Microsoft Defender ATP ile Uçtan Uca Güvenlik

Microsoft Defender ATP ile Uçtan Uca Güvenlik

İçindekiler

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 likten 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 tanıyor diyerek cevaplayabilirim.

Bu yazı serisinde de MDATP' yi bilgim 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 sebentep 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)

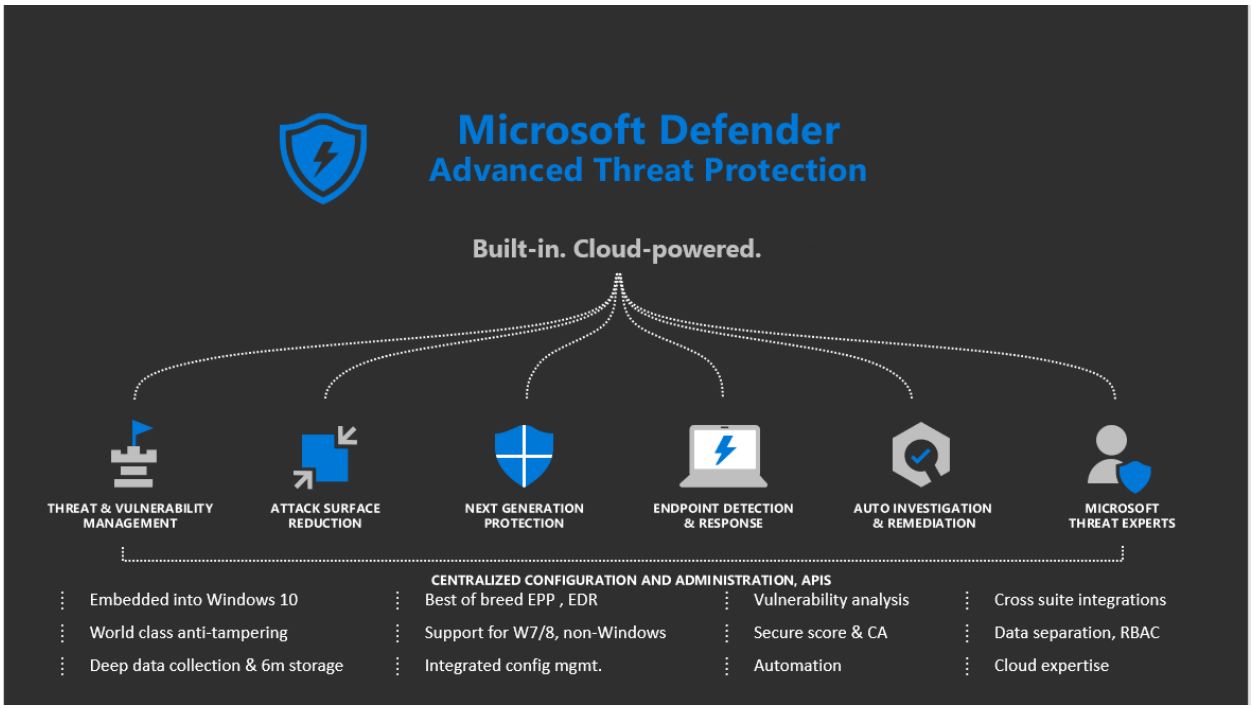
- Windows Server 2019
- Windows Server 2016
- Windows 10

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

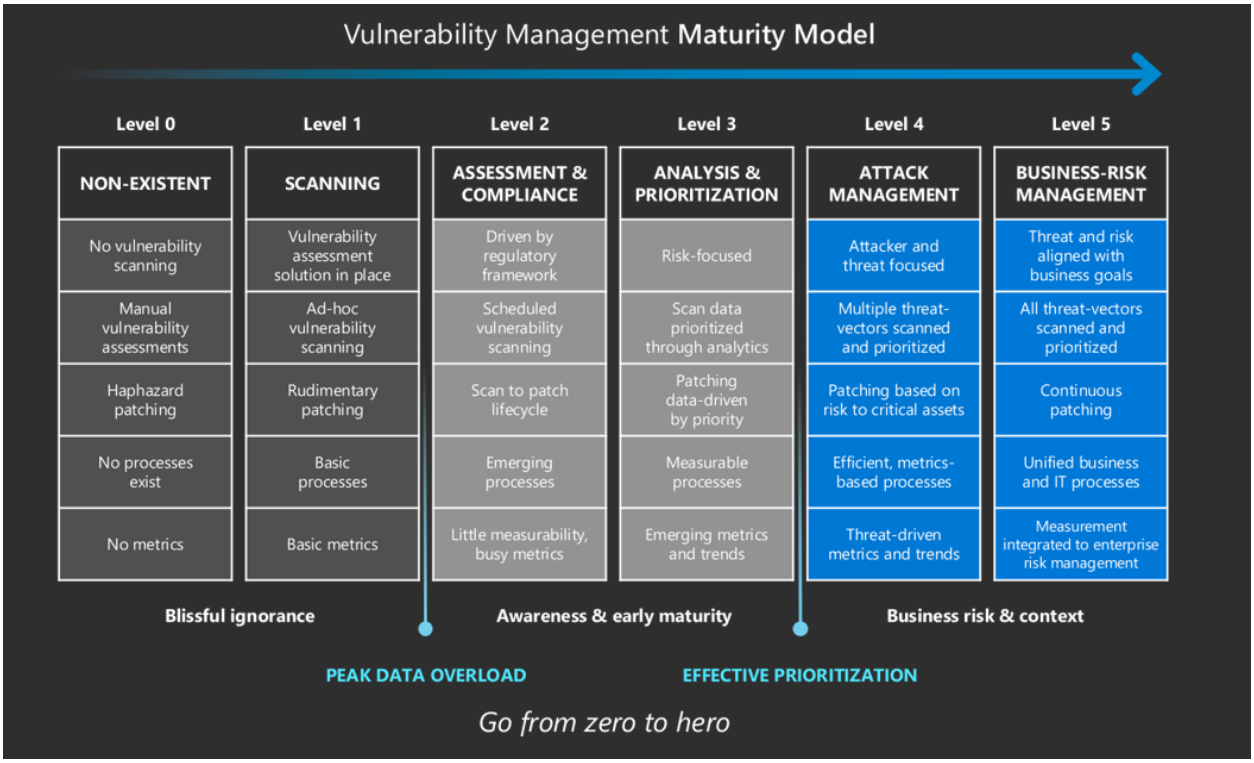
https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/configs/supported-configurations

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

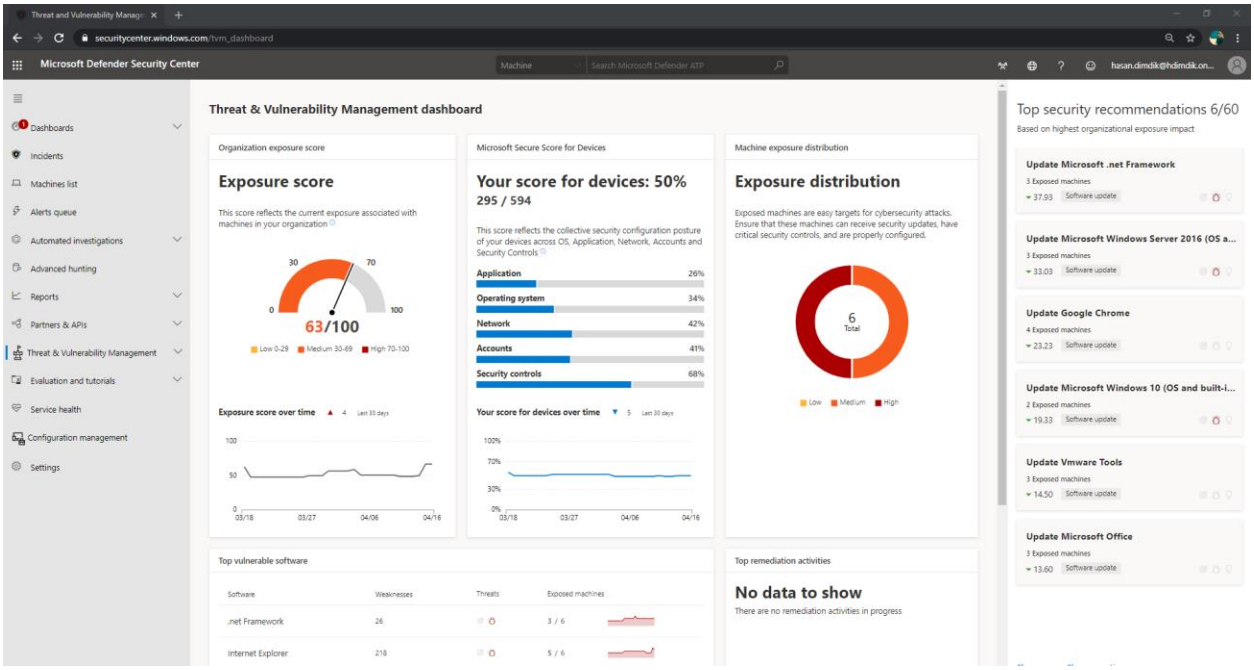


Threat & Vulnurability Management

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.

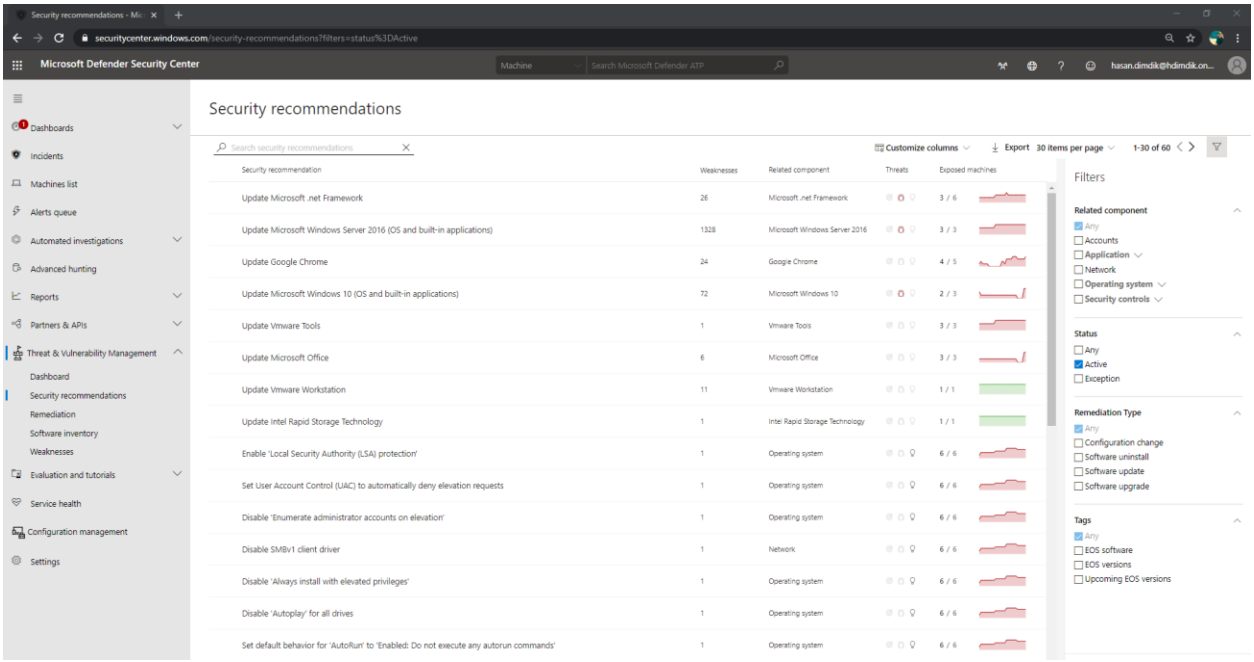


Threat & Vulnurability Management içerisinde yapımızdaki zaafiyetleri tek bir panel içerisinden görebiliyoruz. Bu bize iyileştirmeye nereden başlamamız gerektiğine dair bilgi de vermektedir. Diğer bir ifadeyle zayıf halkanın neresi olduğunu hızlıca belirleyebiliyoruz.

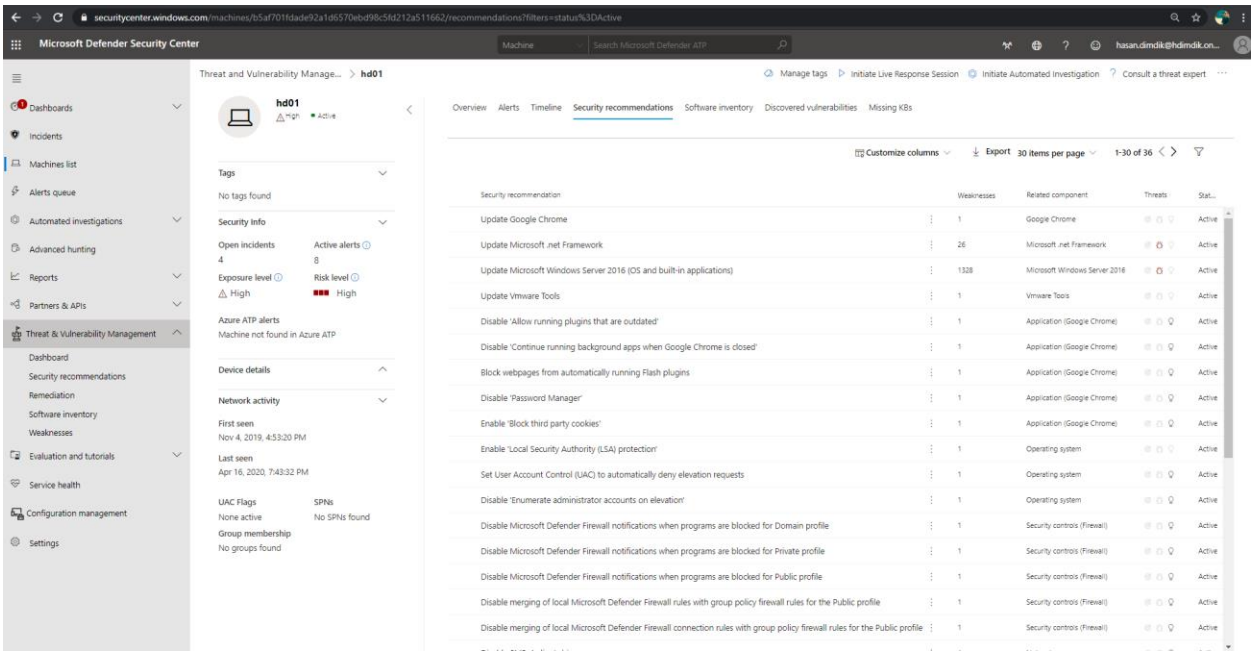


Security Recommendations

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 dait tavsiyelerde yer almaktadır.



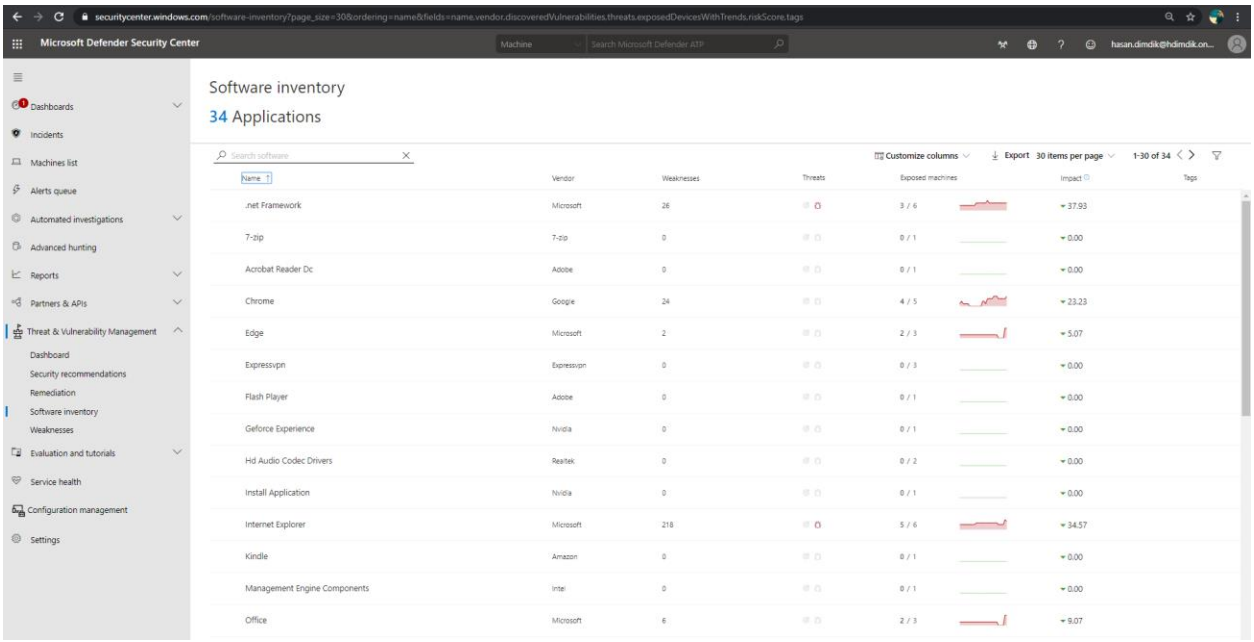
Güvenlik tavsiyelerini endpoint özelinde de raporlayabiliyoruz.



Software Inventory

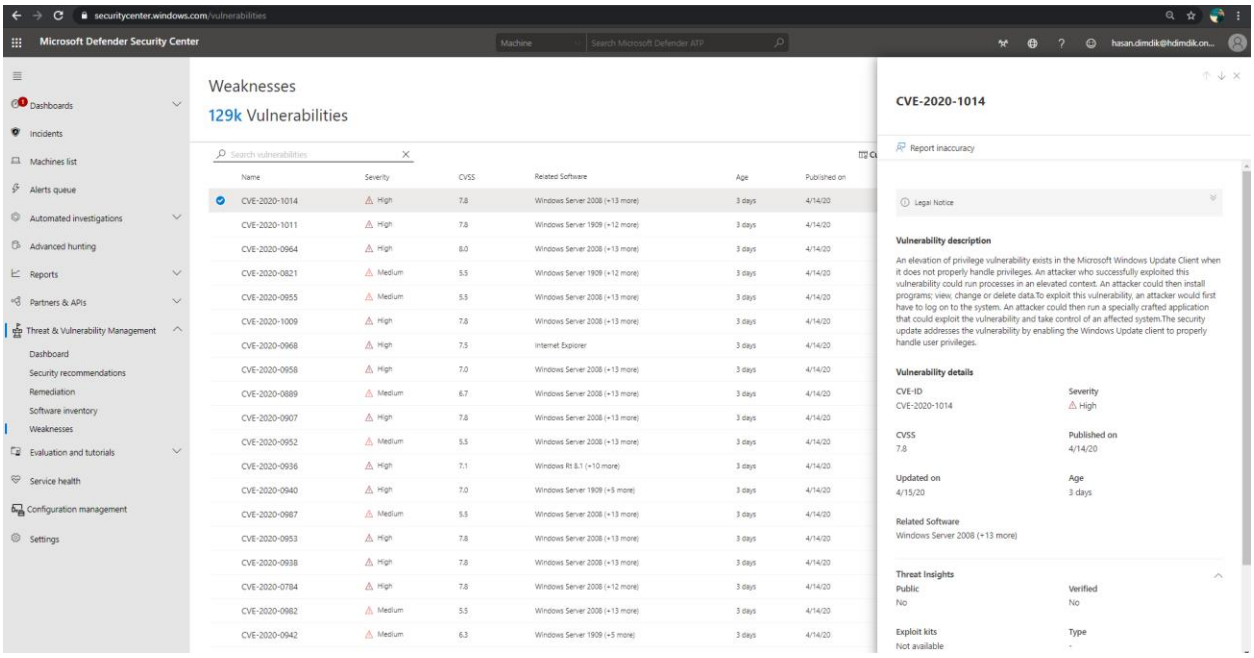
Şirketlerdeki en büyük sorunlardan bir tanesi kurum içerisinde yüklü olan uygulamaların bilinmiyor olması, diğer bir deyişle uygulama envanterine hakim olunamaması. Software inventory adından da anlaşıldığı gibi bu sorunumuzu çözmektedir. Elbette burdaki öncelikli amaç hangi uygulama

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



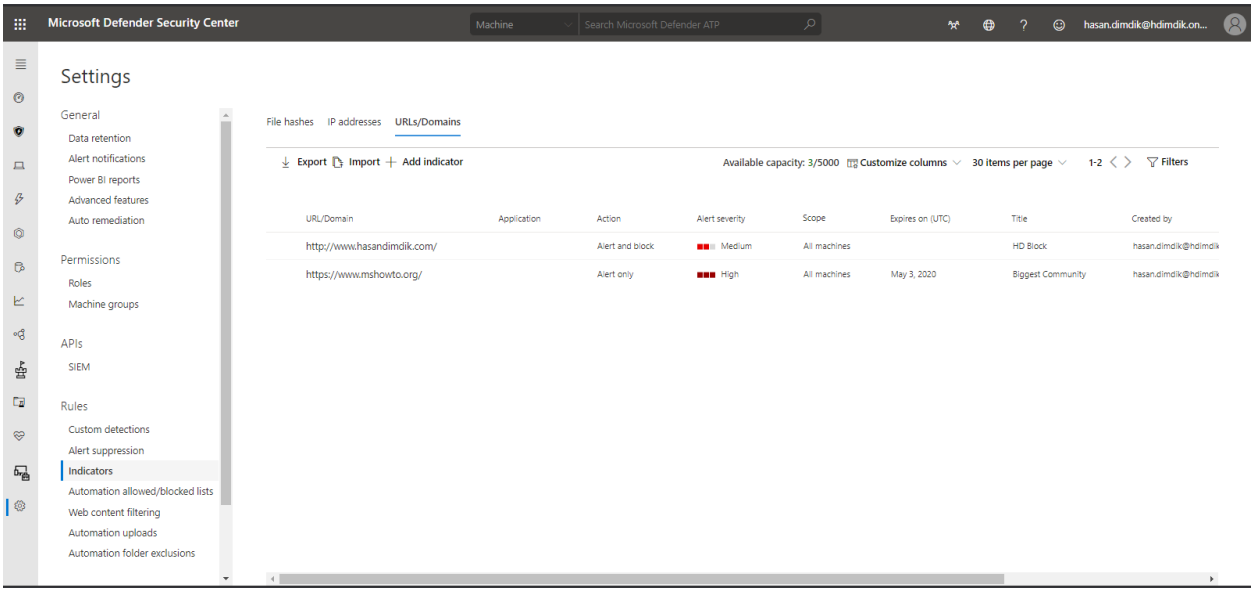
Weaknesses

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



Attack Surface Reduction

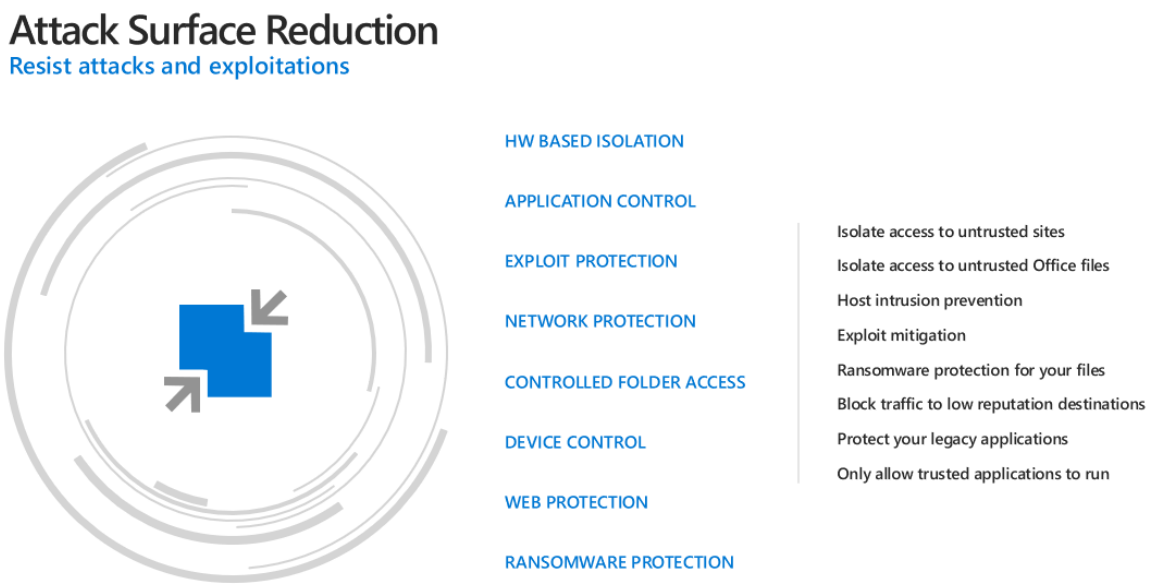
Atak yüzeyi kelimesini irdelediğimiz zaman saldırganın yapımız içerisine sızabileceği noktalar olarak değerlendirebiliriz. Savunan taraf olarak bizim görevimiz bu noktaları belirlemek ve daraltmaktır. Günümüzde artık bilgisayar kullanım alanları tamamen değişti. Bundan beş yıl öncesine baktığımızda herşey 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 heryerden 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 heryerden 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 daraltabilirize 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



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

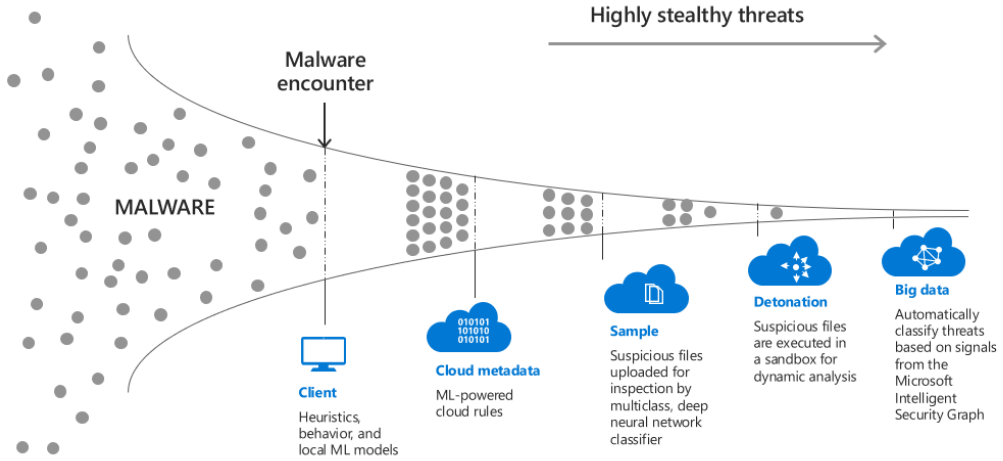
- Block executable files from running unless they meet a prevalence (1000 machines), age (24hrs), or trusted list criteria
- Block untrusted and unsigned processes that run from USB
- Use advanced protection against ransomware

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

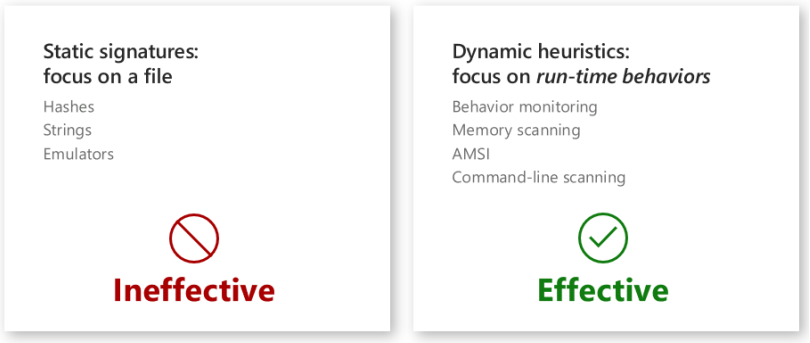
Bildiğiniz üzere imza tabanlı anti virüsler artık bizleri koruyamamaktadır. Kısmende olsa koruyabilmektedir diyebilirim ! (Yorumu size bırakıyorum 😊) Günümüz atakları ise artık daha sofistike , imza tabansız,fileless ve/veya Hardware lerin açıklarından faydalanılarak gerçekleştirilen ataklar olarak karşımıza 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 etmektdir.



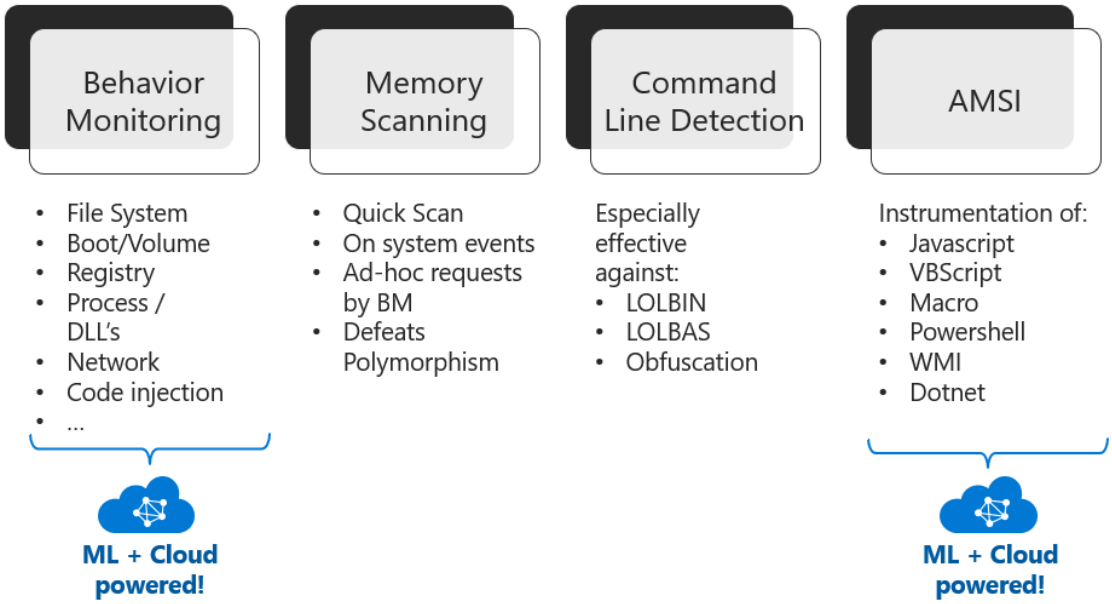
Teknik olarak Next Generation Protection nedir dersek bunu üç başlık altında toplayabiliriz.

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.

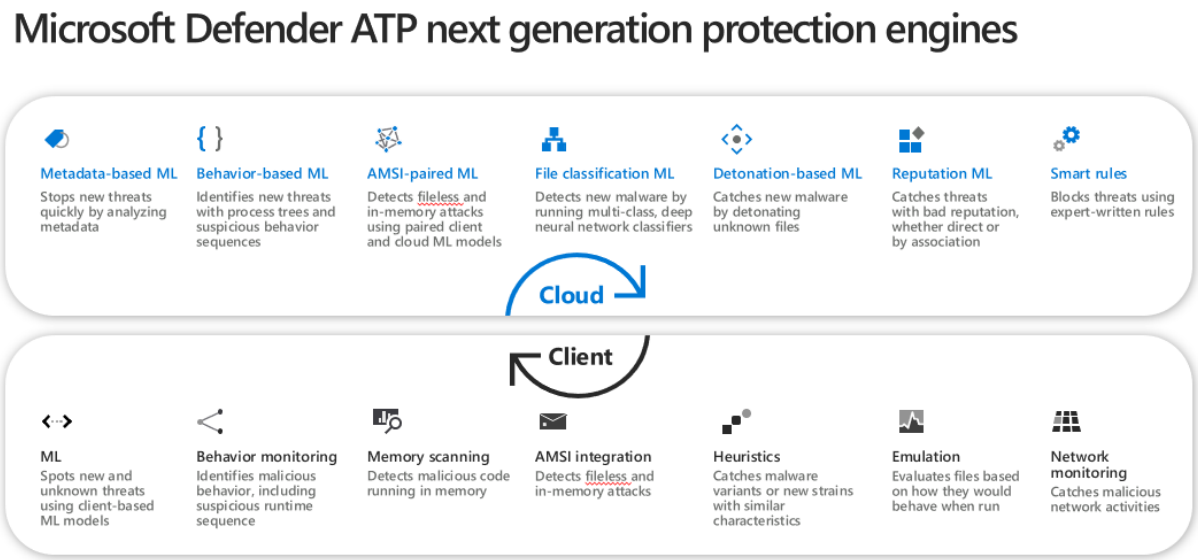


Davranışsal analiz elbette arka planda makina öğrenmesini kullanmaktadır ve aşağıdaki dört başlık altında etkin koruma sağlamaktadır.



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 sıfırıncı gün atağından bahsedecek olursak klasik yöntemlerle bunu koruyamayacağımıza hemfikiriz. ATP ise aşağıda yer alan koruma motorları sayesinde etkin koruma sağlamaktadır.



