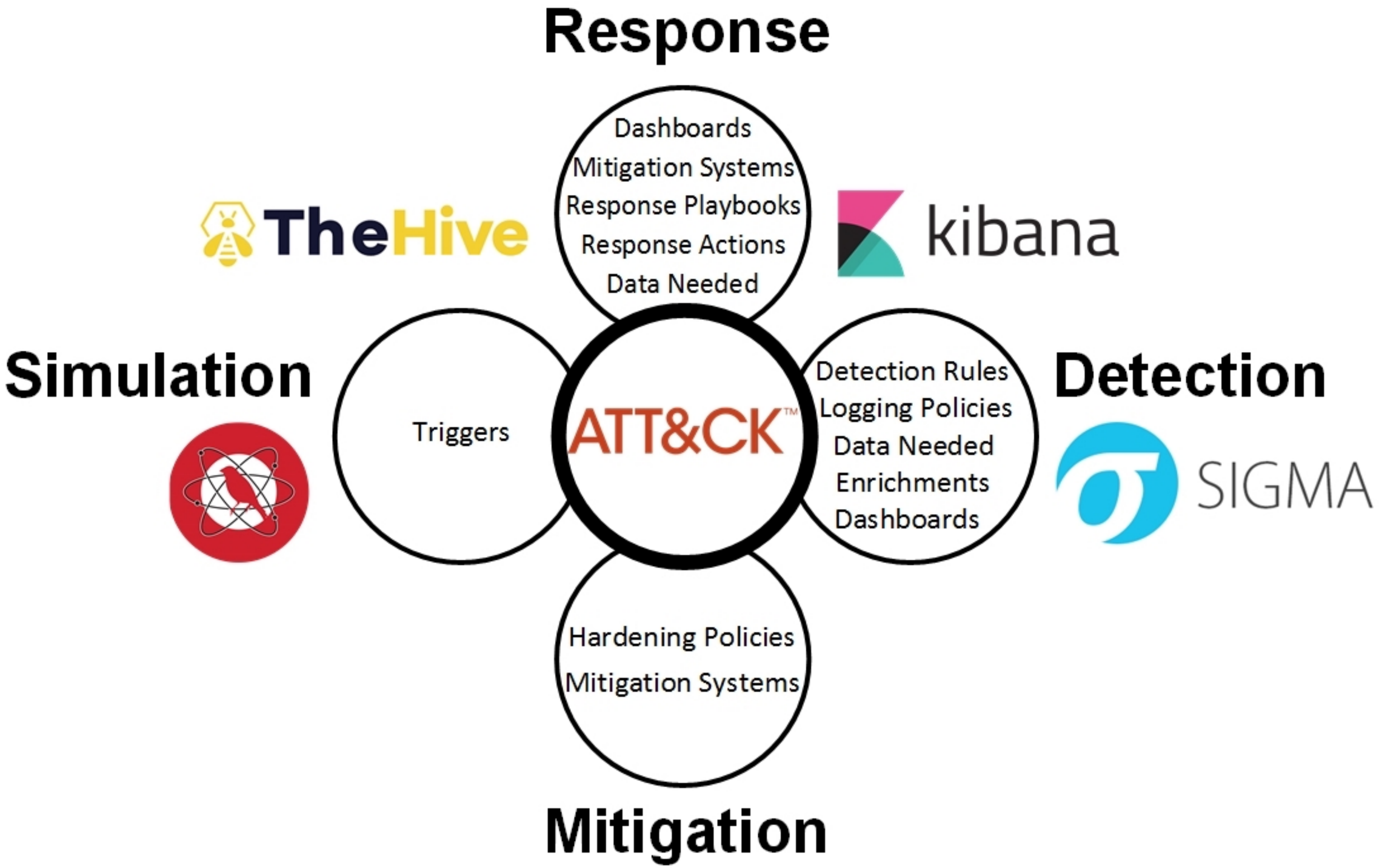
Atomic Threat Coverage

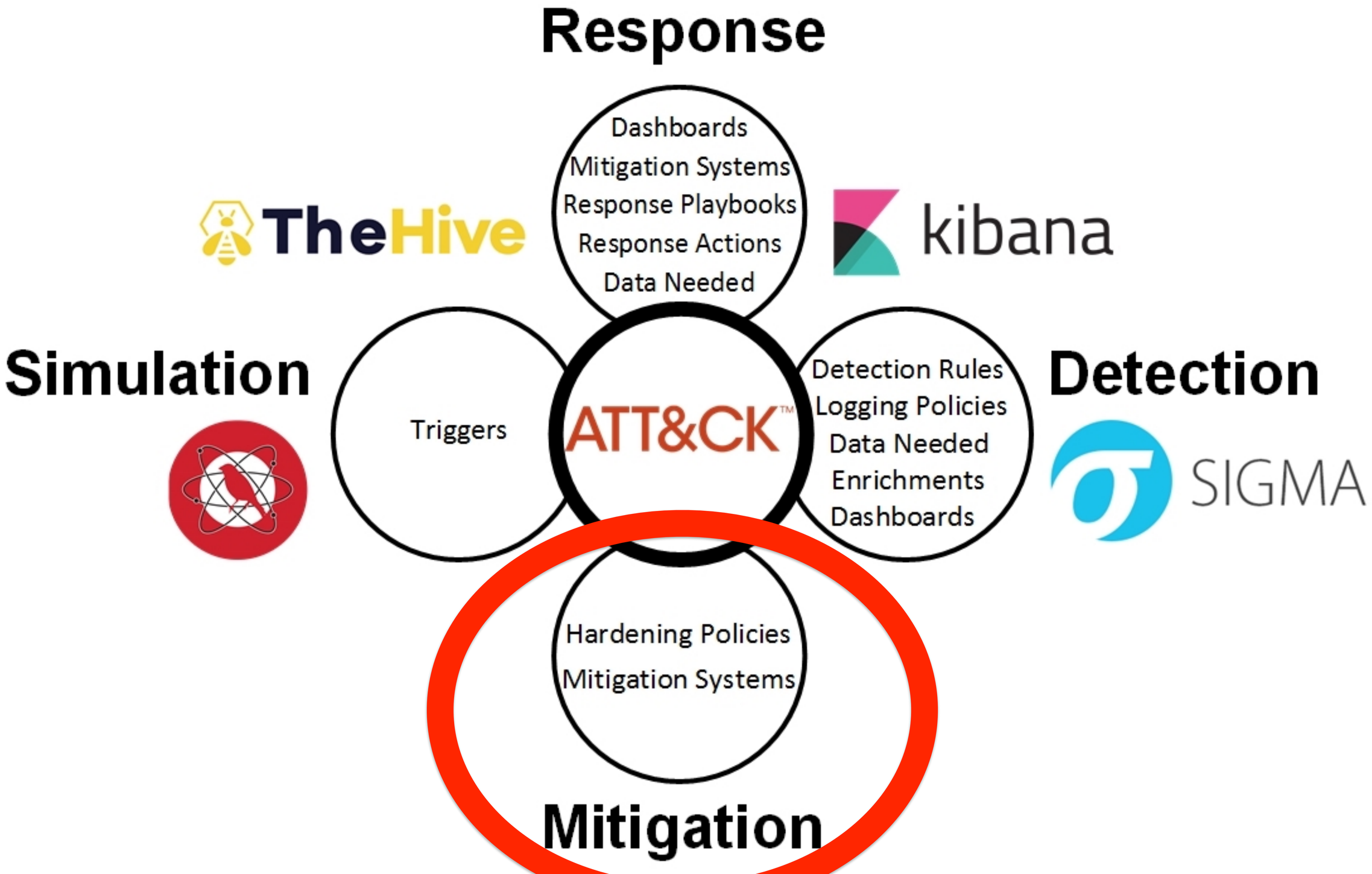
who we are

- Daniil Yugoslavskiy, **@yugoslavskiy**, Head of Threat Detection, Cindicator 🇷🇺
- Mateusz Wydra, **@snOwOtter**, SOC Incident Responder, Tieto 🇵🇱
- Jakob Weinzettl, **@mrblacyk**, SOC Threat Detection specialist, Tieto 🇵🇱
- Mikhail Aksenov, **@AverageS**, SOC Automation Team Lead, BIZONE 🇷🇺

who we are

- Working with MITRE ATT&CK framework for last **3 years**
- It's **3rd** time we are presenting on EU MITRE ATT&CK Workshop
- Use Case Framework -> **Atomic Threat Coverage** project


