BI.ZONE

От офиса до цеха:

комплексный подход к защите конечных точек в IT-инфраструктуре и АСУ ТП

BI.ZONE

Предпосылки

Обнаружение техник атакующих по данным с конечных точек

BI.ZONE

Initial Access
4/10 техник

Execution
13/14 техник

Persistence
18/20 техник

Privillege Escalation
14/14 техник

Defence Evasion
37/43 техник

Credential Access
12/17 техник

Collection
13/17 техник

Command and Control
4/17 техник

Discovery
27/32 техник

Lateral Movement
7/9 техник

Exfiltration
6/9 техник

Impact
10/14 техник

техник и подтехник
матрицы MITRE ATT&CK
можно обнаружить
по данным с конечных точек

Тенденции российского ландшафта угроз

BI.ZONE

- Атаки через подрядчиков
- Использование атакующими легитимного ПО и инструментов
- Рост числа целевых атак

Проблемы при защите конечных точек

BI.ZONE

Недостаточная видимость

Непрозрачность происходящего на конечных точках мешает быстро анализировать угрозы и находить их первопричины

Скорость реагирования ниже желаемой

Реагирование и сбор дополнительных данных занимают много времени, особенно на компьютерах удаленных пользователей

Большое количество событий при аудите ОС

Множество событий потребляют ресурсы лицензии SIEM, а также требуют разработки и поддержки сотен правил корреляции для выявления инцидентов

Сложность поддержки разнородных средств для мониторинга и реагирования

Windows, Linux и macOS используют разные средства мониторинга и реагирования. Для их внедрения и поддержки нужны значительные ресурсы

Основные трудности при защите АСУ ТП

BI.ZONE

Дорогой комплексный аудит

Не хватает человеческих, финансовых и технических ресурсов для комплексного аудита

Низкая осведомленность о рисках

Нет точной информации об инфраструктуре, поэтому сложно находить слабые места и управлять рисками

Множество требований регуляторов

Меняющиеся требования регуляторов усложняют работу, требуют разработки большого количества документов и повышают риск ошибок

Недостаточное количество инструментов

Без специальных инструментов и специалистов сложно быстро выявлять, анализировать и устранять причины киберинцидентов

Разница подходов

BI.ZONE

Офис

- Защита конфиденциальности и целостности данных
- Частые обновления систем
- Слабая или средняя сегментация сети
- Доступ в интернет по умолчанию

Цех

- Обеспечение непрерывности технологических процессов
- Редкие обновления после тщательного тестирования
- Строгая сегментация и изоляция сети

Потребность

BI.ZONE

Цех

Специалист
по кибербезопасности АСУ ТП

- Актуализация перечня активов АСУ ТП и связанных компонентов
- Проверка уязвимостей и оценка рисков
- Проверка избыточности и безопасности открытых сетевых сервисов
- Проверка соответствия требованиям политик кибербезопасности и инструкций по защите АСУ ТП
- Проверка полноты настроек встроенных СЗИ всех компонентов (SCADA, PLC и др.)
- Проверка избыточности прав доступа и наличия стандартных учетных записей
- Мониторинг событий кибербезопасности в системах автоматизации и ПТК (с учетом особенностей журналирования)
- Аудит конфигураций СЗИ: качество, корректность обновлений, режимы работы
- Соблюдение пунктов приказа ФСТЭК России № 239

Примеры проблем

BI.ZONE

Специалист
по кибербезопасности АСУ ТП

Цех 1

- Нет инвентаризационных данных, старая документация
- Аудит не делали никогда, из последних обновлений — только антивирус
- Избыточные права доступа операторов, одна учетная запись для всего
- Были проблемы с работоспособностью АРМ

Цех 2

- Есть инвентаризационные данные но неактуальные
- Несколько лет назад интегратор проводил аудит, что-то исправили
- Используется множество серверов OPC DA
- Обслуживание систем АСУ ТП — на подрядчике с полными правами

