

O'REALLY?



# Azure Sentinel Başlangıç Kılavuzu

**Hasan Dimdik & Ömer Taşkın**

## Yazarlar Hakkında



1993 yılında İstanbul'da doğdum lise ve üniversitede bilgisayar bölümünü okudum iş hayatına ilk olarak bir hastanede sonra ise Hasan abimle birlikte Netaş'da devam ettim. O Allianz için ben ise Glasshouse için aynı ay Netaş'dan ayrıldık yine aynı ay içinde o bugünkü çalıştığı Emirates NBD'ye ben ise halen devam ettiğim Vakıf Emeklilik'e geçiş yaptık. Son zamanlarda yoğunlukla güvenlik üzerine çalışıyorum günlük operasyonun dışında PIM & PAM, SOAR, SIEM tarafıyla da yakından ilgileniyorum.

CEH (Certified Ethical Hacker)

Check Point Certified Security Expert R80 (CCSE)

Check Point Certified Security Administrator R80 (CCSA)

ICSI, Certified Network Security Specialist

Cyberark Trustee

Microsoft MTCC, MCSA, MCSE

Kendisinin Goutetsu olarak gördüğüm çok kıymetli hocam ve abim olan Hasan Dimdik'e bana bu E-Book'da yer verdiği için Gouken olarak kendisine teşekkürü bir borç bilirim.

-Ömer Taşkın



Profesyonel iş hayatımı 2008 yılında başladım. 12 Yıllık dönemde teknikerlikten başlayarak bir çok farklı pozisyonda çalıştım. Dünyanın en büyük sigorta şirketleri arasında yer alan Allianz Türkiye' de Kıdemli Sistem Uzmanı olarak çalışmaktan sonra beni heyecanlandıran bir teklif üzerine Dubai' ye taşındım ve iş hayatımı Emirates NBD bankasında Kıdemli Sistem Mühendisi olarak devam etmekteyim. Profesyonel iş yaşamım dışında yönetim kadrosunda yer aldığım [www.mshowto.org](http://www.mshowto.org) sitesinde gönüllü yazarlık yapmaktadır. 20+ konferansta konuşmacı olarak yer aldım. 150+ makale ve bu yazı serisi ile birlikte dokuzuncu E-Kitabımı yazmanın mutluluğunu yaşamaktayım.

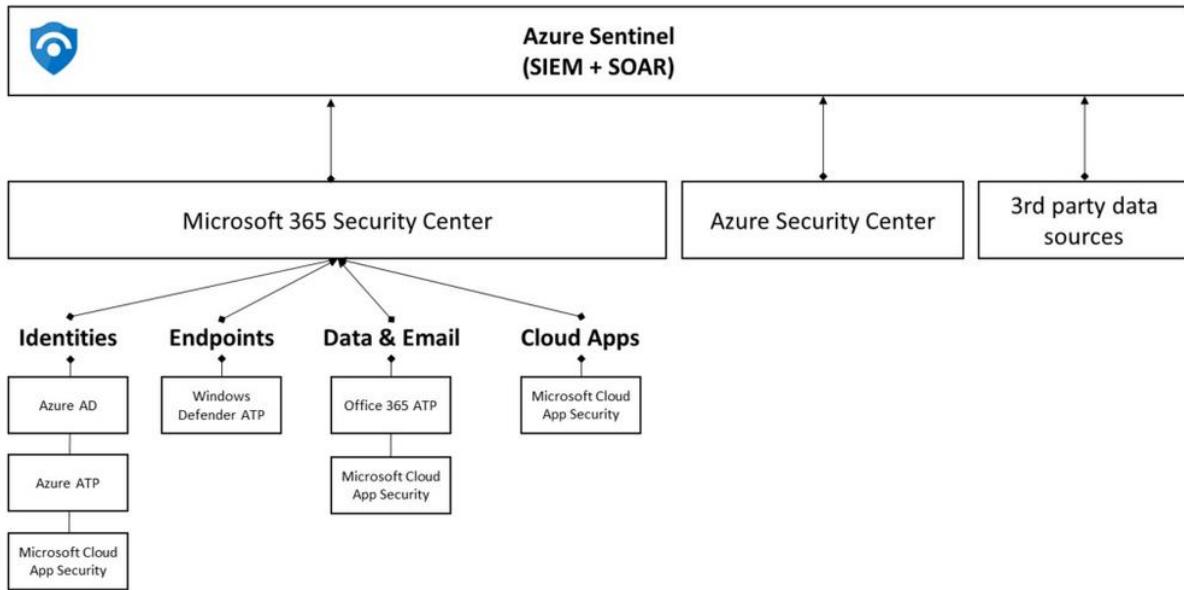
- ✓ CEH | Certified Ethical Hacker
- ✓ MCT | Microsoft Certified Trainer
- ✓ MVP | Cloud and Datacenter 2019-2020
- ✓ MVP | Enterprise Mobility 2016-2017, 2018-2019
- ✓ Microsoft MCSE | MCSA | MCPS | MTCC
- ✓ AZ-900 Microsoft Azure Fundamentals
- ✓ Microsoft Specialist: Server Virtualization with Windows Server Hyper-V and System Center Specialist
- ✓ Tenable Certificate of Proficiency
- ✓ ICSI | CNSS Certified Network Security Specialist
- ✓ Fortinet | NSE1-2 Network Security Associate

Hasan Dimdik

## İçerik

Yazarlar Hakkında.....	2
Azure Sentinel Başlangıç Kılavuzu.....	5
Overview .....	7
New & Guides .....	8
Threat Management .....	8
Data Connectors & Workbooks .....	8
<i>Azure Sentinel Windows Güvenlik Duvarı Entegrasyonu</i> .....	10
<i>Azure Sentinel Office 365 Entegrasyonu</i> .....	14
<i>Azure Sentinel Insecure Protocols Dashboard Entegrasyonu</i> .....	19
<i>Security Events</i> .....	25
<i>ASC Compliance and Protection</i> .....	27
<i>Workbooks / Templates &amp; My Workbooks Farkı Nedir ?</i> .....	30
Analytics & Incidents.....	33
<i>Şablonları Kullanarak Kural Oluşturma</i> .....	34
Hunting.....	40
Notebooks.....	45
Configuration .....	46
Playbooks .....	46
Settings.....	50
Son Söz .....	52

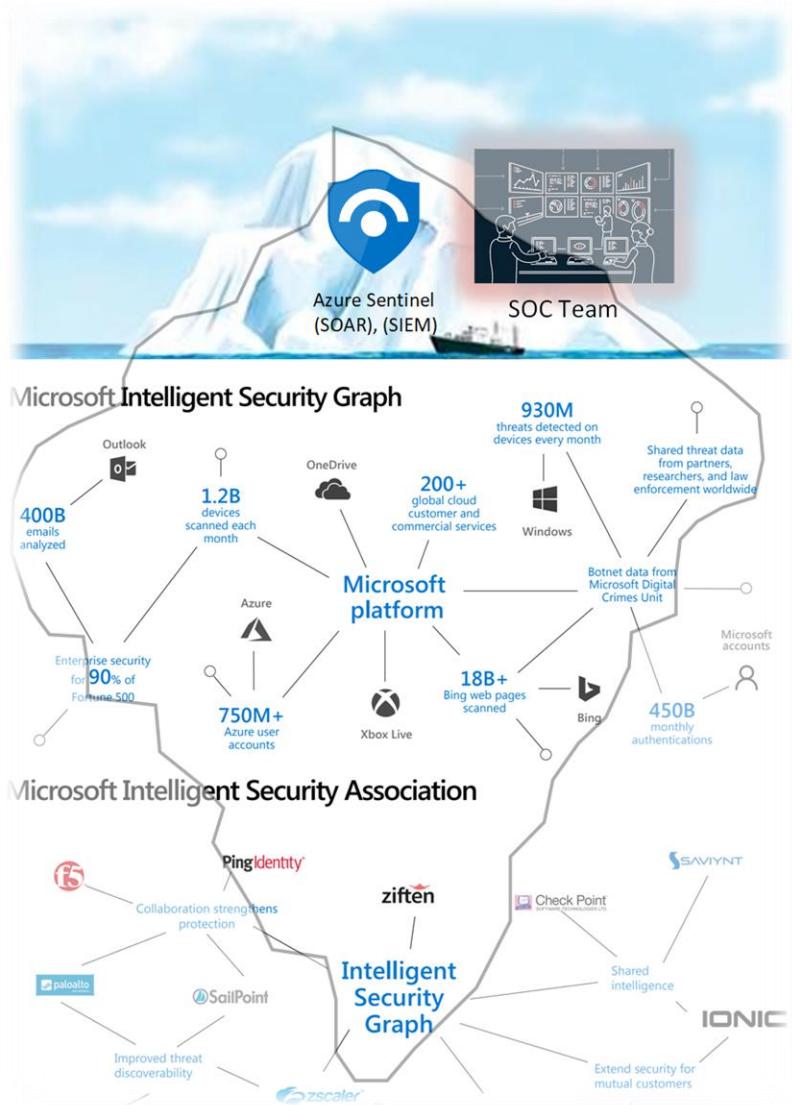
## Azure Sentinel Başlangıç Kılavuzu



Azure Sentinel, bulut tabanlı yeni nesil bir SIEM + SOAR ürünüdür. Azure Sentinel'i kullanabilmemiz için log üreten servis ve uygulamaları ona bağlamamız gerekmektedir. Azure Sentinel'in en önemli avantajlarından birisi bulutun gücünü arkasına alarak ölçeklenebilir olmasıdır. Diğer bir ifade ile sunucu konfigürasyonu ile uğraşmadan ve kaynak sıkıntısı yaşamadan sadece işimize odaklanmamızı sağlar. Örnek olarak Active Directory, Office 365, Windows Güvenlik Duvarı, Palo Alto Fw gibi teknolojileri birkaç tıklama ile entegre edebiliriz.

Günümüzde bulutun gücü artık inkar edilemez hale geldi. Özellikle yapılan ataklara baktığımızda klasik saldırılar yerine daha sofistike ataklar ile saldırganların hedeflerine saldırdıklarını görüyoruz. Bulutun hızlı şekilde ölçeklenebilmesi ve hızlı şekilde güncel tehditlere ayak uyduracak dinamik altyapıya sahip olması bulut tabanlı SIEM ürünlerini artık bir adım öne çıkarmaktadır.

Azure Sentinel bize sınırsız, ölçeklenebilir, bulutun hızını ve gücünü kullanmamıza olanak sağlamaktadır.



### Peki Ben Azure Sentinel kullanmaya neden başlamalıymı ?

- Altyapı yerine tamamen güvenliğe odaklanmamızı sağlar ve bakım gibi bir sorunla yüzleşmemeyiz.
- Tamamen ölçülebilir olması, aynı zamanda depolama ile ilgili sorununuz tamamen ortadan kalkar.
- Azure Sentinel ile birlikte Machine Learning, Logic Apps ve Azure Monitor' ün de gücünü kullanmış oluyoruz.

Azure Sentinel' in temel işlevine baktığımızda üç ana bölümden oluşmaktadır. Azure Sentinel korelasyon için Fusion teknlığını kullanmaktadır. Fusion nedir diye soracak olursanız SecOps için Machine Learning teknolojisi diyebiliriz. Fusion arkada anomaliler arasında ilişki kurmak için graph kullanmaktadır.

- Investigate ile hızlı şekilde atağın tüm anatomisini ve etkisini hızlı şekilde öğrenebilmekteyiz.
- Hunting , Microsoft uzmanlarının MITRE' ye dayanarak hali hazırda yazmış olduğu Built-in sorgular ile şüpheli aktiviteleri bulmamızı sağlar.
- Automate ile bir çok operasyonumuzu otomatik hale getirebilmekteyiz.

## AWS' de Azure Sentinel' e karşılık gelen teknoloji mevcut mu ?

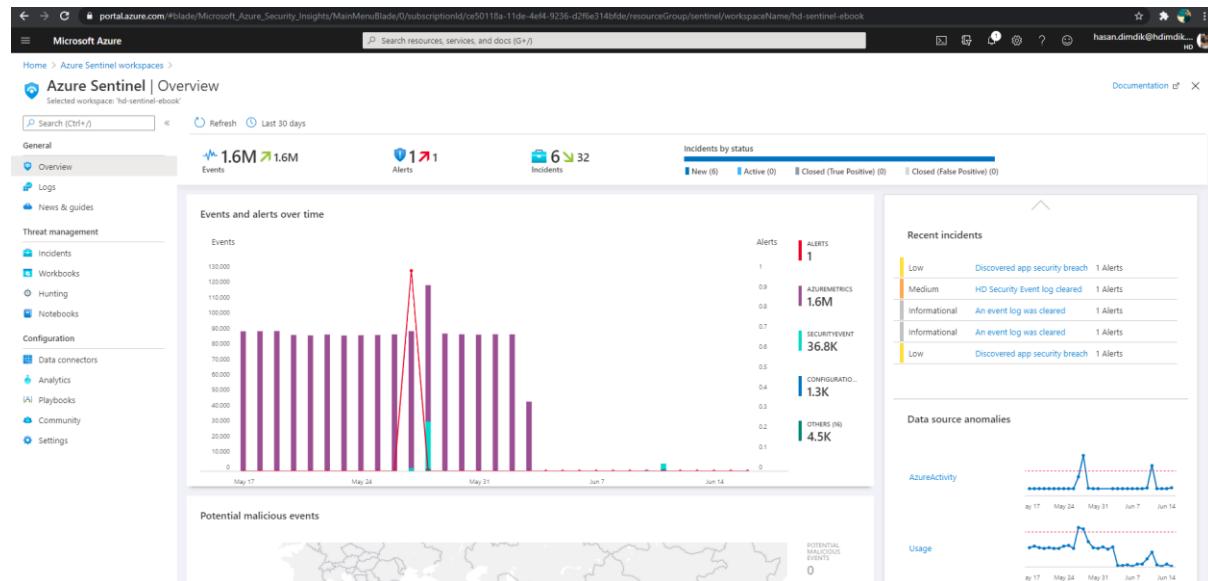
GuardDuty ürünü sadece AWS iş yüklerini korumak için tasarlanmıştır. Bunun yanı sıra Azure Sentinel yakında zamanda AWS Cloudtrail den veri aktarabilecek hale gelecektir.

## Google' da Azure Sentinel' e karşılık gelen teknoloji mevcut mu ?

Google baktığımızda daha yeni Chronicle' i tanıttı fakat tam olarak SIEM ürünü olduğunu hala söyleyemiyoruz. Henüz Automation, orchestration , ML modellerini custome hale getirme ve interaktif araştırma aracı henüz bulunmamaktadır.

## Overview

Azure Sentinel içerisinde oluşanaların, olayları, toplanan logların genel olarak gördüğümüz dashboard umuz. İlgili logların nasıl olduğu, gerekli connector u nasıl ve nereden ekleyeceğiz sorularına yazı içerisinde değineceğiz.



## New & Guides

Azure Sentinel sekmleri arasında boğulmadan üç adımda nasıl dataları toplar, alarm üretir ve alarmlara göre otomasyon kurallarımızı yazarız in tek çatı altında toplandığı sekme diyebiliriz. Bir nevi yeni başlayanlar için adım adım neleri takip etmemiz gerektiğini göstermektedir. Aynı zamanda Azure Sentinel' e gelen yenilikleri What's new sekmesinden takip edebiliyoruz.



