

VB-Trend 2020

 Search  nywhere

SMART Monitor for MITRE ATT&CK

VB-Trend 2020



Search @nywhere



MITRE ATT&CK

ATT&CK (Adversary Technique, Tactic & Common Knowledge)

публичная база знаний, содержащая структурированный набор тактик и техник поведения злоумышленников во внутренней сети организации



ATT&CK[®]

TTPs (Tactics, Techniques and Procedures)

Поведение злоумышленника - что делает злоумышленник для достижения своей цели

Концепция и предпосылки

Поведение злоумышленника

- Фокус на поведении злоумышленников. Типовые индикаторы угроз (IP, hash, domain, registry keys) могут легко изменяться злоумышленниками, полезны только для обнаружения и не дают понимания, как именно злоумышленники взаимодействуют с системами

Существующие концепции жизненного цикла не подходят

- Существующие концепции жизненного цикла (например, Cyber Kill Chain) слишком высокоуровневые для связки поведения и защитных механизмов

Применимость в реальных инфраструктурах

- Техники, тактики и процедуры должны базироваться на основе наблюдаемых, совершенных атак, чтобы быть применимыми к реальной среде

Единая терминология

- Должна быть систематизирована терминология в части описания TTP, используемых разными группами злоумышленников

Термины и объекты: Тактики

Tactics

Тактическая цель, которую преследует злоумышленник: причина совершения действий



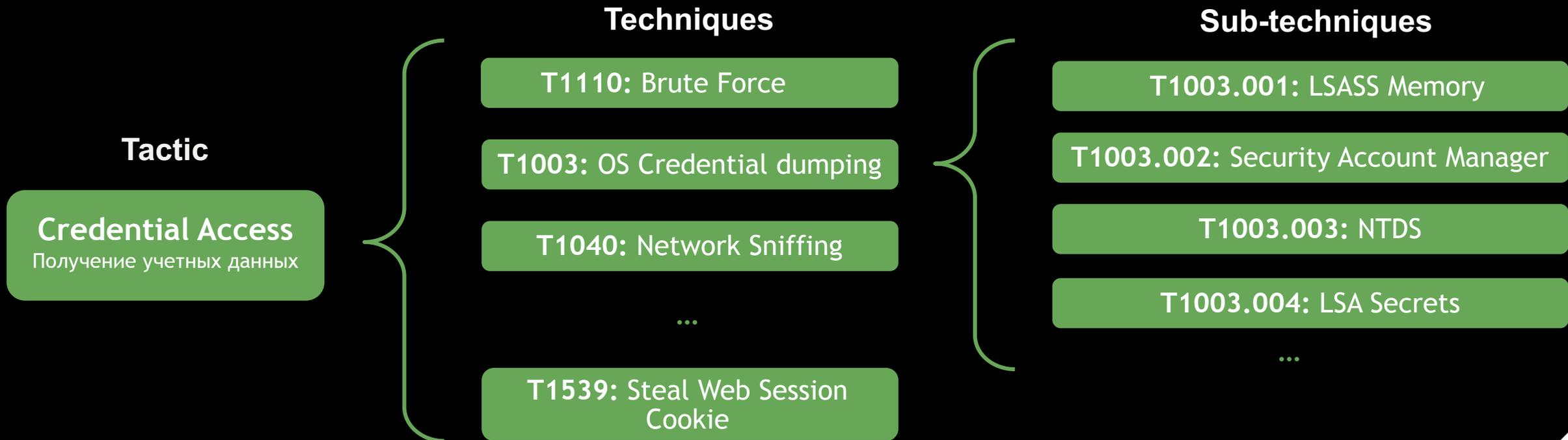
Термины и объекты : Техники

Techniques

Действия, предпринимаемые злоумышленником для достижения определенной цели (тактики)

Sub-techniques

Детализация действий (техники) злоумышленника для выравнивания уровня абстракции техник



