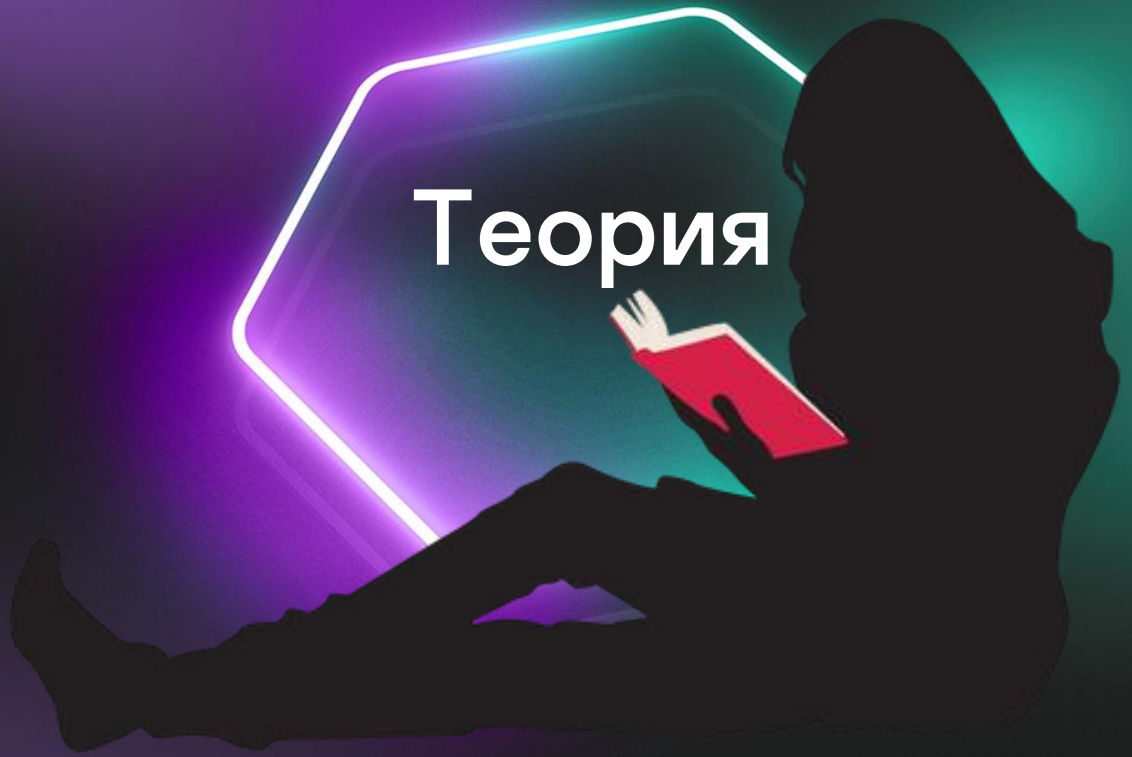
Kaspersky
Security Day
2021

Источники обнаружения в вашем SOC

Сергей Солдатов,
руководитель центра
мониторинга кибербезопасности

kaspersky

Теория



Когда нет\мало практики – от каталогов угроз

Техники атак → **Варианты обнаружения** → **Сенсоры и телеметрия**

Procedure Examples

ID	Name	Description
G0108	Blue Mockingbird	Blue Mockingbird has used JuicyPotato to ab
S0038	Duqu	Duqu examines running system processes fo attached. It can also steal tokens to acquire a
S0363	Empire	Empire can use PowerSploit's `Invoke-TokenM`
G0037	FIN6	FIN6 has used has used Metasploit's named-p

Detection

If an adversary is using a standard command-line shell, analysts can detect token manipulation by auditing default in Windows.[17]

If an adversary is using a payload that calls the Windows token APIs directly, analysts can detect token mar network behavior.

There are many Windows API calls a payload can take advantage of to manipulate access tokens (e.g., `Log` information.

Query systems for process and thread token information and look for inconsistencies such as user owns p

Look for inconsistencies between the various fields that store PPID information, such as the EventHeader F and ParentProcessID (which are also produced from ETW and other utilities such as Task Manager and Pro

ⓘ **Data Sources:** Command: Command Execution, Driver: Driver Load, File: File Creation, File: File Modification, Kernel: Kernel Module Load, Module: Module Load, Process: OS API Execution, Process: Process Creation, Windows Registry: Windows Registry Key Creation, Windows Registry: Windows Registry Key Modification

Wednesday, December 26, 2018

Использование MITRE ATT&CK в работе центров мониторинга

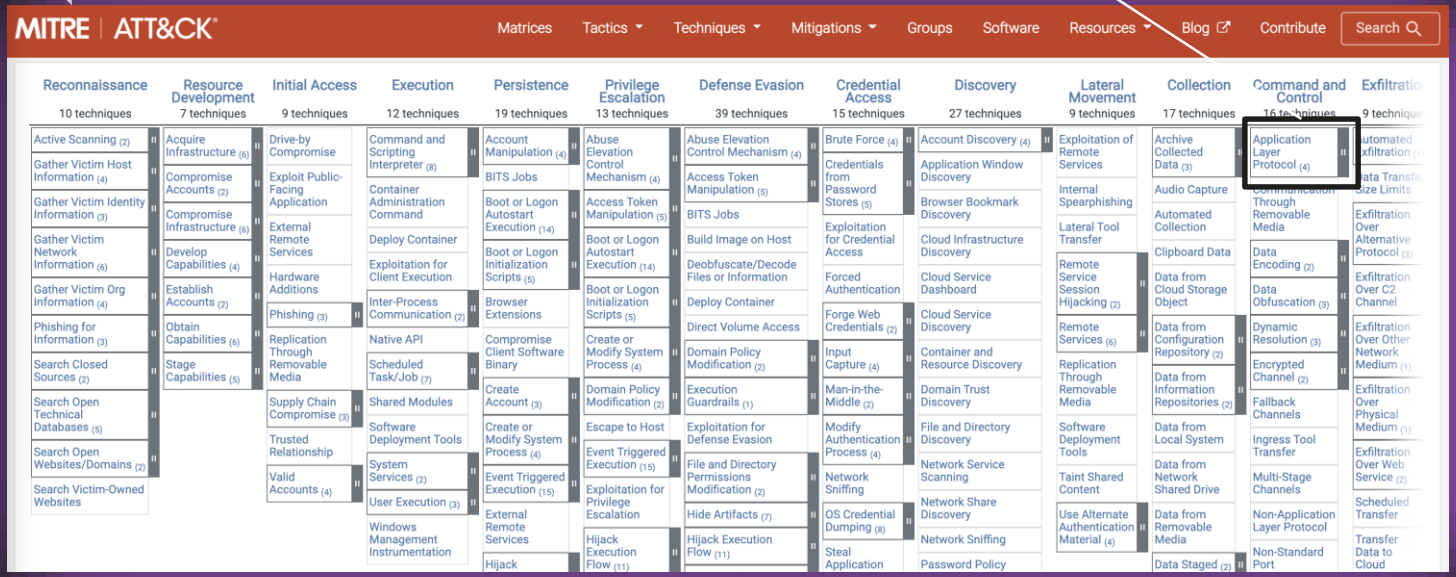
Вчера был на мероприятии, где с коллегой рассказывали о сценариях использования MITRE ATT&CK на практике. Мероприятие транслировалось и имеется запись. Мы немного коснулись технических внутренностей инфраструктуры сервиса KMP, поэтому доклад может быть полезен для практиков, решающих схожие задачи.

