Security And Hacking Conference

Maximizing ROI on cyber security investments: Do you think Adversary Simulation OR Purple teaming holds the key?

ABHIJITH "ABX" B R

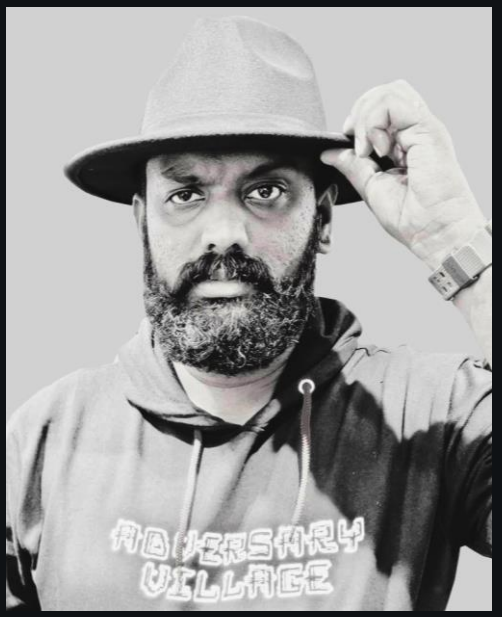
23/Sep/2022

https://tacticaladversary.io/

Who am I?

ABHIJITH B R

- Founder of Adversary Village at DEF CON (https://adversaryvillage.org/)
- Managing Offensive security operations in a global FinTech company
- Former Deputy Manager cyber security at Nissan motor corporation, previously with EY
- A decade of experience in the offensive security domain
- Started running https://tacticaladversary.io project last year
- President and Lead organizer at DEF CON Group (https://dc0471.org/)



@abhijithbr

Adversary Village at DEF CON

Adversary Village is a community torqued combat readiness platform which purely focuses on adversary tactics, adversary simulation/emulation, threat/APT/Ransomware emulation, breach and attack simulation, supply chain security, adversary life, adversary mindset, philosophy, urban survival skills and purple teaming.

https://tacticaladversary.io/

Conceptual Red Team vs Blue Team
Portrayed as native Kerala (India) martial art form “Kalari Payatu”

https://tacticaladversary.io/

*Artwork created for c0c0n conference, 2018

Definitions? Yes, we still need to do this!

Red, Blue, Purple Team


THE RED TEAM
GOES TO INFINITY AND BEYOND!
makeameme.org

Definitions? Yes, we still need to do this!

Adversary Simulation, Emulation, Threat emulation Breach and Attack Simulation

https://tacticaladversary.io/

So, what is the difference?

You need to hear this!


DON'T LISTEN TO HIM
HE JUST MADE THAT SHIT UP
memegenerator.net

Evolving Threat Actors

Threat actors, Ransomware, Insiders

- State sponsored threat actors
- Ransomware groups
- Insider threats
- Zero day exploits! Not fun!
- Extortion groups! Uber?
- Supply chain attacks
- Your worst nightmare, Breaches!

Question for you!

Has your organization faced a targeted threat actor or ransomware attack?


