



SECURITY VISION  
УВИДЕТЬ БЕЗОПАСНОСТЬ

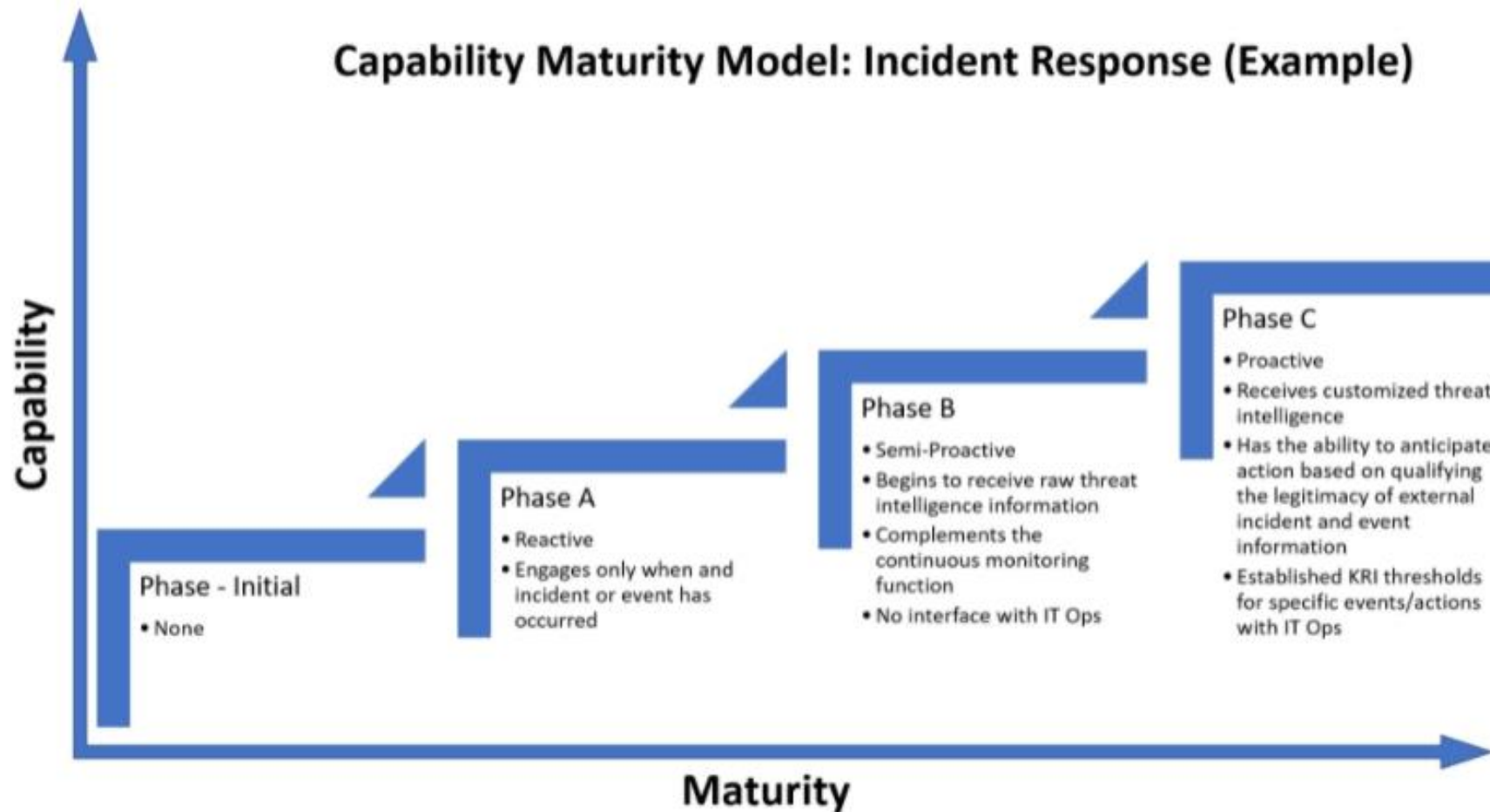
# ТЕХНИКИ И ТЕХНОЛОГИИ

## РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИБ

Луцив Данила  
[dlutsiv@securityvision.ru](mailto:dlutsiv@securityvision.ru)

# ИНЦИДЕНТЫ ИБ:

## ДОРОЖНАЯ КАРТА



# 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

---

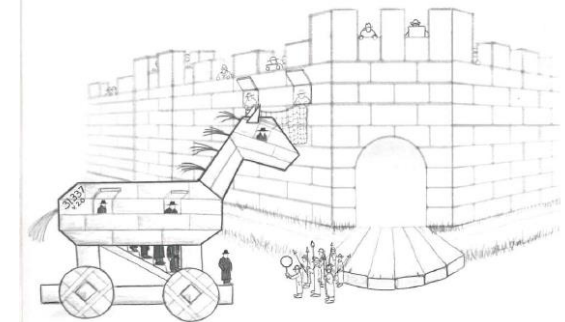
Paul Cichonski  
Tom Millar  
Tim Grance  
Karen Scarfone

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



**Blue Team Handbook:**  
SOC, SIEM, and Threat Hunting Use Cases  
Notes from the Field (V1.02)

*A condensed field guide for  
the Security Operations team.*



Don Murdoch 

<https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/fina>

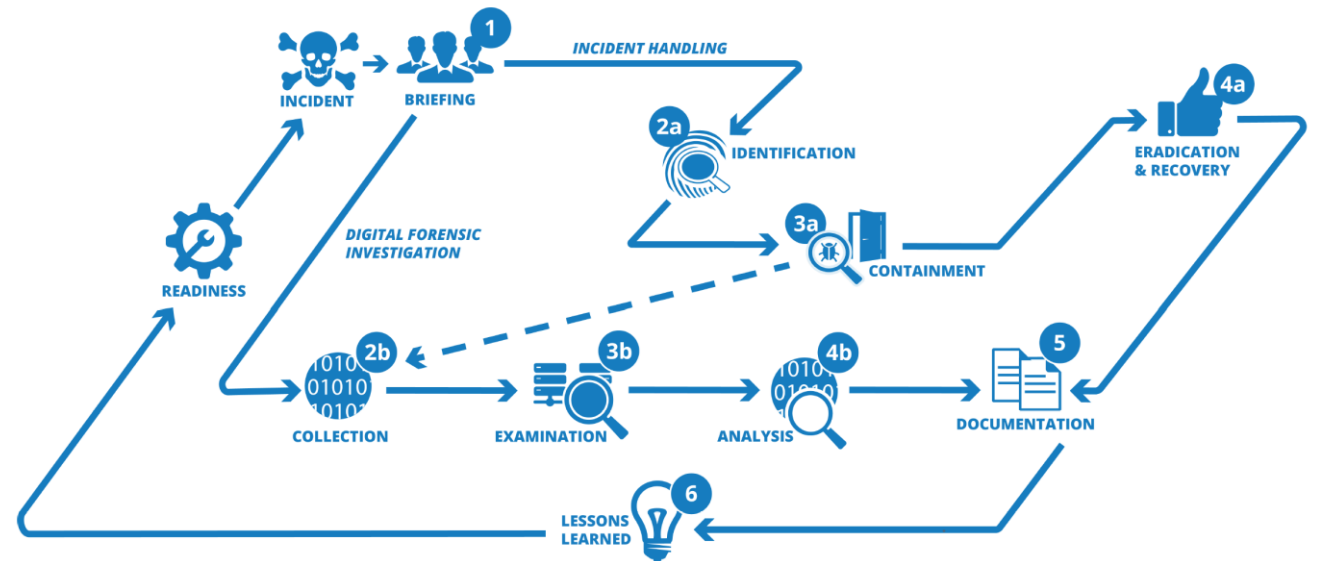
<http://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf>

