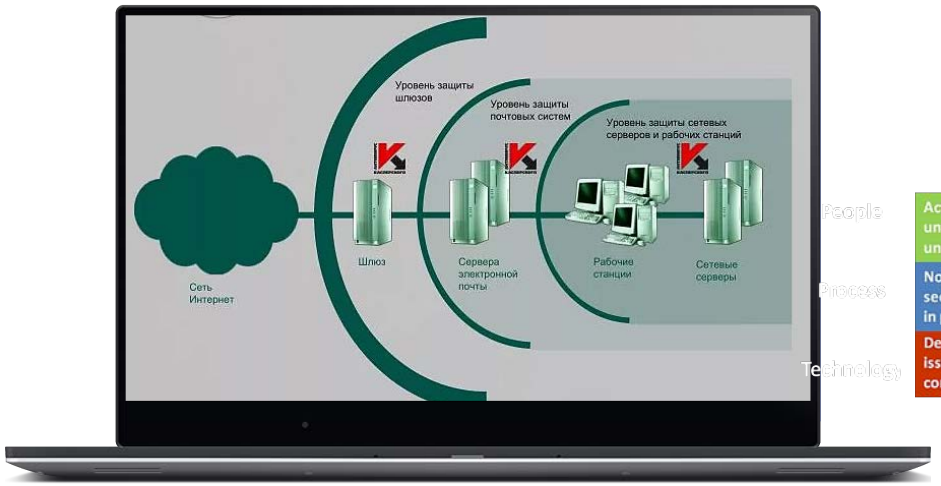
2019

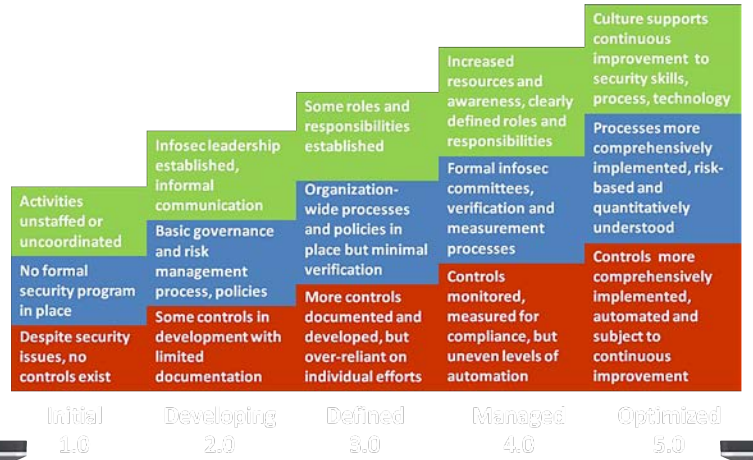
CSIRT VS ЧЕЛОВЕЧЕСКИЙ ФАКТОР ИЛИ МОЖНО ЛИ БОРОТЬСЯ С СОЦИАЛЬНОЙ ИНЖЕНЕРИЕЙ

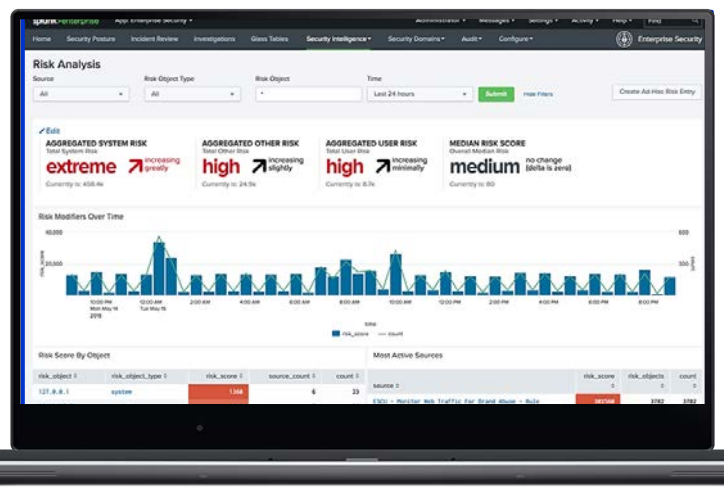
Алексей Мальнев

Руководитель Jet CSIRT
ay.malnev@jet.su / +7 985 849-89-33

ПРЕДСТАВИМ, ЧТО МЫ НЕПЛОХО ЗАЩИТИЛИСЬ

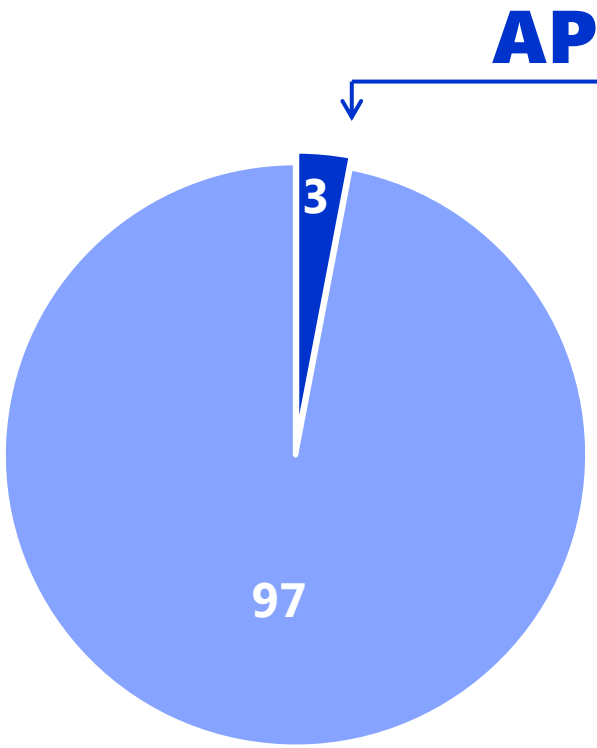






ПРЕДСТАВИМ,
ЧТО МЫ НЕПЛОХО ЗАЩИТИЛИСЬ

НА САМОМ ДЕЛЕ ВСЕ НЕ ТАК ЗДОРОВО



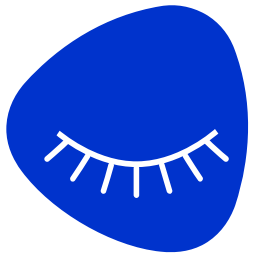
Основной фокус большинства команд ИБ

- Без социальной инженерии
- С социальной инженерией

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ — АТАКУЮЩИЙ МЕТОД №1

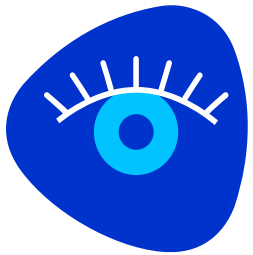
https://www.dogana-project.eu/index.php/social-engineering-blog/11-social-engineering/94-estimates-of-social-engineering-attacks

