

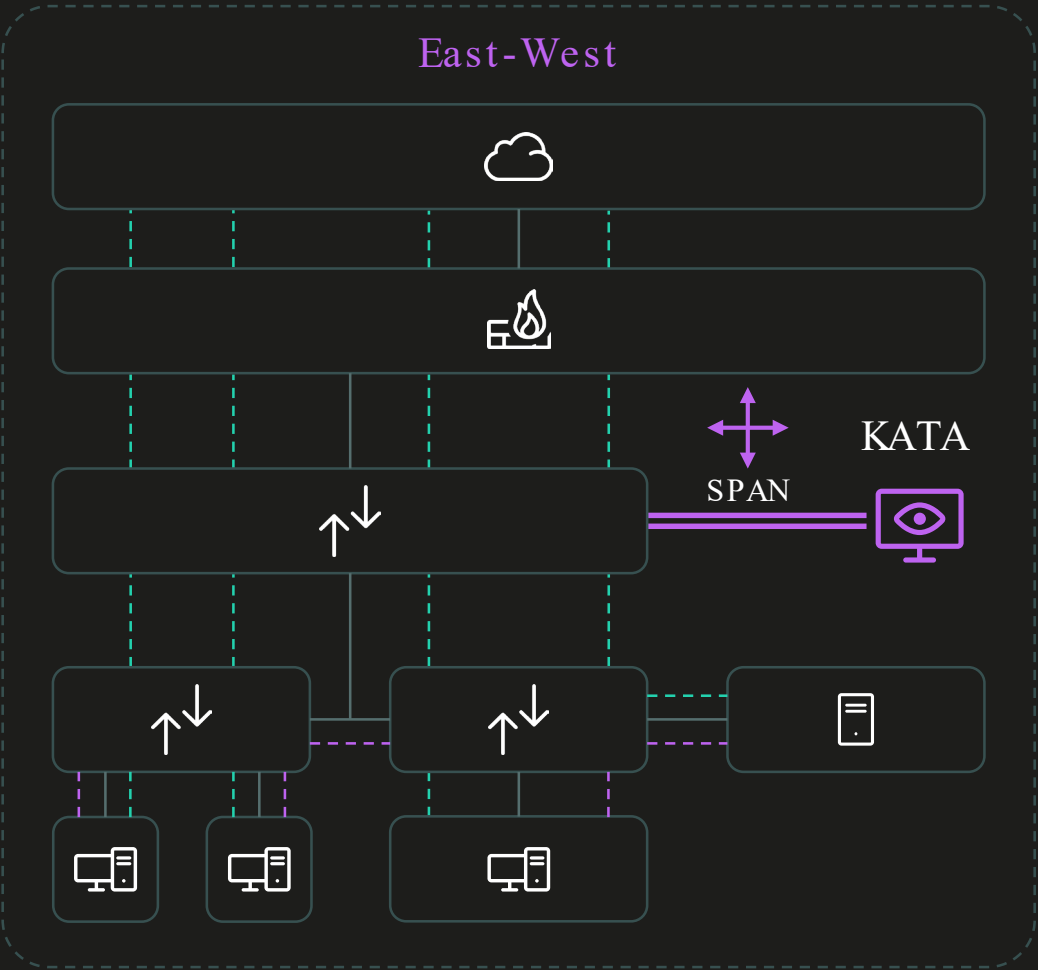
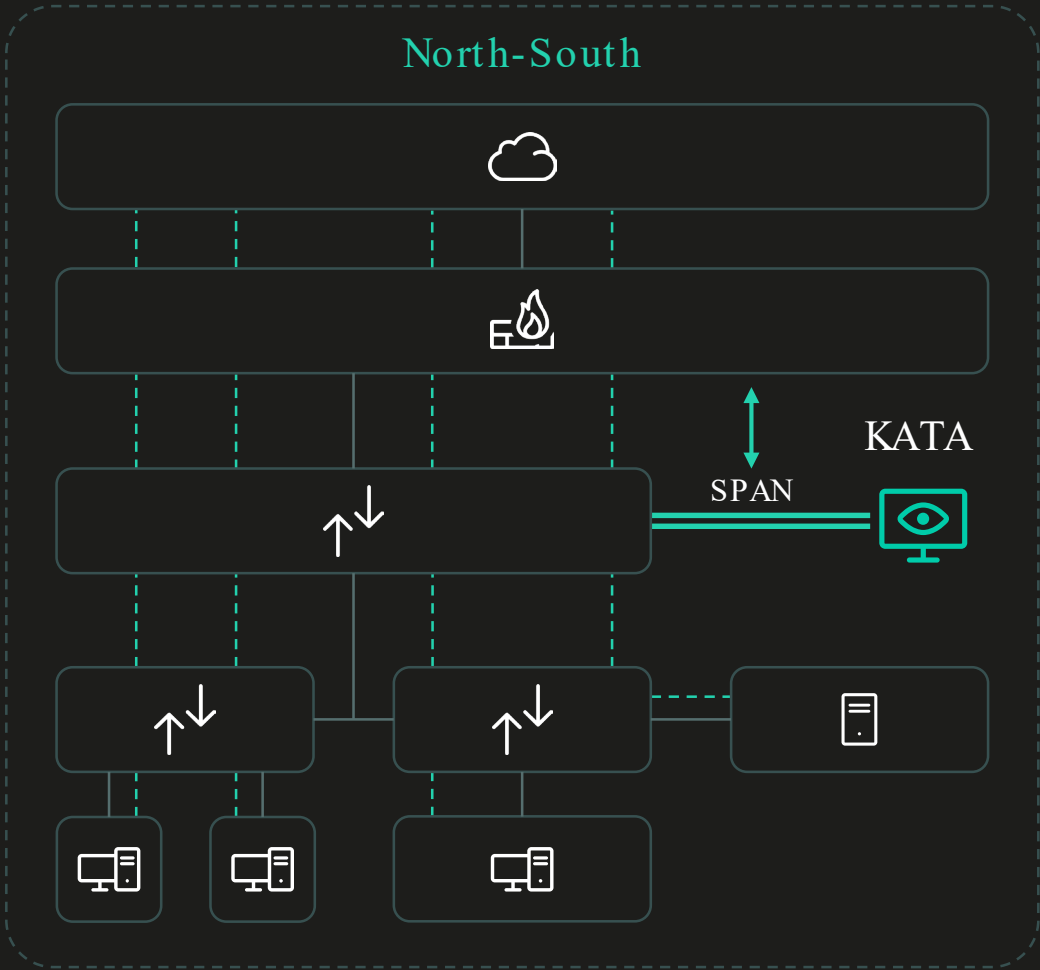
Гибкие возможности для быстрого реагирования в сети и на хостах с помощью Kaspersky NDR

