)	3 days	4/14/20
CVE-2020-0938	High	7.8	Windows Server 2008 (+13 more)	3 days	4/14/20
CVE-2020-0784	High	7.8	Windows Server 2008 (+12 more)	3 days	4/14/20
CVE-2020-0982	Medium	5.5	Windows Server 2008 (+13 more)	3 days	4/14/20
CVE-2020-0942	Medium	6.3	Windows Server 2008 (+5 more)	3 days	4/14/20

CVE-2020-1014

Vulnerability description

An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges. An attacker who successfully exploited this vulnerability could run processes in an elevated context. An attacker could then install programs; view, change or delete data to exploit this vulnerability; an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. The security update addresses the vulnerability by enabling the Windows Update client to properly handle user privileges.

Vulnerability details

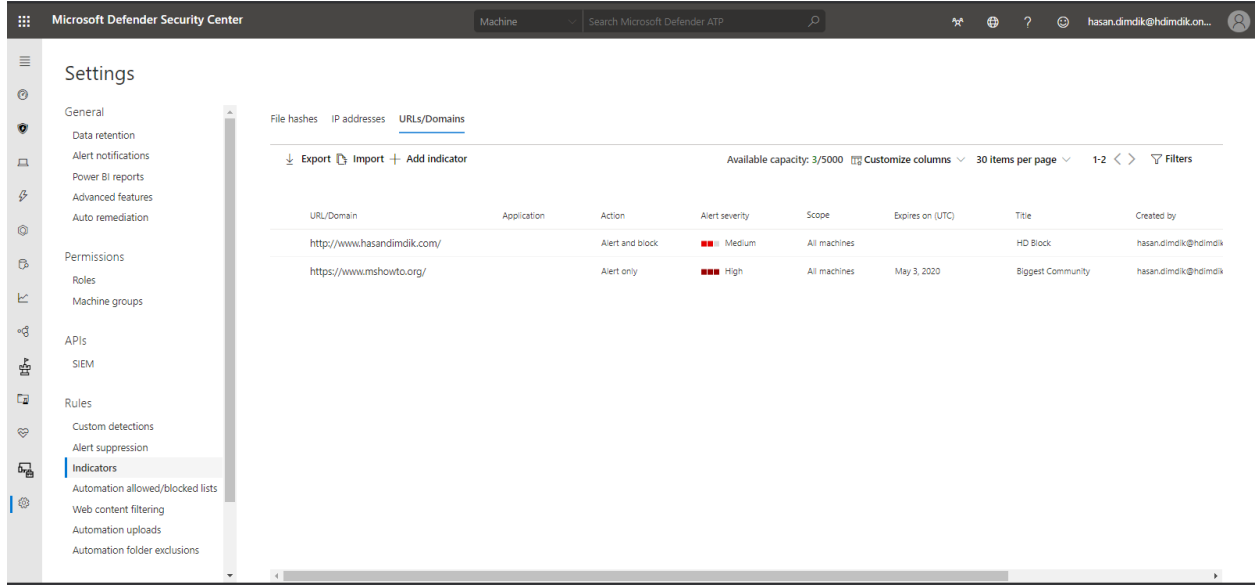
Field	Value
CVE-ID	CVE-2020-1014
Severity	High
CVSS	7.8
Published on	4/14/20
Updated on	4/15/20
Age	3 days
Related Software	Windows Server 2008 (+13 more)

Threat Insights

Field	Value
Public	No
Verified	No
Exploit kits	Not available
Type	-

Attack Surface Reduction

Atak yüzeyi kelimesini irdelediğimiz zaman saldırganın yapımız içerisine sızabileceği noktalar olarak değerlendirebiliriz. Savunan taraf olarak bizim görevimiz bu noktaları belirlemek ve daraltmaktır. Günümüzde artık bilgisayar kullanım alanları tamamen değişti. Bundan beş yıl öncesine baktığımızda herşey güvenlik duvarı arkasında korunmaktaydı. Şimdi ise bu tarz bir kısıtlama bulunmamaktadır. Bring your own device kavramı ile sınırlar kalkmaya başladı, bir sonraki aşamada ise artık her yerden çalışabilir hale geldik. Bu sebepten klasik koruma önlemleri artık yetersizdir. Oyuna artık web tehditleri, yemleme saldırıları, akıllı cihazlar, ransomware, apt saldırıları, nesnelerin interneti gibi n tane kavram dahil oldu, yine bahsettiğim gibi şirket sınırları değişti ve cihazlar her yerden bağlanabilir hale geldi. Attack Surface Reduction ise tam bu noktadaki sıkıntımızı gidermek için tasarlanmıştır. Microsoft hali hazırda tüm tehditleri aktif olarak tarayıp kendi veri tabanını güncellemektedir, elbette davranışsal analizde bir oranda tehditleri engellemektedir. Eğer şirket yapısına özel block rule yazmak isterseniz security center a bağlandıktan sonra **Indicators** sekmesi içerisinde tanımlayabilirsiniz.



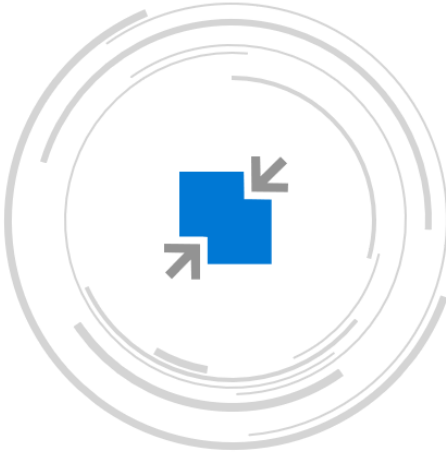
Beş farklı metodla Attack Surface Reduction' ı yapılandırabiliriz. İlerleyen bölümlerde System Center Configuration Manager ve GPO ile nasıl atak yüzeyini daraltabiliriz değineceğiz.

- Microsoft Intune
- Mobile Device Management (MDM)
- Microsoft Endpoint Configuration Manager
- Group Policy
- PowerShell

Kaynak : <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/enable-attack-surface-reduction>

Attack Surface Reduction

Resist attacks and exploitations



HW BASED ISOLATION

APPLICATION CONTROL

EXPLOIT PROTECTION

NETWORK PROTECTION

CONTROLLED FOLDER ACCESS

DEVICE CONTROL

WEB PROTECTION

RANSOMWARE PROTECTION

- Isolate access to untrusted sites
- Isolate access to untrusted Office files
- Host intrusion prevention
- Exploit mitigation
- Ransomware protection for your files
- Block traffic to low reputation destinations
- Protect your legacy applications
- Only allow trusted applications to run

Yunan mitolojisinde bildiğiniz üzere Aşil çok özel bir yere sahiptir ve nerdeyse ölümsüzdür, fakat küçük bir zaafiyeti içermektedir ki bu zaafiyet onun için ölümcüldür. Elbette aşil tendonundan bahsediyorum. Eğer saldırgan bu zafiyeti bilinçli veya şans eseri bulacak olursa etkisi yıkıcı olacaktır. Bu sebepten dolayı yapının sürekli taranıp zaafiyetlerin belirlenmesi güvenlik için önem arz etmektedir. Teknik detaylara ilerleyen bölümlerde değineceğiz.



Bu bölümle ilgili son değinmek istediğim nokta ise bulutun gücü ile birlikte MDATP bizi aşağıdaki atak türlerinden korumaktadır.

Attack Surface Reduction (ASR) Rules



Minimize the attack surface

Signature-less, control entry vectors, based on cloud intelligence. Attack surface reduction (ASR) controls, such as behavior of Office macros.

Productivity apps rules

- Block Office apps from creating executable content
- Block Office apps from creating child processes
- Block Office apps from injecting code into other processes
- Block Win32 API calls from Office macros
- Block Adobe Reader from creating child processes

Email rule

- Block executable content from email client and webmail
- Block only Office communication applications from creating child processes

Script rules

- Block obfuscated JS/VBS/PS/macro code
- Block JS/VBS from launching downloaded executable content

Polymorphic threats

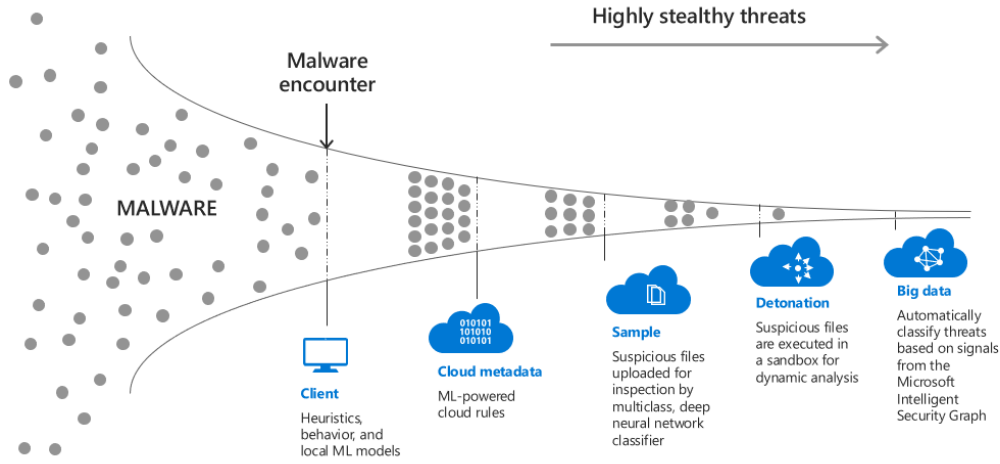
- Block executable files from running unless they meet a prevalence (1000 machines), age (24hrs), or trusted list criteria
- Block untrusted and unsigned processes that run from USB
- Use advanced protection against ransomware

Lateral movement & credential theft

- Block process creations originating from PSEXEC and WMI commands
- Block credential stealing from the Windows local security authority subsystem (lsass.exe)
- Block persistence through WMI event subscription

Next Generation Protection

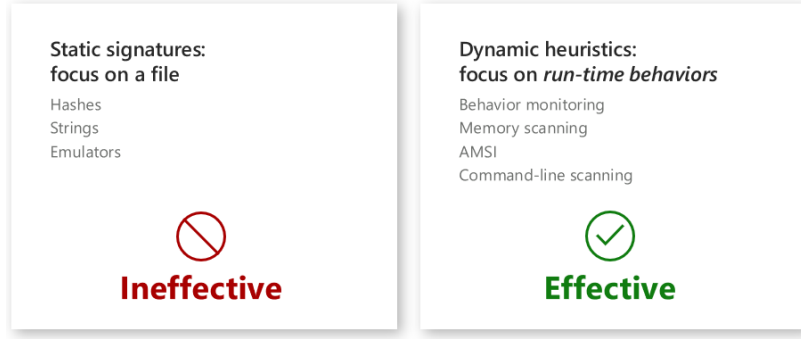
Bildiğiniz üzere imza tabanlı anti virüsler artık bizleri koruyamamaktadır. Kismende olsa koruyabilmektedir diyebilirim ! (Yorumu size bırakıyorum 😊) Günümüz atakları ise artık daha sofistike , imza tabansız,fileless ve/veya Hardware lerin açıklarından faydalanılarak gerçekleştirilen ataklar olarak karşımıza çıkmaktadır. Diğer bir sorun da saldırganların Endpoint Protection ları kolay bir şekilde devre dışı bırakmasıdır. Bu noktada ilgili ürünün bizi kernel seviyesine kadar koruması büyük önem arz etmektedir.



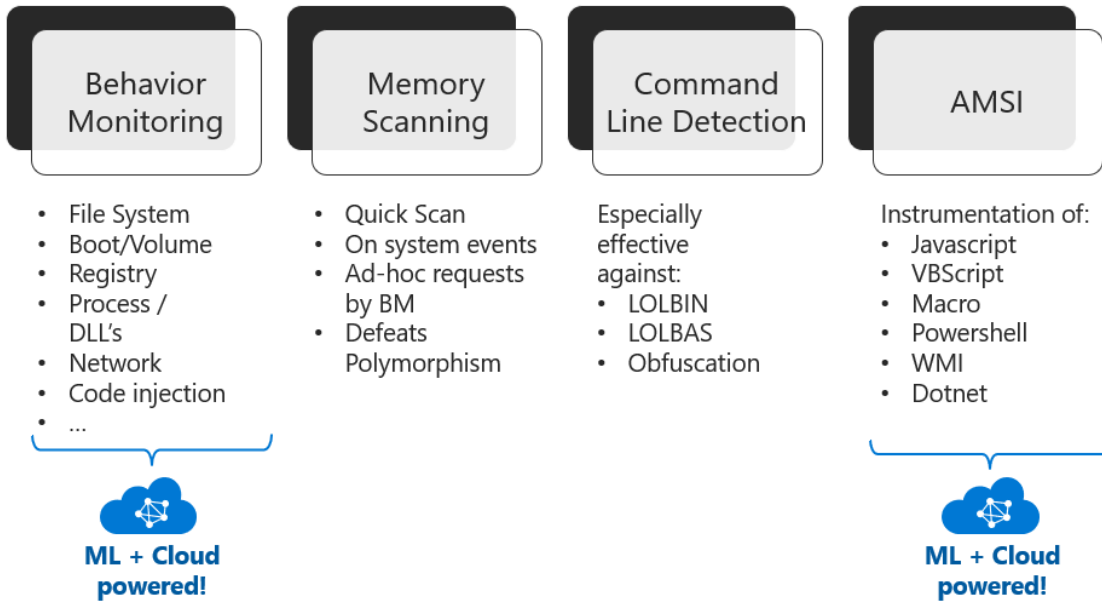
Teknik olarak Next Generation Protection nedir dersek bunu üç başlık altında toplayabiliriz.

Behavior-base, heuristic and real-time antivirus protection

İmza tabanlı anti virüs programı kullanıyorsanız artık çok da fazla günümüz tehditlerini koruyamamaktadır(Umuyorum gerçekten yapınız bu şekilde korunmuyordur).Bu noktada oyuna **Behavior-base, heuristic and real-time antivirus protection** girmektedir. Bu özellik sayesinde artık sadece imza tabanı incelenmemektedir aynı zamanda davranış da işin içine girmektedir.



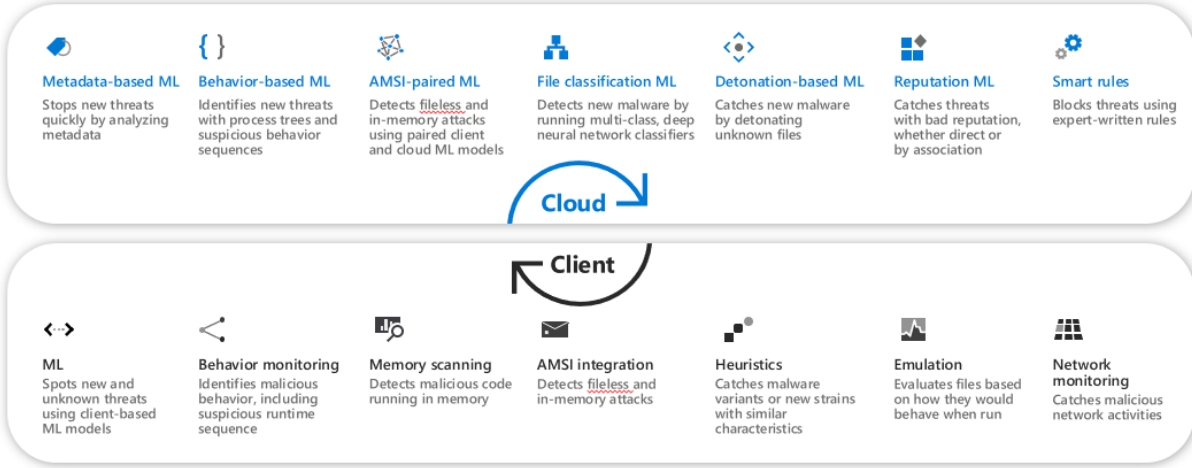
Davranışsal analiz elbette arka planda makina öğrenmesini kullanmaktadır ve aşağıdaki dört başlık altında etkin koruma sağlamaktadır.



Cloud-delivered protection

Bir önceki bölümde kısaca davranışsal analizin artık oyuna girdiğini belirtmiştik. Davranışsal analiz yeni bir tehditi ne kadar hızlı bir şekilde yakalayabilmektedir ? Örneğin sıfırncı gün atağından bahsedecek olursak klasik yöntemlerle bunu koruyamayacağımıza hemfikiriz. ATP ise aşağıda yer alan koruma motorları sayesinde etkin koruma sağlamaktadır.

Microsoft Defender ATP next generation protection engines



Aşağıdaki linkte nasıl koruduğunu anlatan videoyu izleyebilirsiniz.

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/utilize-microsoft-cloud-protection-windows-defender-antivirus>

Dedicated protection and product updates

Tam bir koruma sağlamak istiyorsanız elbette sıkı şekilde gerekli updateleri yapıyor olmamız gerekmektedir. Bu noktada iki farklı update den söz ediyoruz. İlki **Protection updates**. MAPS periyodik olarak güvenlik updatelerini kontrol edip yeni gelen update varsa indirilmektedir. Aynı zamanda **Product Update** ile endpoint ajanlarının güncellenmesi sağlanmaktadır.

Kaynak : <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/manage-updates-baselines-windows-defender-antivirus>

Endpoint Dedection & Response



- CORRELATED POST-BREACH DETECTION
- INVESTIGATION EXPERIENCE
- INCIDENT
- ADVANCED HUNTING
- RESPONSE ACTIONS (+EDR BLOCKS)
- DEEP FILE ANALYSIS
- LIVE RESPONSE
- THREAT ANALYTICS

MDATP nerdeyse gerçek zamanlı olarak tehditleri yakalar ve ilgili zararlıyı etkisiz hale getirir. Elbette burada diğer önemli nokta ise ilgili atağın detaylarını görebilmektir. Bu analiz bize ilgili atağın/zararlıının genel bir saldırı/zararlı olduğu veya şirkete özel sofistike bir atak olup olmadığını belirlememizde faydalı olacaktır. Bu bölümü örnekle açıklamam daha faydalı olacaktır. Portalıma erişip **Alert Queue** geldiğimde yapım içerisinde oluşan tüm alarmları görebiliyorum. Bu aslında Detect kısmına karşılık gelmektedir.

Microsoft Defender Security Center										
Alerts queue										
Title	Severity	Incident	Status	Category	Machine	User	Classification	Investigation state	Last activity	Assigned to
Automated investigation started manually	Informational	17	New	Suspicious activity	hdt1		Not set	Unsupported OS	4/17/20 11:59 AM	Unassigned
2 alerts: Mimikatz high-severity malware was detected	High	2 incidents	New	Grouped by Threat family	hdt1		Multiple	N/A	4/17/20 11:59 AM	Unassigned
Mimikatz high-severity malware was detected	High	18	New	Malware	hdt1		Not set	Unsupported OS	4/17/20 11:59 AM	Unassigned
Mimikatz high-severity malware was detected	High	12	New	Malware	hdt1		True alert	Unsupported OS	4/4/20 11:09 AM	Unassigned
Automated investigation started manually	Informational	16	New	Suspicious activity	windclient		Not set	Unsupported OS	4/17/20 11:38 AM	Unassigned
Automated investigation started manually	Informational	15	New	Suspicious activity	ghostsurface		Not set	No threats found	4/4/20 3:12 PM	Unassigned
Automated investigation started manually	Informational	13	New	Suspicious activity	hdt1		Not set	Unsupported OS	4/4/20 11:24 AM	Unassigned
Automated investigation started manually	Informational	13	New	Suspicious activity	hdt1		Not set	Unsupported OS	4/4/20 11:09 AM	Unassigned
Mimikatz hactool was detected	Low	12	New	Malware	hdt1		Not set	Unsupported OS	4/4/20 11:08 AM	Unassigned
Pynamer malware was detected	Informational	12	New	Malware	hdt1		Not set	Unsupported OS	4/4/20 11:08 AM	Unassigned
Automated investigation started manually	Informational	11	New	Suspicious activity	desktop-virtual		Not set	No threats found	4/4/20 10:39 AM	Unassigned
Automated investigation started manually	Informational	10	New	Suspicious activity	desktop-physical		Not set	No threats found	4/4/20 8:53 AM	Unassigned
Automated investigation started manually	Informational	9	New	Suspicious activity	ghostsurface		Not set	No threats found	4/3/20 9:23 PM	Unassigned
Suspicious behavior by a svchost.exe was observed	Medium	14	New	Execution	hdt1	hdtvnc	Not set	Unsupported OS	4/2/20 8:02 AM	Unassigned
Suspicious behavior by a svchost.exe was observed	Medium	14	New	Execution	hdt1	hdtvnc	Not set	Unsupported OS	4/2/20 8:02 AM	Unassigned

Örneğin ilgili sunucumda mimikatz çalıştırılmak istenmiş ve MDATP tarafından yakalanıp malware olarak kategorilendirilmiş. Detaylı olarak da process ağacını görebiliyoruz.

Microsoft Defender Security Center

Incidents > 12 > 'Mikatz' high-severity malware was detected

Automated investigation does not support OS

'Mikatz' high-severity malware was detected
This alert is part of incident (32)

Actions

Severity: High
Category: Malware
Detection source: Antivirus
Detection technology: Client
Detection status: Prevented

Alert context

Machine: h401

First activity: 04/04/2020 | 11:06:39
Last activity: 04/04/2020 | 11:09:21

Status

State: New
Classification: True alert
Assigned to: Not assigned

Description

High-severity malware refers to tools used by advanced Threat Activity Groups to target victims. Such Activity Groups may target individuals or institutions. They typically engage on industrial, military, diplomatic, and political espionage rather than more mundane activities such as identity theft or denial of service attacks. Some groups engage in acts of deliberate sabotage and destruction in order to cause real-world effects, such as disruptions to the victim's operations.

This category of malware includes tools such as:

- Exploits used to gain access to targeted computers or escalate privileges on infected computers;
- Backdoors used to maintain persistent command and control over infected computers in a stealthy manner;
- Lateral movement tools that permit attackers to scan the local network, locate targets of interest, and access additional computers;
- Counter-forensics tools used to delay and disrupt incident response activities, including destructive malware that can render computers inoperable;
- "Weaponized" tools that enable acts of deliberate sabotage or destruction or denial of service.

[Read more on Microsoft Encylopedia](#)

Recommended actions

1. Validate the alert.
2. Check for other suspicious activities in the machine timeline.
3. Isolate unfamiliar processes in the process tree. Check files for prevalence, their locations, and digital signatures.
4. Submit relevant files for deep analysis and review file behaviors.
5. Identify unusual system activity with system owners.
6. Scope the incident. Find related machines, network addresses, and files in the incident graph.
7. Contain and mitigate the breach. Stop suspicious processes, isolate affected machines, decommission compromised accounts or reset passwords, block IP addresses and URLs, and install security updates.
8. Contact your incident response team, or contact Microsoft support for investigation and remediation services.

Disclaimer: These guidelines are for reference only. They do not guarantee successful threat removal.

[Show less](#)

Alert process tree

mimikatz_trunk.zip detected as HackTool\Win64\Mikatz.exe by Antivirus

mimikatz_trunk.zip detected as HackTool\Win64\Mikatz.exe by Antivirus

mimikatz_trunk.zip detected as HackTool\Win64\Mikatz.exe by Antivirus

mimikatz_trunk.zip detected as HackTool\Win64\Mikatz.exe by Antivirus

Incidents > 12 > 'Mikatz' high-severity malware was detected

mimikatz_trunk.zip detected as HackTool\Win64\Mikatz.exe by Antivirus

Incident graph

Incident graph showing the relationship between the machine h401 and the files mimikatz_trunk.zip, mimikatz_trunk.zip, mimikatz_trunk.zip, mimikatz_trunk.zip, mimikatz_trunk.zip, and mimikatz_trunk.zip.

Artifact timeline

Description	First Observed	Details
04/04/2020		
11:09:21 mimikatz_trunk.zip	04/04/2020 11:08:39	0578eaf51ecb4687983b9c3d4e5d6c85f13e1c
11:06:47 mimikatz_trunk.zip	04/04/2020 11:06:39	505546b2a65f889a82300485409af9ec54ef6
11:06:47 mimikatz_trunk.zip	04/04/2020 11:06:39	6a315a02b7458202a917e58d0c0e695db450a589
11:06:47 mimikatz_trunk.zip	04/04/2020 11:06:39	879f1c108064b28b696a9f8e4d0c098b8a7f
11:06:47 mimikatz_trunk.zip	04/04/2020 11:06:39	a5f1b56615bdaa9803219813436712332001c

Actions' ı tıkladıktan sonra **Open Incident Page** kısmına geliyorum ve üç farklı alarm aldığımı görüyorum.

Incidents > 12

Alerts (3) Machines (1) Investigations (3) Evidence (8) Graph

Manage incident ? Consult a threat expert Comments and history

First activity	Title	Severity	Status	Linked by	Category	Machine	User	Classification	Last activity	Assigned to
4/4/20, 11:06 AM	'Mikatz' high-severity malware was detected	High	New	Same machine	Malware	h401		True alert	4/4/20, 11:09 AM	Unassigned
4/4/20, 11:06 AM	'Mikatz' hacktool was detected	Low	New	Same machine	Malware	h401		Not set	4/4/20, 11:06 AM	Unassigned
4/4/20, 11:06 AM	'Pyraner' malware was detected	Informational	New	Same machine	Malware	h401		Not set	4/4/20, 11:06 AM	hasan.dmdk

Evidence kısmında ise kanıt olarak nelerin şüpheli olarak algılandığını belirtmektedir.