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

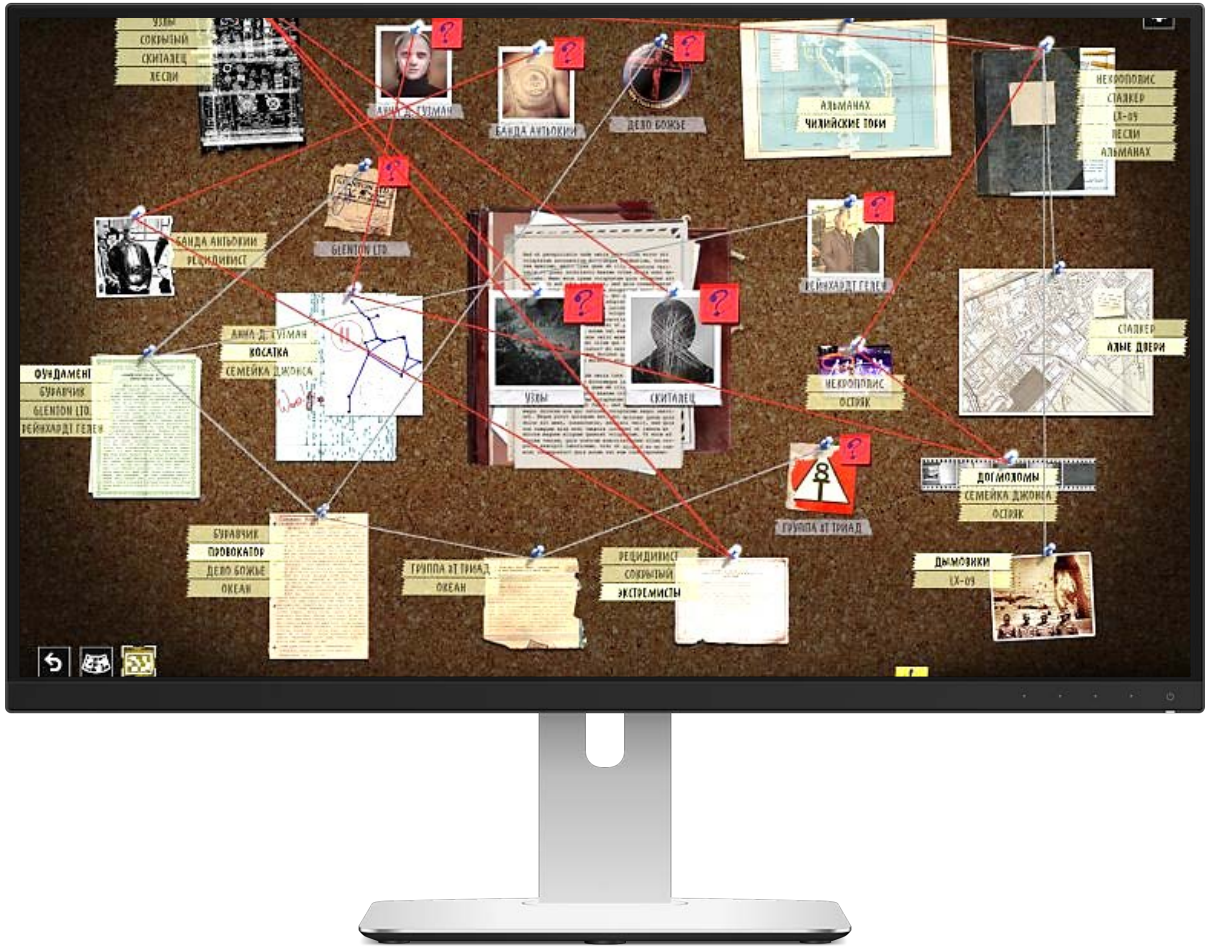
- Социальная инженерия – это «бесконечное» количество комбинаций технических и нетехнических техник и стратегий
- Кибератака может быть частью стратегии социальной инженерии
- Социальная инженерия – всегда таргетирована и фокусна
- Социальная инженерия всегда действует от уровня Security Awareness и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

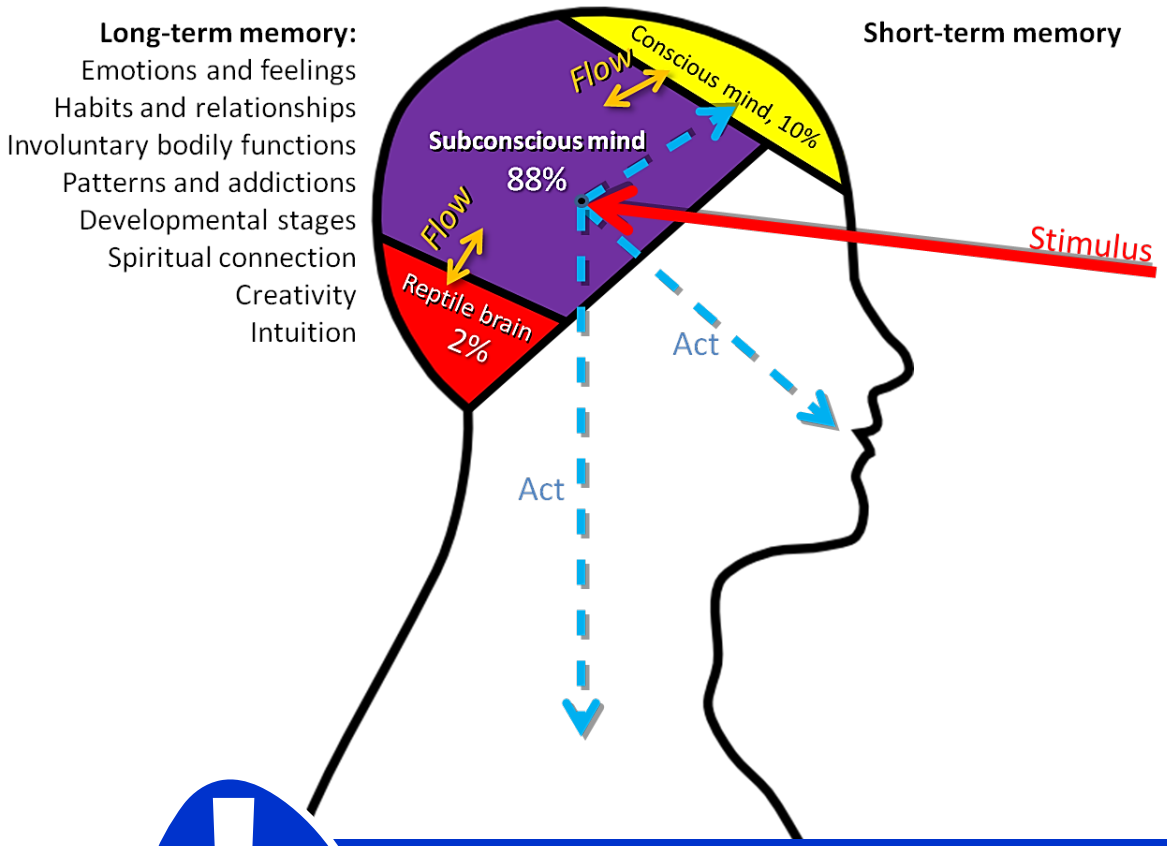
Братья Бадир

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. LIFECYCLE

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ МНОГООБРАЗИЕ ТЕХНИК

- **Техники инициации**
  Естественность, осведомленность, щедрость
- **Первичная обработка**
  Фоновая обработка, загрузка информации
- **Техники предлогов**
  Использование персональных интересов, применение диалектов, махинации с телефонами
- **Техники извлечения информации**
  Апеллирование к эго, «искренний» интерес, подтасовка данных, лесть, волонтёрство, 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

