Партнерские сезоны 2021

Современные угрозы и методы защиты корпоративной инфраструктуры

Михаил Прибочий
Управляющий директор в России и странах СНГ

KSD, Армения 21.08.2021

kaspersky

Современные риски

Общие актуальные риски - 2021

- Риск прерывания бизнеса
- Волатильность рынка
- Острая конкуренция
- 2020 – вспышка пандемии
- Киберинциденты, TOP-3

https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

Киберриски - 2021

- 10% кидеринцидентов - критические
- Малый и средний бизнес - шифровальщики
- Крупный бизнес – APT атаки (сталкивались более 25% компаний)
- 2020 новая тенденция – смешение угроз

https://www.gazeta.ru/prcom/2021/06/30/13686362.shtml

Современные риски

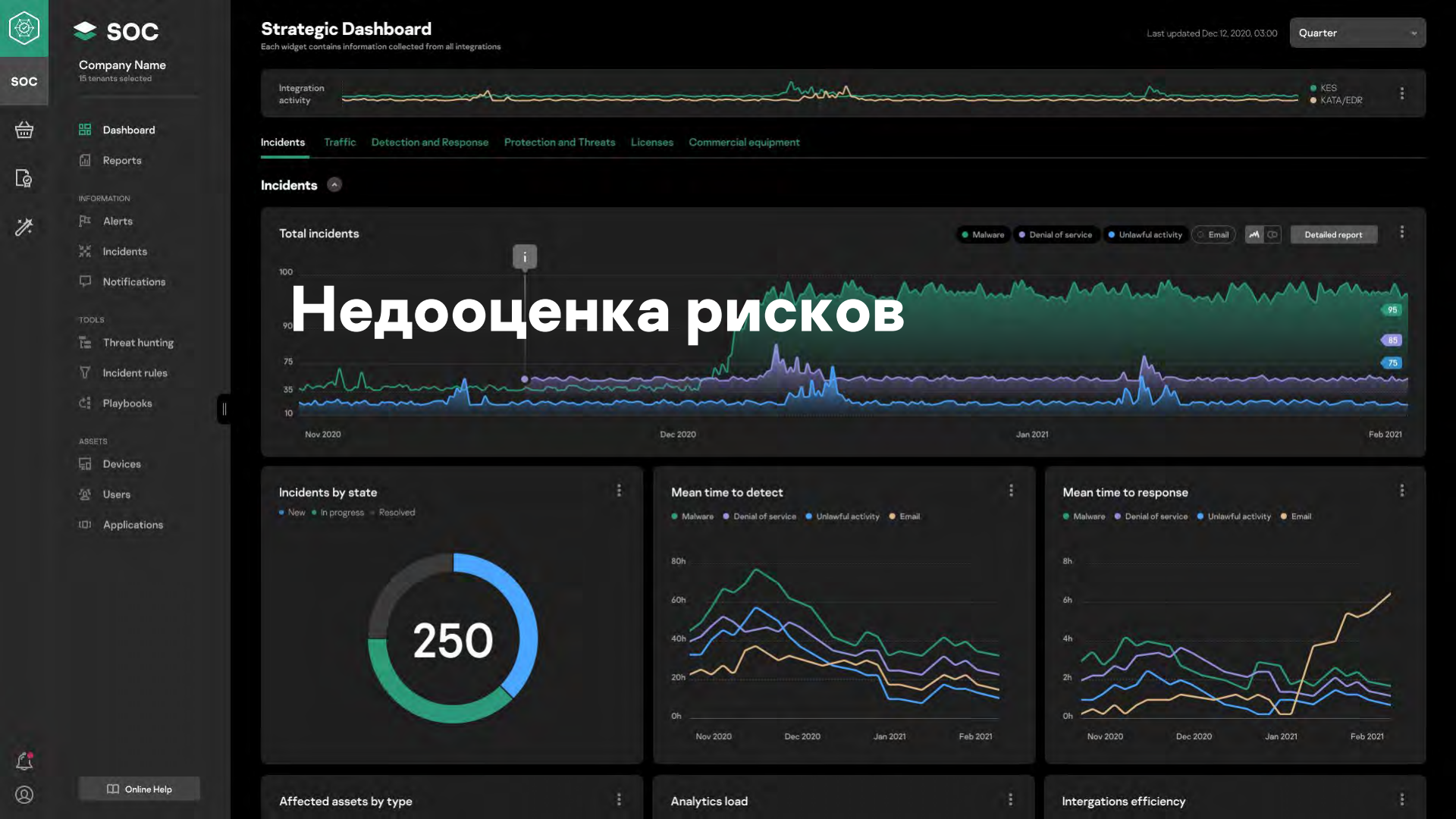
Подход злоумышленников

- Тема COVID-19
- Мультивекторный подход: социальная инженерия, много точек проникновения в инфраструктуру жертв
- Горизонтальное перемещение по сети
- Взлом через контрагентов

Свежие тенденции

- Кража данных
- Государственная разведка
- Активизация Китая (APT - 35)
- Разделение труда в мире киберзлоумышленников
- Атаки на инфраструктуру

kaspersky


SOC
Company Name
15 tenants selected
Dashboard
Reports
INFORMATION
Alerts
Incidents
Notifications
TOOLS
Threat hunting
Incident rules