Response
Dashboards
Mitigation Systems
Response Playbooks
Response Actions
Data Needed
TheHive
kibana
Simulation
Triggers
ATT&CK™
Detection Rules
Logging Policies
Data Needed
Enrichments
Dashboards
Detection
SIGMA
Hardening Policies
Mitigation Systems
Mitigation

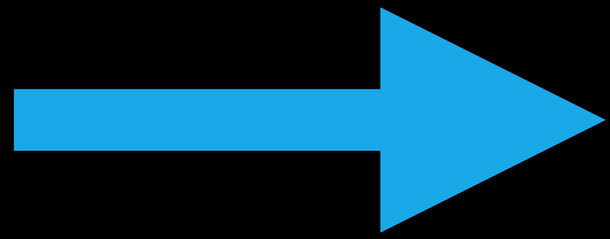

Response
Dashboards
Mitigation Systems
Response Playbooks
Response Actions
Data Needed
TheHive
kibana
Simulation
Triggers
ATT&CK™
Detection Rules
Logging Policies
Data Needed
Enrichments
Dashboards
Detection
SIGMA
Hardening Policies
Mitigation Systems
Mitigation

update: atc-mitigation

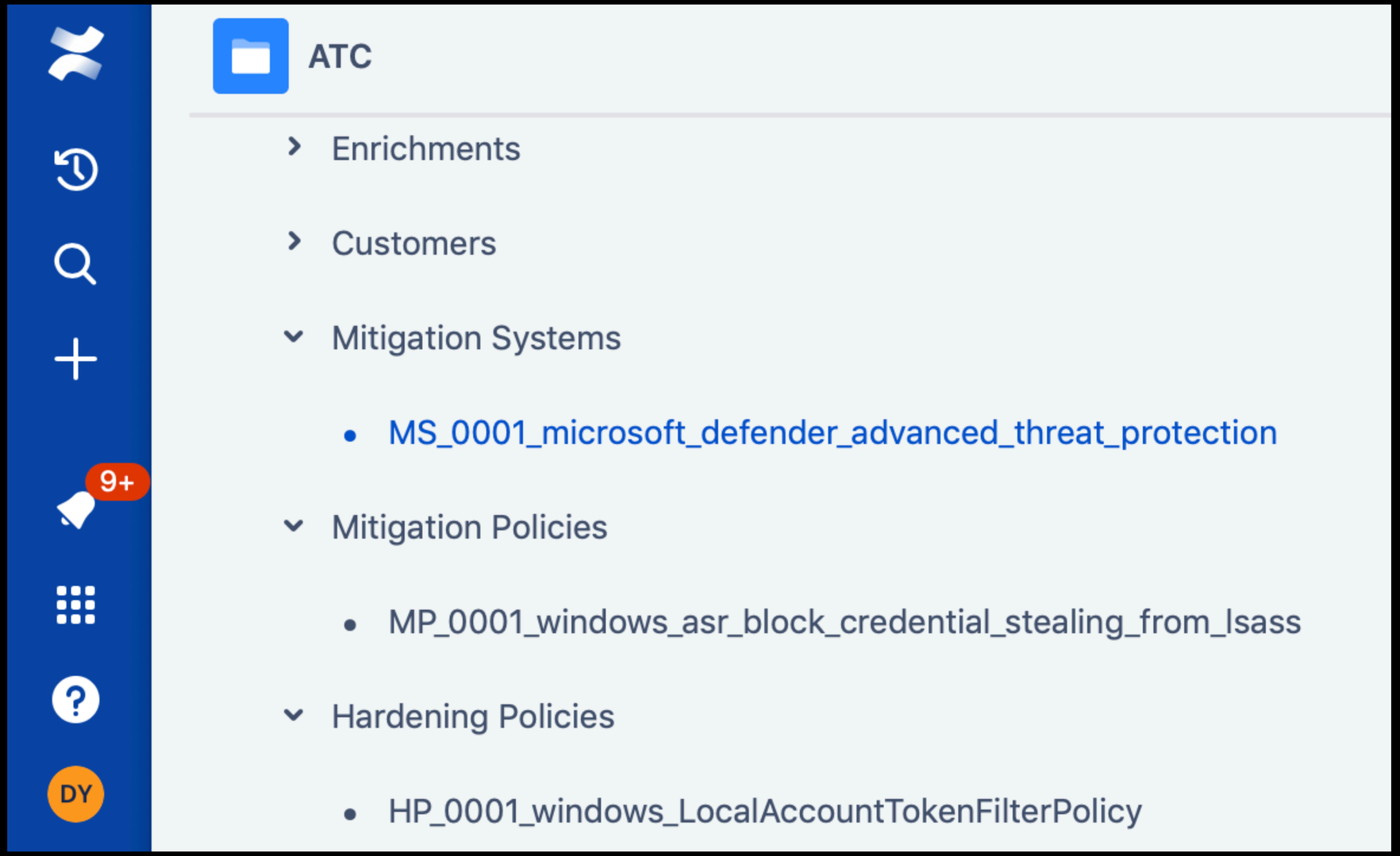
Under the hood

Data in the repository:

```
├── hardening_policies/
│   ├── HP_0001_windows_LocalAccountTokenFilterPolicy.yml
│   └── hardeningpolicies.yml.template
├── mitigation_policies/
│   ├── MP_0001_windows_asr_block_credential_stealing_from_lsass.yml
│   └── mitigation_policy.yml.template
└── mitigation_systems/
    ├── MS_0001_microsoft_defender_advanced_threat_protection.yml
    └── mitigation_system.yml.template
```



update: atc-mitigation



update: atc-mitigation

DN_0051_1121_attack_surface_reduction_blocking_mode_event

Title	DN_0051_1121_attack_surface_reduction_blocking_mode_event
Description	Event generated when an attack surface reduction rule fires in block mode
Mitigation Policy	MP_0001_windows_asr_block_credential_stealing_from_lsass
References	https://github.com/MicrosoftDocs/windows-itpro-docs/blob/d0a832b119a518a2c6b5f19ffd9dc44f0328c9a6/windows/security/threat-protection/windows-defender-exploit-guard/evaluate-attack-surface-reduction.md
Platform	Windows
Type	Applications and Services Logs
Provider	Microsoft-Windows-Windows Defender
Channel	Microsoft-Windows-Windows Defender/Operational
Fields	• EventID

