Adversary Emulation and Its Importance for Improving Security Posture in Organization

CDEF Meetup
25th February 2021

Digit Oktavianto
@digitoktav
https://medium.com/@digit.oktavianto

T1033 : System Owner/User Discovery

- **Infosec Consulting Manager at Mitra Integrasi Informatika**
- **Co-Founder BlueTeam.ID (https://blueteam.id)**
- **Born to be DFIR Team**
- **Community Lead @ Cyber Defense Community Indonesia**
- **Member of Indonesia Honeynet Project**
- **Opreker and Researcher**
- **{GCIH | GMON | GCFE | GICSP | CEH | CSA | ECSA | ECIH | CHFI | CTIA | ECSS} Certifications Holder**

Agenda

- What is Adversary Emulation About?
  - Adversary Emulation vs Adversary Simulation
  - Phase of Security Assessment
- Benefit and Importance of Adversary Emulation
- Developing Adversary Emulation Plan
- Getting Started with Adversary Emulation

What is Adversary Emulation About?

Introduction : Adversary Emulation

Adversary Emulation is a type of red teaming activities which focuses on the emulation of a specific adversaries / threat actor and leverage the threat intelligence to define the behavior and TTPs that will be used in the emulation plan.

Threat Informed Defense

Threat-informed defense applies a deep understanding of adversary tradecraft and technology to protect against, detect, and mitigate cyber-attacks. It's a community-based approach to a worldwide challenge.

More info : https://www.mitre.org/news/focal-points/threat-informed-defense

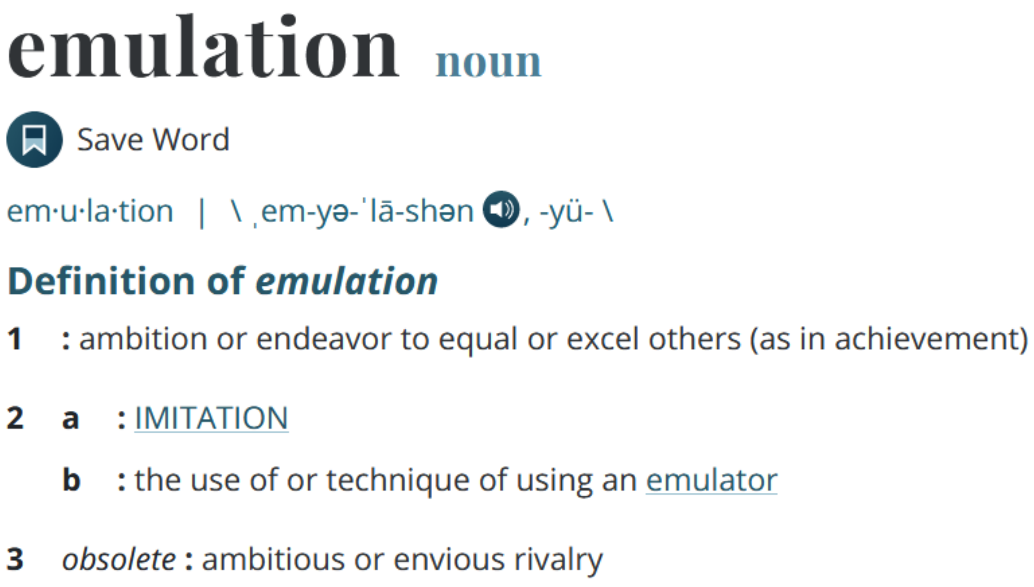
Threat Informed Defense

MITRE Threat Informed Defense Research Focus :

- Increase the global understanding of cyber adversaries and their tradecraft by expanding upon the MITRE ATT&CK knowledge base
- Advance threat-informed defense in cyber operations with open-source software, methodologies, and frameworks
- Publish data sets critical to better understanding adversaries and their movements
- The goal is to change the game on adversaries by relentlessly improving our collective ability to prevent, detect, and respond to cyber attacks.