Playbooks
ASSETS
Devices
Users
Applications
Online Help
Strategic Dashboard
Each widget contains information collected from all integrations
Last updated Dec 12, 2020, 03:00
Quarter
Integration activity
KES
KATA/EDR
Incidents
Traffic
Detection and Response
Protection and Threats
Licenses
Commercial equipment
Incidents
Total incidents
Malware
Denial of service
Unlawful activity
Email
Detailed report
100
90
75
35
10
95
85
75
Nov 2020
Dec 2020
Jan 2021
Feb 2021
Недооценка рисков
Incidents by state
New
In progress
Resolved
250
Mean time to detect
Malware
Denial of service
Unlawful activity
Email
80h
60h
40h
20h
0h
Nov 2020
Dec 2020
Jan 2021
Feb 2021
Mean time to response
Malware
Denial of service
Unlawful activity
Email
8h
6h
4h
2h
0h
Nov 2020
Dec 2020
Jan 2021
Feb 2021
Affected assets by type
Analytics load
Intergations efficiency

Недооценка рисков

Изолированные сети
Автоматика

Трубопровод в Техасе, 40% США под ударом

Ядерный завод в Иране

Кража фонда национального благосостояния

Недооценка рисков

Глобальная цифровизация, IoT (принтеры, климатическое оборудование, IP-камеры, охранные системы, промышленное оборудование)

Атака на казино через аквариум (‼)

«Умный дом/предприятие могут быть опасны для владельца»

