

Automated ATT&CK Technique Chaining

37th Annual FIRST Conference

Presented by Martin Eian
June 27th 2025

A Norwegian in Denmark

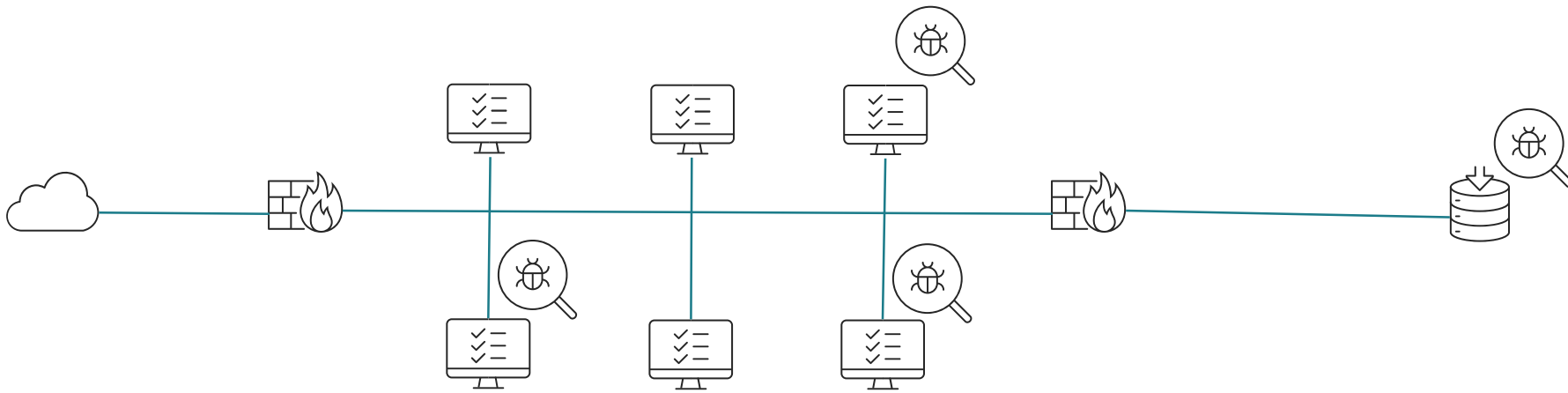
grine

Agenda

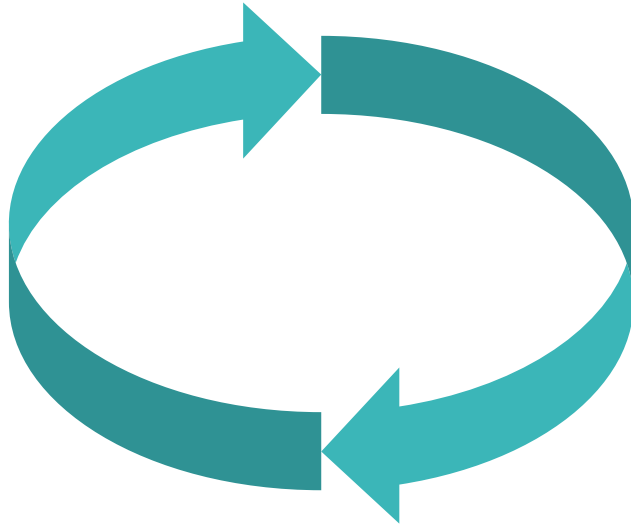


- Incident Response and MITRE ATT&CK
- A Semantic Model of Technique Dependencies
- A Data-Driven Model for Technique Chains
- Discussion and Conclusions

Incident Response



Incident Response



Incident Response Questions

- What did most likely happen prior to this observation?
- What are the adversary's most likely next steps given this observation?

