10 YEARS JETSECURITY CONFERENCE 2019

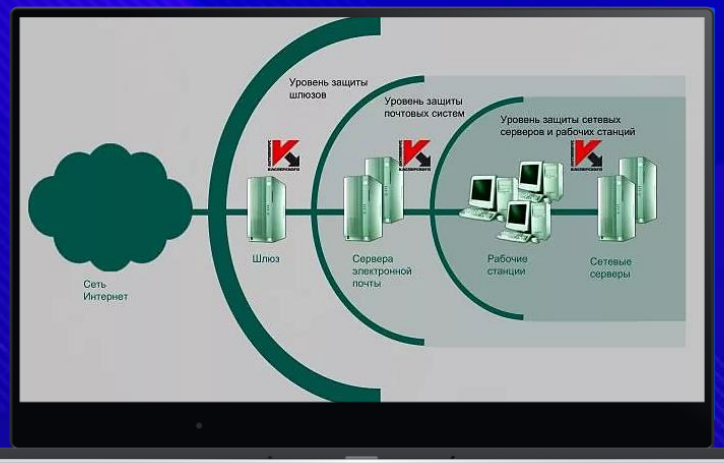
CSIRT VS человеческий фактор или можно ли бороться с социальной инженерией

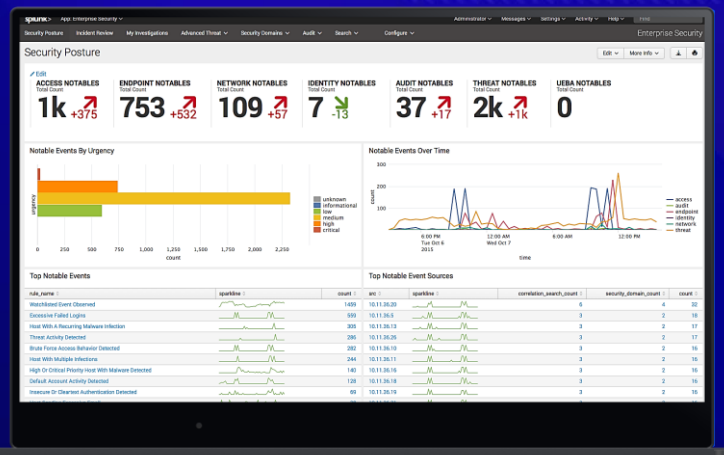
Алексей Мальнев

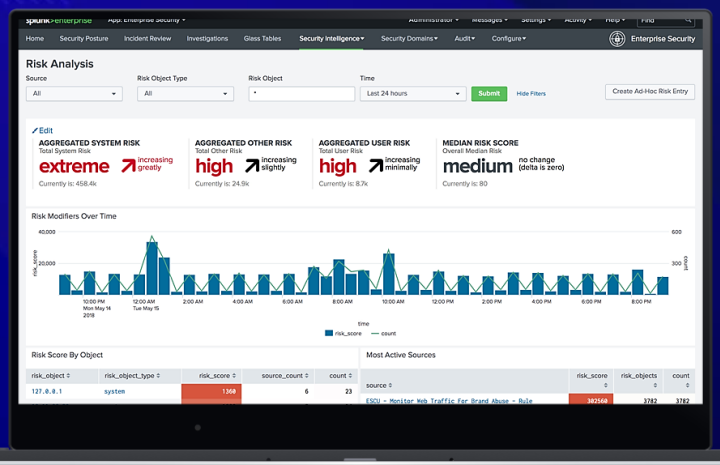
Руководитель Jet CSIRT
ay.malnev@jet.su / +7 985 849-89-33

