black hat ASIA 2023

MAY 11-12

ARSENAL

Prediction System for Lateral movement Based on ATT&CK Using Sysmon

Yukihiro Kozai, Koki Watarai, Takuho Mitsunaga

Yukihiro Kozai

Yukihiro Kozai is a fourth undergraduate student at the Faculty of Information Networking for Innovation and Design (INIAD) of Toyo University. Yukihiro's research interests include cyber-security. He also develops as an infrastructure and software engineer.

Koki Watarai

Koki Watarai is a Tech Engineer at Toyo University. I specialize in web security and try to develop useful tools for safer IT environment.

Takuho Mitsunaga

Takuho Mitsunaga is an Associate Professor at INIAD, Toyo University.
He is also an advisor at Industrial System Security Center of Excellence of Information-technology Promotion Agency and a senior fellow at The Tokyo Foundation for Policy Research and in Japan.
He received a Ph.D. degree from Kyoto University in 2016. He worked at the front line of incident handling and penetration testing at a security organization, where he is engaged in cyber attack analysis including APT cases.
He has also contributed in some cyber security related books as coauthor or editorial supervisor including "CSIRT(NTT Publishing) ", " Fundamentals of Control System Security (NTT Publishing)

Agenda

01. Preliminary

02. Tool Details

03. Demonstration

04. Conclusion

Backgrounds

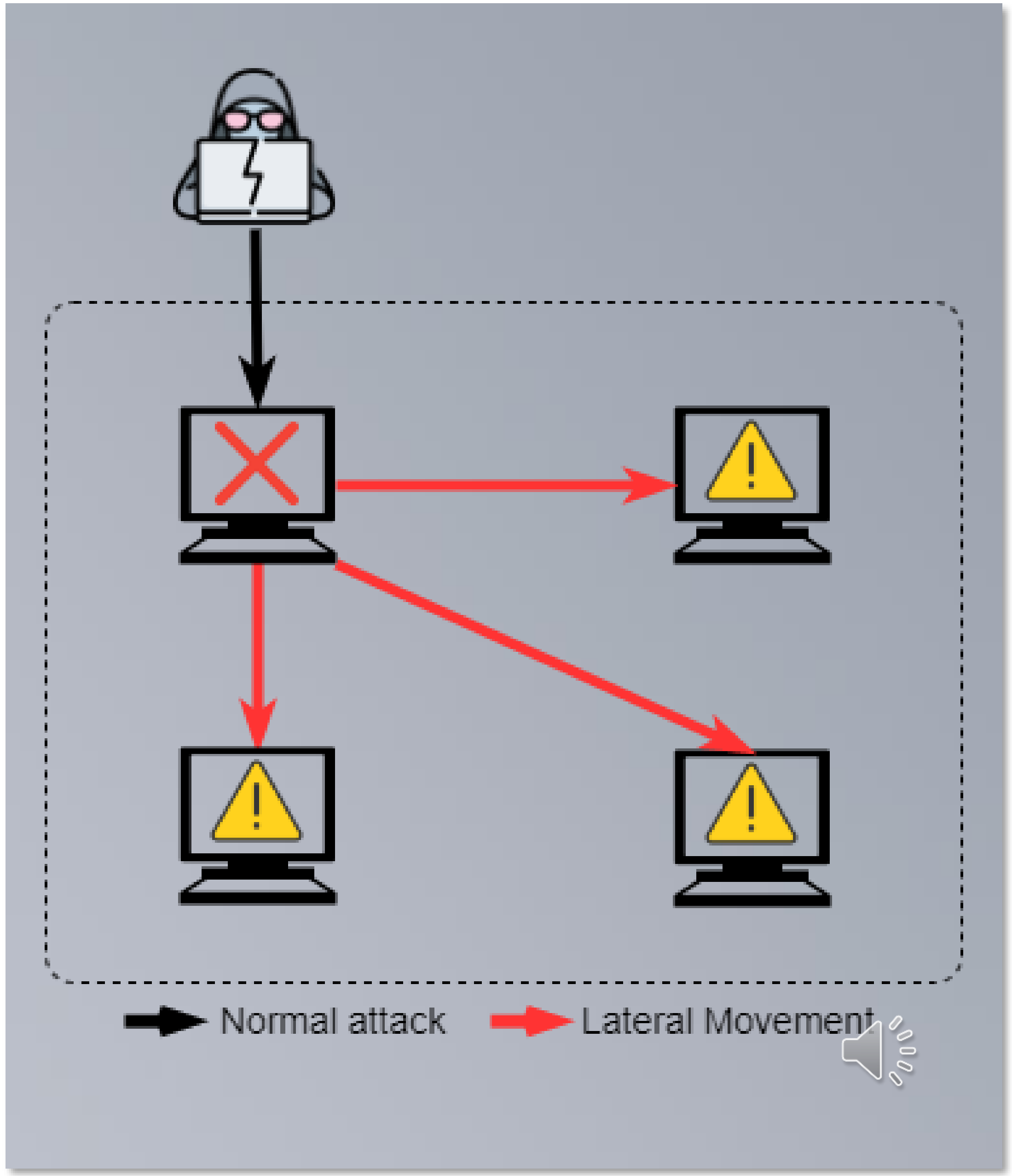
- Cyber attacks are on the rise.
- It is impossible to completely prevent the intrusion of attackers.
- It is important to quickly grasp the infection status when an attacker intrudes.
- It takes a huge **amount of time and effort** to understand the infection status from the logs output from the huge and complicated system.
- We want to understand the infection status **quickly and easily** from logs.

Preliminary

Lateral movement

Lateral movement

- One of the attacks of the infection expansion phase of the cyberattack.
- After breaking into the system, the attacker tries to break into other devices of the same network.
- Attackers get credential information by expanding the infection.

