

Deploying My Own SIEM

In this project I used Microsoft Azure to create my own SIEM. I used Azure because they give you 200 free credits (Which will usually not get you far) but it was plenty for this project.

After I signed in and gave them all my personal information, I began to set up my first virtual machine. I chose to use the windows 10 pro version, named it 2EZVM, and added it to a Resource Group called 2EZVM_Group. This Resource Group acted as the container for everything in this project.

The screenshot shows the Azure portal's 'Virtual machines' blade. At the top, there are navigation links for 'Home >' and 'Virtual machines'. Below that is a 'Default Directory' section. The main area contains a table of VM details. The table has columns for Name, Subscription, Resource group, Location, Status, Operating system, Size, Public IP address, and Disks. One row is visible, showing '2EZVM' as the name, 'Azure subscription 1' as the subscription, '2ezvm_group' as the resource group, 'East US' as the location, 'Running' as the status, 'Windows' as the operating system, 'Standard_B1s' as the size, '40.76.121.146' as the public IP address, and '1' as the number of disks.

Name	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disks
2EZVM	Azure subscription 1	2ezvm_group	East US	Running	Windows	Standard_B1s	40.76.121.146	1

In this project, I allowed the RDP port 3389 to be public because it's very easy to get traffic on this port. This increased the volume of attempted connections which allowed me to detect more security events later in the project.

Next I began to set up a log analytics workspace called 2EZ-LogAnalytics.

The screenshot shows the Azure portal's 'Microsoft Sentinel' blade. At the top, there are navigation links for 'Home >' and 'Microsoft Sentinel'. Below that is a 'Default Directory' section. The main area contains a table of Log Analytics workspace details. The table has columns for Name, Resource group, Location, and Subscription. One row is visible, showing '2EZ-LogAnalytics' as the name, '2ezvm_group' as the resource group, 'East US' as the location, and 'Azure subscription 1' as the subscription.

Name	Resource group	Location	Subscription
2EZ-LogAnalytics	2ezvm_group	East US	Azure subscription 1

I added 2EZ-LogAnalytics to the resource group that 2EZVM was placed in. (2EZVM_Group)

Next, I went back to the VM workspace and navigated to the network settings panel to see if the VM was public facing and receiving traffic. And BOOM! I was already receiving hits on the RDP port.

2EZVM1 | Network settings

Network interface : 2ezvm1921_z2
Virtual network / subnet : 2EZVM1-net / default
Public IP address : 40.76.121.146
Private IP address : 10.0.0.4
Admin security rules : 0 (Configure)

Load balancers : 0 (Configure)
Application security groups : 0 (Configure)
Network security group : 2EZVM1-nsg
Accelerated networking : Disabled
Effective security rules : 0

Rules

Priority	Name	Port	Protocol	Source	Destination	Action
300	RDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInbound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInbound	Any	Any	Any	Any	Deny

After checking this, I added Microsoft sentinel to my LogAnalytics workspace.

Microsoft Sentinel | Overview (Preview)

Selected workspace: '2ez-loganalytics'

Incidents (0)
Last 24 hours (0)
No incidents found
See incidents page for further information
[Incidents](#)

Automation
Last 24 hours (0)
No automation rules found
Add automation rules to centrally manage automation of incident handling and response
[Automation](#)

Data
Last 24 hours (0)
[Data](#)

Analytics
Current status (0)
2 Analytics rules
0 Disabled
0 Auto disabled
2 Enabled
[Analytics](#)

Next, I headed back to the LogAnalytics workspace (2EZ-LogAnalytics) to add the VM's event logs and send them to the Sentinel instance.

To do this I went to the Data connectors tab. In the image below I have already installed the *Windows security events via AMA* and *Security Events via legacy agent*. We will use the

Windows security events AMA because the other option is being phased out.

The screenshot shows the Microsoft Sentinel Data connectors page. At the top, there are navigation links for General, Threat management, Content management, and Configuration. A workspace manager (Preview) link is also present. Below the navigation is a search bar, refresh button, and guides & feedback link. Two status indicators are shown: '2 Connectors' and '2 Connected'. A message states: 'Data Connector with "content source = gallery content" have been removed. All the removed content and more is available in content hub. Click here to reinstate in use.' Another message says: 'Device specific AMA connectors have been deprecated. Learn more >'. The main area displays a table of data connectors. The table has columns for Status, Connector name, and a three-dot ellipsis column. Two entries are listed:

Status	Connector name	
Connected	Security Events via Legacy Agent Microsoft	...
Connected	Windows Security Events via AMA Microsoft	...

