Kaspersky Industrial Cybersecurity Conference 2023

Привилегированный доступ к промышленным объектам

Константин Родин
Руководитель направления
по развитию продуктов

«АйТи Бастион»

kaspersky

Каждая фабрика и каждый завод, посмотри внимательно это вот

1. Эй, лодыри,
работай до одури!
2. Взялись, и вот
результат работы за 17-й год.
3. Опять упала
производительность труда, —
думает буржуй, — проберусь
туда.
4. А вот буржуй сидит и плачет,
сами понимаете, что это
значит.

1924 г.

78% – это целевые атаки

От нескольких сетевых интерфейсов до утилит удаленного доступа

От «временного» решения до человеческой забывчивости

От своих сотрудников до сотрудников подрядных организаций

Вектор атак

Сканирование периметра

DDoS

Эксплуатация известных уязвимостей внешних ресурсов

Изменение

Увеличение сложности атак

Последствия

2 Атаки на цепочку поставок (Backdoor, компрометация инфраструктуры подрядчика)

Компрометация оборудования сотрудника

Попытки развития атак

* по данным расследования заказчика

Основные запросы

на контроль привилегированного доступа в промышленных сетях.

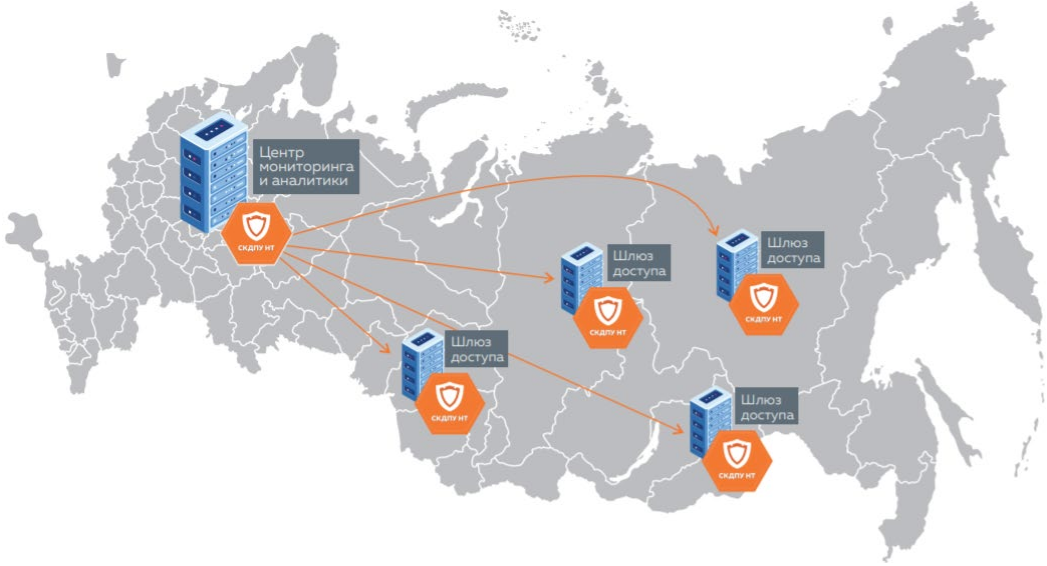
Комплексные проекты
Одного решения мало, требуется полноценная инфраструктура на базе отечественных решений.

«Сырые» данные не интересны
Нет времени и некому разбираться со всем объемом данных – требуются решения аналитики и принятия решений.

«Контролируемый взлом»
Не только выстраивание инфраструктуры для предоставления доступа, но и детектирования атак на его основе.

Внедряйтесь
и взлетайте
и вширь
и ввысь.
Взвивай,
изобретатель,
рабочую
мысль!
С памятник ростом
будут
наши капусты
и наши моркови,
будут лучшими в мире
наши
коровы
и кони.