Groups, Procedure, Software, Mitigations

Groups

Известные группы злоумышленников, совершающие целевые кибератаки, о которых сообщается в отчетах об угрозах (*APT29, Cobalt Group, Lazarus Group, ...*)

Procedure

Конкретные имплементации техник, применяемые группами злоумышленников (*APT29 добавляет Registry Run keys для достижения присутствия - T1547.001*)

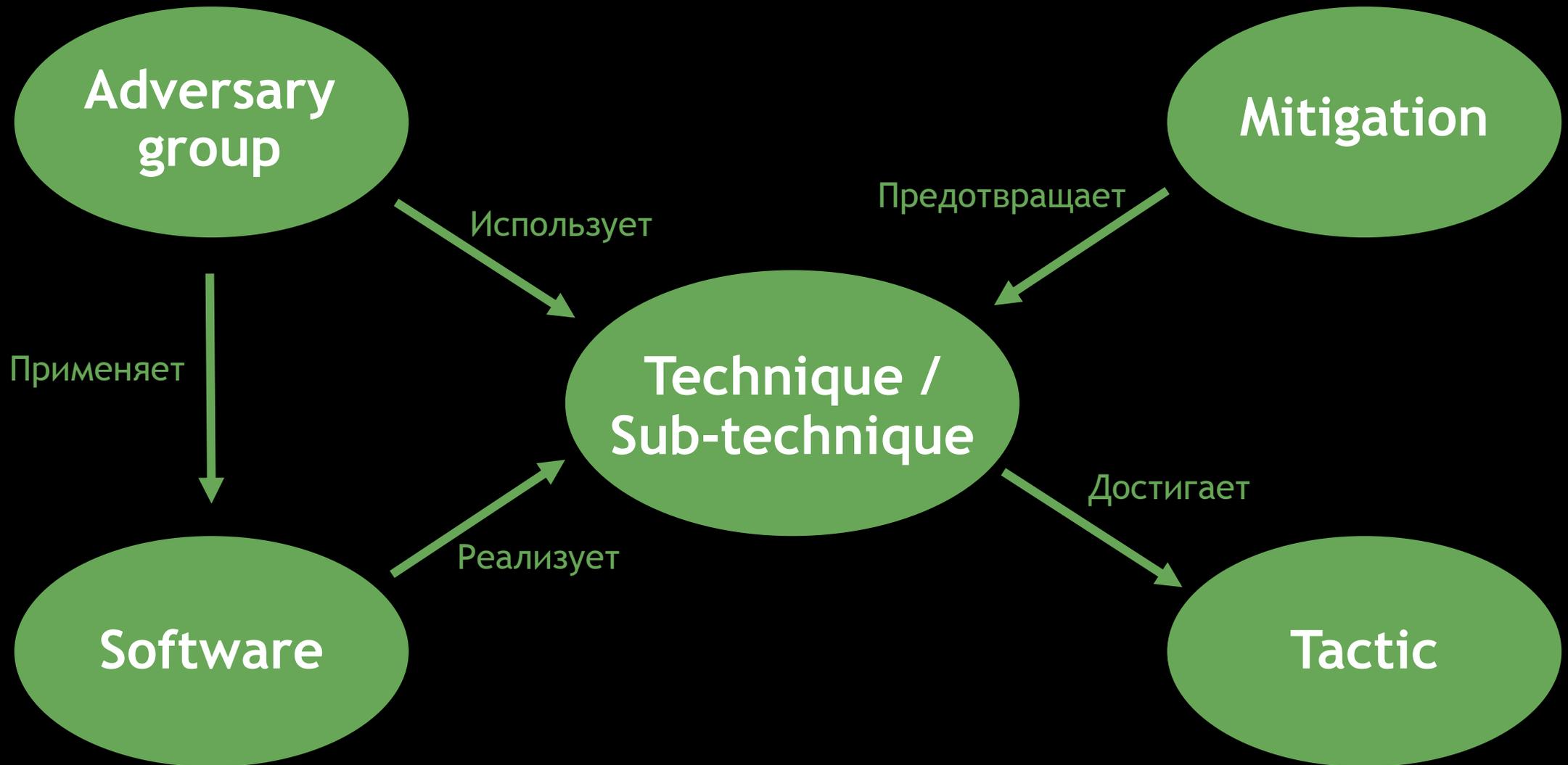
Software

Утилиты и вредоносное программное обеспечение используемые злоумышленниками при кибератаках (*Proxysvc - вредоносная DLL используемая Lazarus Group*)