Adversary Emulation vs Adversary Simulation

Merriam-Webster dictionary translation of emulation and simulation



emulation noun

Save Word

em·u·la·tion | \ ˌem-yə-ˈlā-shən , -yü- \

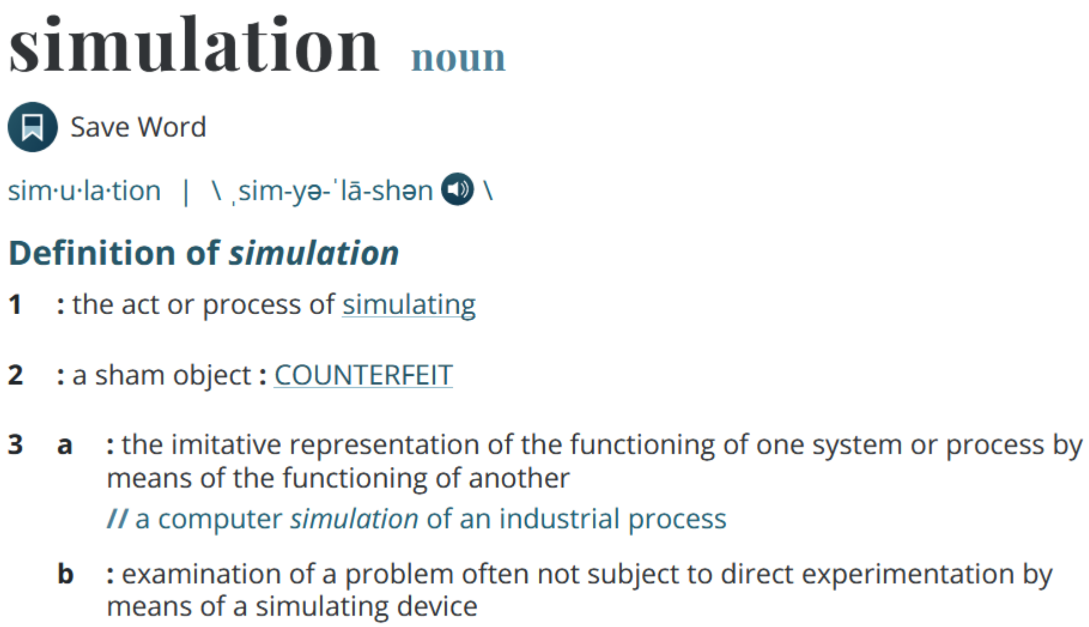
Definition of *emulation*

1 : ambition or endeavor to equal or excel others (as in achievement)

2 a : IMITATION

b : the use of or technique of using an emulator

3 *obsolete* : ambitious or envious rivalry



simulation noun

Save Word

sim·u·la·tion | \ ˌsim-yə-ˈlā-shən \

Definition of *simulation*

1 : the act or process of simulating

2 : a sham object : COUNTERFEIT

3 a : the imitative representation of the functioning of one system or process by means of the functioning of another

// a computer *simulation* of an industrial process

b : examination of a problem often not subject to direct experimentation by means of a simulating device

