



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



2022

# Вектор атак

Сканирование периметра

DDoS

Эксплуатация известных  
уязвимостей внешних ресурсов

2023

4

# 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**

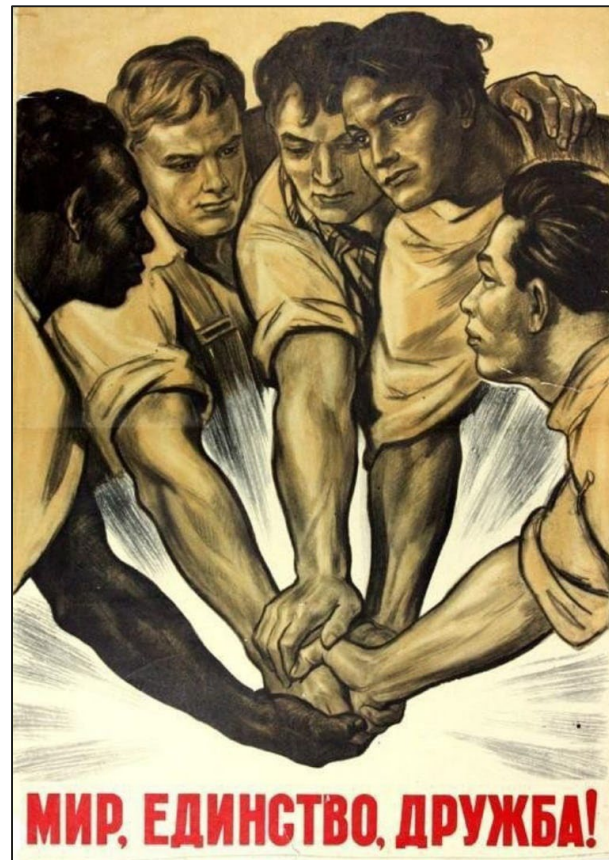
Нет времени и некому разбираться со всем объемом данных – требуются решения аналитики и принятия решений.

## **«Контролируемый взлом»**

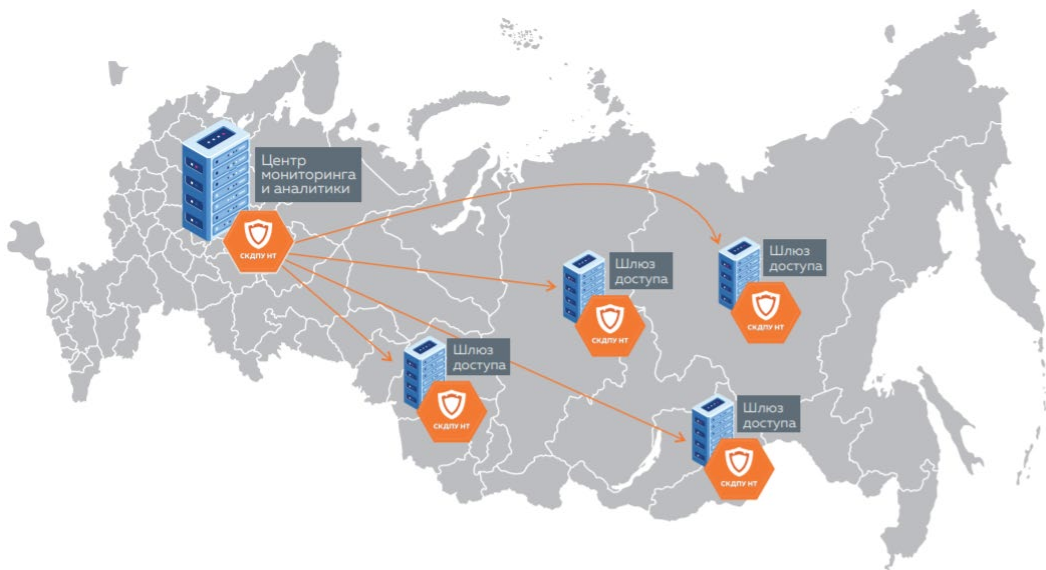
Не только выстраивание инфраструктуры для предоставления доступа, но и детектирования атак на его основе.

“

Внедряйтесь  
и взлетайте  
и вширь  
и ввысь.  
Взвивай,  
изобретатель,  
рабочую  
мысль!  
С памятник ростом  
будут  
наши капуста  
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

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

The screenshot displays the SKDPU-NT web interface. The left sidebar contains navigation options: Мониторинг, Отчёты, Персоны, Сессии, Инциденты (highlighted), Компоненты, Аномалии, Права доступа, Настройки, and Диагностика. The main area shows a list of incidents for the date 31-03-2023, with 1448 incidents found. A table lists incidents with columns for ID, registration date, source, client address, incident type, level, weight, status, cause, assignee, and notification.

