Как использовать MITRE ATT&CK в SOC

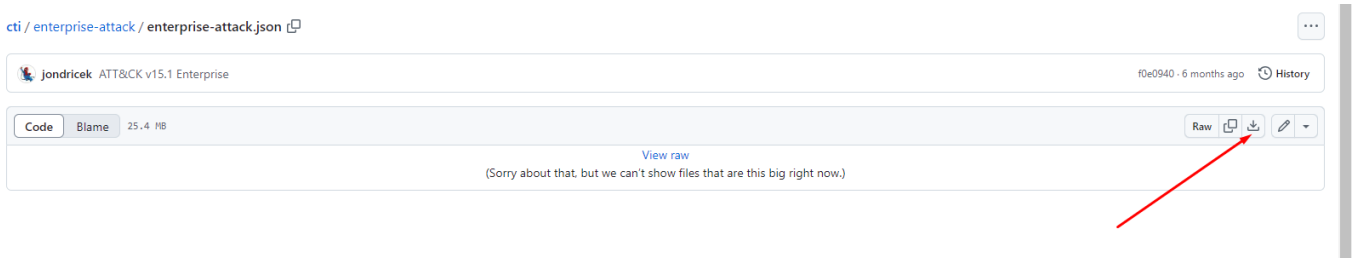
Использование MITRE ATT&CK в Центре управления безопасностью (SOC) может значительно расширить возможности обнаружения угроз и реагирования на них.

> Правила корреляции из коробки в KUMA (SOC Package и Community-Pack) покрываются техниками и тактиками из матрицы MITRE ATT&CK

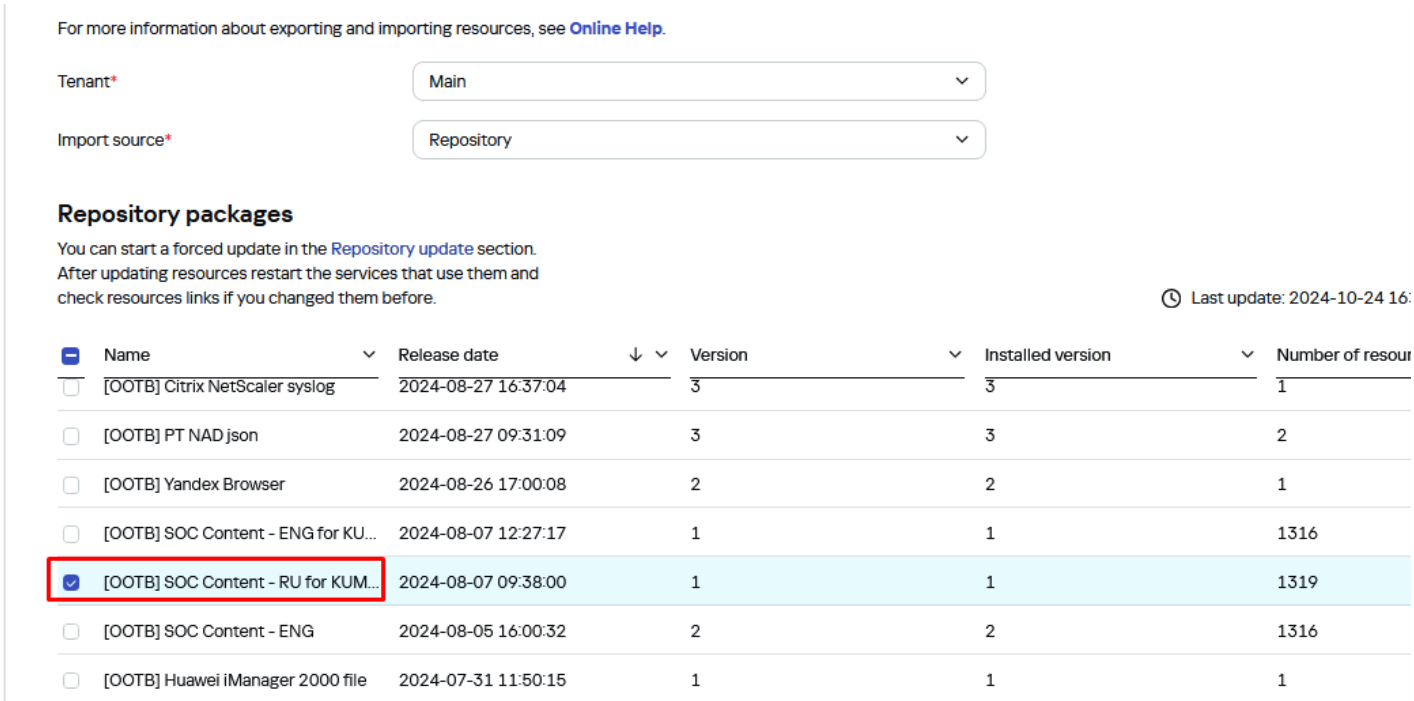
Обогащение Техниками и Тактиками на коррелляторе

