



CSIRT VS человеческий фактор или можно ли бороться с социальной инженерией

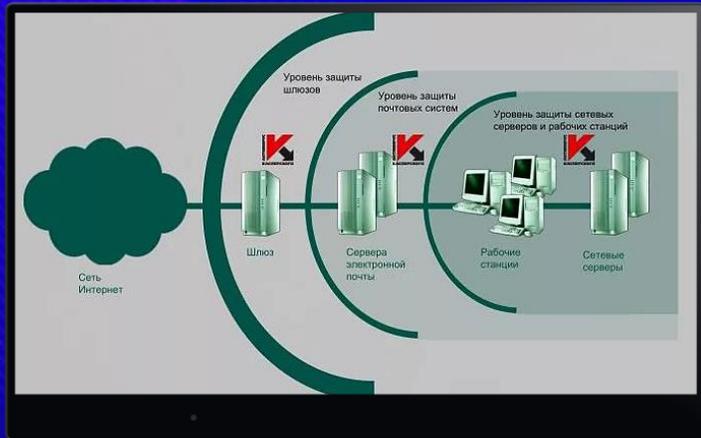
Алексей Мальнев

Руководитель Jet CSIRT

au.malnev@jet.su / +7 985 849-89-33



ПРЕДСТАВИМ, ЧТО МЫ НЕПЛОХО ЗАЩИТИЛИСЬ

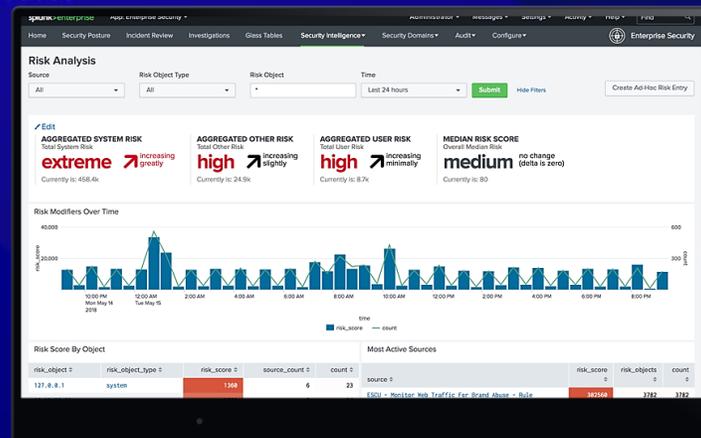
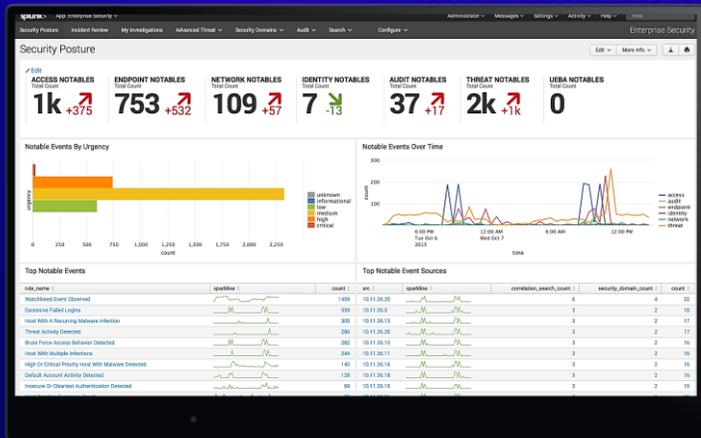


People

Process

Technology

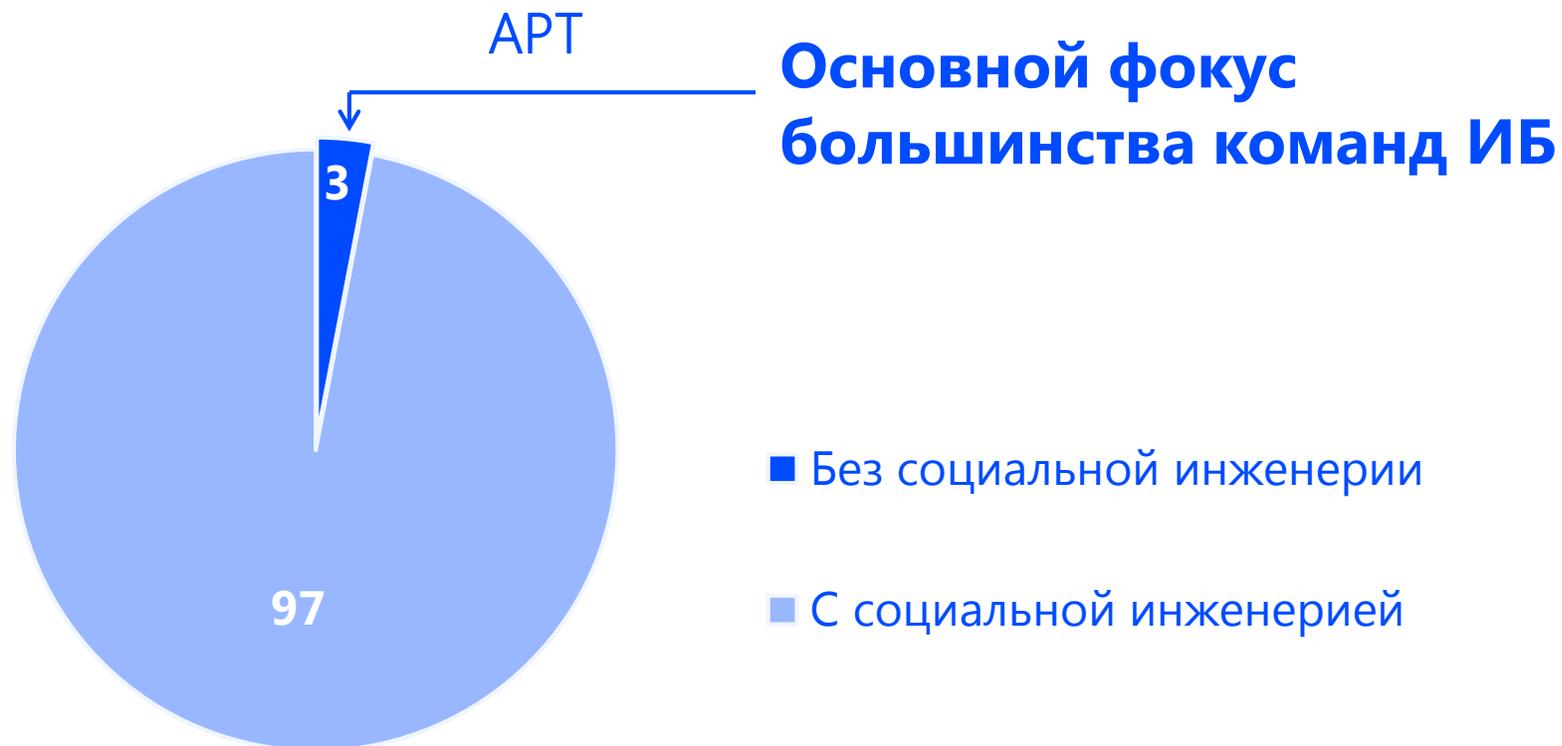
Initial 1.0	Developing 2.0	Defined 3.0	Managed 4.0	Optimized 5.0
Activities unstaffed or uncoordinated	Infosec leadership established, informal communication	Some roles and responsibilities established	Increased resources and awareness, clearly defined roles and responsibilities	Culture supports continuous improvement to security skills, process, technology
No formal security program in place	Basic governance and risk management process, policies	Organization-wide processes and policies in place but minimal verification	Formal infosec committees, verification and measurement processes	Processes more comprehensively implemented, risk-based and quantitatively understood
Despite security issues, no controls exist	Some controls in development with limited documentation	More controls documented and developed, but over-reliant on individual efforts	Controls monitored, measured for compliance, but uneven levels of automation	Controls more comprehensively implemented, automated and subject to continuous improvement



