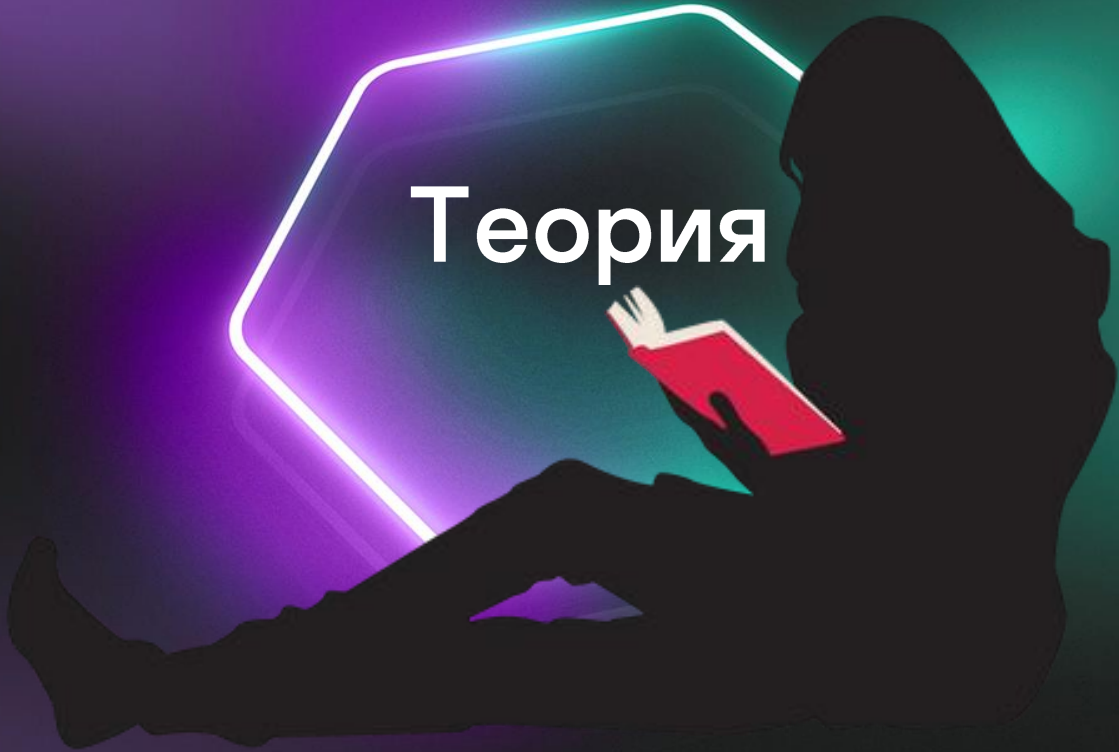


**Kaspersky
Security Day
2021**

Источники обнаружения в вашем SOC

kaspersky

Сергей Солдатов,
руководитель центра
мониторинга кибербезопасности



Теория



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

4

- Больше техник/подтехник
- Как можно раньше

MITRE | ATT&CK

Matrices

Tactics

Techniques

Mitigations

Groups

Software

Resources

Blog

Contribute

Search

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	39 techniques	15 techniques	27 techniques	9 techniques	17 techniques	16 techniques	9 techniques
Active Scanning (2) Gather Victim Host Information (4) Gather Victim Identity Information (3) Gather Victim Network Information (6) Gather Victim Org Information (4) Phishing for Information (3) Search Closed Sources (2) Search Open Technical Databases (5) Search Open Websites/Domains (2) Search Victim-Owned Websites	Acquire Infrastructure (6) Compromise Accounts (2) Compromise Infrastructure (6) Develop Capabilities (4) Establish Accounts (2) Obtain Capabilities (6) Stage Capabilities (5) Supply Chain Compromise (3) Trusted Relationship Valid Accounts (4)	Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (3) Replication Through Removable Media Shared Chain Compromise (3) Software Deployment Tools System Services (2) User Execution (3) Windows Management Instrumentation	Command and Scripting Interpreter (8) Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (2) Native API Scheduled Task/Job (7) Shared Modules Software Deployment Tools System Services (2) User Execution (3) Windows Management Instrumentation	Account Manipulation (4) BITS Jobs Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (5) Boot or Logon Initialization Scripts (5) Browser Extensions Compromise Client Software Binary Create Account (3) Create or Modify System Process (4) Event Triggered Execution (15) Event Triggered Execution (15) External Remote Services HiJack	Abuse Elevation Control Mechanism (4) Access Token Manipulation (5) Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (5) Create or Modify System Process (4) Domain Policy Modification (2) Escape to Host Event Triggered Execution (15) Exploitation for Privilege Escalation HiJack Execution Flow (11)	Abuse Elevation Control Mechanism (4) Access Token Manipulation (5) BITS Jobs Build Image on Host Deobfuscate/Decode Files or Information Deploy Container Direct Volume Access Domain Policy Modification (2) Execution Guardrails (1) Exploitation for Defense Evasion File and Directory Permissions Modification (2) Hide Artifacts (7) HiJack Execution Flow (11)	Brute Force (4) Credentials from Password Stores (5) Exploitation for Credential Access Forced Authentication Forge Web Credentials (2) Input Capture (4) Man-in-the-Middle (2) Modify Authentication Process (4) Network Sniffing OS Credential Retirement (8) Steal Application	Account Discovery (4) Application Window Discovery Browser Bookmark Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Container and Resource Discovery Domain Trust Discovery File and Directory Discovery Network Service Scanning Network Share Discovery Network Sniffing Password Policy	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (2) Remote Services (6) Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (4) Data Staged (2)	Archive Collected Data (3) Audio Capture Automated Collection Clipboard Data Data from Cloud Storage Object Data from Configuration Repository (2) Data from Information Repositories (2) Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged (2)	Application Layer Protocol (4) Communication Through Removable Media Data Encoding (2) Data Obfuscation (3) Dynamic Resolution (3) Encrypted Channel (2) Failback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port	Automated Exfiltration (1) Data Transfer Size Limits Exfiltration Over Alternative Protocol (3) Exfiltration Over C2 Channel Exfiltration Over Other Network Medium (1) Exfiltration Over Physical Medium (1) Exfiltration Over Web Service (2) Scheduled Transfer Transfer Data to Cloud

Тактики и среда обнаружения (на примере Enterprise)

5

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

DLL Side-Loading

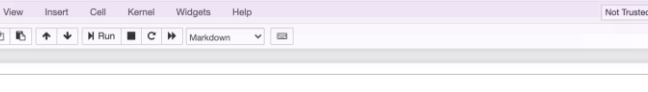
by side-loading DLLs. Similar to [DLL Search Order Hijacking](#), side-loading is not just about planting the DLL within the search order of a process. Instead, adversaries may directly side-load their payloads by bypassing the search order and injecting their payload(s).

ed by the loader by positioning both the victim application and likely use side-loading as a means of masking actions they executed system or software process. Benign executables used to load and execute the payload. Adversary payloads may also be loaded into the memory of the trusted process.^[1]

ID: T1574.002

Sub-technique of: [T1574](#)

- ① **Tactics:** Persistence, Privilege Escalation, Defense Evasion
- ① **Platforms:** Windows
- ① **Data Sources:** **File:** File Creation, **File:** File Modification, **Module:** Module Load, **Process:** Process Creation
- ① **Defense Bypassed:** Anti-virus, Application control
- ① **CAPEC ID:** **CAPEC-641**



The screenshot shows a Jupyter Notebook interface. At the top, the title bar reads 'jupyter ATT&CK-Data-Sources (autosaved)'. Below this is a menu bar with 'File', 'Edit', 'View', 'Insert', 'Cell', 'Kernel', 'Widgets', and 'Help'. On the right, there's a 'Not Trusted' warning and a 'Python 3' environment indicator. The main content area displays a title slide with the heading 'ATT&CK® Data Sources, Components, and Relationships!!'. Below the heading, there is a bulleted list of information:

- **Author:** Jose Luis Rodriguez - @Cyb3rPandaH
- **Organization:** [MITRE ATT&CK](#)
- **Blog Reference:**
 - [Defining ATT&CK Data Sources, Part I: Enhancing the Current State](#)
 - [Defining ATT&CK Data Sources, Part II: Operationalizing the Methodology](#)
 - [Data Sources, Containers, Cloud, and More: What's New in ATT&CK v9?](#)

At the bottom of the slide, the section 'Goal & Scope' is visible, followed by a paragraph stating: 'The present notebook is intended to provide basic examples on how can you get insights from current **data sources metadata** from **ATT&CK v9**. The examples provided consider (sub)techniques for the **enterprise matrix**.'

