📙 Security Insight CyberLab Deployment Guide

🌍 About

Security Insight CyberLab is designed with security analysts in mind. It is easy to use and provides a seamless experience for writing custom analytics and SOAR playbooks for Microsoft Sentinel. With this tool, you can create custom analytics for various use cases such as insider threat detection, network security monitoring, and cloud security. You can also write analytics for compliance and regulatory requirements and playbooks for SOAR.

CyberLab can also be used for training and learning Microsoft Sentinel and the common tools used by security analysis and researchers.

CyberLab enables the deployment of the following into a new Resource Group within Azure.

- Microsoft Sentinel
  - Deployed and configured with data connectors to accept the logging events from lab assets.
  - Default deployment with no Security Insight (custom) analytics
- Windows Domain and Workstations
  - A fully configured Windows Domain environment designed to simulate a typical organisation.
  - Use Azure Bastion to connect.
  - Microsoft Sentinel data collection rules and connectors, and the Azure Monitoring Agent (AMA) pre-configured to capture logs from Windows domain assets
  - Symon pre-installed for enhanced logging.
  - Use the following Log Query for Sysmon logs

```
WindowsEvent
| where Provider == 'Microsoft-Windows-Sysmon'
| limit 100
```

- Kali Linux
  - Execute real-world attacks and techniques against lab assets and view the activity in Microsoft Sentinel.
  - Use Azure Bastion to connect.
- Atomic Red Team
  - Simulate adversarial activity using targeted tests that map directly to the MITRE ATT&CK Framework.
  - Use Azure Bastion to connect.

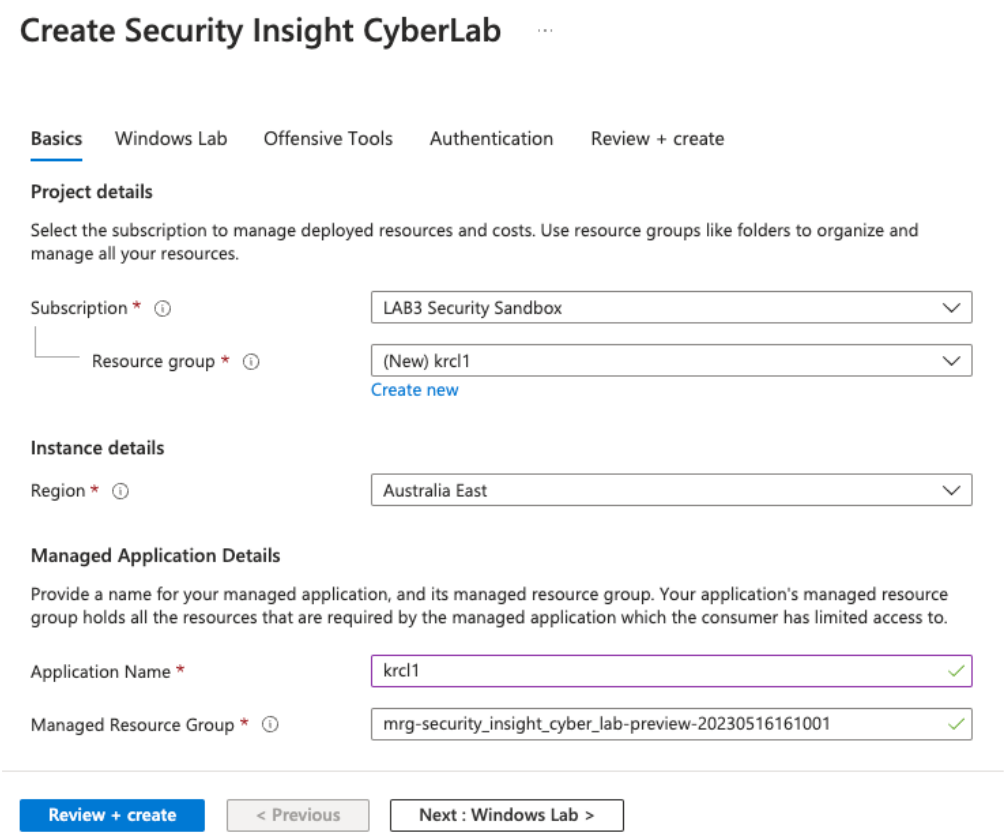
> We do not support or provide instructions for using the included toolsets or for developing custom analytics for Microsoft Sentinel.
>
> Support and documentation is limited to the deployment of Security Insight CyberLab only.