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

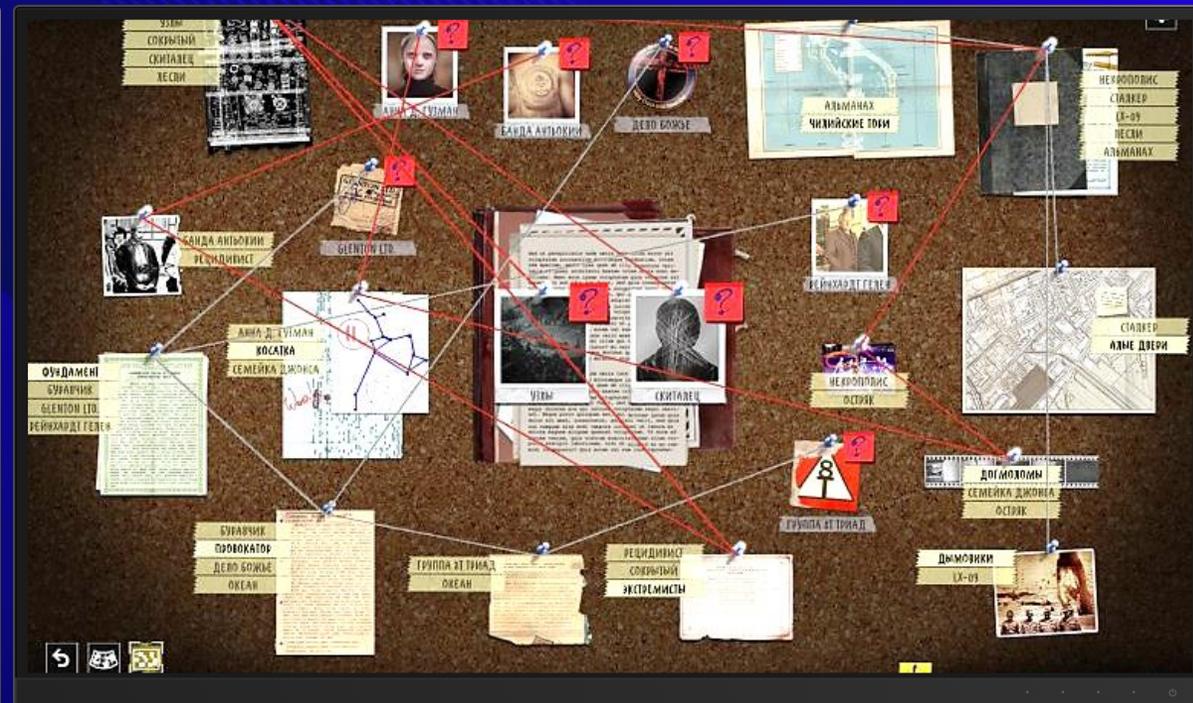
- Социальная инженерия – это «бесконечное» количество комбинаций технических и нетехнических техник и стратегий
- Кибератака может быть частью стратегии социальной инженерии
- Социальная инженерия – всегда таргетирована и фокусна
- Социальная инженерия всегда действует от уровня Security Awareness и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