ID	Дата регистрации	Источник	Адрес клиента	Тип инцидента	Уровень	Влияние	Статус	Причина	Назначен	Уведомления
NA-1001450	31-03-2023 19:21:26	avs@avs16.local	192.168.50.195	Новый доступ	Низкий	1	Новые			
TF-1001449	31-03-2023 19:09:40	avs@avs16.local	192.168.50.195	Необычное время работы	Низкий	10	Новые			
KPE-1001448	31-03-2023 19:07:12	Иванов.Иван	192.168.50.195	Разрыв сессии	Низкий	15	Новые			
TF-1001447	31-03-2023 18:41:13	avs@avs16.local	192.168.50.195	Необычное время работы	Низкий	10	Новые			
MAN-1001446	30-03-2023 23:56:58	Иванов.Иван	172.16.12							
AL-1001344	30-03-2023 19:30:12	downloader	100.100.1							
AL-1001341	30-03-2023 19:30:11	uploader	100.100.1							
RJ-1000202	30-03-2023 18:36:37	mykskv	172.18.24							
CLM-1001414	30-03-2023 18:34:27	volkovds	172.18.17							
RJ-1001071	30-03-2023 18:10:50	zharovma@passp...	172.18.17							
RJ-1001411	30-03-2023 18:08:29	kurdykovds	172.18.16							
CLM-1001201	30-03-2023 18:05:19	borovkovas	172.18.17							
RJ-1000635	30-03-2023 18:04:37	andryuschenkoda	172.18.17							
RJ-1000955	30-03-2023 18:02:03	yarcovas@passp...	172.18.16							
RJ-1000904	30-03-2023 18:01:38	shabanoma	172.18.0:							
RJ-1000579	30-03-2023 18:01:36	andryuschenkoda	172.18.17							

The detailed view for incident CLM-1001414 shows the following information:

- ID:** CLM-1001414
- Дата регистрации:** 30-03-2023 18:34:27
- Персона:** volkovds
- Сессия:** volkovds:rdp-a-kor-fermail011-10.206.85.157 SSH  
С логотипом: volkovds-01r продолжительность: 2:56:07
- Тип инцидента:** Подозрительные команды
- Уровень:** Низкий
- Влияние:** 20
- Статус:** Новые
- Назначен:** Нет владельца
- Адрес клиента:** 172.18.17.56
- Данные:** black, "curl", "h"

Below the details, there is a section for "Подробности: Дата и время записи" with a table:

Дата и время записи	Тип события	Данные
30-03-2023 18:34:27	KBD_INPUT	data curl -H "Cookie: designe- service=qm4pd203gonebnuplqg 946m;

# Реагирование на инциденты

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

Индивидуальные модели реагирования

Взаимодействие с **SOAR/IRP**

The image shows a configuration interface on the left and a shell script on the right. The interface, titled 'Настройки детекторов аномалий', lists various detectors such as 'Детектирование потенциально опасных команд', 'Детектор разрывов сессий', and 'Детектор новых доступов'. The shell script on the right is a Bash script that processes incident data and triggers a response via a REST API.

```
17 do
18 incident=$(echo "${incident}" | base64 --decode)
19 session_id=$(echo "${incident}" | jq -r '.data.event.session_id')
20 event_type=$(echo "${incident}" | jq -r '.data.event.event_type')
21 incident_id=$(echo "${incident}" | jq -r '.data.incident')
22 incident_link=$(echo "${incident}" | jq -r '.incident_link')
23
24 if [ "$event_type" == "NEW_PROCESS" ]; then
25     curl -k -X PUT \
26     -H "X-Auth-Key: $xtoken" \
27     -H "X-Auth-User: $xuser" \
28     -H "Content-Type: application/json" \
29     -d "{\"reason\": \"${incident_id}\n${incident_link}\"} \" \
30     "https://${api_address}/api/sessions?session_id=${session_id}&action=kill"
31 fi
32 done
33
```