📘 Deploy Security Insight CyberLab from the Azure Marketplace

From the Marketplace search for **Security Insight Cyber Lab** and click on ***Create***

1. Complete the ***Basics*** and click ***Next : Windows Lab >***

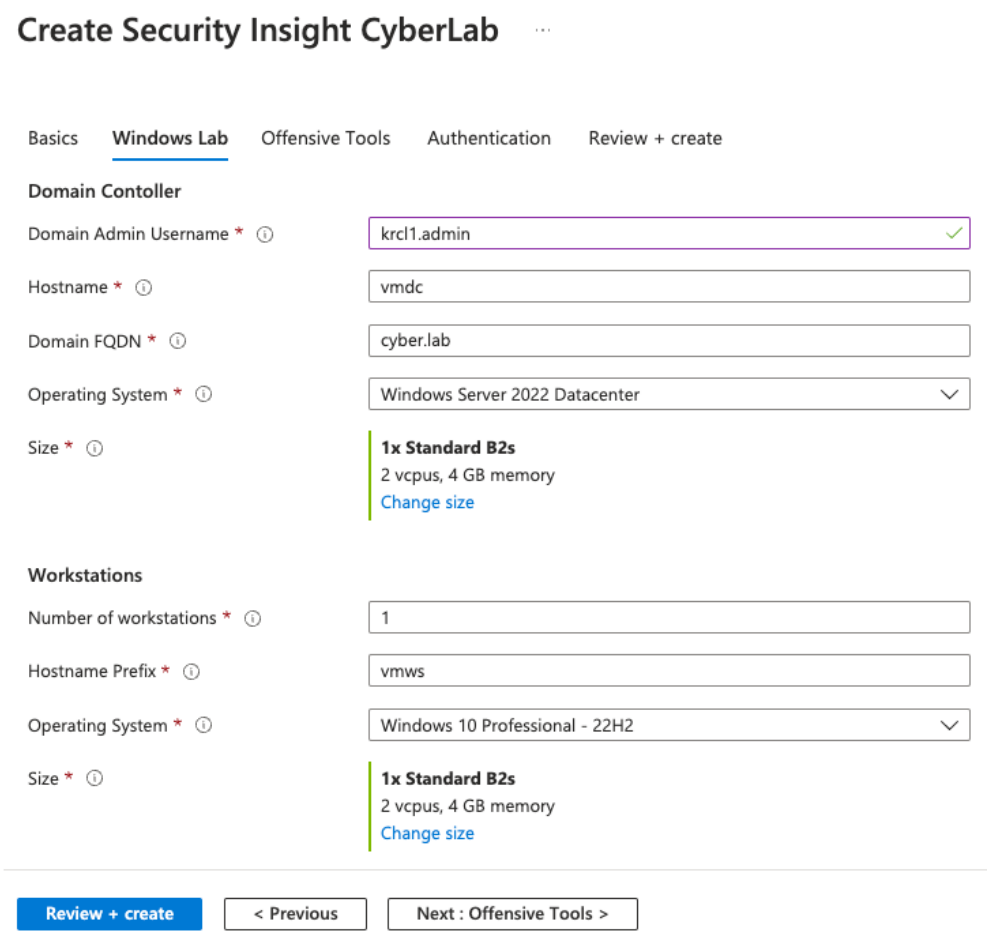
Certain Regions such as Australia Southeast may result in Size not available restrictions when trying to select VM sizes in subsequent screens. If this occurs, select a different region under ***Instance details*** in the ***Basics*** tab.