Microsoft Defender Security Center

Machines list

Machine name	Domain	Risk level	Exposure level	OS platform	Windows 10 version
hd21	hd21	High	High	Windows Server 2016	
desktop-t2v8cuo	Workgroup	Medium	Medium	Windows 10	1909
desktop-ulvudu	Workgroup	No known risks	Low	Windows 10	1903
win81-client	hd21	No known risks	No data available	Windows 8.1	
microsoft	hd21	No known risks	High	Windows Server 2016	
ghost-surface	Workgroup	No known risks	Medium	Windows 10	1909
wac	hd21	No known risks	High	Windows Server 2016	

desktop-t2v8cuo

Risk level: Medium Exposure level: Medium

Open machine page Manage tags Isolate machine Run antivirus scan

Device details

Domain: Workgroup

OS: Windows 10 x64 (version 1909 build 18363)

Asset group: Windows10

Health state: Active

Data sensitivity: None

IP addresses: See IP addresses info

Resources: No resources found

Active alerts

6 active alerts in 6 incidents

Title	Severity	Status	Last activity
Unexpected behavior observed	Medium	New	4/17/20 3:07 PM
Automated investigation started	Informational	New	4/20/20 3:44 PM
Automated investigation started	Informational	New	4/24/20 9:39 AM
Automated investigation started	Informational	New	4/16/20 12:11 PM
Automated investigation started	Informational	New	4/17/20 4:18 PM

Örnek olması açısından canlı oturum başlatıyorum. **Process** komutu ile istemci makinamda çalışan süreçleri görüyorum.

Microsoft Defender Security Center

Machines > Live response #13 on DESKTOP-T2V8CUO

Command console Command log

Live response #13 on DESKTOP-T2V8CUO

Connected to "DESKTOP-T2V8CUO"

View machine details

SESSION GENERAL INFORMATION

Session created by: Hasan Dindik

Session started: 4/23/20 6:48 PM

Session ended: N/A

Duration: 13:50m

Command console

```
C:\> ps
```

Name	PID	Parent ID	Status	User Name	Cpu Cycles (K)	Memory (K)
Registry	144	4	Running	NT AUTHORITY\SYSTEM		
smss.exe	808	4	Running	NT AUTHORITY\SYSTEM		
csrss.exe	916	896	Running	NT AUTHORITY\SYSTEM		
wininit.exe	1016	896	Running	NT AUTHORITY\SYSTEM		
svchost.exe	848	1016	Running	NT AUTHORITY\SYSTEM		
lsass.exe	900	1016	Running	NT AUTHORITY\SYSTEM	489597401	12008
svchost.exe	1148	848	Running	NT AUTHORITY\SYSTEM	246418	920
svchost.exe	1176	848	Running	NT AUTHORITY\SYSTEM	1331310462	24296
fontdevhost.exe	1200	1016	Running	Font Driver Host\WFD-0	246222	1828
WUDFHost.exe	1232	848	Running	NT AUTHORITY\LOCAL SERVICE	124154582	4720
svchost.exe	1304	848	Running	NT AUTHORITY\LOCAL SERVICE	2315084	1448
svchost.exe	1388	848	Running	NT AUTHORITY\NETWORK SERVICE	754810989	13496
svchost.exe	1488	848	Running	NT AUTHORITY\SYSTEM	2316144180	3648
svchost.exe	1784	848	Running	NT AUTHORITY\SYSTEM	10134439	2848
svchost.exe	1792	848	Running	NT AUTHORITY\SYSTEM	310811	2880
svchost.exe	1800	848	Running	NT AUTHORITY\LOCAL SERVICE	4575002	2396
svchost.exe	1816	848	Running	NT AUTHORITY\SYSTEM	411538621	7960
svchost.exe	1916	848	Running	NT AUTHORITY\LOCAL SERVICE	514139	2384
svchost.exe	1956	848	Running	NT AUTHORITY\SYSTEM	2423307	5032
svchost.exe	2016	848	Running	NT AUTHORITY\SYSTEM	742145	2184
svchost.exe	2044	848	Running	NT AUTHORITY\LOCAL SERVICE	5004116	2944
svchost.exe	1612	848	Running	NT AUTHORITY\SYSTEM	5745502	3280
svchost.exe	2084	848	Running	NT AUTHORITY\LOCAL SERVICE	2040266467	19448
svchost.exe	2248	848	Running	NT AUTHORITY\SYSTEM	2701308	2304
lgfcdllservice.exe	2332	848	Running	NT AUTHORITY\SYSTEM	597105	1948
svchost.exe	2396	848	Running	NT AUTHORITY\LOCAL SERVICE	15062315	15088
svchost.exe	2496	848	Running	NT AUTHORITY\LOCAL SERVICE	75623708	2480
svchost.exe	2588	848	Running	NT AUTHORITY\LOCAL SERVICE	497097	1484
WVPlayer.Container.exe	2676	848	Running	NT AUTHORITY\SYSTEM	26991496	5372
svchost.exe	2696	848	Running	NT AUTHORITY\SYSTEM	347441134	7784
svchost.exe	2744	848	Running	NT AUTHORITY\NETWORK SERVICE	146319470	5396
svchost.exe	2824	848	Running	NT AUTHORITY\NETWORK SERVICE	253207902	3636
svchost.exe	2882	848	Running	NT AUTHORITY\SYSTEM	363827	1380
svchost.exe	2880	848	Running	NT AUTHORITY\SYSTEM	653644626	2796
svchost.exe	2824	848	Running	NT AUTHORITY\SYSTEM	127673696	2276
svchost.exe	2932	848	Running	NT AUTHORITY\LOCAL SERVICE	1216426	2372
svchost.exe	3016	848	Running	NT AUTHORITY\LOCAL SERVICE	3109040561	5000
Memory Compression	3032	4	Running	NT AUTHORITY\SYSTEM		
svchost.exe	3164	848	Running	NT AUTHORITY\LOCAL SERVICE	210318551	5060
svchost.exe	3268	848	Running	NT AUTHORITY\LOCAL SERVICE	9700187	1852
svchost.exe	3272	848	Running	NT AUTHORITY\LOCAL SERVICE	2444725	3028
svchost.exe	3428	848	Running	NT AUTHORITY\LOCAL SERVICE	147999718	2284
svchost.exe	3532	848	Running	NT AUTHORITY\SYSTEM	491519927	8184
svchost.exe	3536	848	Running	NT AUTHORITY\SYSTEM	13521930	4288
spoolsv.exe	3644	848	Running	NT AUTHORITY\SYSTEM	8552997	6704

Örneğin Yourphone isimli bir işlem gördüm ve bunun normal olmadığını varsayalım. **Processes 29688** komutu ile işleme ait detay bilgiye ulaşabiliyoruz.

Machines > Live response #13 on DESKTOP-T2V8CUO

Live response #13 on DESKTOP-T2V8CUO

Connected to "DESKTOP-T2V8CUO"

View machine details

SESSION GENERAL INFORMATION

Session created by
Hasan Dimdik

Session started
4/25/20, 6:48 PM

Session ended
N/A

Duration
2834m

Disconnect session Upload file to library

Command console Command log

```
C:\> cls

C:\> Fileinfo "c:\program files\windowsapps\microsoft.yourphone_1.20032.111.0_x64__8wekyb3d8bbwe\yourphone.exe"
{
  "last_raw_access_error": 0,
  "packed": null,
  "size": 19049472,
  "read_only": false,
  "executable_type": 34404,
  "na_verified": false,
  "hidden": false,
  "sha256": "1b8238c12f2d018b7be49ddc61ca509cfd5c8a226188f12327ecae3faad590",
  "mime_type": "application/x-madownload",
  "vendor": "",
  "digital_signature": null,
  "last_access_error": 0,
  "directory_type": [
    "Applications"
  ],
  "downloaded": false,
  "compressed": false,
  "path": "c:\program files\windowsapps\microsoft.yourphone_1.20032.111.0_x64__8wekyb3d8bbwe\yourphone.exe",
  "md5": "fba102f6d94c20f4ee3dfdd4abdb0e0",
  "sha1": "ee85714104b3c1fca3f8d172bb01a0f5e1b988",
  "created": "2020-04-17 17:20:11",
  "file_state_display": [
    "Default"
  ],
  "modified": "2020-04-17 17:20:38",
  "file_state": 0,
  "error": 0
}
```

Elbette üzerinde çalıştığımız, son kullanıcı bilgisayarı olduğu için herşeyin loglanması verilerin manupule edilebilmesinin de önüne geçmektedir.

securitycenter.windows.com/live-response/13/log

Microsoft Defender Security Center

Machines > Live response #13 on DESKTOP-T2V8CUO

Live response #13 on DESKTOP-T2V8CUO

Connected to "DESKTOP-T2V8CUO"

View machine details

SESSION GENERAL INFORMATION

Session created by
Hasan Dimdik

Session started
4/25/20, 6:48 PM

Session ended
N/A

Duration
3332m

Disconnect session Upload file to library

Command console Command log

Cmd start time	# Command	Parameters	Enriches	Duration	Status
4/25/20, 6:48 PM	3 - connect		0	2s	✓ Completed
4/25/20, 6:49 PM	4 - processes		250	10s	✓ Completed
4/25/20, 7:00 PM	5 - processes		254	10s	✓ Completed
4/25/20, 7:04 PM	6 - analyze	process 17182	0		✗ Failed
4/25/20, 7:04 PM	7 - processes		257	10s	✓ Completed
4/25/20, 7:06 PM	8 - analyze	process 29058	0		✗ Failed
4/25/20, 7:06 PM	9 - analyze	processes 29058	0		✗ Failed
4/25/20, 7:06 PM	10 - run	processes 29058	0		✗ Failed
4/25/20, 7:07 PM	11 - analyze	process 29058	0		✗ Failed
4/25/20, 7:07 PM	12 - processes	29058	1	5s	✓ Completed
4/25/20, 7:08 PM	13 - processes	29058	1	12s	✓ Completed
4/25/20, 7:11 PM	14 - analyze	process 29058	0		✗ Failed
4/25/20, 7:15 PM	15 - fileinfo	"c:\program files\windowsapps\microsoft.yourphone_1.20032.111.0_x64__8wekyb3d8bbwe\yourphone.exe"	1	18s	✓ Completed
4/25/20, 7:17 PM	16 - analyze	process 29058	1s		✗ Failed

Kaynak : <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/live-response-command-examples>

Auto Investigation & Remediation

Bu bölümü de teorik anlatmak yerine akılda kalması açısından örnekle anlatmak daha mantıklı olacaktır. Özellikle daha sofistike , karmaşık , akıllı tasarlanmış zararlıları/saldırıları analiz etmek için kullanılmaktadır. Bu özelliğin kullanımı ile ilgili OS seviyesinde kısıt mevcut. Desteklenen işletim sistemi aşağıdadır.

- Windows Server 2019
- Windows 10, version 1709 (OS Build 16299.1085 with **KB4493441**) or later
- Windows 10, version 1803 (OS Build 17134.704 with **KB4493464**) or later
- Later versions of Windows 10

Kaynak : <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/automated-investigations>

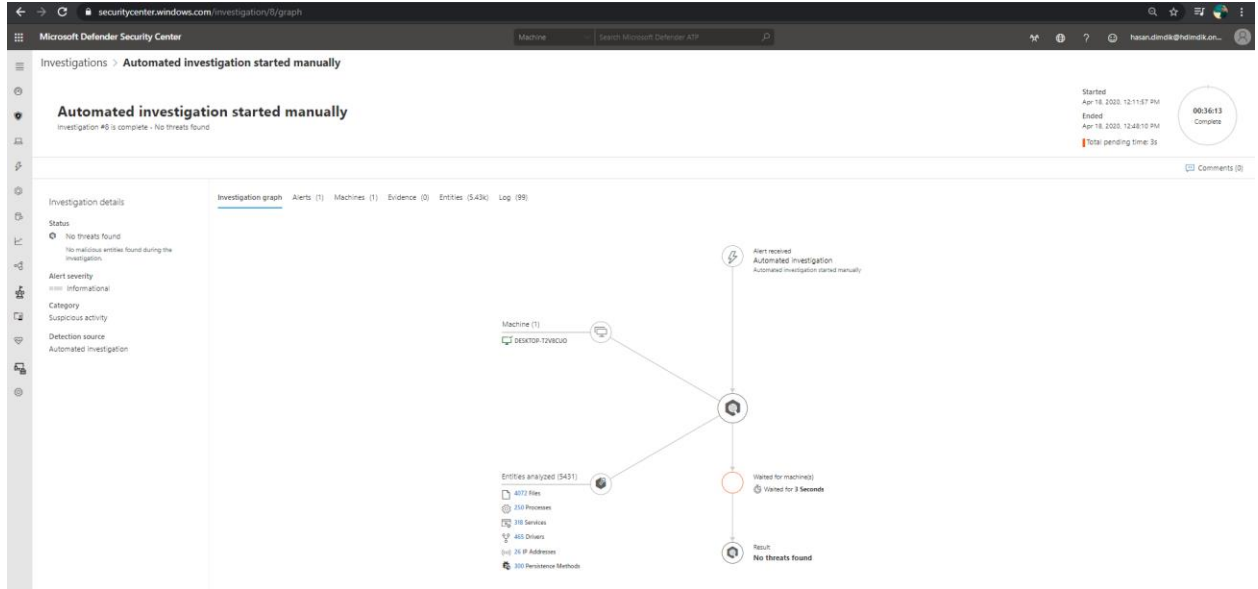
Örneğin aşağıdaki son kullanıcı bilgisayarında **Automated Investigation** başlattım.

The screenshot displays the Microsoft Defender Security Center web interface. On the left, a sidebar menu includes options like Dashboards, Security operations, Threat analytics, Incidents, Machines list, Alerts queue, Automated investigations, Advanced hunting, Reports, Partners & APIs, Threat & Vulnerability Management, Evaluation and tutorials, Service health, Configuration management, and Settings. The main area is titled 'Machines list' and shows a table of machines. The machine 'desktop-t2v8cuo' is selected, and its details are shown on the right. The details panel includes risk level (Medium), exposure level (Medium), and a list of active alerts. A red arrow points from the 'desktop-t2v8cuo' machine in the list to the 'Initiate Automated Investigation' button in the details panel. Below the alerts, there is a section for 'Logged on users (1)' showing 'dimgikhasan57' as a local admin.

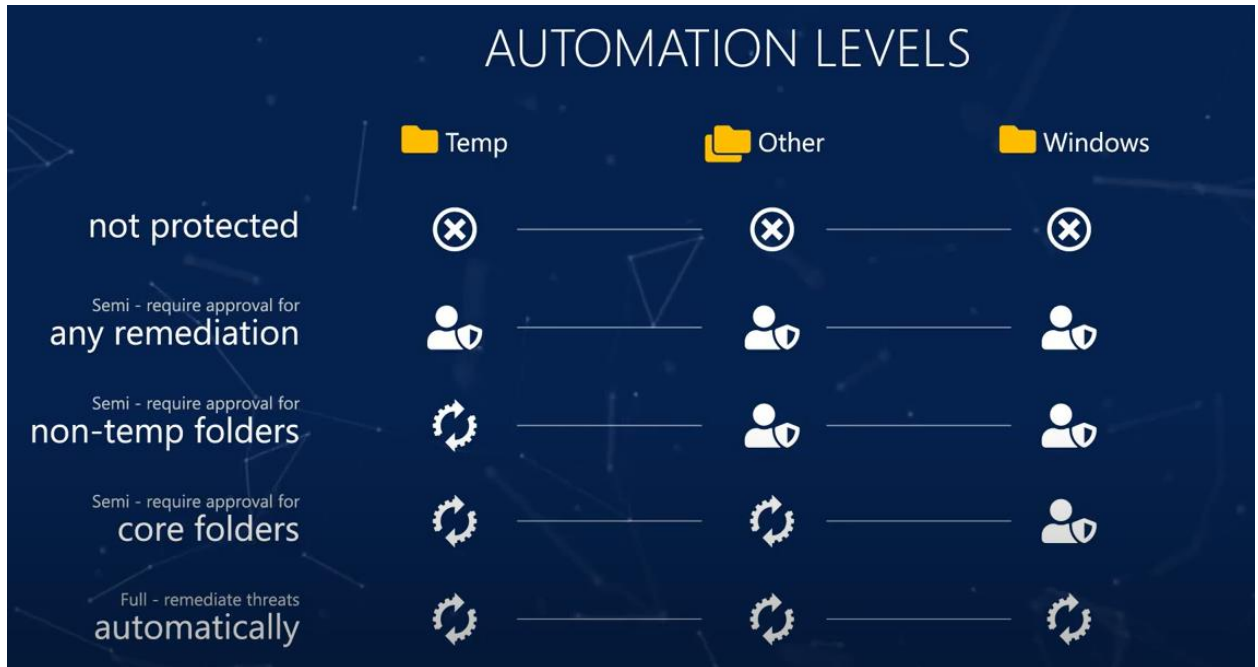
Machine name	Domain	Risk level	Exposure level	OS platform
hd01	hd.local	High	High	Windows Server 2016
desktop-t2v8cuo	Work...	Medium	Medium	Windows 10
desktop-ulluudu	Work...	No known risks	Medium	Windows 10
win81client	hd.local	No known risks	No data available	Windows 8.1
microsoftata	hd.local	No known risks	High	Windows Server 2016
ghost-surface	Work...	No known risks	Medium	Windows 10
wac	hd.local	No known risks	High	Windows Server 2016

Title	Severity	Status	Last activity
Unexpected behavior observed	Medium	New	4/17/20, 3:07 PM
Automated investigation started	Informational	New	4/17/20, 4:18 PM
Automated investigation started	Informational	New	4/4/20, 8:53 AM

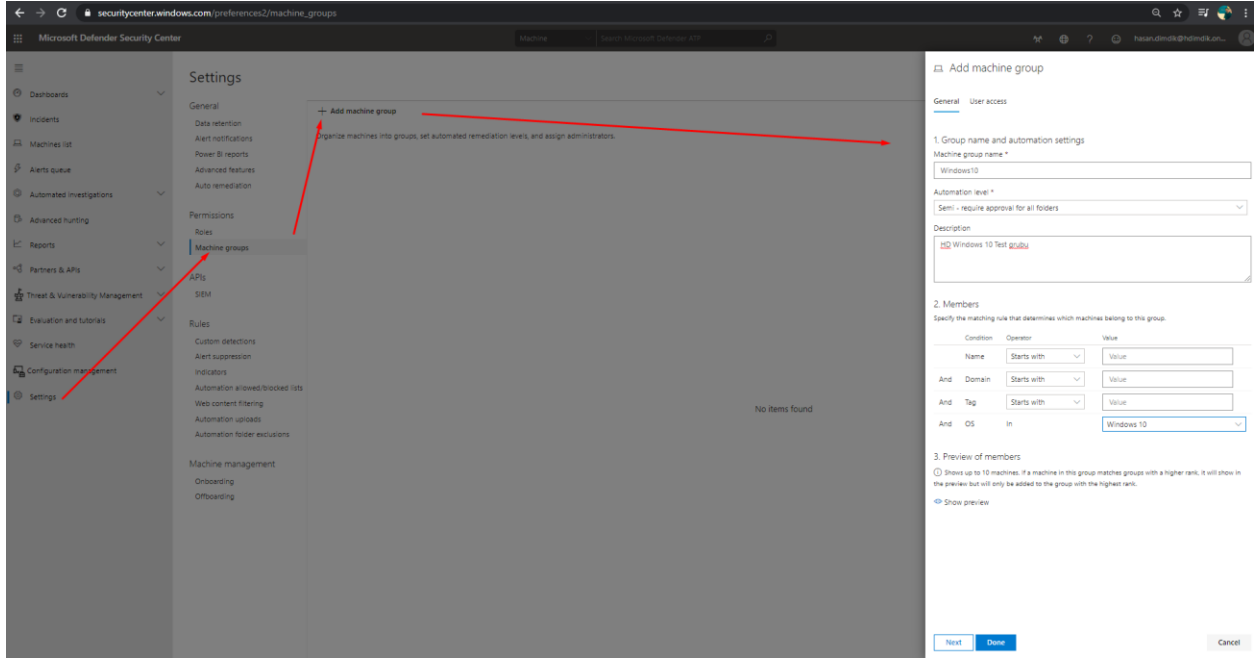
Bu bölümü kullanılmasının en temel sebeplerinden bir tanesi elbette hali hazırda bir zararlı yakalanmıştı veya alarm oluşmuştur ve araştırma başlatılabilir. Örneğimde zararlı olmadığı için daha sade sonuç getirdi. Bu noktadan sonra artık hangi processler başlamış, hangi registry değeri değiştirilmiş veya zararlı nerelere bulaşmış ve başka bir ortama bulaşmış mı gibi durumları görebiliyoruz.



Buraya kadar yaptığımız adımları manuel olarak başlattık fakat adında da anlaşıldığı üzere otomatik araştırmanın amacı insan faktörünü ortadan kaldırarak aksiyon aldırmaaktır. Aşağıdaki tabloda otomasyon seviyesini belirleyebiliyoruz. Burdaki ayrımı elbette yapımızdaki istemci veya sunucu kategorileri, kullanım amacına göre ayırıp gruplandırmak olası bir sorunun da önüne geçmesi açısından önem arz etmektedir.



Settings > Machines Groups sekmesinde **Add machine Group** diyerek gruplarımızı belirliyoruz ve **Automation Level** kısmında otomasyon seviyesini belirleyerek süreçlerin hangi oranda otomatize edileceğini de tanımlamış oluyoruz. Bu noktada yukarıdaki tablo referans olacaktır.

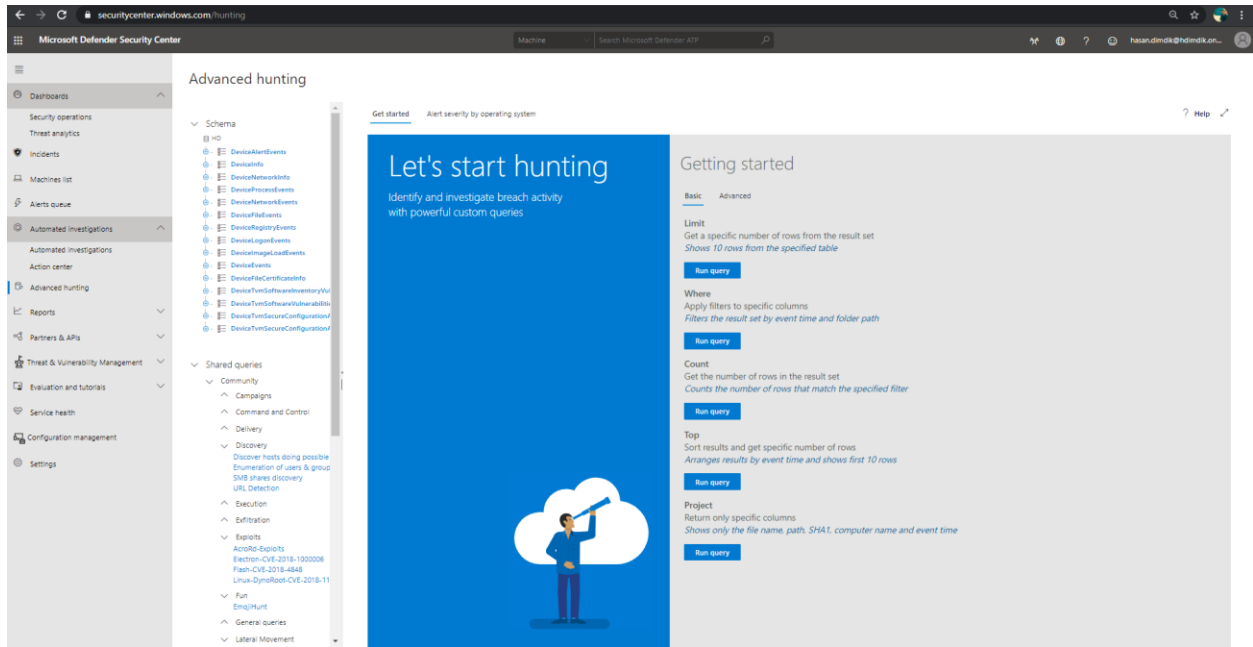


Advanced Hunting

Bu bölüm özellikle SOC ekiplerinin derinlemesine analiz için kullanacağı bir bölüm. Proaktif olarak yapıyı inceleme imkanı sunmaktadır. Şirketiniz için özel sorgular yazabilir veya hazır sorgular ile zararlı/tehdit analizini daha detaylı olarak yapabilirsiniz. Bir kaç örnekle Advanced Hunting özelliğini nasıl kullanabileceğimize bir bakalım.

Akıllara elbette şu soru gelmektedir. Sorgu diline hakim değilim veya bilgim yok, bu durumda ilgili bölümü nasıl kullanacağım. Hemen cevaplayalım,

Microsoft yeterli sayıda hazır sorguları zaten panele eklemiş durumda.