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

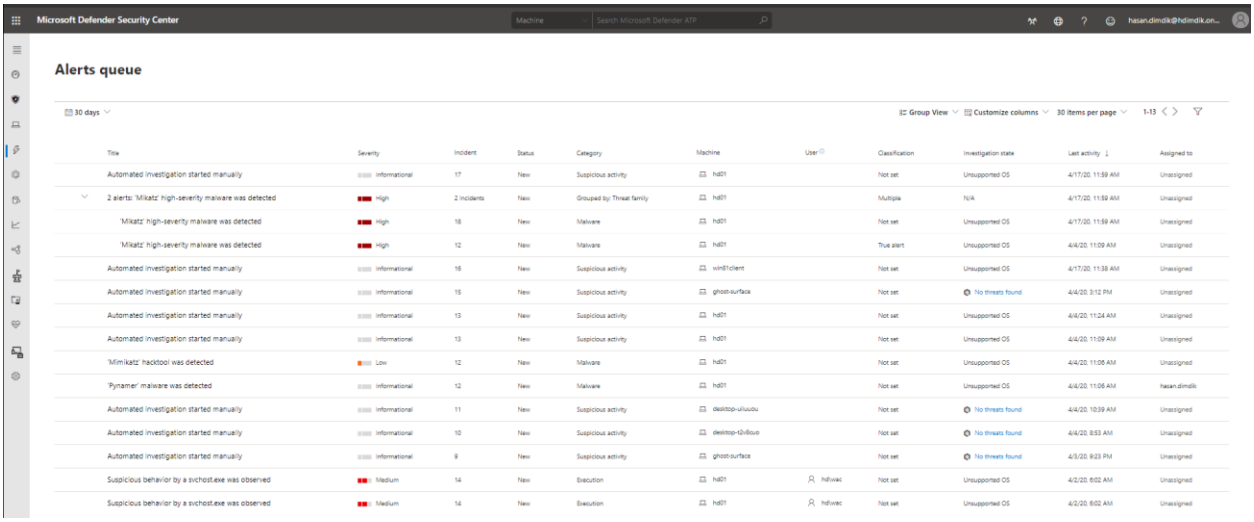
Tam bir koruma sağlamak istiyorsanız elbette sıkı şekilde gerekli updateleri yapıyor olmamız gerekmektedir. Bu noktada iki farklı update den söz ediyoruz. İlki **Protection updates**. MAPS periyodik olarak güvenlik updatelerini kontrol edip yeni gelen update varsa indirilmektedir. Aynı zamanda **Product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

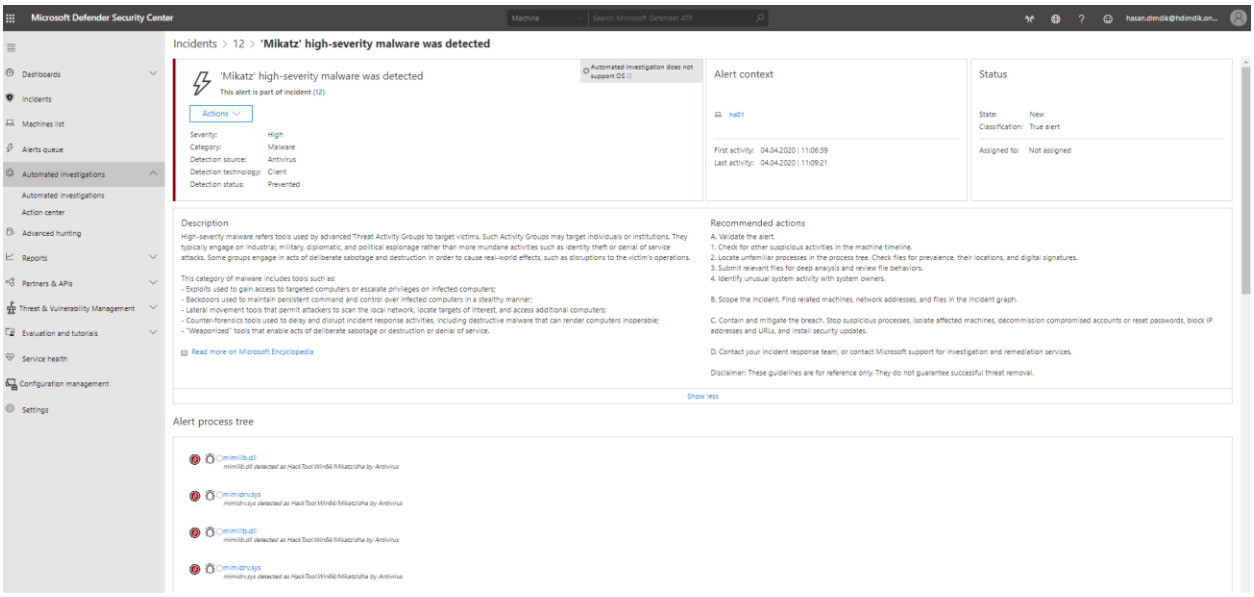
Endpoint Dedection & Response

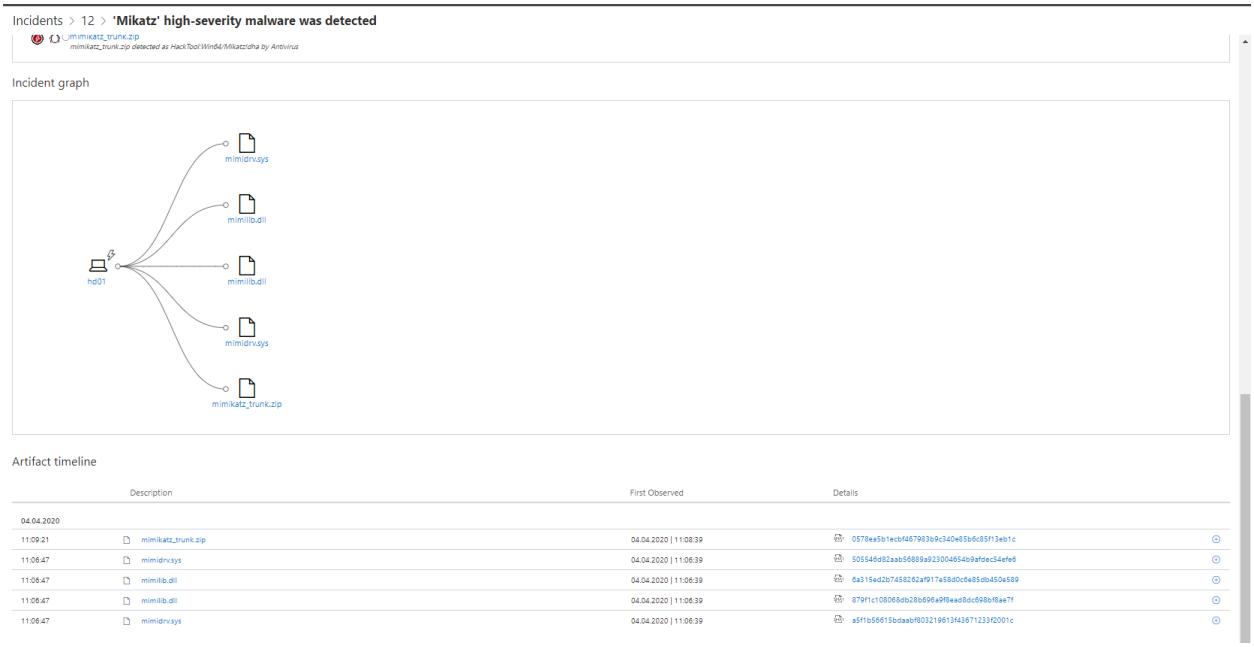
- CORRELATED POST-BREACH DETECTION
- INVESTIGATION EXPERIENCE
- INCIDENT
- ADVANCED HUNTING
- RESPONSE ACTIONS (+EDR BLOCKS)
- DEEP FILE ANALYSIS
- LIVE RESPONSE
- THREAT ANALYTICS

MDATP nerdeyse gerçek zamanlı olarak tehditleri yakalar ve ilgili zararlıyı etkisiz hale getiririr. Elbette burada diğer önemli nokta ise ilgili atağın detaylarını görebilmektir. Bu analiz bize ilgili atağın/zararlının 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.

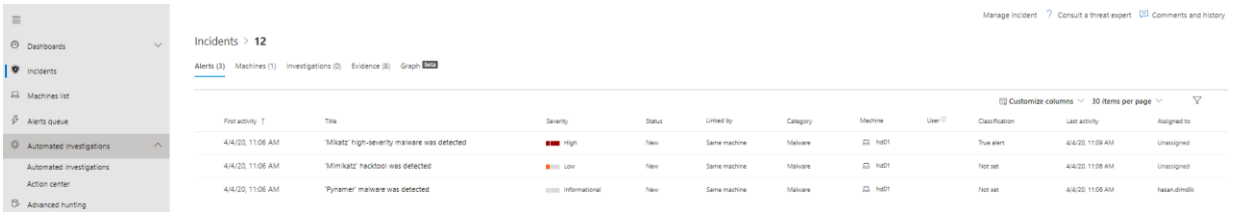


Örneğin ilgili sunucumda mimikatz çalıştırılmak istenmiş ve MDATP tarafından yakalanıp malware olarak kategorilendirilmiş. Detaylı olarak da process ağacını görebiliyoruz.

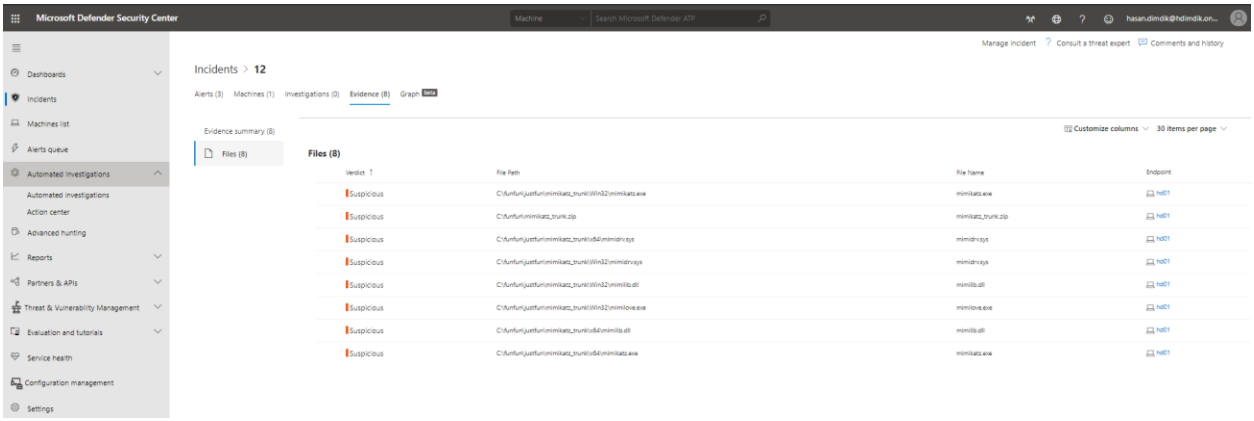




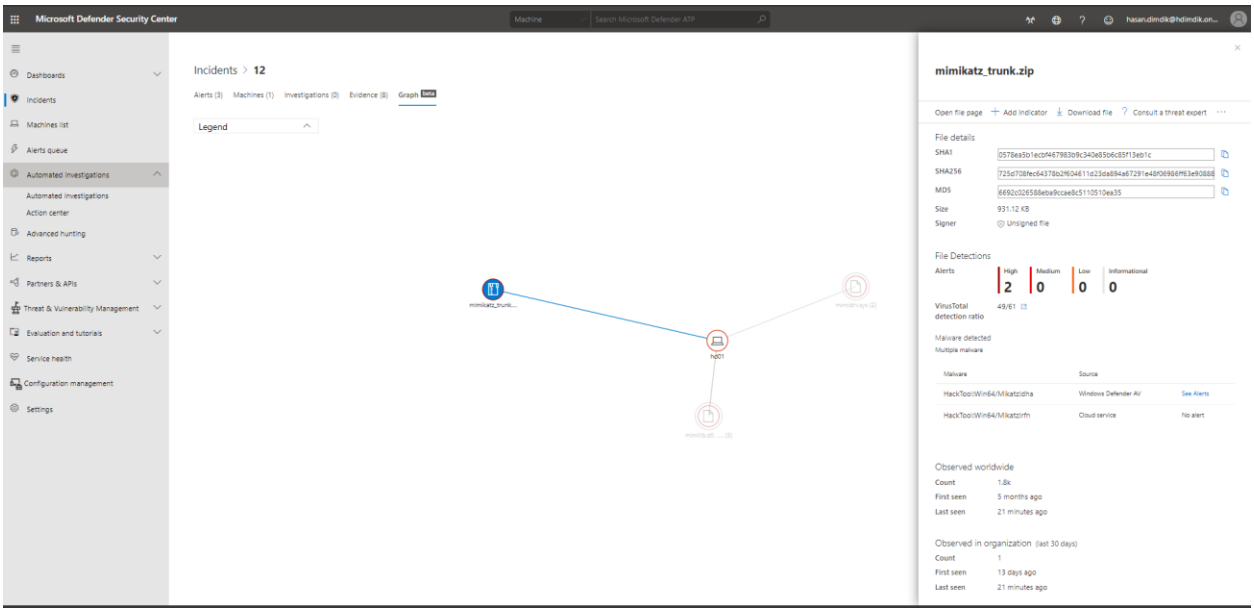
Actions' ı tıkladıktan sonra **Open Incident Page** kısmına geliyorum ve üç farklı alarm aldığımı görüyorum.



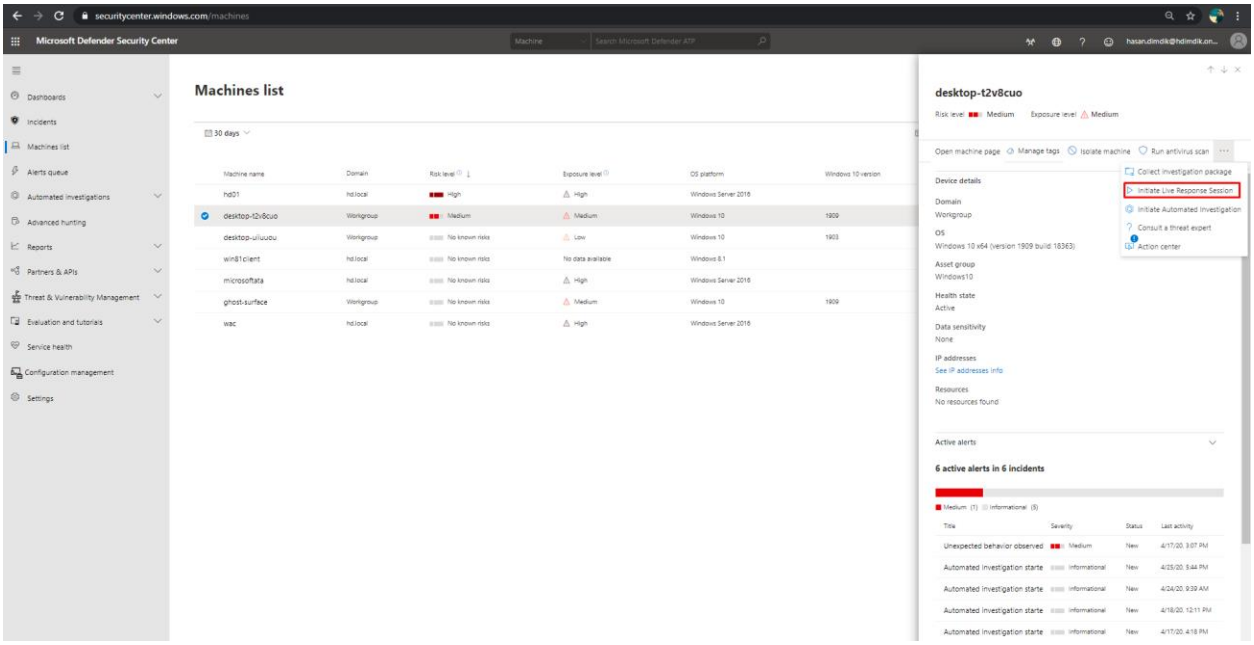
Evidence kısmında ise kanıt olarak nelerin şüpheli olarak algılandığını belirtmektedir.



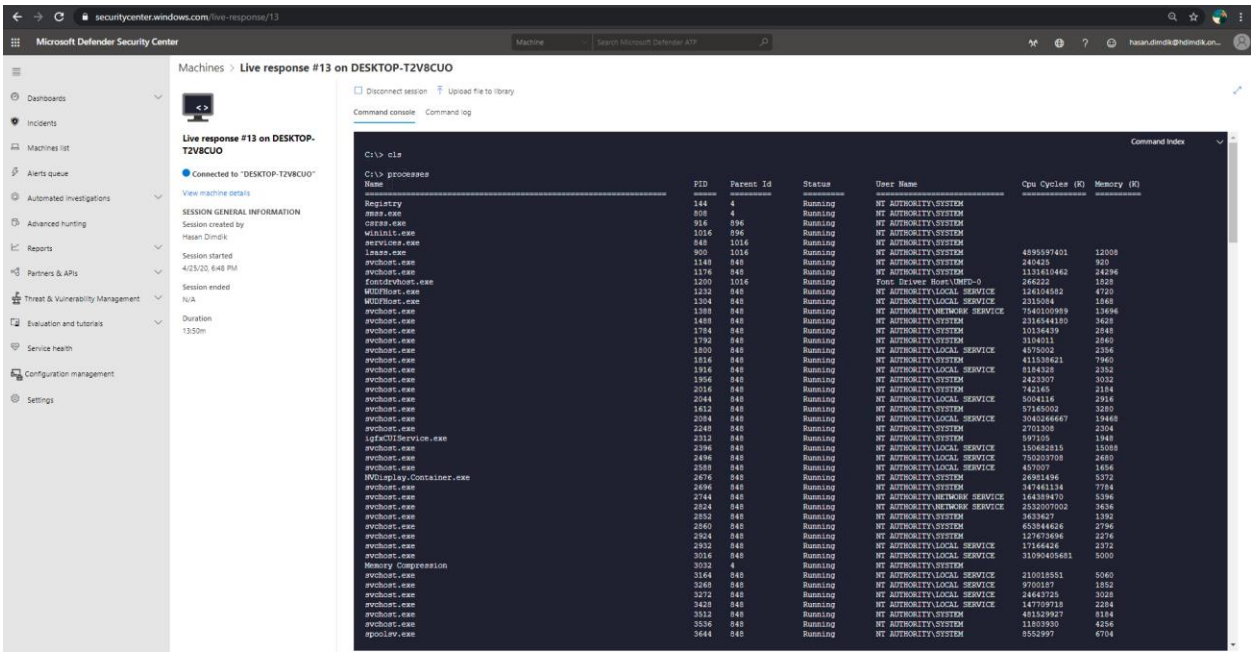
Graph ise, zararlı nereye bulaştı, bulaştığı yerden başka yere geçti mi ? gibi verileri görsel olarak görmemize imkan sağlamaktadır veya diğer bir ifadeyle zararlının davranış analizini görmemize imkan sağlamaktadır.Mimikatz_trunk.zip i tıkladığımda iki farklı servis tarafından zararlı olarak algılandığını görüyoruz. Son olarak indicator seçeneği ile block kuralı oluşturabiliriz.



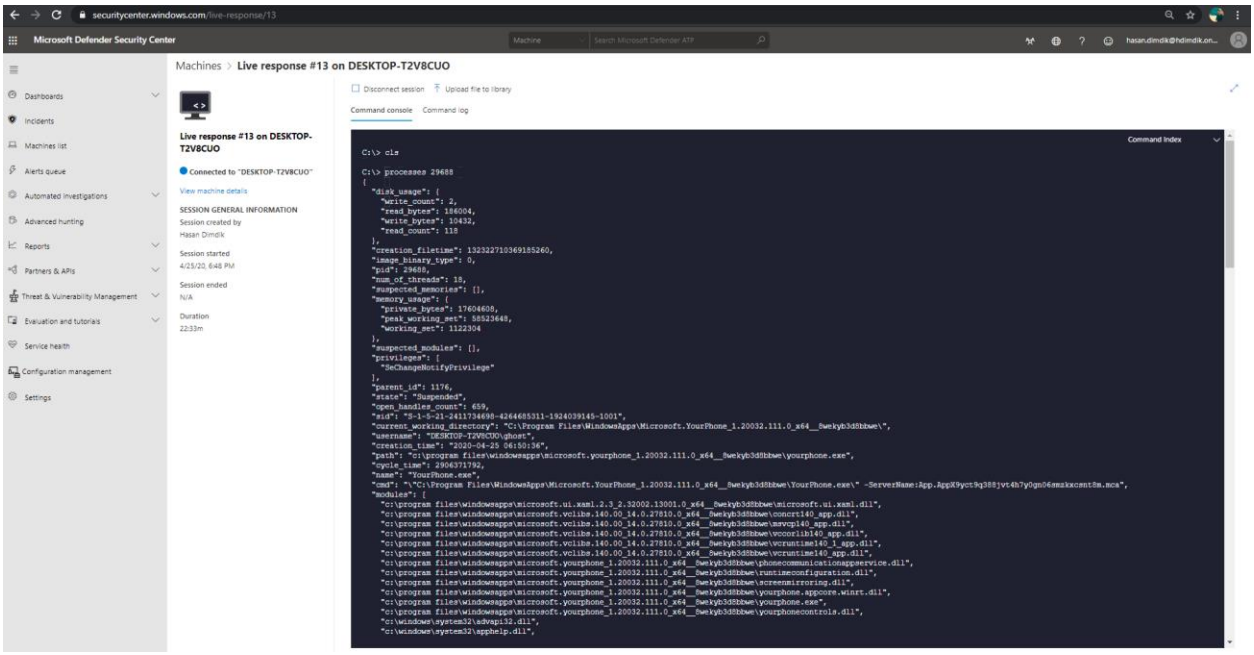
Endpointlerimiz üzerinde Live Session başlatabiliyoruz. Bu sayede canlı olarak şüphe oluşturan bir durum var ise incelenebilmektedir.



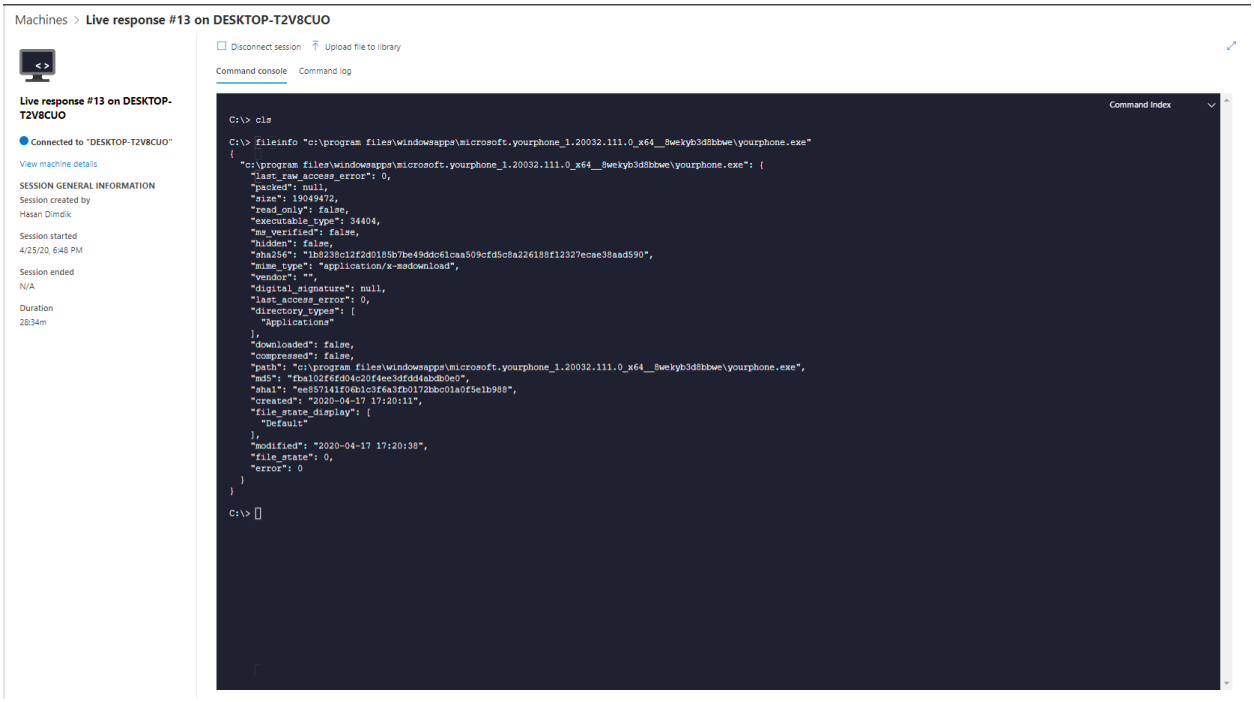
Örnek olması açısından canlı oturum başlatıyorum. **Process** komutu ile istemci makinamda çalışan süreçleri görüyorum.



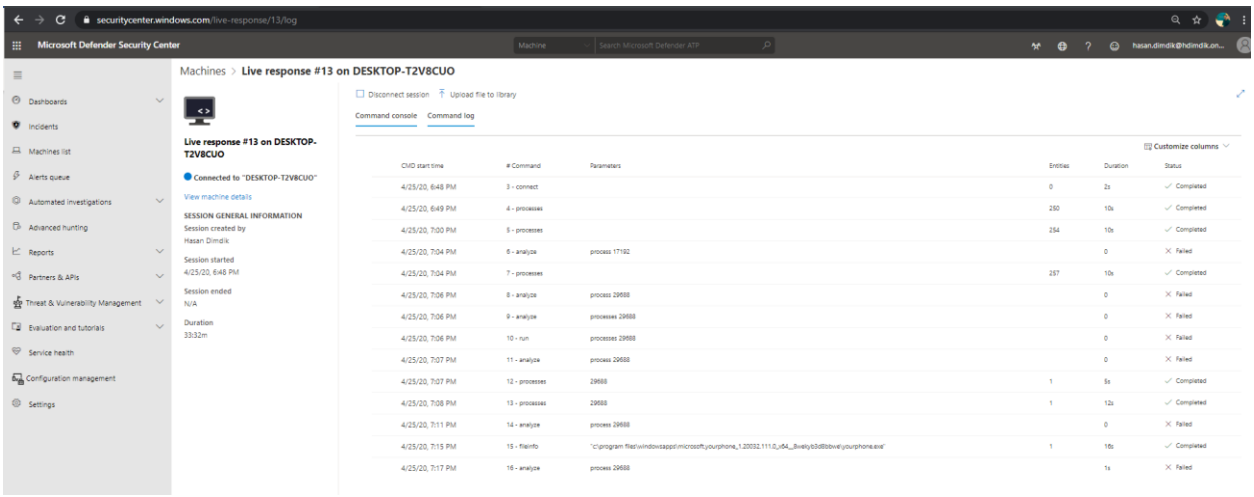
Örneğin Yourphone isimli bir işlem gördüm ve bunun normal olmadığını varsayalım. **Processes 29688** komutu ile işleme ait detay bilgiye ulaşabiliyoruz.



Fileinfo komutu ile dosyamız hakkındaki bilgilere ulaşabiliyoruz ve daha fazlasını komut satırı ile yapabiliyoruz tabiki bunların en önemlisi analiz yapabiliyor olmamızdır. Bunun yanında kendi yazdığınız Powershell scriptleri çalıştırıp iyileştirmelerimizi yapabiliyoruz. Bu özellik özelikkle SOC ekipleri için faydalı olacaktır.



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



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

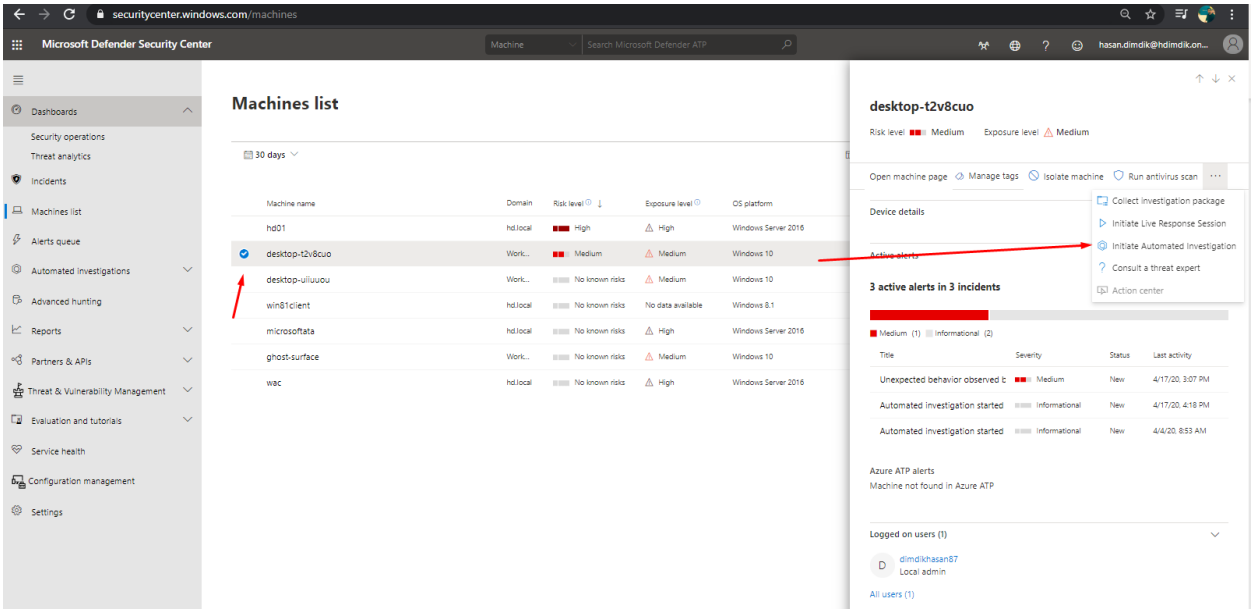
Auto Investigation & Remediation

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.

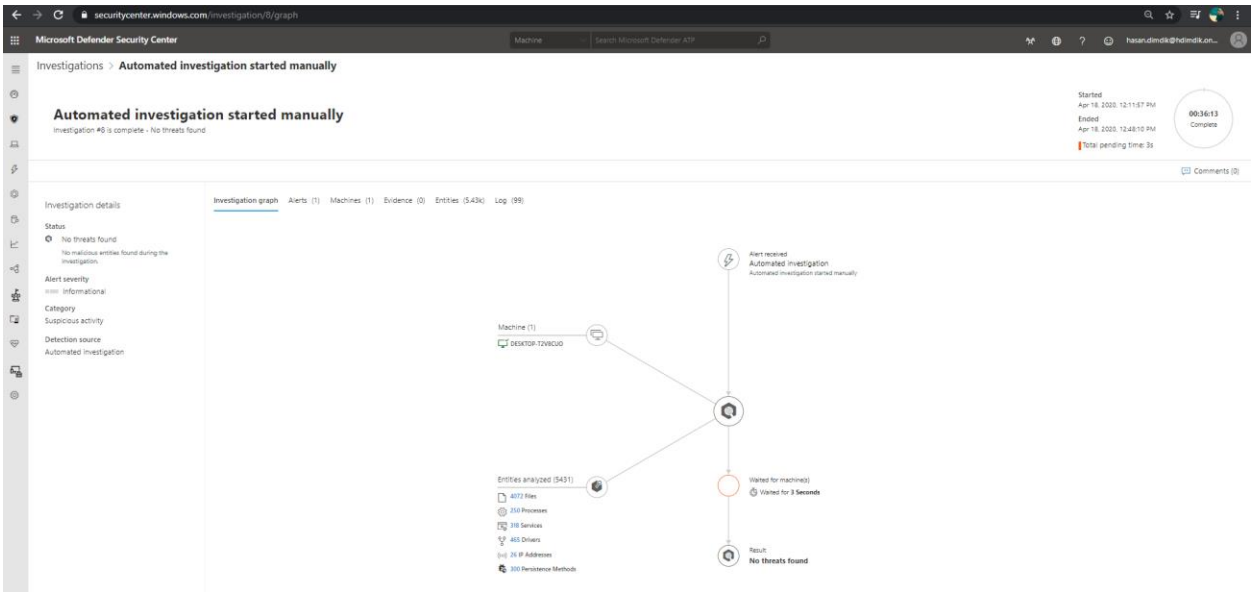
- Windows Server 2019
- Windows 10, version 1709 (OS Build 16299.1085 with **KB4493441**) or later
- Windows 10, version 1803 (OS Build 17134.704 with **KB4493464**) or later
- Later versions of Windows 10

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

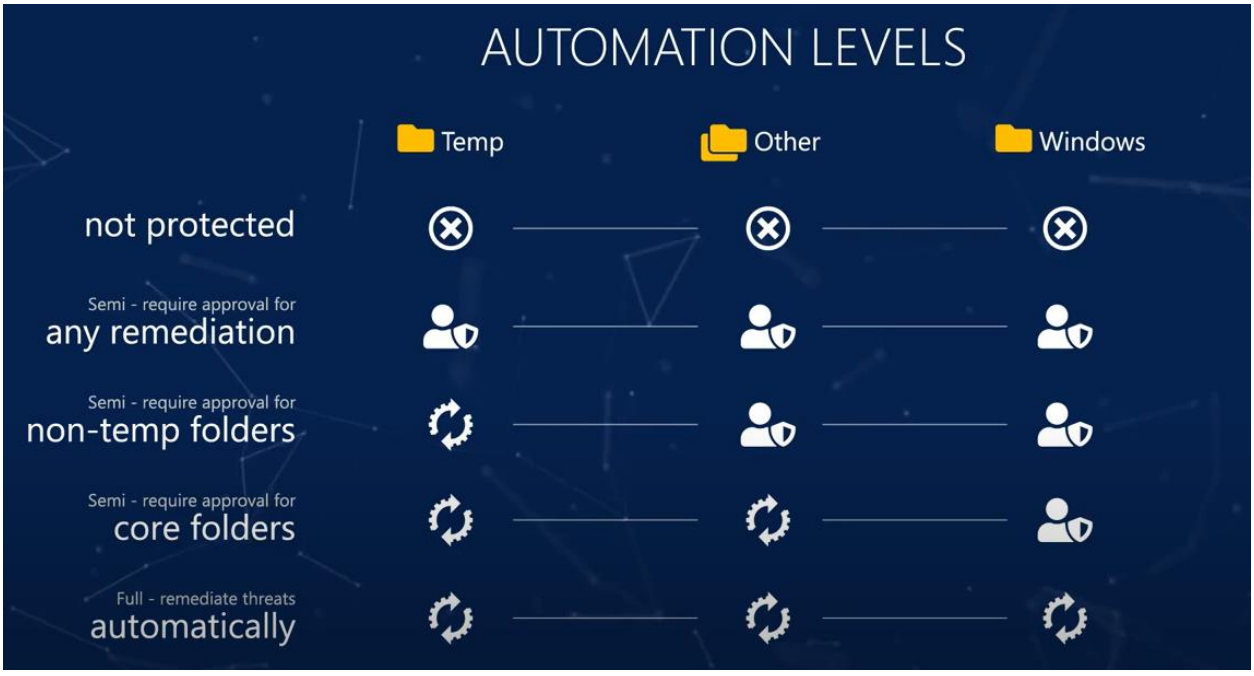
Örneğin aşağıdaki son kullanıcı bilgisayarında **Automated Investigation** başlattım.