MMMMMMMMM, OHHH
FINE DON'T ANSWER ME THEN,

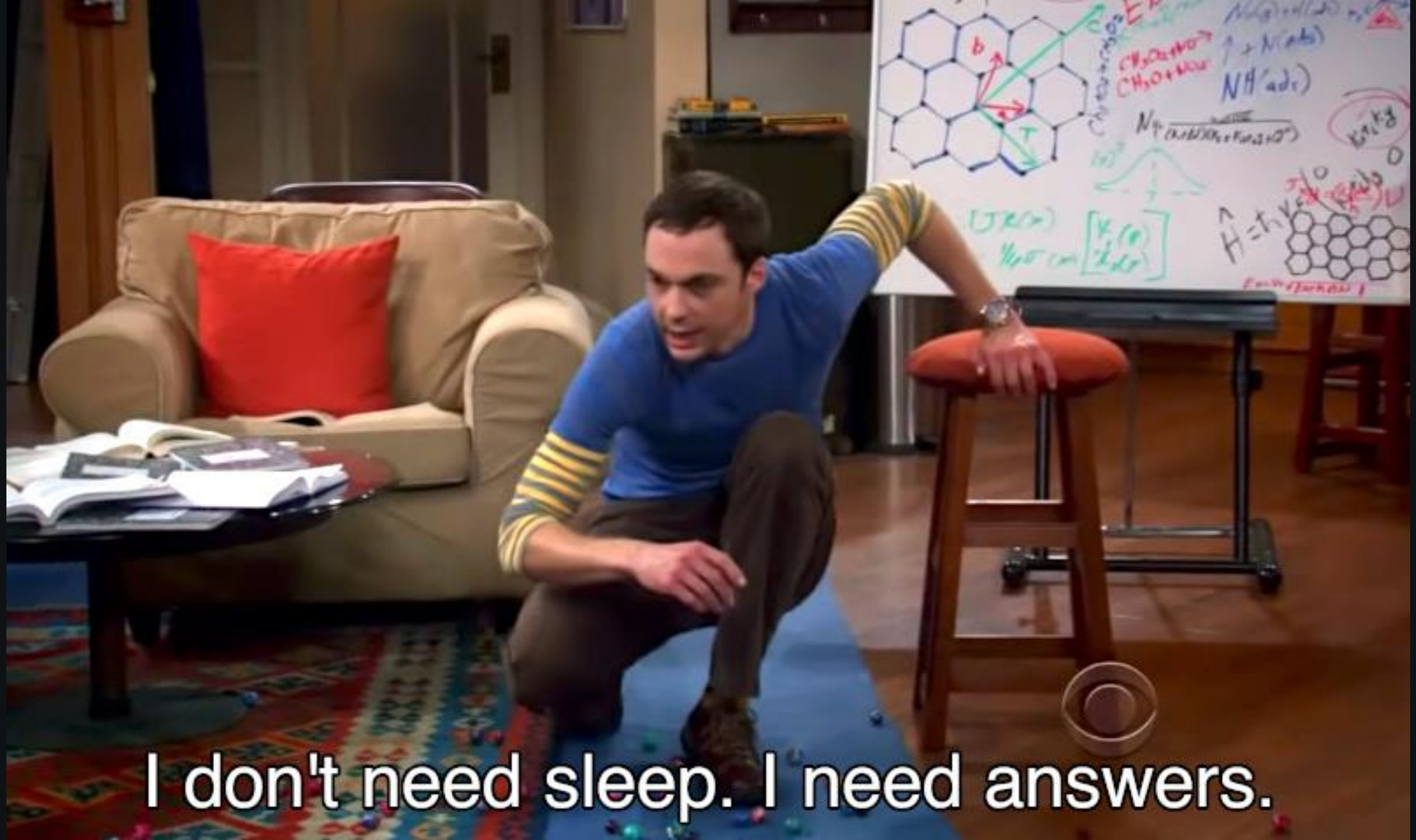
What are your Cyber Security investments?

How much do you spend on security products?

- Security Operations Centre [SOC]
- Endpoint security products
  - Anti-Virus, EDR, EPM, Web proxies, DLP
- Perimeter security products
- Vulnerability scanners and Patch management
- Staff – Acquiring, Retention, Continuous skill development
- What else?

Question for you!

How do you assess the efficacy of your cyber defense products?


I don't need sleep. I need answers.

When can you get started?

Today!!