Недооценка рисков

Атака через цепочку поставок

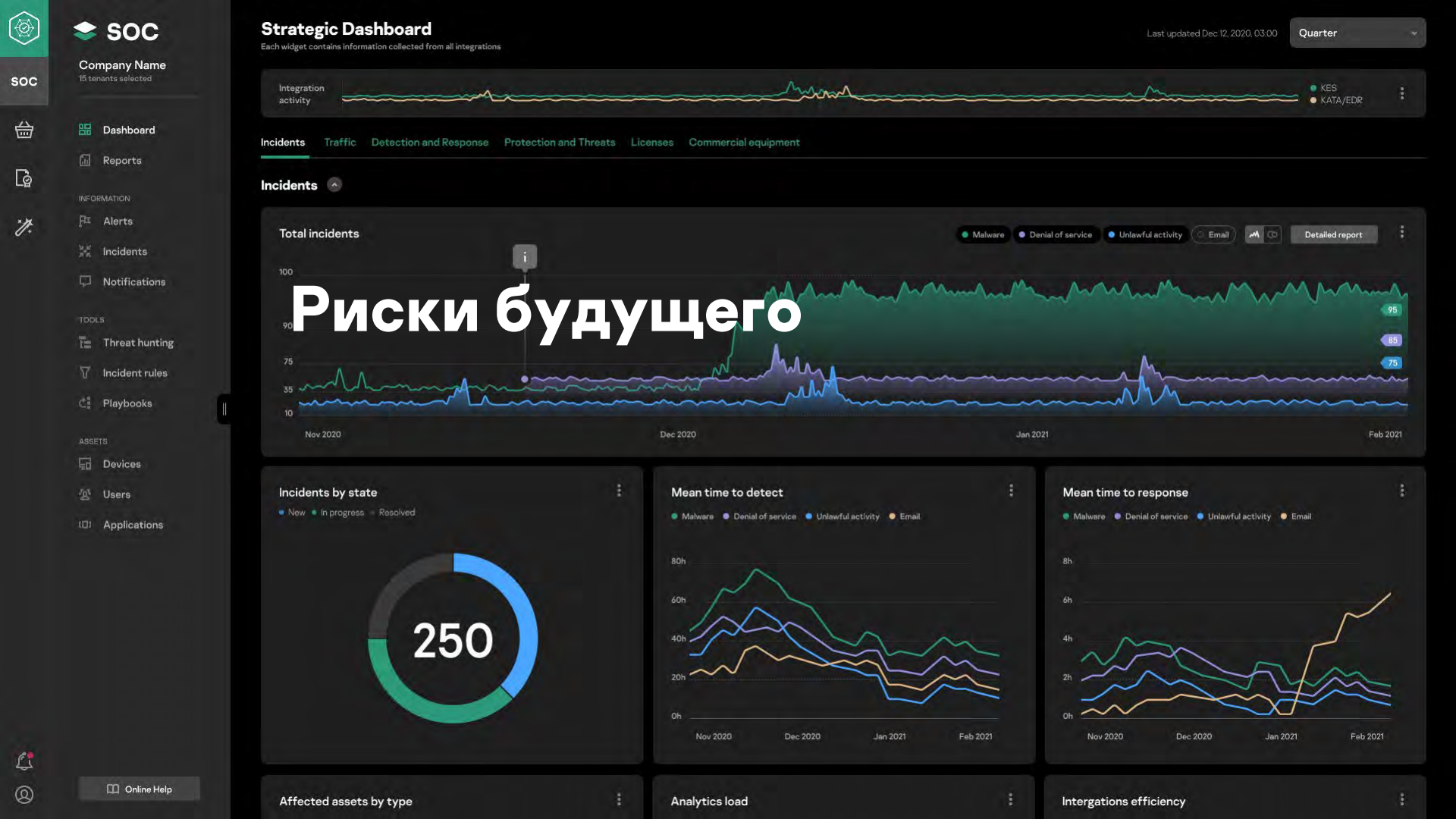
НДВ в ПО

Solar Winds – история, ударившая по всему миру

WikiLeaks – вендоры не могут отказать просьбам государства. Инструкции ANB

Kaspersky Global Transparency Initiative

https://xakep.ru/2020/12/23/solarwinds/


SOC
Company Name
15 tenants selected
Dashboard
Reports
INFORMATION
Alerts
Incidents
Notifications
TOOLS
Threat hunting
Incident rules
Playbooks
ASSETS
Devices
Users
Applications
Online Help
Strategic Dashboard
Each widget contains information collected from all integrations
Last updated Dec 12, 2020, 03:00
Quarter
Integration activity
KES
KATA/EDR
Incidents
Traffic
Detection and Response
Protection and Threats
Licenses
Commercial equipment
Incidents
Total incidents
Malware
Denial of service
Unlawful activity
Email
Detailed report
100
90
75
35
10
95
85
75
Nov 2020
Dec 2020
Jan 2021
Feb 2021
Риски будущего
Incidents by state
New
In progress
Resolved
250
Mean time to detect
Malware
Denial of service
Unlawful activity
Email
80h
60h
40h
20h
0h
Nov 2020
Dec 2020
Jan 2021
Feb 2021
Mean time to response
Malware
Denial of service
Unlawful activity
Email
8h
6h
4h
2h
0h
Nov 2020
Dec 2020
Jan 2021
Feb 2021
Affected assets by type
Analytics load
Intergations efficiency

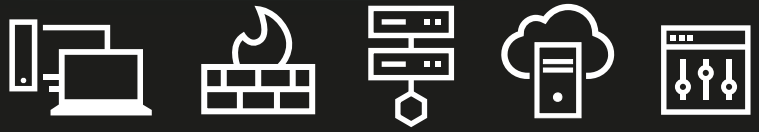
Риски будущего/ настоящего:

- Атаки на машинное обучение
- Атаки на автомобили/ автопилоты
- Дроны и антидроны
- Атаки на инфраструктуру страны
- Сепаратизм государств, спец.служб
- Вечное слабое место - ?