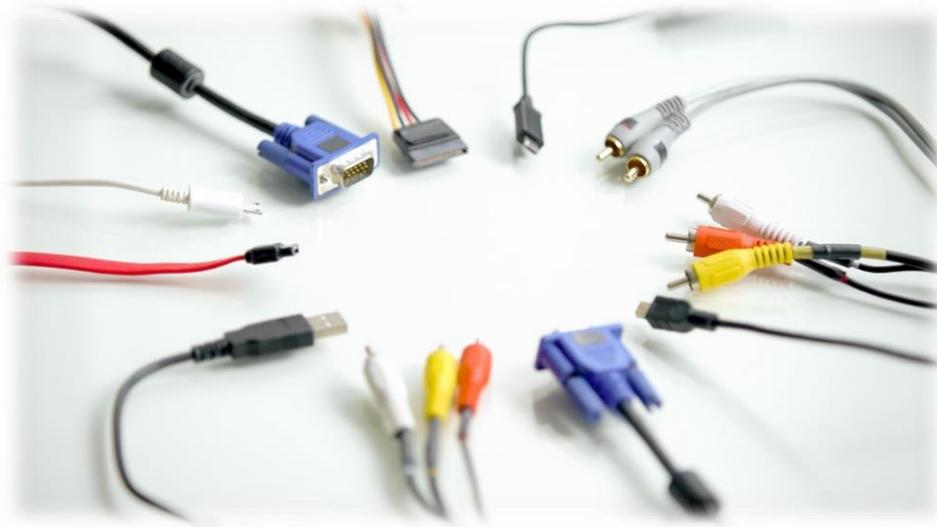
## Threat Management

### Data Connectors & Workbooks

Bildığınız üzere Azure Sentinel aslında boş bir havuz. Havuzu ne kadar fazla ve çeşitli veri ile doldurursak monitör edebileceğimiz alanda o kadar büyük olacaktır ve farkındalığımız artacaktır.



Aynı zamanda ne kadar fazla ve çeşitli veriyi ilgili havuza aktıtabilirsek bu da bizim korelasyonunu yapabileceğimiz o kadar verimiz olduğu anlamına gelecektir. Bu noktada atlanılmaması gereken en önemli noktalardan bir tanesi gerçekten gerekli verilerin bu havuza aktılması olacaktır, aksi takdirde kritik logların gözden kaçması kaçınılmaz olacaktır.



**Data Connectors** ise bu noktada gözden kaçmaması gereken logları bağlayacağımız aracı olacaktır. İlgili sekmeye geldiğimizde ise farklı vendor lara ait connector leri bulabiliyoruz. Yapımız için eklemek istediklerimizi buradan seçebiliyoruz.

The screenshot shows the Azure Sentinel Data connectors page. On the left, there's a sidebar with navigation links like Overview, Logs, News & guides, Threat management, and Configuration. Under Configuration, 'Data connectors' is selected. The main area displays a list of connectors categorized by provider: Vectra AI, Alcide, Amazon, Microsoft, and others. A specific connector, 'AI Vectra Detect (Preview)', is highlighted on the right with its status as 'Not connected'. It includes a description, last log received information, related content (1 workbook, 4 queries, 0 analytic rules templates), and a data received chart. There are also buttons to 'Open connector page' and 'Connect'.

**Connector** lerin entegre edilmesi/eklenmesi son derece kolay. Elbette her ürünün ön gereksinimi farklı olacaktır. Office 365 için tenant bilgisi girilmesi gereklidir, Security Event için ise Log Analytics agent yüklenmesi ön gereksinim olarak karşımıza gelecektir.

Data Connector leri ekledikten sonra toplanan verileri görsel olarak Dashboard larda görmek istersek **Workbooks**ları kullanıyoruz. Workbookları tek başına kullanamazsınız, illa bir Connector ün bağlanmış olması gerekmektedir. Aynı zamanda gerekli olan verinin sağlıklı toplanması gerekmektedir. Örneğin **Identity & Access** workbookunu kullanmak istersek gerekli veri tipini toplayabiliyor olmamız gerekmektedir.

Microsoft Azure

Home > Azure Sentinel workspaces > Azure Sentinel - Workbooks

Selected workspace: HD-Sentinel (last)

Search (Ctrl+F)

Refresh Add workbook

2 Saved workbooks + 39 Templates 0 Updates

My workbooks Templates

Search workbooks

Identity & Access MICROSOFT

Gain insights into Identity and access operations by collecting and analyzing security logs, using the audit and sign-in logs to gather insights into use of Microsoft products.

This template provides a dashboard and reports across login events from all users and machines. This workbook also identifies suspicious entities from login and access events.

Required data types: SecurityEvent

Relevant data connectors: SecurityEvents

Identity & Access MICROSOFT

Insecure Protocols MICROSOFT

Linux machines MICROSOFT

Microsoft Cloud App Security - discovery logs MICROSOFT

Microsoft Web Application Firewall (WAF) - firewall events MICROSOFT

Microsoft Web Application Firewall (WAF) - gateway access events MICROSOFT

## Azure Sentinel Windows Güvenlik Duvarı Entegrasyonu

Haydi Azure Sentinel'i aktif edelim.

Giriş > Tüm kaynaklar > Yeni > Azure Sentinel

Azure Sentinel Microsoft

Azure Sentinel [Olustur] Sonrası On Kaydet

Azure Sentinel is Microsoft's cloud-native SIEM that provides intelligent security analytics for your entire enterprise at cloud scale.

This SIEM as a Service (SIEMaaS) solution is designed as a cloud-based security-monitoring platform that leverages the power of the cloud for analytics and detections.

**Limitless cloud speed and scale**

Azure Sentinel is the first SIEM built into a public cloud platform to help your security analysts focus on what really matters.

**Easily connect your data sources**

Azure Sentinel provides simple and easy integration with signals and intelligence from security solutions whether they are on premises, in Azure, or in other clouds. Azure Sentinel provides seamless integration with Microsoft 365, Azure, and other Microsoft products, including Microsoft's security products.

**Detect suspicious activities in your organization**

Azure Sentinel fuses together unique machine learning algorithms, world-class security research, and the breadth and depth of the critical security data available to Microsoft as a major enterprise vendor. Azure Sentinel helps you detect both known and unknown attack vectors, detecting threats across all stages of the kill chain.

**Investigate and remediate breaches**

Azure Sentinel gives you visibility into all the entities involved in an alert and provides a simple and instinctive UI to investigate the detection, helping you easily understand the scope of the breach.

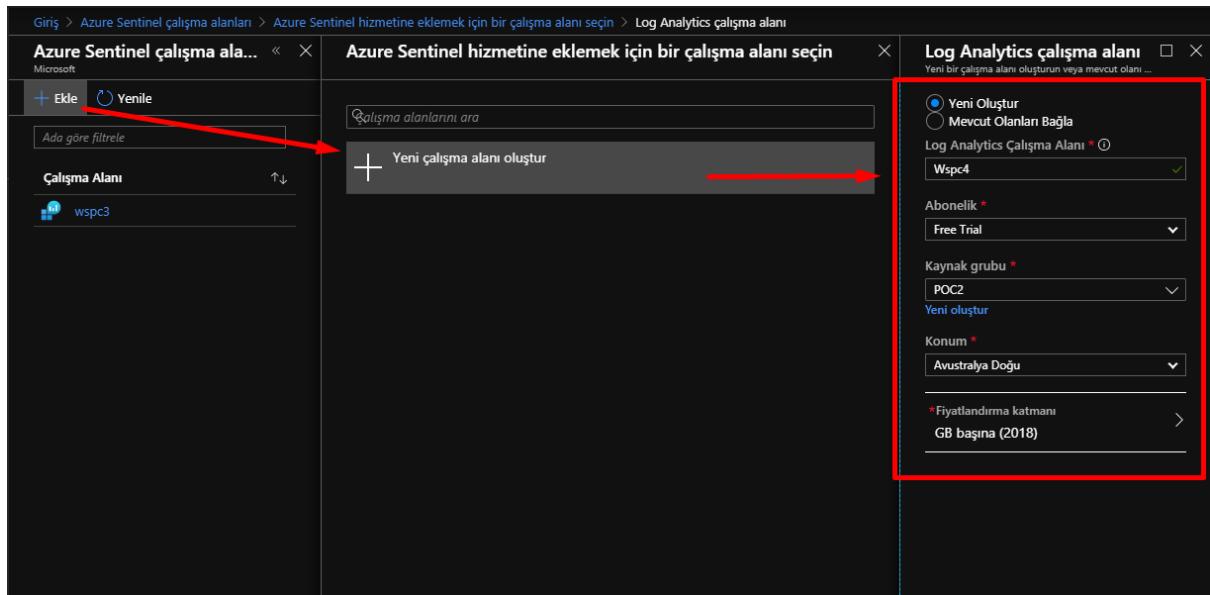
To cut down the volume of alerts you get, Azure Sentinel automatically investigates alerts to help you determine what action to take, enabling you to move from alert to remediation in minutes, at scale.

Leveraging the power of Logic Apps, Azure Sentinel helps you respond to incidents instantly, using built-in orchestration and automation playbooks.

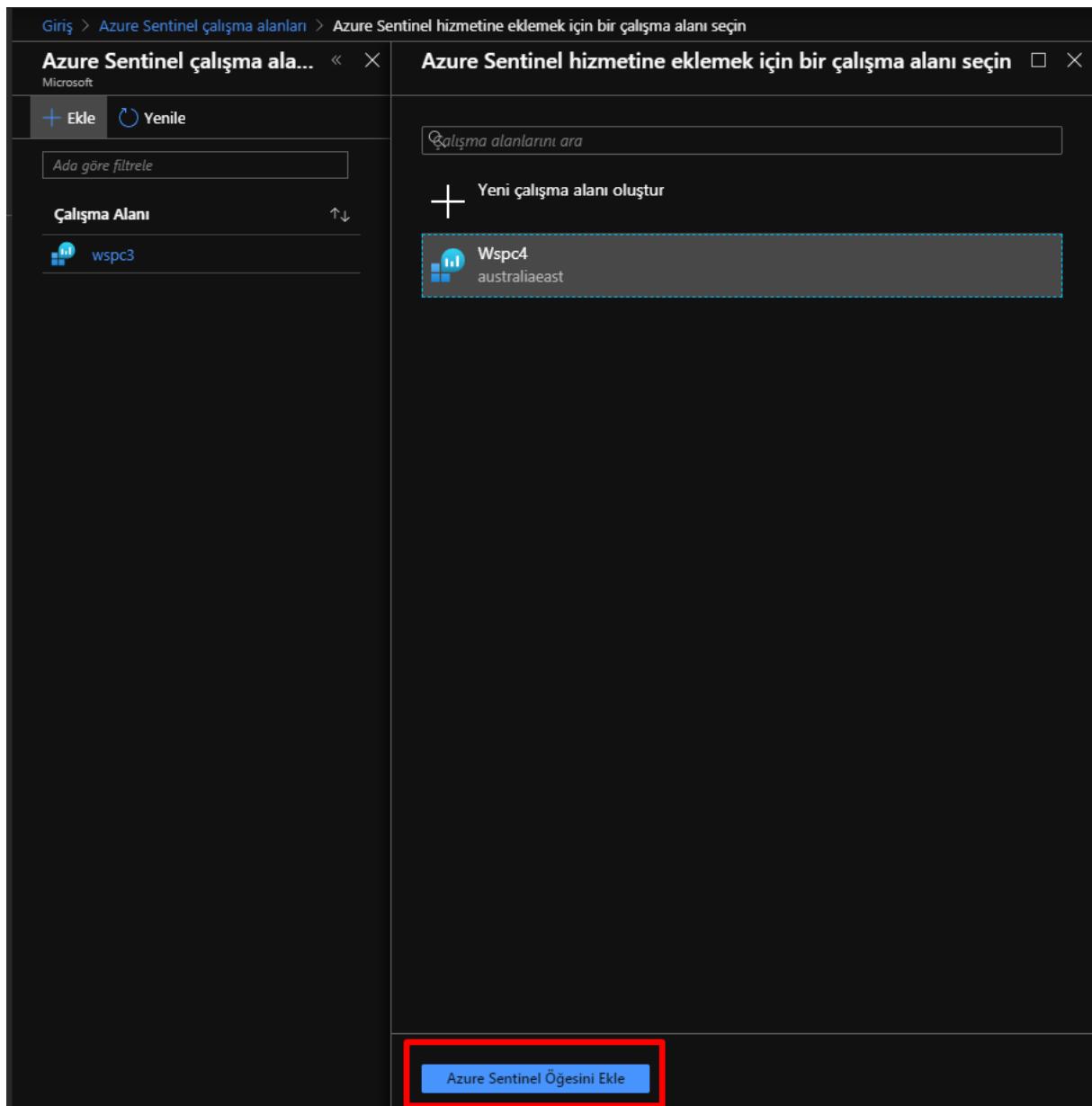
Faydalı Bağlantılar Documentation

WYSIWYG

Normal bir SIEM'e kıyasla burada işler biraz farklı. Azure'da ki çalışma alanı mantığı ile bağlıyoruz, bir çalışma alanında birden fazla log üreten cihaz olabilir. İster yeni bir çalışma alanı oluşturabilir ister var olanı bağlayabiliriz. Ben yeni bir alan oluşturmayı tercih ediyorum. Çalışma alanlarının mantığı için ayrıca bakmanızda fayda var.



Oluşturduğumuz alanı Sentinel'e ekliyoruz.



Menüden Veri Bağlayıcıları sekmesinden “Windows Güvenlik Duvarı” ‘nı bulun ve ok ile gösterdiğim kısımdan Bağlayıcı sayfasını aç ile bir sonraki adıma geçin.

Azure Sentinel - Veri bağlayıcıları

31 Bağlayıcılar 3 Bağlı 1 Yakında

Windows Güvenlik Duvarı

Bağlı DURUM Microsoft SAĞLAYICI ALINAN SON GÜNLÜK

Açıklama

Windows Güvenlik Duvarı, Internetten sisteminize gelen bilgileri filtreleyen ve zararlı olabilecek programları engelleyen bir Microsoft Windows uygulamasıdır. Yazılım, çoğu programın güvenlik duvarı aracılığıyla iletişim kurmasını engeller. Kullanıcıları, bir programın güvenlik duvarı üzerinden iletişim kurmasına izin vermek için programı izin verilen programlar listesine eklemesi yeterlidir. Bir ortak ağ kullanıldığında, Windows Güvenlik Duvarı bilgisayarına yönelik istenmeyen tüm bağlantı girişimlerini engelleyerek sistemin güvenliğini sağlayabilir.

Çözümü yükle ile yüklemeyi gerçekleştirelim, yüklenikten sonra **1.Aracıyı indirin ve yükleyin** bölümünden “Azure Sanal makineleri için arayıcı indirin ve yükleyin” kısmından Azure üzerinde çalışan sanal makinemizi sağlamak için bir sonra ki adıma geçelim.

Windows Güvenlik Duvarı

Windows Güvenlik Duvarı

Bağlı değil DURUM Microsoft SAĞLAYICI ALINAN SON GÜNLÜK

Açıklama

Windows Güvenlik Duvarı, Internetten sisteminize gelen bilgileri filtreleyen ve zararlı olabilecek programları engelleyen bir Microsoft Windows uygulamasıdır. Yazılım, çoğu programın güvenlik duvarı aracılığıyla iletişim kurmasını engeller. Kullanıcıları, bir programın güvenlik duvarı üzerinden iletişim kurmasına izin vermek için programı izin verilen programlar listesine eklemesi yeterlidir. Bir ortak ağ kullanıldığında, Windows Güvenlik Duvarı bilgisayarına yönelik istenmeyen tüm bağlantı girişimlerini engelleyerek sistemin güvenliğini sağlayabilir.