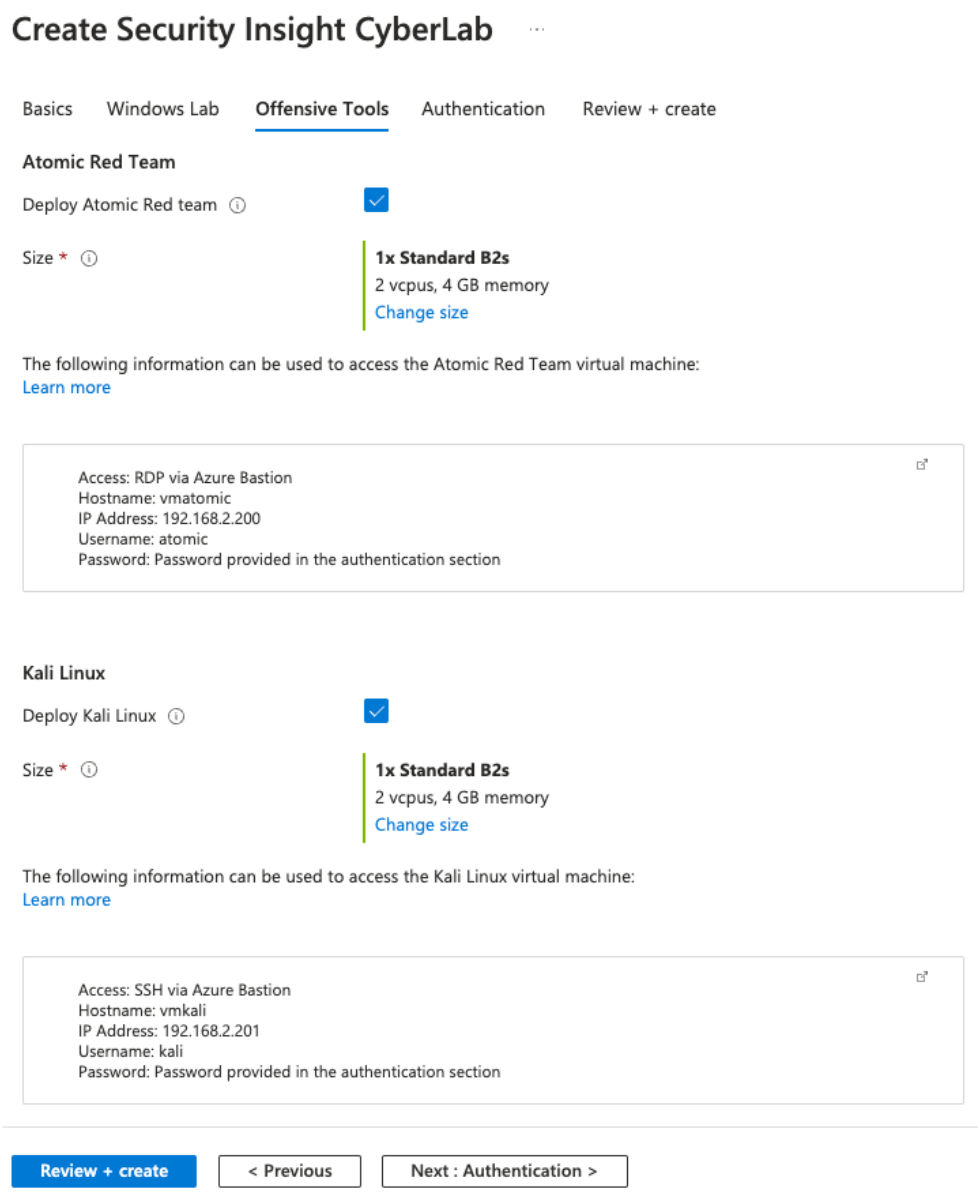
2. Under ***Domain Controller, Domain Admin Username*** enter a username and be sure to take note of the username to be able to login post deployment. Make any changes required, or accept the defaults. Click ***Next : Offensive Tools >***

Ensure that the VM hostnames are unique within the subscription, otherwise the deployment will fail.

