

# **AZURE SENTINEL İLE LOG YÖNETİMİ VE SIEM PROJE RAPORU**

**Hazırlayan  
Ayşenur ÖZKAN**

## İÇİNDEKİLER

İÇİNDEKİLER .....	i
1.GİRİŞ .....	1
2. HATALI GİRİŞLERİ TESPİT ETME VE GÖSTERME .....	1
2.1. Kullanılan Platform .....	1
2.2. Çalışma Ortamını Hazırlama.....	1
2.3. Hatalı Girişleri Toplayıp Log Dosyasını Oluşturma .....	3
2.4. Log Dosyasını Çalışma Alanına Ekleme.....	4
2.5. Hatalı Girişleri Harita Üzerinde Gösterme .....	5
3. HATALI GİRİŞ İŞLEMLERİ İÇİN ALARM OLUŞTURMA .....	6
3.1. Alarm Nedir .....	6
3.2. Tespit Edilen Hatalı Girişler İçin Azure Sentinel İle Alarm Oluşturma .....	7
4. SONUÇ.....	7
KAYNAKÇA.....	8

## **1.GİRİŞ**

Bu çalışmada Azure Platformu üzerinde zafiyetli bir Windows10 sanal makine oluşturulmuş ve tehdit aktörlerinin sanal makineye yaptığı hatalı giriş işlemleri kaydedilmiştir. Toplanan hatalı giriş verilerinin, oluşturduğu log dosyası Azure Sentinel Platformu kullanılarak görselleştirilmiştir. Log dosyasında bulunan ip adreslerinin sahip olduğu konum bilgisi IP Geolocation Api kullanılarak bulunmuş ve Dünya haritası üzerine yerleştirilerek haritalandırma işlemi gerçekleştirilmiştir.

## **2. HATALI GİRİŞLERİ TESPİT ETME VE GÖSTERME**

### **2.1. Kullanılan Platform**

Azure Sentinel, Microsoft'un bulut ortamında sunduğu bir SIEM (Security Information and Event Management) servisidir. Kuruluşun bütününün kuşbakışı olarak gözlemlenmesine olanak sağlar. Azure Sentinel, hedeflenen saldırıların ve veri ihlallerinin erken tespiti ve önlenmesi için olay verilerini gerçek zamanlı olarak analiz eder. Ayrıca, yapay zeka (AI) sayesinde tehdit algılama ve müdahale işlemlerinin daha akıllı ve hızlı hale getirilmesine yardımcı olur. Azure Sentinel, aynı anda birden fazla sorgunun yazılmasına ve bu sorguları birlikte çalıştırılmasına olanak sağlar.

### **2.2. Çalışma Ortamını Hazırlama**

Bu çalışmada Azure tarafından sağlanan sanal makine kullanılacağından öncelikle sanal makinenin kurulum işlemlerinin yapılması gerekmektedir [1]. Yeni bir sanal makine oluşturulup Şekil 2.1.' de gösterildiği gibi ayarlama işlemleri gerçekleştirilir.

[Home](#) > [Virtual machines](#) >

## Create a virtual machine ...

### Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	<input type="text" value="Azure for Students"/>
Resource group *	<input type="text" value="Honeypotlab"/>
	<a href="#">Create new</a>

### Instance details

Virtual machine name *	<input type="text" value="Honeypot-vm"/>
Region *	<input type="text" value="(US) West US 3"/>
Availability options	<input type="text" value="No infrastructure redundancy required"/>
Security type	<input type="text" value="Standard"/>
Image *	<input type="text" value="Windows 10 Pro, version 21H2 - x64 Gen2"/>
	<a href="#">See all images</a>   <a href="#">Configure VM generation</a>
VM architecture	<input type="radio"/> Arm64 <input checked="" type="radio"/> x64

[Review + create](#)

[< Previous](#)

[Next : Disks >](#)

Şekil 2.1. Sanal Makine Ayarları.

Sanal makine oluşturduktan sonra, log faaliyetlerinin izlenmesini ve analiz edilmesini sağlayan çalışma alanı oluşturulmalıdır (Log Analytics Workspace) [2]. Bu işlem Şekil 2.2.' de gösterildiği gibi yapılır.

