SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

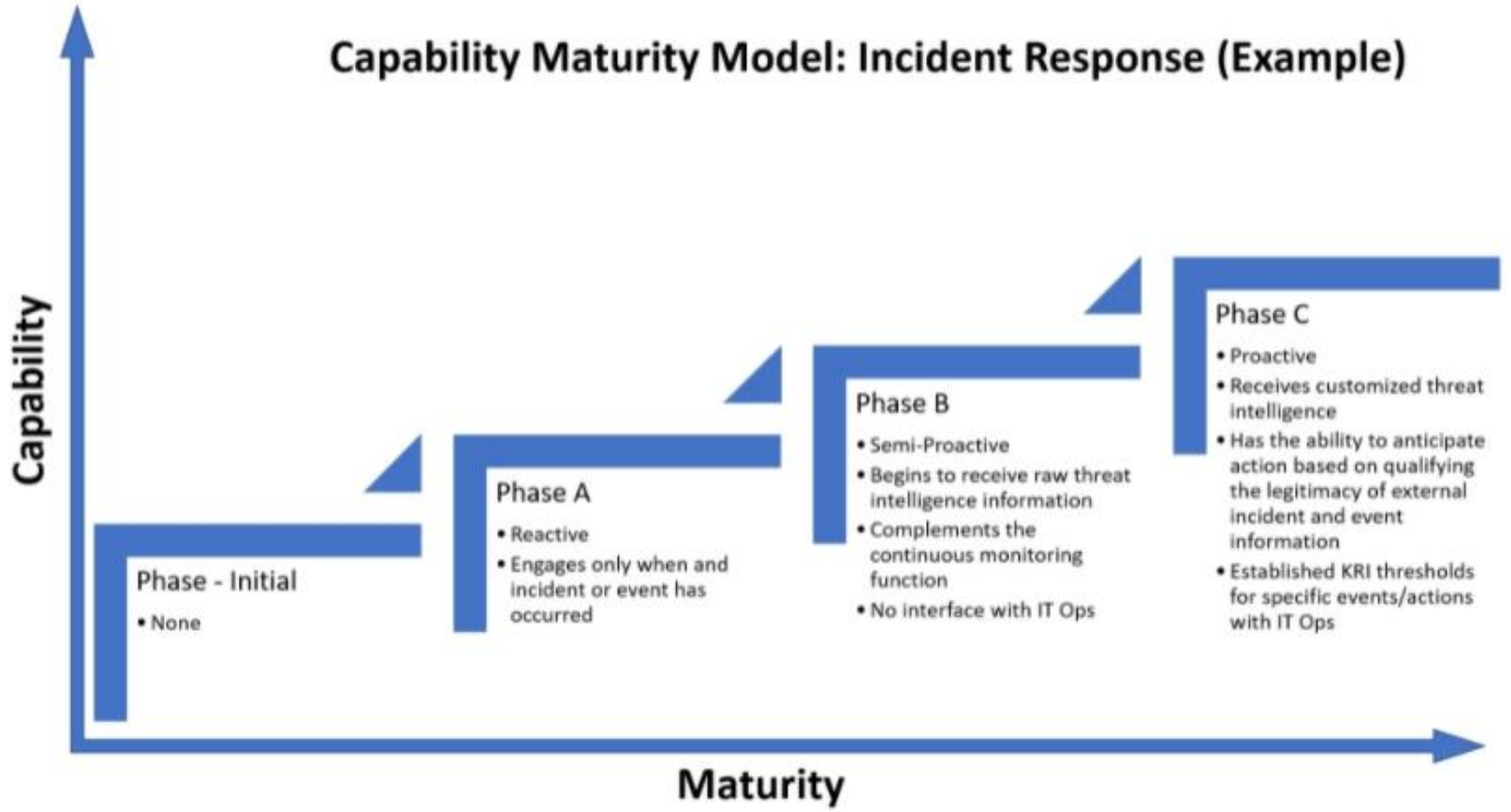
ТЕХНИКИ И ТЕХНОЛОГИИ

РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИБ

Луцив Данила
dlutsiv@securityvision.ru

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

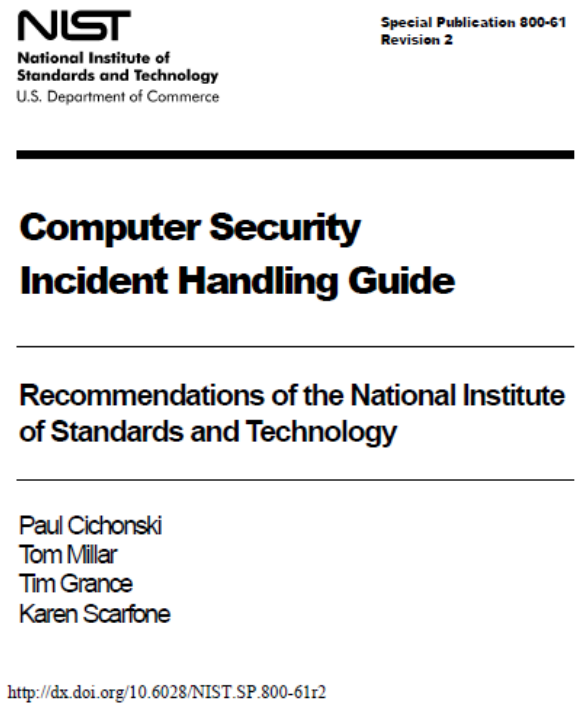
ИНЦИДЕНТЫ ИБ:
ДОРОЖНАЯ КАРТА



SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

ИНЦИДЕНТЫ ИБ:

СТАНДАРТЫ И ЛУЧШИЕ ПРАКТИКИ


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

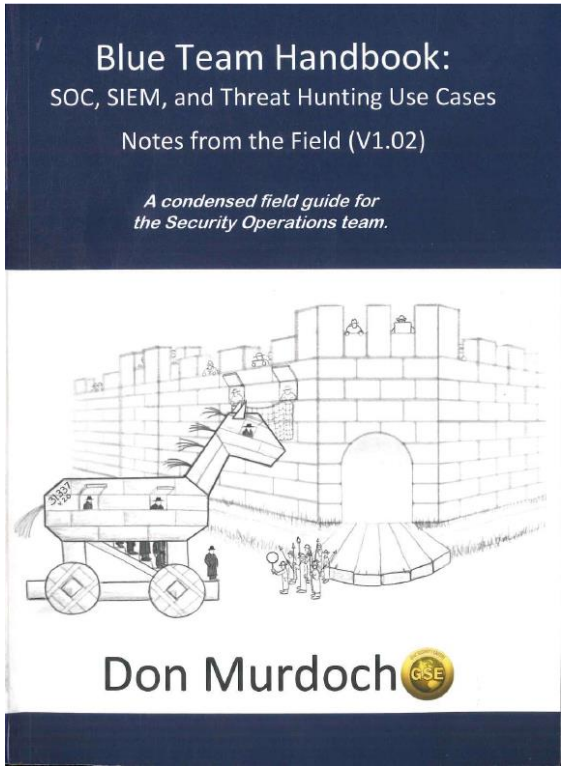
Special Publication 800-61 Revision 2

Computer Security Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-61r2



https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/fina
http://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf
https://www.amazon.com/Blue-Team-Handbook-condensed-Responder/dp/1500734756

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

ИНЦИДЕНТЫ ИБ:

DFIR vs. INCIDENT HANDLING

01 Подготовка

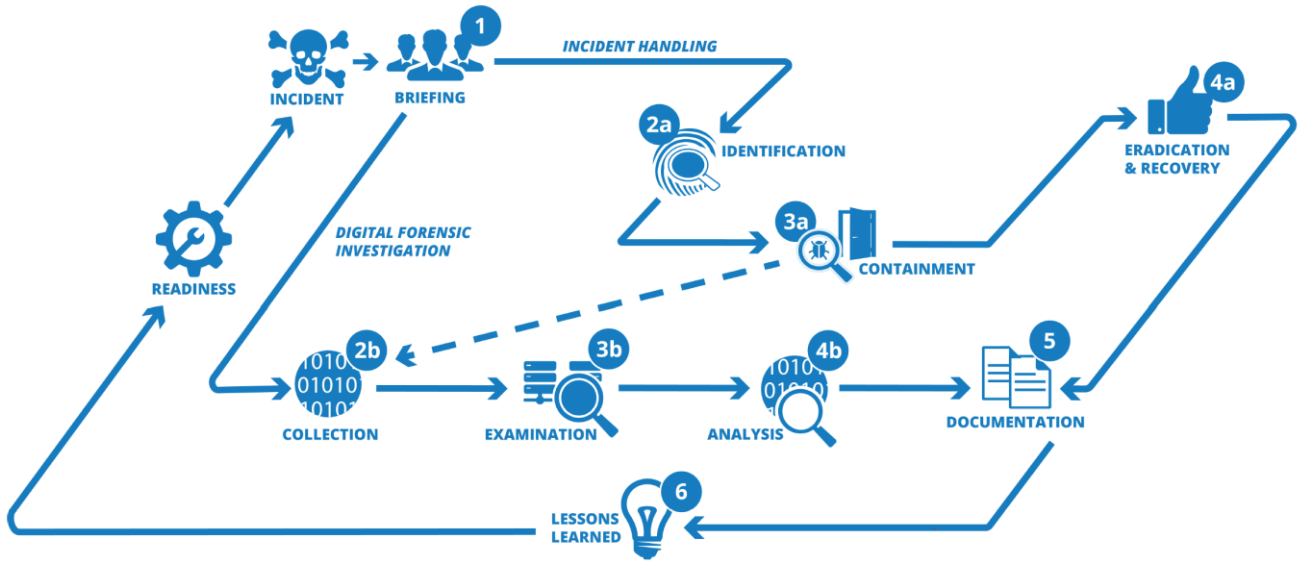
02 Идентификация и сбор данных

03 Сдерживание и обогащение

04 Устранение и аналитика

05 Анализ инцидента

06 Закрепление данных и модернизация контролей



SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

ИНЦИДЕНТЫ ИБ:

АБСТРАКЦИЯ

Чем лучше информация на входе, тем лучше результат на выходе.
«Garbage in, garbage out».