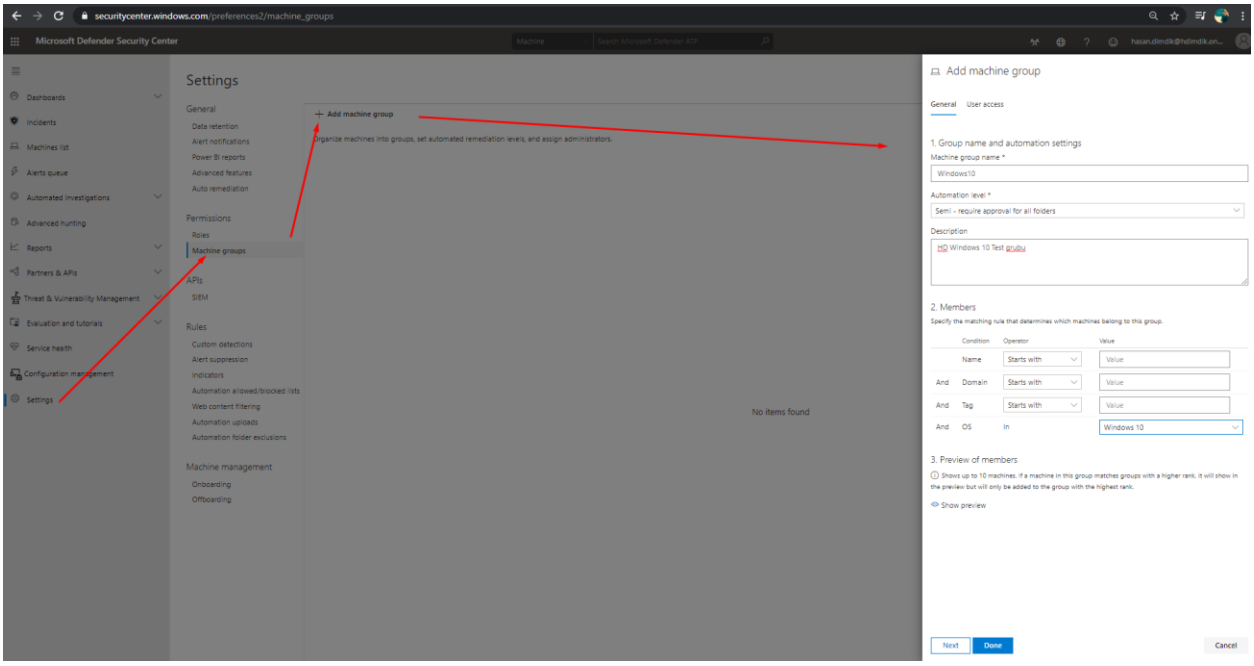
Bu bölümü kullanılmasının en temel sebeplerinden bir tanesi elbette hali hazırda bir zararlı yakalanmıştır veya alarm oluşmuştur ve araştırma başlatılabilir. Örneğimde zararlı olmadığı için daha sade sonuç getirdi. Bu noktadan sonra artık hangi processler başlamış, hangi registry değeri değiştirilmiş 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 aldırmaktır. 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.

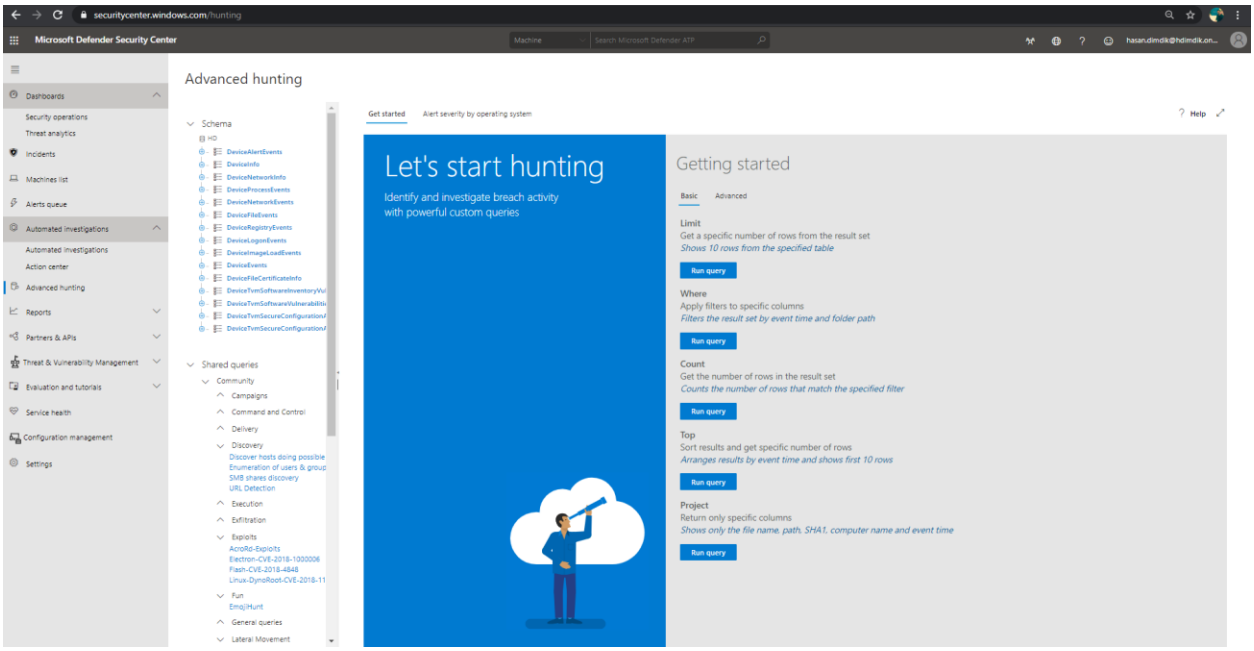


Advanced Hunting

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.

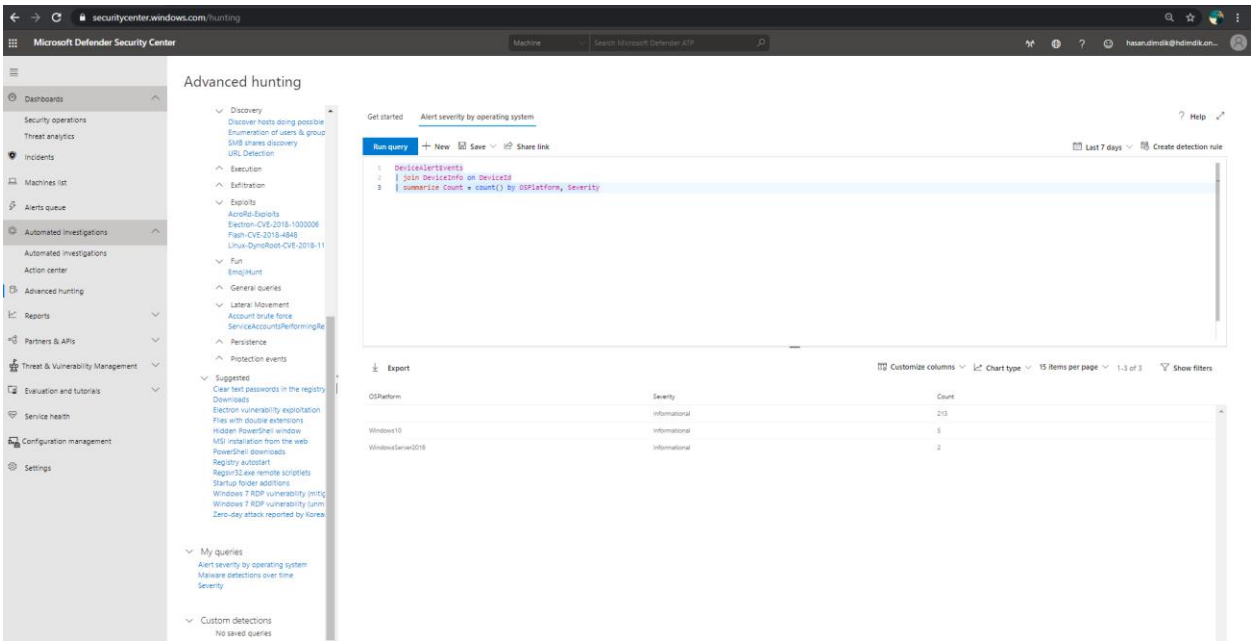
Akıllara elbette şu soru gelmektedir. Sorgu diline hakim değilim veya bilgim yok, bu durumda ilgili bölümü nasıl kullanacağım. Hemen cevaplayalım,

Microsoft yeterli sayıda hazır sorguları zaten panele eklemiş durumda.



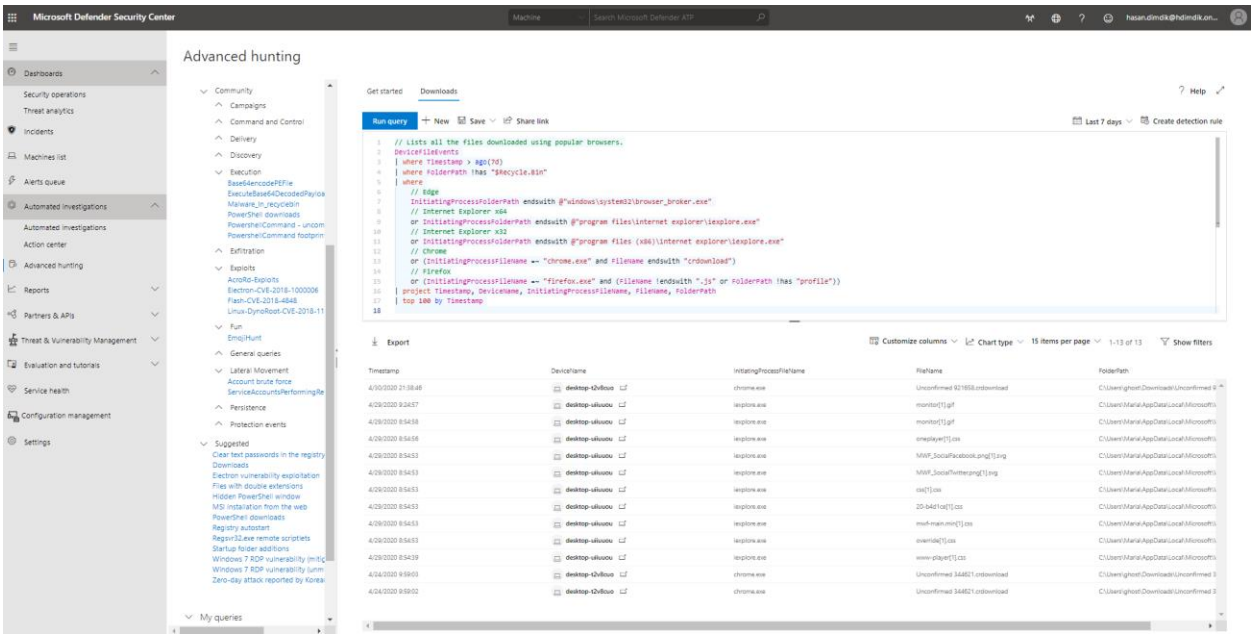
Örneğin aşağıdaki sorgu bize işletim sistemi özelinde alınan alarmları listeyecektir.

```
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
```



Sorgulara baktığımız zaman nerdeyse güncel olan tehditlerin sorguları hali hazırda geldiğini görüyoruz. Elbette sizlerde kendi sorgularınızı yazıp kullanabilirsiniz.

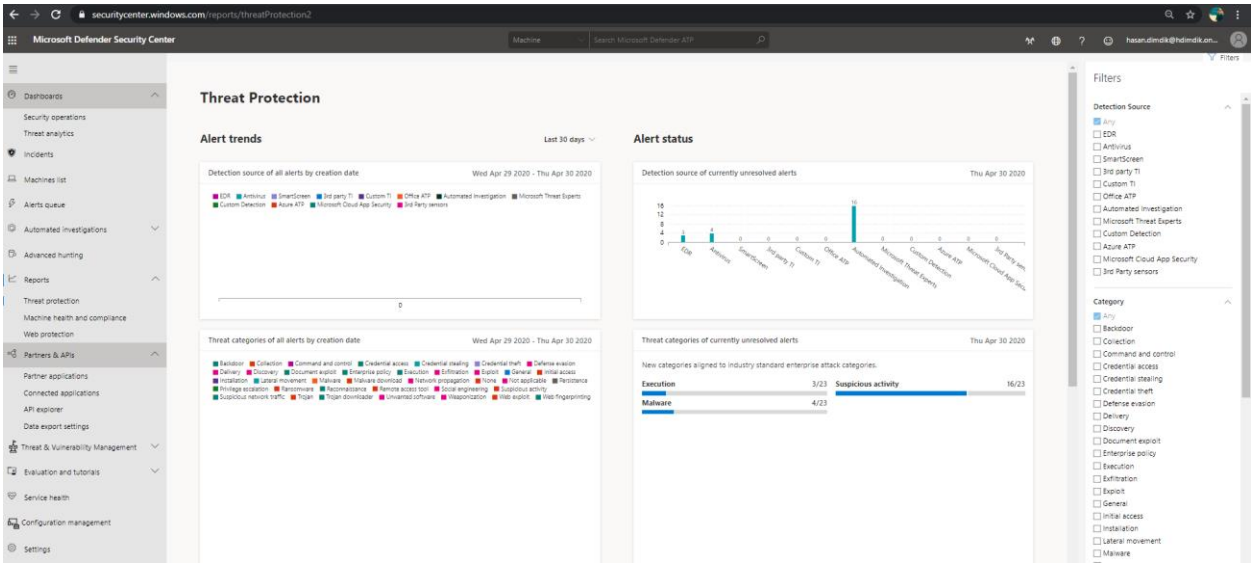
Daha detaylı bilgi için aşağıdaki linkler faydalı olacaktır.

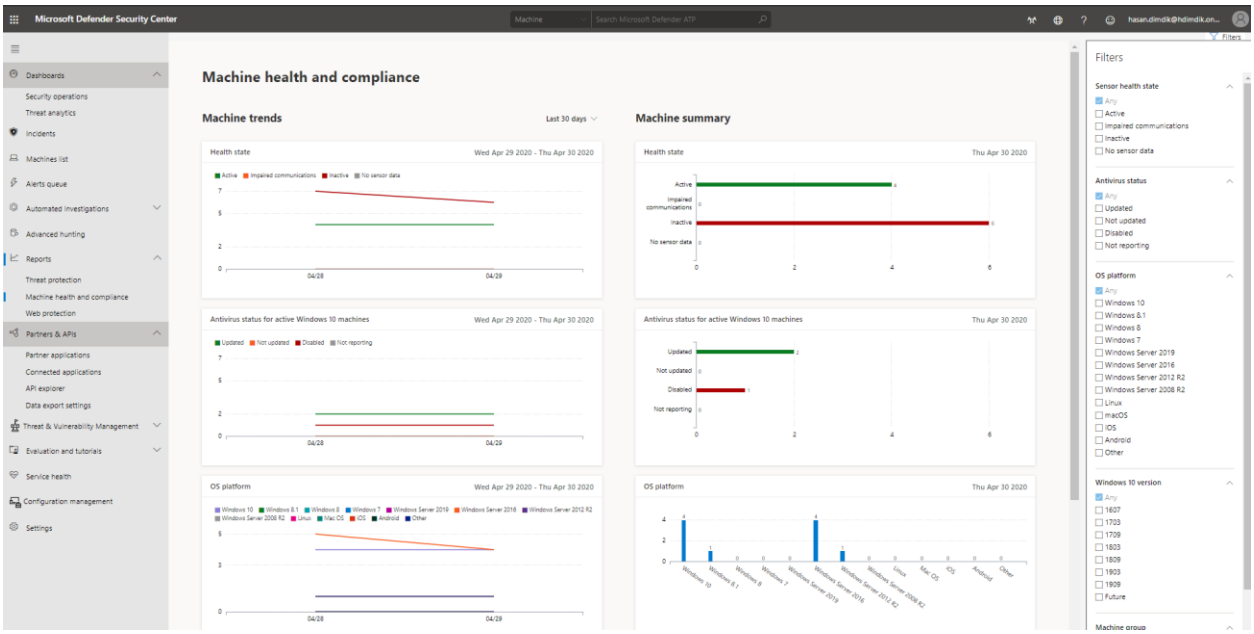
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/advanced-hunting-query-language

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/advanced-hunting-overview

Reports

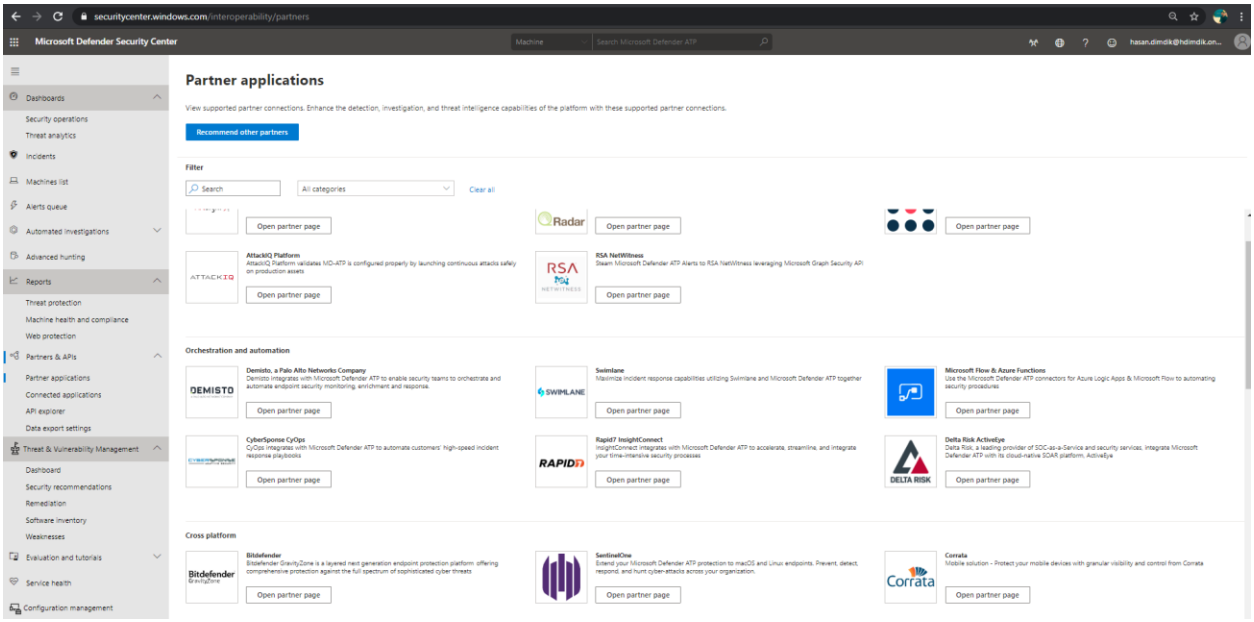
Adında anlaşılacağı gibi yapımızda aktivitelerin raporlandığı , algılanan tehditlerin hangi teknoloji(EDR,Antivirüs vb) tarafından yakalandığı, tehditin alarm seviyesi gibi High Level olayları görsel olarak görebileceğimiz basit anlaşılır arayüze sahip olan raporlama arayüzünün olduğu alan diyebiliriz.





Partners & API

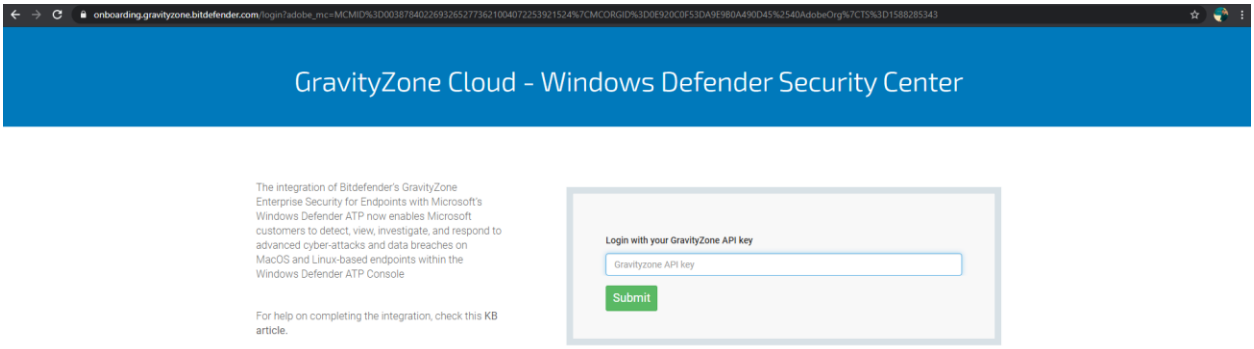
Bildiğiniz üzere Microsoft birden çok 3rd party vendor ile işbirliği yapıyor ve ilgili firmaların çözümleri ile Defender ATP' yi bağlayabiliyoruz.



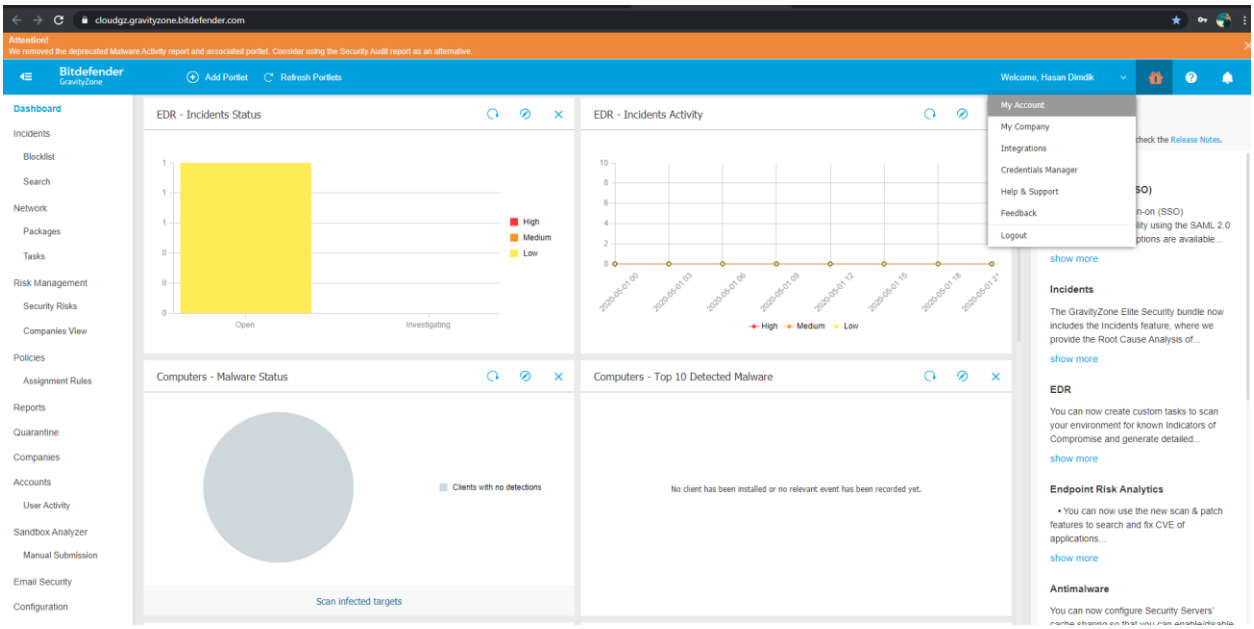
MDATP Bitdefender GravityZone Entegrasyonu

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

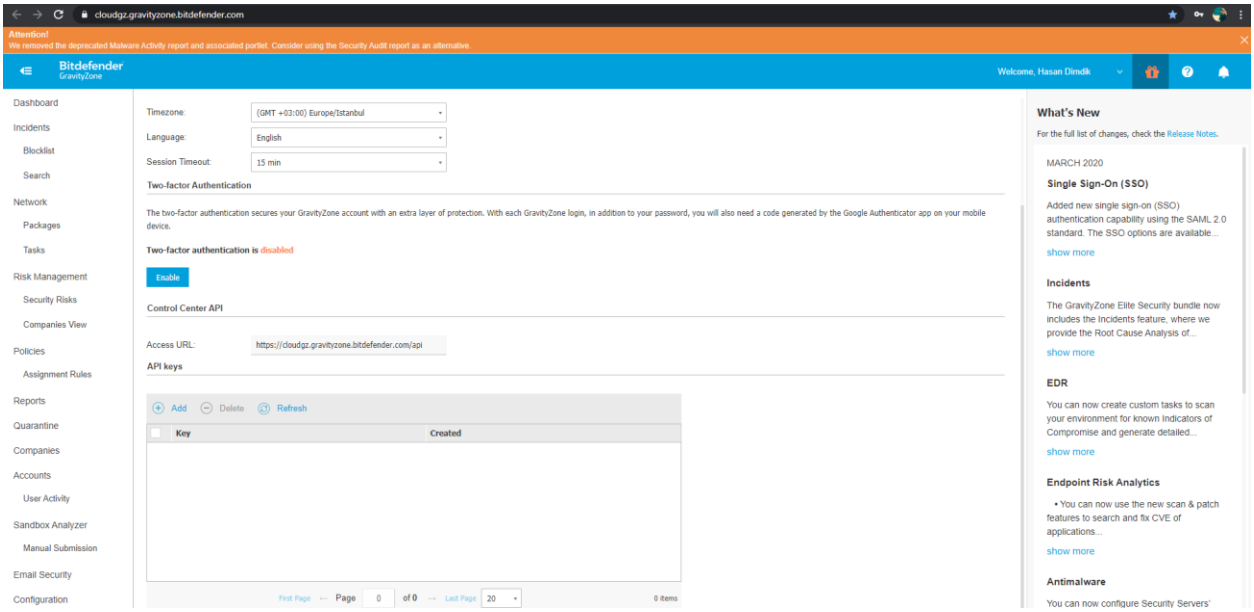
Login butonuna tıkladığımda API key girmem gerektiğini belirtiyor.

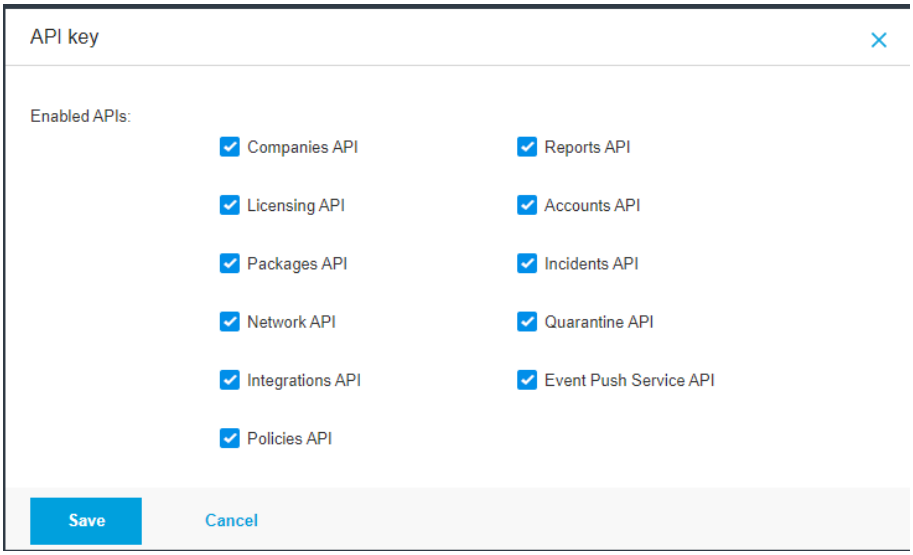


İlgili API Key' i almak için Bitdefender portalında yer alan **My Account** bölümüne geliyorum.

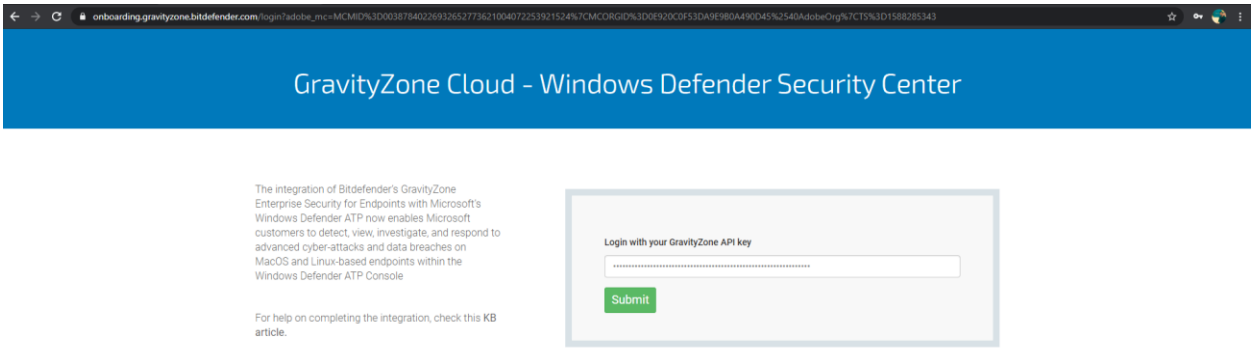


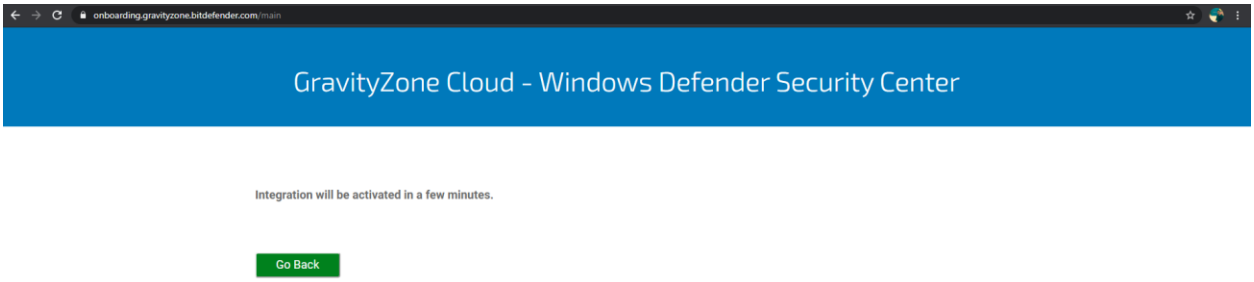
API keys kısmında Add butonuna tıklıyorum.