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



Detect Tactics, Techniques & Combat Threats

Latest version: [1.4.3](#)

To get started with DeTT&CT, check out one of these resources:

- This [page](#) on the Wiki.
- Our [talk](#) at hack.lu 2019.
- Blog: [mbsecure.nl/blog/2019/5/dettact-mapping-your-blue-team-to-mitre-attack](#) or
- Blog: [siriussecurity.nl/blog/2019/5/8/mapping-your-blue-team-to-mitre-attack](#).
- The video from Justin Henderson on data source visibility and mapping.

DeTe&T&C aims to assist blue teams in using ATT&CK to score and compare data log source quality, visibility coverage, detection coverage and threat actor behaviours. All of which can help, in different ways, to get more resilient against attacks targeting your organisation. The DeTe&T&C framework consists of a Python tool, YAML administration files, the [DeTe&T&C Editor](#) and [scoring tables](#) for the different aspects.

Information Security

(English/Russian) run by three information security
security problems? This is the place.

Sunday, January 20, 2019

Системы и Сети

В **предыдущей заметке** рассказывал что база данных MITRE может быть использована для обоснования выбора тех или иных технических контролей и этапности их внедрения. Сейчас хочется коснуться темы эффективности сетевых СЗИ в сравнении с эндпоинтными. Сразу хочется оговориться, что являюсь сторонником многоуровневого подхода, что не раз **отмечал**.

Blog Archive

► 2020 (10)
▼ 2019 (8)

Бизнес без опасности

Бизнес безопасности или безопасность бизнеса? О том и о другом в одном непросветительском блоге от еще неиностранного агента... Имеющий мозг да применит его (6+)

[ГЛАВНАЯ](#) [ЗАКОНОДАТЕЛЬСТВО](#) » [ПЕРСОНАЛЬНЫЕ](#) [РЕГУЛЯТОРЫ](#) » [ИЗМЕРЕНИЕ ИБ](#) » [ТЕНДЕНЦИИ](#) »

АРХИВ БЛОГА

- ▶ 2021 (18)
- ▶ 2020 (89)
- ▼ 2019 (113)
 - ▶ декабря (15)

ПОЧЕМУ ХОСТОВЫЕ СРЕДСТВА ЗАЩИТЫ НЕ ТАК ХОРОШИ, КАК ИХ ОПИСЫВАЕТ СЕРГЕЙ СОЛДАТОВ :-)

22.1.19 архитектура 6 comments

Возвращаюсь к давно забытому формату, когда блогер не согласен с блогером и начинает с ним заочно спорить ([правило двух блогеров](#) от Сергея Борисова). Вот и я сегодня хочу поспорить с Сергеем Солдатовым, который позавчера