<https://www.amazon.com/Blue-Team-Handbook-condensed-Responder/dp/1500734756>

# 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



# 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



# ИСТОЧНИКИ: ПРИОРИТИЗАЦИЯ

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

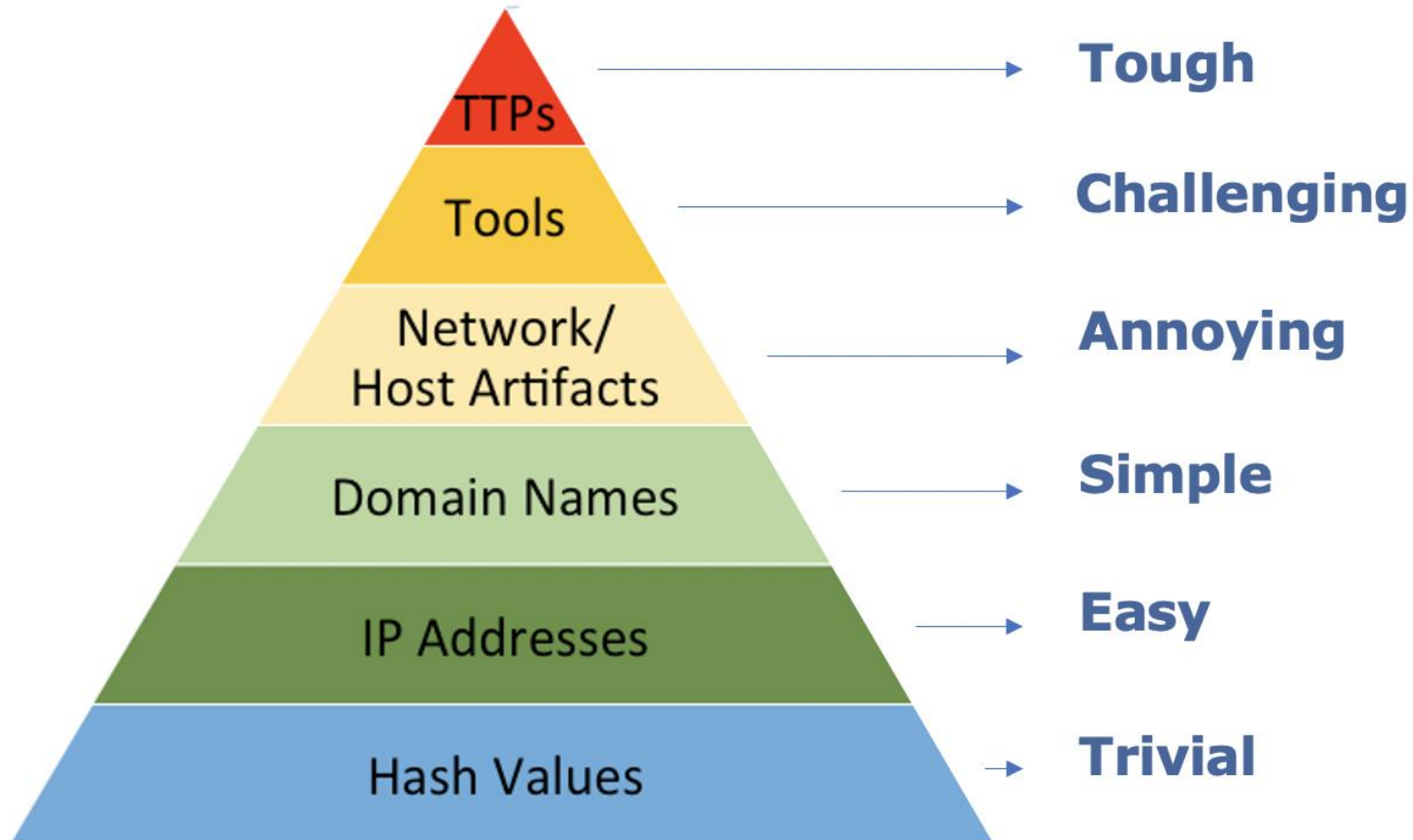
# ИСТОЧНИКИ:

## 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/125927433/Logging+Policies>

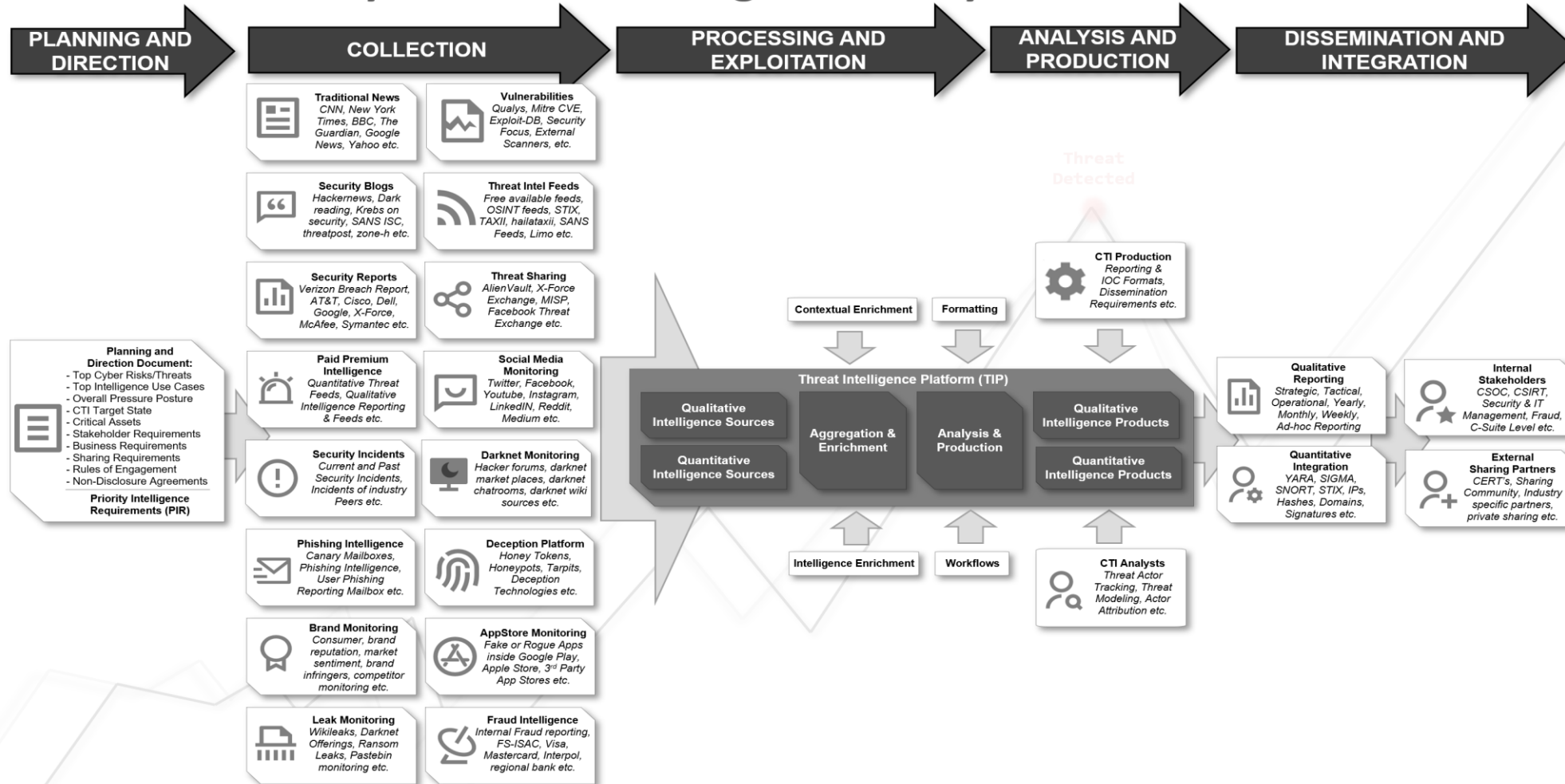


# PYRAMID OF PAIN

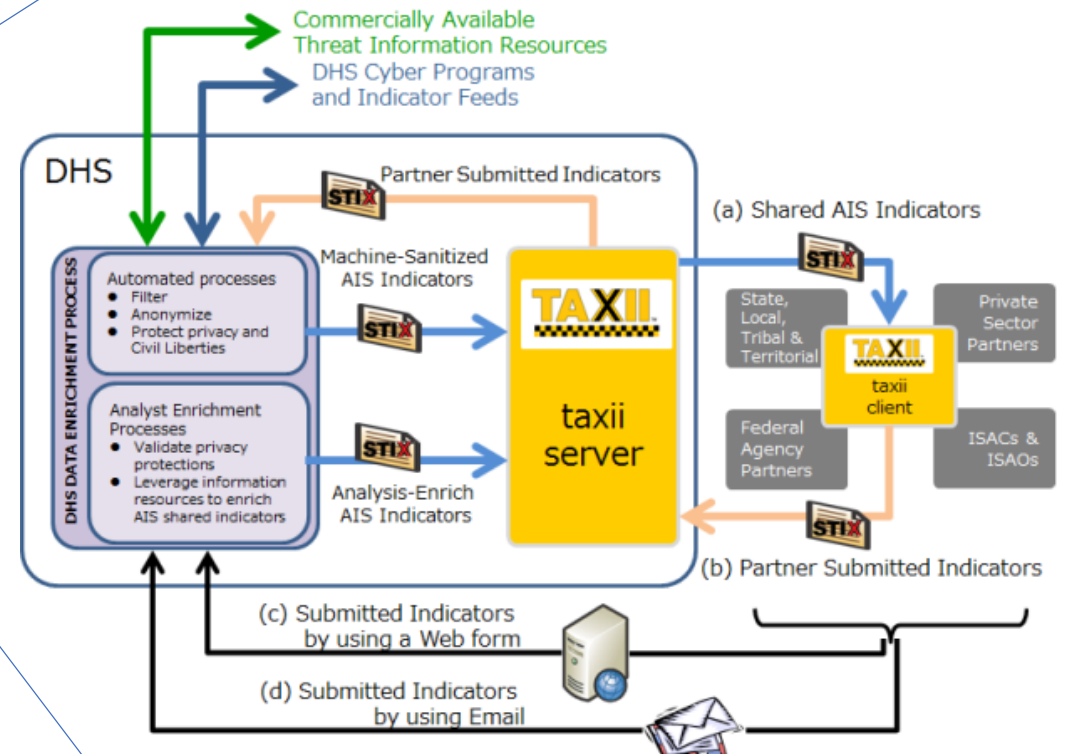
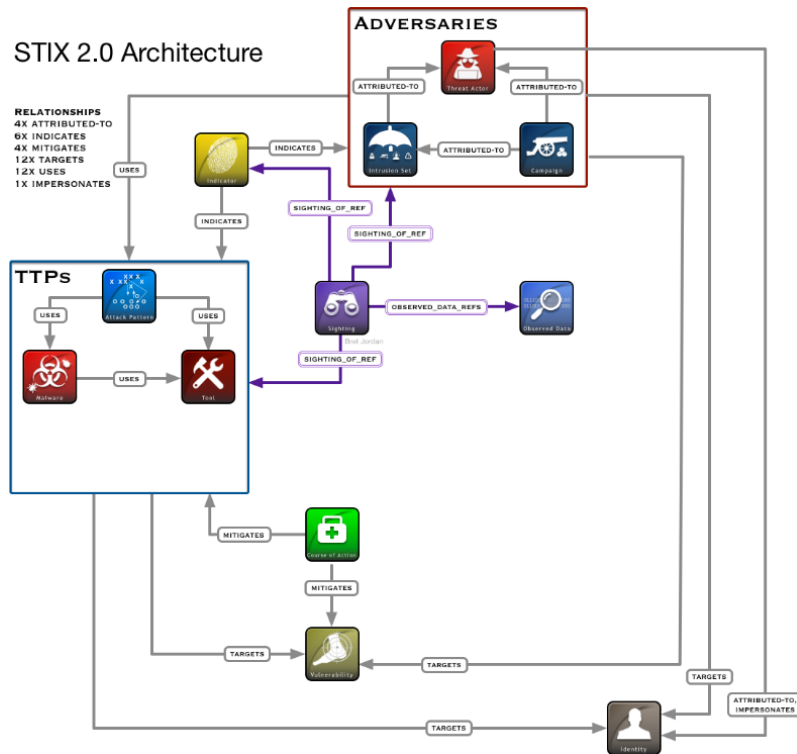


# Threat Intel Lifecycle

## Cyber Threat Intelligence Lifecycle Overview



# STIX/TAXII



# ATT&CK framework

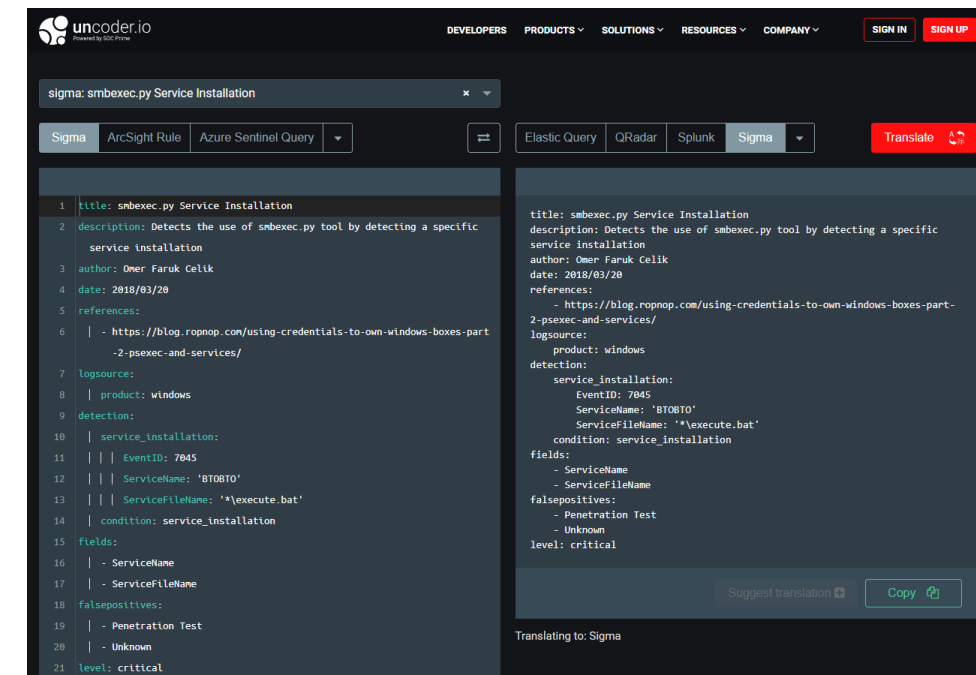
Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Browser Extensions	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Channel	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Deploy Container	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Network Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (7)	Domain Policy Modification (2)	Domain Policy Modification (2)	Direct Volume Access	Man-in-the-Middle (2)	Container and Resource Discovery	Software Deployment Tools	Data from Information Repositories (2)	Fallback Channels	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Escape to Host	Escape to Host	Domain Policy Modification (2)	Modify Authentication Process (4)	File and Directory Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Event Triggered Execution (15)	Execution Guardrails (1)	Network Sniffing	Network Service Scanning	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Exfiltration Over Web Service (2)	Inhibit System Recovery
Search Victim-Owned Websites			System Services (2)	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	Network Share Discovery		Data from Network Shared Drive	Non-Application Layer Protocol	Scheduled Transfer	Network Denial of Service (2)
			User Execution (3)	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Hide Artifacts (7)	Steal Application Access Token	Network Sniffing		Data from Removable Media	Non-Standard Port	Transfer Data to Cloud Account	Resource Hijacking
			Windows Management Instrumentation	Process Injection (11)	Process Injection (11)	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (4)	Password Policy Discovery		Data Staged (2)	Protocol Tunneling		Service Stop
				Scheduled Task/Job (7)	Scheduled Task/Job (7)	Impair Defenses (7)	Indicator Removal on Host (6)	Peripheral Device Discovery		Email Collection (3)	Proxy (4)		System Shutdown/Reboot
				Valid Accounts (4)	Valid Accounts (4)	Indicator Removal on Host (6)	Indirect Command Execution	Permission Groups Discovery (3)		Input Capture (4)	Remote Access Software		
				External Remote Services	External Remote Services	Indirect Command Execution	Masquerading (6)	Process Discovery		Man in the Browser	Traffic Signaling (1)		
				Hijack Execution Flow (11)	Hijack Execution Flow (11)	Masquerading (6)	Modify Authentication Process (4)	Query Registry		Man-in-the-Middle (2)	Web Service (3)		
				Implant Internal Image	Implant Internal Image	Modify Authentication Process (4)	Modify Cloud Compute Infrastructure (4)	Remote System Discovery		Screen Capture			
				Modify Authentication Process (4)	Modify Authentication Process (4)	Modify Cloud Compute Infrastructure (4)		Software Discovery (11)		Video Capture			
				Office Application Startup (6)	Office Application Startup (6)								
				Pre-OS Boot (5)	Pre-OS Boot (5)								