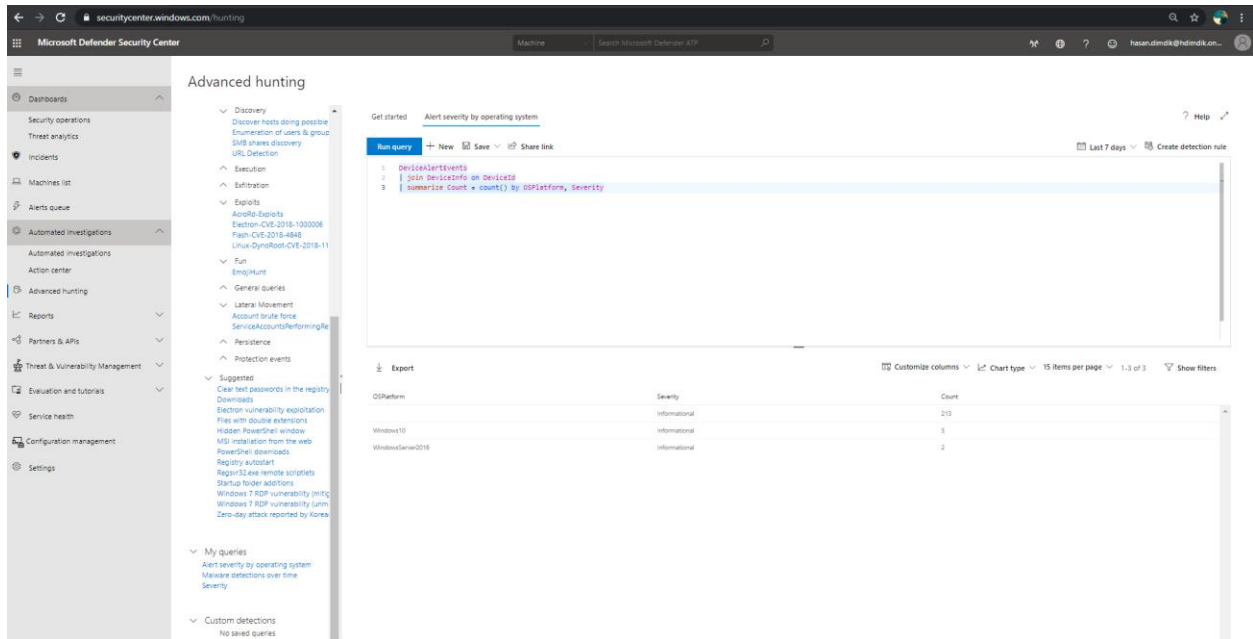


Örneğin aşağıdaki sorgu bize işletim sistemi özelinde alınan alarmları listeyecektir.

DeviceAlertEvents

| join DeviceInfo on DeviceId

| summarize Count = count() by OSPlatform, Severity

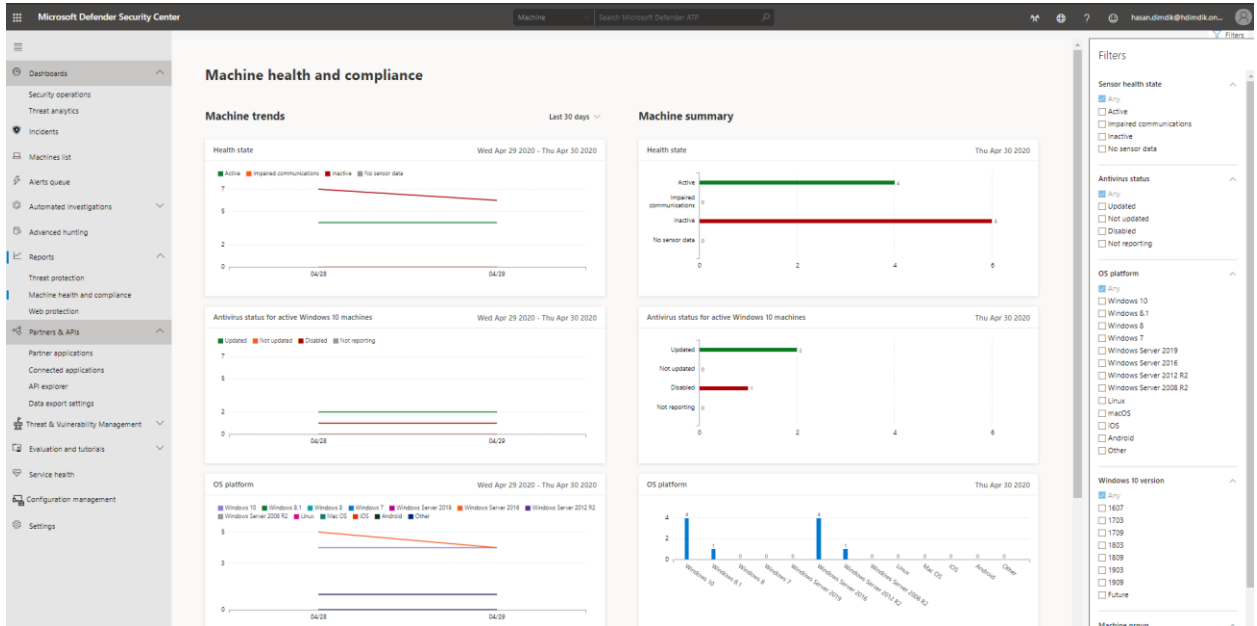
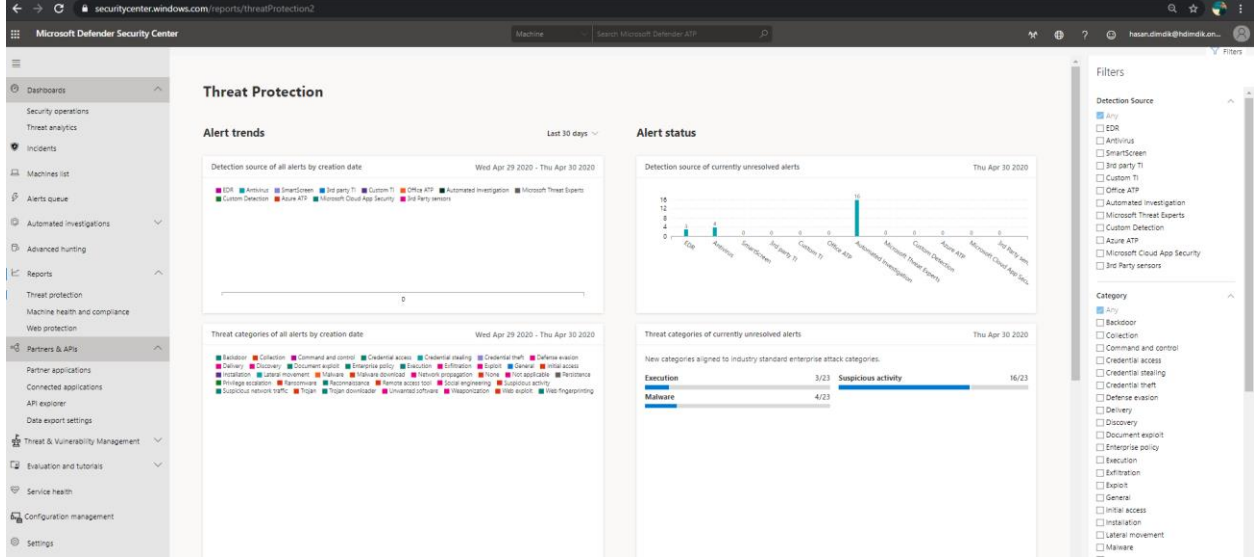


İkinci örneğimiz bize bilgisayar bazında indirilen dosya isimlerini listeleyecektir.

```
// Lists all the files downloaded using popular browsers.
DeviceFileEvents
| where Timestamp > ago(7d)
| where FolderPath !has "$Recycle.Bin"
| where
    // Edge
    InitiatingProcessFolderPath endswith @"windows\system32\browser_broker.exe"
    // Internet Explorer x64
    or InitiatingProcessFolderPath endswith @"program files\internet
explorer\iexplore.exe"
    // Internet Explorer x32
    or InitiatingProcessFolderPath endswith @"program files (x86)\internet
explorer\iexplore.exe"
    // Chrome
    or (InitiatingProcessFileName =~ "chrome.exe" and FileName endswith
"crdownload")
    // Firefox
    or (InitiatingProcessFileName =~ "firefox.exe" and (FileName !endswith ".js"
or FolderPath !has "profile"))
| project Timestamp, DeviceName, InitiatingProcessFileName, FileName, FolderPath
| top 100 by Timestamp
```

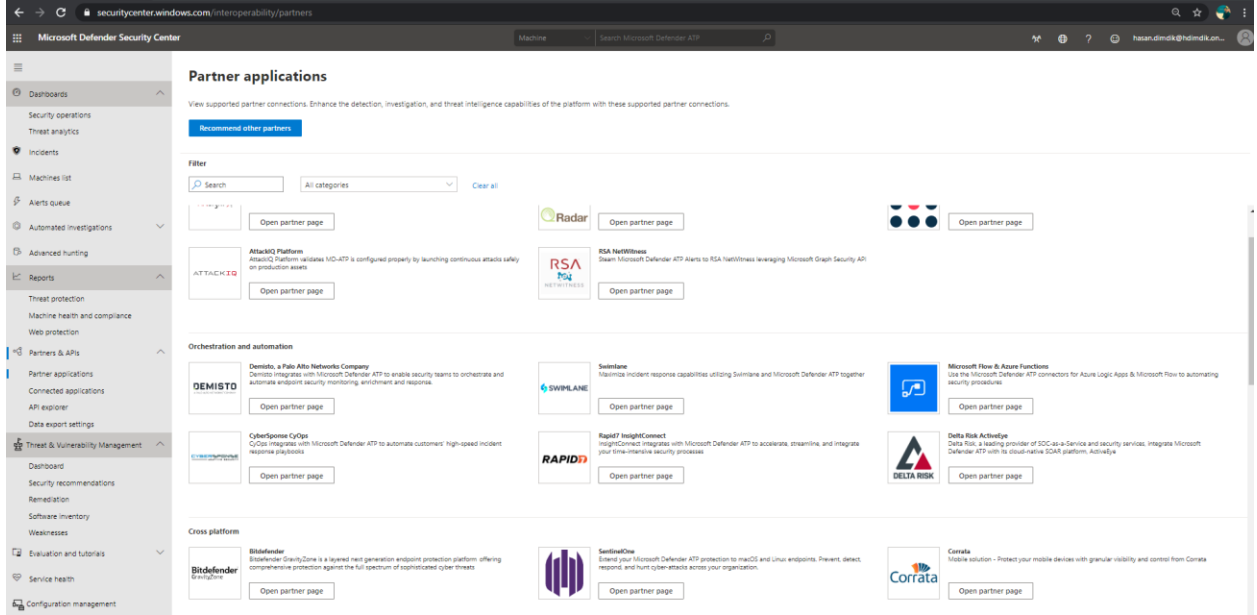

Reports

Adında anlaşılabacağı gibi yapımızda aktivitelerin raporlandığı , algılanan tehditlerin hangi teknoloji(EDR,Antivirüs vb) tarafından yakalandığı, tehditin alarm seviyesi gibi High Level olayları görsel olarak görebileceğimiz basit anlaşılır arayüze sahip olan raporlama arayüzünün olduğu alan diyebiliriz.



Partners & API

Bildiğiniz üzere Microsoft birden çok 3rd party vendor ile işbirliği yapıyor ve ilgili firmaların çözümleri ile Defender ATP'yi bağlayabiliyoruz.

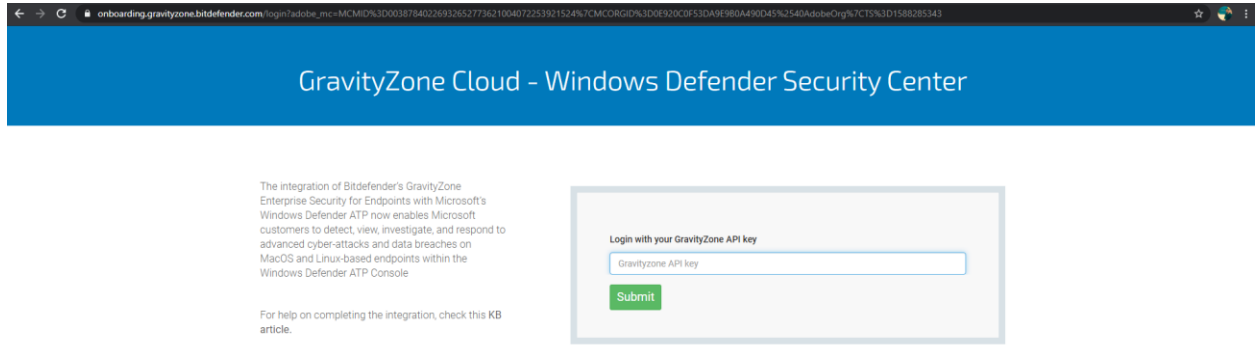


MDATP Bitdefender GravityZone Entegrasyonu

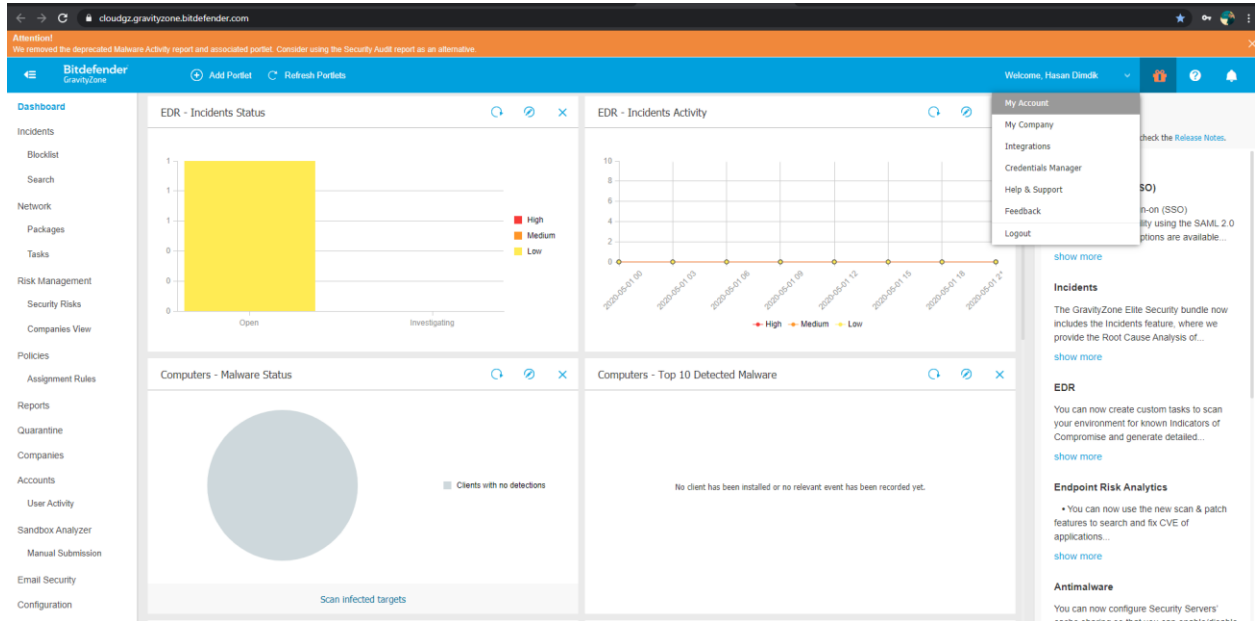
Bu bölümü daha iyi anlamak adına Bitdefender GravityZone ile nasıl bağlayabileceğimize değineceğim. Open Partner page tıklıyorum ve beni partner web sitesine yönlendiriyor.



Login butonuna tıkladığımda API key girmem gerektiğini belirtiyor.



İlgili API Key' i almak için Bitdefender portalında yer alan **My Account** bölümüne geliyorum.



API keys kısmında Add butonuna tıklıyorum.

cloudgz.gravityzone.bitdefender.com

Attention!
We removed the deprecated Malware Activity report and associated portal. Consider using the Security Audit report as an alternative.

Bitdefender GravityZone

Welcome, Hasan Dindik

Dashboard
Incidents
Blocklist
Search
Network
Packages
Tasks
Risk Management
Security Risks
Companies View
Policies
Assignment Rules
Reports
Quarantine
Companies
Accounts
User Activity
Sandbox Analyzer
Manual Submission
Email Security
Configuration

Timezone: (GMT +03:00) Europe/Istanbul
Language: English
Session Timeout: 15 min

Two-factor Authentication

The two-factor authentication secures your GravityZone account with an extra layer of protection. With each GravityZone login, in addition to your password, you will also need a code generated by the Google Authenticator app on your mobile device.

Two-factor authentication is disabled

[Enable](#)

Control Center API

Access URL: https://cloudgz.gravityzone.bitdefender.com/api

API keys

[Add](#) [Delete](#) [Refresh](#)

Key	Created
-----	---------

First Page -- Page 0 of 0 -- Last Page 20 0 items

What's New

For the full list of changes, check the [Release Notes](#).

MARCH 2020

Single Sign-On (SSO)

Added new single sign-on (SSO) authentication capability using the SAML 2.0 standard. The SSO options are available...

[show more](#)

Incidents

The GravityZone Elite Security bundle now includes the Incidents feature, where we provide the Root Cause Analysis of...

[show more](#)

EDR

You can now create custom tasks to scan your environment for known Indicators of Compromise and generate detailed...

[show more](#)

Endpoint Risk Analytics

- You can now use the new scan & patch features to search and fix CVE of applications...

[show more](#)

Antimalware

You can now configure Security Servers

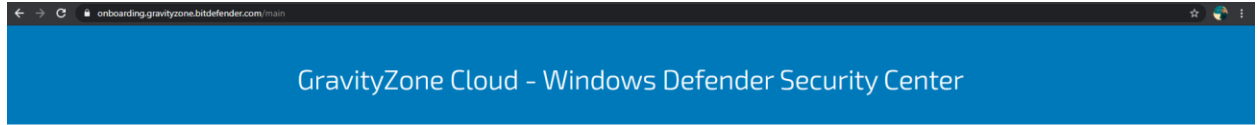
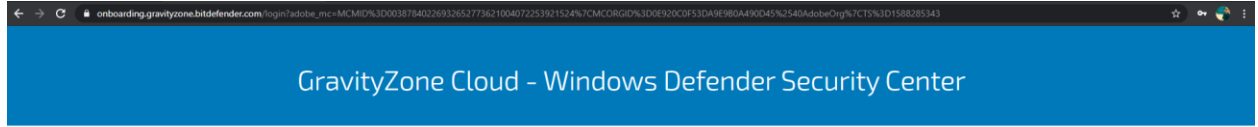
API key

Enabled APIs:

☒ Companies API	☒ Reports API
☒ Licensing API	☒ Accounts API
☒ Packages API	☒ Incidents API
☒ Network API	☒ Quarantine API
☒ Integrations API	☒ Event Push Service API
☒ Policies API	

[Save](#) [Cancel](#)

İlgili ayarları kaydettikten sonra API key ini portala kopyalayıp Submit butonuna tıklıyorum.



Bu adımla birlikte entegrasyonu tamamlamış oluyoruz. Peki bize nasıl bir faydası olacak? Özellikle Linux, android veya MacOS işletim sistemi kullanıyorsanız ilgili entegrasyonla birlikte bu işletim sistemleri üzerindeki zararlı faaliyetleri veya virüs bulunması durumunda Security Center içerisinde de görebilme kabiliyeti kazanıyoruz (Detect and Response)

Kaynak : <https://www.bitdefender.com/support/bitdefender-gravityzone-and-microsoft-windows-defender-atp-integration-1987.html>

MDATP Azure Sentinel Entegrasyonu

Azure Sentinel portalına eriştikten sonra **Data Connectors** sekmesine geliyorum ve **open connector page** butonunu tıklıyorum.

The screenshot shows the Azure Sentinel Data Connectors page. The main table lists various connectors, including Forcepoint ULP, Forcepoint NGFW, Fortinet, Microsoft Cloud App Security, Microsoft Defender Advanced Threat Protection (Preview), Microsoft web application firewall (WAF), Office 365, One Identity Safeguard, and Palo Alto Networks. The 'Microsoft Defender Advanced Threat Protection (Preview)' connector is selected. The sidebar on the right provides details for this connector, including a description, last data received time, and a line graph showing data received over time. A red arrow points to the 'Open connector page' button at the bottom of the sidebar.

Ön gereksinimleri sağladığımıza emin oluyoruz ve **Connect** butonuna basarak entegrasyonu tamamlıyoruz. (Ben daha önceden aktif ettiğim için Disconnect butonu gözükmemektedir)

The screenshot shows the configuration page for the 'Microsoft Defender Advanced Threat Protection (Preview)' connector. The page is divided into two main sections: 'Prerequisites' and 'Configuration'. The 'Prerequisites' section is highlighted with a red box and lists the following requirements:

- ✓ **Workspace:** read and write permissions are required.
- ✓ **Tenant Permissions:** required 'Global Administrator' or 'Security Administrator' on the workspace's tenant.
- ✓ **License:** required Microsoft Defender Advanced Threat Protection.

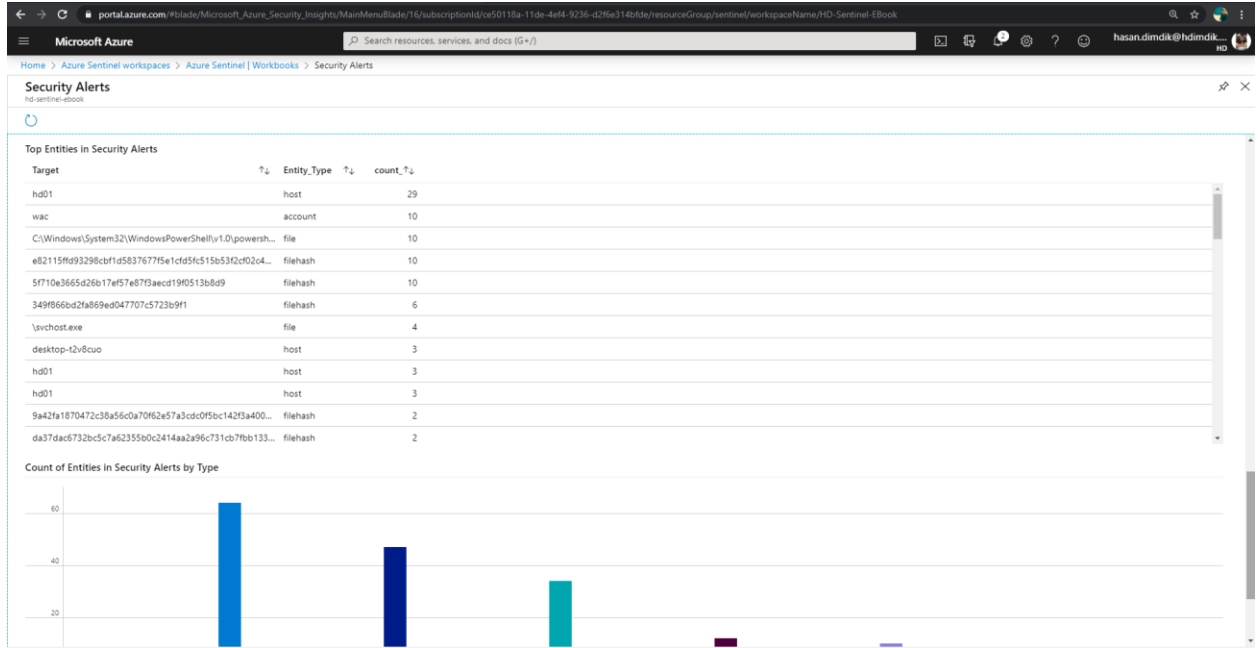
The 'Configuration' section includes instructions on how to connect the connector to Azure Sentinel. A red arrow points to the 'Disconnect' button, which is currently disabled.

Workbooks lar bizim dashboard larımız, kontrol etmek için **Workbooks** sekmesine geliyorum.

The screenshot shows the Microsoft Azure Sentinel Workbooks interface. The left sidebar contains a navigation menu with categories like General, Threat management, and Configuration. The 'Workbooks' item is highlighted. The main content area shows a list of workbooks under the 'Templates' tab. A red arrow points from the 'Workbooks' menu item to the 'Security Alerts' workbook. Another red arrow points from the 'Security Alerts' workbook to a preview of the 'Security Alerts' dashboard on the right side of the page.

İlgili alarmların artık Azure Sentinele geldiğini gözlemliyorum.

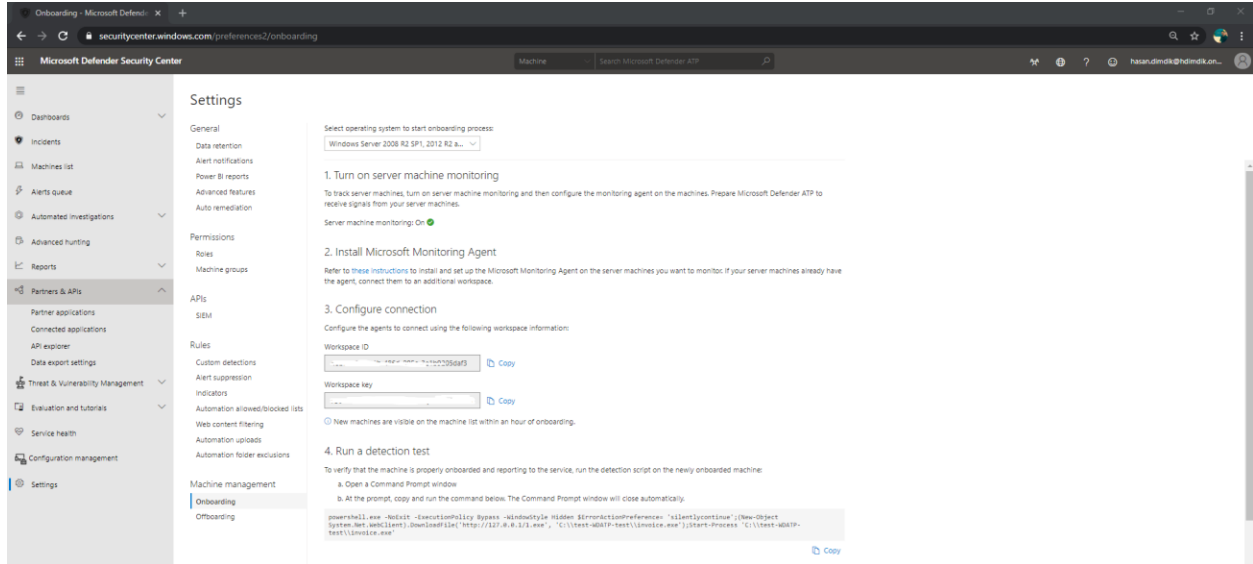
The screenshot shows the Microsoft Azure Sentinel Security Alerts Dashboard. The dashboard displays a summary of security alerts by severity and by product. The 'Security Alerts by Severity' section shows counts for All (47), High (11), Medium (14), Low (4), and Informational (18). The 'Security Alerts by Product' section shows counts for All (47) and Microsoft Defender Adv... (47).



