A Pragmatic Approach to Build a Threat Landscape

2025-10-22 | Thomas Patzke

TLP:CLEAR

Typical Situation

Questions from stakeholders:

- What are the threats relevant to us?
- Who are the threat actors relevant to us?
- Are we affected by this threat everyone is talking about?

Impact

On cyber defense:

- Resources are possibly utilized for less relevant things.
- Analysts skipping around between random topics.

On the organization:

- Money is spent to mitigate threats with low relevance.

Lets Build Something to Answer These Questions

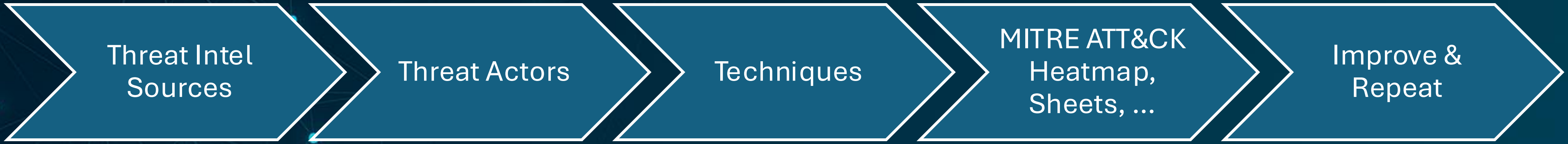
Requirements:

- Practical Applicable
- Actionable
- It should reflect our reality.
- We need to speak a language everyone understands & accepts
- Reproducible results

Constraints:

- Cost savings
- Low effort

High Level Approach



Threat Intel Sources

Threat Actors

Techniques

MITRE ATT&CK Heatmap, Sheets, …

Improve & Repeat

Collection & Sources

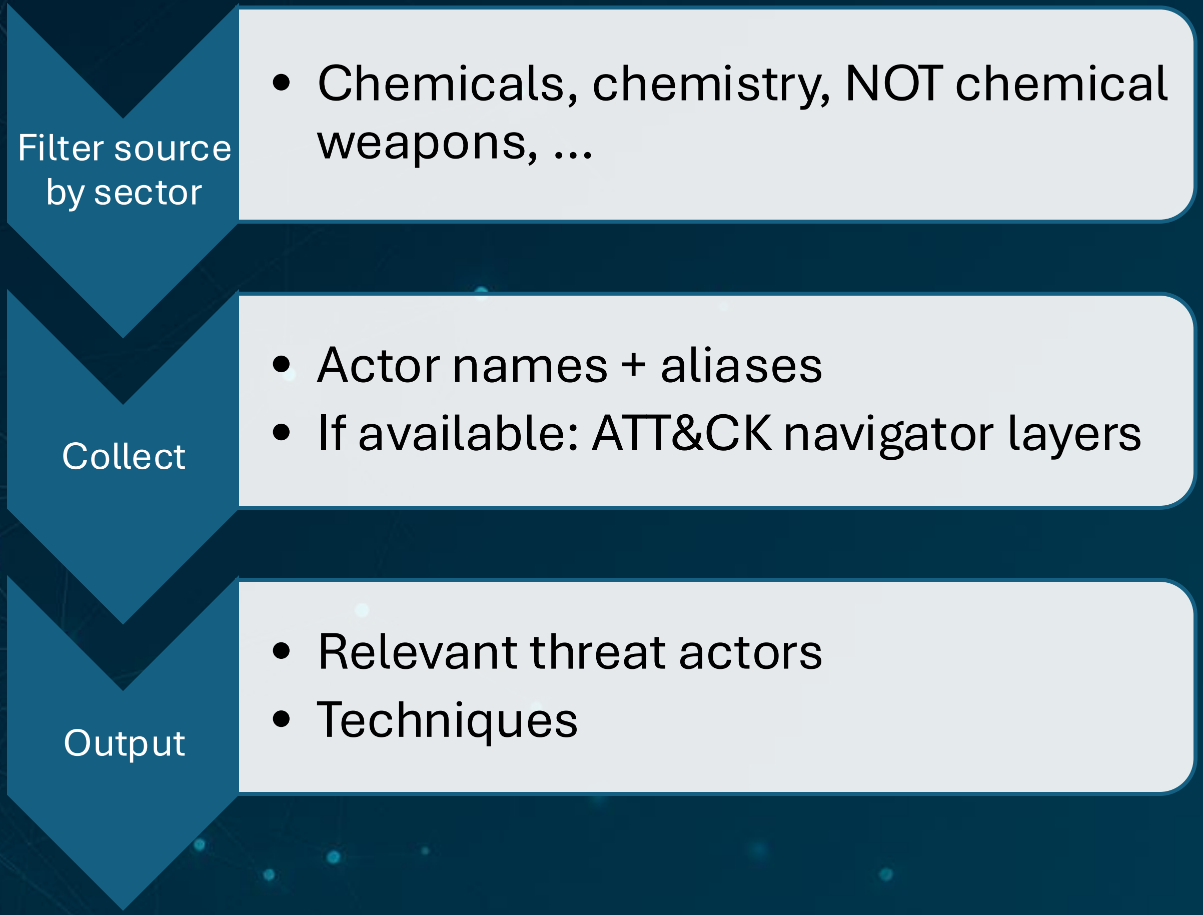
“Take what we have” approach:

- Communities: direct exchange, MISP
- open source or free: MITRE ATT&CK, ORKL, MISP Galaxies
- Subscribed services: Feedreader (Categorization&TTPs based on OSINT)
- What vendors give to us: actor profiles, regular reports.
- Own observations

How to select relevant information?

