Microsoft

Azure Sentinel 'Security Rockstar' Hands On Lab

Roll up 'em sleeves…

Yaniv Shasha @oldShasha
Program Manager Azure Sentinel

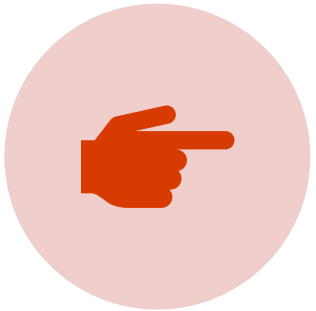
Goal

After this lab you'll be able to:

- Recognize Azure Sentinel's high-level features
- Leverage Workbooks to gain more insights into your environment
- Understand the KQL, Analytics, and Incidents relationship
- Use Azure Sentinel to pivot on multiple data sources to triage a real-world Incident
- Have the resources and tools to continue your journey with Azure Sentinel

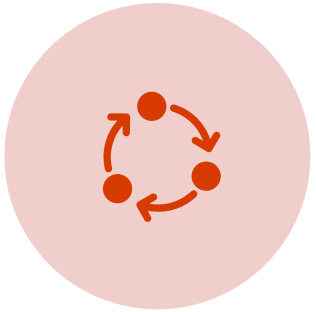
Lab Exercises

Exercise 1: Review Data Connectors



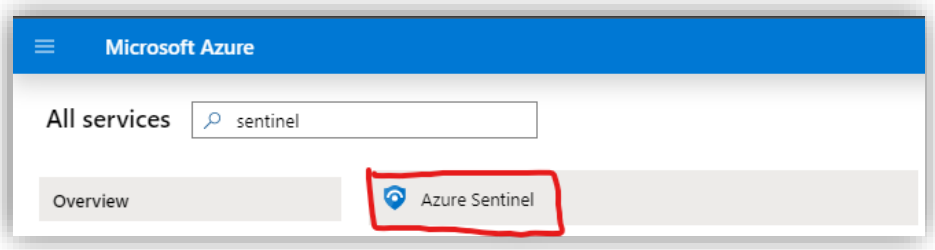
Exercise 2: Setup Analytics and Respond to Incidents

Exercise 3: Rich investigation with Azure Sentinel Workbooks



Exercise 4: Proactively Investigate Potential Threats, Misconfigurations, and Suspicious Activities

Getting started with the lab



Head over to *portal.azure.com*

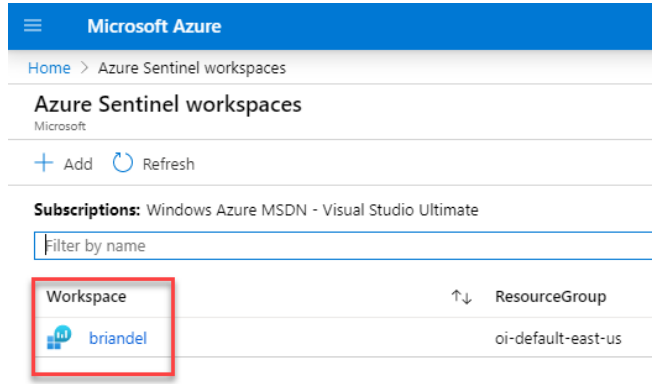
Account: AdminXXXX@sentinellab.xyz

standardXXX@sentinellab.xyz where "XXXX" is the number assigned to you

For example, if I was assigned number 4457, my username would be Admin447@sentinellab.xyz

Username: AdminXX@sentinellab.xyz
Password: SentinelL@b!

In the new Azure, go to "All Services", type in "Sentinel" and select it.



Select the workspace, which all our SOC data is already sending data to:

Lab Walkthrough

Head over to aka.ms/LabsSentinel