Реальность

BI.ZONE

Специалист
по кибербезопасности АСУ ТП

Цех 1 | Цех 2 | Цех 3 | Цех 4 | Цех 5 | Цех 6

Цех 7 | Цех 8 | Цех 9 | Цех 10 | Цех 11 | Цех 12

BI.ZONE

Решение BI.ZONE EDR

Развитие BI.ZONE EDR

BI.ZONE

2017
Формирование требований и старт разработки

2018
Релиз BI.ZONE EDR для Windows

2019
Начало использования в сервисе BI.ZONE TDR

2021
Релиз BI.ZONE EDR для Linux

2022
Партнерства с MSSP

2023
Релиз BI.ZONE EDR для macOS

Защита с помощью BI.ZONE EDR

BI.ZONE

800 тыс.+

агентов

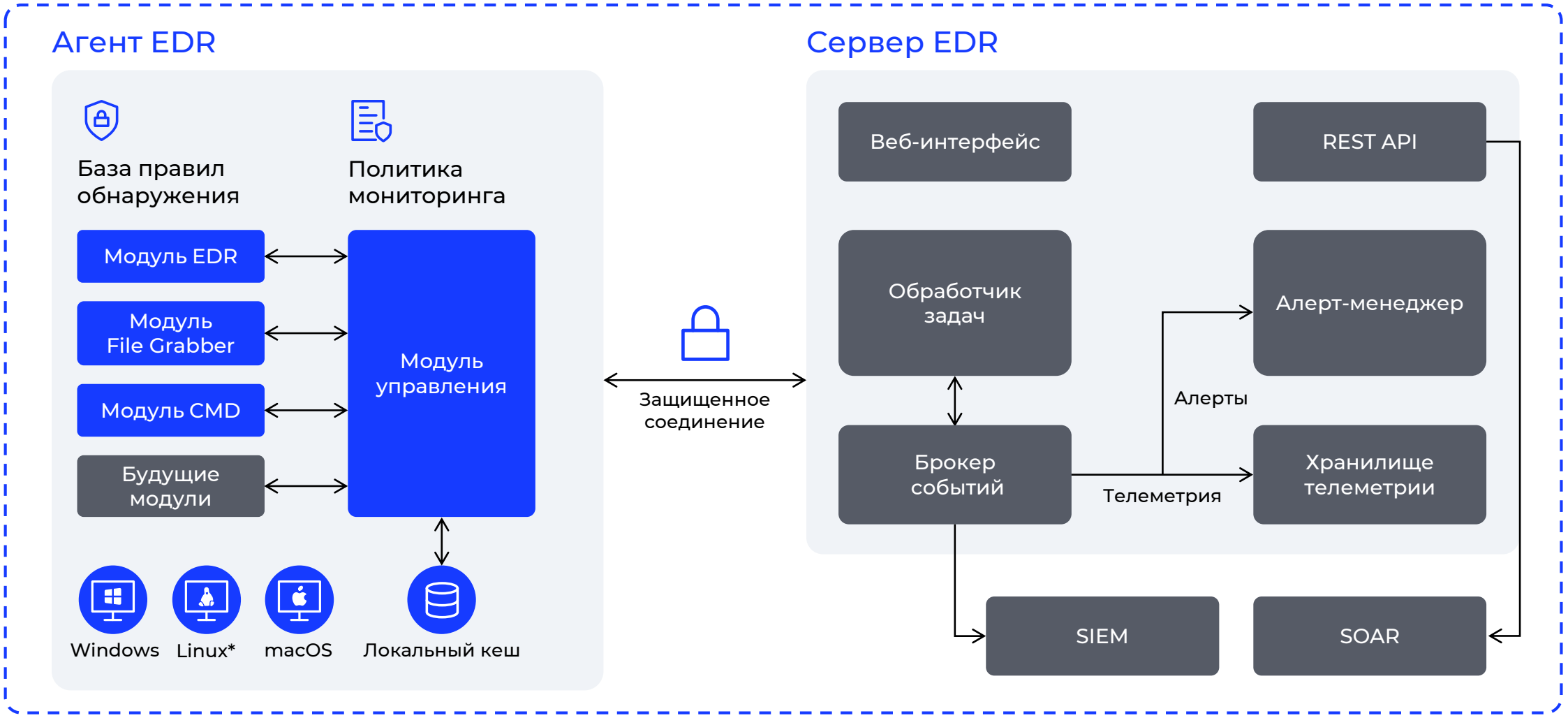
Экспертный опыт
в обнаружении

Модульная
архитектура

Архитектура BI.ZONE EDR

BI.ZONE

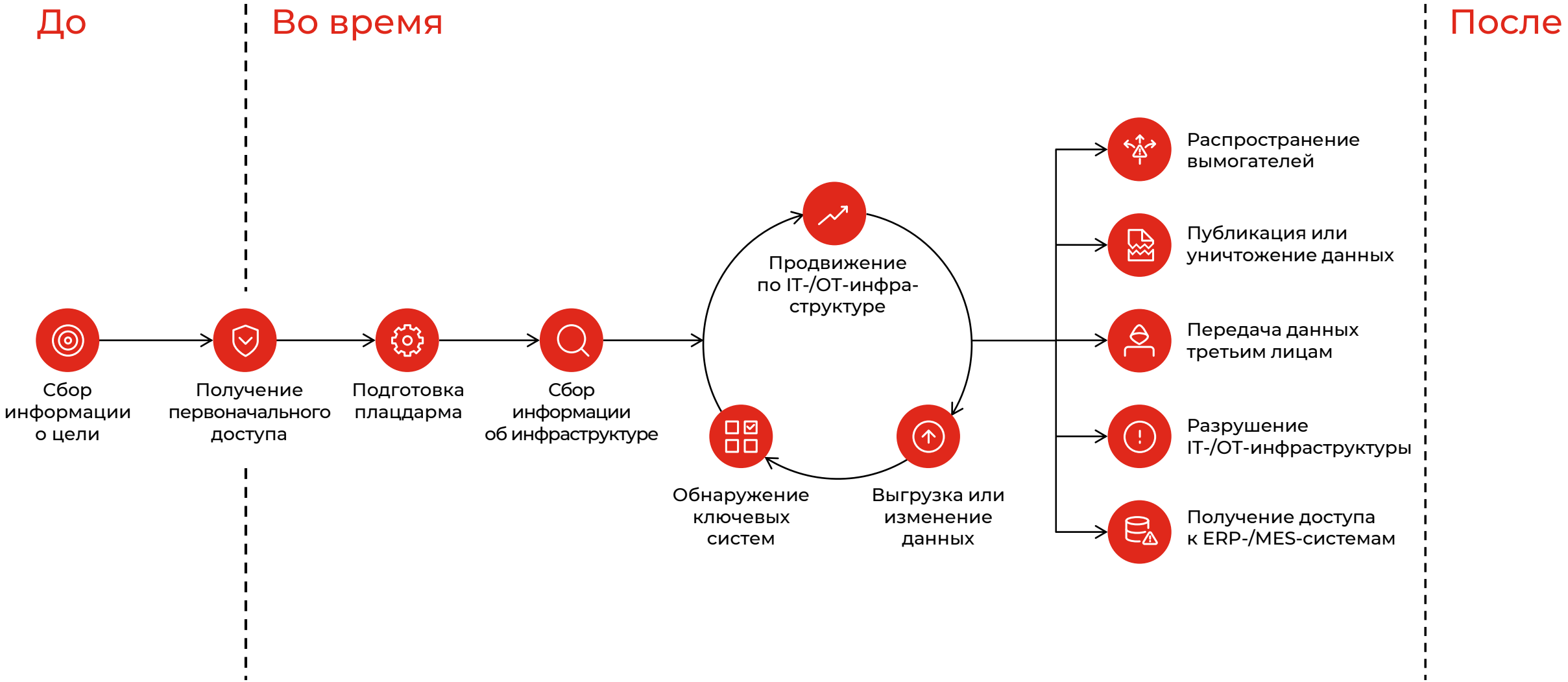
Инфраструктура компании



* В том числе российские дистрибутивы

BI.ZONE EDR на каждом этапе инцидента

BI.ZONE



BI.ZONE EDR до инцидента

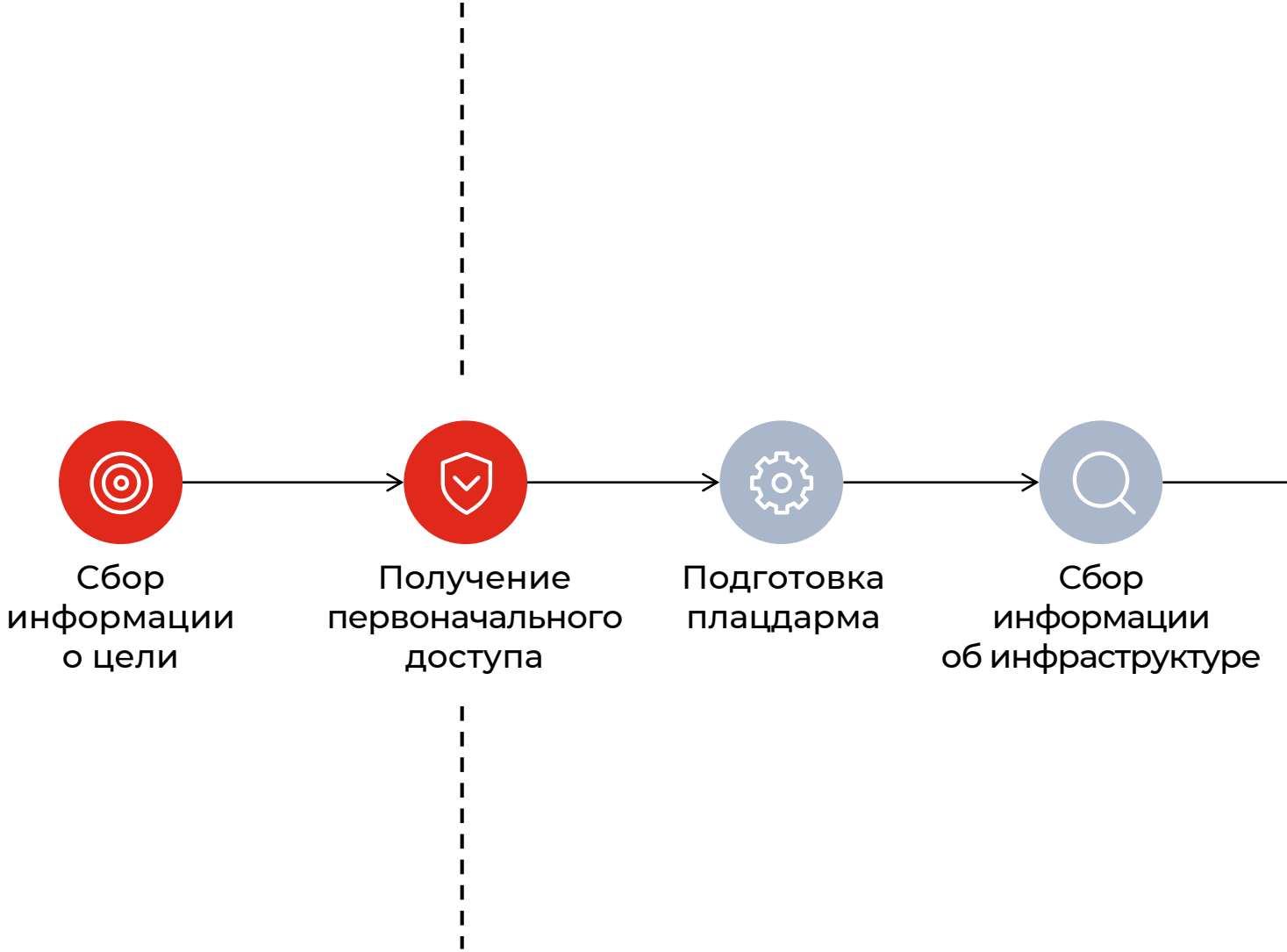
BI.ZONE

Threat prediction

Автоматизированное
выявление уязвимостей
и недостатков инфраструктуры

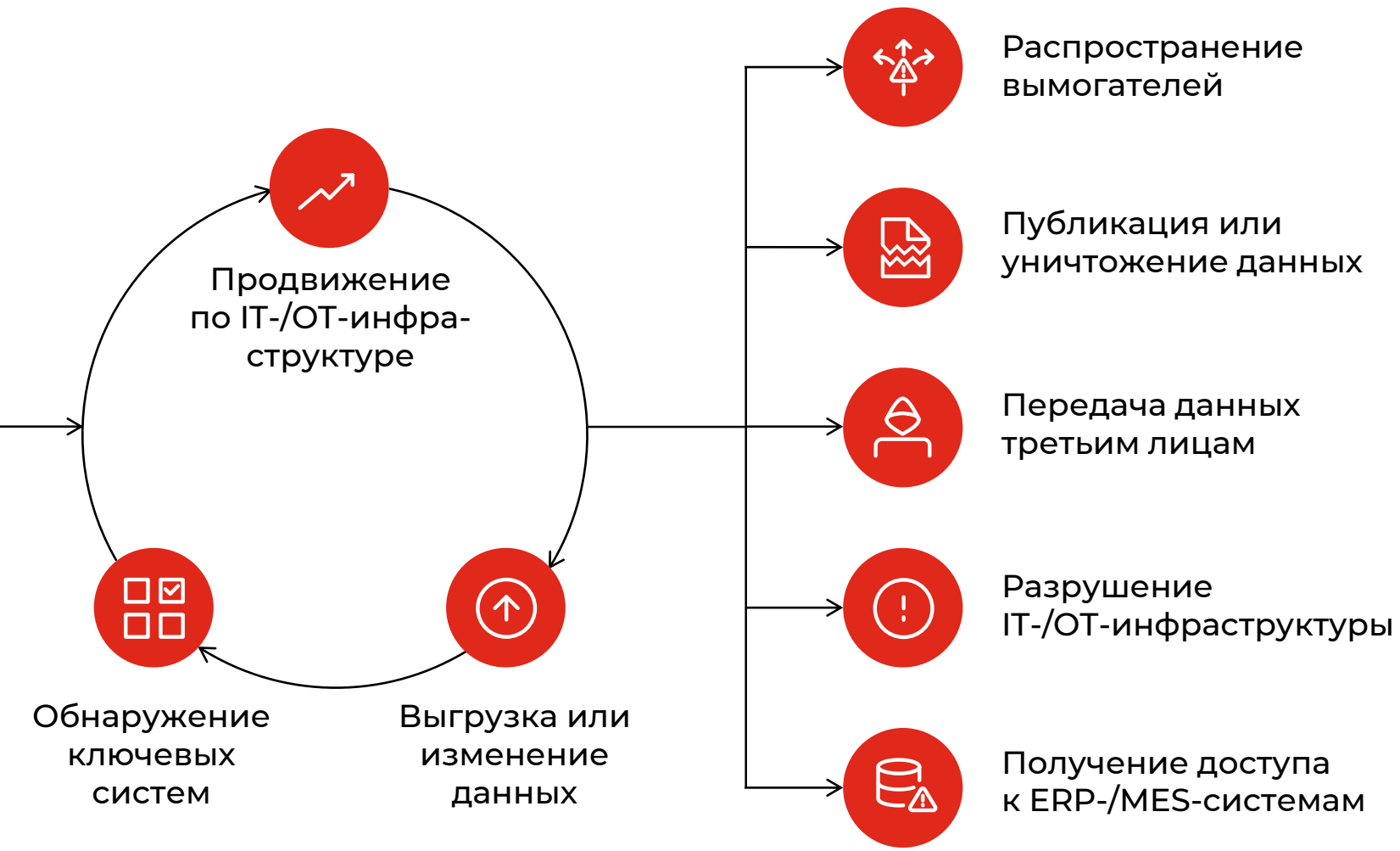
Пример

Обнаружение сервисов
с некорректными
настройками, через которые
можно повысить привилегии