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



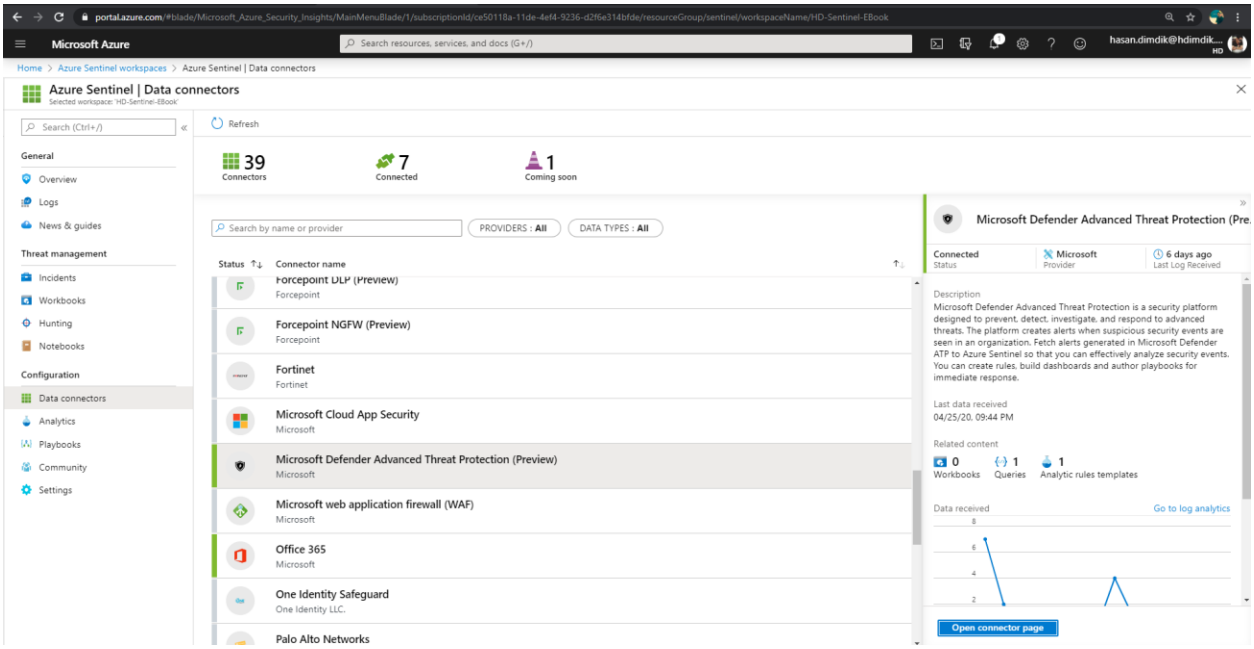


Bu adımla birlikte entegrasyonu tamamlamış oluyoruz. Peki bize nasıl bir faydası olacak? Özellikle Linux,android veya MacOs işletim sistemi kullanıyorsanız ilgili entegrasyonla birlikte bu işletim sistemleri üzerindeki zararlı faliyetleri veya virüs bulunması durumunda Security Center içerisinde de görebilme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

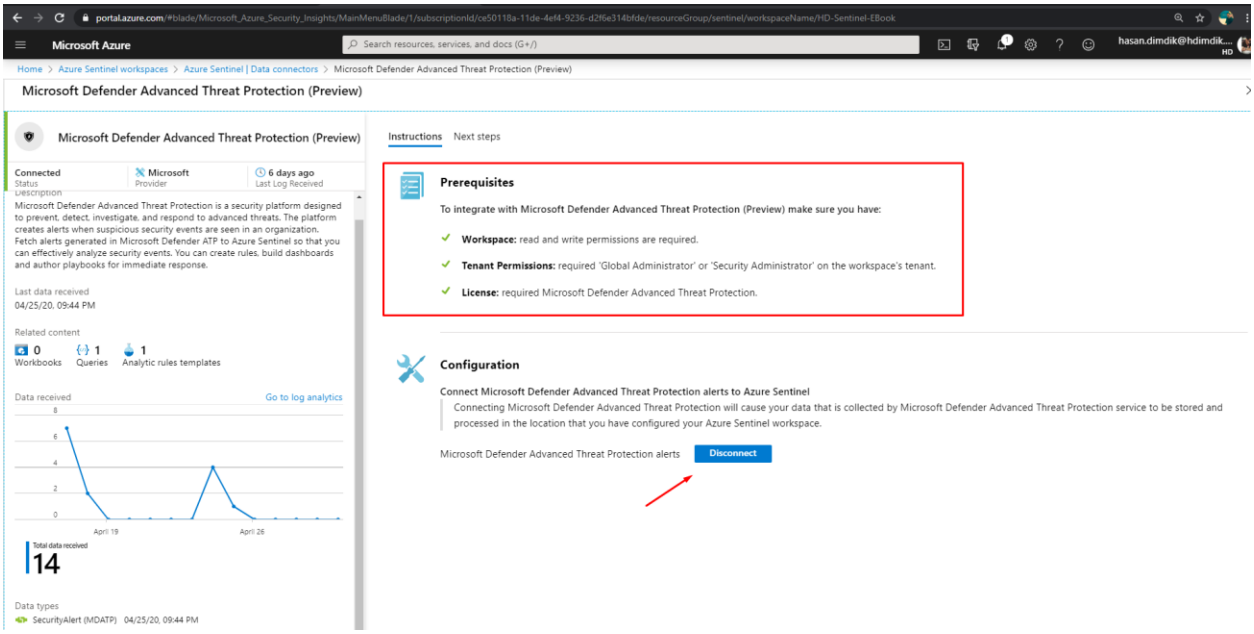
Kaynak : https://www.bitdefender.com/support/bitdefender-gravityzone-and-microsoft-windows-defender-atp-integration-1987.html

MDATP Azure Sentinel Entegrasyonu

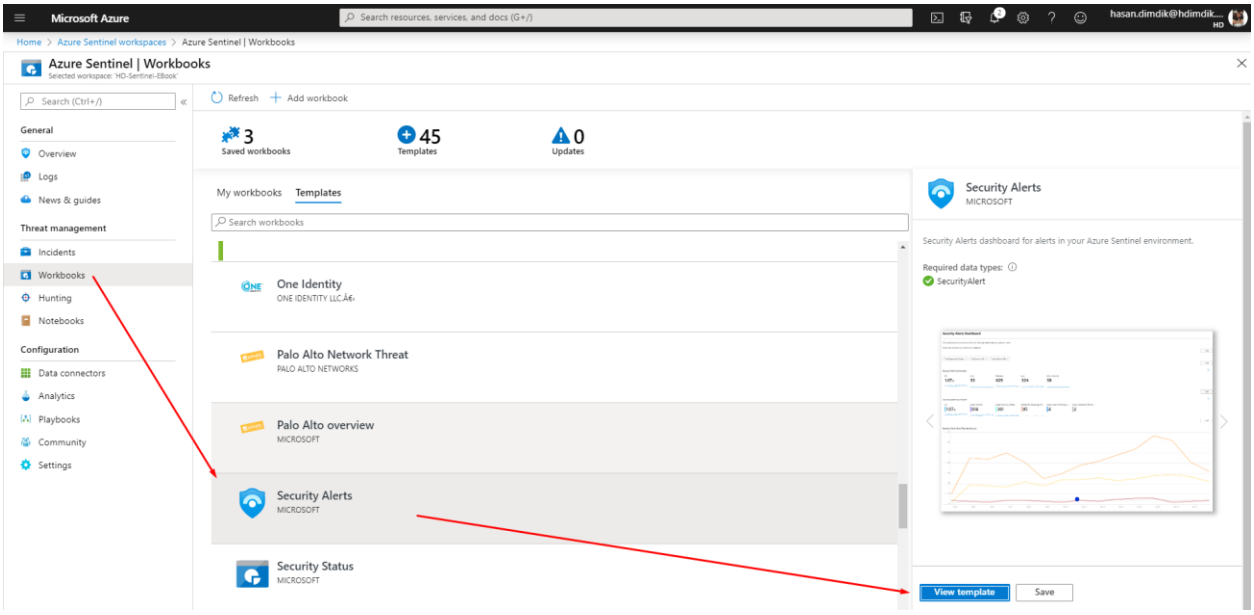
Azure Sentinel portalına eriştikten sonra **Data Connectors** sekmesine geliyorum ve **open connector page** butonunu tıklıyorum.



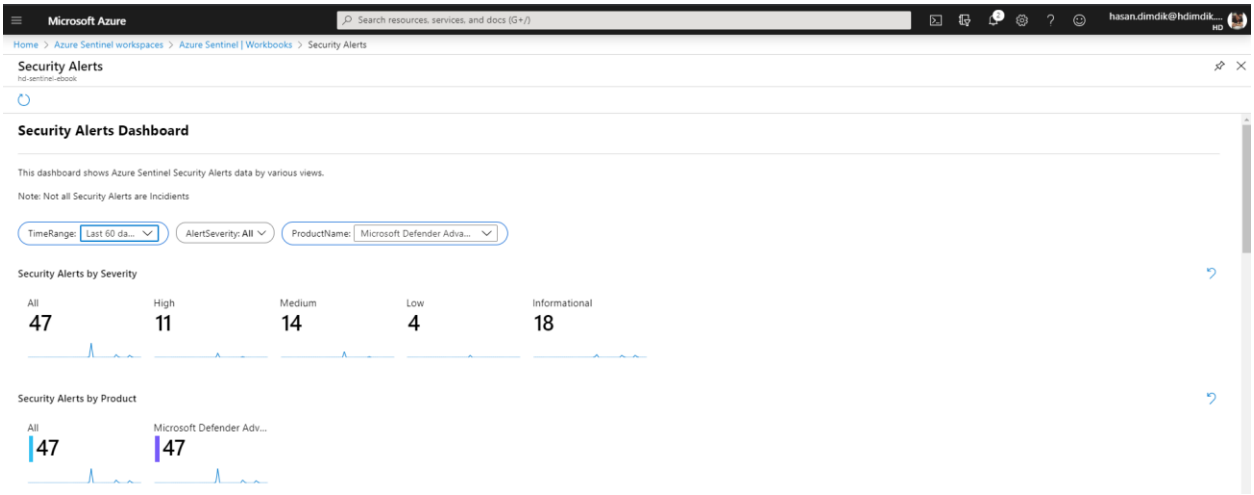
Ön gereksinimleri sağladığımıza emin oluyoruz ve **Connect** butonuna basarak entegrasyonu tamamlıyoruz. (Ben daha önceden aktif ettiğim için Disconnect butonu gözükmektedir)

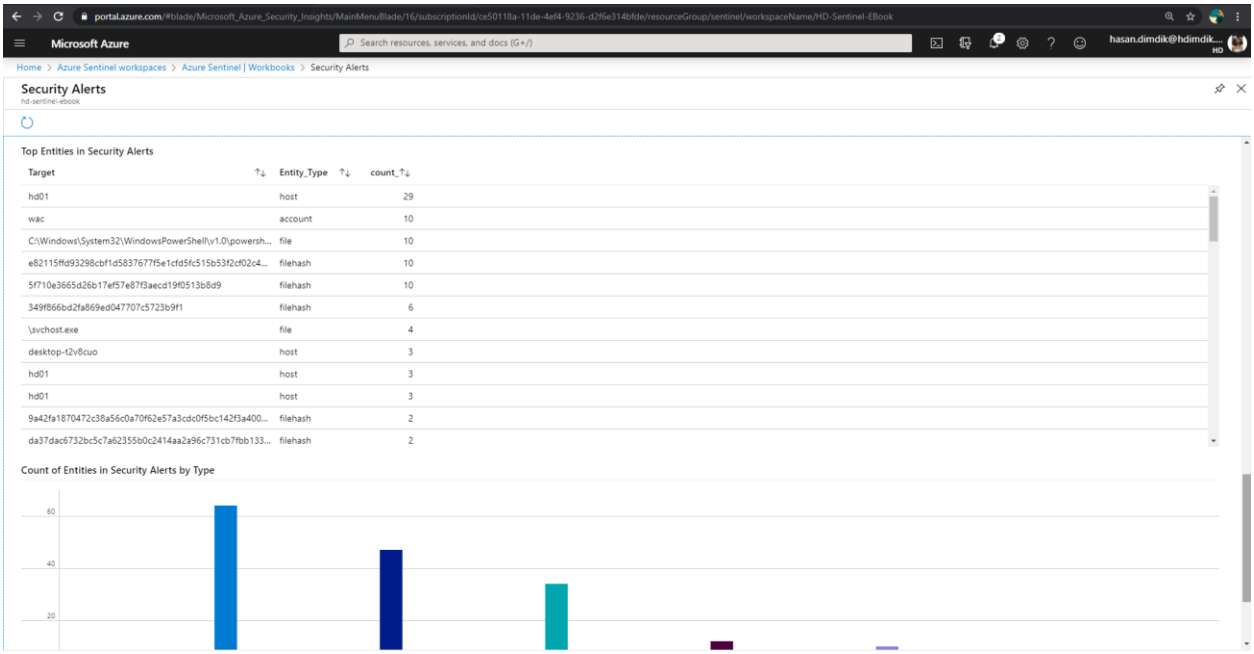


Workbooks lar bizim dashboard larımız, kontrol etmek için **Workbooks** sekmesine geliyorum.



İlgili alarmların artık Azure Sentinele geldiğini gözlemliyorum.

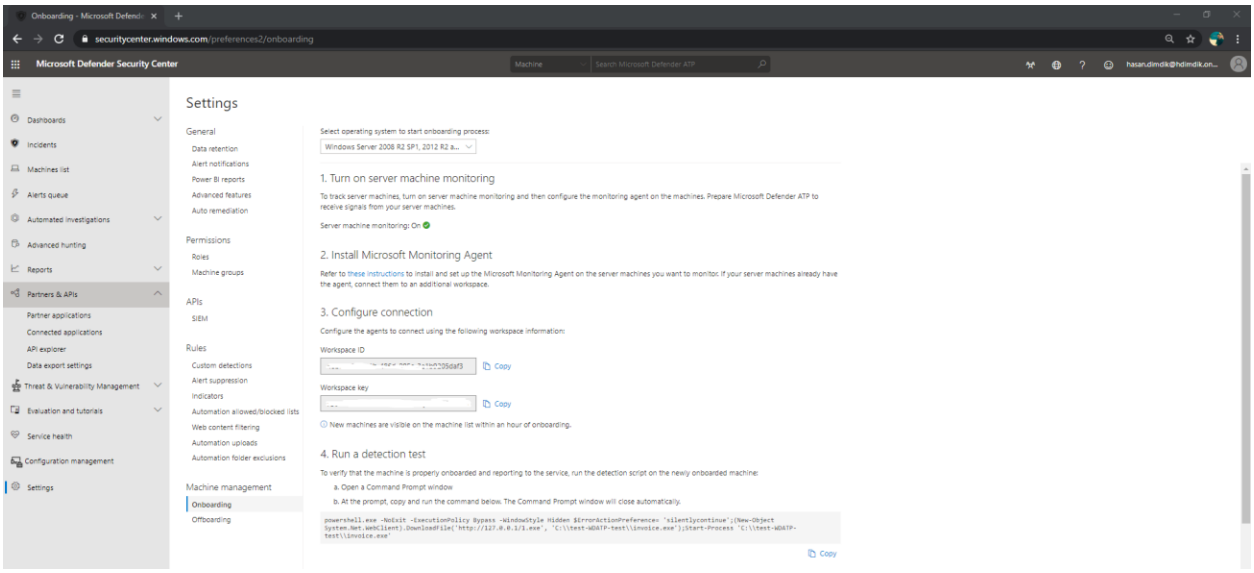




Settings

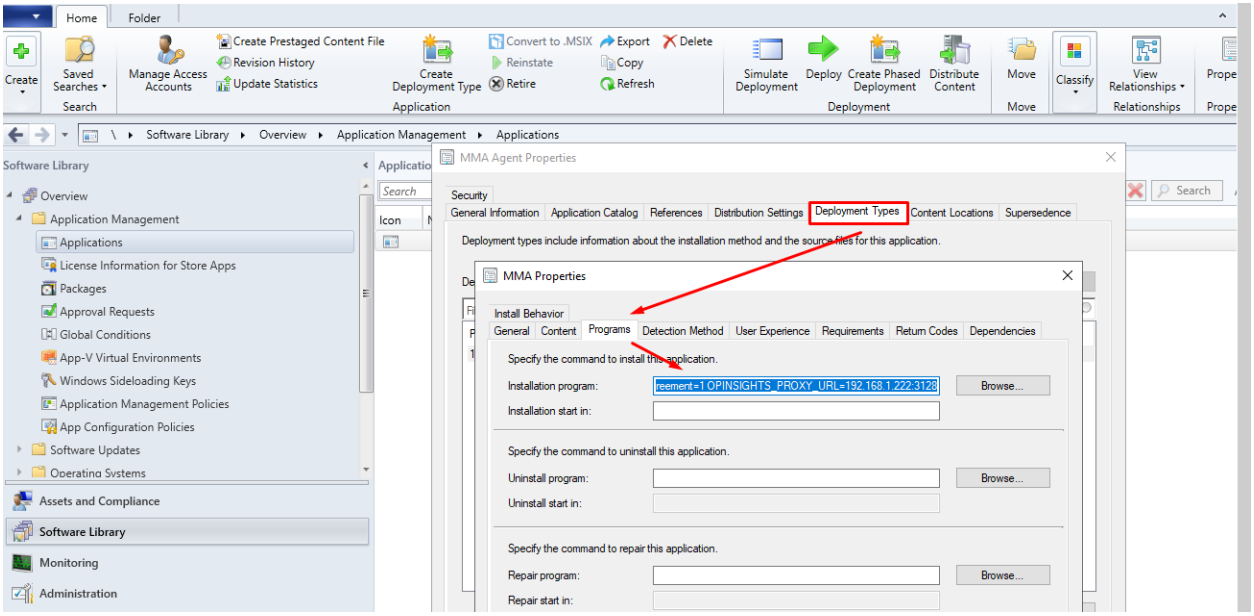
Windows Server 2008 R2 SP1, 2012 R2, 2016 Onboarding

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.



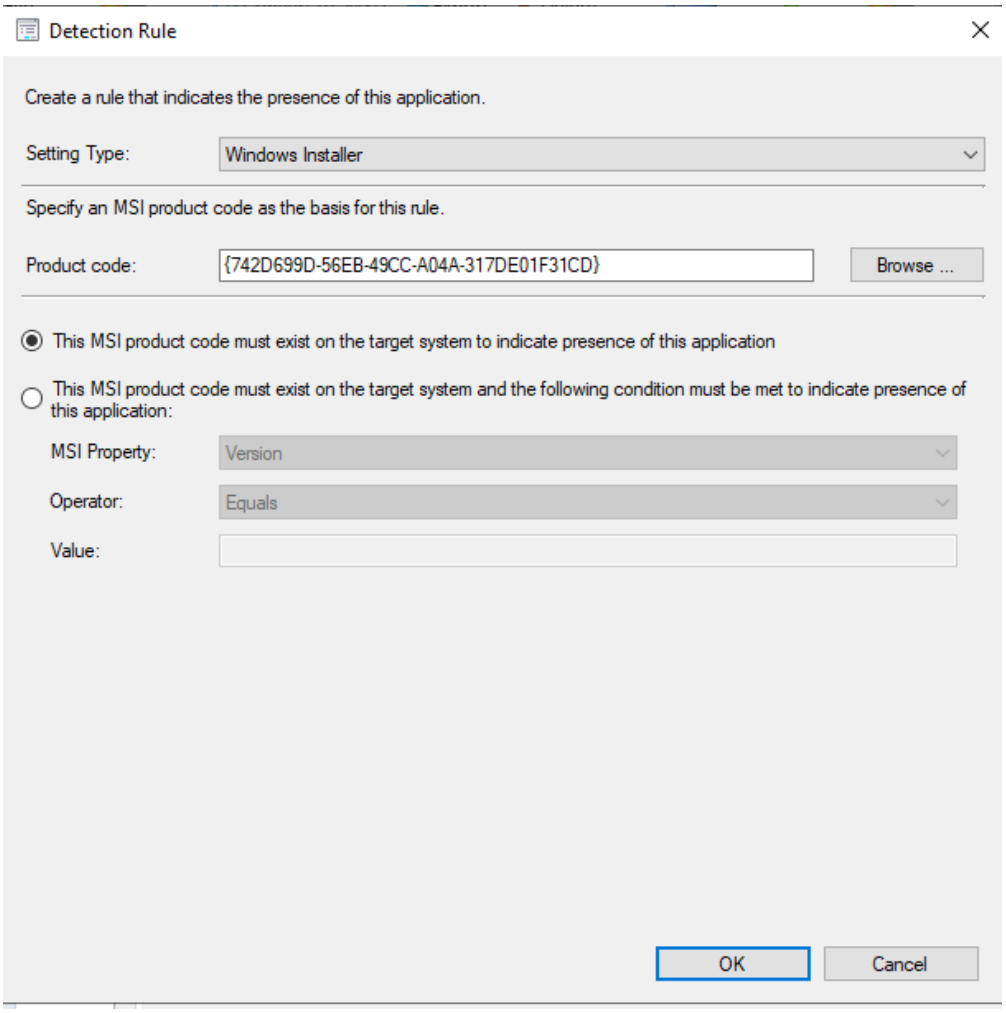
SCCM konsolunu açtıktan sonra applications sekmesine gelerek işlemlere başlıyoruz. **Deployment Types** olarak **Script** seçmiştim. **Programs** sekmesine geliyoruz **Installation progress** kısmına aşağıdaki komutu yapıştırıyoruz. Kırmızı alanları editlemeyi unutmayınız. Demo ortamımda internete proxy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

msiexec /i MMASetup-AMD64.exe /qn NOAPM=1 ADD_OPINSIGHTS_WORKSPACE_AZURE_CLOUD_TYPE=0 OPINSIGHTS_WORKSPACE_ID=xxxxxxxx OPINSIGHTS_WORKSPACE_KEY=xxxxxxxxxxxx AcceptEndUserLicenseAgreement=1 OPINSIGHTS_PROXY_URL=192.168.1.222:3128

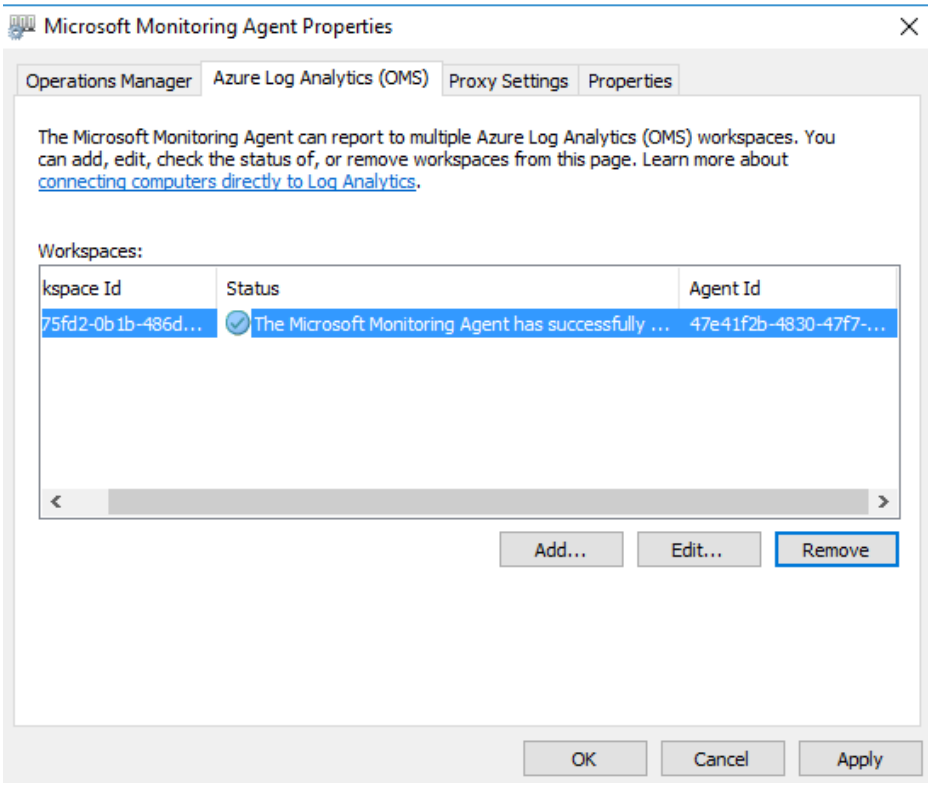


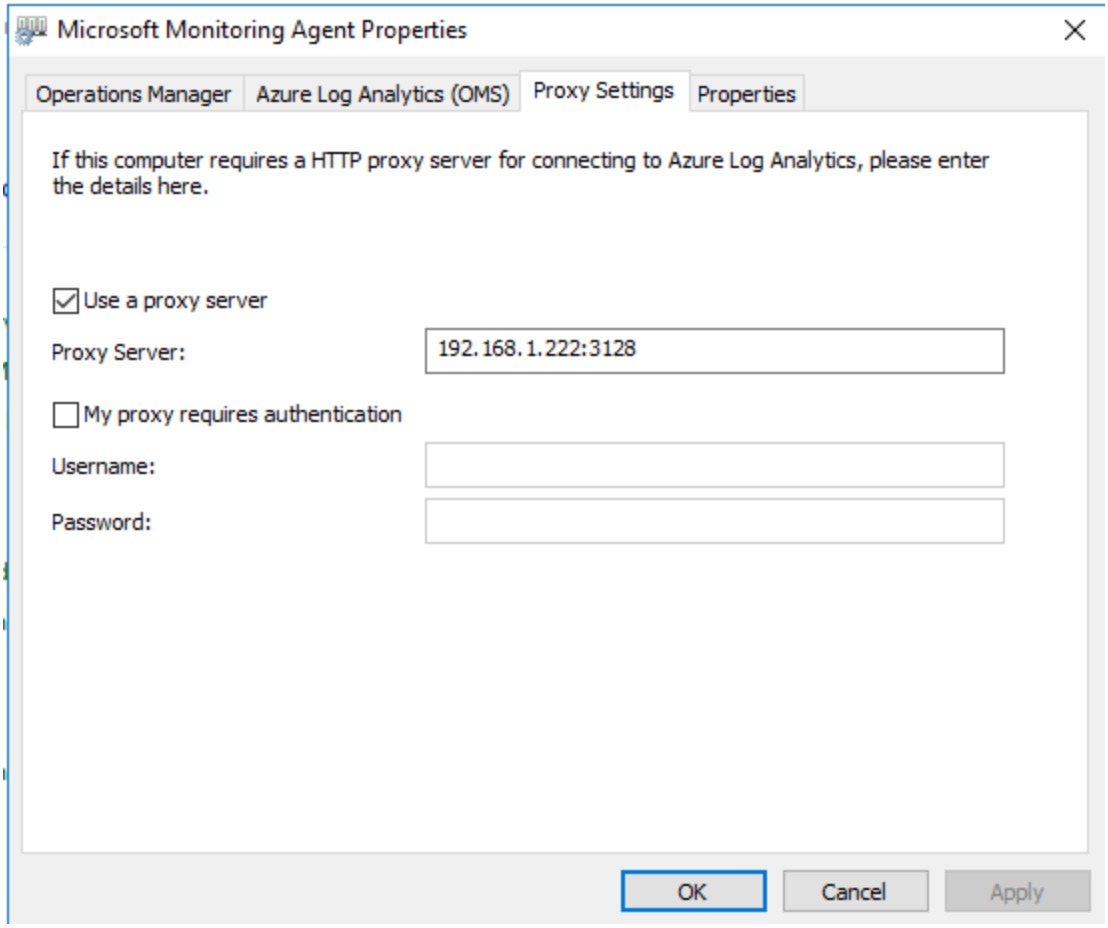
Detection Rule olarak **Windows Installer** seçip ilgili parametreyi ekliyorum ve geriye kalan işin makyaj kısımlarını tamamlıyoruz 😊

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



Son olarak ilgili collection lara mma agent ımı dağıtıyorum.


Microsoft Monitoring Agent Properties
Operations Manager
Azure Log Analytics (OMS)
Proxy Settings
Properties
The Microsoft Monitoring Agent can report to multiple Azure Log Analytics (OMS) workspaces. You can add, edit, check the status of, or remove workspaces from this page. Learn more about connecting computers directly to Log Analytics.
Workspaces:
kspace Id
Status
Agent Id
75fd2-0b1b-486d...
The Microsoft Monitoring Agent has successfully ...
47e41f2b-4830-47f7-...
Add...
Edit...
Remove
OK
Cancel
Apply



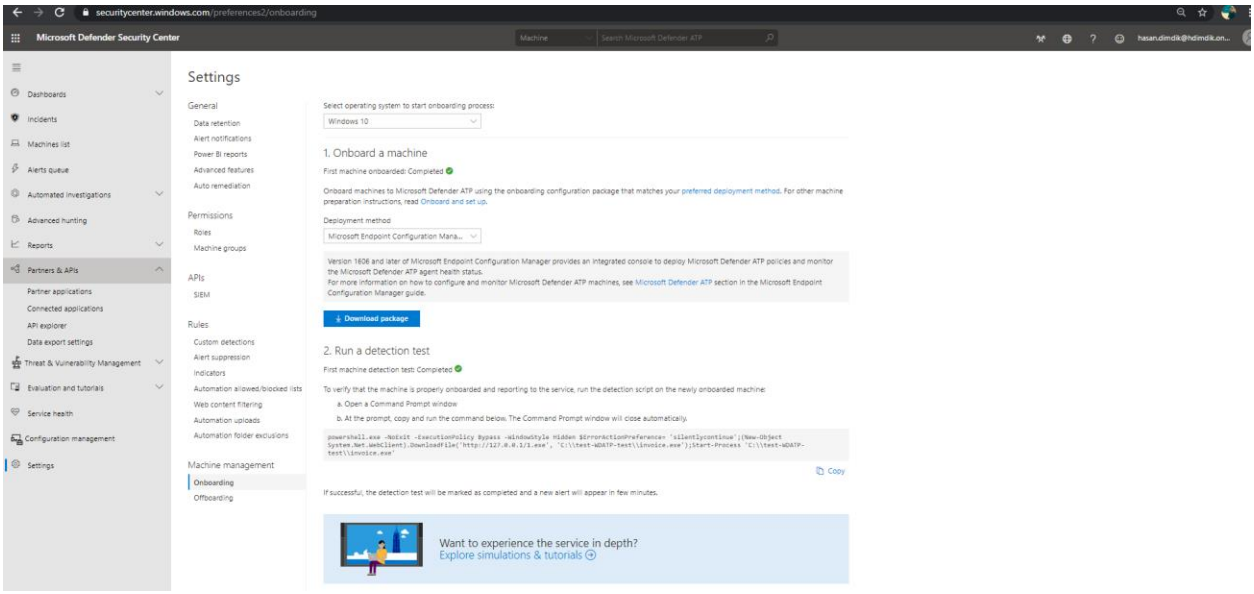
Eğer yapınızda sunucularınız internete direk olarak çıkmıyorsa OMS Gateway yapılandırmamız gerekmektedir. Gerekli port ve URL leri aşağıdaki dökümandan okuyabilirsiniz.

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

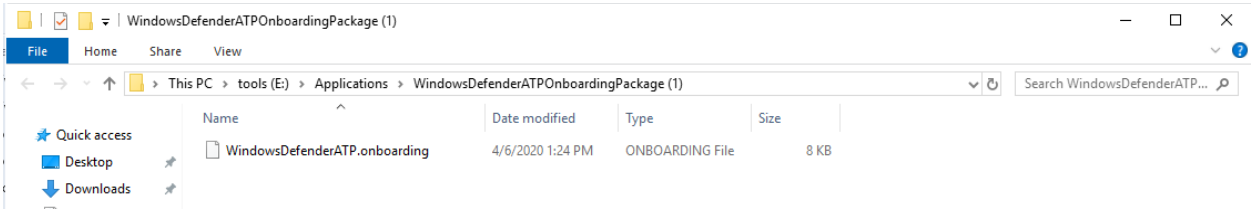
Aynı adımlar Windows 7 SP1 ve Windows 8.1 içinde geçerli. Yazının ilerleyen bölümlerinde Windows Server 2008 R2 SP1, 2012 R2 için SCEP yapılandırmasını göreceğiz. Şimdilik burada bırakıyorum.

