VB-Trend 2020

SMART Monitor for MITRE ATT&CK

VB-Trend 2020

MITRE ATT&CK

ATT&CK (**A**dversary **T**echnique, **T**actic **&** **C**ommon **K**nowledge)

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

Initial Access
Первоначальный доступ

Execution
Выполнение

Persistence
Закрепление

Privilege Escalation
Повышение привилегий

Defense Evasion
Обход защиты

Credential Access
Получение учетных данных

Discovery
Разведка

Lateral movement
Перемещение внутри периметра

Collection
Сбор данных

Command and Control
Управление и контроль

Exfiltration
Эксфильтрация данных

Impact
Воздействие

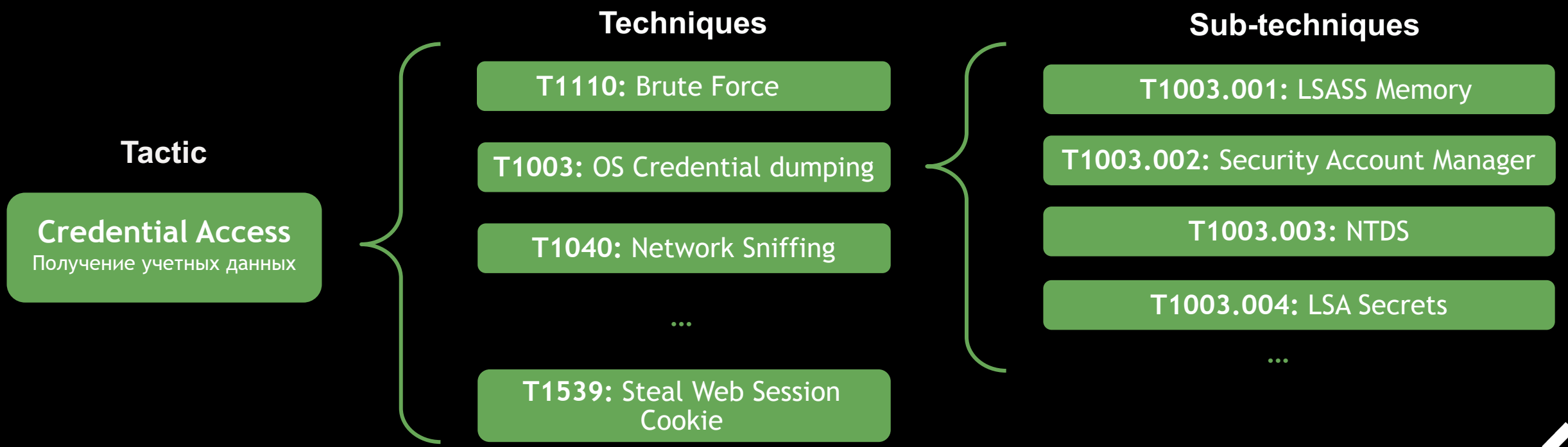
Термины и объекты : **Техники**

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*)