Вопрос практического применения ATT&CK раскрыт и в оригинальных документах MITRE, например, здесь, поэтому отмечу кратко лишь несколько моментов.

https://reply-to-all.blogspot.com/2018/12/mitre-att.html

Эффективность и результативность обнаружения

- Больше техник/подтехник
- Как можно раньше

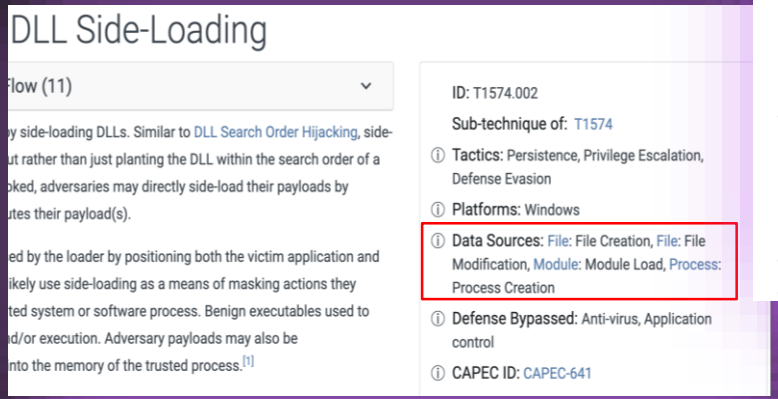


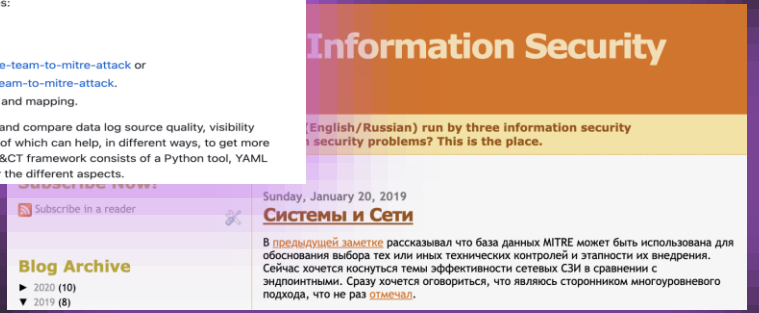
Тактики и среда обнаружения (на примере Enterprise)

Reconnaissance	Network
Resource Development	Threat Intelligence
Initial Access	Network
	Endpoint
Execution	Endpoint
Persistence	Endpoint
Privilege Escalation	Endpoint
Defense Evasion	Network
	Endpoint
Credential Access	Endpoint
Discovery	Network
	Endpoint
Lateral Movement	Network
	Endpoint
Collection	Endpoint
Command and Control	Network
	Endpoint
Exfiltration	Network
	Endpoint
Impact	Network
	Endpoint