INPUT

Представления об атаках:
Правила корреляции, сигнатуры, TI etc.

Получаемые данные:
События с СЗИ, сетевых и конечных устройств etc.

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

OUTPUT

Инциденты ИБ:
Приоритезированные, минимизированные, обладающие достаточностью данных

ИСТОЧНИКИ

СКУД

Proxy сервера

конечные устройства

DLP системы

Антивирусы\EDR

брандмауэры, свитчи и сетевые IPS, VPN

DNS, DHCP

Active Directory, PAM

ИСТОЧНИКИ: ПРИОРИТИЗАЦИЯ

Log source	Volume [11]	IOC Matching	Threat Hunting	Audit Trail [9]	APT Detection [10]
Antivirus	Low	-	++ [3]	+	+++
Windows & Sysmon	Medium [8]	++ [1]	+++ [4]	++	++
Proxy	Medium	++ [2]	+ [5]	++	+
NIDS / NSM [7]	Medium	+ [2]	+	+	+
DNS	High	++ [2]	+ [5]	+	+
Mail [6]	Medium	+	-	+	-
Firewall	High	+ [2]	-	++	-
Linux (auditd)	Medium	-	+	+	-

ПРИОРИТЕТ

ВЫСОКИЙ

НИЗКИЙ

1 Хеш-сумма файлов (MD5,SHA1,SHA256)
2 C2 IP-адреса и домены
3 Antivirus Event Analysis Cheat Sheet, @cyb3rops
4 Sigma правила
5 Подозрительные TLD и UserAgent
6 Эффективен при использовании TI feeds
7 Suricata\Zeek или коммерческие Anti-APT, NTA
8 Напрямую зависит от политики (MS Baseline\sysmon-modular)
9 Полезность в реконструкции инцидентов
10 Полезность при реконструкции продвинутых TTP
11 Напрямую зависит от политик и фильтров

ИСТОЧНИКИ:

ЛУЧШИЕ ПРАКТИКИ

01 **BrandonsProjects WEFC**
https://github.com/BrandonsProjects/WEFC

02 **Palantir Windows Event Forwarding Guidance**
https://github.com/palantir/windows-event-forwarding

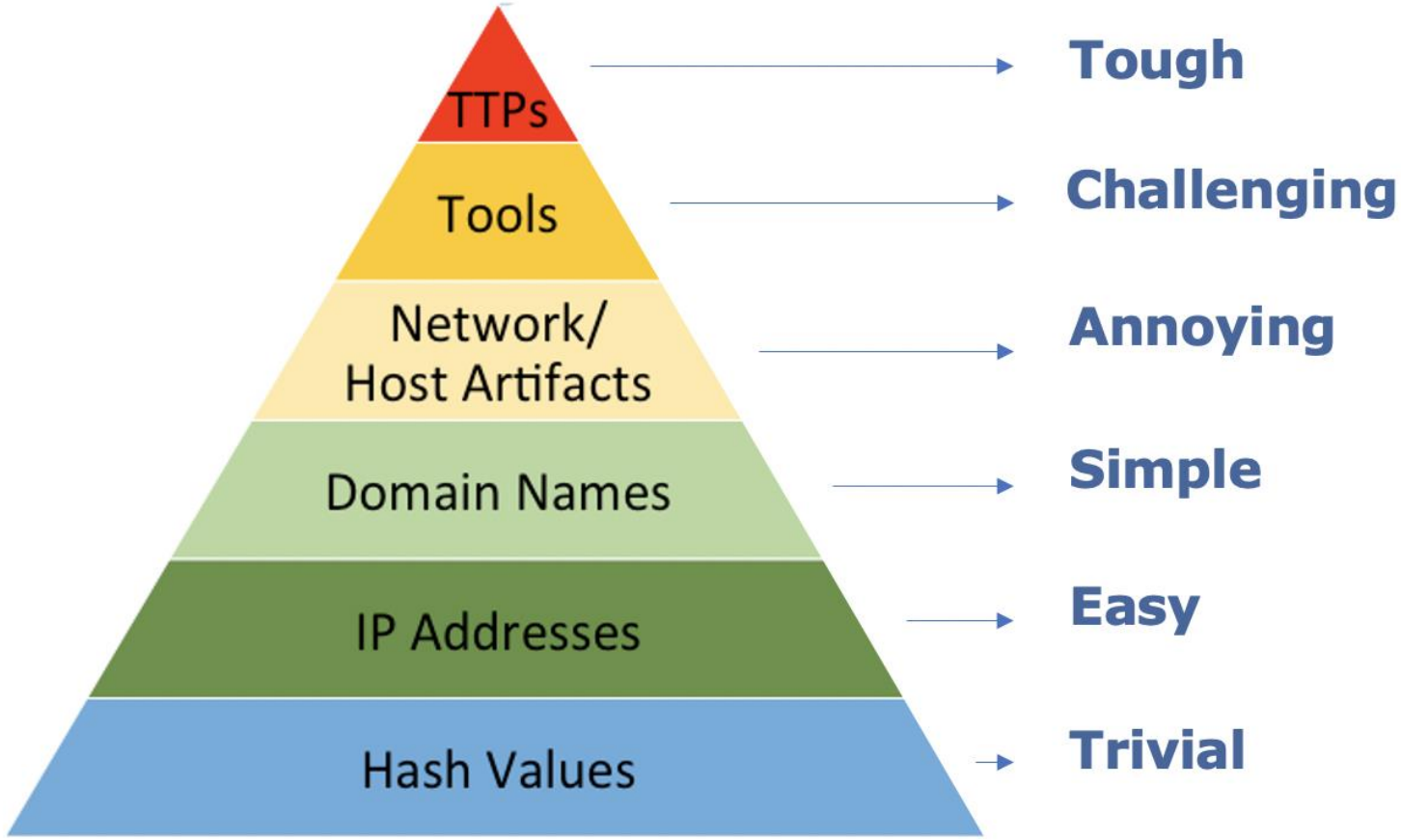
03 **Ultimate Windows Security**
https://www.ultimatewindowssecurity.com/

04 **Sysmon-Modular**
https://github.com/olafhartong/sysmon-modular

05 **ATT&CK Data Sources**
https://github.com/mitre-attack/attack-datasources

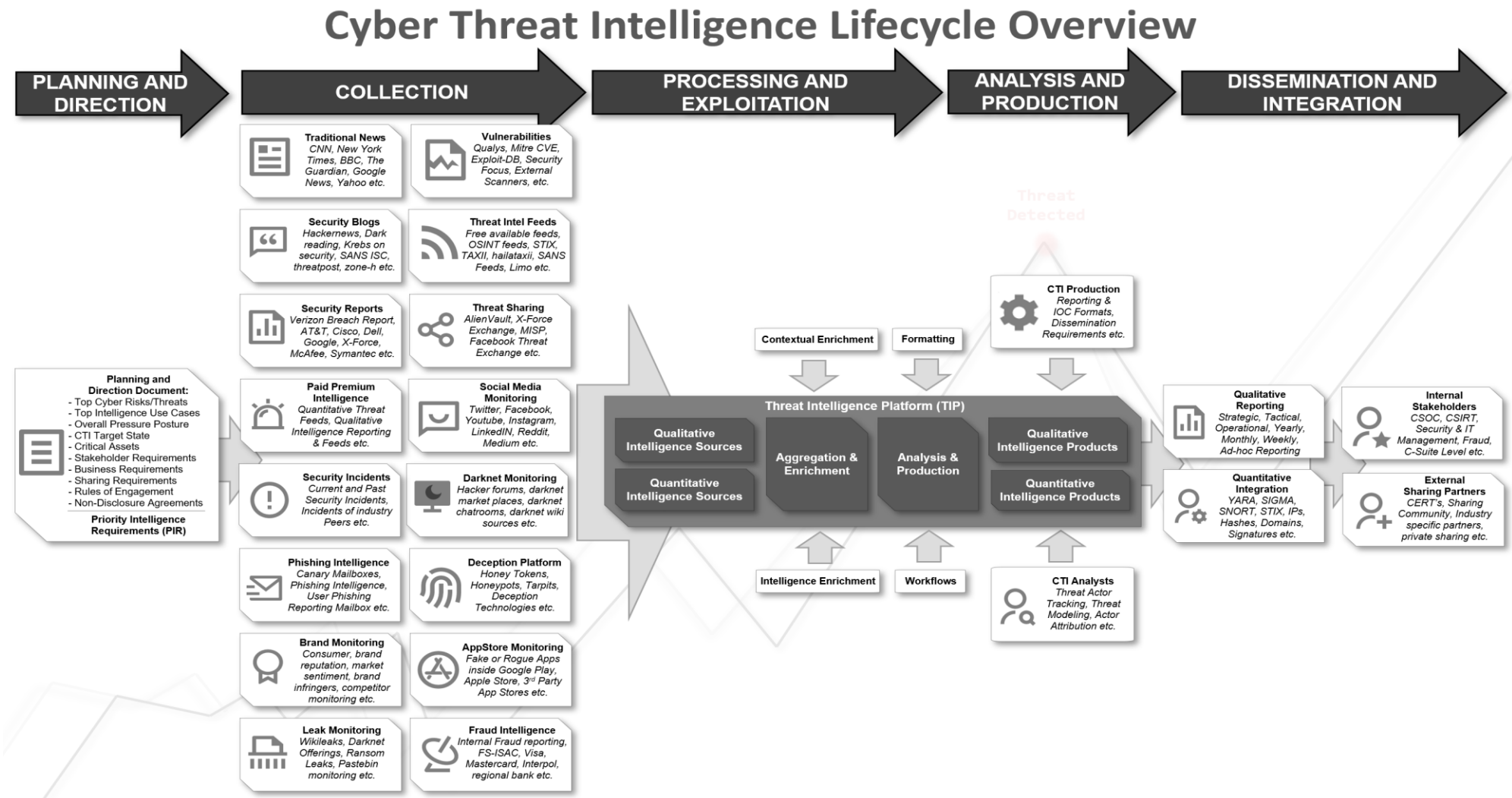
06 **Atomic Threat Coverage**
https://atomicthreatcoverage.atlassian.net/wiki/spaces/ATC/pages/12592743 3/Logging+Policies