# ATT&CK: Sigma rules



```

win_susp_lsass_dump.yml x win_susp_failed_logons_single_source.yml win_susp_failed_logon_reas
1 title: Password Dumper Activity on LSASS
2 description: Detects process handle on LSASS process with certain access mask and object type SAM_DOMAIN
3 status: experimental
4 reference: https://twitter.com/jackcr/status/807385668833968128
5 logsource:
6   product: windows
7 detection:
8   selection:
9     EventLog: Security
10    EventID: 4656
11    ProcessName: 'C:\Windows\System32\lsass.exe'
12    AccessMask: '0x705'
13    ObjectType: 'SAM_DOMAIN'
14 condition: selection
15 falsepositives:
16   - Unkown
17 level: high
18
  
```



uncoder.io  
DEVELOPERS PRODUCTS SOLUTIONS RESOURCES COMPANY SIGN IN SIGN UP

sigma: smbexec.py Service Installation

Sigma ArcSight Rule Azure Sentinel Query Elastic Query QRadar Splunk Sigma Translate

```

1 title: smbexec.py Service Installation
2 description: Detects the use of smbexec.py tool by detecting a specific
  service installation
3 author: Omer Faruk Celik
4 date: 2018/03/20
5 references:
6   - https://blog.ropnop.com/using-credentials-to-own-windows-boxes-part-2-psexec-and-services/
7 logsource:
8   product: windows
9 detection:
10  | service_installation:
11  | | EventID: 7045
12  | | ServiceName: 'BT08T0'
13  | | ServiceFileName: '*\execute.bat'
14  | condition: service_installation
15 fields:
16  | - ServiceName
17  | - ServiceFileName
18 falsepositives:
19  | - Penetration Test
20  | - Unknown
21 level: critical
  
```

title: smbexec.py Service Installation  
description: Detects the use of smbexec.py tool by detecting a specific service installation  
author: Omer Faruk Celik  
date: 2018/03/20  
references:  
- https://blog.ropnop.com/using-credentials-to-own-windows-boxes-part-2-psexec-and-services/  
logsource:  
product: windows  
detection:  
service\_installation:  
EventID: 7045  
ServiceName: 'BT08T0'  
ServiceFileName: '\*\execute.bat'  
condition: service\_installation  
fields:  
- ServiceName  
- ServiceFileName  
falsepositives:  
- Penetration Test  
- Unknown  
level: critical

Suggest translation Copy

Translating to: Sigma

<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

<b>Title</b>	DLL Load via LSASS
<b>Description</b>	Detects a method to load DLL via LSASS process using an un
<b>ATT&amp;CK Tactic</b>	TA0002: Execution
<b>ATT&amp;CK Technique</b>	T1177: LSASS Driver
<b>Data Needed</b>	<ul style="list-style-type: none"> <li>DN_0016_12_windows_sysmon_RegistryEvent</li> <li>DN_0017_13_windows_sysmon_RegistryEvent</li> </ul>
<b>Trigger</b>	T1177: LSASS Driver
<b>Severity Level</b>	high
<b>False Positives</b>	Unknown
<b>Development Status</b>	experimental
<b>References</b>	<ul style="list-style-type: none"> <li><a href="https://blog.xpnsec.com/exploring-mimikatz-part-1/">https://blog.xpnsec.com/exploring-mimikatz-part-1/</a></li> <li><a href="https://twitter.com/SBousseaden/status/1183745981189">https://twitter.com/SBousseaden/status/1183745981189</a></li> </ul>
<b>Author</b>	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

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

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

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:

- `eventvwr.exe` 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)

### Atomic Tests

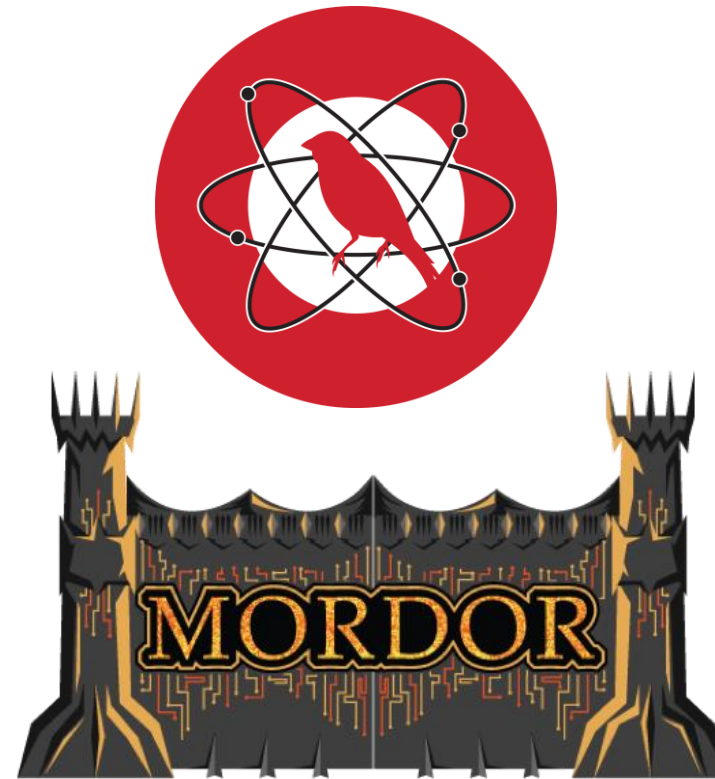
- Atomic Test #1 - Bypass UAC using Event Viewer (cmd)
- Atomic Test #2 - Bypass UAC using Event Viewer (PowerShell)
- Atomic Test #3 - Bypass UAC using Fodhelper
- Atomic Test #4 - Bypass UAC using Fodhelper - PowerShell
- Atomic Test #5 - Bypass UAC using ComputerDefaults (PowerShell)
- Atomic Test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

## Detection Rules

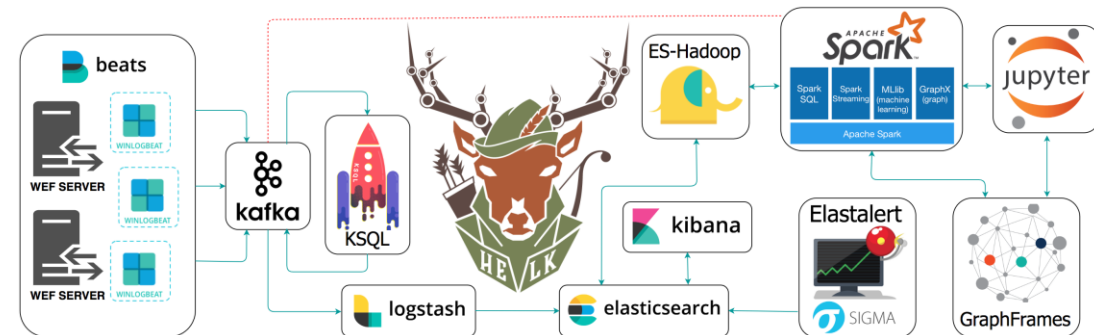
▼ Sigma rule

```
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
```

