



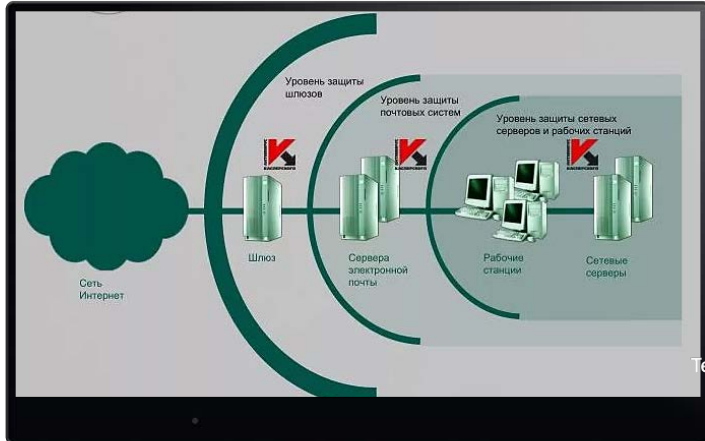
**2019**

# **CSIRT VS ЧЕЛОВЕЧЕСКИЙ ФАКТОР ИЛИ МОЖНО ЛИ БОРОТЬСЯ С СОЦИАЛЬНОЙ ИНЖЕНЕРИЕЙ**

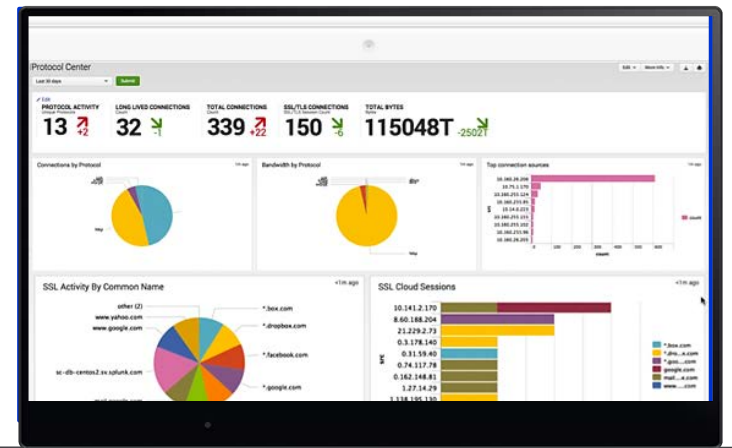
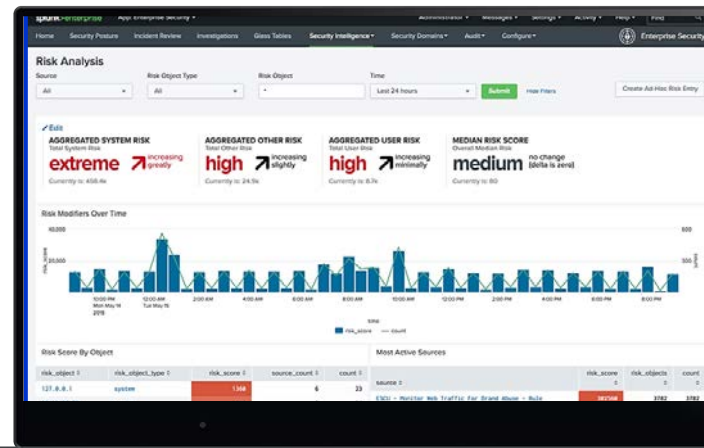
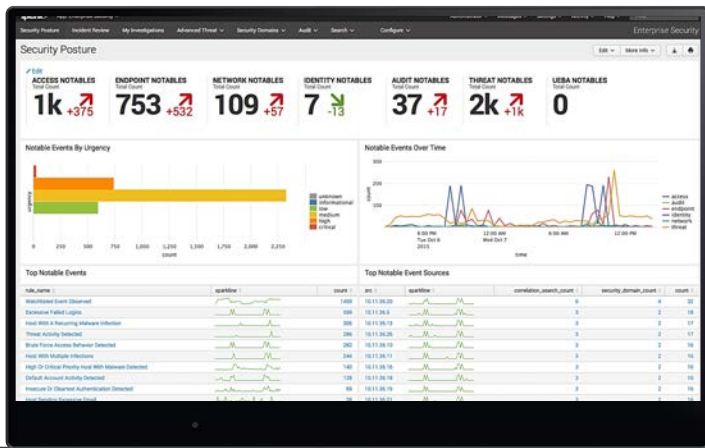
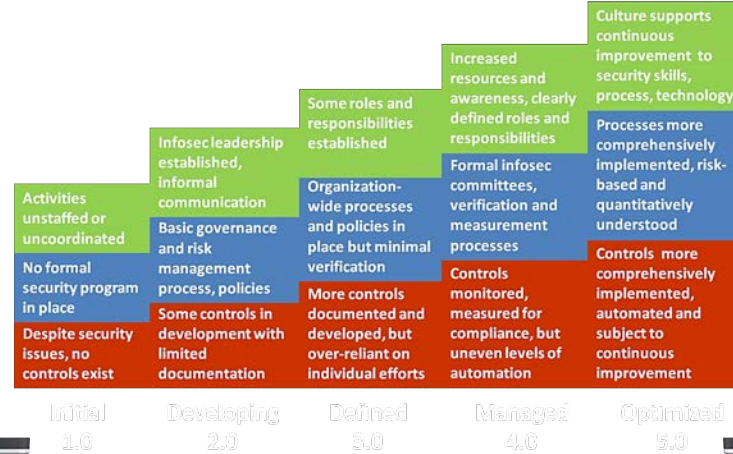
**Алексей  
Мальнев**

Руководитель Jet CSIRT  
[ay.malnev@jet.su](mailto:ay.malnev@jet.su) / +7 985 849-89-33

# ПРЕДСТАВИМ, ЧТО МЫ НЕПЛОХО ЗАЩИТИЛИСЬ



People  
Process  
Technology



# ПРЕДСТАВИМ, ЧТО МЫ НЕПЛОХО ЗАЩИТИЛИСЬ



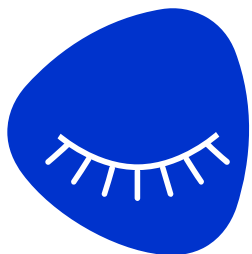
# НА САМОМ ДЕЛЕ ВСЕ НЕ ТАК ЗДОРОВО



**СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ — АТАКУЮЩИЙ МЕТОД №1**

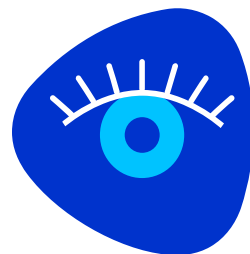
<https://www.dogana-project.eu/index.php/social-engineering-blog/11-social-engineering/94-estimates-of-social-engineering-attacks>

# ЧТО МЫ ЗНАЕМ О СОЦИНЖЕНЕРИИ?



## ЗАБЛУЖДЕНИЯ

- Социальная инженерия – это фишинг, подкинутые флэшки, обман в соцсетях, телефонное мошенничество
- Социальная инженерия – часть кибератаки
- С социальной инженерией можно столкнуться случайно
- Социальная инженерия возможна вследствие низкого уровня Security Awareness или низкого зрелости ИБ



## РЕАЛЬНОСТЬ

- Социальная инженерия – это «бесконечное» количество комбинаций технических и нетехнических техник и стратегий
- Кибератака может быть частью стратегии социальной инженерии
- Социальная инженерия – всегда таргетирована и фокусна
- Социальная инженерия всегда действует от уровня Security Awareness и зрелости ИБ