Settings

Windows Server 2008 R2 SP1, 2012 R2, 2016 Onboarding

Yazım içerisinde iki temel parçanın olduğuna değinmiştim. İlki mma ajanları. Bu bize EDR özelliği kazandırıyor. İlk yapmamız gereken ilgili ajanları endpoint lerimize kurmak olacak. Büyük bir yapıda elbette tek tek kuramayacağımıza göre merkezi olarak dağıtmamız mantıklı olacaktır. Ben örneğimde SCCM kullanacağım. (Tüm adımları göstermeyeceğim) İlk olarak portala eriştikten sonra **Setings** sekmesi içerisinde **Onboarding** sekmesini tıklıyorum. **Configuration connection** içerisindeki parametreleri bir yere kopyalıyoruz.



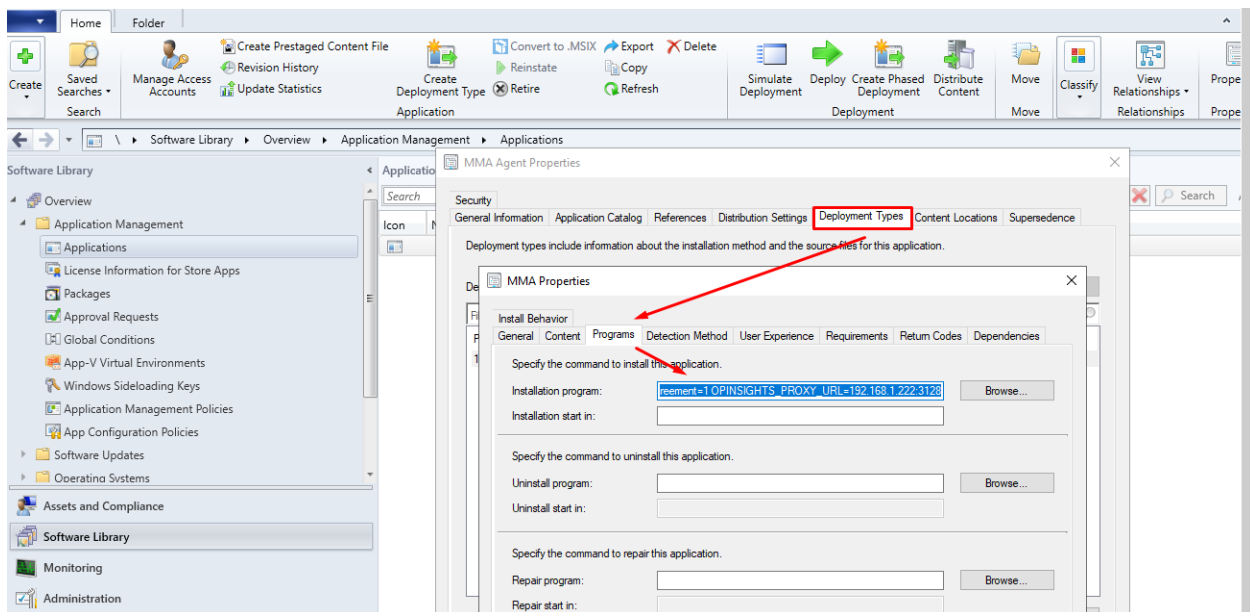
SCCM konsolunu açtıktan sonra applications sekmesine gelerek işlemlere başlıyoruz. **Deployment Types** olarak **Script** seçmiştik. **Programs** sekmesine geliyoruz **Installation progress** kısmına aşağıdaki komutu yapıştırıyoruz. Kırmızı alanları editlemeyi unutmayınız. Demo ortamımda internete proxy üzerinden çıktığım için komuta dahil ettim.

msiexec /i MMASetup-AMD64.exe /qn NOAPM=1

ADD_OPINSIGHTS_WORKSPACE_AZURE_CLOUD_TYPE=0 OPINSIGHTS_WORKSPACE_ID=XXXXXXXXXX

OPINSIGHTS_WORKSPACE_KEY=XXXXXXXXXXXXX AcceptEndUserLicenseAgreement=1

OPINSIGHTS_PROXY_URL=192.168.1.222:3128



Detection Rule olarak **Windows Installer** seçip ilgili parametreyi ekliyorum ve geriye kalan işin makyaj kısımlarını tamamlıyoruz 😊

{742D699D-56EB-49CC-A04A-317DE01F31CD}

Detection Rule

Create a rule that indicates the presence of this application.

Setting Type: Windows Installer

Specify an MSI product code as the basis for this rule.

Product code: {742D699D-56EB-49CC-A04A-317DE01F31CD} Browse ...

☒ This MSI product code must exist on the target system to indicate presence of this application

☐ This MSI product code must exist on the target system and the following condition must be met to indicate presence of this application:

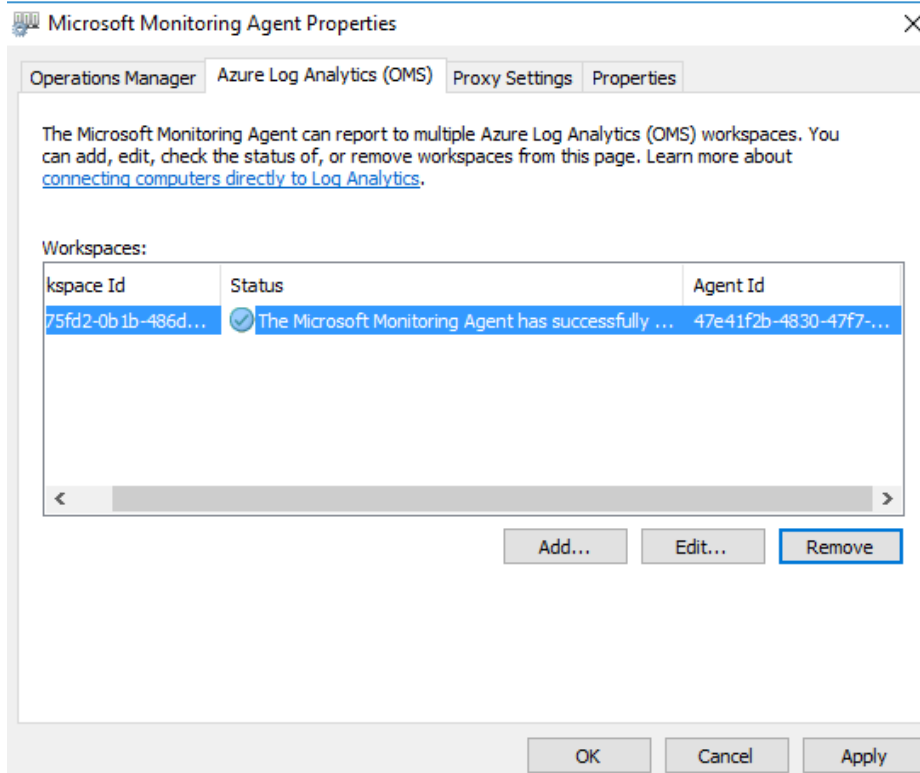
MSI Property: Version

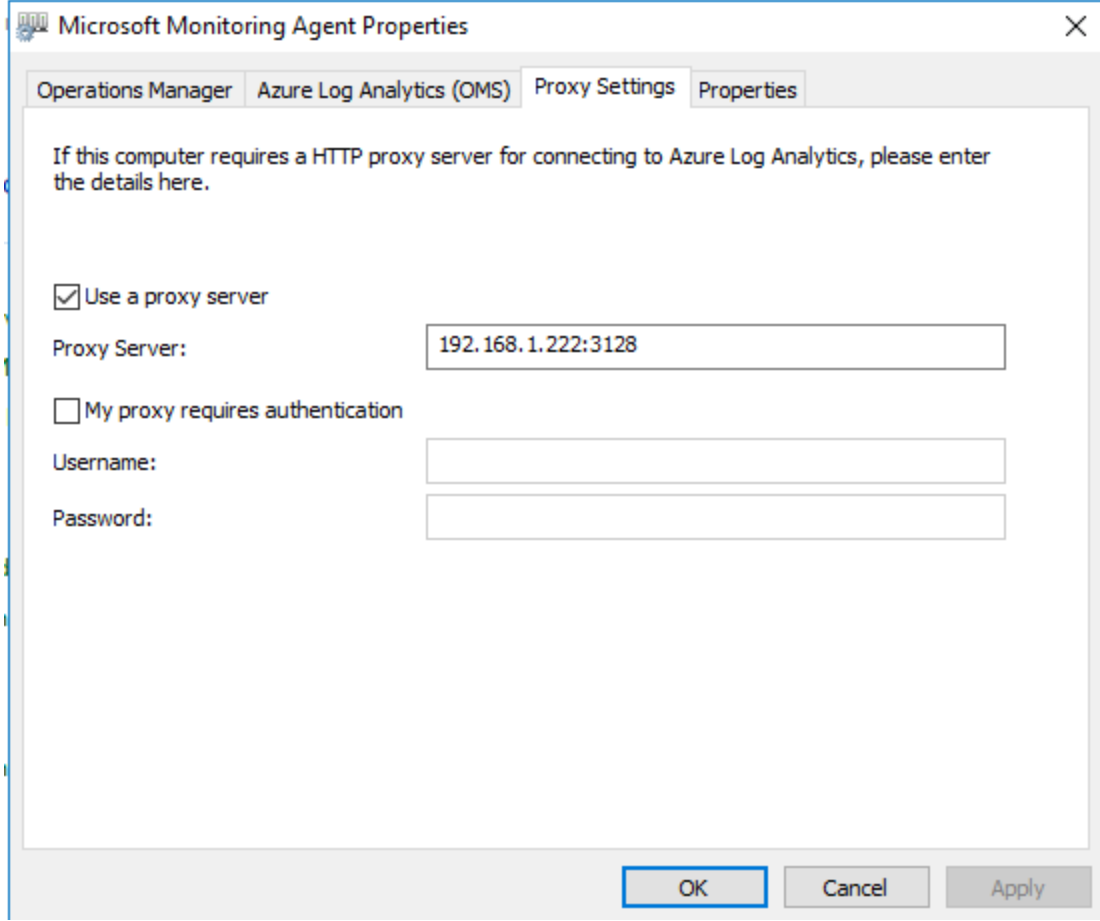
Operator: Equals

Value:

OK Cancel

Son olarak ilgili collection lara mma agent ımı dağıtıyorum.





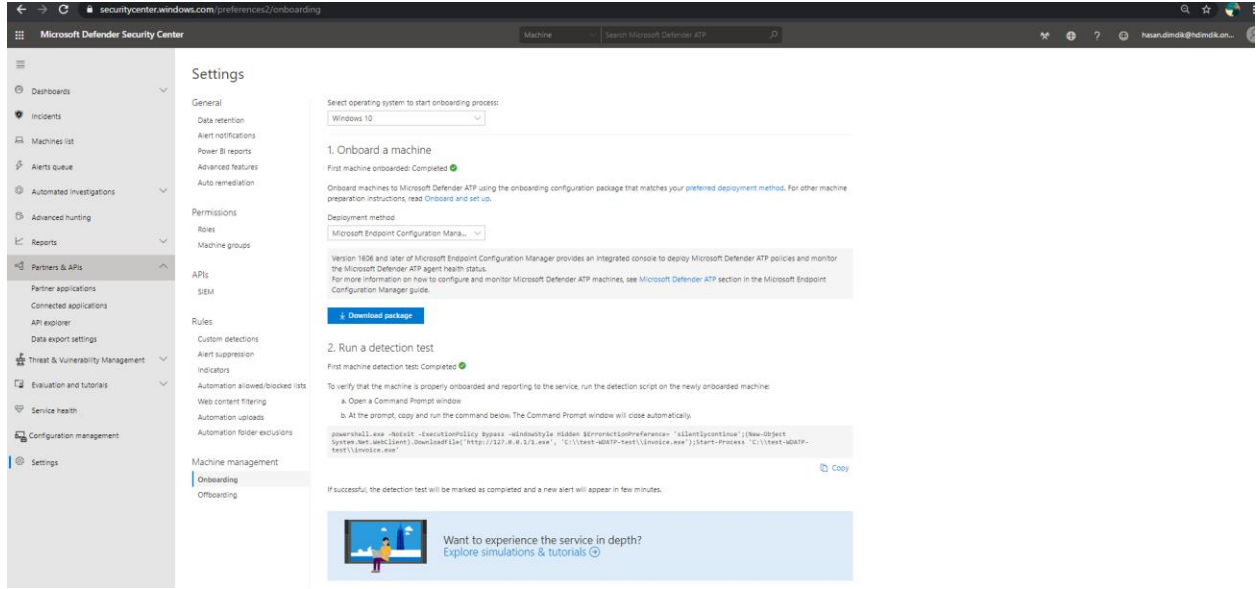
Eğer yapınızda sunucularınız internete direk olarak çıkmıyorsa OMS Gateway yapılandırmamız gerekmektedir. Gerekli port ve URL leri aşağıdaki dökümandan okuyabilirsiniz.

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/log-analytics-agent>

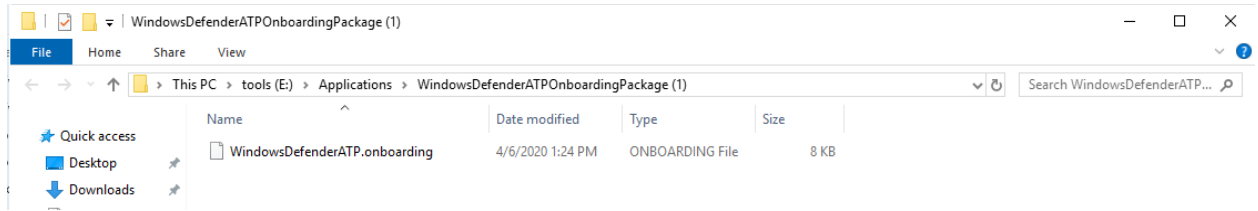
Aynı adımlar Windows 7 SP1 ve Windows 8.1 içinde geçerli. Yazının ilerleyen bölümlerinde Windows Server 2008 R2 SP1, 2012 R2 için SCEP yapılandırmasını göreceğiz. Şimdilik burada bırakıyorum.

Windows 10 Onboarding

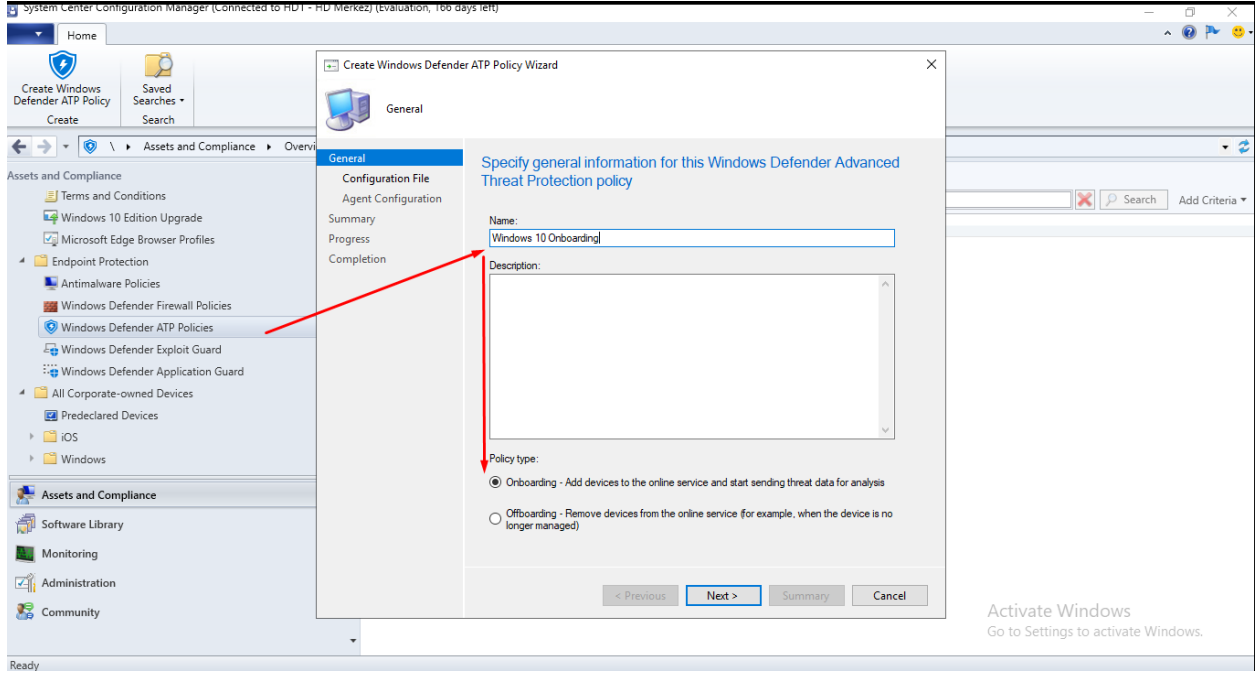
Bu adımda işlemler biraz daha basitleşiyor. İlgili ajanları group policy veya SCCM ile dağıtabiliyoruz. Örneğimde SCCM ile nasıl onboarding işlemi tamamlayabileceğimizi göstereceğim. Panelimde Onboarding sekmesini açıyorum ve işletim sistemi olarak **Windows 10** u seçip **Download package** ile gerekli onboarding yükleme dosyasını indiriyorum ve SCCM sunucuma kopyalıyorum.



Dosyanın uzantısının .onboarding olduğunu kontrol ediniz.



SCCM konsolumuzu açtıktan sonra asset and Compliance sekmesi içerisinde yer alan Windows Defender ATP Policies sekmesini sağ tıklayıp **Create Windows Defender ATP Policy** diyerek işlemimize başlıyoruz. Onboarding yapacağımız için onboarding seçeneğini seçip devam ediyorum.



Portaldan indirmiş olduğum onboarding dosyasını gösteriyorum ve devam ediyorum.

Create Windows Defender ATP Policy Wizard

Configuration File

General
Configuration File
Agent Configuration
Summary
Progress
Completion

Import the Windows Defender Advanced Threat Protection configuration file

An administrator of your organization's Windows Defender Advanced Threat Protection online service tenant must export this configuration file for import to this policy. Delete the file after importing or store it in a secure location.

Configuration File:
E:\Applications\WindowsDefenderATPOnboardingPackage (1)\Windo Browse...

Organization ID:
2-2dd363882c55

< Previous Next > Summary Cancel

Bu bölüm tamamen yapınız ile alakalı. Analiz dosyalarının cloud a gönderilmesine izin verecek miyiz gibi ayarları yapıyoruz . İşlemi tamamladıktan sonra Windows 10 istemcilerimin olduğu collection a dağıtıyorum.

Create Windows Defender ATP Policy Wizard

Agent Configuration

General
Configuration File
Agent Configuration
Summary
Progress
Completion

Specify the Windows Defender Advanced Threat Protection agent configuration settings

Specify which file samples are shared for analysis by the Windows Defender ATP online service: All file types

Telemetry reporting frequency: Normal

< Previous Next > Summary Cancel

Activate
Go to Setti

Onboarding işleminin başarılı olması için diagtrack servisinin AUTO_START olması gerekmektedir. Sorun yaşıyorsanız bu bilgi bir köşede dursun 😊


```
Command Prompt
Microsoft Windows [Version 10.0.18363.778]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\ghost>sc qc diagtrack
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: diagtrack
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE           : 2    AUTO_START
        ERROR_CONTROL         : 1    NORMAL
        BINARY_PATH_NAME      : C:\WINDOWS\System32\svchost.exe -k utcsvc -p
        LOAD_ORDER_GROUP      :
        TAG                   : 0
        DISPLAY_NAME          : Connected User Experiences and Telemetry
        DEPENDENCIES          : RpcSs
        SERVICE_START_NAME    : LocalSystem

C:\Users\ghost>
```

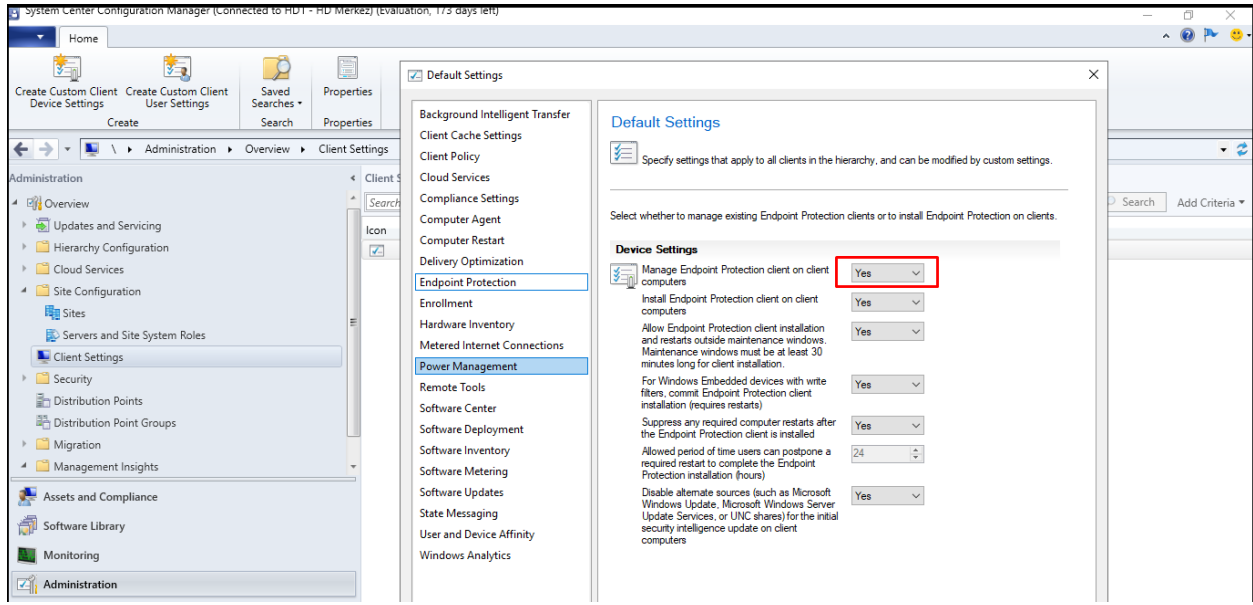
Buraya kadar olan kısımda Onboarding işlemlerini tamamladık. EDR çözümümüz artık çalışır durumda.

System Center Configuration Manager SCEP Yapılandırması

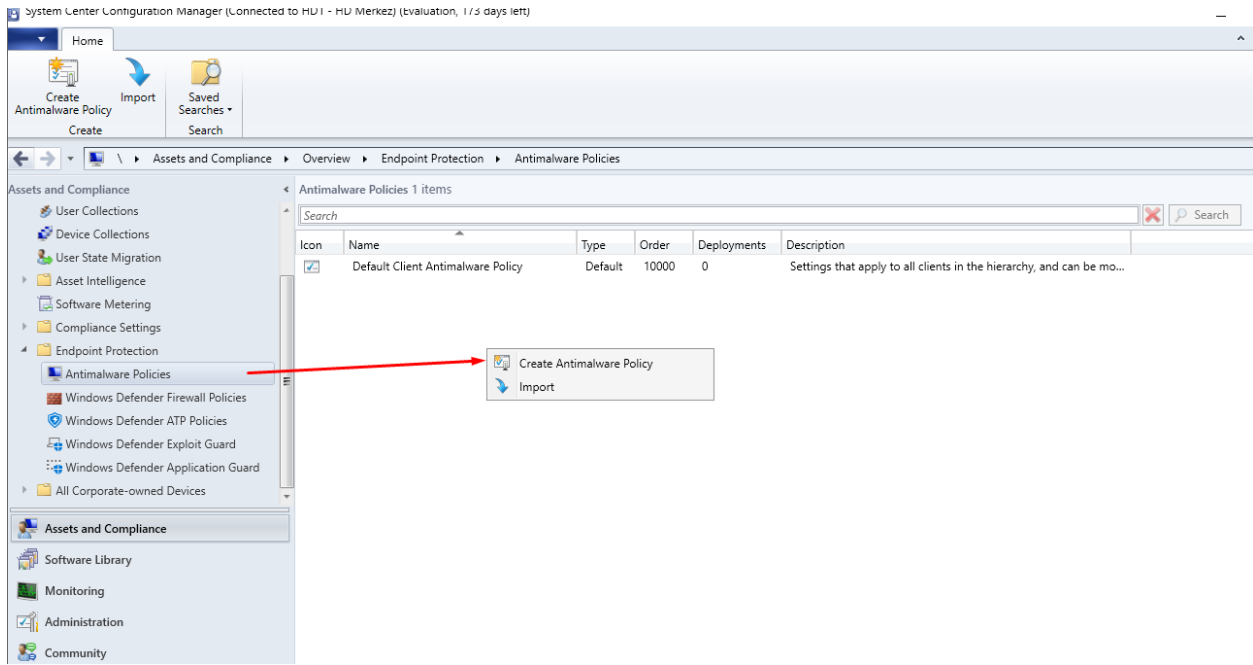
Giriş bölümünde **Attack Surface Reduction** kısmını SCCM ile yapılandıracağımızdan bahsetmiştik. MDATP ve SCEP konularına hakim değilseniz neden buna ihtiyaç var sorusu akıllara gelecektir. Hemen bu soruyu cevaplayalım. Yapıyı incelediğimiz zaman EDR teknolojisinden faydalanmak için MMA ajanlarını sunucularımıza yüklememiz gerekiyor, bu sayede MDATP portalında sunucularımızı görebiliyoruz ve yukarıda detaylıca bahsettiğimiz CVE açıklığı varmı sunucu envanteri gibi verileri artık raporlayabilir hale geliyoruz. Fakat bu bize koruma sağlamamaktadır. Bu noktada da yapıyı ikiye ayırıyoruz. Eğer sunucu tarafında Windows Server 2016 veya üstü, istemci tarafında ise Windows 10 OS leriniz mevcut ise varsayılan olarak Defender ATP gelmektedir ve Defender ATP ajanı aktif ise koruma sağlayabiliyoruz. Fakat bu versiyonlardan düşük işletim sistemi sürümlerine sahipseniz System Center Endpoint Manager' dan yararlanmamamız gerekiyor.