Для актуальных версий: Воспользуйтесь справкой - https://support.kaspersky.com/help/KUMA/3.2/ru-RU/272743.htm

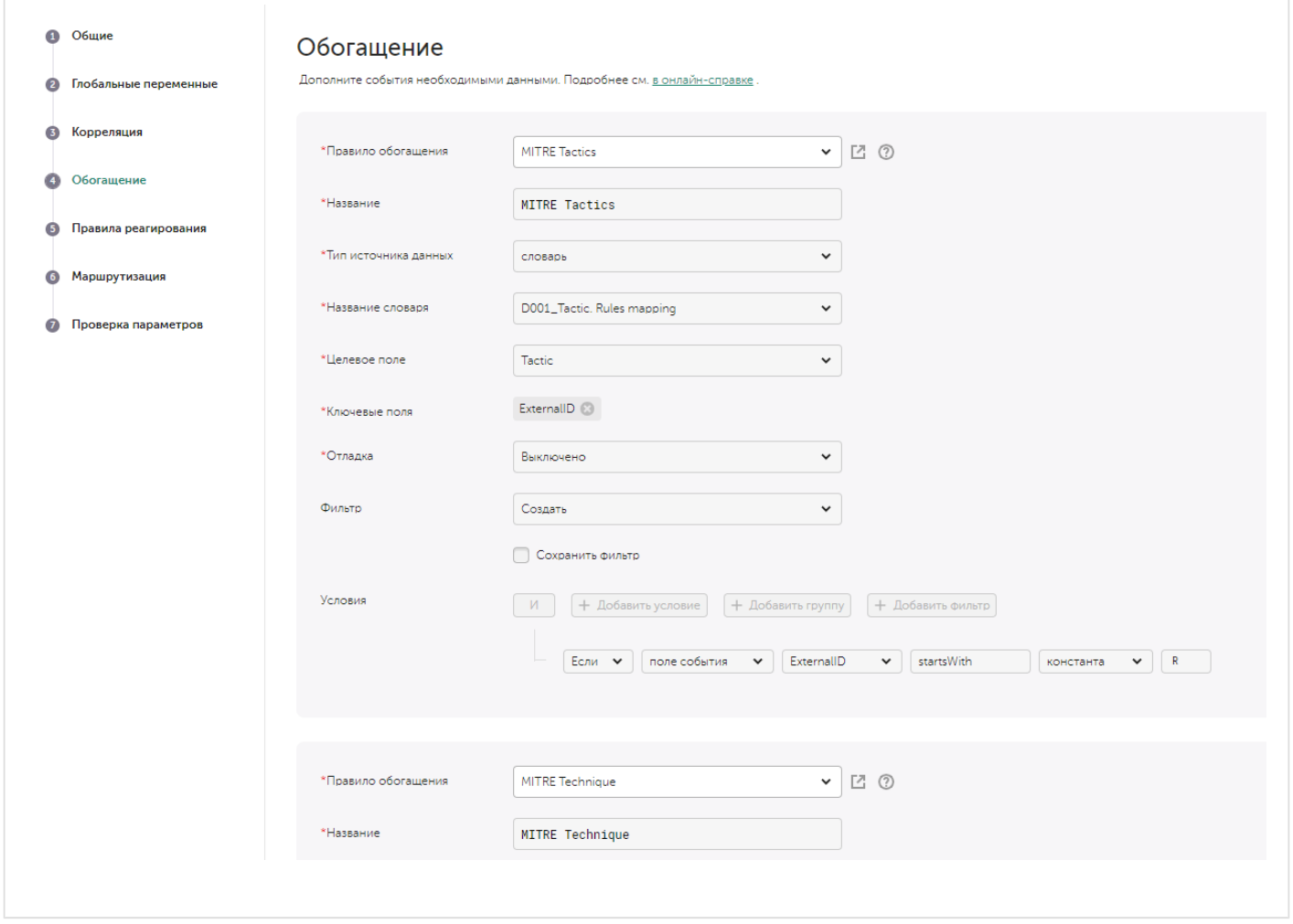
Скачайте справочник техник MITRE ATT&CK на портале GitHub



