Применяемые решения информационной безопасности

Дмитрий Дронов

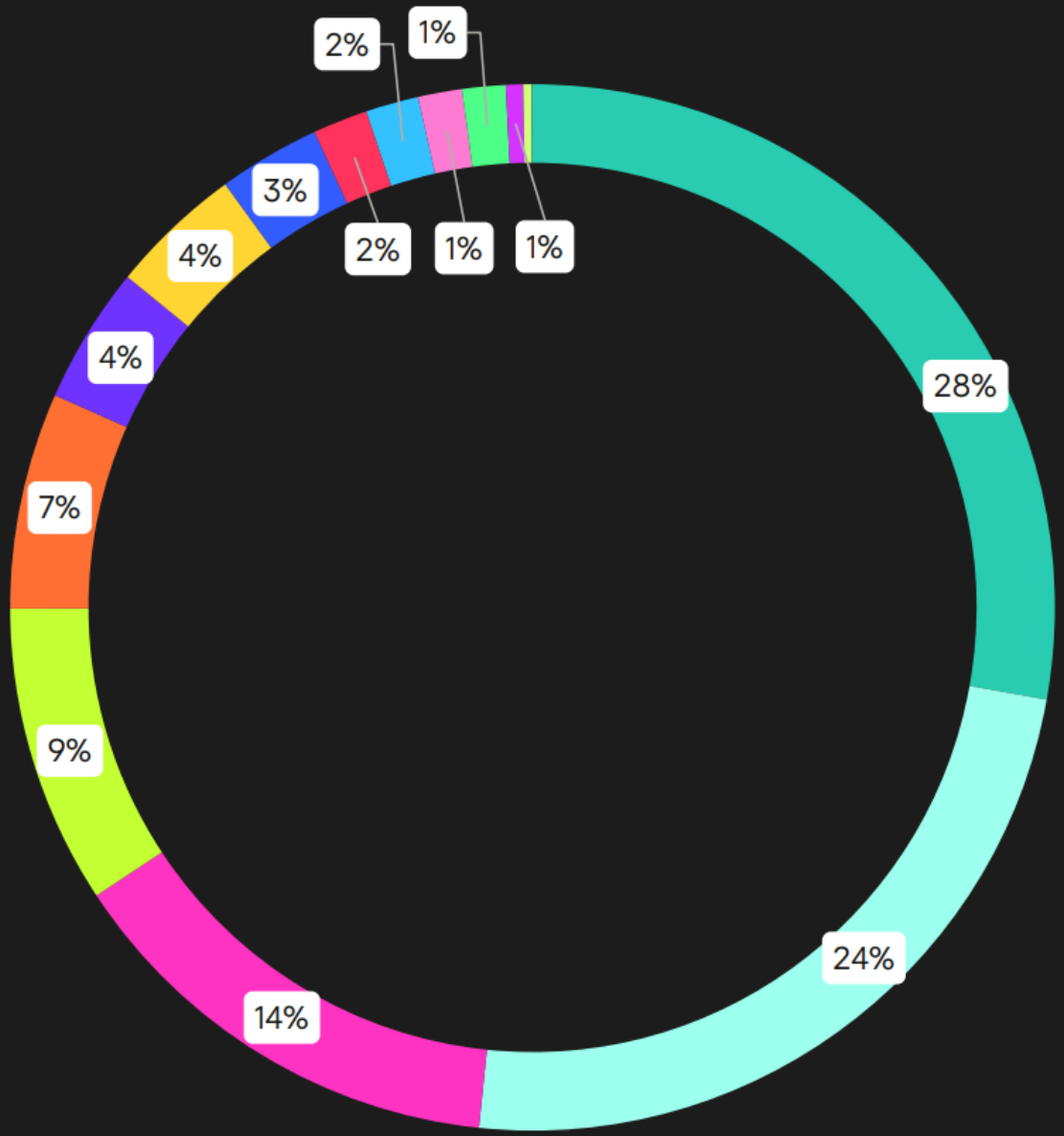
Старший инженер предпродажной поддержки, Лаборатория Касперского

kaspersky

Кто является целью?

Индустрии, которые **чаще** остальных секторов экономики **сталкивались с угрозами** за 2024 год

- Финансы
- Строительство
- Производство
- Транспорт
- Образование
- Правительство
- Розничная торговля
- Технология
- Здравоохранение
- Энергетика
- Телекоммуникации
- Гостиничный бизнес
- Развлечения