The image below shows the UI after you click into the content hub to find the tool you're looking to install.

Content hub ...

The screenshot shows the Content hub interface. At the top, there are buttons for Refresh, Install/Update, Delete, SIEM Migration, and Guides & Feedback. Key statistics are displayed: 374 Solutions, 307 Standalone contents, 1 Installed, and 0 Updates. A search bar contains 'azure monitor agent'. Below the search bar are filters for Status: All, Content type: Data connector (289), Support: All, Provider: All, Category: All, and Content sources: All. The main area is a table listing data connectors. One entry is highlighted: 'Windows Security Events' with a green checkmark indicating it is installed. Other entries show various providers like Microsoft, Delinea, and RidgeSecurity, and categories like IT Operations, Security - Threat Protection, and Networking.

Content title	Status	Content source	Provider	Support	Category	Content type
Common Event Format	Not installed	Solution	Microsoft	Microsoft	IT Operations	Data connector (2) Workbook
Delinea Secret Server Azure Monitor...	Not installed	Solution	Delinea	Delinea	Security - Threat Protection	Data connector Workbook
Fortinet FortiWeb Cloud WAF-as-a-S...	Not installed	Solution	Microsoft	Microsoft	Security - Automation (SOAR)	Analytics rule Data connector +4
Ridge Security RidgeBot	Not installed	Solution	RidgeSecurity	RidgeSecurity	Security - Vulnerability Management	Analytics rule (2) Data connector
Syslog	Not installed	Solution	Microsoft	Microsoft	IT Operations	Analytics rule (7) Data connector +3
Windows Firewall	Not installed	Solution	Microsoft	Microsoft	Security - Network	Data connector (2) Workbook
Windows Forwarded Events	Not installed	Solution	Microsoft	Microsoft	IT Operations	Analytics rule (2) Data connector
Windows Security Events	Installed	Solution	Microsoft	Microsoft	Security - Threat Protection	Analytics rule (20) Data connector (2) +2
Windows Server DNS	Not installed	Solution	Microsoft	Microsoft	Networking	Analytics rule (5) Data connector (2) +2

After this was installed, I created a new data collection rule seen below within *Windows security events AMA*. I then added a rule name and the resource group for the data collection rule. In the resources tab I selected the 2EZVM which also selected the group and subscription for me.

I also

Edit Data Collection Rule

Data collection rule management

Basic Resources Collect Review + create

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

Rule details

Rule name

WindowsEventstoSentinel

Subscription

Azure subscription 1

Resource group

2EZVM_Group

I also created a rule in the collect portion of the data collection rule to return all security events. After this I began receiving logs.

Next I wanted to create a Sentinel rule to detect successful login attempts via RDP from users that we're not a system account.

For this I navigated to the Logs tab in the sentinel workspace and created a new security incident query seen below.

```
Run Time range : Last 24 hours Save Share New alert rule Export Pin to Format query ...
1 SecurityEvent
2 | where Activity contains "success" and Account !contains "system"
```

After this, I went to the analytics window to see my new rule. You can see in the image below my rule is the medium level incident.

Active rules

Severity	Name	Rule t...	Status	Tactics	Techniques	Sub techniques	Source name	Last modified
<input checked="" type="checkbox"/> Medium	Successful_Loca...	Scl	Enabled	Initial Access			Custom Content	1/9/2025, 4:38...
<input type="checkbox"/> High	Advanced Multi...	Fu:	Enabled	Collection +11			Gallery Content	1/9/2025, 3:57...

Successful_Local_Sign_In

Info

ID: ccd8b65-2120-4a4b-935e-e419826cd63a

Description: Logs of successful log in attempts over the past 24 hours that are not from system.