Not: Kafa karışıklığına sebep olmamak için her bir konu başlığında ilgili özelliğin desteklediği işletim sistemlerini paylaşacağım. Lütfen ilgili linkleri dikkatlice okuyunuz. (Özellikle Windows Defender Exploit Guard bölümündeki paylaştığım kaynakları dikkatlice okuyunuz)

SCCM Portalımıza eriştikten sonra yapılandırmamıza **Client Settings'** den başlıyoruz. **Endpoint Protection** sekmesine geliyoruz. **Manage Endpoint Protection client on client computers** ayarını **yes** olarak değiştiriyoruz.



İkinci adımda ise **Antimalware Policy** oluşturuyoruz.



Tam koruma sağlaması açısından tüm seçenekleri seçiyorum.

Create Antimalware Policy

General

Scheduled scans

Scan settings

Default actions

Real-time protection

Exclusion settings

Advanced

Threat overrides

Cloud Protection Service

Security Intelligence updates

Endpoint Protection Antimalware Policy

Specify the name and a description for this Endpoint Protection antimalware policy. The settings defined in this policy override the default settings when this policy is assigned to a collection.

Name:

Description:

☒ Scheduled scans

☒ Scan settings

☒ Default actions

☒ Real-time protection

☒ Exclusion settings

☒ Advanced

☒ Threat overrides

☒ Cloud Protection Service

☒ Security Intelligence updates

OK

Cancel

Page 48

AntiMalware Policy

Desteklenen sürümler (Server,Client)

System Center Configuration Manager (SCCM) Current Branch (CB)

Microsoft Defender Antivirus

- Windows Server 2019
- Windows Server 2016
- Windows 10

System Center Endpoint Protection

- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1
- Windows Server 2008 SP2
- Windows 8.1
- Windows 8
- Windows 7 SP1
- Windows Vista

Scheduled Scan sekmesinde tarama tipini, gününü , saatini CPU kullanımını kısıtlama gibi ayarları yapabiliyoruz.

Create Antimalware Policy

General

Scheduled scans

Scan settings

Default actions

Real-time protection

Exclusion settings

Advanced

Threat overrides

Cloud Protection Service

Security Intelligence updates

Scheduled scans

The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.

Specify scheduled scan settings

Run a scheduled scan on client computers: Yes

Scan type: Full Scan

Scan day: Saturday

Scan time: 3:00 AM

Run a daily quick scan on client computers: No

Daily quick scan schedule time: 2:00 AM

Check for the latest security intelligence updates before running a scan: Yes

Start a scheduled scan only when the computer is idle: Yes

Force a scan of the selected scan type if client computer is offline during two or more scheduled scans: Yes

Limit CPU usage during scans to (%): 30

OK Cancel

Scan Settings sekmesinde nelerin taranacağı(harici cihazlar, arşiv alanları, e mail içerisindeki ekler, network dosyaları vb..) kullanıcılara kontrol verip vermeyeceğimizi belirleyebiliyoruz.

Create Antimalware Policy

General

Scheduled scans

Scan settings

Default actions

Real-time protection

Exclusion settings

Advanced

Threat overrides

Cloud Protection Service

Security Intelligence updates

Scan settings

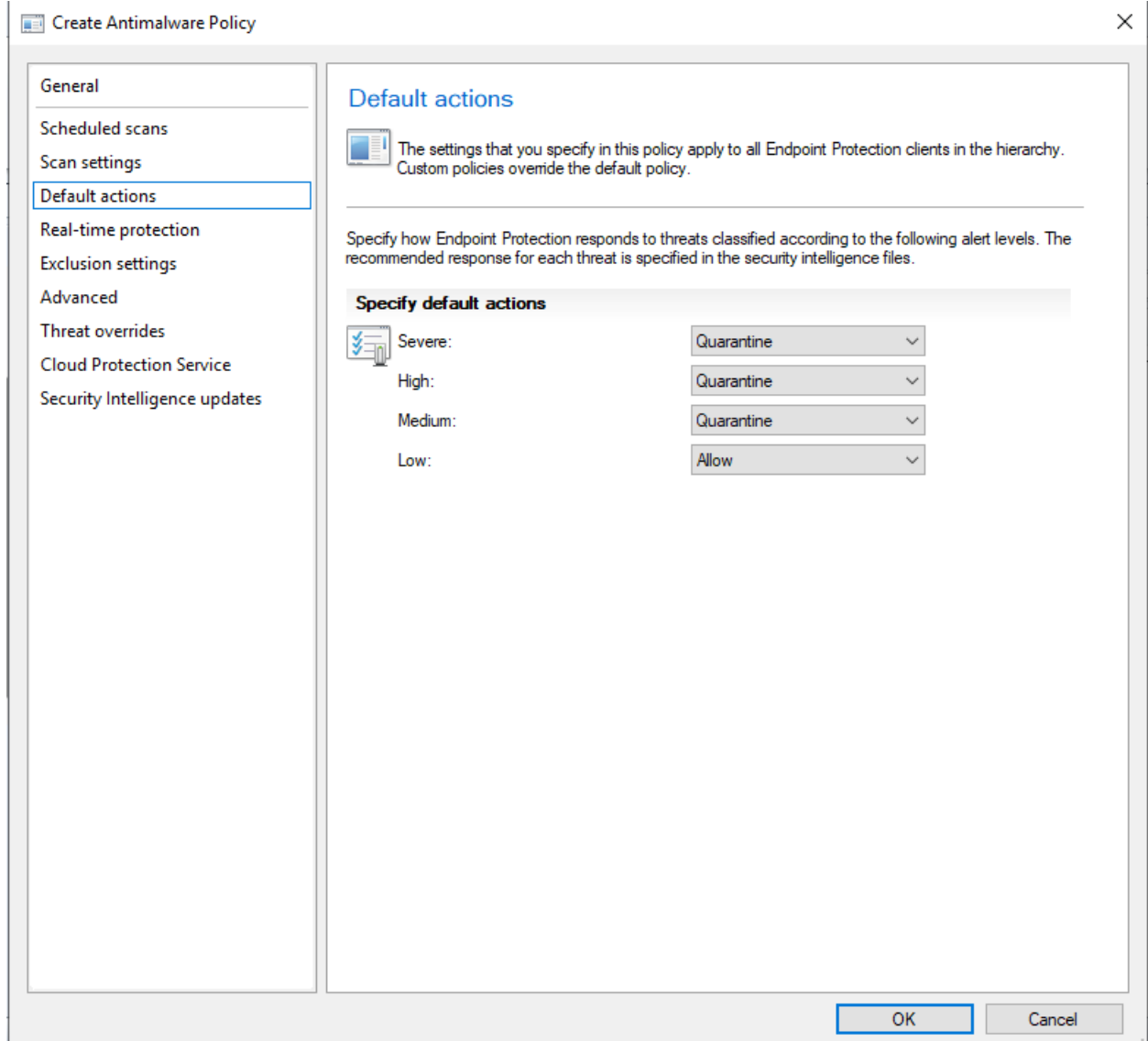
The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.

Specify scan settings

Scan email and email attachments:	Yes
Scan removable storage devices such as USB drives:	Yes
Scan network files:	Yes
Scan mapped network drives when running a full scan:	Yes
Scan archived files:	Yes
Allow users to configure CPU usage during scans:	No
User control of scheduled scans:	No control

OK Cancel

Default Action sekmesinde zararlı yakalandığı zaman nasıl aksiyon alınacağını belirliyoruz.



Real-time protection ayarlarımız içerisinde dikkatlice yapılandırmamız gereken sekmelerden en kritik olanı diyebilirim. Endpoint lerimizdeki dosya veya uygulamaların aktivitesini, davranışsal analizi aktif edebileceğimiz , Network tabanlı exploit lere karşı koruma sağladığımız ve gelen/ giden dosyaların taranıp taranmayacağını belirleyeceğimiz ayarların bulunduğu bölümdür.

Create Antimalware Policy

General

Scheduled scans

Scan settings

Default actions

Real-time protection

Exclusion settings

Advanced

Threat overrides

Cloud Protection Service

Security Intelligence updates

Real-time protection

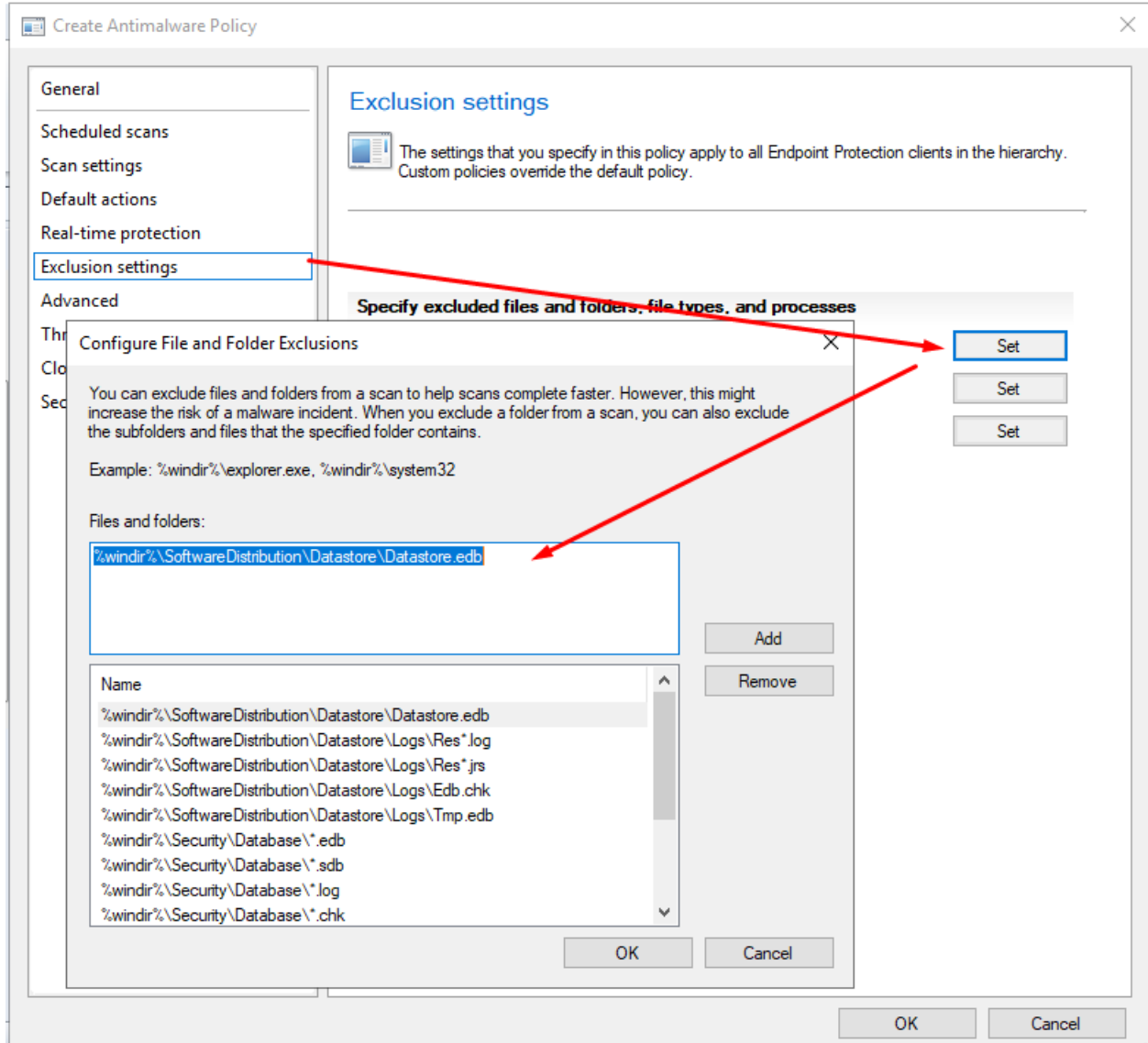
The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.

Specify real-time protection settings

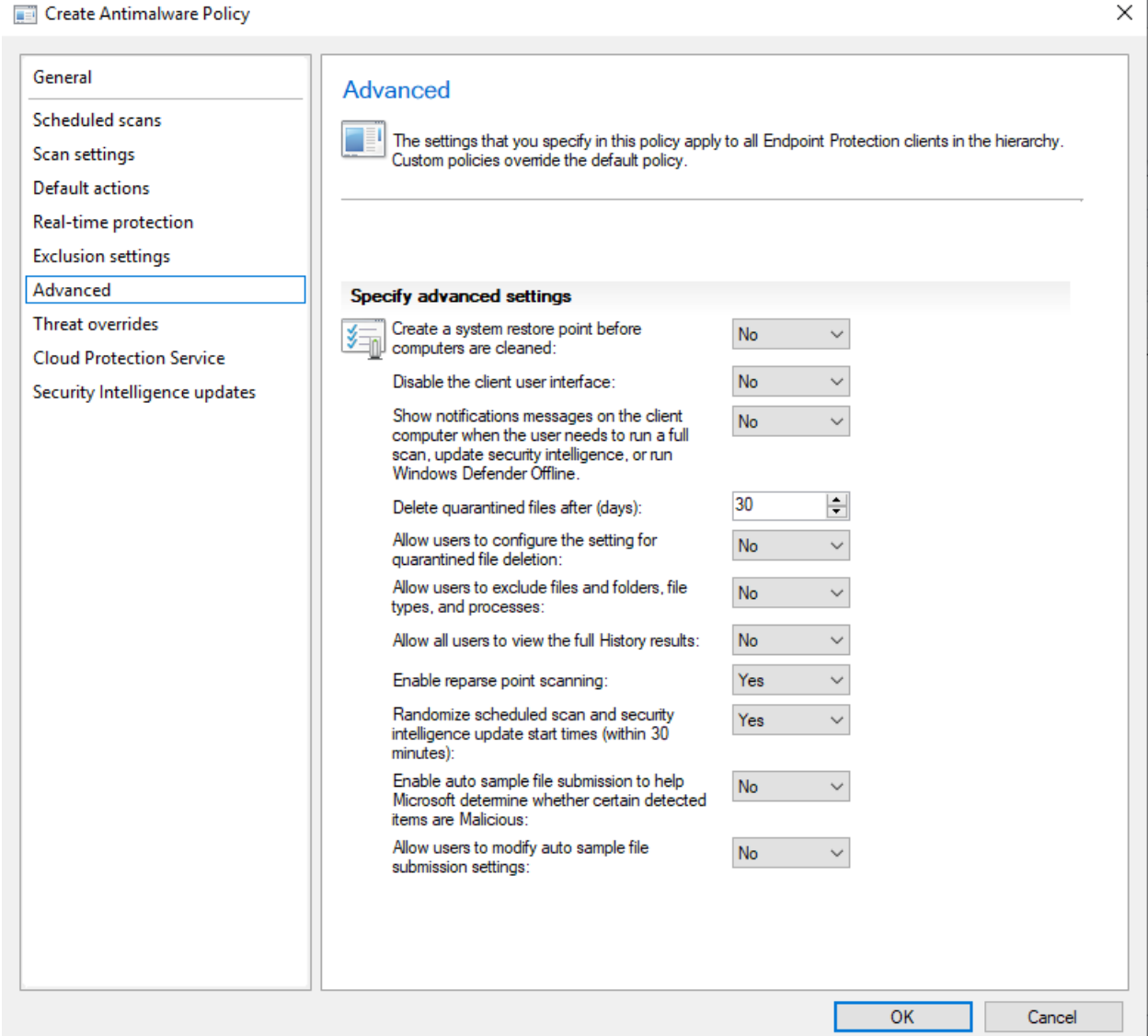
Enable real-time protection:	Yes
Monitor file and program activity on your computer:	Yes
Scan system files:	Scan incoming and outgoing files
Scan all downloaded files and enable exploit protection for Internet Explorer:	Yes
Enable behavior monitoring:	Yes
Enable protection against network-based exploits:	Yes
Allow users on client computers to configure real-time protection settings:	No
Enable protection against Potentially Unwanted Applications at download and prior to installation:	Yes

OK Cancel

Exclusion Settings sekmesinde ise taranmasını istemediğimiz dosya, dizin vb. var ise tanımlayabiliyoruz.



Advanced sekmesinde ise bir tarama başlatıldığında son kullanıcıya bunu pop-up çıkarıp gösterecek miyiz ? Yakalanan bir zararlı temizlenmeden önce restore point oluşturacak mıyiz ? Kullanıcıya bu zararlıyı silme için yetki verecekmiyiz? Karantinaya alınan bir zararlıyı ne zaman sileceğiz ? gibi ayarları yapılandırabiliyoruz.



Security Intelligence Updates sekmesinde ise endpointlerin kaç saatte bir kontrol edileceği ayarını belirliyoruz. Bu bölümde yapılandırmamız gereken kritik bir ayar bulunmaktadır. **Set Source** butonunu tıklayarak hangi kaynaklardan bu update lerin alınacağını belirliyoruz.

Create Antimalware Policy

General

Scheduled scans

Scan settings

Default actions

Real-time protection

Exclusion settings

Advanced

Threat overrides

Cloud Protection Service

Security Intelligence updates

Security Intelligence updates

The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.

Configure how Endpoint Protection clients will receive security intelligence updates

☒ Check for Endpoint Protection security intelligence at a specific interval (hours): (0 = disable check on interval) 4

Check for Endpoint Protection security intelligence daily at: (Only configurable if interval-based check is disabled) 2:00 AM

Force a security intelligence update if the client computer is offline for more than two consecutive scheduled updates: Yes

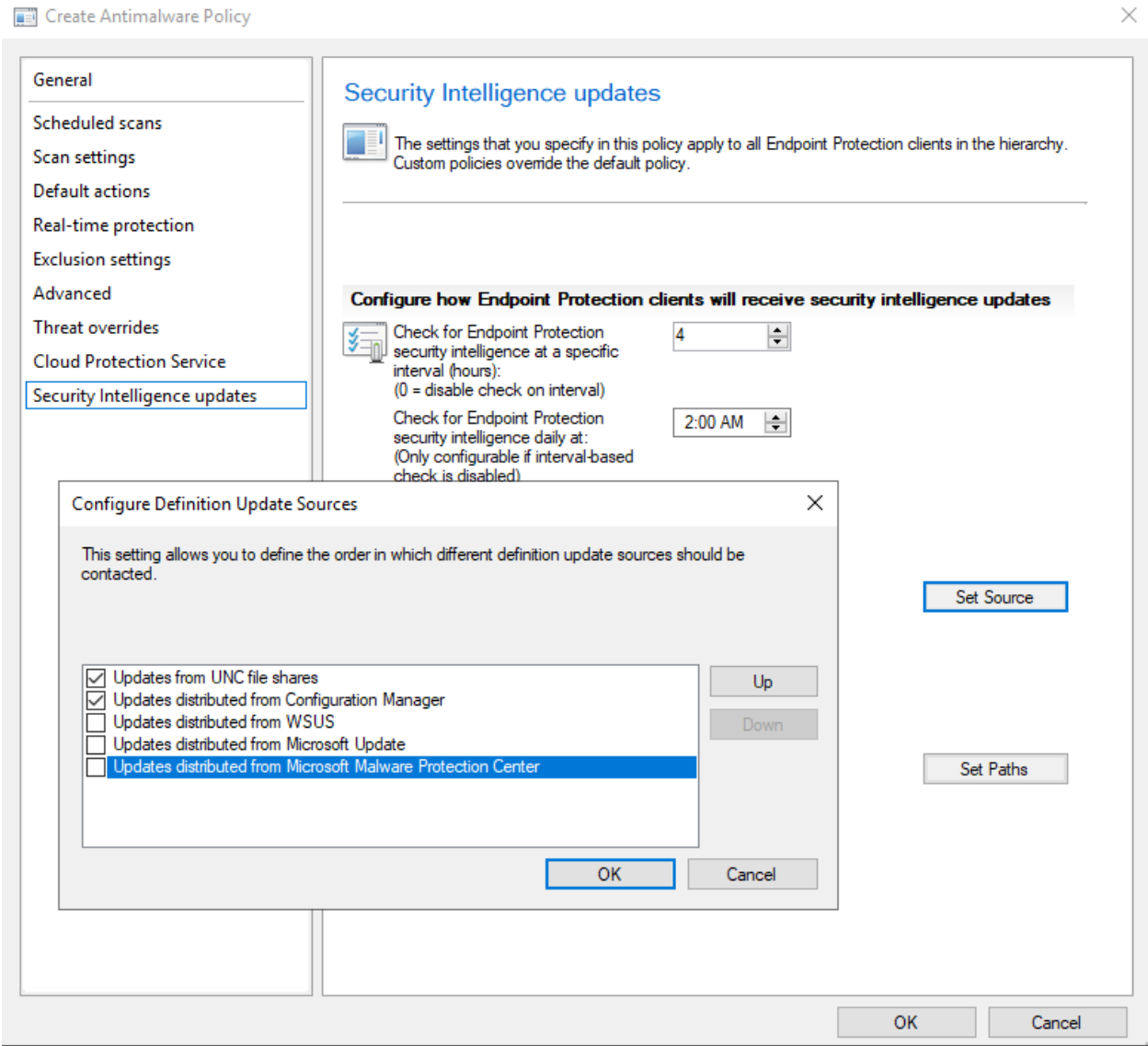
Set sources and order for Endpoint Protection security intelligence updates: 4 sources selected [Set Source](#)

If Configuration Manager is used as a source for security intelligence updates, clients will only update from alternative sources if security intelligence is older than (hours): 24

If UNC file shares are selected as a security intelligence update source, specify the UNC paths: (none) [Set Paths](#)

OK Cancel

Örneğimde ilk seçenek olarak UNC Path' den kontrol etmesini ve değişiklik var ise ilgili update leri almasını istiyorum. İkinci seçenek olarak SCCM' i seçiyorum.

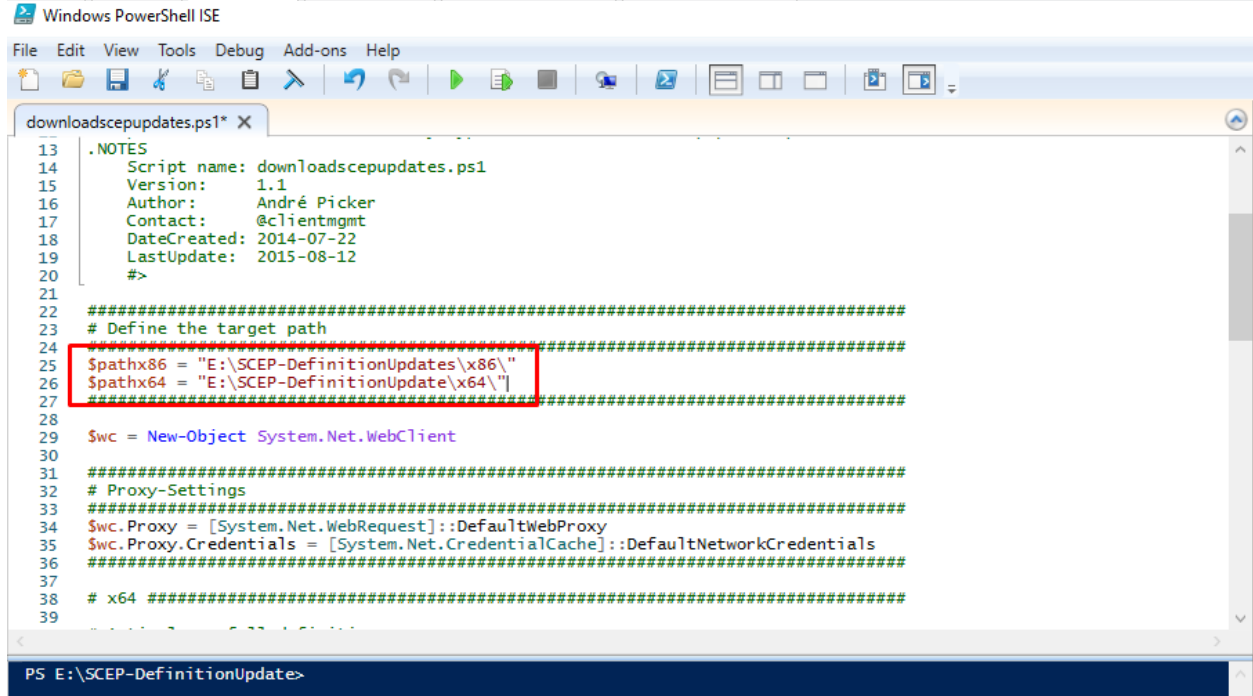


Bu noktada akıllara şu soru gelmektedir. UNC Path belirttik iyi hoş ama nasıl otomatik olarak güncellemeleri indirip sunucu ve istemcilere göndereceğiz ?