Make sure to note the username so that you can log in.

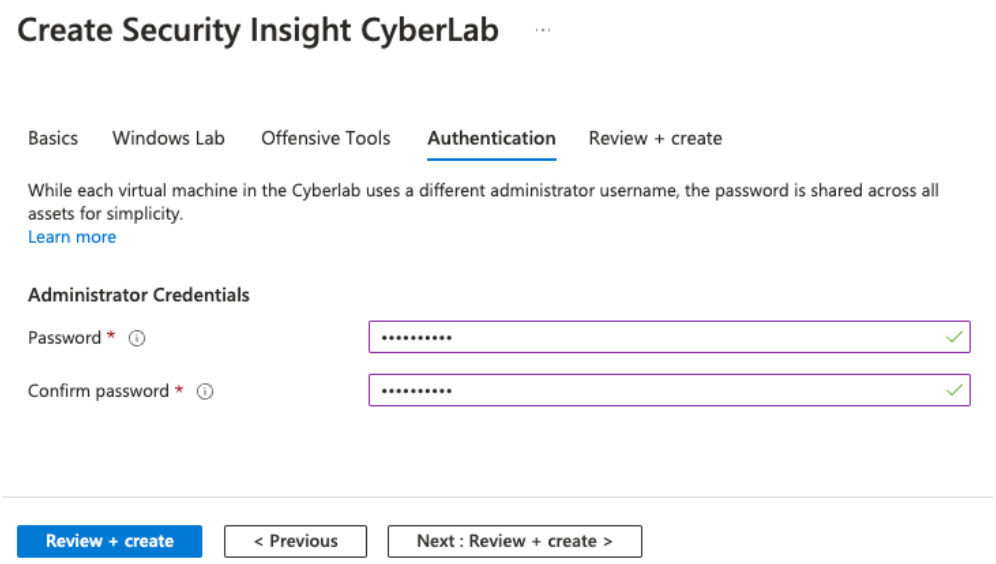


3. Under ***Offensive Tools*** either customise the settings or accept the defaults and then click ***Next : Authentication >***