# ЧЕЛОВЕК – САМОЕ СЛАБОЕ ЗВЕНО



**«Никогда не стоит  
недооценивать  
предсказуемость  
человеческой  
глупости»**

*(с) х/ф «Большой куш»*



# СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ



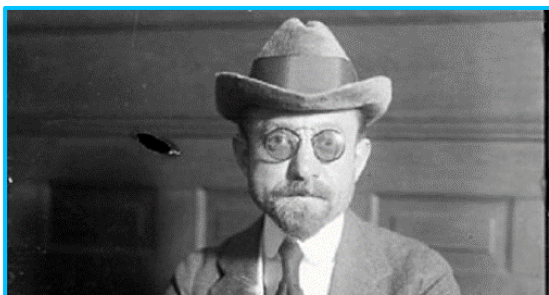
**Виктор Люстиг**



**Фрэнк Абигнейл**



**Артур Фергюсон**



**Джозеф Уэйл**



**Кевин Митник**



**Братья Бадир**

# СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. LIFECYCLE



# СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ МНОГООБРАЗИЕ ТЕХНИК

- **Техники инициации**

Естественность, осведомленность, щедрость

- **Первичная обработка**

Фоновая обработка, загрузка информации

- **Техники предложений**

Использование персональных интересов, применение диалектов, махинации с телефонами

- **Техники извлечения информации**

Апеллирование к эго, «искренний» интерес, подтасовка данных, лесть, волонтерство, игнорирование, алкоголь, техника хорошего слушателя, техники управляемых вопросов

- **Техники влияния**

Услуга за услугу, подарки, уступки, искусственный дефицит, влияние авторитетом, юридическое, социальное и организационное, симпатия, последовательный переход, подмена реальности

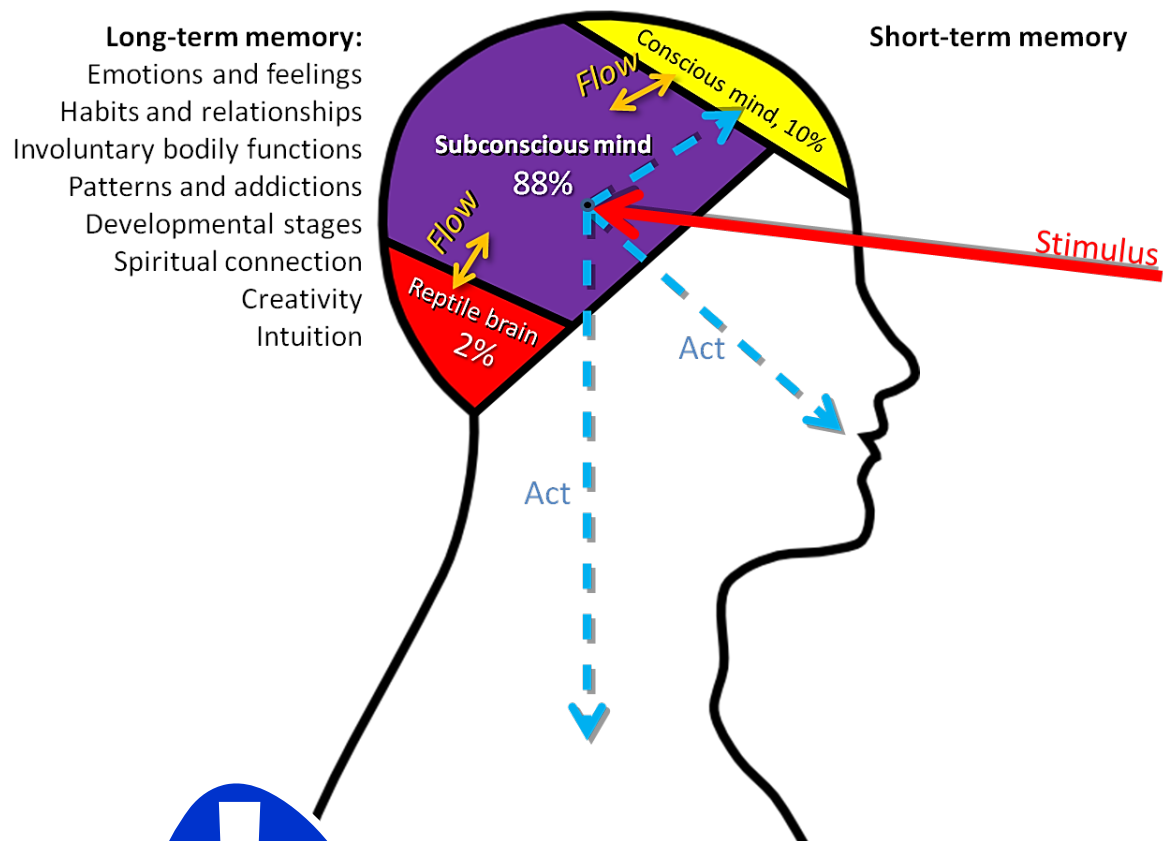
- **Обман и манипуляции**

Отвлечение, повышение предсказуемости, контроль окруж. обстановки, сомнение, слабость, наказание, шантаж, комплименты, работа по типу мышления (аудиалы-визуалы-кинестетики), работа с микроэкспрессиями (злость, отвращение, презрение, страх, удивление, печаль, радость), противоречия, колебания, фиксация изменения поведения, жесты и мимика, невербалика

- **НЛП**

Мета-моделирование, воздействия на убеждения, воздействие на восприятие, воздействие звуками, воздействие интонацией, воздействие вербальными образами, «buffer overflow»

# АТАКА НА СОЗНАНИЕ И ПОДСОЗНАНИЕ



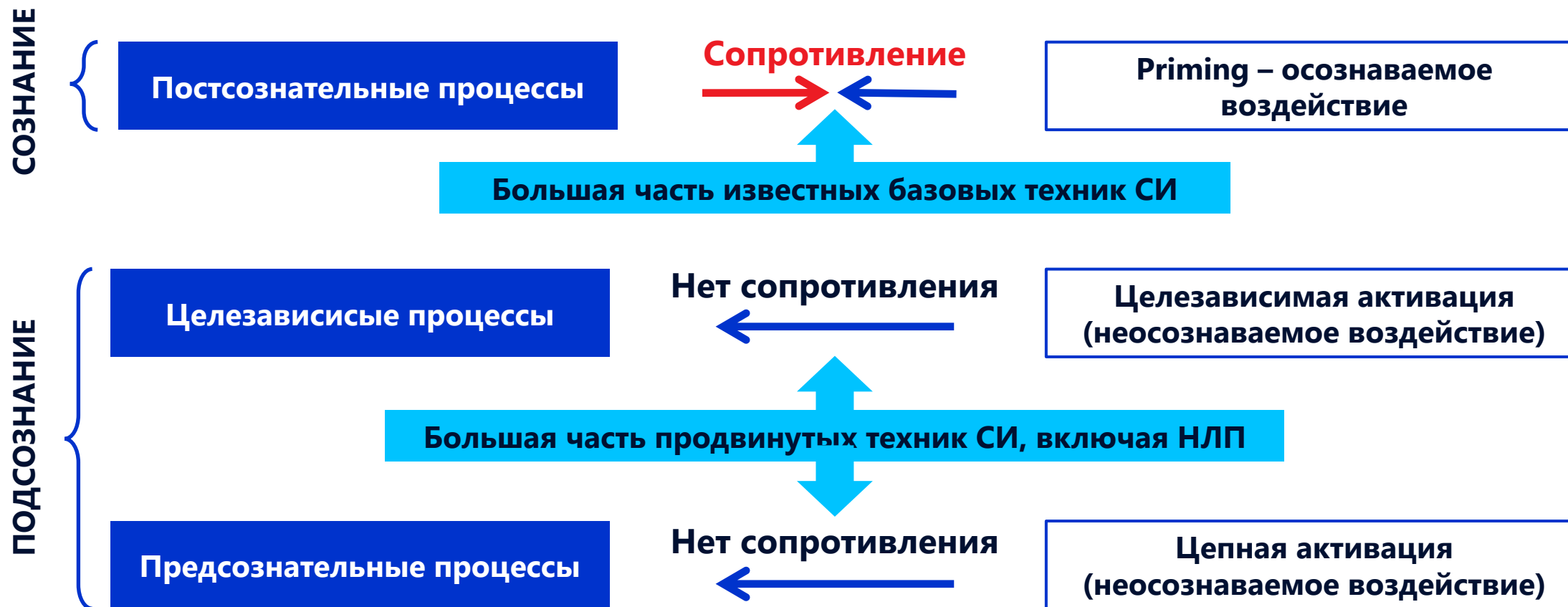
- от 95% до 99,99% вычислительной мощности мозга сосредоточены в подсознании
- Около 95% когнитивной деятельности сосредоточены в подсознании
- Сознание очень ограничено