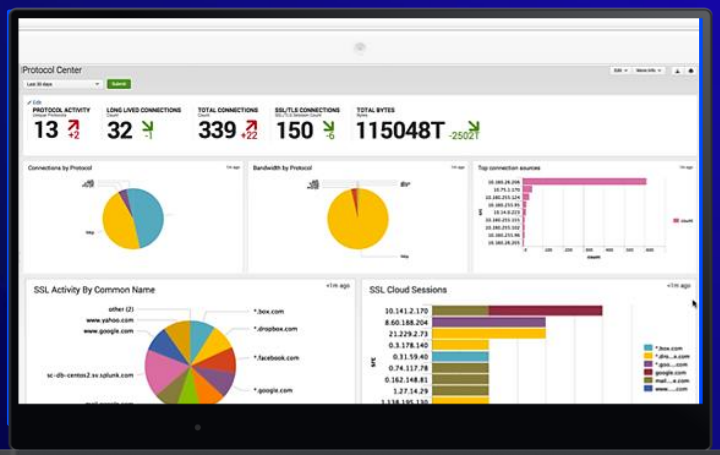
© 2019 Инфосистемы Джет

ПРЕДСТАВИМ, ЧТО МЫ НЕПЛОХО ЗАЩИТИЛИСЬ







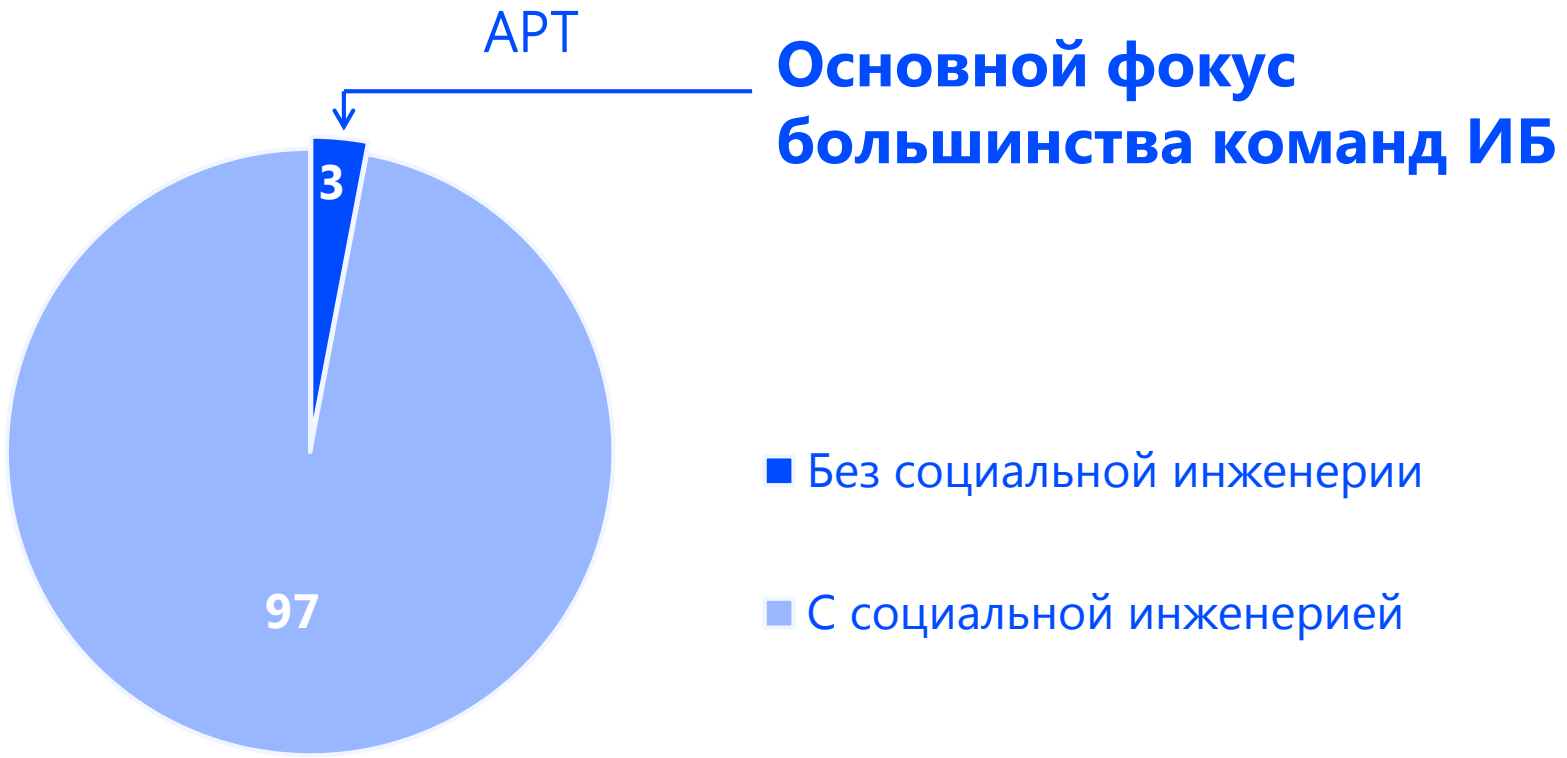


© 2019 Инфосистемы Джет

ПРЕДСТАВИМ,
ЧТО МЫ НЕПЛОХО ЗАЩИТИЛИСЬ

© 2019 Инфосистемы Джет

НА САМОМ ДЕЛЕ ВСЕ НЕ ТАК ЗДОРОВО



Основной фокус большинства команд ИБ

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ – АТАКУЮЩИЙ МЕТОД №1

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

© 2019 Инфосистемы Джет

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

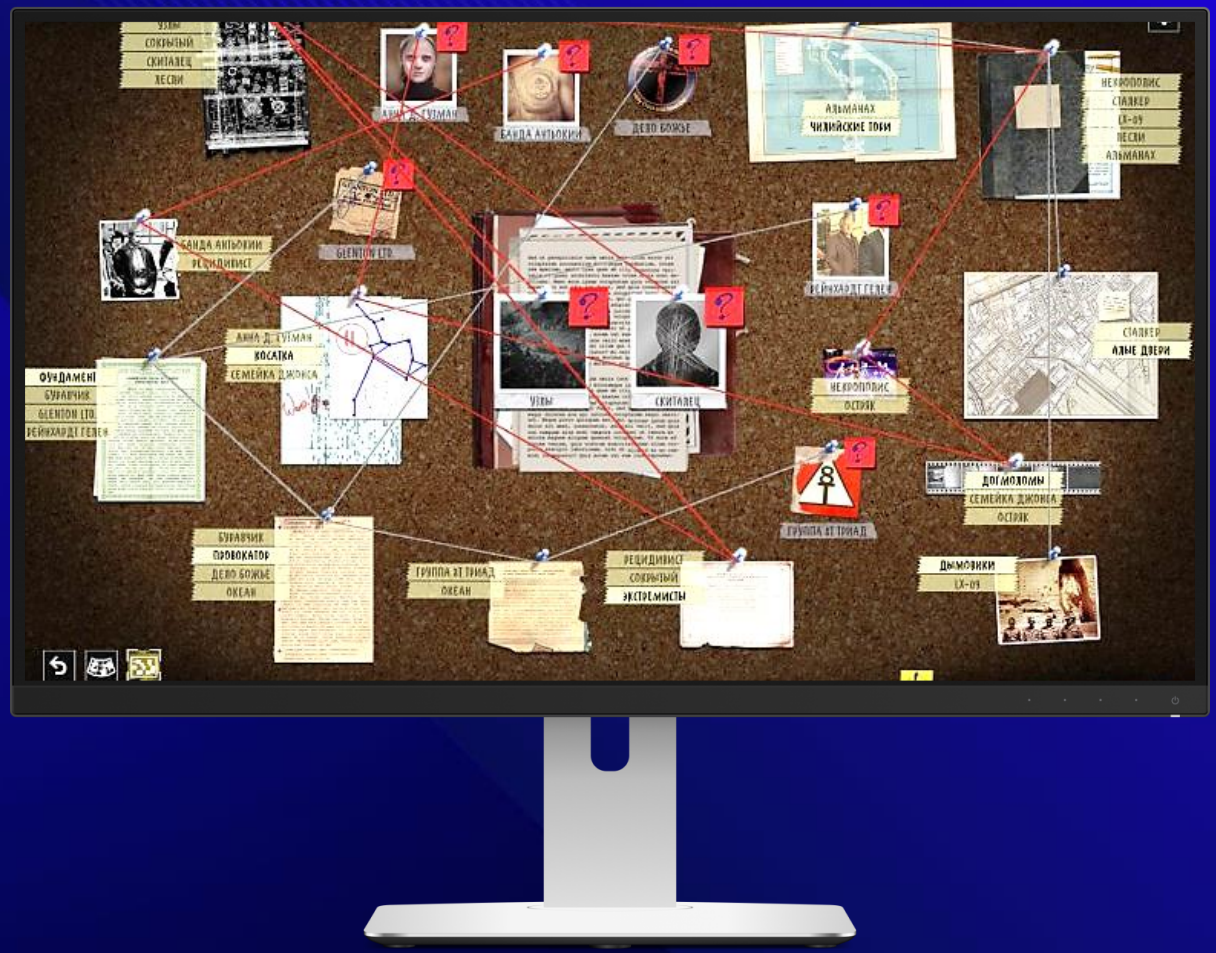
© 2019 Инфосистемы Джет

ЧЕЛОВЕК – САМОЕ СЛАБОЕ ЗВЕНО

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

© 2019 Инфосистемы Джет

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ



© 2019 Инфосистемы Джет

10 YEARS JETSECURITY CONFERENCE 2019

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Виктор Люстиг

Фрэнк Абигнейл

Артур Фергюсон

Джозеф Уэйл

Кевин Митник