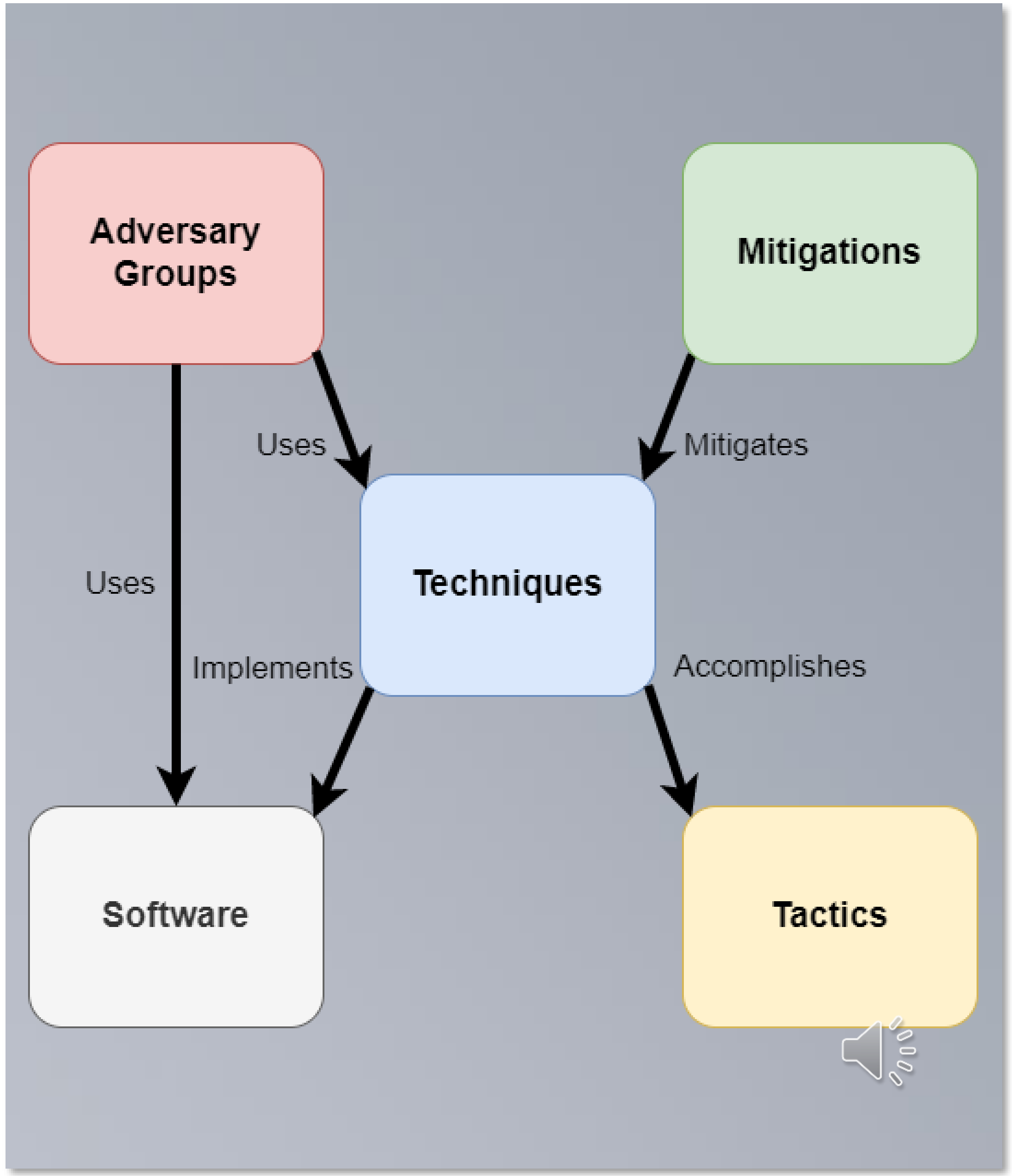


MITRE ATT&CK

MITRE ATT&CK

- A knowledge base of cyber attack tactics and techniques based on past cyberattacks.

- It consists of the following five elements.
  - **Adversary Groups:** Groups of attackers
  - **Tactics:** Objective of attack
  - **Techniques:** Technique used in attacks
  - **Software:** Tools used in attacks
  - **Mitigations:** Mitigations for Attacks