- Sector. Challenge: which one?
  - Chemicals – not much threat intel associated with the chemical sector or not explicit.
  - Is the pharma or biotech sector relevant if you supply them with chemicals?
  - Inaccuracy: some sources map chemical companies to the manufacturing sector.
- Opportunistic threats
- Is a threat actor with last documented activity 10 years ago still relevant?

Collection: Relevant Actors



Filter source by sector

- Chemicals, chemistry, NOT chemical weapons, …

Collect

- Actor names + aliases
- If available: ATT&CK navigator layers

Output

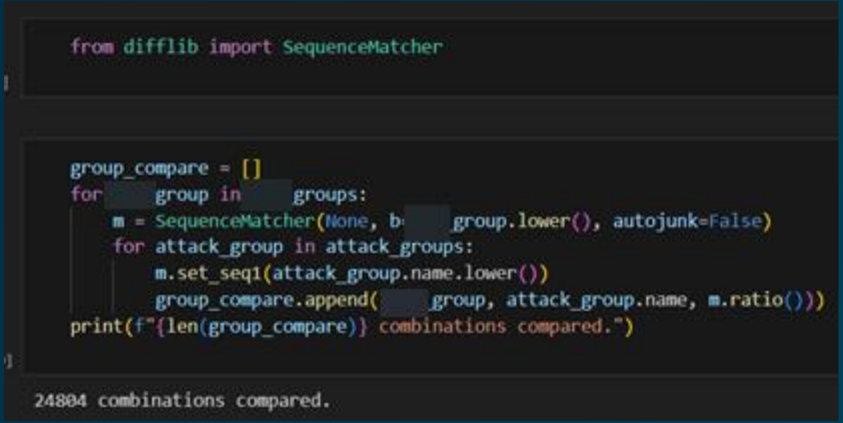
- Relevant threat actors
- Techniques

Introduction of own Observations to the Data

- Your own cases = your own (very realistic) threats, ideal for this purpose.
- Introduces some threats that are underrepresented in reporting or not reported in sector.
- Introduces techniques from the reconnaissance and resource development tactics.
- Also introduces opportunistic threats, e.g. initial access brokers, ransomware actors, traffic distribution systems.
- Weighted with a bonus in scoring on introduced techniques. What we observe is definitely a threat.
- Information must be actively collected.

From Actors to Techniques: Analysis

- Clustering & normalizing actors
  - “APT41” vs “APT 41”: Python SequenceMatcher
  - “APT41”, “Winnti”, “WICKED PANDA”, …
    - Alias mappings in sources
    - But: clusters are not equal – accepted inaccuracy.
- Mapping actors to techniques: vendor threat actor profiles, Newsfeed, ATT&CK group to technique mappings.



```
from difflib import SequenceMatcher
```

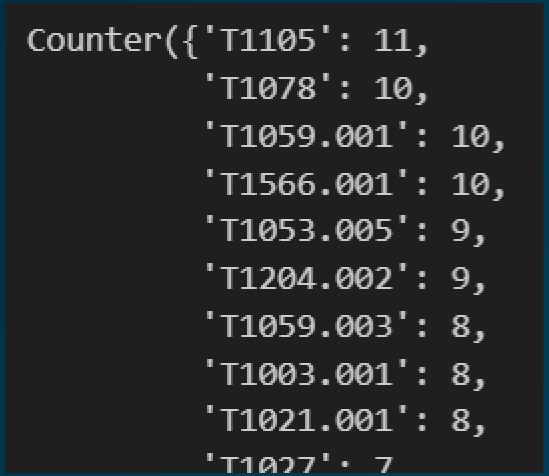
```
group_compare = []
for [redacted]group in [redacted]groups:
    m = SequenceMatcher(None, b[redacted]group.lower(), autojunk=False)
    for attack_group in attack_groups:
        m.set_seq1(attack_group.name.lower())
        group_compare.append([redacted]group, attack_group.name, m.ratio()))
print(f"{len(group_compare)} combinations compared.")
```

```
24804 combinations compared.
```

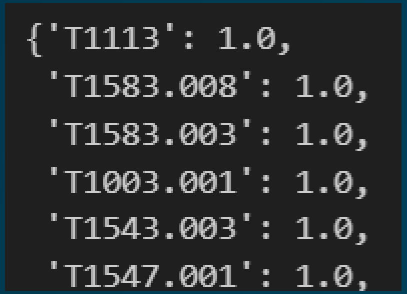
Analysis

Confidence score: how confident are we that a technique is relevant?