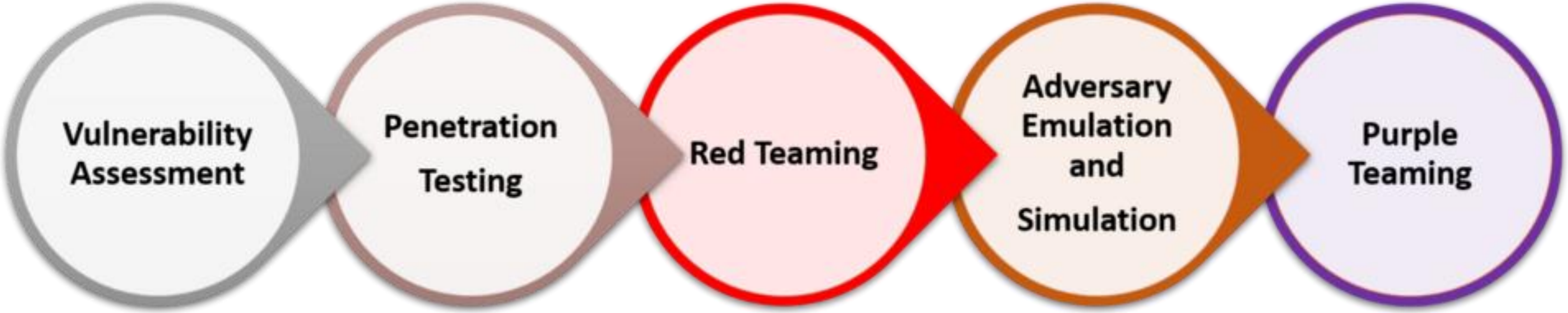
Adversary Emulation vs Adversary Simulation

- **Adversary Emulation** : a process of **imitate the activities or mimicking or copying** the adversaries or threat actor behavior.
- **Adversary Simulation** : a process of **simulate or represent the functioning of adversaries** or threat actor behavior when attacking the target.

Tim MalcomVetter mentioned in his blog post (https://malcomvetter.medium.com/emulation-simulation-false-flags-b8f660734482) about this :

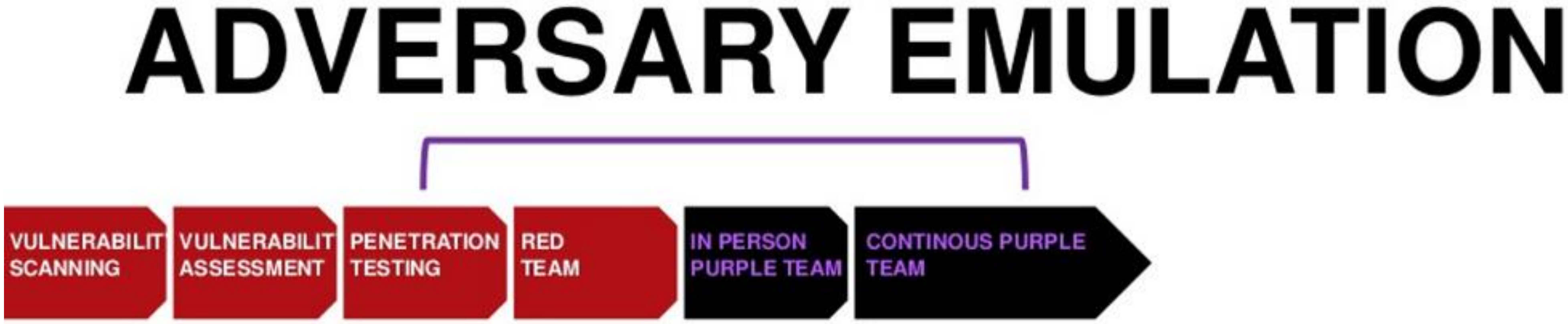
- ***Emulation*** implies an **EXACTNESS** to the copy, whereas ***Simulation*** only implies **SIMILARITY** with some freedom to be different. I am totally agree with his opinion.

Introduction : Adversary Emulation



Phase of Security Assessment

Introduction : Adversary Emulation



Jorge Orchilles's Slide About Adversary Emulation (https://www.slideshare.net/jorgeorchilles/adversary-emulation-and-red-team-exercises-educause)

Introduction : Adversary Emulation

- Jorge Orchilles and Scythe in their blogpost differentiate term of red teaming, adversary emuation / simulation and purple teaming in this statement :
- *"Adversary Emulations may be performed in a* ***blind manner (Red Team Engagement)*** *or* ***non-blind (Purple Team)*** *with the* ***Blue Team having full knowledge of the engagement.****"*
- Based on that statement, it can be conclude that Red Teaming and Purple Teaming is part of Adversary Emulation. It depends on the engagement, if the engagement performed without Blue Team knowing the activities, than it is called as red teaming. If the engagement involved blue team, then it is called purple teaming.