КРИТЕРИИ	СОЗНАНИЕ	ПОДСОЗНАНИЕ
Масса мозга	17%	83%
Скорость распространения импульса	120-140 миль в час	Свыше 100000 миль в час
Бит в секунду	2000	400 миллиардов
Управление восприятием и поведением	2-4%	96-98%
Функции	Сознательные	Несознаваемые
Время	Прошое и будущее	Настоящее
Глубина памяти	До 20 секунд	Бесконечно



**СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ — АТАКУЮЩИЙ МЕТОД №1**

# ВОЗДЕЙСТВИЕ НА ПОДСОЗНАНИЕ И СОЗНАНИЕ



**СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ — АТАКУЮЩИЙ МЕТОД №1**

# «УЯЗВИМОСТИ» МОЗГА VS УЯЗВИМОСТИ ПО



## Количество состояний мозга



### Количество нейронов и количество нейронных связей

100 млрд нейронов, 100 трлн связей  
Квадриллион (1 000 000 000 000 000) байт =  
1 миллион гигабайт =  
1000 терабайт = 1 петабайт

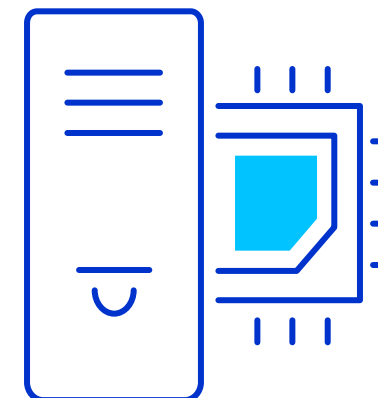
>>>

## Множество всех состояний программы



Размер кода и объема памяти данных ограничивает кол-во состояний программы и кол-во уязвимостей

## Количество состояний ПО стандартной программы на стандартном ПК



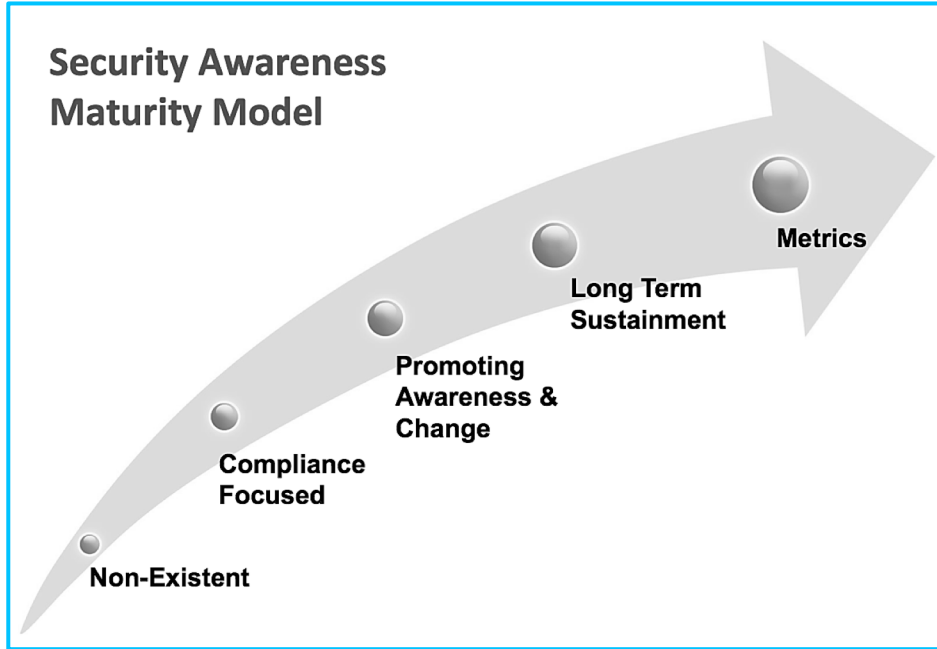
Количество памяти ограничено RAM, HDD и памяти CPU



---

# CSIRT/SOC VS СОЦИНЖЕНЕРИЯ

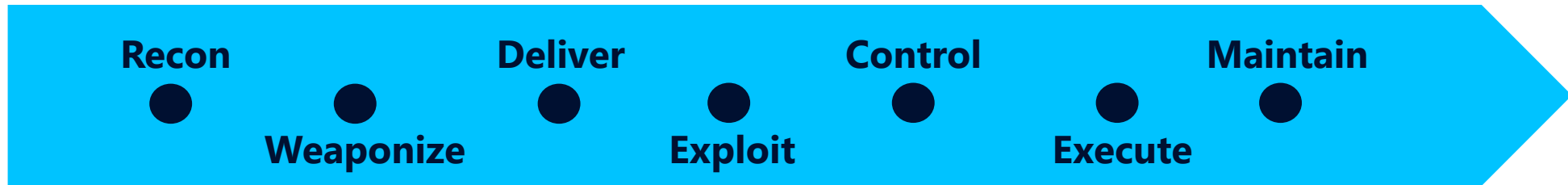
# SECURITY AWARENESS VS СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ



УРОВЕНЬ	SECURITY AWARENESS	СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ
1	Ничего нет	Базовые простейшие техники
2	Только для соответствия (формально)	Базовые простейшие техники
3	Есть программа	Базовые техники/сочетание с техническими векторами
4	Есть долгосрочный процесс, SA как часть культуры организации	Сложные техники/сочетание с техническими векторами
5	Разработаны метрики SA и они достигнуты по всей компании	Комплексные операции

<https://www.sans.org/security-awareness-training/blog/security-awareness-maturity-model>

# ATT&CK MITRE



## PRE-ATT&CK

### Priority Definition

- Planning, Direction

### Target Selection

### Information Gathering

- Technical, People, Organizational Weakness Identification
- Technical, People, Organizational