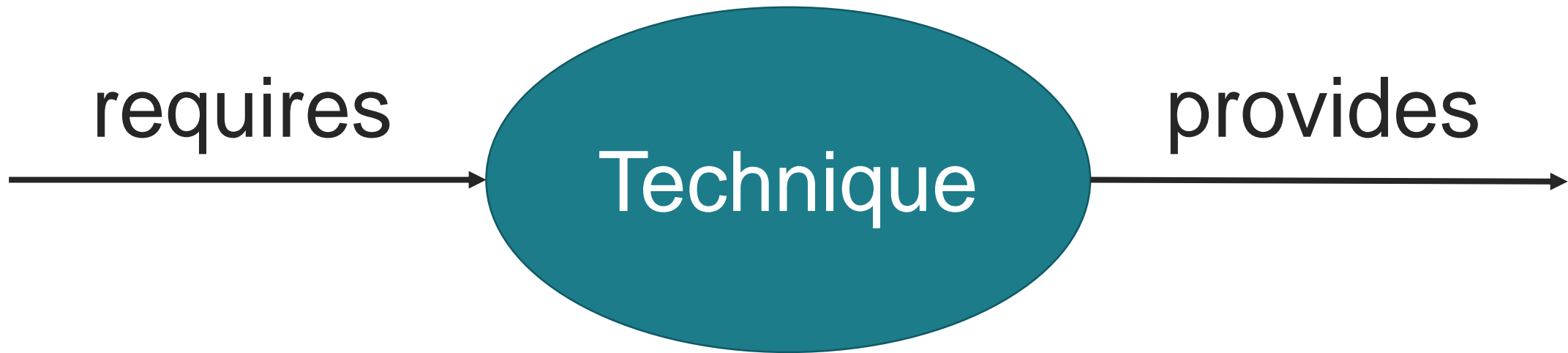
“MITRE ATT&CK is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary’s attack lifecycle and the platforms they are known to target.”

ATT&CK®

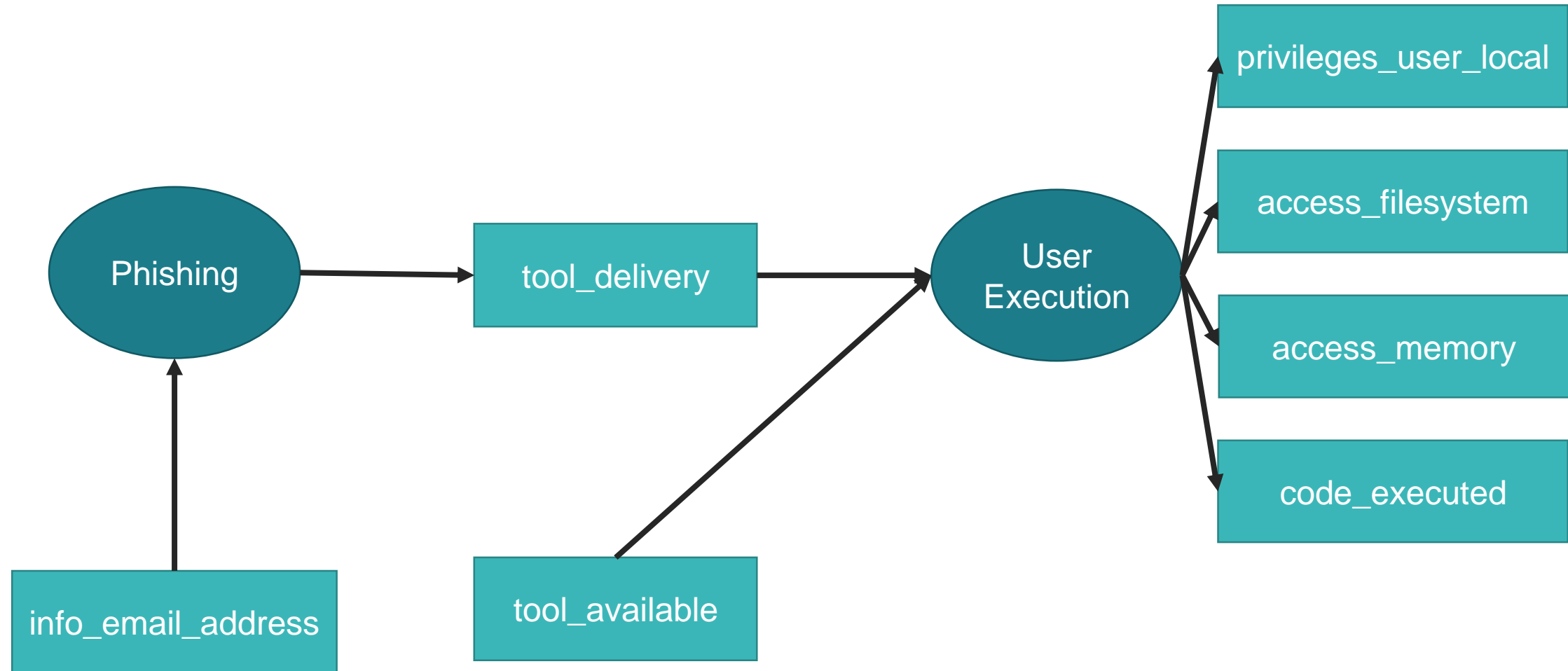
Incident Response Information Sharing – Cyber Threat Intelligence (CTI)