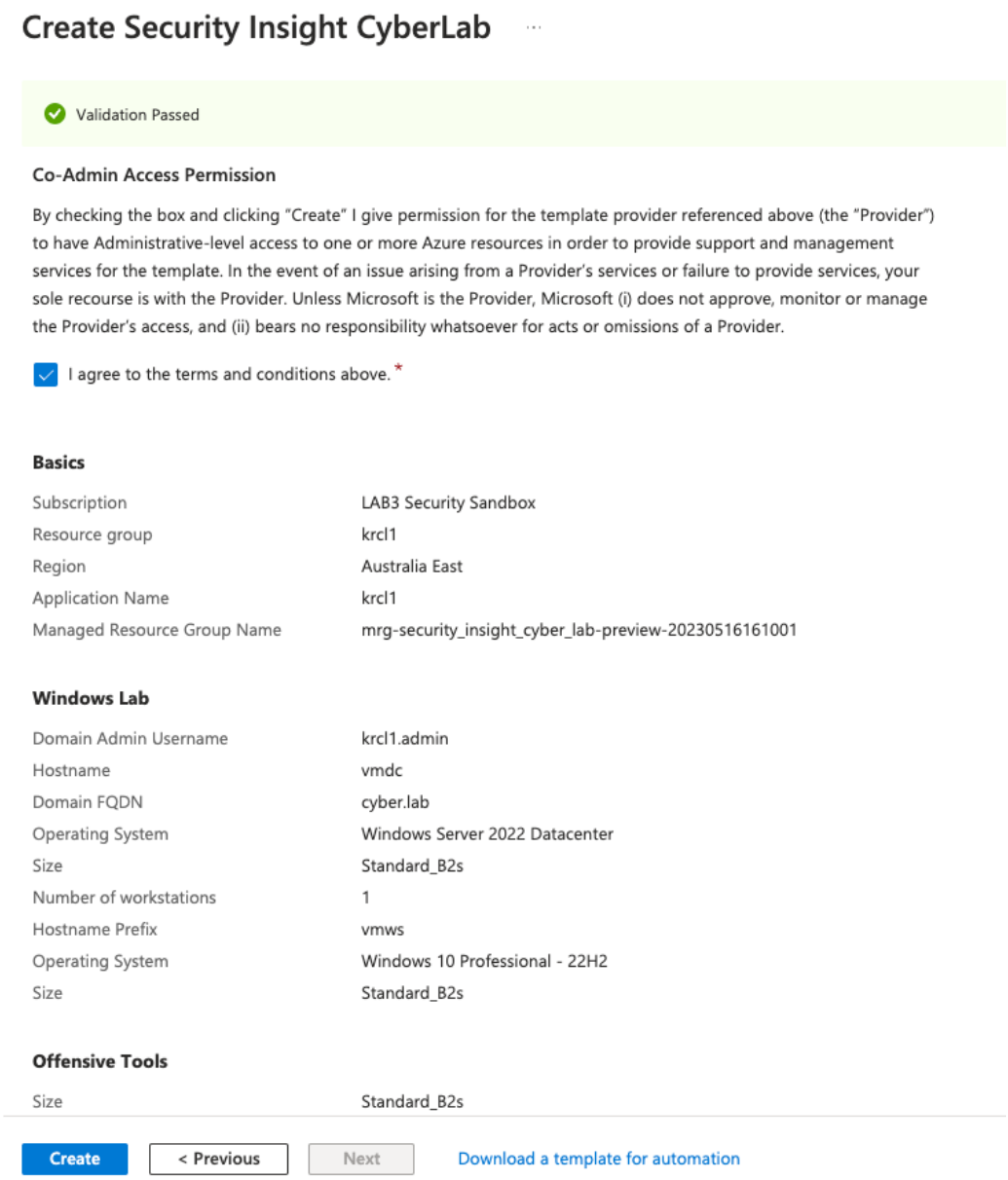


4. Under ***Authentication*** set an Administrator password to be able to log in to each tool. Click ***Next : Review + create >***

⚠ Note or remember the password or passphrase that you set so that you can log in.

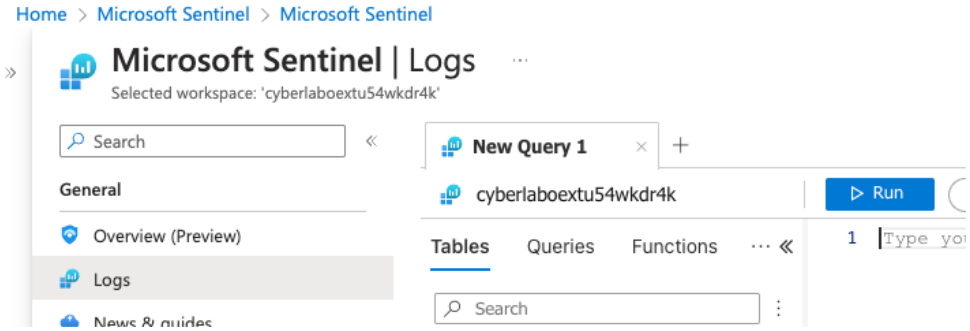


6. Review the configuration and check the ***Co-Admin Access Permission*** then click ***Create*** to start the deployment.