ЧЕЛОВЕК – САМОЕ СЛАБОЕ ЗВЕНО



**«Никогда не стоит недооценивать предсказуемость человеческой глупости»
(с) х/ф «Большой куш»**

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ



СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ



Виктор Люстиг



Фрэнк Абигнейл



Артур Фергюсон



Джозеф Уэйл



Кевин Митник



Братья Бадир

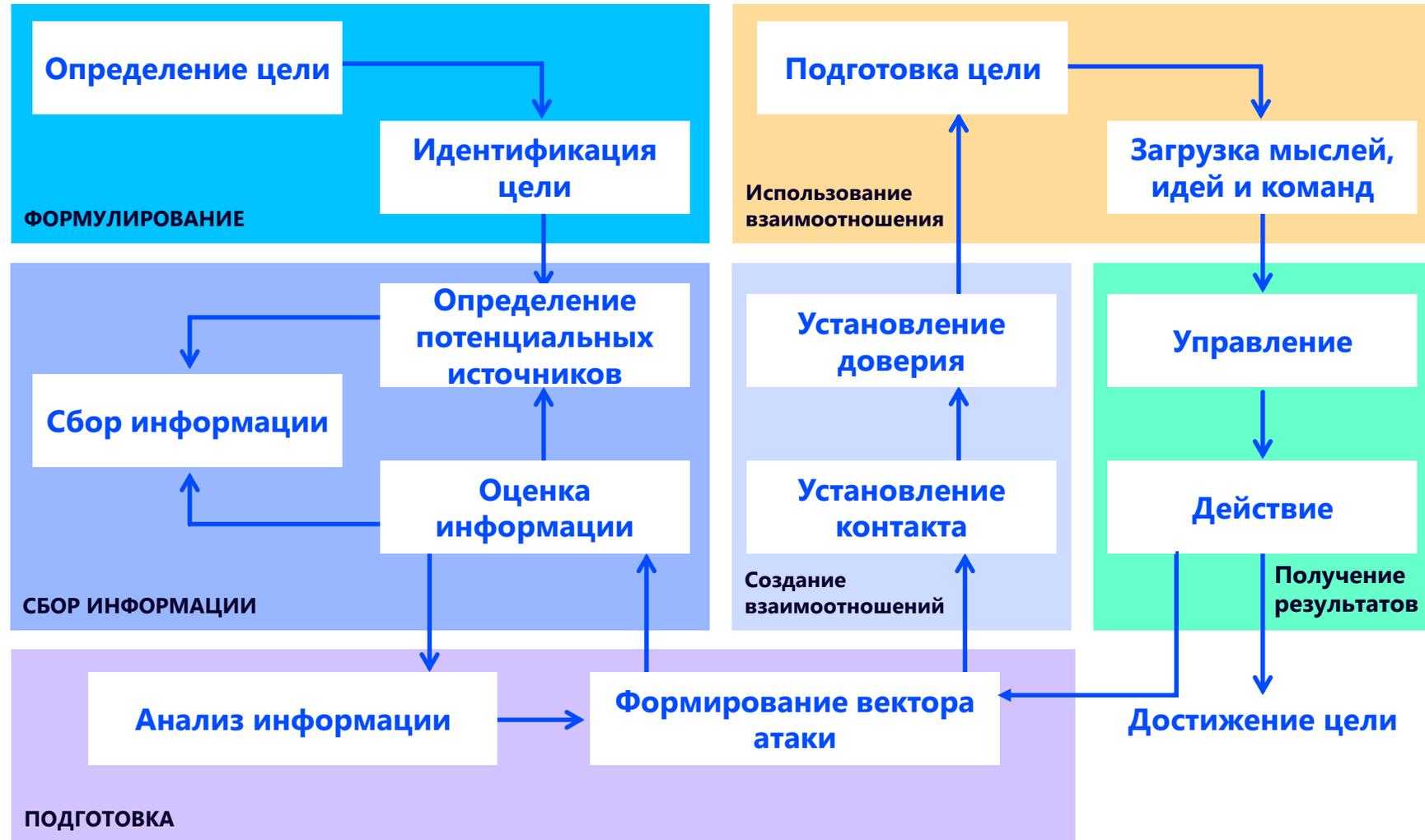
СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. LIFECYCLE





СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. FRAMEWORK

Social engineering roadmap





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

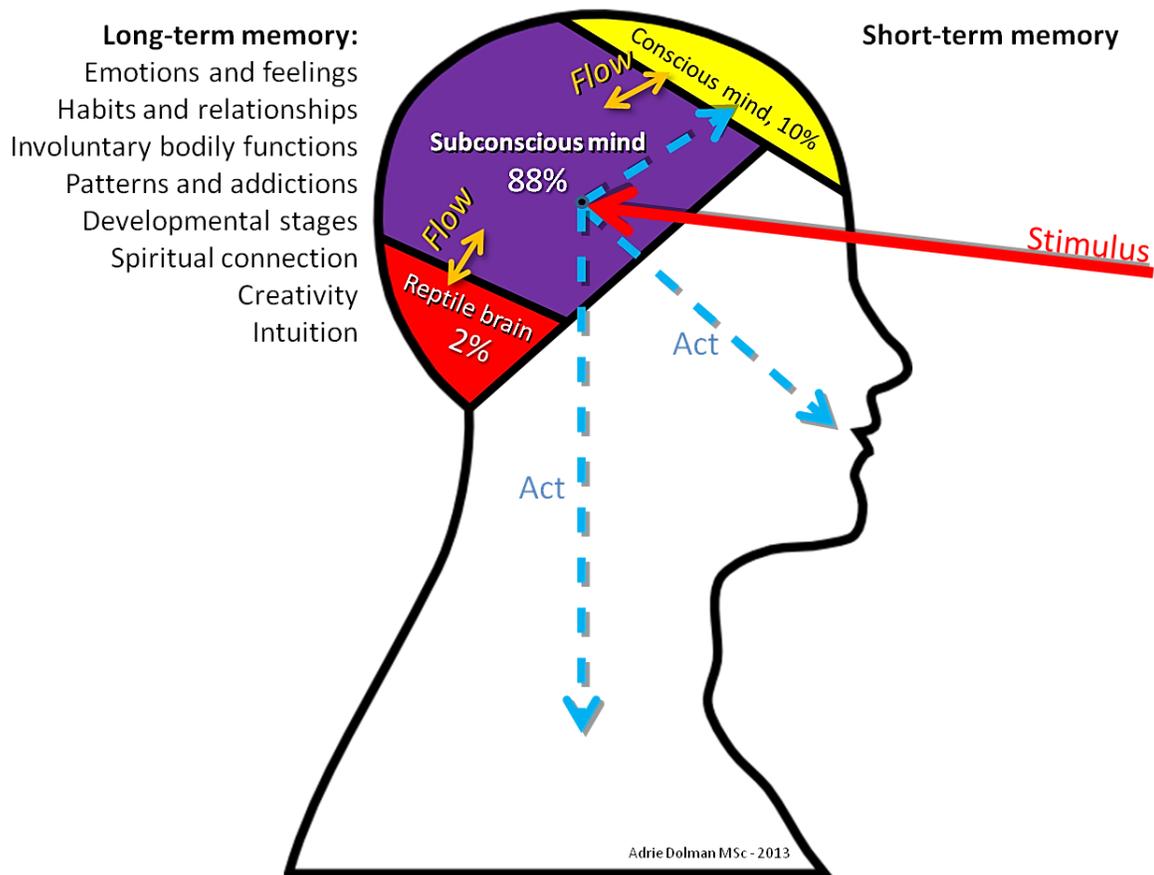
Обман и манипуляции

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

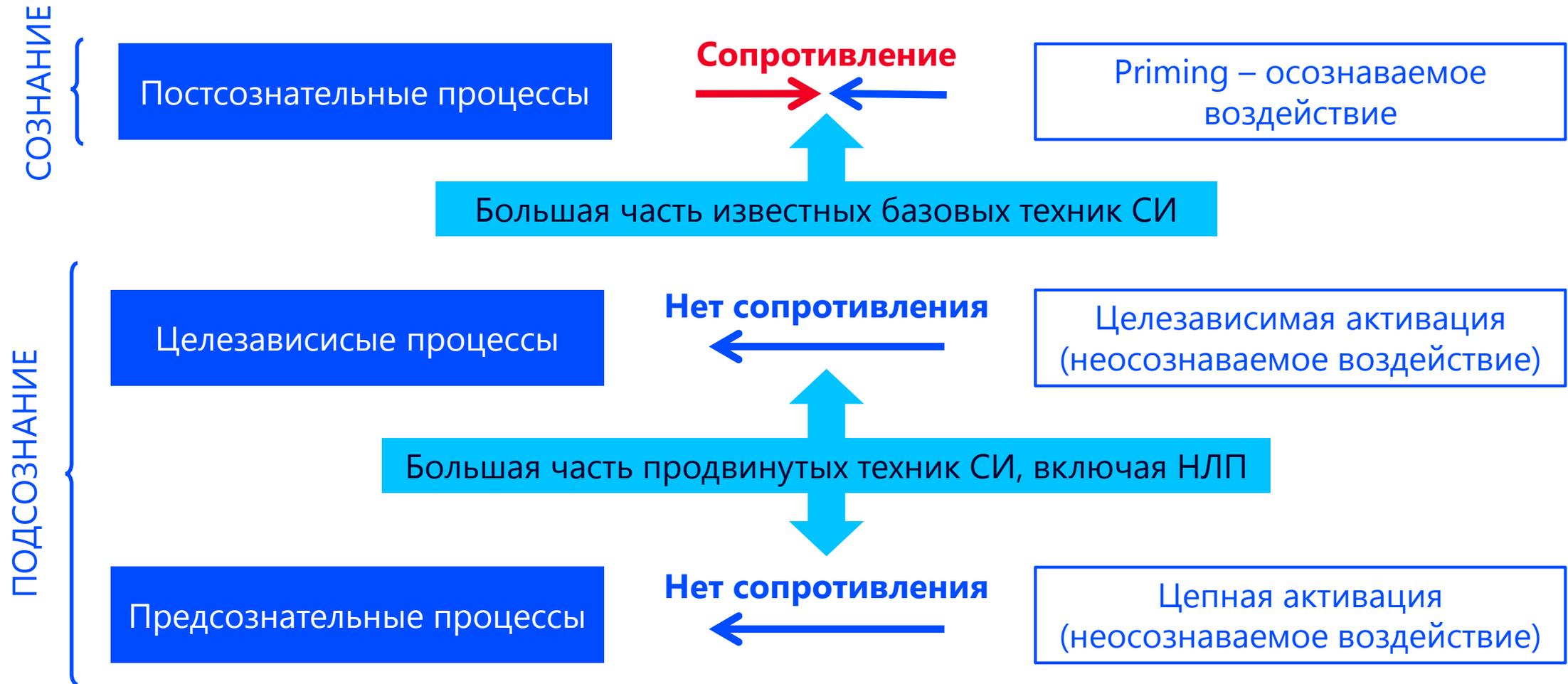


- от 95% до 99,99% вычислительной мощности мозга сосредоточены в подсознании
- Около 95% когнитивной деятельности сосредоточены в подсознании
- Сознание очень ограничено