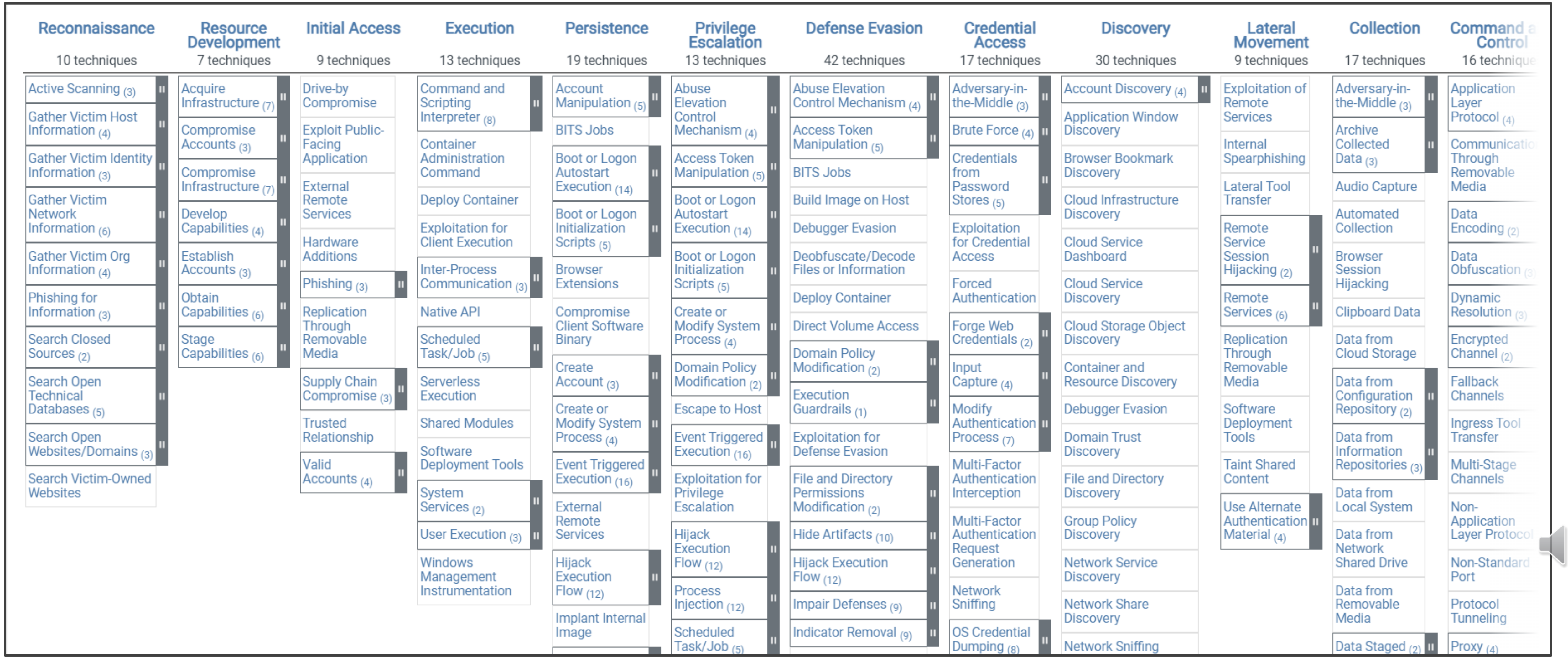


ATT&CK Matrix

Tactics

Less Progressive → High Progressive

Techniques



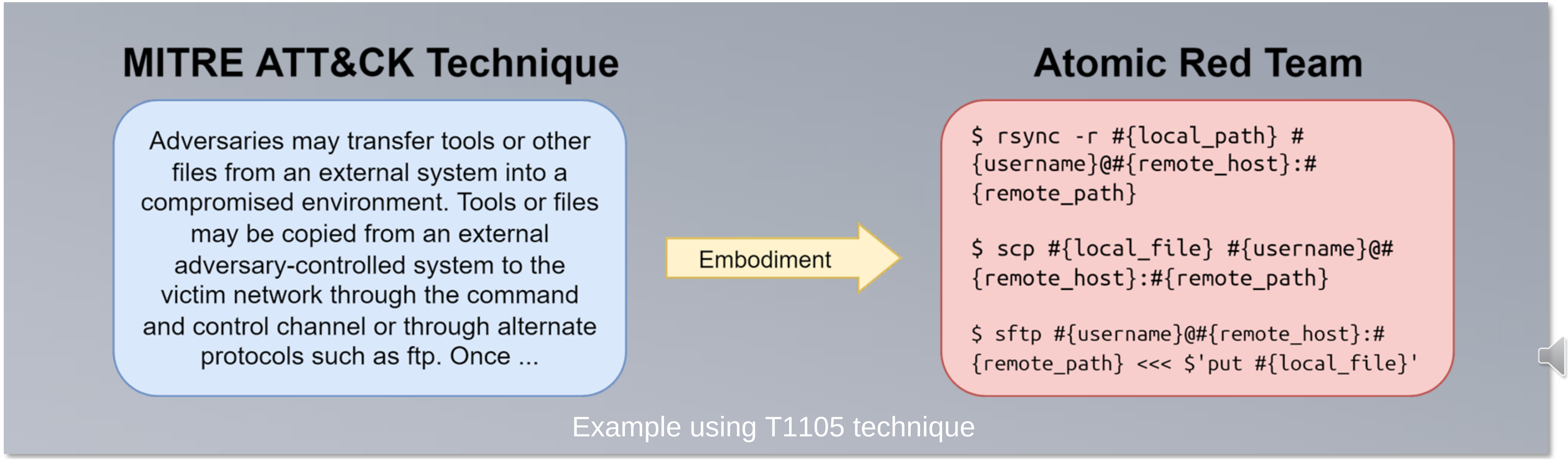
Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command a Control 16 technique
Active Scanning (3)	Acquire Infrastructure (7)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)
Gather Victim Host Information (4)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communicatio Through Removable Media
Gather Victim Identity Information (3)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3
Gather Victim Org Information (4)	Establish Accounts (3)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Create or Modify System Process (4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)
Search Closed Sources (2)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Escape to Host	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels
Search Open Technical Databases (5)		Trusted Relationship	Serverless Execution	Create or Modify System Process (4)	Event Triggered Execution (16)	Direct Volume Access	Modify Authentication Process (7)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer
Search Open Websites/Domains (3)		Valid Accounts (4)	Shared Modules	Event Triggered Execution (16)	Exploitation for Privilege Escalation	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Hijack Execution Flow (12)	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protoco
			System Services (2)	Hijack Execution Flow (12)	Process Injection (12)	Exploitation for Defense Evasion	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port
			User Execution (3)	Implant Internal Image	Scheduled Task/Job (5)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	Group Policy Discovery		Data from Removable Media	Protocol Tunneling
			Windows Management Instrumentation			Hide Artifacts (10)		Network Service Discovery		Data Staged (2)	Proxy (4)
						Hijack Execution Flow (12)		Network Share Discovery			
						Impair Defenses (9)		Network Sniffing			
						Indicator Removal (9)					

Information Classification: General

Atomic Red Team

Atomic Red Team

- An open-source library of test based on MITER ATT&CK.
- You can use it to simulate adversarial activity in their environments.