Benefit and Importance of Adversary Emulation

Benefit and Importance of Adversary Emulation

Red Team using Adversary Emulation plan to develop an attack emulation and/or simulation and execute it against your enterprise infrastructure.

These activities leverage real-world attacks and TTPs by Threat Actor, so you can identify and finding the gaps in your defense *before* the actual adversary attacking your infrastructure.

Adversary Emulation also help security team greater visibility into their environment.

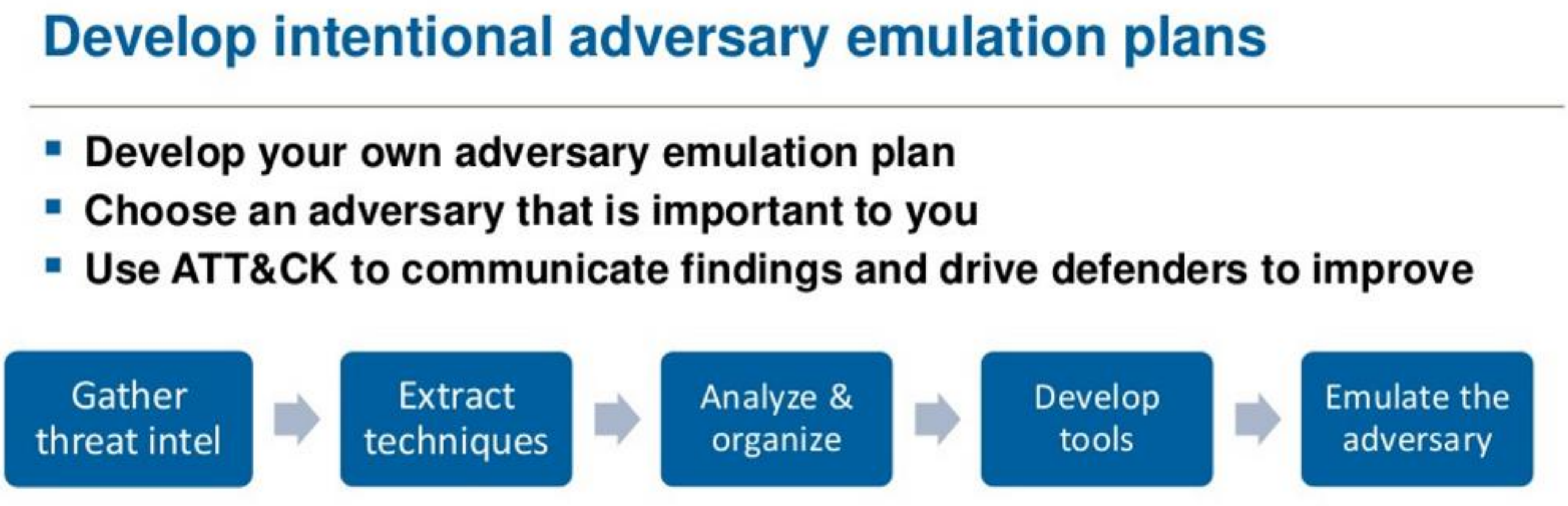
Performing Adversary Emulation continuously to strengthen and tune your defense over the time.

Benefit and Importance of Adversary Emulation

- Adversary Emulation is just like IR and Tabletop Exercise, but in different perspective. This exercise allows your organization to test your security team against the latest threats used by real threat actor which posing the greatest risk to your organization in specific industry.
- Adversary emulation giving proof of how a targeted attacker could penetrate your infrastructure and compromise sensitive assets, and/or documentation.
- Adversary emulation showing that defensive capabilities succeed / failed in preventing + responding the simulated attack. It is giving you analysis of your organization’s strengths and weaknesses based on the result of the simulation.
- Adversary emulation can help you not only to prioritize current existing technology capability improvement, but also also giving you a recommendation for future investments and provide recommendations for maturing your cybersecurity posture.
  - A focus on objective-based testing demonstrates the effectiveness of your security controls
- Adversary Emulation can help you to measure your organization’s cybersecurity maturity level by evaluating it across the kill chain phases of the MITRE ATT&CK® framework or other relevant frameworks.