Windows 10 Onboarding

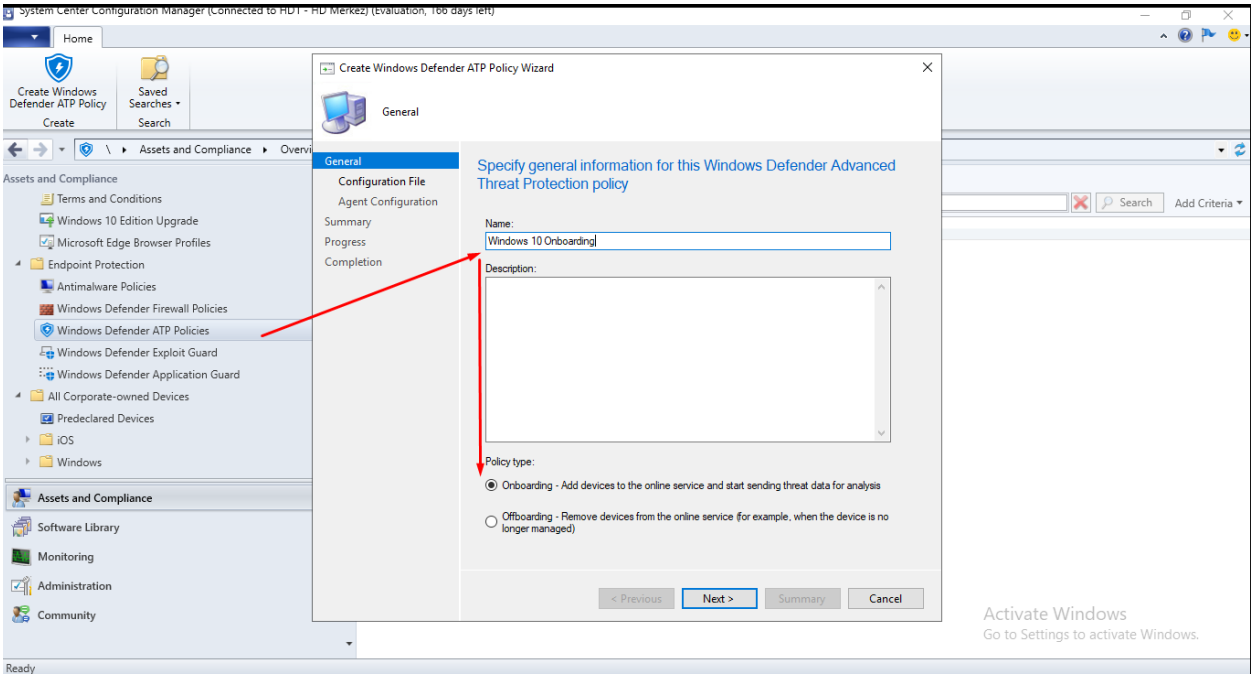
Bu adımda işlemler biraz daha basitleşiyor. İlgili ajanları group policy veya SCCM ile dağıtabiliyoruz. Örneğimde SCCM ile nasıl onboarding işlemini tamamlayabileceğimizi göstereceğim. Panelimde Onboarding sekmesini açıyorum ve işletim sistemi olarak **Windows 10** u seçip **Download package** ile gerekli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



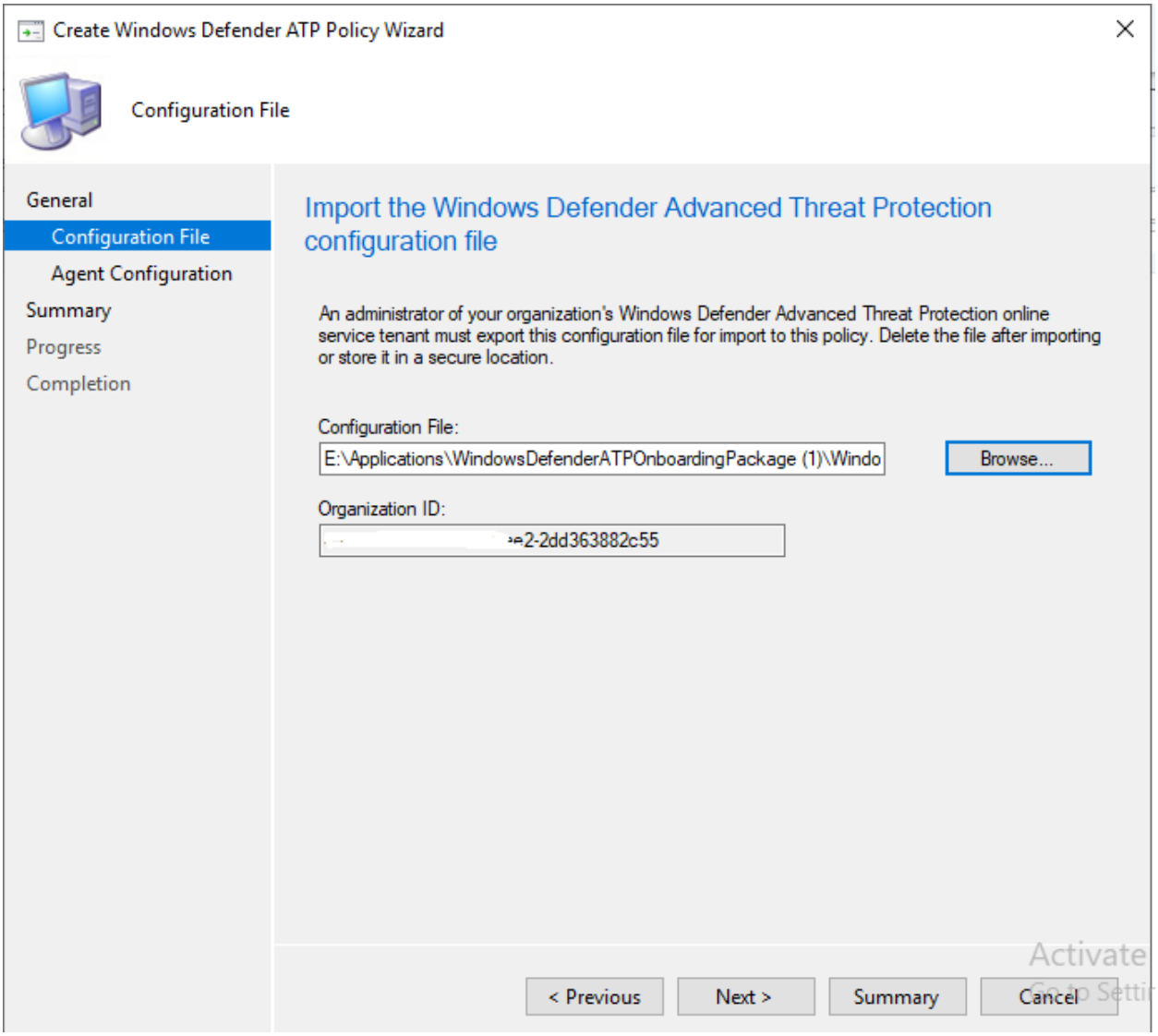
Dosyanın uzantısının .onboarding olduğunu kontrol ediniz.



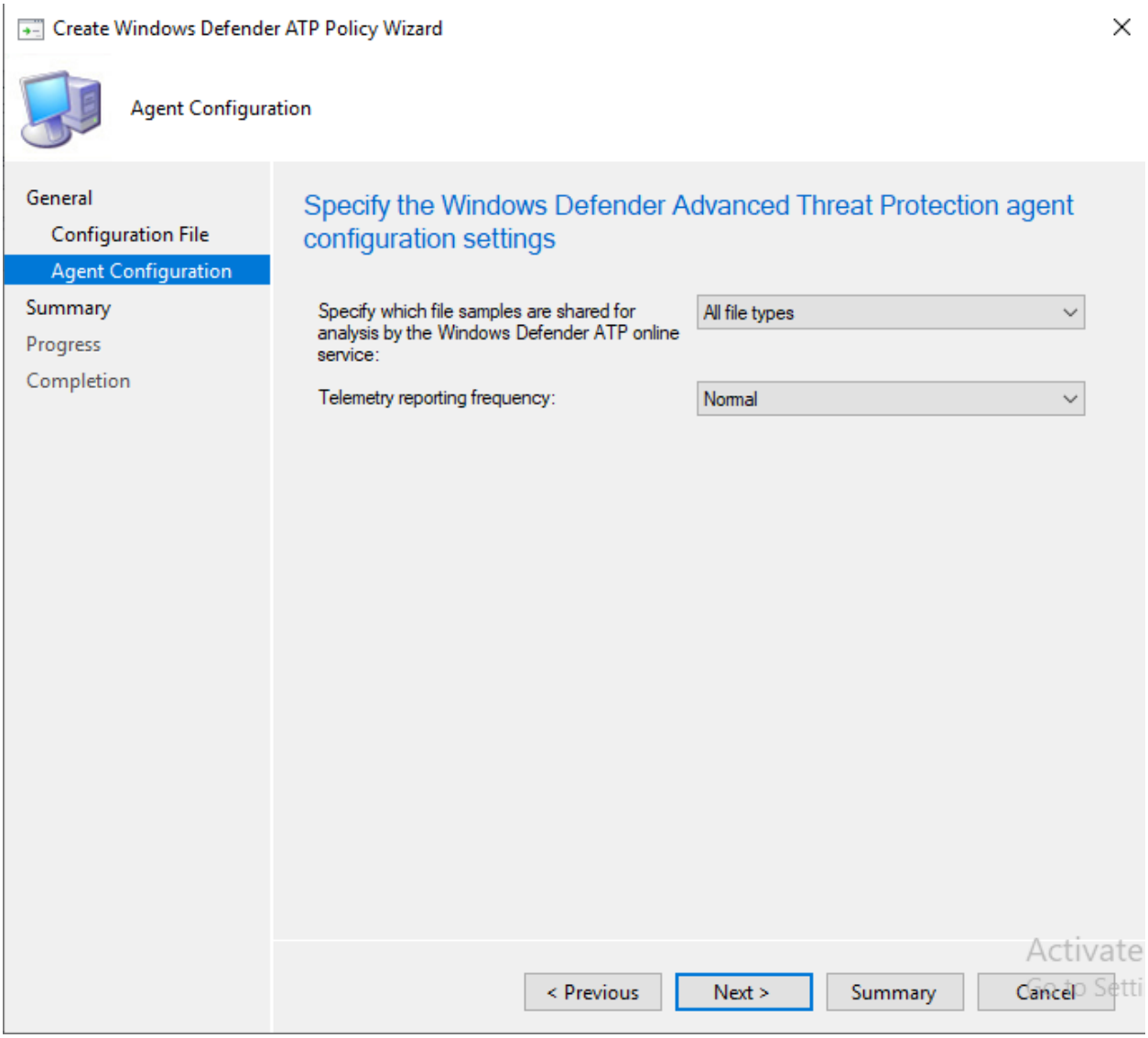
SCCM konsolumuzu açtıktan sonra asset and Compliance sekmesi içerisinde yer alan Windows Defender ATP Policies sekmesini sağ tıklayıp **Create Windows Defender ATP Policy** diyerek işlemimize başlıyoruz. Onboarding yapacağımız için onboarding seçeneğini seçip devam ediyorum.



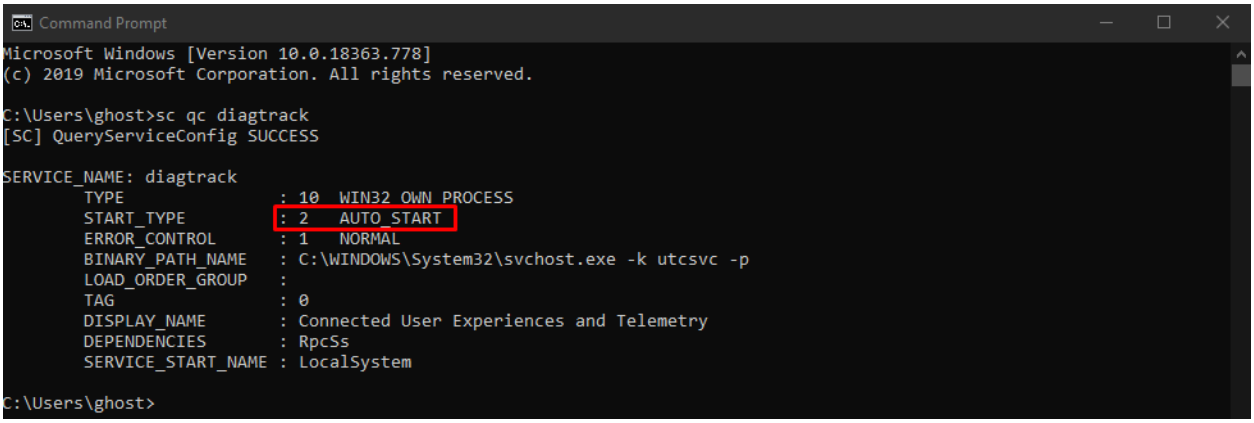
Portaldan indirmiş olduğum onboarding dosyasını gösteriyorum ve devam ediyorum.



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.



Onboarding işleminin başarılı olması için diagtrack servisinin AUTO_START olması gerekmektdir. Sorun yaşarsanız bu bilgi bir köşede dursun 😉



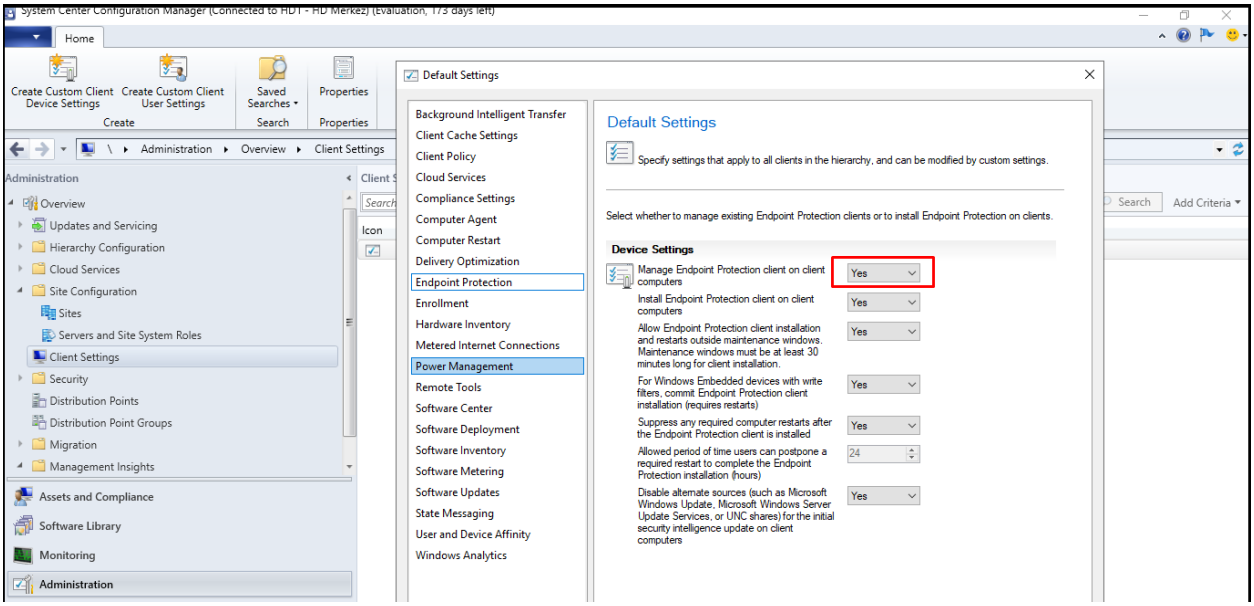
Buraya kadar olan kısımda Onboarding işlemlerini tamamladık. EDR çözümümüz artık çalışır durumda.

System Center Configuration Manager SCEP Yapılandırması

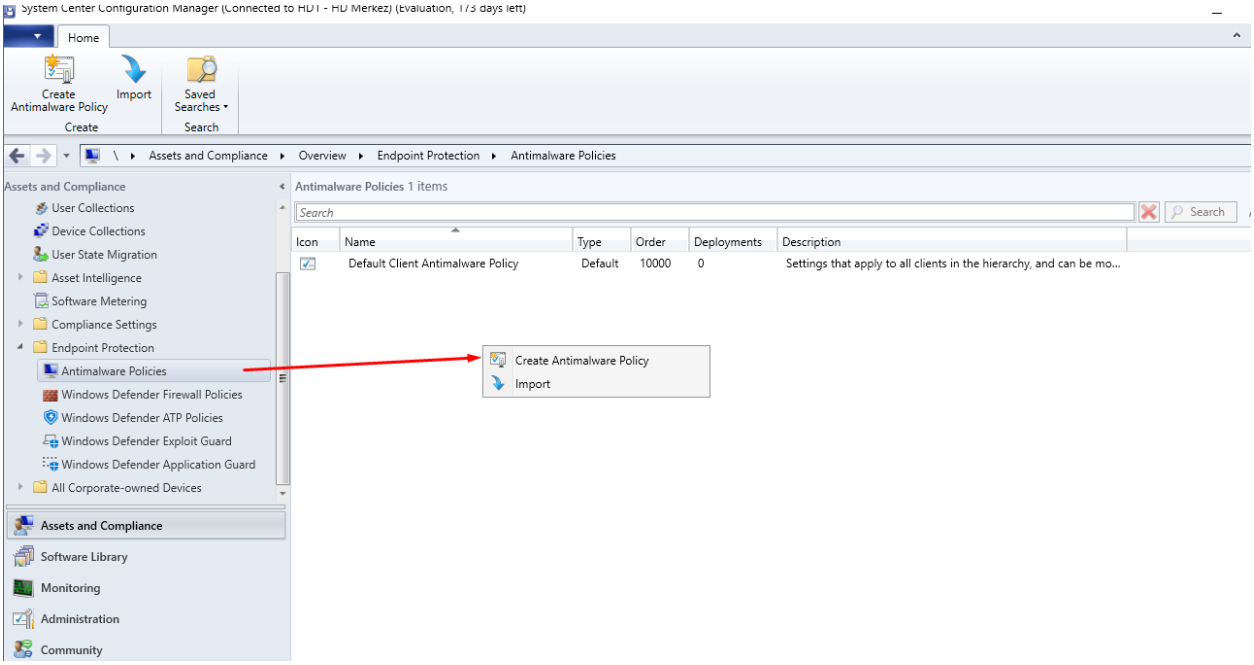
Giriş bölümünde **Attack Surface Reduction** kısmını SCCM ile yapılandıracağımızdan bahsetmiştik. MDATP ve SCEP konularına hakim değilseniz neden buna ihtiyaç var sorusu akıllara gelecektir. Hemen bu soruyu cevaplayalım. Yapıyı incelediğimiz zaman EDR teknolojisinden faydalanmak için MMA ajanlarını sunucularımıza 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)

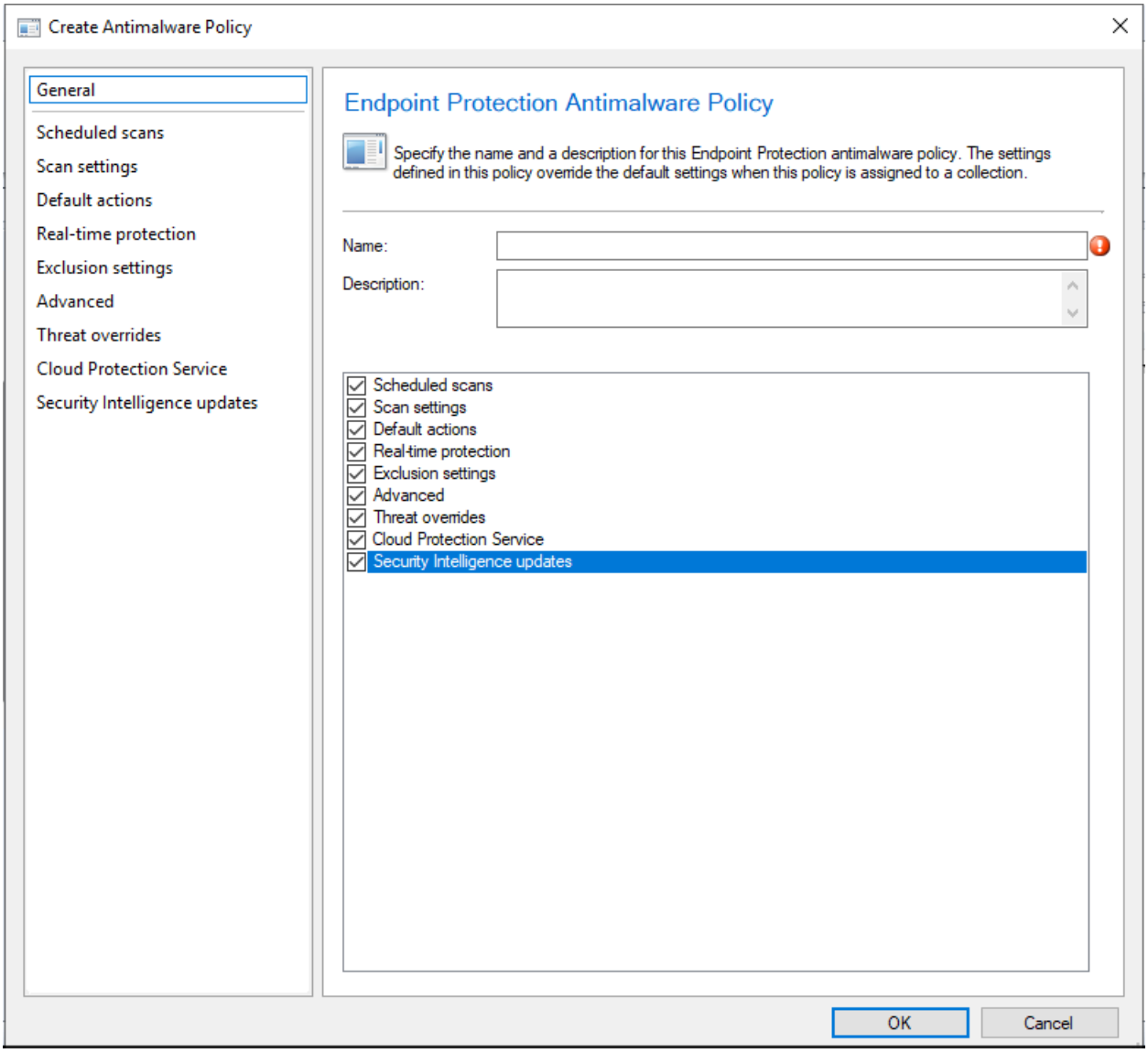
SCCM Portalımıza eriştikten sonra yapılandırmamıza **Client Settings'** den başlıyoruz. **Endpoint Protection** sekmesine geliyoruz. **Manage Endpoint Protection client on client computers** ayarını **yes** olarak değiştiriyoruz.



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

AntiMalware Policy

Desteklenen sürümler (Server,Client)

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

Microsoft Defender Antivirus

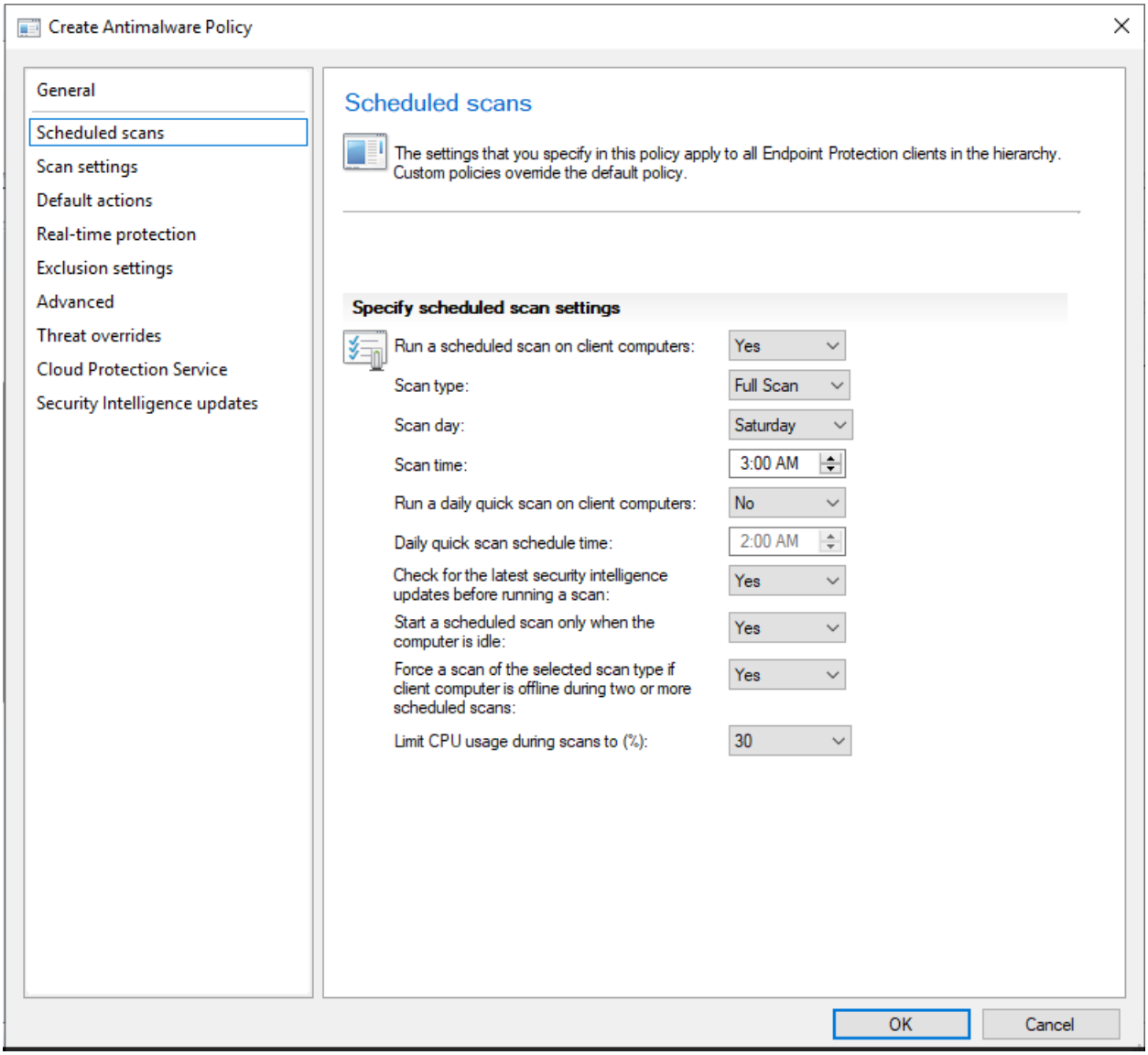
- Windows Server 2019
- Windows Server 2016
- Windows 10

System Center Endpoint Protection

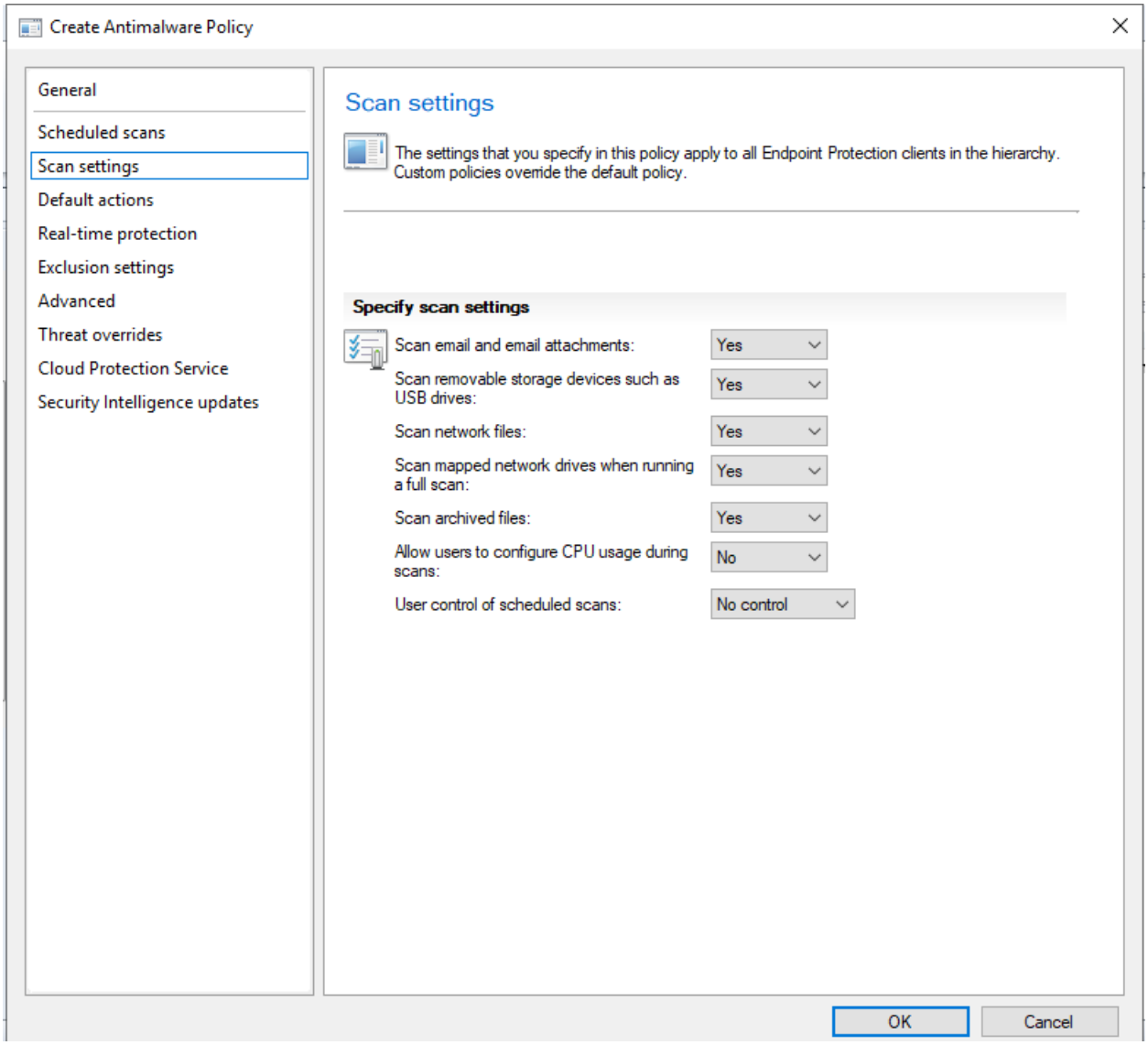
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1
- Windows Server 2008 SP2

- Windows 8.1
- Windows 8
- Windows 7 SP1
- Windows Vista

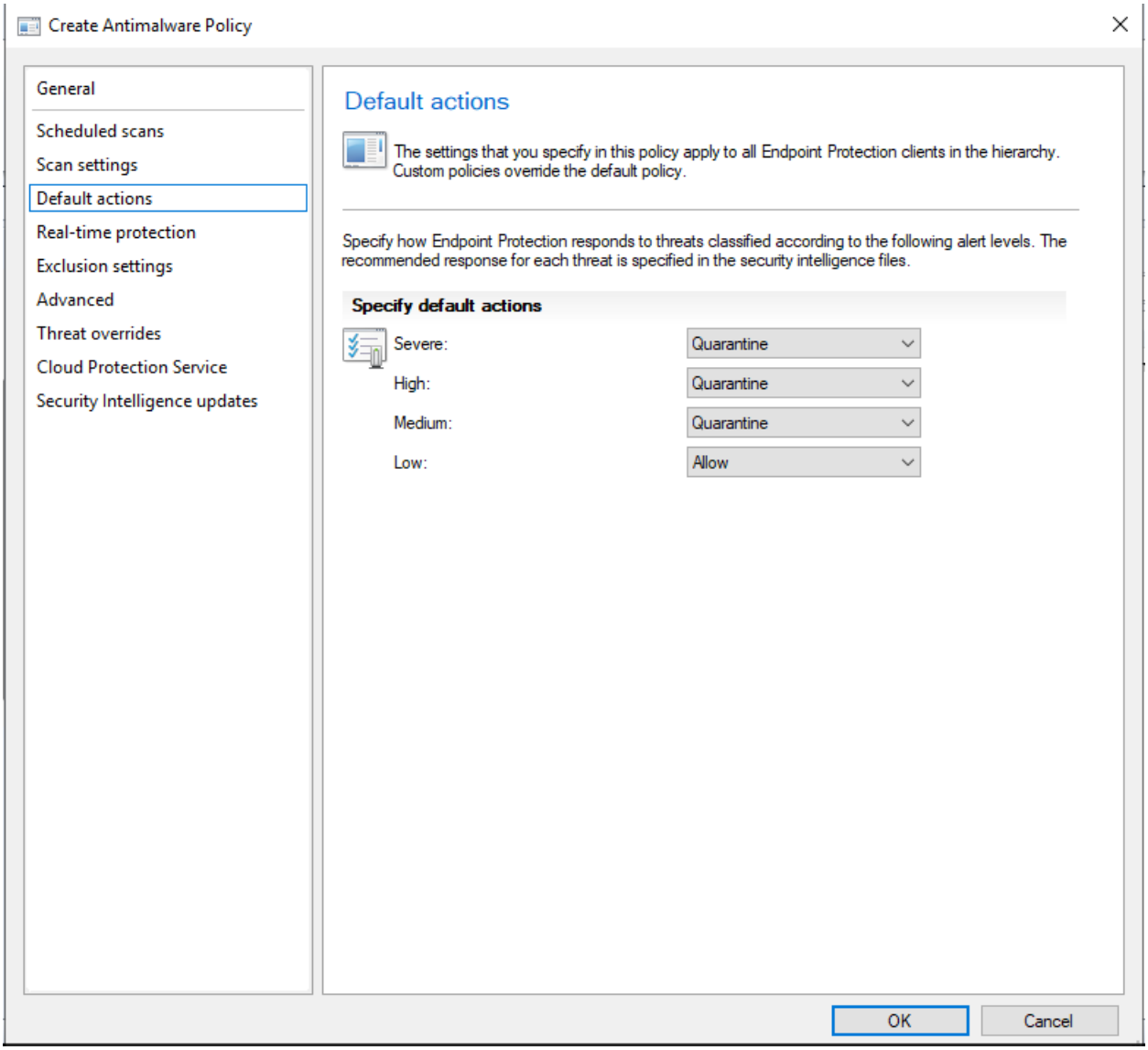
Scheduled Scan sekmesinde tarama tipini, gününü , saatini CPU kullanımını kısıtlama gibi ayarları yapabiliyoruz.



