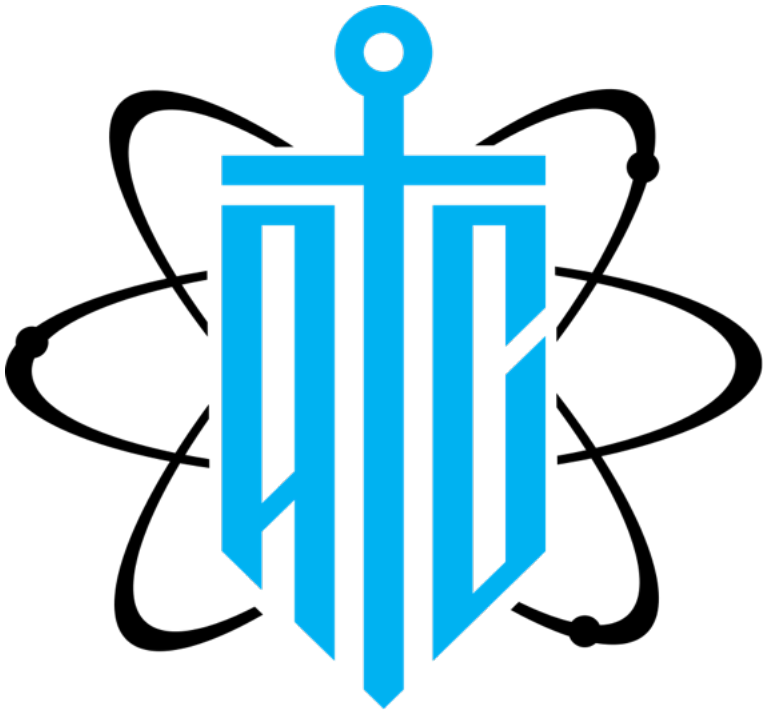


Atomic Threat Coverage

Who are we?

Daniil Yugoslavskiy
@yugoslavskiy
Head of Threat Detection
Cindicator

Mateusz Wydra
@sn0w0tter
Incident Responder
Tieto

Jakob Weinzettl
@mrblacyk
Threat Detection Specialist
Tieto

Mikhail Aksenov
@AverageS
Automation Team Lead
BIZONE

2011: networking ->

2013: **network** security ->

2014: **computer** security ...

Where all of these people get **correlation rules** from..?

Intelligence Driven Defense


ATT&CK™

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
				Deobfuscate/Decod							

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
										Data Compressed	Data Encrypted for Impact
										Data Encrypted	Defacement
										Data Transfer Size Limits	Disk Content Wipe
										Exfiltration Over Alternative Protocol	Disk Structure Wipe
										Exfiltration Over Command and Control Channel	Endpoint Denial of Service
										Exfiltration Over Other Network Medium	Firmware Corruption
										Exfiltration Over Physical Medium	Inhibit System Recovery
										Scheduled Transfer	Network Denial of Service
											Resource Hijacking
											Runtime Data Manipulation
											Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
				Deobfuscate/Decod							

Exfiltration Over Alternative Protocol

Data exfiltration is performed with a different protocol from the main command and control protocol or channel. The data is likely to be sent to an alternate network location from the main command and control server. Alternate protocols include FTP, SMTP, HTTP/S, DNS, or some other network protocol. Different channels could include Internet Web services such as cloud storage.

Exfiltration Over Alternative Protocol

Technique

ID	T1048
Tactic	Exfiltration
Platform	Linux, macOS, Windows
Data Sources	User interface, Process monitoring, Process use of network, Packet capture, Netflow/Enclave netflow, Network protocol analysis
Requires Network	Yes

Examples

- FIN8 has used FTP to exfiltrate collected data.[1]
- Lazarus Group malware SierraBravo-Two generates an email message via SMTP containing information about newly infected victims.[2]
- OilRig has exfiltrated data over FTP separately from its primary C2 channel over DNS.[3]
- can be used to create BITS Jobs to upload files from a compromised host.[4]
- Cherry Picker exfiltrates files over FTP.[5]
- CosmicDuke exfiltrates collected files over FTP or WebDAV. Exfiltration servers can be separately configured from C2 servers.[6]

Mitigation

Follow best practices for network firewall configurations to allow only necessary ports and traffic to enter and exit the network. For example, if services like FTP are not required for sending information outside of a network, then block FTP-related ports at the network perimeter. Enforce proxies and use dedicated servers for services such as DNS and only allow those systems to communicate over respective ports/protocols, instead of all systems within a network.[11] These actions will help reduce command and control and exfiltration path opportunities.

