Как использовать MITRE ATT&CK в SOC

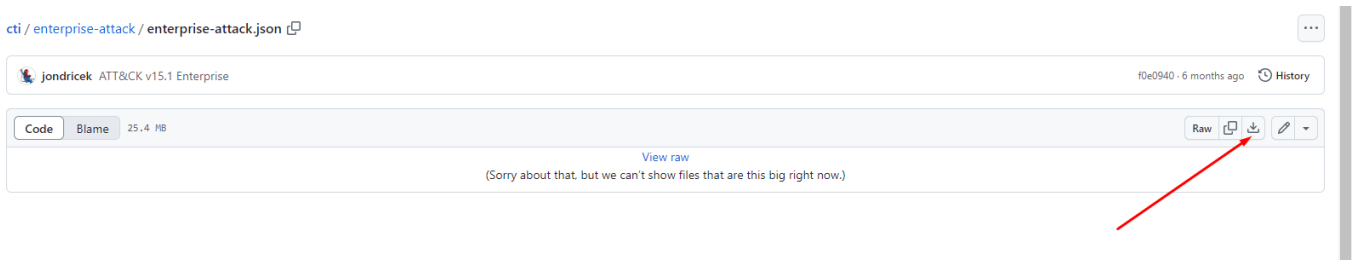
????????????? MITRE ATT&CK ? ?????? ?????????? ????????????? (SOC) ????? ??????????? ????????? ??????????? ??????????? ????? ? ???????????? ?? ???.

??????? ?????????? ?? ??????? ? KUMA (SOC Package ? Community-Pack) ??????????? ????????? ? ????????? ?? ??????? MITRE ATT&CK

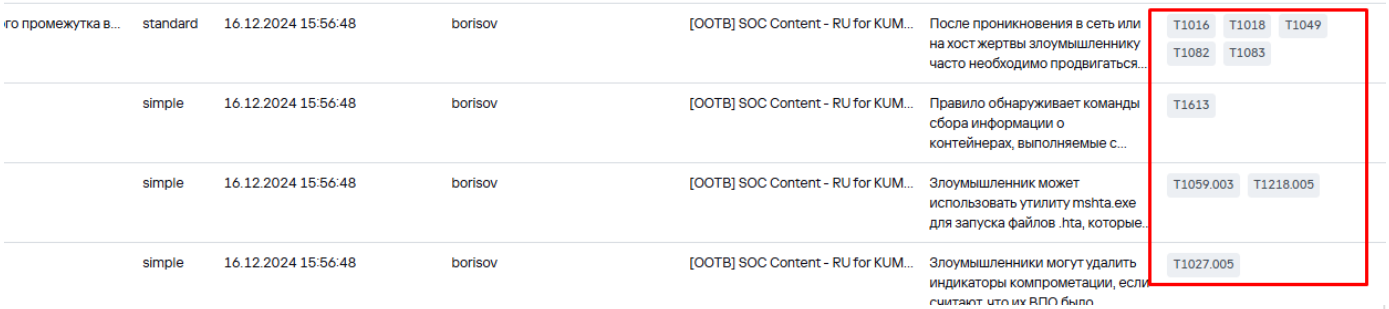
Обогащение Техниками и Тактиками на коррелляторе

??? ?????????? ??????: ????????????? ???????? - https://support.kaspersky.com/help/KUMA/3.2/ru-RU/272743.htm