MITRE ATT&CK Technique

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as ftp. Once ...

Atomic Red Team

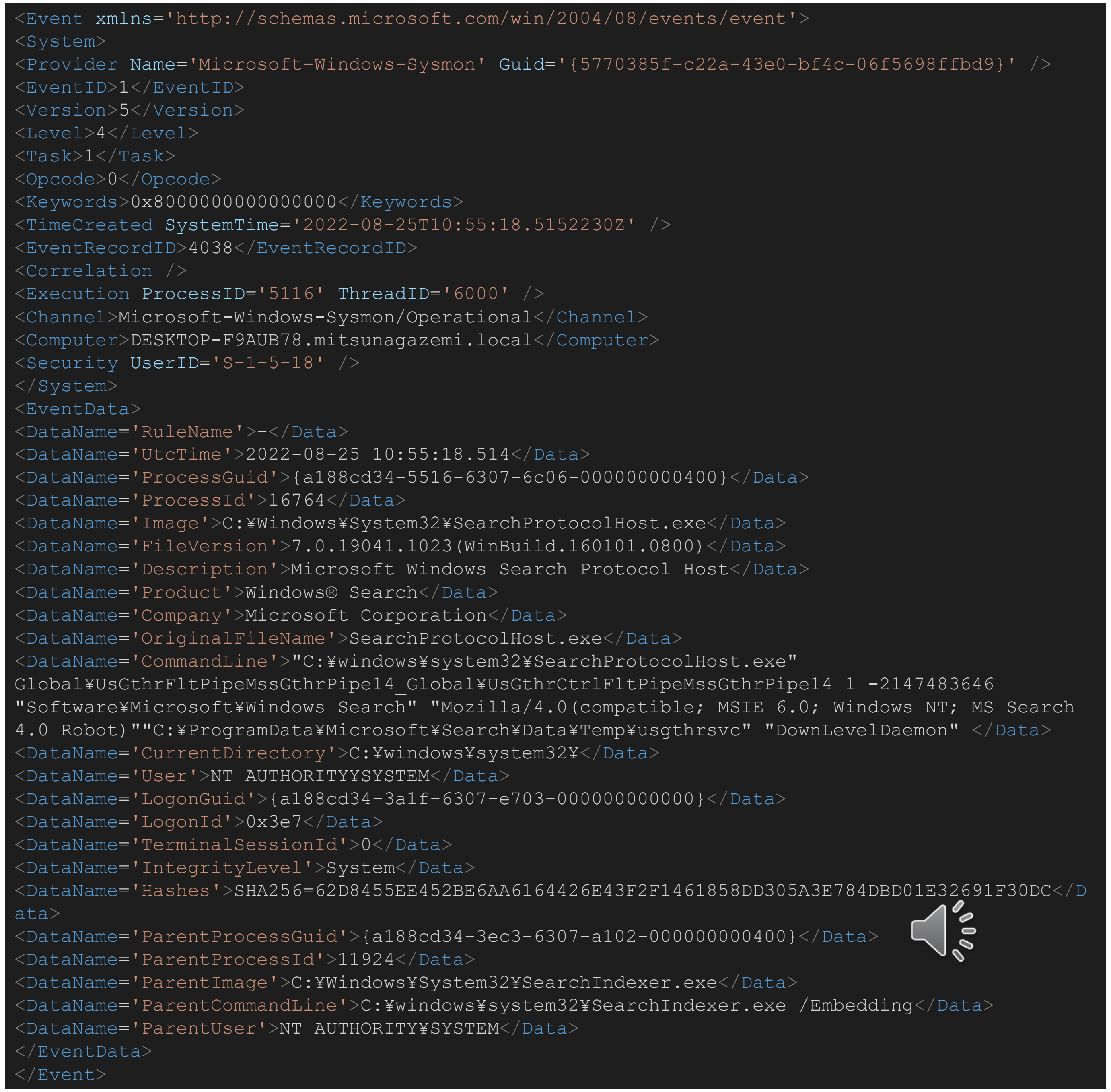
```
$ rsync -r #{local_path} #
{username}@#{remote_host}:#
{remote_path}

$ scp #{local_file} #{username}@#
{remote_host}:#{remote_path}

$ sftp #{username}@#{remote_host}:#
{remote_path} <<< $'put #{local_file}'
```

Example using T1105 technique

Sysmon

Sysmon

- Sysmon is a tool for recording Windows system activity.
- We can investigate the cause and behavior of the system.