## Create Log Analytics workspace ...

[Basics](#) [Tags](#) [Review + Create](#)

**i** A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. [Learn more](#)

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

### Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

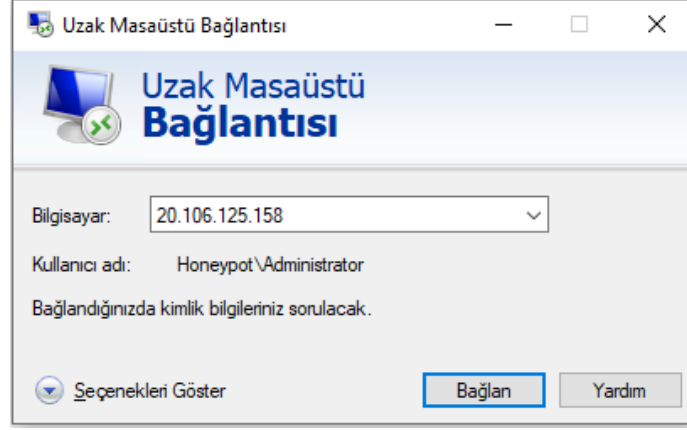
Subscription *	<input type="text" value="Azure for Students"/>
Resource group *	<input type="text" value="Honeypotlab"/>
	<a href="#">Create new</a>

### Instance details

Name *	<input type="text" value="law-honeypotlab"/>
Region *	<input type="text" value="West US 3"/>

Şekil 2.2. Log Analytics Workspace Oluşturma.

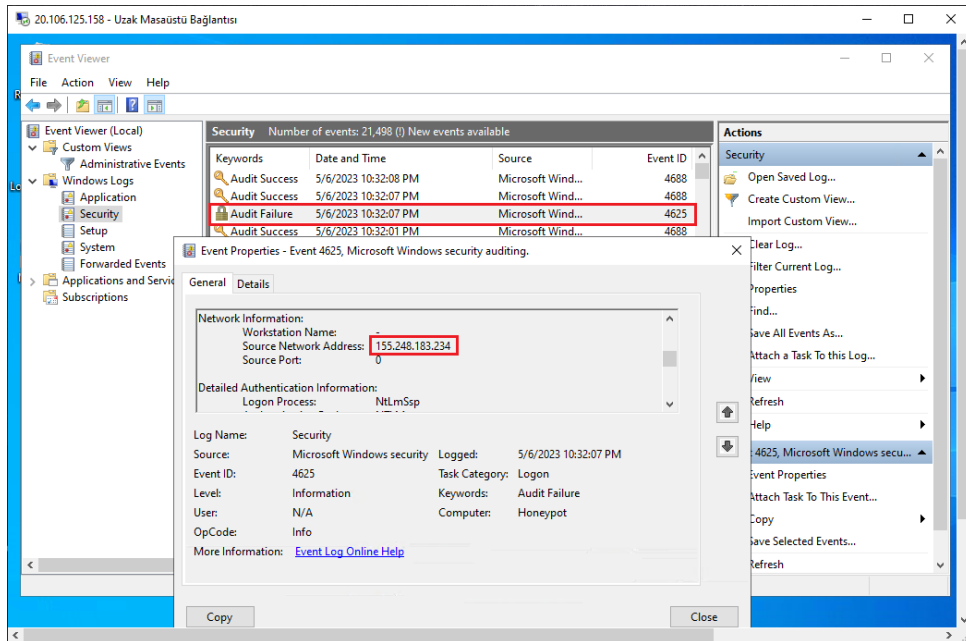
Azure' un sanal makinemize atadığı public ip adresini ve uzak masaüstü bağlantısını kullanarak Windows10 makinemize erişelim. Şekil 2.3.



Şekil 2.3. Uzak Masaüstü ile Sanal Makineye Bağlanma.