Узнать больше:
https://clck.ru/3CtHA9

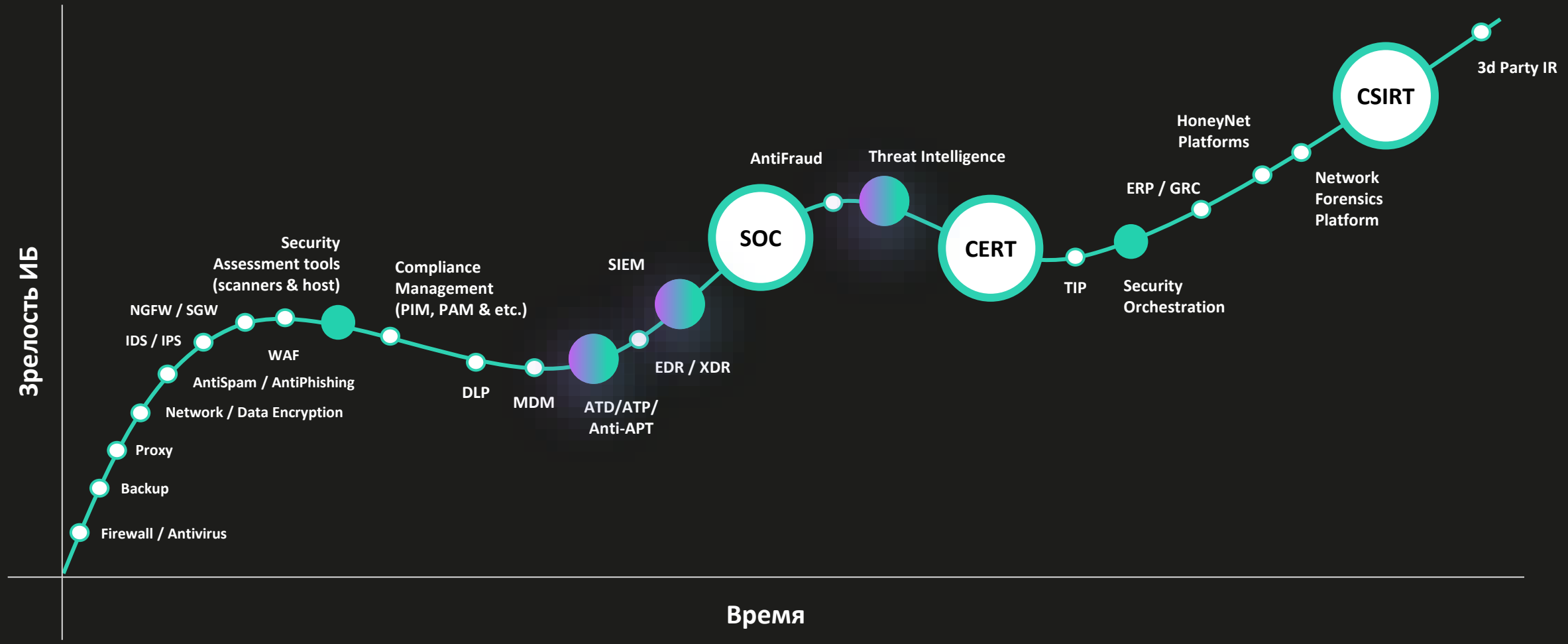
Как действуют атакующие?

Управление и контроль	25,58%[3]	AnyDesk, SystemBC, Revsocks, gs-netcat, Proxifier, dchelp, Earthworm, Remote Desktop, SSH, WebShell, Custom Linux bot
Подготовка к атаке	20,93%	Advanced IP Scanner, SoftPerfect Network Scanner, BloodHound, Fscan, Acunetix, Angry IP Scanner, Nbtscan, Nessus, netscan.exe
Выполнение	20,93%	PsExec, PowerShell, WMIC, PowerTool x64, WMI Exec, DarkKomet, ASPXspy2, MARIJUANA
Горизонтальные перемещения	11,63%	Cobalt Strike, Metasploit, Impacket, CrackMapExec, Meterpreter
Ущерб	4,65%	DiskCryptor, MHDDoS
Повышение привилегий	4,65%	Mimikatz, EfsPotato
Сбор информации	4,65%	7zip, Adminer
Эксфильтрация	2,33%	MEGASync
Первоначальный доступ	2,33%	PhishingKit
Доступ к учетным записям	2,33%	MetaStealer