Зашрузите следующий пакет правил из репозитория:



Для обогащения техниками и тактиками в событии добавьте словарь в обогащении на коррелляторе KUMA:



Ниже шаги для эффективного использования в SOC:

Ознакомьтесь с MITRE ATT&CK

- Понять назначение и структуру платформы MITRE ATT&CK. Может помочь эта статья на русском: https://xakep.ru/2021/03/17/mitre-att-ck/
- Посетите веб-сайт ATT&CK (https://attack.mitre.org/) и ознакомьтесь с матрицей ATT&CK, техниками, тактиками и подтехниками.

Сопоставьте ATT&CK с вашей средой

- Определите соответствующие методы и тактики MITRE ATT&CK, соответствующие инфраструктуре, процессам, приложениям и данным вашей организации.
- Сопоставьте методы MITRE ATT&CK с вашими существующими средствами безопасности, такими как МЭ, системы обнаружения вторжений, решения для защиты конечных точек и др.

Создайте правила обнаружения

- Разработайте правила обнаружения и варианты использования на основе конкретных методов и тактик MITRE ATT&CK.
- Используйте свою систему SIEM или платформы аналитики угроз для создания правил, создающие оповещения при обнаружении подозрительных действий, связанных с определенными методами ATT&CK.

Реализуйте поиск угроз (Threat Hunting)

- Используйте MITRE ATT&CK в качестве руководства для упреждающих упражнений по поиску угроз.
- Найдите индикаторы компрометации (IOC), связанные с известными методами ATT&CK, и используйте их для выявления потенциальных угроз в вашей среде.

Улучшайте реагирование на инциденты

- Включите MITRE ATT&CK в свои процедуры реагирования на инциденты.
- Разрабатывайте сценарии и планы реагирования, соответствующие конкретным методам и тактикам ATT&CK, чтобы эффективно справляться с угрозами и смягчать их последствия.
- Полезные материалы на русском:
  - Примеры плейбуков - https://github.com/certsocietegenerale/IRM/tree/main/RU
  - Руководство по реагирования ЛК - https://box.kaspersky.com/f/26b68439676f4739baa6/