Братья Бадир

© 2019 Инфосистемы Джет

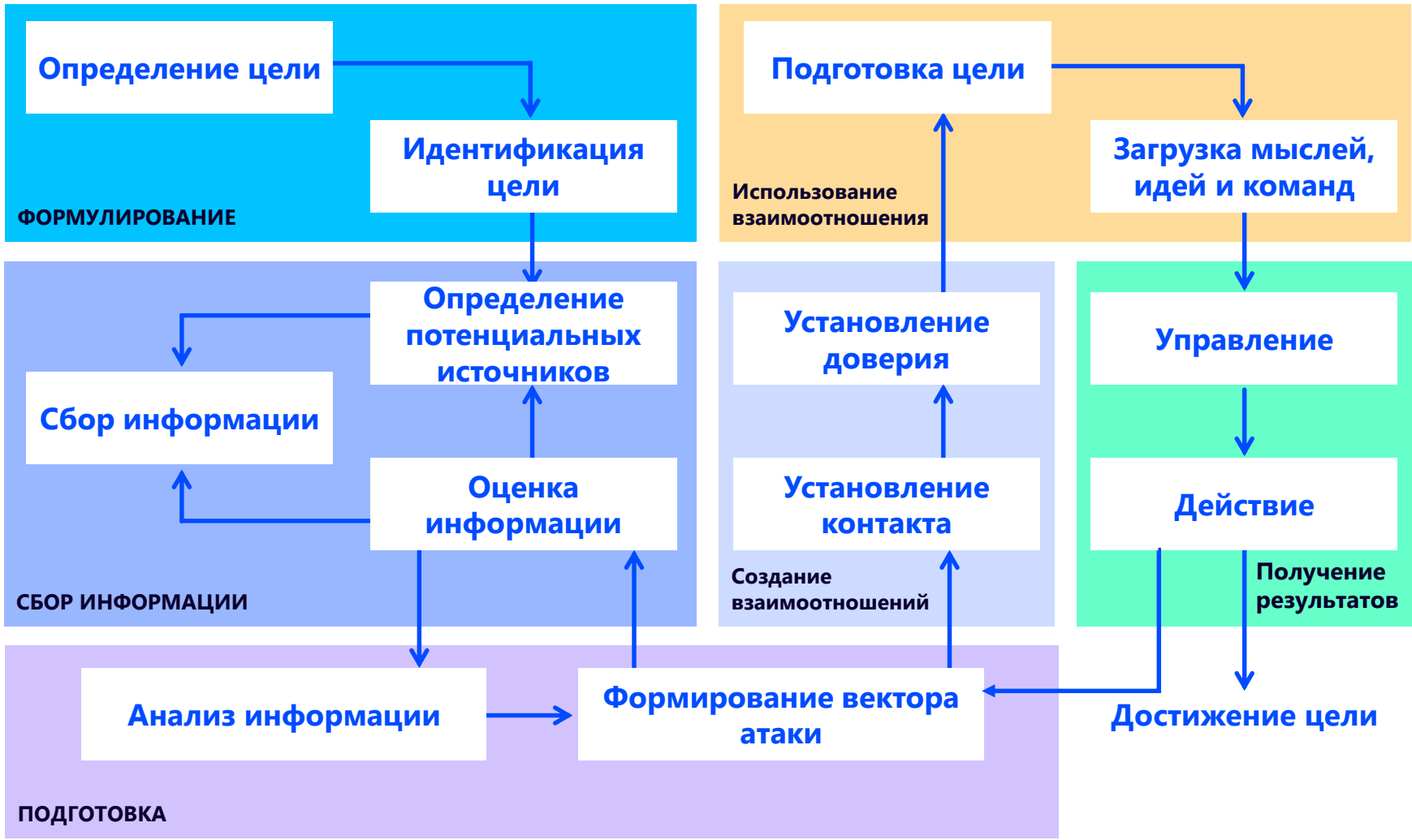
10 YEARS JETSECURITY CONFERENCE 2019

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. LIFECYCLE

© 2019 Инфосистемы Джет

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. FRAMEWORK

Social engineering roadmap



© 2019 Инфосистемы Джет

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

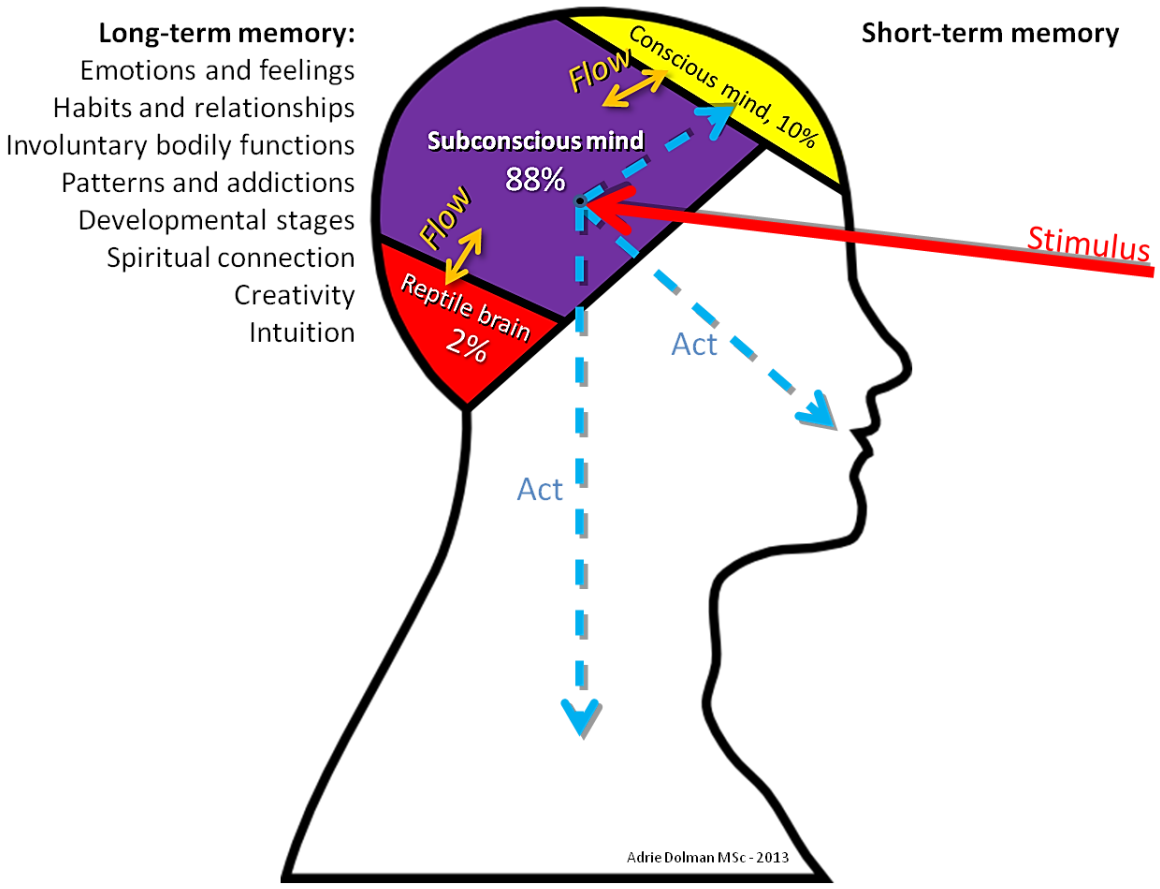
Техники влияния
услуга за услугу, подарки, уступки, искусственный дефицит, влияние авторитетом, юридическое, социальное и организационное, симпатия, последовательный переход, подмена реальности

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»

© 2019 Инфосистемы Джет

АТАКА НА СОЗНАНИЕ И ПОДСОЗНАНИЕ



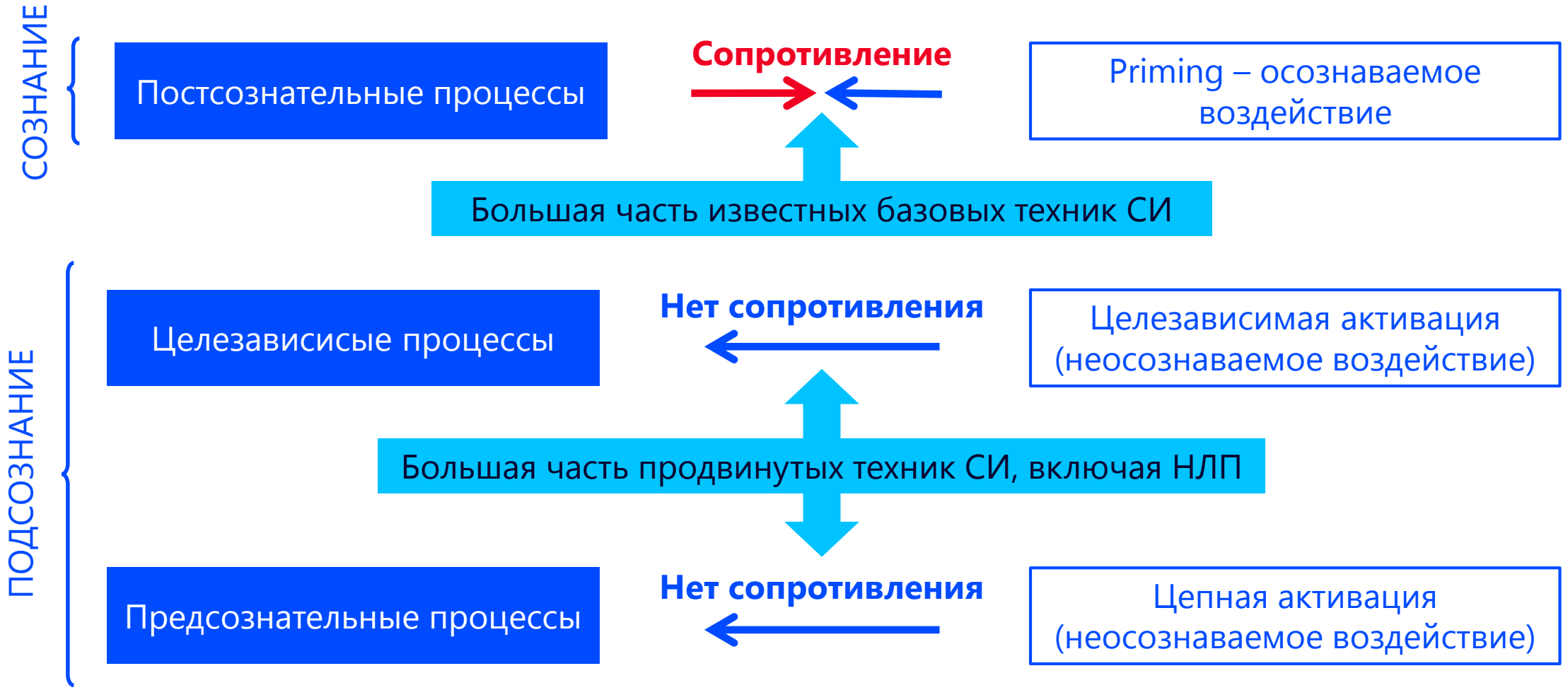
- от 95% до 99,99% вычислительной мощности мозга сосредоточены в подсознании
- Около 95% когнитивной деятельности сосредоточены в подсознании
- Сознание очень ограничено