BI.ZONE EDR во время инцидента

BI.ZONE



Threat detection

Выявление активных атак

Threat response

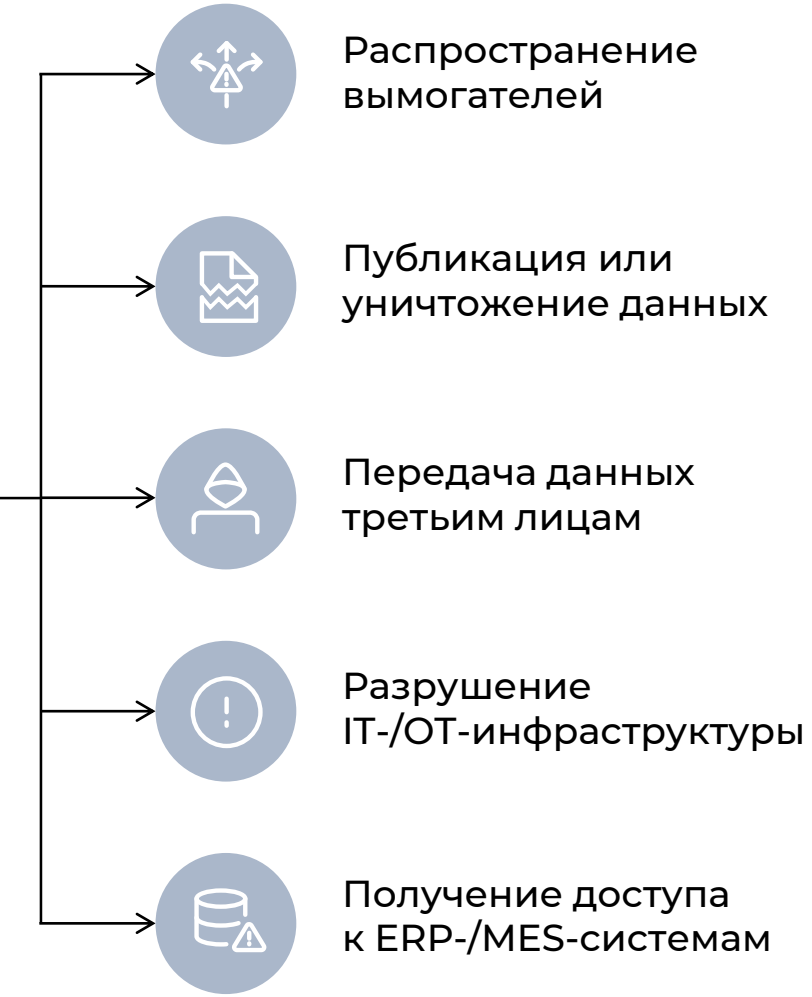
Реагирование на атаки и их расследование

Примеры

- Детектирование IoA
- Скачивание файла для анализа
- Остановка процесса
- Изоляция хоста

BI.ZONE EDR после инцидента

BI.ZONE



Threat archeology

Автоматизированное выявление прошлых атак, неактивных в настоящий момент

Пример

Обнаружены артефакты прошлого использования утилиты Mimikatz

BI.ZONE

Особенности решения

Возможности BI.ZONE EDR

BI.ZONE

Обнаружение

Threat prediction
Автоматизированное выявление недостатков инфраструктуры

IoC
Автоматизированное выявление следов атакующих

Офлайн
Выявление атак без доступа к серверу управления

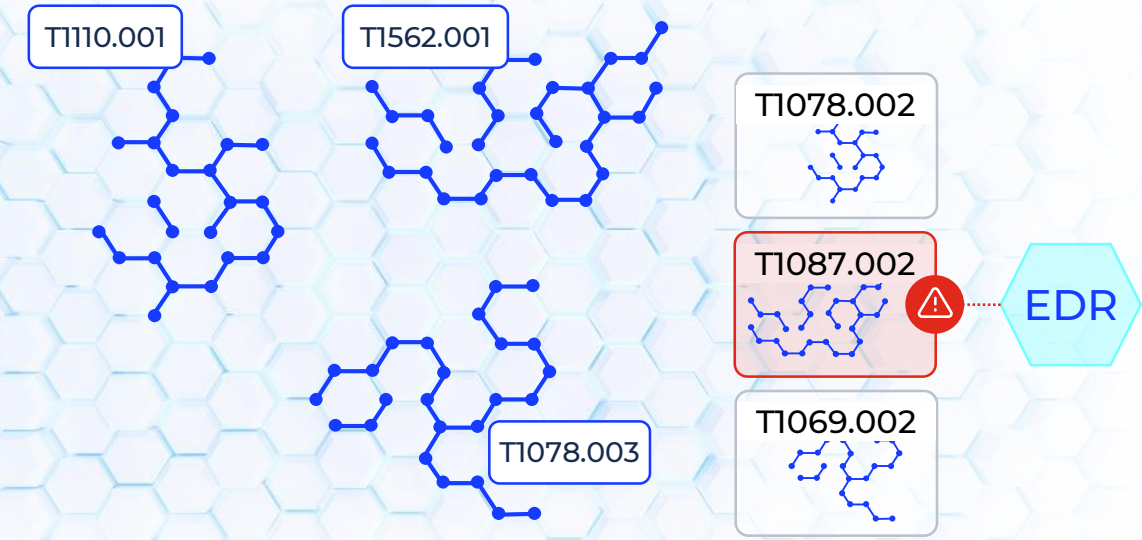
IoA
Автоматизированное выявление TTP атакующих

Deception
Выявление атакующих с помощью хостовых ловушек

Threat hunting
Ручной проактивный поиск следов и TPP атакующих

Мониторинг (сбор телеметрии)

- Процессы
- Файловая система
- Реестр
- Сетевая активность
- Память
- Учетные записи
- Входы, сессии
- Именованные каналы
- WMI
- Контейнеры
- Скрипты (PS, AMSI)



Расследование и реагирование

- Скачивание и загрузка файлов
- Завершение процесса
- Удаление файлов
- Выполнение действия через API
- Изоляция хоста
- Интерактивная консоль
- Запуск команд и скриптов
- Автоматическое реагирование

Телеметрия
Передача собранных событий

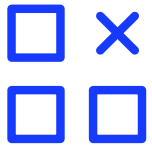
Обнаружение
Передача обнаружений по внутренним правилам

Реагирование
Возможность запуска команд по расследованию и реагированию

Интеграции с внешними СЗИ

Сбор телеметрии

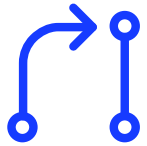
BI.ZONE



Нет необходимости
в сторонних программах

Собственный драйвер
на Windows

Современные технологии
получения событий (eBPF, ESF)



Гибкость сбора
и обогащения событий

40+

событий инвентаризации

180+

событий мониторинга

20 МБ

средний объем телеметрии
с одного агента в сутки

Профили сбора данных

BI.ZONE

Базовый профиль

Мониторинг

Инвентаризация

Высокая сетевая активность

Убираем мониторинг сети

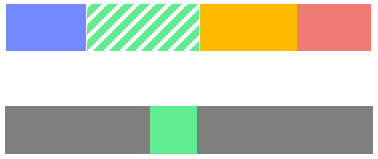
Фокусируемся на инвентаризации долгоживущих соединений

Высокая процессная активность

Убираем мониторинг запуска процессов

Фокусируемся на инвентаризации процессов в polling-режиме

Высокая файловая активность



Убираем мониторинг файловых операций

Фокусируемся на инвентаризации критичных файлов

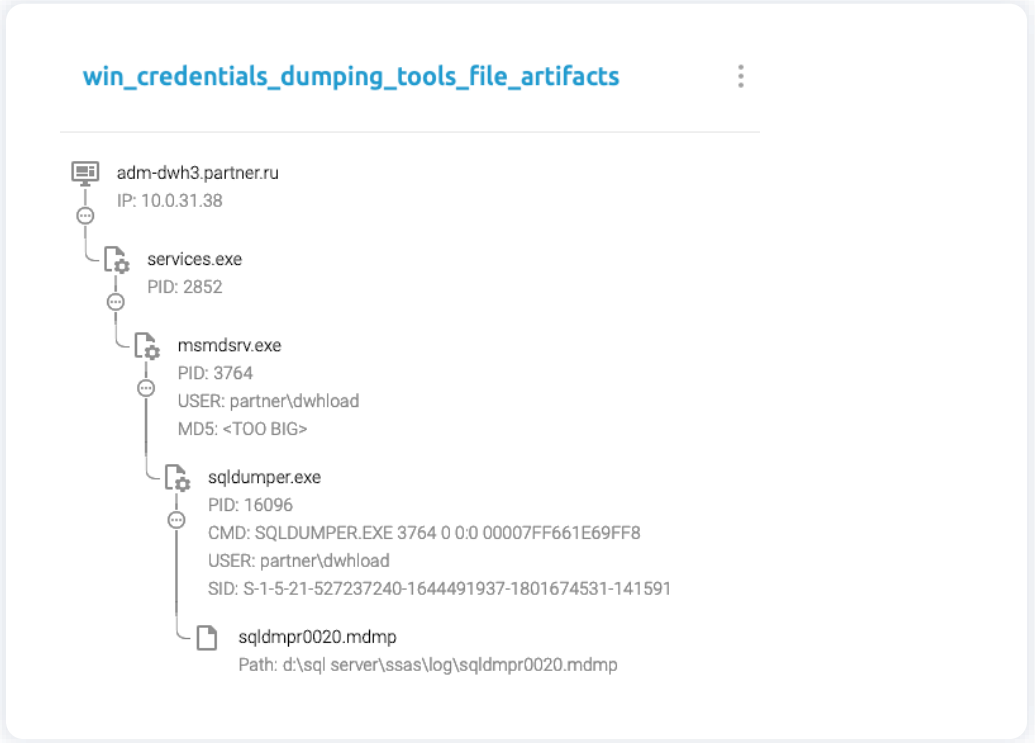
Обнаружение

BI.ZONE

- Различные технологии обнаружения: IoC, YARA, IoA
- Пользовательские правила и исключения
- Офлайн-детектирование без общения с сервером
- Дополнительный модуль Deception, хостовые приманки