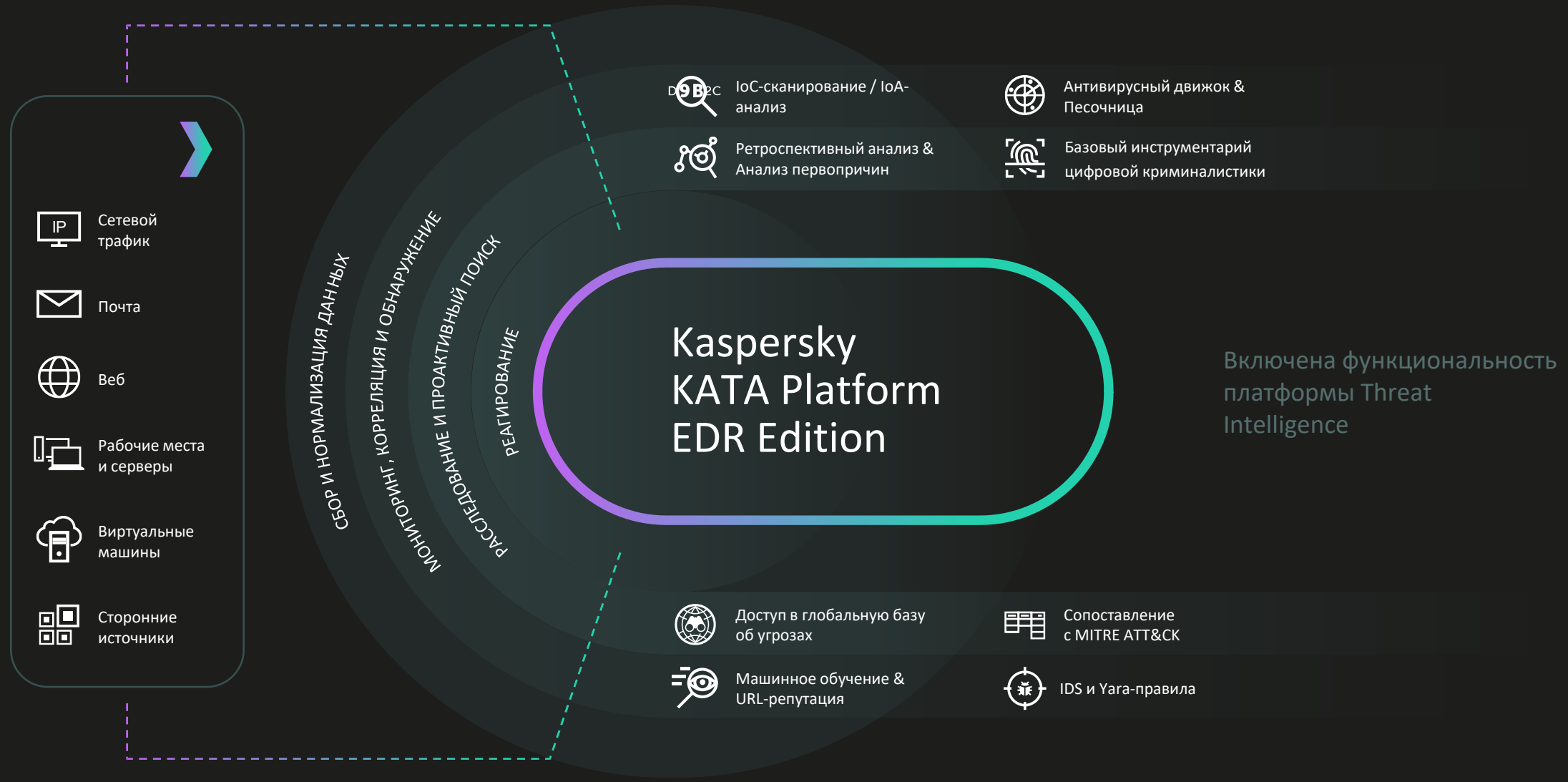
Mimikatz и PsExec остаются самыми часто используемыми инструментами

Узнать больше:
https://clck.ru/3CtLqp

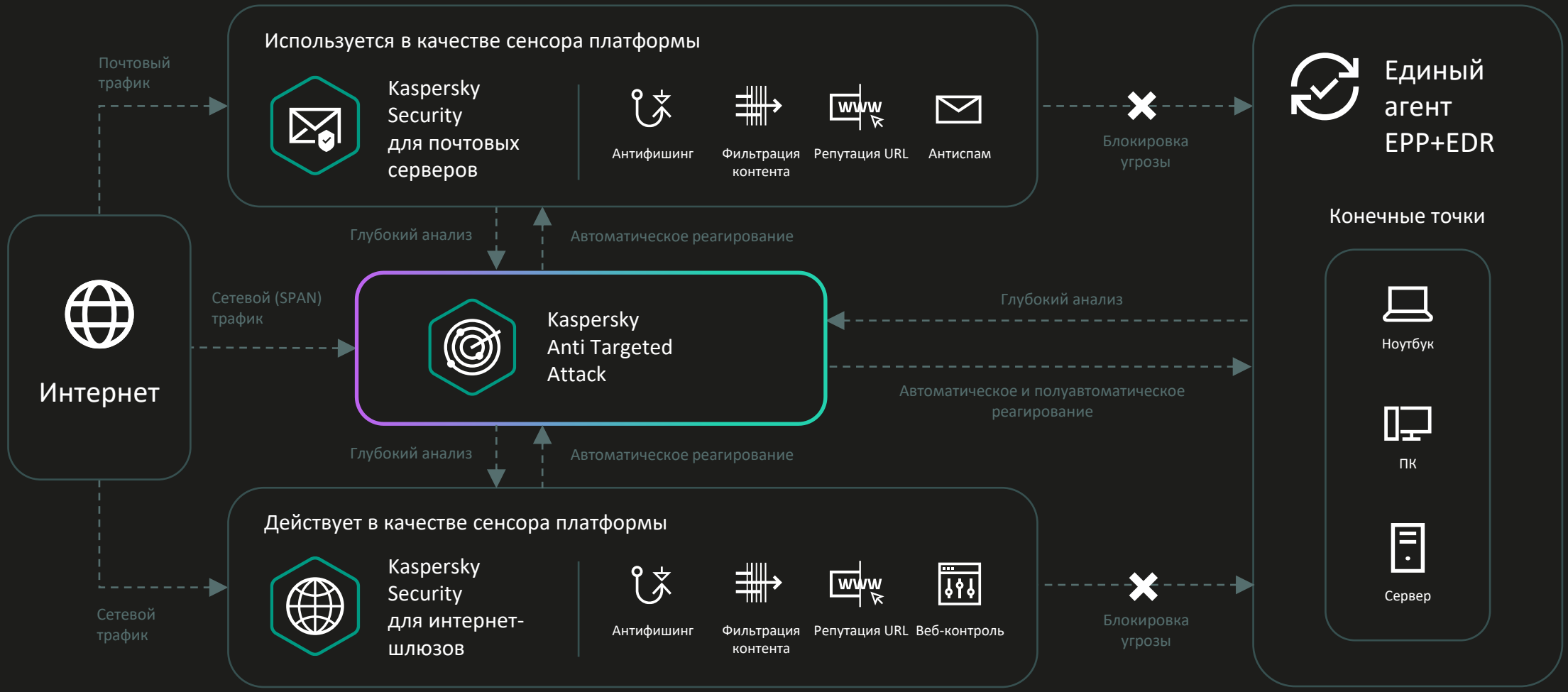
Как и чем защищаться?