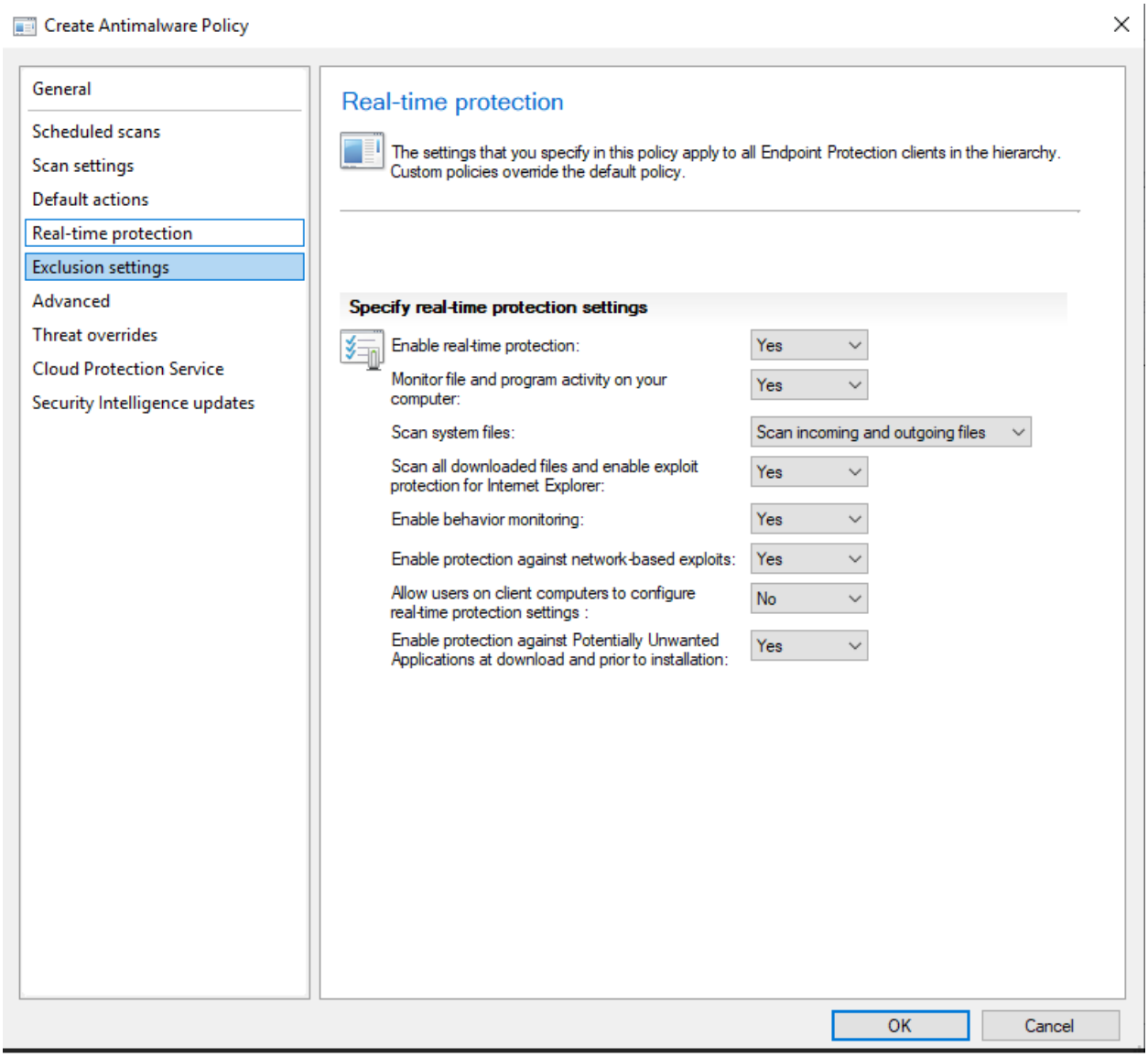
Scan Settings sekmesinde nelerin taranacağı(harici cihazlar, arşiv alanları, e mail içerisindeki ekler, network dosyaları vb..) kullanıcılara kontrol verip vermeyeceğimizi belirleyebiliyoruz.



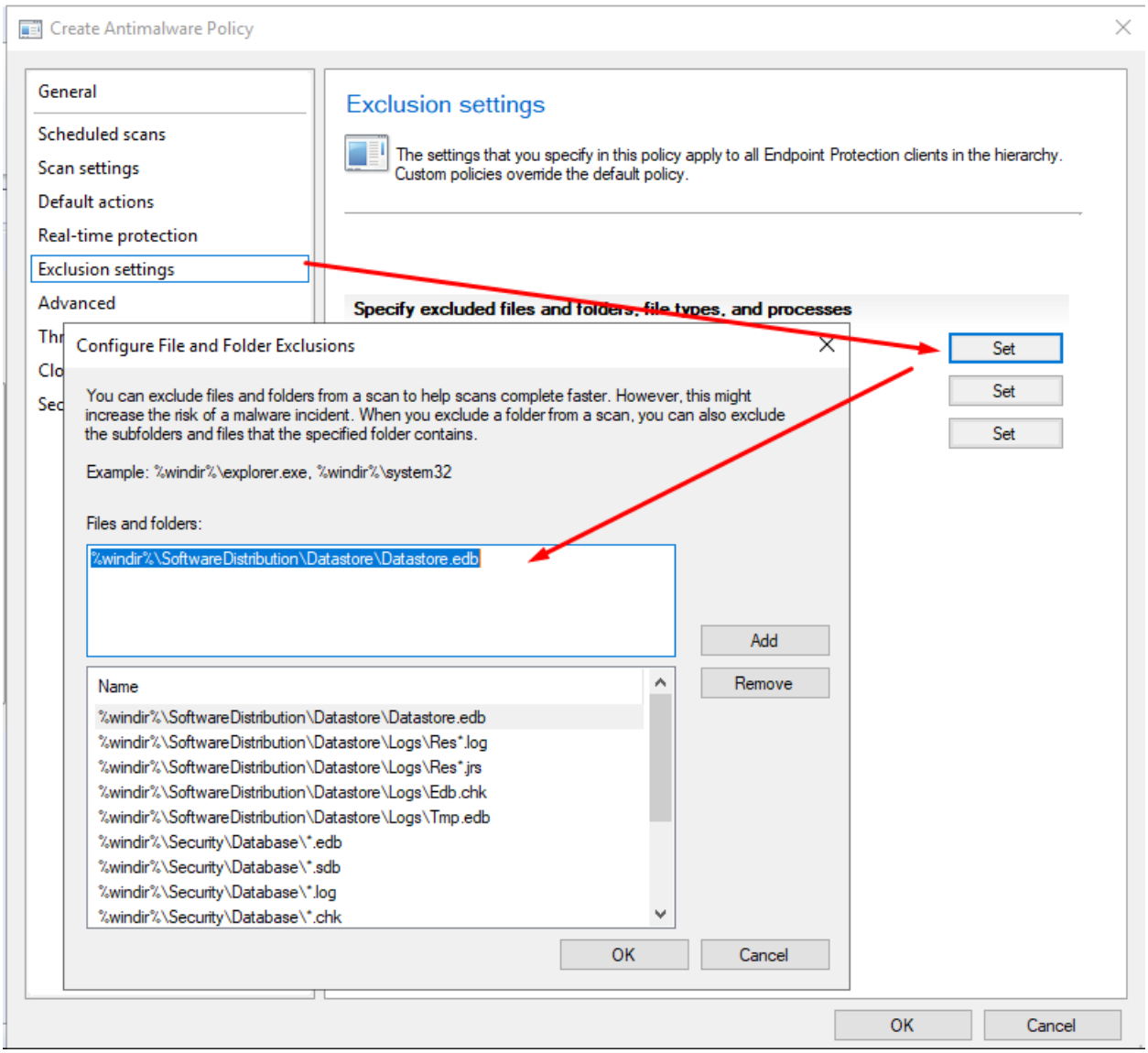
Default Action sekmesinde zararlı yakalandığı zaman nasıl aksiyon alınacağını belirliyoruz.



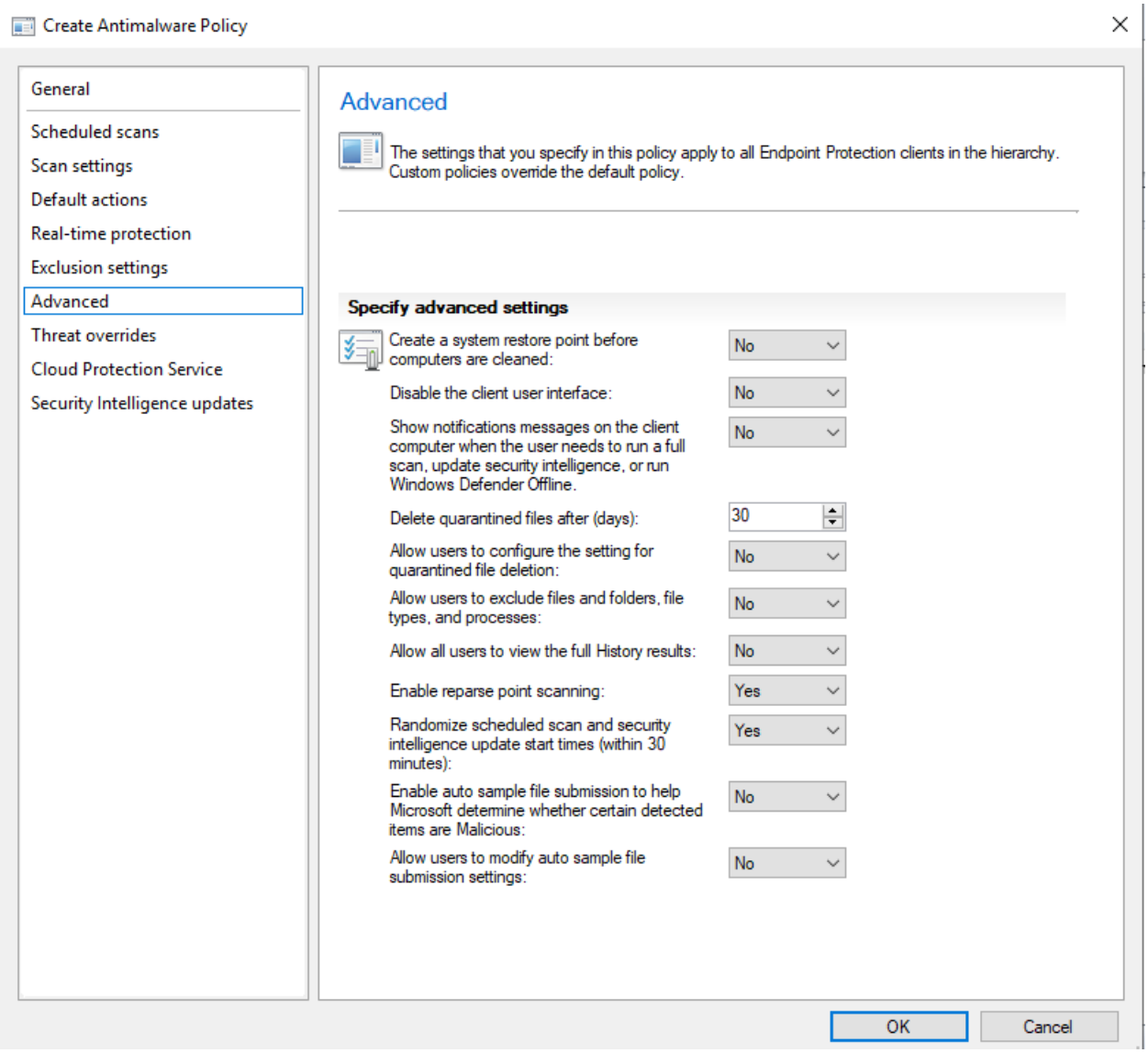
Real-time protection ayarlarımız içerisinde dikkatlice yapılandırmamız gereken sekmelerden en kritik olanı diyebilirim. Endpoint lerimizdeki dosya veya uygulamaların aktivitesini, davranışsal analizi aktif edebileceğimiz , Network tabanlı exploit lere karşı koruma sağladığımız ve gelen/ giden dosyaların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



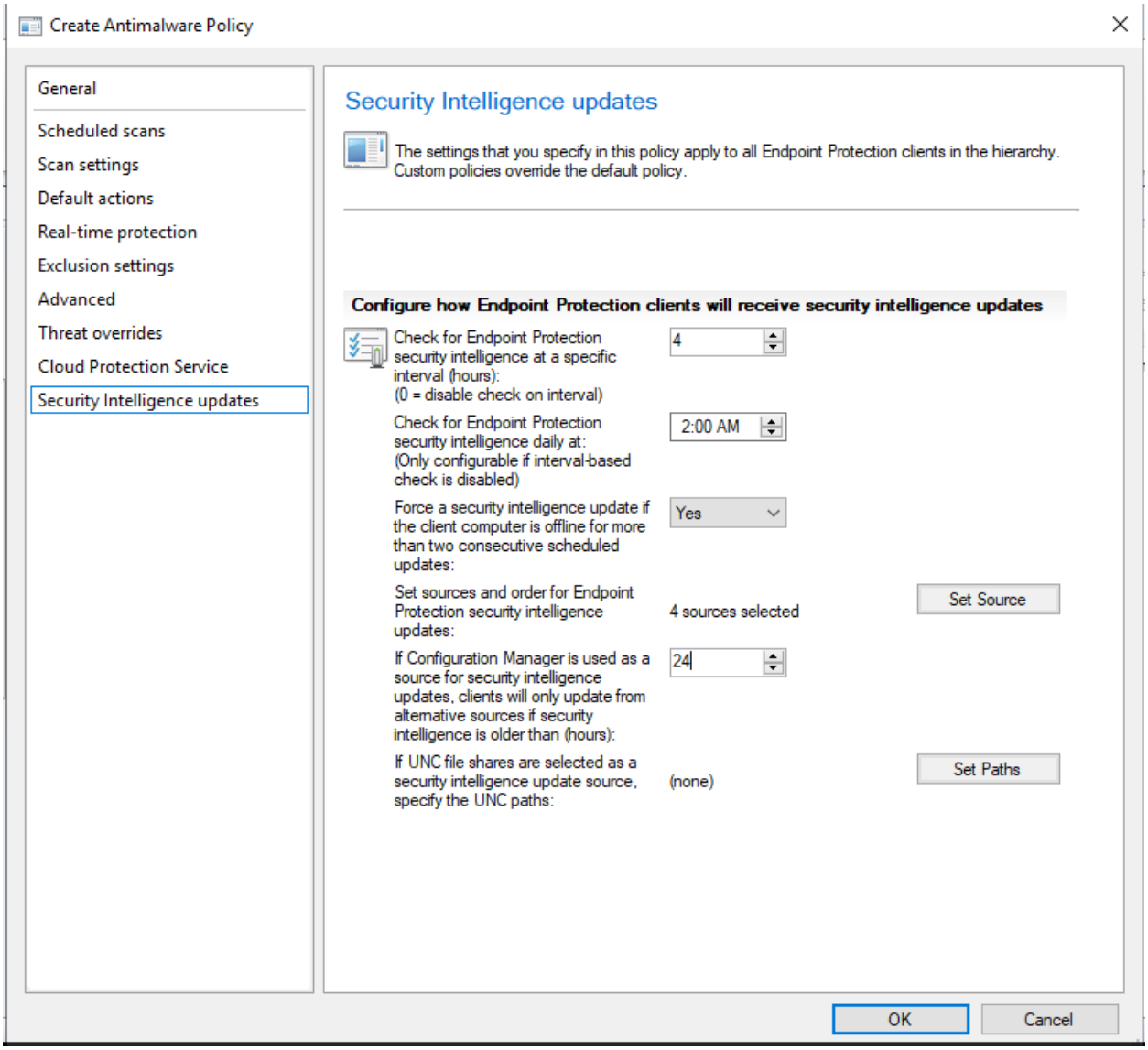
Exclusion Settings sekmesinde ise taranmasını istemediğimiz dosya, dizin vb. var ise tanımlayabiliyoruz.



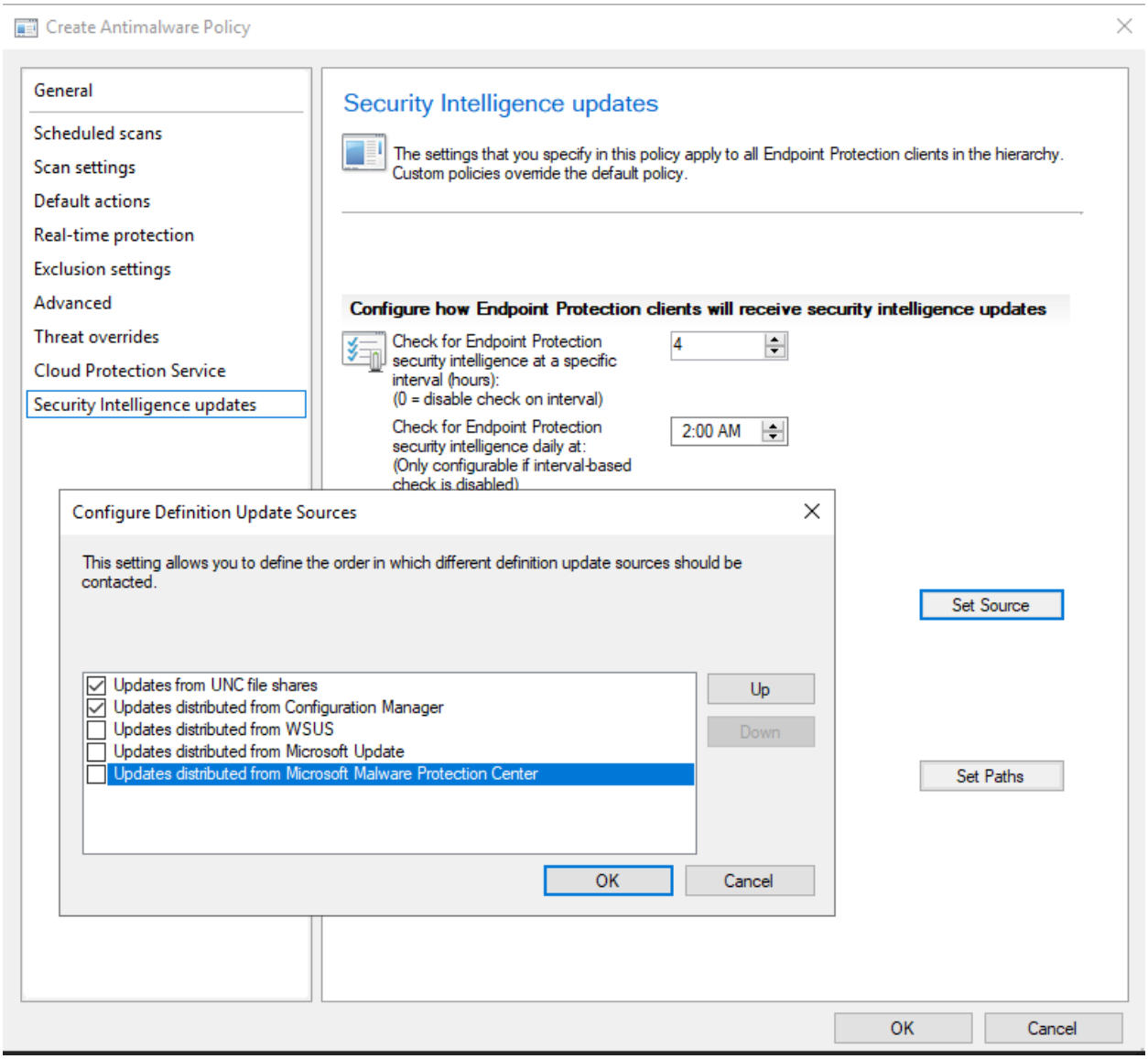
Advanced sekmesinde ise bir tarama başlatıldığında son kullanıcıya bunu pop-up çıkarıp gösterecek miyiz ? Yakalanan bir zararlı temizlenmeden önce restore point oluşturacak mıyız ? Kullanıcıya bu zararlıyı silme için yetki verecekmiyiz? Karantinaya alınan bir zararlıyı ne zaman sileceğiz ? gibi ayarları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



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

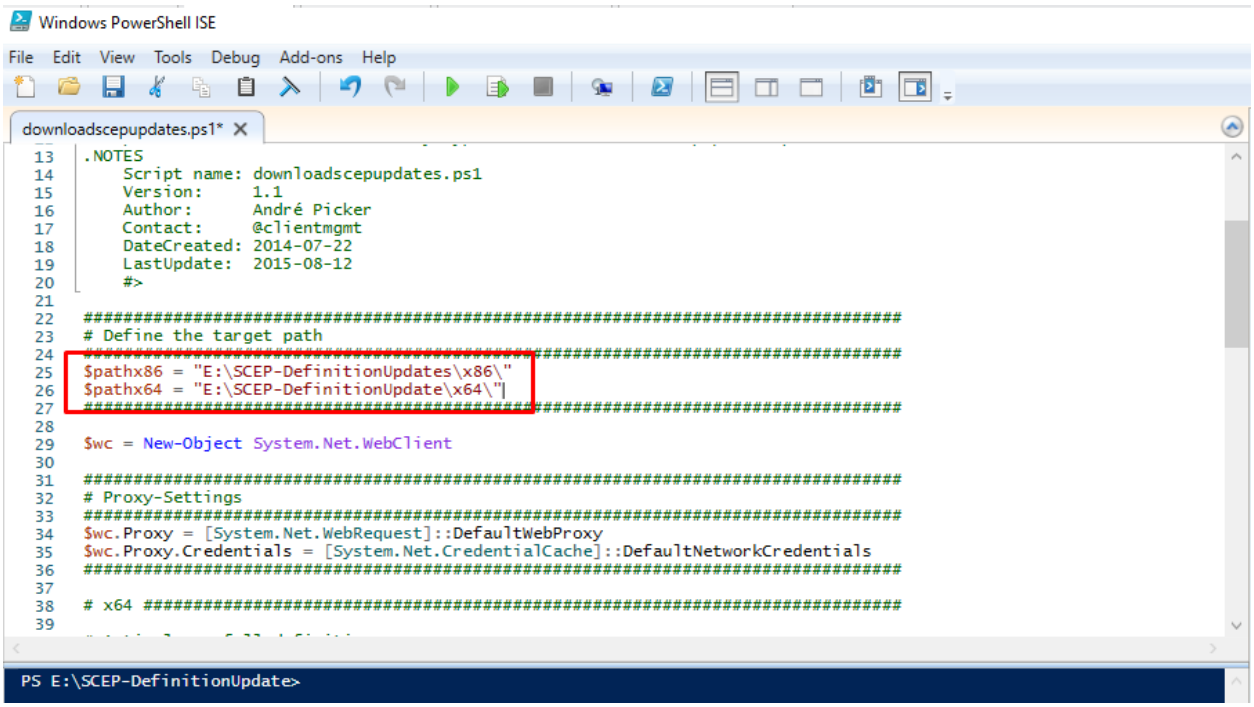


Bu noktada akıllara şu soru gelmektedir. UNC Path belirttik iyi hoş ama nasıl otomatik olarak güncellemeleri indirip sunucu ve istemcilere göndereceğiz ?

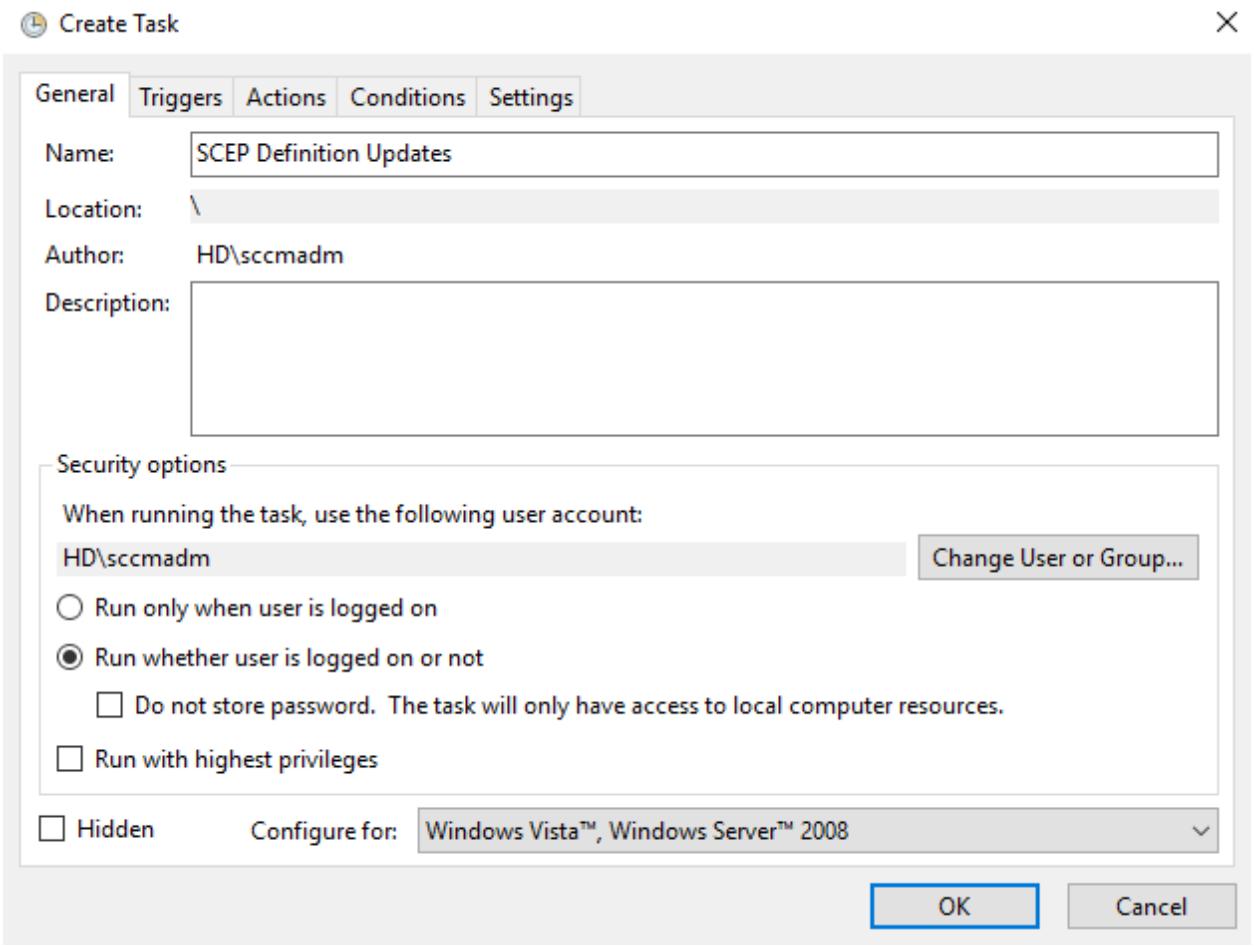
İlk olarak aşağıdaki linkte yer alan Powershell Script' i indiriyoruz ve yazana teşekkür etmeyi unutmuyoruz.

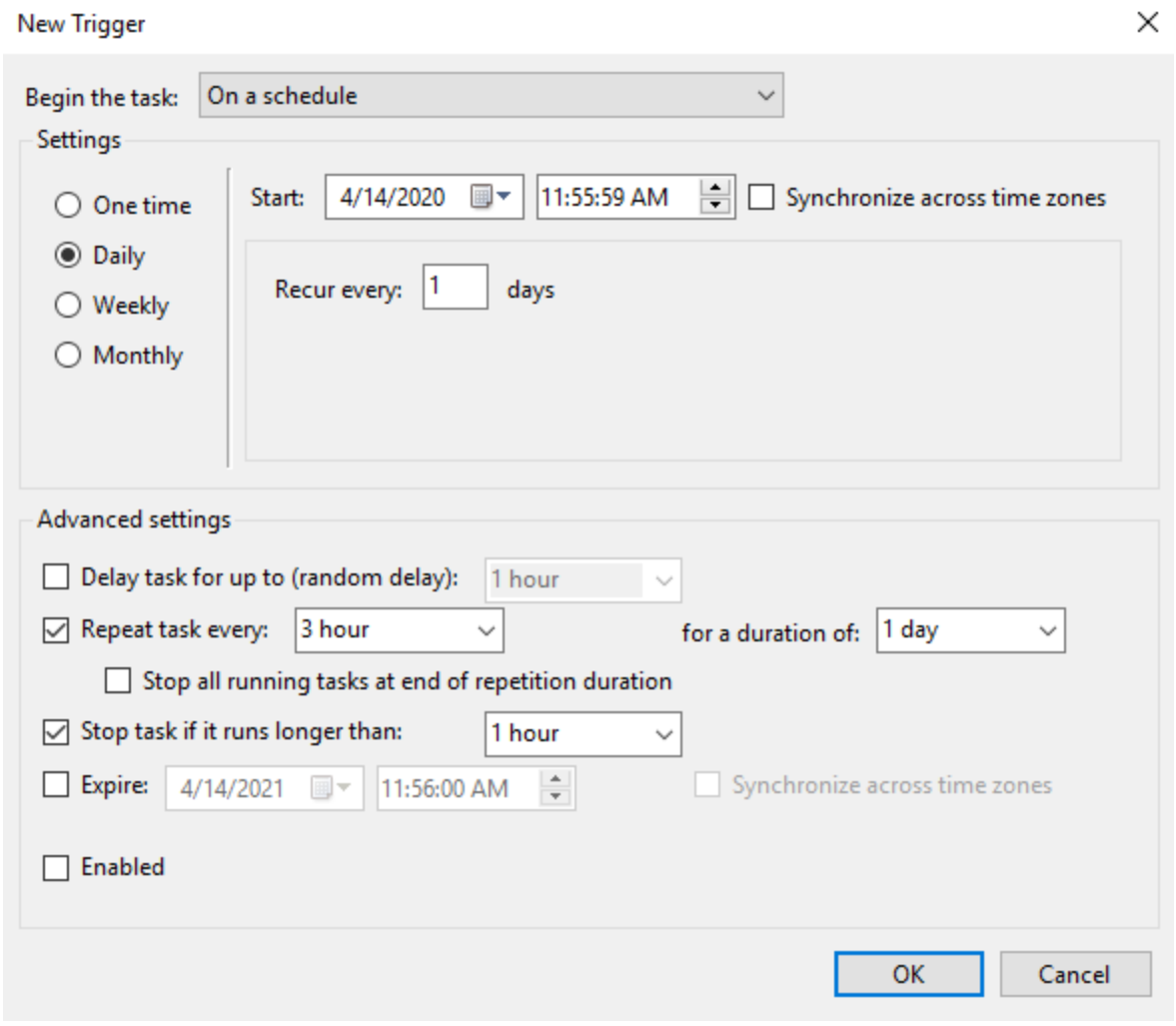
https://gallery.technet.microsoft.com/scriptcenter/SCEP-Definition-Updates-to-fde57ebf

Yapımıza göre ilgili paketlerin indirileceği bölümü değiştiriyoruz.



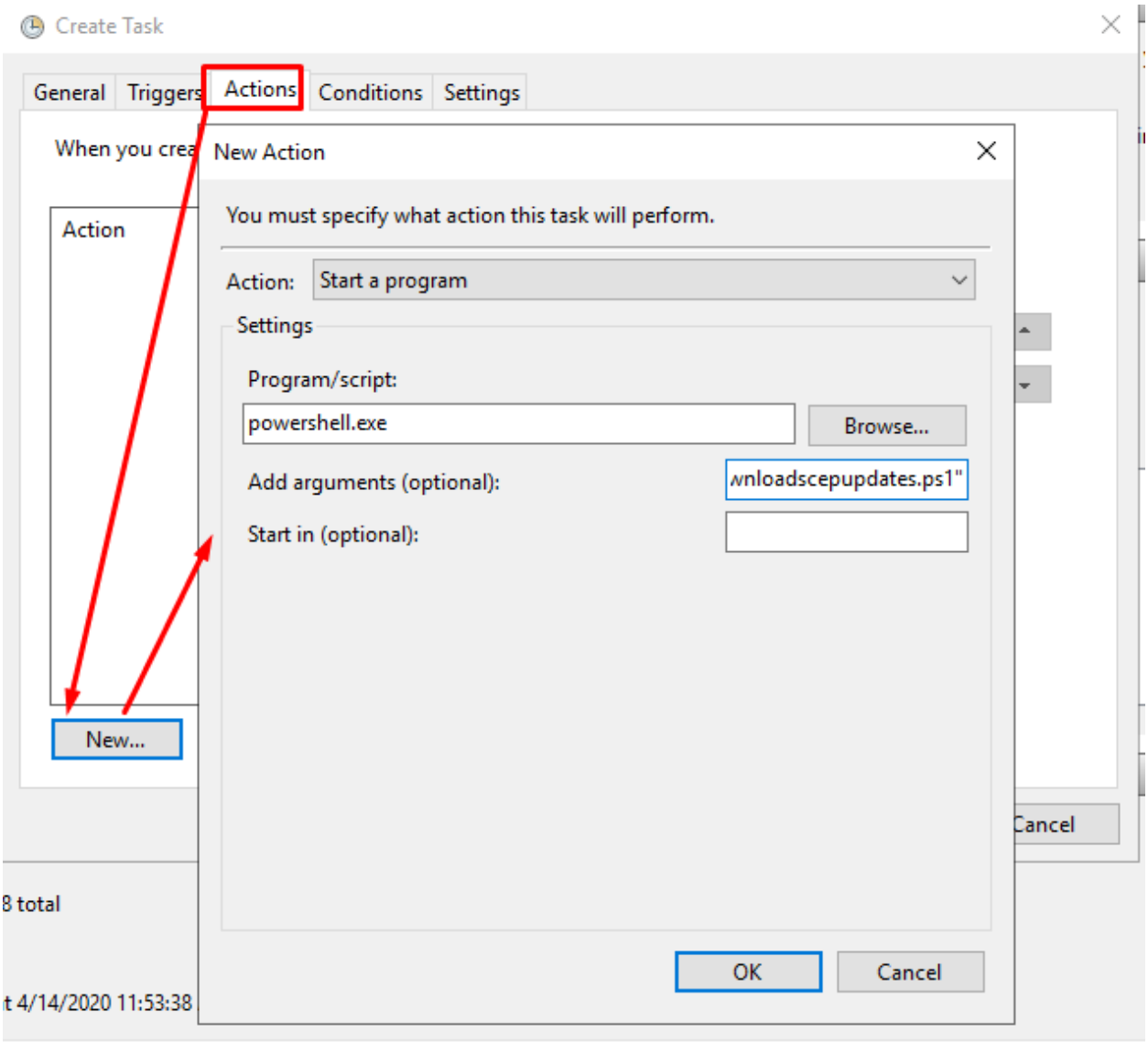
İlgili Powershell Script' i sürekli manuel çalıştıramayacağımıza göre Task Schedular ile bu bölümü otomatize ediyoruz.