900+
IoA-правил

2500+
YARA-правил



Технический аудит ОС и ПО

BI.ZONE

- Различные источники идей: CIS, NSA, ФСТЭК России
- Разработка на основе экспертного опыта
- Пользовательские правила и исключения
- Офлайн-детектирование без общения с сервером

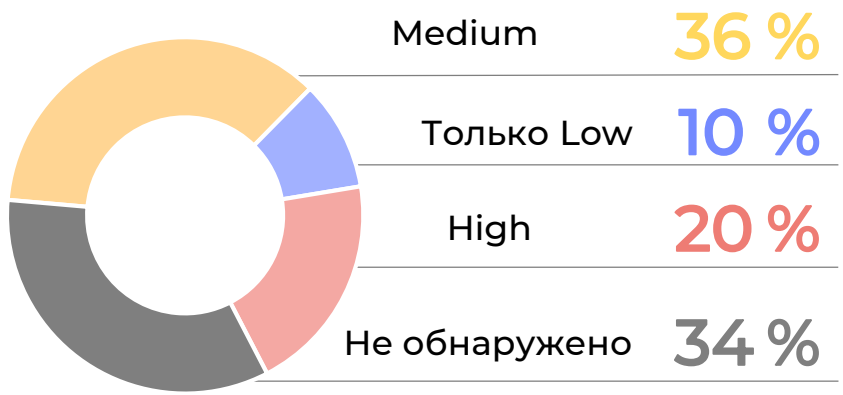
2 из 3

корпоративных компьютеров содержат хотя бы одну мисконфигурацию*

1 из 50

корпоративных локальных пользователей использует слабый пароль*

Распределение хостов по критичности выявленных мисконфигураций



* По данным BI.ZONE TDR (свыше 150 компаний и более 290 000 конечных точек)

Защита АСУ ТП

BI.ZONE

Возможность работы без драйвера

Легковесный конфиг мониторинга

Комплексные автоматические проверки:

- уязвимого ПО и небезопасных настроек
- контроля доступа, паролей и привилегий
- настроек сети и режима киоска
- событий кибербезопасности

Поддерживаемые системы:

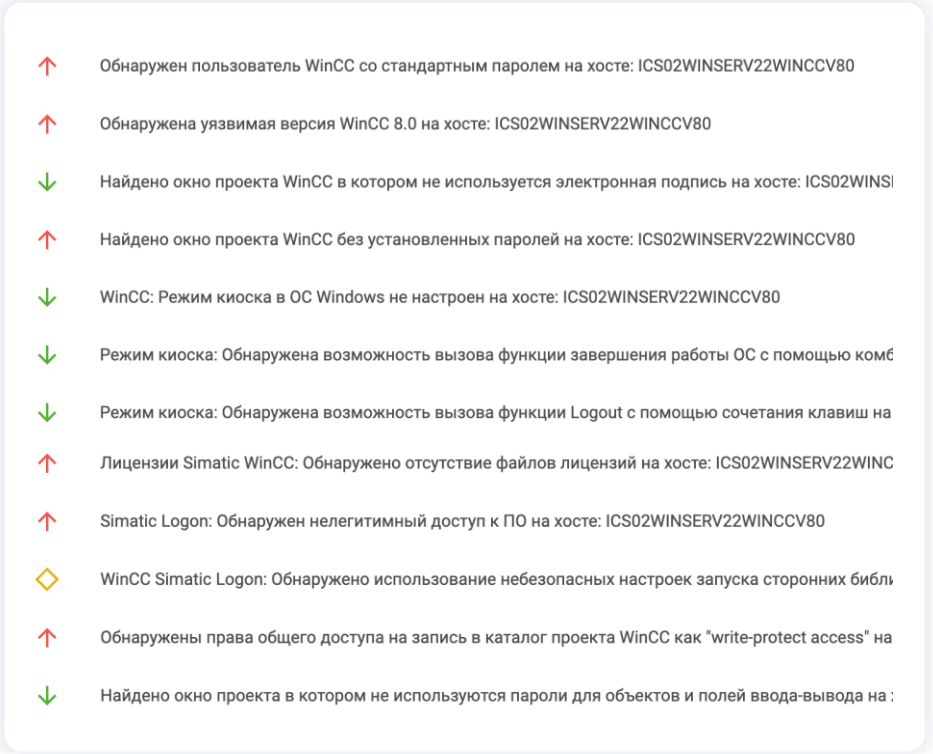
- WinCC Professional (версии 8.0–8.1)
- MasterSCADA 4D (версии 1.3.7–1.3.8)

Планируемые системы:

- Альфа-платформа
- TRACE MODE
- КАСКАД
- КРУГ-2000
- Redkit 2.0

45+
проверок для WinCC

40+
проверок для MasterSCADA 4D



Возможности BI.ZONE EDR для АСУ ТП

BI.ZONE

01

Определение публичных уязвимостей
в версиях поддерживаемого ПО АСУ ТП
с оценками и рекомендациями

02

Проверка прикладного и инженерного ПО
на небезопасные конфигурации:

- Ненастроенные параметры безопасности по security guide и другим материалам производителя систем автоматизации
- Наличие пользователей со слабыми паролями и без паролей
- Избыточные права доступа пользователей
- Небезопасные настройки веб-сервера или сетевого соединения
- Небезопасные настройки среды исполнения (режим киоска)
- Файлы проектов без паролей, неполное журналирование и др.

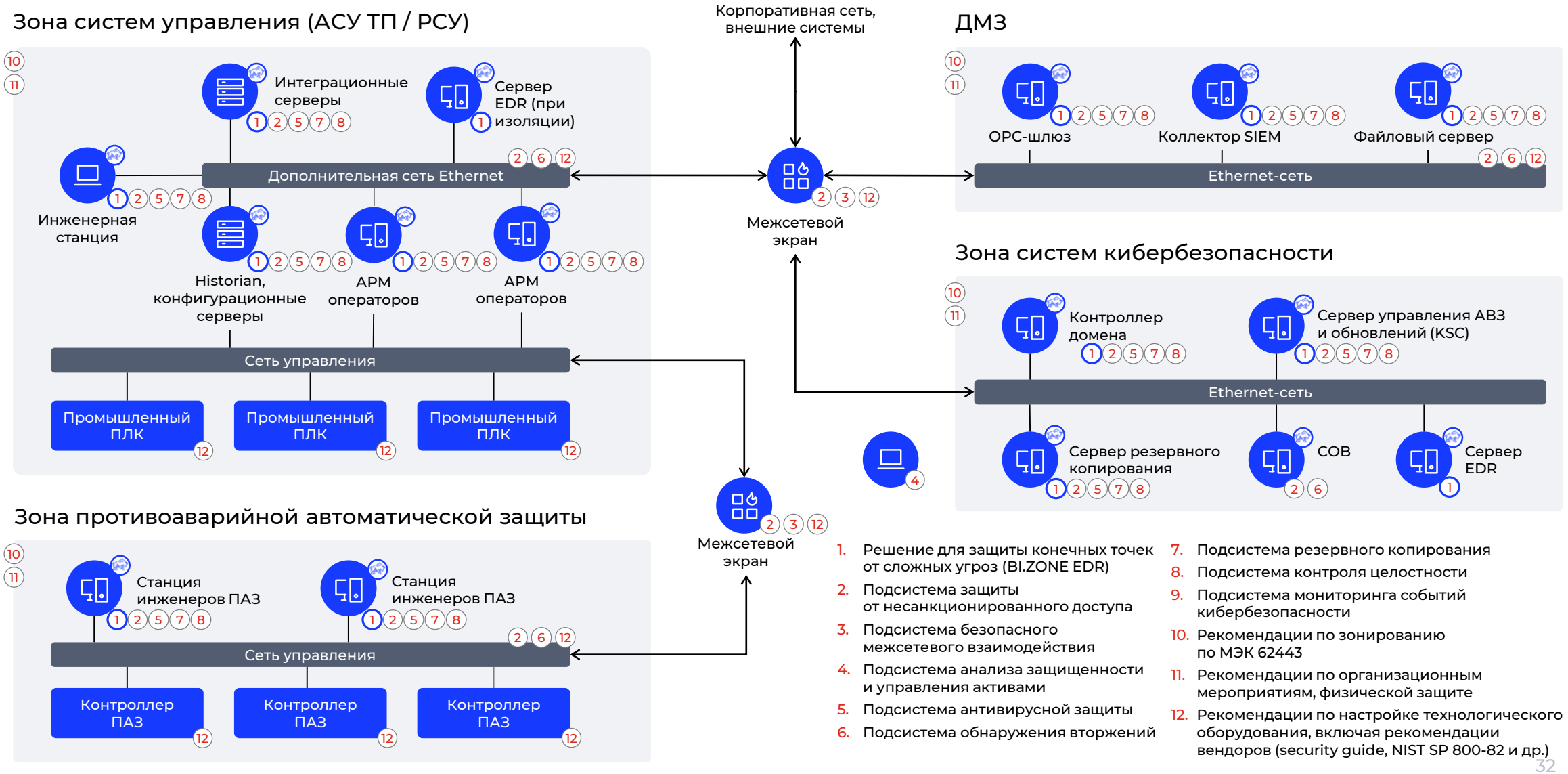
03

Регулярные проверки
воздействий/угроз:

- Запуск генераторов ключей и активаторов
- Очистка журналов событий безопасности
- Изменение файлов проекта, настроек БД, перебор паролей
- Удаление лицензий/ пользователей и др.