Kaspersky Anti Targeted Attack Platform

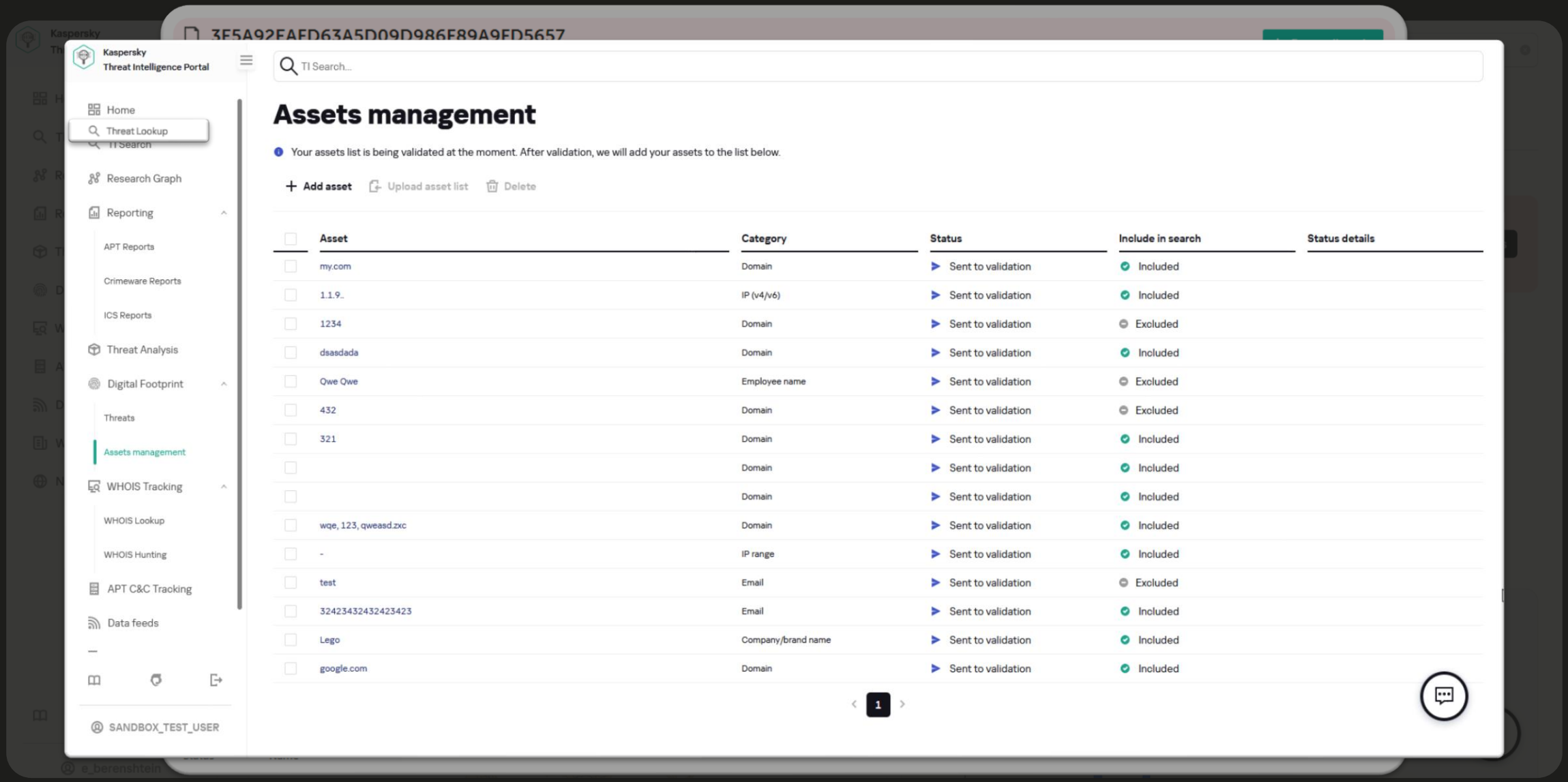


Сценарии взаимодействия

