Shaddy Elhamad 11/3/2024

How I built a Honeypot VM, using Azure Sentinel to Track Malicious RDP Connections

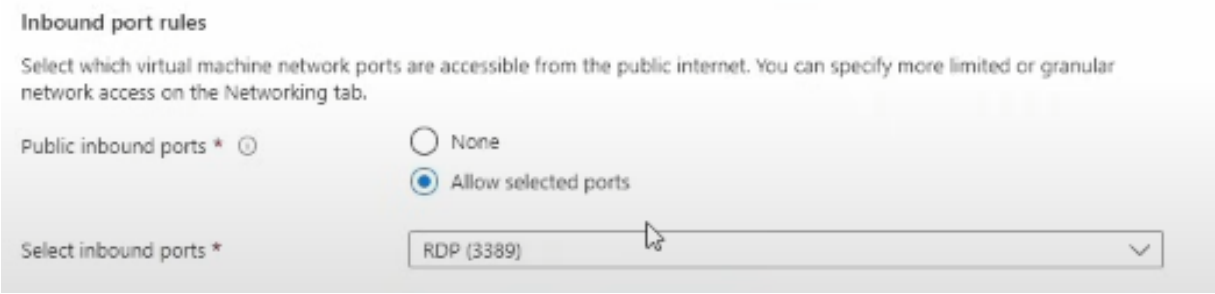
Lately, I've been diving into Azure Sentinel and learning how to use it to strengthen cybersecurity defenses. One project that allowed me to apply my skills in log analysis and cloud security was setting up a honeypot using an Azure Virtual Machine with an exposed RDP port to see who would try to break in. The process involved a combination of configuring **Azure Sentinel**, setting up a **Log Analytics Workspace**, and using **Kusto Query Language (KQL)** to dig into the logs. Here's how I got it all working.

Why a Honeypot?

Honeypots are interesting because they attract malicious activity in a controlled, deceptive way, allowing you to observe and analyze real attacks. Remote Desktop Protocol (RDP) is a very important port that allows people to have remote access to your computer over the internet, so for this project, I wanted to track potential brute-force RDP attacks from high-risk regions like China and Russia. The goal was to log these attempts and automate alerts using Azure Sentinel for real-time monitoring.