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

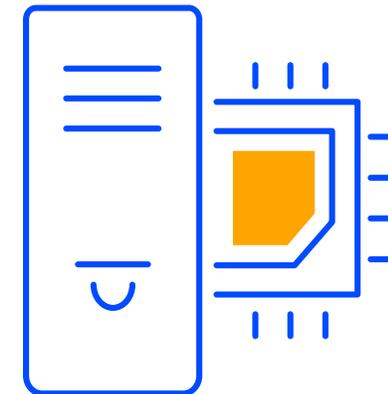
>>>

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



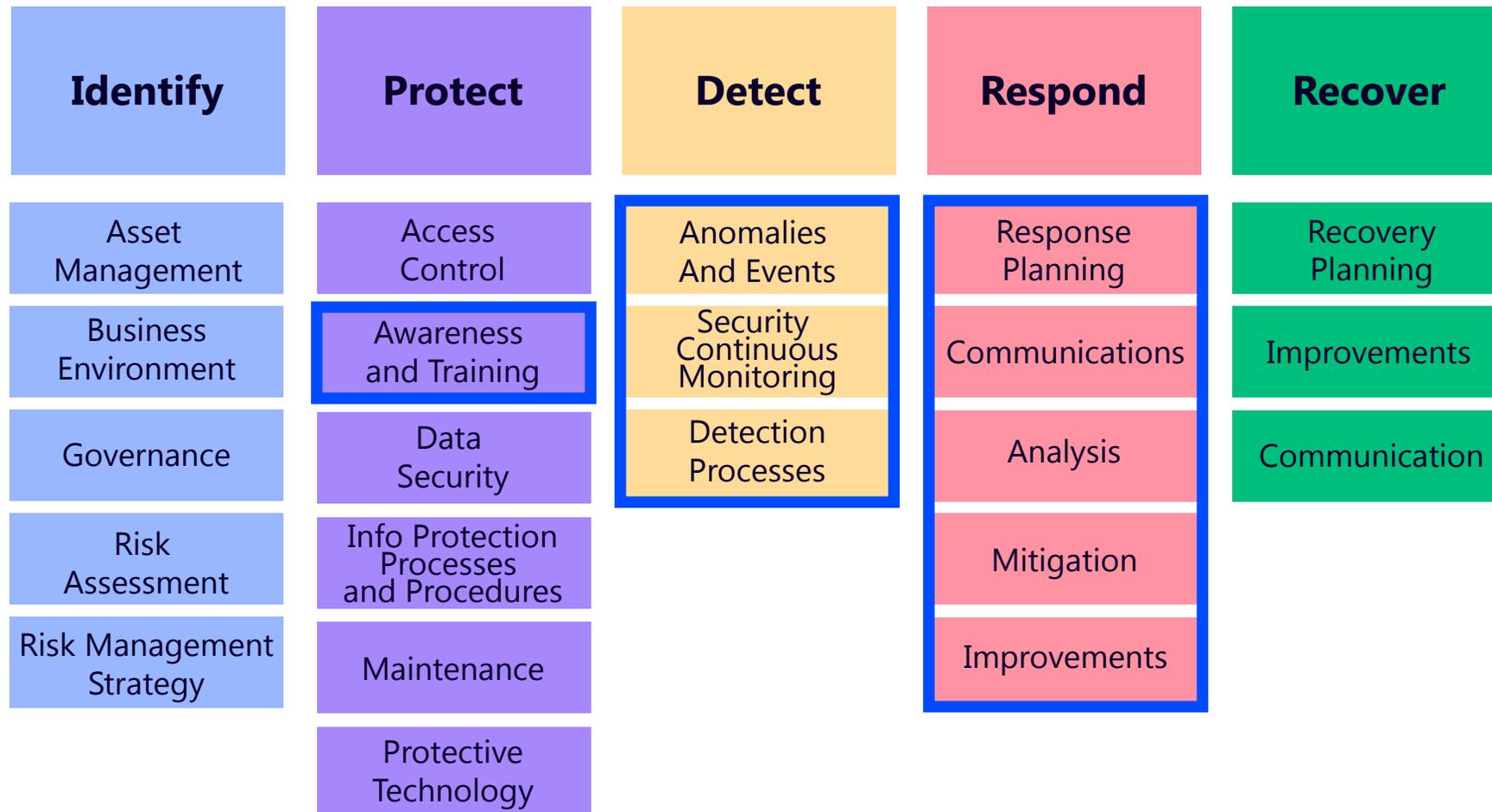
Количество памяти ограничено RAM, HDD и памяти CPU