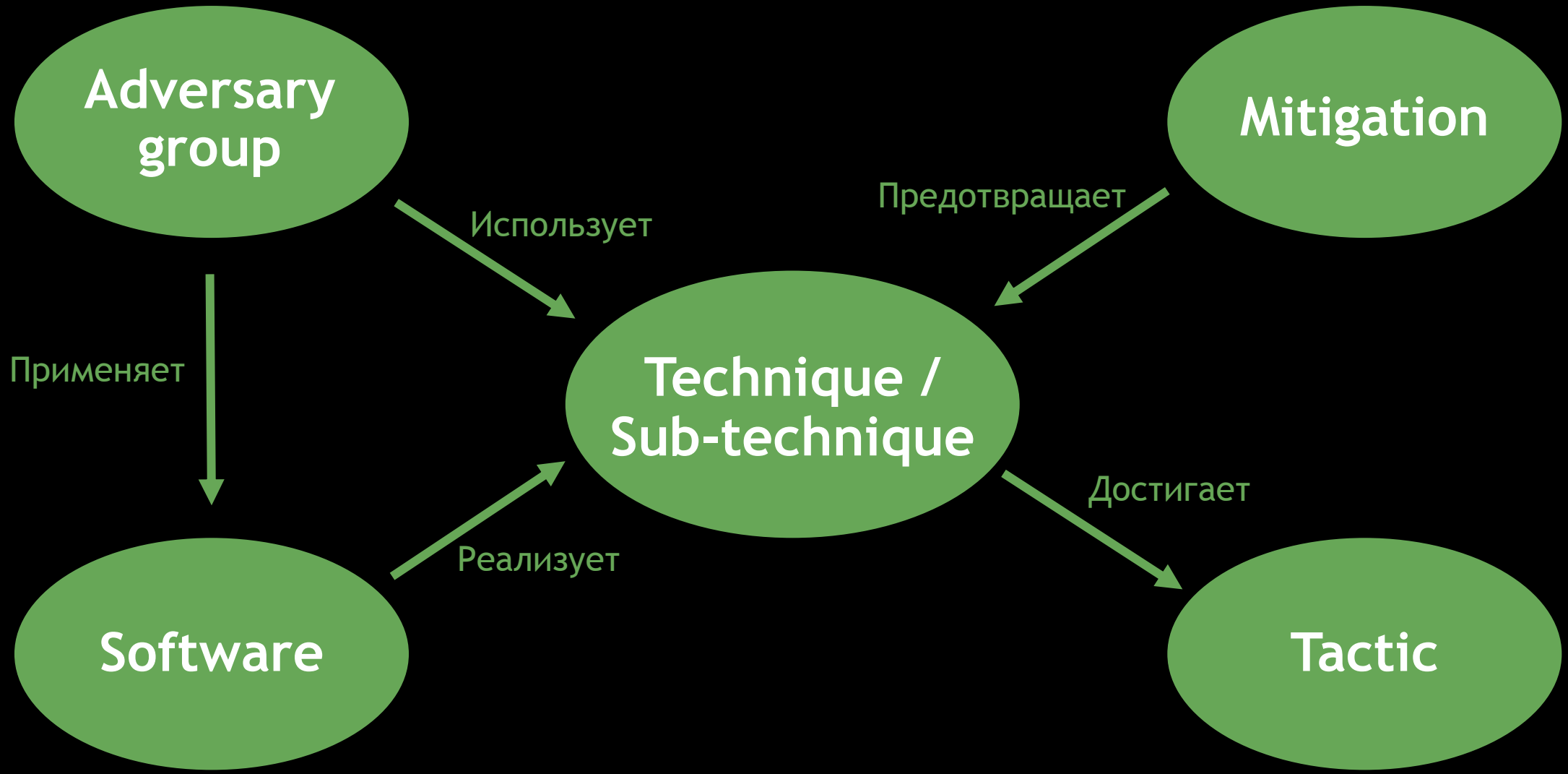
Software

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

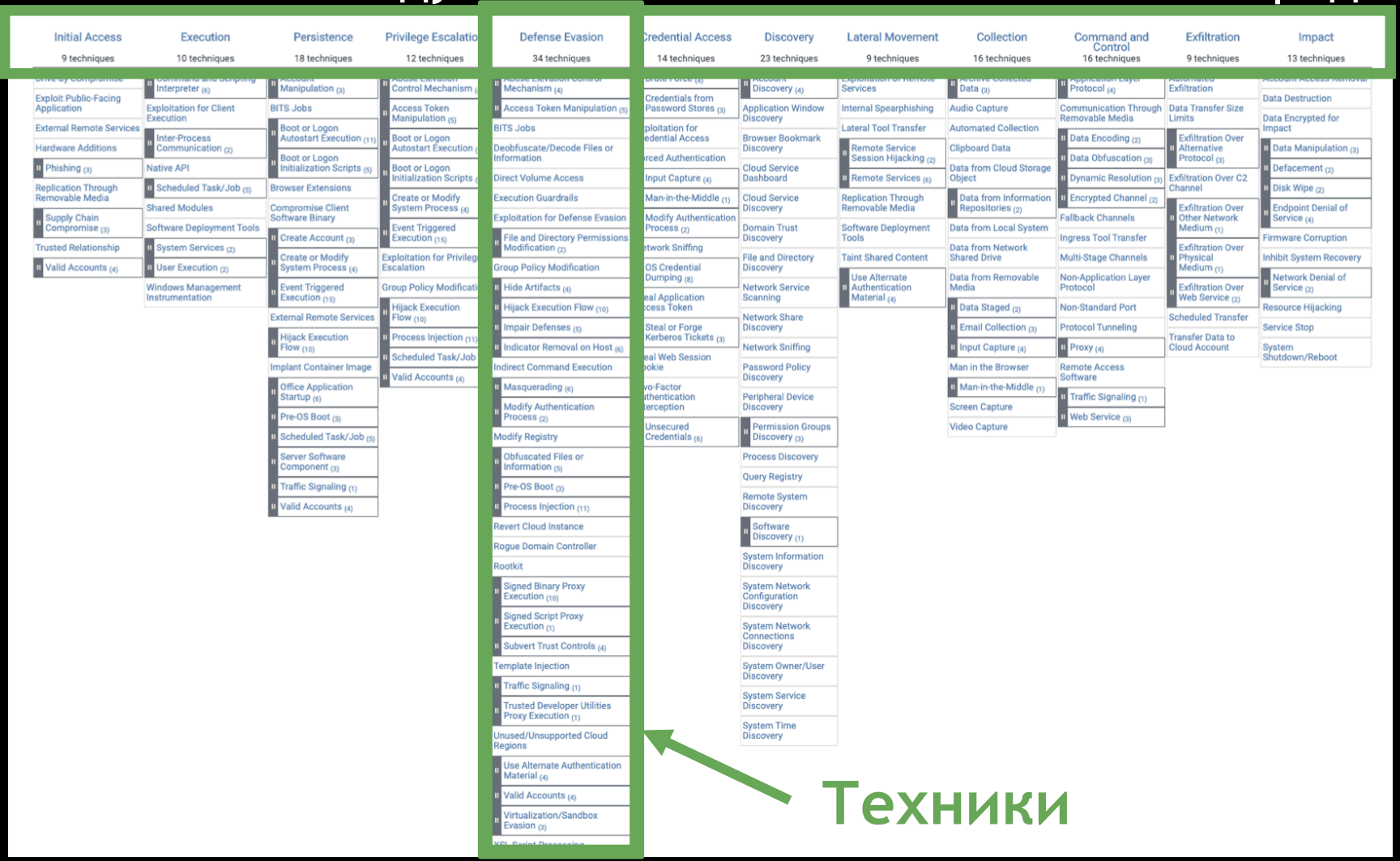
Взаимосвязь объектов модели ATT&CK



Взаимосвязь объектов модели ATT&CK

Матрицы MITRE ATT&CK