Дмитрий Мокреев,

Эксперт по системам защиты от целевых атак
«Лаборатории Касперского»

kaspersky

Kaspersky NDR — это же
«та самая КАТА и всё»?



Initial Access	External Remote Services	Phishing	Valid Accounts	Exploit Public-Facing Application				
Execution	Exploitation for Client Execution	Command and Scripting Interpreter	System Services					
Persistence	Boot or Logon Autostart Execution	Browser Extensions	Hijack Execution Flow	External Remote Services	Server Software Component	Valid Accounts		
Privilege Escalation	Boot or Logon Autostart Execution	Hijack Execution Flow	Valid Accounts	Exploitation for Privilege Escalation				
Defense Evasion	Rootkit	Hijack Execution Flow	Valid Accounts	Obfuscated Files or Information				
Credential Access	Input Capture	Network Sniffing	Adversary-in-the-Middle	Brute Force	Exploitation for Credential Access	OS Credential Dumping	Steal or Forge Kerberos Tickets	
Discovery	Network Sniffing	Account Discovery	Domain Trust Discovery	Network Service Discovery	Permission Groups Discovery	Remote System Discovery	Software Discovery	System Network Configuration Discovery
Lateral Movement	Exploitation of Remote Services	Remote Service Session Hijacking	Lateral Tool Transfer	Remote Services				
Collection	Adversary-in-the-Middle	Automated Collection	Clipboard Data	Data from Local System	Input Capture	Screen Capture		
Command and Control	Encrypted Channel	Web Service	Application Layer Protocol	Ingress Tool Transfer	Non-Application Layer Protocol	Protocol Tunneling	Proxy	Remote Access Software
Exfiltration	Exfiltration Over C2 Channel							
Impact	Data Encrypted for Impact	Endpoint Denial of Service	Network Denial of Service	Resource Hijacking				