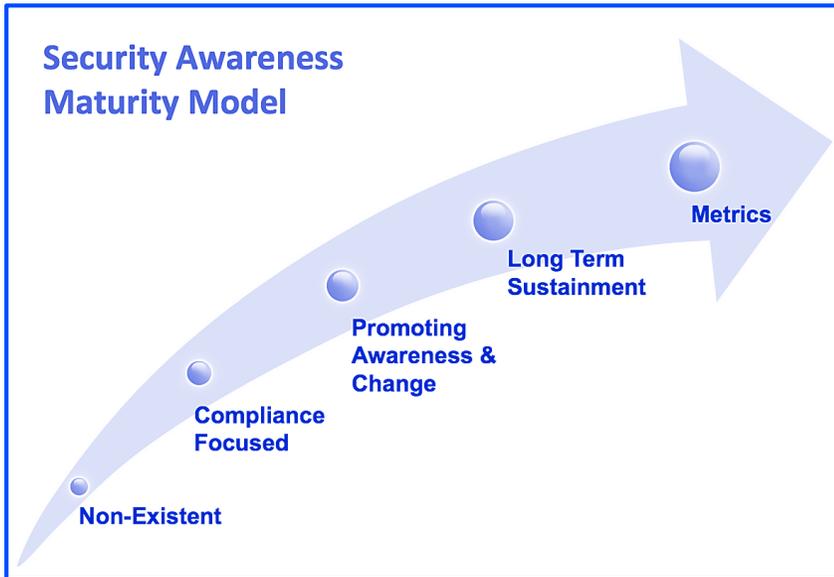
#CSIRT/SOC VS СОЦИНЖЕНЕРИЯ

О ЧЕМ ПОЙДЕТ РЕЧЬ

NIST Cyber Security Framework

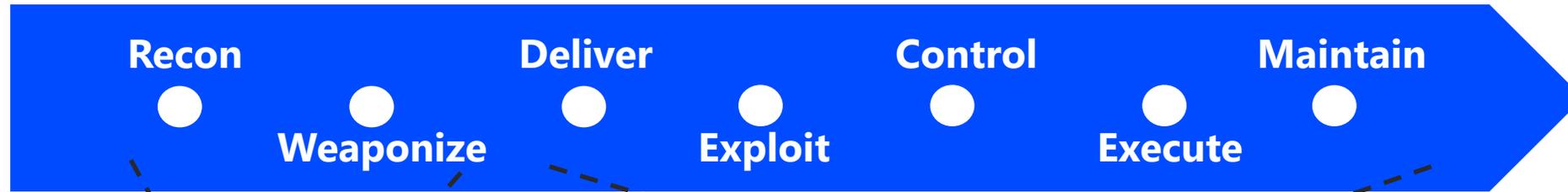


SECURITY AWARENESS VS СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ



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

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

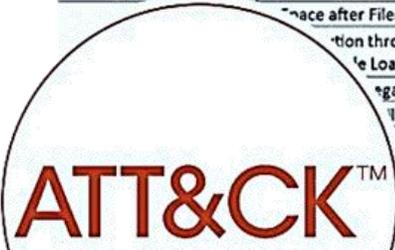
Collection

Exfiltration

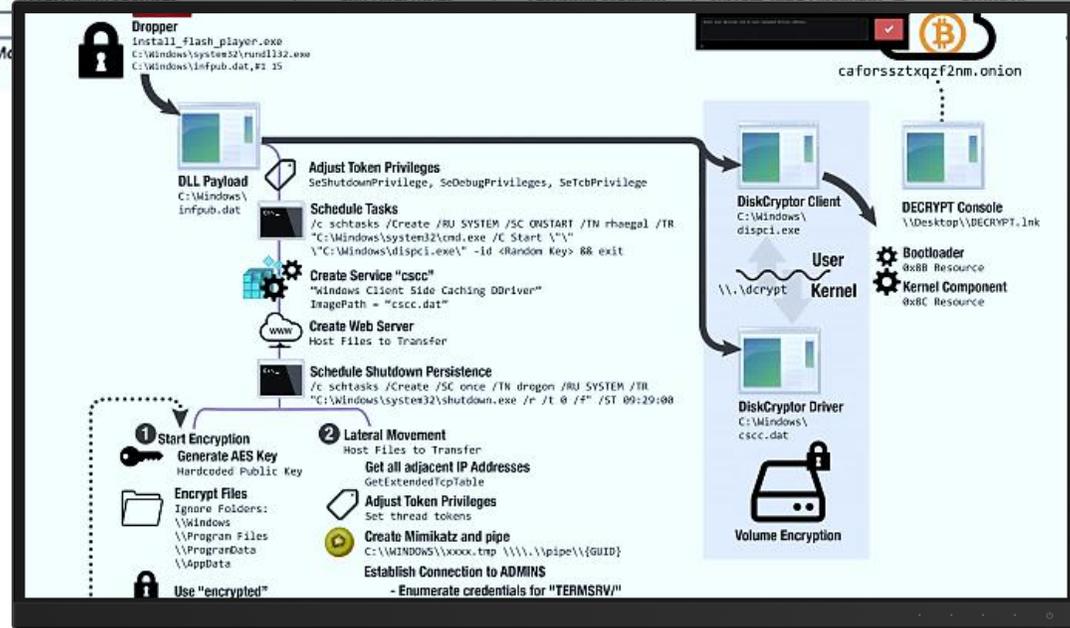
Command and Control

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	Port Knocking
Supply Chain Compromise	Local Job Scheduling	Trap	Access Token Manipulation	Bypass User Account Control	Forced Authentication	Peripheral Device Discovery	Remote File Copy	Audio Capture	Exfiltration Over Command and Control Channel	Multi-hop Proxy
Spearphishing Attachment	Launchctl	Image File Execution Options Injection	Process Injection	Hooking	Password Filter DLL	File and Directory Discovery	Pass the Ticket	Automated Collection	Data Encrypted	Domain Fronting
Exploit Public-Facing Application	Staged Binary Proxy Execution	Plist Modification	Valid Accounts	LLMNR/NBT-NS Poisoning		Permission Groups Discovery	Replication Through Removable Media	Email Collection	Automated Exfiltration	Multi-Stage Channels
Replication Through Removable Media	Exploitation for Client Execution	DLL Search Order Hijacking	Private Keys	Keychain	Input Prompt	System Network Connections Discovery	Windows Admin Shares	Screen Capture	Exfiltration Over Other Network Medium	Web Service
Spearphishing via Service	CMSTP	Appoert DLLs	Signed Script Proxy Execution	DCShadow	Bash History	System Owner/User Discovery	Pass the Hash	Data Staged	Exfiltration Over Alternative Protocol	Standard Non-Application Layer Protocol
Spearphishing Link	Dynamic Data Exchange	Startup Items	Port Knocking	Two-Factor Authentication Interception	System Network Configuration Discovery	Application Window Discovery	Third-party Software	Input Capture	Data from Network Shared Drive	Connection Proxy
Drive-by Compromise	Mshta	Launch Daemon	Indirect Command Execution	Port Knocking	System Owner/User Discovery	Application Window Discovery	Shared Webroot	Shared Drive	Data from Local System	Multilayer Encryption
Valid Accounts	AppleScript	Dylib Hijacking	Application Shimming	Indirect Command Execution	System Owner/User Discovery	Application Window Discovery	Logon Scripts	Man in the Browser	Data Compressed	Standard Application Layer Protocol
	Source	Application Shimming	Appinit DLLs	BITS Jobs	Replication Through Removable Media	Application Window Discovery	Windows Remote Management	Data from Removable Media	Scheduled Transfer	Commonly Used Port
	Trace after Filename	Web Shell	Service Registry Permissions Weakness	Control Panel Items	Input Capture	Application Window Discovery	Application Deployment Software			Standard Cryptographic Protocol
	Execution through the Load	New Service	File System Permissions Weakness	Process Doppelgänger	Network Sniffing	Application Window Discovery	SSH Hijacking			Custom Cryptographic Protocol
	Regasm	File System Permissions Weakness	Path Interception	Hidden Files and Directories	Credential Dumping	Application Window Discovery	AppleScript			Data Obfuscation
	h API	Path Interception	Path Interception	Kernel Memory	Kernel Memory	Application Window Discovery	Target Shared Content			Custom Command and Control Protocol
		Path Interception	Path Interception	Kernel Memory	Kernel Memory	Application Window Discovery	Remote Desktop Protocol			Communication



MITRE



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	Personas 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 skillsets 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 skillsets 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	C2 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 skillsets 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 target of interest	Create custom payloads	Test malware to evade detection	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 visibility gap of security vendors			Data Hiding	Dynamic DNS		Identify resources required to build capabilities		
Develop KITs/KIQs			Discover target logon/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					
			Spearphishing via email/social						Obfuscate 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