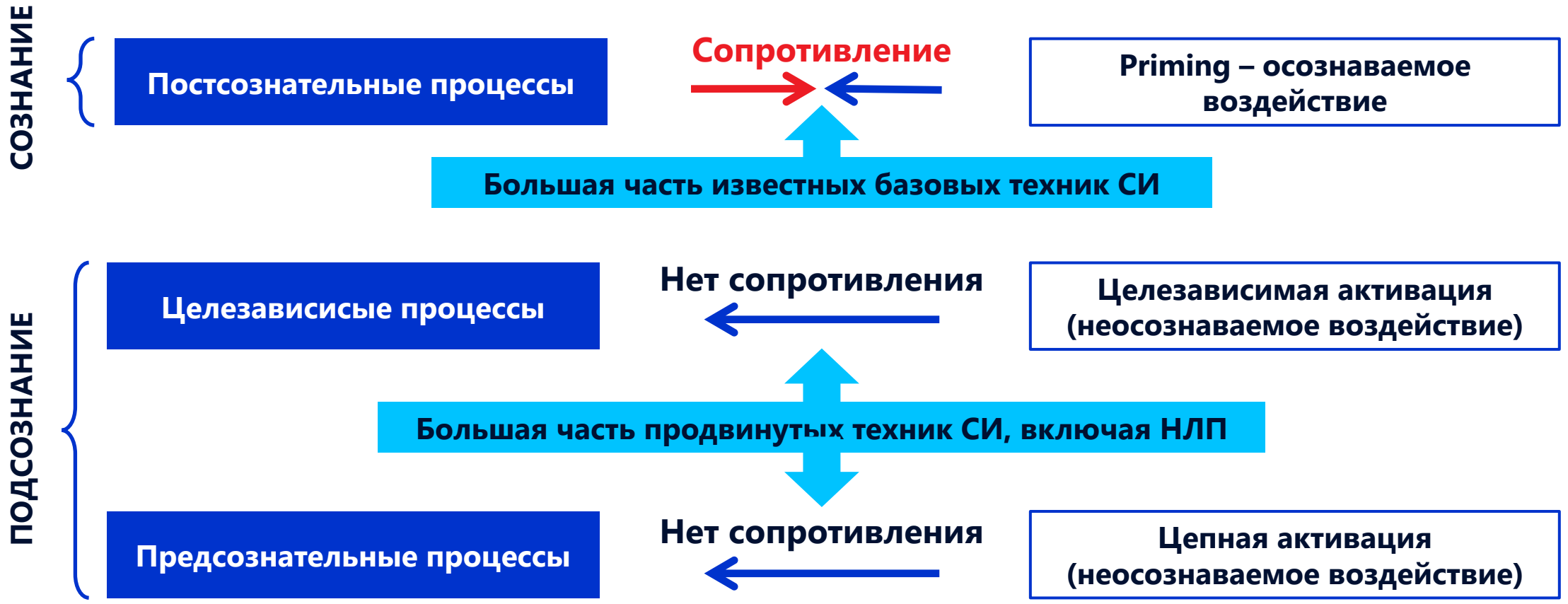


- от 95% до 99,99% вычислительной мощности мозга сосредоточены в подсознании
- Около 95% когнитивной деятельности сосредоточены в подсознании
- Сознание очень ограничено

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	Прошлое 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

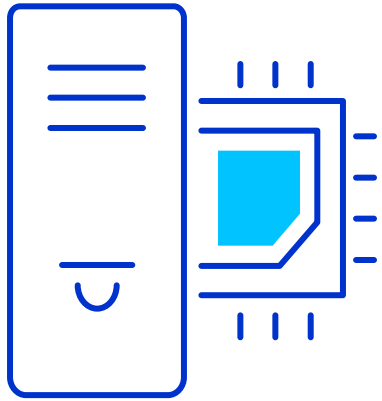
Квадриллион (1 000 000 000 000 000) байт =
1 миллион гигабайт =
1000 терабайт = 1 петабайт

> > >

Множество всех состояний программы

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

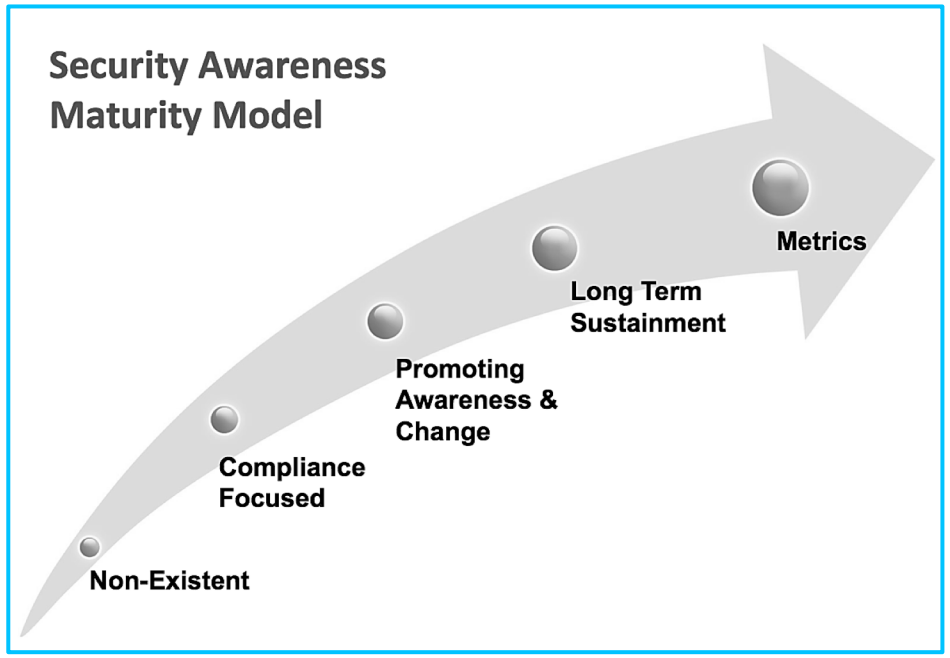
Количество состояний ПО стандартной программы на стандартном ПК



Количество памяти ограничено RAM, HDD и памяти CPU

CSIRT/SOC VS СОЦИНЖЕНЕРИЯ

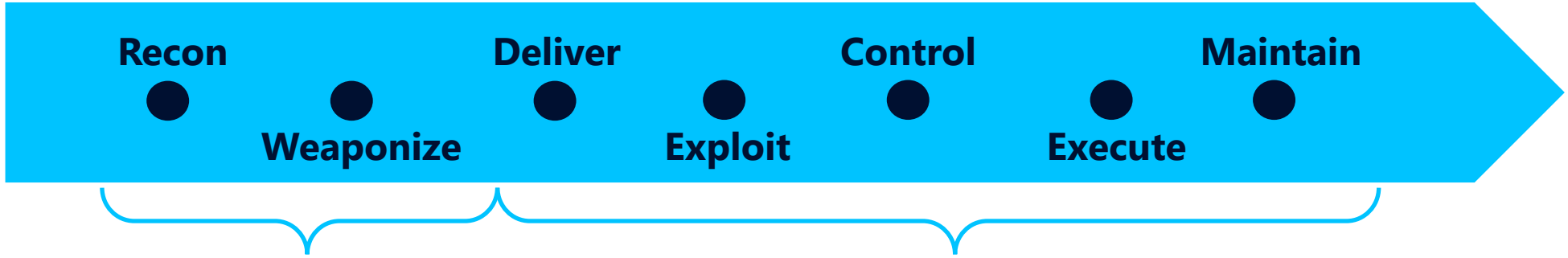
SECURITY AWARENESS VS СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ



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

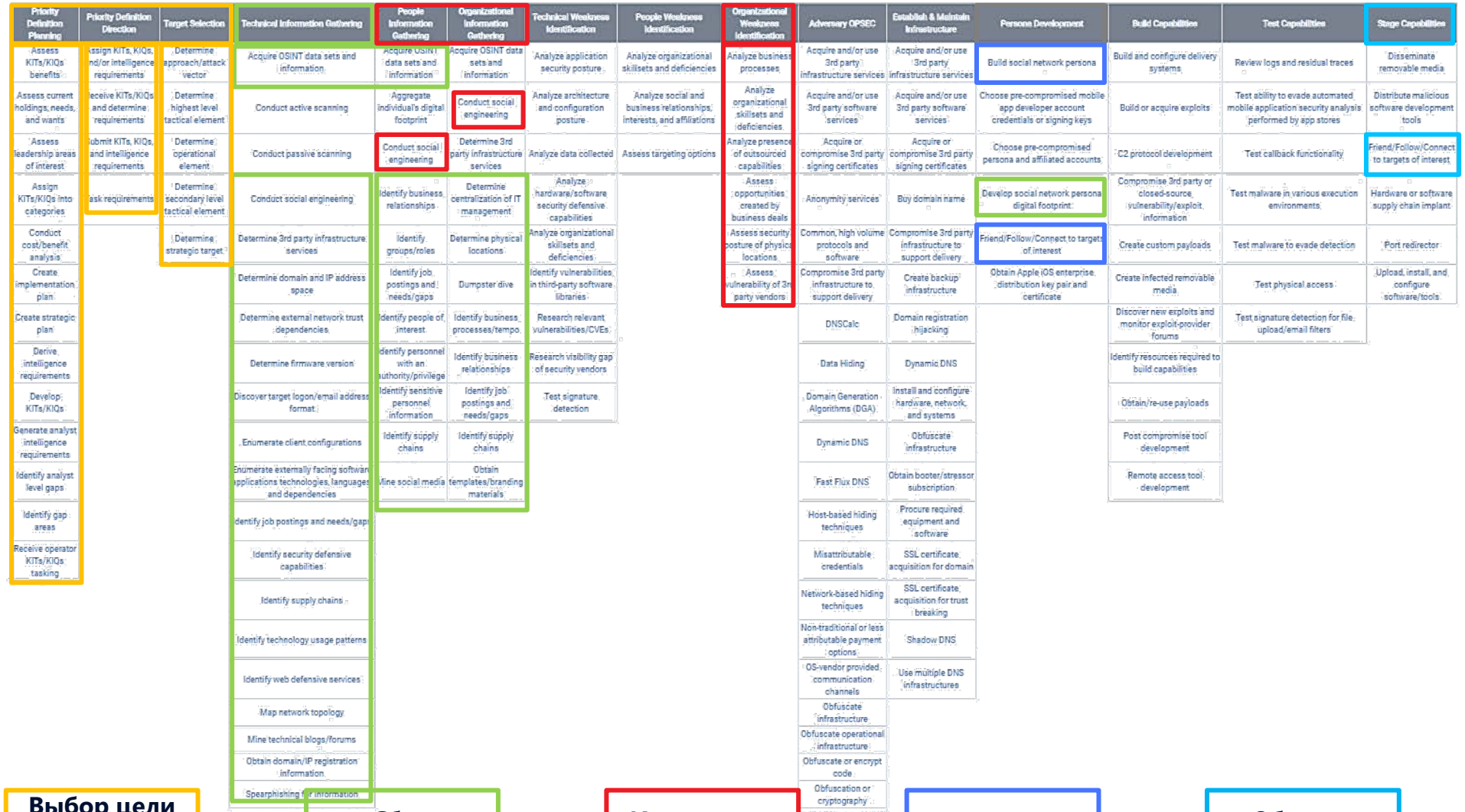
Lateral Movement

Collection

Exfiltration

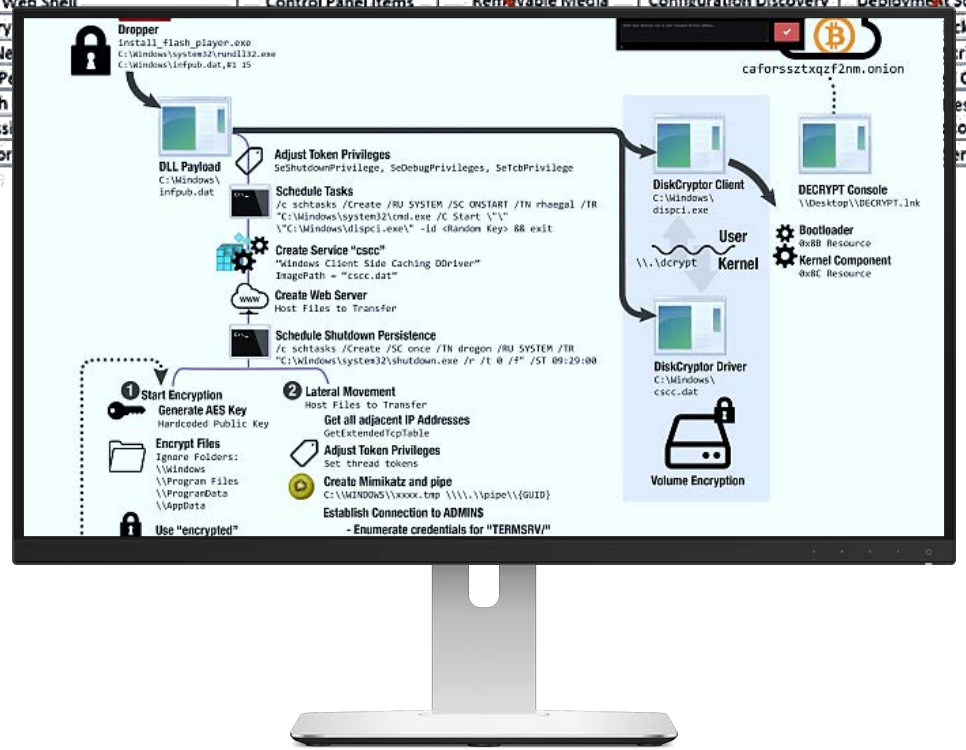
Command and Control

МАТРИЦА MITRE PRE ATT&CK