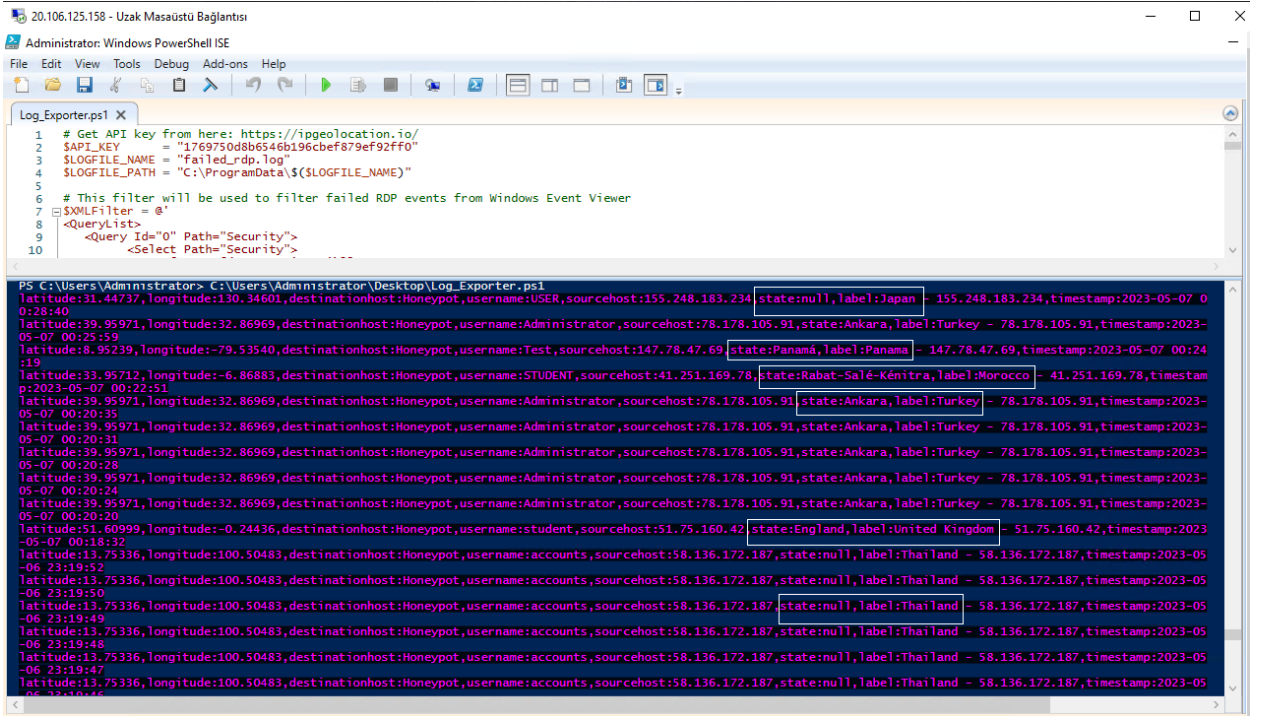
### 2.3. Hatalı Girişleri Toplayıp Log Dosyasını Oluşturma

Windows10 içerisinde Olay Görüntüleyicisi (Event Wiewer) ile sistemdeki olay günlüklerini inceleyebiliriz. Biz çalışmamızda hatalı giriş işlemlerini incelemek istediğimiz için olay yöneticisinde olay numarası 4625 olan olayları inceleyeceğiz [3]. Sisteme hatalı bir giriş olduğunda, olay görüntüleyicisi girişin yapıldığı ip adresini, olay numarasını (event id), giriş tarihini ve saatini Şekil 2.4.' de gösterildiği gibi tutar.



Şekil 2.4. Olay Görüntüleyicisi.

Burada amacımız bu ip adreslerinin konumlarını bularak sisteme girmeye çalışan kişilerin konumu tespit etmek. Bu işlem için Custom\_Security\_Log\_Exporter.ps1 [4] adında bir kod dosyası kullanacağız. Bu dosya hatalı giriş yapılan ip adreslerinin IP Geolocation Api'ye gönderilip konumlarının tespit edilmesini sağlayacak. Aynı zamanda içerisinde tespit edilen konumların da olduğu bir log dosyası oluşturacak. Kod dosyanın ürettiği sonucu Şekil 2.5.' de görebiliriz. Şekil üzerinde işaretlenmiş bölgeler ip adreslerinin tespit edilen konumlarıdır.



```
20.106.125.158 - Uzak Masaüstü Bağlantısı
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Log_Exporter.ps1 X
1 # Get API key from here: https://ipgeolocation.io/
2 $API_KEY = "1769750d8b6546b196cbef879ef92ff0"
3 $LOGFILE_NAME = "Failed_rdp_log"
4 $LOGFILE_PATH = "C:\ProgramData\$($LOGFILE_NAME)"
5
6 # This filter will be used to filter failed RDP events from Windows Event Viewer
7 $XMLFilter = @"
8 <QueryList>
9   <Query Id="0" Path="Security">
10     <Select Path="Security">
11       *
12     </Select>
13   </Query>
14 </QueryList>
15 @"
```