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

© 2019 Инфосистемы Джет

ВОЗДЕЙСТВИЕ НА ПОДСОЗНАНИЕ И СОЗНАНИЕ



СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ – АТАКУЮЩИЙ МЕТОД №1

© 2019 Инфосистемы Джет

«УЯЗВИМОСТИ» МОЗГА VS УЯЗВИМОСТИ ПО

Количество состояний мозга

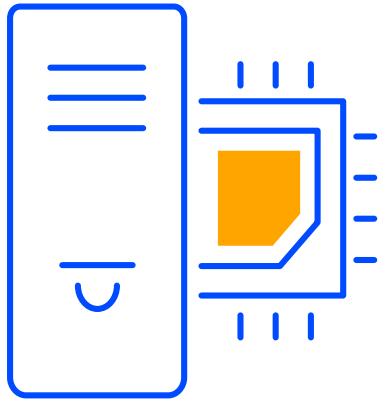
Количество нейронов и количество нейронных связей
100 млрд нейронов, 100 трлн связей
Квадриллион (1 000 000 000 000 000) байт =
1 миллион гигабайт =
1000 терабайт = 1 петабайт

> > >

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



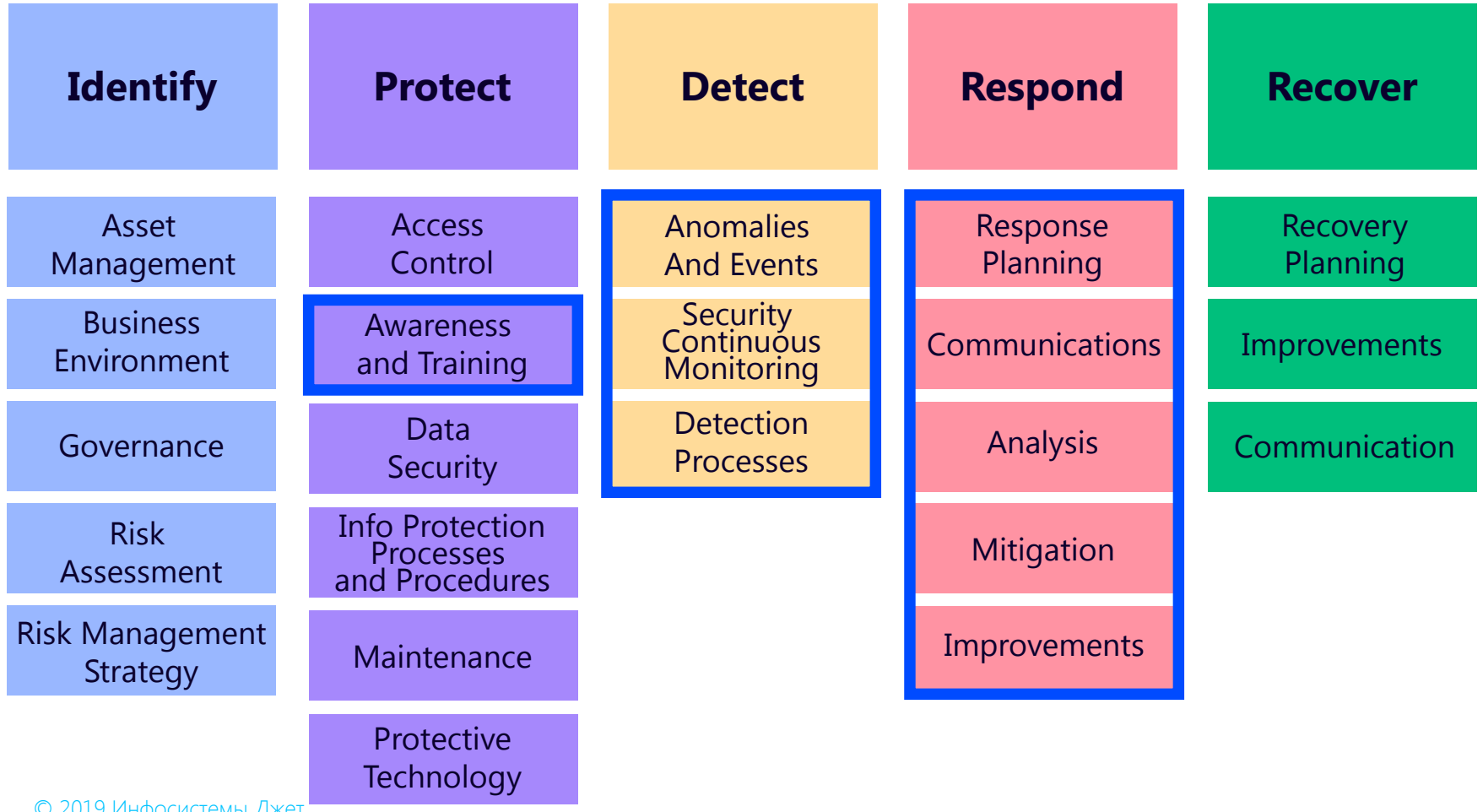
Количество памяти ограничено RAM, HDD и памяти CPU

© 2019 Инфосистемы Джет


#CSIRT/SOC VS СОЦИНЖЕНЕРИЯ

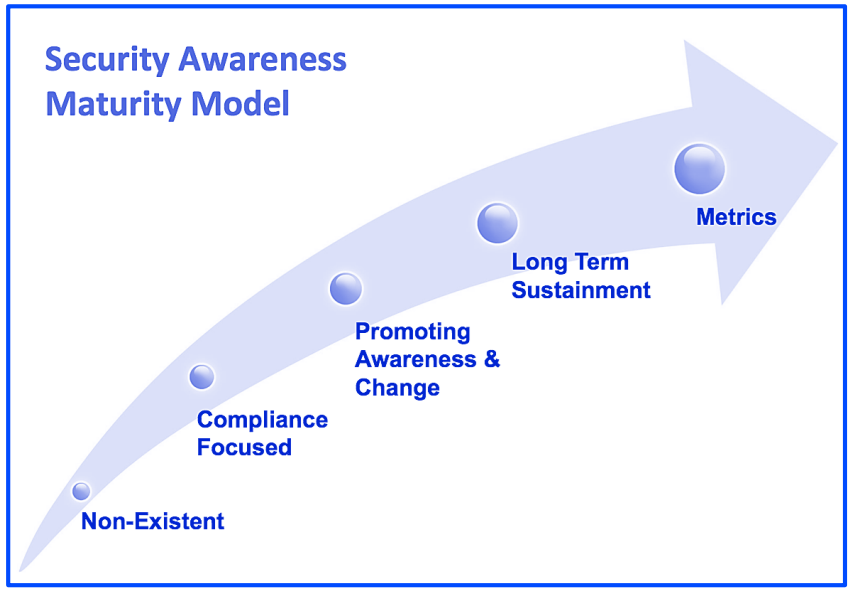
О ЧЕМ ПОЙДЕТ РЕЧЬ

NIST Cyber Security Framework



© 2019 Инфосистемы Джет

SECURITY AWARENESS VS СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

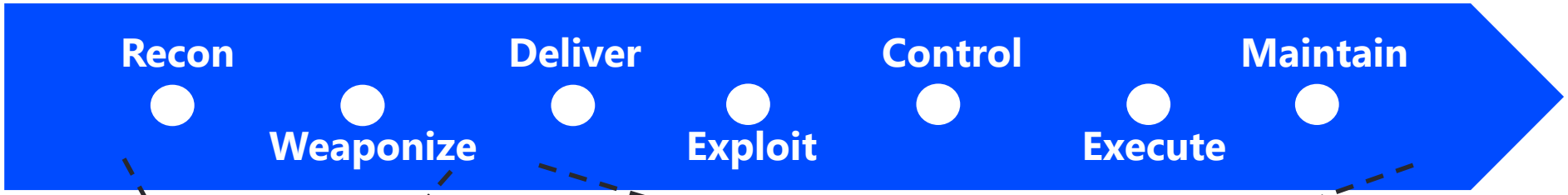


УРОВЕНЬ	SECURITY AWARENESS	СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ
1	Ничего нет	Базовые простейшие техники
2	Только для соответствия (формально)	Базовые простейшие техники
3	Есть программа	Базовые техники/сочетание с техническими векторами
4	Есть долгосрочный процесс, SA как часть культуры организации	Сложные техники/сочетание 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