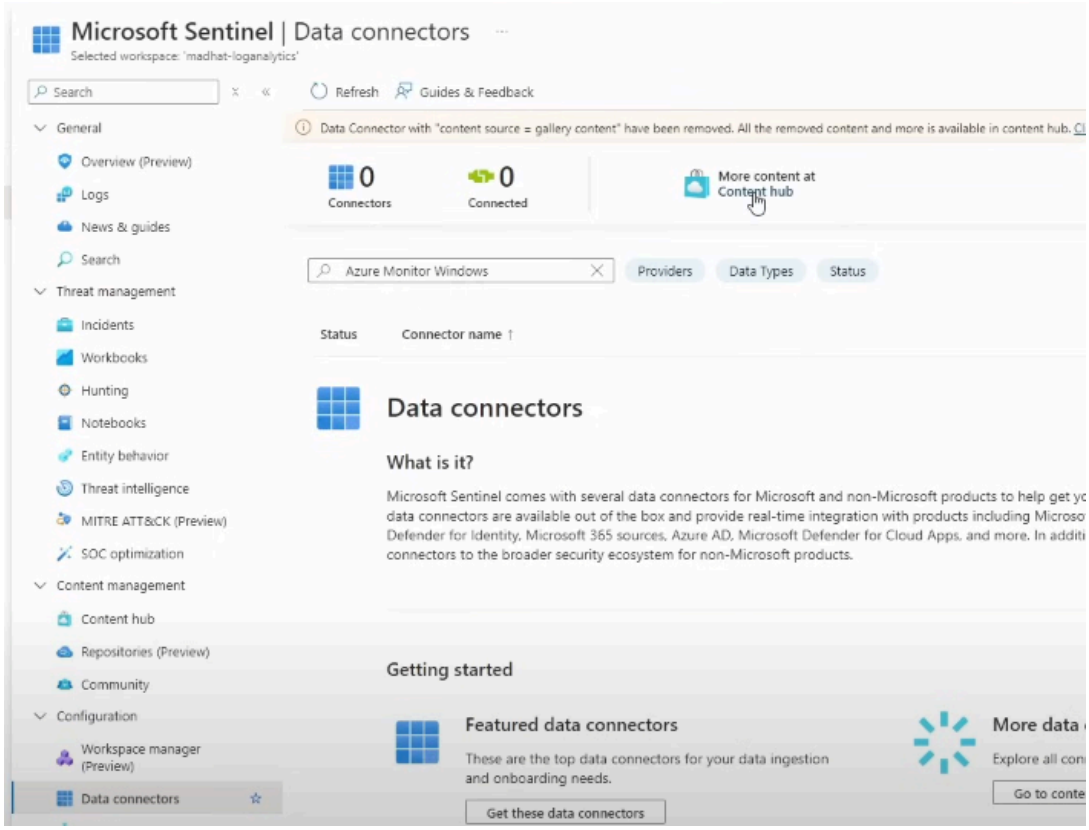
Setting Up the Azure Virtual Machine

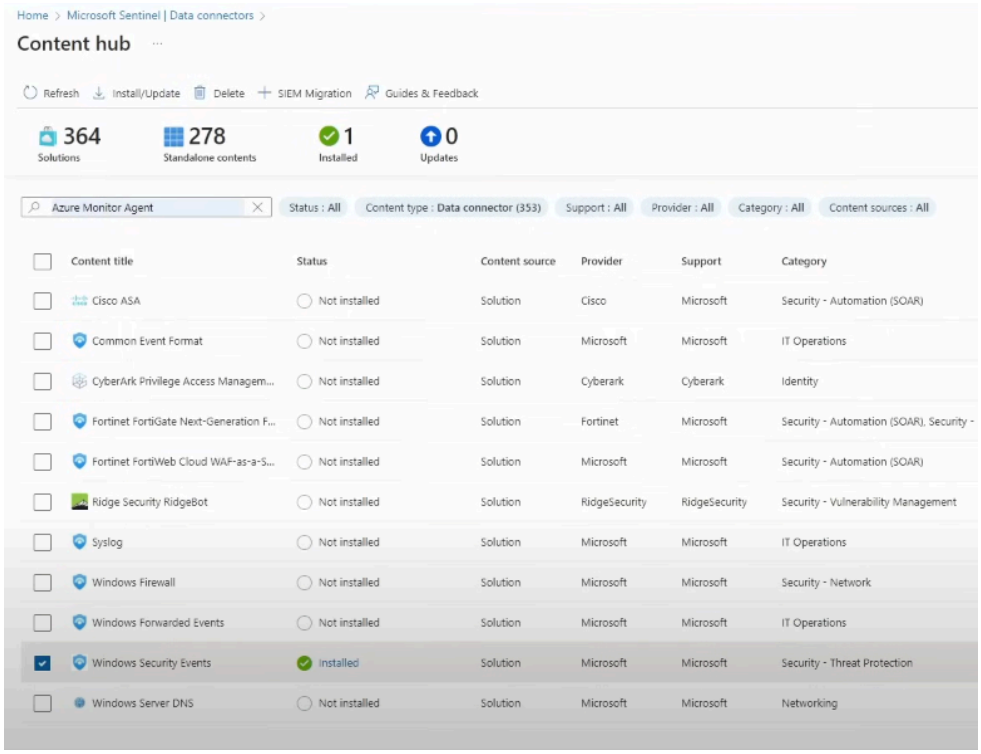
First things first, I created a virtual machine in Azure. I opted for Windows Server because I wanted to target RDP, which is pretty common in real-world attacks. After setting it up, I made sure to open **Port 3389** (RDP) in the **Networking** section. This is risky in the real world, but perfect for this project since it exposes the VM to potential attackers. Port 3389 is essentially a signal flare to every bot in the universe that dinner is ready.



Integrating Log Analytics

Next, I had to make sure all the incoming RDP attempts would be logged and sent to a central platform. I created a **Log Analytics Workspace** in Azure, which serves as the backbone for logging and analyzing the data after the Windows VM logs its data as it usually does. Then, I added a data connector to the VM to push the logs to the workspace. This is where all the connection data from incoming RDP attempts would end up for analysis. We then go to More content at Content Hub and install the Windows Security Events into our Sentinel's data connector.