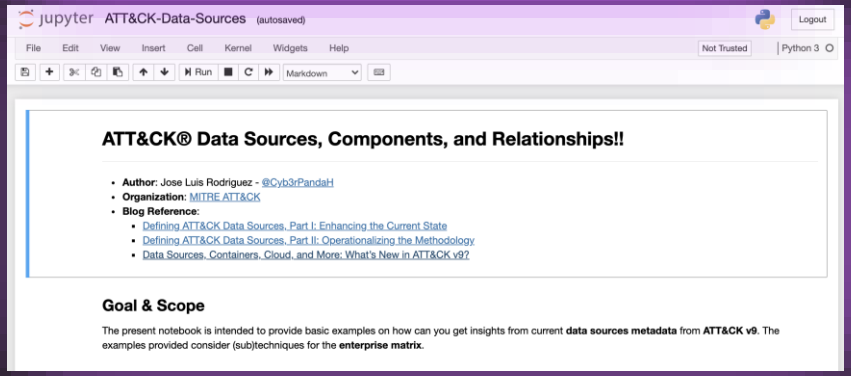
От техник к источникам событий

https://github.com/rabobank-cdc/DeTTECT

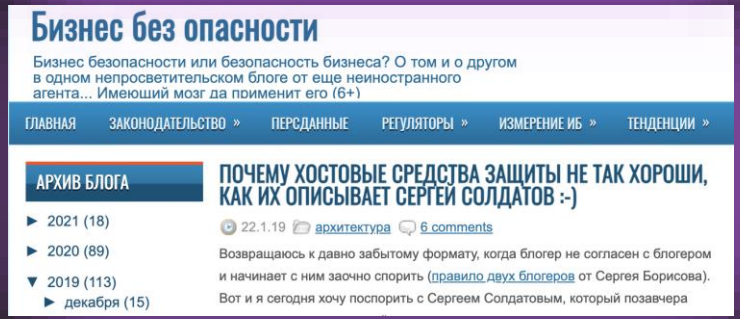




https://reply-to-all.blogspot.com/2019/01/blog-post.htm



https://github.com/mitre-attack/attack-datasources



https://lukatsky.blogspot.com/2019/01/blog-post_22.html

Категории детекторов от MITRE

Ничего

Телеметрия

Низкоуровневые события, никакого контекста

General

Что-то плохое случилось. Не ясно Что делают и Как

Тактика

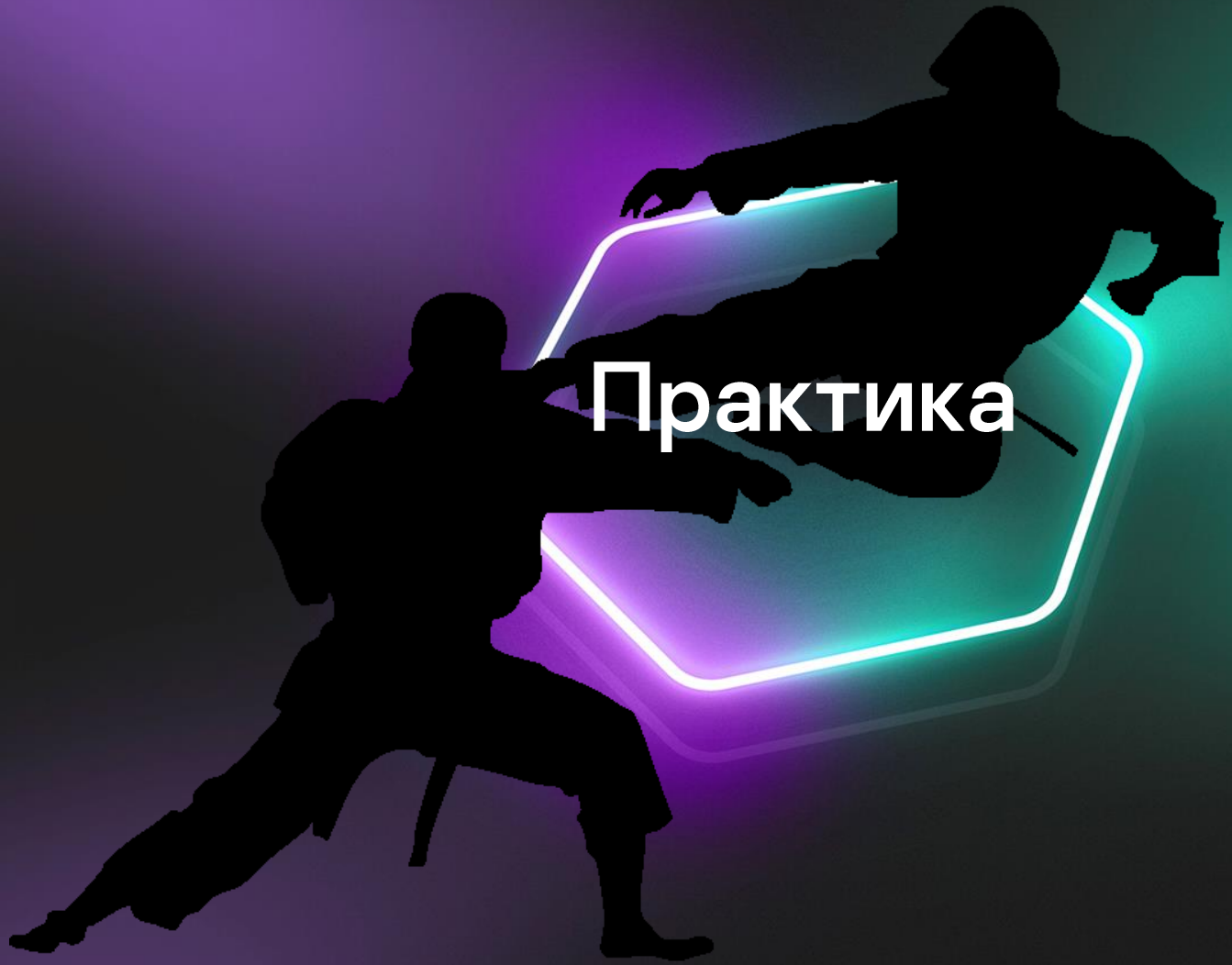
Ясно Что делают

Техника

Ясно Что и Как делают

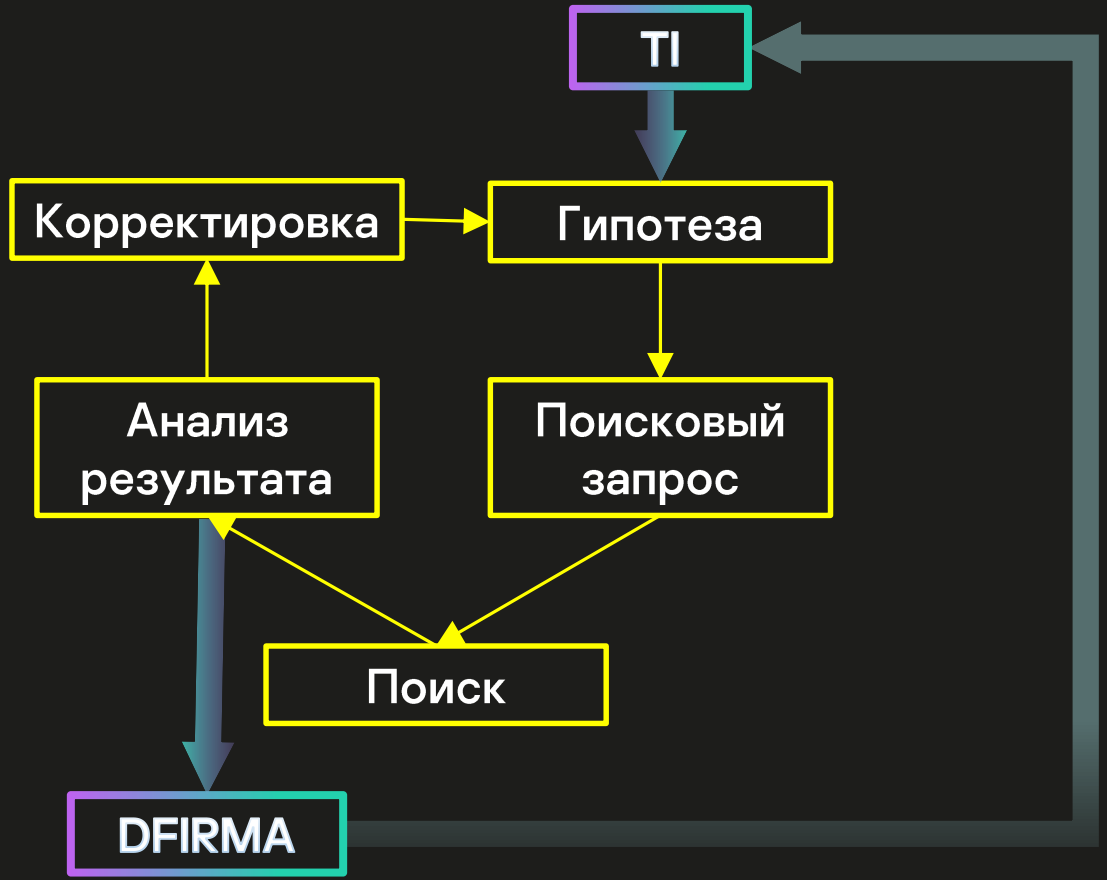
Больше контекста

https://attackevals.mitre-engenuity.org/enterprise/carbanak_fin7/detection-categories.html



Практика

Категории детекторов или история Хантов



Категории детекторов или история Хантов

Тактика

Техника

TI

Гипотеза

Поисковый запрос

Поиск

Анализ результата

Корректировка

DFIRMA

IoA (Hunts)