- Human readable reports
- Indicator lists
- Technique lists

A Semantic Model of Technique Dependencies



Example: Phishing and User Execution



Approach

1. Develop vocabulary of abilities
2. Review all (sub-)techniques
 - Define “requires” and “provides”
3. Develop tool
 - <https://github.com/mnemonic-no/provreq>

Example Tool Execution

Abilities

Stage

Techniques


Example Tool Execution

Abilities

Stage	Techniques
1	Gather Victim Identity Information: Email Addresses
	Obtain Capabilities: Malware

Example Tool Execution

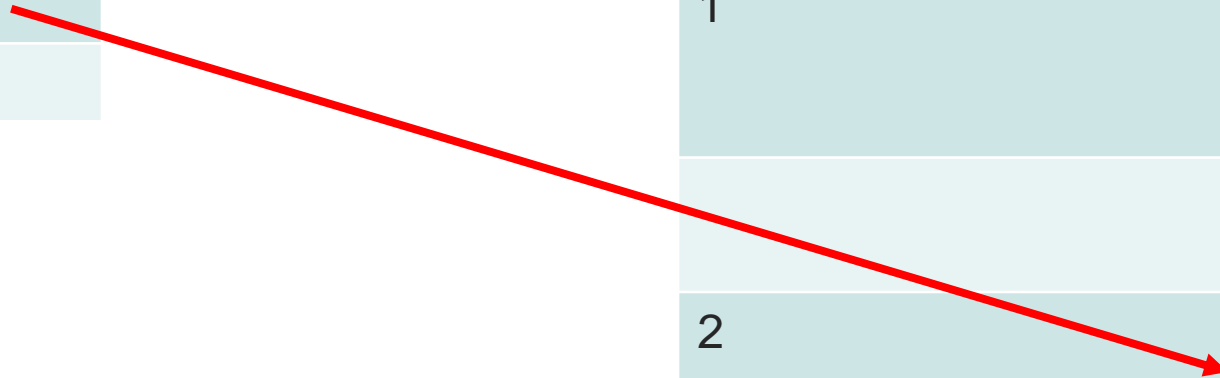
Abilities	Stage	Techniques
info_email_address ←	1	Gather Victim Identity Information: Email Addresses
tool_available ←		Obtain Capabilities: Malware



Example Tool Execution

Abilities
info_email_address
tool_available

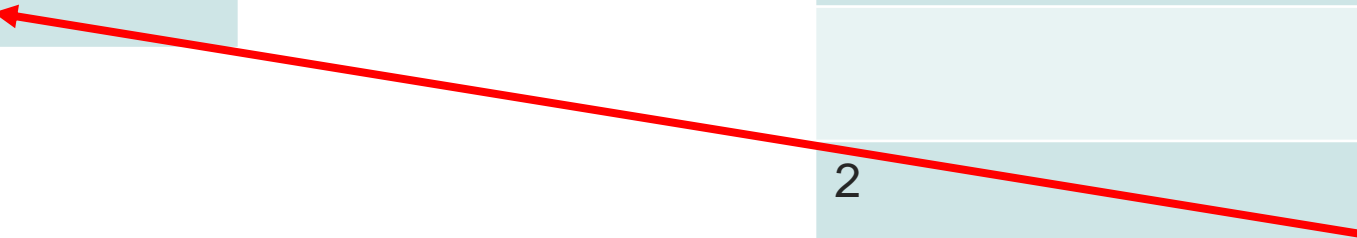
Stage	Techniques
1	Gather Victim Identity Information: Email Addresses
	Obtain Capabilities: Malware
2	Phishing: Spearphishing Attachment



Example Tool Execution

Abilities
info_email_address
tool_available
tool_delivery

Stage	Techniques
1	Gather Victim Identity Information: Email Addresses
	Obtain Capabilities: Malware
2	Phishing: Spearphishing Attachment




Example Tool Execution

Abilities
info_email_address
tool_available
tool_delivery

Stage	Techniques
1	Gather Victim Identity Information: Email Addresses
	Obtain Capabilities: Malware
2	Phishing: Spearphishing Attachment
3	User Execution

Example Tool Execution

Abilities	Stage	Techniques
info_email_address	1	Gather Victim Identity Information: Email Addresses
tool_available		
tool_delivery		
access_filesystem		Obtain Capabilities: Malware
access_memory	2	Phishing: Spearphishing Attachment
code_executed		
privileges_user_local	3	User Execution



The diagram illustrates the mapping of techniques to abilities. Red arrows originate from the 'User Execution' technique in Stage 3 and point to the following abilities: 'access_filesystem', 'access_memory', 'code_executed', and 'privileges_user_local'.