# ATT&CK: Red canary Mordor HELK etc.



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

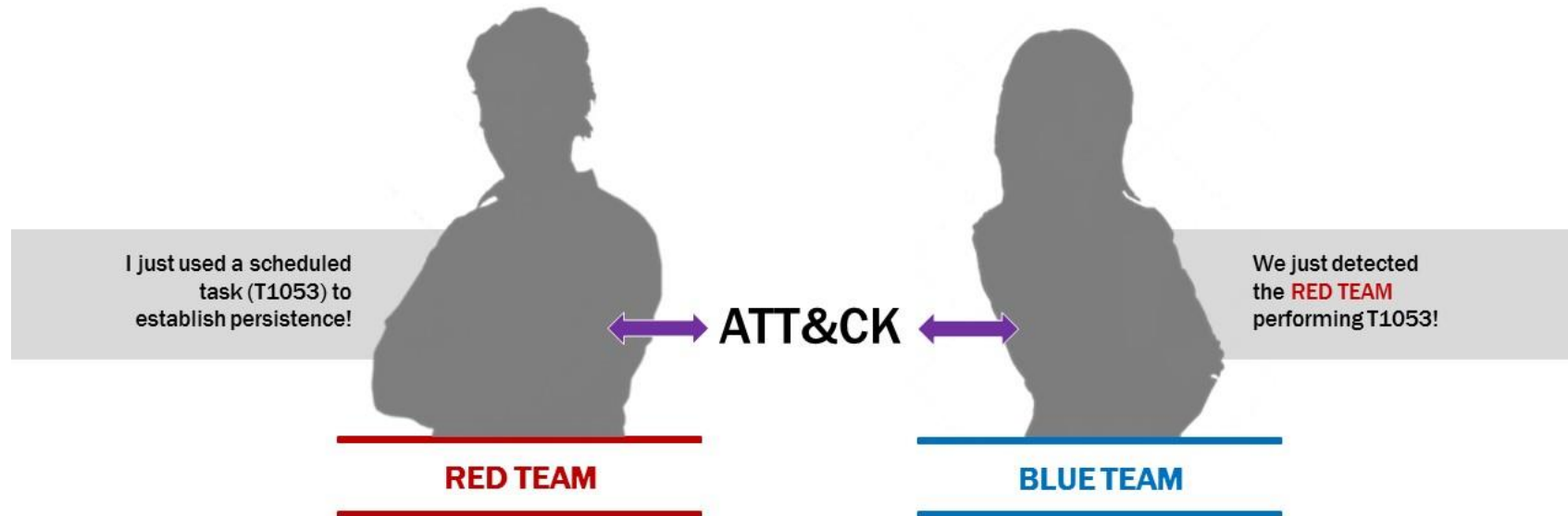






# ATT&CK: Red&Blue

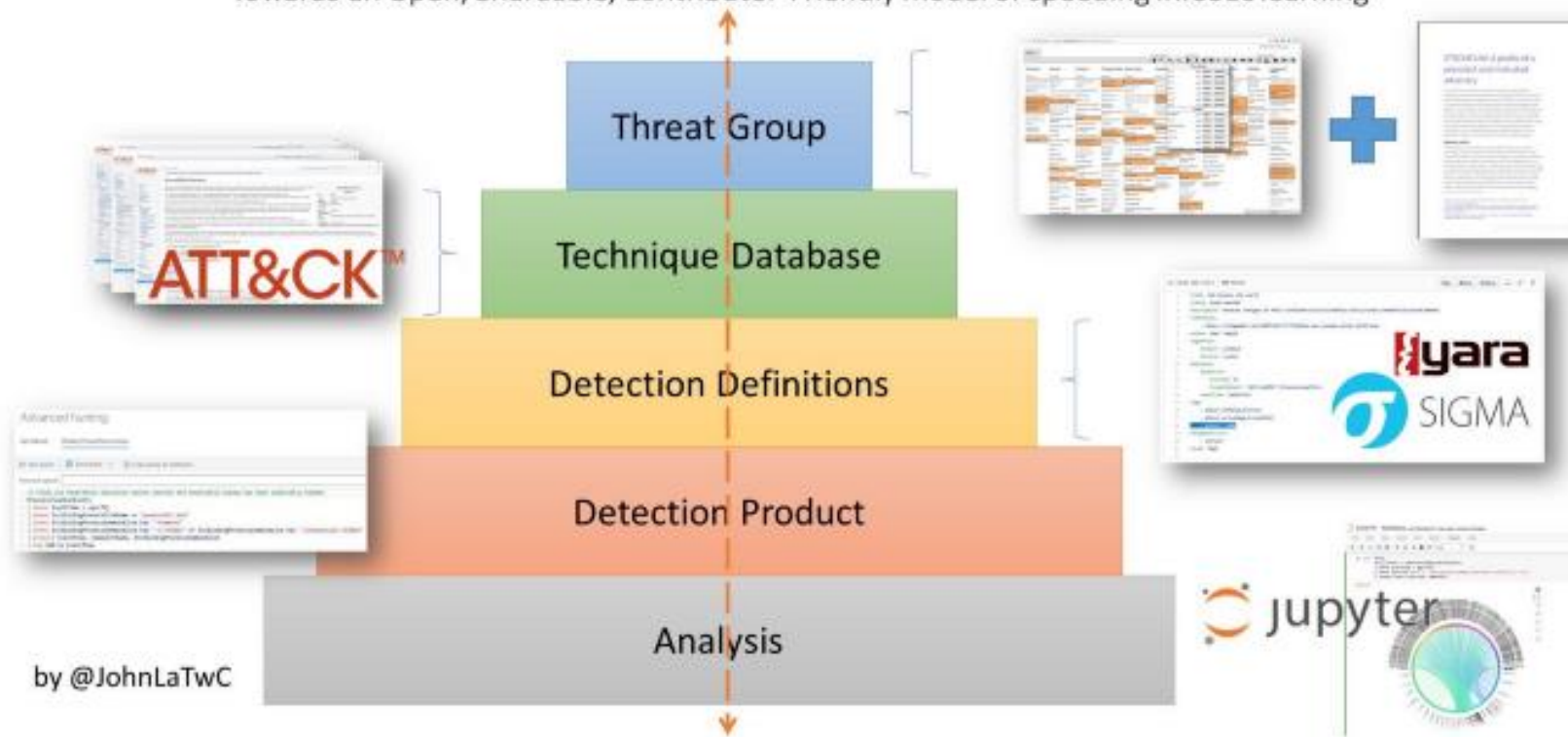
## PURPLE TEAMING WITH ATT&CK



# ATT&CK: Peer2Peer

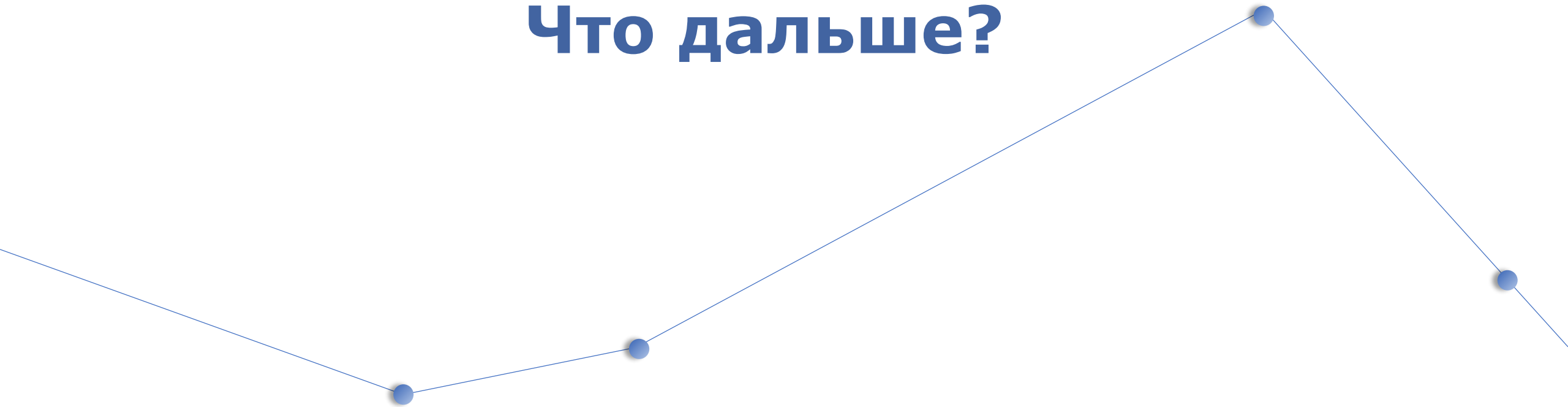
## “Githubification” of Infosec

Towards an Open, Shareable, Contributor-Friendly model of speeding InfoSec learning



# After ATT&CK

Что дальше?