PYRAMID
OF PAIN

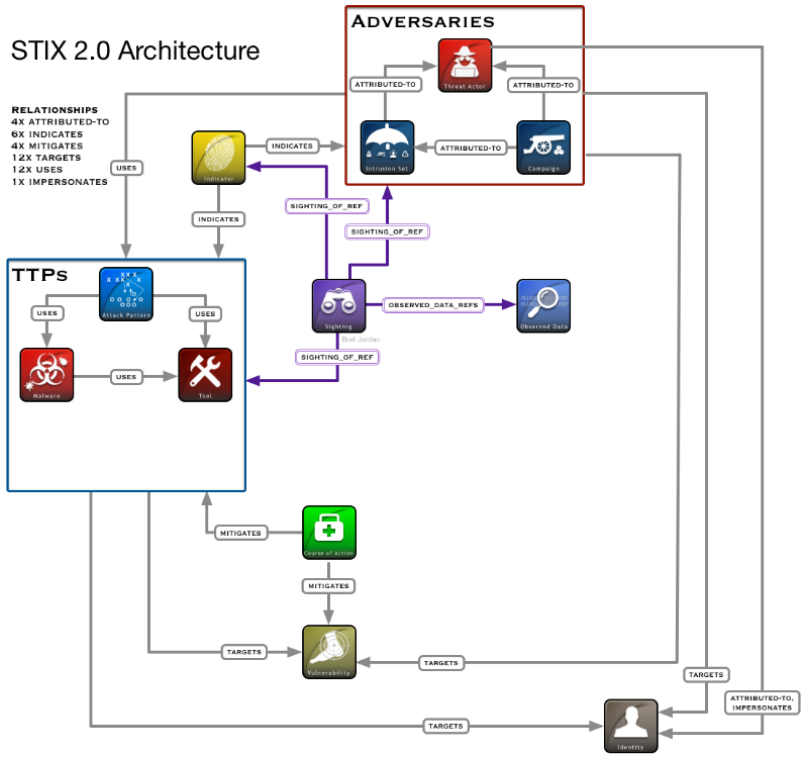


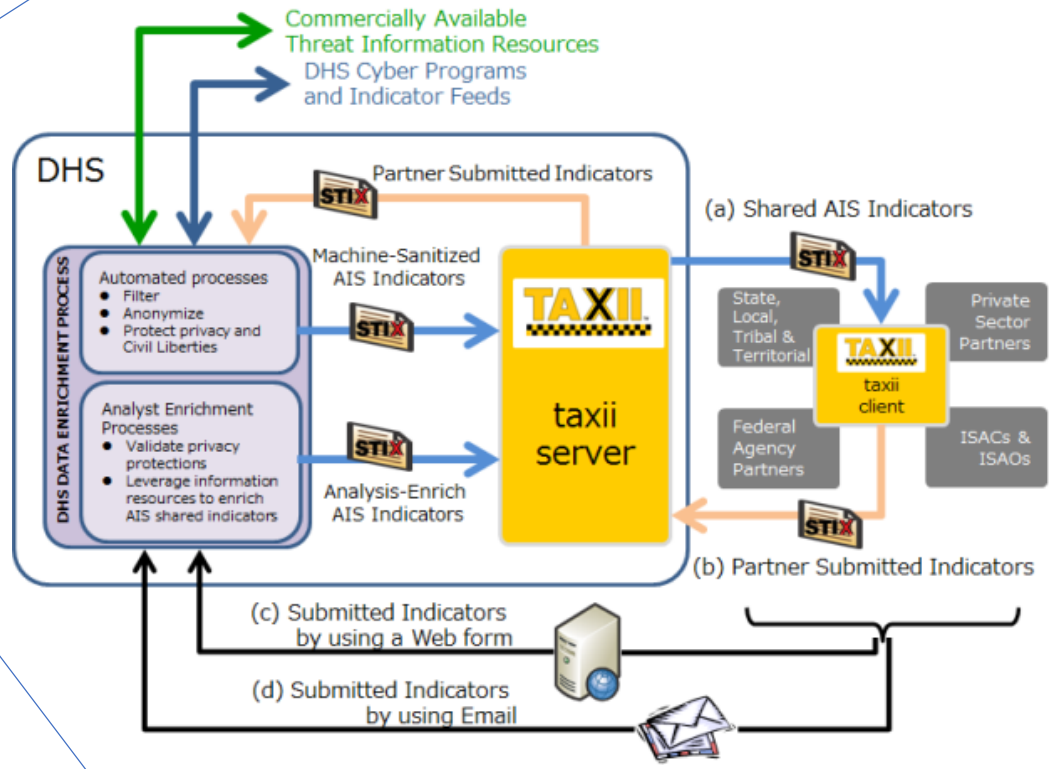
https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Threat Intel Lifecycle