Критичность

Точность

Агрегация

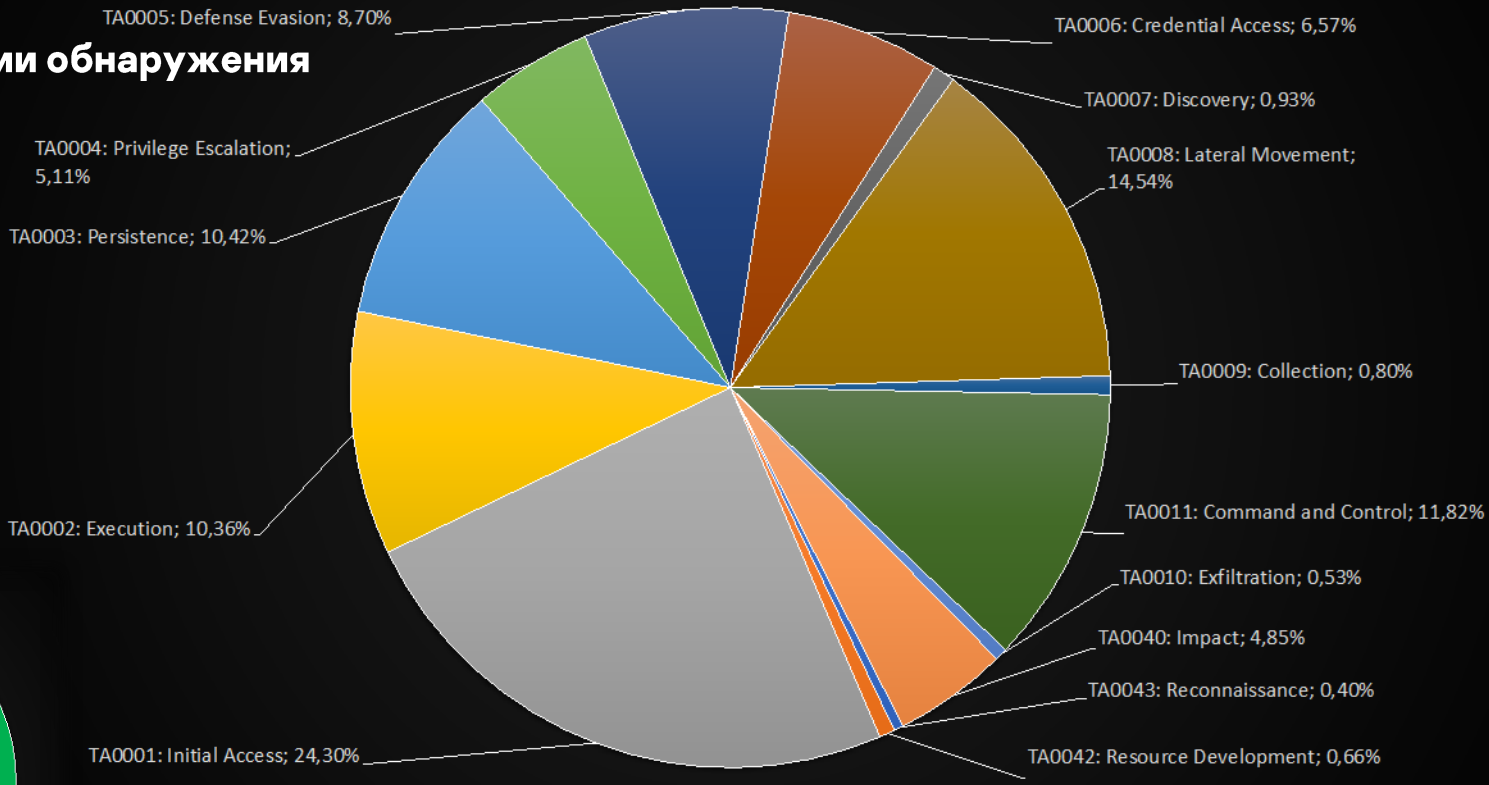
Корреляция

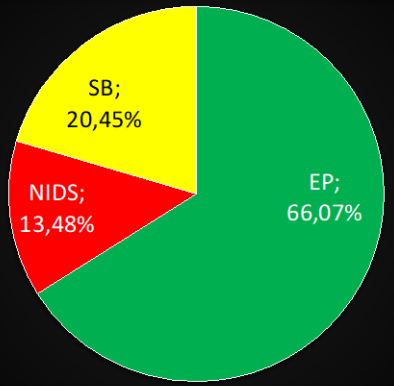
Алерты

OFFTOPIC: Метрики хантов

- Эффективность (конверсия, %)
- Результативность (вклад, %)
- Среднее время на анализ Аналитиком (мин)
- Корректность интерпретации Аналитиком (%)