МАТРИЦА MITRE ATT&CK ENTERPRISE

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Insider Spoofing	AppletScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Port Discovery	AppletScript	Audio Capture	Automated Exfiltration	Proxy Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	File Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Component Firmware	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkits	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-Stage Channels
	InstallUI	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		Multi-hop Proxy
	LSASS Driver	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	SSH Hijacking	Screen Capture		Multiband Communication
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DLL Search Order Hijacking	Keychain	Remote System Discovery	Shared Webroot	Video Capture		Multilayer Encryption
	Local Job Scheduling	Create Account	Launch Daemon	DLL Side-Loading	LLMNR/NTNS Poisoning	Security Software Discovery	Taint Shared Content			Port Knocking
	Mshta	DLL Search Order Hijacking	New Service	Deobfuscate/Decode Files or Information	Network Sniffing	System Information Discovery	Third-party Software			Remote Access Tools
	PowerShell	Dylib Hijacking	Path Interception	Disabling Security Tools	Password Filter DLL	System Network Configuration Discovery	Windows Admin Shares			Remote File Copy
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion	Private Keys	System Network Connections Discovery	Windows Remote Management			Standard Application Layer Protocol
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection	Securityd Memory	System Owner/User Discovery				Standard Cryptographic Protocol
	Rundll32	Hidden Files and Directories	Process Injection	File Deletion	Two-Factor Authentication Interception	System Service Discovery				Standard Non-Application Layer Protocol
	Scheduled Task	Hooking	SID-History Injection	File Permissions Modification		System Time Discovery				Uncommonly Used Port
	Scripting	Hypervisor	Scheduled Task	File System Logical Offsets						Web Service
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Gatekeeper Bypass						
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	HISTCONTROL						
	Signed Script Proxy Execution	LC_LOAD_DYLIB Addition	Startup Items	Hidden Files and Directories						
	Source	LSASS Driver	Sudo Caching	Hidden Users						
	Space after Filename	Launch Agent	Sudo	Hidden Window						
	Third-party Software	Launch Daemon	Valid Accounts	Image File Execution Options Injection						
	Trap	Launchctl	Web Shell	Indicator Blocking						
	Trusted Developer Utilities	Local Job Scheduling		Indicator Removal from Tools						
	User Execution	Login Item		Indicator Removal on Host						
	Windows Management Instrumentation	Logon Scripts		Indirect Command Execution						
	Windows Remote Management	Modify Existing Service		Install Root Certificate						
	XSL Script Processing	Netsh Helper DLL		InstallUI						
		New Service		LC_MAIN Hijacking						
		Office Application Startup		Launchctl						
		Path Interception		Masquerading						
		Plist Modification		Modify Registry						
		Port Knocking		Mshta						
		Port Monitors		NTFS File Attributes						
		Port Monitors		Network Share Connection Removal						
		Rc-common		Obfuscated Files or Information						
		Re-opened Applications		Plist Modification						
		Redundant Access		Port Knocking						
		Registry Run Keys / Startup Folder		Process Doppelgänger						
		SIP and Trust Provider Hijacking		Process Hollowing						
		Scheduled Task								

Выбор цели и первичная разведка

Сбор информации

Извлечение информации

Предлог

Обман и манипуляция

Убеждение и влияние



В ЧЕМ СУТЬ ПОДХОДА

ЗРЕЛОСТЬ INCIDENT RESPONSE



Maturity Level		Ad-hoc		Maturing		Strategic
		As Needed	Dedicated Part-time	Full-time	SOC/IR+	Fusion
Возможности Incident Response	Команда	0-1	1-3	2-5	~10	15+
	Процессы	<ul style="list-style-type: none"> Chaotic and relying on individual heroic; reactive General purpose run-book Tribal knowledge 	<ul style="list-style-type: none"> Situation run books; some consistency Email-based processes 	<ul style="list-style-type: none"> Requirements and workflow documented as standards business process Some improvement over time 	<ul style="list-style-type: none"> Process measured via metrics Minimal Threat Sharing Shift turnover SLAs 	<ul style="list-style-type: none"> Processes are constantly improved and optimized Broad Threat sharing Hunt teams
	Технологии	AV/FW/IDS	SIEM/Sandboxing	<ul style="list-style-type: none"> Continuous monitoring Endpoint forensics Tactical Intelligence 	<ul style="list-style-type: none"> Malware Analysis Additional Intelligence IT Operation integration 	<ul style="list-style-type: none"> Intel+IR Drives Security Program Strategic Intelligence Coordination with Physical Security Intelligence
CMM Эквивалент		Initial	Repeatable	Defined	Managed	Optimized