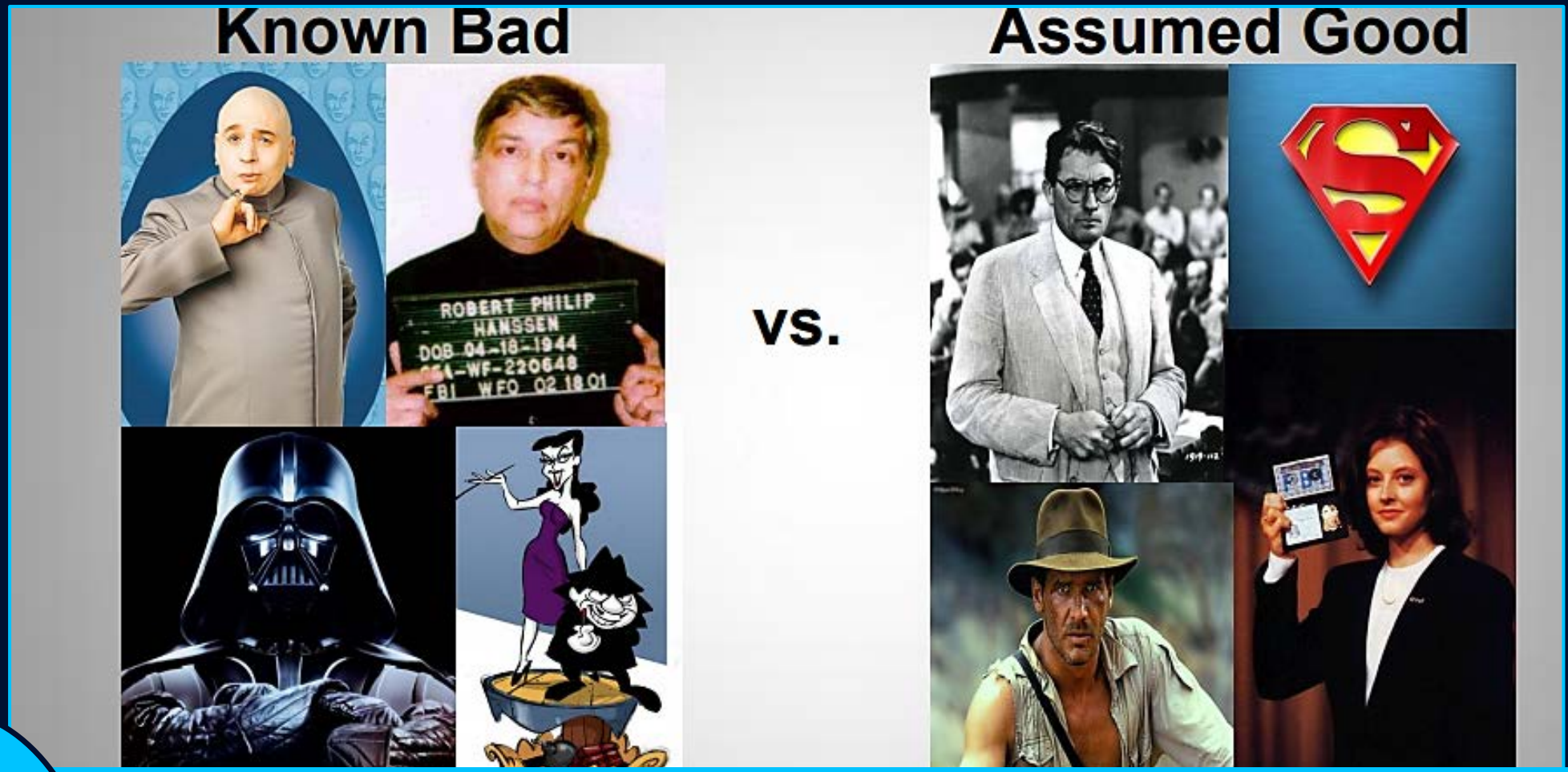


ATT&CK MITRE

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

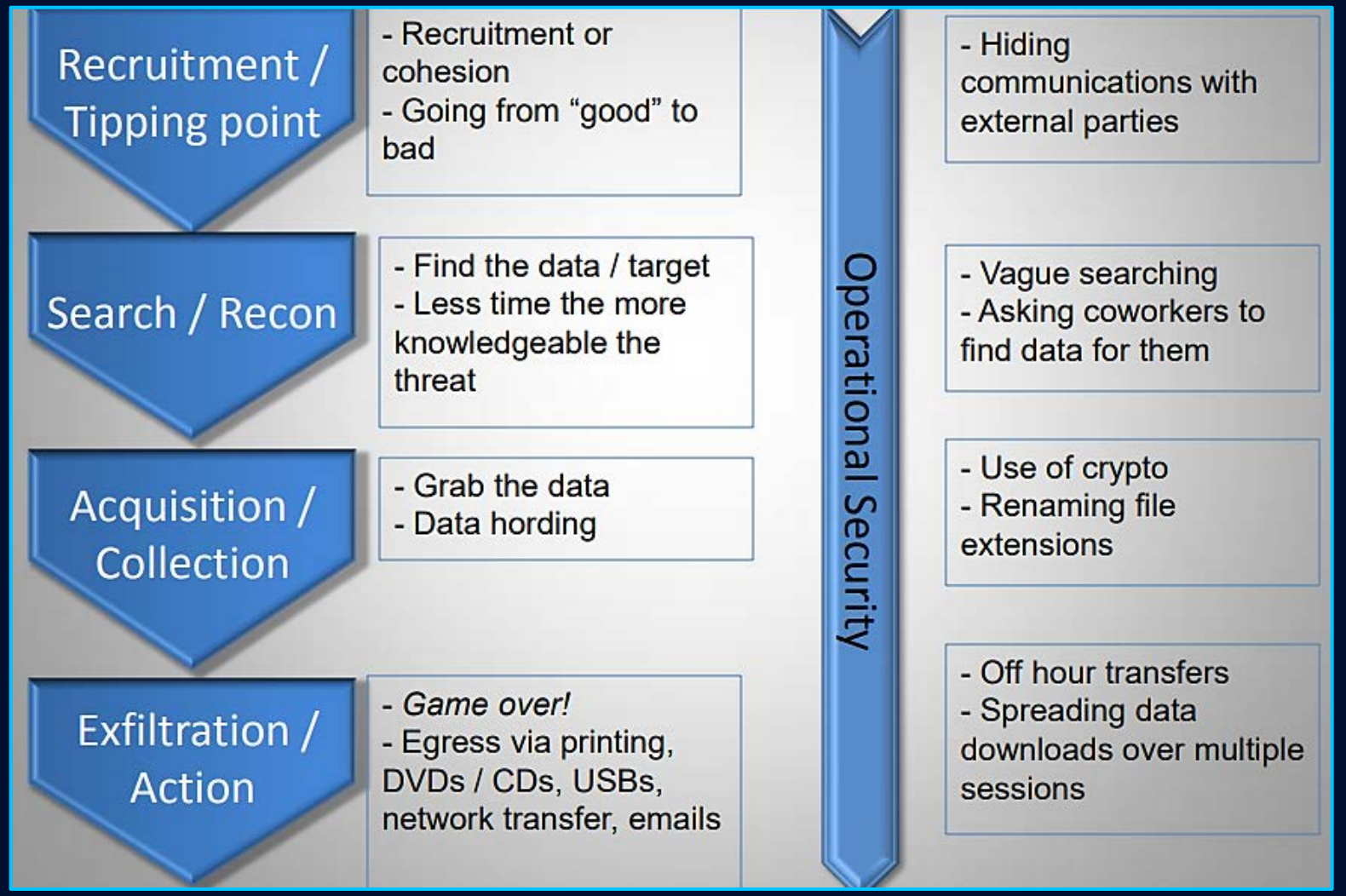


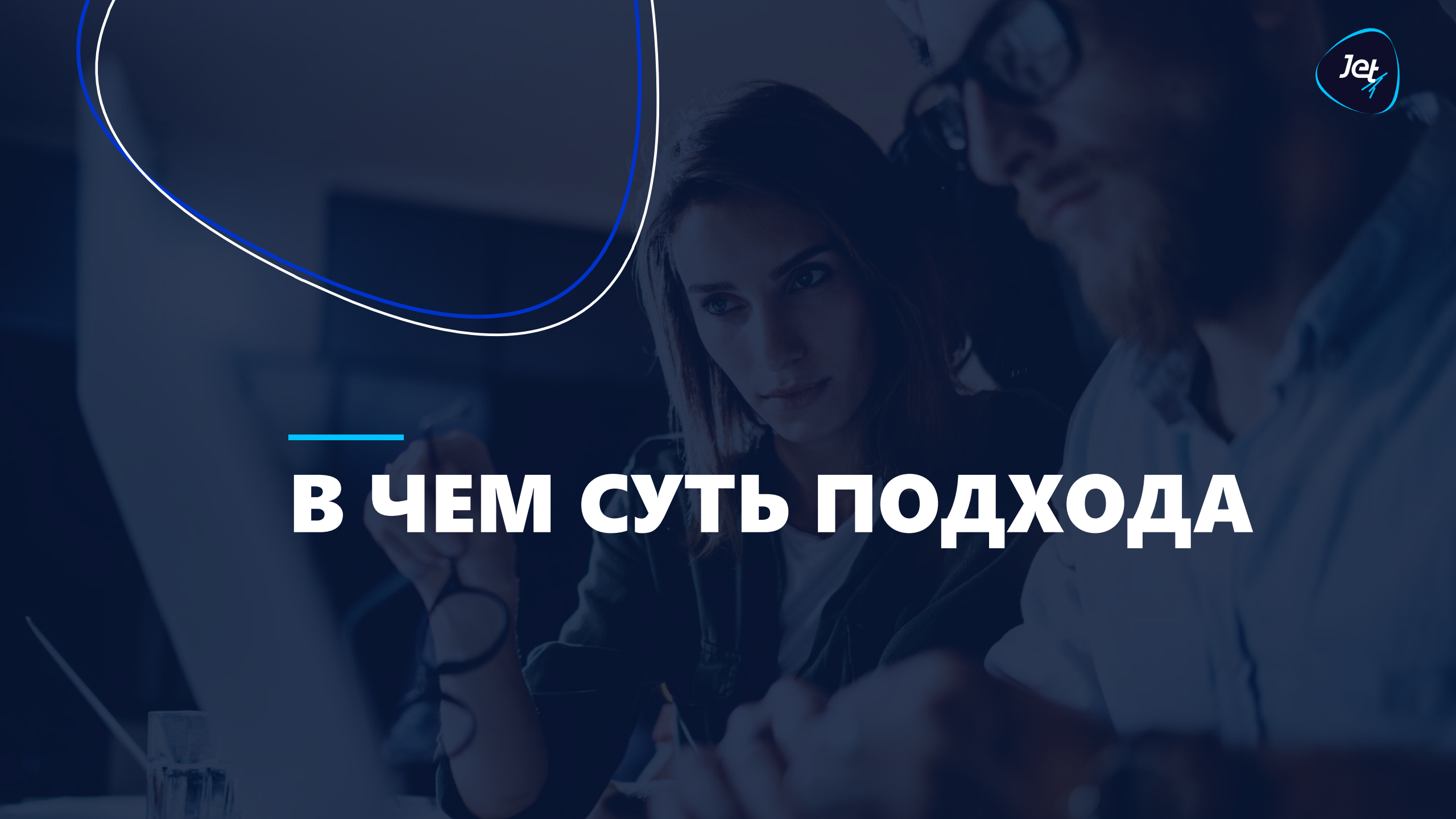
А ЕСЛИ ИСХОДНЫЙ ВЕКТОР SE НЕ ТЕХНИЧЕСКИЙ?