ongoing work: new architecture

we will make our toolset:

- Faster
- Extendable
- Flexible
- Integratable

with power of:


django
REST
framework

ATC REST API

```
GET /api/v1/atc/
```

```
HTTP 200 OK
Allow: GET, HEAD, OPTIONS
Content-Type: application/json
Vary: Accept
```


```
{
    "category": "http://atc-rest-api.eastus.cloudapp.azure.com/api/v1/atc/category/",
    "platform": "http://atc-rest-api.eastus.cloudapp.azure.com/api/v1/atc/platform/",
    "logtype": "http://atc-rest-api.eastus.cloudapp.azure.com/api/v1/atc/logtype/",
    "channel": "http://atc-rest-api.eastus.cloudapp.azure.com/api/v1/atc/channel/",
    "provider": "http://atc-rest-api.eastus.cloudapp.azure.com/api/v1/atc/provider/",
    "volume": "http://atc-rest-api.eastus.cloudapp.azure.com/api/v1/atc/volume/",
    "logfield": "http://atc-rest-api.eastus.cloudapp.azure.com/api/v1/atc/logfield/",
    "stage": "http://atc-rest-api.eastus.cloudapp.azure.com/api/v1/atc/stage/",
    "eventid": "http://atc-rest-api.eastus.cloudapp.azure.com/api/v1/atc/eventid/",
    "tag": "http://atc-rest-api.eastus.cloudapp.azure.com/api/v1/atc/tag/",
    "references": "http://atc-rest-api.eastus.cloudapp.azure.com/api/v1/atc/references/",
    "loggingpolicy": "http://atc-rest-api.eastus.cloudapp.azure.com/api/v1/atc/loggingpolicy/",
    "dataneeded": "http://atc-rest-api.eastus.cloudapp.azure.com/api/v1/atc/dataneeded/",
    "enrichment": "http://atc-rest-api.eastus.cloudapp.azure.com/api/v1/atc/enrichment/",
    "responseaction": "http://atc-rest-api.eastus.cloudapp.azure.com/api/v1/atc/responseaction/",
    "responseplaybook": "http://atc-rest-api.eastus.cloudapp.azure.com/api/v1/atc/responseplaybook/",
    "detectionrule": "http://atc-rest-api.eastus.cloudapp.azure.com/api/v1/atc/detectionrule/"
}
```