Применение BI.ZONE EDR для АСУ ТП

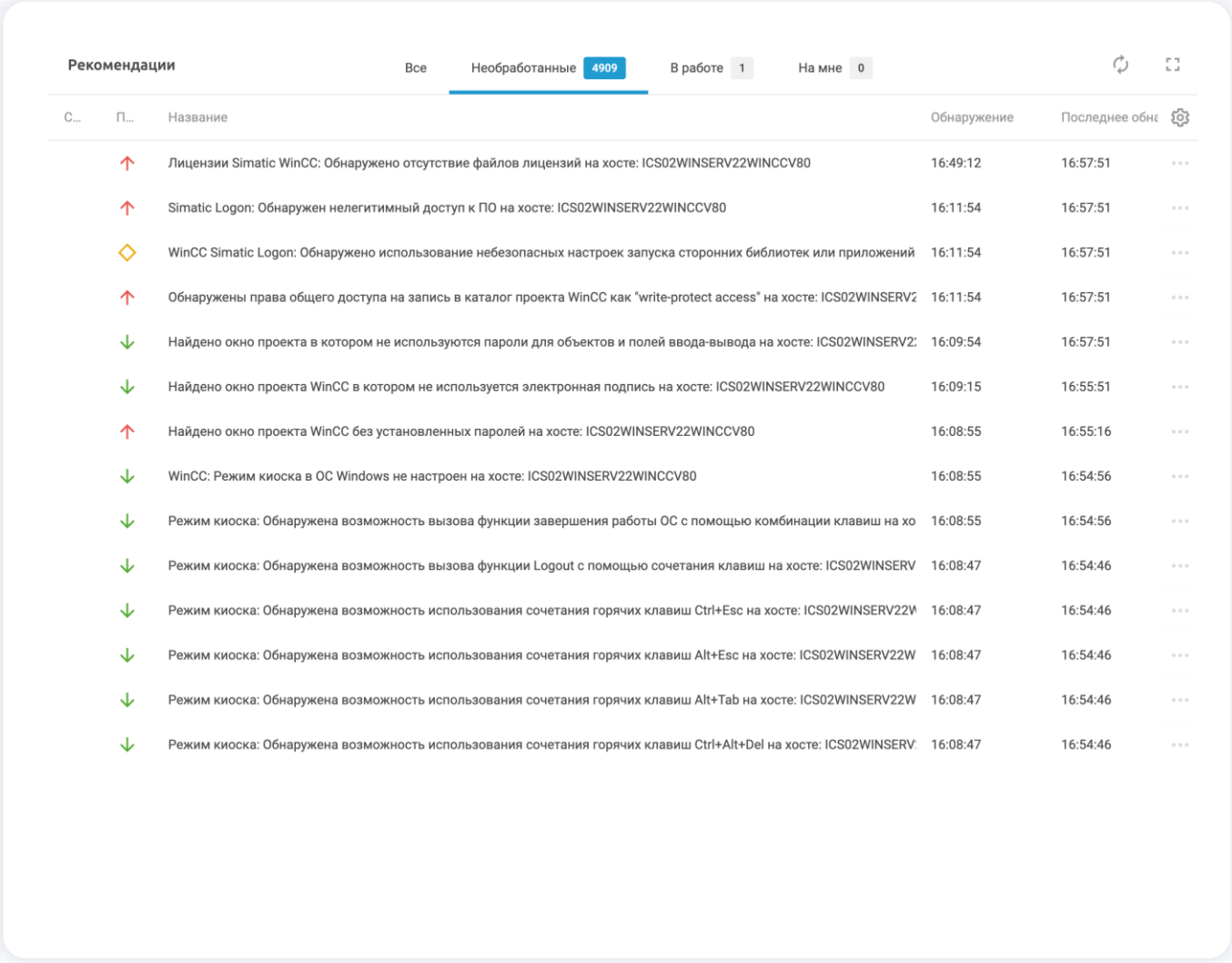
BI.ZONE

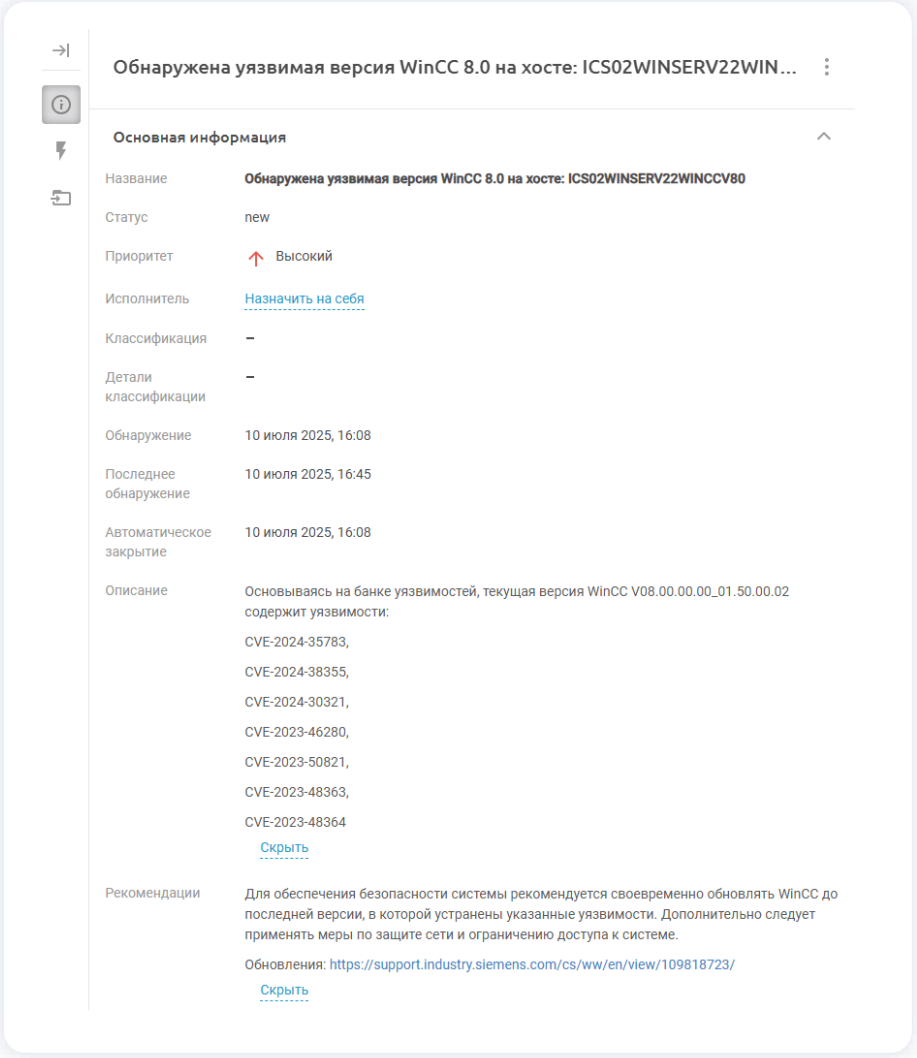


1. Решение для защиты конечных точек от сложных угроз (BI.ZONE EDR)
2. Подсистема защиты от несанкционированного доступа
3. Подсистема безопасного межсетевого взаимодействия
4. Подсистема анализа защищенности и управления активами
5. Подсистема антивирусной защиты
6. Подсистема обнаружения вторжений
7. Подсистема резервного копирования
8. Подсистема контроля целостности
9. Подсистема мониторинга событий кибербезопасности
10. Рекомендации по зонированию по МЭК 62443
11. Рекомендации по организационным мероприятиям, физической защите
12. Рекомендации по настройке технологического оборудования, включая рекомендации вендоров (security guide, NIST SP 800-82 и др.)