Тактики и технологии обнаружения



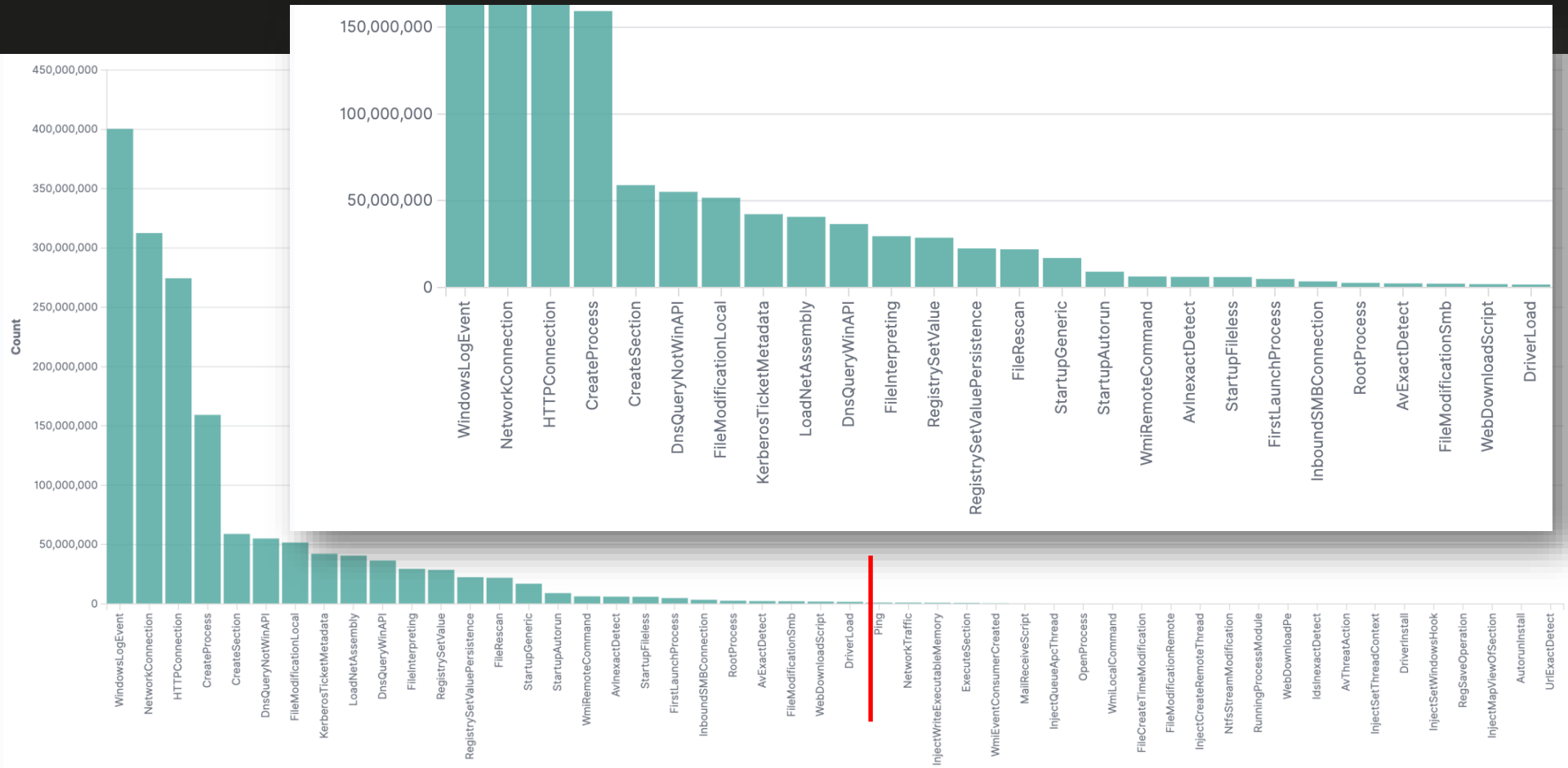


Тактики и технологии обнаружения

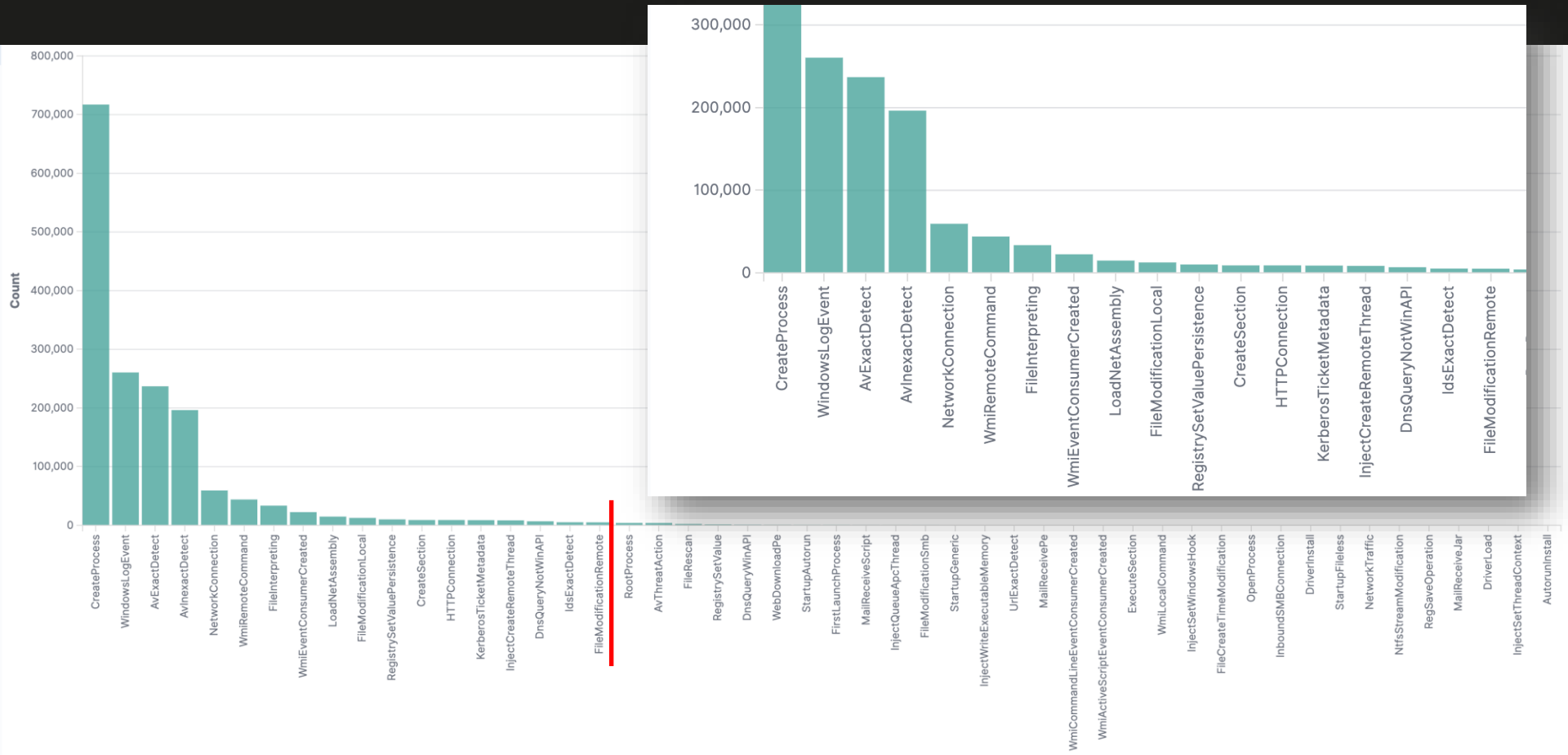
	TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion	TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
SB	0,00%	0,00%	20,32%	0,13%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%
NIDS	0,27%	0,00%	1,06%	0,07%	0,07%	0,00%	0,00%	0,20%	0,20%	1,00%	0,00%	9,83%	0,53%	0,27%
EP	0,13%	0,66%	2,92%	10,16%	10,36%	5,11%	8,70%	6,37%	0,73%	13,55%	0,80%	1,99%	0,00%	4,58%

Посмотрим ближе...