Developing Adversary Emulation Plan

Developing Adversary Emulation Plan



Develop intentional adversary emulation plans

- Develop your own adversary emulation plan
- Choose an adversary that is important to you
- Use ATT&CK to communicate findings and drive defenders to improve

Gather threat intel
Extract techniques
Analyze & organize
Develop tools
Emulate the adversary

Adam Pennington's Slide : Leveraging MITRE ATT&CK for Detection, Analysis & Defense (https://www.slideshare.net/AdamPennington4/rhisac-summit-2019-adam-pennington-leveraging-mitre-attck-for-detection-analysis-defense)

Developing Adversary Emulation Plan

I quote a paragraph from Tim MalcomVetter About Emulation Plan in Practice (https://malcomvetter.medium.com/emulation-simulation-false-flags-b8f660734482):

“In practice, *emulating* is very hard. **First**, not all threat actors have publicly or privately available intelligence in the format necessary to complete all of the threat actors’ steps with the precision required to meet the definition. **Second**, even for those that do, certain key steps may be out of bounds, legally, for the person “replaying them” (such as compromising third party infrastructure). **Third**, the “programmed TTPs” were collected at a single point in time, and techniques that were used during that string of events may not be reused in the future by that threat actor, so replaying them with *precision* may not be that valuable of an exercise.”

Developing Adversary Emulation Plan

Adversary emulation plans are based on known-adversary TTPs (Tactic, Technique, and Procedure) and designed to empower red teams to emulate a specific threat actor in order to test and evaluate defensive capabilities from a threat-informed perspective.