Yönergeler Sonraki adımlar

Yapılandırma

1. Aracıyı indirin ve yükleyin

Aracıyı yüklemek istediğiniz yeri seçin:

Install agent on Azure Windows Virtual Machine

Download the agent on the relevant machine and follow the instructions.  
Azure Windows Sanal makineleri için aracıyı indirin ve yükleyin >

Install agent on non-Azure Windows Machine

2. Windows Güvenlik Duvarı çözümünü yükleyin

Çözümü yükle

İlgili makineyi seçip soldaki panelden **Bağlan** butonuyla işlemi başlatıp çok kısa bir süre beklettikten sonra yükleme işlemi tamamlanacaktır.

The screenshot shows the Azure Sentinel interface. On the left, the 'Sanal makineler' (Virtual Machines) blade is open, displaying a list of VMs with filters applied. The list includes 'vm1' (Bağlı değil, Windows, POC2, westeurope) and 'vm2' (Diğer çalışma alanı, Windows, d3381180-6b78-4222..., POC2, westeurope). On the right, a detailed view of 'vm1' is shown with the following properties:

- Durum: Bağlı değil
- Çalışma Alanı Adı: Yok
- İleti: VM, Loc Analytics'e bağlı değil.

Alarm üretilmesi için yaklaşık olarak 24 saat beklemek gerekebilir.

The screenshot shows the Azure Sentinel Overview page. Key statistics displayed are:

- Olaylar: 66.5K (11.6K)
- Uyarılar: 0
- Olaylar: 0

Under 'DURUMA GÖRE OLAYLAR' (Events by Status), the counts are:

- YENİ (0)
- SÜRÜYOR (0)
- KAPALI (MISKIN POZİTİF) (0)
- KAPALI (HATALI) (0)

The main dashboard features a chart titled 'Zaman içindeki olaylar ve uyarılar' (Events and Alerts over time) showing daily event counts from 18 to 12. To the right, there are three cards: 'Son olaylar' (Recent events) which says 'Veri bulunamadı' (Data not found), 'Veri kaynağı anomalileri' (Data source anomalies) showing a line graph for 'SecurityEvent', and a summary card for 'SECURITYEVENT' with a value of 65K.

## Azure Sentinel Office 365 Entegrasyonu

Microsoft Azure portalına eriştiğten sonra Azure Sentinel' i açıyoruz. **Overview** arayüzünde **Data connectors** sekmesini tıklıyoruz. Office 365 ile entegrasyon yapacağımız için Office 365 connector' ü seçiliyken **Open connector page** i tıklıyoruz.

The screenshot shows the Microsoft Azure Azure Sentinel - Data connectors page. On the left sidebar, under Configuration, 'Data connectors' is highlighted with a red box and a red arrow pointing to it. In the main pane, the 'Office 365' connector is selected, also highlighted with a red box and a red arrow pointing to it. The status bar indicates 'Not connected'.

**Configuration** altında yer alan **Add tenant** i tıklıyoruz ve eklemek istediğimiz tenant i buraya tanımlıyoruz ve **Install solution** i tıklıyoruz.

The screenshot shows the 'Office 365' configuration page. Under the 'Prerequisites' section, there is a note: 'To integrate with Office 365 make sure you have:'. It lists three requirements: 'Workspace: read and write permissions are required.', 'Solutions: read and write permissions are required.', and 'Tenant Permissions: required "Global Admin" or "Security Admin" on the workspace's tenant.' Below this, under the 'Configuration' section, there is a 'Install solution' button. At the bottom of the page, there is a 'TENANT' search bar with a '+ Add tenant' button, which is highlighted with a red box and a red arrow pointing to it.

İşleminim başarılı şekilde tamamlandı.

The screenshot shows a browser window with the URL <https://weurp.asazure.com:4433/OfficeOnboard?workspaceId=2cd0c83-b684-46c8-8bcc-47d3391507ca>. The page displays the message: 'The tenant was successfully on-boarded to the workspace.'

Dikkat ettiyseniz eğer mailbox auditing yapmak istiyorsanız yapmanız gereken ek bazı adımlar olduğunu belirtiyor. Nasıl mailbox auditing yapabileceğinize aşağıdaki linkten ulaşabilirsiniz.

<https://docs.microsoft.com/tr-tr/microsoft-365/compliance/enable-mailbox-auditing>

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu includes 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES' (with 'Resource groups' selected), 'All resources', 'App Services', 'SQL databases', 'Azure Cosmos DB', 'Virtual machines', 'Load balancers', 'Storage accounts', 'Virtual networks', 'Azure Active Directory', 'Security Center', 'Monitor', 'Advisor', 'Cost Management + Billing', 'Help + support', 'Azure Information Protection...', and 'Intune'. The main content area is titled 'Office 365' under 'PREVIEW'. It shows a status of 'Not connected' with a 'Microsoft Provider' icon and a 'LAST LOG RECEIVED' timestamp. A 'Description' section explains the connector provides insight into ongoing user activities. Below it, 'Last data received' shows 100 items. A 'Related content' section lists '3 Workbooks' and '2 Queries'. A 'Data received' chart shows values from 0 to 100. On the right, the 'Configuration' tab is active, with '1. Enable the Office 365 solution on your workspace' and '2. Connect tenants to Azure Sentinel' steps. Under 'Install solution', there's a 'Save' button. Under 'Connect tenants to Azure Sentinel', there's a 'Search' bar and a table with a row for '7ccb9027-dff7-4579-b9e1-56201c710c71' with checkboxes for 'SharePoint' and 'Exchange' both checked. A red box highlights this row.

Loglarının gelip gelmediğini kontrol etmek için **Workbooks** sekmesini tıklıyorum. Office 365 I seçtiğten sonra **View template** i tıklıyorum.

The screenshot shows the 'Azure Sentinel - Workbooks' page. The left sidebar has 'General', 'Overview', 'Logs', 'News & guides', 'Threat management', 'Incidents', 'Workbooks' (which is selected and highlighted in blue), 'Hunting', 'Notebooks', 'Configuration', 'Data connectors', 'Analytics', 'Playbooks', 'Community', and 'Workspace settings'. The main area shows '2 Saved workbooks', '31 Templates', and '0 Updates'. Under 'My workbooks', there are several entries: 'Microsoft Web Application Firewall (WAF) - overview' (highlighted with a red arrow), 'Office 365' (highlighted with a red arrow), 'Palo Alto Network Threat', 'Palo Alto overview', 'SharePoint & OneDrive', and 'Threat Intelligence'. To the right, there's a preview of the 'Office 365' workbook with sections for 'Required data types' (OfficeActivity), 'Data sources' (Office365), and a preview dashboard. A red arrow points to the 'View template' button at the bottom of the preview pane.

Loglarının geldiğini gözlemliyorum. Tekrar hatırlatmakta fayda var şuan toplanan loglarım içerisinde mailbox auditing mevcut değil.

Microsoft Azure

Home > Azure Sentinel workspaces > Azure Sentinel - Workbooks > Office 365

Office 365

hd-loganalytics

Refresh

TimeRange: Last 90 days | Workload: All | UserType: All

## General overview

Office activity, by workload

Activity, by workload

Activity, by type

Exchange 14 | SharePoint 1

Microsoft Azure

Home > Azure Sentinel workspaces > Azure Sentinel - Data connectors > Office 365 > Workbooks > Exchange Online

Exchange Online

hd-loganalytics

Refresh

Activities, by time

User type activities

User activities

Name	Type	Operation Count	Trend
NT AUTHORITY\SYSTEM (Microsoft.Exchange.ServicesHost)	Userid	98	↑
Set-Mailbox	Operation	49	↑
Set-TransportConfig	Operation	21	↑
Add-MailboxPermission	Operation	7	↔
Enable-AddressListPaging	Operation	7	↔
Set-OverseasMailboxPolicy	Operation	7	↔
Set-TenantObjectVersion	Operation	7	↔

Admin activities

The screenshot shows the Microsoft Azure Azure Sentinel Workbooks interface. The left sidebar shows 'Office 365' selected under 'hd-loganalytics'. The main area displays a table of logs with columns: TimeGenerated, RecordType, Operation, UserKey, OfficeWorkload, UserId, and Parameters. The table lists several Exchange-related events from September 26, 2019, such as 'ExchangeAd... Set-TransportConfig' and 'ExchangeAd... Set-Mailbox'. The top navigation bar includes a search bar, refresh button, and user info.

Aynı şekilde Sharepoint & OneDrive Workbooksunu seçip View template i tıklıyorum. Tenant eklerken Sharepoint kutucuğu da seçili olduğundan Sharepoint ile alakalı ilgili logları da toplayabiliyorum.

The screenshot shows the Microsoft Azure Azure Sentinel Workbooks interface. The left sidebar shows 'Sharepoint & OneDrive' selected under 'hd-logAnalytics'. The main area displays a list of workbooks: 'Palo Alto Network Threat' (PALO ALTO NETWORKS), 'Palo Alto overview' (MICROSOFT), 'SharePoint & OneDrive' (MICROSOFT, highlighted with a red arrow), 'Threat Intelligence' (MICROSOFT), 'VM insights' (MICROSOFT), and 'Zscaler Firewall' (ZSCALER). On the right, there's a preview pane with a chart and text about SharePoint and OneDrive analysis. A red arrow points to the 'View template' button at the bottom right of the preview pane.

The screenshot shows the Microsoft Azure SharePoint & OneDrive dashboard. At the top, there are filters for TimeRange (Last 30 days), Operations (All), and Users (All). The General overview section displays counts for SharePoint (1) and All (1). The Operation summary section shows a table of operations:

Name	Type	Operations Count	Trend
SearchQueryPerformed	Operation	1	
hasan.dimdik@hdimdik.onmicrosoft.com	UserId	1	

The screenshot shows the Microsoft Azure SharePoint & OneDrive dashboard. The left sidebar includes a 'Sites' section. The main area displays a donut chart with a value of 1 and an IP address count of 1 (40.127.200.177). The 'Sites details' section is visible on the left, and the 'IP addresses details' section is on the right, showing a table of IP address details:

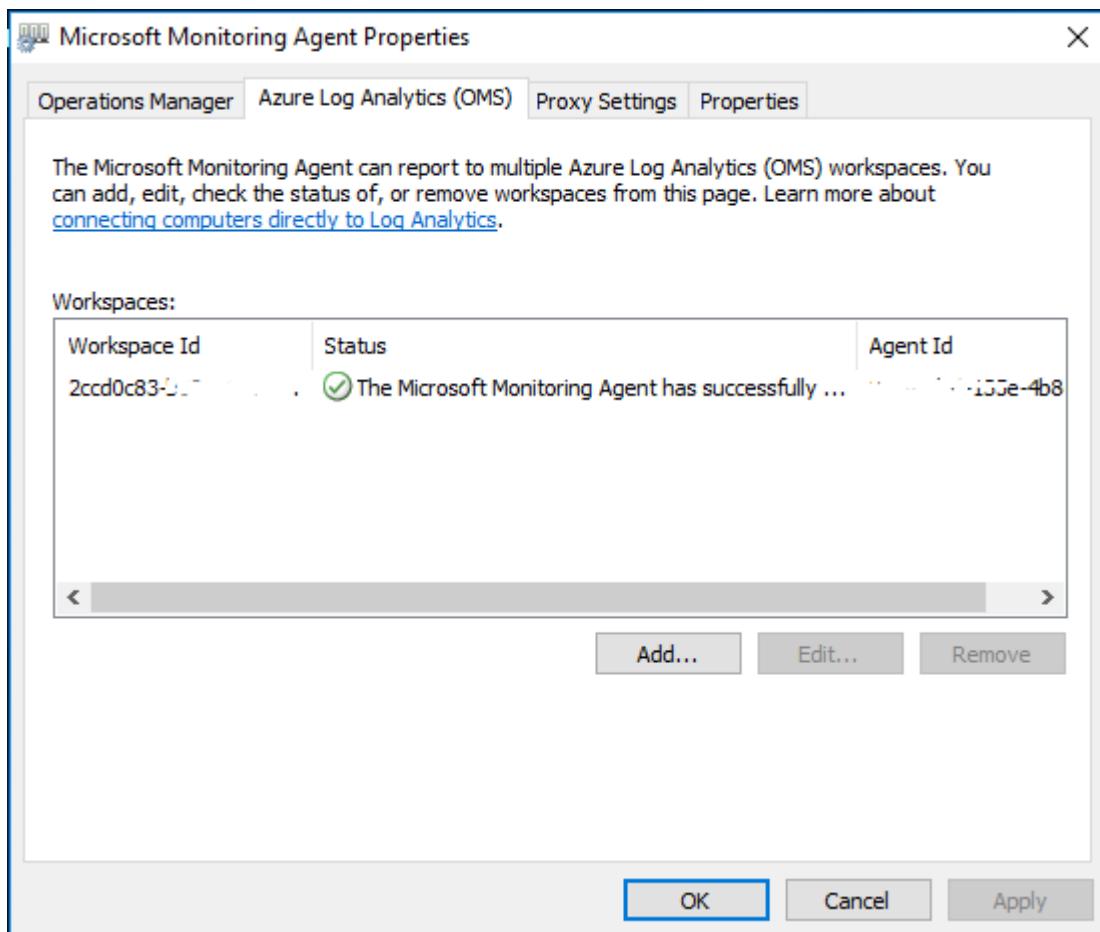
ClientIP	Userid	Operation	TimeGenerated
40.127.200.177	hasan.dimdik@hdimdik.onmicrosoft.com	SearchQueryPerform...	Saturday, September 21, 2019, 4...

## Azure Sentinel Insecure Protocols Dashboard Entegrasyonu

Şirketlerin özellikle migration projeleri yaparken karşılaştığı en büyük sorunlardan bir tanesi ortamda kullanılan ciphers, protocols, NTLMv1/v2 vb tespit edilememesi diğer sorun ise gerçekte ihtiyaç olup olmadığından dahi bilinmemesidir. Bu durum iki sorunu doğurmaktadır. Migration aşamasında gri alanın kalması çünkü tam olarak ortama ve gereksinimlerimize hakim değiliz, diğer sorun ise elbette güvenlik. Yapıımızda sıkıştırma yapmak istediğimizde zayıf halkaları biliyor olmamız ve bu alanları iyileştirmemiz gerekmektedir. Aksi takdirde bu durum iş sürekliliğini etkileyecektir. Tam da bu noktada ilgili çözüm imdadımıza yetişmektedir.

Yapilandırmamıza başlamak için ilk olarak Microsoft Monitoring aracını yapımız içerisindeki Domain Controller lara yükliyoruz. Elbette canlı ortamdaki Domain Controller'ların internet çıkışının olmayacağı ve büyük ihtimalle Proxy ortam içerisinde olacaktır, bu durumda yükleme adımları biraz

değişiklik göstermektedir. Demo yapımda tek DC ve direk internet bağlantım olduğu için herhangi Proxy yapılandırması yapmadım veya Proxy Gateway yapılandırmadım.