География



Распределенные ИТ-инфраструктуры

Организация независимых точек доступа к каждому филиалу

Построение доступа через резервный канал и точку входа

Требования по гарантированной работе с другими средствами ИБ

Открытость миру для реализации комплексного подхода в ИБ

1. Система обнаружения вторжений
2. Средства виртуализации и облачные сервисы
3. Многофакторная аутентификация
4. Отечественные ОС
5. IRP/SOAR
6. Песочницы и антивирусы*
7. SIEM-системы
8. Безопасные рабочие места, тонкие клиенты и т.п.
9. Криптошлюзы и VPN-туннели
10. Token и Smart Card
11. DLP*
12. Threat Intelligence*

Основные запросы

на контроль привилегированного доступа в промышленных сетях.

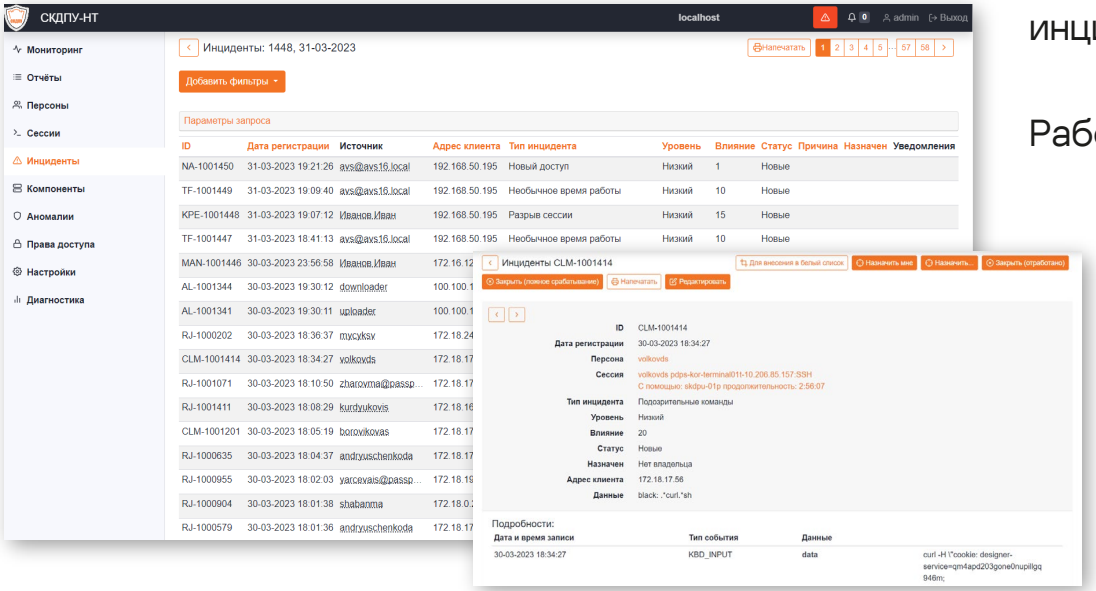
Комплексные проекты
Одного решения мало, требуется полноценная инфраструктура на базе отечественных решений.

«Сырые» данные не интересны
Нет времени и некому разбираться со всем объемом данных – требуются решения аналитики и принятия решений.

«Контролируемый взлом»
Не только выстраивание инфраструктуры для предоставления доступа, но и детектирования атак на его основе.

Крошка сын
к отцу пришёл,
и спросила кроха:
— Что такое
хорошо
и что такое
плохо? —
У меня
секретов нет, —
слушайте, детишки, —
папы этого
ответ
помещаю
в книжке.