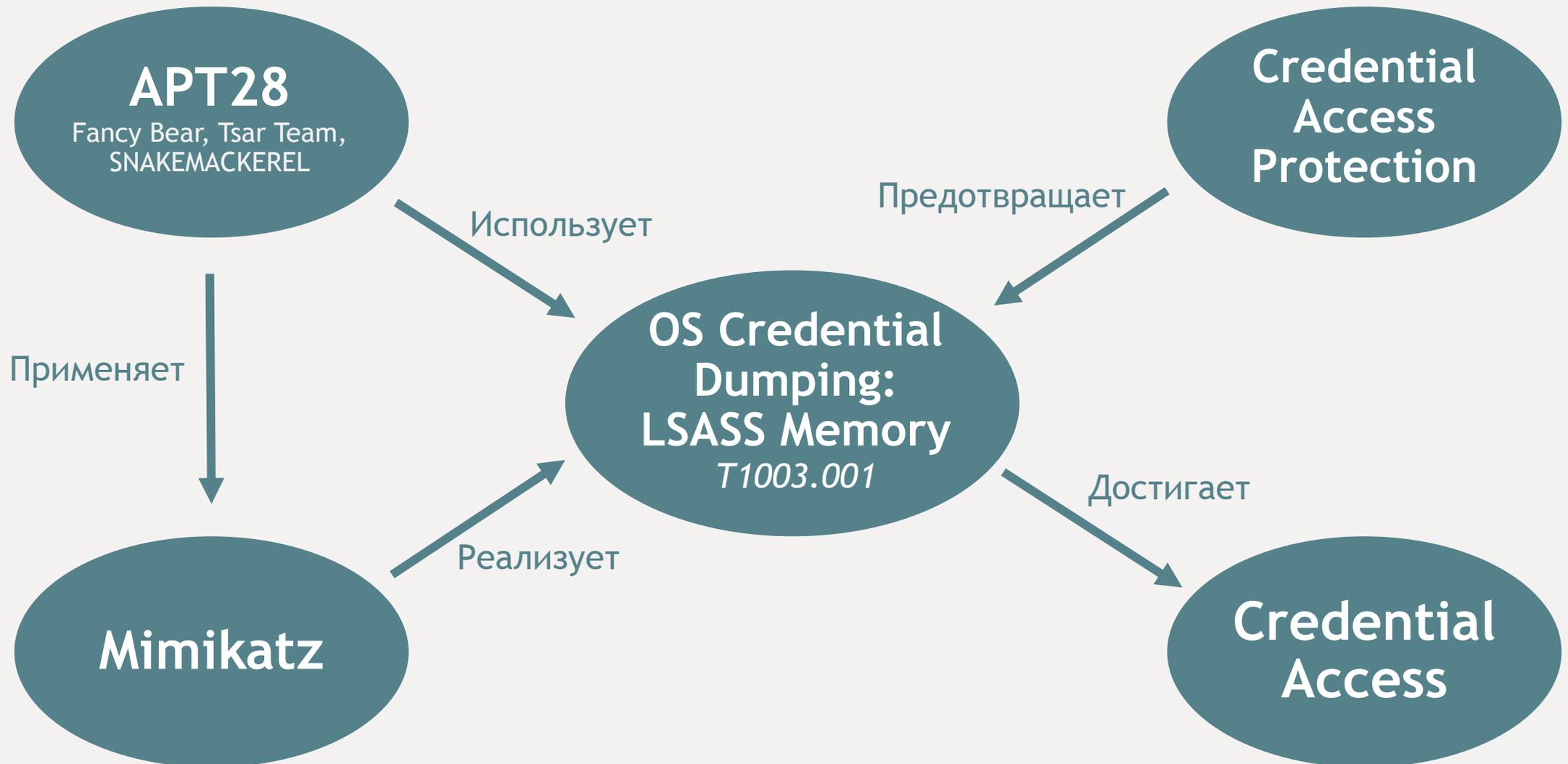
Mitigations

Способы и средства усложняющие или предотвращающие возможность использования техник

Взаимосвязь объектов модели ATT&CK



Взаимосвязь объектов модели ATT&CK



Матрицы MITRE ATT&CK

Отношения между тактиками и техниками обычно представляется в виде матриц

Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 34 techniques	Credential Access 14 techniques	Discovery 23 techniques	Lateral Movement 9 techniques	Collection 16 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing Replication Through Removable Media Supply Chain Compromise Trusted Relationship Valid Accounts	Command and Scripting Interpreter Exploitation for Client Execution Inter-Process Communication Native API Scheduled Task/Job Shared Modules Software Deployment Tools System Services User Execution Windows Management Instrumentation	Resonance Manipulation BITS Jobs Boot or Logon Autostart Execution Boot or Logon Initialization Scripts Browser Extensions Compromise Client Software Binary Create Account Create or Modify System Process Event Triggered Execution Group Policy Modification Hijack Execution Flow Process Injection Scheduled Task/Job Valid Accounts	Abuse Elevation Control Mechanism Access Token Manipulation BITS Jobs Boot or Logon Autostart Execution Boot or Logon Initialization Scripts Create or Modify System Process Event Triggered Execution Exploitation for Privilege Escalation Group Policy Modification Hijack Execution Flow Process Injection Scheduled Task/Job Valid Accounts	Abuse Elevation Control Mechanism Access Token Manipulation BITS Jobs Deobfuscate/Decode Files or Information Direct Volume Access Execution Guardrails Exploitation for Defense Evasion File and Directory Permissions Modification Group Policy Modification Hide Artifacts Hijack Execution Flow Impair Defenses Indicator Removal on Host Indirect Command Execution Masquerading Modify Authentication Process Modify Registry Obfuscated Files or Information Pre-OS Boot Process Injection Revert Cloud Instance Rogue Domain Controller Rootkit Signed Binary Proxy Execution Signed Script Proxy Execution Subvert Trust Controls Template Injection Traffic Signaling Trusted Developer Utilities Proxy Execution Unused/Unsupported Cloud Regions Use Alternate Authentication Material Valid Accounts Virtualization/Sandbox Evasion	Brute Force Credentials from Password Stores Exploitation for Credential