### Adversary OpSec

### Establish & Maintain Infrastructure

### Persona Development

### Build Capabilities

### Test Capabilities

### Stage Capabilities

## Enterprise ATT&CK

### Initial Access

### Execution

### Persistence

### Privilege Escalation

### Defense Evasion

### Credential Access

### Discovery

### Lateral Movement

### Collection

### Exfiltration

### Command and Control

# МАТРИЦА MITRE PRE ATT&CK



Priority Definition Planning	Priority Definition Direction	Target Selection	Technical Information Gathering	People Information Gathering	Organizational Information Gathering	Technical Weakness Identification	People Weakness Identification	Organizational Weakness Identification	Adversary OPSEC	Establish & Maintain Infrastructure	Person Development	Build Capabilities	Test Capabilities	Stage Capabilities
Assess KITs/KIQs benefits	Assign KITs, KIQs, and/or intelligence requirements	Determine approach/attack vector	Acquire OSINT data sets and information	Acquire OSINT data sets and information	Acquire OSINT data sets and information	Analyze application security posture	Analyze organizational skillssets and deficiencies	Analyze business processes	Acquire and/or use 3rd party infrastructure services	Acquire and/or use 3rd party infrastructure services	Build social network persona	Build and configure delivery systems	Review logs and residual traces	Disseminate removable media
Assess current holdings, needs, and wants	Receive KITs/KIQs and determine requirements	Determine highest level tactical element	Conduct active scanning	Aggregate individual's digital footprint	Conduct social engineering	Analyze architecture and configuration posture	Analyze social and business relationships, interests, and affiliations	Analyze organizational skillssets and deficiencies	Acquire and/or use 3rd party software services	Acquire and/or use 3rd party software services	Choose pre-compromised mobile app developer account credentials or signing keys	Build or acquire exploits	Test ability to evade automated mobile application security analysis performed by app stores	Distribute malicious software development tools
Assess leadership areas of interest	Submit KITs, KIQs, and intelligence requirements	Determine operational element	Conduct passive scanning	Conduct social engineering	Determine 3rd party infrastructure services	Analyze data collected	Assess targeting options	Analyze presence of outsourced capabilities	Acquire or compromise 3rd party signing certificates	Acquire or compromise 3rd party signing certificates	Choose pre-compromised persona and affiliated accounts	IC2 protocol development	Test callback functionality	Friend/Follow/Connect to targets of interest
Assign KITs/KIQs into categories	Task requirements	Determine secondary level tactical element	Conduct social engineering	Identify business relationships	Determine centralization of IT management	Analyze hardware/software security defensive capabilities		Assess opportunities created by business deals	Anonymity services	Buy domain name	Develop social network persona digital footprint	Compromise 3rd party or closed-source vulnerability/exploit information	Test malware in various execution environments	Hardware or software supply chain implant
Conduct cost/benefit analysis		Determine strategic target	Determine 3rd party infrastructure services	Identify groups/roles	Determine physical locations	Analyze organizational skillssets and deficiencies		Assess security posture of physical locations	Common, high volume protocols and software	Compromise 3rd party infrastructure to support delivery	Friend/Follow/Connect to targets of interest	Create custom payloads	Test malware to evade deflection	Port redirector
Create implementation plan			Determine domain and IP address space	Identify job postings and needs/gaps	Dumpster dive	Identify vulnerabilities in third-party software libraries		Assess vulnerability of 3rd party vendors	Compromise 3rd party infrastructure to support delivery	Create backup infrastructure	Obtain Apple iOS enterprise distribution key pair and certificate	Create infected removable media	Test physical access	Upload, install, and configure software/tools
Create strategic plan			Determine external network trust dependencies	Identify people of interest	Identify business processes/tempo	Research relevant vulnerabilities/CVEs			DNSCache	Domain registration hijacking		Discover new exploits and monitor exploit-provider forums	Test signature detection for file upload/email filters	
Derive intelligence requirements			Determine firmware version	Identify personnel with an authority/privilege	Identify business relationships	Research viability gap of security vendors			Data Hiding	Dynamic DNS		Identify resources required to build capabilities		
Develop KITs/KIQs			Discover target login/email address format	Identify sensitive personnel information	Identify job postings and needs/gaps	Test signature detection			Domain Generation Algorithms (DGA)	Install and configure hardware, network, and systems		Obtain/re-use payloads		
Generate analyst intelligence requirements			Enumerate client configurations	Identify supply chains	Identify supply chains				Dynamic DNS	Obfuscate infrastructure		Post compromise tool development		
Identify analyst level gaps			Enumerate externally facing software applications technologies, languages and dependencies	Mine social media	Obtain templates/branding materials				Fast Flux DNS	Obtain booter/stressor subscription		Remote access tool development		
Identify gap areas			Identify job postings and needs/gaps						Host-based hiding techniques	Procure required equipment and software				
Receive operator KITs/KIQs tasking			Identify security defensive capabilities						Misattributable credentials	SSL certificate acquisition for domain				
			Identify supply chains						Network-based hiding techniques	SSL certificate acquisition for trust breaking				
			Identify technology usage patterns						Non-traditional or less attributable payment options	Shadow DNS				
			Identify web defensive services						OS-vendor provided communication channels	Use multiple DNS infrastructures				
			Map network topology						Obfuscate infrastructure					
			Mine technical blogs/forums						Obfuscate operational infrastructure					
			Obtain domain/IP registration information						Obfuscate or encrypt code					
			Spearpishing for information						Obfuscation or cryptography					
									Private whois services					
									Proxy/protocol relays					
									Secure and protect					

