Let us Defend :

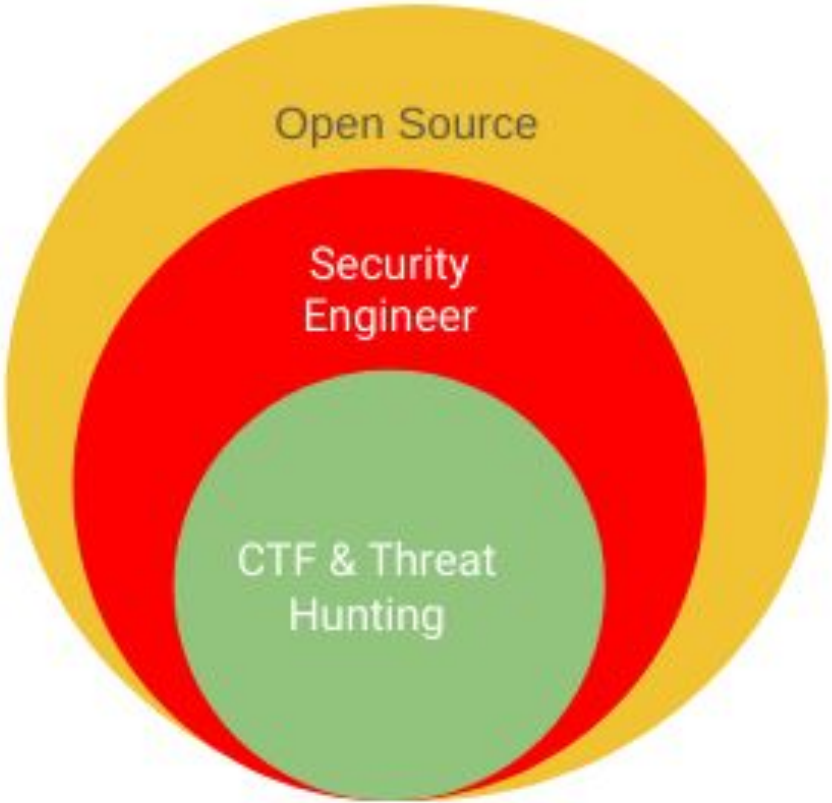
Microsoft Sentinel Guided Approach

$whoami

Shubhendu Shubham

“sudo rm -rf / problems”

aka “Troubleshooter”



CTF BADGES

CERTIFICATIONS

SC 100

AZ 305

AZ 104

AZ 500

AZ 700

Community

Disclaimer

“Learning Defense improves the Attack”

Src: MS Designer DALLE3

Statistics

- 4000 Password attacks per second (Year 2023) , 579(Year 2022)
- 72 minutes Median time for an attacker to access your private data if you open a phishing email
- 3.5 million Global shortage of skilled cybersecurity professionals

Source : Microsoft Digital Defence Report 2023

What is MS Sentinel ?

Microsoft Sentinel is a cloud-native security information and event management (SIEM) platform that uses built-in AI to help analyze large volumes of data across an enterprise—fast. Microsoft Sentinel aggregates data from all sources, including users, applications, servers, and devices running on premises or in any cloud, letting you reason over millions of records in a few seconds. It includes built-in connectors for easy onboarding of popular security solutions. Collect data from any source with support for open standard formats like Common Event Format (CEF) and Syslog.

Applied Skills

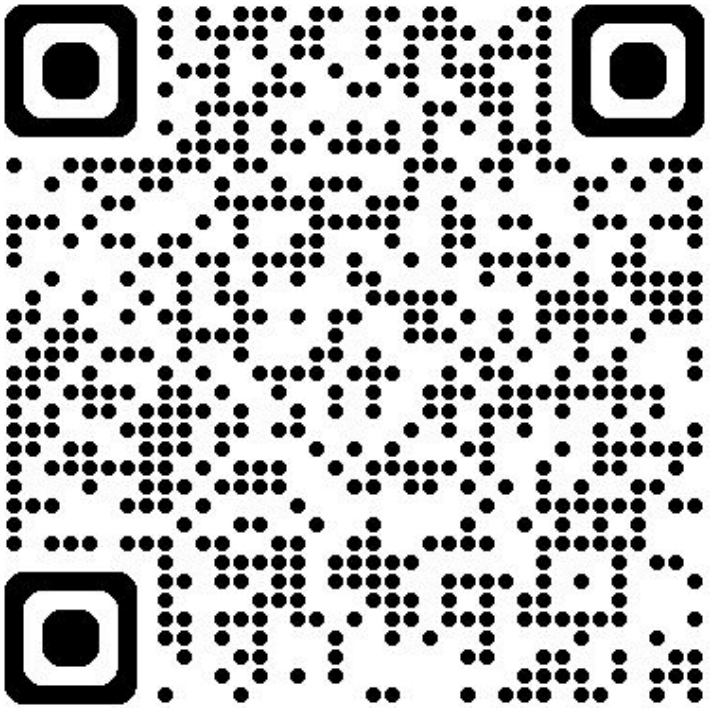
References

https://learn.microsoft.com/en-us/credentials/

https://learn.microsoft.com/en-us/credentials/applied-skills/configure-siem-security-operations-using-microsoft-sentinel/

What's Next ?

This is not Phishing QR ,It's my LinkedIn **Don't Trust** Always verify



Thank you!