Access Forced Authentication Input Capture Man-in-the-Middle Modify Authentication Process OS Credential Dumping Real Application Access Token Steal or Forge Kerberos Tickets Real Web Session Cookie Two-Factor Authentication Interception Unsecured Credentials Use Alternate Authentication Material Valid Accounts	Account Discovery Application Window Discovery Browser Bookmark Discovery Cloud Service Dashboard Man-in-the-Middle Modify Authentication Process Network Sniffing OS Credential Dumping Network Service Scanning Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Permission Groups Discovery Process Discovery Query Registry Remote System Discovery Software Discovery System Information Discovery System Network Configuration Discovery System Network Connections Discovery System Owner/User Discovery System Service Discovery System Time Discovery	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking Remote Services Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material Network Sniffing Password Policy Discovery Peripheral Device Discovery Permission Groups Discovery Process Discovery Query Registry Remote System Discovery Software Discovery System Information Discovery System Network Configuration Discovery System Network Connections Discovery System Owner/User Discovery System Service Discovery System Time Discovery	Archive Collected Data Audio Capture Automated Collection Clipboard Data Data from Cloud Storage Object Data from Information Repositories Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged Email Collection Input Capture Man in the Browser Man-in-the-Middle Screen Capture Video Capture	Application Layer Protocol Communication Through Removable Media Data Encoding Data Obfuscation Dynamic Resolution Encrypted Channel Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Proxy Remote Access Software Traffic Signaling Web Service	Automated Exfiltration Data Transfer Size Limits Exfiltration Over Alternative Protocol Exfiltration Over C2 Channel Exfiltration Over Other Network Medium Exfiltration Over Physical Medium Exfiltration Over Web Service Scheduled Transfer Transfer Data to Cloud Account	Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation Defacement Disk Wipe Endpoint Denial of Service Firmware Corruption Inhibit System Recovery Network Denial of Service Network Denial of Service Resource Hijacking Service Stop System Shutdown/Reboot