90%

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

Риски при реализации

Высокие

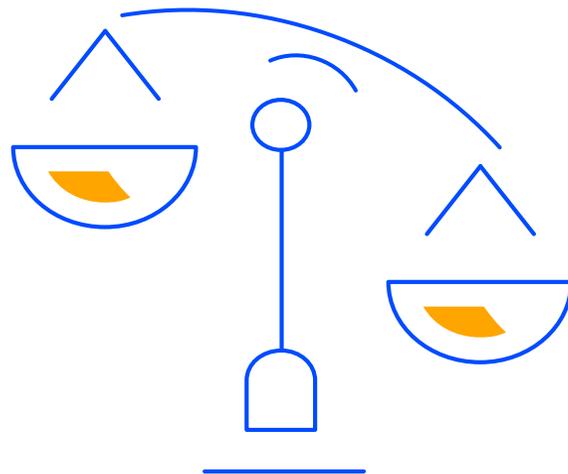
Средние

Низкие

Сложность и стоимость реализации



РИСК ЗЛОУМЫШЛЕННИКА ОПРЕДЕЛЯЕТСЯ ЦЕЛЬЮ



Деньги



Шпионаж



Дестабилизация



Пром.авария

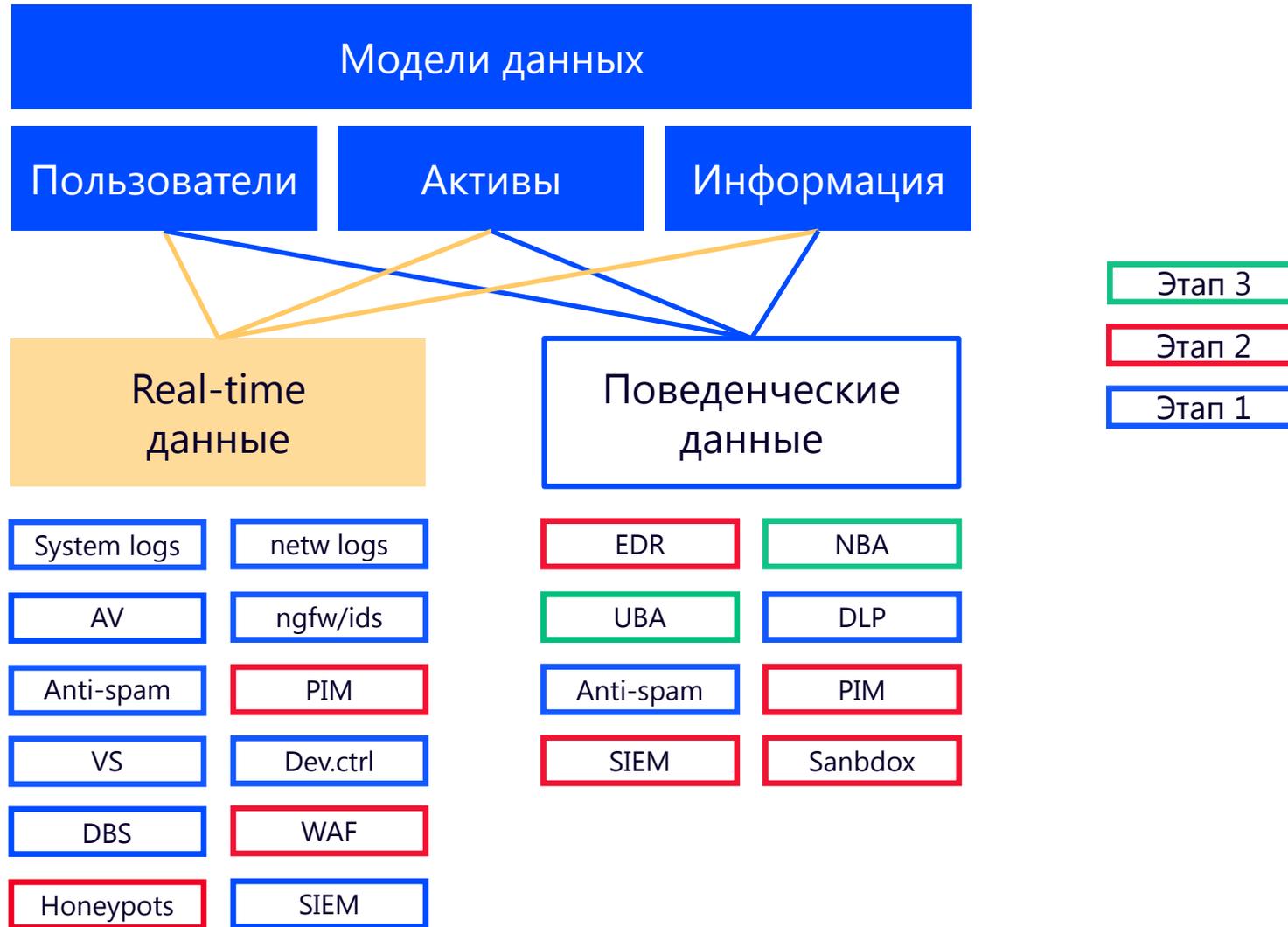




ПОВЫШЕНИЕ ЗРЕЛОСТИ CSIRT/SOC



ПРИМЕР. ИСТОЧНИКИ СОБЫТИЙ





ПОВЫШЕНИЕ ЗРЕЛОСТИ МОНИТОРИНГА ИНЦИДЕНТОВ

Следующий уровень зрелости



ДОПОЛНИТЕЛЬНЫЙ ФОКУС НА МАРКЕРАХ СОЦИНЖЕНЕРИИ

Прямые сценарии по техвекторам SE:

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



Косвенные сценарии SE:

- DLP сценарии
- UBA сценарии
- TBA сценарии

The screenshot displays a configuration page for a security rule. At the top, there is a metadata section with fields like name, category, killchain, and severity. Below this is a 'Логика срабатывания' (Trigger Logic) section with a descriptive paragraph. The 'Известные false positive' (Known False Positives) section is empty. The 'Правила' (Rules) section contains a detailed XML configuration for the rule 'Exe launched from portable disk'. The XML includes details about the rule's activation, description, customer scope, incident definition, and dynamic watchlist definitions.

```
<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-011</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=ExeFromPo
</IncidentDef>
<DynWatchListDef/>
<PatternClause window="300">
<SubPattern id="38635568" name="ExeFromPortable">
<SingleEvtConstr>eventType = "Win-Security-4688" AND procName CONTAIN "\\Device\\HarddiskVolume"</SingleEvtConstr>
<GroupEvtConstr>COUNT(*) &gt;= 1</GroupEvtConstr>
<GroupByAttr>user,fileName,procName,destName,destIpAddr,reprDevIpAddr</GroupByAttr>
</SubPattern>
</PatternClause>
<userRoles>
<roles custId="0">1686400</roles>
</userRoles>
<TriggerEventDisplay>
<AttrList>phRecvTime,eventType,reprDevIpAddr,rawEventMsg,destIpAddr,destName,procName,user</AttrList>
</TriggerEventDisplay>
</Rule>
```

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.

From: YourCEO@yourorganization.com
 To: You@yourorganization.com
 Date: Monday December 12, 2018 3:00 pm
 Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag. Could you wire me \$300 via Bank of America? They gave me a special link so this goes right into my account and I can buy a ticket home:

<http://www.bankofamerica.com>

Thanks so much! This really helps me out!

Your CEO

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.?

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.

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?

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 — the "m" is really two characters — "r" and "n."

© 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.



СПАСИБО ЗА ВНИМАНИЕ!

Алексей Мальнев

Руководитель Jet CSIRT

au.malnev@jet.su / +7 985 849-89-33