# ИБ-ландшафт



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

# ИБ-ландшафт (RU)

## ЗАЩИТА ИНФРАСТРУКТУРЫ INFRASTRUCTURE PROTECTION

**Анализаторы сетевого трафика**  
Network Traffic Analysis

**Защита от DDoS-атак**  
DDoS Defence

**Промышленная безопасность**  
Industrial Security

**Виртуальные частные сети**  
Virtual Private Networks

**Безопасность мобильных решений**  
Mobile Security

**Защита веб-приложений**  
Web Application Firewall

**Межсетевые экраны нового поколения, Шлюзы безопасности**  
Next Gen Firewall / Unified Threat Management

**Защита конечных точек (вкл. антивирус)**  
Endpoint Detection & Response (incl. antivirus)

**Системы контентной фильтрации**  
Content Filtering, DPI

**Защита устройств интернета вещей**  
IoT Security

**Безопасность облачных и виртуальных сред**  
Cloud & Virtual Security

## МОНИТОРИНГ, ИССЛЕДОВАНИЕ, АНАЛИЗ MONITORING, RESEARCH, ANALYSIS

**Выявление и управление инцидентами**  
Security Information and Event Management

**Системы анализа защищенности. Средства безопасной разработки**  
Vulnerability Assessment Tools, DevSecOps

**Защита от утечек и расследование инцидентов**  
Data Leak Prevention

**Системы управления процессами информационной безопасности**  
Security Governance, Risk, Compliance

**Центр мониторинга и реагирования на инциденты**  
Security Operations Center

**Платформы поиска и обнаружения атак**  
Threat Intelligence Platform

**Охота на угрозы**  
Threat Hunting

**Повышение осведомленности в сфере ИБ и обучение сотрудников**  
Security Awareness & Training

**Мониторинг действий сотрудников**  
Employee Monitoring Software

**Система анализа поведения пользователей и сущностей**  
User and Entity Behavior Analytics

**Средства криптографической защиты информации**

**Средства защиты информации от несанкционированного доступа**

**Средства защиты файлов и баз данных**  
Files & Database Security

**Электронная подпись**  
Digital Signature

## ЗАЩИТА ДАННЫХ DATA PROTECTION

**Управление учетными записями и доступом**  
Identity and Access Management / Identity Governance and Administration / Single Sign-On / Two Factor Authentication

**Модули доверенной загрузки**  
Trusted Security Modules

**Системы управления ключевыми носителями**  
Public Key Infrastructure

**Контроль действий привилегированных пользователей**  
Privileged Access Management

**Биометрические системы аутентификации**  
Biometric Authentication

**Средства криптографической защиты информации**

**Средства защиты информации от несанкционированного доступа**

**Средства защиты файлов и баз данных**  
Files & Database Security

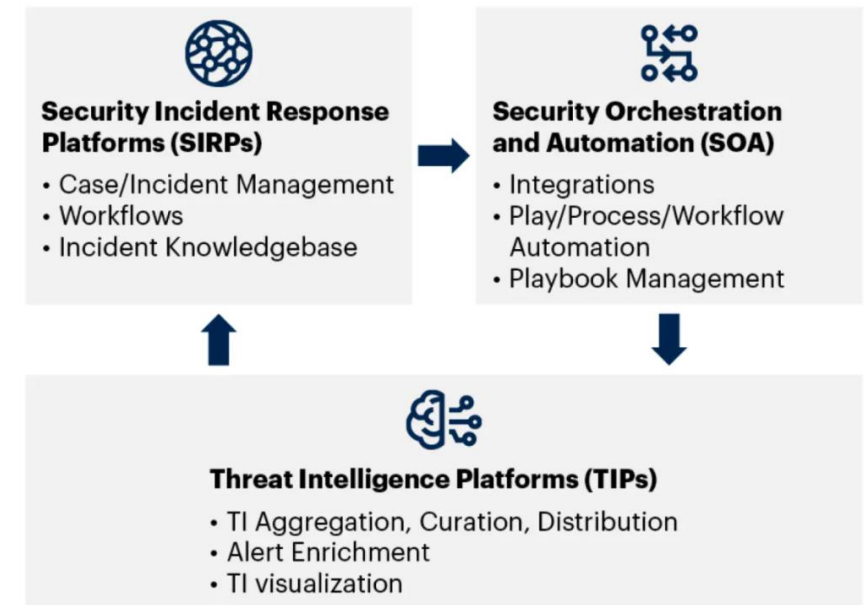
**Электронная подпись**  
Digital Signature

# Gartner: SOAR

## Security Orchestration, Automation and Response: An Overview



## SOAR Convergence of Three Technologies (SIRP, SOA and TIP)



# 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

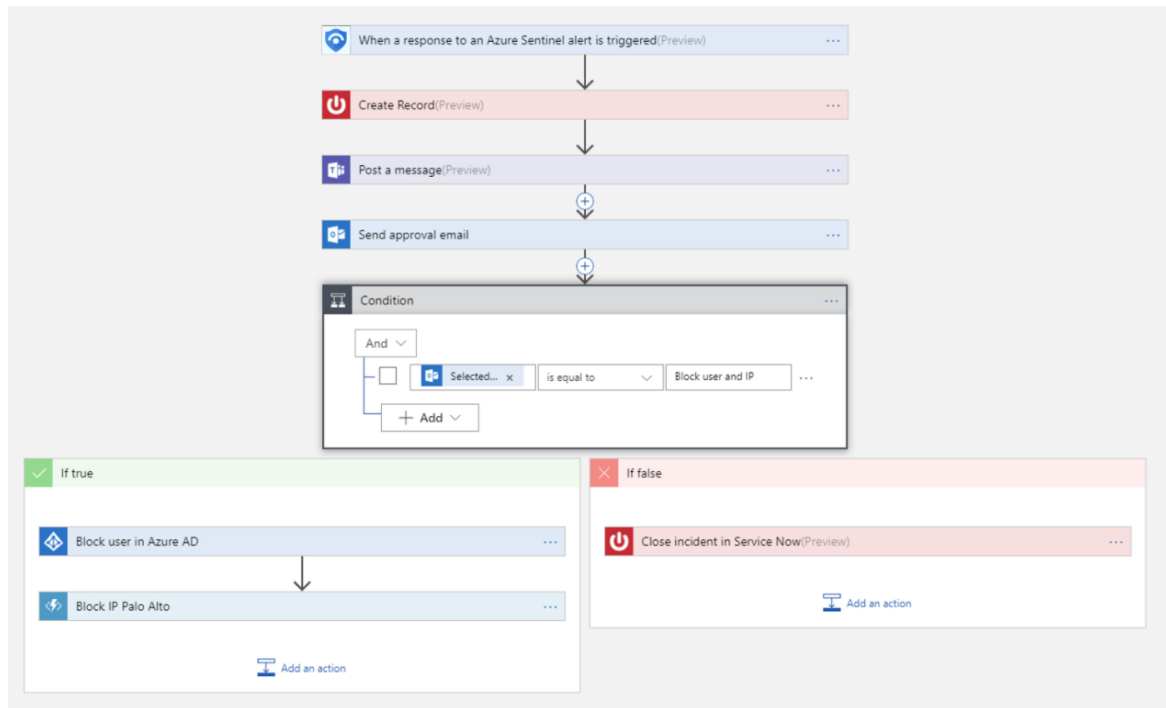
Kaspersky  
McAfee  
Nessus  
Qualys  
Active Directory  
FW, Switches  
Windows, Linux  
LiveForensic