← Тактики

- PRE-ATT&CK Matrix
- Enterprise Matrix
- Mobile Matrices
- ATT&CK® for Industrial Control Systems

→ Техники

SM & MITRE ATT&CK



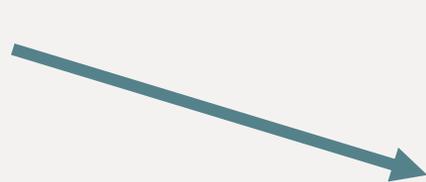
TAXII Server

или



enterprise-attack.json

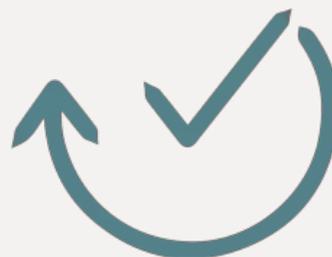
<https://github.com/mitre/cti/blob/master/enterprise-attack/enterprise-attack.json>



stix2



SM for
MITRE ATT&CK



Инициализация/
обновление

Команды SPL:

- | `gettactics`
- | `gettechniques`
- | `getsubtechniques`
- | `getgroupsandprocedures`
- | `getmitigations`
- | `getsoftware`



Threat Intelligence

Threat Intelligence

Layer: VB-Trend 2020 ×
 Tactics: All ×
 Data Sources: All ×
 Platforms: All ×
 Technique ID: All ×
 Technique Name: * Hide F

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	
Phishing	Command and Scripting Interpreter	Boot or Logon	Boot or Logon	Process Injection	Brute Force	Network Sniffing	Remote Services	Archive	
Valid Accounts		Autostart Execution	Autostart Execution	Impair Defenses		Network Sniffing	Permission Groups Discovery	Internal Spearphishing	Collected Data
Hardware Additions	Scheduled Task/Job	Create Account	Event Triggered Execution	Indirect Command Execution	OS Credential Dumping	Process Discovery	Remote Service Session Hijacking	Input Capture	
Drive-by Compromise	System Services	Event Triggered Execution	Process Injection	Masquerading		/etc/passwd and /etc/shadow	Account Discovery	Use Alternate Authentication Material	Data Staged
Exploit Public-Facing Application	Exploitation for Client Execution	Scheduled Task/Job	Scheduled Task/Job	Modify Registry		Cached Domain Credentials	Domain Trust Discovery	Lateral Tool Transfer	Email Collection
External Remote Services	Inter-Process Communication	Valid Accounts	Valid Accounts	Use Alternate Authentication Material		DCSync	File and Directory Discovery	Exploitation of Remote Services	Audio Capture
Replication Through Removable Media	Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Valid Accounts		LSA Secrets	Network Share Discovery	Replication Through Removable Media	Automated Collection
Supply Chain Compromise	Shared Modules	Account Manipulation	Group Policy Modification	Group Policy Modification		LSASS Memory	Remote System Discovery	Software Deployment Tools	Clipboard Data
Trusted Relationship	Software Deployment Tools	BITS Jobs	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism		NTDS	Software Discovery	Software Deployment Tools	Data from Cloud Storage Object
	User Execution	Browser Extensions	Access Token Manipulation	Access Token Manipulation		Proc Filesystem	Application Window Discovery	Taint Shared Content	Data from Information Repositories
	Windows Management Instrumentation	Compromise Client Software Binary	Access Token Manipulation	Access Token Manipulation		Security Account Manager	Password Policy Discovery		Data from Local System
		Create or Modify System Process	Create or Modify System Process	BITS Jobs		Input Capture	System Information Discovery		Data from Network Shared Drive
		External Remote	Exploitation for Privilege Escalation	Deobfuscate/Decode Files or Information	Unsecured Credentials			Data from	
				Direct Volume Access	Credentials from Password Stores				
					Exploitation for Credential Access				
					Forced Authentication				
					Man-in-the-Middle				