Microsoft Sentinel | Data connectors
Selected workspace: 'madhat-loganalytics'
Search
Refresh
Guides & Feedback
General
Overview (Preview)
Logs
News & guides
Search
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence
MITRE ATT&CK (Preview)
SOC optimization
Content management
Content hub
Repositories (Preview)
Community
Configuration
Workspace manager (Preview)
Data connectors
Data Connector with "content source = gallery content" have been removed. All the removed content and more is available in content hub.
0
Connectors
0
Connected
More content at Content hub
Azure Monitor Windows
Providers
Data Types
Status
Status
Connector name
Data connectors
What is it?
Microsoft Sentinel comes with several data connectors for Microsoft and non-Microsoft products to help get yo
data connectors are available out of the box and provide real-time integration with products including Microso
Defender for Identity, Microsoft 365 sources, Azure AD, Microsoft Defender for Cloud Apps, and more. In additi
connectors to the broader security ecosystem for non-Microsoft products.
Getting started
Featured data connectors
These are the top data connectors for your data ingestion and onboarding needs.
Get these data connectors
More data
Explore all con
Go to conte


Home > Microsoft Sentinel | Data connectors >
Content hub
Refresh
Install/Update
Delete
SIEM Migration
Guides & Feedback
364
Solutions
278
Standalone contents
1
Installed
0
Updates
Azure Monitor Agent
Status : All
Content type : Data connector (353)
Support : All
Provider : All
Category : All
Content sources : All
Content title
Status
Content source
Provider
Support
Category
Cisco ASA
Not installed
Solution
Cisco
Microsoft
Security - Automation (SOAR)
Common Event Format
Not installed
Solution
Microsoft
Microsoft
IT Operations
CyberArk Privilege Access Managem...
Not installed
Solution
Cyberark
Cyberark
Identity
Fortinet FortiGate Next-Generation F...
Not installed
Solution
Fortinet
Microsoft
Security - Automation (SOAR), Security -
Fortinet FortiWeb Cloud WAF-as-a-S...
Not installed
Solution
Microsoft
Microsoft
Security - Automation (SOAR)
Ridge Security RidgeBot
Not installed
Solution
RidgeSecurity
RidgeSecurity
Security - Vulnerability Management
Syslog
Not installed
Solution
Microsoft
Microsoft
IT Operations
Windows Firewall
Not installed
Solution
Microsoft
Microsoft
Security - Network
Windows Forwarded Events
Not installed
Solution
Microsoft
Microsoft
IT Operations
Windows Security Events
Installed
Solution
Microsoft
Microsoft
Security - Threat Protection
Windows Server DNS
Not installed
Solution
Microsoft
Microsoft
Networking

Windows Security Events via AMA

Windows Security Events via AMA (Azure Monitor Agent) refers to the process of collecting security event logs from Windows machines (such as virtual machines) using the AMA. AMA is the modern agent used by Azure to collect monitoring data from machines, replacing the older legacy Log Analytics agent.