STIX\TAXII

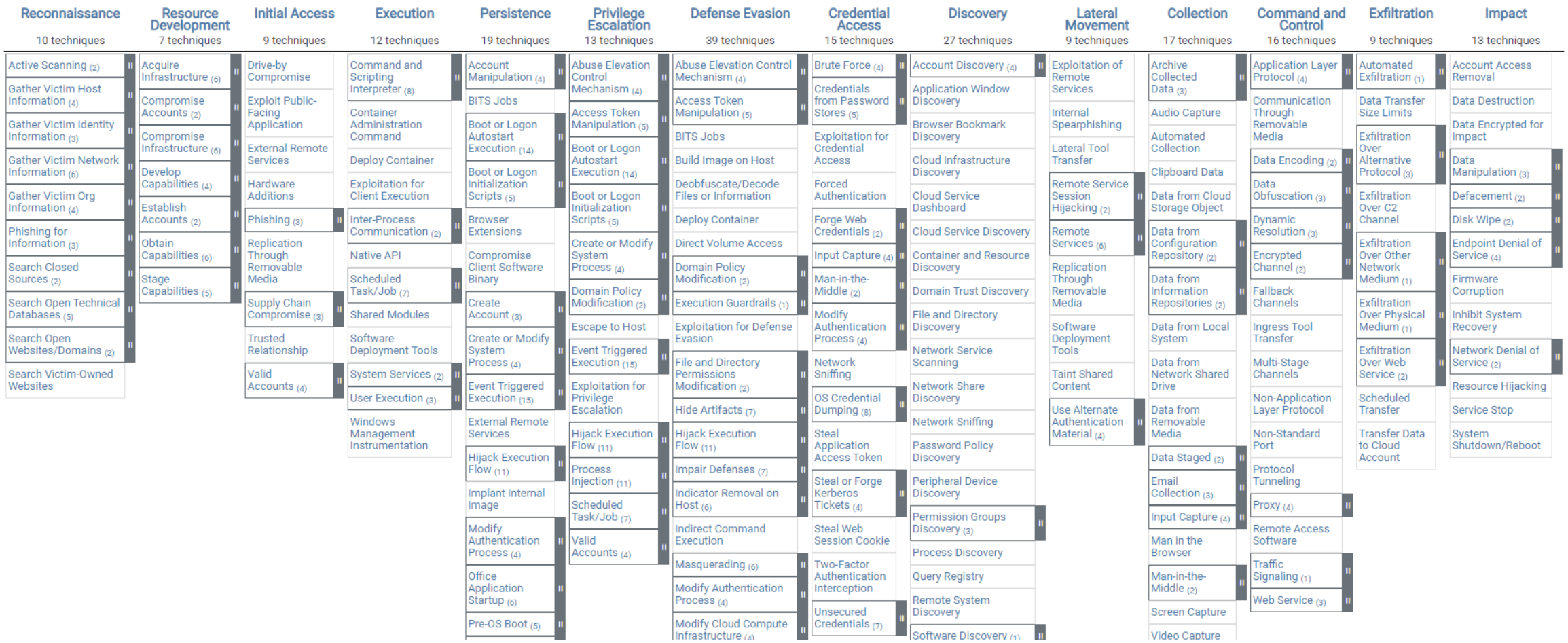




https://www.hitachi.com/hirt/publications/hirt-pub17007/index.html

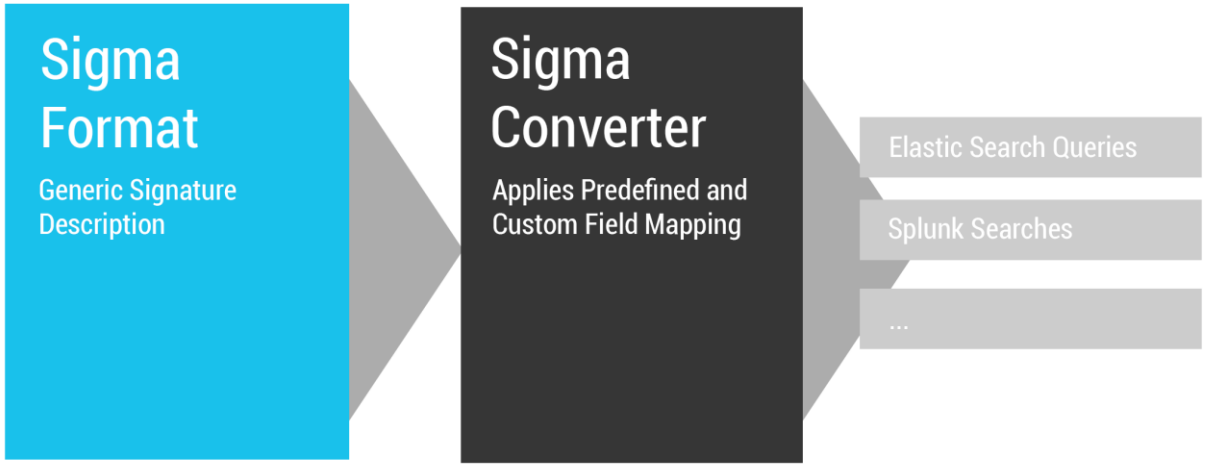
SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

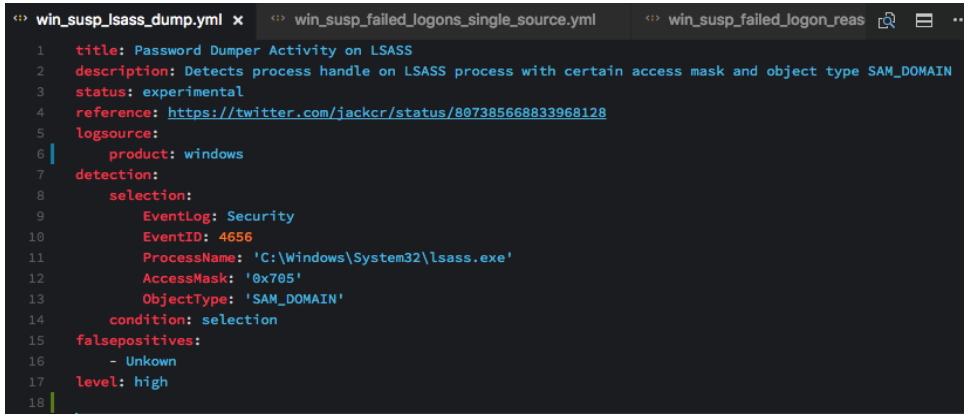
ATT&CK framework

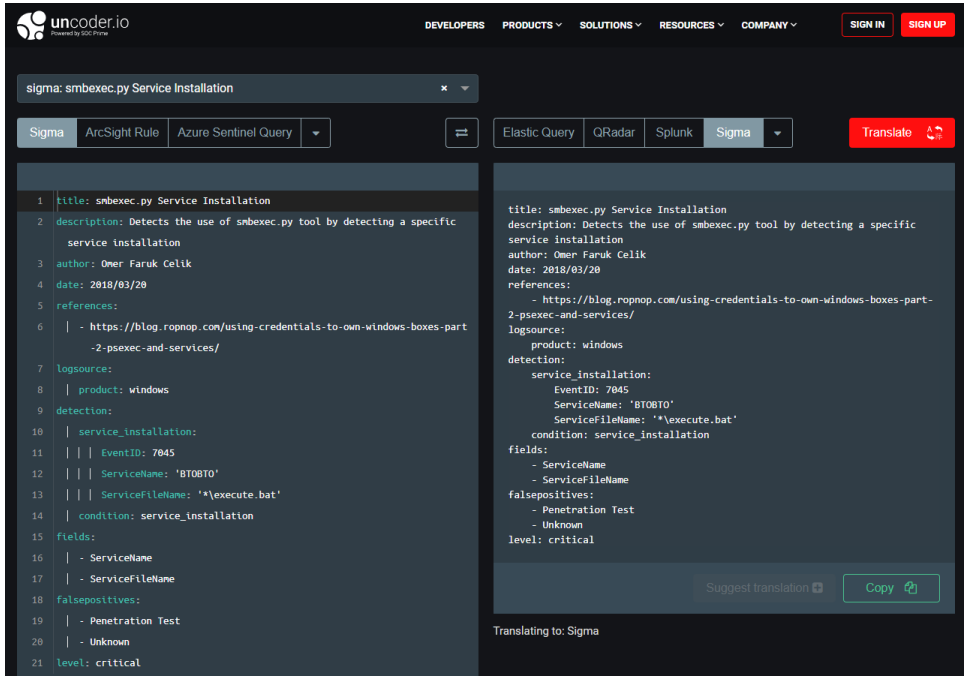


https://attack.mitre.org/
https://mitre-attack.github.io/attack-navigator/

ATT&CK: Sigma rules







https://github.com/SigmaHQ/sigma
https://atomicthreatcoverage.atlassian.net/
https://uncoder.io/

ATT&CK: ATC

ATC / Detection Rules

DLL Load via LSASS

DY Created by Daniil Yugoslavskiy
Last updated Mar 23, 2020

Title	DLL Load via LSASS
Description	Detects a method to load DLL via LSASS process using an u
ATT&CK Tactic	TA0002: Execution
ATT&CK Technique	T1177: LSASS Driver
Data Needed	• DN_0016_12_windows_sysmon_RegistryEvent • DN_0017_13_windows_sysmon_RegistryEvent
Trigger	T1177: LSASS Driver
Severity Level	high
False Positives	Unknown
Development Status	experimental
References	• https://blog.xpnsec.com/exploring-mimikatz-part-1/ • https://twitter.com/SBousseaden/status/1183745981189
Author	Florian Roth

Detection Rules

Sigma rule

```
title: DLL Load via LSASS
id: b3503044-60ce-4bf4-bbcb-e3db98788823
status: experimental
description: Detects a method to load DLL via LSASS process using an undocumented Registry key
author: Florian Roth
```

ATC / Data Needed

DN_0016_12_windows_sysmon_RegistryEvent

T DY MA Created by TestMateo
Last updated Nov 04, 2020 by Daniil Yugoslavskiy

Title	DN_0016_12_windows_sysmon_RegistryEvent
Author	@atc_project
Description	Registry key and value create and delete operations map to this event type,
Logging Policy	None
Mitigation Policy	None
References	• https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/eve • https://github.com/Cyb3rWard0g/OSSEM/blob/master/data_dictionaries
Platform	Windows
Type	Applications and Services Logs
Provider	Microsoft-Windows-Sysmon
Channel	Microsoft-Windows-Sysmon/Operational
Fields	• EventID • Computer • Hostname • EventType • UtcTime • ProcessGuid • ProcessId • Image • TargetObject

ATC / Triggers

T1088: Bypass User Account Control

T DY MA Created by TestMateo
Last updated Mar 23, 2020 by Daniil Yugoslavskiy • 0 min read

Atomic Trigger

T1088 - Bypass User Account Control

Description from ATT&CK

<blockquote>Windows User Account Control (UAC) allows a program to elevate its privileges to perform a task under administrator-level permissions by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action. (Citation: TechNet How UAC Works)

If the UAC protection level of a computer is set to anything but the highest level, certain Windows programs are allowed to elevate privileges or execute some elevated COM objects without prompting the user through the UAC notification box. (Citation: TechNet Inside UAC) (Citation: MSDN COM Elevation) An example of this is use of rundll32.exe to load a specifically crafted DLL which loads an auto-elevated COM object and performs a file operation in a protected directory which would typically require elevated access. Malicious software may also be injected into a trusted process to gain elevated privileges without prompting a user. (Citation: Davidson Windows) Adversaries can use these techniques to elevate privileges to administrator if the target process is unprotected.