Example Tool Execution

Abilities
info_email_address
tool_available
tool_delivery
access_filesystem
access_memory
code_executed
privileges_user_local

Stage	Techniques
1	Gather Victim Identity Information: Email Addresses
	Obtain Capabilities: Malware
2	Phishing: Spearphishing Attachment
3	User Execution

Example Output: SolarWinds Incident

stage	techniques	new promises @end-of-stage	tactics
Attack stage 1	Develop Capabilities (Resource Development) Develop Capabilities:Malware (Resource Development) Domain Trust Discovery (Discovery) Obtain Capabilities (Resource Development) Obtain Capabilities:Code Signing Certificates (Resource Development) Supply Chain Compromise (Initial Access) Supply Chain Compromise:Compromise Software Supply Chain (Initial Access)	exploit_available info_domain_trust infrastructure_certificate privileges_user_local tool_available tool_delivery	Discovery Initial Access Resource Development
Attack stage 2	Command and Scripting Interpreter (Execution) Command and Scripting Interpreter:PowerShell (Execution) Command and Scripting Interpreter:Windows Command Shell (Execution) Scheduled Task/Job (Execution,Persistence,Privilege Escalation)	defense_evasion execute_code file_transfer persistence	Execution Persistence Privilege Escalation
Attack stage 3	Application Layer Protocol (Command and Control) Application Layer Protocol:Web Protocols (Command and Control)	access_filesystem access_host access_network command_and_control	Command and Control
Attack stage 4	Account Discovery: Local Account (Discovery) Dynamic Resolution (Command and Control) [*] Dynamic Resolution:Domain Generation Algorithms (Command and Control) [*] Event Triggered Execution (Persistence,Privilege Escalation) [*] Ingress Tool Transfer (Command and Control) [*] Permission Groups Discovery (Discovery) Permission Groups Discovery:Domain Groups (Discovery) Process Discovery (Discovery) Unsecured Credentials (Credential Access) Unsecured Credentials:Private Keys (Credential Access)	credentials_user_domain credentials_user_local credentials_user_thirdparty info_groupname info_process_info info_target_employee info_username	Command and Control Credential Access Discovery Persistence Privilege Escalation
Attack stage 5	Account Manipulation:Additional Cloud Credentials (Persistence) [*] Cloud Service Discovery (Discovery) Email Collection:Remote Email Collection (Collection)	info_cloud_services privileges_user_domain target_information	Collection Discovery Persistence
Attack stage 6	Archive Collected Data (Collection) Archive Collected Data:Archive via Utility (Collection) Data Staged (Collection) Data Staged:Remote Data Staging (Collection) Exfiltration Over Web Service (Exfiltration)	objective_exfiltration staged_data	Collection Exfiltration

Incident Response Questions

- What did most likely happen prior to this observation?
- What are the adversary's most likely next steps given this observation?

A Data-Driven Model for Technique Chains

Approach

1. Collect available data on observed technique execution «in the wild»
2. Compute statistics for use in our tool
 - How many times have a given technique provided a given ability?
3. Run Markov chain Monte Carlo simulations to explore the most likely attack chains