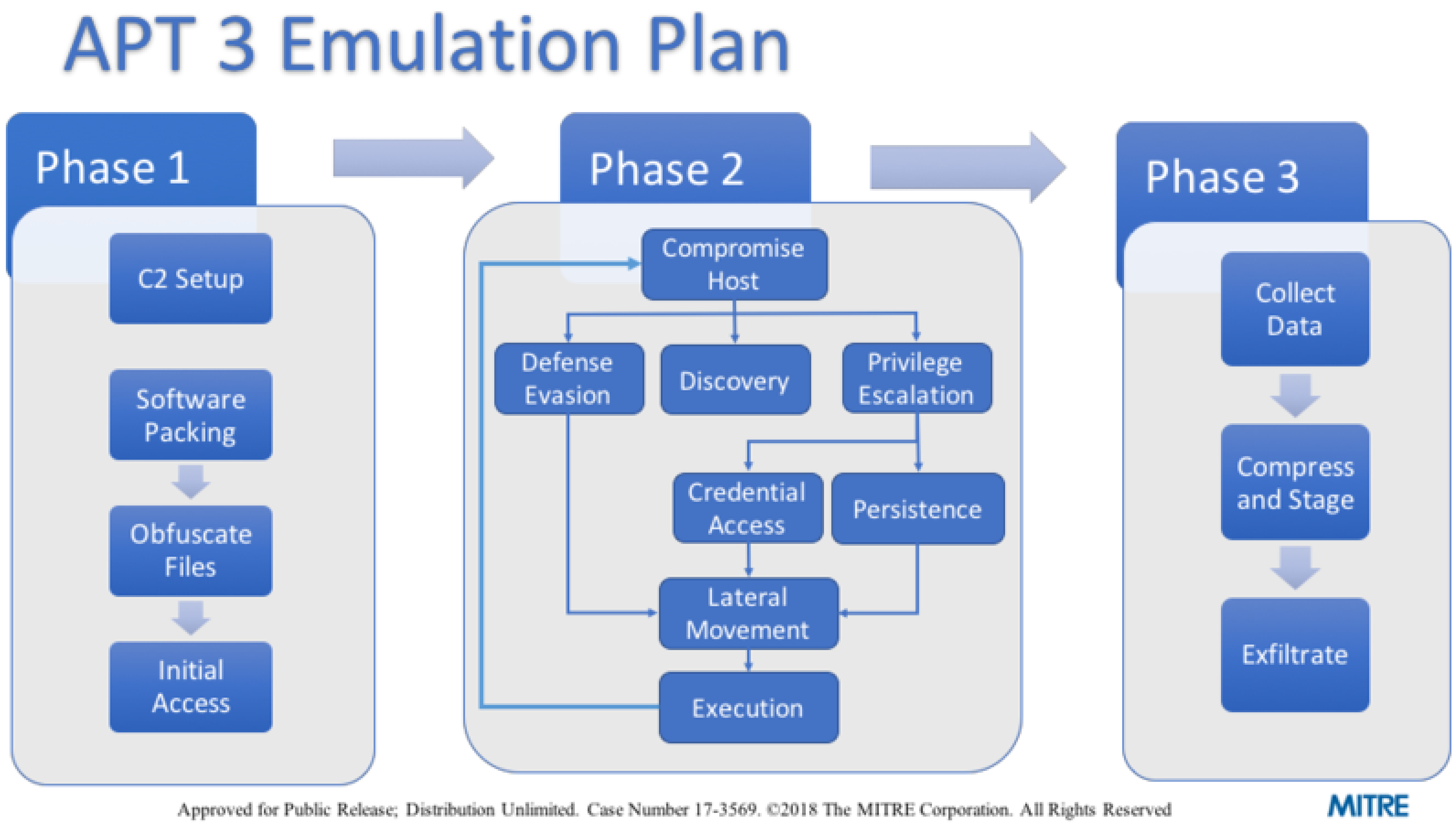
- Each emulation plan focuses on a specific named threat actor.
- Each adversary emulation plan is gathered from threat intelligence reports and other artifacts that capture and describe breaches and campaigns publicly attributed to a specific named threat actor
- To develop each plan, Red Team should do the research and model each threat actor, focusing not only on what they do (e.g.: gather credentials from victims) but also how (using what specific tools/utilities/commands?) and when (during what stage of a breach?)
- Red Team then develop the emulation content that *mimics* the underlying behaviors utilized by the threat actor
- To describe the details flow of emulation plan, Red Team should develop the operational flow which provides a high-level summary of the captured scenario(s).
- The scenario(s) of emulation plan is broken down into step-by-step procedures provided in both human and machine-readable formats. (like **.yaml** in Caldera for example). Scenarios can be executed end-to-end or as individual tests.
- The emulation plan scenarios will vary based on the adversary and available intelligence, but typically follow a sequential progression of how the actor breaches then works towards achieving their operational objectives within a victim environment

Developing Adversary Emulation Plan

For example, the MITRE The ATT&CK Evaluations of APT29 Emulation Plan (https://github.com/mitre-attack/attack-arsenal/blob/master/adversary_emulation/APT29/Emulation_Plan/APT29_EmuPlan.pdf) signaled a significant evolution to the process and established a close-to-ideal structure of components that made up the emulation plan. Those were:

- Intelligence Summary: An overview of the adversary and references to cited Intelligence
- Operational Flow: Chains techniques together into a logical flow of the major steps that commonly occur across the selected adversary’s operations
- Emulation Plan: The TTP-by-TTP, command-by-command walkthrough to implement the adversary’s operational tradecraft as described in the Intelligence Summary and the Operational Flow