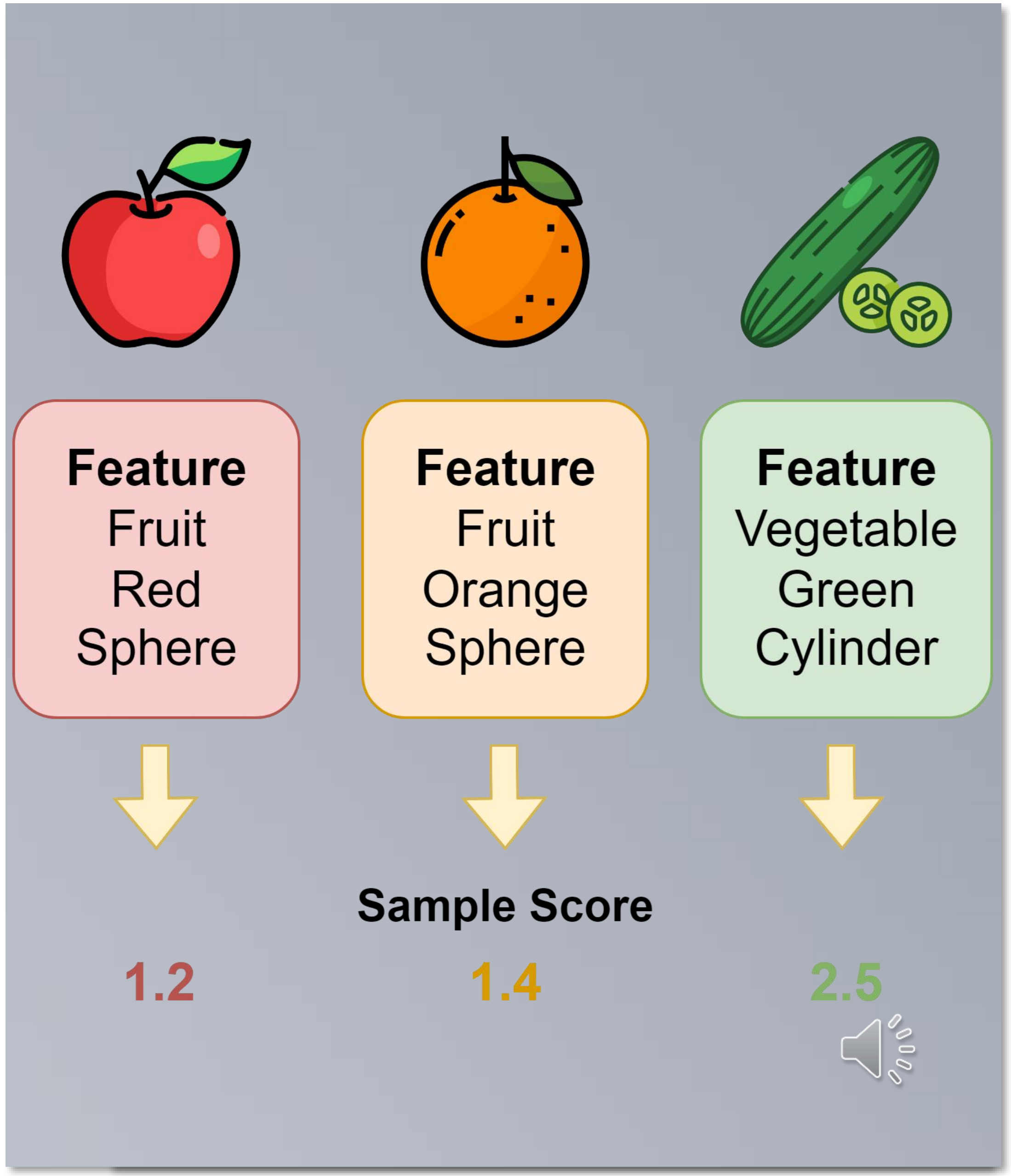
```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'>
<System>
<Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}' />
<EventID>1</EventID>
<Version>5</Version>
<Level>4</Level>
<Task>1</Task>
<Opcode>0</Opcode>
<Keywords>0x8000000000000000</Keywords>
<TimeCreated SystemTime='2022-08-25T10:55:18.5152230Z' />
<EventRecordID>4038</EventRecordID>
<Correlation />
<Execution ProcessID='5116' ThreadID='6000' />
<Channel>Microsoft-Windows-Sysmon/Operational</Channel>
<Computer>DESKTOP-F9AUB78.mitsunagazemi.local</Computer>
<Security UserID='S-1-5-18' />
</System>
<EventData>
<DataName='RuleName'>-</Data>
<DataName='UtcTime'>2022-08-25 10:55:18.514</Data>
<DataName='ProcessGuid'>{a188cd34-5516-6307-6c06-000000000400}</Data>
<DataName='ProcessId'>16764</Data>
<DataName='Image'>C:¥Windows¥System32¥SearchProtocolHost.exe</Data>
<DataName='FileVersion'>7.0.19041.1023(WinBuild.160101.0800)</Data>
<DataName='Description'>Microsoft Windows Search Protocol Host</Data>
<DataName='Product'>Windows® Search</Data>
<DataName='Company'>Microsoft Corporation</Data>
<DataName='OriginalFileName'>SearchProtocolHost.exe</Data>
<DataName='CommandLine'>"C:¥windows¥system32¥SearchProtocolHost.exe"
Global¥UsGthrFltPipeMssGthrPipe14_Global¥UsGthrCtrlFltPipeMssGthrPipe14 1 -2147483646
"Software¥Microsoft¥Windows Search" "Mozilla/4.0(compatible; MSIE 6.0; Windows NT; MS Search
4.0 Robot)""C:¥ProgramData¥Microsoft¥Search¥Data¥Temp¥usgthrsvc" "DownLevelDaemon" </Data>
<DataName='CurrentDirectory'>C:¥windows¥system32¥</Data>
<DataName='User'>NT AUTHORITY¥SYSTEM</Data>
<DataName='LogonGuid'>{a188cd34-3a1f-6307-e703-000000000000}</Data>
<DataName='LogonId'>0x3e7</Data>
<DataName='TerminalSessionId'>0</Data>
<DataName='IntegrityLevel'>System</Data>
<DataName='Hashes'>SHA256=62D8455EE452BE6AA6164426E43F2F1461858DD305A3E784DBD01E32691F30DC</D
ata>
<DataName='ParentProcessGuid'>{a188cd34-3ec3-6307-a102-000000000400}</Data>
<DataName='ParentProcessId'>11924</Data>
<DataName='ParentImage'>C:¥Windows¥System32¥SearchIndexer.exe</Data>
<DataName='ParentCommandLine'>C:¥windows¥system32¥SearchIndexer.exe /Embedding</Data>
<DataName='ParentUser'>NT AUTHORITY¥SYSTEM</Data>
</EventData>
</Event>
```

The Quantification Theory Type 3

The Quantification Theory Type 3

- One of the multivariate analysis.
- This analyzes similarity.
- Sample scores are obtained by calculating what elements are in each sample.
- The quantification theory type 3 analyzes the similarity based on the proximity of the sample scores.