Threat Intelligence

ДЕМОНСТРАЦИЯ



SMART Monitor for
MITRE ATT&CK

Threat Intelligence

Интерфейс в виде интерактивной матрицы с наборами фильтров

Поддержка «слоев» для анализа в разных разрезах

Инструменты для анализа угроз в разрезе групп злоумышленников, источников данных, платформ

Доступ к информации из базы знаний непосредственно из интерфейса

История изменений приоритетов техник

Поддержка актуального состояния базы



SMART Monitor for
MITRE ATT&CK

Detection

Выявление действий злоумышленников

Использование собранных журналов событий для последующего анализа и выявления подозрительных действий

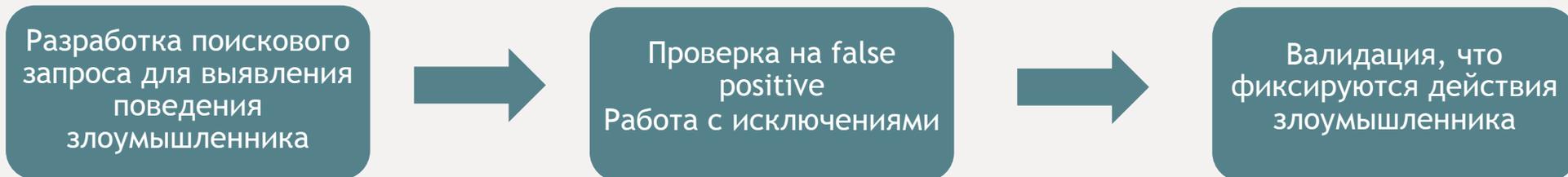
Для выбранных техник анализ источников данных, необходимых для детектирования

Поиск на основе готовой аналитики ([MITRE Cyber Analytics Repository](#), [Sigma](#), и др.)

Поиск на основе отчетов ранее зафиксированных в организации атак

Формирование правил детектирования использования техник

Работа с исключениями для разрешенного поведения



Detection: Risk scoring



Правила, которые базируются на детектировании процедур отдельных техник, содержат **недостаточно контекста** и работа по ним **неэффективно** расходует время аналитика

Цели Risk Scoring

- Повышение точности алертинга

- Привязка к объектам инфраструктуры и пользователям

- Дополнительный контекст в срабатываниях

- Повышение эффективности использования времени аналитика

- ”Плавность” масштабирования: больше правил \neq больше времени аналитика

Detection: Risk Scoring

Типы объектов Risk Scoring:

- Пользователь
- Система (IP, host)



- Превышение порога Risk Score
- Детектирование техник из различных тактик
- Большое число уникальных техник
- Внезапное увеличение количества техник
- Срабатывание правил, базирующихся на различных источниках данных