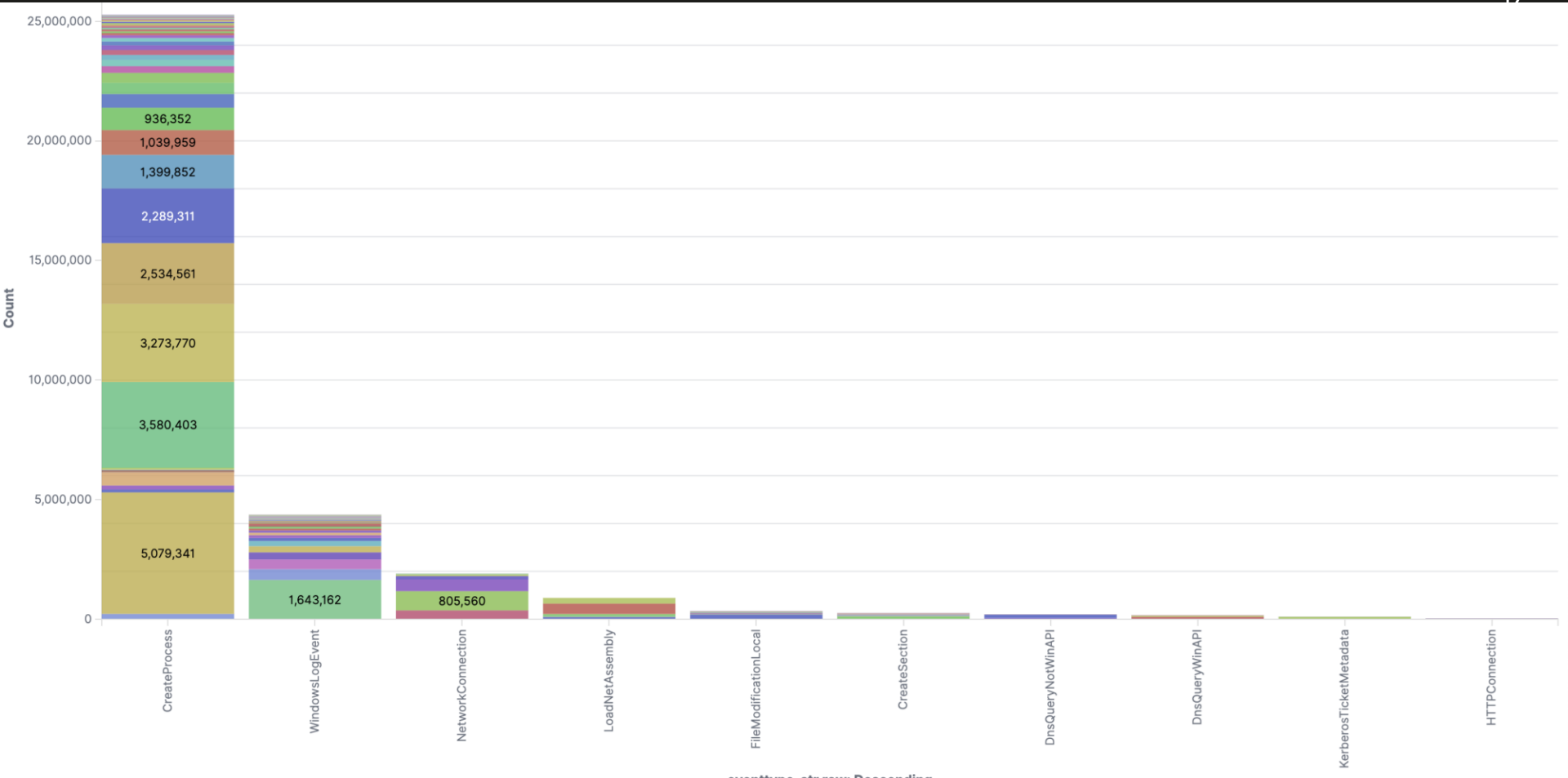
TOP 50 событий за 24 часа



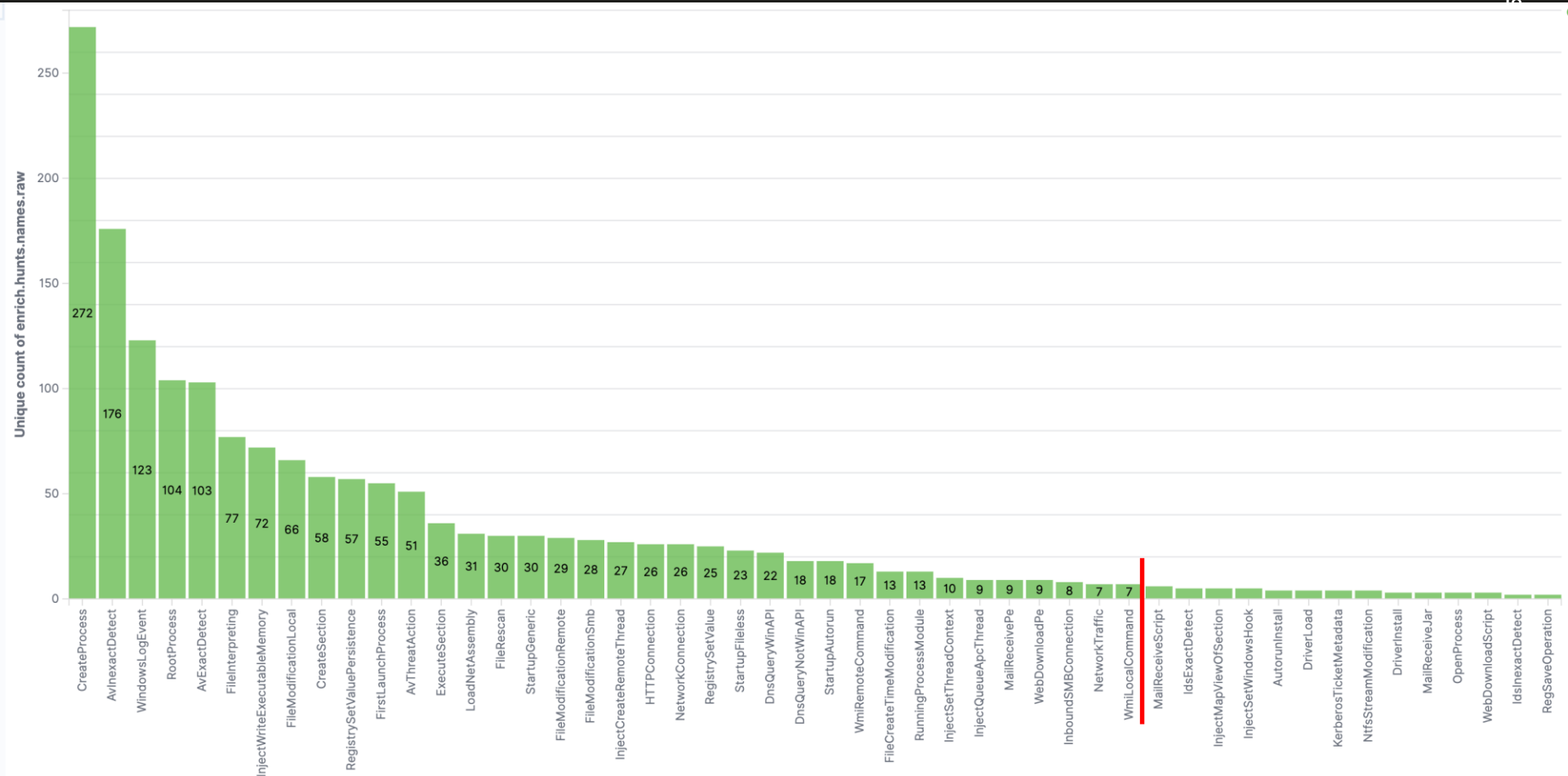
TOP 50 событий за 24 часа, размеченных хантами



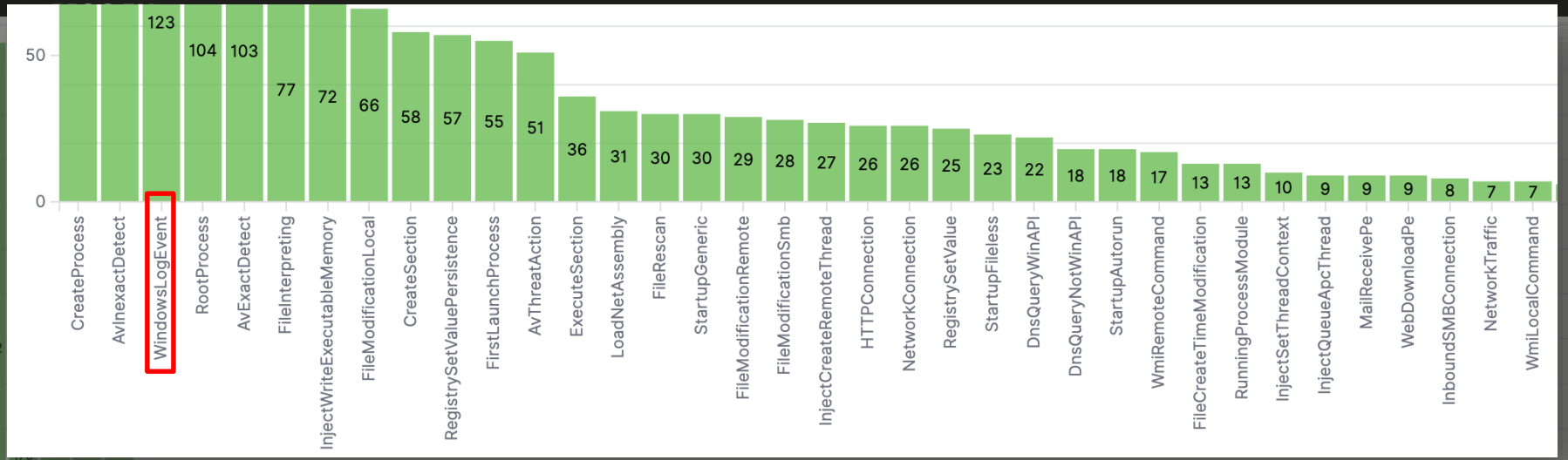
TOP 10 событий, размеченных хантами за последний месяц