- Quantitative: # of actors mapped to technique.
- Own observations get full confidence + 20% bonus
- Finally scores are normalized to 100



```
Counter({'T1105': 11,
         'T1078': 10,
         'T1059.001': 10,
         'T1566.001': 10,
         'T1053.005': 9,
         'T1204.002': 9,
         'T1059.003': 8,
         'T1003.001': 8,
         'T1021.001': 8,
         'T1027': 7
```

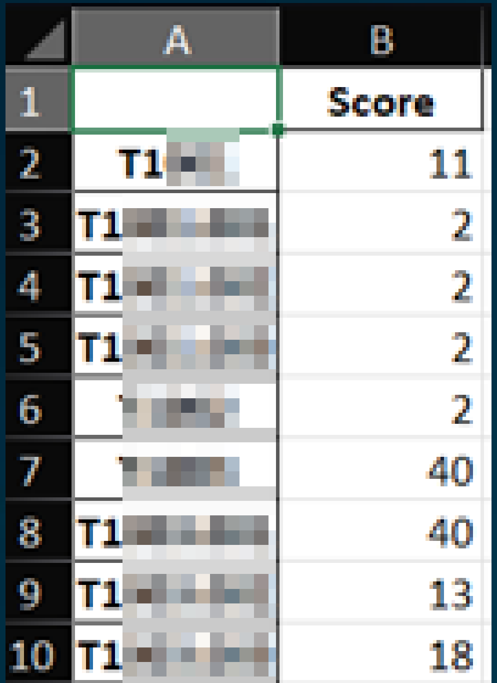


```
{'T1113': 1.0,
 'T1583.008': 1.0,
 'T1583.003': 1.0,
 'T1003.001': 1.0,
 'T1543.003': 1.0,
 'T1547.001': 1.0,
```

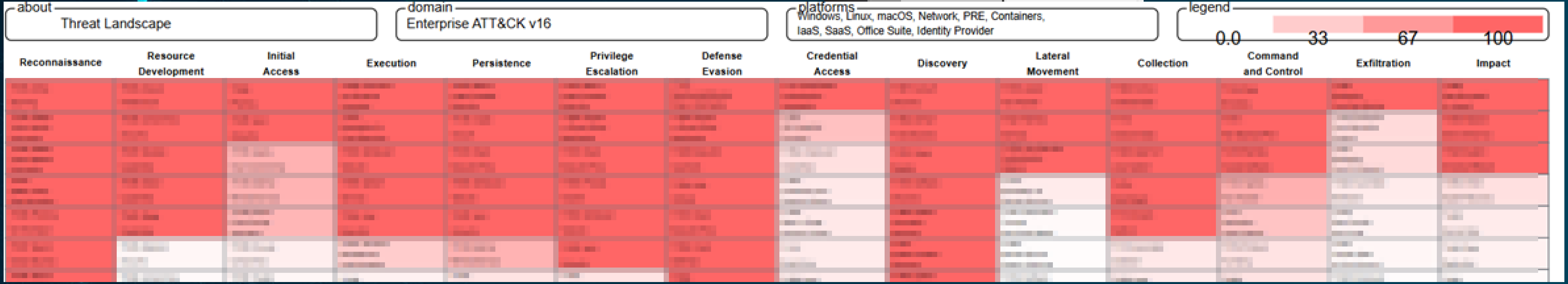
Creation of Reports

Different formats for different stakeholders:

- ATT&CK Navigator layer
- Export as PNG and SVG
- Simple spreadsheet with technique-score-mapping.
- Advanced spreadsheet with mappings to mitigations, data sources, ART tests etc.



	A	B
1		Score
2	T1[redacted]	11
3	T1[redacted]	2
4	T1[redacted]	2
5	T1[redacted]	2
6	[redacted]	2
7	[redacted]	40
8	T1[redacted]	40
9	T1[redacted]	13
10	T1[redacted]	18



about: Threat Landscape

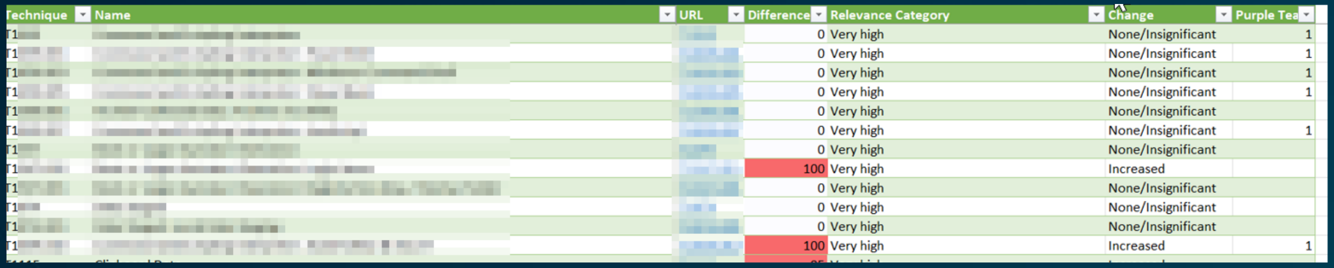
domain: Enterprise ATT&CK v16

platforms: Windows, Linux, macOS, Network, PRE, Containers, IaaS, SaaS, Office Suite, Identity Provider