NDR TTPs

5

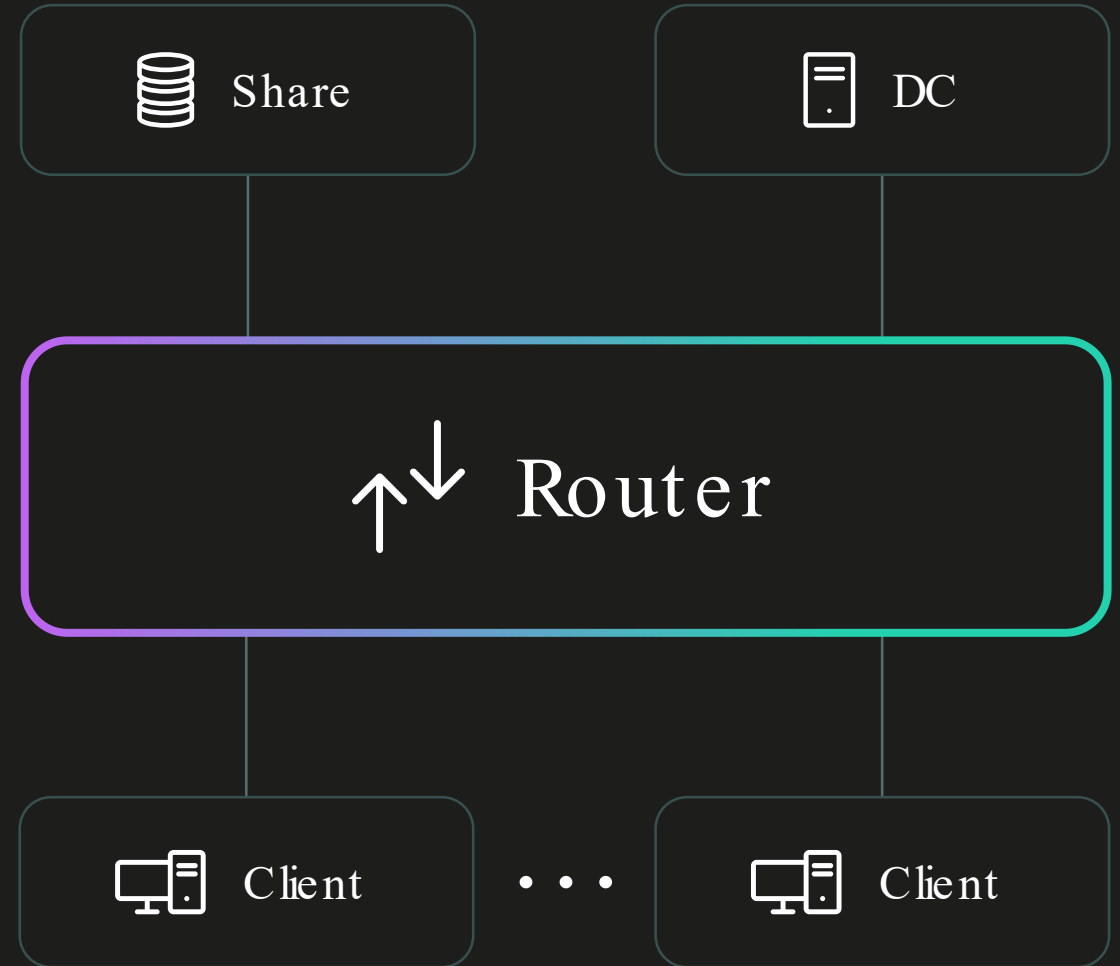
NDR TTPs

6

NDR TTPs

7

- Domain Enumeration
- Domain Privilege Escalation
- Domain Persistence
- Lateral Movement





Аномалия — нарушение
ожидаемого процесса работы
сети из-за действий
злоумышленника





Shadow IT

Видеть всю сеть.
Учитывать все устройства
Ничего не забыть и не потерять.



BYOD

Видим подключение личных устройств.
Определяем их параметры, запоминаем и смотрим,
что они делают.



Rogue Gateway

Обнаружение сторонних каналов выхода
в Интернет.



Control Device Profile

Обнаруживаем изменения в конфигурациях ассетов.
Изменение и добавление адресов подсетей, смена ОС,
появление новых сетевых сервисов и др.