İlk olarak aşağıdaki linkte yer alan Powershell Script' i indiriyoruz ve yazana teşekkür etmeyi unutmuyoruz.

<https://gallery.technet.microsoft.com/scriptcenter/SCEP-Definition-Updates-to-fde57ebf>

Yapımıza göre ilgili paketlerin indirileceği bölümü değiştiriyoruz.



```
Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
downloadsccepupdates.ps1* X
13 .NOTES
14   Script name: downloadsccepupdates.ps1
15   Version:    1.1
16   Author:     André Picker
17   Contact:    @clientmgmt
18   DateCreated: 2014-07-22
19   LastUpdate: 2015-08-12
20   #>
21
22 #####
23 # Define the target path
24 #####
25 $pathx86 = "E:\SCEP-DefinitionUpdates\x86\"
26 $pathx64 = "E:\SCEP-DefinitionUpdate\x64\"
27 #####
28
29 $wc = New-Object System.Net.WebClient
30
31 #####
32 # Proxy-Settings
33 #####
34 $wc.Proxy = [System.Net.WebRequest]::DefaultWebProxy
35 $wc.Proxy.Credentials = [System.Net.CredentialCache]::DefaultNetworkCredentials
36 #####
37
38 # x64 #####
39
```

PS E:\SCEP-DefinitionUpdate>

İlgili Powershell Script' i sürekli manuel çalıştıramayacağımıza göre Task Scheduler ile bu bölümü otomatize ediyoruz.

Create Task

General Triggers Actions Conditions Settings

Name: SCEP Definition Updates

Location: \

Author: HD\sccmadm

Description:

Security options

When running the task, use the following user account:

HD\sccmadm Change User or Group...

☐ Run only when user is logged on

☒ Run whether user is logged on or not

☐ Do not store password. The task will only have access to local computer resources.

☐ Run with highest privileges

☐ Hidden

Configure for: Windows Vista™, Windows Server™ 2008

OK Cancel

New Trigger ✕

Begin the task: On a schedule ▾

Settings

☐ One time Start: 4/14/2020  11:55:59 AM  ☐ Synchronize across time zones

☒ Daily Recur every: 1 days

☐ Weekly

☐ Monthly

Advanced settings

☐ Delay task for up to (random delay): 1 hour ▾

☒ Repeat task every: 3 hour ▾ for a duration of: 1 day ▾

☐ Stop all running tasks at end of repetition duration

☒ Stop task if it runs longer than: 1 hour ▾

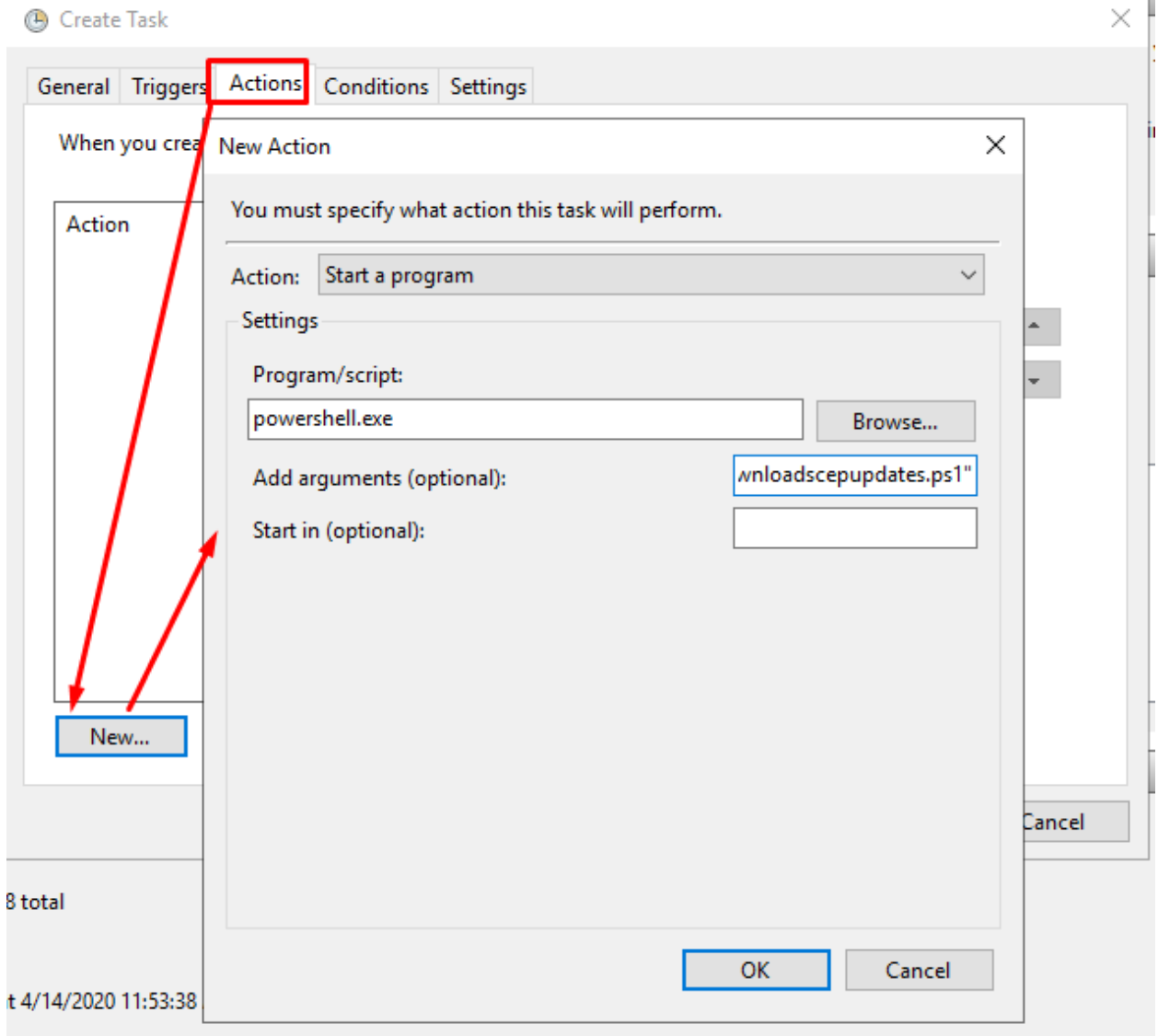
☐ Expire: 4/14/2021  11:56:00 AM  ☐ Synchronize across time zones

☐ Enabled

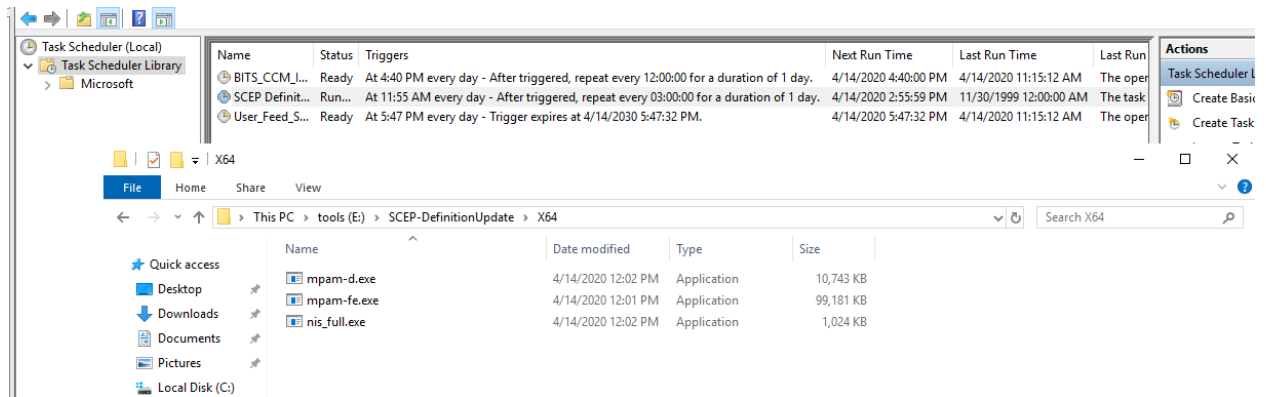
OK Cancel

Action kısmında scriptimizi tanımlıyoruz.(Yapınıza göre editlemeyi unutmayınız)

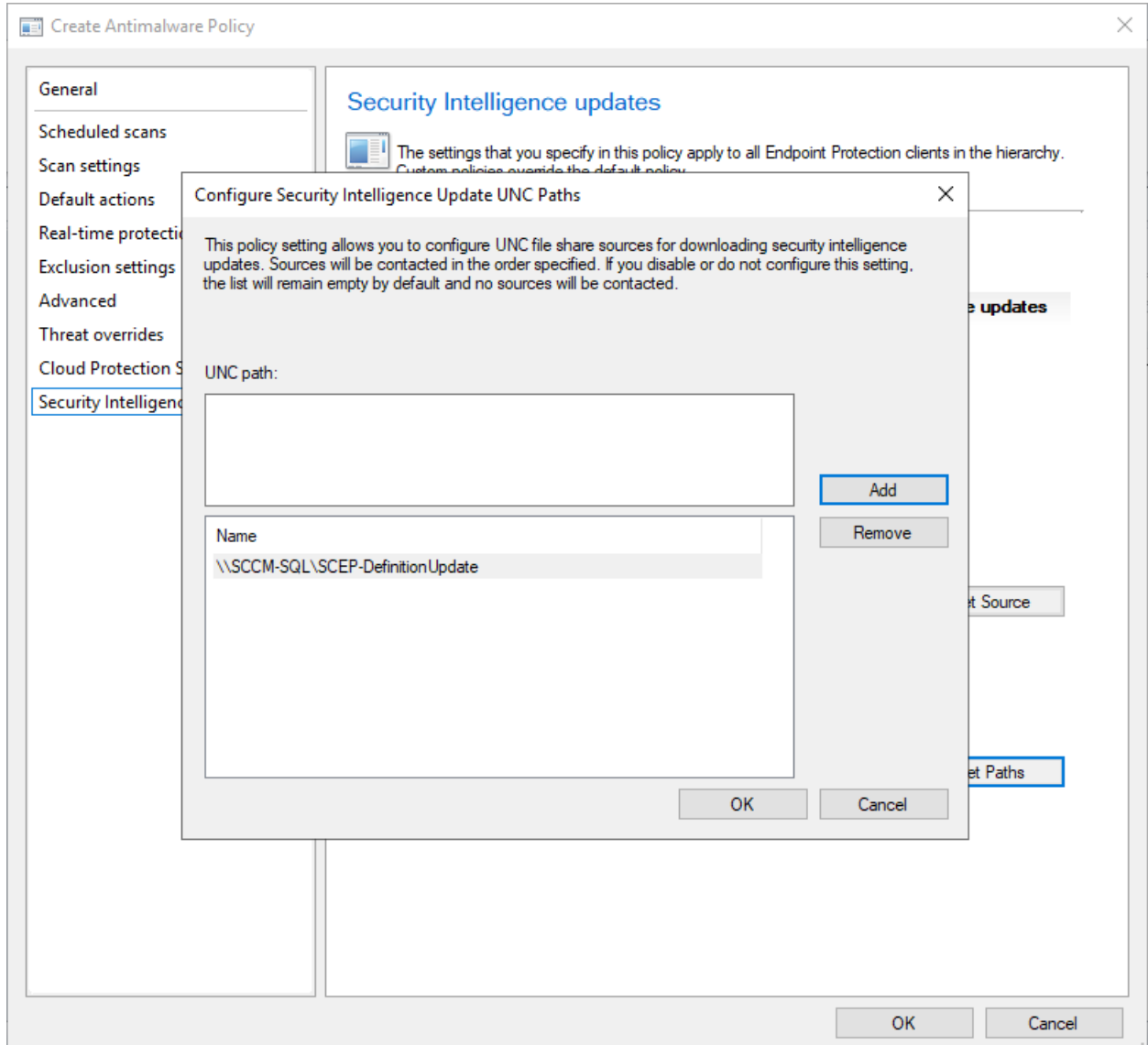
-file "E:\SCEP-DefinitionUpdate\downloadscepupdates.ps1"



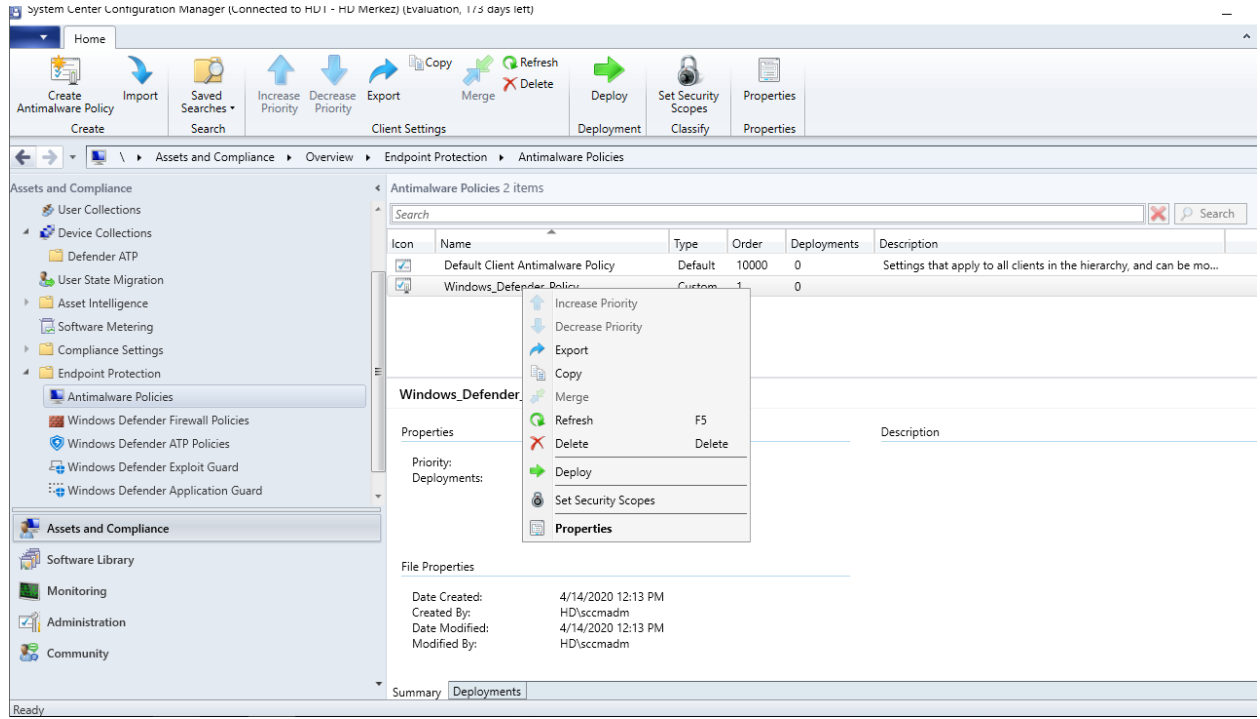
Test için manuel olarak çalıştırıyorum ve başarılı şekilde ilgili dosyalarımın indirildiğini görüyorum.



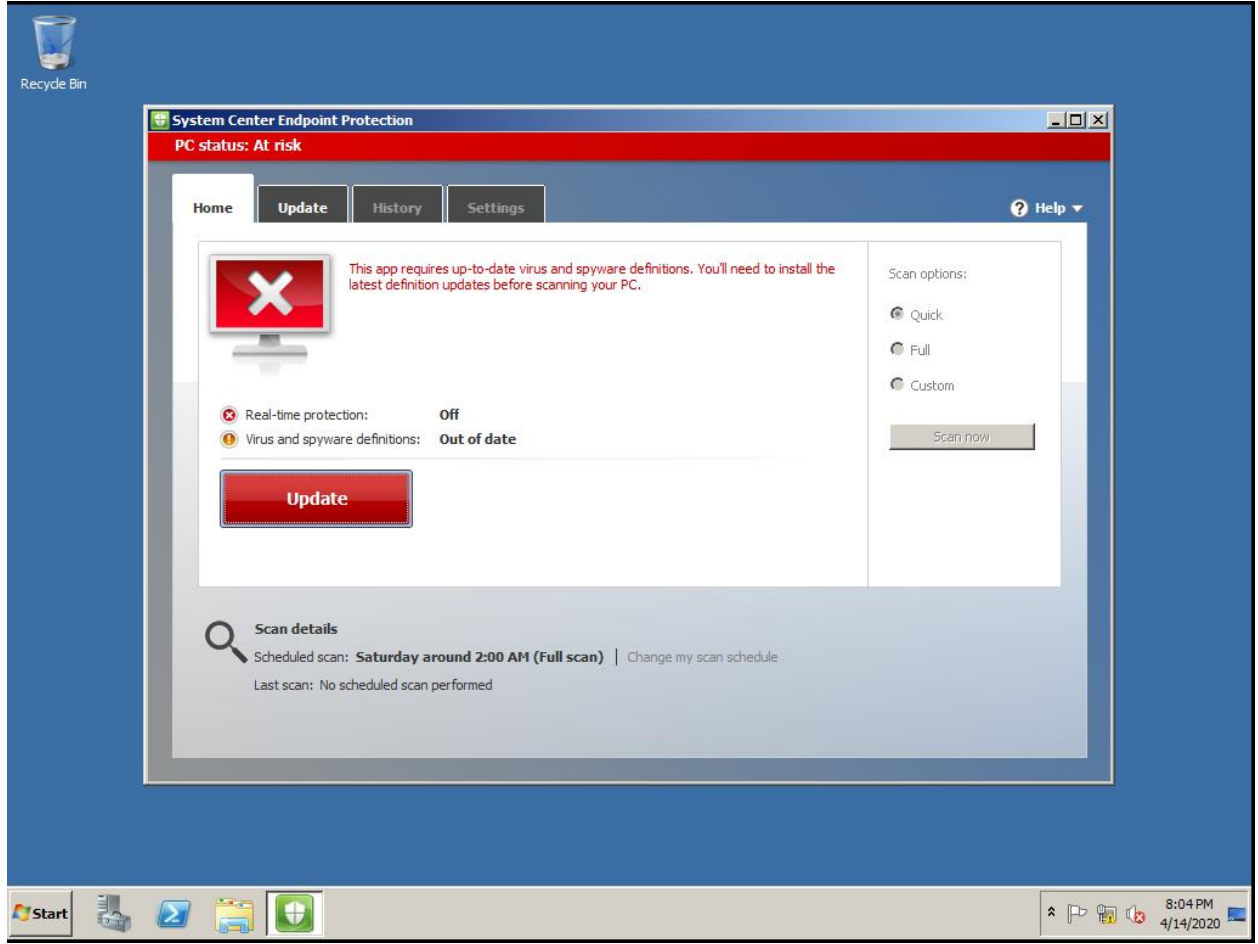
Daha sonra ilgili Path i aşağıdaki UNC Path bölümünde tanımlıyorum.



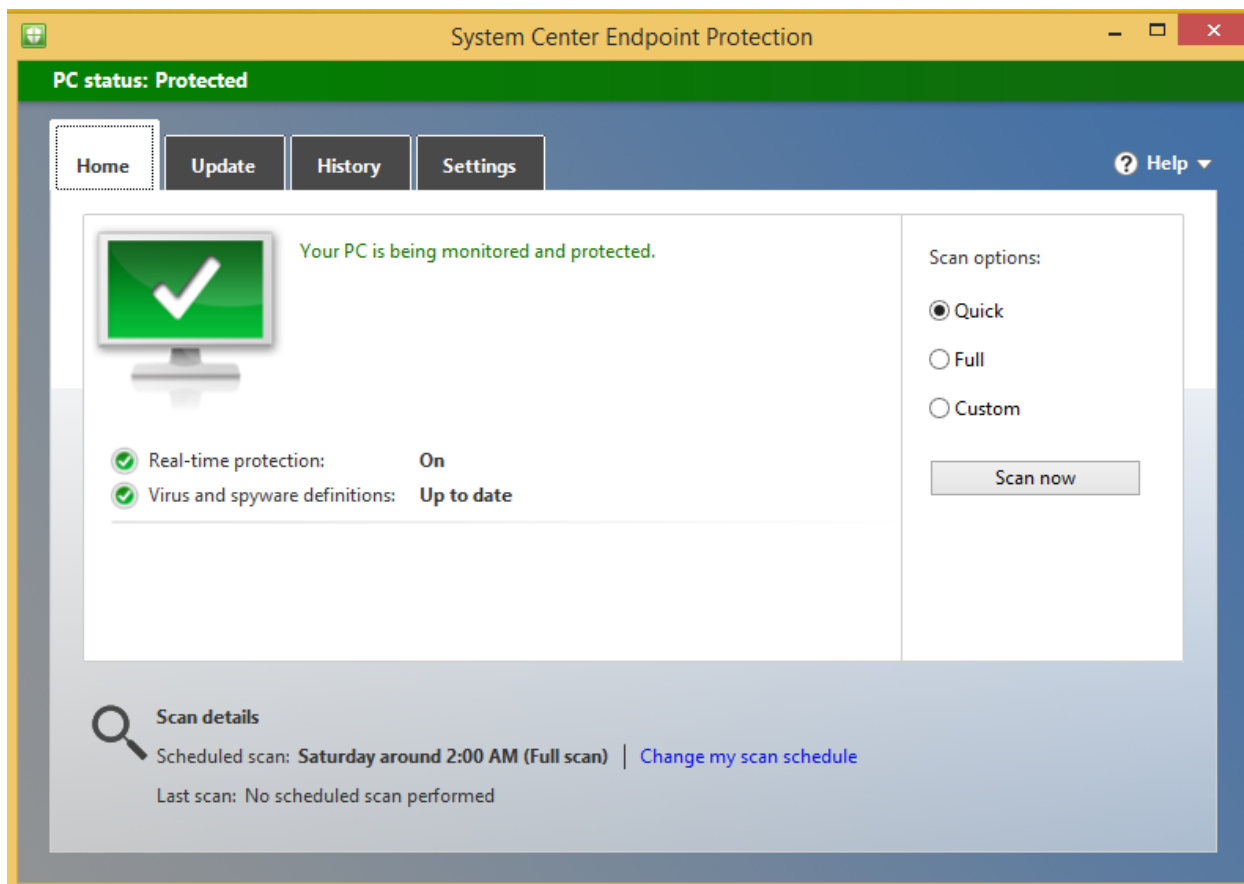
Yapılandırmamızı tamamladıktan sonra Antimalware Policy ayarını ilgili Collection' lara dağıtmayı unutmayınız.



Windows Server 2008 R2 sunucumda Endpoint Protection ajanının yüklendiğini görüyorum fakat güncel değil.



Update butonunu tıklıyorum ve başarılı şekilde ilgili UNC Path' den güncellemerin çekildiğini gözlemliyorum.