PS C:\Users\Administrator> C:\Users\Administrator\Desktop\Log\_Exporter.ps1

Latitude:31.44737,longitude:130.34601,destinationhost:Honeybot,username:USER,sourcehost:155.248.183.234,state:null,label:Japan - 155.248.183.234,timestamp:2023-05-07 00:28:40

Latitude:39.95971,longitude:32.86969,destinationhost:Honeybot,username:Administrator,sourcehost:78.178.105.91,state:Ankara,label:Turkey - 78.178.105.91,timestamp:2023-05-07 00:25:59

Latitude:8.95239,longitude:-79.53540,destinationhost:Honeybot,username:Test,sourcehost:147.78.47.69,state:Panamá,label:Panama - 147.78.47.69,timestamp:2023-05-07 00:24:19

Latitude:33.95712,longitude:-6.86883,destinationhost:Honeybot,username:STUDENT,sourcehost:41.251.169.78,state:Rabat-Salé-Kénitra,label:Morocco - 41.251.169.78,timestamp:2023-05-07 00:22:51

Latitude:39.95971,longitude:32.86969,destinationhost:Honeybot,username:Administrator,sourcehost:78.178.105.91,state:Ankara,label:Turkey - 78.178.105.91,timestamp:2023-05-07 00:20:35

Latitude:39.95971,longitude:32.86969,destinationhost:Honeybot,username:Administrator,sourcehost:78.178.105.91,state:Ankara,label:Turkey - 78.178.105.91,timestamp:2023-05-07 00:20:31

Latitude:39.95971,longitude:32.86969,destinationhost:Honeybot,username:Administrator,sourcehost:78.178.105.91,state:Ankara,label:Turkey - 78.178.105.91,timestamp:2023-05-07 00:20:28

Latitude:39.95971,longitude:32.86969,destinationhost:Honeybot,username:Administrator,sourcehost:78.178.105.91,state:Ankara,label:Turkey - 78.178.105.91,timestamp:2023-05-07 00:20:24

Latitude:39.95971,longitude:32.86969,destinationhost:Honeybot,username:Administrator,sourcehost:78.178.105.91,state:Ankara,label:Turkey - 78.178.105.91,timestamp:2023-05-07 00:20:20

Latitude:51.60999,longitude:-0.24436,destinationhost:Honeybot,username:student,sourcehost:51.75.160.42,state:England,label:United Kingdom - 51.75.160.42,timestamp:2023-05-07 00:18:32

Latitude:13.75336,longitude:100.50483,destinationhost:Honeybot,username:accounts,sourcehost:58.136.172.187,state:null,label:Thailand - 58.136.172.187,timestamp:2023-05-06 23:19:52

Latitude:13.75336,longitude:100.50483,destinationhost:Honeybot,username:accounts,sourcehost:58.136.172.187,state:null,label:Thailand - 58.136.172.187,timestamp:2023-05-06 23:19:50

Latitude:13.75336,longitude:100.50483,destinationhost:Honeybot,username:accounts,sourcehost:58.136.172.187,state:null,label:Thailand - 58.136.172.187,timestamp:2023-05-06 23:19:49

Latitude:13.75336,longitude:100.50483,destinationhost:Honeybot,username:accounts,sourcehost:58.136.172.187,state:null,label:Thailand - 58.136.172.187,timestamp:2023-05-06 23:19:46

Latitude:13.75336,longitude:100.50483,destinationhost:Honeybot,username:accounts,sourcehost:58.136.172.187,state:null,label:Thailand - 58.136.172.187,timestamp:2023-05-06 23:19:47

Latitude:13.75336,longitude:100.50483,destinationhost:Honeybot,username:accounts,sourcehost:58.136.172.187,state:null,label:Thailand - 58.136.172.187,timestamp:2023-05-06 23:19:45

Şekil 2.5. Custom\_Security\_Log\_Exporter.ps1 Dosyasının Çıktısı.