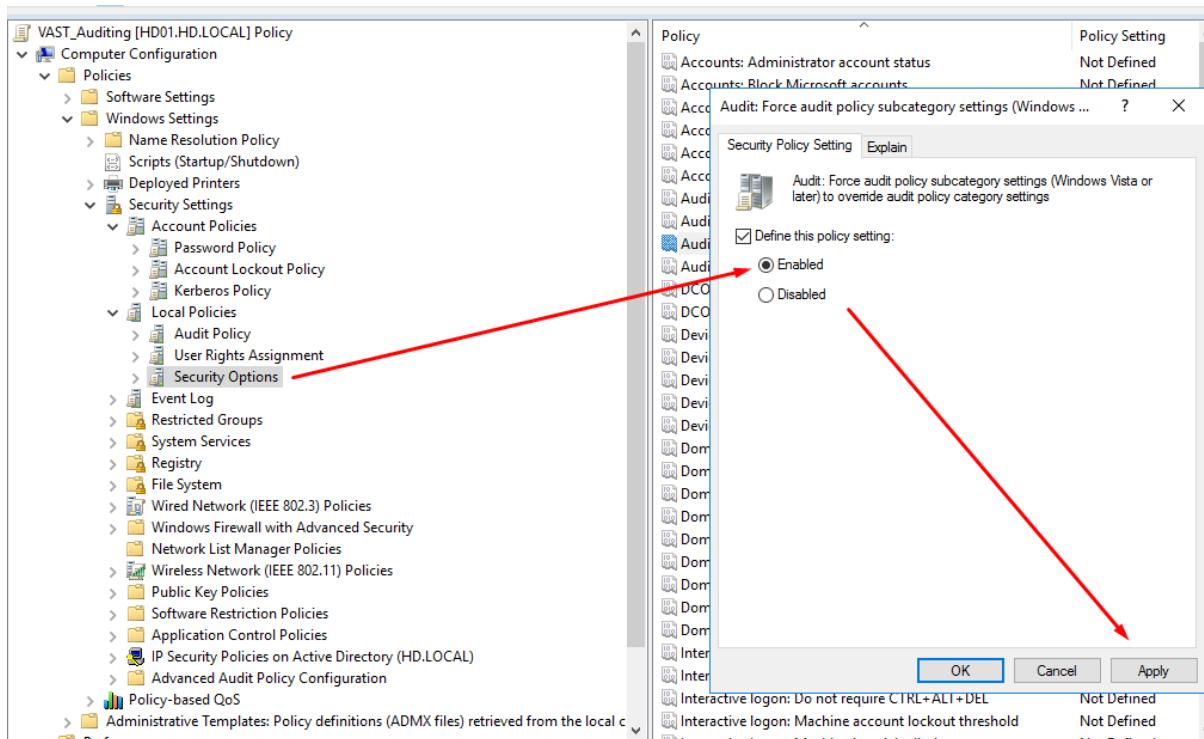
İlgili ajanı yükledikten sonra portalda yansidiğini görüyorum.

```
Heartbeat
| where OSType == 'Windows'
| summarize arg_max(TimeGenerated, *) by SourceComputerId
| top 50000 by Computer asc
| render table
```

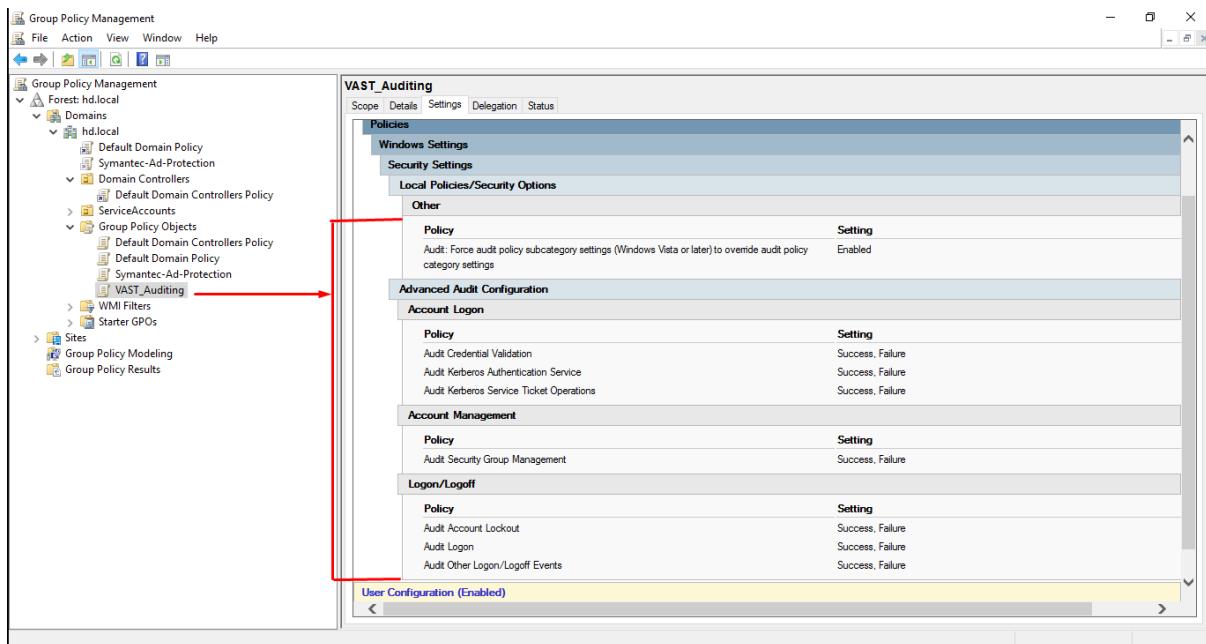
Monitoring ajanlarını yükledikten sonra Auditing ayarlarını yapılandırmamız gerekmektedir. Auditing yapılandırırken dikkat etmemiz gereken bazı trik noktaları bulunmaktadır. Özellikle sizin环境中 Basic Logging kullanıyorsanız Advanced Auditing yapılandırdığınızda Basic Auditing duracaktır.

## Active Directory Auditing Yapılandırma

Auditing yapılandırmam için yeni bir policy oluşturdum ve **Auditing: Force audit policy subcategory settings(Windows Vista or later) to override audit policy category settings** Enable kutucuğunu tıkladıktan sonra apply butonunu tıklıyoruz. Yukarıda bahsettiğim gibi bu policy uygulanırken kesinlikle ortamdaki Auditing yapılandırması bilinmelidir.



İkinci adımımız ise **Advanced Audit Policy** yapılandırması olacak. Yapılandırılmış olduğunuz kuralın uygulanıp uygulanmadığını görmek için **auditpol /get /category:\*** komutunu kullanabilirsiniz.



Kuralı uyguladıktan sonra Domain Controller Security Event Loglarında aşağıdaki logların üretildiğini kontrol etmelisiniz.

- 4776 - Non-Kerberos Authentication
- 4771 - Kerberos Pre-auth Failure
- 4740 – Account Lockout
- 4624 - Successful Logon
- 4625 - Failed Logon
- 4768 - TGT request
- 4769 - TGS request
- 4627 – Group membership change

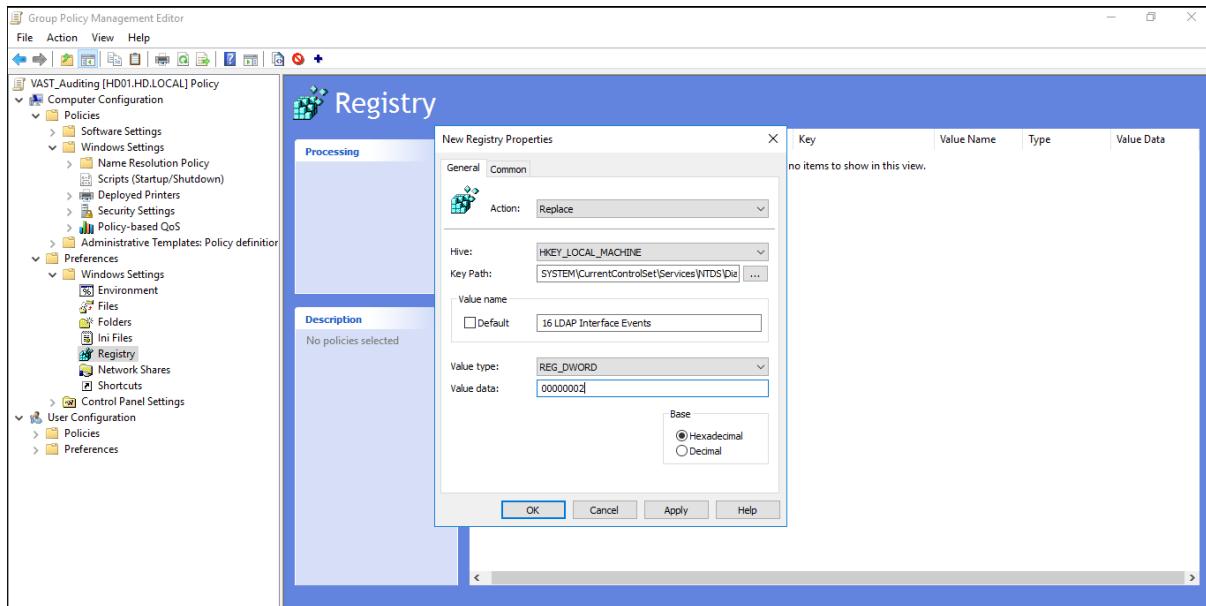
#### Logging of unsigned LDAP Binds Yapılandırması

Yapımız içerisindeki Insecure LDAP bağlantılarını izleyebilmek için DC ler üzerinde yer alan bir registry kaydını değiştireceğiz ve bunu gpo ile tüm DC lere uygulayacağız. Amacımız EventID 2889'un olmasını sağlamak olacak. İlgili event id nedir diye soracaksanız aşağıdaki linkten bilgi sahibi olabilirsiniz.

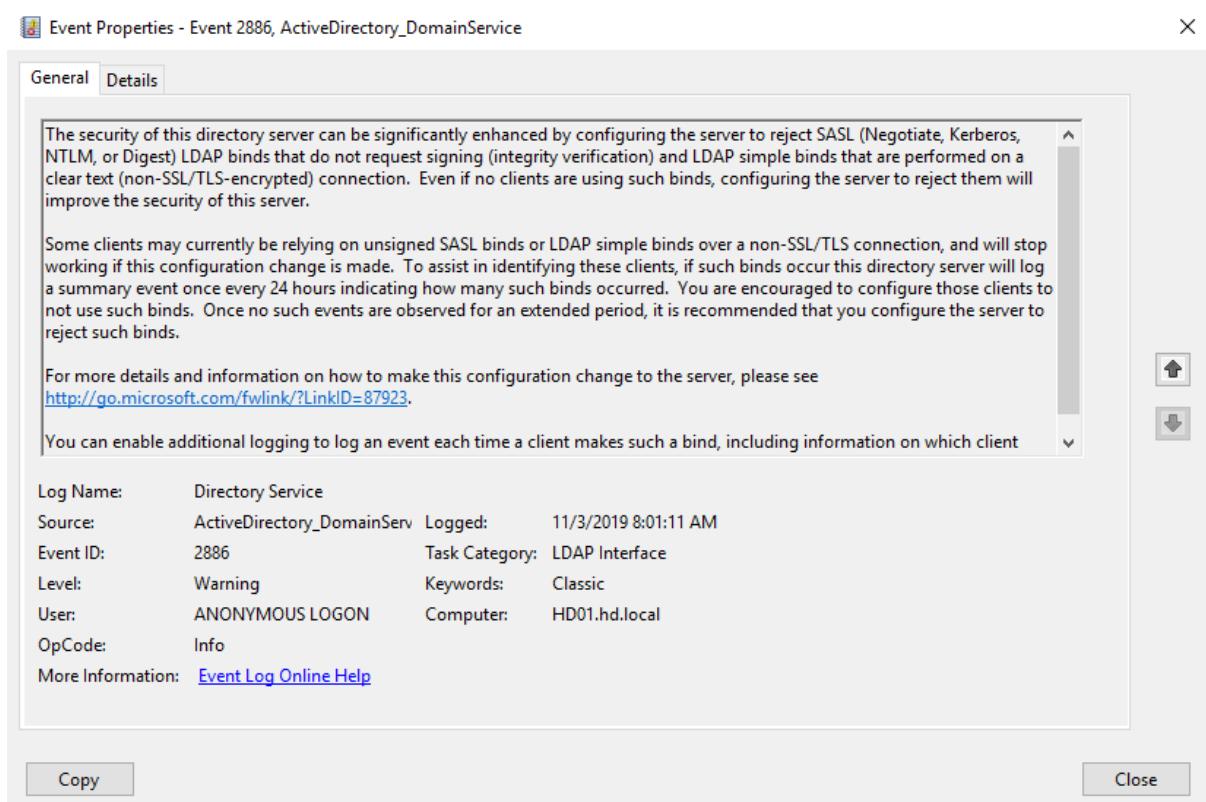
<https://blogs.technet.microsoft.com/russellt/2016/01/13/identifying-clear-text-ldap-binds-to-your-dcs/>

İlgili logu üretebilmek için aşağıdaki şekilde registry dosyasında değişiklik yapıyoruz.

```
Reg Add HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics  
/v "16 LDAP Interface Events" /t REG_DWORD /d 2
```

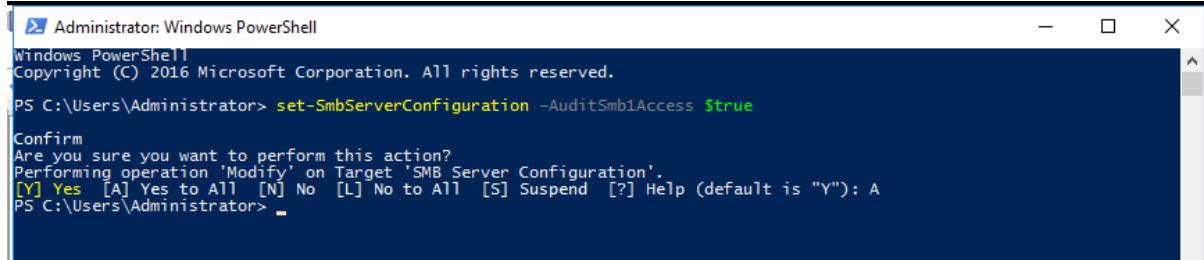


Yapilandırmamdan sonra kontrol ettiğimde DC üzerinde ilgili logun üretildiğini görüyorum.