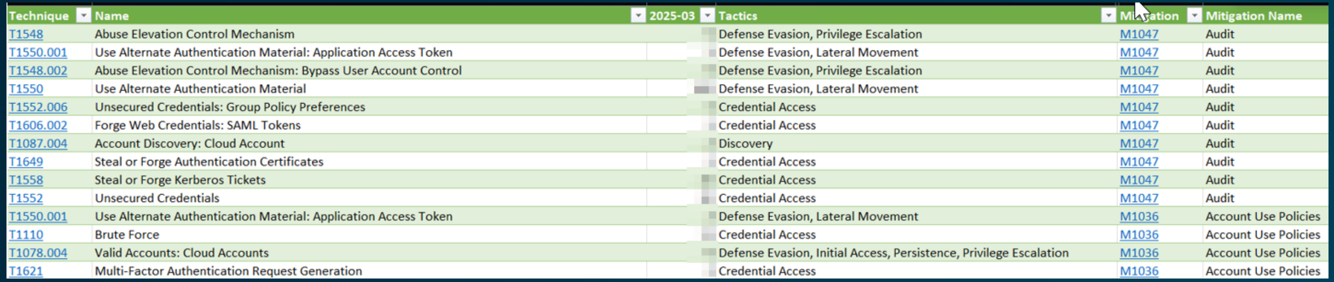
legend: 0.0 33 67 100

Advanced Spreadsheet

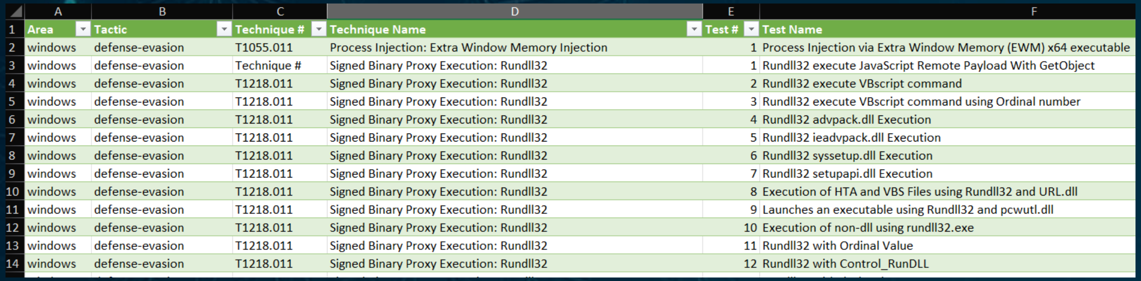
- Techniques with relevance categories, changes, …
- Mapping to mitigations
- Mapping to data sources
- Mapping to Atomic Red Team test cases



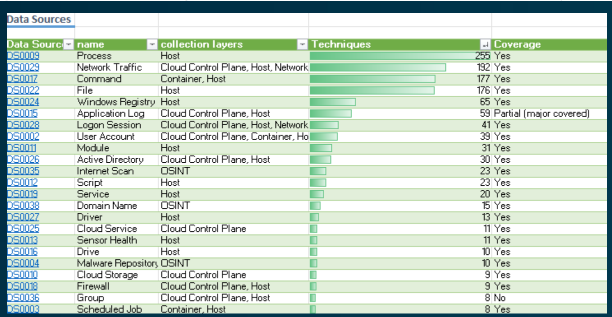
Technique	Name	URL	Difference	Relevance Category	Change	Purple Tea
T1[redacted]	[redacted]	[redacted]	0	Very high	None/Insignificant	1
T1[redacted]	[redacted]	[redacted]	0	Very high	None/Insignificant	1
T1[redacted]	[redacted]	[redacted]	0	Very high	None/Insignificant	1
T1[redacted]	[redacted]	[redacted]	0	Very high	None/Insignificant	1
T1[redacted]	[redacted]	[redacted]	0	Very high	None/Insignificant	
T1[redacted]	[redacted]	[redacted]	0	Very high	None/Insignificant	1
T1[redacted]	[redacted]	[redacted]	0	Very high	None/Insignificant	
T1[redacted]	[redacted]	[redacted]	100	Very high	Increased	
T1[redacted]	[redacted]	[redacted]	0	Very high	None/Insignificant	
T1[redacted]	[redacted]	[redacted]	0	Very high	None/Insignificant	
T1[redacted]	[redacted]	[redacted]	0	Very high	None/Insignificant	
T1[redacted]	[redacted]	[redacted]	100	Very high	Increased	1