Developing Adversary Emulation Plan



APT 3 Emulation Plan

Phase 1

C2 Setup

Software Packing

Obfuscate Files

Initial Access

Phase 2

Compromise Host

Defense Evasion

Discovery

Privilege Escalation

Credential Access

Persistence

Lateral Movement

Execution

Phase 3

Collect Data

Compress and Stage

Exfiltrate

Approved for Public Release; Distribution Unlimited. Case Number 17-3569. ©2018 The MITRE Corporation. All Rights Reserved

MITRE

APT3 Operational Flow

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

Getting Started with The Adversary Emulation

Getting Started with the Adversary Emulation

When starting the Adversary Emulation Exercise, Emulation Plan is one of the most critical part. The *Emulation Plan* section is a specific, detailed breakdown of the tactics of the adversary group.

1. For developing the *Emulation Plan*, red team firstly must gather the threat intelligence document related to threat actor group that they want to emulate.
2. Red team must identify the tactics the adversary group uses for an attack, along with the particular techniques and procedures for each tactic. Mostly the TTPs defined based on MITRE ATTCK Framework as a standard.
3. To detail an emulation plan in exercise, red team must breakdown the tools that they will use to emulate the particular TTP. This information is available as part of the MITRE ATT&CK description of the adversary group, and also from Threat Intelligence Report.
4. Red Team also need to build the infrastructure as part of the emulation plan such as C2 Infrastructure, or Infrastructure for collecting sensitive data after exfiltration phase (if any)
5. Execute the emulation plan as procedure and workflow defined in the exercise. Follow up the result of the exercise.

Notable Tools and Resources for Adversary EMulation

Some notable tools for adversary emulation :

- Caldera (MITRE)
- Atomic Red Team (Red Canary)
- APT Simulator
- Red Team Automation (Endgame)
- Infection Monkey (Guardicore)
- Blue Team Toolkit (BT3) (Encripto)
- AutoTTP (https://github.com/jymcheong/AutoTTP)
- Purple Team ATT&CK Automation (https://github.com/praetorian-inc/purple-team-attack-automation)
- ATTPwn (https://github.com/ElevenPaths/ATTPwn)
- PurpleSharp (https://github.com/mvelazc0/PurpleSharp)
- Prelude Operator (https://www.prelude.org/)