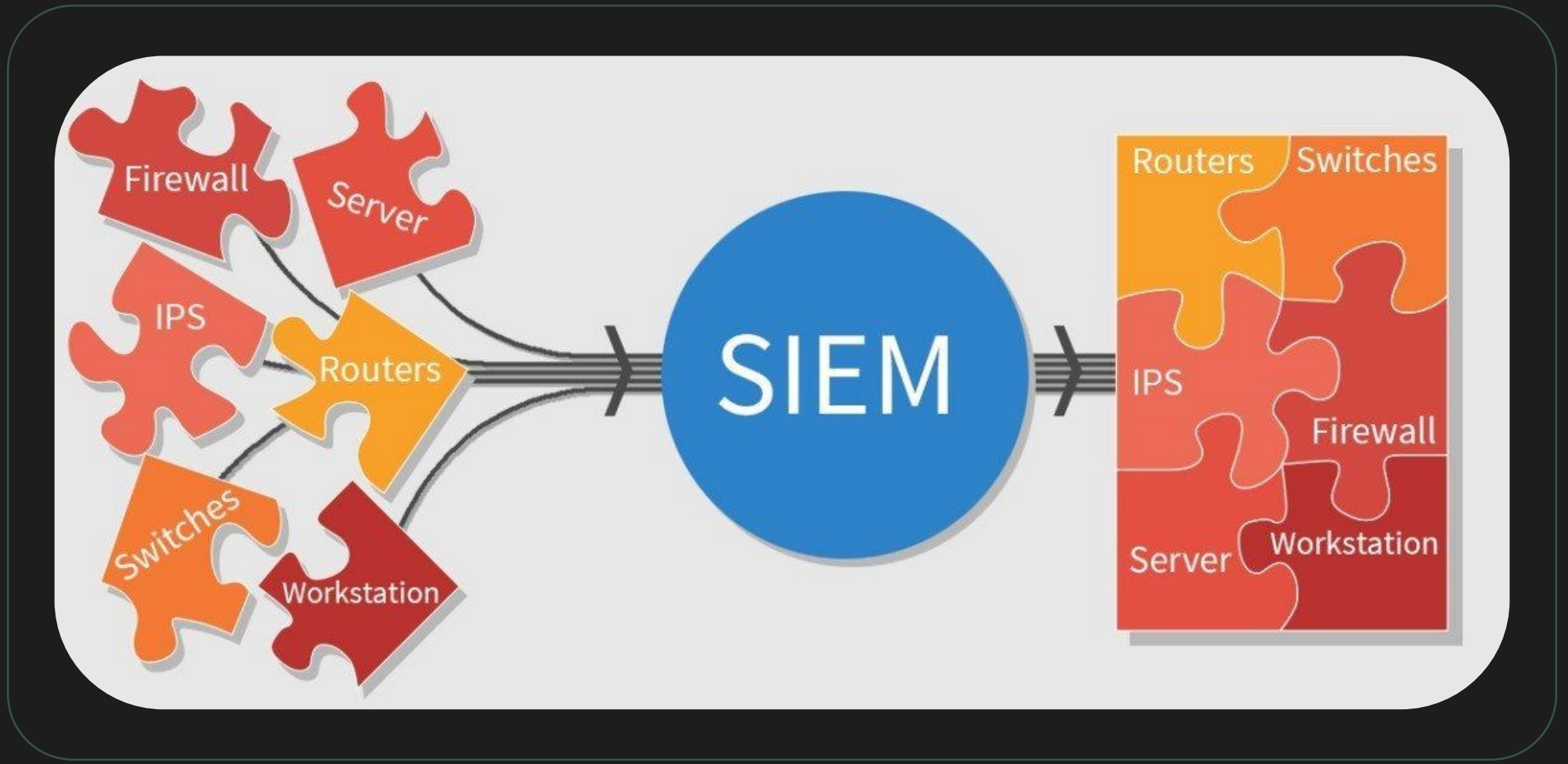


Kaspersky Threat Intelligence

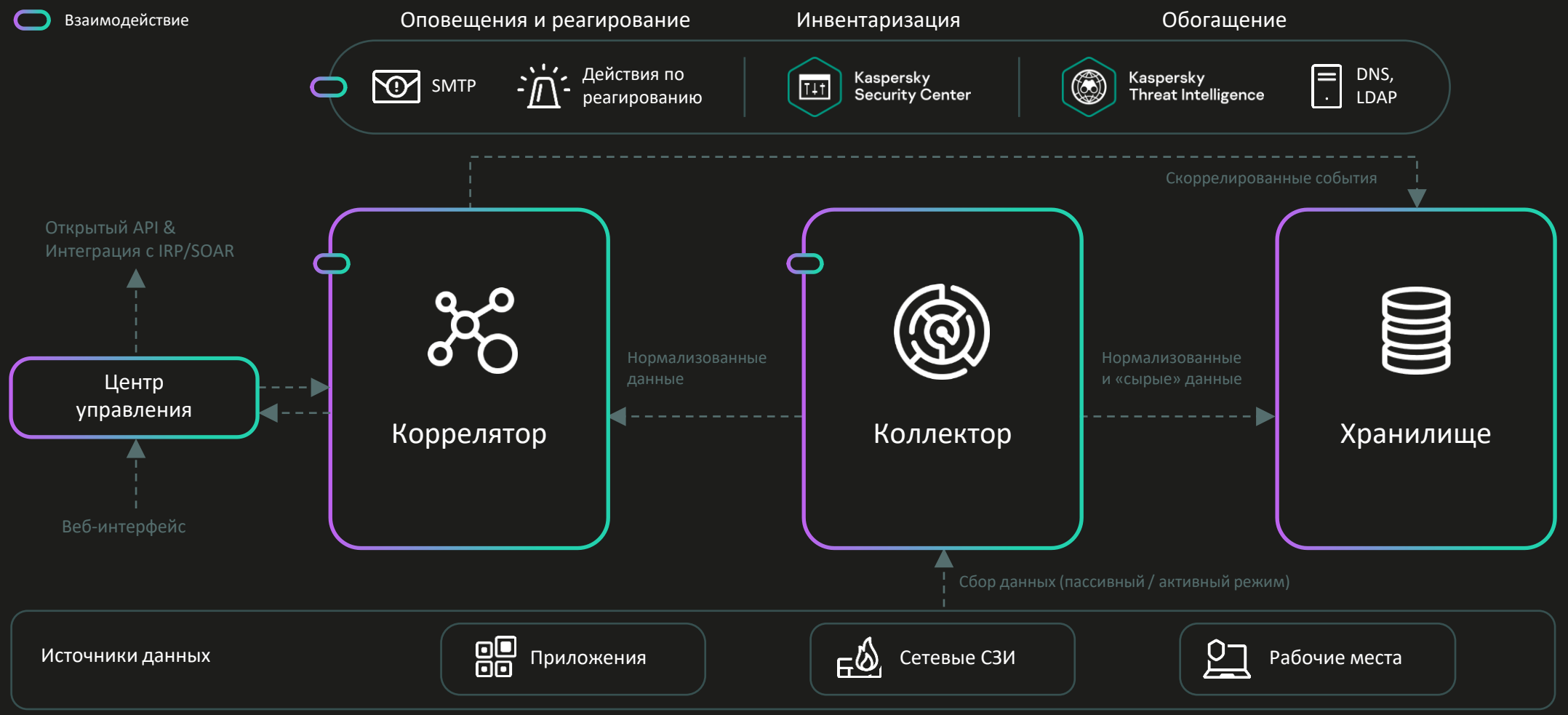