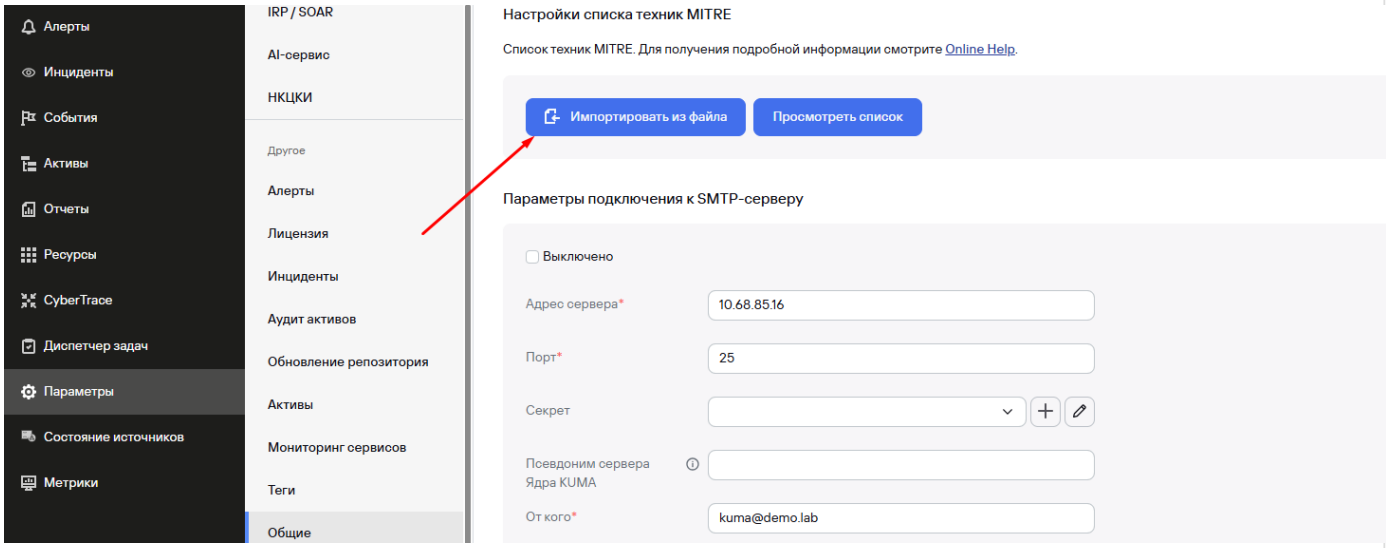
???????? ?????????? ?????? MITRE ATT&CK ?? ??????? GitHub



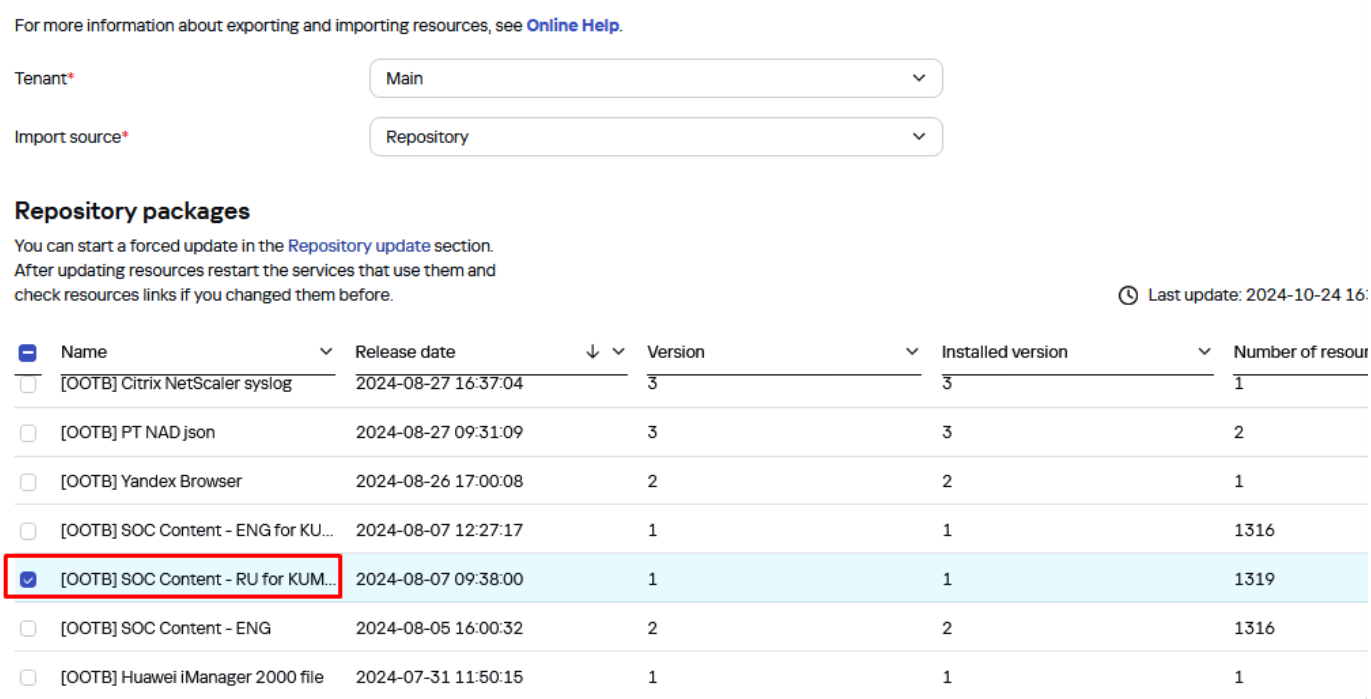
?????? ?????????? ?????????:



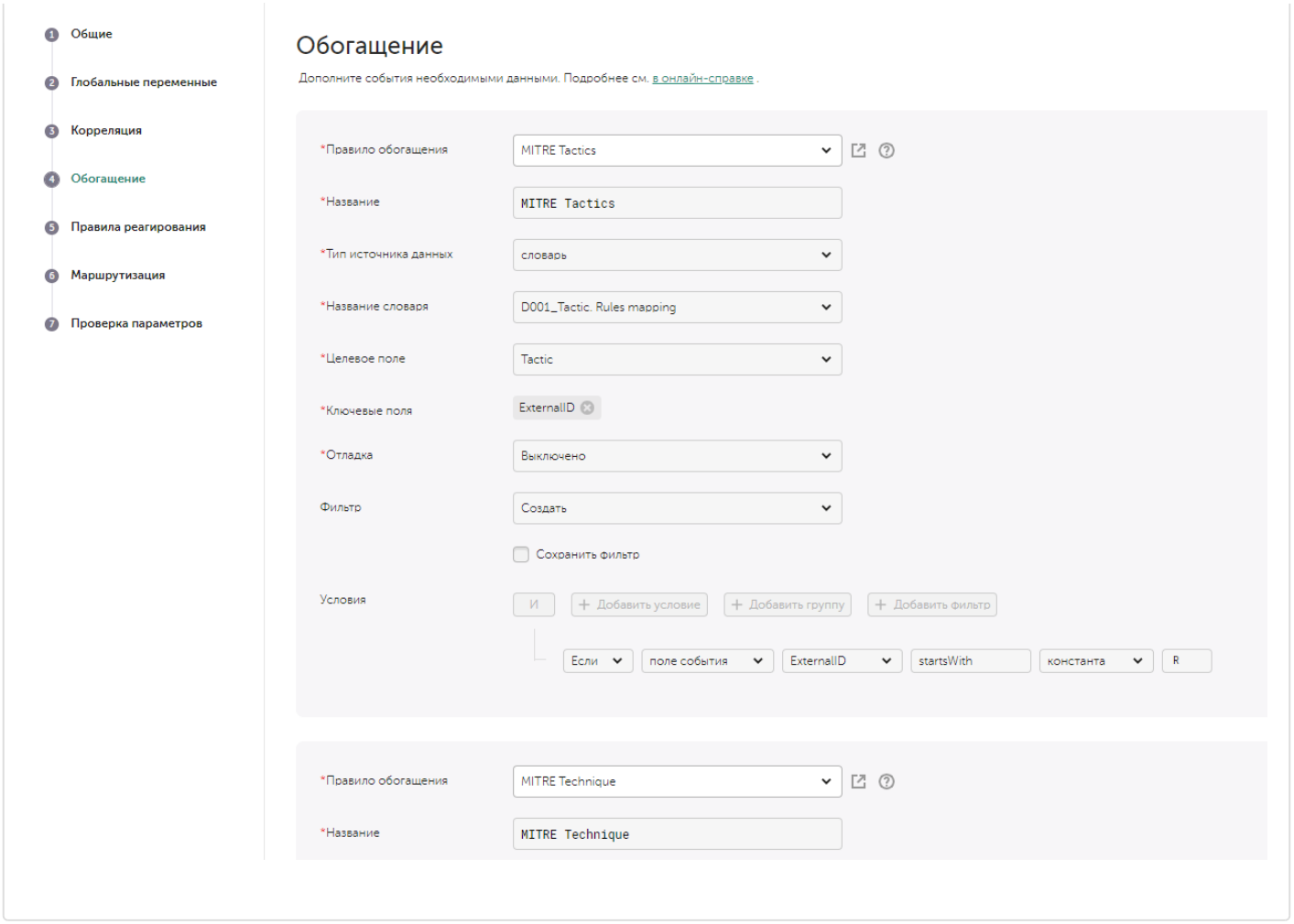
?????????? ???? ???? ????????? - ????? - ????????? ?????? ?????? MITRE:


Алерты
Инциденты
События
Активы
Отчеты
Ресурсы
CyberTrace
Диспетчер задач
Параметры
Состояние источников
Метрики
IRP / SOAR
AI-сервис
НКЦКИ
Другое
Алерты
Лицензия
Инциденты
Аудит активов
Обновление репозитория
Активы
Мониторинг сервисов
Теги
Общие
Настройки списка техник MITRE
Список техник MITRE. Для получения подробной информации смотрите Online Help.
Импортировать из файла
Просмотреть список
Параметры подключения к SMTP-серверу
Выключено
Адрес сервера*
10.68.85.16
Порт*
25
Секрет
Псевдоним сервера Ядра KUMA
От кого*
kuma@demo.lab

????????? ????????? ????? ?????? ?? ???????????:


For more information about exporting and importing resources, see Online Help.
Tenant*
Main
Import source*
Repository
Repository packages
You can start a forced update in the Repository update section.
After updating resources restart the services that use them and check resources links if you changed them before.
Last update: 2024-10-24 16:
Name
Release date
Version
Installed version
Number of resour
[OOTB] Citrix NetScaler syslog
2024-08-27 16:37:04
3
3
1
[OOTB] PT NAD json
2024-08-27 09:31:09
3
3
2
[OOTB] Yandex Browser
2024-08-26 17:00:08
2
2
1
[OOTB] SOC Content - ENG for KU...
2024-08-07 12:27:17
1
1
1316
[OOTB] SOC Content - RU for KUM...
2024-08-07 09:38:00
1
1
1319
[OOTB] SOC Content - ENG
2024-08-05 16:00:32
2
2
1316
[OOTB] Huawei iManager 2000 file
2024-07-31 11:50:15
1
1
1

??? ?????????? ????????? ? ????????? ? ??????? ???????? ??????? ? ?????????? ?? ?????????? KUMA:



???? ???? ??? ???????????? ????????????? ? SOC:

Ознакомьтесь с MITRE ATT&CK

- ?????? ?????????? ? ????????? ????????? MITRE ATT&CK. ????? ?????? ??? ?????? ?? ???????: https://xakep.ru/2021/03/17/mitre-att-ck/
- ???????? ???-???? ATT&CK (https://attack.mitre.org/) ? ???????????? ? ???????? ATT&CK, ?????????, ????????? ? ????????????.

Сопоставьте ATT&CK с вашей средой

- ?????????? ?????????????? ?????? ? ??????? MITRE ATT&CK, ?????????????? ?????????????, ?????????, ??????????? ? ?????? ????? ???????????.
- ??????????? ?????? MITRE ATT&CK ? ?????? ????????????? ?????????? ????????????, ?????? ??? ??, ??????? ??????????? ?????????, ??????? ??? ?????? ???????? ????? ? ??.

Создайте правила обнаружения

- ???????????? ??????? ??????????? ? ???????? ????????????? ?? ?????? ?????????? ??????? ? ?????? MITRE ATT&CK.

- ?????????? ???? ??????? SIEM ??? ????????? ????????? ????? ??? ???????? ??????, ????????? ?????????? ??? ?????????? ????????????? ????????, ????????? ? ????????????? ???????? ATT&CK.

Реализуйте поиск угроз (Threat Hunting)

- ?????????? MITRE ATT&CK ? ???????? ?????????? ??? ?????????? ?????????? ?? ?????? ?????.
- ??????? ?????????? ????????????? (IOC), ????????? ? ?????????? ???????? ATT&CK, ? ?????????? ?? ??? ????????? ????????????? ????? ? ????? ?????.

Улучшайте реагирование на инциденты

- ???????? MITRE ATT&CK ? ???? ????????? ??????????? ?? ????????.
- ????????????? ???????? ? ????? ???????????, ?????????????? ?????????? ??????? ? ???????? ATT&CK, ????? ?????????? ?????????? ? ???????? ? ???????? ?? ??????????.
- ???????? ????????? ?? ???????:
  - ??????? ????????? - https://github.com/certsocietegenerale/IRM/tree/main/RU
  - ?????????? ?? ???????????? ?? - https://box.kaspersky.com/f/26b68439676f4739baa6/