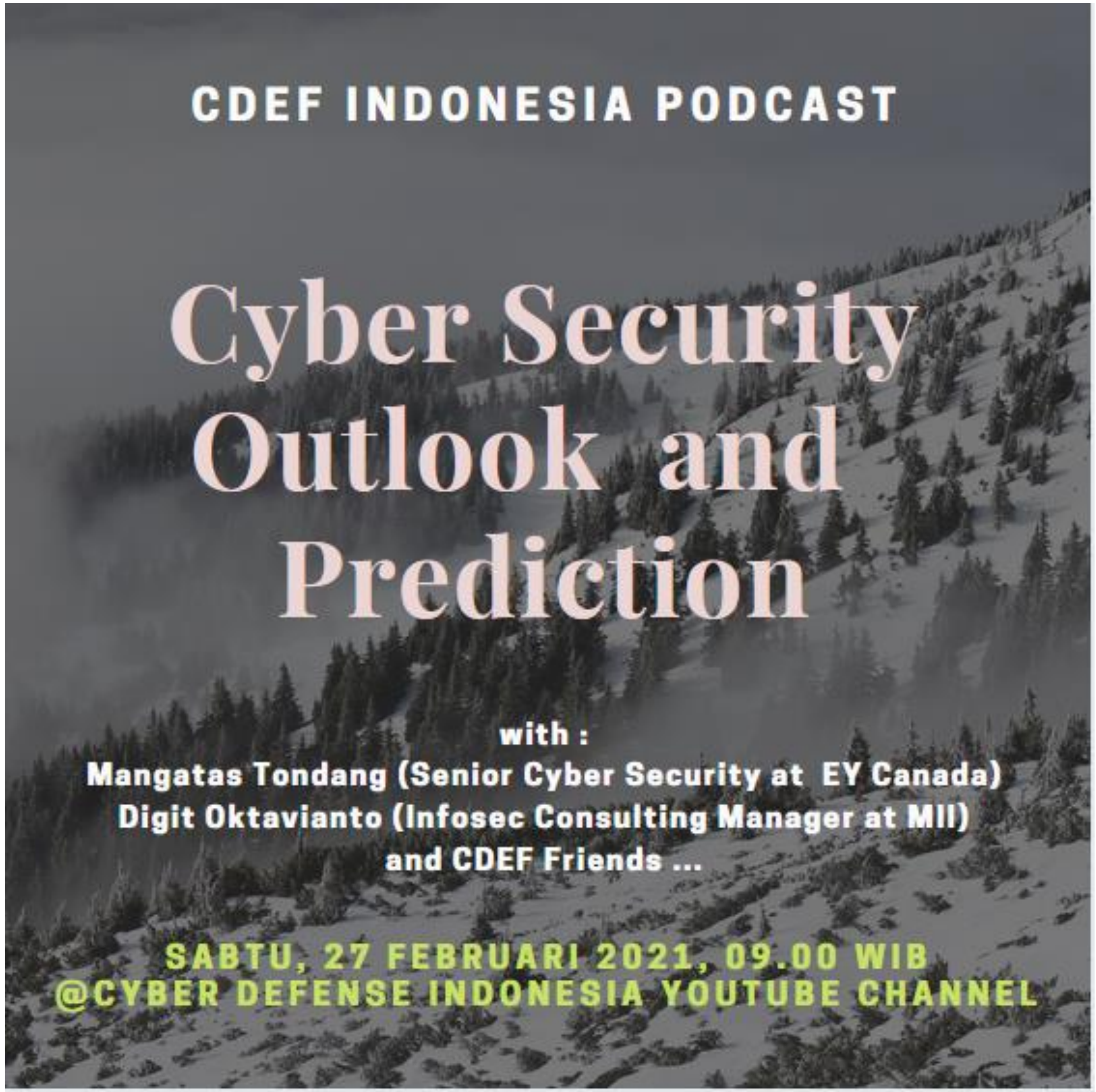
Notable Tools and Resources for Adversary EMulation

Some notable tools for developing adversary emulation :

- MITRE ATT&CK Navigator
- NSA Unfetter (https://nsacyber.github.io/unfetter/)
- MITRE Cyber Analytical Repository (https://car.mitre.org/)
- VECTR (More into for your Purple Teaming)
- **_YOUR THREAT INTEL REPORT_** Provider

TLDR ; Summary and Key Takeaway

- Adversary emulation is needed by organization to fill the gaps for their current existing security assessment activity
- Adversary emulation is HARD. Combining the threat intelligence and Adversary TTPs is not a simple task to do.
- Threat-informed defense approach needed by every organization to get a deep understanding of adversary tradecraft and technology to protect against, detect, and mitigate cyber-attacks.
- Developing Adversary Emulation Plan is a Critical part in Adversary Emulation Exercise before the Execution of scenarios defined.
- Adversary Emulation showing that defensive capabilities succeed / failed in preventing + responding the simulated attack. It is giving you analysis of your organization’s strengths and weaknesses based on the result of the simulation
- Adversary Emulation can help you to measure your organization’s cybersecurity maturity level by evaluating it across the kill chain phases of the MITRE ATT&CK framework or other relevant frameworks.



CDEF INDONESIA PODCAST

Cyber Security Outlook and Prediction

with :
Mangatas Tondang (Senior Cyber Security at EY Canada)
Digit Oktavianto (Infosec Consulting Manager at MII)
and CDEF Friends ...

SABTU, 27 FEBRUARI 2021, 09.00 WIB
@CYBER DEFENSE INDONESIA YOUTUBE CHANNEL

THANK YOU
Q & A