Kaspersky Threat Lookup



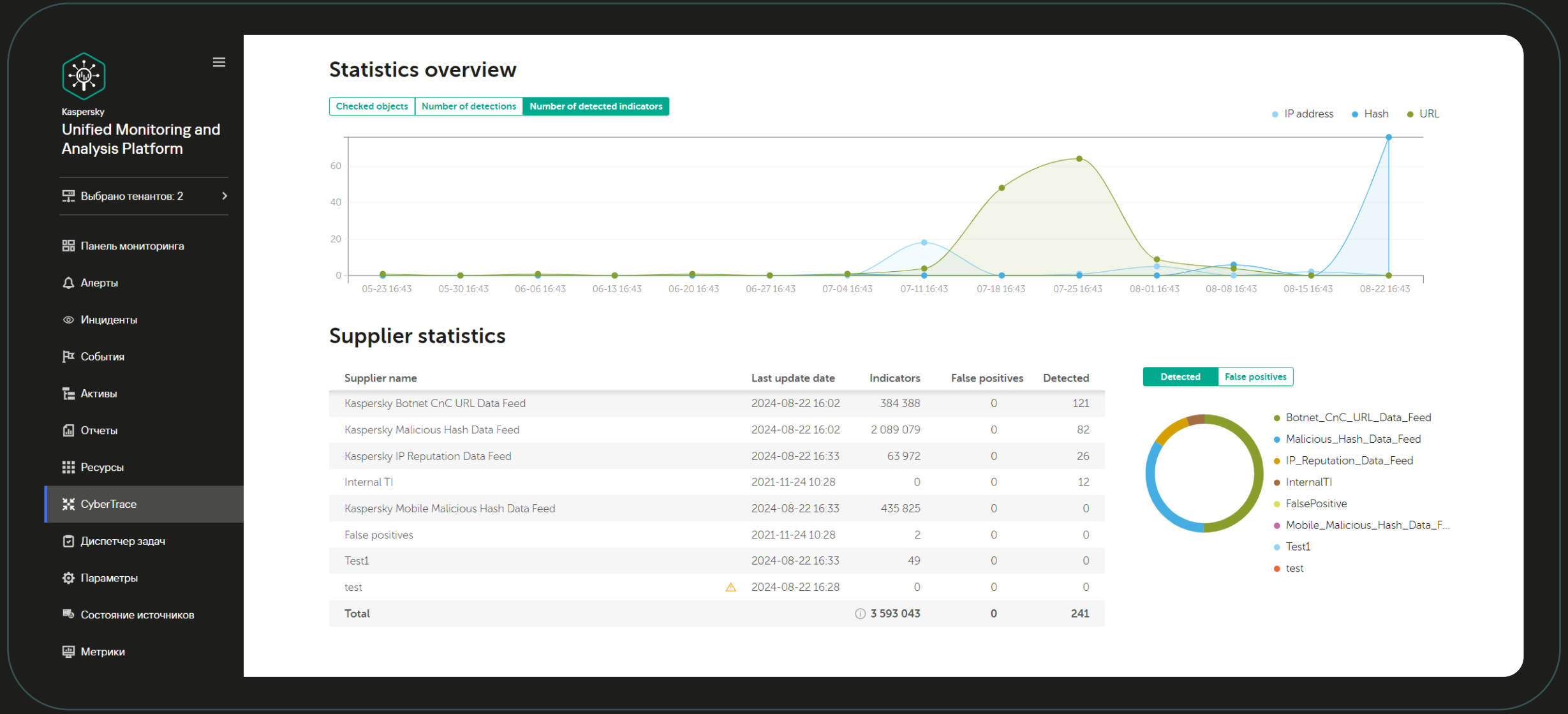
Security Information and Event Management



