

# EU ATT&CK Workshop #5

Daniil Yugoslavskiy  
Head of Threat Detection  
Cindicator SOC, RU/ES

# agenda

---

## Part 1: RE&CT

- RE&CT intro
- RE&CT use cases
- Operationalization
- Demo
- To be discussed

## Part 2: OSCD




- OSCD intro
- OSCD Sprint #1 Results
- OSCD Sprint #2 Announcement



Atomic Threat Coverage

# who we are

---

- Daniil [@yugoslavskiy](#), Head of Threat Detection, Cindicator 
- Mateusz Wydra, [@sn0w0tter](#), Threat Intelligence Analyst, Relativity 
- Jakob Weinzettl, [@mrblacyk](#), Incident Responder, Tieto 
- OSCP[x3](#), GCFA[x3](#), GNFA, CCNP Security, etc

# who we are

---

- Working with the ATT&CK framework for almost **4 years**
- It's **4th** time we're speaking on the EU ATT&CK Workshop
- RE&CT is a part of the **Atomic Threat Coverage** project

# what is RE&CT

---

- ATT&CK-alike framework for **Incident Response** techniques
- Threat Actor → **Incident Responder**
- Tactics → **Response Stages** (the “why”)
- Techniques → **Response Actions** (the “how”)



# RE&CT Enterprise Matrix

Response Stages and Response Actions, colorized by Categories

- General
- Network
- Email
- File
- Process
- Configuration
- Identity

## Categories

TLP: White

Preparation 95 items	Identification 56 items	Containment 26 items	Eradication 8 items	Recovery 14 items	Lessons Learned 2 items
Practice	List victims of security alert	Patch vulnerability	Report incident to external companies	Reinstall host from golden image	Develop incident report
Take trainings	List host vulnerabilities	Block external IP address	Remove rogue network device	Restore data from backup	Conduct lessons learned exercise
Raise personnel awareness	Put compromised accounts on monitoring	Block internal IP address	Delete email message	Unblock blocked IP	
Make personnel report suspicious activity	List hosts communicated with internal domain	Block external domain	Remove file	Unblock blocked domain	
Set up relevant data collection	List hosts communicated with internal IP	Block internal domain	Remove registry key	Unblock blocked URL	
Set up a centralized long-term log storage	List hosts communicated with internal URL	Block external URL	Remove service	Unblock blocked port	
Develop communication map	Analyse domain name	Block internal URL	Revoke authentication credentials	Unblock blocked user	
Make sure there are backups	Analyse IP	Block port external communication	Remove user account	Unblock domain on email	
Get network architecture map	Analyse uri	Block port internal communication		Unblock sender on email	
Get access control matrix	List hosts communicated by port	Block user external communication		Restore quarantined email message	
Develop assets knowledge base	List hosts connected to VPN	Block user internal communication		Restore quarantined file	
Check analysis toolset	List hosts connected to intranet	Block data transferring by content pattern		Unblock blocked process	
Access vulnerability management system logs	List data transferred	Block domain on email		Enable disabled service	
Access external network flow logs	Collect transferred data	Block sender on email		Unlock locked user account	
Access internal network flow logs	Identify transferred data	Quarantine email message			
Access internal HTTP logs	List hosts communicated with external domain	Quarantine file by format			
Access external HTTP logs	List hosts communicated with external IP	Quarantine file by hash			
Access internal DNS logs	List hosts communicated with external URL	Quarantine file by path			
Access external DNS logs	Find data transferred by content pattern	Quarantine file by content pattern			
Access VPN logs	List users opened email message	Block process by executable path			
Access DHCP logs	Collect email message	Block process by executable metadata			
Access internal packet capture data	List email message receivers	Block process by executable hash			
Access external packet capture data	Make sure email message is phishing	Block process by executable format			
Get ability to block external IP address	Extract observables from email message	Block process by executable content pattern			
Get ability to block internal IP address	List files created	Disable system service			
Get ability to block external domain	List files modified	Lock user account			
Get ability to block internal domain	List files deleted				
Get ability to block external URL	List files downloaded				
Get ability to block internal URL	List files with tampered timestamps				
Get ability to block port external communication	Find file by path				
Get ability to block port internal communication	Find file by metadata				
Get ability to block user external communication	Find file by hash				
Get ability to block user internal communication	Find file by format				
Get ability to find data transferred by content pattern	Find file by content pattern				
Get ability to block data transferring by content pattern	Collect file				
Get ability to list data transferred	Analyse file hash				
Get ability to collect transferred data	Analyse Windows PE				
Get ability to identify transferred data	Analyse macos macho				
Find data transferred by content pattern	Analyse Unix ELF				
Get ability to list users opened email message	Analyse MS office file				
Get ability to list email message receivers	Analyse PDF file				
Get ability to block email domain	Analyse script				
Get ability to block email sender	List processes executed				
Get ability to delete email message	Find process by executable path				
Get ability to quarantine email message	Find process by executable metadata				
Get ability to collect email message	Find process by executable hash				
Get ability to list files created	Find process by executable format				
Get ability to list files modified	Find process by executable content pattern				
Get ability to list files deleted	List registry keys modified				
Get ability to list files downloaded	List registry keys deleted				
Get ability to list files with tampered timestamps	List registry keys accessed				
Get ability to find file by path	List registry keys created				
Get ability to find file by metadata	List services created				
Get ability to find file by hash	List services modified				
Get ability to find file by format	List services deleted				
Get ability to find file by content pattern	List users authenticated				
Get ability to collect file					
Get ability to quarantine file by path					
Get ability to quarantine file by hash					
Get ability to quarantine file by format					
Get ability to quarantine file by content pattern					
Get ability to remove file					
Get ability to analyse file hash					
Get ability to analyse Windows PE					
Get ability to analyse macos macho					