Windows Defender Exploit Guard

Desteklenen İşletim Sistemleri

System Center Configuration Manager (SCCM) Current Branch (CB)

Microsoft Defender Antivirus

- Windows Server 2019
- Windows 10 1909
- Windows 10 1903
- Windows 10 1809
- Windows Server, 1803
- Windows 10 1803
- Windows 10 1709

Desteklenmeyen İşletim Sistemleri

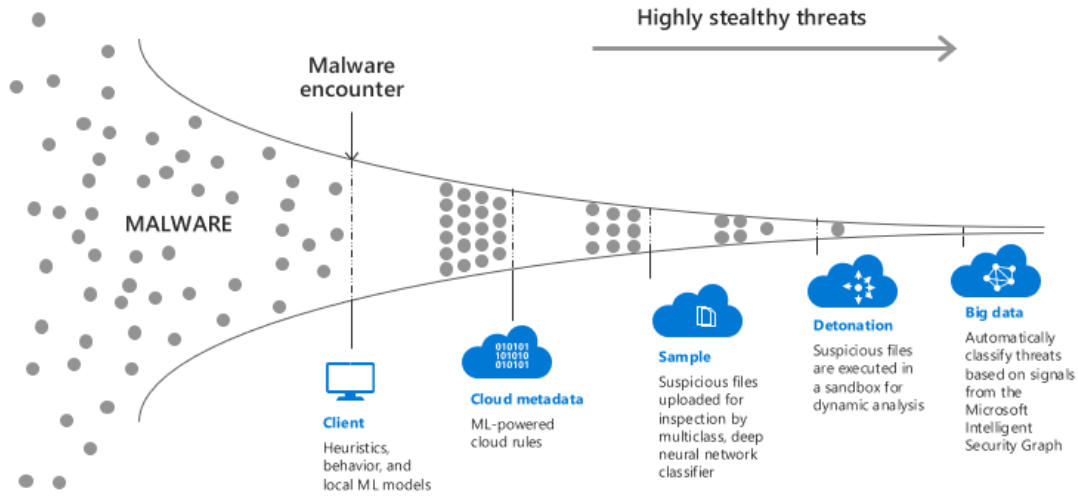
Microsoft Defender Antivirus

- Windows Server 2016
- Windows 10 1703
- Windows 10 1607
- Windows 10 1511
- Windows 10 1507

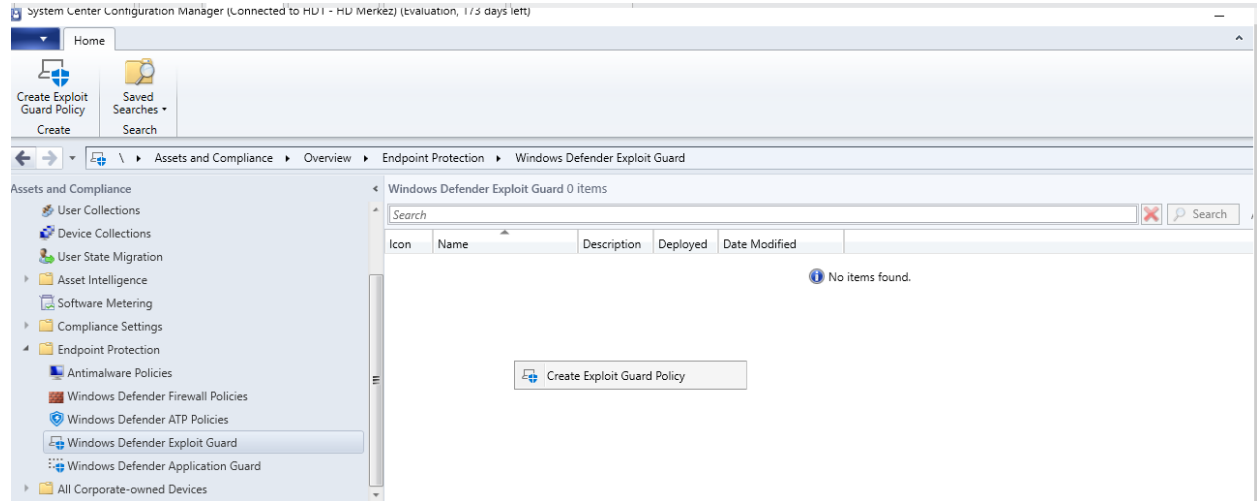
System Center Endpoint Protection

- Windows Server 2012 R2
- Windows 8.1
- Windows Server 2012
- Windows 8
- Windows Server 2008 R2 SP1
- Windows 7 SP1
- Windows Server 2008 SP2
- Windows Vista

Exploit Guard özelliği sayesinde özellikle sıfırıncı gün saldırıları, kötü amaçlı yazılımlar, sofistike saldırılar, imza tabansız zararlılar, Fileless tehditler, Ransomware atakları, Hardware lere karşı yapılan saldırılar ve daha fazlasına karşı koruma sağlamaktadır.



Kısa açıklamadan sonra yapılandırmamıza geçebiliriz. SCCM konsolumuzu açıyoruz ve Endpoint Protection sekmesi içerisinde yer alan Windows Defender Exploit Guard sekmesine geliyoruz ve **Create Exploit Guard Policy** ile işlemimize başlıyoruz.



Kuralımıza isim veriyoruz ve Exploit Guard içerisinde neleri aktif etmek istiyorsak ilgili seçenekleri seçiyoruz.

Create Windows Defender Exploit Guard Policy

General

Specify general information

Windows Defender Exploit Guard provides intrusion prevention rules and policies that make vulnerabilities more difficult to exploit in Windows 10.

[Learn more about Exploit Guard](#)

Name:
Attack Surface Policy

Description:

Enable Exploit Guard components:

- ☒ Attack Surface Reduction
- ☒ Controlled folder access
- ☐ Exploit protection
- ☒ Network protection

< Previous Next > Summary Cancel

Dikkatli Okuyunuz ! Batman olmaya çalışmayınız, projedeki bir hata sizi Joker yapabilir 😊

- Yapılandırmaya kesinlikle **Audit Mode** olarak başlayınız.
- İlgili ayarları tüm yapıya dağıtmadan testlerinizi var ise test ortamında yapınız.
- Eğer bu proje bir ürünü diğer ürünle değiştirme(Replacement) ise exclusionları çok dikkatli şekilde eski ortamdan yeni ortama taşıyınız.
- Hypervisor katmanında bir koruma sağlıyorsanız ve bunu MDATP + Scep ile yeniliyorsanız Performans testlerini yapmanızı tavsiye ederim. İlgili testte başlamadan önce özellikle Storage üzerindeki I/O değerlerini not alınız ve Full Scan vb testleri başlatıp tekrar değerleri kontrol ediniz.

Not: Tüm ayarların açıklamasına tek tek girmeyeceğim. Lütfen detay bilgi için erişimi çok zor olan Bing' den yararlanınız.

System Center Configuration Manager (SCCM) Current Branch (CB)

Desteklenen İşletim Sistemleri

Microsoft Defender Antivirus

- Windows Server 2019
- Windows 10 1909
- Windows 10 1903
- Windows 10 1809
- Windows Server, 1803
- Windows 10 1803
- Windows 10 1709

Desteklenmeyen İşletim Sistemleri

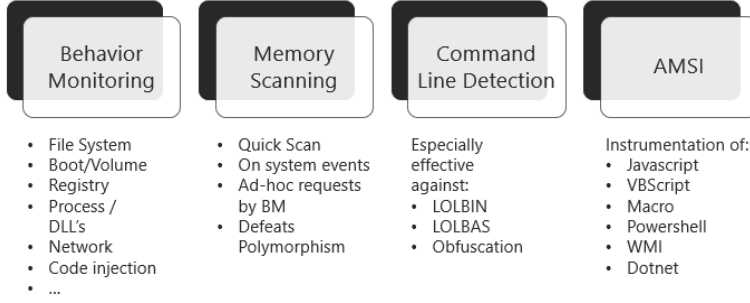
Microsoft Defender Antivirus

- Windows Server 2016
- Windows 10 1703
- Windows 10 1607
- Windows 10 1511
- Windows 10 1507

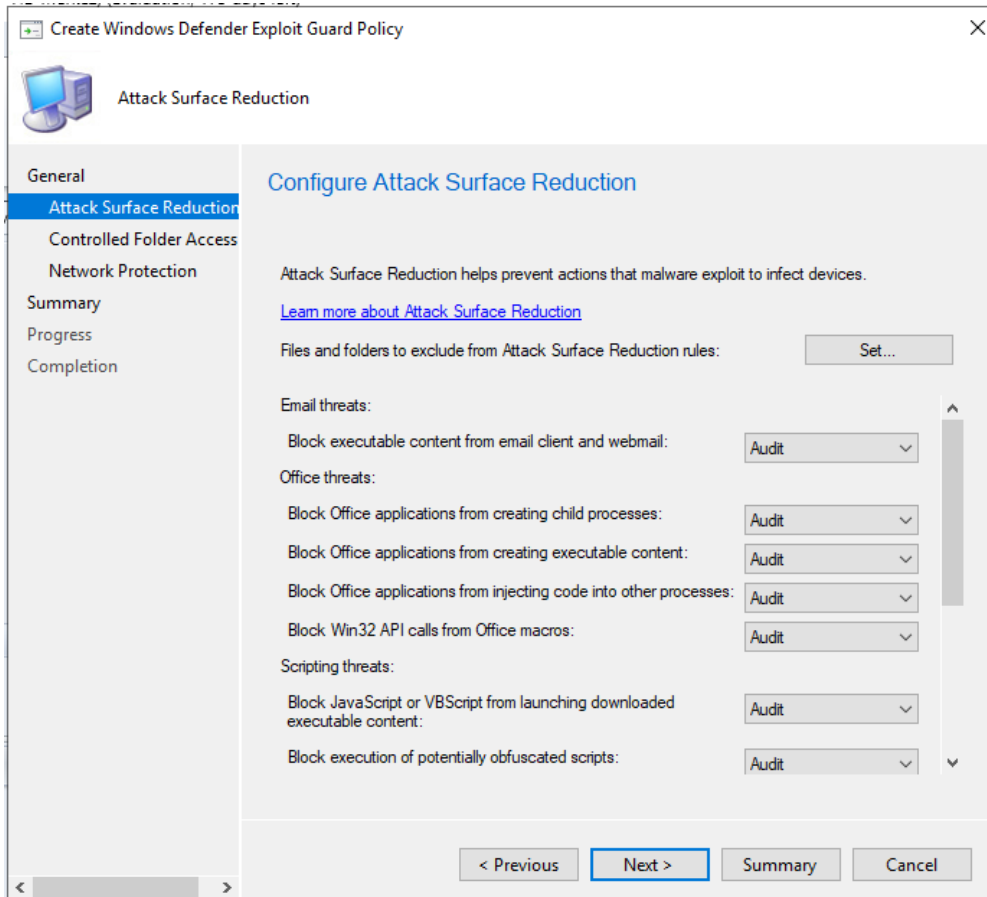
System Center Endpoint Protection

- Windows Server 2012 R2
- Windows 8.1
- Windows Server 2012
- Windows 8
- Windows Server 2008 R2 SP1
- Windows 7 SP1
- Windows Server 2008 SP2
- Windows Vista

ASR ile birlikte aşağıdaki atak vektörlerine karşı koruma sağladığımızı belirtmiştik.



Zararlılar en fazla ofis dökümanları, phishing saldırıları, Javascript, Vbscript ler üzerinden bulaşmaktadır. Attack surface reduction özelliği ile birlikte malware lere karşı etkin koruma sağlayabiliyoruz.



Eğer yapınız içerisinde harici cihazları(USB, External HDD vb) bloklamak istiyorsanız ayarımızı burada yapıyoruz.

Ransomware threats:

Use advanced protection against ransomware: Audit

Operating system threats:

Block credential stealing from the Windows local security authority subsystem: Audit

Block executable files from running unless they meet a prevalence, age, or trusted list criteria: Audit

External device threats:

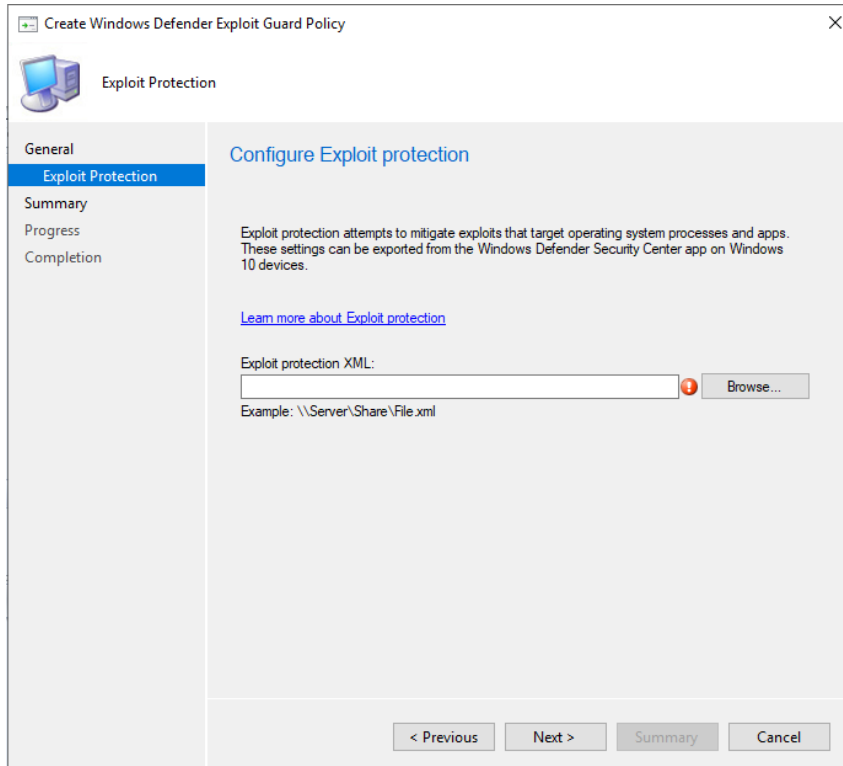
Block untrusted and unsigned processes that run from USB: Audit

< Previous **Next >** Summary Cancel

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction>

Exploit Protection

Bildiğiniz üzere exploit protection Enhanced Mitigation Experience Toolkit(EMET) in yerine geldi diyebiliriz. Bildiğiniz üzere EMET 31 Temmuz 2018' de expire oldu.Hali hazırda EMET kullanıyorsanız ilgili kuralı **ConvertTo-ProcessMitigatinPolicy -EMETFile.xml -outfilepath file.xml** şeklinde export edip Exploit protection içerisinde tanımlayabilirsiniz.



<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/exploit-protection>

Control Folder Access

Desteklenen İşletim Sistemleri

System Center Configuration Manager (SCCM) Current Branch (CB)

Microsoft Defender Antivirus

- Windows Server 2019
- Windows 10 1909
- Windows 10 1903
- Windows 10 1809
- Windows Server, 1803
- Windows 10 1803
- Windows 10 1709

Desteklenmeyen İşletim Sistemleri

Microsoft Defender Antivirus

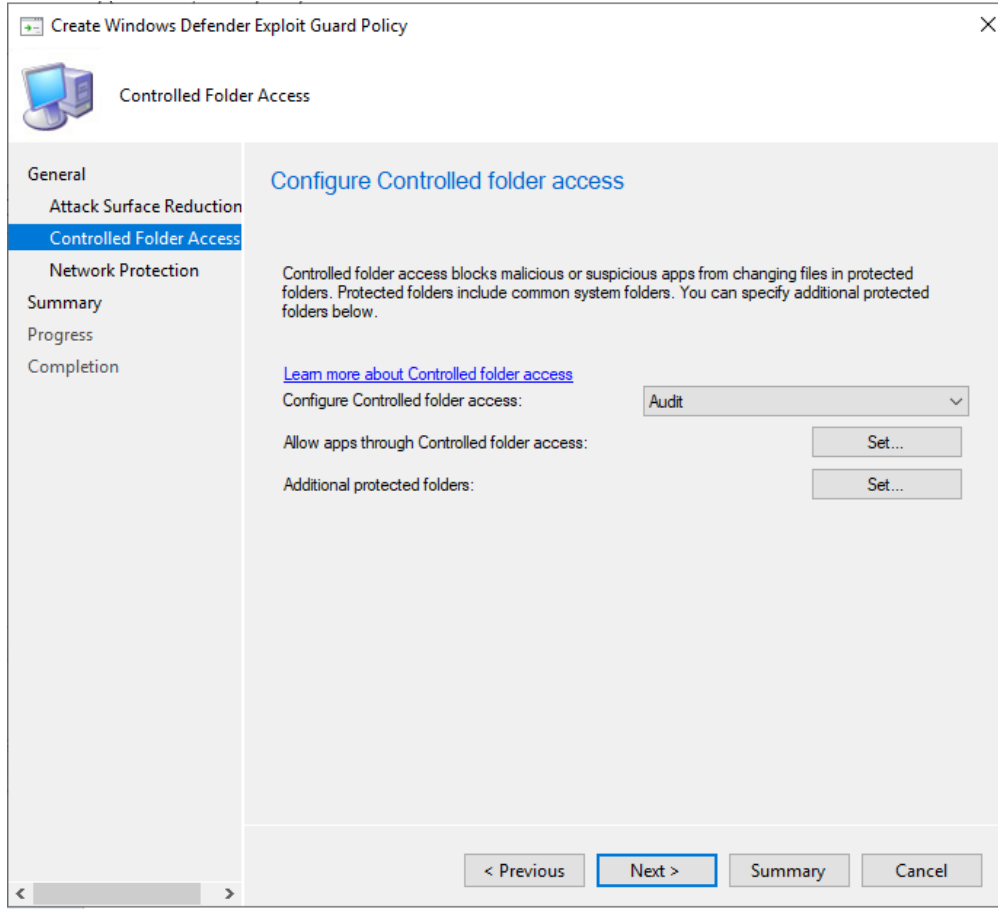
- Windows Server 2016

- Windows 10 1703
- Windows 10 1607
- Windows 10 1511
- Windows 10 1507

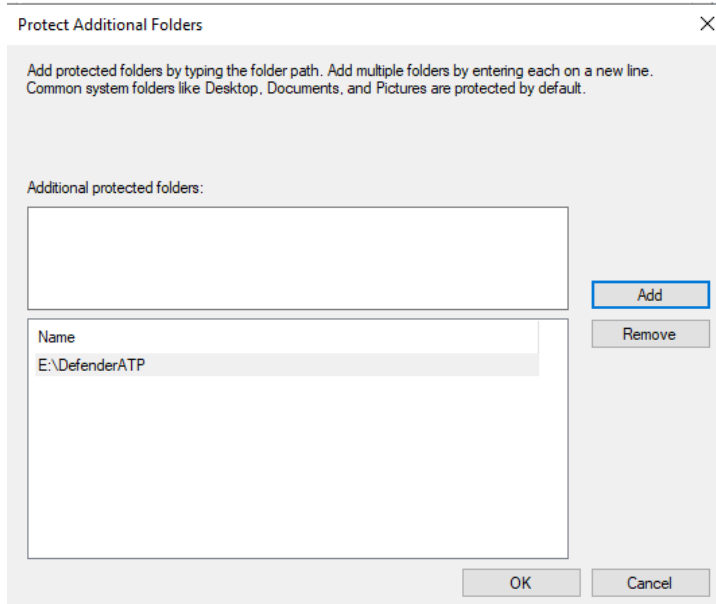
System Center Endpoint Protection

- Windows Server 2012 R2
- Windows 8.1
- Windows Server 2012
- Windows 8
- Windows Server 2008 R2 SP1
- Windows 7 SP1
- Windows Server 2008 SP2
- Windows Vista

Son senelerde bildiğiniz üzere Ransomware atakları ciddi artış gösterdi ve firmalar çok ciddi veri ve para kaybettiler. İlgili ayar ile bu atağın önüne geçebiliyoruz. Bu bölümde Audit Disk Sector Only seçeneğini de seçebilirsiniz ve bir sonraki aşamada Block rule olarak Block Disk Sector şeklinde yapılandırabilirsiniz. Bu tamamen neyi ne kadar korumak istediğiniz ve yapınız ile alakalı.



Örneğin **Additional protected folders** seçeneği ile korumak istediğiniz dosyaların dizinlerini burada tanımlayabilirsiniz. Aynı kısıtlamayı uygulamalar içinde yapabiliyoruz.



<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/controlled-folders>

Network Protection

Desteklenen İşletim Sistemleri

System Center Configuration Manager (SCCM) Current Branch (CB) running:

Microsoft Defender Antivirus

- Windows Server 2019
- Windows 10 1909
- Windows 10 1903
- Windows 10 1809
- Windows Server, 1803
- Windows 10 1803
- Windows 10 1709

Desteklenmeyen İşletim Sistemleri

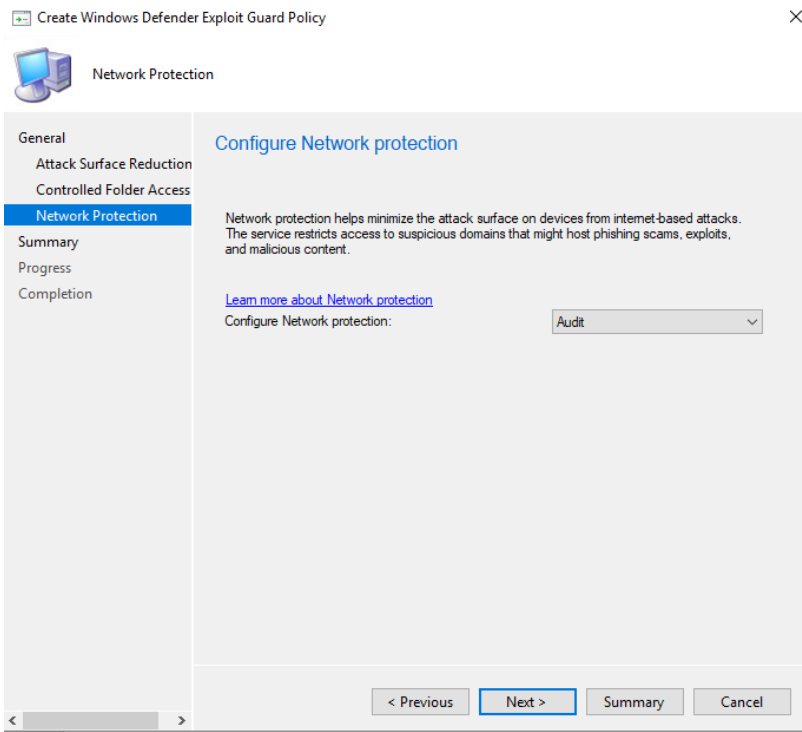
Microsoft Defender Antivirus

- Windows Server 2016
- Windows 10 1703
- Windows 10 1607
- Windows 10 1511
- Windows 10 1507

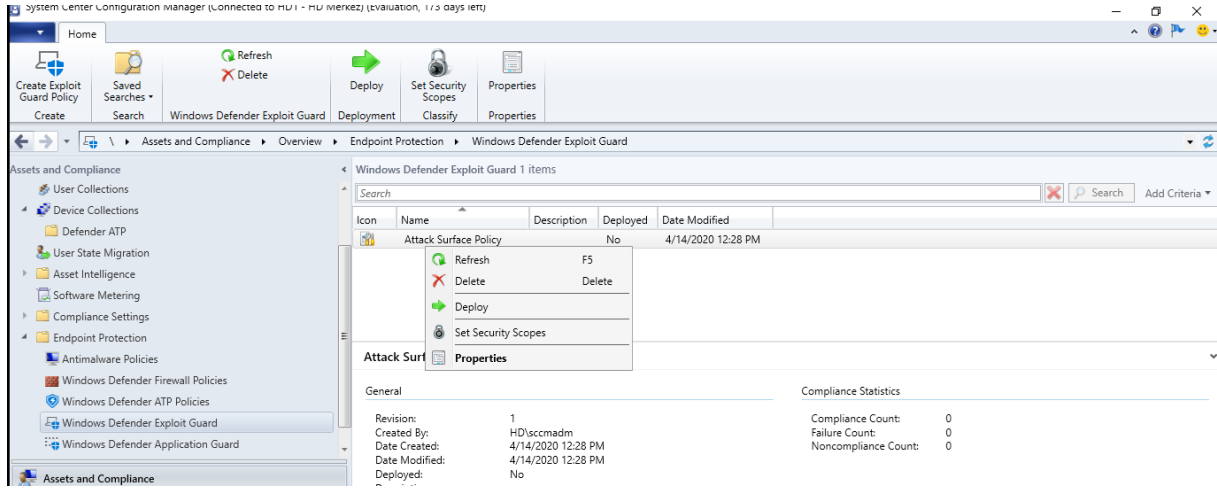
System Center Endpoint Protection

- Windows Server 2012 R2
- Windows 8.1
- Windows Server 2012
- Windows 8
- Windows Server 2008 R2 SP1
- Windows 7 SP1
- Windows Server 2008 SP2
- Windows Vista

İlgili seçeneğin yapılandırılması halinde reputasyonu düşük olan Domain lerle olan bağlantı engellenecektir. Bu ayarı aslında Microsoft Defender SmartScreen' in devamı gibi düşünebilirsiniz. Microsoft Defender SmartScreen bizi yemleme saldırıları, zararlı içeren web siteleri, uygulamalar, indirilen ve potansiyel tehdit oluşturan tehditlere karşı korumaktadır.



Bu adımla birlikte artık yapılandırmamızı tamamlıyoruz. Son olarak da ilgili ayarı ilgili Collection' a uyguluyoruz.