Выбор цели и первичная разведка

Сбор информации

Извлечение информации

Предлог

Обман и манипуляция

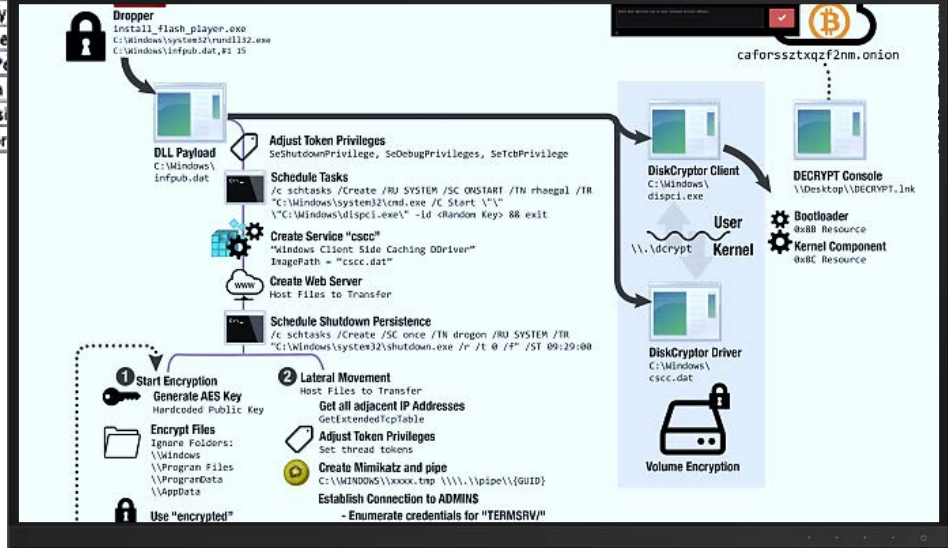
Убеждение и влияние



# ATT&CK MITRE

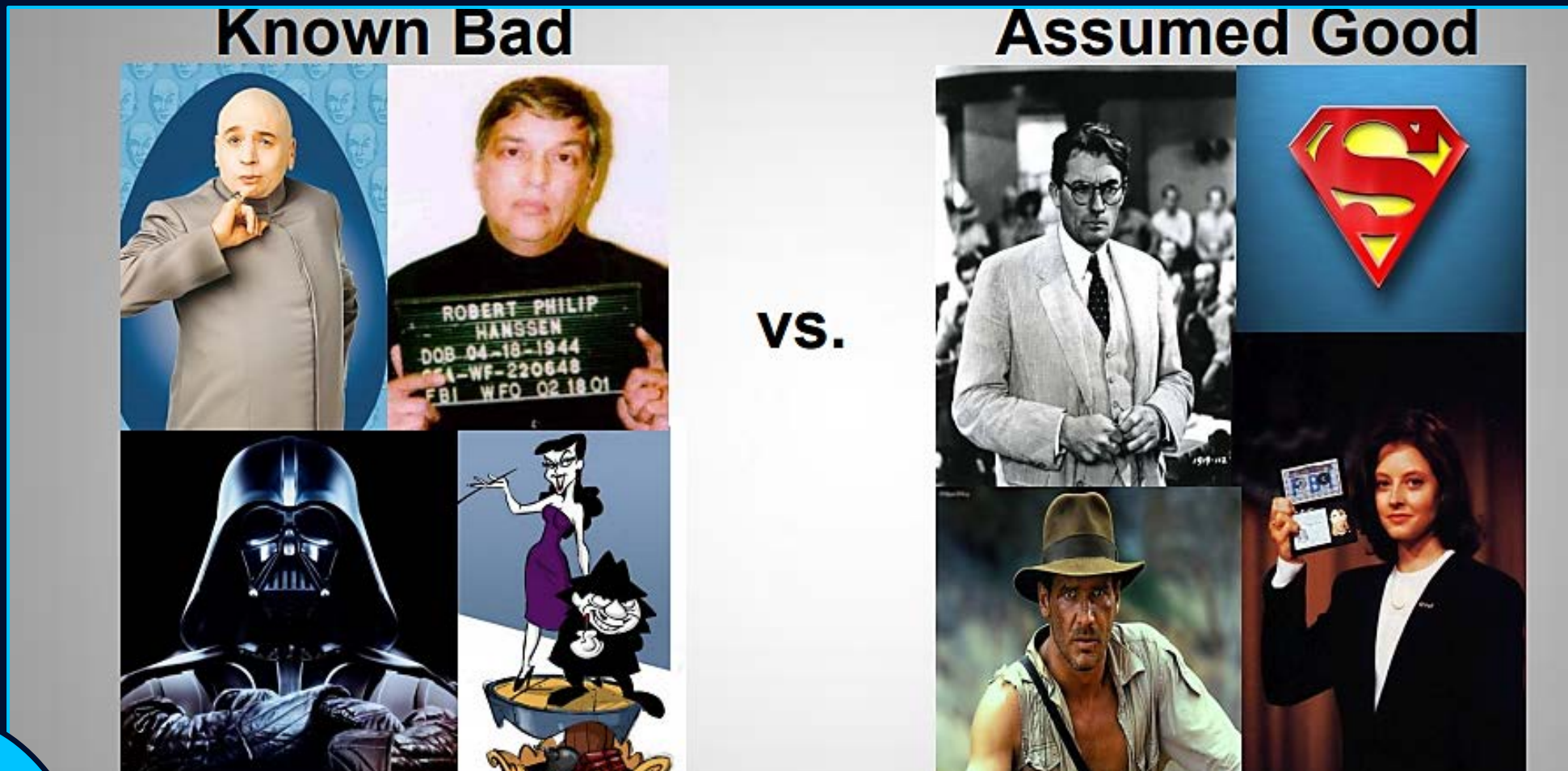


Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Hardware Additions		Scheduled Task		Binary Padding	Credentials in Registry	Browser Bookmark Discovery	Exploitation of Remote Services	Data from Information Repositories	Exfiltration Over Physical Medium	Remote Access Tools
Trusted Relationship	LSASS Driver		Extra Window Memory Injection		Exploitation for Credential Access	Network Share Discovery	Distributed Component Object Model	Video Capture	Exfiltration Over Command and Control Channel	Multi-hop Proxy
Supply Chain Compromise	Local Job Scheduling		Access Token Manipulation		Forced Authentication	Peripheral Device Discovery	Remote File Copy	Audio Capture	Exfiltration Over Command and Control Channel	Domain Fronting
Spearphishing Attachment	Trap	Launchers	Bypass User Account Control		Hooking	File and Directory Discovery	Pass the Ticket	Automated Collection	Data Encrypted	Remote File Copy
Exploit Public-Facing Application	Spoofed Binary Proxy Execution		Image File Execution Options Injection		Password Filter DLL	Permission Groups Discovery	Replication Through Removable Media	Email Collection	Automated Exfiltration	Multi-Stage Channels
Replication Through Removable Media	User Execution		Plist Modification		LLMNR/NBT-NS Poisoning	System Network Connections Discovery	Windows Admin Shares	Screen Capture	Exfiltration Over Other Network Medium	Web Service
Spearphishing via Service	Exploitation for Client Execution		Valid Accounts		Private Keys	System Owner/User Discovery	Pass the Hash	Data Staged	Exfiltration Over Alternative Protocol	Standard Application Layer Protocol
Spearphishing Link	CMSTP	Appoert DLLs	DLL Search Order Hijacking	Signed Script Proxy Execution	Keychain	System Network Configuration Discovery	Third-party Software	Input Capture	Data Transfer Size Limits	Connection Proxy
Drive-by Compromise	Dynamic Data Exchange	Startup Items	Hooking	DCShadow	Input Prompt		Shared Webroot	Shared Drive	Data Compressed	Multilayer Encryption
Valid Accounts	Mshta	Launch Daemons	Port Knocking	Port Knocking	Bash History		Logon Scripts	Data from Local System	Scheduled Transfer	Standard Application Layer Protocol
	AppleScript	Dylib Hijacking	Indirect Command Execution	Indirect Command Execution	Two-Factor Authentication Interception		Windows Remote Management	Man in the Browser		Commonly Used Port
	Source	Application Shimming	BITS Jobs	Control Panel Items	Replication Through Removable Media		Application Deployment Software	Data from Removable Media		Standard Cryptographic Protocol