Анализ рисков в разных временных окнах, например: 24 часа, 7 дней, 30 дней

Adversary Emulation

Эмуляция действий злоумышленников

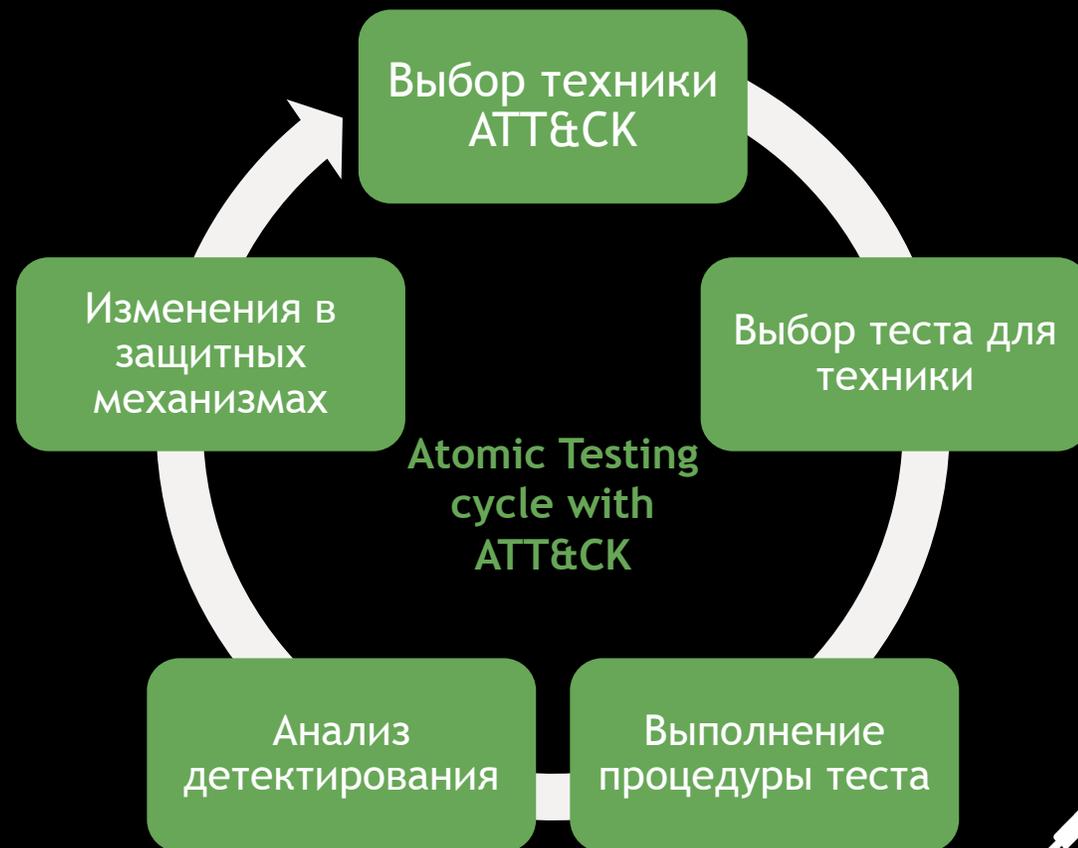
Эмуляция действий злоумышленника для анализа известной угрозы

Проверка, как действует защита против эмулированного поведения злоумышленника

На основе данных о процедурах из базы АТТ&СК и отчетах об атаках, собственного опыта отраженных атак

С использованием библиотеки тестов [Atomic Red Team](#)

Использование [CALDERA](#) (автоматизированная система эмуляции действий злоумышленников)



Adversary Emulation

Эмуляция действий злоумышленников

Пример сценария CALDERA

Discovery

Defense Evasion

Impact

Credential Access

Collection

1 **Current User** ✕
DISCOVERY | SYSTEM OWNER/USER DISCO...
 

3 **Disable Microsoft Defender Firewall** ✕
DEFENSE-EVASION | IMPAIR DEFENSES: DIS...
 