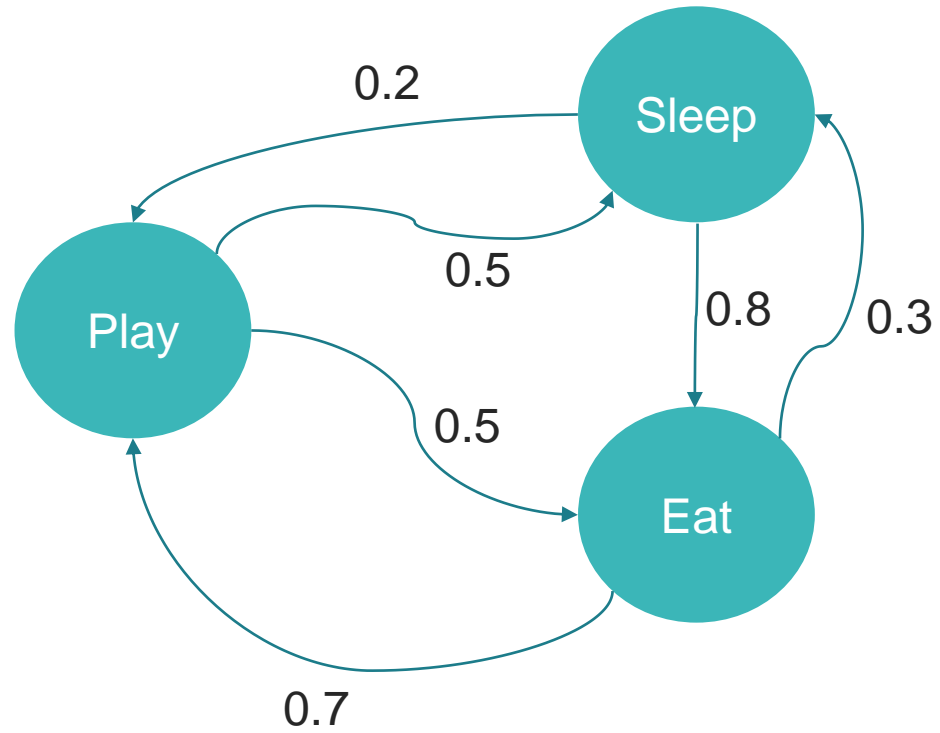
Data sources

- ATT&CK Adversary Groups
- ATT&CK Campaigns
- ATT&CK Navigator Layers from incident reports
- Published Adversary Emulation Plans (CTID)
- Unit 42 Adversary Playbooks (Palo Alto)
- <https://thedfirreport.com/>

Statistics

```
"tool_available": {  
  "T1587.001": 14,  
  "T1588.002": 59,  
  "T1588.001": 9,  
  "T1588.003": 5,  
  "T1588.004": 2,  
  "T1588.006": 1,  
  "T1587.002": 2,  
  "T1587.003": 2,  
  "T1587": 3,  
  "T1588": 2,  
  "T1588.005": 1  
},
```

Markov Chain



Markov Chain

Technique	Requires	Provides
User Execution	tool_available	access_filesystem
	tool_delivery	access_memory
		code_executed
		privileges_user_local

Markov Chain

```
"tool_available": {  
  "T1587.001": 14,  
  "T1588.002": 59,  
  "T1588.001": 9,  
  "T1588.003": 5,  
  "T1588.004": 2,  
  "T1588.006": 1,  
  "T1587.002": 2,  
  "T1587.003": 2,  
  "T1587": 3,  
  "T1588": 2,  
  "T1588.005": 1  
},
```

Technique	Requires	Provides
User Execution	tool_available	access_filesystem
	tool_delivery	access_memory
		code_executed
		privileges_user_local

Markov Chain

Technique	Requires	Provides
User Execution	tool_available	access_filesystem
Obtain Capabilities: Tool	tool_delivery	access_memory
		code_executed
		privileges_user_local
		tool_available