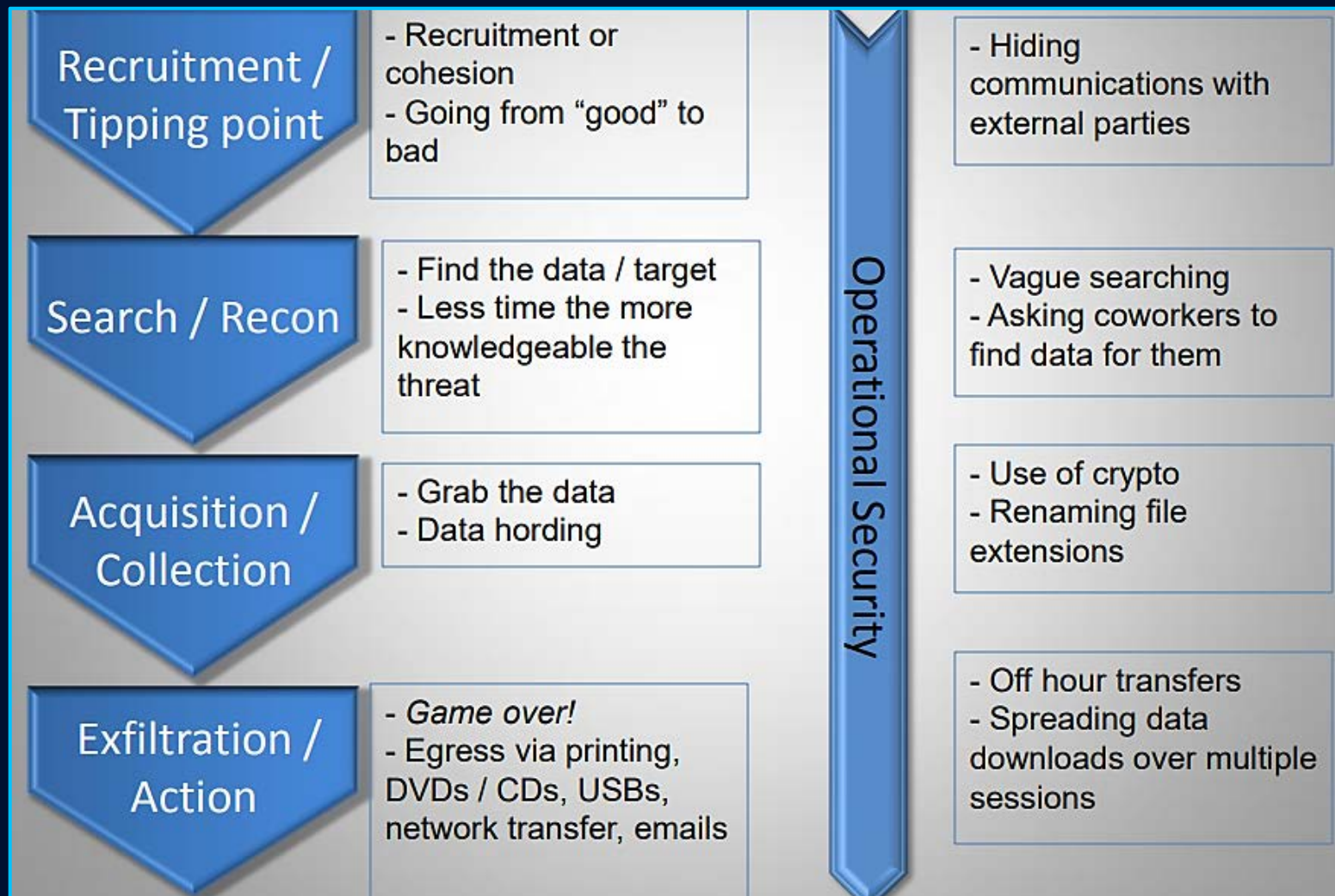
MITRE

# А ЕСЛИ ИСХОДНЫЙ ВЕКТОР SE НЕ ТЕХНИЧЕСКИЙ?



Имеем дело с осознанным или неосознанным Insider Threat Agent

# KILL CHAIN ДЛЯ INSIDER





---

**В ЧЕМ СУТЬ ПОДХОДА**

# ЛОГИКА АТАКУЮЩЕЙ СТОРОНЫ



Зрелость атакуемой системы ИБ	Ad-Hoc	Maturing	Strategic
Используемые векторы атак	Нетехнические 	Нетехнические 	Нетехнические 
	Технические и нетехнические 	Технические и нетехнические 	Технические и нетехнические 
	Технические 	Технические 	Технические 