<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/network-protection>

Windows Defender ATP Policies

System Center Configuration Manager (SCCM) Current Branch (CB)

Microsoft Defender Advanced Threat

Desteklenen İşletim Sistemleri

- Windows 10, version 1909, 1809 , 1803, 1709
- Windows Server 2019

<https://support.microsoft.com/en-us/lifecycle/search?alpha=Windows%2010%201909>

<https://support.microsoft.com/en-us/lifecycle/search?alpha=Windows%2010%201903>

<https://support.microsoft.com/en-us/lifecycle/search?alpha=Windows%2010%201809>

<https://support.microsoft.com/en-us/lifecycle/search?alpha=Windows%2010%201803>

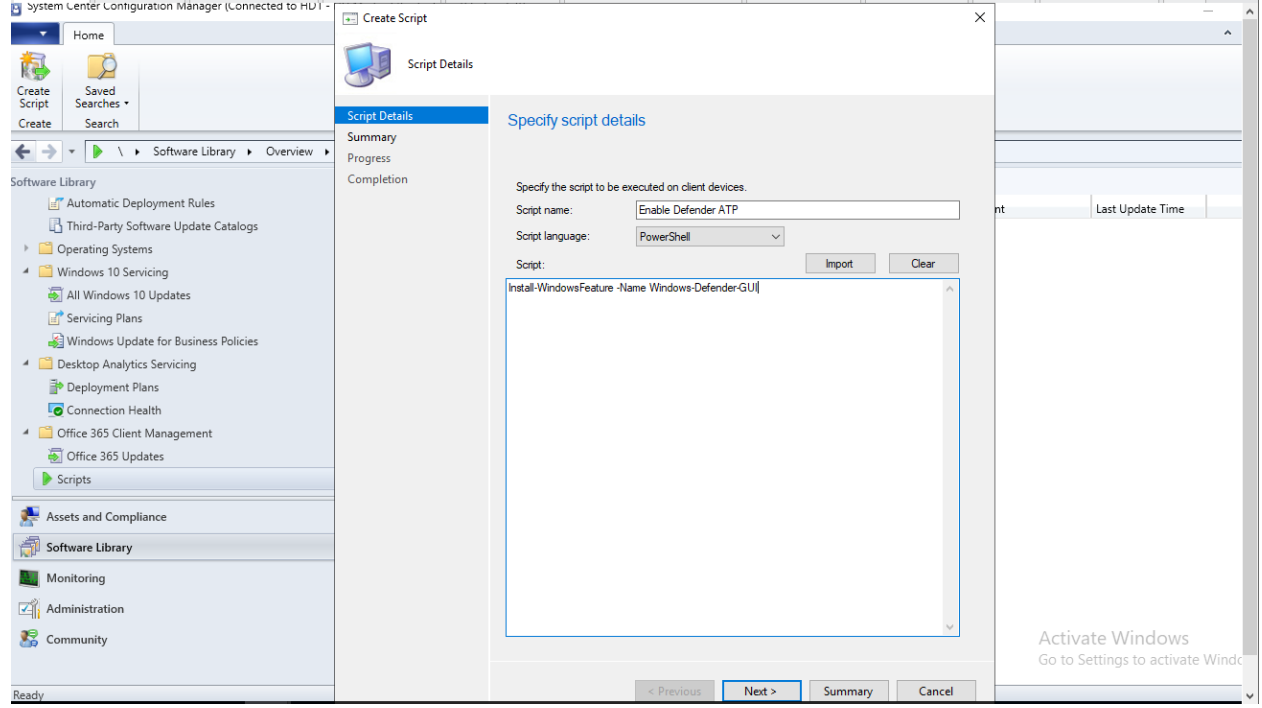
<https://support.microsoft.com/en-us/lifecycle/search?alpha=Windows%2010%201709>

İlgili bölüm Windows 10 Onboarding başlığı altında anlatılmıştır.

Windows Server 2016 Defender ATP Kurulumu

Bir önceki bölümümüzde Windows Server 2008 R2 SP1, 2012 R2 , Windows 7/8.1 işletim sistemlerine SCEP ajanı kurulumunu anlatmıştım. Windows Server 2016 işletim sisteminde hali hazırda bu özellik

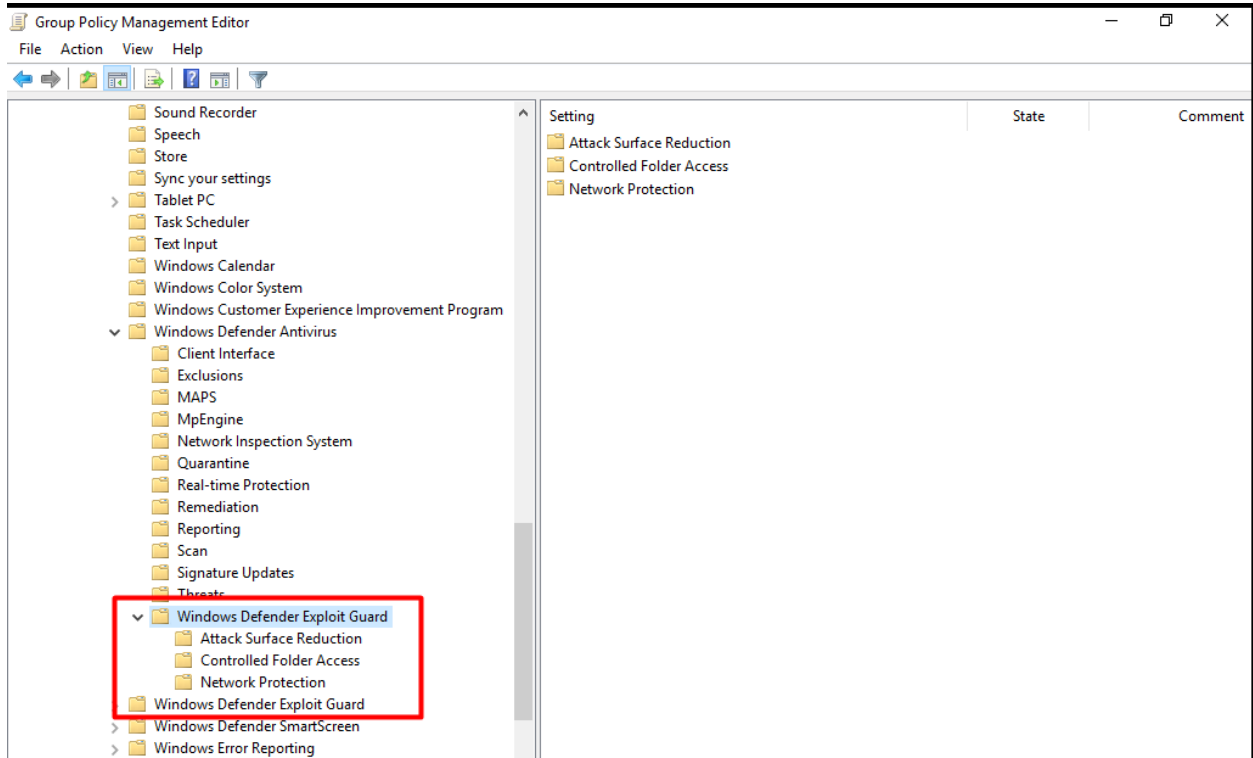
mevcut fakat aktif olmadığını varsayalım. Yine imdadımıza SCCM yetiştiriyor bu sefer Powershell' den küçük bir yardım alacağız. Bildiğiniz üzere SCCM içerisinde script özelliği mevcut ve Powershell' i destekliyor. Bende bunu kullanarak Defender ATP' yi aktif hale getireceğim. **Install-WindowsFeature -Name Windows-Defender-GUI** komutunu script içerisine kopyalıyorum, elbette script dili powershell olmalı. Daha sonra next next diyerek işlemimi tamamliyorum ve ilgil script i Windows Server 2016 Collection larına dağıtıyorum. Bu işlemten sonra sunucuların restart edilmesi gerekmektedir !!!



Group Policy ile Windows Defender Exploit Guard Yapılandırma

Attack Surface Reduction

Configure Attack Surface Reduction Rules



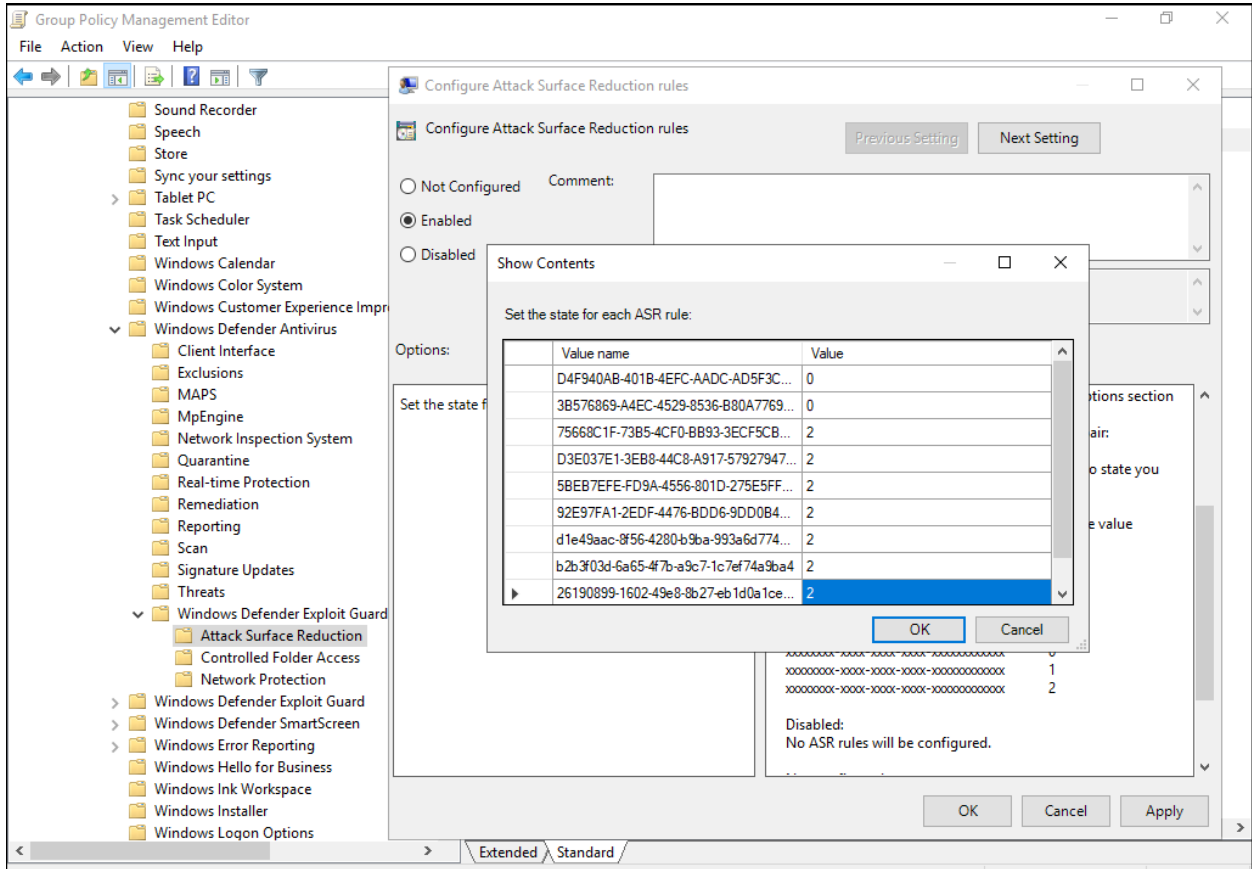
Group Policy ile yapılandırma kısmı malesef biraz daha meşakatli diyebilirim. Bu bölümde de değere 2 vererek başlangıç için Audit olarak yapılandırıyorum.

Rule Description Rule GUID	
Block all Office applications from creating child processes	D4F940AB-401B-4EFC-AADC-AD5F3C50688A
Block Office applications from creating executable content	3B576869-A4EC-4529-8536-B80A7769E899
Block Office applications from injecting code into other processes	75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84
Block JavaScript or VBScript from launching downloaded executable content	D3E037E1-3EB8-44C8-A917-57927947596D
Block execution of potentially obfuscated scripts	5BEB7EFE-FD9A-4556-801D-275E5FFC04CC
Block Win32 API calls from Office macro	92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B

Block process creations originating from PSEXEC and WMI commands	d1e49aac-8f56-4280-b9ba-993a6d77406c
Block untrusted and unsigned processes that run from USB	b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4
Block only Office communication applications from creating child processes	26190899-1602-49e8-8b27-eb1d0a1ce869

Daha fazlasına aşağıdaki linkten erişebilirsiniz.

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction>

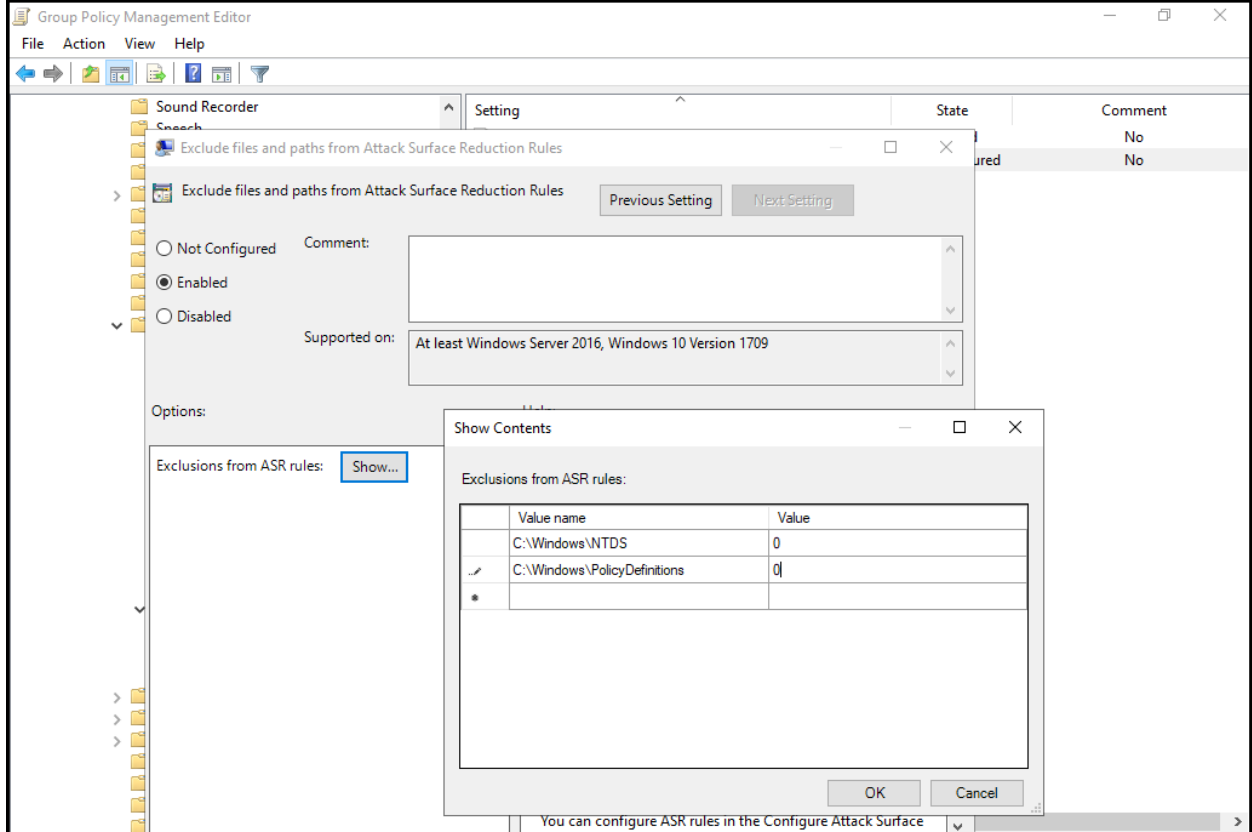


Peki yapılandırmamızı Audit olarak yapılandırdık. Takibini nasıl yapacağız ?

- Event ID 1121 -- blocking mode events
- Event ID 1122 -- audit mode events
- Event ID 5007 -- changing settings events

Exclude files and paths from Attack Surface Reduction (ASR) rules

Yapınıza göre ve uygulama sunucularınızın çeşidine göre ASR kuralı için exclusion yazmanız gerekirse aşağıdaki örnekte olduğu gibi yapılandırabilirsiniz.



Controlled Folder Access

Configure Allowed Applications

Aşağıdaki örnekte olduğu gibi kurumunuza ait kullanılmasına izin vereceğiniz uygulamaları aşağıdaki şekilde belirleyebiliyoruz.

Configure allowed applications

Configure allowed applications

Previous Setting

Next Setting

☐ Not Configured

☒ Enabled

☐ Disabled

Comment:

Supported on:

At least Windows Server 2016, Windows 10 Version 1709

Options:

Help:

Enter the applications that should be trusted:

Show...

Show Contents

Enter the applications that should be trusted:

	Value name	Value
	C:\Program Files (x86)\Windows Media Player\wmplayer.exe	0
*		

OK

Cancel

Add additional applications that should be considered "trusted" by controlled folder access. These applications are allowed to modify or delete files in controlled folder access folders. Windows Defender Antivirus automatically determines which applications should be trusted. You can configure this setting to add additional applications.

Enabled:

Specify additional allowed applications in the Options section..

Disabled:

No additional applications will be added to the trusted list.

Not configured:

Same as Disabled.

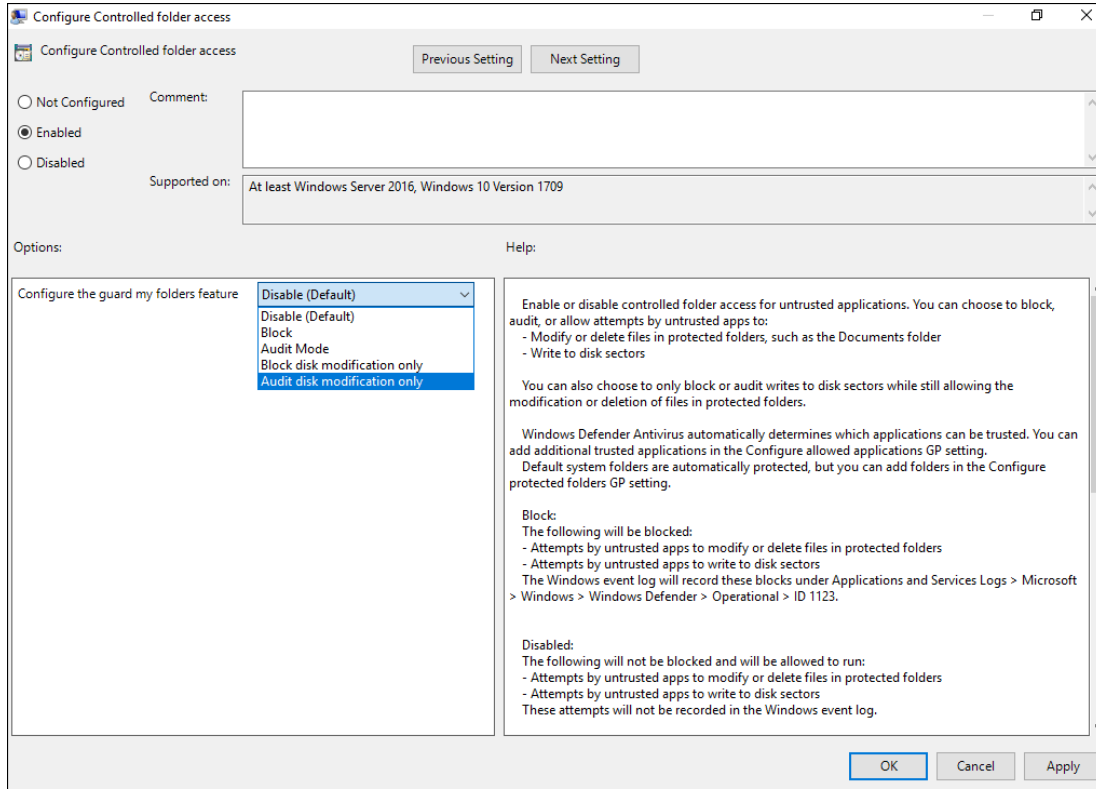
You can enable controlled folder access in the Configure controlled folder access GP setting.

Default system folders are automatically guarded, but you can add folders in the configure protected folders GP setting.

Page82

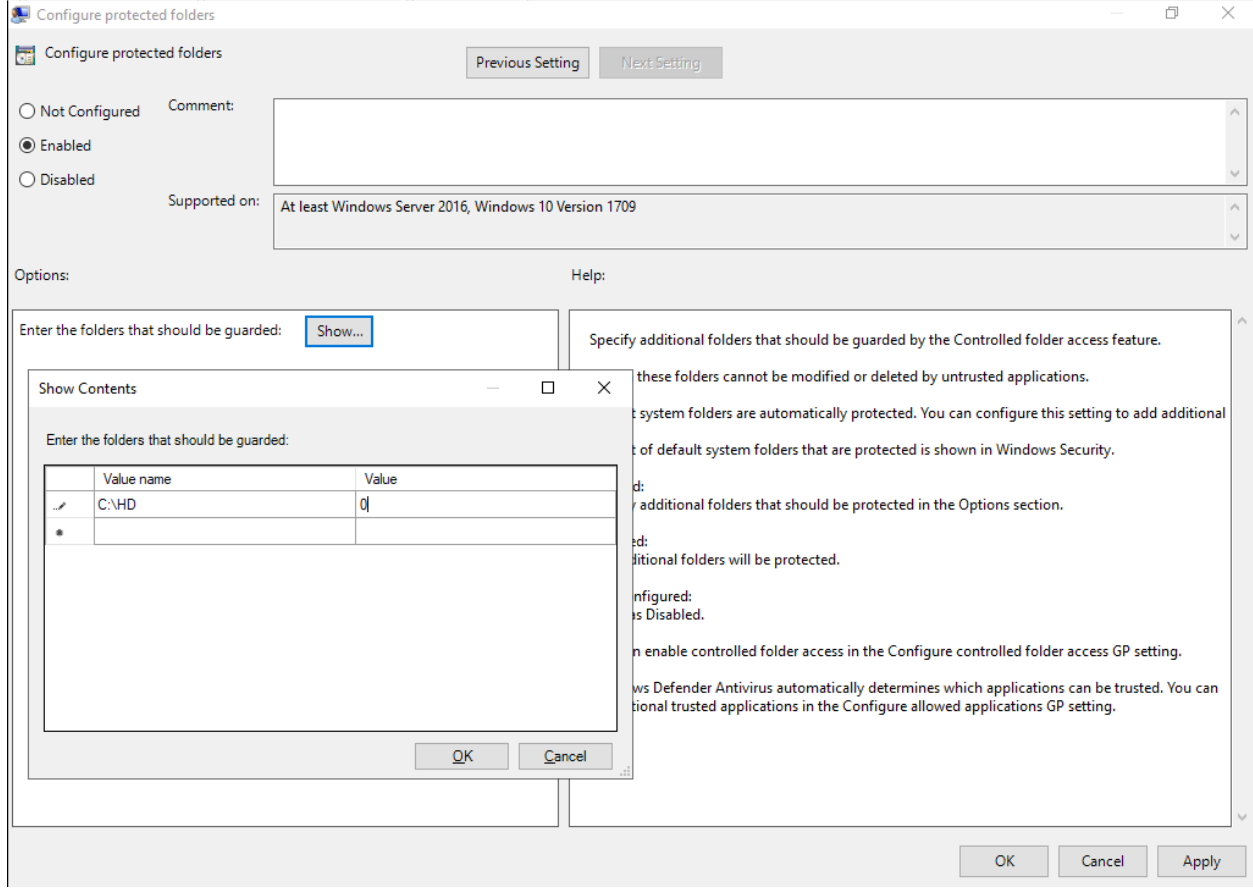
Configure Controlled Folder Access

Bu bölüme Exploit Guard bölümünde değinmiştım. Aynı ayarları Gpo ile de yapılandırabiliyoruz.



Configure Protected Folders

Yapınız içerisinde sizin önemli olan bir klasörün olduğunu varsayalım ve bu klasör üzerinde kesinlikle değişiklik yapılmasını istemiyorsanız bu kuralı aktif edebilirsiniz.



Network Protection

Prevent users and apps from accessing dangerous websites

İlgili kuralın aktif edilmesi durumunda reputasyonu düşük, tehlikeli kategoride yer alan domain lerden uygulama indirilmesi engellenmektedir. Audit mode ile başlanmasını tavsiye ederim.

Youtube Videoları

- <https://www.youtube.com/watch?v=6TiHx6Pbgns&t=2s>
- <https://www.youtube.com/watch?v=C5TNKypFNaQ&t=555s>

Faydalanılan Kaynaklar

- <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction-faq>
- <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/next-gen-threat-and-vuln-mgt>
- <https://docs.microsoft.com/en-us/windows/security/threat-protection/>
- <https://techcommunity.microsoft.com/t5/microsoft-defender-atp/introducing-a-risk-based-approach-to-threat-and-vulnerability/ba-p/377845>
- <https://techcommunity.microsoft.com/t5/microsoft-defender-atp/bg-p/MicrosoftDefenderATPBlog>
- <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/onboarding#endpoint-detection-and-response>
- <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/enable-attack-surface-reduction#group-policy>
- <https://yongrhee.wordpress.com/>

SON SÖZ

Güvenlik kavramını ele alırken öenmle dikkat etmemiz gereken bir nokta var hiç bir aman %100 güvende olmayacağız. Saldırı ve savunma bir satranç oyunudur. Bunu lütfen aklınızdan hiç bir zaman çıkarmayınız.



Yazmış olduğum bu E-Kitabı genç yaşta Mide Kanserine yenik düşen meslektaşım,dostum ve üstadıma adıyorum. En son konuştuğumuzda Hasanım yeni E-Kitabın ne zaman bitiyor, yayınla da artık okuyayım demiştin. Okumanı çok isterdim, yorumlarını duymak güzel olurdu ama olmadı,bu yaptığın olmadı güzel kardeşim 😞 Mekanın cennet olsun dostum.....



Acı Kaybımız, Uğur Demir' i Kaybettik

Zor günler geçirdiğimiz şu dönemde uzun süredir mide kanseri ile mücadele eden değerli ekip arkadaşımız Uğur Demir' in vefat haberi ile bir kez daha sarsıldık. Uzun süredir kanser ile mücadele eden değerli dostumuz ne yazık ki bugün mücadelesini kaybetmiştir.

En son görüştüğümüzde uzun süredir özlediği sektöre tekrar dönmek, eskisi gibi sektör için üretmek ve eko sistemi desteklemek için çok hevesliydi. Ancak bu isteği ne yazık ki gerçekleştiremedi. Çok sevdiğimiz bir kardeşimizi kaybetmenin acısını yaşıyoruz ve bu acının bir tarifi yok.

Kendisine Allah'tan rahmet, yakınlarına baş sağlığı diliyoruz.

ÇP
ÇözümPark
ÇEVRESEL MÜHÜRÜMÜZ

Bu E-Kitap çok değerli meslektaşım **Uğur DEMİR** anısına ithafen yazılmıştır.

Saygılarımla

Hasan DİMDİK | CEH | MVP | MCT