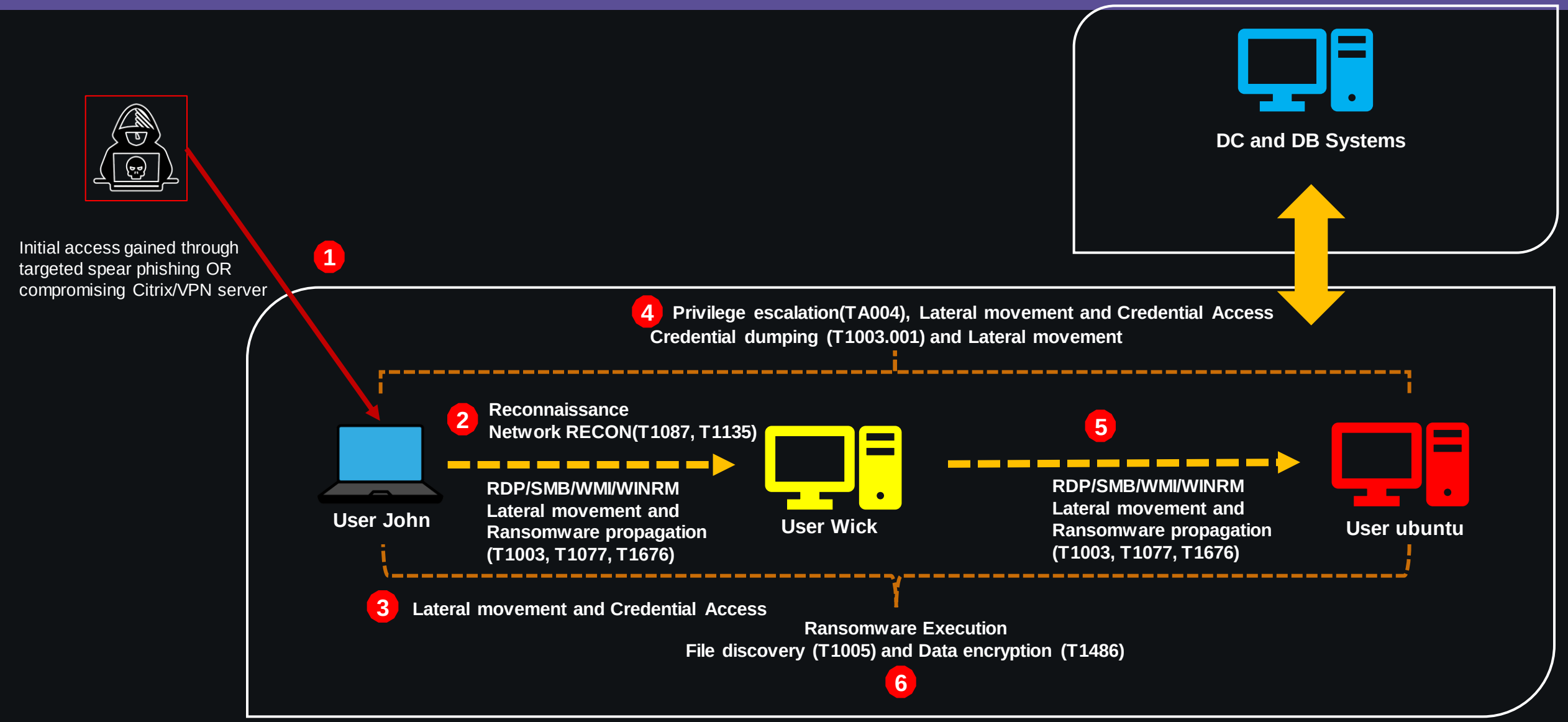
https://tacticaladversary.io/

Visit Adversary Village Track 4 at c0c0n

https://tacticaladversary.io/

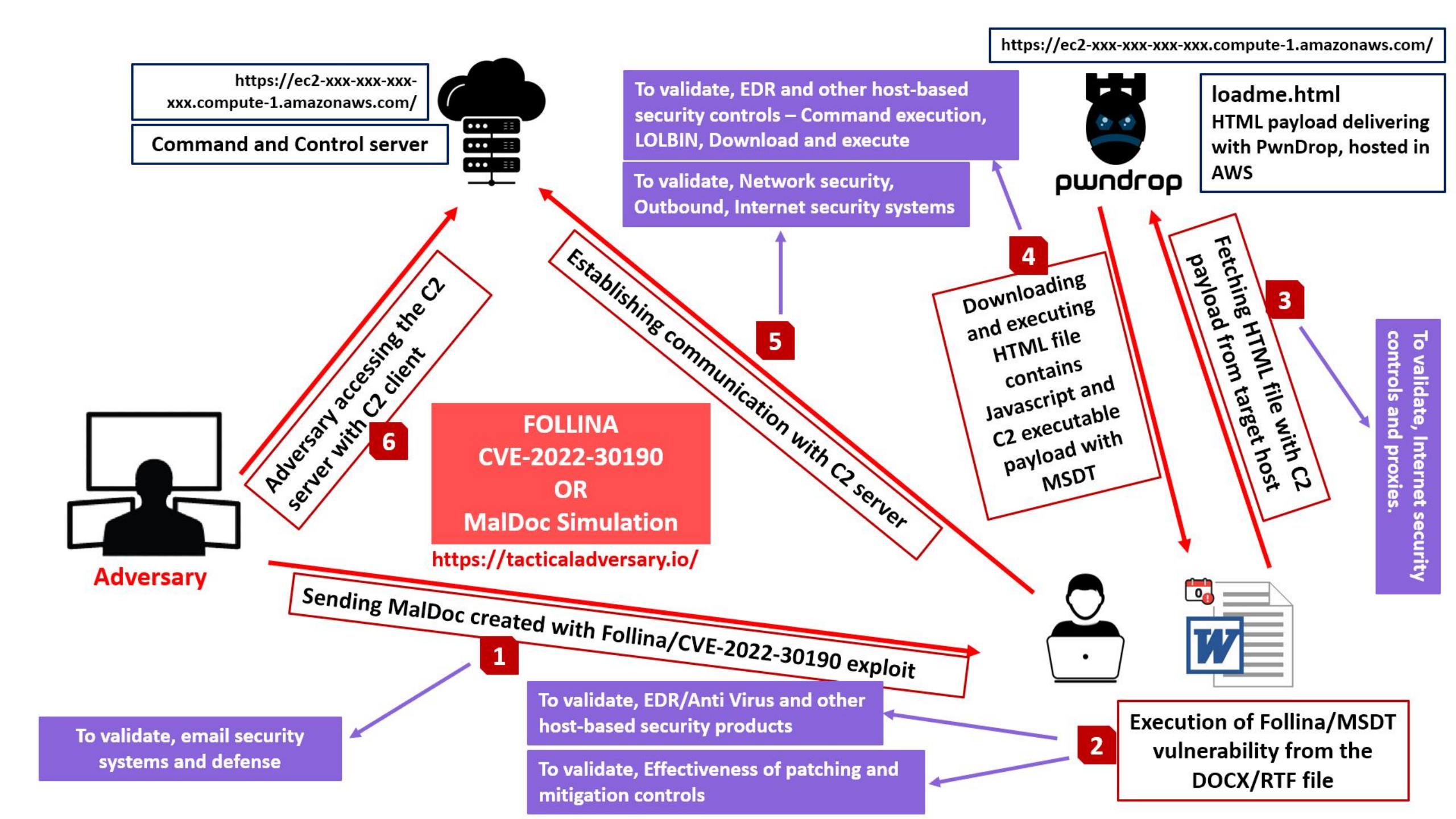
Live Maze Ransomware Simulation

Adversary Village at c0c0n 2022



Example Mini Simulation

Follina aka MalDoc


https://ec2-xxx-xxx-xxx-xxx.compute-1.amazonaws.com/
Command and Control server
https://ec2-xxx-xxx-xxx-xxx.compute-1.amazonaws.com/
loadme.html
HTML payload delivering with PwnDrop, hosted in AWS
pwndrop
To validate, EDR and other host-based security controls – Command execution, LOLBIN, Download and execute
To validate, Network security, Outbound, Internet security systems
5
4
Downloading and executing HTML file contains Javascript and C2 executable payload with MSDT
3
Fetching HTML file with C2 payload from target host
To validate, Internet security controls and proxies.
Establishing communication with C2 server
Adversary accessing the C2 server with C2 client
6
FOLLINA
CVE-2022-30190
OR
MalDoc Simulation
https://tacticaladversary.io/
Adversary
Sending MalDoc created with Follina/CVE-2022-30190 exploit
1
To validate, email security systems and defense
To validate, EDR/Anti Virus and other host-based security products
To validate, Effectiveness of patching and mitigation controls
2
Execution of Follina/MSDT vulnerability from the DOCX/RTF file

How to get started?

Adversary Simulation | Purple Teaming | BAS

- Phase one: your internal offensive security OR red team. Even your internal penetration testing team can get it started.
- Phase two: Hundreds of open-source frameworks and scripts. Examples: Caldera, Prelude Operator, APT Simulator, Atomic red team, C2 Matrix
- Phase three: Enterprise Breach and attack simulation products Example: SafeBreach, AttackIQ, Scythe, Prelude Operator enterprise etc

https://tacticaladversary.io/

How to get started?