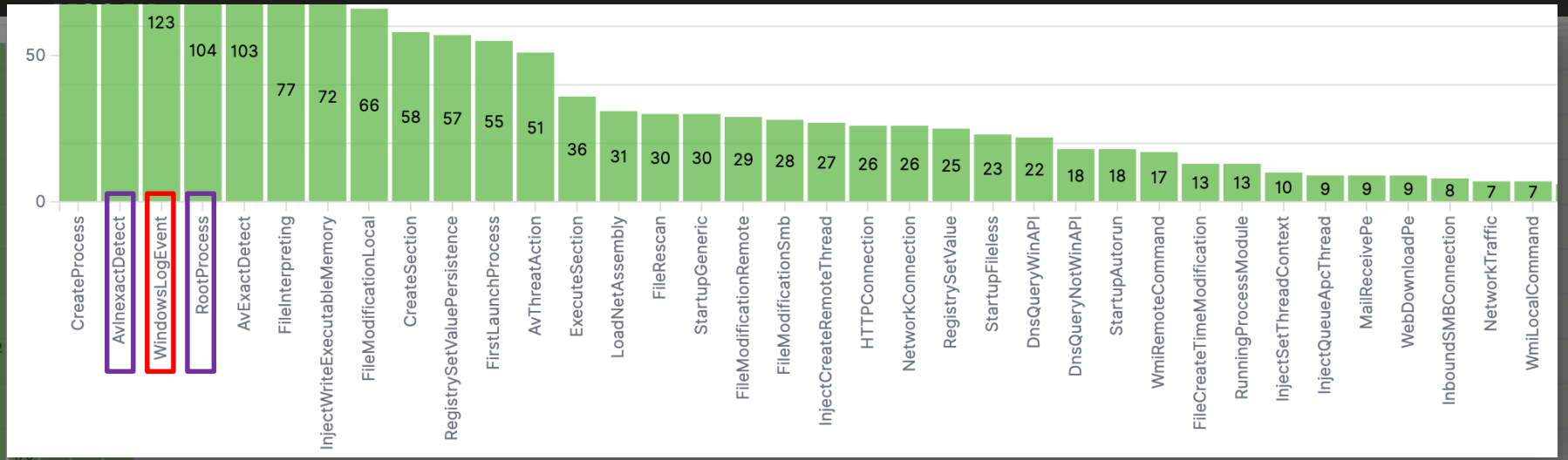
TOP 50 событий, размеченных уникальными хантами за последний месяц



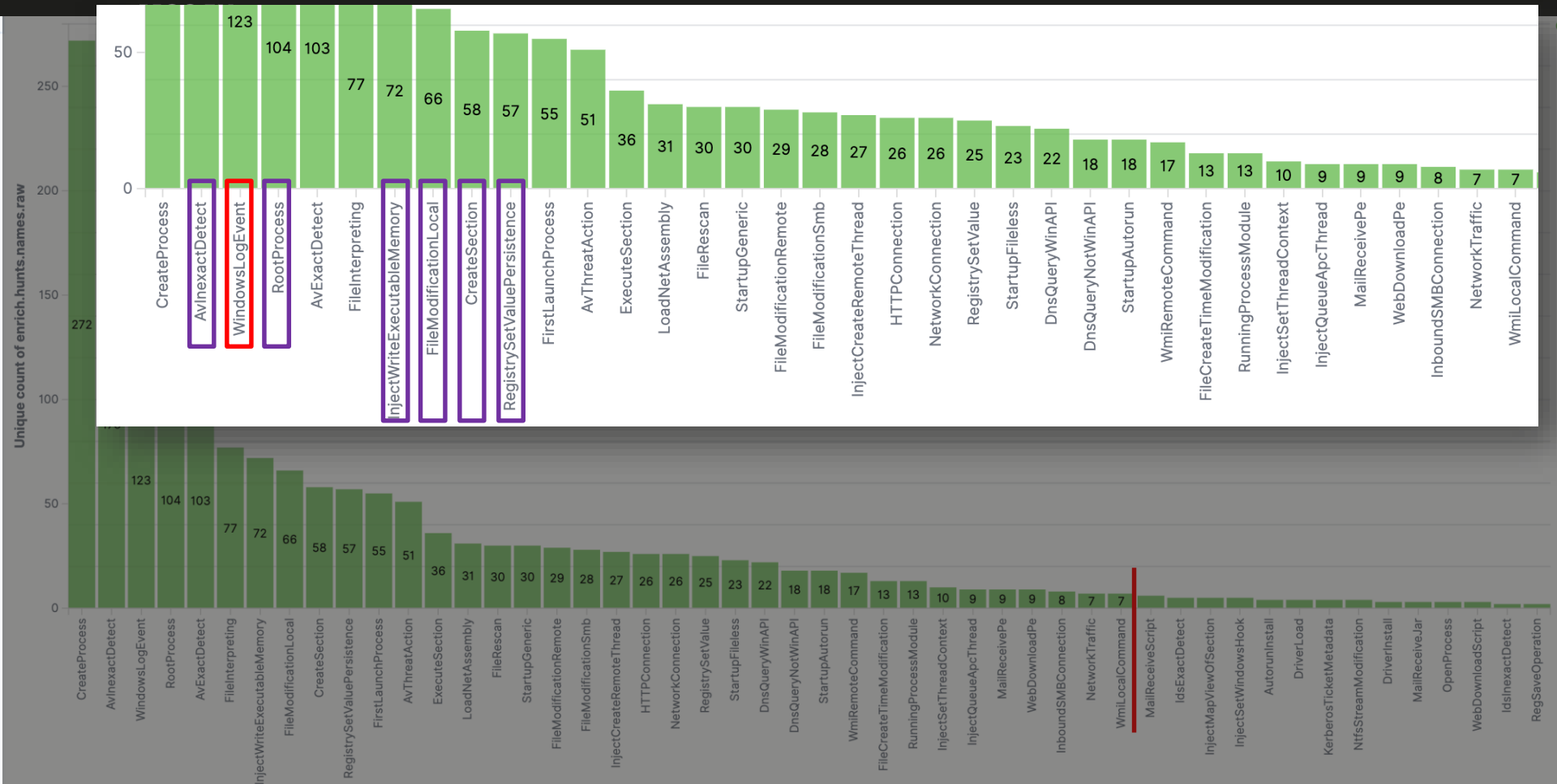
TOP 50 событий, размеченных уникальными хантами за последний



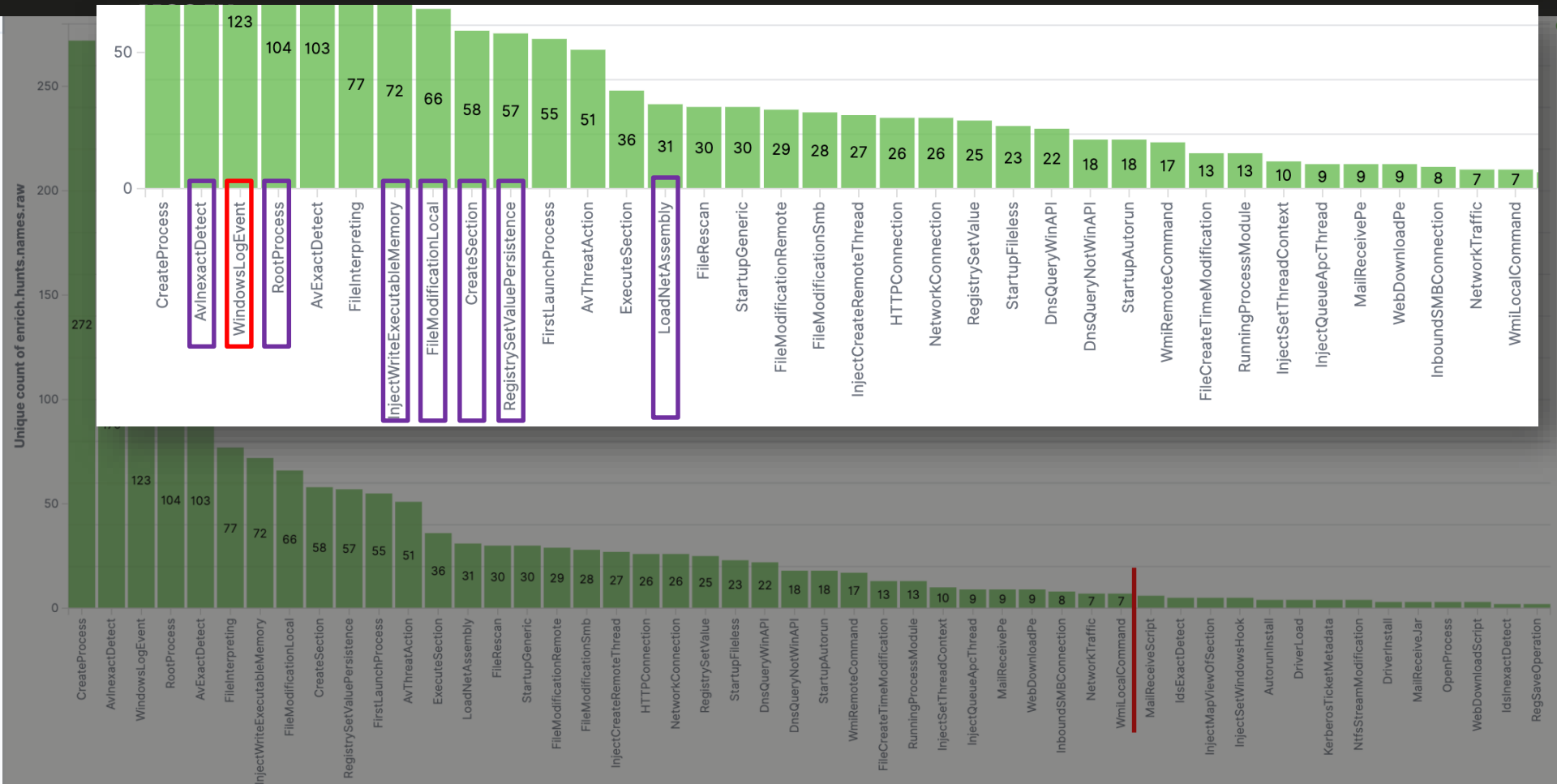
TOP 50 событий, размеченных уникальными хантами за последний