Technique	Name	2025-03	Tactics	Mitigation	Mitigation Name
T1548	Abuse Elevation Control Mechanism		Defense Evasion, Privilege Escalation	M1047	Audit
T1550.001	Use Alternate Authentication Material: Application Access Token		Defense Evasion, Lateral Movement	M1047	Audit
T1548.002	Abuse Elevation Control Mechanism: Bypass User Account Control		Defense Evasion, Privilege Escalation	M1047	Audit
T1550	Use Alternate Authentication Material		Defense Evasion, Lateral Movement	M1047	Audit
T1552.006	Unsecured Credentials: Group Policy Preferences		Credential Access	M1047	Audit
T1606.002	Forge Web Credentials: SAML Tokens		Credential Access	M1047	Audit
T1087.004	Account Discovery: Cloud Account		Discovery	M1047	Audit
T1649	Steal or Forge Authentication Certificates		Credential Access	M1047	Audit
T1558	Steal or Forge Kerberos Tickets		Credential Access	M1047	Audit
T1552	Unsecured Credentials		Credential Access	M1047	Audit
T1550.001	Use Alternate Authentication Material: Application Access Token		Defense Evasion, Lateral Movement	M1036	Account Use Policies
T1110	Brute Force		Credential Access	M1036	Account Use Policies
T1078.004	Valid Accounts: Cloud Accounts		Defense Evasion, Initial Access, Persistence, Privilege Escalation	M1036	Account Use Policies
T1621	Multi-Factor Authentication Request Generation		Credential Access	M1036	Account Use Policies



	A	B	C	D	E	F
1	Area	Tactic	Technique #	Technique Name	Test #	Test Name
2	windows	defense-evasion	T1055.011	Process Injection: Extra Window Memory Injection	1	Process Injection via Extra Window Memory (EWM) x64 executable
3	windows	defense-evasion	Technique #	Signed Binary Proxy Execution: Rundll32	1	Rundll32 execute JavaScript Remote Payload With GetObject
4	windows	defense-evasion	T1218.011	Signed Binary Proxy Execution: Rundll32	2	Rundll32 execute VBscript command
5	windows	defense-evasion	T1218.011	Signed Binary Proxy Execution: Rundll32	3	Rundll32 execute VBscript command using Ordinal number
6	windows	defense-evasion	T1218.011	Signed Binary Proxy Execution: Rundll32	4	Rundll32 advpack.dll Execution
7	windows	defense-evasion	T1218.011	Signed Binary Proxy Execution: Rundll32	5	Rundll32 ieadvpack.dll Execution
8	windows	defense-evasion	T1218.011	Signed Binary Proxy Execution: Rundll32	6	Rundll32 syssetup.dll Execution
9	windows	defense-evasion	T1218.011	Signed Binary Proxy Execution: Rundll32	7	Rundll32 setupapi.dll Execution
10	windows	defense-evasion	T1218.011	Signed Binary Proxy Execution: Rundll32	8	Execution of HTA and VBS Files using Rundll32 and URL.dll
11	windows	defense-evasion	T1218.011	Signed Binary Proxy Execution: Rundll32	9	Launches an executable using Rundll32 and pcwutl.dll
12	windows	defense-evasion	T1218.011	Signed Binary Proxy Execution: Rundll32	10	Execution of non-dll using rundll32.exe
13	windows	defense-evasion	T1218.011	Signed Binary Proxy Execution: Rundll32	11	Rundll32 with Ordinal Value
14	windows	defense-evasion	T1218.011	Signed Binary Proxy Execution: Rundll32	12	Rundll32 with Control_RunDLL