Many methods have been discovered to bypass UAC. The Github readme page for UACMe contains an extensive list of methods (Citation: Github UACMe) that have been discovered and implemented within UACMe, but may not be a comprehensive list of bypasses. Additional bypass methods are regularly discovered and some used in the wild, such as:

- <code>eventvwr.exe</code> can auto-elevate and execute a specified binary or script. (Citation: enigma0x3 Fileless UAC Bypass) (Citation: Fortinet Fareit)

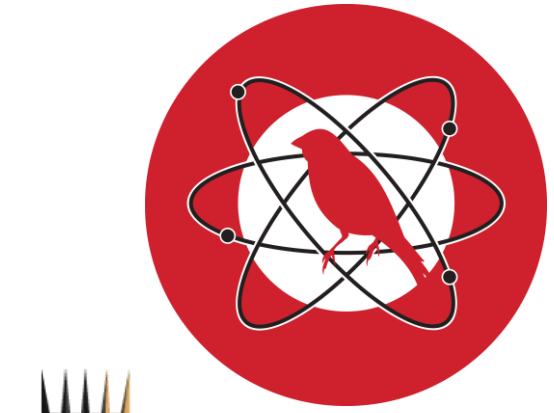
Another bypass is possible through some Lateral Movement techniques if credentials for an account with administrator privileges are known, since UAC is a single system security mechanism, and the privilege or integrity of a process running on one system will be unknown on lateral systems and default to high integrity. (Citation: SANS UAC Bypass)</blockquote>

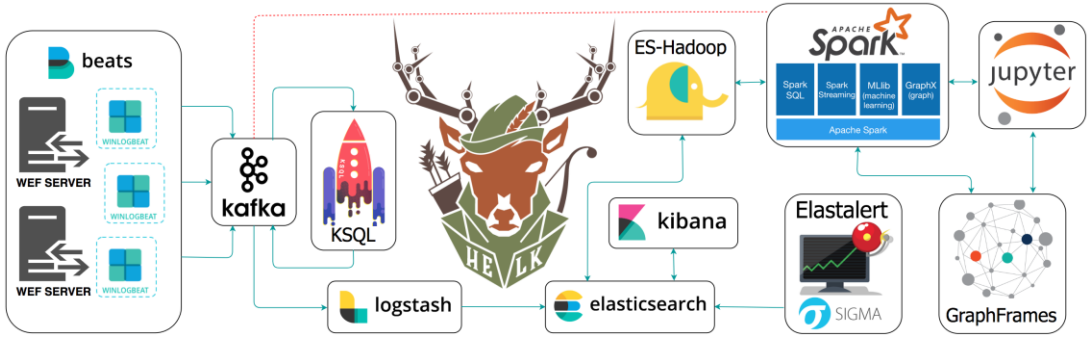
Atomic Tests

- Atomic Test #1 - Bypass UAC using Event Viewer (cmd)
- Atomic Test #2 - Bypass UAC using Event Viewer (PowerShell)
- Atomic Test #3 - Bypass UAC using Fodhelper
- Atomic Test #4 - Bypass UAC using Fodhelper - PowerShell
- Atomic Test #5 - Bypass UAC using ComputerDefaults (PowerShell)
- Atomic Test #6 - Bypass UAC by Mocking Trusted Directories

https://atomicthreatcoverage.atlassian.net/wiki/spaces/ATC

ATT&CK:
Red canary
Mordor
HELK
etc.

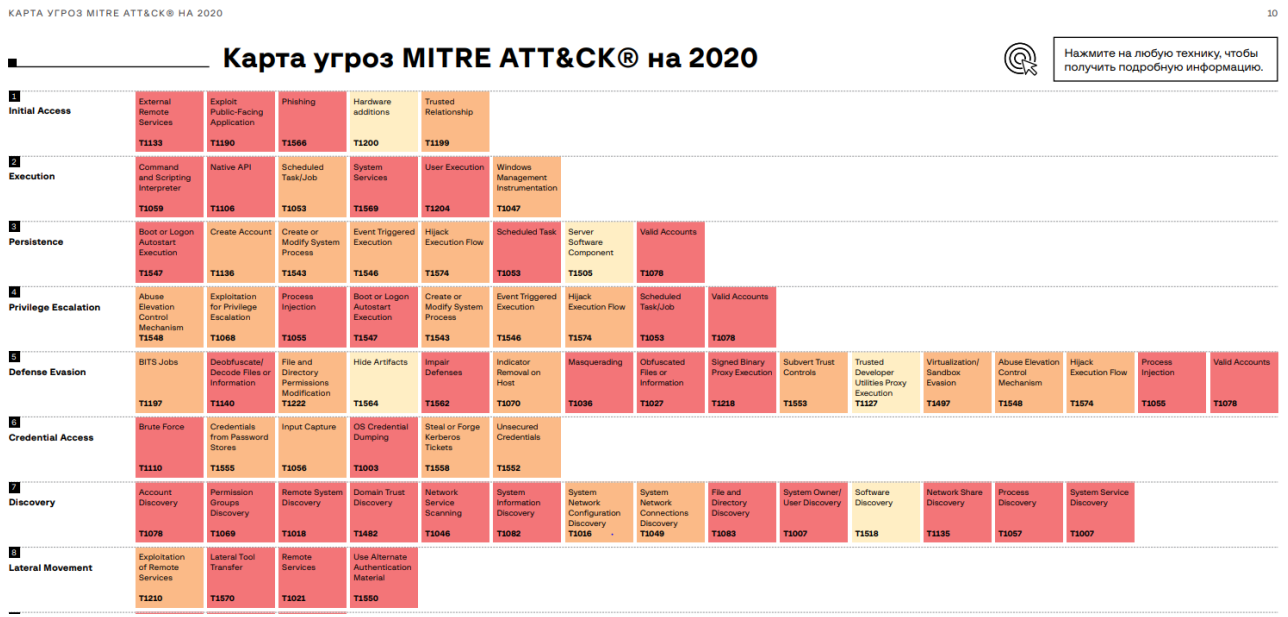




https://github.com/redcanaryco/atomic-red-team
https://mordordatasets.com/introduction.html
https://thehelk.com/intro.html