# РИСК ЗЛОУМЫШЛЕННИКА ОПРЕДЕЛЯЕТСЯ ЦЕЛЬЮ



**Деньги**



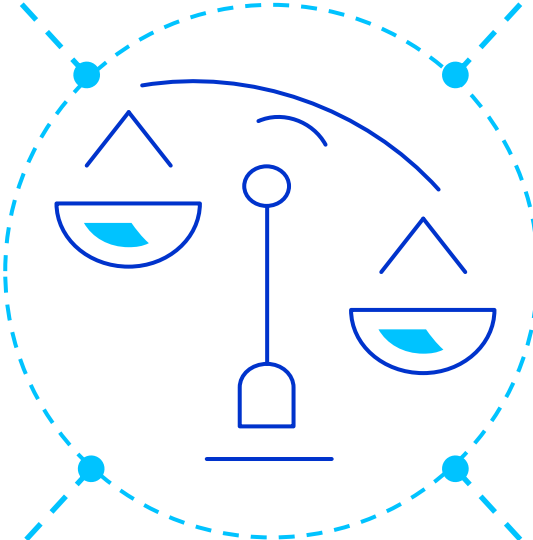
**Дестабилизация**



**Шпионаж**



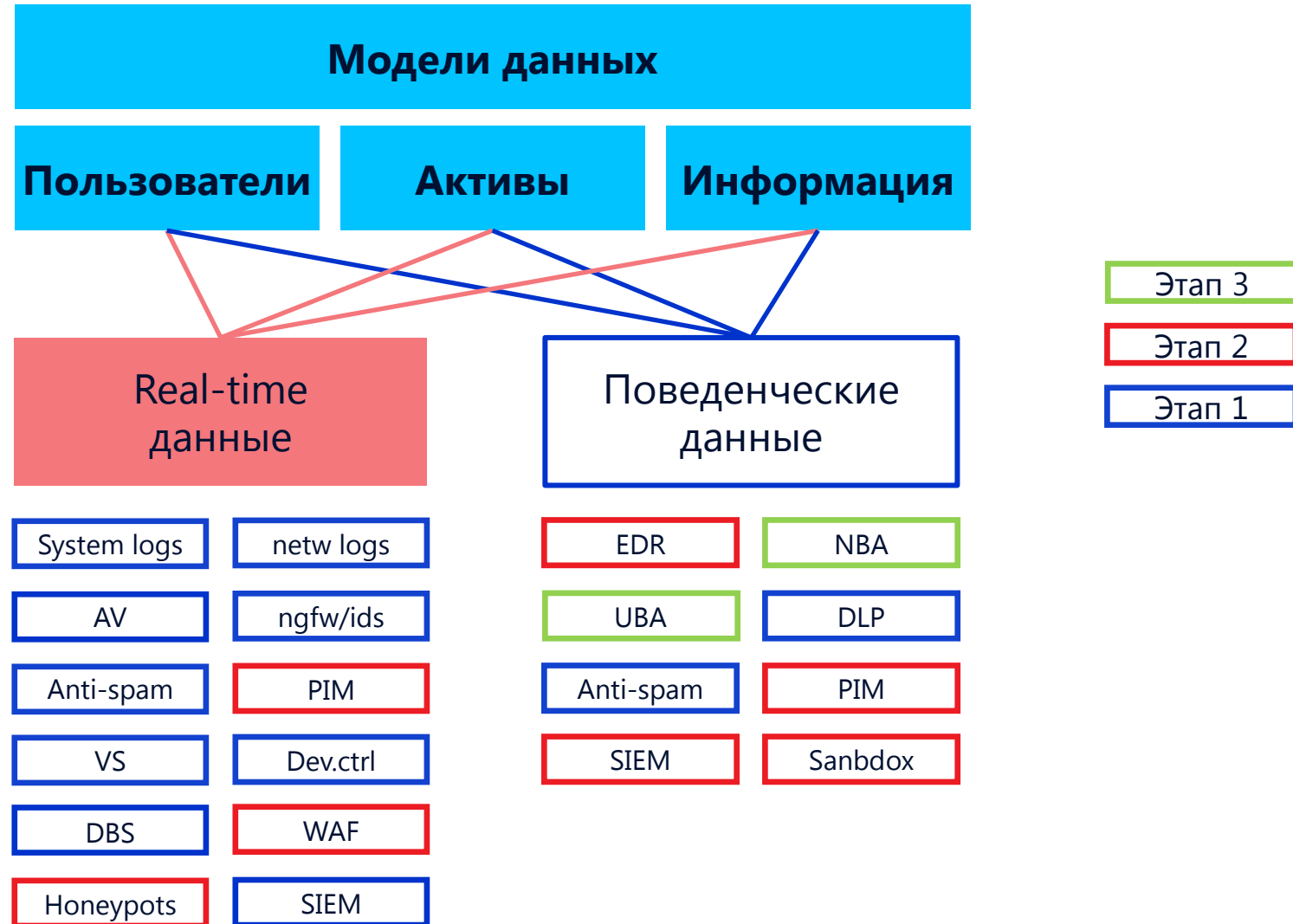
**Пром.авария**



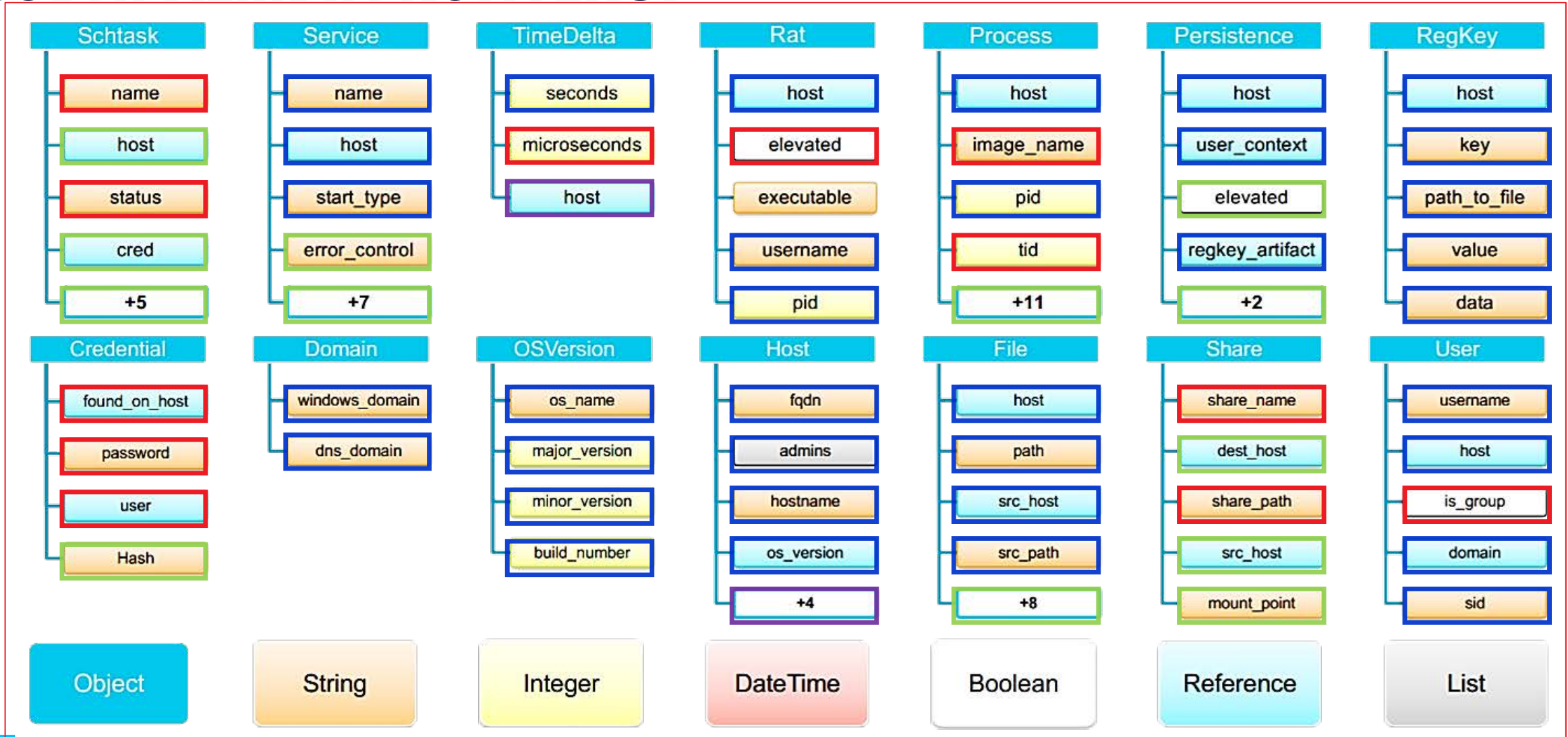
# ПОВЫШЕНИЕ ЗРЕЛОСТИ CSIRT/SOC



# ПРИМЕР. ИСТОЧНИКИ СОБЫТИЙ



# ПРИМЕР. МОДЕЛЬ АКТИВОВ. СОБИРАЕМЫЙ КОНТЕКСТ



# ПОВЫШЕНИЕ ЗРЕЛОСТИ МОНИТОРИНГА ИНЦИДЕНТОВ

## Следующий уровень зрелости



# ДОПОЛНИТЕЛЬНЫЙ ФОКУС НА МАРКЕРАХ СОЦИНЖЕНЕРИИ

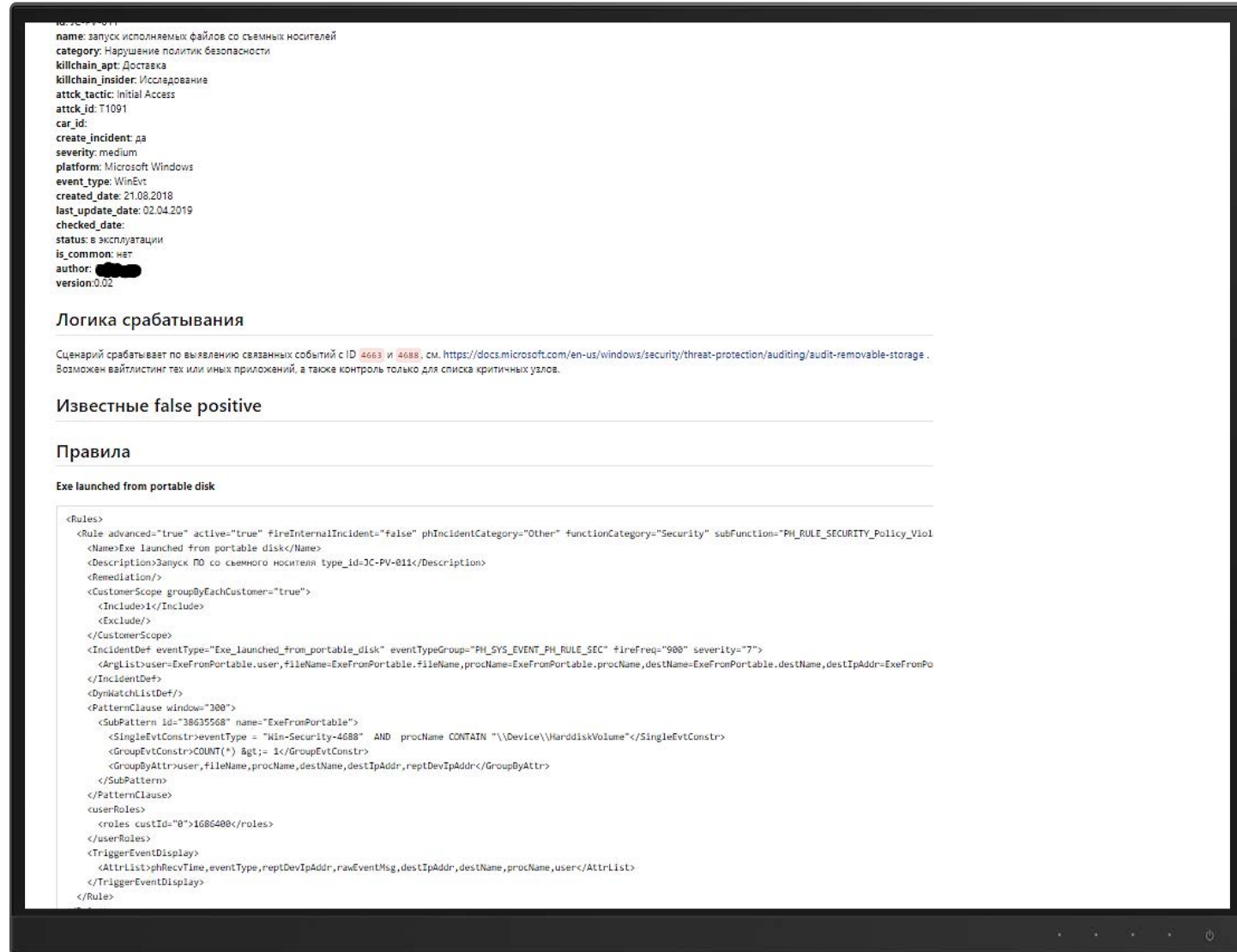
## Технические вектора SE:

- Phishing
- Watering Hole
- Typesquoting
- Whaling Attack
- Baiting
- Piggybacking
- SMiShing



## Нетехнические вектора SE:

- DLP правила
- UBA правила
- TBA правила
- EDR правила
- MDM правила



name: запуск исполняемых файлов со съемных носителей  
category: Нарушение политик безопасности  
killchain\_apr: Доставка  
killchain\_insider: Исследования  
attck\_tactic: Initial Access  
attck\_id: T1091  
car\_id:  
create\_incident: да  
severity: medium  
platform: Microsoft Windows  
event\_type: WinEvt  
created\_date: 21.08.2018  
last\_update\_date: 02.04.2019  
checked\_date:  
status: в эксплуатации  
is\_common: нет  
author: ██████████  
version: 0.02

### Логика срабатывания

Сценарий срабатывает по выделению связанных событий с ID 4663 и 4688, см. <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-removable-storage>. Возможен вайтлистинг тех или иных приложений, а также контроль только для списка критичных узлов.

### Известные false positive

### Правила

Exe launched from portable disk

```
<Rules>
<Rule advanced="true" active="true" #fireInternalIncident="false" phIncidentCategory="Other" functionCategory="Security" subFunction="PH_RULE_SECURITY_Policy_Viol
<Name>Exe launched from portable disk</Name>
<Description>Запуск ПО со съемного носителя type_id=3C-PV-811</Description>
<Remediation/>
<CustomerScope groupByEachCustomer="true">
<Include>1</Include>
<Exclude/>
</CustomerScope>
<IncidentDef eventType="Exe_launched_from_portable_disk" eventTypeGroup="PH_SYS_EVENT_PH_RULE_SEC" #fireFreq="900" severity="7">
<ArgList>user=ExeFromPortable.user, fileName=ExeFromPortable.fileName, procName=ExeFromPortable.procName, destName=ExeFromPortable.destName, destIpAddr=ExeFromPor
</IncidentDef>
<DynMatchListDef>
<PatternClause window="300">
<SubPattern id="3B635568" name="ExeFromPortable">
<SingleEvtConstr>eventType = "Win-Security-4688" AND procName CONTAIN "\\Device\\HarddiskVolume"</SingleEvtConstr>
<GroupEvtConstr>COUNT(*) &gt;= 1</GroupEvtConstr>
<GroupByAttr>user, fileName, procName, destName, destIpAddr, reptDevIpAddr</GroupByAttr>
</SubPattern>
</PatternClause>
</userRoles>
<roles custId="0">1686400</roles>
</userRoles>
<TriggerEventDisplay>
<AttrList>#hrefcTime, eventType, reptDevIpAddr, rawEventMsg, destIpAddr, destName, procName, user</AttrList>
</TriggerEventDisplay>
</Rule>
```

# СЦЕНАРИИ ДЕТЕКТИРОВАНИЯ ТЕХНИЧЕСКИХ ВЕКТОРОВ SE



ТИП СЦЕНАРИЯ	PHISHING	WATERING HOLE	TYPESQUOTING	WHALING ATTACK	BAITING	PIGGYBACKING	SMISHING
Стадии атаки 1: Первичное воздействие	<b>SecAwareness</b> - NGWF (Cisco + AMP, Checkpoint + Sandbox, Fortigate + Sandbox), - TI IoC event - Cisco Email Sec App, FortiMail, Kaspersky AS event	<b>SecAwareness</b> - NGWF (Cisco + AMP, Checkpoint + Sandbox, Fortigate + Sandbox), - TI IoC event - McAfee Web GW, Cisco Web Sec Appliance, Bluecoat ProxySG, NGFW	<b>SecAwareness</b> NGFW + TI IoC event, - Cisco Email Sec App, FortiMail, Kaspersky AS event	<b>SecAwareness</b> NGWF (Cisco + AMP, Checkpoint + Sandbox, Fortigate + Sandbox), - TI IoC event - Cisco Email Sec App, FortiMail, Kaspersky AS event	<b>SecAwareness</b> - MS event 4663 4668 - Kaspersky KES, Lumention DC, Zecurion DLP	<b>SecAwareness</b> - PACS event	<b>SecAwareness</b> MobileIron event + Zimperium MTD event Airwatch Event + Zimperium MTD, Blackberry UEM Event
Стадии атаки 2: Реакция атакуемого	- McAfee Web GW, Cisco Web Sec Appliance, Bluecoat ProxySG, - NGFW + TI events - Kaspersky KEDR/CB EDR	- McAfee Web GW, Cisco Web Sec Appliance, Bluecoat ProxySG, - NGFW + TI events - Kaspersky KEDR/CB EDR	- Cisco Umbrella Infoblox, F5 Big-IP DNS - McAfee Web GW, Cisco Web Sec Appliance, Bluecot ProxySG, NGFW - Kaspersky KEDR/CB EDR	- McAfee Web GW, Cisco Web Sec Appliance, Bluecoat ProxySG, - NGFW + TI events - Kaspersky KEDR/CB EDR	- Kaspersky KEDR/CB EDR	- MS event 4624 (logon type 2 event) + PACS event	- MobileIron event + Zimperium MTD event Airwatch Event + Zimperium MTD, Blackberry UEM Event

# СЦЕНАРИИ ДЕТЕКТИРОВАНИЯ НЕТЕХНИЧЕСКИХ ВЕКТОРОВ SE




ТИП СЦЕНАРИЯ	ОБМАН	МАНИПУЛЯЦИИ	ШАНТАЖ	УГРОЗЫ	УБЕЖДЕНИЕ	ЛЮБОПЫТСТВО	НЛП
Первичный вектор (детектирование атакующего)	<b>SecAwareness</b>	<b>SecAwareness</b>	<b>SecAwareness</b>	<b>SecAwareness</b>	<b>SecAwareness</b>	<b>SecAwareness</b>	<b>SecAwareness</b> (мало эффективно)
Вторичный вектор (детектирование атакуемого)	DLP events (Solar Dozor, Infowatch TM, Symantec DLP, Zecurion DLP, McAfee DLP) UBA events (MF Interset, Splunk UBA, IBM Qradar, Exabeam UEBA) TBA events (Cisco Threat Defense, Netscout-Arbor Peakflow) EDR events (Kaspersky KEDR, Carbon Black Response, Checkpoint Sandblast Agent, Trend Micro Apex One) MDM events (MobileIron, Airwatch + Zimperium MTD, Blackberry UEM) UAM events (Falcongaze, Searchinform, Veriato-Spectorsoft) Threat Hunting						

# ДОПОЛНИТЕЛЬНЫЙ ФОКУС НА МАРКЕРАХ СОЦИНЖЕНЕРИИ



## Social Engineering Red Flags



**FROM**

- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- I **don't know the sender personally** and they **were not vouched for** by someone I trust.
- I **don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

**TO**

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

**HYPERLINKS**

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big red flag**.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, [www.bankofamerica.com](http://www.bankofamerica.com) — the "m" is really two characters — "r" and "n."

**DATE**

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

**SUBJECT**

- Did I get an email with a subject line that is **irrelevant or does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?

**ATTACHMENTS**

- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt file**.

**CONTENT**

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar or spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd or illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

© 2017 KnowBe4, LLC. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

KnowBe4  
Human error. Conquered.



**2019**

**СПАСИБО ЗА ВНИМАНИЕ!**

**Алексей  
Мальнев**

Руководитель Jet CSIRT  
[ay.malnev@jet.su](mailto:ay.malnev@jet.su) / +7 985 849-89-33