Пример правил для WinCC

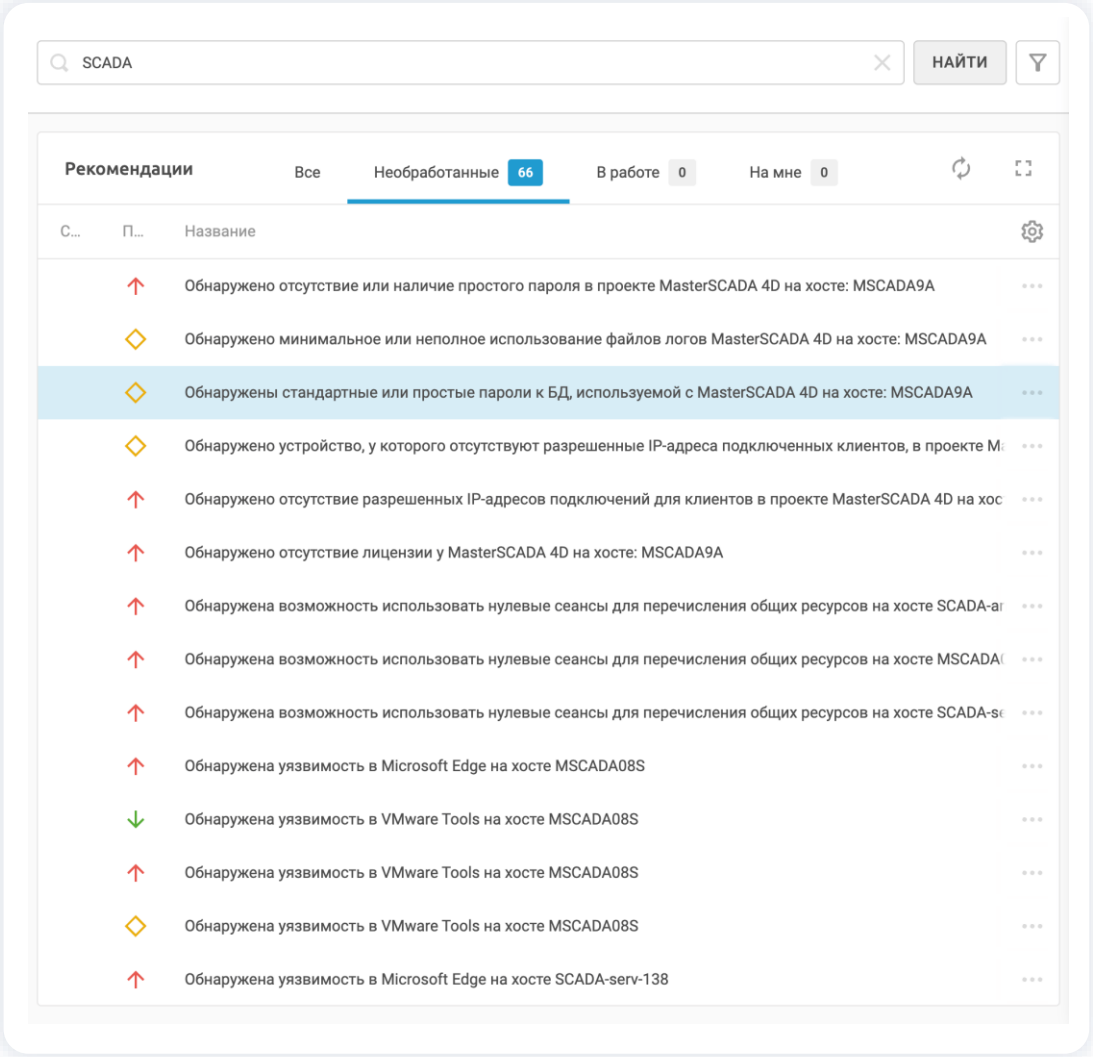
BI.ZONE

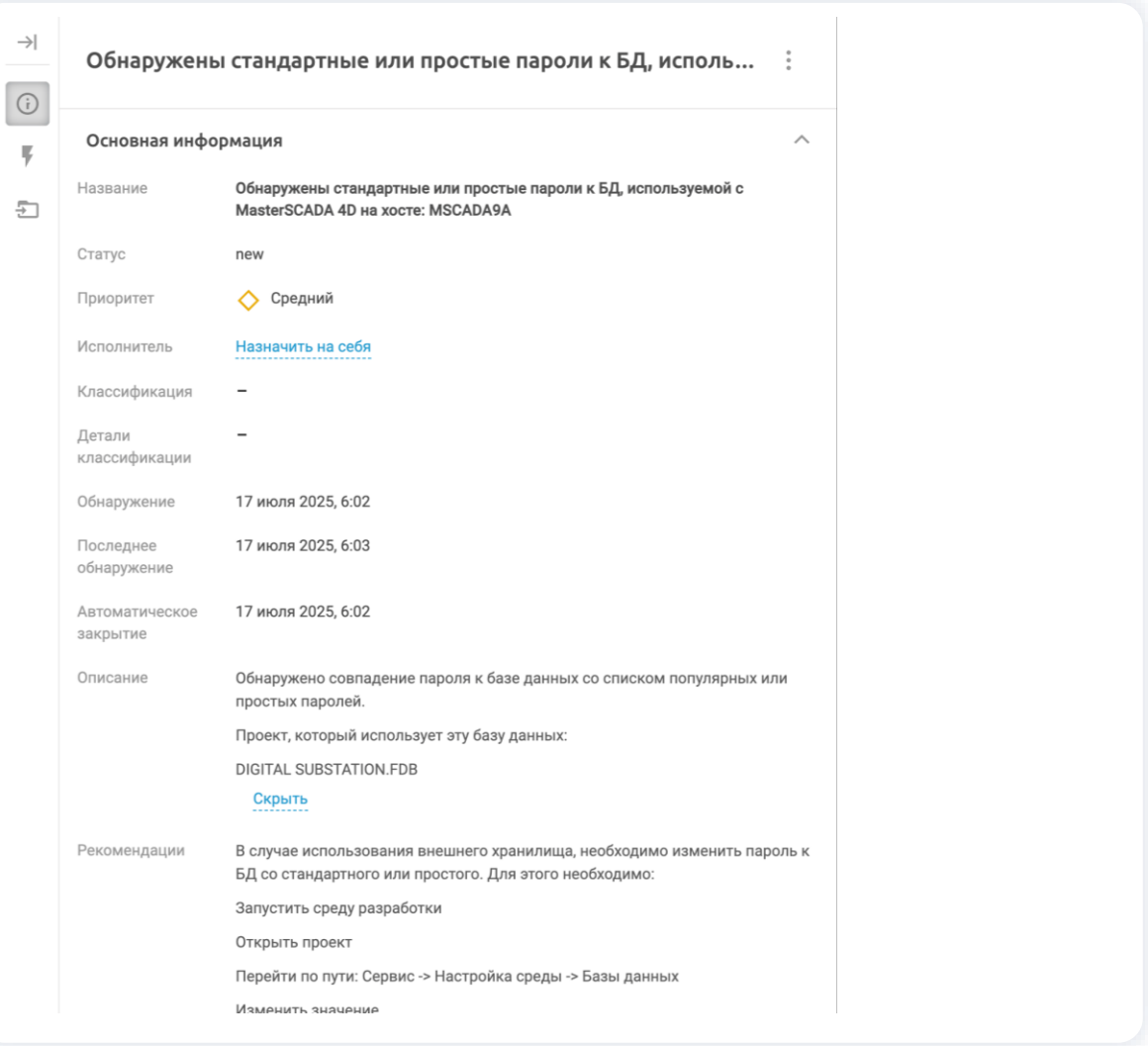




Пример правил для MasterSCADA 4D

BI.ZONE





Сценарий применения в WinCC

BI.ZONE

На множестве хостов обнаружили небезопасные настройки, в т. ч. уязвимости WinCC, стандартные имена и пароли пользователей, отсутствие паролей на окнах проекта и ненастроенный режим киоска

Отправили уведомления, обговорили время изменения

Обнаружили действия по изменению настроек безопасности в WinCC

Зафиксировали уменьшение количества окон без паролей и небезопасных настроек, однако повторно обнаружили пользователей с избыточными привилегиями и небезопасные настройки SIMATIC Logon

Сообщили о выявленных проблемах, требующих дополнительной настройки

Пример мисконфигурации в WinCC

BI.ZONE

Сценарий применения в WinCC

BI.ZONE

На множестве хостов обнаружили небезопасные настройки, в т. ч. уязвимости WinCC, стандартные имена и пароли пользователей, отсутствие паролей на окнах проекта и ненастроенный режим киоска

Сценарий применения в MasterSCADA 4D

BI.ZONE

Обнаружили на инженерной станции MasterSCADA 4D проект без пароля и отключенное журналирование, на сервере заметили стандартные настройки веб-сервера и другие небезопасные конфигурации

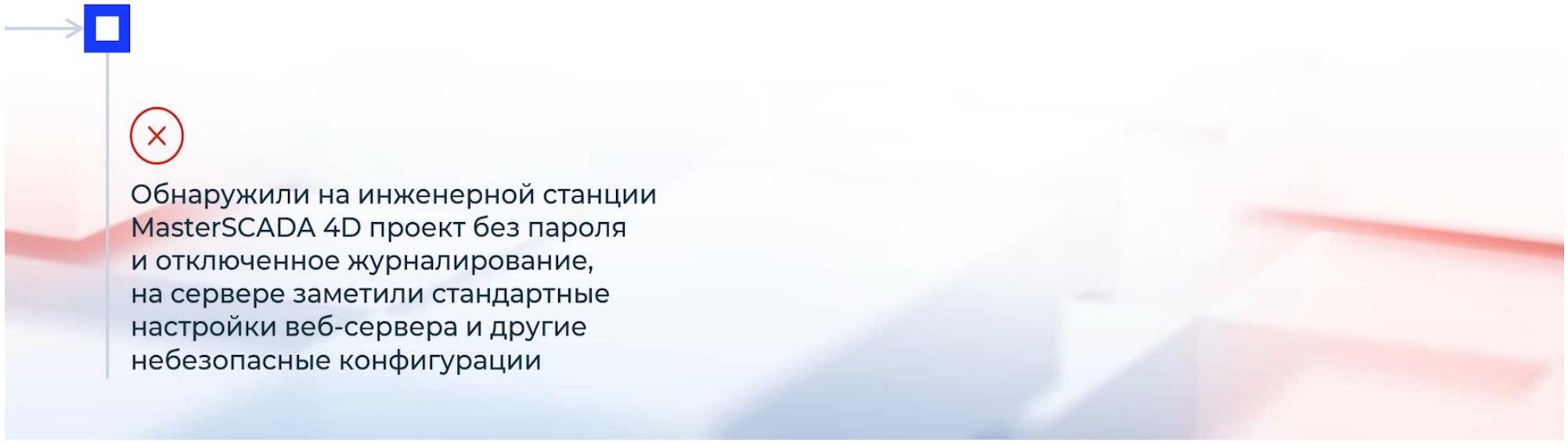
Отправили уведомление и внесли нужные изменения в проект и настройки веб-сервера

Выявили при повторной проверке на инженерной станции простой пароль от проекта, отключенное полное журналирование действий и отсутствие настройки списков разрешенных IP-адресов для клиентов и устройств

Сообщили о выявленных проблемах для дополнительной настройки

Пример мисконфигурации в MasterSCADA 4D BI.ZONE

Сценарий применения в MasterSCADA 4D BI.ZONE



Возможный сценарий развития воздействия (DC + OPC gate)

BI.ZONE

Злоумышленники собирают всю возможную информацию в корпоративной сети о системах АСУ ТП и их пользователях