The apple sample score is close to orange!



Feature	Feature	Feature
Fruit Red Sphere	Fruit Orange Sphere	Vegetable Green Cylinder

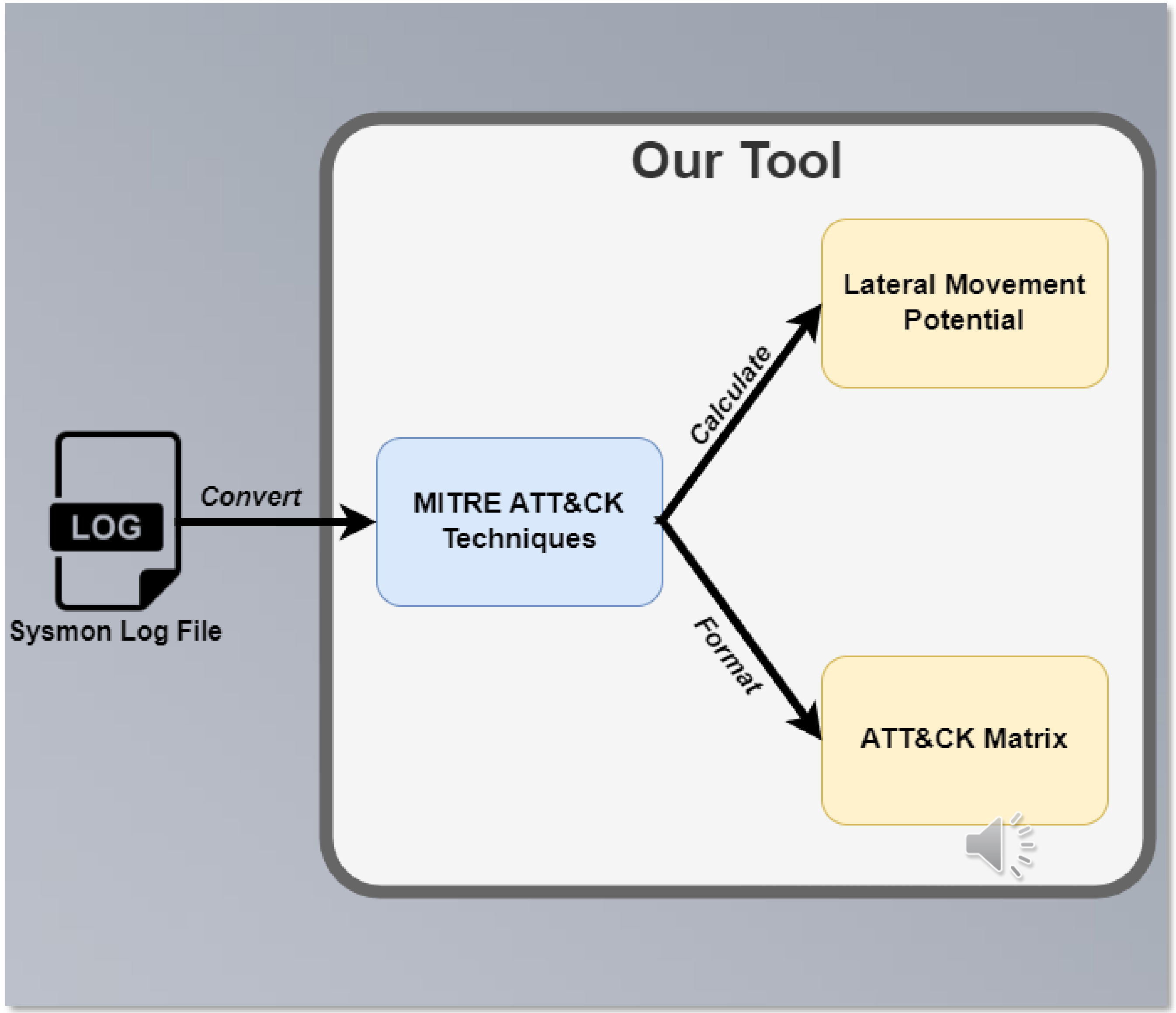
Sample Score

1.2	1.4	2.5

Tool Details

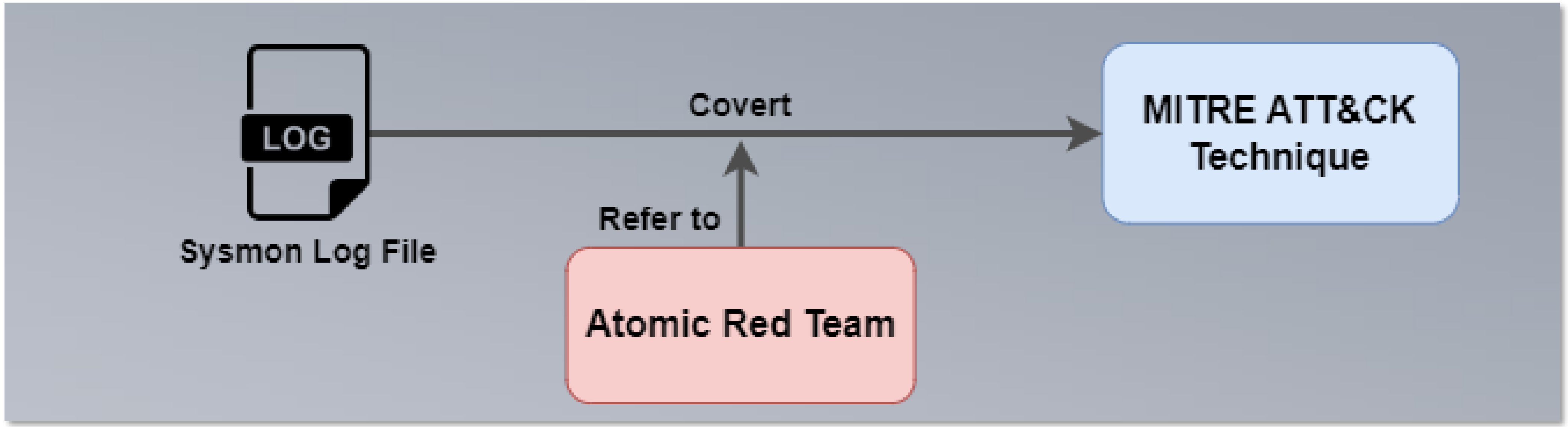
Overview

- Convert Sysmon log to ATT&CK Techniques
- Arrange ATT&CK matrix format
