

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

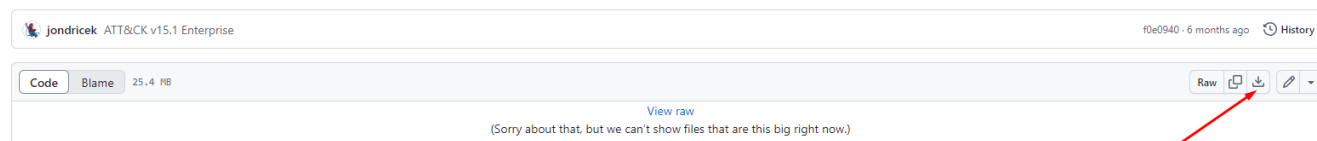
Обогащение Техниками и Тактиками на корреляторе

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](#)

cti / enterprise-attack / enterprise-attack.json



Должно получиться следующее:

| | | | | | | |
|--------------------|----------|---------------------|---------|------------------------------------|---|----------------------------------|
| го промежутка в... | standard | 16.12.2024 15:56:48 | borisov | [OOTB] SOC Content - RU for KUM... | После проникновения в сеть или на хост жертвы злоумышленнику часто необходимо продвигаться... | T1016 T1018 T1049 T1082 T1083 |
| | simple | 16.12.2024 15:56:48 | borisov | [OOTB] SOC Content - RU for KUM... | Правило обнаруживает команды сбора информации о контейнерах, выполняемые с... | T1613 |
| | simple | 16.12.2024 15:56:48 | borisov | [OOTB] SOC Content - RU for KUM... | Злоумышленник может использовать утилиту mshta.exe для запуска файлов .hta, которые... | T1059.003 T1218.005 |
| | simple | 16.12.2024 15:56:48 | borisov | [OOTB] SOC Content - RU for KUM... | Злоумышленники могут удалить индикаторы компрометации, если считают что их РПО было... | T1027.005 |

Подгрузите файл сюда Параметры - Общие - Настройки списка техник MITRE:

- Алерты
- Инциденты
- События
- Активы
- Отчеты
- Ресурсы
- CyberGate
- Диспетчер задач
- Параметры**
- Состояние источников
- Метрики

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*

Порт*

Секрет + ✎

Поевдоним сервера Ядра KUMA

От кого*

Загрузите следующий пакет правил из репозитория:

For more information about exporting and importing resources, see [Online Help](#).

Tenant*

Import source*

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:

| <input type="checkbox"/> | Name | Release date | Version | Installed version | Number of resour |
|-------------------------------------|------------------------------------|---------------------|---------|-------------------|------------------|
| <input type="checkbox"/> | [OOTB] Citrix NetScaler syslog | 2024-08-27 16:37:04 | 3 | 3 | 1 |
| <input type="checkbox"/> | [OOTB] PT NAD json | 2024-08-27 09:31:09 | 3 | 3 | 2 |
| <input type="checkbox"/> | [OOTB] Yandex Browser | 2024-08-26 17:00:08 | 2 | 2 | 1 |
| <input type="checkbox"/> | [OOTB] SOC Content - ENG for KU... | 2024-08-07 12:27:17 | 1 | 1 | 1316 |
| <input checked="" type="checkbox"/> | [OOTB] SOC Content - RU for KUM... | 2024-08-07 09:38:00 | 1 | 1 | 1319 |
| <input type="checkbox"/> | [OOTB] SOC Content - ENG | 2024-08-05 16:00:32 | 2 | 2 | 1316 |
| <input type="checkbox"/> | [OOTB] Huawei iManager 2000 file | 2024-07-31 11:50:15 | 1 | 1 | 1 |

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

- 1 Общие
- 2 Глобальные переменные
- 3 Корреляция
- 4 Обогащение
- 5 Правила реагирования
- 6 Маршрутизация
- 7 Проверка параметров

Обогащение

Дополните события необходимыми данными. Подробнее см. [в онлайн-справке](#).

*Правило обогащения 🔗 ?

*Название

*Тип источника данных

*Название словаря

*Целевое поле

*Ключевые поля

*Отладка

Фильтр

Сохранить фильтр

Условия + Добавить условие + Добавить группу + Добавить фильтр

Если ExternalID константа

*Правило обогащения 🔗 ?

*Название

Ниже шаги для эффективного использования в SOC:

???????????? ? 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.

???????????? ATT&CK ? ?????? ???????

- 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.

????????? ?????????? ???????????????

- 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 АТТ&СК.