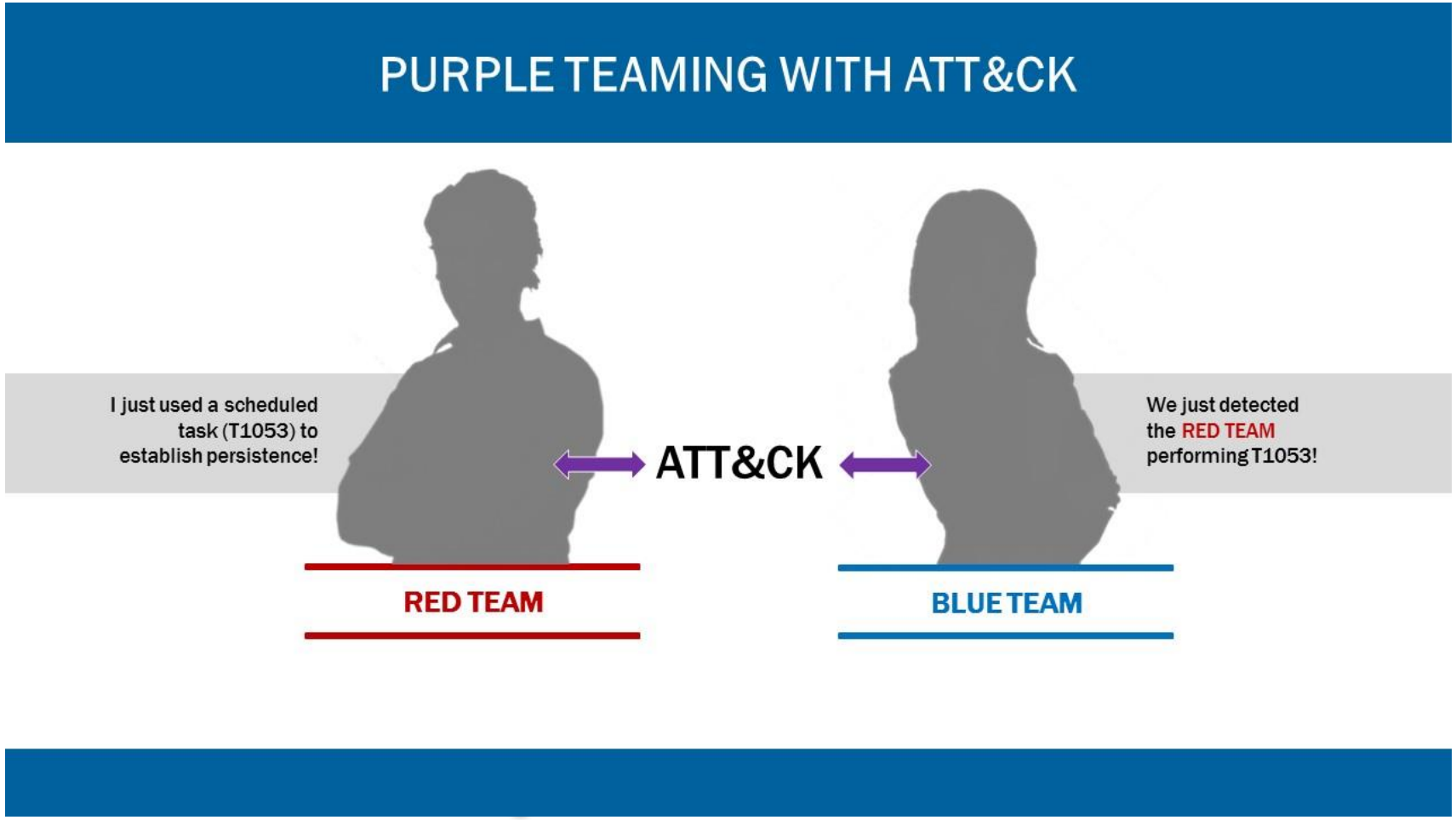
ATT&CK: в отчетах

PARINACOTA attack chain	MITRE ATT&CK
Initial access via RDP brute force	T1190 | Exploit Public-Facing Application
Security controls turned off	T1089 - Disabling Security Tools
Credential dumping using Mimikatz	T1003 - Credential Dumping
Scanning for additional targets on ports 3389 (RDP), 445 (SMB), and 22 (SSH)	T1046 - Network Service Scanning T1047 - Windows Management Instrumentation
Lateral movement	
Brute force on targets via SMB and SSH using Hydra	T1110 - Brute Force
Stolen credentials used to connect to multiple other servers via RDP	T1076 - Remote Desktop Protocol
On a particular server, WMI and PsExec used to allow remote desktop connections	T1047 - Windows Management Instrumentation
Blocking on 3389 disabled in the firewall using netsh	T1089 - Disabling Security Tools
Connection via RDP, all services stopped	T1076 - Remote Desktop Protocol
Compromised server used to distribute ransomware to the server infrastructure	T1471 - Data Encrypted for Impact



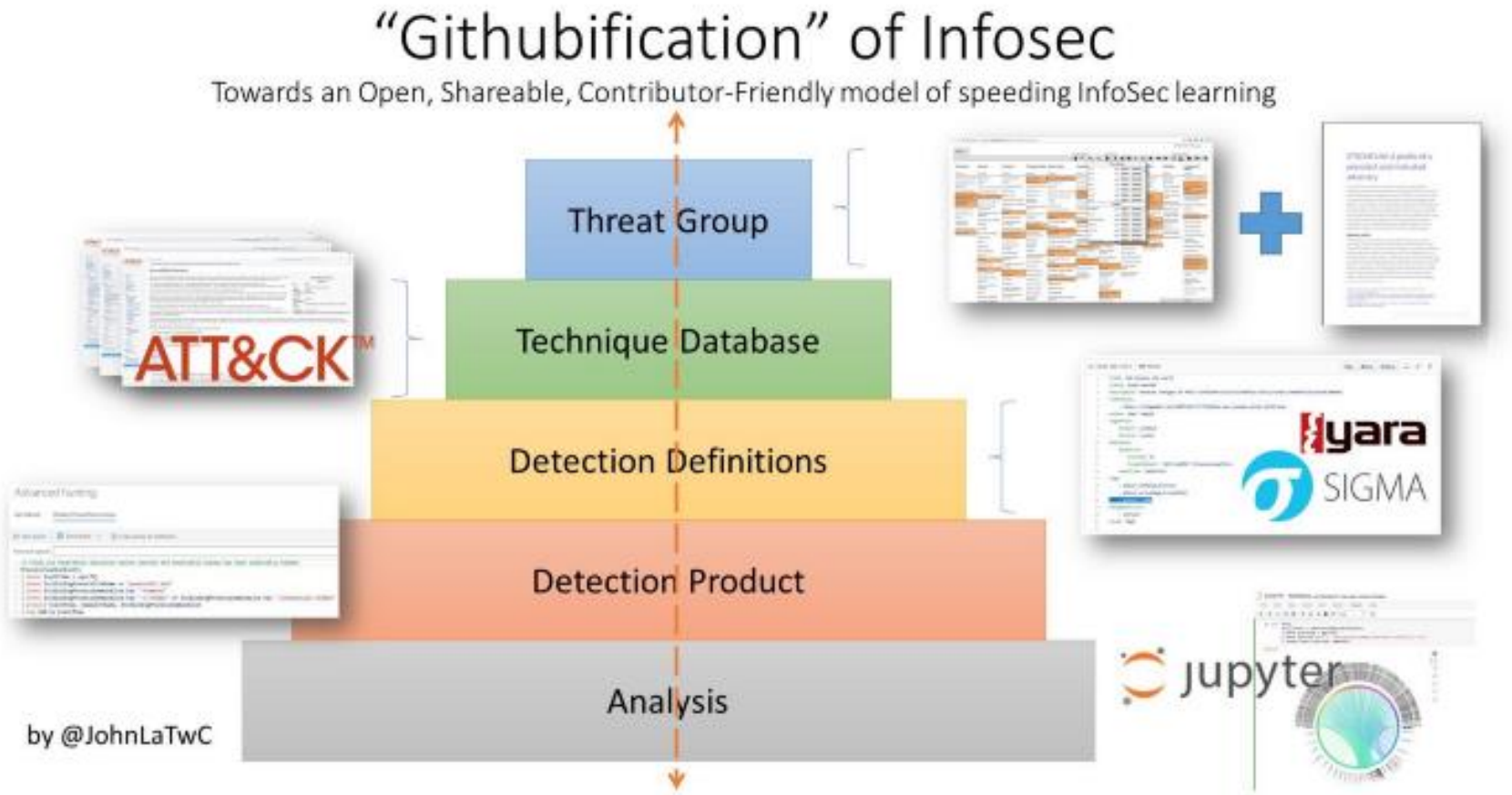
https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
https://www.group-ib.ru/resources/threat-research/ransomware-2021.html

ATT&CK: Red&Blue



https://blog.shi.com/cybersecurity/how-to-improve-threat-detection-and-response-with-mitre-attck/

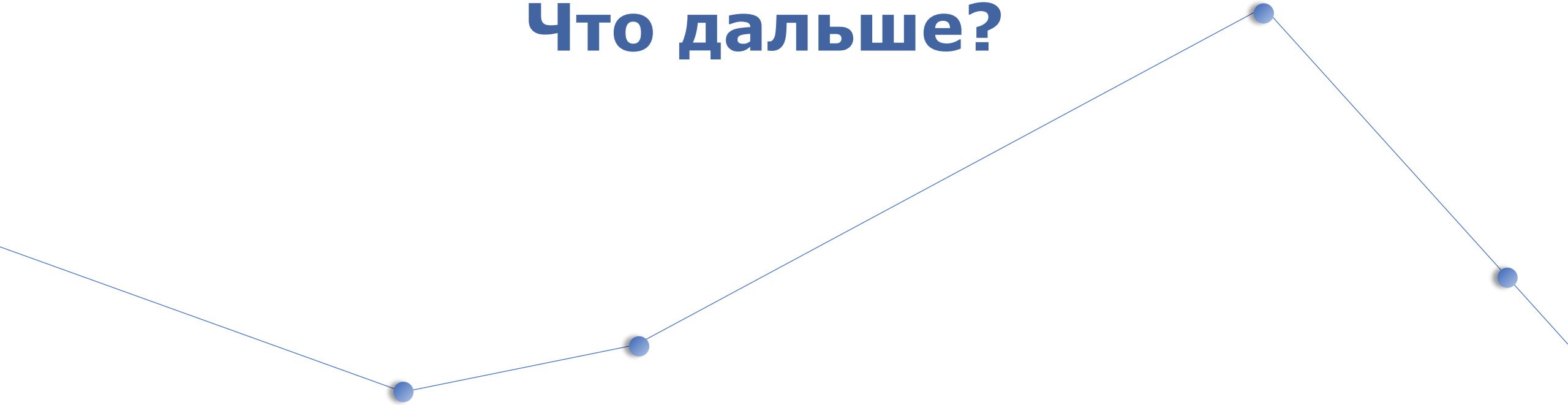
ATT&CK: Peer2Peer



https://medium.com/@johnlatwc/the-githubification-of-infosec-afbdbfaad1d1

After ATT&CK

Что дальше?