Архитектура

Анализ
внутрисетевого
трафика

Выявление точных
первопричин
появления алерта

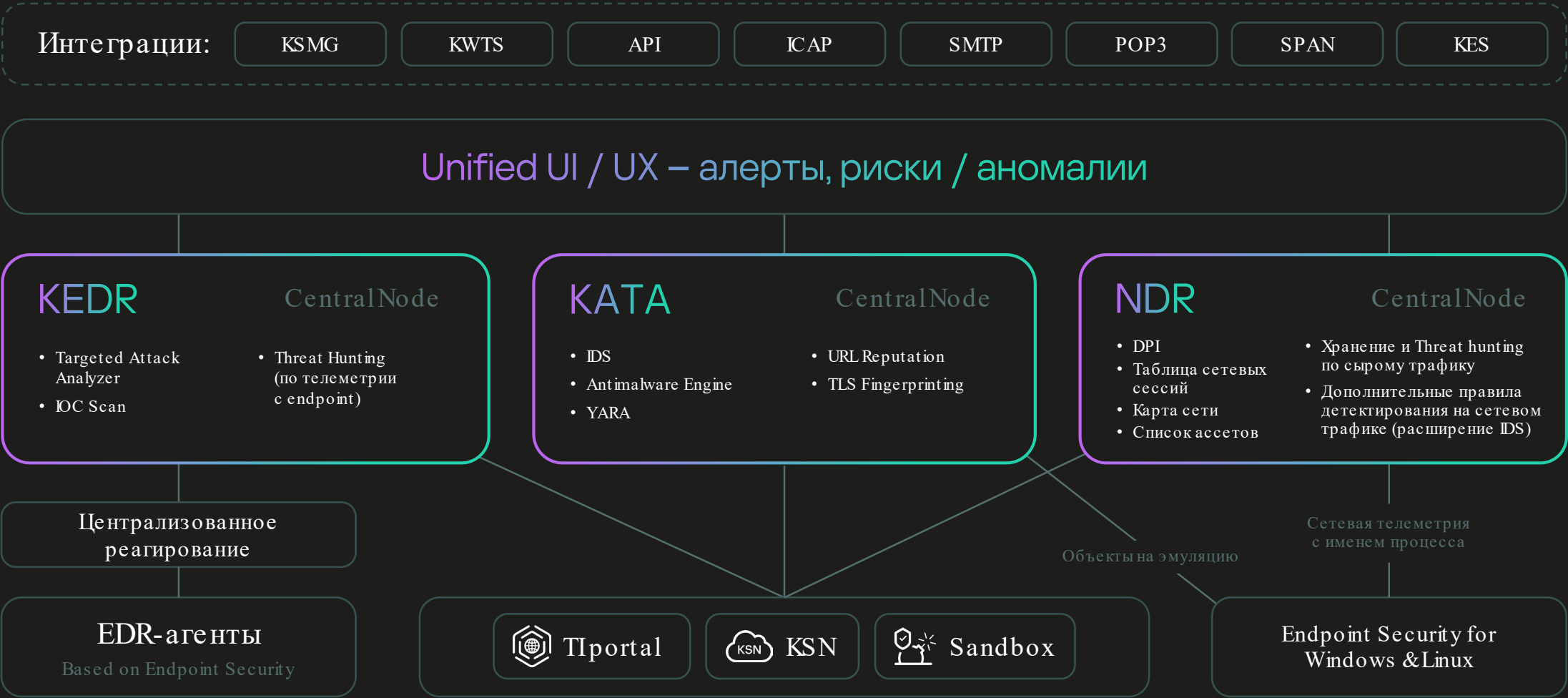
Исследование
сетевых аномалий

Какие задачи
решает
Kaspersky NDR?