?????????? ?????? ?????? (Threat Hunting)

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

?????????? ??????????????? ?? ???????????

- Включите MITRE АТТ&СК в свои процедуры реагирования на инциденты.
- Разрабатывайте сценарии и планы реагирования, соответствующие конкретным методам и тактикам АТТ&СК, 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/>

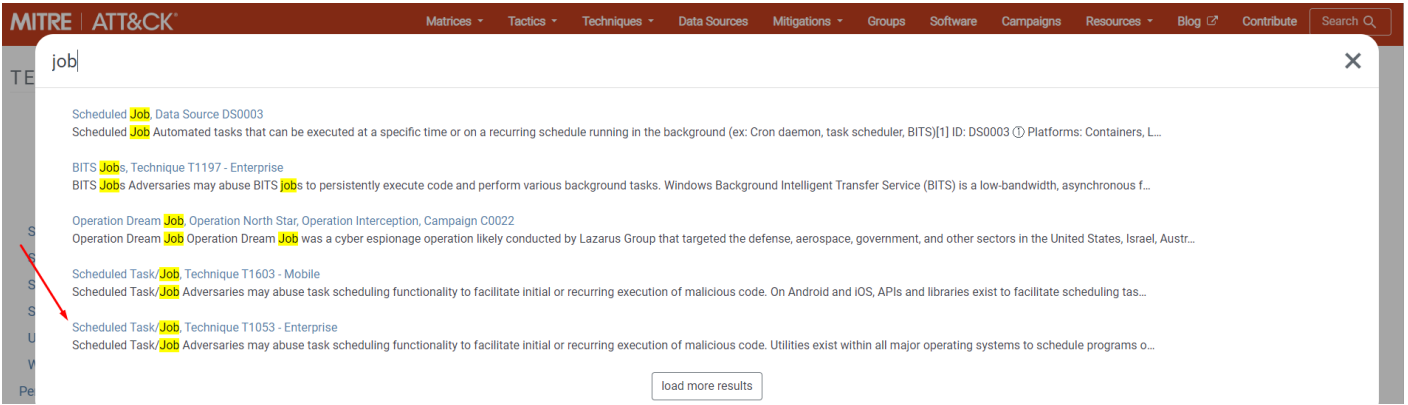
?????????? ? Threat Intelligence

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

????????? ??????????

????????? ??????????

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:

Scheduled Task/Job

Sub-techniques (5)

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.^[1]

Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges). Similar to [System Binary Proxy Execution](#), adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process.^[2]

ID: T1053

Sub-techniques: [T1053.002](#), [T1053.003](#), [T1053.005](#), [T1053.006](#), [T1053.007](#)

① Tactics: [Execution](#), [Persistence](#), [Privilege Escalation](#)

① Platforms: [Containers](#), [Linux](#), [Windows](#), [macOS](#)

① Permissions Required: [Administrator](#), [SYSTEM](#), [User](#)

① Effective Permissions: [Administrator](#), [SYSTEM](#), [User](#)

① Supports Remote: [Yes](#)

Contributors: [Alain Homewood](#), [Insomnia Security](#), [Andrew Northern](#), [@ex_raritas](#), [Brvan Camobell](#)

???????? ??????????

- Ознакомьтесь с общей структурой АТТ&СК
- Найти параметры и инструменты, которые злоумышленник должен использовать для реализации АТТ&СК.
- Поищите о технике или подтехнике на других ресурсах.
- Прочтите раздел «Примеры процедур» - Узнайте, как группы или инструменты используют технику или подтехнику.

???????? ????? ???????

- 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 <code>HKLM\SYSTEM\CurrentControlSet\Control\Local\SubmitControl</code> . 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 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 |

???????????? TTP (????????, ????????? ? ??????????) ? ????????? ?
SIEM

- Найдите правило обнаружения в проекте MITRE CAR -

https://car.mitre.org/analytics/by_technique

| | | |
|---|---|--|
| T1049: System Network Connections Discovery | (N/A - technique only) | <ul style="list-style-type: none"> • CAR-2013-04-002: Quick execution of a series of suspicious commands |
| T1053: Scheduled Task/Job | T1053.005: Scheduled Task | <ul style="list-style-type: none"> • 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 | <ul style="list-style-type: none"> • 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 | <ul style="list-style-type: none"> • 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("*SHTASKS*") 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="*SHTASKS*" (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 #10

Created 2023-08-16 12:12:06 UTC by Boris RZR

Updated 2025-05-27 12:09:04 UTC by Boris RZR