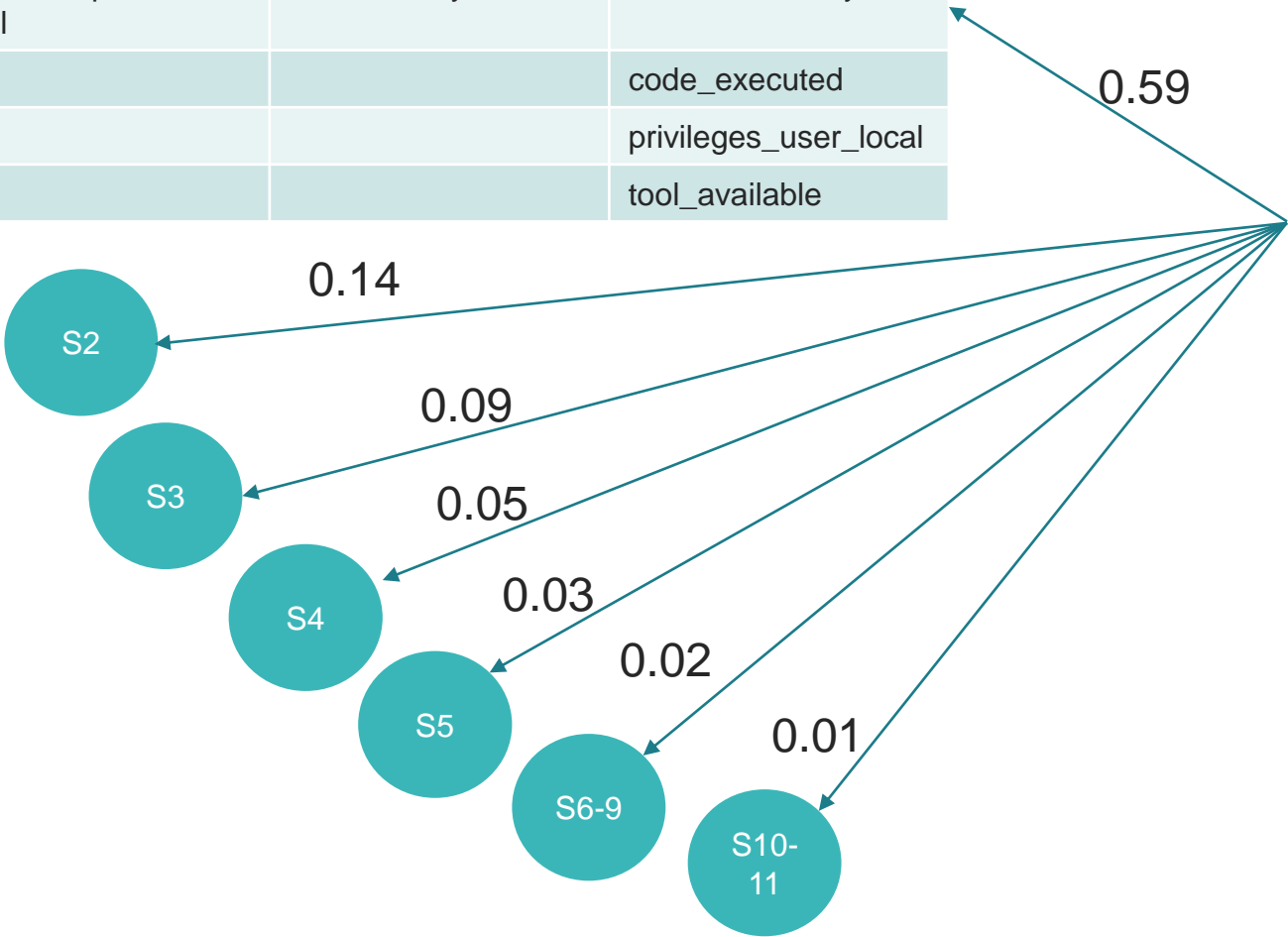
0.59

Technique	Requires	Provides
User Execution	tool_available	access_filesystem
	tool_delivery	access_memory
		code_executed
		privileges_user_local

Markov Chain

Technique	Requires	Provides
User Execution	tool_available	access_filesystem
Obtain Capabilities: Tool	tool_delivery	access_memory
		code_executed
		privileges_user_local
		tool_available