### DATA LAKES

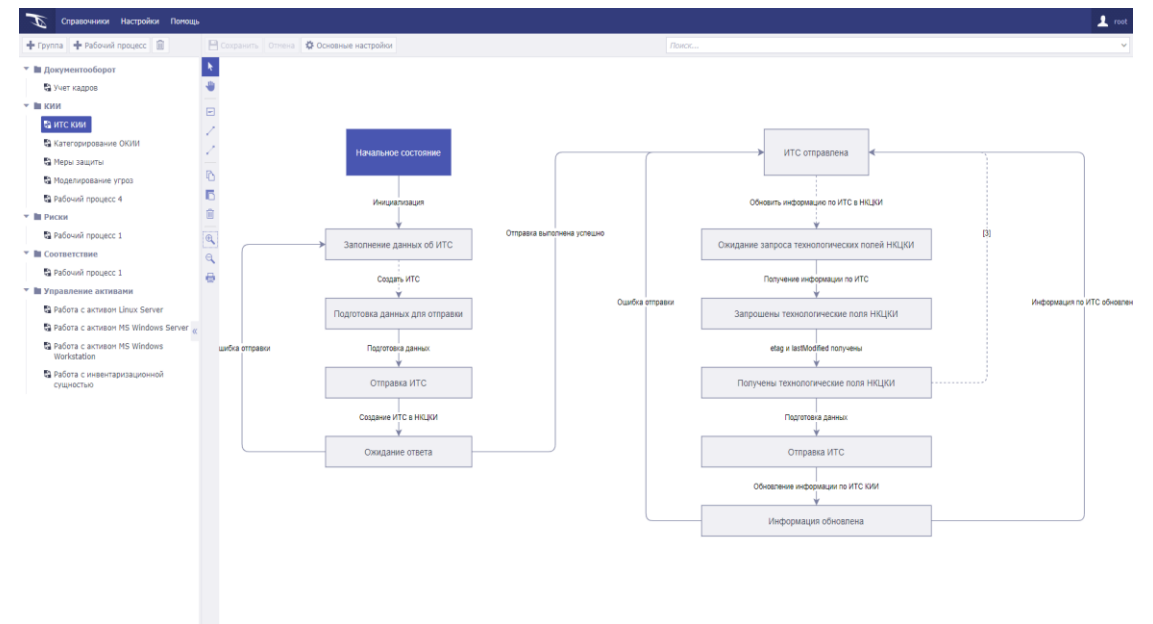
Kafka  
Spark  
Zeppelin  
...

