



Azure Sentinel 'Security Rockstar' Hands On Lab

Roll up 'em sleeves...



Goal

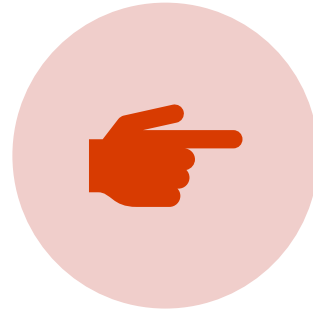
After this lab you'll be able to:

- 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



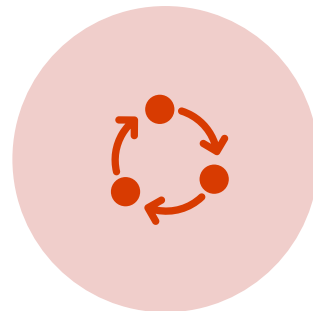
Exercise 1: Review Data Connectors



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

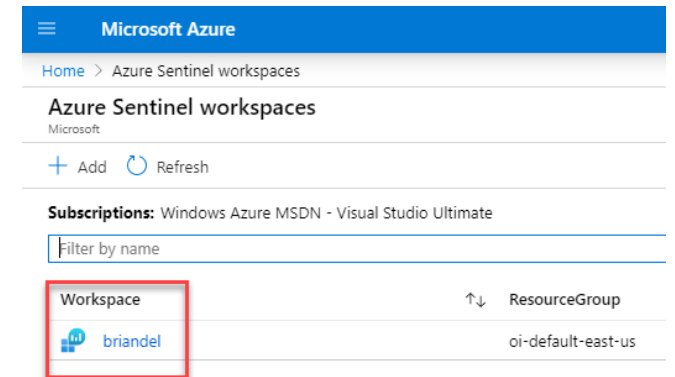
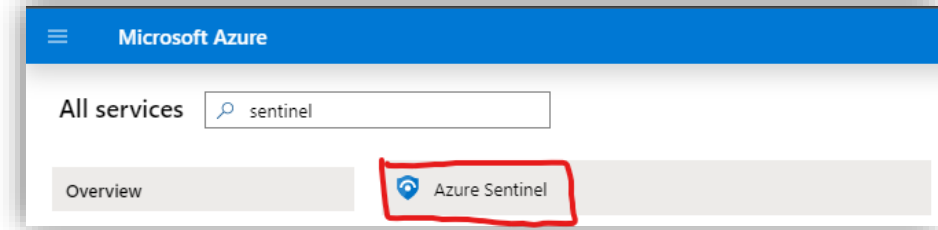
For example, if I was assigned number 4457, my username would be Admin447@sentinellab.xyz

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

The screenshot shows a GitHub repository page for 'Sentinel' by 'Yaniv-Shasha'. The repository has 3 watches, 11 stars, and 5 forks. The 'Code' tab is selected, showing a file tree with folders 'LAB01', 'LAB02', 'LAB03', 'LAB04', and a file 'README.MD'. The 'README.MD' file is open, displaying an 'Introduction' section with 'Objectives' and 'Prerequisites'.

Yaniv-Shasha / Sentinel

Watch 3 Star 11 Fork 5

Code Issues 0 Pull requests 0 Actions Projects 0 Security 0 Insights

Branch: master Sentinel / Labs / Create new file Find file History

Yaniv-Shasha Update README.MD Latest commit c371210 on Sep 11, 2019

LAB01	commit	8 months ago
LAB02	Update README.MD	7 months ago
LAB03	Update README.MD	8 months ago
LAB04	Update README.MD	7 months ago
README.MD	order	8 months ago

README.MD

Introduction

Objectives:

After completing this lab, you will be able to:

- Deploy Azure Sentinel as a platform for visualizing, investigating, and alerting on your customer's security big data
- Confidently use Sentinel to render your customer's visualized data truly actionable
- Respond to security incidents and Indicators of Compromise discovered with Sentinel
- Proactively hunt for misconfigurations and Indicators of Compromise with hunting queries

Prerequisites:

Before working on this lab, the following helps:

- Working knowledge of SIEM and SOAR technology
- Familiarity with common attack scenarios and techniques
- Familiarity with Azure Playbooks and automation