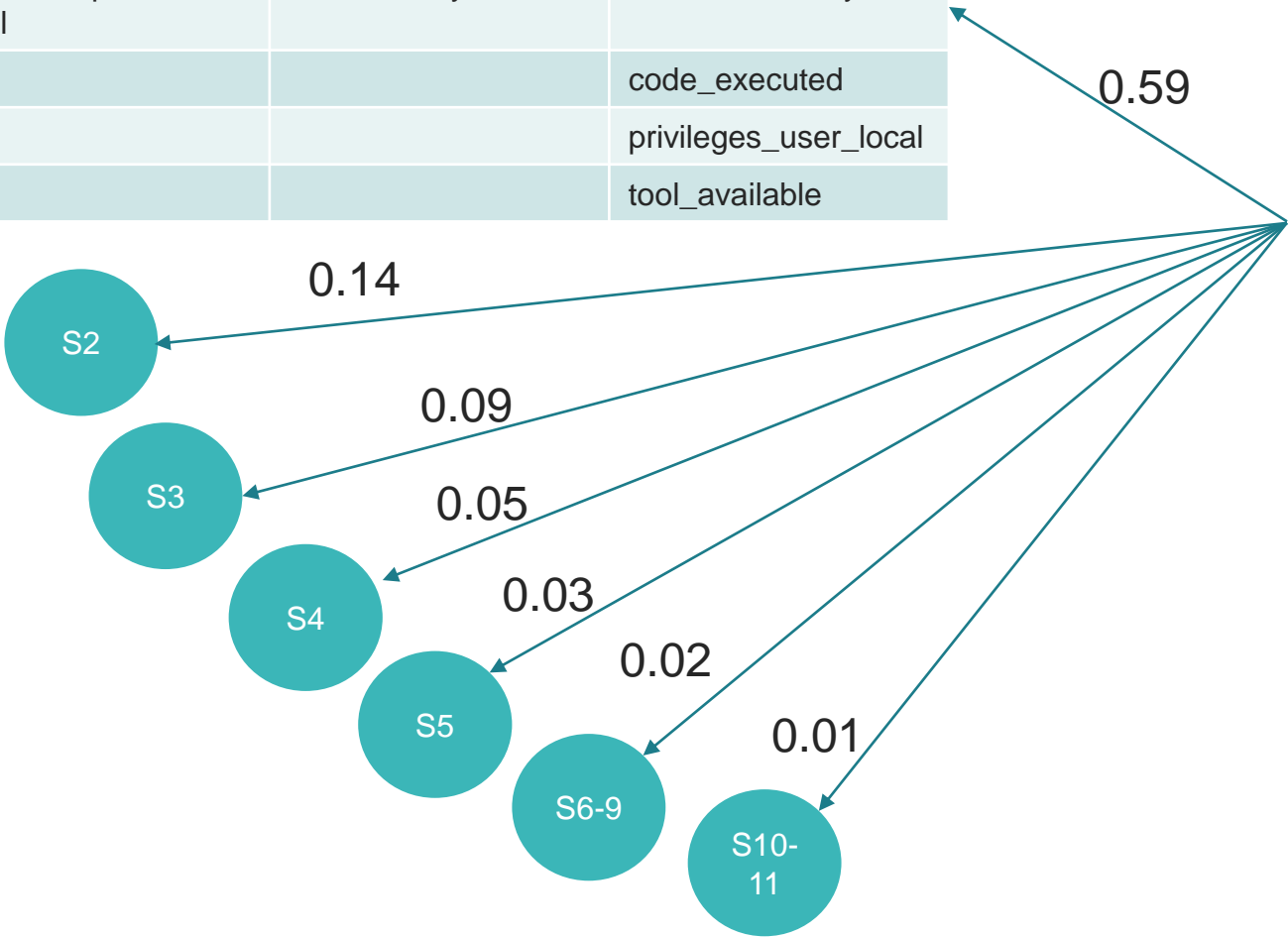
Technique	Requires	Provides
User Execution	tool_available	access_filesystem
	tool_delivery	access_memory
		code_executed
		privileges_user_local



Markov Chain

Technique	Requires	Provides
User Execution	tool_available	access_filesystem
Obtain Capabilities: Tool	tool_delivery	access_memory
		code_executed
		privileges_user_local
		tool_available

Technique	Requires	Provides
User Execution	tool_available	access_filesystem
	tool_delivery	access_memory
		code_executed
		privileges_user_local



Example: User Execution

69.77% (n=69769)

stage	techniques	new promises @end-of-stage	tactics
1	Phishing (Initial Access)	credentials_user_domain credentials_user_local tool_delivery	Initial Access
2	User Execution (Execution)	access_filesystem access_memory code_executed privileges_user_local	Execution

Example: Exfiltration Over C2 Channel

2.02% (n=2018)

stage	techniques	new promises @end-of-stage	tactics
1	Phishing (Initial Access)	credentials_user_domain credentials_user_local tool_delivery	Initial Access
2	User Execution (Execution)	access_filesystem access_memory code_executed privileges_user_local	Execution
3	Abuse Elevation Control Mechanism (Defense Evasion,Privilege Escalation) Application Layer Protocol (Command and Control)	access_network adversary_controlled_communication_channel defense_evasion file_transfer persistence privileges_admin_local privileges_system_local	Command and Control Defense Evasion Privilege Escalation
4	OS Credential Dumping (Credential Access)	access_password_store credentials_users	Credential Access
5	Remote Services (Lateral Movement)	moved_laterally	Lateral Movement
6	Data From Local System (Collection)	target_information	Collection
7	Exfiltration Over C2 Channel (Exfiltration)	objective_exfiltration	Exfiltration

Incident Response Questions

- What did most likely happen prior to this observation?
- What are the adversary's most likely next steps given this observation?