Adversary Emulation Library | MITRE Engenuity CTID

In collaboration with Center Participants, the Center for Threat-Informed Defense (Center) has built a library of adversary emulation plans to allow organizations to evaluate their defensive capabilities against the real-world threats they face. Emulation plans are an essential component in testing current defenses for organizations that are looking to prioritize their defenses around actual adversary behavior. Focusing our energies on developing a set of common emulation plans that are available to all means that organizations can use their limited time and resources to focus on understanding how their defenses actually fare against real-world threats.

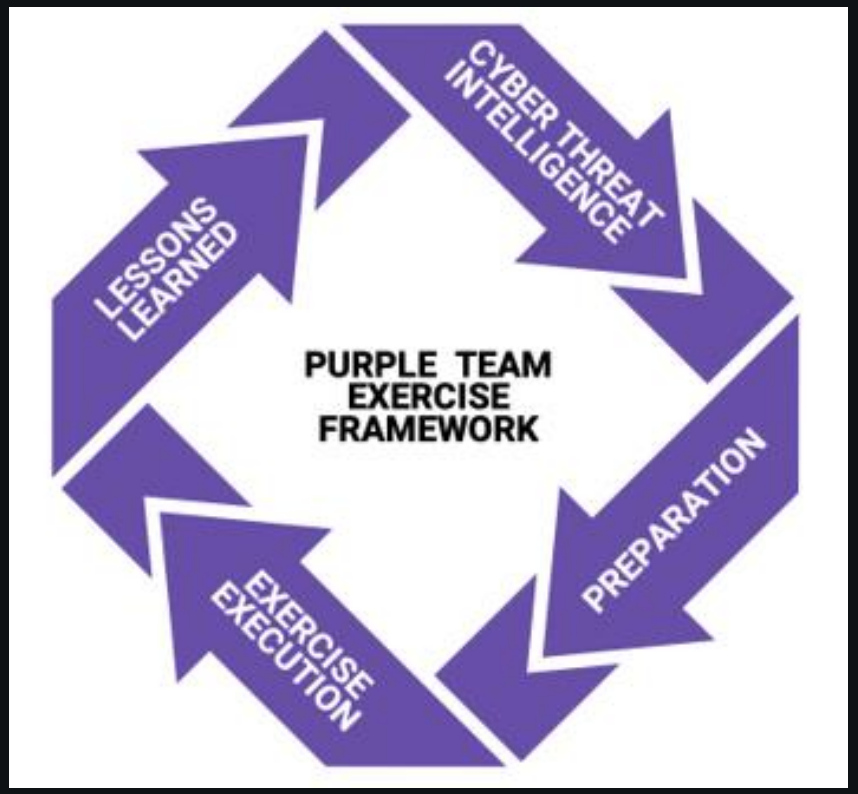
The library contains two types of adversary emulation plans: full emulation and micro emulation.

Adversary Emulation Library: https://github.com/center-for-threat-informed-defense/adversary_emulation_library

Adversary Emulation Plans: https://attack.mitre.org/resources/adversary-emulation-plans/

How to get started?

Purple Team Exercise Framework from Scythe



Purple Team Exercise Framework (PTEF):
https://github.com/scythe-io/purple-team-exercise-framework

https://tacticaladversary.io/

Created and provided to the community by the team at SCYTHE. Please consider contributing by submitting pull requests.

Executive Summary

This document defines a **Purple Team Exercise Framework (PTEF) **to facilitate the creation of a formal **Purple Team Program**. Purple Team Exercises are an efficient method to test, measure, and improve your organization's resilience to an attack. A Purple Team focuses on fostering collaboration with your entire security stack including people, process, and technology.

What is a Purple Team?

A Purple Team is a collaboration of various information security skill sets:

- Cyber Threat Intelligence - research and provide adversary tactics, techniques, and procedures (TTPs)
- Red Team - offensive team in charge of emulating adversaries and TTPs
- Blue Team - the defenders. May include but is not limited to Security Operations Center (SOC), Hunt Team, Digital Forensics and Incident Response (DFIR), and/or Managed Security Service Providers (MSSP).

Conclusion

Takeaway

- Get the maximum out of your cyber security investments
  There is no point in having and AV or EDR if you have configured it poorly.
- Extend your simulation scenarios to each security products and services then create full attack sim scenarios to assess the full attack chain
- **Good luck!**

Thank you!

https://tacticaladversary.io/