Данные инцидентов

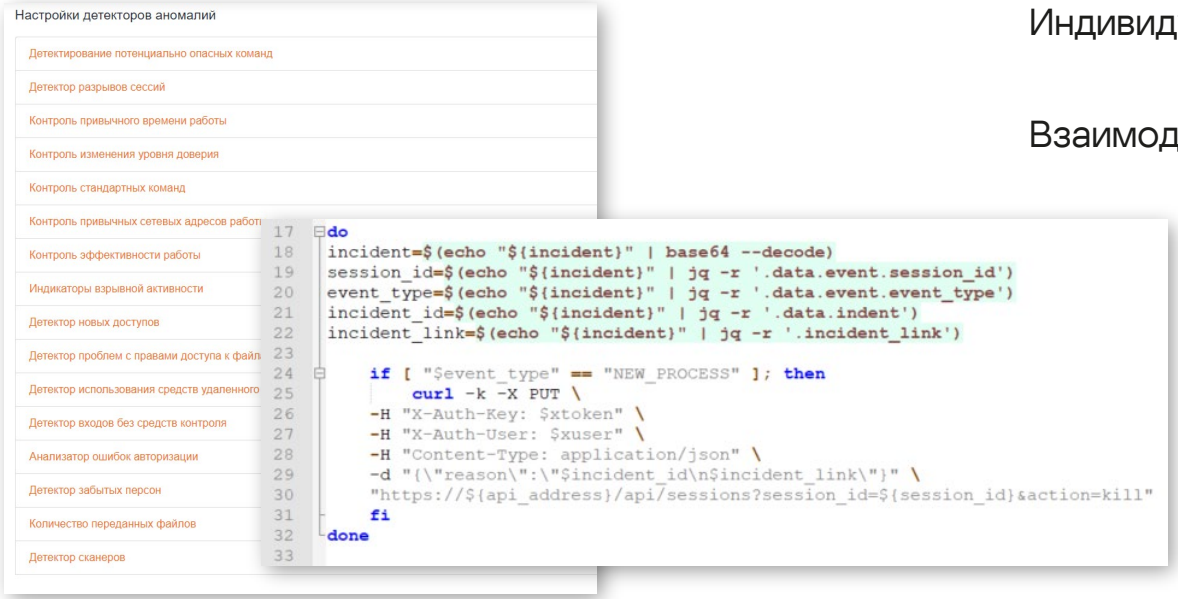


Обучаемая модель детектирования аномального поведения пользователей

Настраиваемые веса степени «тяжести» инцидентов

Рабочий процесс обработки инцидентов

Реагирование на инциденты



Подключение функций **реагирования на инциденты** и интеграция в единую систему реагирования

Индивидуальные модели реагирования

Взаимодействие с **SOAR/IRP**

Опыт заказчика

Анализ запущенных процессов

Сбор и накопление стандартных команд и процессов

Детектирование аномалий

«В правилах стоял детект на типичные thread injection, и в случае выполнения тех или иных команд даже в фоновом режиме - сессия сотрудника обрывалась. Удалось задетектировать подобную вредоносную активность, расследовать её комплексом сзи и отозвать доступ к системам компании N.»

Основные запросы

на контроль привилегированного доступа в промышленных сетях.

Комплексные проекты
Одного решения мало, требуется полноценная инфраструктура на базе отечественных решений.

«Сырые» данные не интересны
Нет времени и некому разбираться со всем объемом данных – требуются решения аналитики и принятия решений.