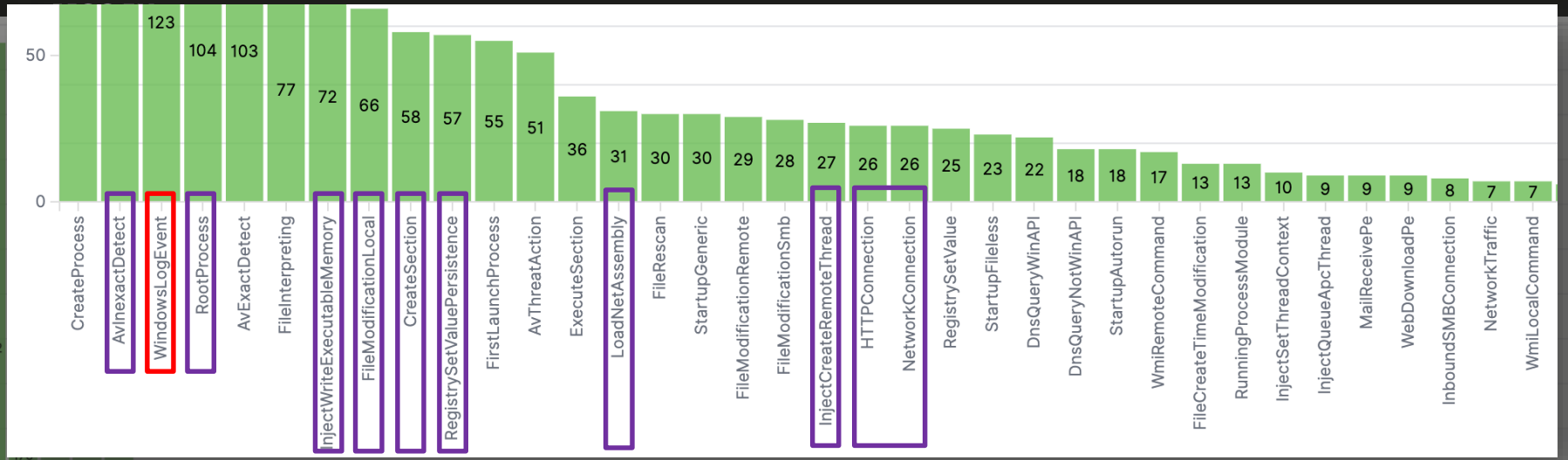
TOP 50 событий, размеченных уникальными хантами за последний



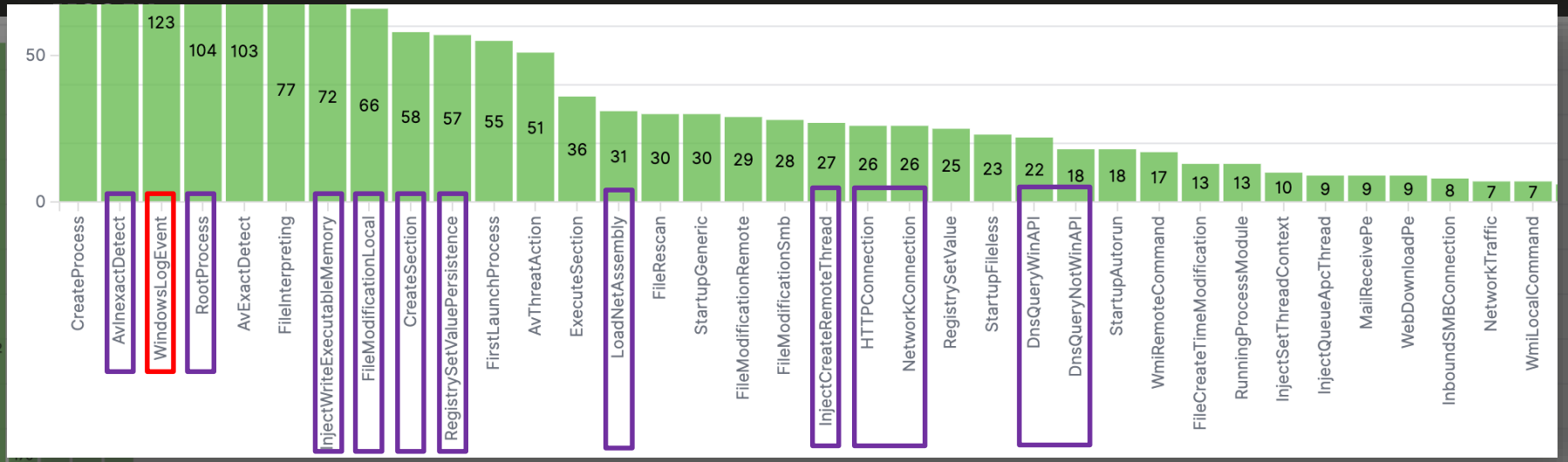
TOP 50 событий, размеченных уникальными хантами за последний



TOP 50 событий, размеченных уникальными хантами за последний

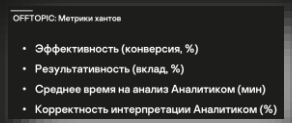


TOP 50 событий, размеченных уникальными хантами за последний



Выводы

- Обнаруживайте и на конечной точке и на сети
- События ОС очень важны
- Но есть масса других очень важных событий
- Начните с MITRE ATT&CK
- Постоянно измеряйте ваши детекторы
- Переиспользуйте практики SOC & DFIRMA для улучшения детекторов



Спасибо!

kaspersky