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary command and control infrastructure and malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools.[12]

Detection

Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.[12]

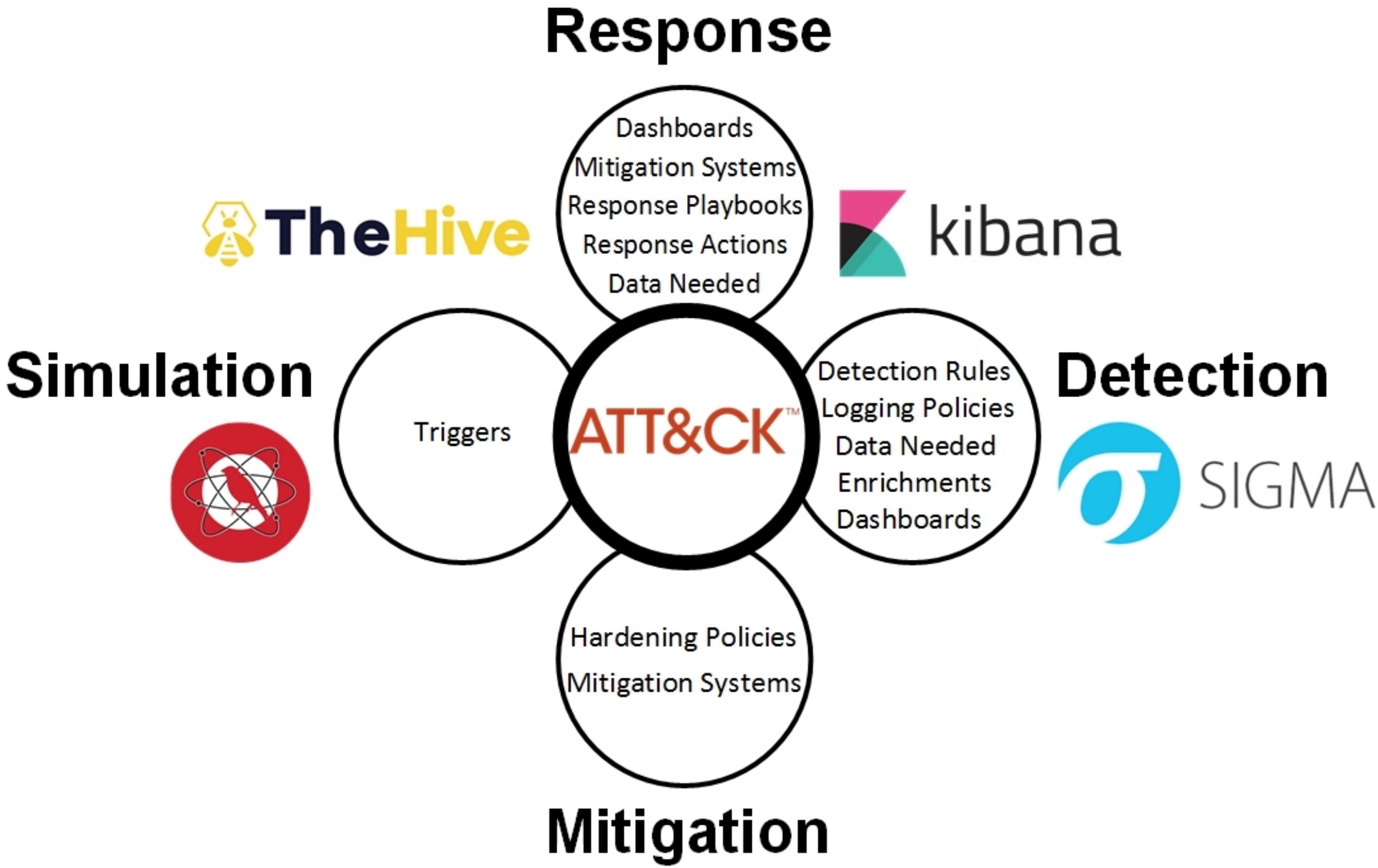
References

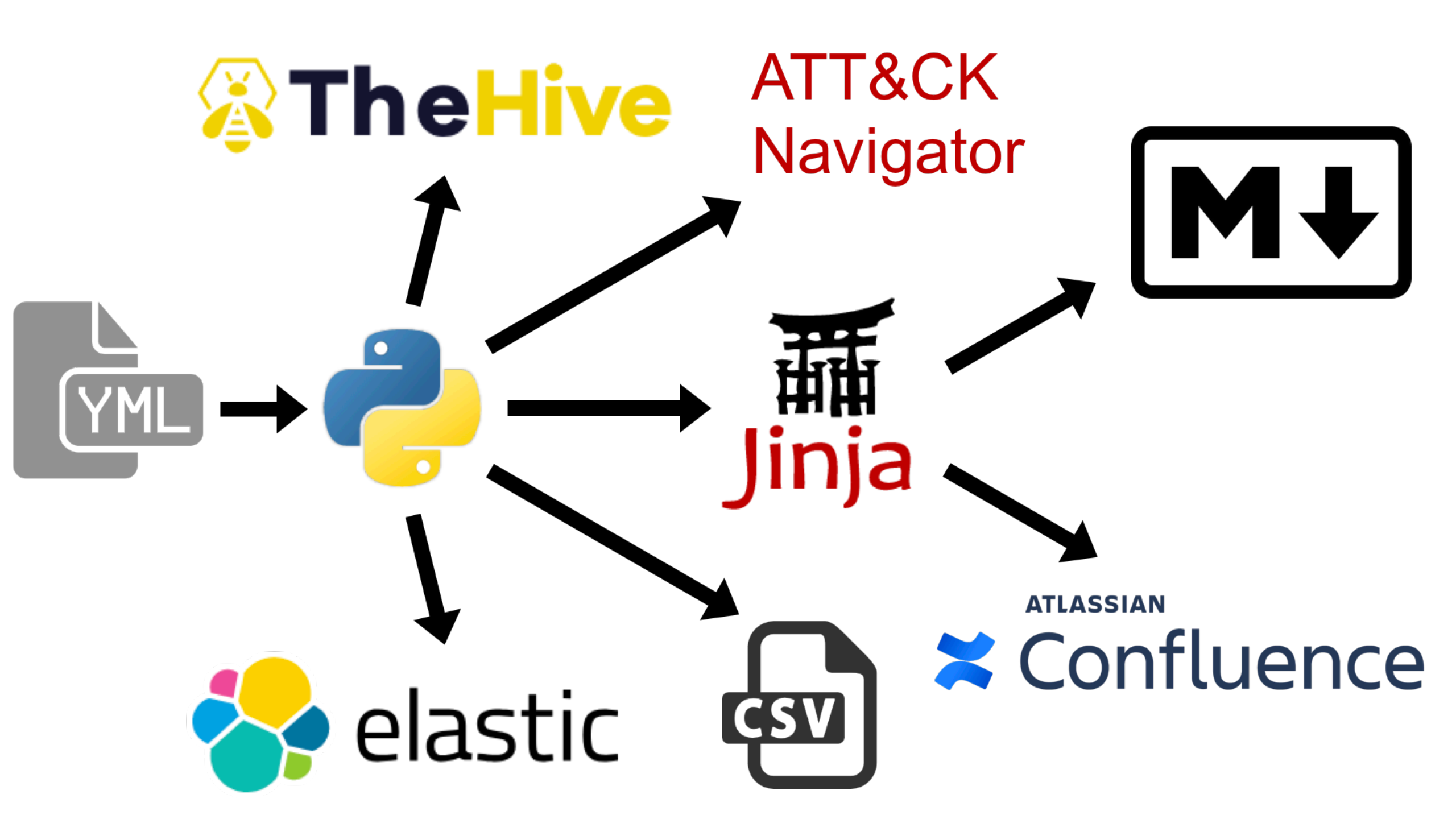
1. ^ ↑ Elovitz, S. & Ahl, I. (2016, August 18). Know Your Enemy: New Financially-Motivated & Spear-Phishing Group. Retrieved February 26, 2018.
2. ^ ↑ Novetta Threat Research Group. (2016, February 24). Operation Blockbuster: Remote Administration
7. ^ ↑ Wikipedia. (2016, June 15). File Transfer Protocol. Retrieved July 20, 2016.
8. ^ ↑ FireEye Labs. (2015, July). HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group. Retrieved September 17, 2015.