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

Категории детекторов от MITRE

Ничего

Телеметрия



General



Тактика

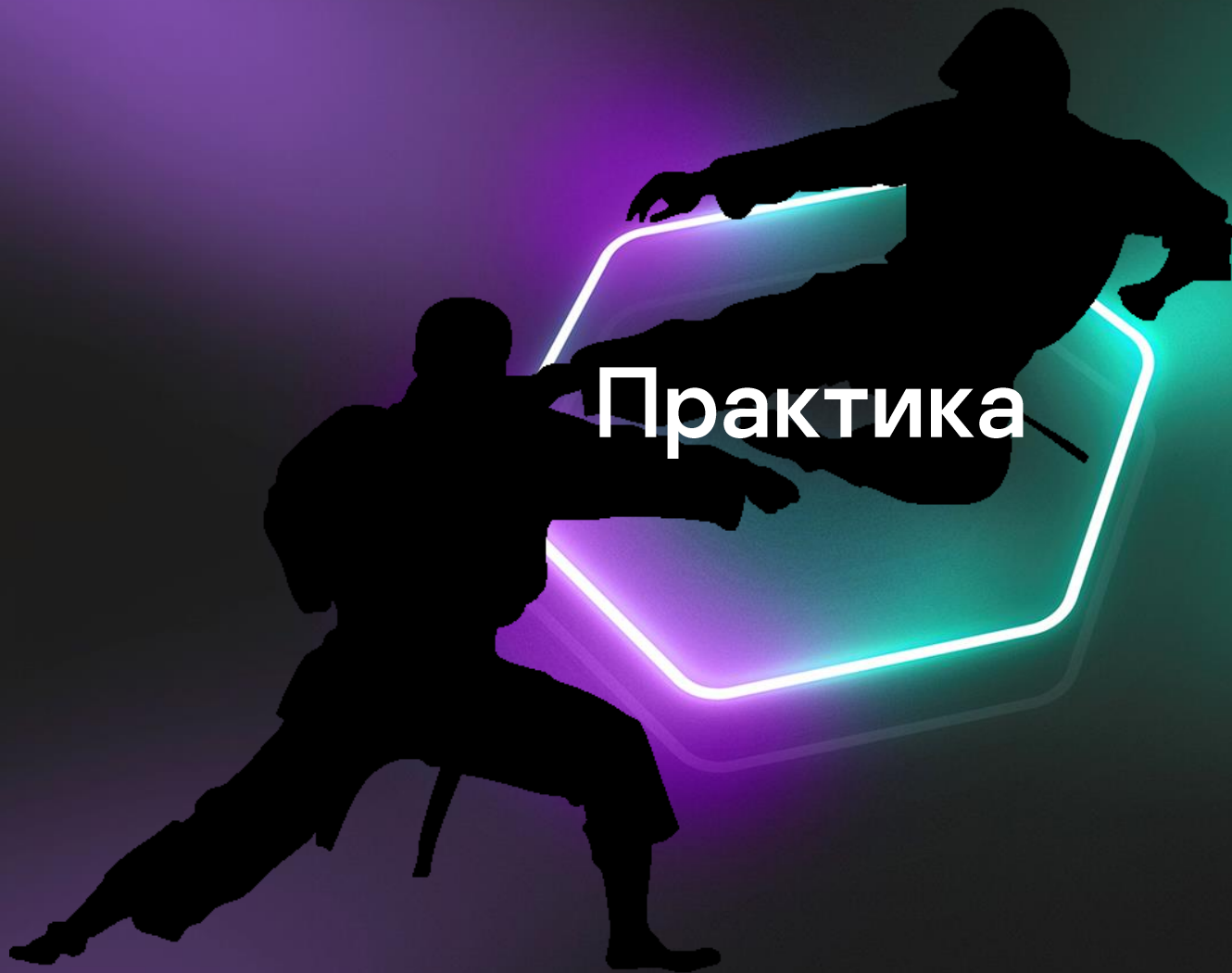


Техника



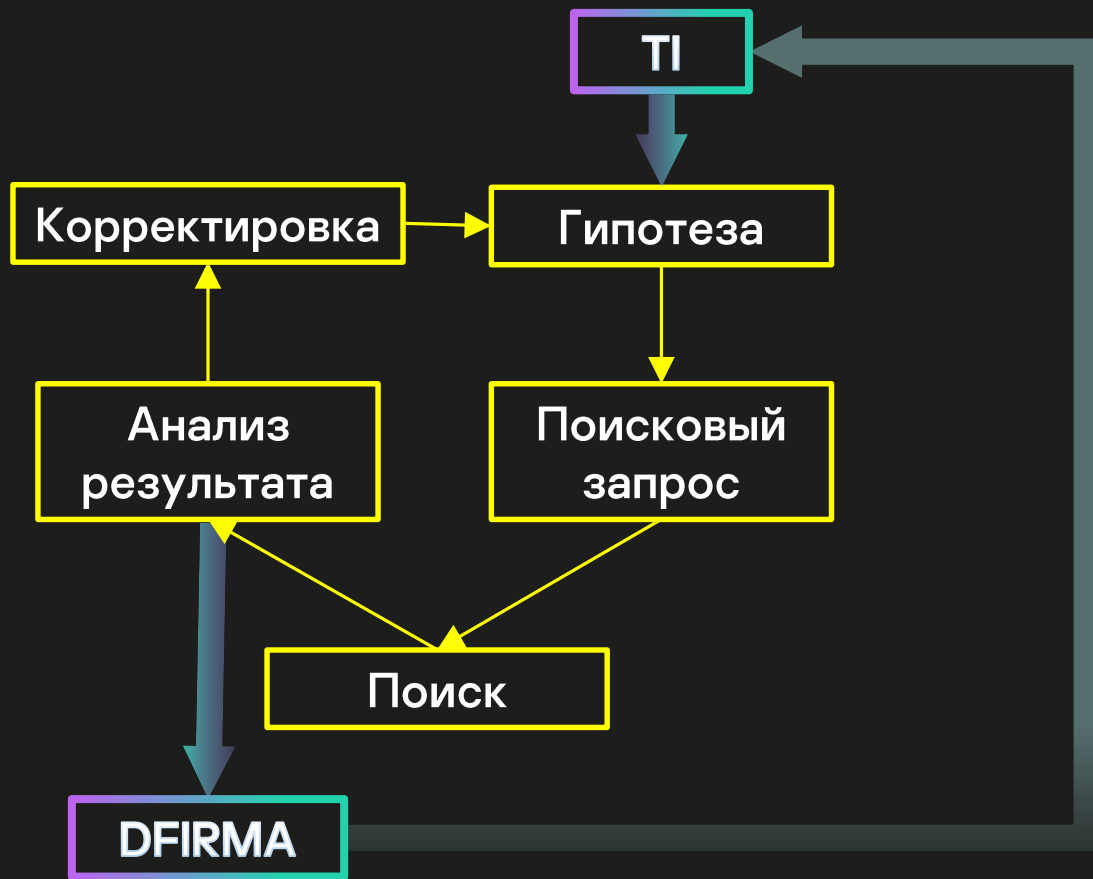
Больше
контекста

Практика



Категории детекторов или история Хантов

9



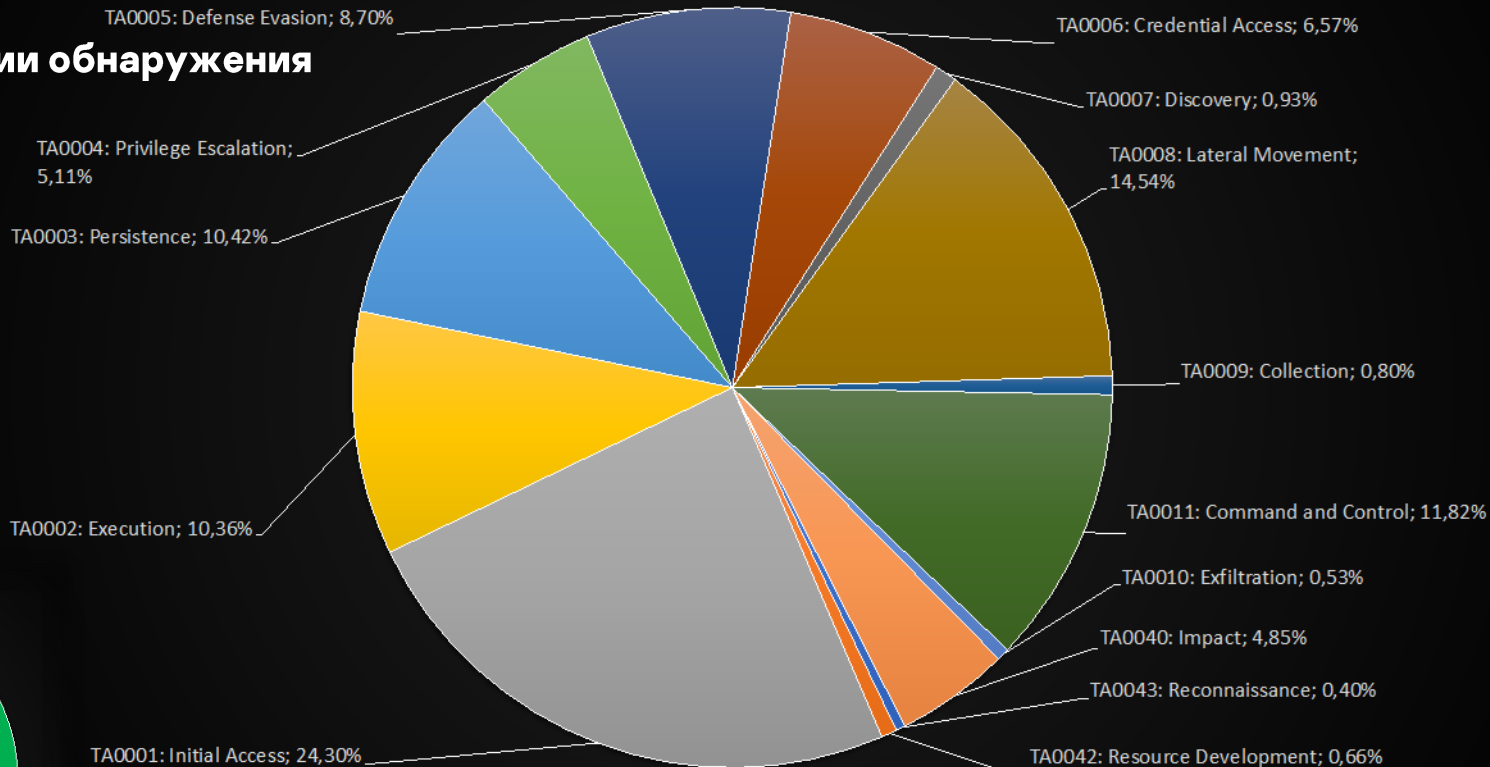
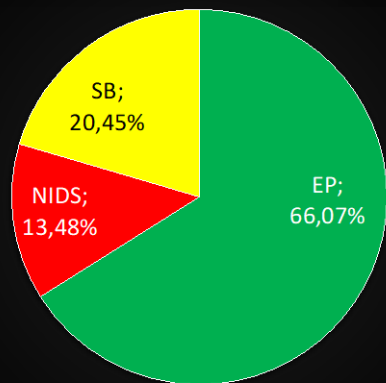
Категории детекторов или история Хантов

10



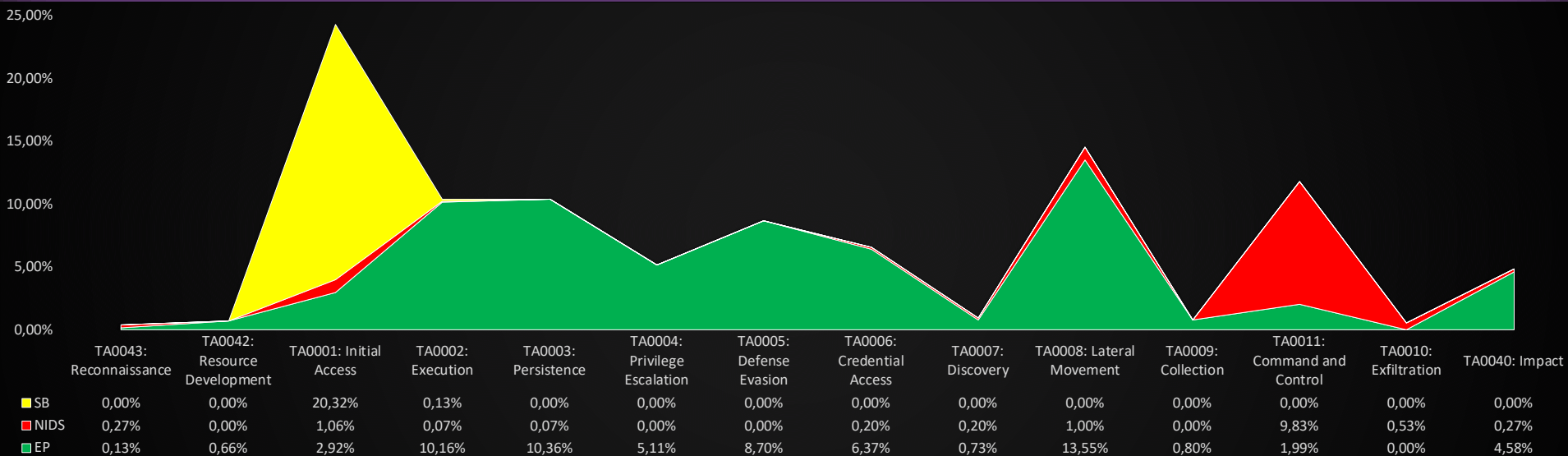
- Эффективность (конверсия, %)
- Результативность (вклад, %)
- Среднее время на анализ Аналитиком (мин)
- Корректность интерпретации Аналитиком (%)