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

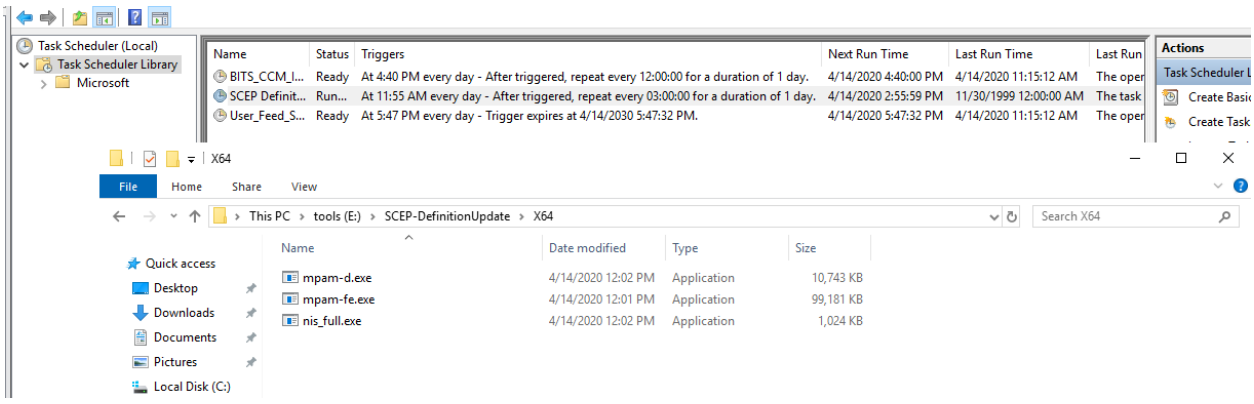


Action kısmında scriptimizi tanımlıyoruz.(Yapınıza göre editlemeyi unutmayınız)

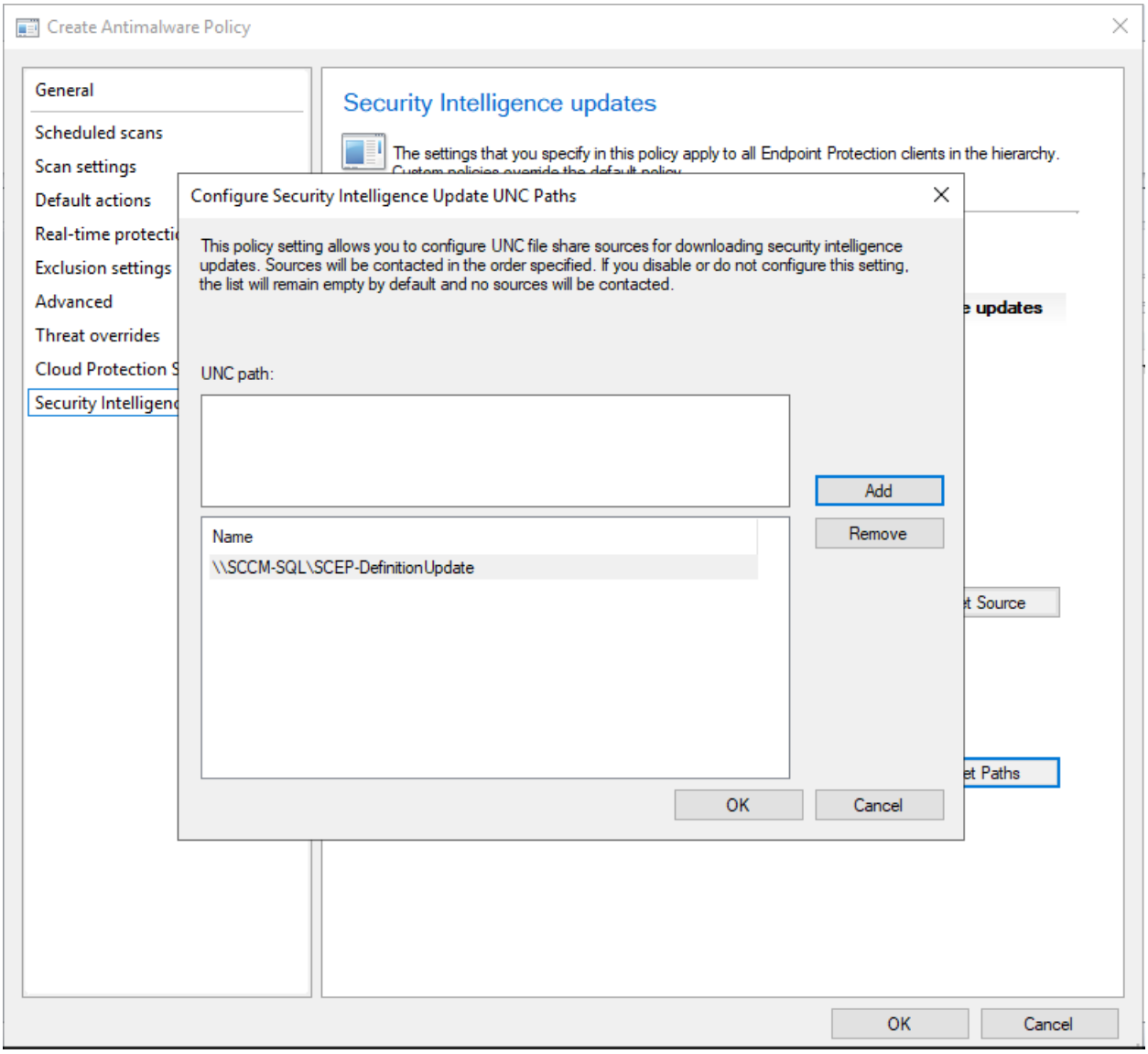
-file "E:\SCEP-DefinitionUpdate\downloadscepupdates.ps1"



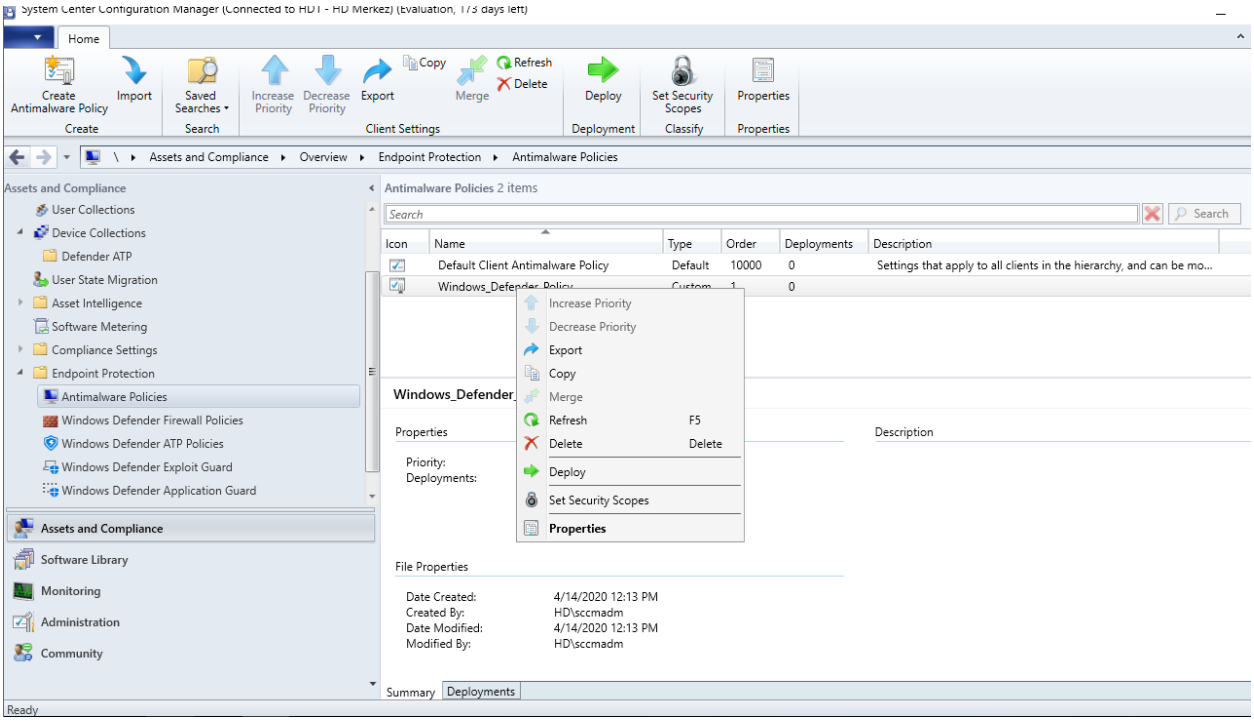
Test için manuel olarak çalıştırıyorum ve başarılı şekilde ilgili dosyalarımın indirildiğini görüyorum.



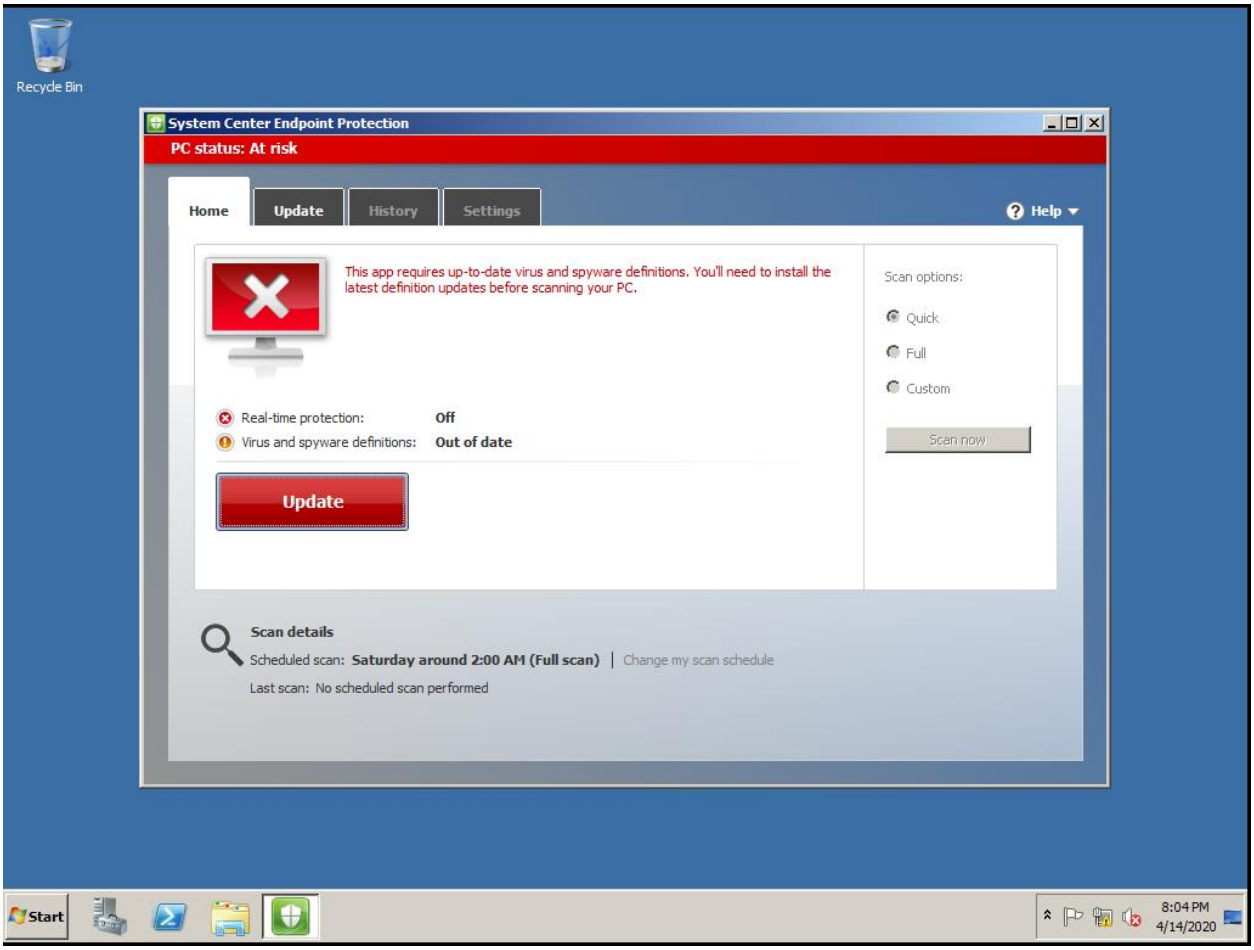
Daha sonra ilgili Path i aşağıdaki UNC Path bölümünde tanımlıyorum.



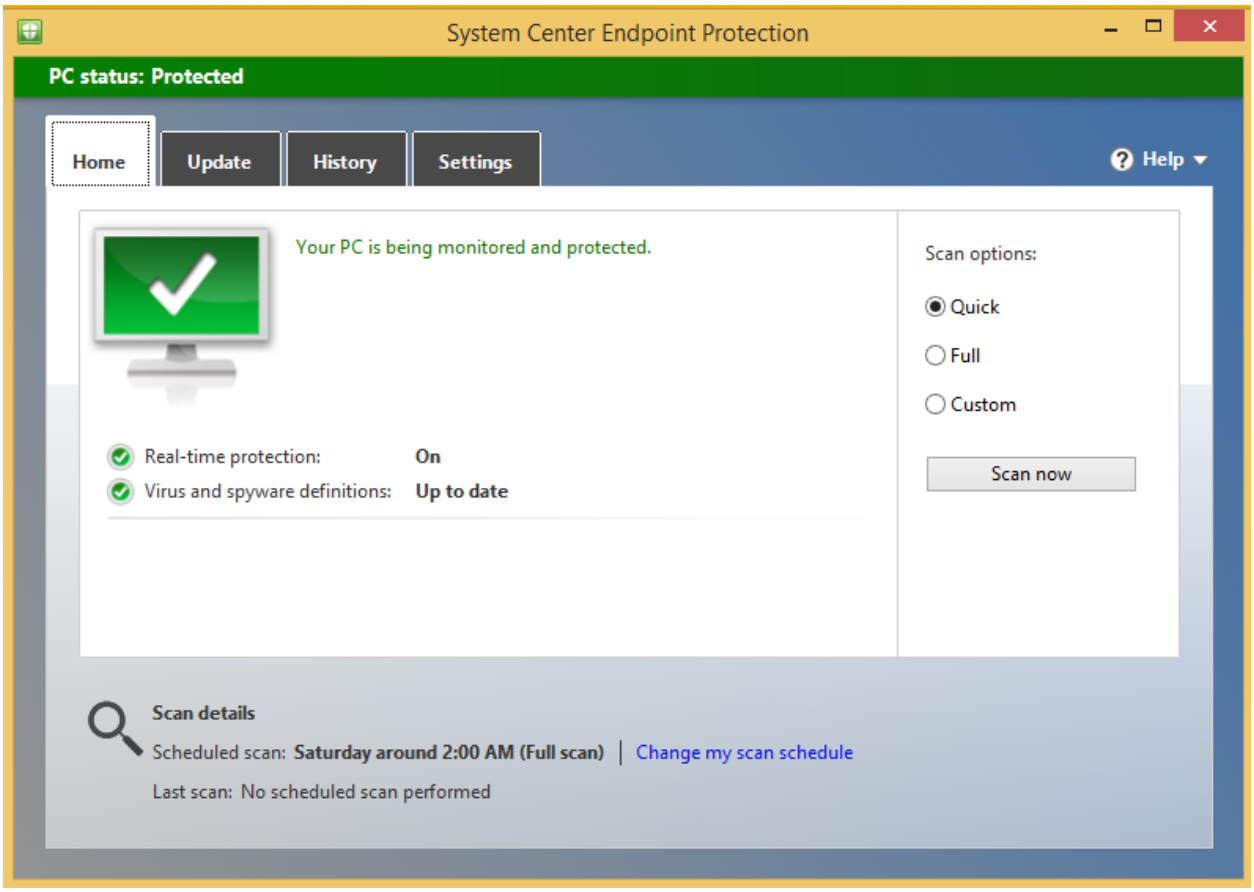
Yapılandırmamızı tamamladıktan sonra Antimalware Policy ayarını ilgili Collection' lara dağıtmayı unutmayınız.



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.


System Center Endpoint Protection
PC status: Protected
Home
Update
History
Settings
Help
Your PC is being monitored and protected.
Real-time protection: On
Virus and spyware definitions: Up to date
Scan options:
Quick
Full
Custom
Scan now
Scan details
Scheduled scan: Saturday around 2:00 AM (Full scan)
Change my scan schedule
Last scan: No scheduled scan performed

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

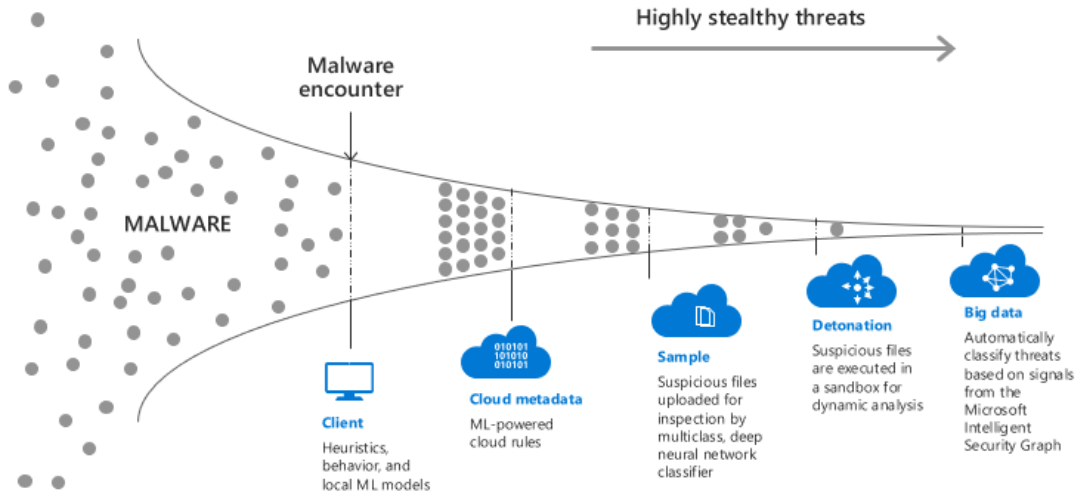
Microsoft Defender Antivirus

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

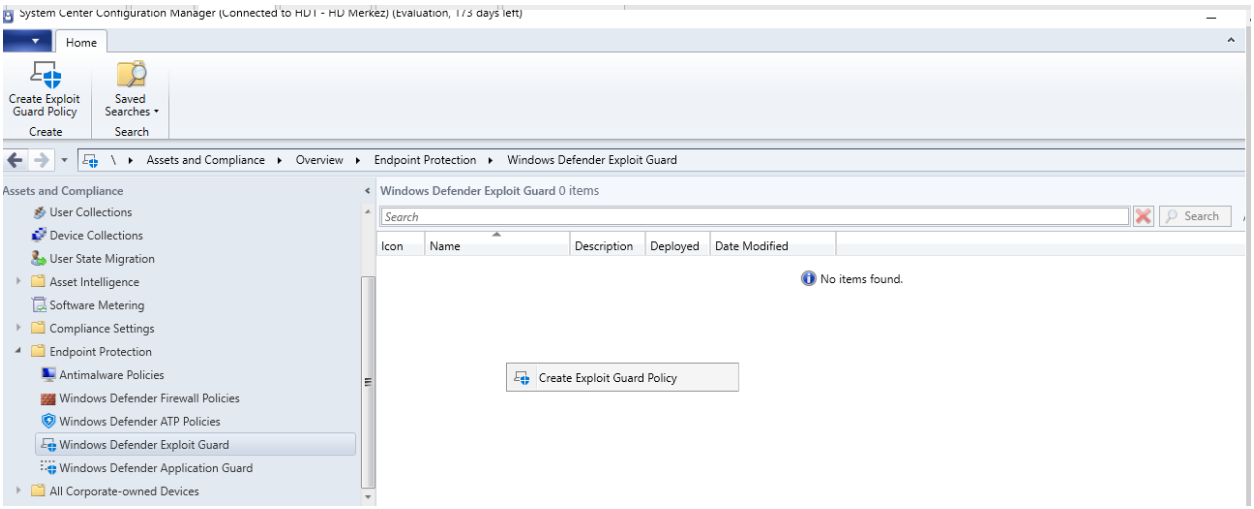
System Center Endpoint Protection

- 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

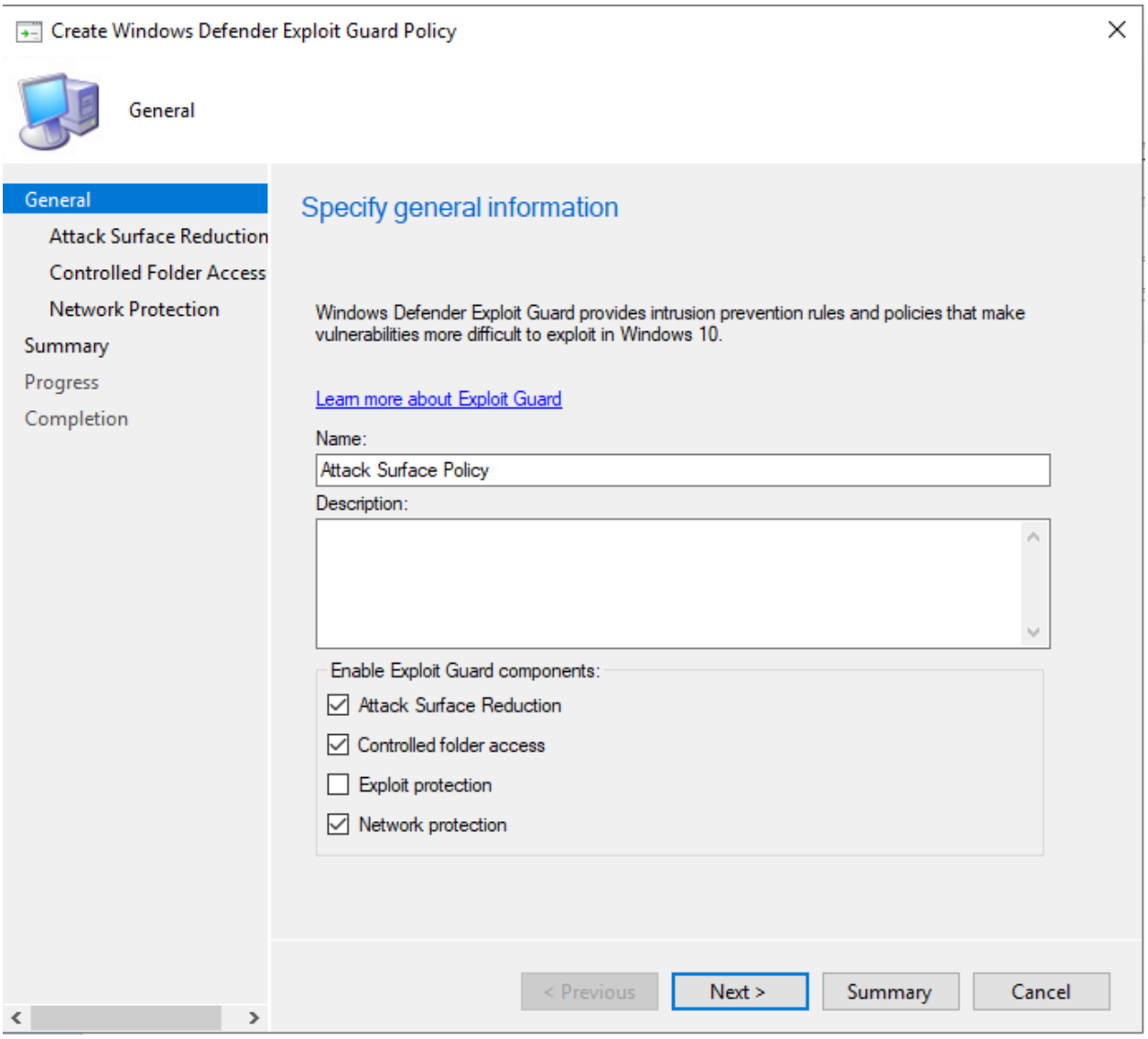
Exploit Guard özelliği sayesinde özellikle sıfırıncı gün saldırıları, kötü amaçlı yazılımlar, sofistike saldırılar,imza tabansız zararlılar, Filess tehditler, Ransomware atakları, Hardware lere karşı yapılan saldırılar ve daha fazlasına karşı koruma sağlamaktadır.



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.



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.

Attack Surface Reduction

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

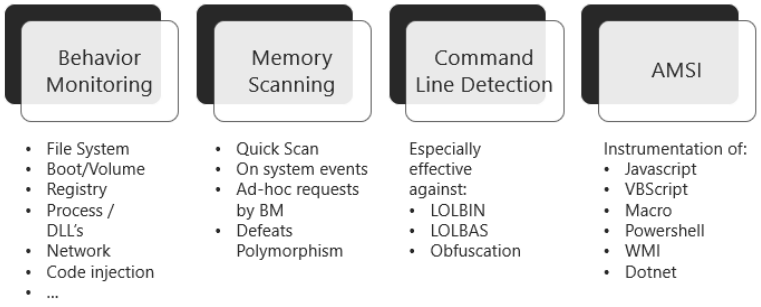
Microsoft Defender Antivirus

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

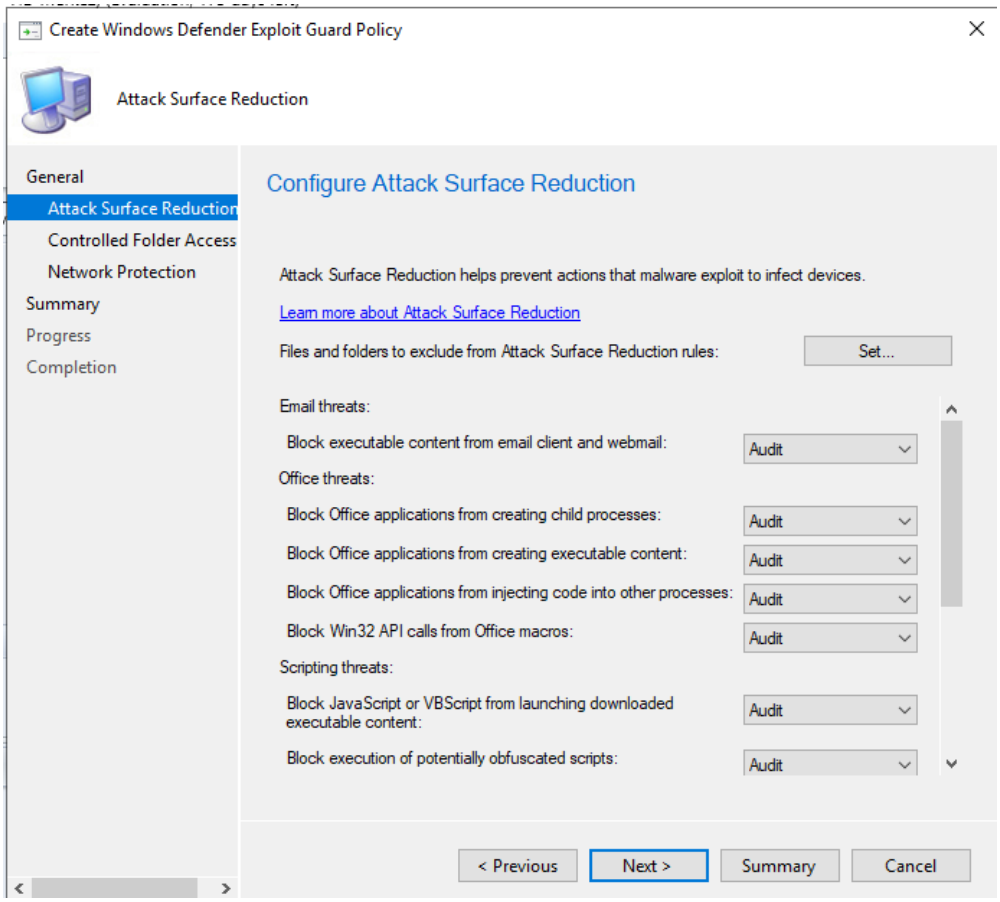
System Center Endpoint Protection

- 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

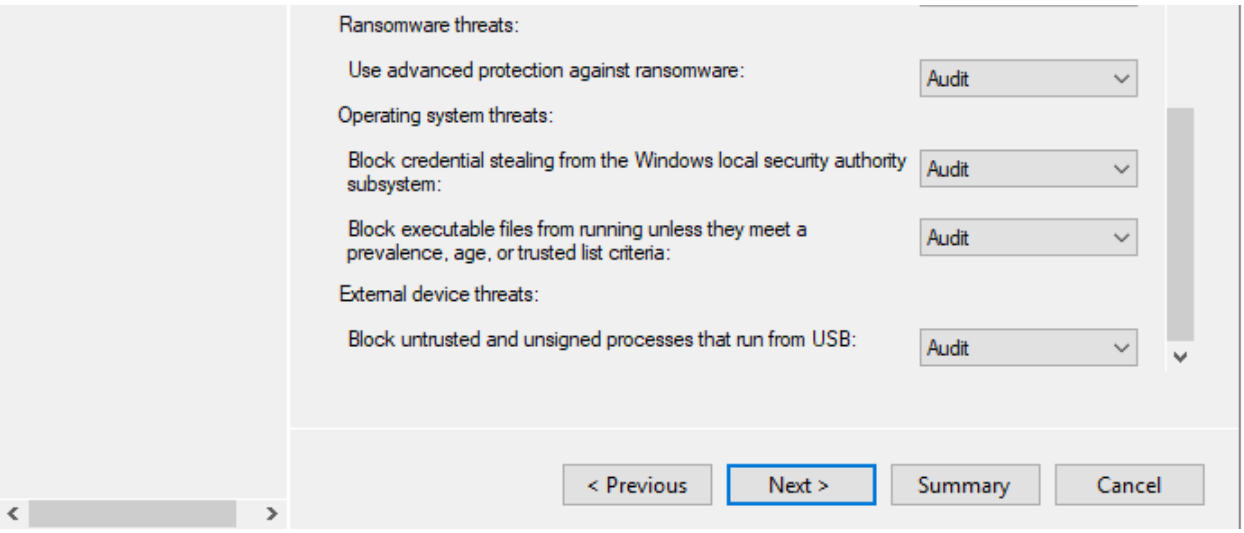
ASR ile birlikte aşağıdaki atak vektörlerine karşı koruma sağladığımızı belirtmiştik.