4 **Windows - Stop service using net.exe** ✕
IMPACT | SERVICE STOP
 

5 **Dump LSASS.exe Memory using ProcDump** ✕
CREDENTIAL-ACCESS | OS CREDENTIAL DU...
 

8 **Compress Data for Exfiltration With PowerShell** ✕
COLLECTION | ARCHIVE COLLECTED DATA
 

2 **Enumerate all accounts (Domain)** ✕
DISCOVERY | ACCOUNT DISCOVERY: DOM...
 

6 **Registry parse with pypykatz** ✕
CREDENTIAL-ACCESS | OS CREDENTIAL DU...
 

7 **Dumping LSA Secrets** ✕
CREDENTIAL-ACCESS | OS CREDENTIAL DU...
 

Detection & Emulation

ДЕМОНСТРАЦИЯ



SMART Monitor for
MITRE ATT&CK

Detection

Инструменты для создания правил с дополнительными метаданными для привязки к техникам, тактикам, источникам данных и др.

Базовый набор правил детектирования типовых процедур

Аналитика по срабатываниям правил в разрезе техник и тактик

Инструменты Risk Scoring для объектов пользователей и систем

Risk-based правила

Инструменты для работы с исключениями



SMART Monitor for
MITRE ATT&CK

Coverage Assessment

Оценка покрытия техник

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
<ul style="list-style-type: none"> Valid Accounts Hardware Additions Phishing 	<ul style="list-style-type: none"> Command and Scripting Interpreter Scheduled Task/Job System Services 	<ul style="list-style-type: none"> Boot or Logon Autostart Execution Create Account Scheduled Task/Job Event Triggered Execution Valid Accounts Boot or Logon Initialization Scripts 	<ul style="list-style-type: none"> Boot or Logon Autostart Execution Scheduled Task/Job Event Triggered Execution Process Injection Valid Accounts Boot or Logon Initialization Scripts Group Policy Modification 	<ul style="list-style-type: none"> Indirect Command Execution Modify Registry Hide Artifacts Impair Defenses Use Alternate Authentication Material Process Injection Valid Accounts Group Policy Modification Masquerading 	<ul style="list-style-type: none"> Network Sniffing OS Credential Dumping Unsecured Credentials Brute Force Credentials from Password Stores Input Capture 	<ul style="list-style-type: none"> Account Discovery Domain Trust Discovery Permission Groups Discovery System Owner/User Discovery Network Share Discovery Network Sniffing Process Discovery System Network Configuration Discovery File and Directory Discovery Remote System Discovery Application Window Discovery Password Policy Discovery 	<ul style="list-style-type: none"> Remote Service Session Hijacking Use Alternate Authentication Material Remote Services Internal Spearphishing Lateral Tool Transfer 	<ul style="list-style-type: none"> Archive Collected Data Data Staged Email Collection Input Capture

Coverage Assessment

Оценка покрытия техник

ДЕМОНСТРАЦИЯ



SMART Monitor for
MITRE ATT&CK

Coverage Assessment

Оценка покрытия техник

Интерфейс в виде интерактивной матрицы с наборами фильтров

Работа только с актуальными техниками, выбранными на этапе анализа угроз

Оценка покрытия техник: none, low, medium, enough

Валидация оценки, в зависимости от наличия правил детектирования

История изменений и отслеживание прогресса



SMART Monitor for
MITRE ATT&CK

SMART Monitor for MITRE ATT&CK



Предоставление инструментов для реализации основных сценариев применения **ATT&CK**

Инструменты для анализа и **приоритезации** угроз

Механизмы для **детектирования** потенциального поведения злоумышленников в информационных системах

Оценка **покрытия** актуальных техник

Анализ детектирования поведения в контексте объектов риска: **пользователей и систем**



Risk-based контекст пользователя может быть передан в модуль **SM UBA** для анализа в разрезе типового для пользователя поведения

Спасибо за внимание!