Отношения между тактиками и техниками обычно представляется в виде матриц



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

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

collections

tactics
techniques
subtechniques
...
mitigations

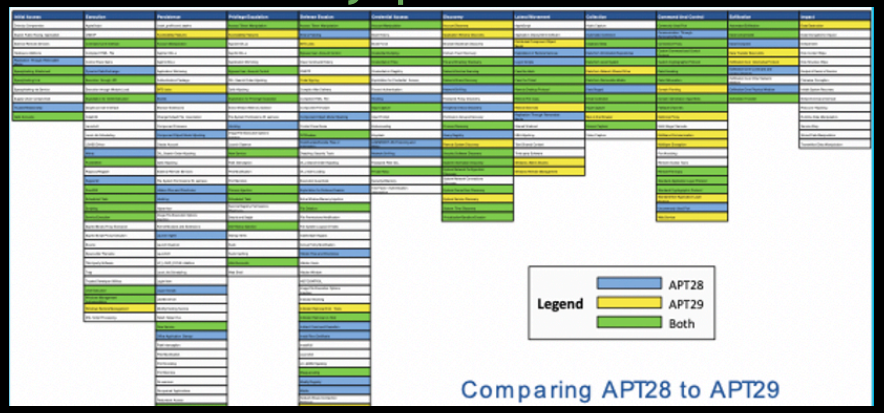
Команды SPL:

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

Сценарии использования ATT&CK

Threat Intelligence

Анализ угроз/техник



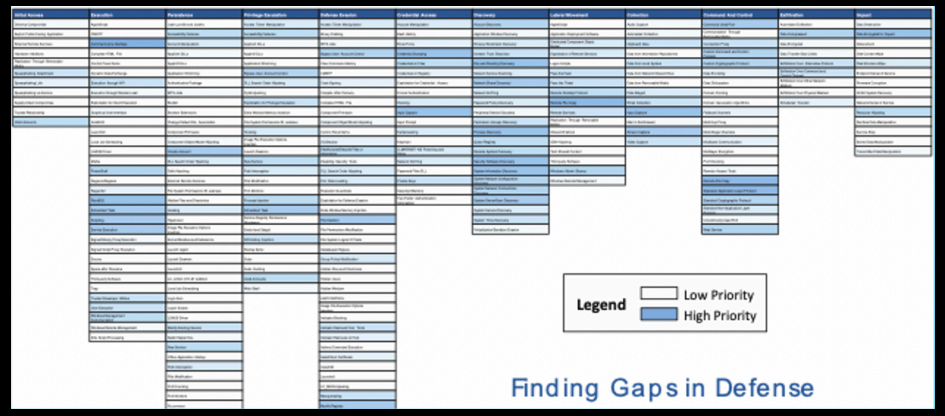
Detection

Обнаружение использования техник

```
processes = search Process:Create
reg = filter processes where (exe == "reg.exe" and parent_exe
== "cmd.exe")
cmd = filter processes where (exe == "cmd.exe" and
parent_exe != "explorer.exe"")
reg_and_cmd = join (reg, cmd) where (reg.ppid == cmd.pid and
reg.hostname == cmd.hostname)
output reg_and_cmd
```