# Рабочие процессы:

## ДРЕВОВИДНЫЕ



## ЦИКЛИЧЕСКИЕ

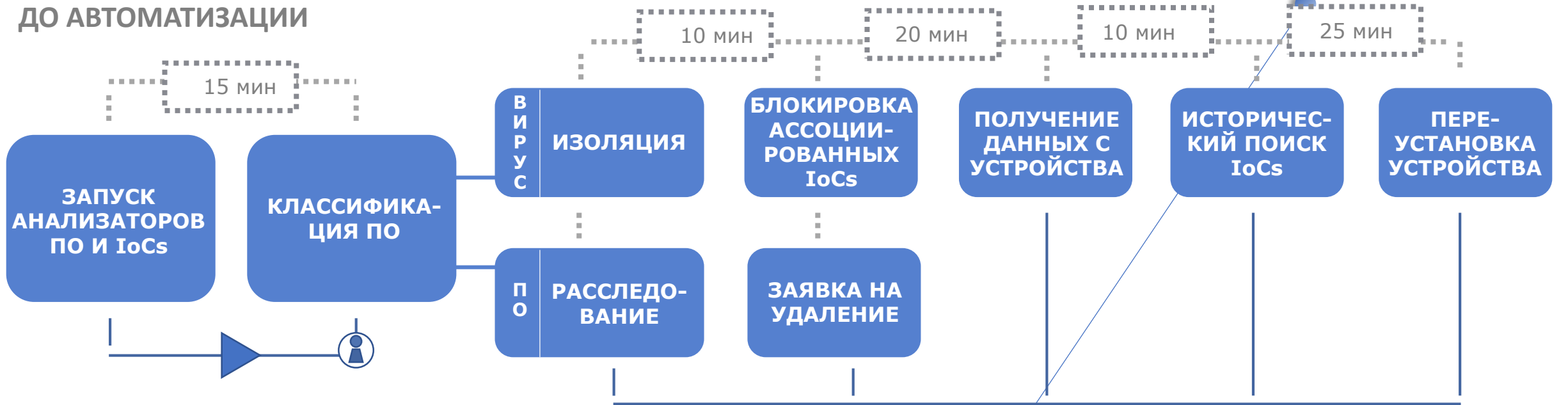




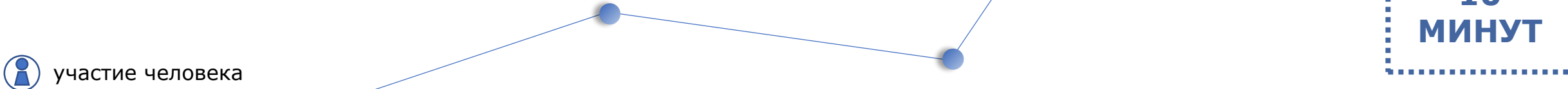
# ЗАРАЖЕНИЕ

80 МИНУТ → 10 МИНУТ С SOAR

ДО АВТОМАТИЗАЦИИ



ПОСЛЕ АВТОМАТИЗАЦИИ

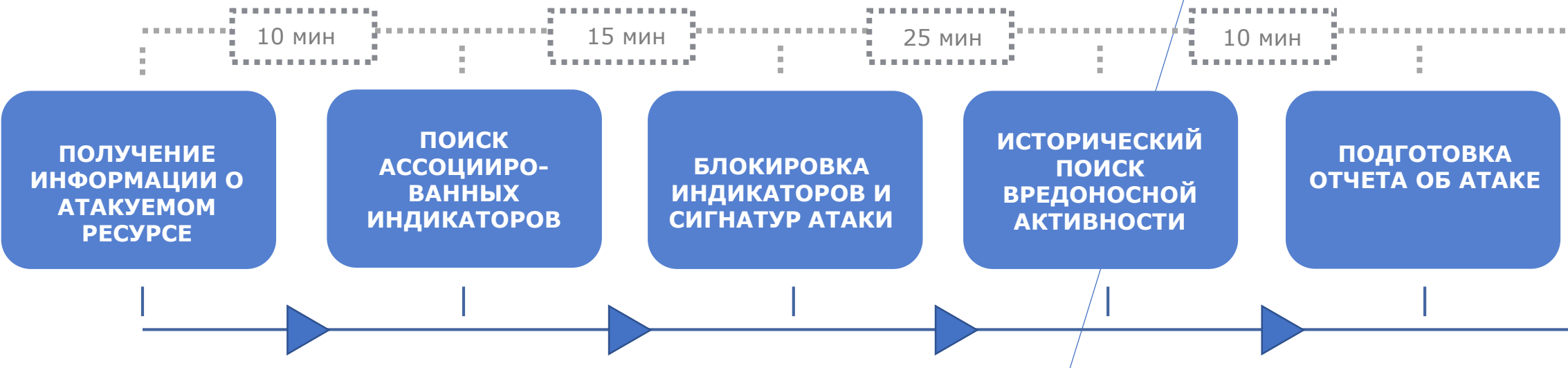


участие человека

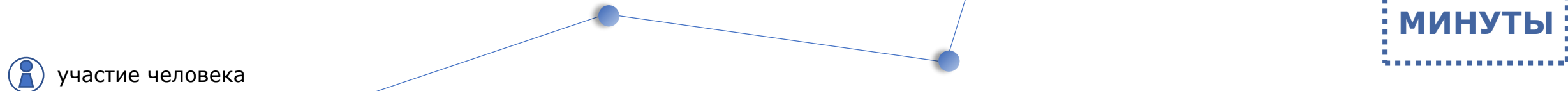
# АТАКА НА ВНЕШНИЙ САЙТ

70 МИНУТ → 5 МИНУТЫ С SOAR

ДО АВТОМАТИЗАЦИИ



ПОСЛЕ АВТОМАТИЗАЦИИ



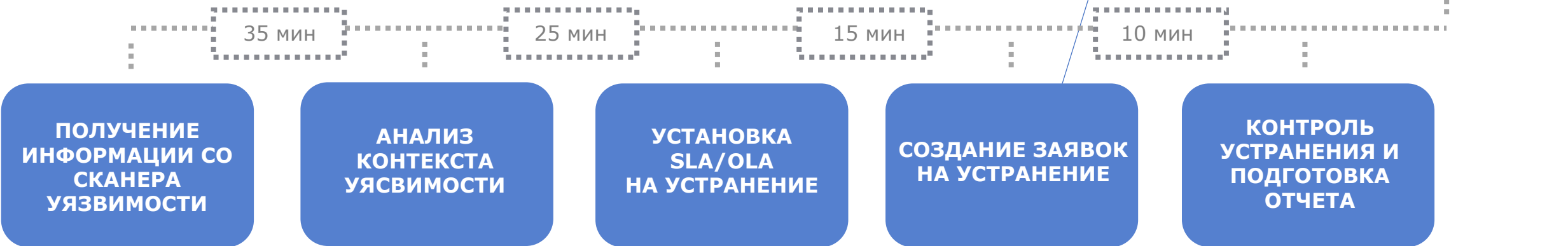
# АНАЛИЗ

## ОБНАРУЖЕННЫХ УЯЗВИМОСТЕЙ

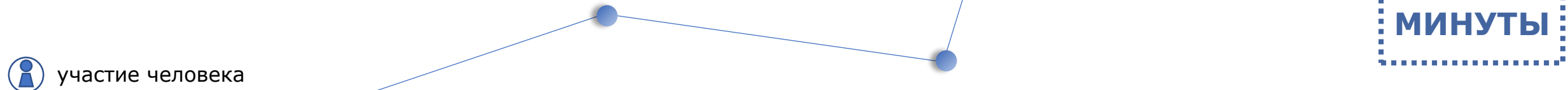
85 МИНУТ

2 МИНУТЫ С SOAR

ДО АВТОМАТИЗАЦИИ



ПОСЛЕ АВТОМАТИЗАЦИИ



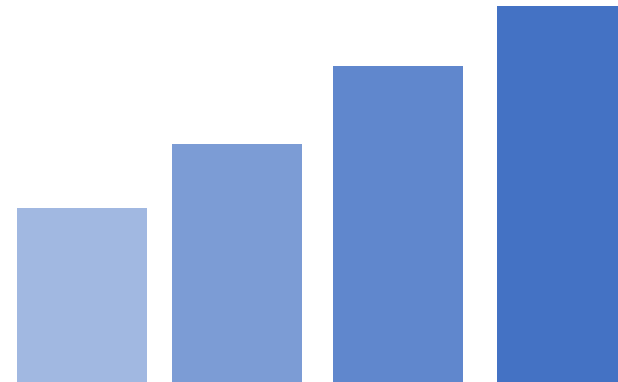
 участие человека

# МЕТРИКИ эффективности

## MEAN TIME TO

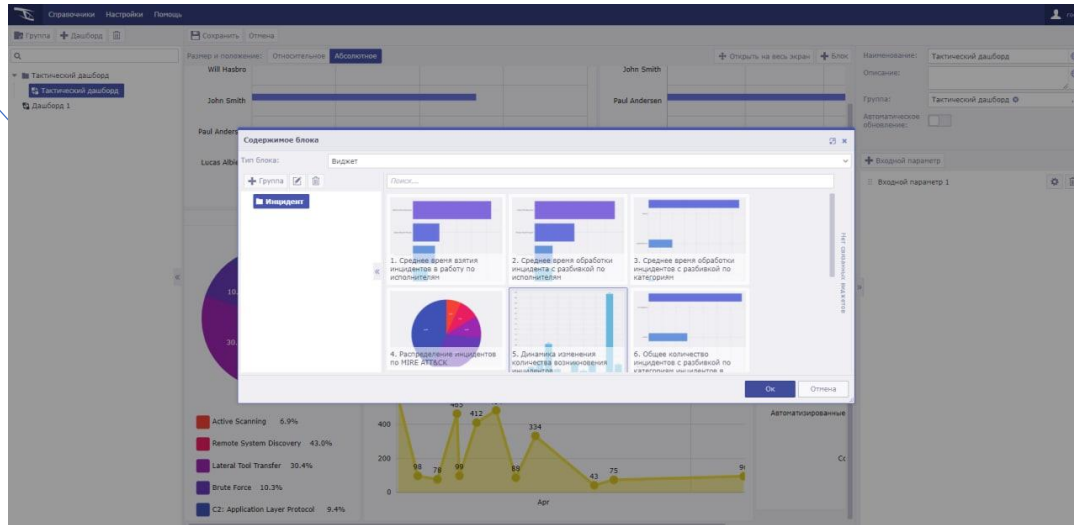
Triage  
Qualify  
Investigate  
Mitigate  
Recover  
Detect  
Response  
Acknowledge  
Contain

## ROI



# IRP (SOAR)

## SECURITY VISION



Инцидент	Создан	Исполнитель	Категория	Наименование на критическом оборудовании	Описание	Приоритет	Статус инцидента	IP-адрес источника
93	5/11/2021 5:22:06 PM	Шимкин Василий Петрович		Обнаружено новое оборудование		Low		153.237.65.78
94	5/11/2021 5:40:17 PM	Полухин Георгий Игоревич		DDOS-атака		Low		227.202.178.141
95	5/11/2021 5:40:19 PM	Говоров Петр Васильевич		Обнаружено новое оборудование		Low		227.202.178.141
96	5/11/2021 5:40:21 PM	Полухин Георгий Игоревич		Отключение питания на критическом оборудовании		Medium		105.67.253.14
97	5/11/2021 5:40:25 PM	Шимкин Василий Петрович		Обнаружено новое оборудование		Medium		153.237.65.78
123	5/25/2021 4:53:14 PM	John Smith	Persistence	Exchange PrivyLogon	Execution of a public POW to abuse Exchange vulnerabilities	High	In work	192.168.14.10
124	5/25/2021 4:55:31 PM	Andrew Pittersen	Persistence	Elevated WMI Eventing	User leveraged WMI subscriptions locally for persistence.	Medium	Closed	192.168.45.10
125	5/25/2021 4:57:12 PM	Lucas Albery	Privilege escalation	Manipulated Process DLL Injection	Injecting a malicious DLL into a process.	Medium	Closed	192.168.48.64
126	5/25/2021 4:57:54 PM	Paul Andersen	Credential Access	Malware VBScript Execute PowerShell	Leveraging mshta.exe to proxy execute malicious powershell commands via vbscript.	High	Closed	192.168.49.35
127	5/25/2021 4:58:35 PM	Will Hadbro	Credential Access	Powercat LSA Secrets Dump	Using powercat to run reg.exe as system and dump LSA secrets.	High	New	192.168.48.47
128	5/25/2021 5:00:47 PM	John Smith	Discovery	Covenant GetDomainGroup Domain Admins	User enumerated the domain groups via LDAP.	Low	Closed	192.168.10.10
129	5/25/2021 5:01:38 PM	Paul Andersen	Lateral Movement	Remote Scheduled Task Creation	User created a scheduled task remotely using schtasks.	Medium	Closed	192.168.48.65
130	5/25/2021 5:03:45 PM	Lucas Albery	Lateral Movement	Over-Pass-The-Hash	User talked a hash/key for a domain-based user into a fully-fledged malware TOT.	Low	Closed	192.168.10.10
131	5/25/2021 5:04:48 PM	Paul Andersen	Defense Evasion	Bitsadmin Download Malicious File	Leveraging bitsadmin.exe to download a file.	Low	Closed	192.168.49.64

Общая информация

Наименование: Powercat LSA Secrets Dump

Описание: Using powercat to run reg.exe as system and dump LSA secrets.

Дата и время обнаружения: 192.168.48.47

IP-адрес источника: 192.168.48.47

IP-адрес назначения: 192.168.48.47

Обработка инцидента

Исполнитель: Will Hadbro


Дата возникновения: 192.168.48.47

Статус инцидента: New

Приоритет: High

Категория: Credential Access

Статистика связанных инцидентов за неделю



Настройки Команды Конфигурация

Группа Команда Шаг

Наименование: Аутентификация

Настройка шага Результат шага

Задержка перед выполнением шага: 0 мсек

Задержка после выполнения шага: 0 мсек

Действие в случае ошибки: Остановить выполнение команды

Ограничение на выполнение шага: Не задано мсек

Условие успешности шага: Хотя бы один запрос должен выполниться успешно

Условие успешности шага, если входные параметры шага имели множественное значение и было сформировано несколько запросов на их основе

Тип запроса: POST

Вызываемый метод: /api/v1/account/login

Заголовки запроса:

Название	Значение
Authorization	Bearer MAGIC_SYSTEM_ACCESS_TOKEN

Запрос: ("login" |<login> "password" |<password>)

Тип контента: application/json

Кодировка контента: UTF-8

Параметры: Antifraud, Attachments, Impacts, Location, apiRequestId, assistance, closeDateAt, department, description, events, final\_description, fixationAt, URL, Адрес подключения, Логин, Пароль, Порт, Токен



SECURITY VISION  
УВИДЕТЬ БЕЗОПАСНОСТЬ

**СПАСИБО**

**ЗА ВНИМАНИЕ**