Имеем дело с осознанным или неосознанным Insider Threat Agent

KILL CHAIN ДЛЯ INSIDER





В ЧЕМ СУТЬ ПОДХОДА

ЛОГИКА АТАКУЮЩЕЙ СТОРОНЫ

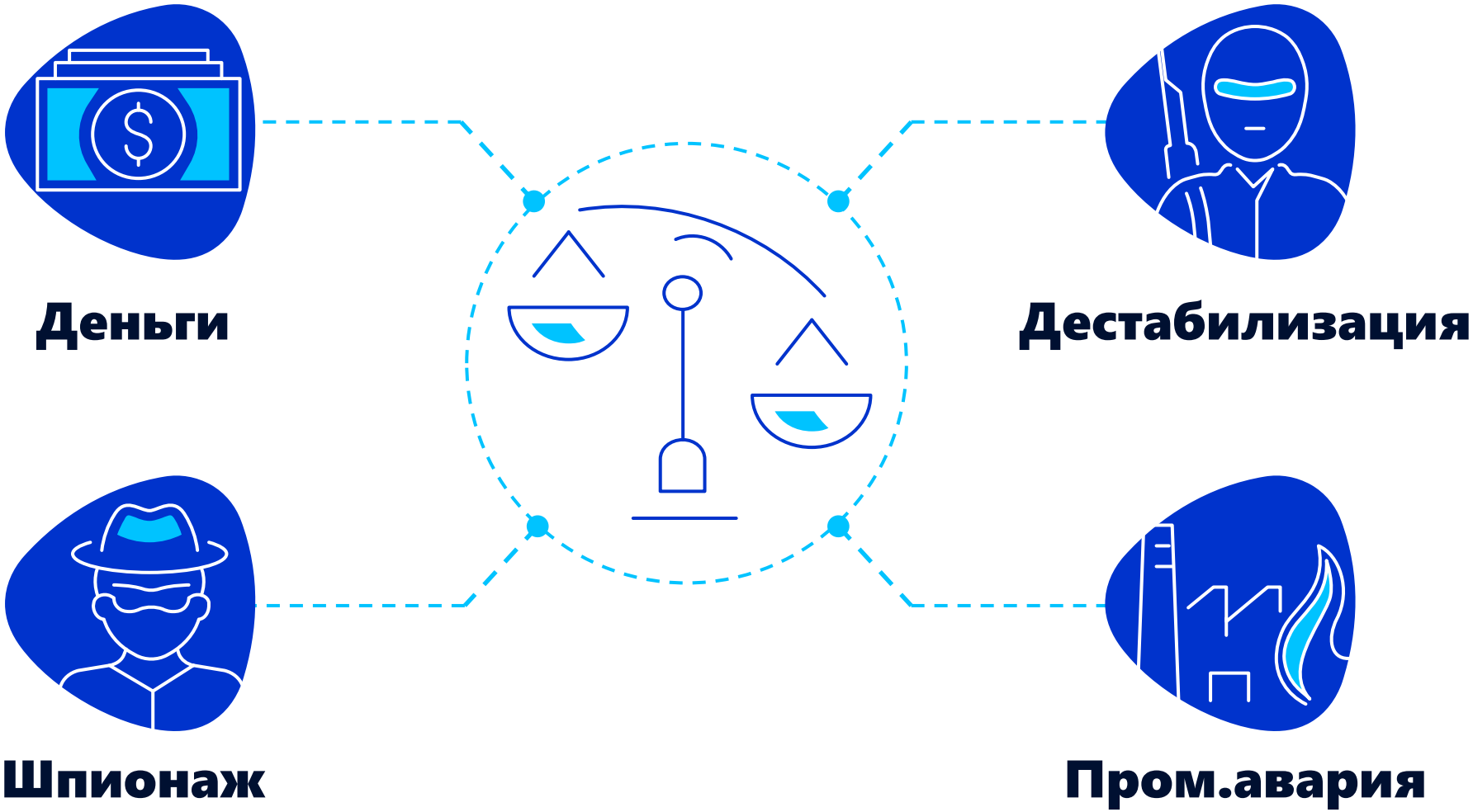
Зрелость атакуемой системы ИБ	Ad-Hoc	Maturing	Strategic
Используемые векторы атак	Нетехнические	Нетехнические	Нетехнические
	Технические и нетехнические	Технические и нетехнические	Технические и нетехнические
	Технические	Технические	Технические