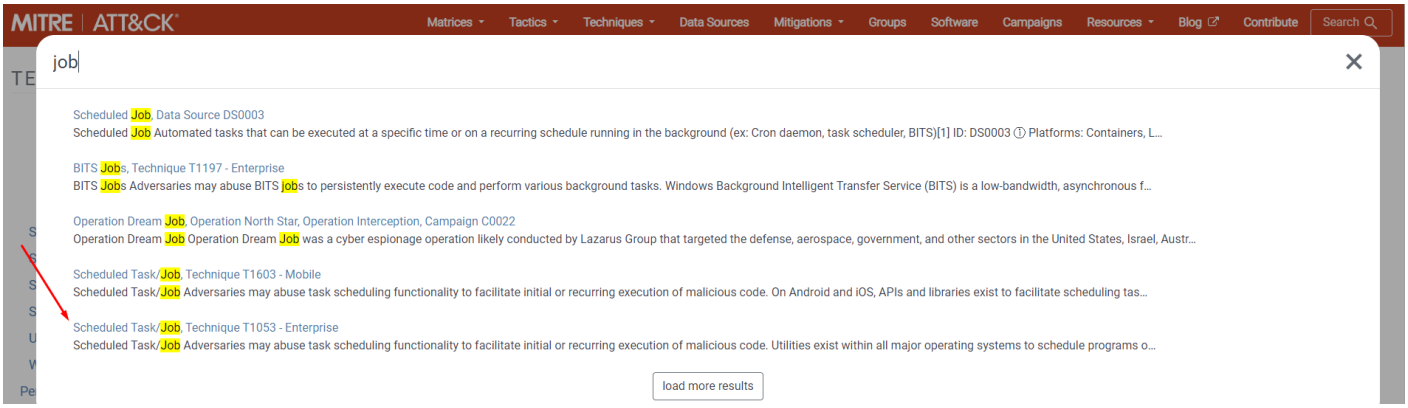
Работайте с Threat Intelligence

- Используйте внешние источники информации об угрозах, соответствующие MITRE ATT&CK.
- Будьте в курсе последних отчетов об угрозах, в которых упоминаются методы и тактика ATT&CK.
- Полезные материалы:
  - Бесплатный TI портал ЛК - https://opentip.kaspersky.com/

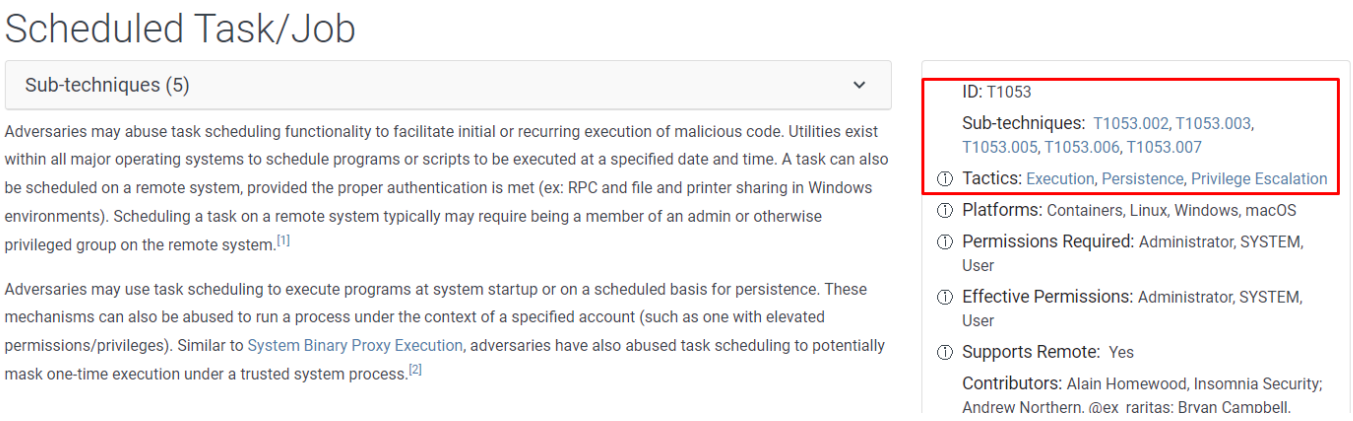
Пример работы

Находим технику

Например, нам интересен вектор атаки через планировщик задач, для этого можно воспользоваться поиском вверху справа на сайте https://attack.mitre.org/:



Переходим на интересующую тематику:



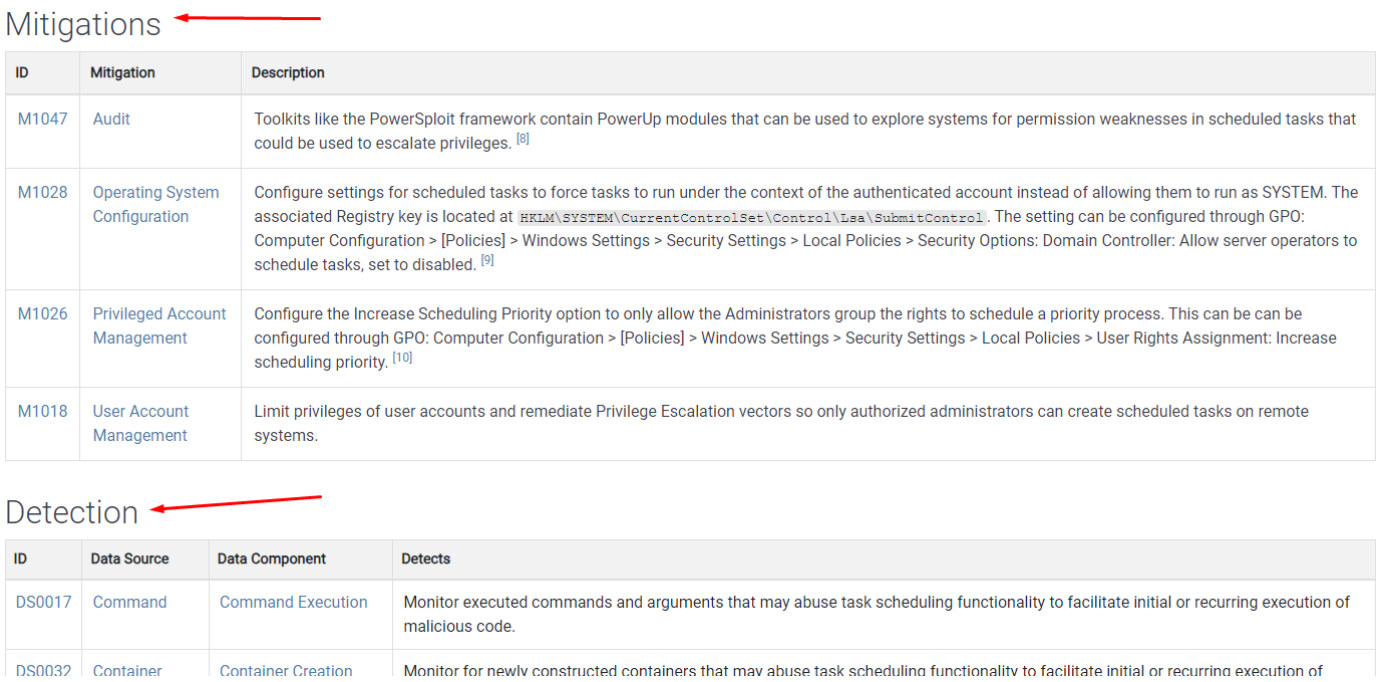
Изучаем материал

- Ознакомьтесь с общей структурой ATT&CK
- Найти параметры и инструменты, которые злоумышленник должен использовать для реализации ATT&CK.
- Поищите о технике или подтехнике на других ресурсах.

- Прочтите раздел «Примеры процедур» - Узнайте, как группы или инструменты используют технику или подтехнику.

Изучаем меры защиты

- Раздел митигации (снижений последствий) - Найдите митигацию
- Раздел обнаружения - Найдите способы обнаружения этой техники