# 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**

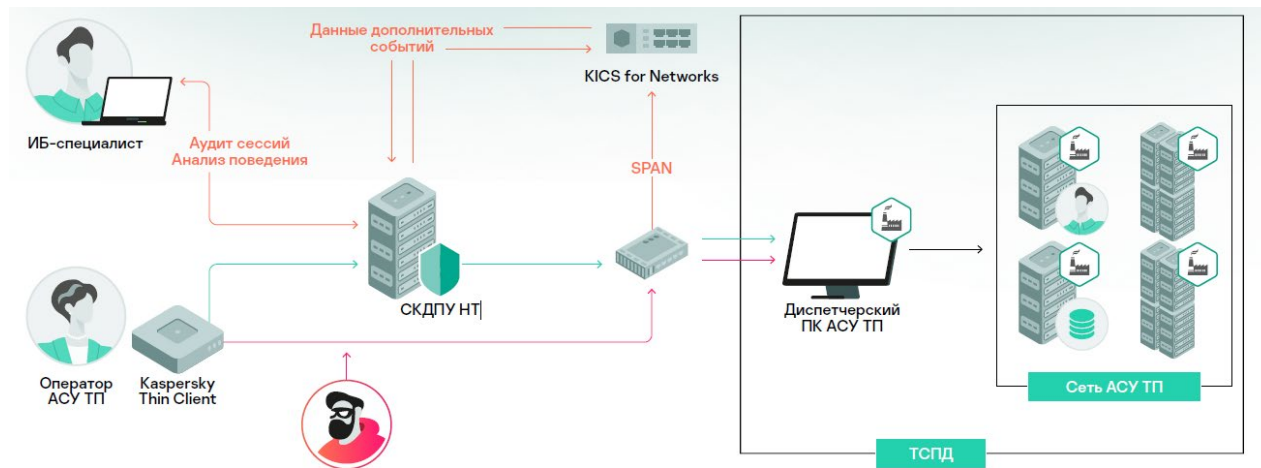
Нет времени и некому разбираться со всем объемом данных – требуются решения аналитики и принятия решений.

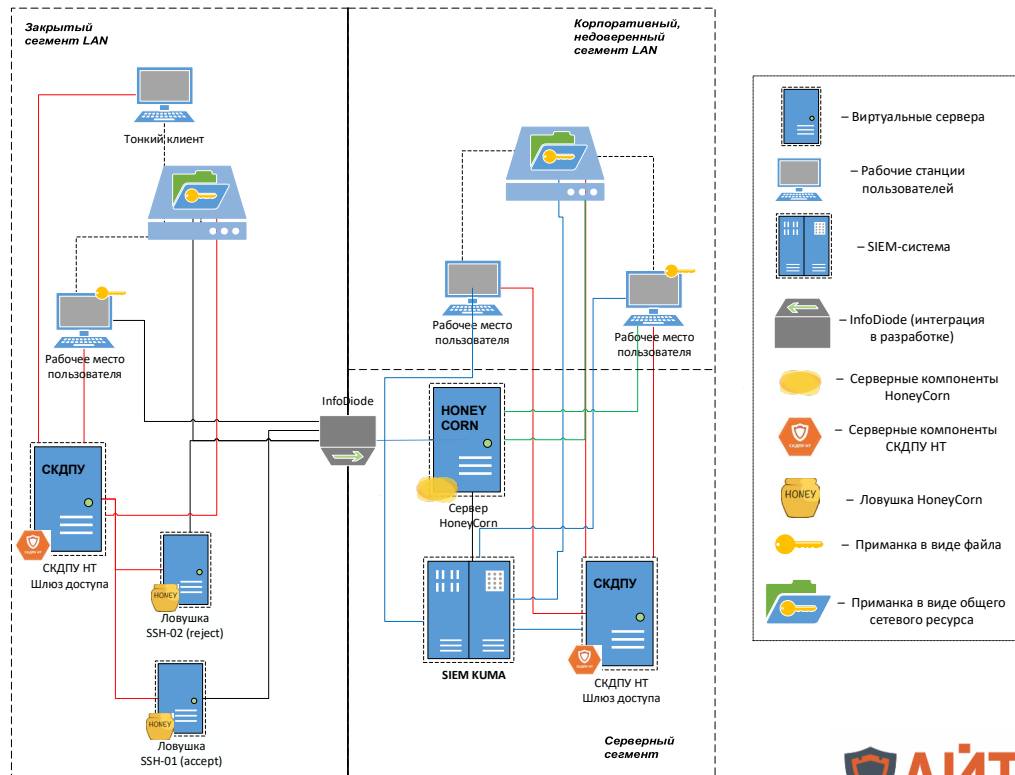
## **«Контролируемый взлом»**

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**





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

# 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



Родин Константин

Руководитель направления по  
развитию продуктов

«АйТи Бастион»  
[k.rodin@it-bastion.com](mailto:k.rodin@it-bastion.com)

**kaspersky**