## SMB1 Auditing

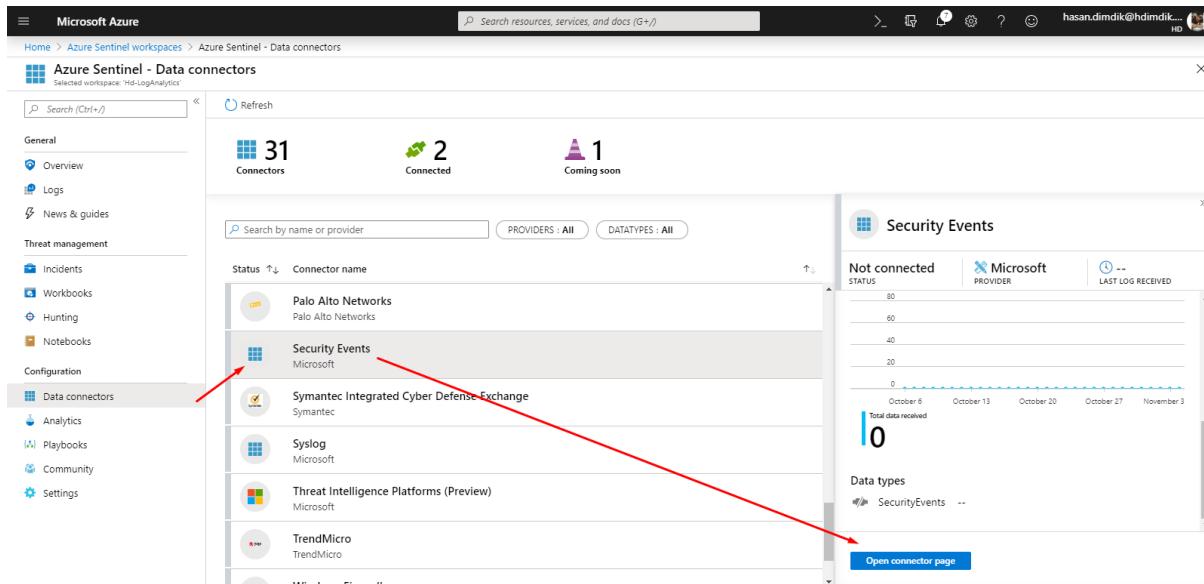
SMBv1 auditing adımını yapılandırmamız için sunucularımızın işletim sistemi seviyesi en düşük Windows Server 2012 R2 olmalıdır. Yani siz Windows Server 2008 R2 ise bu adımı es geçebilirsiniz.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> set-SmbServerConfiguration -AuditSmb1Access $true
Confirm
Are you sure you want to perform this action?
Performing operation 'Modify' on Target 'SMB Server Configuration'.
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): A
PS C:\Users\Administrator>
```

Uzun bir yapılandırmadan sonra tüm ön gereksinimleri artık karşılamış oluyoruz ve Azure Sentinel Insecure Protocols yapılandırmasına geçebiliriz. Insecure Protocols yapılandırmak için Data connectors ü tıklıyoruz. **Connector** seçenekleri arasından **Security Event'** i seçip **Open Connector page** i tıklıyoruz.



Microsoft Azure

Home > Azure Sentinel workspaces > Azure Sentinel - Data connectors

Azure Sentinel - Data connectors

Selected workspace: Hd-LogAnalytics

Search resources, services, and docs (G+/-)

hasan.dimdik@hdimdik... HD

General

Overview

Logs

News & guides

Threat management

Incidents

Workbooks

Hunting

Notebooks

Configuration

Data connectors

Analytics

Playbooks

Community

Settings

Refresh

31 Connectors

2 Connected

1 Coming soon

Search by name or provider

PROVIDERS : All

DATATYPES : All

Status ↑ Connector name

Palo Alto Networks

Security Events

Symantec Integrated Cyber Defense - Exchange

Syslog

Threat Intelligence Platforms (Preview)

TrendMicro

Windows Firewall

Security Events

Not connected

Microsoft PROVIDER

LAST LOG RECEIVED

80  
60  
40  
20  
0

October 6 October 13 October 20 October 27 November 3

Total data received: 0

Data types

SecurityEvents --

Open connector page

## Security Events

The screenshot shows the 'Security Events' configuration page in the Azure portal. The status is 'Not connected'. In the 'Configuration' section, the 'All Events' radio button is selected. A red arrow points to the 'Apply Changes' button.

Kısa bir süre sonra connector'un yeşile döndüğünü görüyoruz.

The screenshot shows the 'Security Events' configuration page in the Azure portal after changes were applied. The status is now 'Connected'. The 'Selected data point' is highlighted with a red box, showing 'SecurityEvents 11/04/19, 10:35 PM'.

Log Analytics içerisinde aşağıdaki komutu çalıştırarak logların yansıyıp yansımadığını görebilirsiniz.

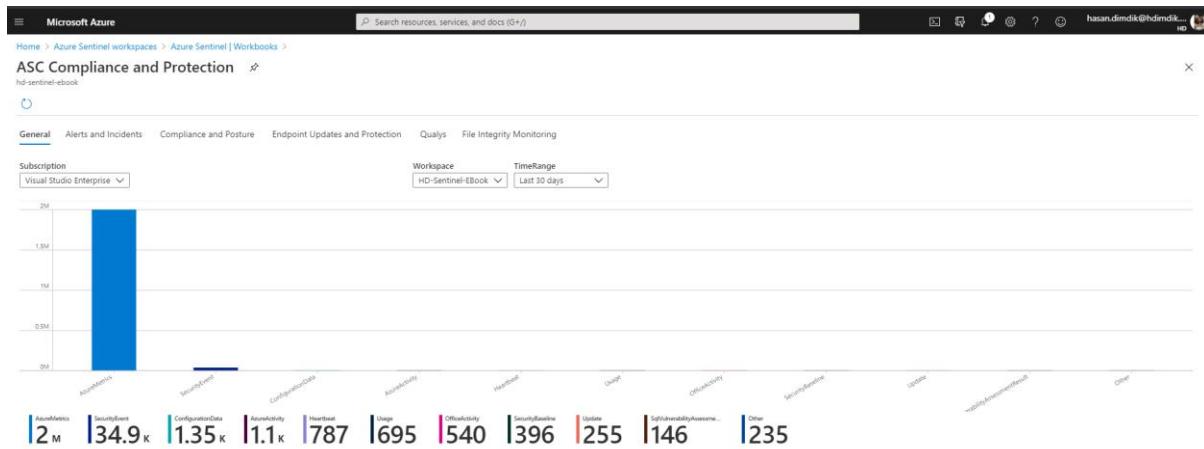
```
SecurityEvent  
| sort by TimeGenerated
```

**Workbooks** u tıklıyoruz ve hazır template ler içerisinde **Insecure Protocols** ü seçip **View Template** butonunu tıklıyoruz.

## ASC Compliance and Protection

The screenshot shows the Azure Sentinel Workbooks page. On the left, there's a sidebar with navigation links like General, Threat management, Configuration, and Settings. The main area displays a list of workbooks under 'My workbooks'. One workbook titled 'ASC Compliance and Protection' is highlighted with a red arrow pointing to it. This workbook is described as being from the 'AZURE SENTINEL COMMUNITY'. It has a preview pane showing a dashboard with various metrics and a 'View template' button. A callout box on the right lists 'Required data types:' including SecurityAlert, ProtectionStatus, SecurityRecommendation, SecurityBaseline, ConfigurationSummary, Update, and ConfigurationChange. Another callout box below it lists 'Relevant data connectors:' including AzureSecurityCenter.

Portala son zamanlarda eklenen ASC Compliance and Protection' a deðinmeden geçemeyeceðim. Bildiðiniz üzere Azure Security Center üzerinde oluþan alarmları veya olayları Azure Sentinel' e aktarabiliyoruz. Buradaki asıl amaçlardan birisi iki ürün arasındaki ilişkisi güçlendirmek, ekiplerin araştırma yapmalarını kolaylaştırmak. Bu noktada ilgili workbook bize son derece faydalı bazı özellikler kazandırmaktadır. Ilgili workbook u kullanılmak için yukarıda veri tiplerinin saðlıklı şekilde alınabiliyor olması gerekmektedir.



Alerts and Incidents bize hangi sensörlerden alarmların toplandığını ve kritiklik seviyelerini göstermektedir. AlertType burada SOC analizcilerinin en fazla takip edeceği sekmelerden biri olacaktır.

Microsoft Azure

Home > Azure Sentinel workspaces > Azure Sentinel | Workbooks >

### ASC Compliance and Protection

hd-sentinel-ebook

General Alerts and Incidents Compliance and Posture Endpoint Updates and Protection Qualys File Integrity Monitoring

Subscription Visual Studio Enterprise Workspace HD-Sentinel-EBook TimeRange Last 30 days

Alerts by Severity

43 Medium 25 Low 13 Informational 5

43 MDRP 35 Detection 4 MCAS 3 A3 Scheduled Alerts 1

ProductSelection SeveritySelect All All

Select All

Resources

	name	SystemAlertId	ResourceId	AlertType	StartTime	EndTime	RemediateState
Azure Security Center	20d6851f-b621-1555-e114-c4d31b1a2c64			VM.Windows_SystemEventLogCleared	5/27/2020, 8:47:43 PM	5/27/2020, 8:47:43 PM	[*, Validate]
Azure Sentinel	47643b30-2c03-6bd9-bc67-3fc0479c3b14			VM.Windows_SecurityEventLogCleared	5/27/2020, 8:47:33 PM	5/27/2020, 8:47:33 PM	[*, Validate]
Microsoft Cloud App Security	2516117027460709071_8df22251-4e30-4635-b927-5148...			VM.Windows_SystemEventLogCleared	5/27/2020, 8:47:33 PM	5/27/2020, 8:47:33 PM	[*, Validate]
Microsoft Defender Advanced Threat Protection	2518117027381958310_a16bd4bb-5ba0-4d66-a1cd-0d6...			VM.Windows_SystemEventLogCleared	5/27/2020, 8:47:43 PM	5/27/2020, 8:47:43 PM	[*, Validate]
Informational	Microsoft Azure Sentinel	30270077-6639-7aae-67a2-161256539995			7f66cf90-9527-4b63-140259a6be2_08862353-303...	5/27/2020, 8:46:41 PM	5/27/2020, 8:51:41 PM
Medium	Microsoft Microsoft Defender Advanced Threat Protection	579b8402-5c89-0405-2e3d-ac2d74e34de9			7f1c3609-a3ff-4ce2-995b-c01770161d68	5/13/2020, 1:22:16 PM	5/13/2020, 1:22:16 PM
Medium	Microsoft Microsoft Azure Sentinel	30270077-6639-7aae-67a2-161256539995			7f66cf90-9527-4b63-140259a6be2_08862353-303...	5/27/2020, 8:46:41 PM	5/27/2020, 8:51:41 PM

Compliance and Posture sekmesinde şirketinizin tabi olduğu belirli sertifikasyonlar veya süreçler var ise hangi maddelerden geçip hangilerinden geçemediğimizi görebiliyoruz. Bu durum da bize şirketinizin ilgili sertifiaksiyona göre duruşunu göstermiş oluyor.

Microsoft Azure

Home > Azure Sentinel workspaces > Azure Sentinel | Workbooks >

### ASC Compliance and Protection

hd-sentinel-ebook

General Alerts and Incidents Compliance and Posture Endpoint Updates and Protection Qualys File Integrity Monitoring

Subscription Visual Studio Enterprise Workspace HD-Sentinel-EBook TimeRange Last 90 days

Current Compliance Details

name	passedControls	failedControls	unsupportedControls	skippedControls	subscriptionId
Azure-CIS-1.1.0-(New)	52	10	49	0	ce50118a-11de-4ef4-9236-d2f6e314bfde
PCI-DSS-3.2.1	40	5	197	0	ce50118a-11de-4ef4-9236-d2f6e314bfde
Azure-CIS-1.1.0	24	0	87	0	ce50118a-11de-4ef4-9236-d2f6e314bfde
ISO-27001	17	4	93	0	ce50118a-11de-4ef4-9236-d2f6e314bfde
SOC-TSP	12	1	24	0	ce50118a-11de-4ef4-9236-d2f6e314bfde

Örneğin ISO-27001' e göre iyileştirmem gereken maddeleri görebiliyorum.

Microsoft Azure

Home > Azure Sentinel workspaces > Azure Sentinel | Workbooks >

### ASC Compliance and Protection

hd-sentinel-ebook

General Alerts and Incidents Compliance and Posture Endpoint Updates and Protection Qualys File Integrity Monitoring

Subscription Visual Studio Enterprise Workspace HD-Sentinel-EBook TimeRange Last 90 days

SelectCompliance selectState ISO-27001 Failed

ControlName name Status description

ControlName	name	Status	description
ISO-27001	A11.2.2	Failed	Supporting utilities
ISO-27001	A18.1.3	Failed	Protection of records
ISO-27001	A9.4.2	Failed	Secure log-on procedures
ISO-27001	A14.2.1	Failed	Secure development policy
ISO-27001	A11.2.5	Failed	Removal of assets
ISO-27001	A11.2.7	Failed	Secure disposal or re-use of equipment
ISO-27001	A6.2.2	Failed	Labelling of information
ISO-27001	A11.1.1	Failed	Physical security perimeter
ISO-27001	A14.2.7	Failed	Outsourced development
ISO-27001	A12.2.1	Failed	Controls against malware
ISO-27001	A14.1.3	Failed	Protecting application services transactions

Endpoint Protection Status kısmında antivirüs ajanlarının durumunu ve algılanan tehdit veya zararlı varsa buradan takip edebiliyoruz. Aynı şekilde en fazla savunmasız sunucu/istemcilerimizi gözlemleyebiliyoruz.

The screenshot shows the ASC Compliance and Protection interface. The top navigation bar includes General, Alerts and Incidents, Compliance and Posture, Endpoint Updates and Protection (which is selected), Qualys, and File Integrity Monitoring. Below the navigation is a search bar and filter options for Subscription (Visual Studio Enterprise) and Workspace (HD-Sentinel-EBook) with a TimeRange of 'Last 30 days'. The main area displays two tables: 'Endpoint Protection Status' and 'Threats Over Last 'Last 30 days''. The 'Endpoint Protection Status' table lists resources (DESKTOP-4MAV7D4.hd.local, SCCM-SQL.hd.local, DC01.hd.local, win2008-member.hd.local) with their protection status (Protected or No Anti-Malware Tool was detected) and threat status (No threats detected or Real time protection). The 'Threats Over Last 'Last 30 days'' table lists events with columns for Time Generated, Resource, Action Taken, Event Summary, Malicious Artifact, and Details.

Update edilmesi gereken kaynaklarımızı KB isimleri ile görebiliyoruz, aynı şekilde üçüncü parti yazılımlarıda takip edebiliyoruz.

The screenshot shows the Microsoft Azure portal. The top navigation bar includes Microsoft Azure, Search resources, services, and docs (Q+), and a user profile (hasan.udmuk@hdindik.hk). Below the navigation is a breadcrumb trail: ie > Azure Sentinel workspaces > Azure Sentinel | Workbooks > ASC Compliance and Protection. The main area displays two tables: 'Resource Security Baselines Summary' and 'Updates Needed for Resource'. The 'Resource Security Baselines Summary' table lists resources (win2008-member.hd.local, SCCM-SQL.hd.local, DESKTOP-4MAV7D4.hd.local, DC01.hd.local) with their number of logs. The 'Updates Needed for Resource' table lists updates for specific resources (SCCM-SQL.hd.local) with columns for Time Generated, Product, Classification, Title, KBID, Resource, and Update Status.

Azure Security Center'ı standart tier olarak kullanıyorsanız Qualys bize yapımızda açıkkık var ise ASC içerisinde raporlamaktadır.

File Intergrity Monitor sekmesinde sunucularımız üzerindeki registry değişikliği, sizin için önemli olan ve Azure Security Center üzerinde belirttiğiniz bir dosya veya dizin varsa burada olay olarak görebiliyoruz. Aynı şekilde Linux tarafı da desteklenmetedir. Örneğin /bin/passwd monitor etmek istiyorsanız bu da mümkün. Son olarak ise Windows Servislerindeki değişiklikleri de gözlemleyebiliyoruz.

The screenshot shows the Microsoft Azure File Integrity Monitoring interface. At the top, there are tabs for General, Alerts and Incidents, Compliance and Posture, Endpoint Updates and Protection, Qualys, and File Integrity Monitoring. The File Integrity Monitoring tab is selected. Below the tabs, there are dropdown menus for Subscription (Visual Studio Enterprise) and Workspace (HD-Sentinel-Ebook). A TimeRange dropdown shows 'Last 90 days'. The main area is titled 'Events Per Resource within "Last 90 days"' and contains a table with columns: Resource, Action, Area, Count, ChangeCategory, ConfigChangeType, RegistryKey, ValueName, and FileSystemPath. The table lists various registry changes across different resources like SCCM-SQL.hd.local and DC01.hd.local.

Kaynak : <https://techcommunity.microsoft.com/t5/azure-sentinel/compliance-reporting-for-azure/ba-p/1259574>

## Workbooks | Templates & My Workbooks Farkı Nedir ?

Yeni başlayanların en çok sorduğu sorulardan biri olduğu için bu bölümde yer vermek istedim.

The screenshot shows the Microsoft Azure Workbooks interface. The left sidebar includes sections for Overview, Logs, News & guides, Threat management (Incidents, Workbooks, Hunting, Notebooks), Configuration (Data connectors, Analytics, Playbooks, Community, Settings), and a workspace dropdown for 'hd-sentinel-ebook'. The main area has tabs for 'My workbooks' and 'Templates'. A search bar is above the template list. The 'Templates' tab is selected, showing a list of available workbooks: AI Vectra Detect (VECTRA AI), ASC Compliance and Protection (AZURE SENTINEL COMMUNITY), AWS Network Activities (MICROSOFT), AWS User Activities (MICROSOFT), Azure Activity (MICROSOFT), Azure AD Audit logs (MICROSOFT), Azure AD Audit, Activity and Sign-in logs (AZURE SENTINEL COMMUNITY), Azure AD Sign-in logs (MICROSOFT), Azure Firewall (MICROSOFT), and Azure Information Protection - Usage Report (MICROSOFT). To the right, a preview pane for the 'ASC Compliance and Protection' template is shown, along with sections for Required data types and Relevant data connectors.

Örnek üzerinden farklılığı açıklamak daha mantıklı olacaktır. Örneğim için ASC Compliance and Protection Wokrbook' unu seçiyorum. View template seçip ilgili Dashboard' u açtığında editlenemediğini görüyorum.

AlertSeverity	VendorName	ProductName	SystemAlertId	ResourceId	AlertType	StartTime	EndTime	RemediationSteps
Medium	Microsoft	Microsoft Defender Advanced Threat Protection	dbc83945-5bd7-8694-9cd7-3fe0e95d9ffcc	77632844-9985-4405-9d5b-8e1af724a1fd		6/25/2020, 10:32:55 PM	6/25/2020, 10:32:55 PM	[...]
Medium	Microsoft	Microsoft Defender Advanced Threat Protection	07488b3b-78b0-d1fb-9951-29c38177a296	376178de-428e-4ea8-894f-ddca14f04118		6/25/2020, 10:32:55 PM	6/25/2020, 10:32:55 PM	[...]
Medium	Microsoft	Microsoft Defender Advanced Threat Protection	07488b3b-78b0-d1fb-9951-29c38177a296	376178de-428e-4ea8-894f-ddca14f04118		6/25/2020, 10:32:47 PM	6/25/2020, 10:32:47 PM	[...]
Medium	Microsoft	Microsoft Defender Advanced Threat Protection	07488b3b-78b0-d1fb-9951-29c38177a296	376178de-428e-4ea8-894f-ddca14f04118		6/25/2020, 10:34:05 PM	6/25/2020, 10:34:05 PM	[...]

Aynı workspace i bu sefer save diyerek kaydedelim ve ilgili workbook' u kaydedeceğimiz lokasyonu seçelim.

Kaydetmiş olduğum Workbook' u artık My workbooks altındada görüyoruz. Şuana kadar yazım içerisinde template seçerek ilerlemiştim. Şimdi ise My workbooks içerisinde View saved workbook u seçiyorum. Aynı kutucuğun hemen yanında yer alan ise yine sizi template e götürecektr.

The screenshot shows the Microsoft Azure Azure Sentinel Workbooks interface. On the left, there's a navigation sidebar with links like General, Overview, Logs, News & guides, Threat management, Incidents, Workbooks (which is selected and highlighted in blue), Hunting, Notebooks, Configuration, and Data connectors. The main area has tabs for 'My workbooks' (selected) and 'Templates'. A search bar says 'Search workbooks'. Below is a list of workbooks: 'ASC Compliance and Protection' (Azure Sentinel Community), 'Identity & Access' (Microsoft), 'Insecure Protocols' (Microsoft), 'Microsoft Cloud App Security - discovery logs' (Microsoft), and 'Office 365' (Microsoft). To the right, there's a detailed description of the 'ASC Compliance and Protection' workbook, listing required data types (SecurityAlert, ProtectionStatus, SecurityRecommendation, SecurityBaseline, SecurityBaselineSummary, Update, ConfigurationChange) and relevant data connectors (AzureSecurityCenter).

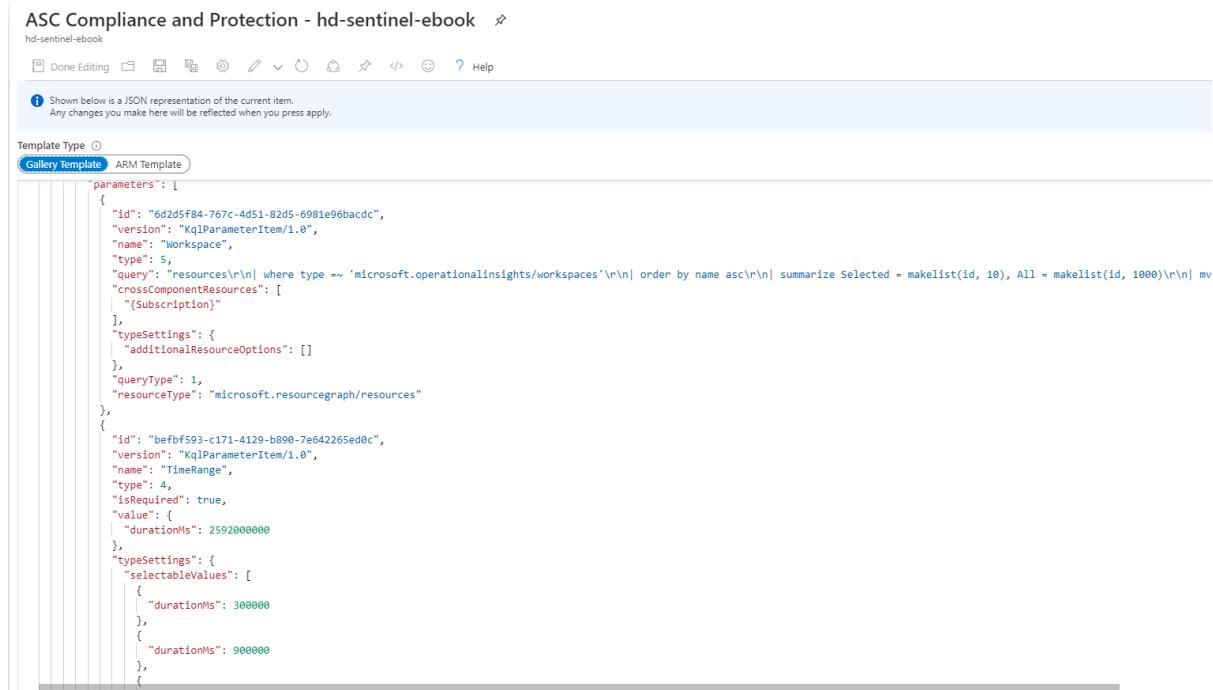
Workbook u açtığımda ise artık editlenebilir olduğunu gözlemliyorum, çünkü bu workbook artık bana ait. İstediğim şekilde değişiklik yapabilirim.

The screenshot shows the 'ASC Compliance and Protection' workbook in edit mode. At the top, there are tabs for General, Alerts and Incidents, Compliance and Posture, Endpoint Updates and Protection, Qualys, and File Integrity Monitoring. The General tab is selected. Below are filter controls for DefaultSubscription\_Id, Subscription (Visual Studio Enterprise), Workspace (HD-Sentinel-EBook), and TimeRange (Last 30 days). The main area features a bar chart with categories: AzureMetrics (approx. 300K), SecurityEvent (approx. 20K), ConfigurationData (approx. 10K), and others (0K). The x-axis labels are: AzureMetrics, SecurityEvent, ConfigurationData, AzureActivity, Heartbeat, OfficeActivity, Update, Usage, Dynamics365Activity, Event, and Other. There are 'Edit' buttons for each bar.

Örneğin, Alerts an Incidents' i türkçe olarak kullanmak istersek aşağıdaki adımları izleyerek gerekli değişiklikleri yapabiliriz.

The screenshot shows the 'Editing links item: links - 9' configuration screen. It lists items under 'Update Links': General, Alarmlar ve Olaylar (highlighted with a red box), Compliance and Posture, and Endpoint Updates and Protection. Each item has settings for Action (Set a parameter value, Tab), Value (Tab), Setting (General, Alerts, Compliance, EP), and Context Blade? (checkbox). At the bottom, there are buttons for Done Editing, Add, Move, Clone, and Remove. A red arrow points to the 'Alarmlar ve Olaylar' item.

Daha detaylı değişiklikleri ise Advanced Editor den yararlanarak yapabiliyoruz.



The screenshot shows the Azure Sentinel Advanced Editor interface. At the top, it displays the title "ASC Compliance and Protection - hd-sentinel-ebook" and the file name "hd-sentinel-ebook". Below the title is a toolbar with various icons for editing, saving, and help. A message bar indicates that the shown content is a JSON representation of the current item, with changes reflected upon apply. The main area is titled "Template Type" and shows two options: "Gallery Template" (selected) and "ARM Template". The JSON code below defines parameters for a log query:

```
parameters": [ { "id": "6d2d5f84-767c-4d51-82d5-6981e96bacdc", "version": "KqlParameterItem/1.0", "name": "Workspace", "type": 5, "query": "resources\r\n| where type ~ 'microsoft.operationalinsights/workspaces'\r\n| order by name asc\r\n| summarize Selected = makelist(id, 10), All = makelist(id, 1000)\r\n| mv", "crossComponentResources": [ "Subscription" ], "typeSettings": { "additionalResourceOptions": [] }, "queryType": 1, "resourceType": "microsoft.resourcegraph/resources" }, { "id": "befbf593-c171-4129-b890-7e642265ed0c", "version": "KqlParameterItem/1.0", "name": "TimeRange", "type": 4, "isRequired": true, "value": { "durationMs": 2592000000 }, "typeSettings": { "selectableValues": [ { "durationMs": 300000 }, { "durationMs": 900000 } ] } }
```

## Analytics & Incidents

Veri kaynaklarınızı Sentinel'e bağladınız peki ya sonra?

Bunu örnekleyle size anlatayım, bu sefer Azure AD üzerinden gidelim. Yapınız büyük olabilir onlarca server, client ve user olabilir her birinden yüzlerce log geliyor. Bunları takip etmek izlemek neredeyse imkânsız.

Bir sisteme sizmanın çeşitli yolları var bunlardan biri ise parolayı ele geçirmek. Peki birileri bir kullanıcının parolasını sürekli deniyorsa? Bunların logları elbette oluşuyor ama nasıl takip edeceğiz?

Azure Sentinel'de Analiz kısmında hazır şablonlar mevcut ve her geçen gün bir yenisini ekleniyor.

Mesela,

**Distributed Password Cracking attempts** şablonunun altında aşağıdaki 3 evet id'yi içeriyor. Oldukça iyi bir diğer güzel kısım ise düzenleyebiliyorsunuz mesela ek olarak 50057'yi de ekleyebiliriz.

["50053: Account is locked because the user tried to sign in too many times with an incorrect user ID or password.](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-sign-ins-error-codes)

[50055: Invalid password, entered expired password.](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-sign-ins-error-codes)

[50126: Invalid username or password, or invalid on-premises username or password.](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-sign-ins-error-codes)

[50057 User account is disabled. The account has been disabled by an administrator.](https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-sign-ins-error-codes)"

Diğerleri için: <https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-sign-ins-error-codes>

### Şablonları Kullanarak Kural Oluşturma

Bir önceki ekrandaki “Kural Oluşturma” butonu ile başlıyoruz 4 ekran var ve her şey hazır geliyor.

Geldik diğer sekmeye yukarıda size düzenleyebileceğinizi söylemiştim işte burada bir virgül koyarak bir event id daha ekleyebiliriz.

Ayrıca dilediğiniz gibi değişiklikler yapabilir ya da baştan aşağı kendi sorgunuzu yazabilirisiniz.

Kural oluşturma sihirbazı

✓ Doğrulama başarılı oldu.

Genel Kural mantığını ayarla **Otomatik yanıt** Gözden geçirin ve oluşturun

Yeni analitik kuralınız için mantığı tanımlayın.

Kural sorgusu

```
| where TimeGenerated >= ago(timeRange)
| where OperationName == "Sign-in activity"
// Error codes that we want to look at as they are related to the use of incor
| where ResultType in ("50126", "50053", "50055", "50056")
| extend OS = DeviceDetail.operatingSystem, Browser = DeviceDetail.browser
| extend LocationString= strcat(tostring(LocationDetails["countryOrRegion"])),
```

Burada ayarlanan tüm saat ayrıntıları, Sorgu zamanlama alanlarında aşağıda tanımlanan kapsam içinde olacaktır.  
[Sorgu sonuçlarını görüntüle >](#)

Varlıklar eşle - **daha fazla varlık yakında geliyor!**

[Önceki](#) [Sonraki: Otomatik yanıt >](#)

Ve son sekme, üçüncü sekmeyi es geçiyorum çünkü bize bir PlayBook'un olmadığını söyleyecek bir Playbook hazırlayacağım bundan sonraki aşamada. Oluştur diyerek işlemimize başlıyoruz. (Yazının devamı Playbook sekmesi altındadır)

Kural oluşturma sihirbazı

✓ Doğrulama başarılı oldu.

Genel Kural mantığını ayarla **Otomatik yanıt** **Gözden geçirin ve oluşturun**

Analitik kural ayrıntıları

Ad	Distributed Password cracking attempts
Açıklama	Identifies distributed password cracking attempts from the Azure Active Directory SigninLogs. The query looks for unusually high number of failed password attempts coming from multiple locations for a user account. References: <a href="https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-sign-ins-error-codes">https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-sign-ins-error-codes</a> 50053 Account is locked because the user tried to sign in too many times with an incorrect user ID or password. 50055 Invalid password, entered expired password. 50056 Invalid or null password - Password does not exist in store for this user. 50126 Invalid username or password, or invalid on-premises username or password.
Taktikler	Credential Access
Önem Derecesi	Orta

[Önceki](#) [Oluştur](#)

## Security Event Log Cleared Şablonu ile Incident Oluşturma

Analytics sekmesi içerisindeki hazır kuralları kullanarak Security Events in silinmesi durumunda incident oluşmasını sağlayacağız. Kuralımıza tanımlamak için Analytics sekmesini tıklıyoruz. Rule Templates içerisinde Security Event log cleared tıklayıp create rule u tıklıyoruz.

The screenshot shows the Azure Sentinel Analytics blade. On the left, there's a sidebar with various navigation options like General, Threat management, Configuration, and Analytics. The 'Analytics' option is highlighted with a red arrow. In the main area, there's a search bar at the top. Below it, there's a section titled 'Rules by severity' with a color-coded bar for HIGH (red), MEDIUM (orange), LOW (yellow), and INFORMATIONAL (green). The 'Active rules' tab is selected, showing a list of various security incidents. To the right, a specific rule template is displayed: 'Security Event log cleared'. This template is categorized under 'Medium severity' and 'Scheduled rule type'. It has sections for 'Description', 'Data sources' (Security Events), 'Tactics' (Defense Evasion), 'Rule query' (a complex PowerShell-like query), 'Rule period' (Last 1 day data), 'Rule frequency' (Every 1 day), 'Rule threshold' (Trigger alert if query returns more than 0 results), and 'Suppression' (Not configured). At the bottom right of this card, there's a blue 'Create rule' button. A second red arrow points to this 'Create rule' button.

Kuralımıza isim veriyoruz. Açıklama kısmını okuduğumuzda ilgili kuralın 1102 event id si olduğu yani olay günlüklerinin silindiğinde oluşacağını anlıyoruz. Next: set rule logic> tıklıyoruz.

Home > Azure Sentinel - Analytics > Analytic rule wizard - Create new rule from template

### Analytic rule wizard - Create new rule from template

Security Event log cleared

General Set rule logic Automated response Review and create

Create an analytic rule that will run on your data to detect threats.

**Analytic rule details**

Name \* HD Security Event log cleared ✓

Description Checks for event id 1102 which indicates the security event log was cleared. It uses Event Source Name "Microsoft-Windows-Eventlog" to avoid generating false positives from other sources, like AD FS servers for instance.

Tactics Defense Evasion ✓

Severity Medium ✓

Status Enabled

**Next : Set rule logic >**

İlgili alarmın ne zaman tetikleneceğini ve kuralımızın ne kadar zamanda çalışacağını belirliyoruz. Kural içerisinde değişiklik yapmak isterseniz **Rule query** içerisinde ilgili değişiklikleri yapabiliyoruz. Çok fazla alarm almak istemiyorsanız Alert threshold içerisinde ilgili event in belirli sayıda oluşmasından sonra alarm olmasını sağlayabilirsiniz.(Örneğimizdeki kural için elbette bu kuralın bu şekilde kalmasını tavsiye ederim.) Automation kısmını Playbooks bölümünde işyeceğiz. Next diyerek devam ediyoruz.

Define the logic for your new analytic rule.