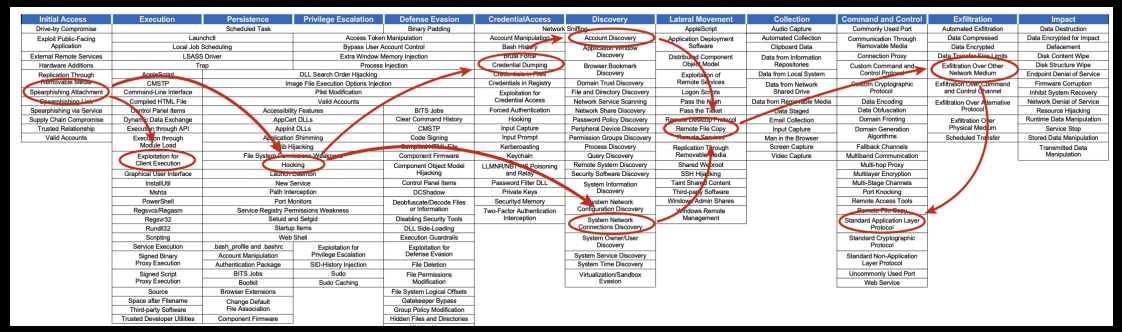
Coverage Assessment

Оценка покрытия



Adversary Emulation

Эмуляция действий злоумышленника



Threat Intelligence

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

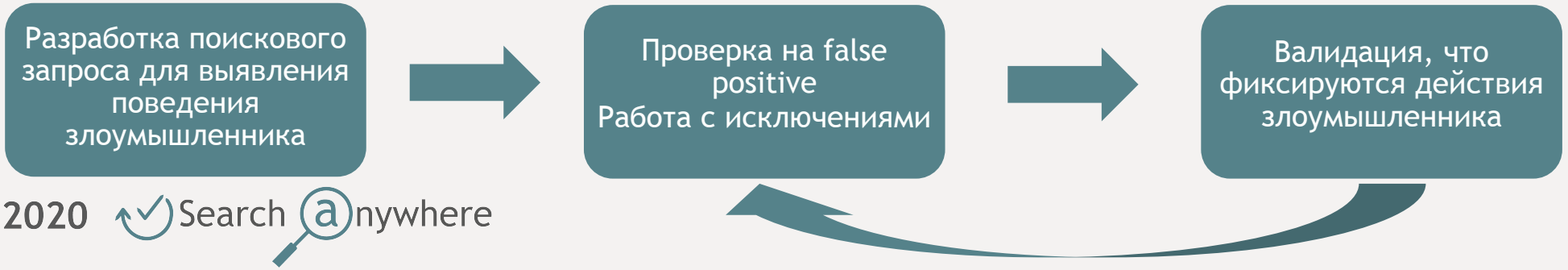
SMART Monitor for MITRE ATT&CK

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

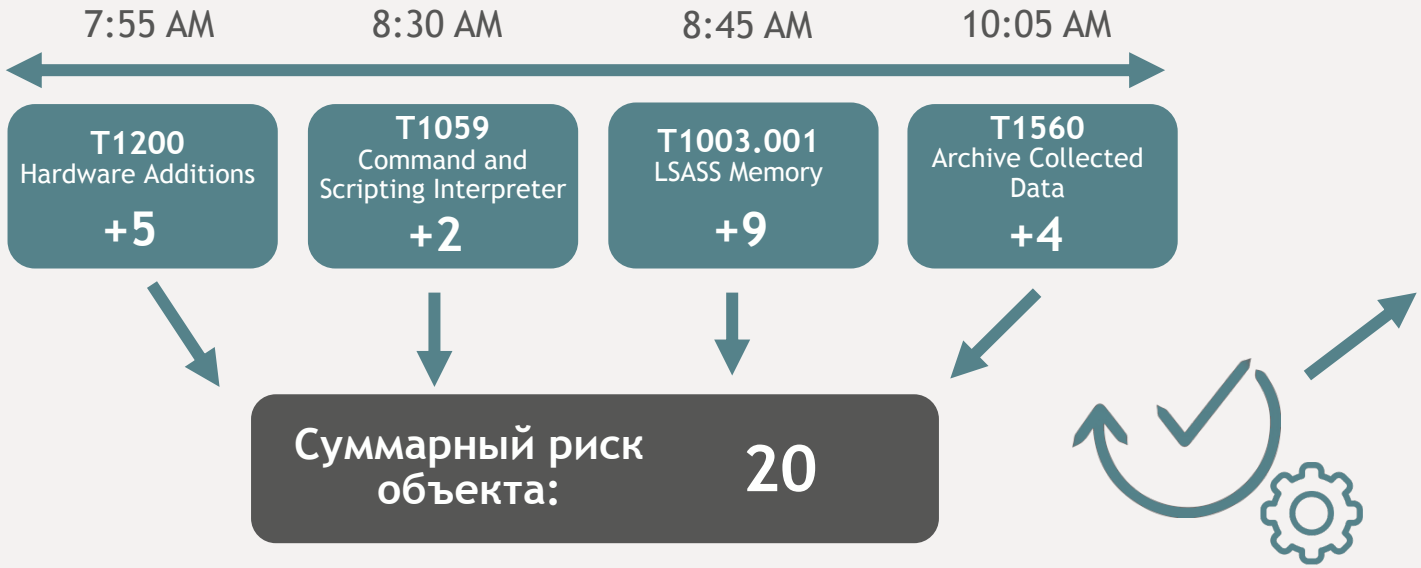
Цели Risk Scoring

- Повышение точности алертинга
- Привязка к объектам инфраструктуры и пользователям
- Дополнительный контекст в срабатываниях
- Повышение эффективности использования времени аналитика
- ”Плавность” масштабирования: больше правил ≠ 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

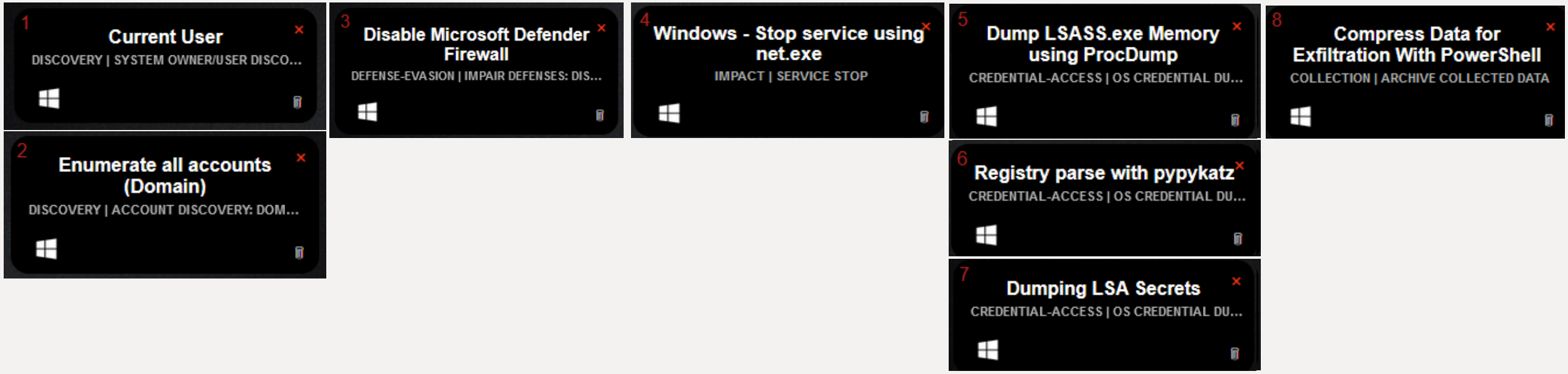
Проверка, как действует защита против эмулированного поведения злоумышленника