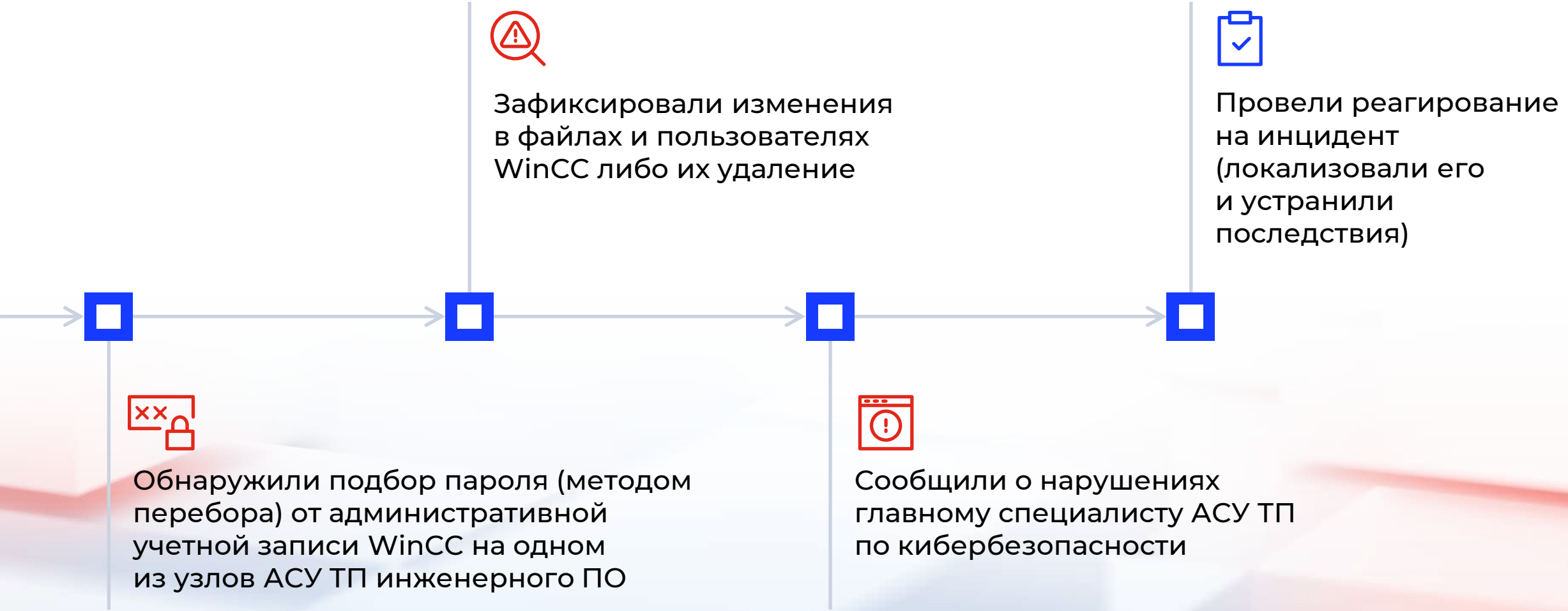
Сообщили о возможной атаке или нелегитимных действиях

Злоумышленники получили права администратора DC за счет методов атак типа LLMNR/NBT-NS spoofing + Responder или PetitPotam + NTLM relay

Зафиксировали дамп LSASS на одном из гейтов с OPC-клиентом для получения хешей паролей локальных учетных записей, которые используются для небезопасных протоколов OPC

Сценарий применения воздействий в WinCC

BI.ZONE



Пример воздействий на WinCC

BI.ZONE

Сценарий применения воздействий в WinCC

BI.ZONE

BI.ZONE

Планы развития и сертификация

Сертификация и партнерства

BI.ZONE

Реестр отечественного ПО

Сертификат ОАЦ при Президенте Республики Беларусь

Сертификаты ФСТЭК России:

- СОВ 4-го класса (октябрь 2025 г.)
- Антивирус (скоро)
- EDR (скоро)

Сертификаты совместимости с российским ОС:

- Astra Linux
- ALT Linux
- «РЕД ОС»

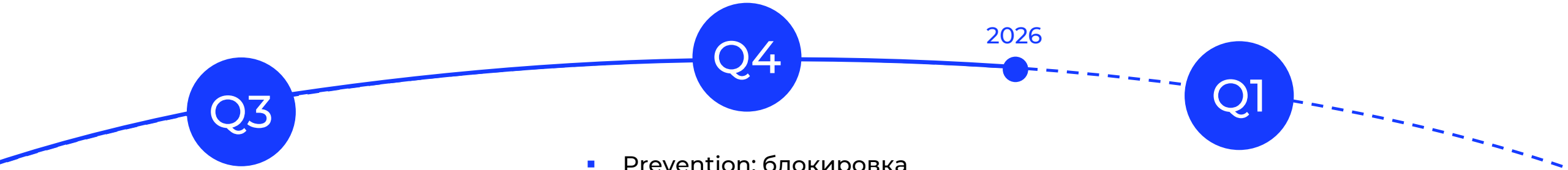
Сертификация на совместимость:

- SCADA решения (скоро)

Совместимость с популярными CAB3- и DLP-решениями

Стратегия развития BI.ZONE EDR

BI.ZONE



- IoC-сканер
- Улучшенный CMDB
- Сетевая изоляция Linux
- Мониторинг консольного ввода Windows
- АСУ ТП: WinCC и MasterSCADA 4D, дополнительные проверки

- Prevention: блокировка запуска и открытия файлов
- Коррелятор на сервере
- Deception (новые ОС и приманки)
- АСУ ТП: MasterSCADA 4D Linux и Альфа Платформа
- Сетевой сканер: порты

- Поиск неуправляемых устройств
- Конструктор правил в UI
- АСУ ТП: Поддержка других SCADA решений
- Сетевой сканер: обнаружение