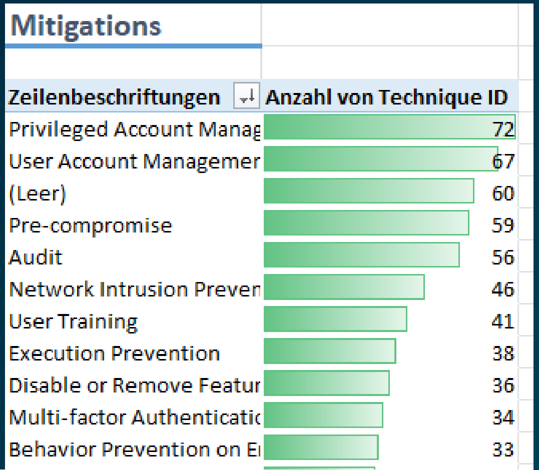


Data Sources

Data Source	name	collection layers	Techniques	Coverage
DS0009	Process	Host	255	Yes
DS0029	Network Traffic	Cloud Control Plane, Host, Network	192	Yes
DS0017	Command	Container, Host	177	Yes
DS0022	File	Host	176	Yes
DS0024	Windows Registry	Host	65	Yes
DS0015	Application Log	Cloud Control Plane, Host	59	Partial (major covered)
DS0028	Logon Session	Cloud Control Plane, Host, Network	41	Yes
DS0002	User Account	Cloud Control Plane, Container, Ho	39	Yes
DS0011	Module	Host	31	Yes
DS0026	Active Directory	Cloud Control Plane, Host	30	Yes
DS0035	Internet Scan	OSINT	23	Yes
DS0012	Script	Host	23	Yes
DS0019	Service	Host	20	Yes
DS0038	Domain Name	OSINT	15	Yes
DS0027	Driver	Host	13	Yes
DS0025	Cloud Service	Cloud Control Plane	11	Yes
DS0013	Sensor Health	Host	11	Yes
DS0016	Drive	Host	10	Yes
DS0004	Malware Repository	OSINT	10	Yes
DS0010	Cloud Storage	Cloud Control Plane	9	Yes
DS0018	Firewall	Cloud Control Plane, Host	9	Yes
DS0036	Group	Cloud Control Plane, Host	8	No
DS0003	Scheduled Job	Container, Host	8	Yes

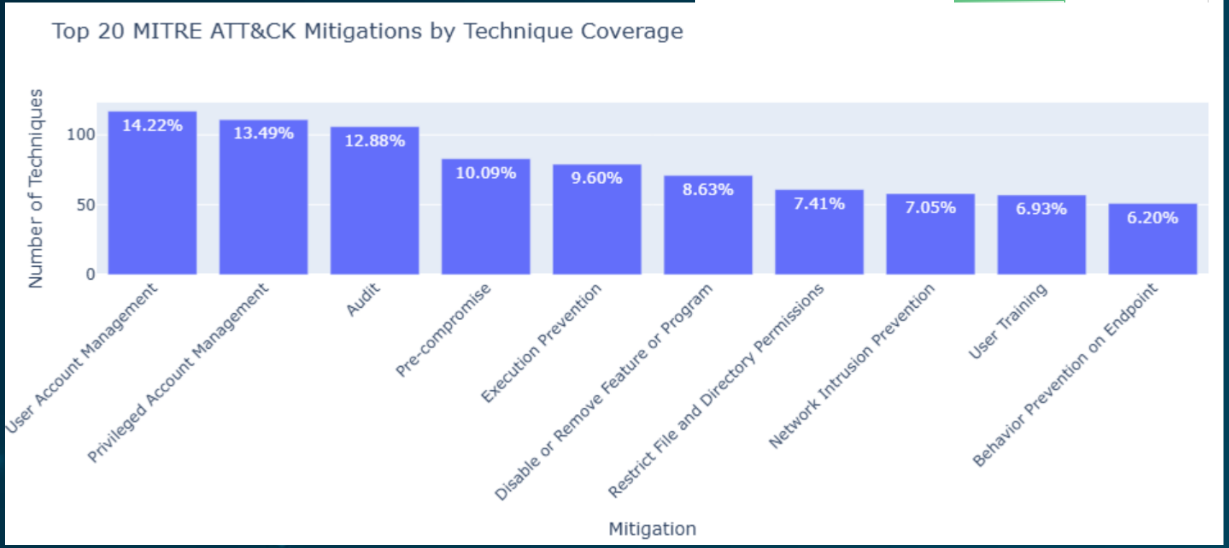
Mitigations

- Mapping of relevant techniques to mitigations as mapped by MITRE.
- Mapped mitigations not necessarily mitigate a technique completely.
  - Defense in depth required
- Some mitigations are very specific, others very generic.
  - Overrepresented mitigations
- Different interpretation of mitigations.



Mitigations

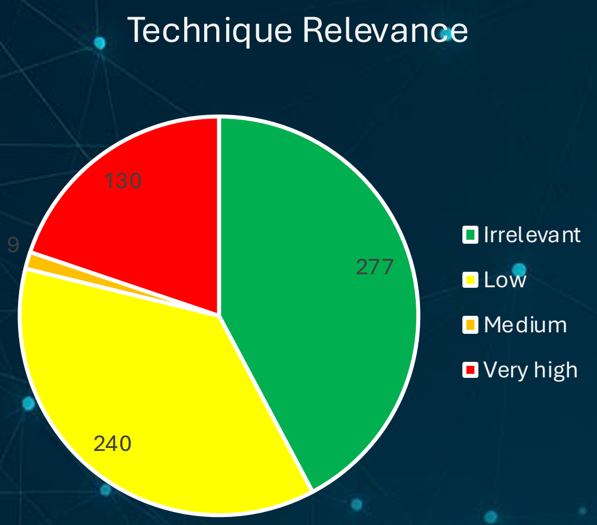
Zeilenbeschriftungen	Anzahl von Technique ID
Privileged Account Manag	72
User Account Managemer	67
(Leer)	60
Pre-compromise	59
Audit	56
Network Intrusion Preven	46
User Training	41
Execution Prevention	38
Disable or Remove Featur	36
Multi-factor Authenticatic	34
Behavior Prevention on E	33