- Calculate Lateral movement potential



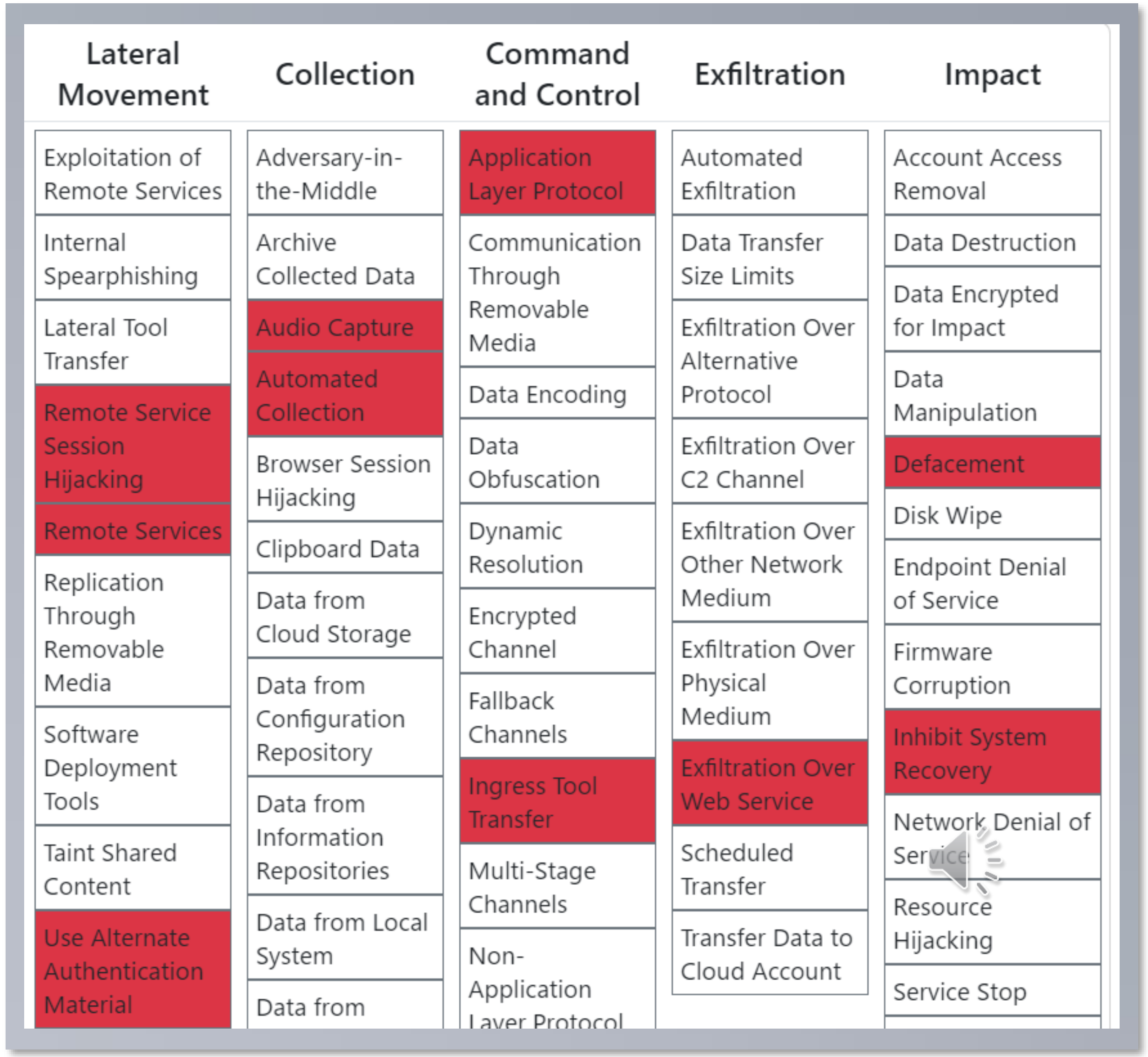
Function 1: Convert Sysmon Log to ATT&CK Technique

- It consults Atomic Red Team information, extracts from the Log those that apply to the Techniques and converts them.
  - We have created a database that shows the relationship between ATT&CK and Atomic Red Team.