Kaspersky подход

От защиты конечных точек — к информационной безопасности компании

Инфраструктура



Сложные угрозы

Экспертные сервисы

SOC

Решение:

КОНЦЕПЦИЯ SECURITY FRAMEWORKS

Сложность угроз	Размер организации. Зрелость команды ИБ		Пакеты решений	Основные продукты «Лаборатории Касперского»
Угрозы национального уровня	CERT	Экспертная команда	National Cybersecurity	• Содействие национальным органам • Построение национального SOC
Целевые атаки и взломы	2500+	Служба ИБ	Kaspersky Expert Security	Kaspersky Anti Targeted Attack Platform; Kaspersky Endpoint Detection and Response; Kaspersky Threat Intelligence; Kaspersky Unified Monitoring and Analysis Platform
Сложные угрозы	500-2500	Выделенные сотрудники ИБ	Kaspersky Optimum Security	Kaspersky Sandbox; Kaspersky Endpoint Detection and Response Optimum; Kaspersky Security Awareness; Kaspersky Managed Detection and Response
Базовые угрозы	<500	ИТ	Kaspersky Security Foundations	Kaspersky Endpoint Security for Business; Kaspersky Hybrid Cloud Security; Kaspersky Security for Mail Server; Kaspersky Security for Internet Gateway

Таргетированные атаки (APT)

Профессиональные целевые атаки

Масштаб

Более 500 таргетированных вредоносных кампаний

Атрибуция

Язык, часовые пояса, ошибки, утечки, код

Решения

Kaspersky Anti Targeted Attack

Kaspersky Anti Targeted Attack

Kaspersky Endpoint Detection and Response

Kaspersky Endpoint Detection And Response

Kaspersky Threat Intelligence Portal

Узнать больше: https://kas.pr/3c7k

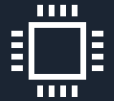
Решение:

Threat intelligence portal

Экспертное расследование угроз

Портал для анализа угроз

- **Источники данных:** KSN, бот-фермы, APT расследования, OSINT, ханипоты, спам ловушки...
- **Инструменты для умного поиска:** Research Sandbox, Threat Attribution Engine, Similarity
- **Экспертиза GReAT**



Реальные данные об угрозах

- Обнаружение угроз
- Валидация и приоритизация
- Автоматизированные расследования и реагирование (CVE, IoC, IoA)
- Активный поиск угроз
- Кастомизированные отчеты

Узнать больше: https://kas.pr/thi

Автоматизация с использованием SIEM платформы

- Запросы собственной службы ИБ, приобретение команды разработки
- Высокая производительность
- Модульность, микросервисность – гибкость использования под разные задачи
- Интегральная связанность с другими продуктами ЛК
- Встроенный движок Threat Intelligence
- Возможность автоматических проверок по контролам и поддержка концепции XDR

Решение:

KASPERSKY SINGLE MANAGEMENT PLATFORM

КОРПОРАТИВНАЯ КИБЕРБЕЗОПАСНОСТЬ

- EPP + EDR (PC, Laptop, Server, VM, Mobile)
- Анализ сетевого трафика
- Sandbox
- SIEM
- Почтовый и веб шлюзы
- Защита виртуальных и облачных сред
- Взаимодействие со сторонними решениями
- Threat Intelligence (TI платформа, потоки об угрозах, lookup, отчеты, др.)