https://**oscd.**community

- Open Security Collaborative Development (**OSCD**)
- An initiative aiming to improve **MITRE ATT&CK** coverage of the Open Source **Sigma Project** ruleset
- Organised by group of friendly Open Source Security projects

https://oscd.community

49

participants from:

- MDR/MSSPs
- CERTs
- Banks
- Government Services
- Fintech companies
- Independent Researchers

74

Sigma rules contributed so far by:

BSI 🇩🇪

Tieto 🇵🇱

PT ESC 🇷🇺

Help AG 🇷🇺

Cindicator 🇷🇺

GKU TO CITTO 🇷🇺

Hydro Tasmania 🇦🇺

Angara Technologies Group 🇷🇺

expecting x2 more in the end of sprint

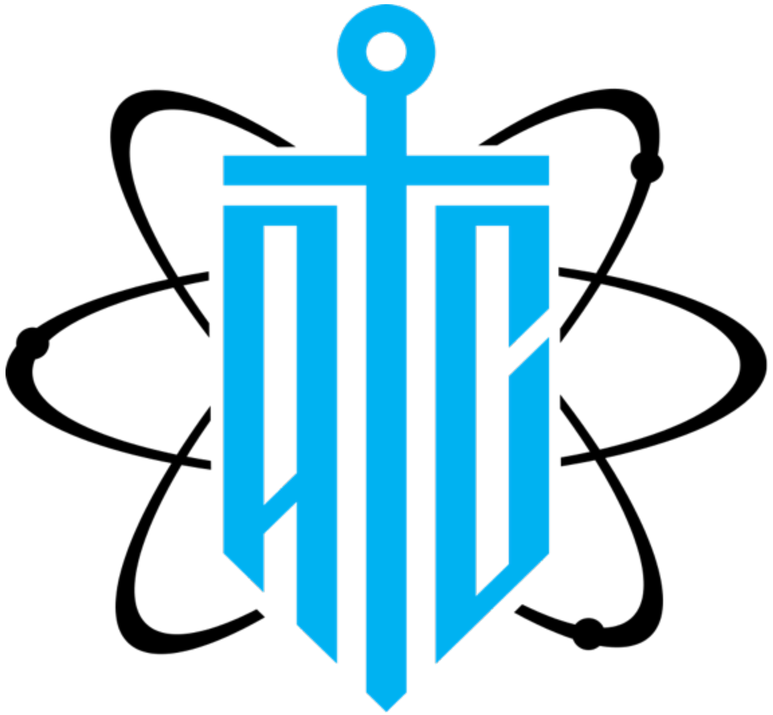
ongoing work

- Improvement of **ATT&CK Navigator** profile generator
- Full SIGMA coverage
- Collaboration with **OSSEM** project

ideas for discussion

- Sigma profiles for **severity level** customisation
- **Transparency** for MITRE ATT&CK development process
- Definition of sub-techniques list (in)**completeness**

Thank you!



We warmly welcome any **feedback** and **suggestions** to improve the project, as well as **contributions**.

List of issues is open!

Demo Confluence:	https://atomicthreatcoverage.atlassian.net
Demo Dashboard:	https://kibana.atomicthreatcoverage.com (demo:password)
GitHub Repo:	https://github.com/atc-project/atomic-threat-coverage
Twitter:	https://twitter.com/atc_project