Mitigations

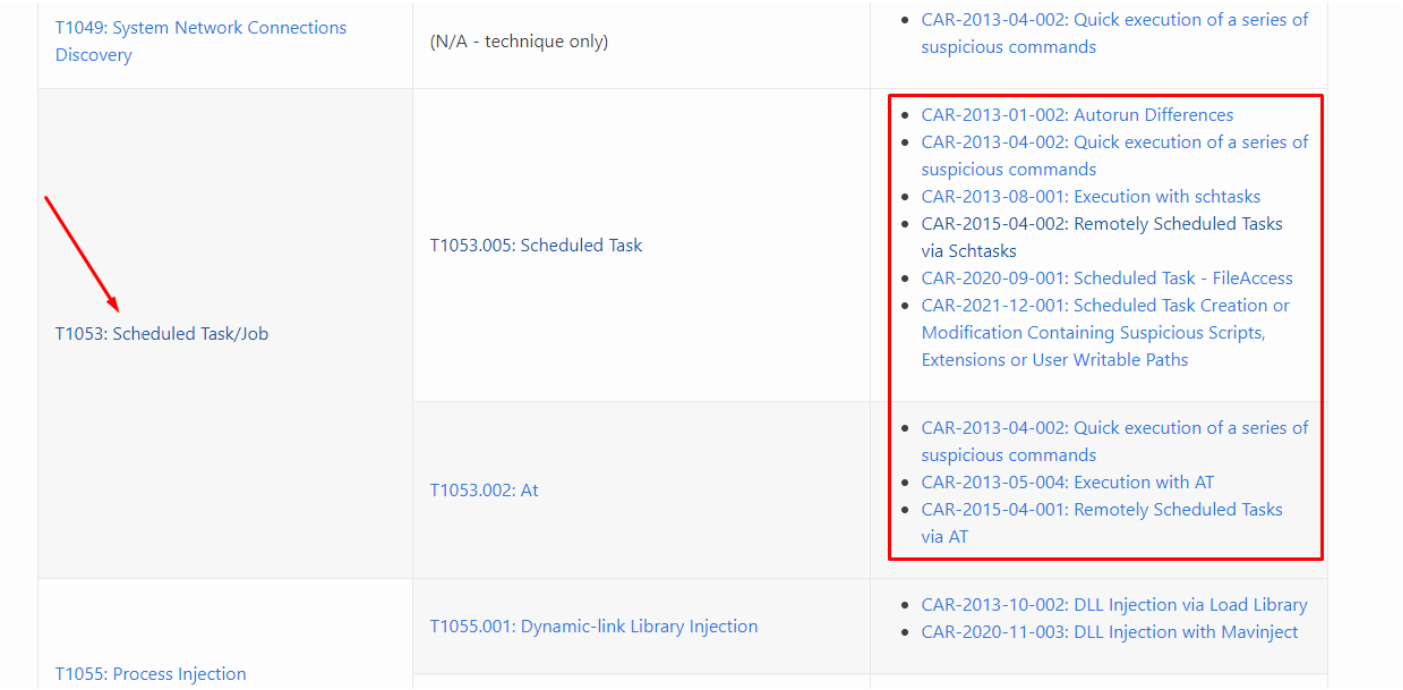
ID	Mitigation	Description
M1047	Audit	Toolkits like the PowerSploit framework contain PowerUp modules that can be used to explore systems for permission weaknesses in scheduled tasks that could be used to escalate privileges. [8]
M1028	Operating System Configuration	Configure settings for scheduled tasks to force tasks to run under the context of the authenticated account instead of allowing them to run as SYSTEM. The associated Registry key is located at `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl`. The setting can be configured through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > Security Options: Domain Controller: Allow server operators to schedule tasks, set to disabled. [9]
M1026	Privileged Account Management	Configure the Increase Scheduling Priority option to only allow the Administrators group the rights to schedule a priority process. This can be can be configured through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Increase scheduling priority. [10]
M1018	User Account Management	Limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create scheduled tasks on remote systems.

Detection

ID	Data Source	Data Component	Detects
DS0017	Command	Command Execution	Monitor executed commands and arguments that may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code.
DS0032	Container	Container Creation	Monitor for newly constructed containers that may abuse task scheduling functionality to facilitate initial or recurring execution of

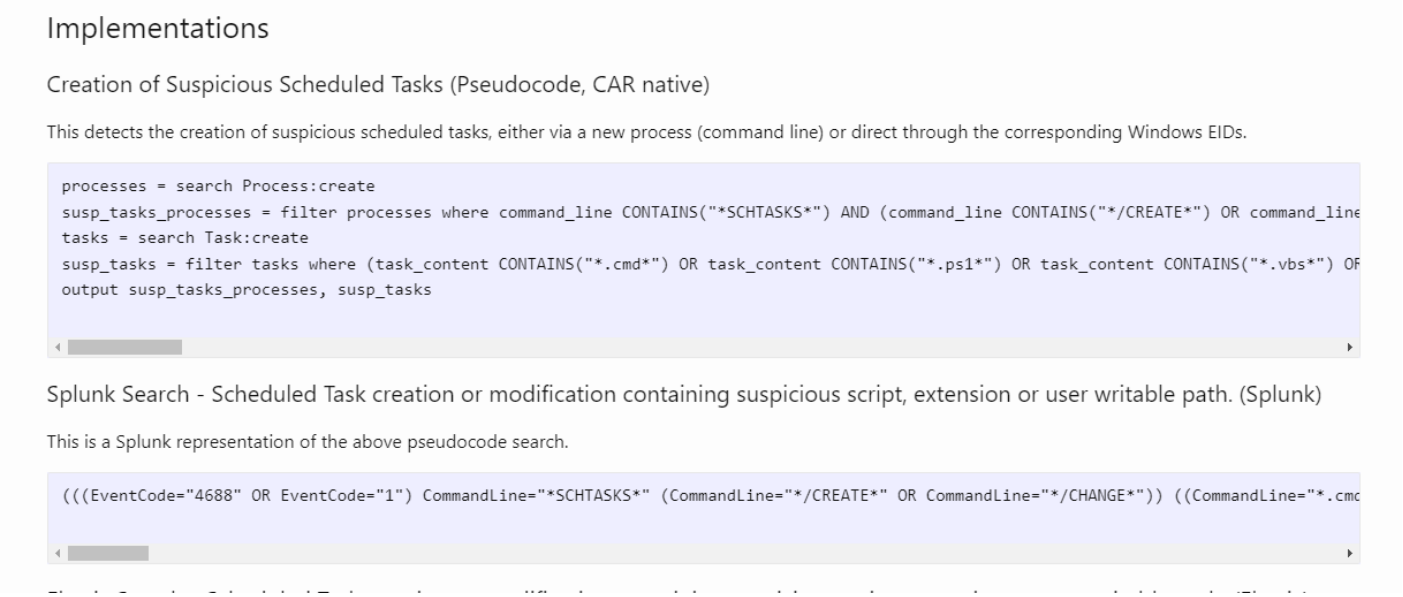
Преобразуйте TTP (Техники, Тактики и Процедуры) в правила в SIEM