ЗАЩИТА ИНДУСТРИАЛЬНЫХ ИНФРАСТРУКТУР

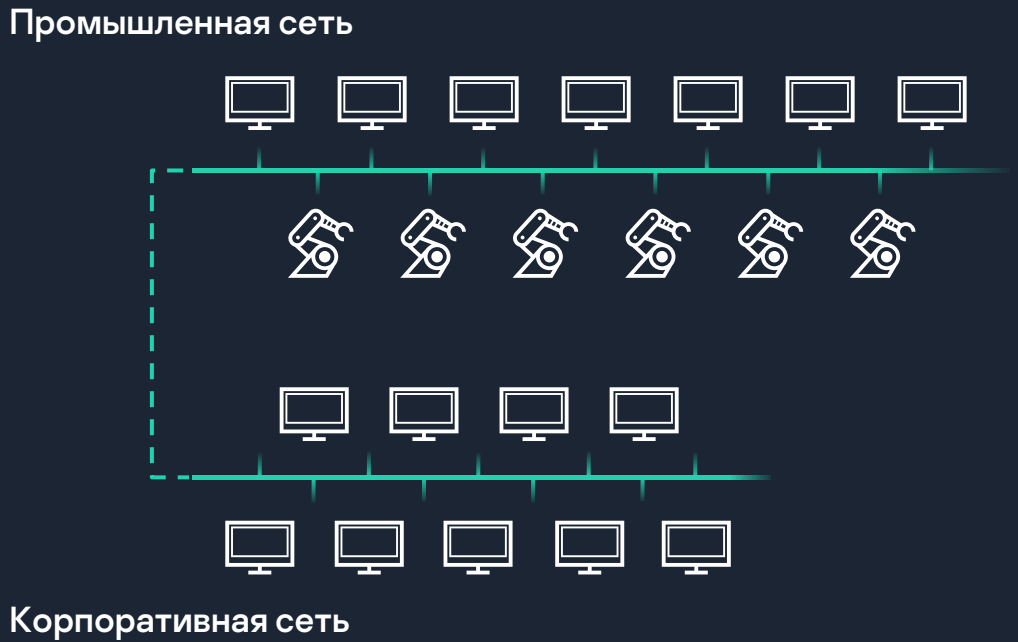
- Industrial CyberSecurity for Nodes
- Industrial CyberSecurity for Network
- Embedded Security: ATM
- ICS Threat Intelligence
- Financial Threat Intelligence

- Расширенные возможности обнаружения и реагирования
- Защита ключевых точек проникновения в инфраструктуру
- Полная картина происходящего, контроль и управление
- Высокий уровень автоматизации и внутренняя корреляция
- Управление инцидентами и расширенное реагирование

Решение:

Kaspersky Industrial Cybersecurity

- Инвентаризация АСУ ТП/DCS сети
- Песочница для обнаружения индустриальных угроз
- Обнаружение аномалий в сетевом трафике
- Проверка целостности ПЛК



Узнать больше: https://kas.pr/vgj1

Kaspersky Antidrone для объектов любого масштаба и назначения

Промышленность
~$ 450 K

Заводы,
производства
и т.д.

Частная собственность
~$ 50 K

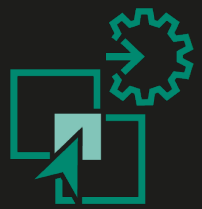
Виллы, яхты,
и т.д.