```
Rule query
let timeframe = 1d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
| summarize count() by StartTimeUtc = TimeGenerated, Computer, Account, Activity
| extend timestamp = StartTimeUtc, AccountCustomEntity = Account, HostCustomEntity = Computer
```

Any time range or field you will be using the scope defined below in the Query scheduling tab.  
View query results?

**Map entities - more entities coming soon!**

Map the entities recognized by Azure Sentinel to the appropriate columns available in your query results. This enables Azure Sentinel to recognize the entities that are part of the alerts for further analysis. Entity types can be a string or dynamic.

Entity Type	Column
Account	Defined in query
Host	Defined in query
IP	Choose column
URL	Choose column

**Query scheduling**

Run query every \* 5 Minutes

Lookup data from the last \* 5 Minutes

Stop running query after alert is generated  On  Off

**Alert threshold**

Generate alert when number of query results  > greater than

**Next : Automated response**

Tüm ayarları yapılandırdıktan sonra **create** butonunu tıklayarak işlemimizi tamamlıyoruz.

**Analytics rule details**

**Name:** HD Security Event log cleared

**Description:** Checks for event ID 1102 which indicates the security event log was cleared. It uses Event Source Name "Microsoft-Windows-Eventlog" to avoid generating false positives from other sources, like AD FS servers for instance.

**Tactics:** Defense Evasion

**Severity:** Medium

**Status:** Enabled

**Analytic rule settings**

**Rule query:**

```
let timeframe = 1d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
| summarize count() by StartTimeUtc = TimeGenerated, Computer, Account, Activity
| extend timestamp = StartTimeUtc, AccountCustomEntity = Account, HostCustomEntity = Computer
```

**Rule frequency:** Every 5 minutes

**Rule period:** Last 5 minutes data

**Rule threshold:** Trigger alert if query returns **more than 0** results

**Suppression:** Not configured

**Mapped entities**

Account  
Host

**Automated response**

Selected playbook: Not configured

**Create**

Active rules sekmesi içerisinde kuralımızın oluşturulduğunu gözlemliyoruz.

Microsoft Azure

Azure Sentinel - Analytics

Selected workspace: HD Sentinel Block

General

Logs

News & guides

Threat management

Incidents

Windows

Hunting

Notebooks

Configuration

Data connectors

Analytics

Rules by severity

Active rules Rule templates

NAME RULE TYPE STATUS TACTICS LAST MODIFIED

CREATE INCIDENTS BASED ON AZURE SECURITY CENTER ALERTS Microsoft Security (Revised) Enabled 12/11/18, 10:28 PM ...

HD SECURITY EVENT LOG CLEARED Scheduled Enabled Defense Evasion 01/10/20, 07:11 PM ...

Oluşturduğumuz kuralı test etmek için test ortamında Security Loglarını sildim. Incident sekmesine geldiğimde alarmın olduğunu gözlemliyorum.

İlgili alarmı tıklayıp **Investigate** butonunu tıklıyorum.

Microsoft Azure

Azure Sentinel - Incidents

Selected workspace: HD Sentinel Block

General

Logs

News & guides

Threat management

Incidents

Windows

Hunting

Notebooks

Configuration

Data connectors

Analytics

Playbooks

Community

Search (Ctrl+F)

Last 24 hours Actions

Open incidents by severity

Open incidents

New incidents

In progress

SEVERITY: Informational, Low, Medium, High, Critical

STATUS: New, In Progress

PRODUCT NAME: All

OWNER: All

Incident ID Title Alerts Product name Created Time Last update time Owner Status

3 HD Security Event log cleared 1 Azure Sentinel 01/10/20, 07:22 PM 01/10/20, 07:22 PM Unassigned New

2 Security Event log cleared 1 Azure Sentinel 01/10/20, 06:47 PM 01/10/20, 06:47 PM Unassigned New

1 Security Event log cleared 1 Azure Sentinel 01/10/20, 06:42 PM 01/10/20, 06:42 PM Unassigned New

HD Security Event log cleared

Incident ID: 3

Medium Severity

New Status

Unassigned Owner

Description

Checks for events of type 102 which indicates the security event log was cleared. Look for Source Name: 'Microsoft-Windows-EventLog' to avoid generating false positives from other sources like the AD FS servers for instance.

Incident link

Tags

+

Last update time

01/10/20, 07:22 PM

Creation time

01/10/20, 07:22 PM

Close reason

N/A

Evidence

2 Events 1 Alerts 0 Bookmarks

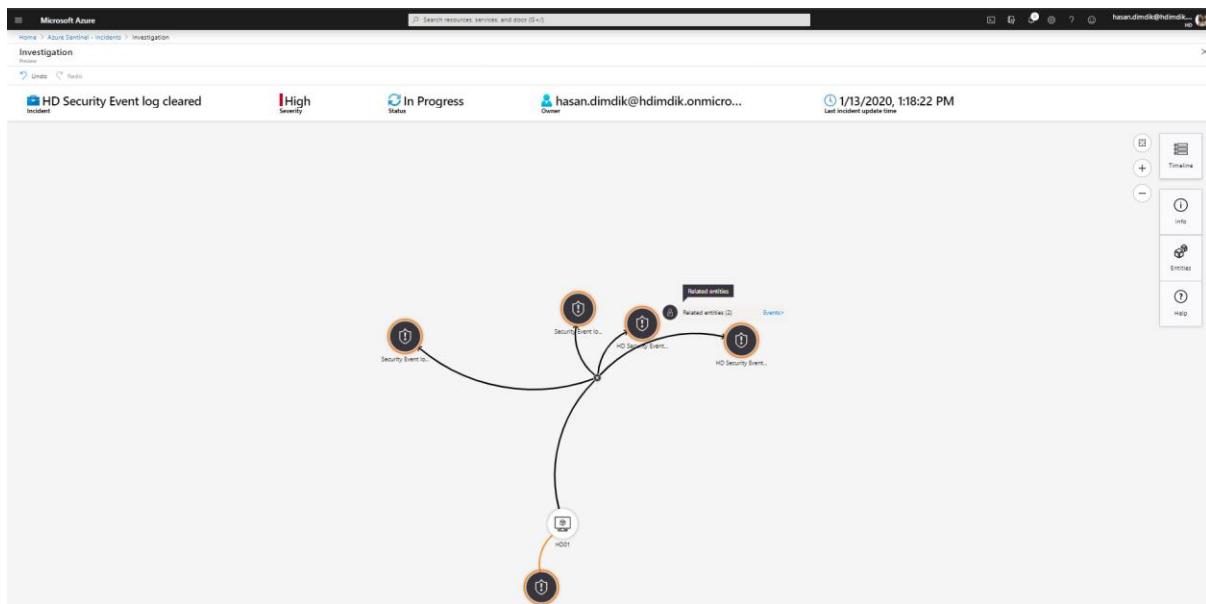
Entities

0 Account 2 Host 0 IP 0 URL

Last comment

Investigate [View available] View full details

Grafiksel olarak da neler olduğunu gözlemliyoruz. Eğer oluşan vaka ile benzerlik gösteren incident ler var ise onları da gözlemliyoruz.



## Hunting

Proaktif olarak yapınıza gelen saldırıları veya tehditleri araştırmak isterseniz Hunting özelliği yüzlerce veri arasından sizlere anlamlı çıktılar üretir. Bir tehditi bulmak için en önemli noktalardan bir tanesi doğru soruyu kullanmaktadır. Hunting özelliği bize bunu built-in sorgular ile sağlamaktadır.

Örnek olarak hazır gelen sorgulardan **Summary of failed user logons by reason of failure** seçtim ve Run Query butonunu tıkladım.

Query	Provider	Data Source	Results	Tactics
Scheduled Task Aggregation	Microsoft	Syslog	0	
SharePointFileOperation via clientIP with previously unseen...	Microsoft	OfficeActivity	0	Exfiltration
SharePointFileOperation via devices with previously unseen...	Microsoft	OfficeActivity	0	Exfiltration
Signin Logs with expanded Conditional Access Policies	Microsoft	SigninLogs	0	Impact
Squid commonly abused TLDs	Microsoft	Syslog	0	Command and Control
Squid malformed requests	Microsoft	Syslog	0	Discovery
<b>Summary of failed user logons by reason of failure</b>	Microsoft	SecurityEvent	1	
Summary of user logons by logon type	Microsoft	SecurityEvent	4	
Summary of users created using uncommon/undocumented...	Microsoft	SecurityEvent	0	

View Result butonuna tıkladıktan sonra sorgumun çıktılarını görebiliyorum. İncelediğimde ise yanlış parola girildiğini gözlemliyorum. Sorgum sonucu oluşan çıktınin benim için önemli olduğunu varsayılm ve tekrarlanması durumuna karşılık alarm oluşturalım.

Reason	timestamp [UTC]	StartTimeUtc [UTC]	EndTimeUtc [UTC]	count_
Incorrect password	6/25/2020, 6:23:54.593 PM	6/25/2020, 6:23:54.593 PM	6/25/2020, 6:24:00.830 PM	6

Incorrect password in yanındaki kutucuğu işaretliyoruz ve New Alert Rule tıklıyoruz.

Reason	timestamp [UTC]	StartTimeUtc [UTC]	EndTimeUtc [UTC]	count_
Incorrect password	6/25/2020, 6:23:54.593 PM	6/25/2020, 6:23:54.593 PM	6/25/2020, 6:24:00.830 PM	6

Kuralımıza isim verip açıklaması kısmını dolduruyorum. Set Rule Logic ile işlemime devam ediyorum.

#### Analytic rule wizard - Create new rule

General   Set rule logic   Incident settings (Preview)   Automated response   Review and create

Create an analytic rule that will run on your data to detect threats.

**Analytic rule details**

Name \*  
Summary of failed user logons by reason of failure - HD

Description  
Summary of failed user logons by reason of failure

Tactics  
Credential Access

Severity  
Low

Status  
Enabled

[Next : Set rule logic >](#)

Örneğim için herhangi bir entities tanımlamıyorum **Incident settings (Preview)** butonunu tıklıyorum

#### Analytic rule wizard - Create new rule

Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

```
let timeframe = $id;
securityEvent
| where TimeGenerated >= ago(timeframe)
| where AccountType == "User" and EventID == 4625
| extend Reason = case(SubStatus == '0xc000005e', 'No logon servers available to service the logon request', S
| summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated), count() by Reason
View query results >
```

Map entities

Map the entities recognized by Azure Sentinel to the appropriate columns available in your query results. This enables Azure Sentinel to recognize the entities that are part of the alerts for further analysis. Entity type must be a string or Datetime.

Entity Type	Column	Score
Account	Choose column	0.8
Host	Choose column	0.6
IP	Choose column	0.5
URL	Choose column	0.5

Previous **Next : Incident settings (Preview) >**

İlgili alarm oluşturuğunda incident olarak görmek istiyorum.

#### Analytic rule wizard - Create new rule

General Set rule logic **Incident settings (Preview)** Automated response Review and create

**Incident settings (Preview)**

Azure Sentinel alerts can be grouped together into an Incident that should be looked into. You can set whether the alerts that are triggered by this analytics rule should generate incidents.

Create incidents from alerts triggered by this analytics rule

Enabled  Disabled

---

**Alert grouping**

Set how the alerts that are triggered by this analytics rule, are grouped into incidents. Grouping alerts into incidents provides the context you need to respond and reduces the noise from single alerts.

Group related alerts, triggered by this analytics rule, into incidents

Enabled  Disabled

---

Limit the group to alerts created within the selected time frame

5 Hours

Group alerts triggered by this analytics rule into a single incident by

Grouping alerts into a single incident if all the entities match (recommended)

Grouping all alerts triggered by this rule into a single incident

Combining alerts into a single incident if the selected entities match

Previous **Next : Automated response >**

Azure Sentinel' in mottosuna baktığımız zaman SIEM+ SOAR olduğunu görüyoruz. Bu kısım tam olarak SOAR' a karşılık gelmektedir. Yazmış olduğunuz veya hali hazırda Github' dan elde ettiğiniz Playbook'ları burada ilgili kuralla eşleşmesi durumunda çalıştırabilirsiniz.

Microsoft Azure

Home > Azure Sentinel workspaces > Azure Sentinel | Hunting > Logs >

Analytic rule wizard - Create new rule

General Set rule logic Incident settings (Preview) Automated response Review and create

Select a playbook to be run automatically when your analytic rule generates an alert.

You only see playbooks in your selected subscriptions and for which you have permissions.

Selected playbook: Run-MDATPAntivirus

Search

Name	Trigger kind	Status
Get-MDATPVulnerabilities	Azure Sentinel Alert	Enabled
Run-MDATPAntivirus	Azure Sentinel Alert	Enabled

Previous Next: Review >

Kuralımın özetini görüyorum **create** diyerek işlemimi tamamlıyorum.

Home > Azure Sentinel | Hunting > Logs >

Analytic rule wizard - Create new rule

Validation passed.

Analytic rule details

Name	Summary of failed user logons by reason of failure - HD
Description	Summary of failed user logons by reason of failure
Tactics	Credential Access
Severity	Low
Status	Enabled

Analytic rule settings

Rule query