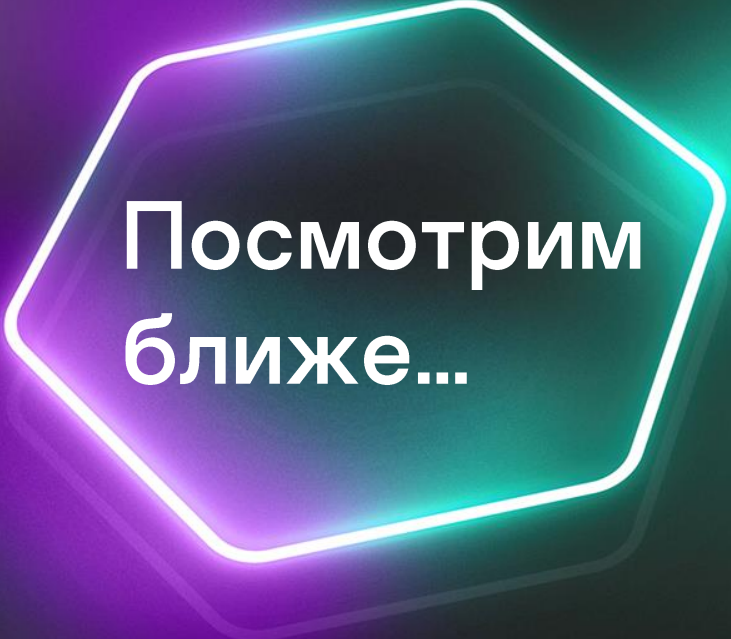
Тактики и технологии обнаружения



Тактики и технологии обнаружения

13

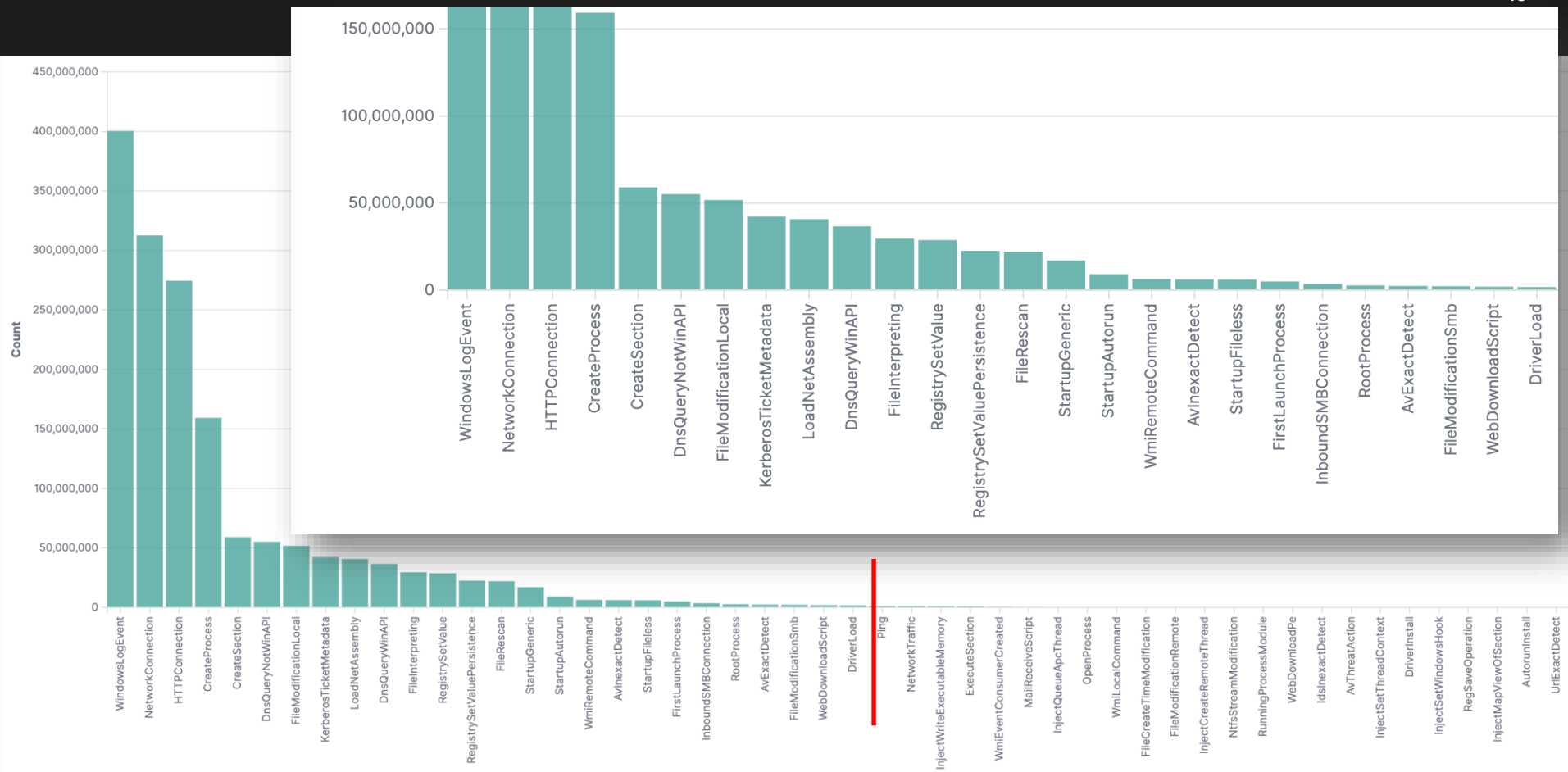




Посмотрим
ближе...