Публичные мероприятия
~ $ 150 K

Стадионы, концерты,
шествия

Критическая инфраструктура
~$ 1 M

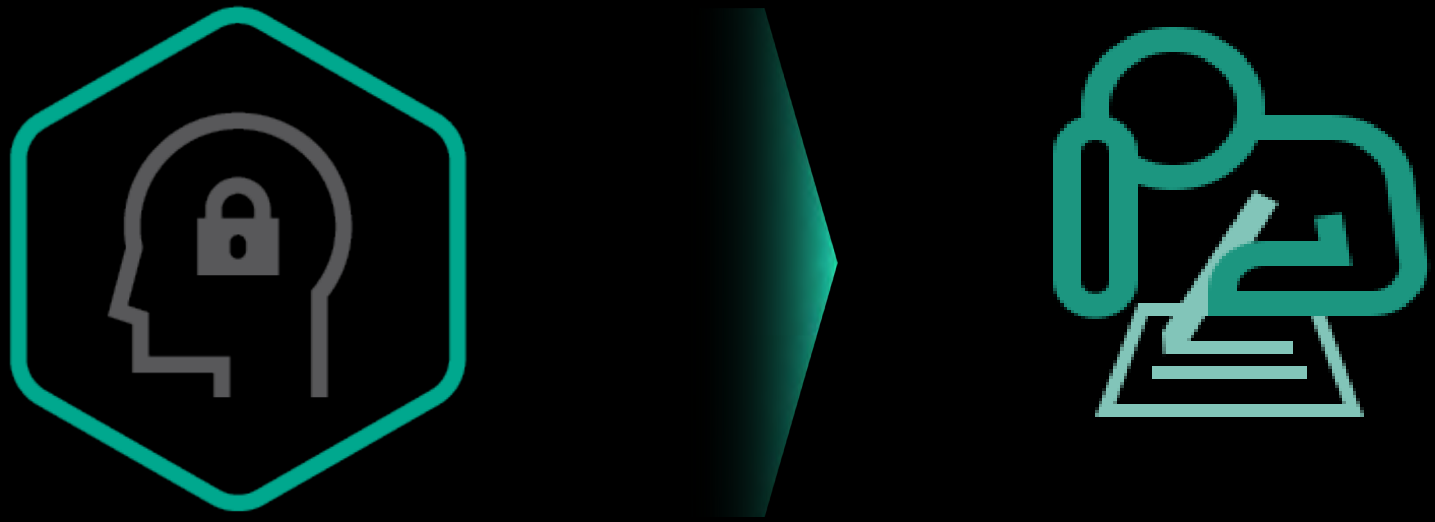
Порты,
электростанции,
аэропорты



Интеграция ПО $ 10 K

Все типы
объектов

БЕЗОПАСНЫЕ ВЫБОРЫ – ЧАСТЬ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ



Решение:

Polys обеспечивает эти требования

Приложение
для голосования

Устройства
для голосования

Блокчейн

Шифрование

Слепая подпись

Polys

Система электронного голосования должна обеспечивать:

1. **Невозможность подделать голос и повлиять на подсчет результатов**

2. **Невозможность узнать результаты до завершения голосования**

3. **Анонимность голосов**

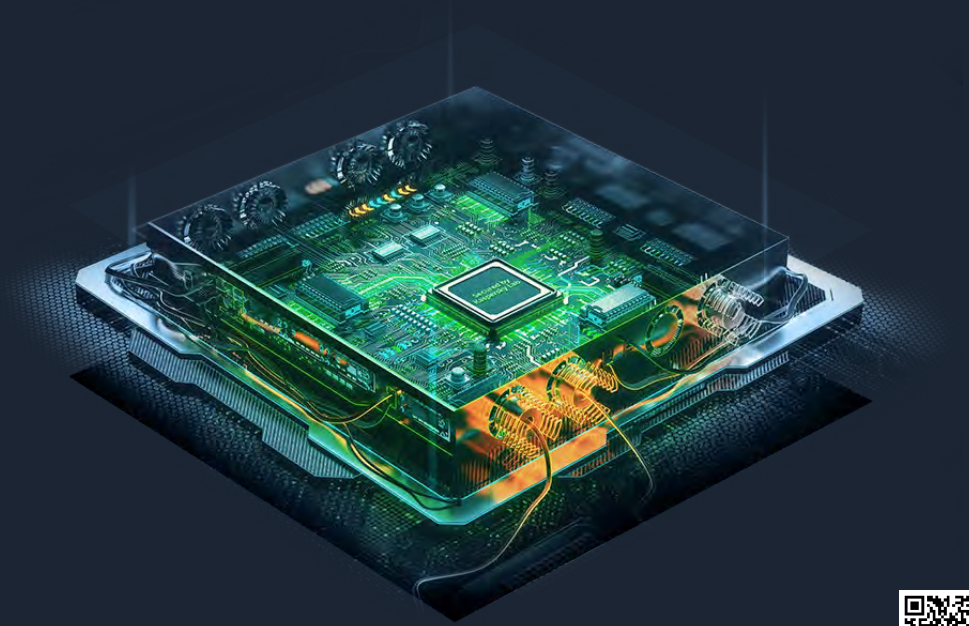
4. **Доступность и простоту голосования**

5. **Возможность вести «бумажный лог»**

Решение:

KasperskyOS

- Приоритетное направление развития компании
- Стратегия голубого океана – у нас нет конкурентов
- Многолетние разработки и многомиллионные инвестиции
- Прицел на глобальный рынок



Узнать больше: https://kas.pr/jgi8