```
let timeframe = 1d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where AccountType == "User" and EventID == 4625
| extend Reason = case(SubStatus == "0x0000005e", "No logon servers available to service the logon request", SubStatus == "0x0c000062", "Account name is not properly formatted", SubStatus == "0x0c000064", "Account name does not exist", SubStatus == "0x0c00006a", "Incorrect password", SubStatus == "0x0c00006d", "Bad user name or password", SubStatus == "0x0c00006f", "User logon blocked by account restriction", SubStatus == "0x0c00006f", "User logon outside of restricted logon hours", SubStatus == "0x0c000070", "User logon blocked by workstation restriction", SubStatus == "0x0c000072", "Password has expired", SubStatus == "0x0c000073", "Account is disabled", SubStatus == "0x0c000133", "Clocks between DC and other computer too far out of sync", SubStatus == "0x0c00015b", "The user has not been granted the requested logon right for this machine", SubStatus == "0x0c000193", "Account has expired", SubStatus == "0x0c000224", "User is required to change password at next logon", SubStatus == "0x0c000234", "Account is currently locked out", strcat("Unknown reason substatus:", SubStatus))
| summarize StartTime = min(TimeGenerated), EndTimeUTC = max(TimeGenerated), count() by Reason
| extend timestamp = StartTimeUTC
```

Rule frequency

Last 5 hours

Rule period

Trigger alert if query returns **more than 0** results

Rule threshold

Not configured

Suspension

Mapped entities

Not configured

Previous Create

Aynı olay tekrarlandığında incident sekmesi altında artık görebiliyorum.

Microsoft Azure

Home > Azure Sentinel workspaces > Azure Sentinel | Incidents

Selected workspace: 'hd-sentinel-ebook'

Search (Ctrl+)

Refresh Last 30 days Actions

General Overview Logs News & guides Threat management Threat management Incidents Workbooks Hunting Notebooks Configuration Data connectors Analytics Playbooks Community Settings

Open incidents by severity

10 Open incidents 10 New incidents 0 Active incidents

SEVERITY : All STATUS : New, Active PRODUCT NAME : All OWNER : All

Open incidents by severity

High (0) Medium (3) Low (4) Informational (3)

Summary of failed user logons by reason of failure

Incident ID: 118

Description: Summary of failed user logons by reason of failure

Incident link: https://portal.azure.com/#asset/Microsoft\_Azure\_Security\_Insights/118

Tactics: Credential Access

Tags: +

Last update time: 06/25/20, 10:57 PM

Creation time: 06/25/20, 10:57 PM

Classification: N/A

The investigation graph requires that your incident includes entities (for example user, host, ip, etc.). Use the entity mapping option when defining your alerts. Learn more >

Investigate View full details

Playbook' un başarılı şekilde çalıştığını gözlemliyorum.

Microsoft Azure

Home > Azure Sentinel workspaces > Azure Sentinel | Playbooks > Run-MDATPAntivirus

Search (Ctrl+)

Run Trigger Refresh Edit Delete Disable Update Schema Clone Export

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Development Tools Logic app designer Logic app code view Versions API connections Quick start guides Release notes Settings Workflow settings Authorization Access keys Identity

Resource group: Sentinel

Location: West Europe

Subscription: Visual Studio Enterprise

Subscription ID: ce50118a-11de-4ef4-9236-d2f6e314bfde

Definition: 1 trigger, 6 actions

Status: Enabled

Runs last 24 hours: 1 successful, 0 failed

Integration Account: ---

Summary

Trigger: AZURESENTINEL\_1 (When a response to an Azure Sentinel alert is triggered)

Actions: COUNT 6 actions View in Logic Apps designer

FREQUENCY: EVALUATION (Evaluated 1 times, fired 1 times in the last 24 hours. See trigger history)

Runs history

All	Start time earlier than	Pick a date	Pick a time
Specify the run identifier to open monitor view directly			
Status	Start time	Identifier	Duration
Succeeded	6/25/2020, 11:00 PM	08586084952334170380279348748CU178	2.02 Seconds
			Static Results

Hunting kavramını toparlayacak olursak n tane güvenlik cihazından üretilen ve anlamlandırılması zor olan samanlıktaki iğneyi bulmamıza yardımcı olmaktadır.

<https://docs.microsoft.com/en-us/azure/sentinel/hunting>

<https://github.com/Azure/Azure-Sentinel/tree/master/Hunting%20Queries>

## Notebooks

Notebook sekmesini özellikle SOC uzmanları daha detay sorgular yazmak için kullanmaktadır. Kusto sorgu dili, python veya Jupyter dillerini kullanarak şirkete özel hunting kurallarını oluşturabilmektedirler. İleri düzey bir konu olduğu için ilgili başlığın detaylarına yazı içerisinde yer vermeyeceğiz.

The screenshot shows the Azure Sentinel Notebooks page. On the left, there's a sidebar with navigation links like General, Threat management, Configuration, and Notebooks. The main area displays a list of notebooks with columns for name, provider, status, and last update. One notebook, 'Guided Investigation - Alert Triage', is highlighted with a detailed modal overlay. The modal shows the notebook's description, which mentions it's a guided investigation for alert triage using Microsoft Threat Intelligence and OSINT. It also lists required data types (SecurityAlert) and data sources (Security Alert). A preview of the notebook's content is shown at the bottom.

Notebook lar ile ilgili detay bilgiye aşağıdaki kaynaklardan erişebilirsiniz.

<https://docs.microsoft.com/en-us/azure/sentinel/notebooks>

<https://security.wortell.nl/timeline/azure-sentinel-automating-your-use-cases-with-powershell-and-azsentinel-technical>

<https://www.youtube.com/watch?v=-NjEP-dXSmM>

<https://www.youtube.com/watch?v=cT27HMFbCv0>

## Configuration

### Playbooks

Senaryomuz şöyle, bir uyarı oluştığunda bunu bize Slack üzerinden bildirecek. Hali hazırda kuruluşunuzda bu işlerden sorumlu kişilerin aktif olarak kullandığı ya da yeni bir tane Slack kanalı oluşturup kenarda hazır olarak bekletmekte fayda var.Yeni bir kural oluşturup isimlendirin ve gerekli öğeleri seçin.

The screenshot shows the 'Mantıksal Uygulama' (Logical App) creation form in the Azure Sentinel interface. The form includes fields for 'Ad' (Name), 'Abonelik' (Subscription), 'Kaynak grubu' (Resource Group), 'Konum' (Location), 'Log Analytics' (On/Off switch), and 'Log Analytics çalışma alanı' (Log Analytics workspace). The 'Ad' field is set to 'Sentinel', 'Abonelik' to 'Free Trial', 'Kaynak grubu' to 'POC2', 'Konum' to 'Orta ABD', 'Log Analytics' is turned 'On', and the 'Log Analytics çalışma alanı' is set to 'wspc3'. At the bottom, there are 'Oluştur' (Create) and 'Otomasyon seçenekleri' (Automation options) buttons.

Giriş > Azure Sentinel - Playbook'lar > Mantıksal Uygulama Oluştur

**Mantıksal Uygulama**

Ad \*

Sentinel

Abonelik \*

Free Trial

Kaynak grubu \* ⓘ

Yeni oluştur  Var olanı kullan

POC2

Konum \*

Orta ABD

Log Analytics ⓘ

On Off

Log Analytics çalışma alanı \*

wspc3

Oluştur Otomasyon seçenekleri

Boş mantıksal uygulamayı seçin.

## Logic Apps Tasarımcısı

### Şablonlar

Mantıksal Uygulamanızı oluşturmak için aşağıdan bir şablon seçin.

Kategori: Güvenlik

Sıralama ölçü

Boş Mantıksal Uygulama



Get a notification email when Security Center creates a recommendation



Get a notification email when Security Center detects a threat

Arama kutusundan yararlanarak Azure Sentinel'i bulun.

Bağlayıcılar ve tetikleyiciler içinde ara

Sizin İçin

Tümü

Yerleşik

Standart

Kuruluş

Özel

Son görüntülenen

Temizle



Slack



Azure Sentinel



İstek

Azure Sentinel

Eylem olarak Slack'i seçin.

 When a response to an Azure Sentinel alert is triggered (Önizleme) ...

↓

 Eylem seçin X

Bağlayıcılar ve eylemler içinde ara

Sizin İçin    Tümü    Yerleşik    Standart    Kuruluş    Özel

Son görüntülenen Temizle

 Azure Sentinel

 Slack

 Slack tek

Slack'in ne yapması istedğini seçin.

 When a response to an Azure Sentinel alert is triggered (Önizleme) ...

↓

 Slack X

Bağlayıcılar ve eylemler içinde ara

Tetikleyiciler    **Eylemler**

 Grup oluştur  
Slack ⓘ

 İleti gönder  
Slack ⓘ

 Kanal oluştur  
Slack ⓘ

İletinin hangi kanala ve bilgileri ileteceğini seçin.

Ve şimdi bir önceki adımda oluşturduğumuz Kurala geri dönelim ve 3.sekmeye gelelim işte Sentinel adındaki PlayBook burada bunu seçip tamam diyoruz.

Ad	Durum	Tetikleyici tipi
[Analist] Analiz	Etkin	Azure Sentinel
[Analist] Sentinel	Etkin	Azure Sentinel

Bu arada Slack'i test etmeyi unutmayın!

Github' da yer alan playbookları kullanarak sizinzdaki ihtiyaçlara göre yapılandırma yapabilirsiniz.

<https://github.com/Azure/Azure-Sentinel/tree/master/Playbooks>

## Settings

Ayarlar sekmesinde ücretlendirme, data kullanımı ve log analytic ile ilgili bilgilere ulaşabiliyorsunuz. Pricing sekmesi özellikle kullanım yaparken maliyet avantajı sağlama açısından bizlere son derece faydalı bilgiler vermektedir. Bu bilgi sayesinde hangi model bizim için uygunsa seçebiliyoruz.

The screenshot shows the Azure Sentinel Settings page. On the left, there's a sidebar with navigation links like Overview, Logs, News & guides, Threat management, Configuration, and Settings. The main content area has tabs for Pricing, Settings, and Workspace settings. The Pricing tab is selected. It displays a chart titled "Data ingestion (Last 31 days)" showing data usage over time, with a peak around May 24. Below the chart, it says "You consumed 0.5 GB data." Another chart titled "Data retained per solution (Last 31 days)" shows retention levels for various solutions, with a large blue bar for LogManagement. A note at the bottom says "You can increase your workspace data retention to 90 days for free because you are an Azure Sentinel customer. Configure retention".

**Settings** sekmesinde varsayılan olarak **How do we use your data ?** aktiftir. Bu benim için ne ifade ediyor diyecek olursanız, Microsoft mühendislerinin analitik modellerin oluşturulmasına, test edilmesine ve optimize edilmesine yardımcı olmak için verilerinize erişmesine ve bunları kullanmasına izin verdığınız anlamına gelmektedir. Diğer bir seçenek ise Azure Sentinel i workspace silmemize olanak sağlıyor.

The screenshot shows the Azure Sentinel Settings page. The sidebar and tabs are the same as the previous screenshot. The main content area has a heading "How do we use your data?" with a toggle switch set to "On". Below it is a section titled "Remove Azure Sentinel". It contains a "Before you go..." list with items like "After the disconnection is identified, the offboarding process begins.", "For connector-specific offboarding instructions see Remove Azure Sentinel from your workspace.", "You must manually delete your playbooks, saved workbooks, saved hunting queries, notebooks, and any additional log type.", and "After 30 days, your incidents, analytic rules, and bookmarks are deleted from your workspace.". There's also a "Sorry to see you go. Let us know why you're leaving" section with checkboxes for "Moving to another workspace", "Missing features", "Too expensive", and "Other". An "Additional details:" text area is present. At the bottom, a note says "Within 48 hours, the data and analytic rules (including real-time automation configuration) will no longer be accessible or viewable in Azure Sentinel."

Workspace settings sekmesi bizi Log Analytics'e yönlendirmektedir. Bu bölümde bir çok ayar mevcut fakat özellikle müşteri odaklı düşündüğümüzde usage and estimated costs kısmında Log Analytics kullanım oranı ve ücretlendirmesini görebiliyoruz.

Microsoft Azure

Search resources, services, and docs (Q+)

hasan.dimdik@hdimdik... HD

**HD-Sentinel-EBook | Usage and estimated costs**

Log Analytics workspace

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Settings Locks Export template Agents management Advanced settings General Quick Start Workspace summary View Designer Workbooks Logs Solutions Saved searches Pricing tier Usage and estimated costs Properties Service Map Workspace Data Sources

Usage details Daily cap Data Retention Help

Your Log Analytics cost depends on your choice of pricing tier, data retention and which solutions are used. Here you can see the estimated monthly cost for each of the available pricing tiers, based on your last 31-days of Log Analytics data ingested. These cost estimates can be used to help you select the best pricing tier based on your data ingestion patterns. These estimates include the 500MB/VM/day data allowances from Azure Security Center. If you have questions about using this page, contact us. Learn more about Log Analytics pricing.

**Pricing Tiers**

**Pay-as-you-go** Per GB

The Per GB 2019 pricing tier is a pay-as-you-go tier offering flexible consumption pricing in which you are charged per GB of data ingested. There are additional charges if you increase the data retention above the 31 day included retention (or 90 day included retention if using Sentinel on this workspace). Learn more about Log Analytics pricing.

**Estimated costs**

Item type	Price	Monthly usage (last 31 days)	Estimated monthly cost
Log data ingestion	TRY 16.76	0.55 GB	TRY 9.20
Log data retention (beyond 90 days)	TRY 0.73	0.00 GB	TRY 0.00
<b>Total</b>			<b>TRY 9.20</b>

(The log data ingestion includes the 500 MB/VM/day data allowances from Azure Security Center)

This is the current pricing tier.

Select

100 GB/day Capacity Reservation 15% discount over Pay-as-you-go

200 GB/day Capacity Reservation 20% discount over Pay-as-you-go

300 GB/day Capacity Reservation 25% discount over Pay-as-you-go

**Usage Charts**

Billable data ingestion per solution (last 31 days)

Data ingested per solution (last 90 days)

LogManagement 2.26 GB  
Security 2.18 GB  
ChangeTrig 10 MB

Umuyorum Faydası Dokunmuştur.

## Son Söz



İlgili döküman Köy Enstitüsü' nün yetiştirdiği adını gururla taşıdığım dedem Hasan DİMDİK' e ithafen Ömer ile beraber kaleme aldık...

Köy enstitüsünün yetiştirdiği Hasan Dimdik öğretmenim... Ulu bir çınar düştü toprağa. Yıldızlar içinde uyu... Yıldızlı yumruğun yoldaşın olsun....

Sorulan her yaşam ve hayat sorusuna, şiir kıtaları ile yanıt verirdi. Her kıta bir ilham kaynağıydı.

Tırpanı, orağı, örsü, çekici tanımlarken; "Alın teri, emek ve bereket" derdi.

Toprağı, doğayı tanımlarken "Ana, bir çift yürek, karın ve arı" derdi...

Ellerinden öpüyorum öğretmenim.

"Kara oğlum dikkat et... Yaşamın çok ağır geçecek, bu düzen ve düzeni savunanlar dilini susturmak için ellerinden geleni yaparlar" demişti...

İşte köy enstitüsünün yetiştirdiği çınarların yurdumuza saçtığı daneler... Varın siz düşünün.

*Mekanın cennet olsun huzur içinde uyu...*

**27 Haziran 2020**