## 2.4. Log Dosyasını Çalışma Alanına Ekleme

Oluşturulan Log dosyasının haritalandırılabilmesi için çalışma alanına yüklenmesi gerekmektedir. Çalışma alanı içerisinde Tables/Create/New Custom Log (MMA- based) adımları takip edilerek ilgili log dosyası bu dizine yüklenmelidir [5]. Yükleme işlemi gerçekleştirildikten sonra, log dosyasına çalışma alanı içerisinden de erişilebilir. Şekil 2.6.' da görüldüğü gibi dosyanın yüklenme işlemi başarılı bir şekilde gerçekleştirildi.

	timestamp_CF [UTC]	label_CF	country_CF	state_CF
3.destinationhostHoney...	5/7/2023, 12:22:51.000 AM	Morocco - 41.251.169.78	Morocco	Rabat-Salé-Kénitra
19.destinationhostHoney...	5/7/2023, 12:20:35.000 AM	Turkey - 78.178.105.91	Turkey	Ankara
19.destinationhostHoney...	5/7/2023, 12:20:31.000 AM	Turkey - 78.178.105.91	Turkey	Ankara
19.destinationhostHoney...	5/7/2023, 12:20:28.000 AM	Turkey - 78.178.105.91	Turkey	Ankara
19.destinationhostHoney...	5/7/2023, 12:20:24.000 AM	Turkey - 78.178.105.91	Turkey	Ankara
19.destinationhostHoney...	5/7/2023, 12:20:20.000 AM	Turkey - 78.178.105.91	Turkey	Ankara
6.destinationhostHoney...	5/7/2023, 12:18:32.000 AM	Kingdom - 51.75.160.42	United Kingdom	England
183.destinationhostHone...	5/6/2023, 11:19:52.000 PM	Thailand - 58.136.172.187	Thailand	null
183.destinationhostHone...	5/6/2023, 11:19:50.000 PM	Thailand - 58.136.172.187	Thailand	null

Şekil 2.6. Log Dosyası.

## 2.5. Hatalı Girişleri Harita Üzerinde Gösterme

Bu işleme haritalandırma adı verilmektedir. Haritalandırma yapabilmek için Azure Sentinel altında yeni bir workbook oluşturulmalıdır. Oluşturulan workbook için Şekil 2.7.' de görüldüğü gibi, ilgili sorgu çalıştırılır ve harita üzerine yerleştirilecek olan verilerin ayrıştırılma işlemi gerçekleştirilir [2]. Aynı zamanda Şekil 2.7.' de gösterildiği gibi Visualization seçeneği Map yapılarak sorgu sonucunda elde edilen çıktı harita üzerine yerleştirilir.

Failed RDP World Map

law-honeypot

Done Editing Open Settings Advanced Settings Style Advanced Editor

Query (change) Time Range Last 24 hours Visualization Map Size Medium Map Settings