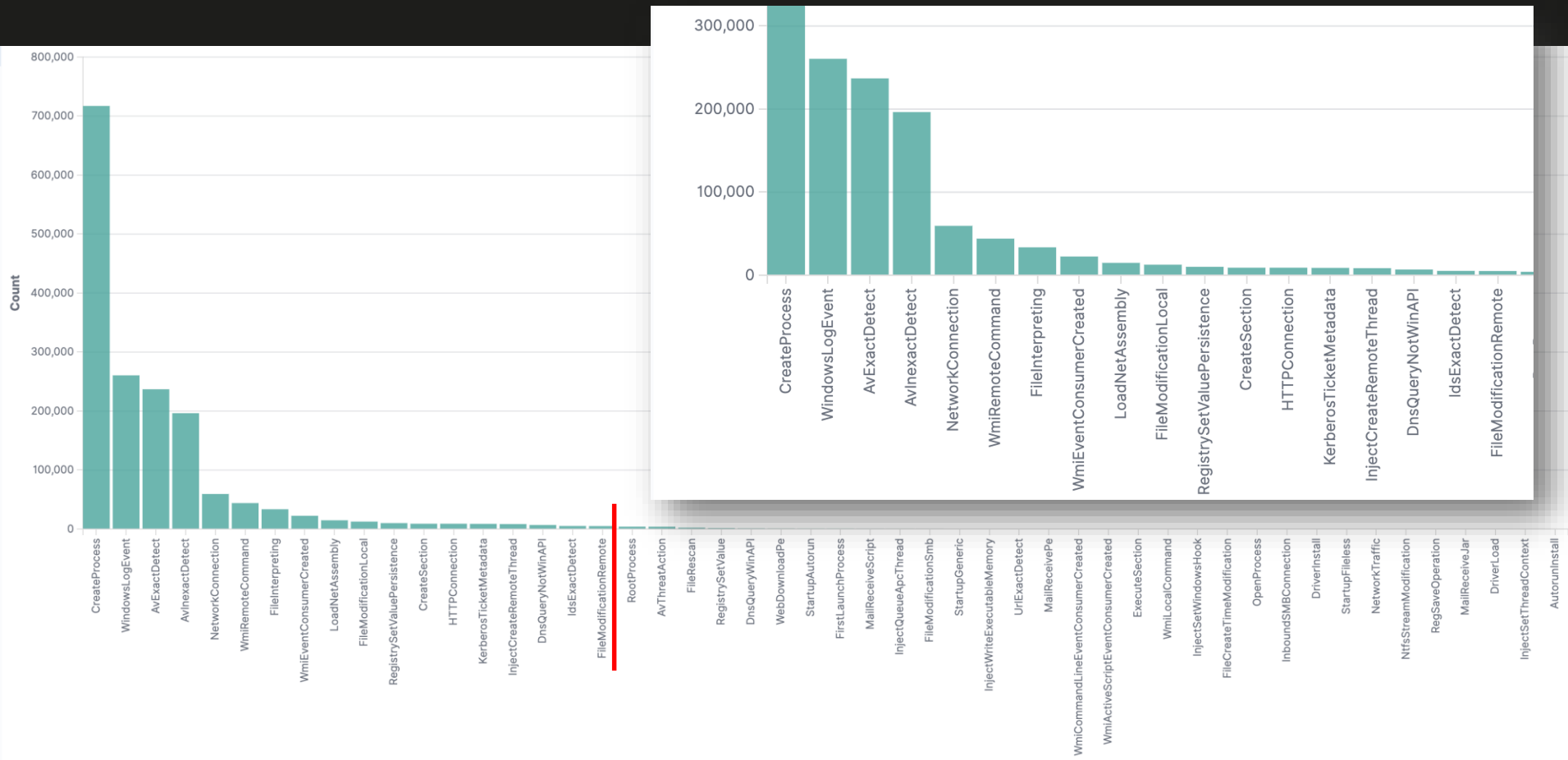
TOP 50 событий за 24 часа

15



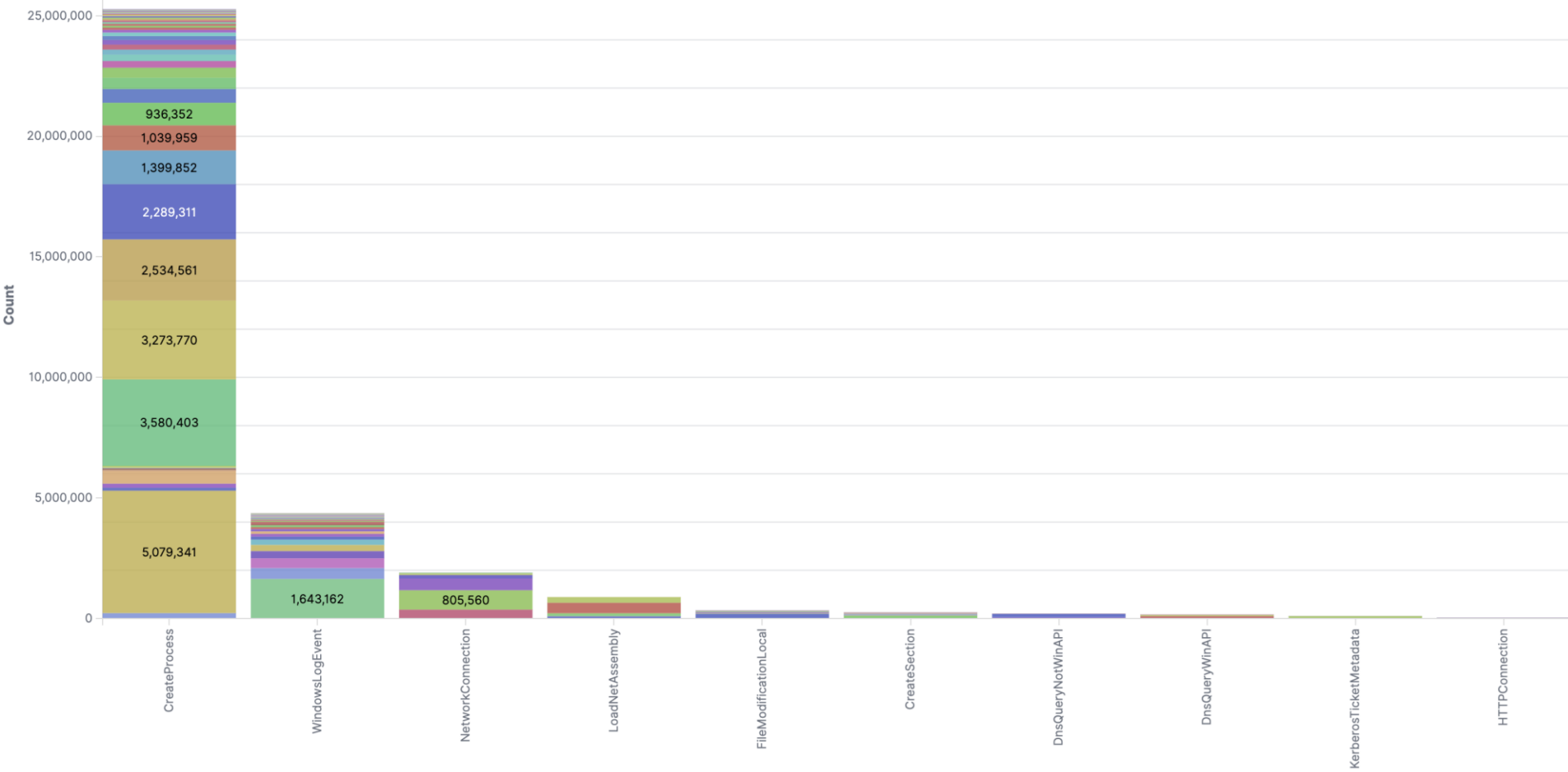
TOP 50 событий за 24 часа, размеченных хантами

16



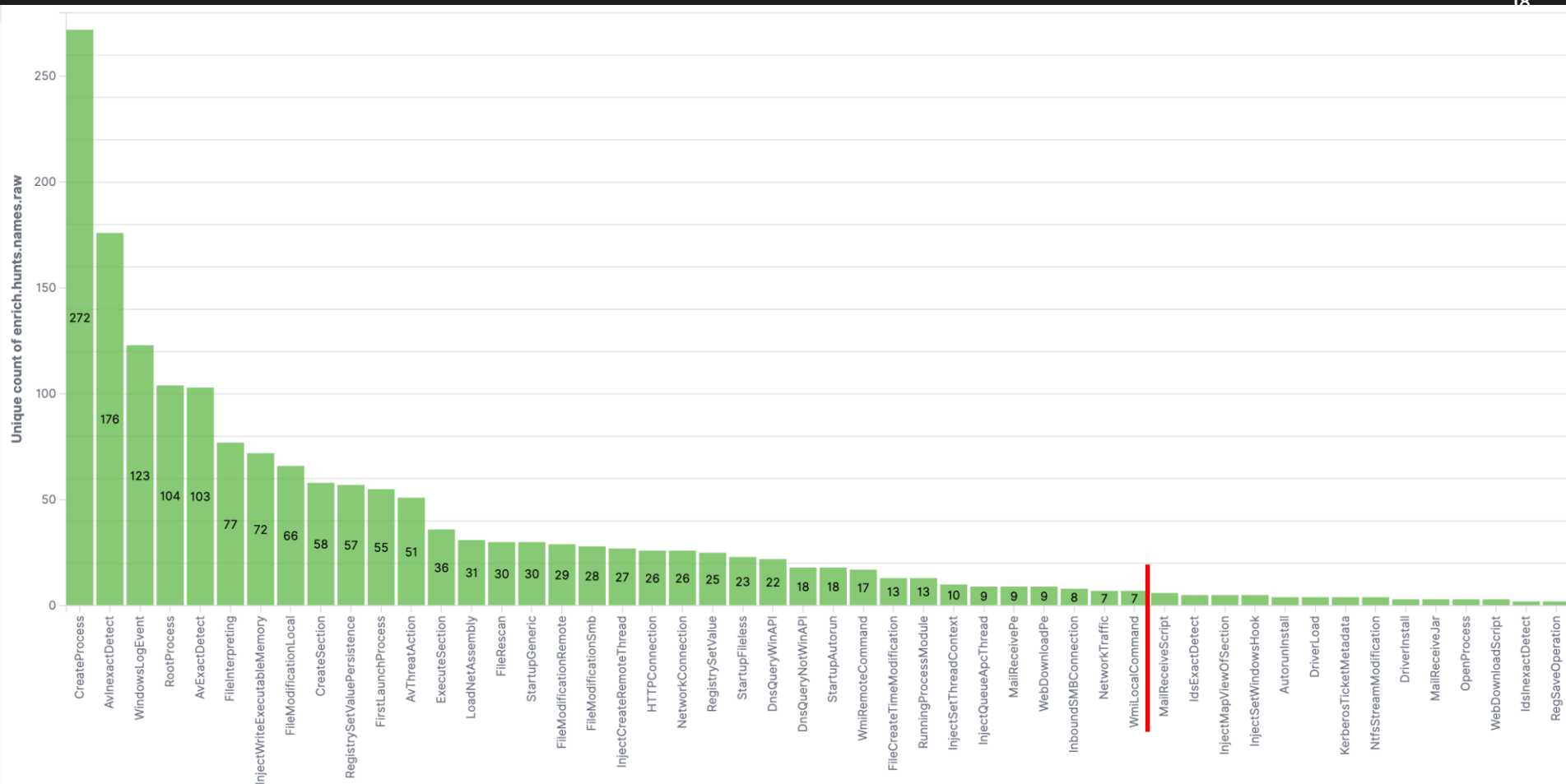
TOP 10 событий, размеченных хантами за последний месяц