BI.ZONE

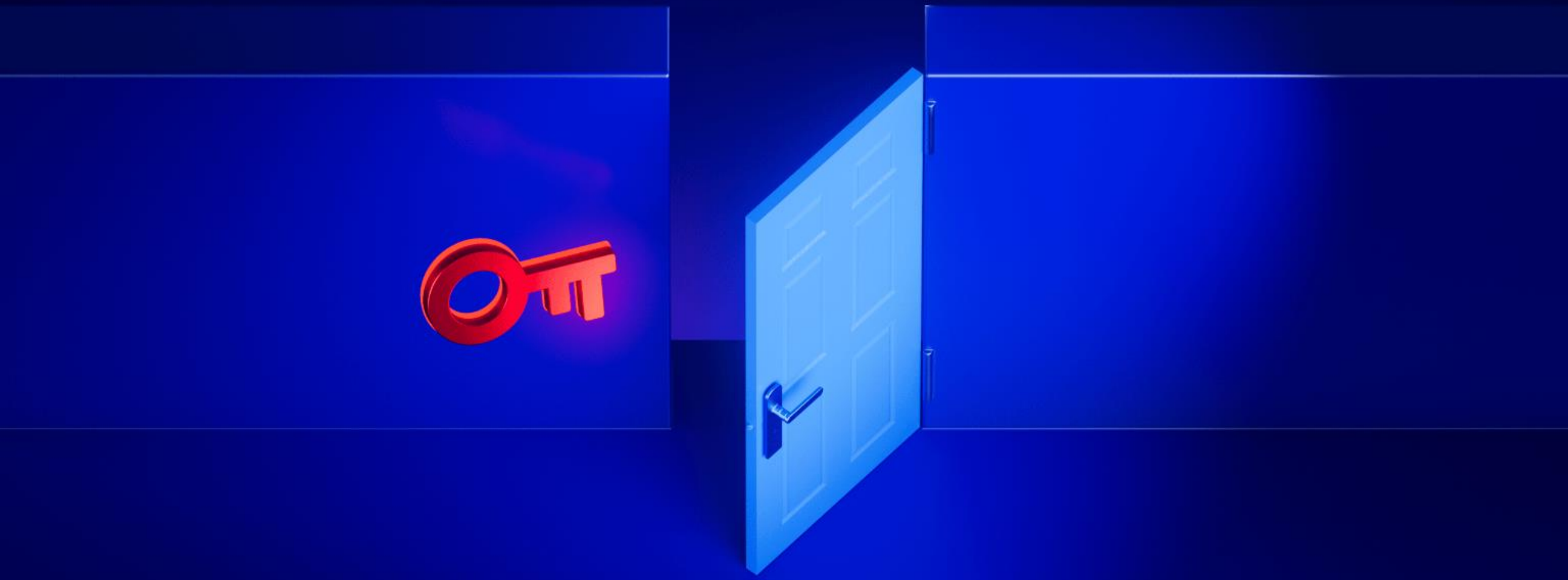
Сравнение антивируса, SIEM и EDR

Антивирус: базовая защита

BI.ZONE

Антивирус: базовая, но уязвимая защита

BI.ZONE

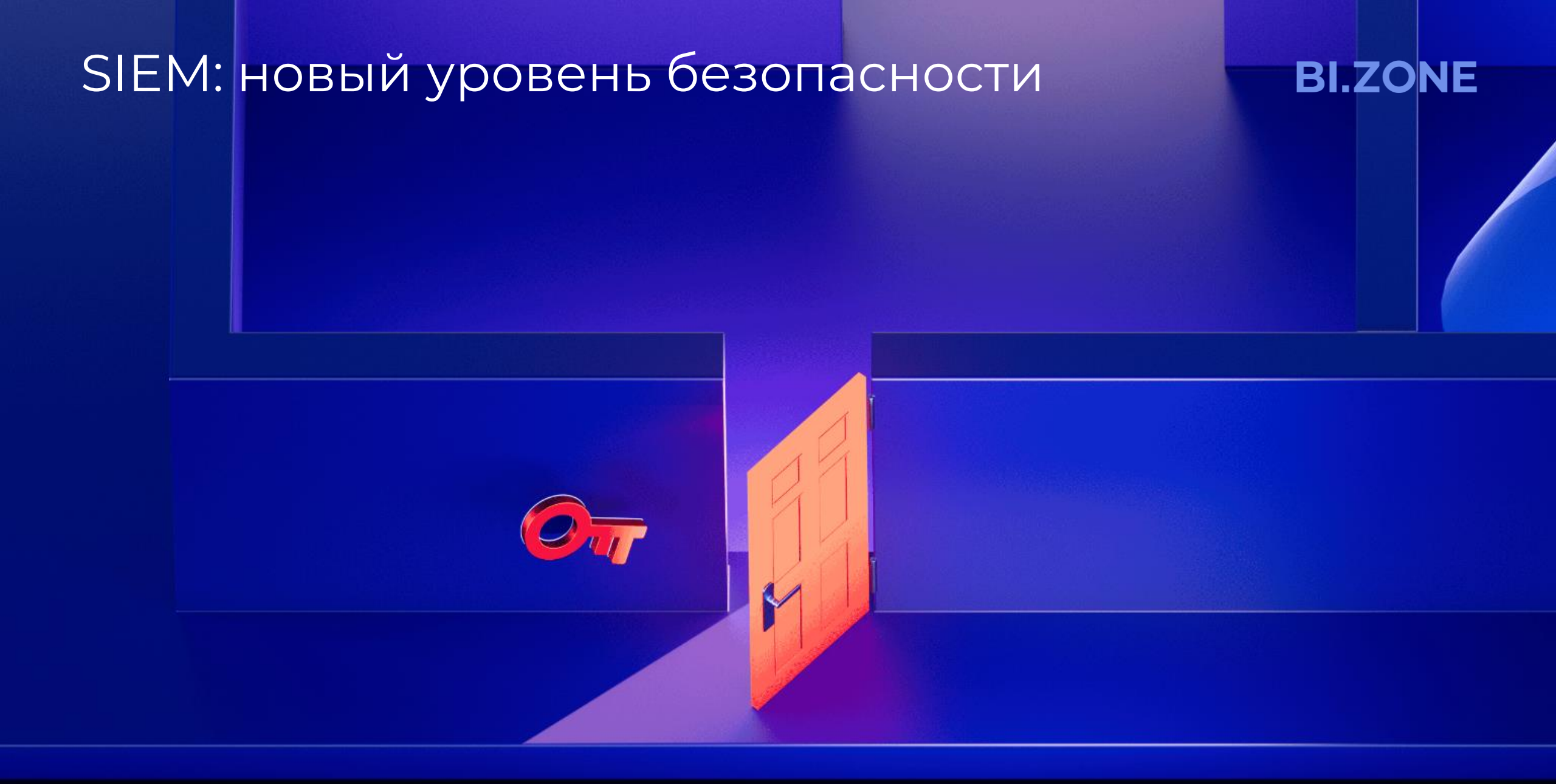


Антивирус: базовая, но уязвимая защита

BI.ZONE

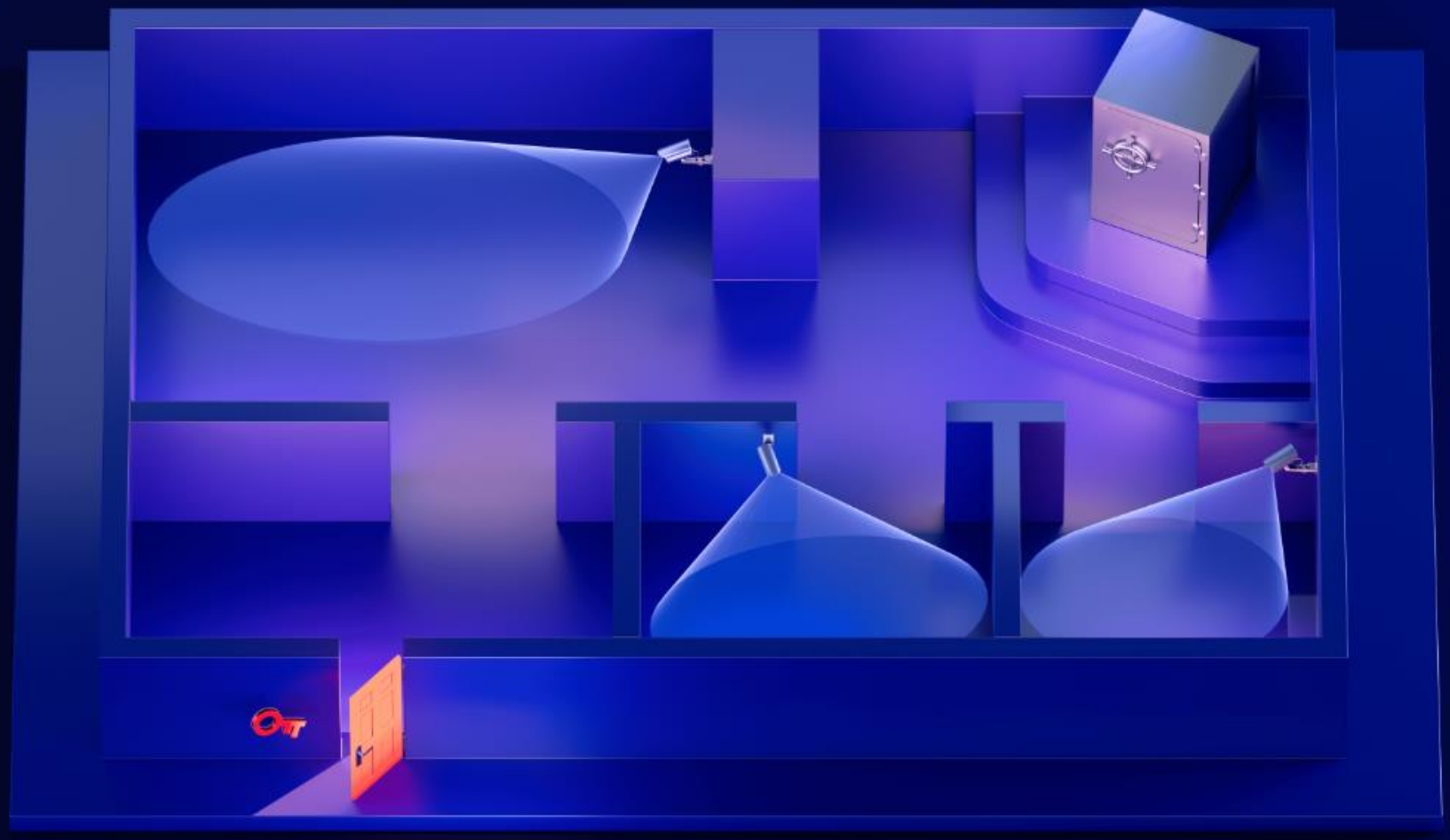
SIEM: новый уровень безопасности

BI.ZONE



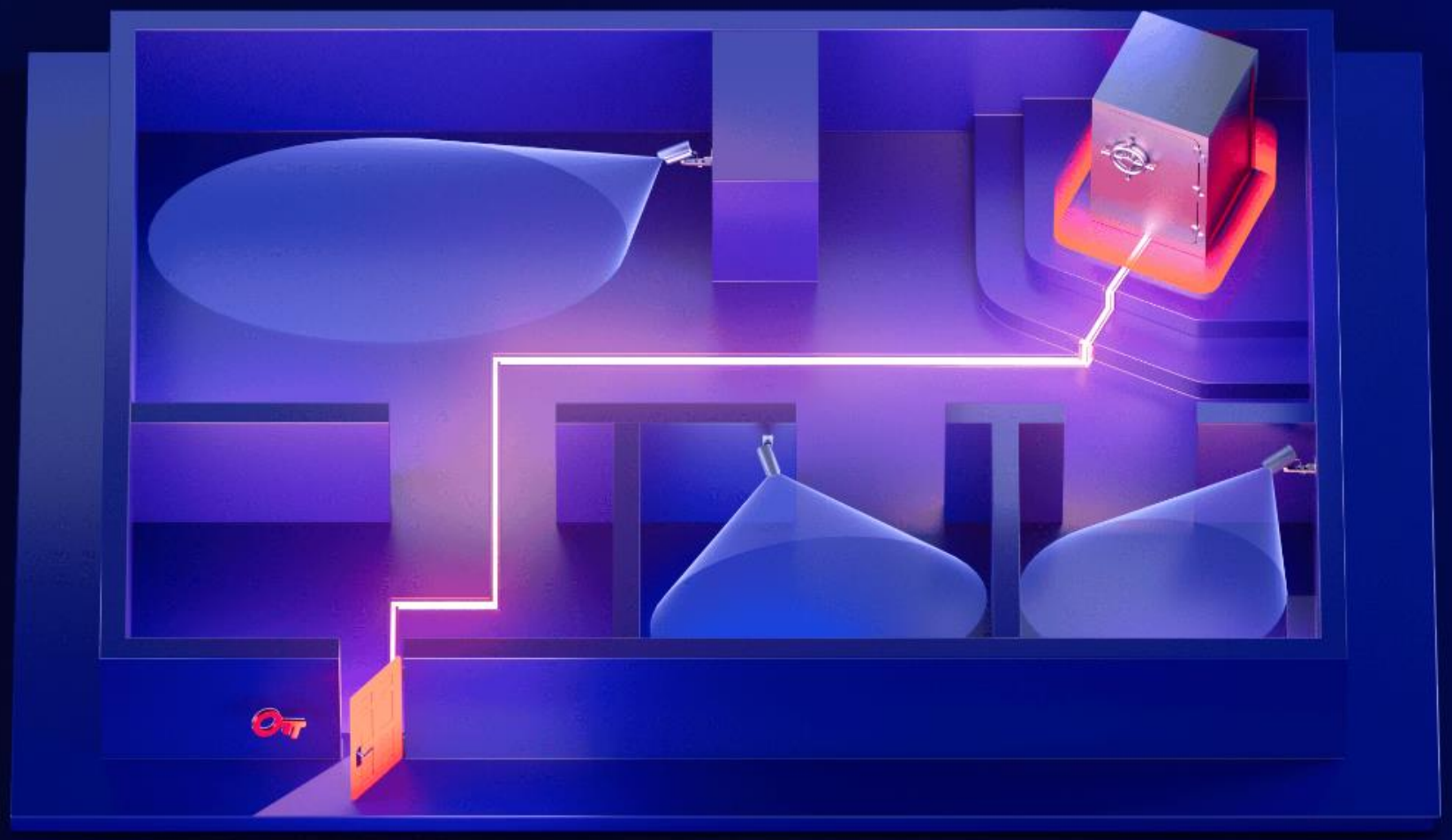
SIEM: новый уровень безопасности

BI.ZONE



SIEM: безопасность, но со слепыми зонами

BI.ZONE



EDR: гибкая защита и реагирование

BI.ZONE

BI.ZONE

Спасибо!
Вопросы?

Перейти в телеграм-канал BI.ZONE

Узнать больше о BI.ZONE EDR