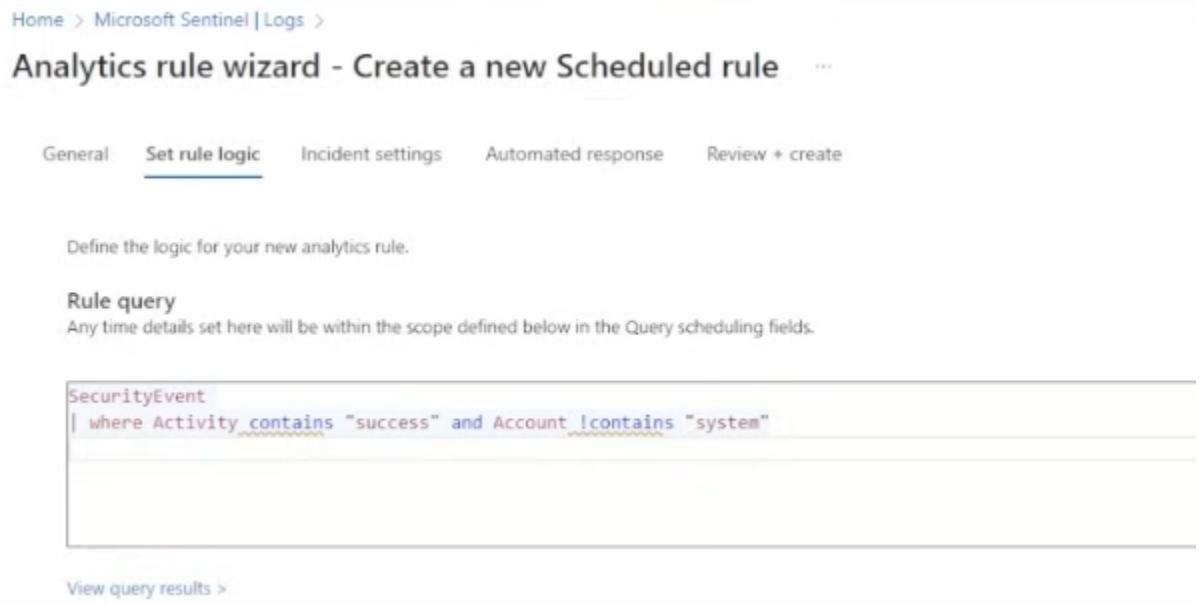
We want to click on that data connector and click **“open connector page”** and create a data collection rule called **“WindowsEventsToSentinel”**. We will then click resources and select our VM. Then, we want to select all security events. After that data collection rule is created then we will soon see logs being collected and ingested into our Microsoft Sentinel.

Creating Rules

Windows Security Events are logs generated by the Windows Security system. These include important security related events like login attempts, account changes, privilege use, and access control changes. Examples of these event types include:

Event ID 4624: Successful login
Event ID 4625: Failed login
Event ID 4672: Special privileges assigned to a new logon

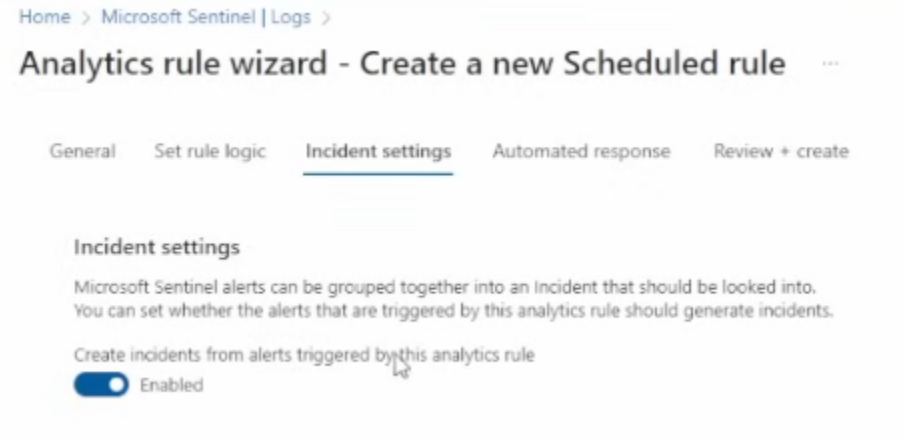
You can make rules based on various parameters such as ID’s that match certain conditions but we will start off by creating a SecurityEvent rule that detects any activity that is successful, BUT, the account can’t be from the system itself. Therefore, alerting us when any incoming successful RDP connections occur.



We then want to go to “New Alert Rule” and create a sentinel rule called “Sucessful Local Sign Ins”, describing the rule we just created. You can go down further into the settings and establish Alert thresholds, defining how many events it would require for an alert to go off, as well as