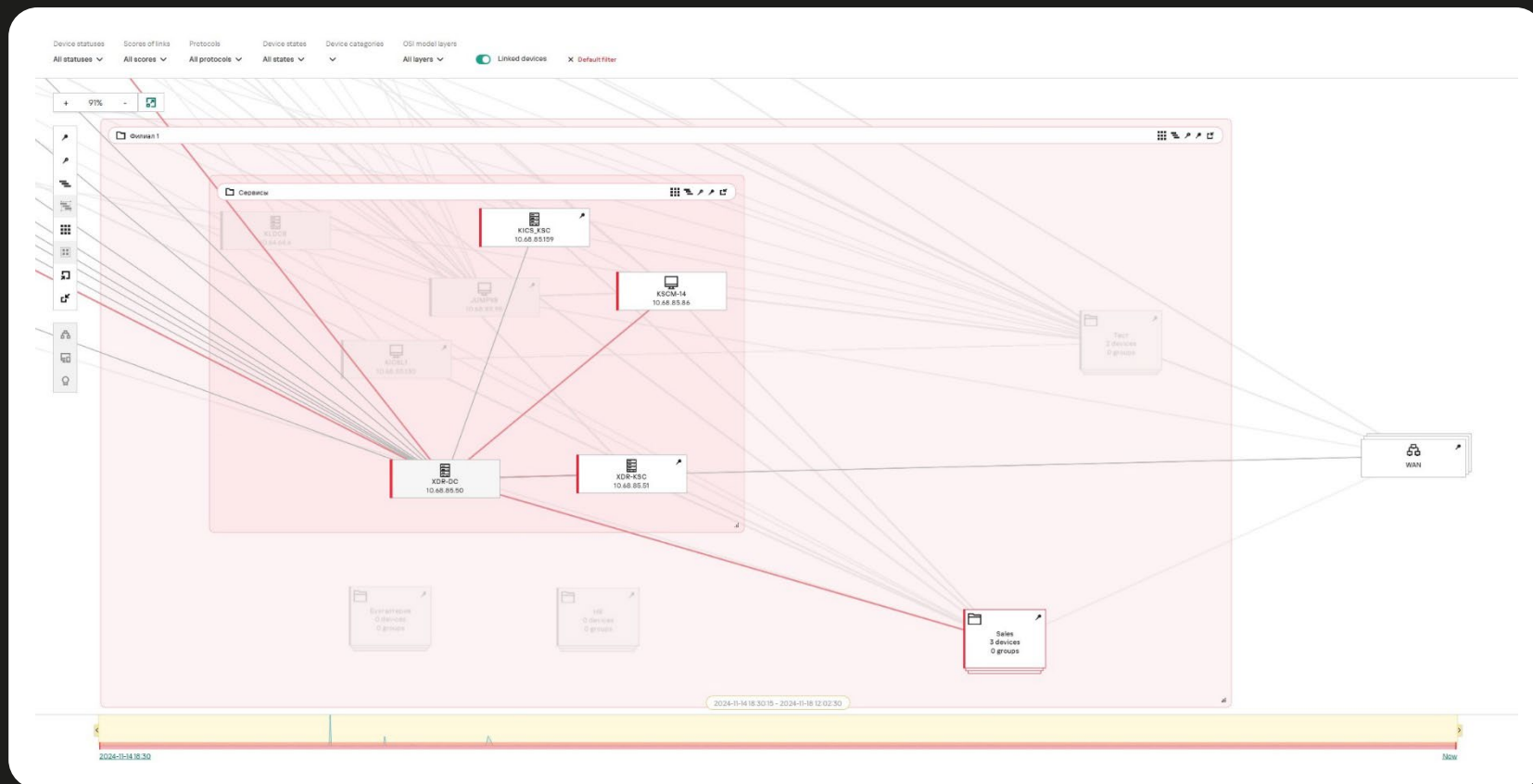
Тестирование
гипотез

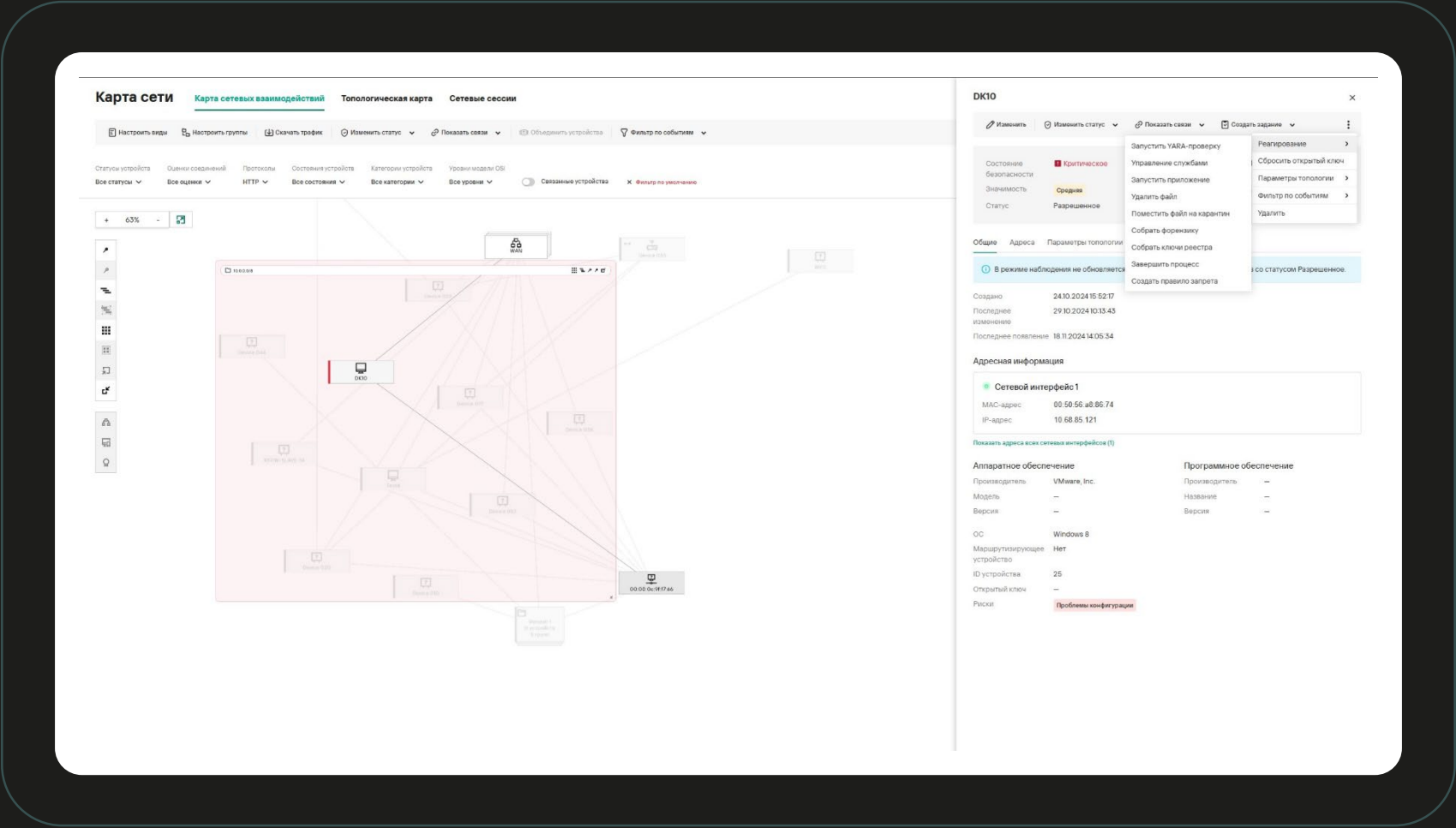
Ретроспективный
анализ ранее
записанной копии
трафика

Повышение
видимости во всех
сегментах сети



Инструменты





Карта сети

Карта сетевых взаимодействий

Топологическая карта

Сетевые сессии

Показать связи

Скачать трафик

Экспорт в CSV-файл

Поиск по пакетам

Обновление

Статус	Сторона 1	Порт сторон...	Сторона 2	Порт стороны 2	Устройство 1	Устройство 2	Протокол переда...	Прото...
☐ Активна	10.68.85.145	5140	10.68.85.50	64433	kuma34	DEMO	TCP	HTTP
☐ Активна	10.68.85.26	5550	10.68.85.50	64434	Устройство 028	DEMO	TCP	HTTP
☐ Активна	10.68.85.45	5550	10.68.85.50	64435	Устройство 013	DEMO	TCP	HTTP
☐ Активна	10.68.85.4	3260	10.68.85.202	21964	Устройство 021	Устройство 024	TCP	TCP
☐ Активна	10.68.85.253	1985	224.0.0.102	1985	Устройство 004		UDP	UDP
☐ Активна	10.68.85.254	1985	224.0.0.102	1985	Устройство 009		UDP	UDP
☐ Активна	10.68.85.65	52038	10.68.85.180	443	dFi20	SuperSCADA	TCP	TLS v1.
☐ Активна	10.68.85.201	60333	10.68.85.4	3260	Устройство 020	Устройство 021	TCP	TCP
☐ Активна					a6f716402f02	PC-4	Ethernet II	ARP
☐ Активна	10.68.85.33	52658	10.68.85.200	443	KSCW-SLAVE-14	saleslab.kaspers...	TCP	HTTPS
☐ Активна	10.68.85.50	53548	10.68.85.13	443	DEMO	a6f716402f02	TCP	TLS v1.2
☐ Активна					Устройство 025		Ethernet II	ARP