© 2019 Инфосистемы Джет

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

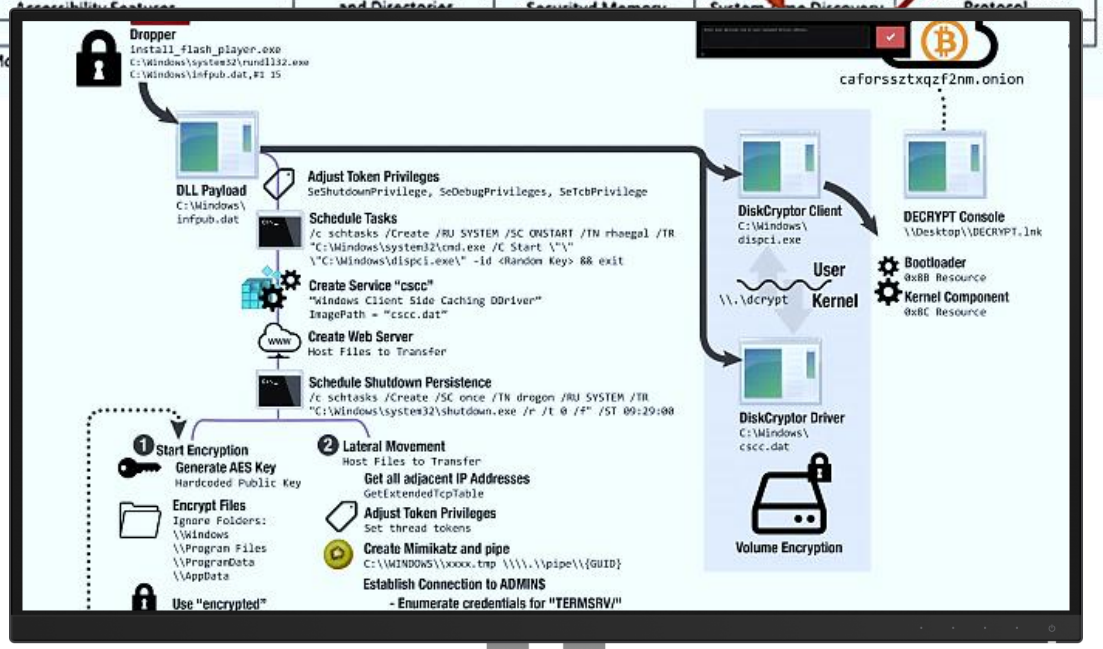
Exfiltration

Command and Control

© 2019 Инфосистемы Джет

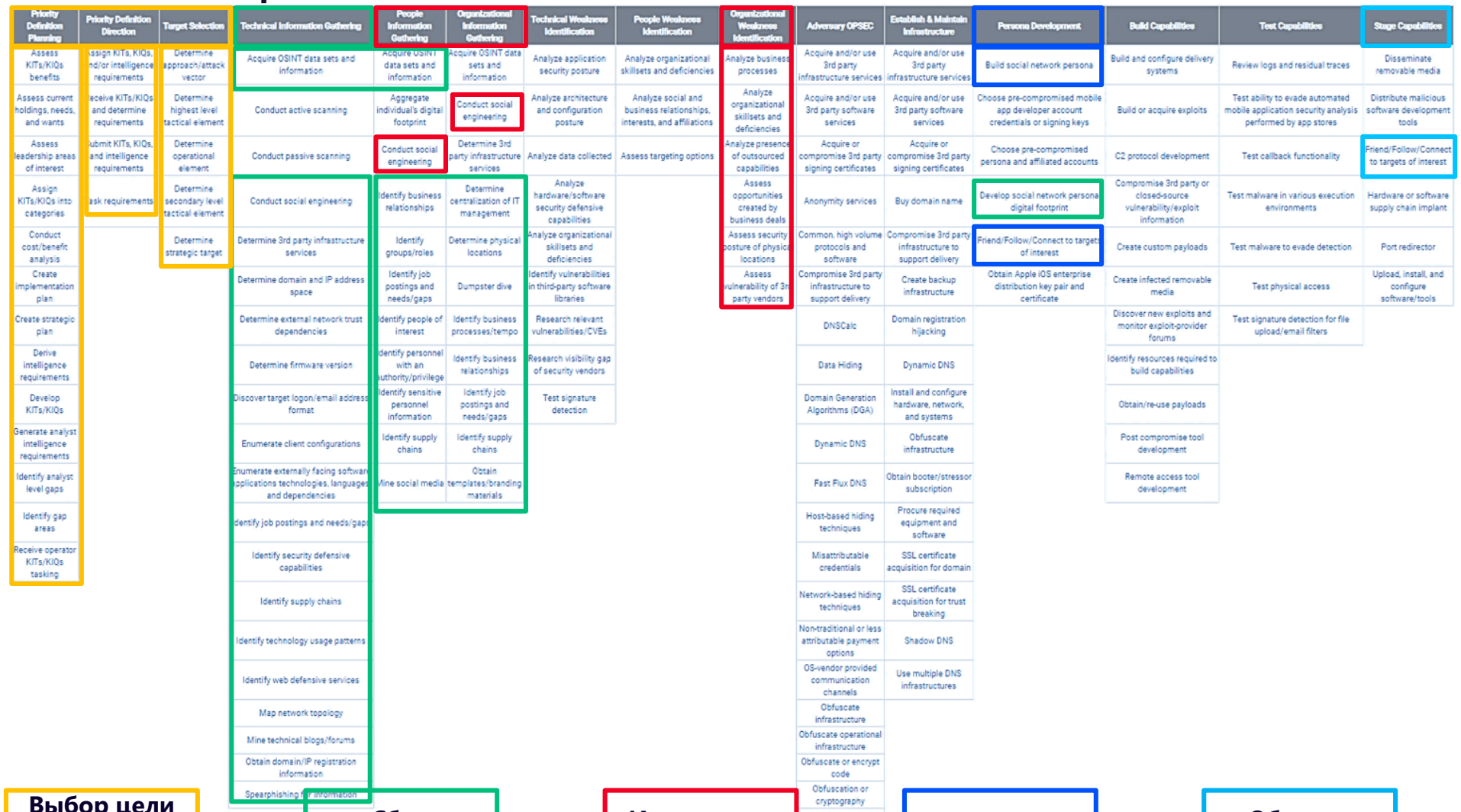
ATT&CK MITRE

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	Peripheral Device Discovery	Remote File Copy	Audio Capture		Multi-hop Proxy
Spearphishing Attachment	Trap		Bypass User Account Control		Hooking	File and Directory Discovery	Pass the Ticket	Automated Collection		Domain Fronting
Exploit Public-Facing Application	Launchctl		Process Injection		Password Filter DLL	Permission Groups 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	Process Discovery	Windows Admin Shares	Email Collection	Automated Exfiltration	Remote File Copy
Spearphishing via Service	User Execution		Plist Modification		Private Keys	System Network Configuration 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	Exfiltration Over Alternative Protocol	Web Service
Drive-by Compromise	CMSTP		DLL Search Order Hijacking		Input Prompt	System Owner/User Discovery	Shared Webroot	Input Capture	Data Transfer Size Limits	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 Compressed	Connection Proxy
	Mshta		Hooking	DCShadow	Two-Factor Authentication Interception	Application Window Discovery	Windows Remote Management	Data from Local System	Scheduled Transfer	Multilayer Encryption
	AppleScript		Startup Items	Port Knocking	Replication Through Removable Media	Password Policy Discovery	Application Deployment Software	Man in the Browser		Standard Application Layer Protocol
	Source		Launch Daemon	Indirect Command Execution	Input Capture	Remote Desktop Protocol	SSH Hijacking	Data from Removable Media		Commonly Used Port
	Space after Filename		Dylib Hijacking	BITS Jobs	Network Sniffing		AppleScript			Standard Cryptographic Protocol
	Execution through API		Application Shimming	Control Panel Items	Credential Dumping		Taint Shared Content			Custom Cryptographic Protocol
	Execution through Module Load		AppInit DLLs	CMSTP	Kerberoasting		Remote Desktop Protocol			Data Obfuscation
	Regsvcs/Regasm		Web Shell	Process Doppelgänging						Custom Command and Control Protocol
	InstallUtil		Service Registry Permissions Weakness	Mshta						Communication
	Kernel Modules		New Service	Hidden Files						
			File System Permissions Weakness							
			Path Interception							