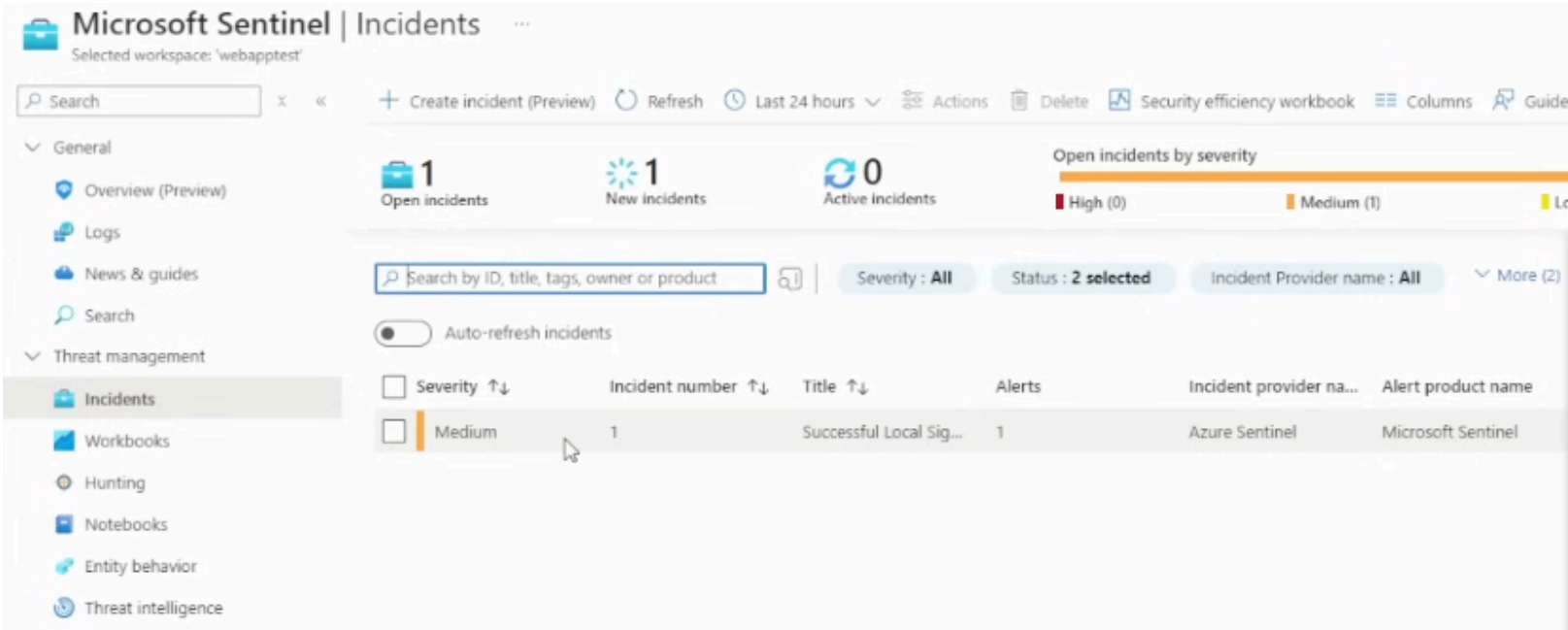
Query Scheduling which would run our query every X minutes, either automatically or at specific times.

Lastly, we want to make sure Microsoft Sentinel alerts can be grouped into an incident that can be looked into, so you want to enable **“Create incidents from alerts triggered by the analytics rule”** .



Testing

Now that we have the rules created, and the data connectors established between the VM and the Log Analytics workspace, our honeypot VM with an exposed RDP port is ready to be tested. I went on to sign in to the VM via RDP and lo and behold, an alert appeared on our Microsoft Sentinel Incidents dashboard.



Lessons Learned

This project gave me excellent hands-on experience with several key cybersecurity tools and techniques. I got to create an isolated honeypot VM in Azure to analyze malicious traffic through the use of a SIEM, connecting cloud services such as **Azure Sentinel** and **Log Analytics Workspace** with the use of a data connector agent. These are critical skills in the field of cybersecurity. Plus, setting up the honeypot and watching live attacks unfold was quite interesting. It's one thing to read about cybersecurity threats, but seeing attackers actively trying to break into your system takes it to another level.

It also reinforced the importance of monitoring and alerting in real time. The automated alerts in Sentinel are a game changer for detecting and responding to threats. And the best part is that this setup can be easily scaled or modified for other attack vectors due to Azure's elasticity.

Final Thoughts

Building this project was a great way to strengthen my Azure security skills and get some practical experience with real-world attacks. If you're looking to build out your cybersecurity toolkit, I'd highly recommend trying something similar. It's a great way to understand how attackers operate and how tools like Azure Sentinel can help you stay one step ahead.

I'm already thinking about my next project, maybe expanding the honeypot with different types of services or logging more advanced attack methods. Well see…