17



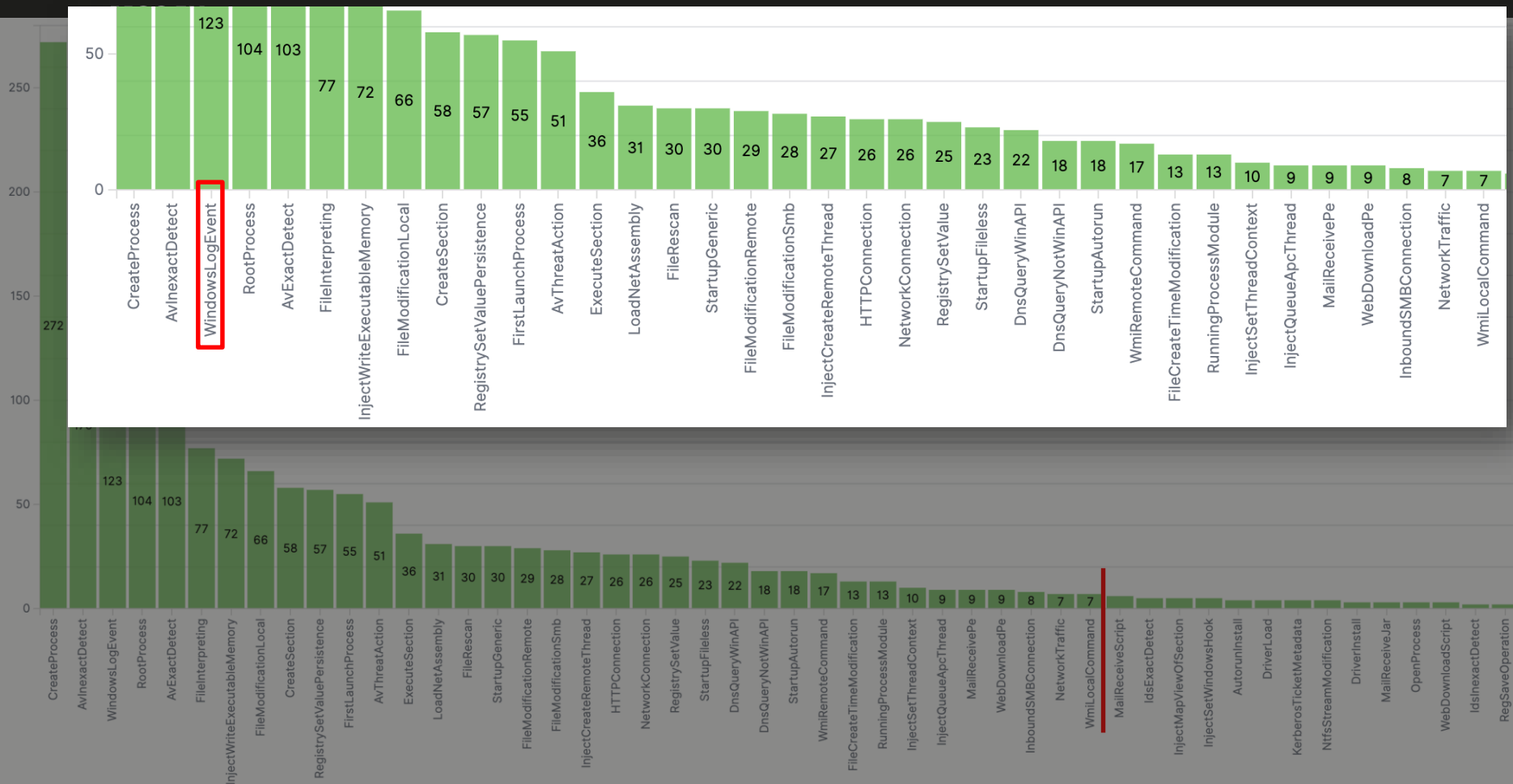
TOP 50 событий, размеченных уникальными хантами за последний месяц

18



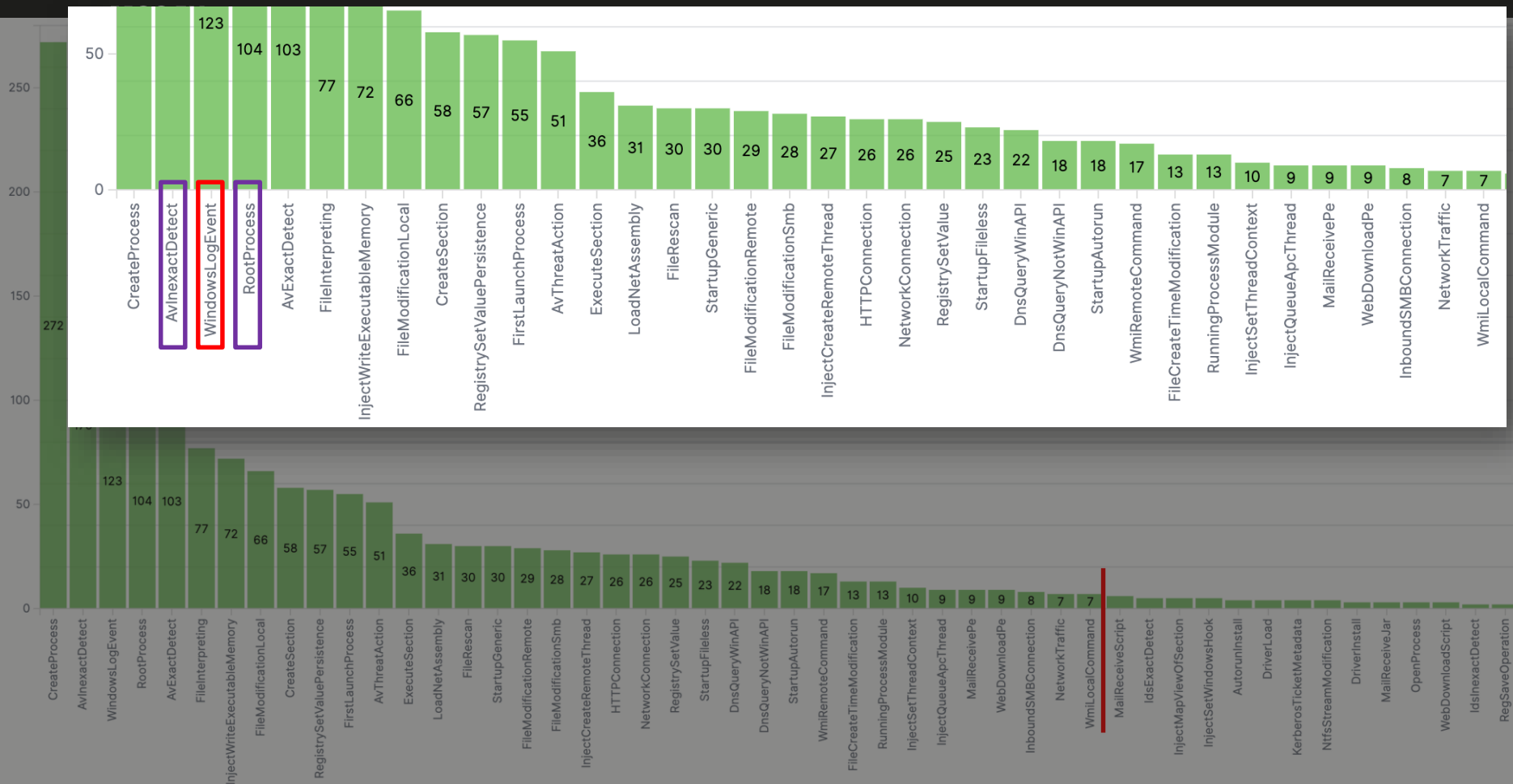
TOP 50 событий, размеченных уникальными хантами за последний