© 2019 Инфосистемы Джет

МАТРИЦА MITRE PRE ATT&CK



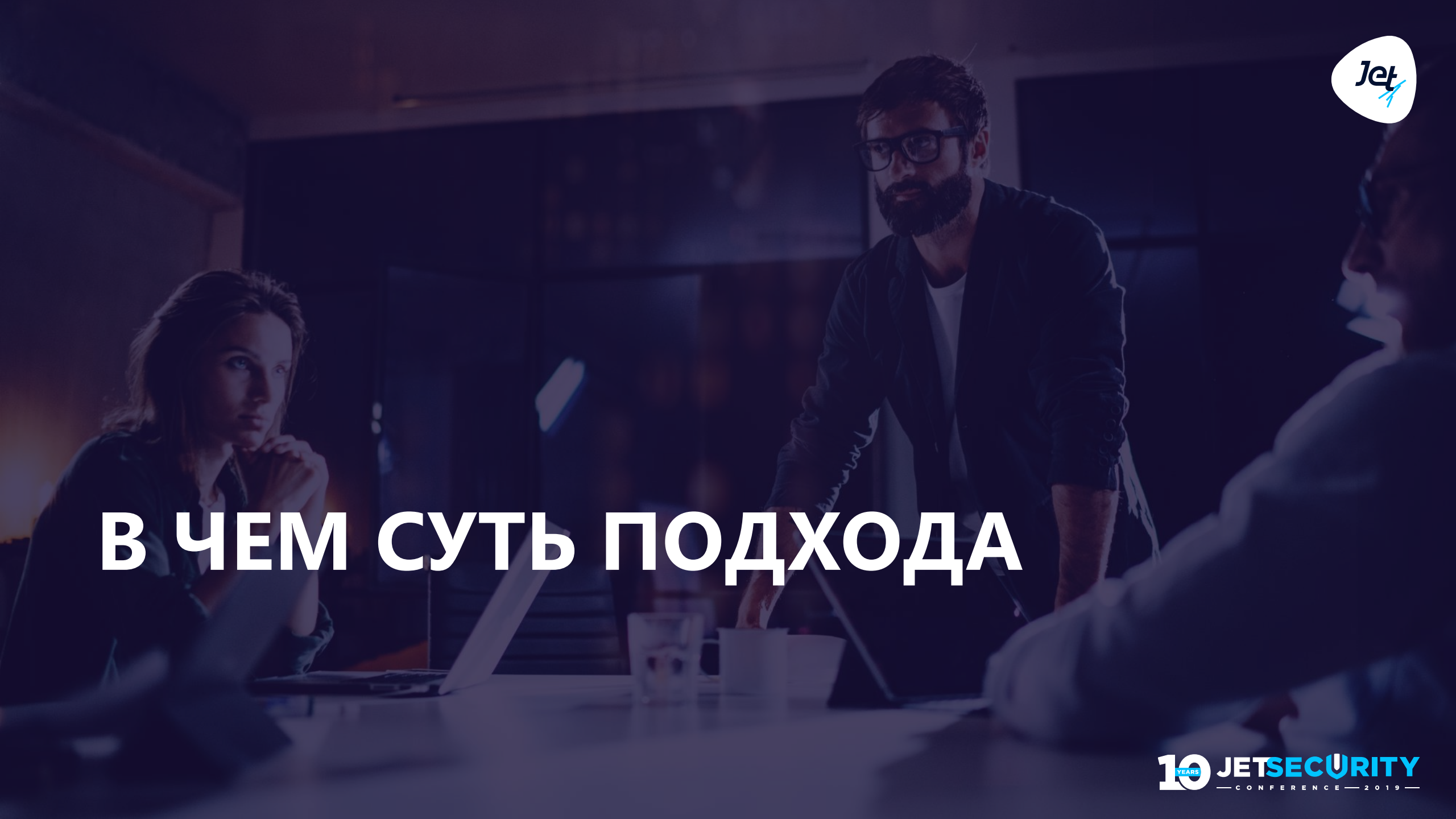
© 2019 Инфосистемы Джет

МАТРИЦА MITRE ATT&CK ENTERPRISE

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly 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	Data 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	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	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
	InstallUtil	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/NBT-NS 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		InstallUtil						
		New Service		LC_MAIN Hijacking						
		Office Application Startup		Launchctl						
		Path Interception		Masquerading						
		Plist Modification		Modify Registry						
		Port Knocking		Mshta						
		Port Monitors		NTFS File Attributes						
		Rc.common		Network Share Connection Removal						
		Re-opened Applications		Obfuscated Files or Information						
		Redundant Access		Plist Modification						
		Registry Run Keys / Startup Folder		Port Knocking						
		SIP and Trust Provider Hijacking		Process Doppelgänging						
		Scheduled Task		Process Hollowing						

Выбор цели и первичная разведка → **Сбор информации** → **Извлечение информации** → **Предлог** → **Обман и манипуляция** → **Убеждение и влияние**

© 2019 Инфосистемы Джет



В ЧЕМ СУТЬ ПОДХОДА

10 YEARS JETSECURITY CONFERENCE 2019

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	• Chaotic and relaying on individual heroic; reactive • General purpose run-book • Tribal knowledge	• Situation run books; some consistency • Email-based processes	• Requirements and workflow documented as standards business process • Some improvement over time	• Process measured via metrics • Minimal Threat Sharing • Shift turnover • SLAs	• Processes are constantly improved and optimized • Broad Threat sharing • Hunt teams
	Технологии	AV/FW/IDS	SIEM/Sandboxing	• Continuous monitoring • Endpoint forensics • Tactical Intelligence	• Malware Analysis • Additional Intelligence • IT Operation integration	• Intel+IR Drives Security Program • Strategic Intelligence • Coordination with Physical Security Intelligence
CMM Эквивалент		Initial	Repeatable	Defined	Managed	Optimized