MITRE ATT&CK: Initial Access

Rule query:

```
SecurityEvent
| where Activity contains "success" and Account !contains "Local System"
| where TimeGenerated > ago(24h)
```

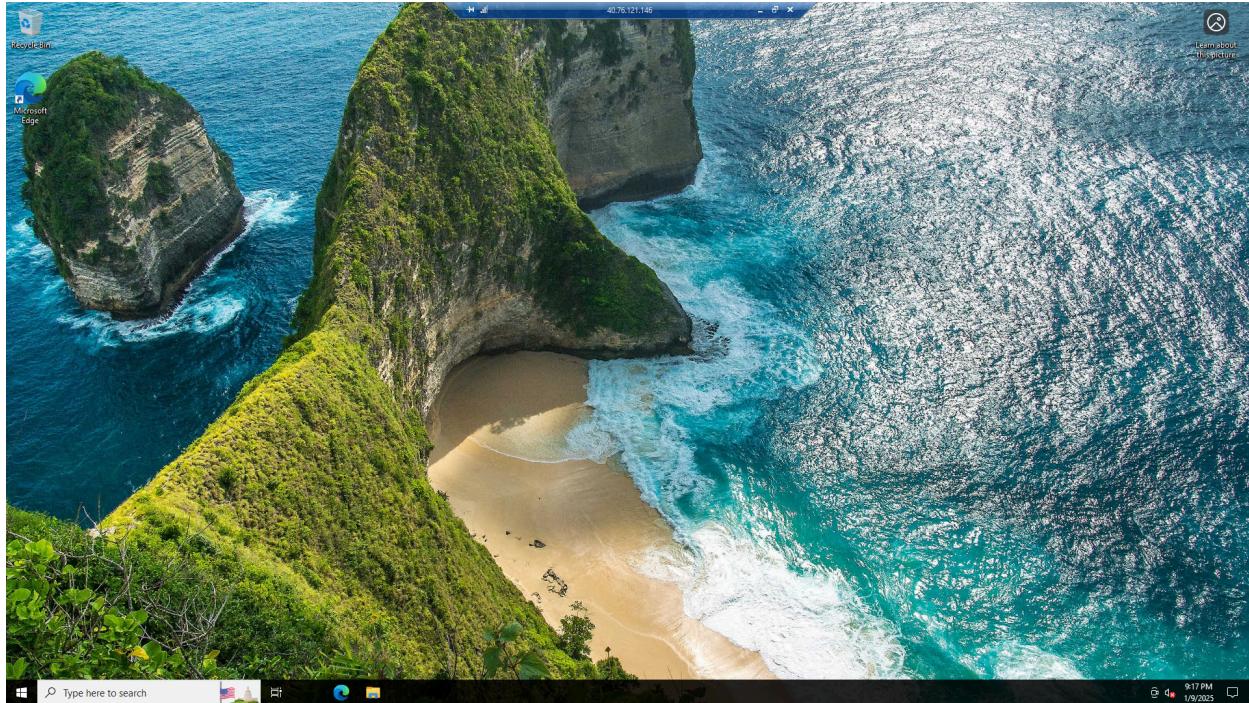
Rule frequency: Run query every 5 minutes

Rule period: Last 5 hours data

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

Insights

This was set to run every 5 minutes so I went to log in myself to test the rule. Below is me logged into the VM successfully.



To check if this triggered an alert for my rule, I then went to the incidents page within sentinel and boom, the alert was there.

Home > Microsoft Sentinel

Microsoft Sentinel | Incidents

Selected workspace: 'zez-loganalytics'

Search << + Create incident (Preview) Refresh Last 24 hours Actions Delete Security efficiency workbook Columns Guides & Feedback

General Threat management Incidents Workbooks Hunting Notebooks Entity behavior Threat intelligence MITRE ATT&CK (Preview) SOC optimization Content management

Open incidents: 1
New incidents: 1
Active incidents: 0

Open incidents by severity:

Severity	Count
High (0)	0
Medium (1)	1
Low (0)	0
Informational (0)	0

Auto-refresh incidents:

Search by ID, title, tags, owner or product:

Severity: All Status: 2 selected Incident Provider name: All Alert product name: All Owner: All

Severity	Incident number	Title	Alerts	Incident provider na...	Alert product name	Created time	Last update
Medium	1	Successful_Local_Sign_Ins	1	Azure Sentinel	Microsoft Sentinel	01/09/25, 04:38 PM	01/09/25, 04

This project gave me plenty of insight into how to set up not only a virtual machine, but also how to use the tools within Azure to monitor activity on an endpoint. In the future, I plan to do more projects like this to extend my knowledge of this ecosystem. Unfortunately, this will cost money as my free trial will run out of credits soon. So if you'd like to see more projects like this please hire me!