Log Analytics workspace Logs Query

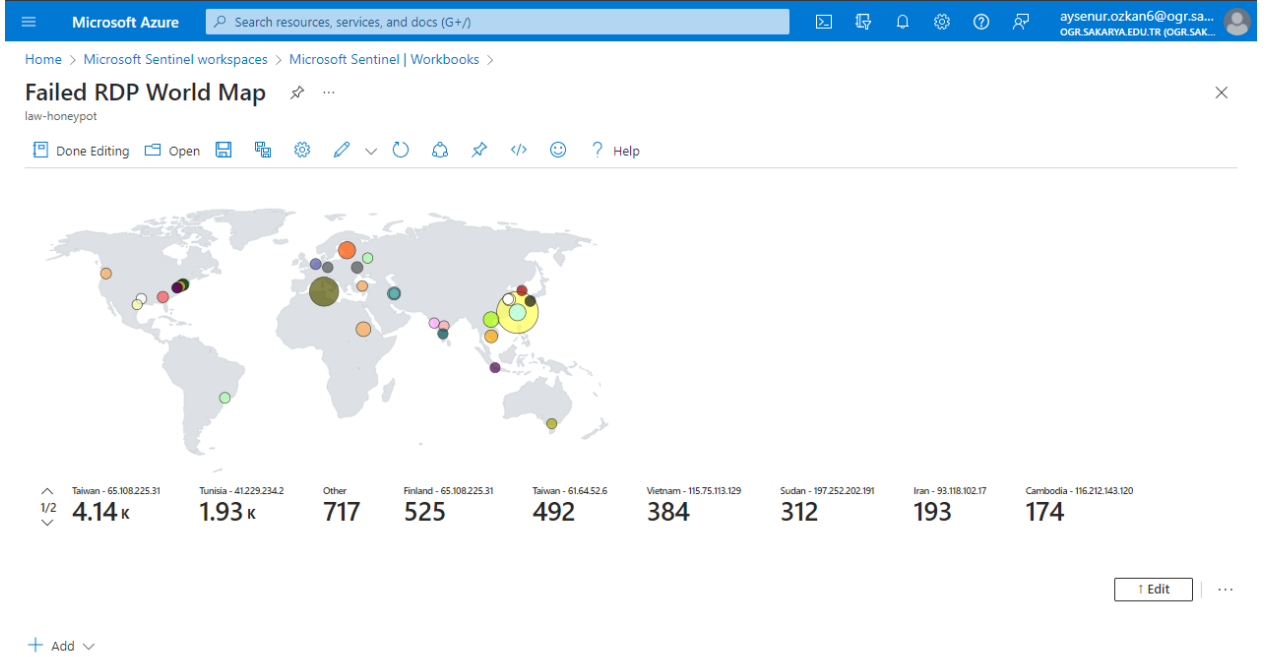
```

FAILED_RDP_WITH_GEO_CL | summarize event_count=count() by sourcehost_CF, latitude_CF, longitude_CF, country_CF, label_CF, destinationhost_CF
| where destinationhost_CF != "samplehost"
| where sourcehost_CF != ""

```

Şekil 2.7. Çalıştırılan Sorgu.

24 saat boyunca Windows10 sanal makineye yapılan hatalı giriş işlemlerini kaydedildi ve oluşan log dosyası harita üzerine yerleştirildi. Çalışma sonucunda elde edilen sonuç Şekil 2.8.' de gösterilmiştir.



Şekil 2.8. Çalışma Sonucu.

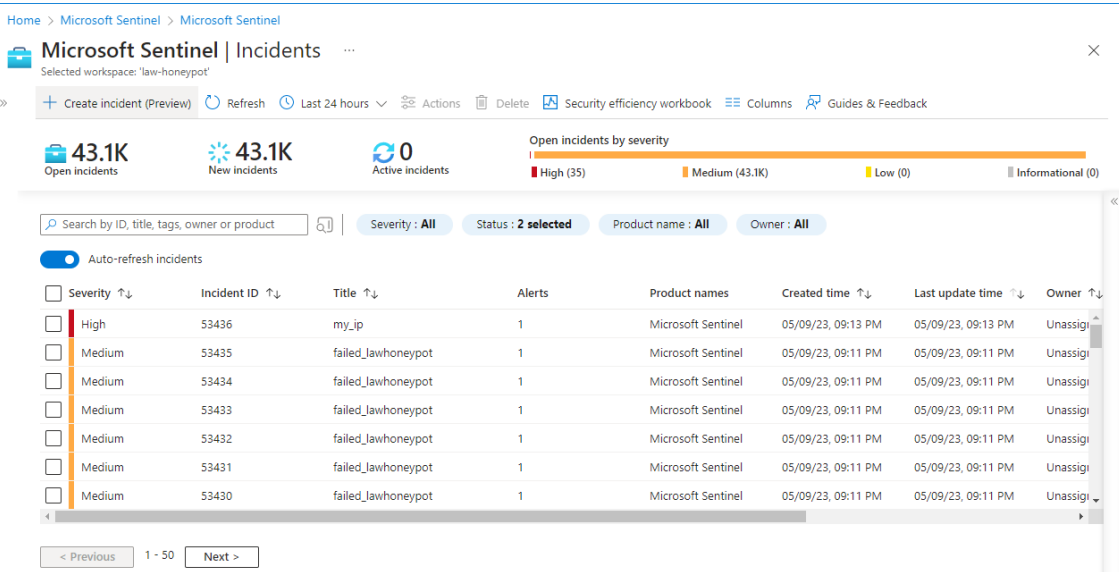
### 3. HATALI GİRİŞ İŞLEMLERİ İÇİN ALARM OLUŞTURMA