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



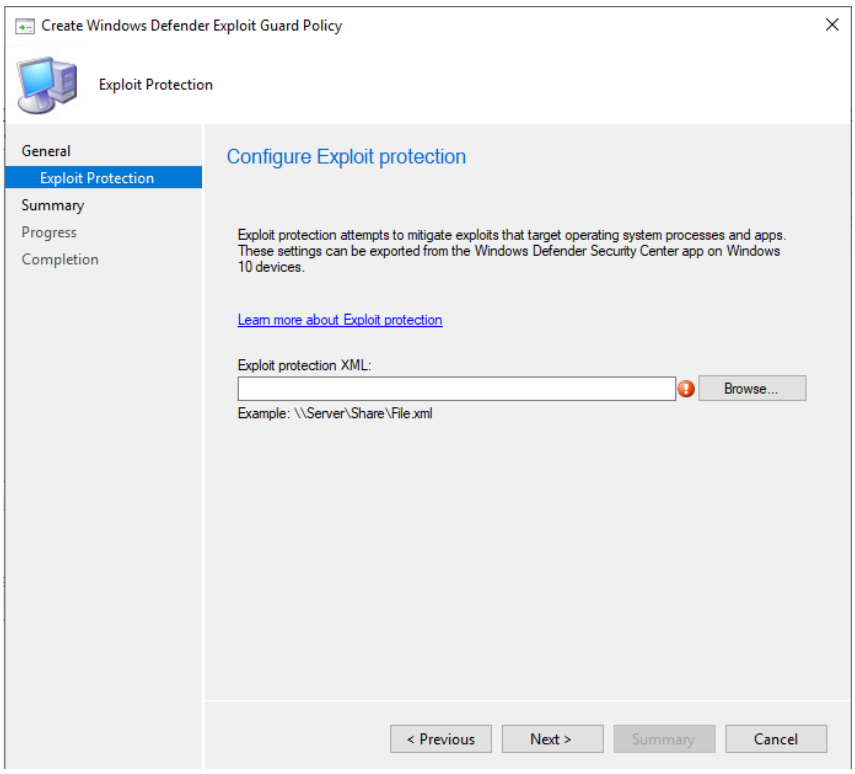
Eğer yapınız içerisinde harici cihazları(USB, External HDD vb) bloklamak istiyorsanız ayarımızı burada yapıyoruz.



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

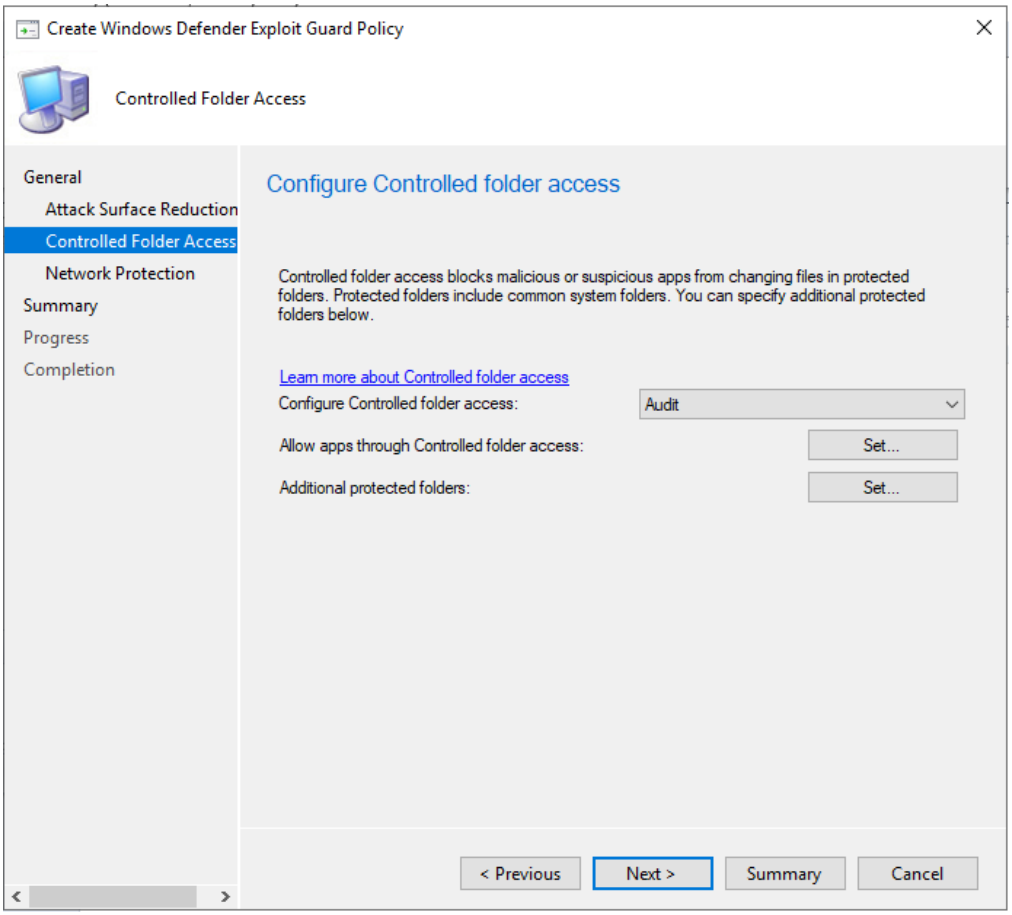
- Windows Server 2016

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

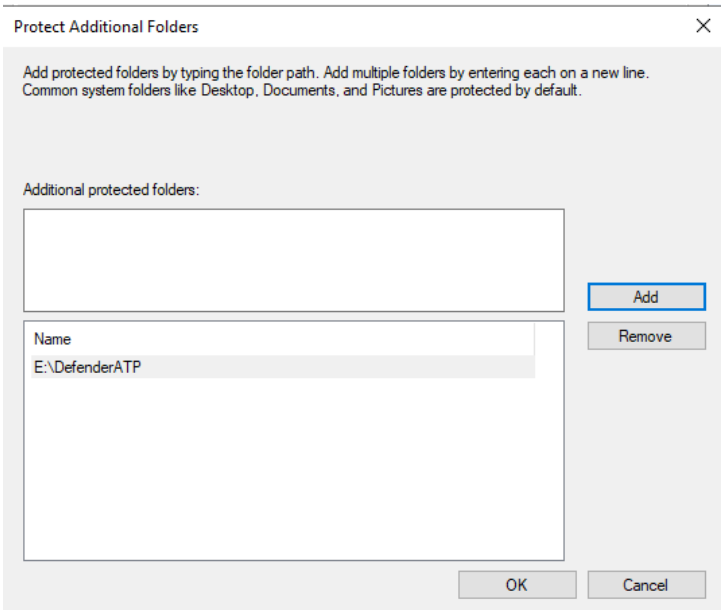
System Center Endpoint Protection

- 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

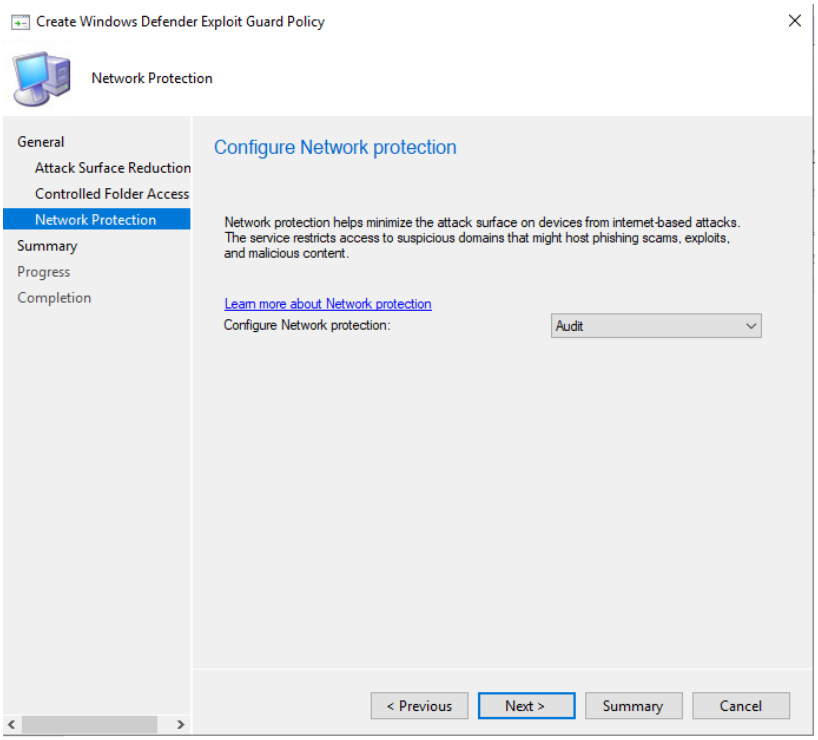
Microsoft Defender Antivirus

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

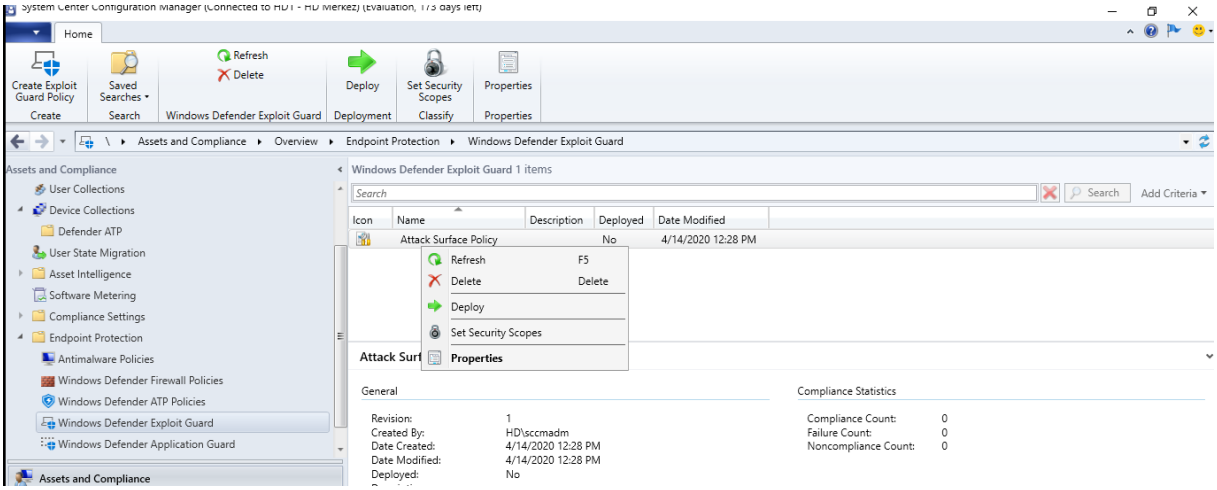
System Center Endpoint Protection

- 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 Sistemeri

- 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

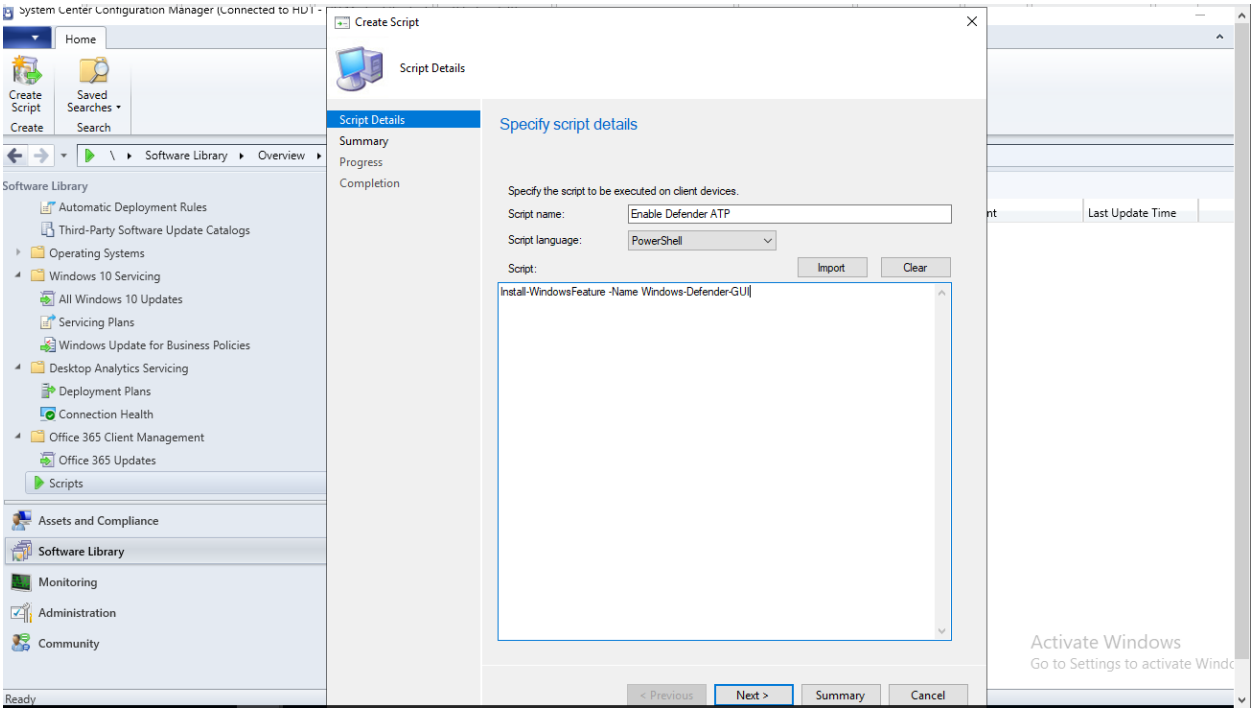
https://support.microsoft.com/en-us/lifecycle/search?alpha=Windows%2010%201709

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

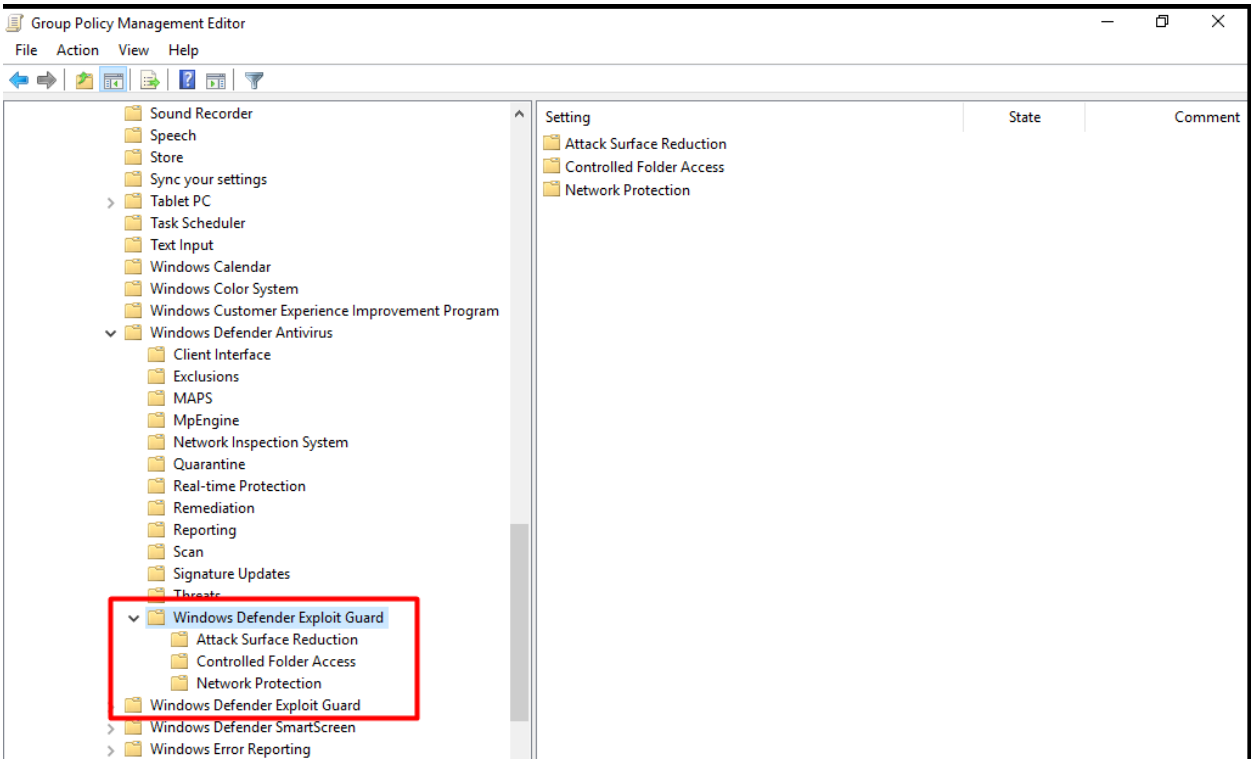
mevcut fakat aktif olmadığını varsayalım. Yine imdadımıza SCCM yetişiyor bu sefer Powershell' den küçük bir yardım alağacağız. Bildiğiniz üzere SCCM içerisinde script özelliği mevcut ve Powershell' i destekliyor. Bende bunu kullanarak Defender ATP' yi aktif hale getireceğim. **Install-WindowsFeature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



Group Policy ile Windows Defender Exploit Guard Yapılandırma

Attack Surface Reduction

Configure Attack Surface Reduction Rules



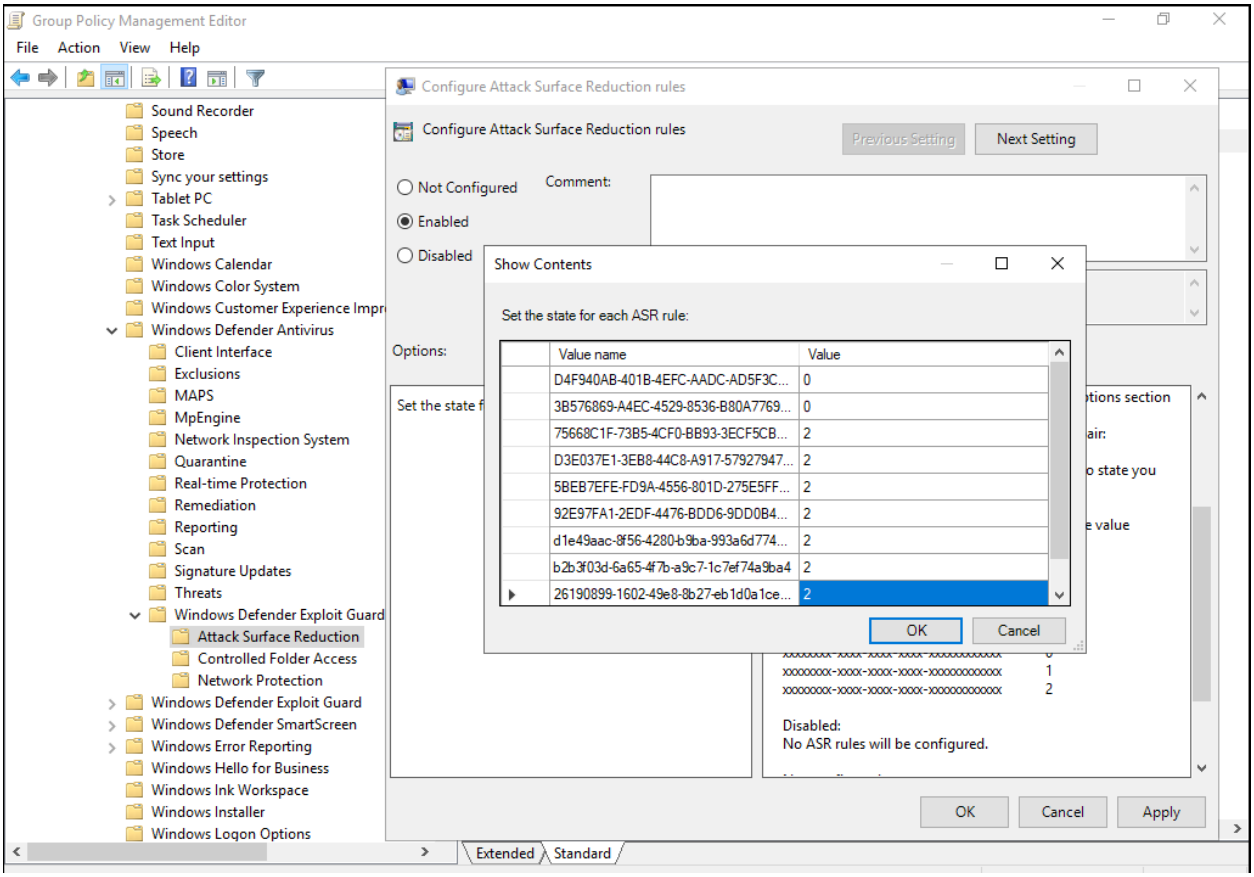
Group Policy ile yapılandırma kısmı malesef biraz daha meşakatli diyebilirim. Bu bölümde de değere 2 vererek başlangıç için Audit olarak yapılandırıyorum.

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

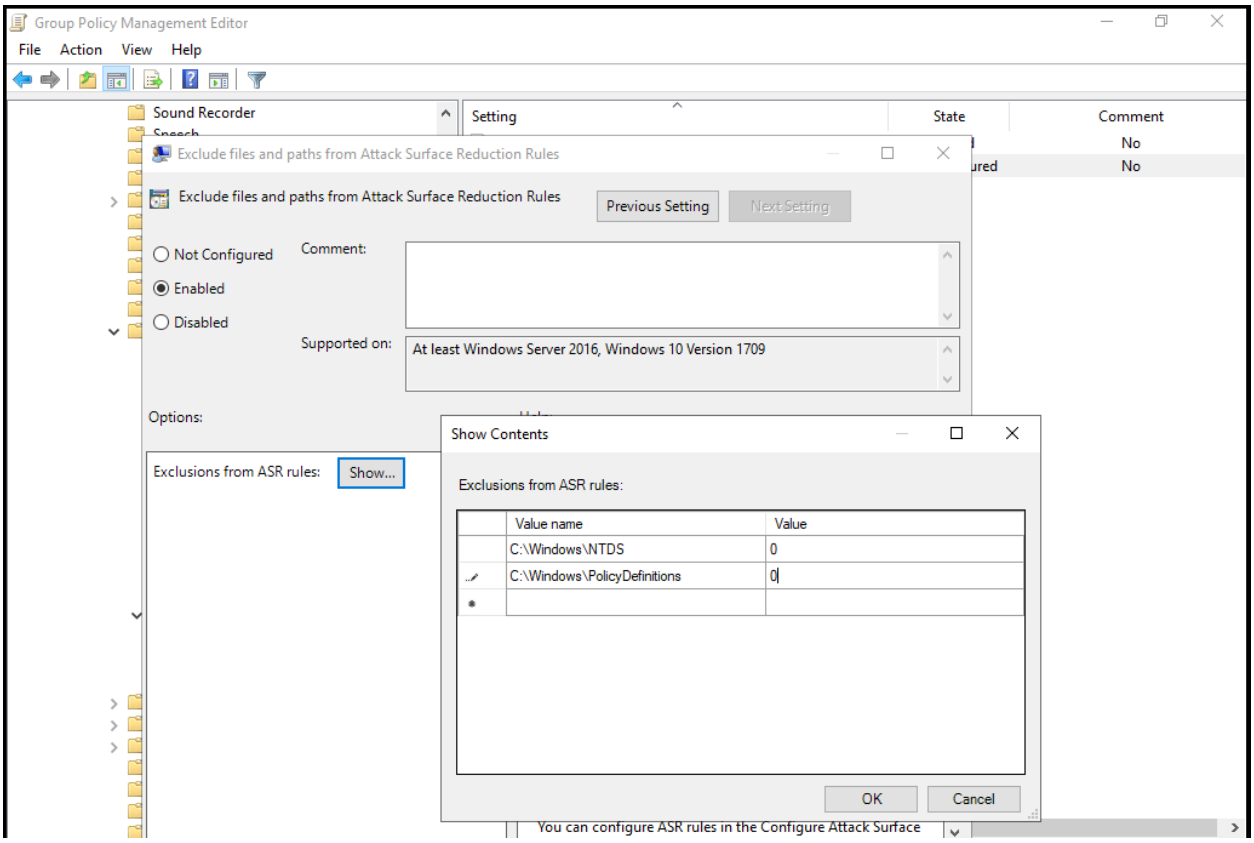


Peki yapılandırmamızı Audit olarak yapılandırdık. Takibini nasıl yapacağız ?

- 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

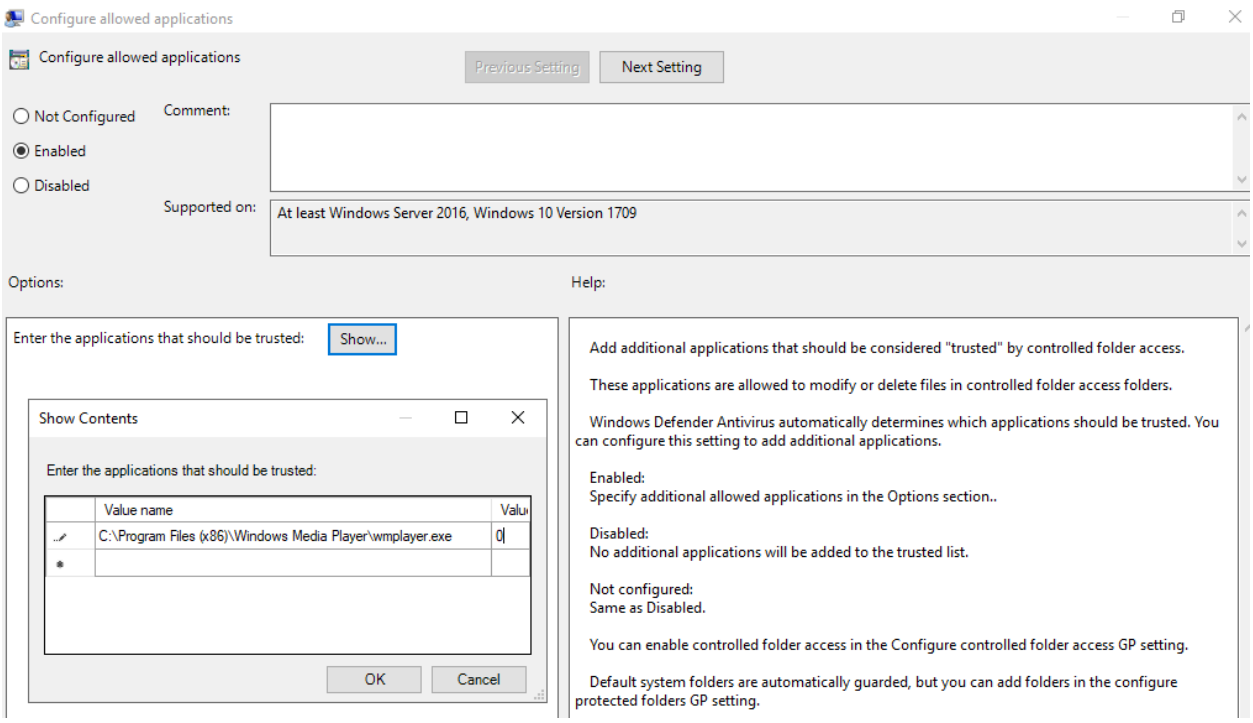
Yapınıza göre ve uygulama sunucularınızın çeşidine göre ASR kuralı için exclusion yazmanız gerekirse aşağıdaki örnekte olduğu gibi yapılandırabilirsiniz.



Controlled Folder Access

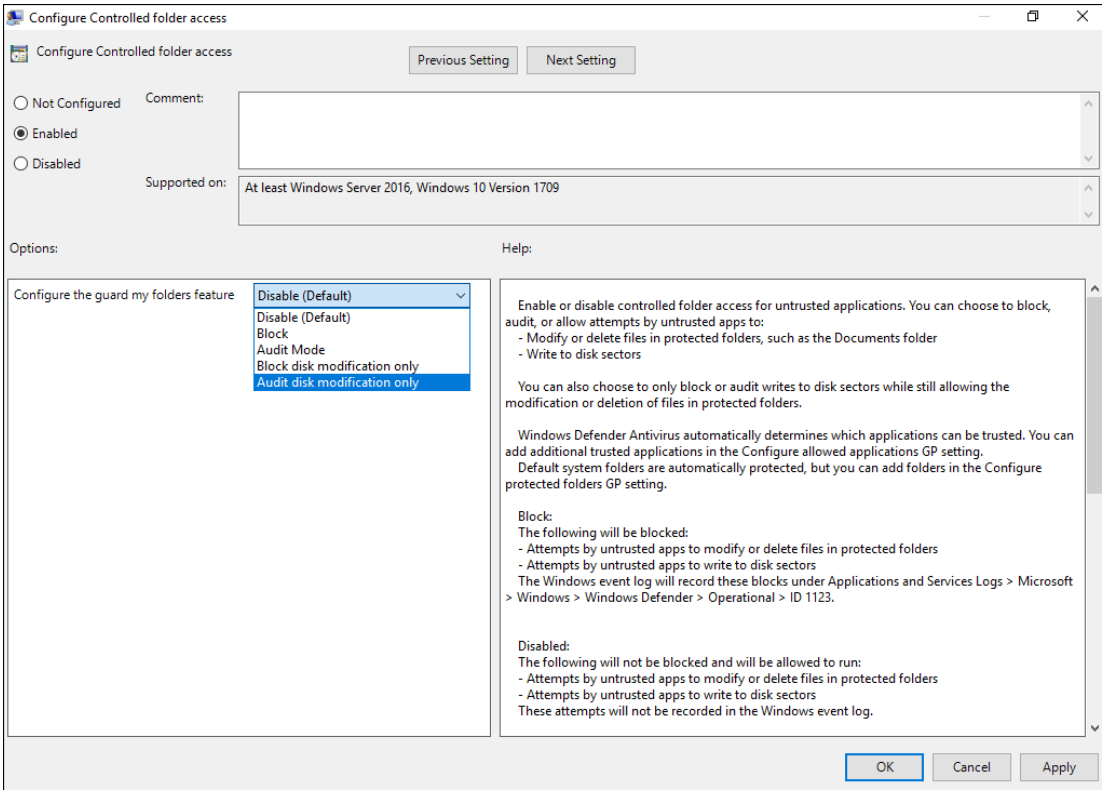
Configure Allowed Applications

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
C:\Program Files (x86)\Windows Media Player\wmplayer.exe
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.

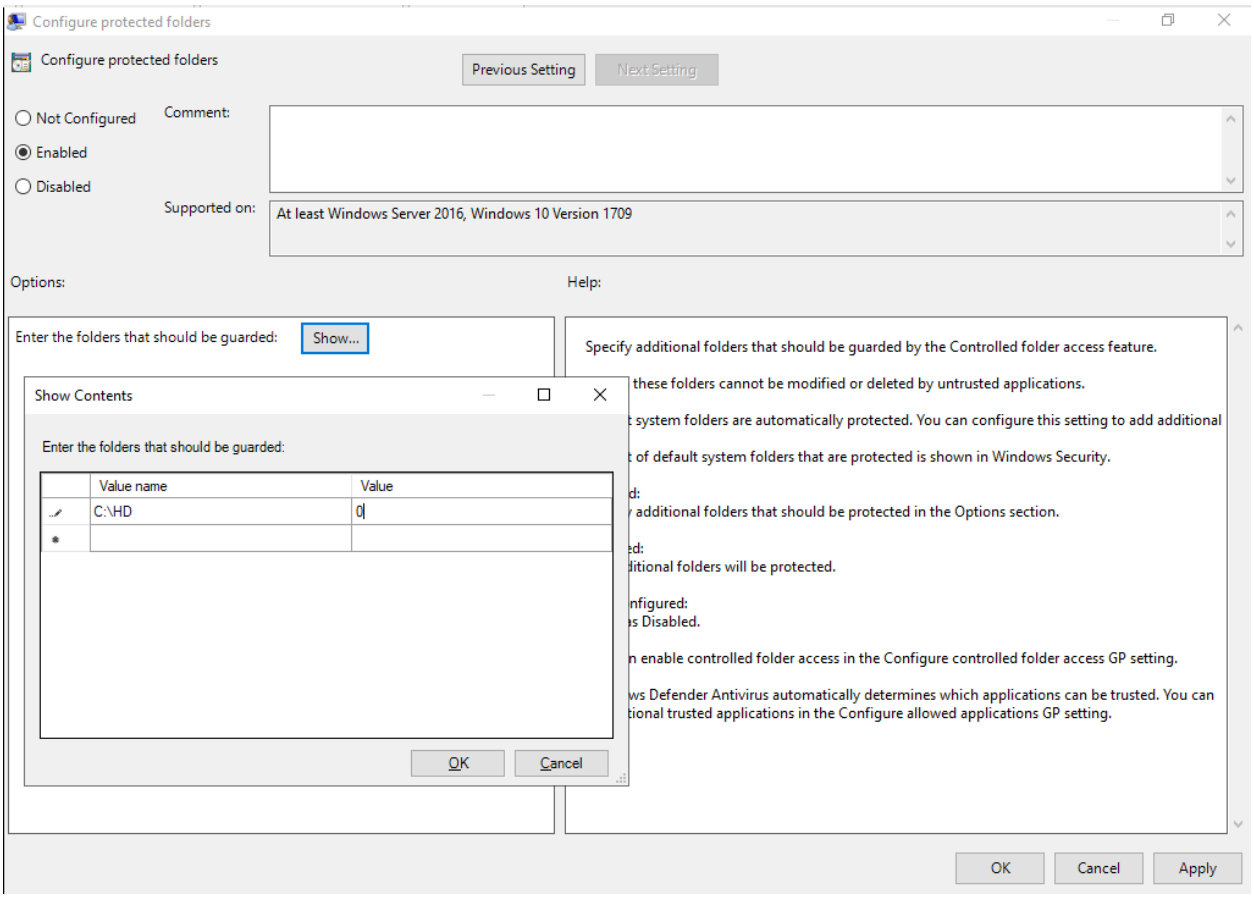
Configure Controlled Folder Access

Bu bölüme Exploit Guard bölümünde değinmiştim. 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=6TiHx6Pbqns&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.....

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

Saygılarımla

Hasan DİMDİK | CEH | MVP |MCT