7. The deployment will take between 30 minutes to an hour to complete.

8. Once the deployment is completed you can access the Sentinel deployment. Look for the Sentinel instance starting with cyberlab within a resource group that starts with the marketplace offer name and ends with the deployment date.



9. Each VM (toolsets) can be accessed using Azure Bastion from the managed resource group within the resource group created in ***Basics*** as part of the deployment.

10. When finished to remove all resources simply delete the Resource Group created under ***Basics*** as part of the deployment.

> CyberLab is designed to be instantiated and destroyed on an as needed basis. If you wish to keep CyberLab over a period of time then you can also shutdown the VM's or set to auto-shutdown to save on Azure compute costs.

Further Information

Create custom analytics rules to detect threats with Microsoft Sentinel

Learn how to create custom analytics rules to detect security threats with Microsoft Sentinel. Take advantage of event grouping, alert grouping, and alert enrichment, and understand AUTO DISABLED.

MicrosoftLearn

Create and use Microsoft Sentinel automation rules to manage response

This article explains how to create and use automation rules in Microsoft Sentinel to manage and handle incidents, in order to maximize your SOC's efficiency and effectiveness in response to security threats.

MicrosoftLearn

Kali Docs | Kali Linux Documentation

Updated on 20 Jan 2023

Home of Kali Linux, an Advanced Penetration Testing Linux distribution used for Penetration Testing, Ethical Hacking and network security assessments.

Kali Linux

Kali Tools | Kali Linux Tools

Updated on 14 Jul 2022

Home of Kali Linux, an Advanced Penetration Testing Linux distribution used for Penetration Testing, Ethical Hacking and network security assessments.

Kali Linux

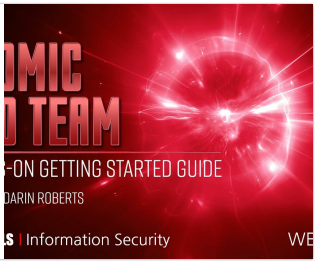
BHIS | Atomic Red Team Hands on Getting Started Guide | Carrie & Darin Roberts | 1 Hour

Updated on 21 Apr 2022

TWO HOURS OF HANDS-ON LAB TIME! —— Chat in Discord: Join the BHIS Community Discord: https://discord.gg/bhis —— Slides: https://rb.gy/mkl158 Emulate adversaries with the Atomic Red Team library of scripted cyber attacks. These scripted attacks, called atomic test…

YouTube

Full screen view



Explore Atomic Red Team

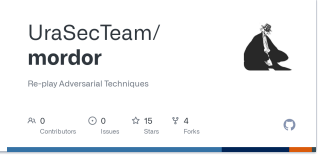
This site is designed to help you explore and navigate the Atomic Red Team™ library of tests, as they are mapped to the MITRE ATT&CK® framework and the platforms they support.

Explore Atomic Red Team

GitHub - UraSecTeam/mordor: Re-play Adversarial Techniques

Re-play Adversarial Techniques. Contribute to UraSecTeam/mordor development by creating an account on GitHub.

GitHub



MITRE ATT&CK®

Mitre

📋 Support & Feedback

> The most common reason for deployment failures is as a result of resource limits in the Azure subscription for available public IP's and/ or VM type. Check that subscription limits have not been reached and then delete the failed deployment and try a new deployment. Occasionally a deployment may fail when installing the Azure VM extensions. This is typically as a result of a transient Azure issue and a new deployment is generally successful. Consider trying a different region. If the deployment fails please email the error reason to SI.Support@altra.cloud.

Email support is available for product deployment issues relating to CyberLab. This does not include any Azure problems or issues. Please email SI.Support@altra.cloud including any error messages and we will endeavour to respond within two business days.

We are unable to assist with any other issues or provide any assistance in terms of using CyberLab such as using the toolsets or writing custom analytics or playbooks.

Any feedback or feature requests may also be sent to SI.Support@altra.cloud.