#### 3.1. Alarm Nedir

SIEM alarmları, ağ veya sistem içindeki potansiyel güvenlik tehditlerinin veya kötü niyetli faaliyetlerin erken uyarısını sağladığı için güvenlik açısından önemlidir. Bu uyarılar, organizasyonların ciddi zarar veya hasara uğramadan önce güvenlik olaylarını hızlı bir şekilde tespit etmelerine ve yanıtlamalarına olanak tanır. SIEM alarmları, başarısız giriş denemeleri, izinsiz erişim veya şüpheli ağ trafiği gibi anormal faaliyetler tespit edildiğinde oluşturulur. Oluşturulan bu alarmlar, güvenlik ekiplerine gönderilir ve olayın incelenmesi sağlanır.

### 3.2. Tespit Edilen Hatalı Girişler İçin Azure Sentinel ile Alarm Oluşturma

Sisteme hatalı bir giriş yapıldığında Azure Sentinel'in bu hatalı giriş için bir alarm üretmesi sağlanmak isteniyor. Bunu için Microsoft Sentinel/Analytics/Create yolu izlenerek istenilen alarm oluşturulabilir. Bu çalışmada hatalı girişler üzerinde çalışıldığı için oluşturulan alarmda Initial Access ve Valid Accounts seçenekleri aktif edilmiş ve alarm derecesi Medium olarak belirlenmiştir. Alarm kuralları ise, alarm sorgusunu 5 dakikada bir çalıştır ve bir kaynaktan 2'den fazla hatalı giriş yapılırsa alarm üret şeklinde ayarlanmıştır. Yapılan hatalı girişler için sistem tarafından oluşturulan alarmlar Şekil 3.1.'de görülmektedir. Çalışmada kendi ip adresimiz için özel bir alarm kuralı oluşturduk. Sanal makinemize kendi bilgisayarımızın ip adresinden 2' den fazla hatalı giriş işlemi yapıldığında alarm derecesi High olan alarmlar üretilecektir. İlgili durumda üretilen alarmları Şekil 3.1.'de görebiliriz.



Şekil 3.1. Çalışma Sonucunda Üretilen Alarmlar.

## 4. SONUÇ

Çalışmanın birinci aşamasında zafiyetli Windows10 sanal makine üzerinden hatalı giriş olayları toplanmış ve Azure Sentinel ürünü kullanılarak hatalı girişler harita üzerine yerleştirilmiştir. Çalışmanın ikinci aşamasında ise Azure Sentinel ürünü kullanılarak hatalı girişler için alarm oluşturulması sağlanmıştır. Yapılan çalışma ile sisteme gelen saldırıların sebep olabileceği hasarların, erken dönemde engellenmesi amaçlanmıştır.

## KAYNAKÇA

- [1] «Microsoft,» Microsoft, 09 01 2022. [Çevrimiçi]. Available: <https://learn.microsoft.com/en-us/azure/virtual-machines/windows/quick-create-portal>. [Erişildi: 27 04 2023].
- [2] «Microsoft,» 11 02 2023. [Çevrimiçi]. Available: <https://learn.microsoft.com/tr-tr/azure/azure-monitor/logs/log-analytics-overview>. [Erişildi: 28 04 2023].
- [3] M. Huculak, «Windows Central,» 17 05 2022. [Çevrimiçi]. Available: <https://www.windowscentral.com/how-use-event-viewer-windows-10>. [Erişildi: 29 04 2023].
- [4] J. Madakor, «Github,» 01 11 2021. [Çevrimiçi]. Available: [https://github.com/joshmadakor1/Sentinel-Lab/blob/main/Custom\\_Security\\_Log\\_Exporter.ps1](https://github.com/joshmadakor1/Sentinel-Lab/blob/main/Custom_Security_Log_Exporter.ps1). [Erişildi: 29 04 2023].
- [5] T. Roberts, «Youtube,» 08 Şubat 2018. [Çevrimiçi]. Available: <https://www.youtube.com/watch?v=N-aYZ3WDRII&t=664s>. [Erişildi: 30 04 2023].