Unique count of enrich.hunts.names.raw



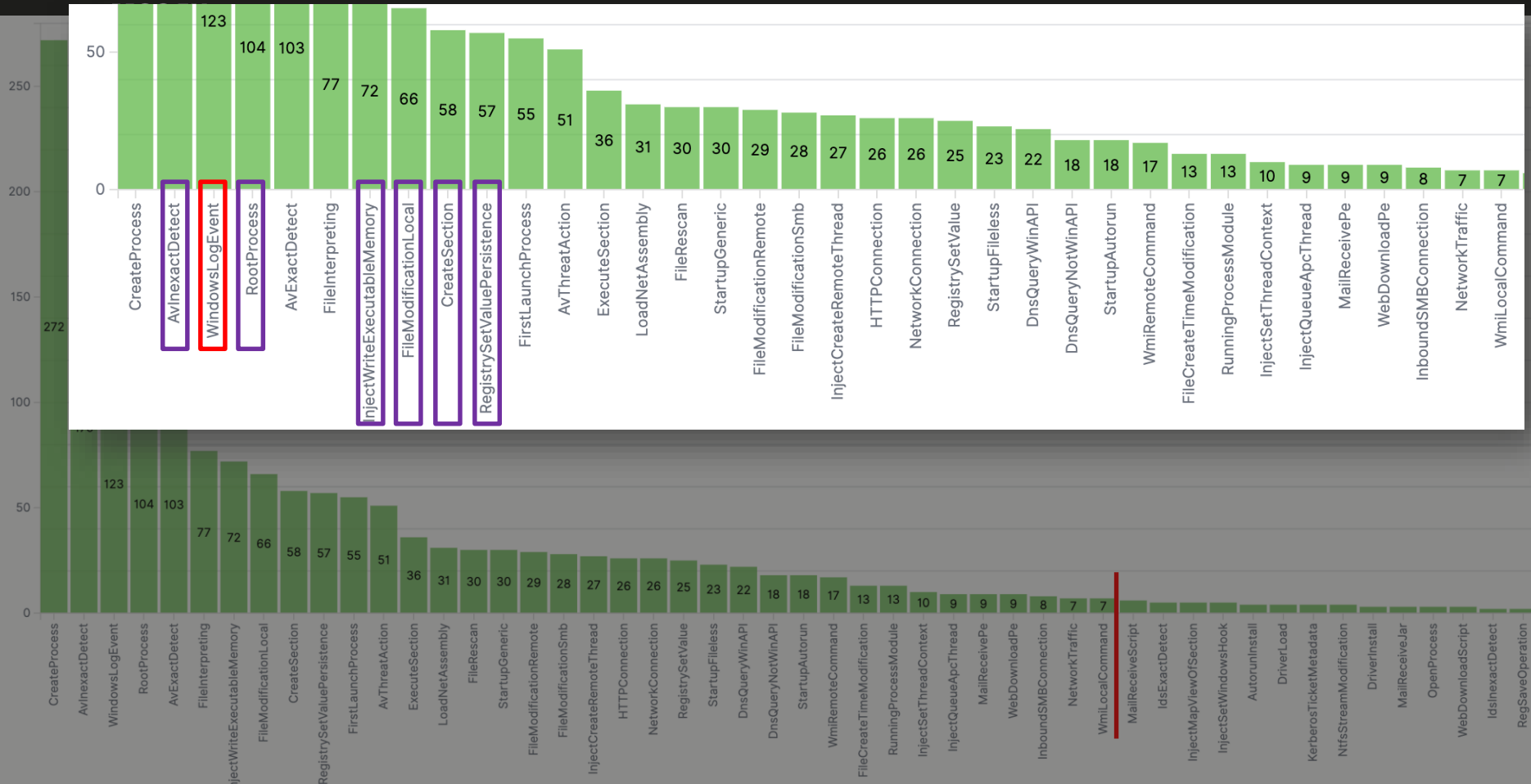
TOP 50 событий, размеченных уникальными хантами за последний

Unique count of enrich.hunts.names.raw



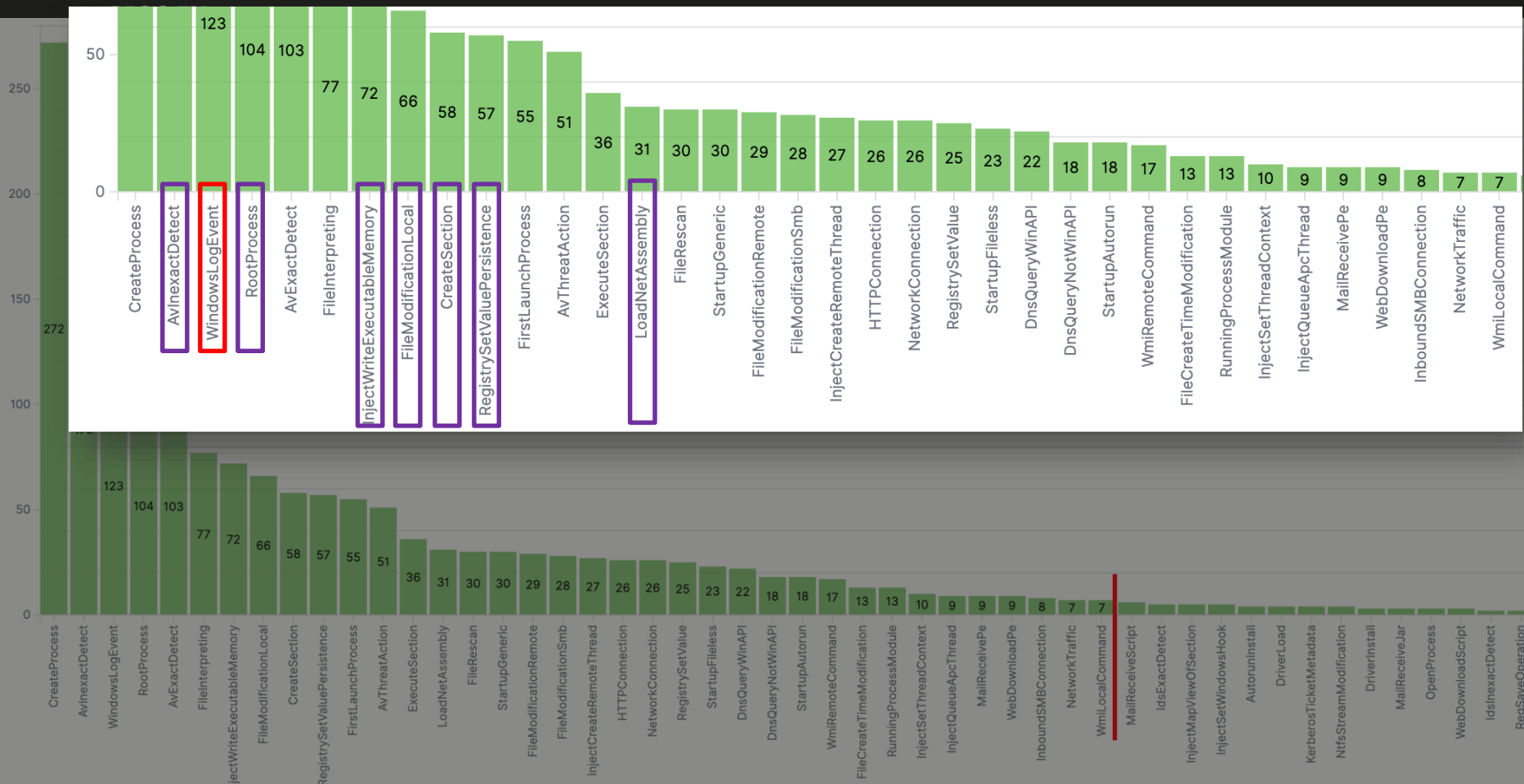
TOP 50 событий, размеченных уникальными хантами за последний