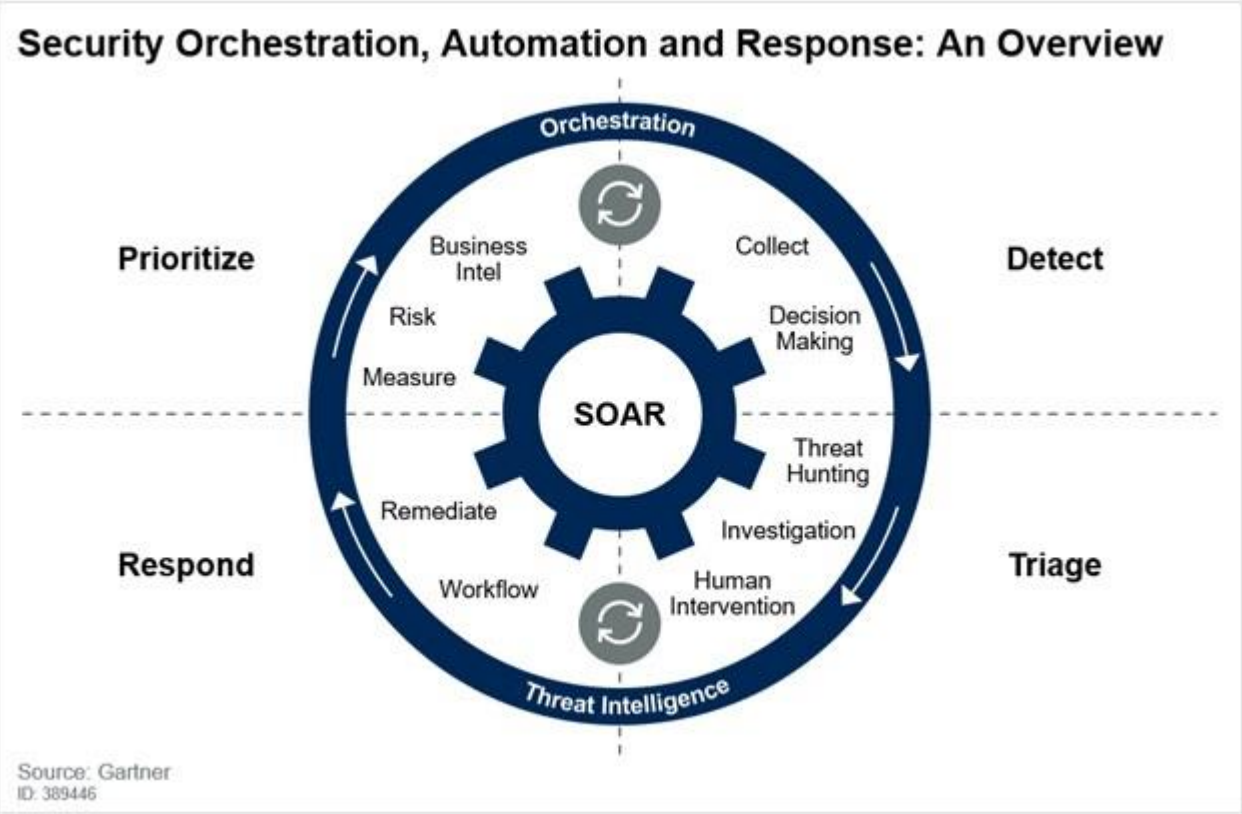
ИБ-ландшафт

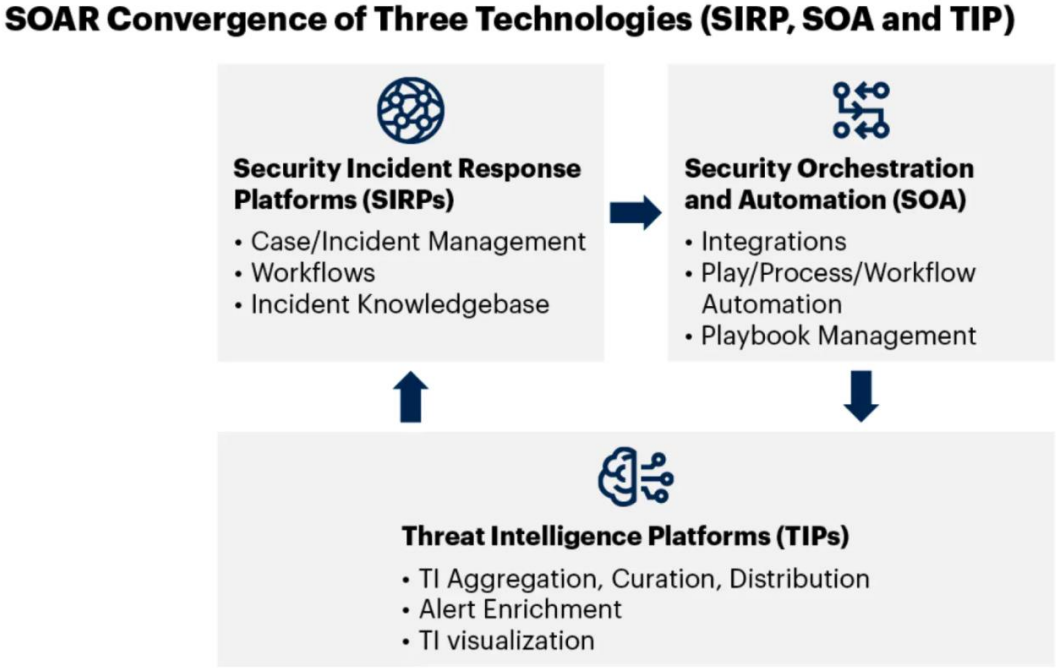
https://www.optiv.com/navigating-security-landscape-guide-technologies-and-providers

ИБ-ландшафт (RU)

https://www.tadviser.ru/images/a/a8/ISecurity_%285%29.jpg

Gartner: SOAR





https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

Интеграции:

ПОЛУЧЕНИЕ ДАННЫХ и АКТИВНОЕ РЕАГИРОВАНИЕ

ВНЕШНИЕ СЕРВИСЫ

Virustotal
Threatgread
Whois
Urlscan.io
HybridAnalysis
Shodan
…

SIEM\LM СИСТЕМЫ

Splunk
ArcSight
Qradar
MP SIEM
ElasticSearch
…

СЗИ, ИНФРА, ENDPOINTS

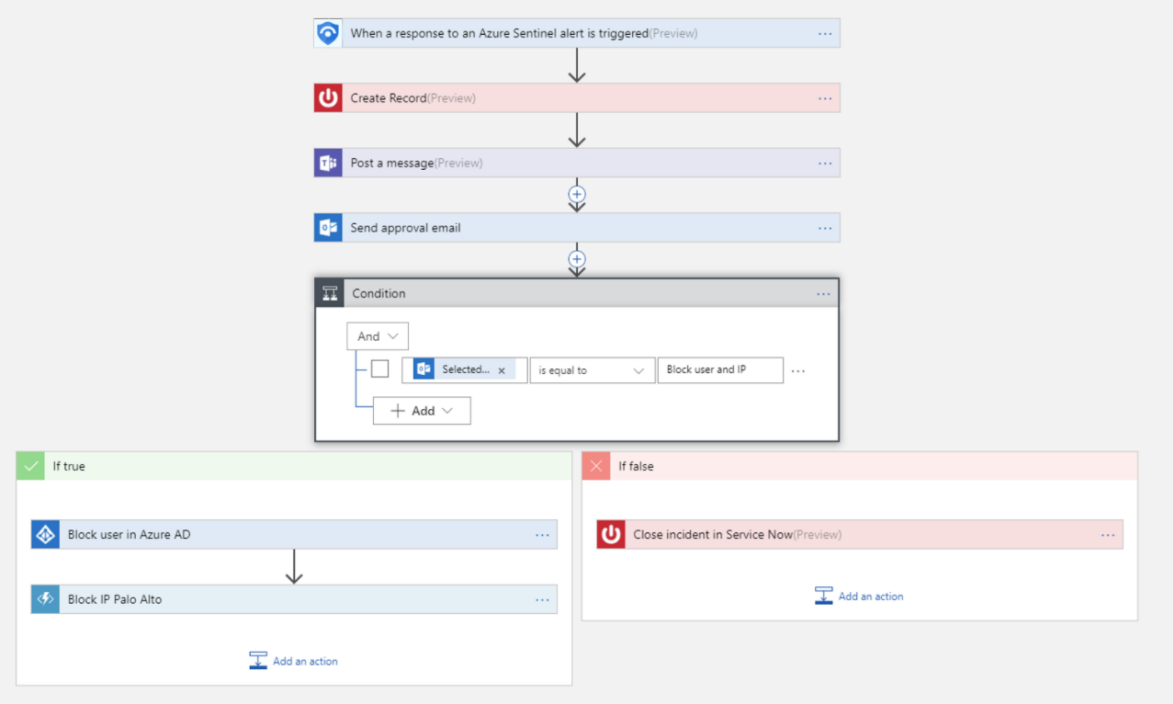
Kaspersky
McAfee
Nessus
Qualys
Active Directory
FW, Switches
Windows, Linux
LiveForensic

DATA LAKES

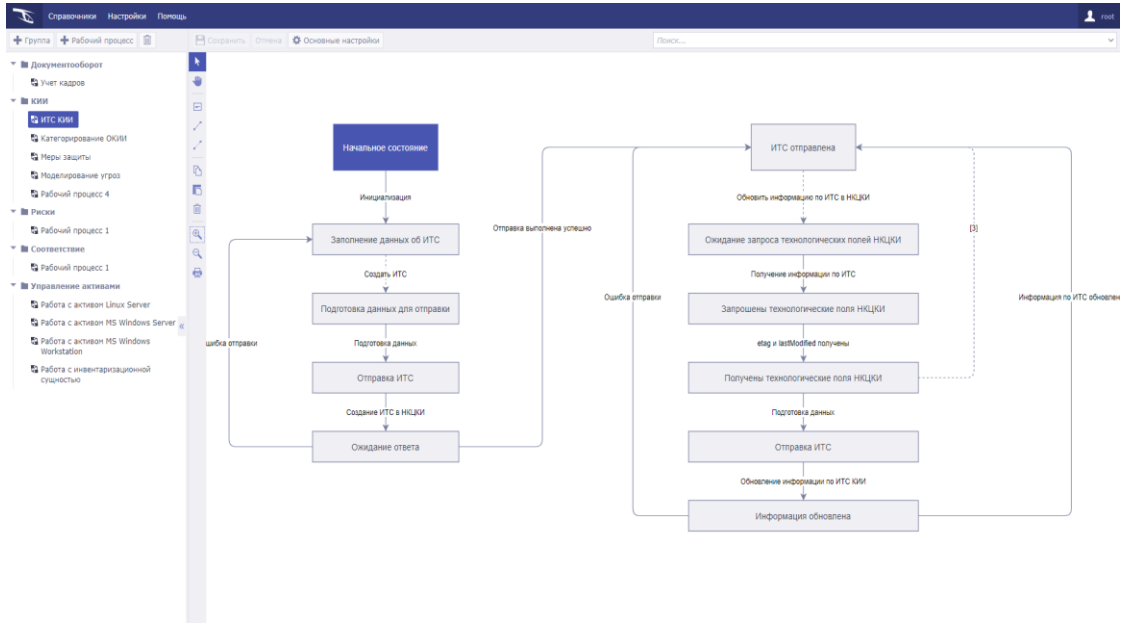
Kafka
Spark
Zeppelin
…

Рабочие процессы:

ДРЕВОВИДНЫЕ



ЦИКЛИЧЕСКИЕ



ЗАРАЖЕНИЕ

80 МИНУТ → 10 МИНУТ С SOAR

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

АТАКА НА ВНЕШНИЙ САЙТ

70 МИНУТ → 5 МИНУТЫ С SOAR

ДО АВТОМАТИЗАЦИИ

70 МИНУТ

10 мин | 15 мин | 25 мин | 10 мин

1. ПОЛУЧЕНИЕ ИНФОРМАЦИИ О АТАКУЕМОМ РЕСУРСЕ
2. ПОИСК АССОЦИИРО-ВАННЫХ ИНДИКАТОРОВ
3. БЛОКИРОВКА ИНДИКАТОРОВ И СИГНАТУР АТАКИ
4. ИСТОРИЧЕСКИЙ ПОИСК ВРЕДОНОСНОЙ АКТИВНОСТИ
5. ПОДГОТОВКА ОТЧЕТА ОБ АТАКЕ

ПОСЛЕ АВТОМАТИЗАЦИИ

5 МИНУТЫ

участие человека

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

АНАЛИЗ ОБНАРУЖЕННЫХ УЯЗВИМОСТЕЙ

85 МИНУТ → 2 МИНУТЫ С SOAR

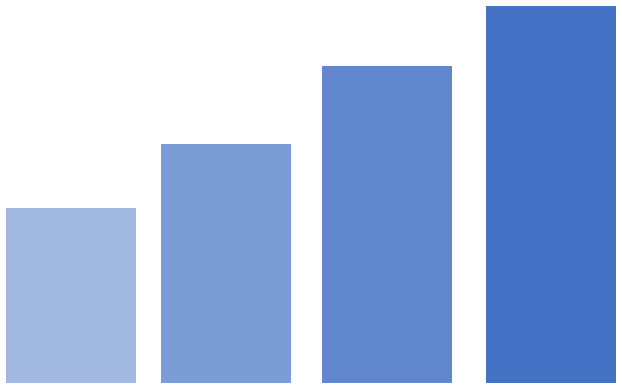
SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

МЕТРИКИ
эффективности

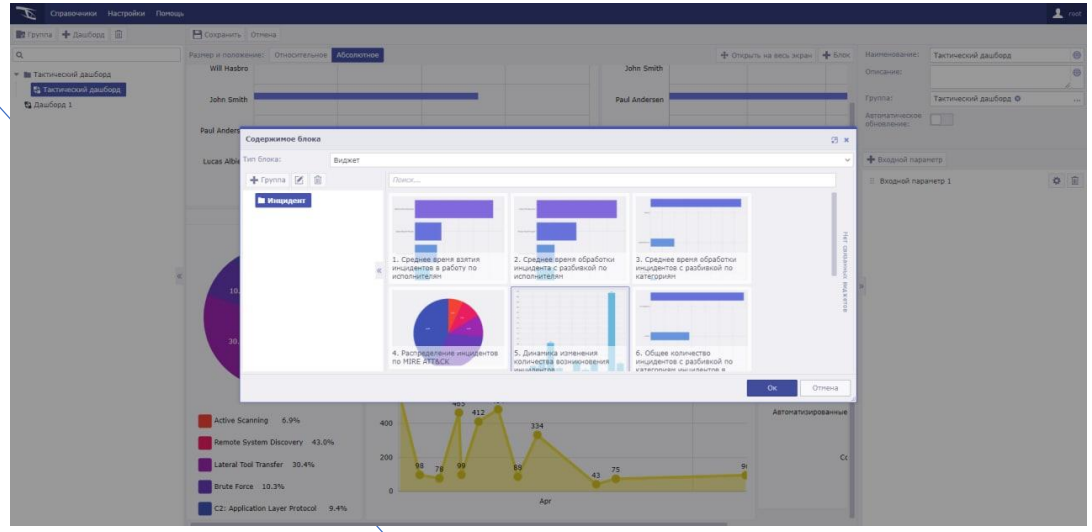
MEAN TIME TO

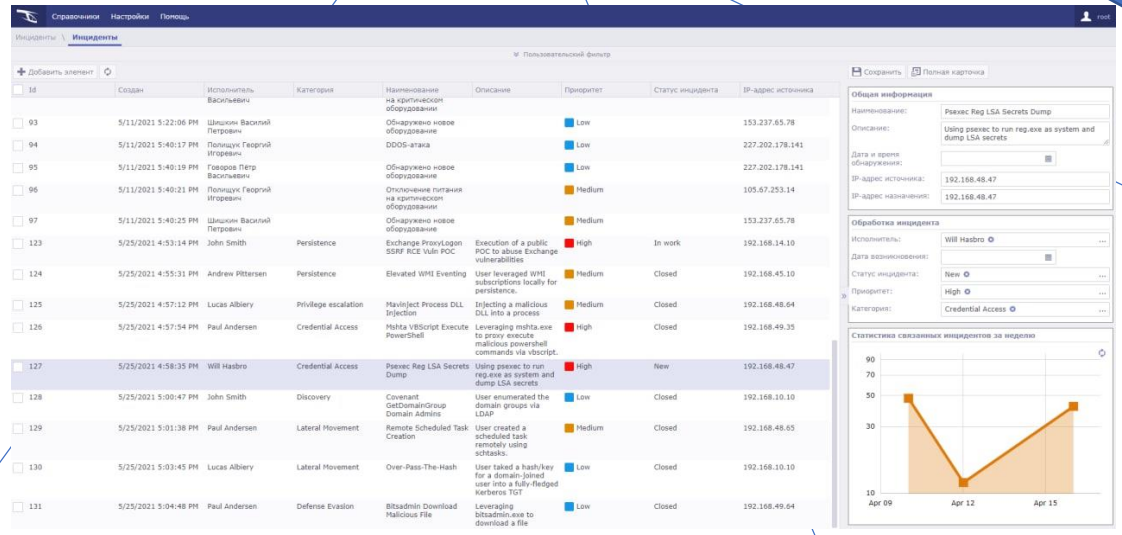
- Triage
- Qualify
- Investigate
- Mitigate
- Recover
- Detect
- Response
- Acknowledge
- Contain

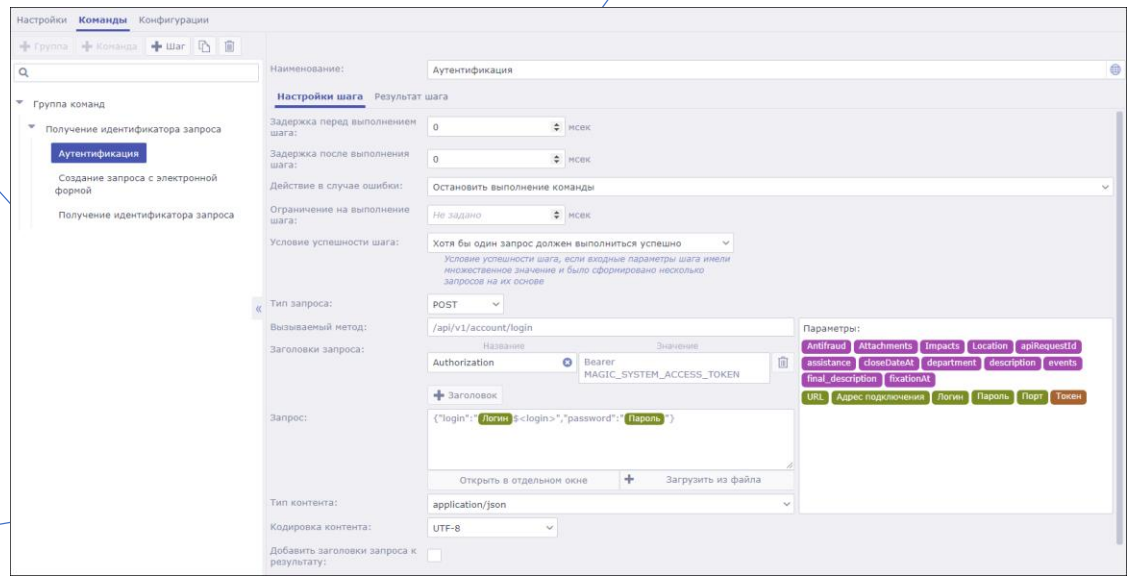
ROI



IRP (SOAR) SECURITY VISION







SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

СПАСИБО ЗА ВНИМАНИЕ