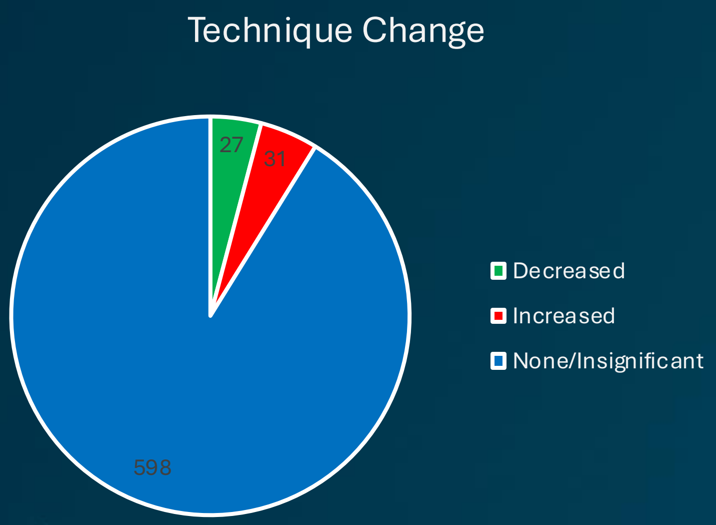


Top 20 MITRE ATT&CK Mitigations by Technique Coverage

Threat Landscape Statistics: Techniques

- 79% of ATT&CK techniques not observed or not/rarely reported for scope.
  → Focus on 21%
- 9% relevance changes between 2023-12 and 2025-03
  → Interval sufficient.





Can we ignore the 79%?

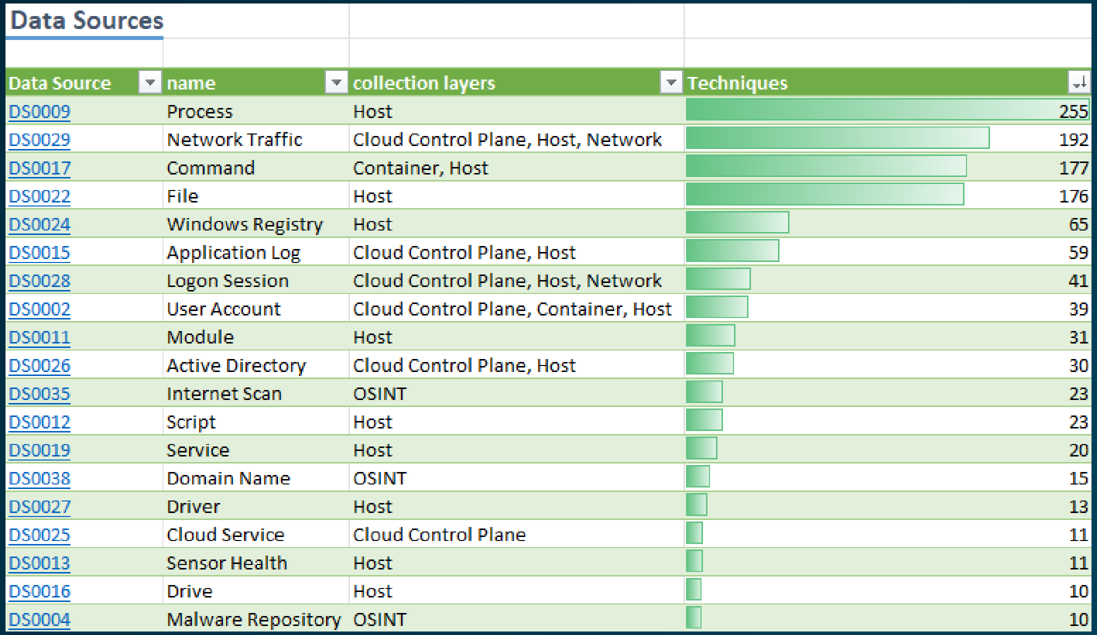
- No!
- Sources are biased:
  - EDR vendor data focuses on endpoint techniques.
  - Mail vendor only sees threats received via mail.
  - Own observations don’t see threats in visibility gaps.
- Threats change & evolve, reporting is behind the development.

Instead:

- Identify gaps
- Focus on the probable but don’t forget the improbable and expect everything.

Mitigations & Data Sources

- Are all relevant techniques covered by data sources for detection and investigation?
- Shows importance of particular logs.
- Justifies expensive high-volume log sources.