- Найдите правило обнаружения в проекте MITRE CAR - https://car.mitre.org/analytics/by_technique



T1049: System Network Connections Discovery	(N/A - technique only)	• CAR-2013-04-002: Quick execution of a series of suspicious commands
T1053: Scheduled Task/Job	T1053.005: Scheduled Task	• CAR-2013-01-002: Autorun Differences • CAR-2013-04-002: Quick execution of a series of suspicious commands • CAR-2013-08-001: Execution with schtasks • CAR-2015-04-002: Remotely Scheduled Tasks via Schtasks • CAR-2020-09-001: Scheduled Task - FileAccess • CAR-2021-12-001: Scheduled Task Creation or Modification Containing Suspicious Scripts, Extensions or User Writable Paths
	T1053.002: At	• CAR-2013-04-002: Quick execution of a series of suspicious commands • CAR-2013-05-004: Execution with AT • CAR-2015-04-001: Remotely Scheduled Tasks via AT
T1055: Process Injection	T1055.001: Dynamic-link Library Injection	• CAR-2013-10-002: DLL Injection via Load Library • CAR-2020-11-003: DLL Injection with Mavinject

Например, такое правило MITRE CAR - Scheduled Task Creation or Modification Containing Suspicious Scripts, Extensions or User Writable Paths (https://car.mitre.org/analytics/CAR-2021-12-001/). В нем можно увидеть множество вариаций правил, как в псевдокоде, так и в популярных зарубежных SIEM системах.



Implementations

Creation of Suspicious Scheduled Tasks (Pseudocode, CAR native)

This detects the creation of suspicious scheduled tasks, either via a new process (command line) or direct through the corresponding Windows EIDs.

```
processes = search Process:create
susp_tasks_processes = filter processes where command_line CONTAINS("*SCHTASKS*") AND (command_line CONTAINS("*/CREATE*") OR command_line
tasks = search Task:create
susp_tasks = filter tasks where (task_content CONTAINS("*.cmd*") OR task_content CONTAINS("*.ps1*") OR task_content CONTAINS("*.vbs*") OR
output susp_tasks_processes, susp_tasks
```

Splunk Search - Scheduled Task creation or modification containing suspicious script, extension or user writable path. (Splunk)

This is a Splunk representation of the above pseudocode search.

```
(((EventCode="4688" OR EventCode="1") CommandLine="*SCHTASKS*" (CommandLine="*/CREATE*" OR CommandLine="*/CHANGE*")) ((CommandLine="*.cmd
```

ATT&CK Navigator

ATT&CK Navigator — это веб-инструмент для разметки и изучения матриц ATT&CK. Его можно использовать для визуализации покрытия средств защиты, планирования красно-синих команд, частоты обнаруженных приемов и многого другого. Сайт - https://mitre-attack.github.io/attack-navigator/

Revision #8
Created 16 August 2023 12:12:06 by Boris Rzr
Updated 30 October 2024 10:18:24 by Boris Rzr