Unique count of enrich.hunts.names.raw



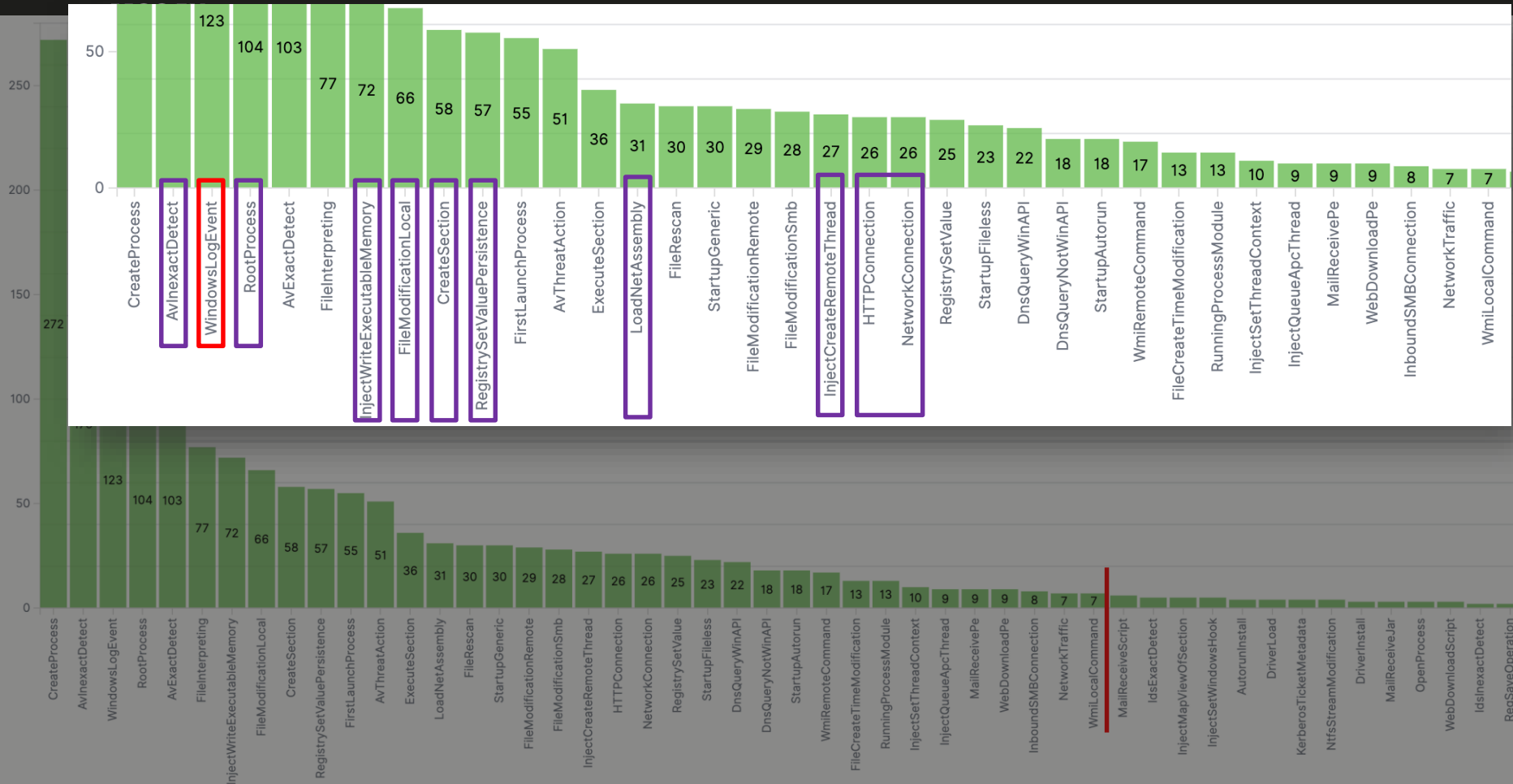
TOP 50 событий, размеченных уникальными хантами за последний

Unique count of enrich.hunts.names.raw



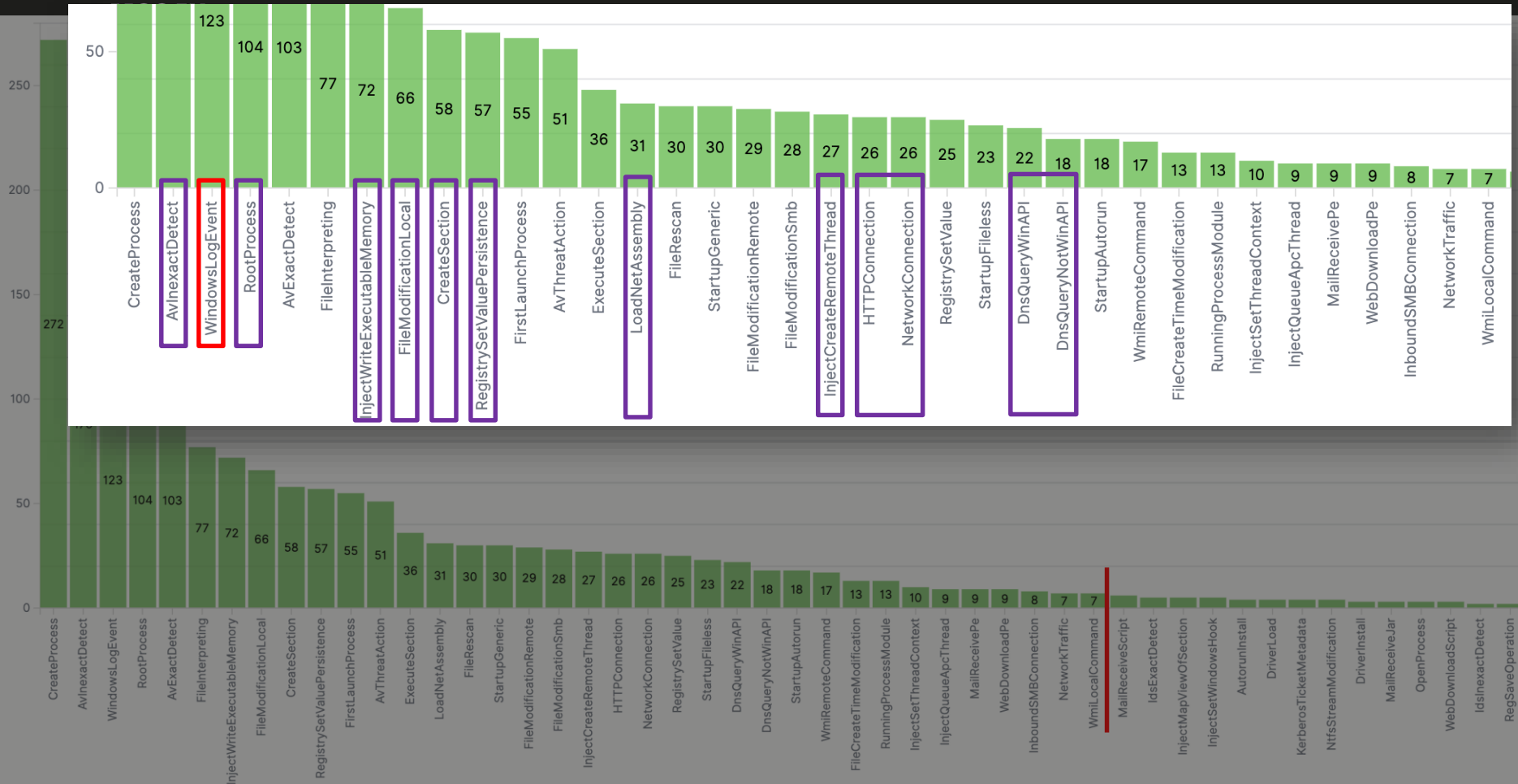
TOP 50 событий, размеченных уникальными хантами за последний

Unique count of enrich.hunts.names.raw



TOP 50 событий, размеченных уникальными хантами за последний

Unique count of enrich.hunts.names.raw



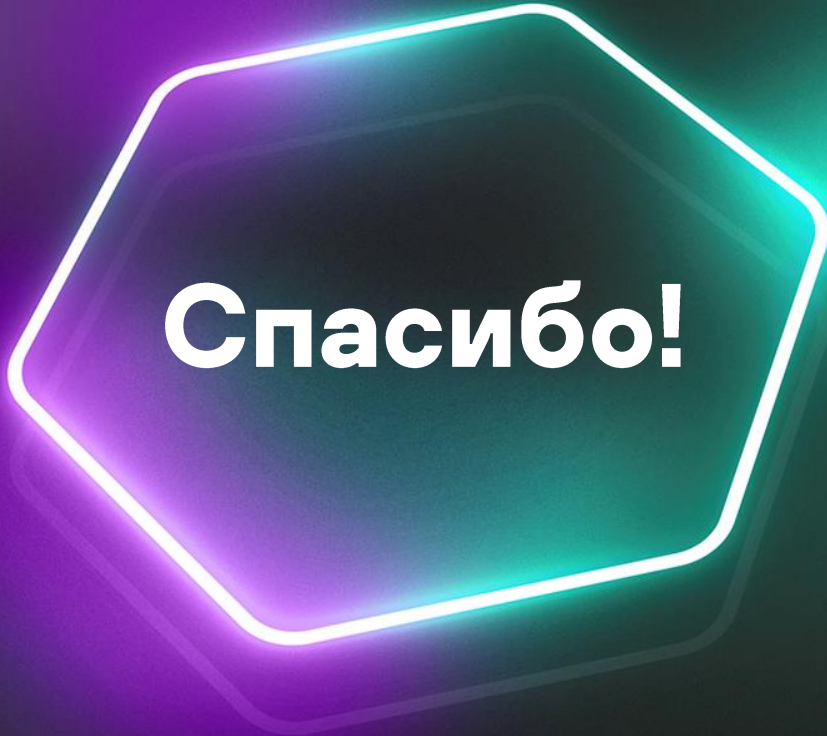
- Обнаруживайте и на конечной точке и на сети
 - События ОС очень важны 
 - Но есть масса других очень важных событий
 - Начните с MITRE ATT&CK 
 - Постоянно измеряйте ваши детекторы
 - Переиспользуйте практики SOC & DFIRMA для улучшения детекторов



OFFTOPIC: Метрики хантов

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





Спасибо!

kaspersky