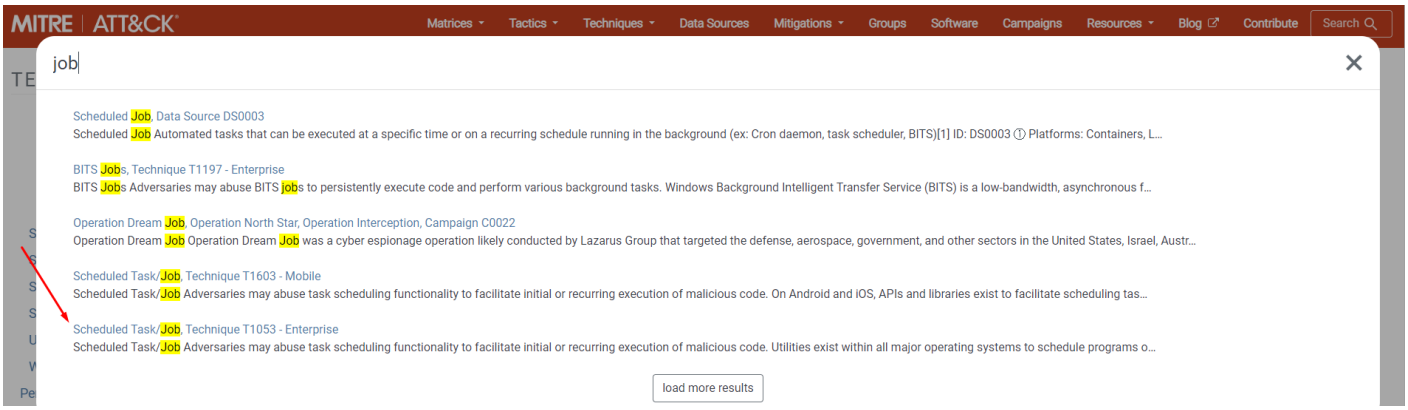
Работайте с Threat Intelligence

- ?????????? ??????? ????????? ?????????? ?? ???????, ?????????????? MITRE ATT&CK.
- ?????? ? ????? ????????? ??????? ?? ???????, ? ??????? ?????????? ?????? ? ??????? ATT&CK.
- ???????? ?????????:
  - ?????????? TI ?????? ?? - https://opentip.kaspersky.com/

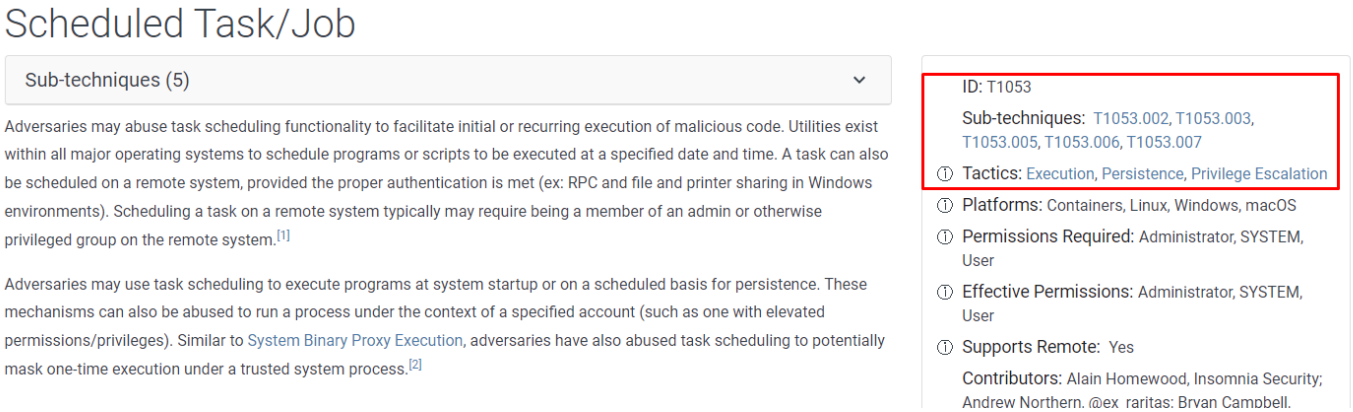
Пример работы

Находим технику

????????, ??? ????????? ?????? ????? ????? ?????????? ?????, ??? ????? ????? ?????????????? ??????? ?????? ?????? ?? ????? https://attack.mitre.org/:



????????? ?? ???????????? ????????:



Изучаем материал

- ???????????? ? ????? ?????????? ATT&CK
- ????? ????????? ? ???????????, ??????? ????????????? ?????? ???????????? ??? ?????????? ATT&CK.
- ??????? ? ??????? ??? ?????????? ?? ?????? ????????.
- ???????? ?????? «??????? ????????» - ???????, ??? ?????? ??? ??????????? ?????????? ??????? ??? ??????????.