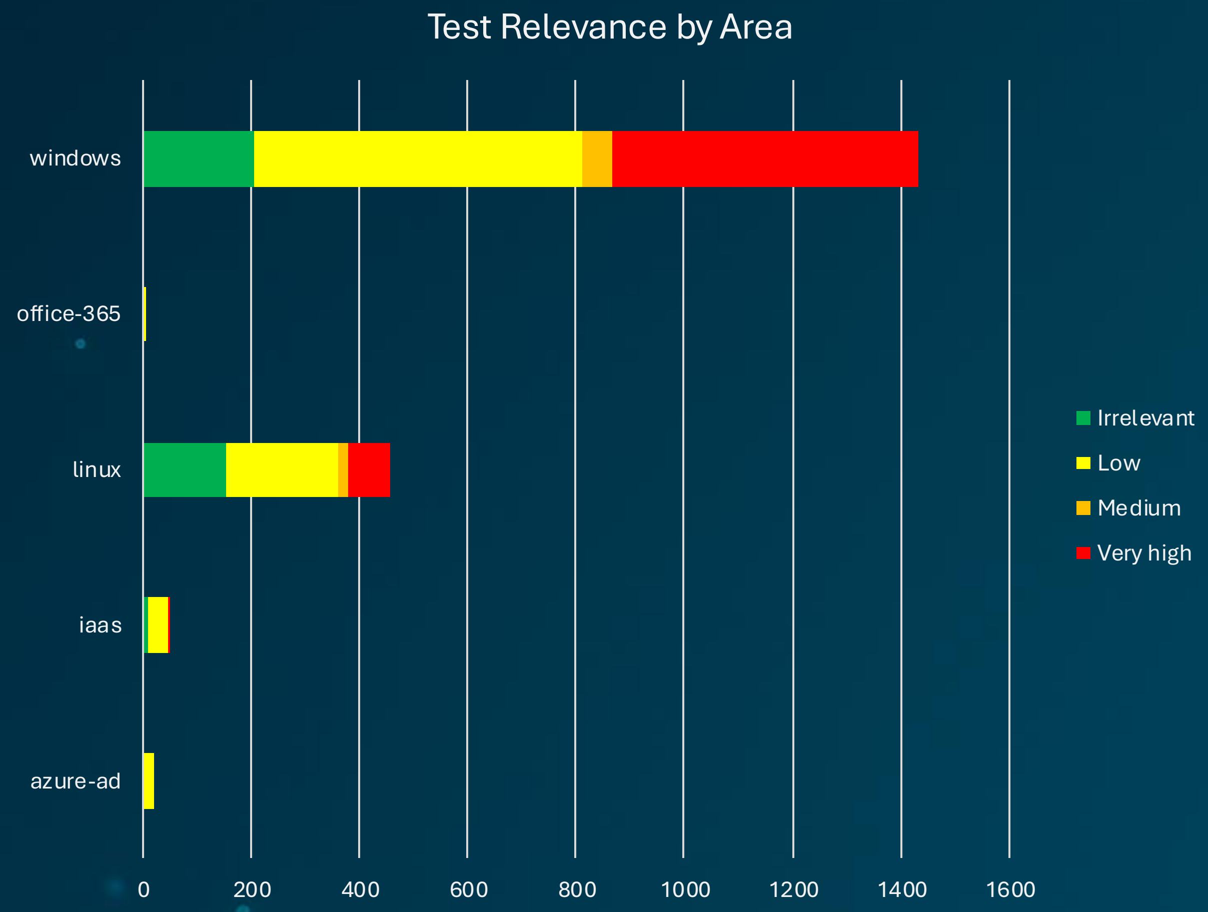


Data Sources

Data Source	name	collection layers	Techniques
DS0009	Process	Host	255
DS0029	Network Traffic	Cloud Control Plane, Host, Network	192
DS0017	Command	Container, Host	177
DS0022	File	Host	176
DS0024	Windows Registry	Host	65
DS0015	Application Log	Cloud Control Plane, Host	59
DS0028	Logon Session	Cloud Control Plane, Host, Network	41
DS0002	User Account	Cloud Control Plane, Container, Host	39
DS0011	Module	Host	31
DS0026	Active Directory	Cloud Control Plane, Host	30
DS0035	Internet Scan	OSINT	23
DS0012	Script	Host	23
DS0019	Service	Host	20
DS0038	Domain Name	OSINT	15
DS0027	Driver	Host	13
DS0025	Cloud Service	Cloud Control Plane	11
DS0013	Sensor Health	Host	11
DS0016	Drive	Host	10
DS0004	Malware Repository	OSINT	10

(Atomic) Red Teaming

- Which techniques should be tested?
- Threat landscape helps to select and prioritize tests.



(Dis)Advantages

Advantages:

- Quick creation & update, partially automated with Jupyter Notebooks.
- Efficiently reproducible: procedure documented, reasonable handover efforts.
- Mix of different sources.
- Different formats for different stakeholders.
- Accepted result: the creation process is systematic and documented, ATT&CK generally accepted as “language”.

Disadvantages or challenges:

- Lack of differentiation between sources and actors.
- Opportunistic threats are underrepresented.
- Own observations requires that TI analyst is connected to case handling (regular exchange with case handlers, handling cases, review)

Ideas for Future Iterations

- Now +20% for own observations
- Fine-grained weighting
  - Giving newer threats a higher score than old ones.
  - By relevance: Own observations > Reporting specific to our sector > Reporting specific to related sectors (different levels?)
  - By credibility of source?
- Opportunistic threats
  - Idea: there‘s a possiblity that they target us, but it‘s lower than for a targeted threat because they can also target everyone else.
  - Valid?

Lets Discuss it!

Interested in more details or exchange?

Get in touch:

thomas@patzke.org