Discussion and Conclusions

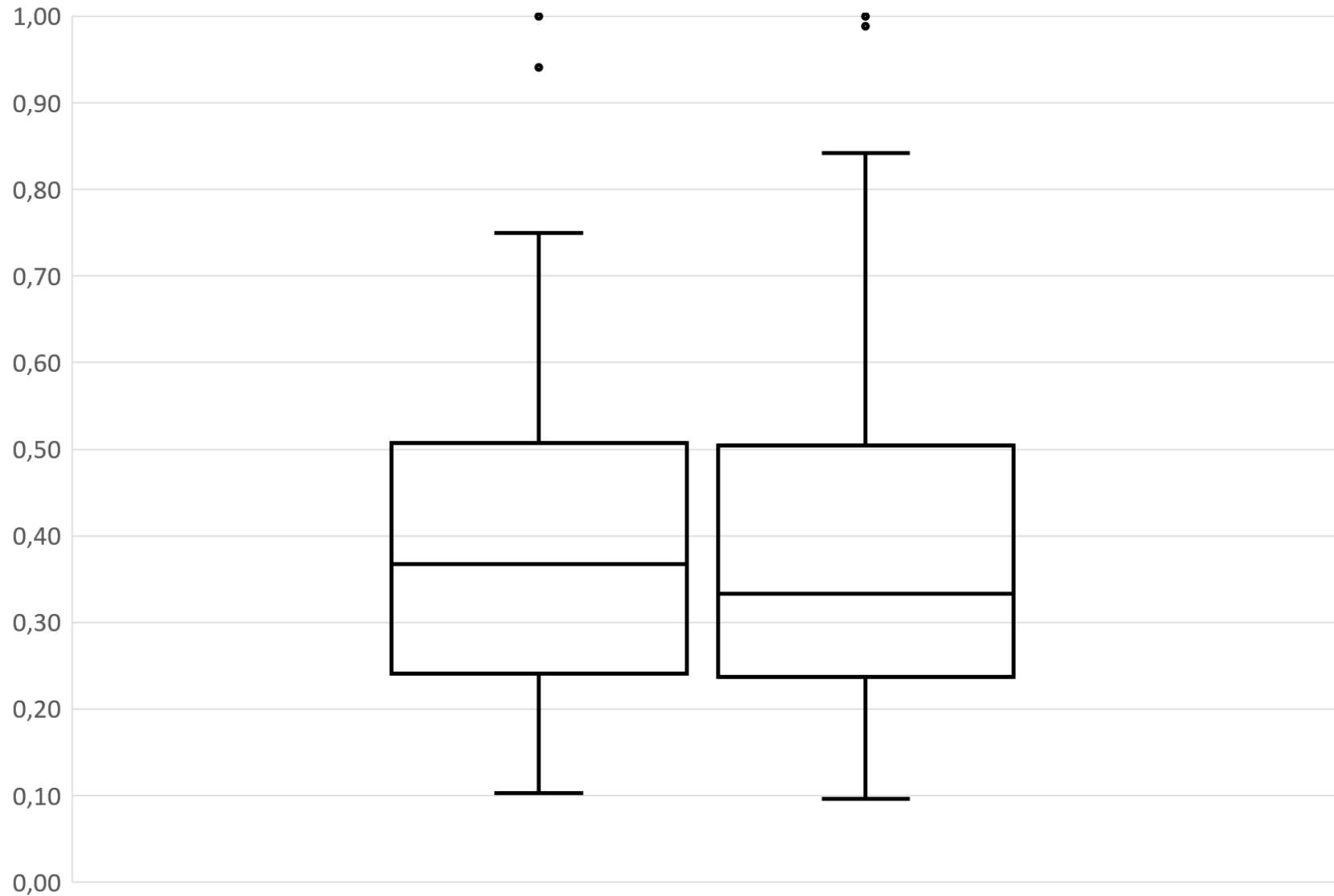
Weaknesses

- Bias
 - Human
 - Visibility
 - Detection coverage
- Not enough training data
- No infrastructure model
- Does not work on long attack chains

Related work: MITRE Engenuity Technique Inference Engine (TIE)

- Recommender system
 - No concept of «before» and «after»
- Public training data set
 - 6000+ incidents

Evaluation of TIE Data Set



Paper and Open Source Tools

- <https://dl.acm.org/doi/10.1145/3696013>
- <https://github.com/mnemonic-no/provreq>
- <https://github.com/mnemonic-no/provreq-mcmc>

THANK YOU!



Martin Eian
meian@mnemonic.no



Geir Skjøtskift
geir@mnemonic.no



Siri Bromander
siri@mnemonic.no