# RE&CT use cases

---

- Prioritization of Incident Response **capabilities development**
- **Gap analysis** – determine "coverage" of existing capabilities



# operationalization

---

1. Download
2. Modify
3. Export
4. Profit

# Demo time!

# to be discussed

---

- Connect RE&CT with Threat Detection/Hunting
- Add multiple languages support
- RE&CT for Cloud
- RE&CT for ICS

Join discussions in **GitHub Issues!**



**Open Security Collaborative Development**

# <https://oscd.community>

---

The First OSCD sprint:

- Started in October 2019
- Finished in November 2019
- Results added to `master` branch in February 2020

<https://oscd.community>

TLP: **White**

Sigma rules:

493 ↑

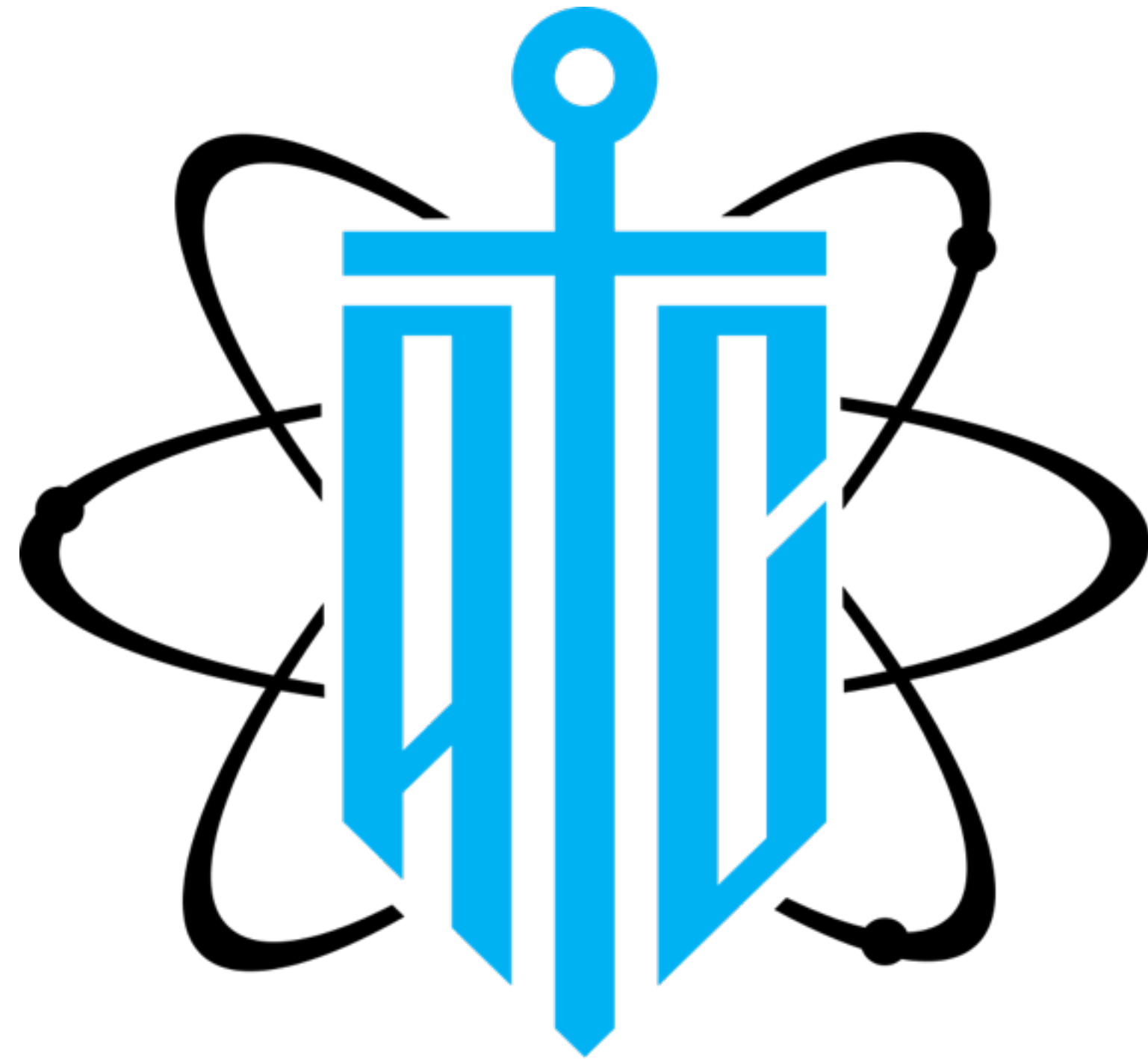
+144 (40.45%)





OSCD Sprint #2 will take place  
beginning of **August 2020**

# Thank you!



RE&CT web site:



ATC GitHub Org:



ATC Twitter:



ATC Demo Confluence:



OSCD Twitter:

<https://atc-project.github.io/atc-react/>

<https://github.com/atc-project/>

[https://twitter.com/atc\\_project](https://twitter.com/atc_project)

<https://atomicthreatcoverage.atlassian.net>

[https://twitter.com/oscd\\_initiative](https://twitter.com/oscd_initiative)