Изучаем меры защиты

- ?????? ????????? (???????? ???????????) - ??????? ?????????
- ?????? ??????????? - ??????? ??????? ??????????? ???? ???????

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

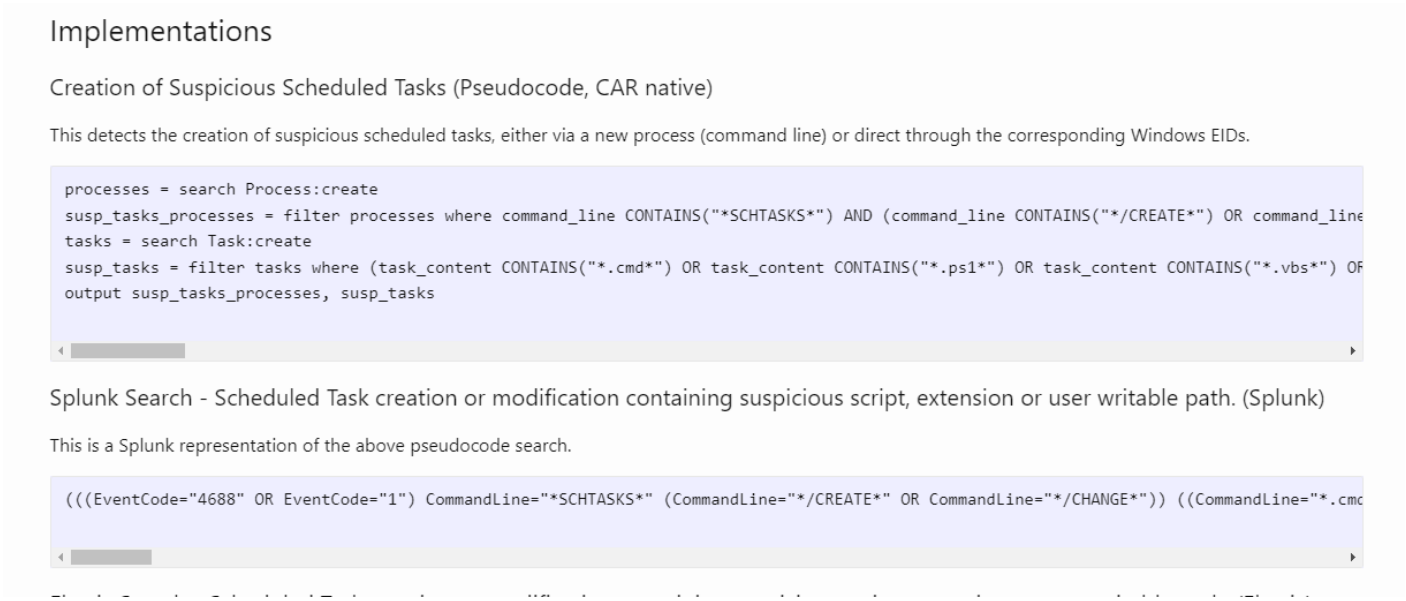
ID	Data Source	Data Component	Detects
DS0017	Command	Command Execution	Monitor executed commands and arguments that may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code.
DS0032	Container	Container Creation	Monitor for newly constructed containers that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

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

- ??????? ??????? ??????????? ? ??????? 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

????????, ????? ??????? MITRE CAR - Scheduled Task Creation or Modification Containing Suspicious Scripts, Extensions or User Writable Paths (https://car.mitre.org/analytics/CAR-2021-12-001/). ? ??? ????? ??????? ????????? ???????? ??????, ??? ? ??????????, ??? ? ? ?????????? ?????????? SIEM ????????.



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 — ??? ???-?????????? ??? ???????? ? ???????? ?????? ATT&CK. ??? ????? ???????????? ??? ???????????? ???????? ??????? ??????, ???????????? ??????-????? ??????, ??????? ???????????? ??????? ? ??????? ???????. ???? - https://mitre-attack.github.io/attack-navigator/

Revision #10
Created 2023-08-16 12:12:06 UTC by Boris Rzr
Updated 2025-05-27 12:09:04 UTC by Boris Rzr