Риски при реализации

- Высокие
- Средние
- Низкие

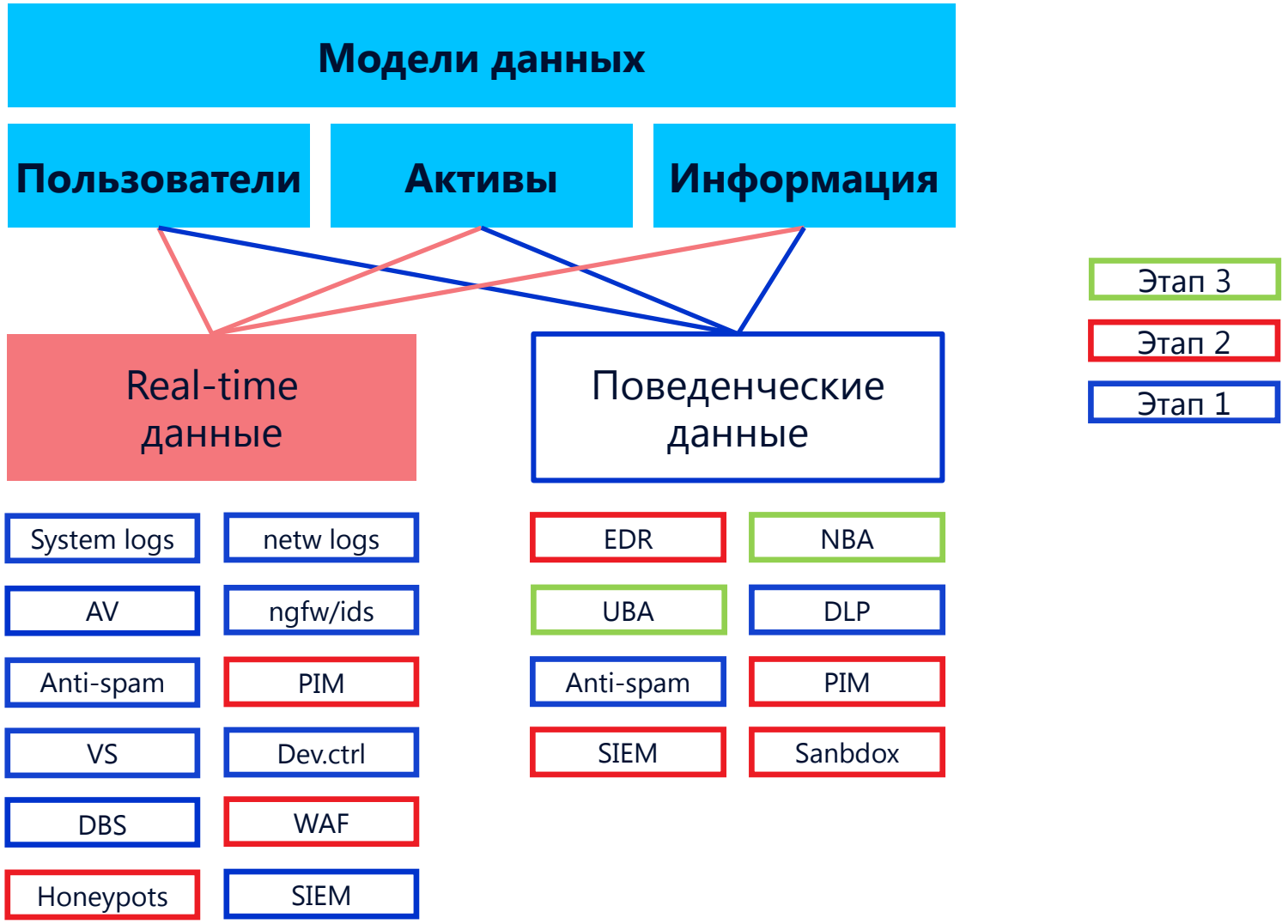
Сложность и стоимость реализации

РИСК ЗЛОУМЫШЛЕННИКА ОПРЕДЕЛЯЕТСЯ ЦЕЛЬЮ

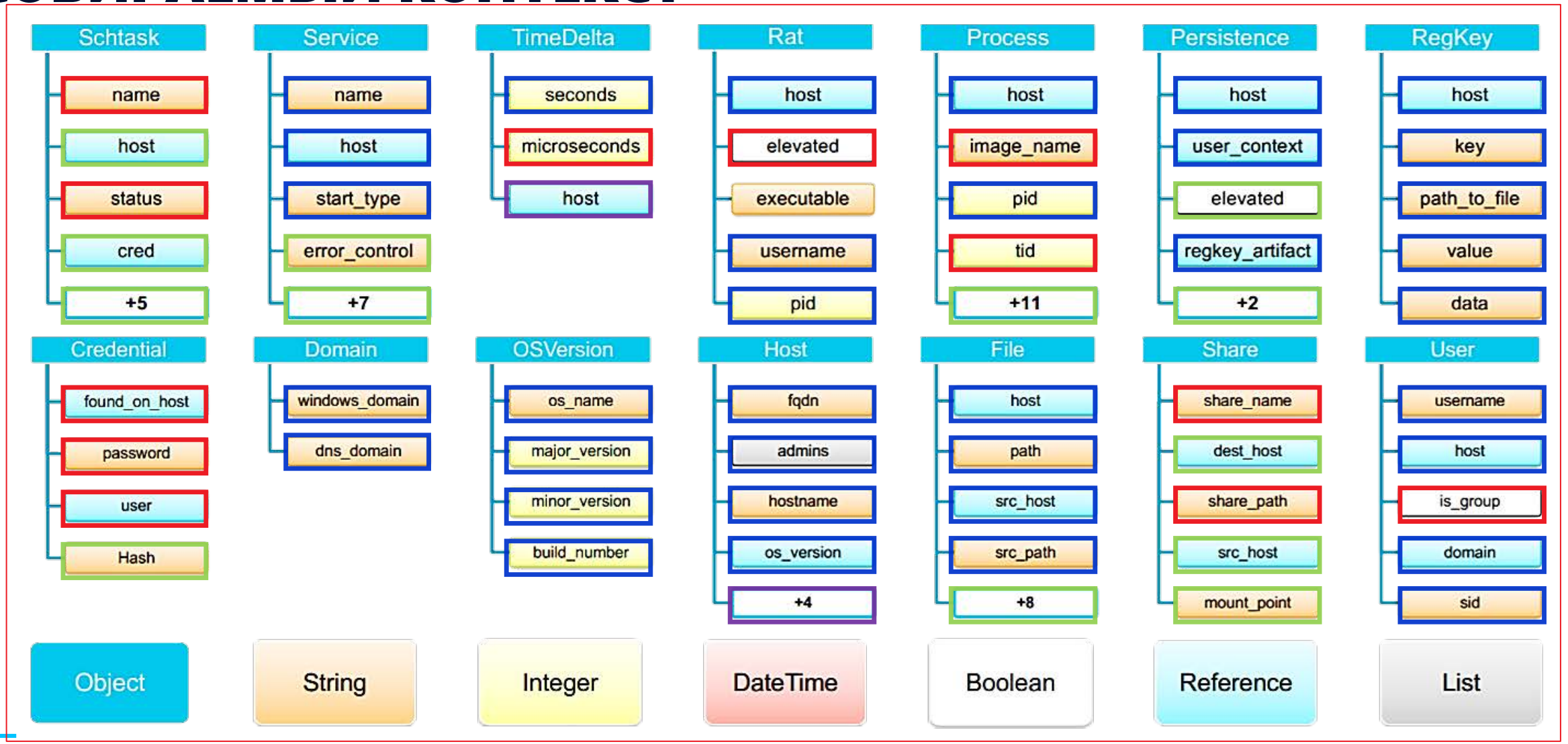


ПОВЫШЕНИЕ ЗРЕЛОСТИ CSIRT/SOC

ПРИМЕР. ИСТОЧНИКИ СОБЫТИЙ



ПРИМЕР. МОДЕЛЬ АКТИВОВ. СОБИРАЕМЫЙ КОНТЕКСТ



ПОВЫШЕНИЕ ЗРЕЛОСТИ МОНИТОРИНГА ИНЦИДЕНТОВ

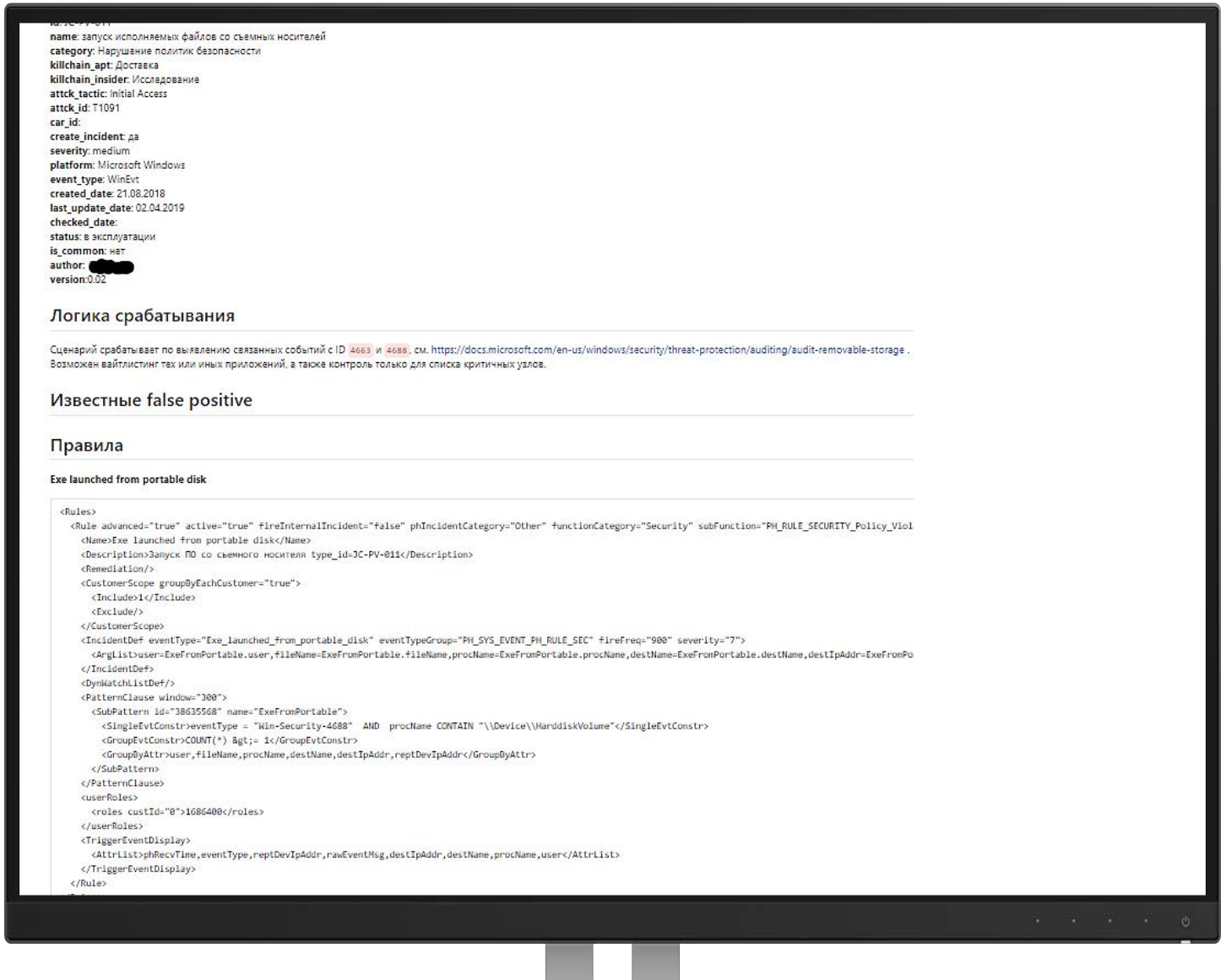
ДОПОЛНИТЕЛЬНЫЙ ФОКУС НА МАРКЕРАХ СОЦИНЖЕНЕРИИ

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



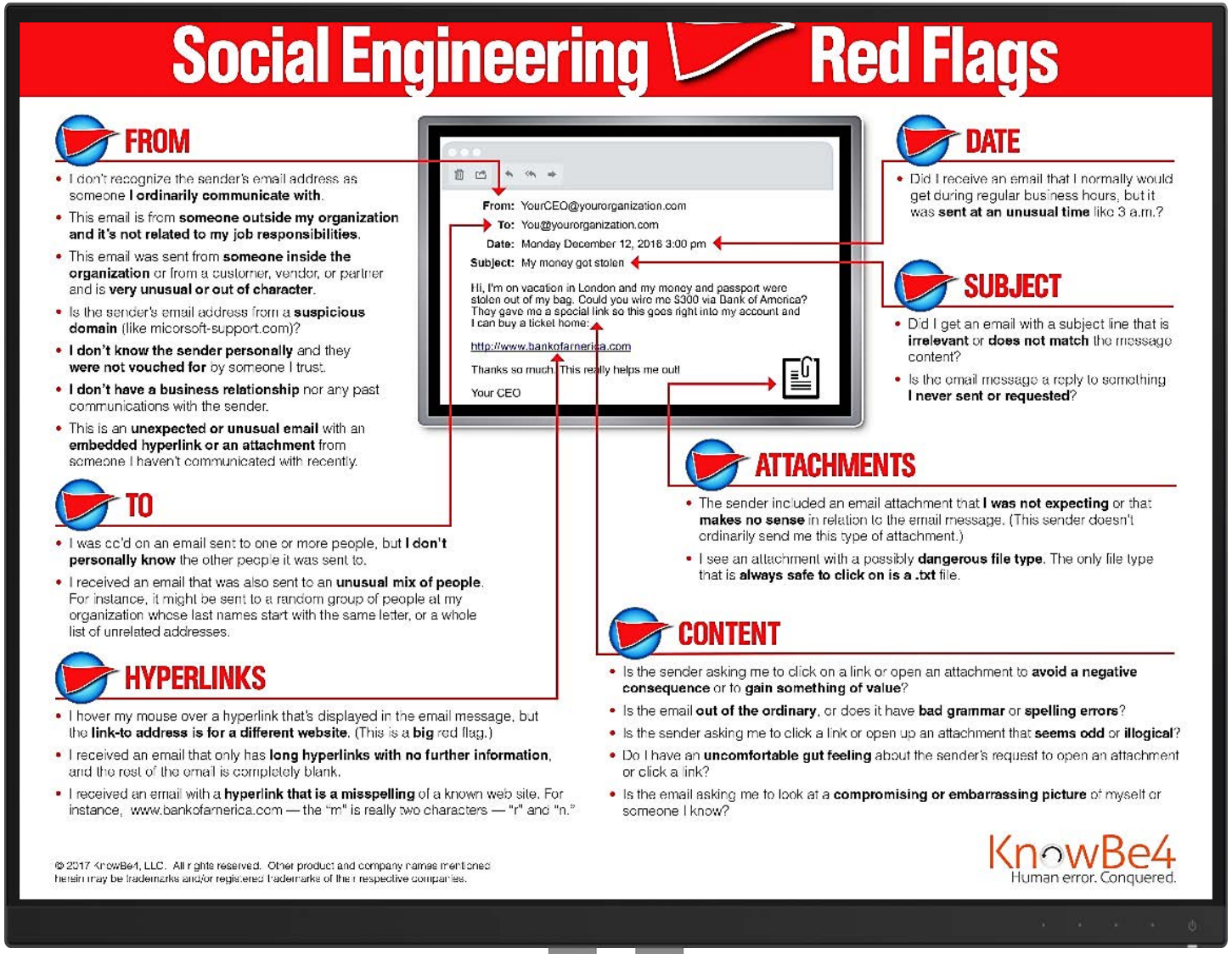
СЦЕНАРИИ ДЕТЕКТИРОВАНИЯ ТЕХНИЧЕСКИХ ВЕКТОРОВ SE

ТИП СЦЕНАРИЯ	PHISHING	WATERING HOLE	TYPESQUOTING	WHALING ATTACK	BAITING	PIGGYBACKING	SMISHING
Стадии атаки 1: Первичное воздействие	**SecAwareness** - NGWF (Cisco + AMP, Checkpoint + Sandbox, Fortigate + Sandbox), - TI IoC event - Cisco Email Sec App, FortiMail, Kaspersky AS event	**SecAwareness** - NGWF (Cisco + AMP, Checkpoint + Sandbox, Fortigate + Sandbox), - TI IoC event - McAfee Web GW, Cisco Web Sec Appliance, Bluecoat ProxySG, NGFW	**SecAwareness** NGFW + TI IoC event, - Cisco Email Sec App, FortiMail, Kaspersky AS event	**SecAwareness** NGWF (Cisco + AMP, Checkpoint + Sandbox, Fortigate + Sandbox), - TI IoC event - Cisco Email Sec App, FortiMail, Kaspersky AS event	**SecAwareness** - MS event 4663 4668 - Kaspersky KES, Lumention DC, Zecurion DLP	**SecAwareness** - PACS event	**SecAwareness** 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)	**SecAwareness**	**SecAwareness**	**SecAwareness**	**SecAwareness**	**SecAwareness**	**SecAwareness**	**SecAwareness** (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, Netcsout-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



2019

СПАСИБО ЗА ВНИМАНИЕ!

Алексей Мальнев

Руководитель Jet CSIRT
ay.malnev@jet.su / +7 985 849-89-33