- На основе данных о процедурах из базы ATT&CK 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



Detection & Emulation

ДЕМОНСТРАЦИЯ

SMART Monitor for
MITRE ATT&CK

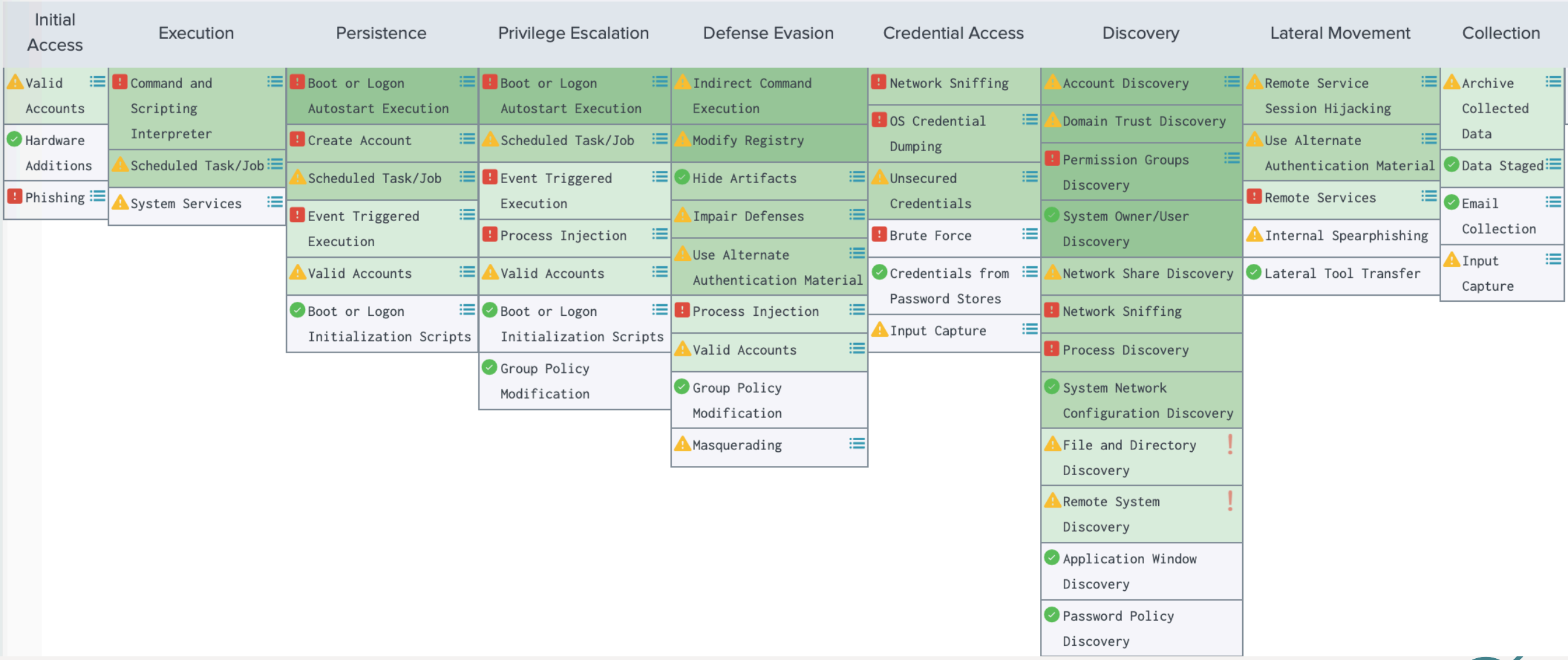
Detection

- Инструменты для создания правил с дополнительным 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



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!