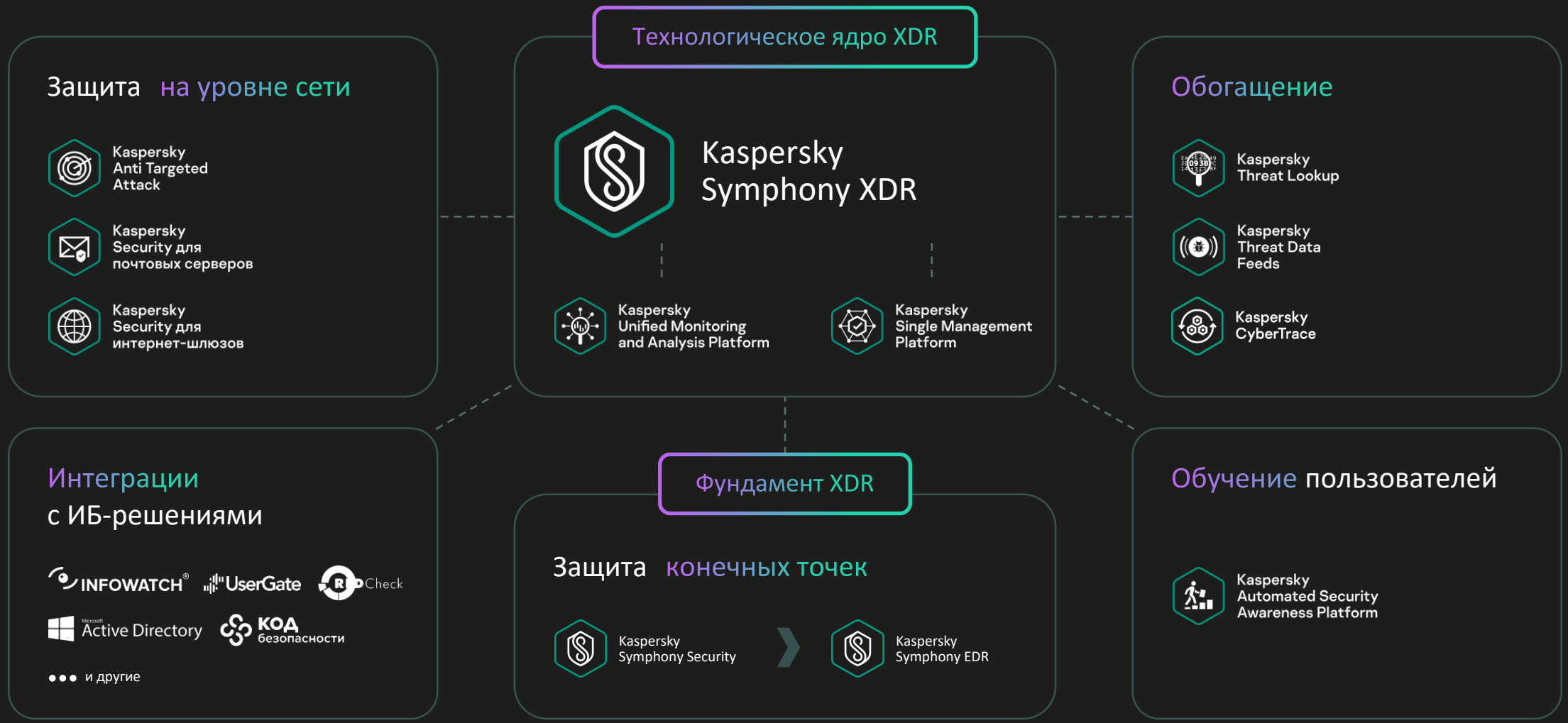
Архитектура KUMA

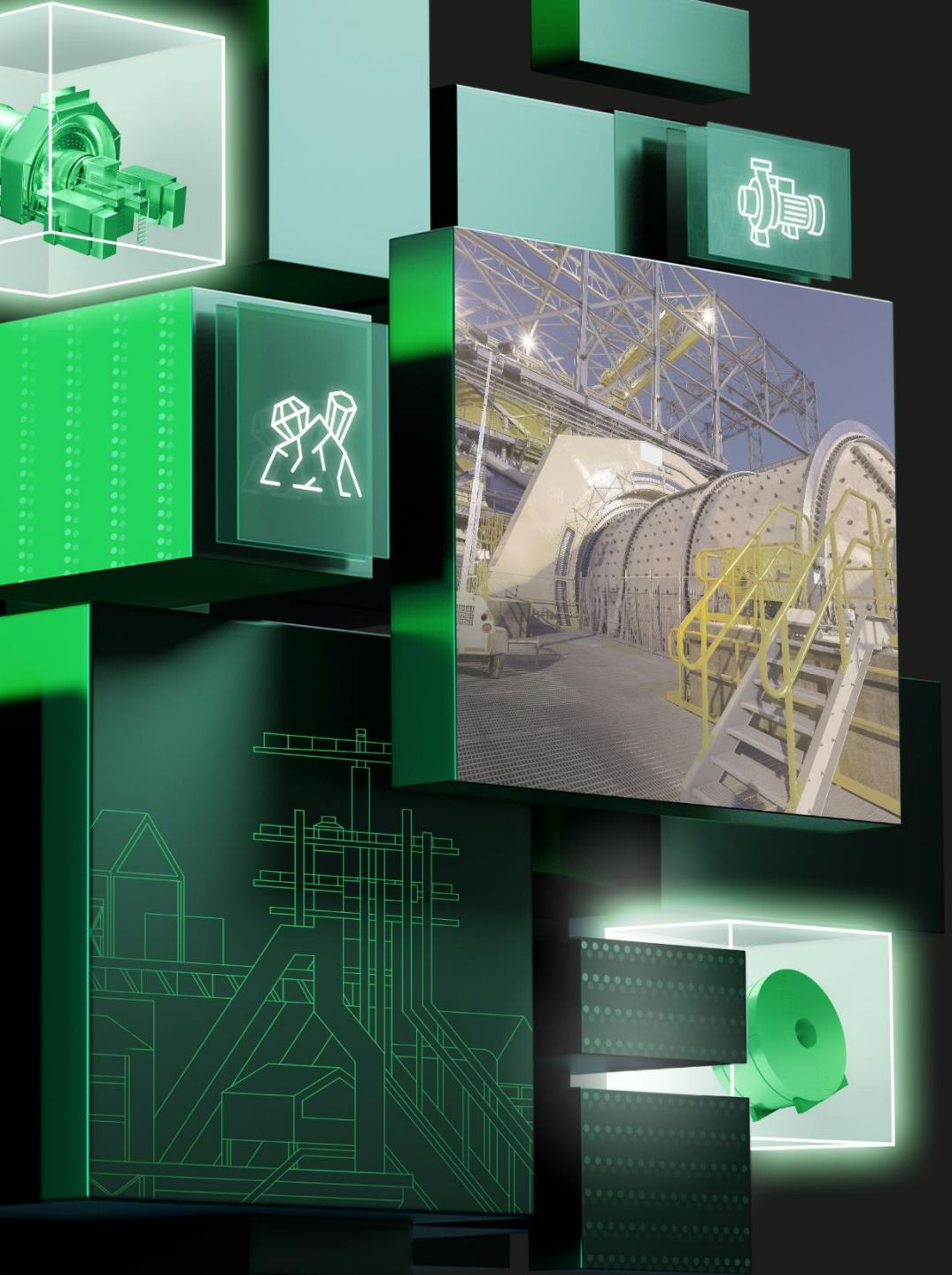


Синергия SIEM и TI-платформы



Технологическое ядро Kaspersky Symphony XDR





Спасибо!

dmitry.dronov@kaspersky.com