90%

© 2019 Инфосистемы Джет

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

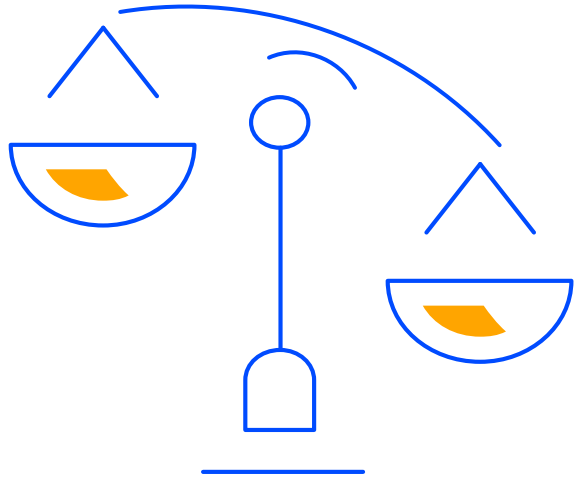
Риски при реализации

- Высокие
- Средние
- Низкие

Сложность и стоимость реализации

© 2019 Инфосистемы Джет

РИСК ЗЛОУМЫШЛЕННИКА ОПРЕДЕЛЯЕТСЯ ЦЕЛЬЮ



Деньги

Шпионаж

Дестабилизация

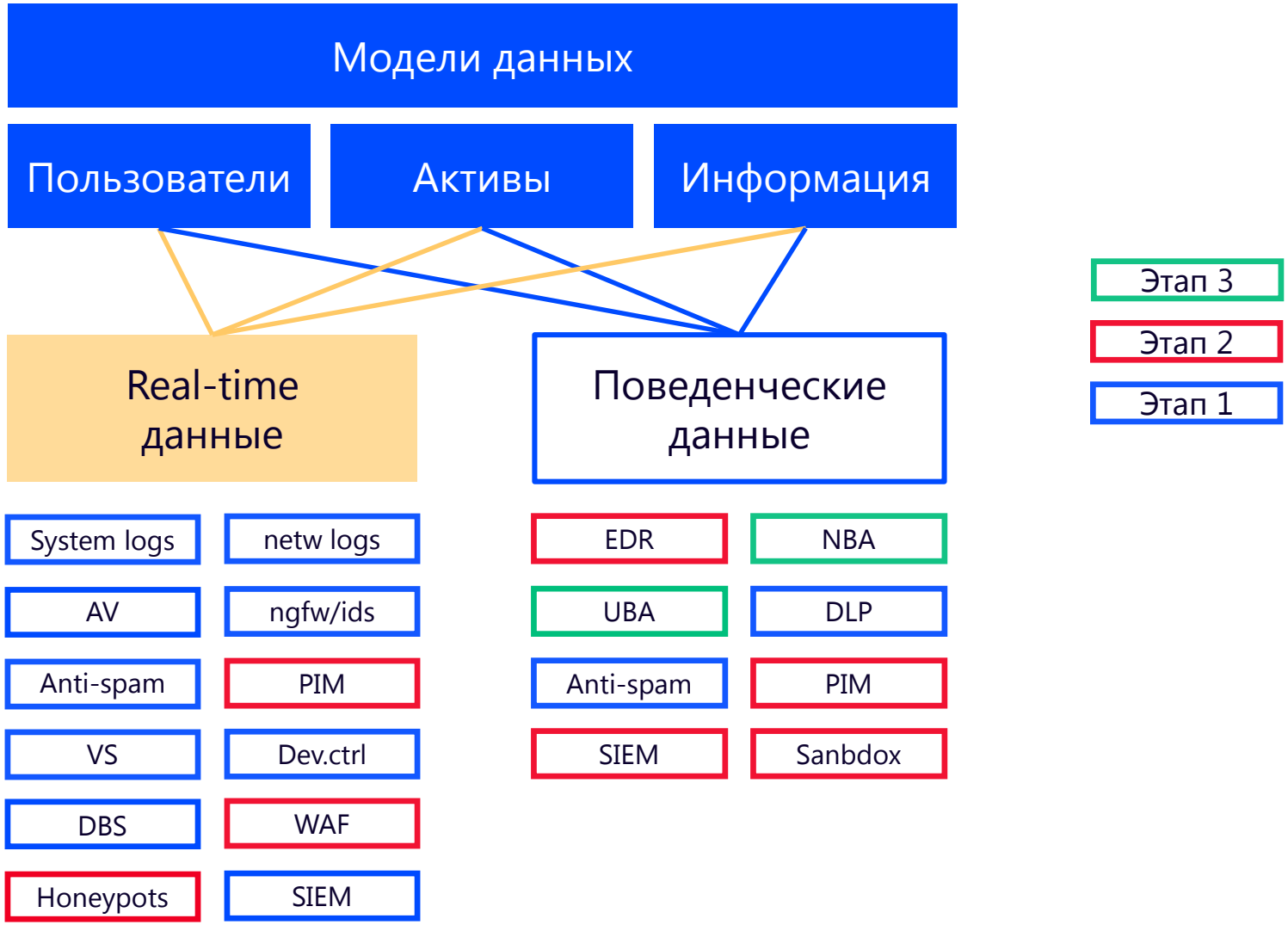
Пром.авария

© 2019 Инфосистемы Джет

ПОВЫШЕНИЕ ЗРЕЛОСТИ CSIRT/SOC

© 2019 Инфосистемы Джет

ПРИМЕР. ИСТОЧНИКИ СОБЫТИЙ



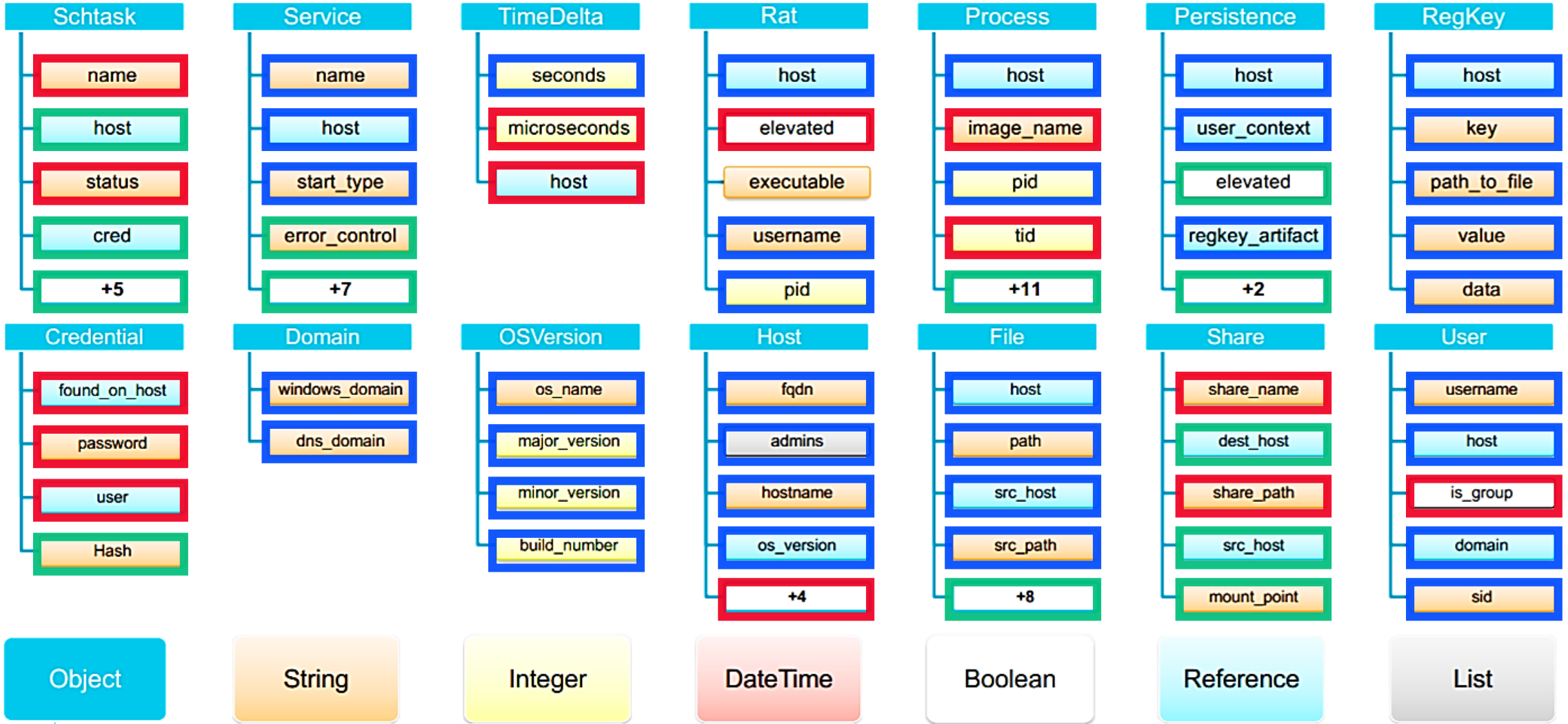
Этап 3

Этап 2

Этап 1

© 2019 Инфосистемы Джет

ПРИМЕР. МОДЕЛЬ АКТИВОВ. СОБИРАЕМЫЙ КОНТЕКСТ



Этап 1 Этап 2 Этап 3

© 2019 Инфосистемы Джет