Operationalization problems

- Description from MITRE ATT&CK is too high level, **not actionable**
- Lack of ability to **explain requirements** and **goals** with compelling arguments
- Reporting to **leadership**: coverage, progression

Atomic Threat Coverage!


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


TheHive
ATT&CK
Navigator
YML
Jinja
elastic
CSV
ATLASSIAN
Confluence

$ make

- Update submodules - SIGMA, ART
- Setup Confluence and markdown repository
- Create ATT&CK Navigator profiles
- Export playbooks to TheHive templates
- Export data to Elasticsearch index

Demo

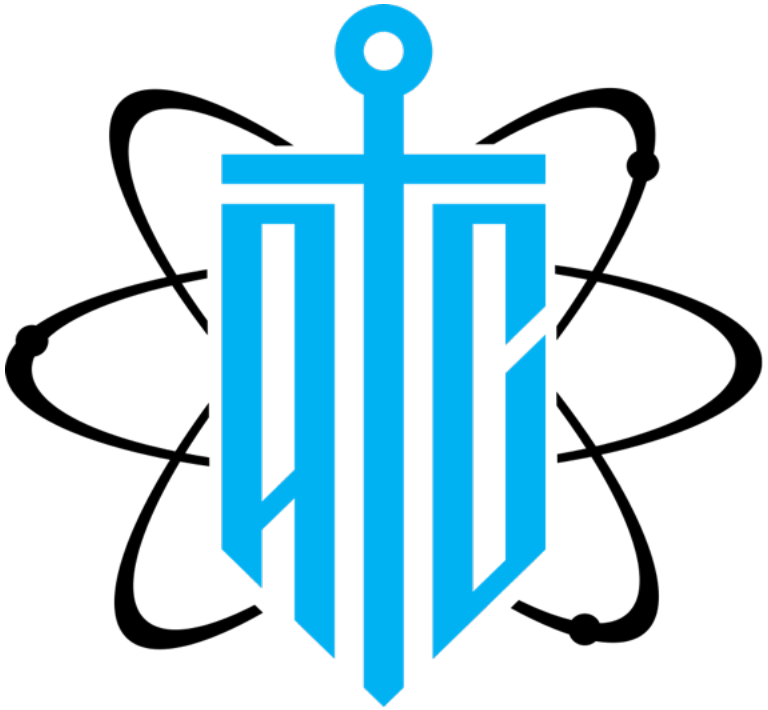
Conclusions

- MITRE ATT&CK **detailed** enough for operationalizitaion
- Analytics as a code: work only with **plain text yaml** files
- Total **automation**: exports, mappings, upload and update
- **Visualisation** of existing analytics for analysis
- Automated **coverage** representation

Ongoing work

- Full coverage mappings in **ATT&CK Navigator**
- Full **SIGMA** support
- **Community** Threat Detection Development Sprint
- Collaboration with **OSSEM** project
- Split project into **modules**
- **MISP** Galaxy
- **Web** application

Q&A



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