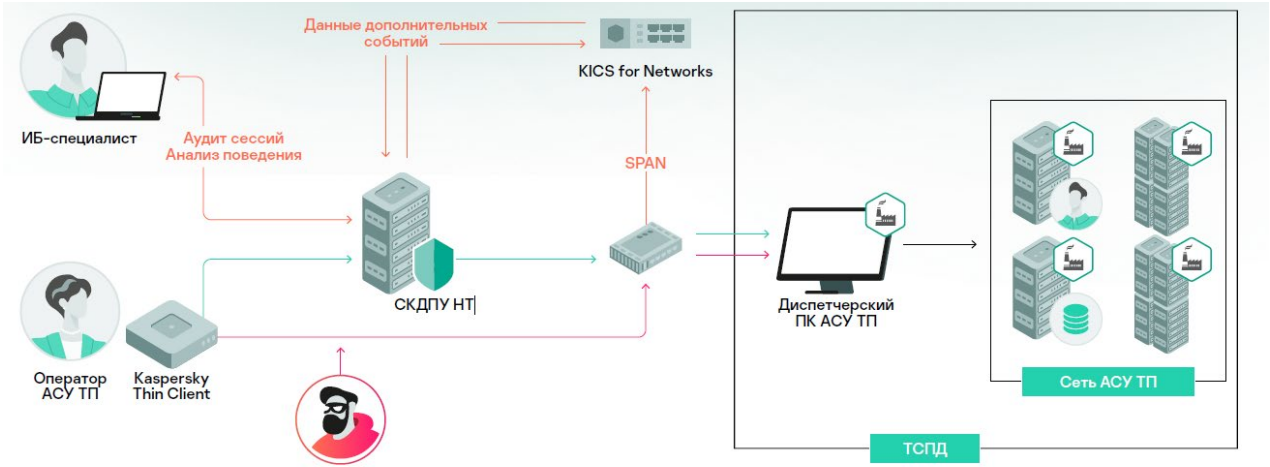
«Контролируемый взлом»
Не только выстраивание инфраструктуры для предоставления доступа, но и детектирования атак на его основе.

Сегментирование и ограничение доступа

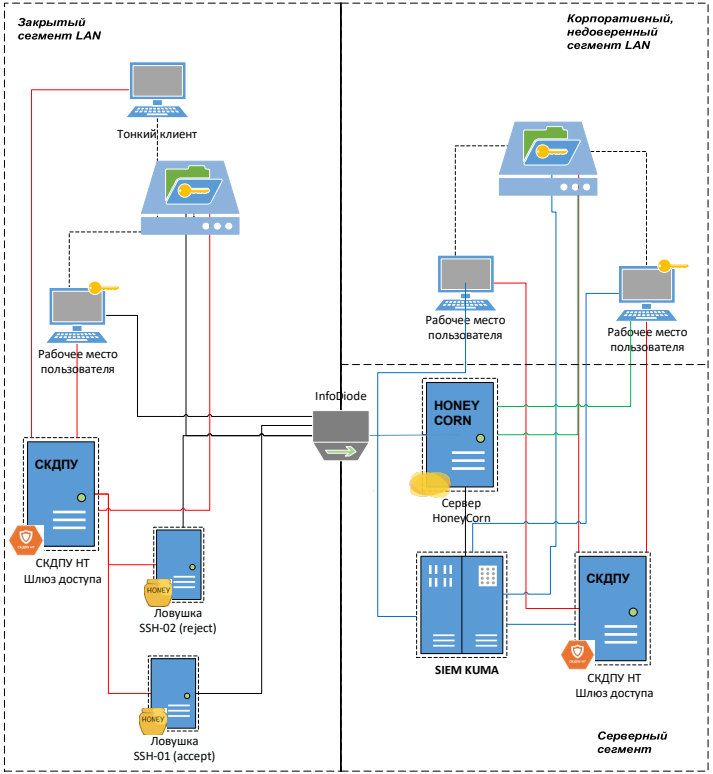
Регламентированный доступ из внешнего помещения через
систему контроля удаленного доступа с защищенного тонкого клиента

АЙТИБАСТИОН

kaspersky



Опыт 2023 года – интеграция в систему ловушек HoneyCorn



СКДПУ НТ является частью инфраструктуры как «боевой», так и инфраструктуры ловушек.

Развёртывание ловушек производится в автоматическом режиме

Фиксация факта срабатывания ловушек и возможность наблюдения за действиями нарушителя

АЙТИБАСТИОН

axxtel

Повышение осведомленности

Минимизация затрат за счет определения рисков

Комплексный подход к решению вопросов информационной безопасности

Диалог между производителем ПО и заказчиком

Спасибо!

Каждая фабрика и каждый завод, посмотри внимательно это вот:
привилегированный доступ к промышленным объектам

АЙТИБАСТИОН

Родин Константин

Руководитель направления по развитию продуктов

«АйТи Бастион»
k.rodin@it-bastion.com

kaspersky