Sign in

Azure / SimuLand Public

Notifications | Fork 80 | Star 701

Code | Issues 5 | Pull requests | Discussions | Actions | Projects | Security | Insig

main | Go to file | Code

- docs
- resources/scripts
- .gitignore
- CODE_OF_CONDUC...
- LICENSE
- README.md
- SECURITY.md
- SUPPORT.md

README | Code of conduct | MIT license | Security

SimuLand

> See the announcement on the Microsoft Security Blog.

About • Purpose • Structure • Labs • Contributing • Trademarks

About

Understand adversary tradecraft and improve detection strategies

- Readme
- MIT license
- Code of conduct
- Security policy
- Activity
- Custom properties
- 701 stars
- 27 watching
- 80 forks

Report repository

Releases

No releases published

Packages

No packages published

Contributors 9

About

SimuLand is an open-source initiative by Microsoft to help security researchers around the world deploy lab environments that reproduce well-known techniques used in real attack scenarios, actively test and verify effectiveness of related Microsoft 365 Defender, Azure Defender and Microsoft Sentinel detections, and extend threat research using telemetry and forensic artifacts generated after each simulation exercise.

These lab environments will provide use cases from a variety of data sources including telemetry from Microsoft 365 Defender security products, Azure Defender and other integrated data sources through Microsoft Sentinel data connectors.

Site: https://simulandlabs.com

Purpose

As we build out the SimuLand framework and start populating lab environments, we will be working under the following basic principles:

- Understand the underlying behavior and functionality of adversary tradecraft
- Identify mitigations and attacker paths by documenting preconditions for each attacker action
- Expedite the design and deployment of threat research lab environments
- Stay up-to-date with the latest techniques and tools used by real threat actors
- Identify, document, and share relevant data sources to model and detect adversary actions
- Validate and tune detection capabilities

Structure

Languages

● **PowerShell** 100.0%

Folder	Description
Lab Environments	Azure Resource Manager (ARM) Templates and documents to deploy lab environments. Some environments contributed through this initiative require at least a Microsoft 365 E5 license (paid or trial) and an Azure tenant. Depending on the lab guide being worked on, the design of the network environments might change a little. While some labs would replicate a hybrid cross-domain environment (on-prem -> Cloud), others would focus only on resources in the cloud.
Lab Guides	Step-by-step lab guides summarizing simulation scenarios. From a defensive perspective, simulation steps are also mapped to detection queries and alerts from Microsoft 365 Defender, Azure Defender, and Microsoft Sentinel. We believe this would help guide some of the extended threat research generated from the simulation exercise.

Contributing

This project welcomes contributions and suggestions. Most contributions require you to agree to a Contributor License Agreement (CLA) declaring that you have the right to, and actually do, grant us the rights to use your contribution. For details, visit https://cla.opensource.microsoft.com.

When you submit a pull request, a CLA bot will automatically determine whether you need to provide a CLA and decorate the PR appropriately (e.g., status check, comment). Simply follow the instructions provided by the bot. You will only need to do this once across all repos using our CLA.

This project has adopted the Microsoft Open Source Code of Conduct. For more information see the Code of Conduct FAQ or contact opencode@microsoft.com with any additional questions or comments.

Trademarks

This project may contain trademarks or logos for projects, products, or services. Authorized use of Microsoft trademarks or logos is subject to and must follow Microsoft's Trademark & Brand Guidelines. Use of Microsoft trademarks or logos in modified versions of this project must not cause confusion or imply Microsoft sponsorship. Any use of third-party trademarks or logos are subject to those third-party's policies.

Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information