Function 2: Arrange ATT&CK Matrix format

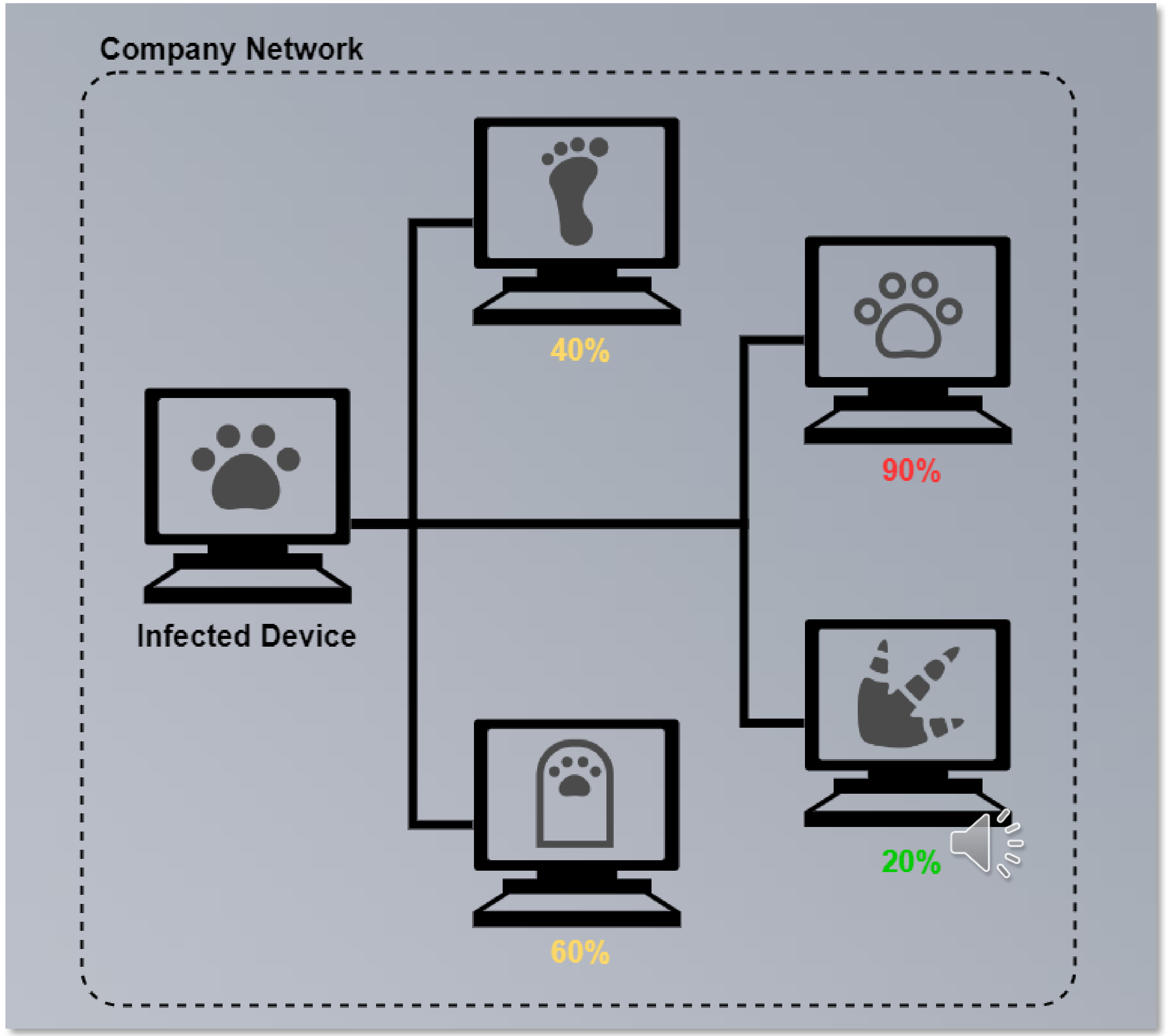
- It plots the converted Technique on the ATT&CK Matrix and displays the corresponding Technique in color.
- Seeing it in matrix format makes it easy to review the tactic phases of attacks.



Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Lateral Tool Transfer	Audio Capture	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Remote Service Session Hijacking	Automated Collection	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Remote Services	Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Replication Through Removable Media	Clipboard Data	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Taint Shared Content	Data from Configuration Repository	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Use Alternate Authentication Material	Data from Information Repositories	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
	Data from Local System	Non-Application Layer Protocol		Network Denial of Service
	Data from			Resource Hijacking
				Service Stop

Function 3: Calculate Lateral movement Potential

- Our tool allows multiple Sysmon Log entries.
  - One log for an infected device and up to 10 logs for possible Lateral movement devices.
- After converting the infected log and the other logs to Technique, we find the similarity between them using the quantification theory type 3.



Demonstration

Insert Demo Video

Conclusion

Future Work

- Our tool can effortlessly assess the Lateral movement potential of each device using multiple Sysmon logs.
- However, there are two drawbacks.
  - Computational complexity
  - Similarity calculation

Future Work

- Computational complexity
  - This tool proves to be valuable in larger and more complex environments
    - Easily detect Lateral movement
  - However, increasing the number of logs leads to longer processing times to obtain results.
    - Therefore, the current upload limit is set to a maximum of 10 logs.
  - Optimization of the program is necessary.

Future Work

- Similarity calculation
  - There are limitations to the method of measuring similarity by simply comparing the techniques used in initial infection devices and other devices.
    - Initial infection devices possess unique techniques used during network intrusions and Lateral movements.
  - New parameters are needed to bridge the gap between initial infection devices and other devices.

Summary

- We propose a web application that converts Sysmon logs into MITRE ATT&CK techniques and calculates the probability of Lateral movement based on similarities.
- Our tool converts contributes to quickly defending against attacks.

Thank you for listening.

Any question?