ПОВЫШЕНИЕ ЗРЕЛОСТИ МОНИТОРИНГА ИНЦИДЕНТОВ

Следующий уровень зрелости

© 2019 Инфосистемы Джет

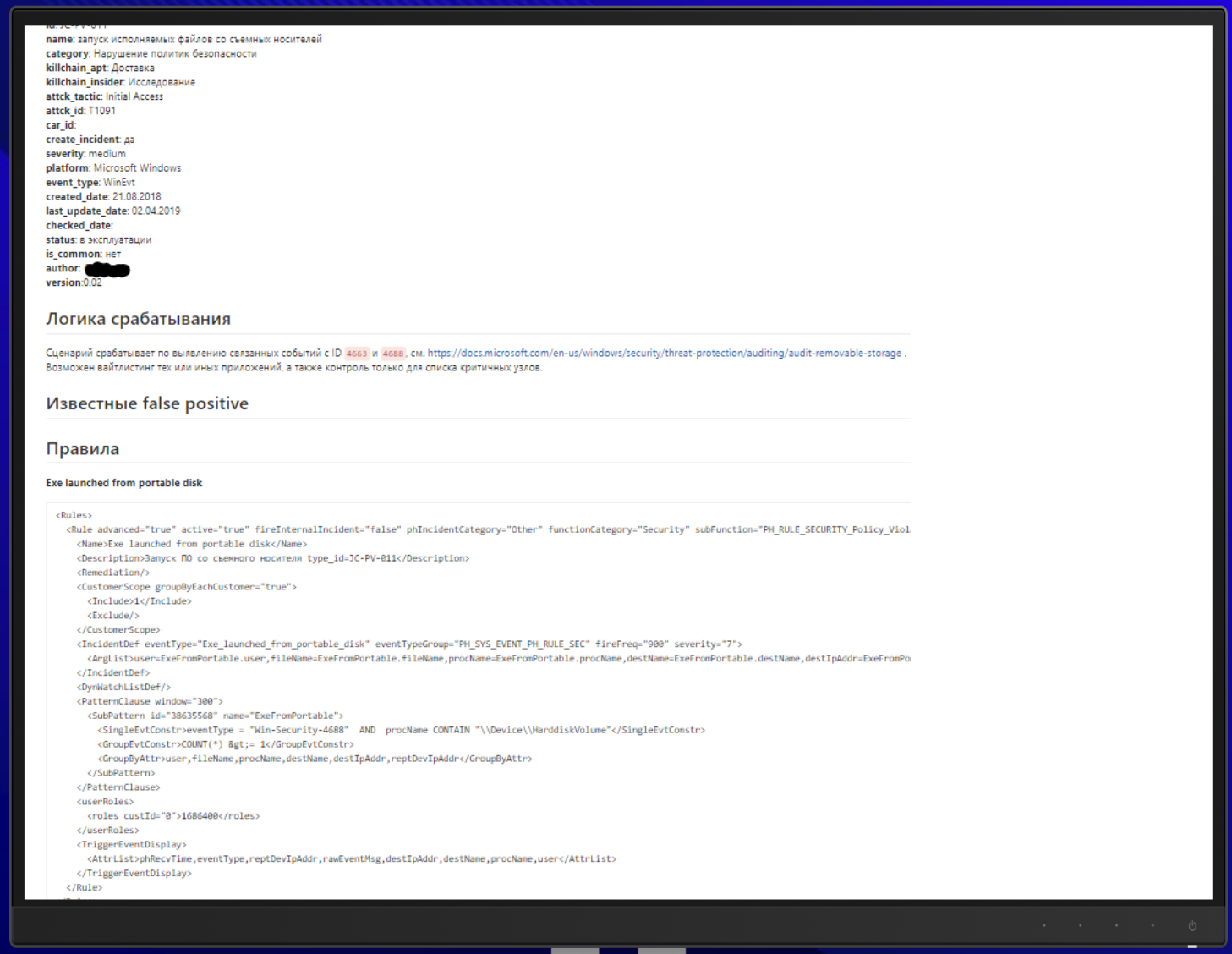
ДОПОЛНИТЕЛЬНЫЙ ФОКУС НА МАРКЕРАХ СОЦИНЖЕНЕРИИ

Прямые сценарии по техвекторам SE:

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

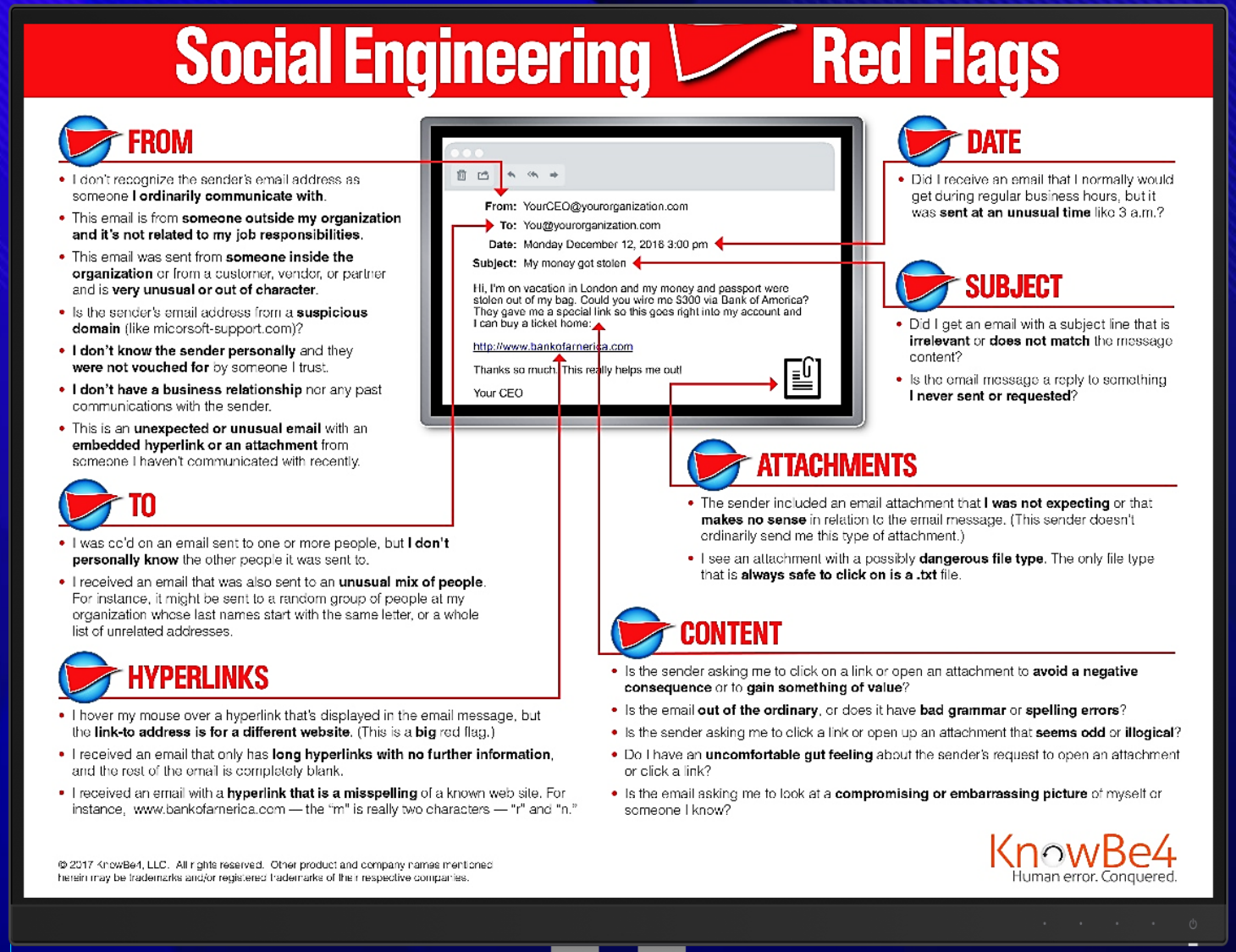
Косвенные сценарии SE:

- DLP сценарии
- UBA сценарии
- TBA сценарии



© 2019 Инфосистемы Джет

ДОПОЛНИТЕЛЬНЫЙ ФОКУС НА МАРКЕРАХ СОЦИНЖЕНЕРИИ



10 YEARS JETSECURITY CONFERENCE 2019

10 YEARS JETSECURITY CONFERENCE 2019

СПАСИБО ЗА ВНИМАНИЕ!

Алексей Мальнев

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

© 2019 Инфосистемы Джет