Поиск по пакетам

Если поиск будет длиться больше 5 секунд он попадет в категорию длинных операций

Период

06.12.2024 09:31:28 - 06.12.2024 10:31:28

Фильтрация с использованием BPF

Включить фильтрацию

Выражение для фильтрации (пример: tcp port 102 or tcp port 502)

Не задано

Фильтрация с использованием регулярных выражений

Включить фильтрацию

Выражение для фильтрации (пример: *test.*\xAB\xCD)

Не задано

Фильтрация по точкам мониторинга

Включить фильтрацию

Точки мониторинга

Точки мониторинга не выбраны

Фильтрация по адресным пространствам

Включить фильтрацию

Трафик в адресных пространствах

Выберите адресные пространства

Поиск

Отмена

Новый режим работы KES – NDR. Дополнительный источник знаний о сети

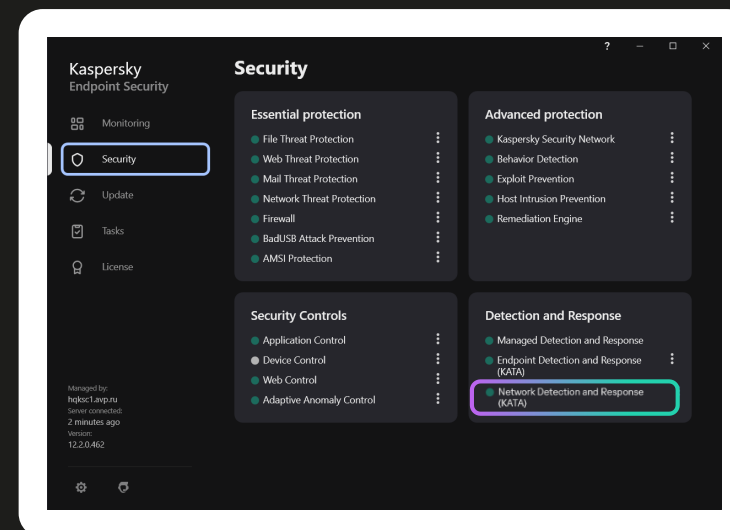
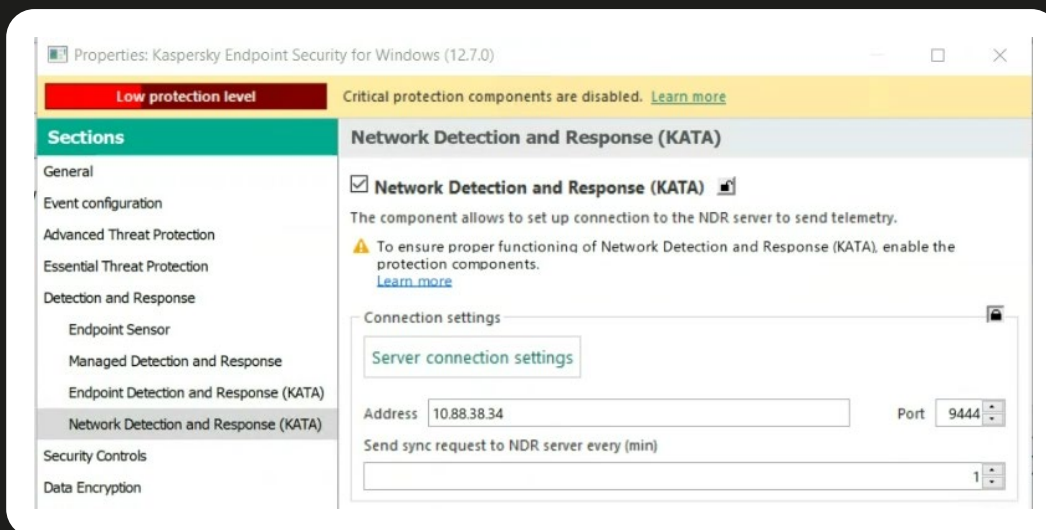
18

KATA NDR

KES Windows & Linux
(Sensor)

(Q4 '24)

- Сетевая видимость
- Наполнение базы Ассетов
- Таблица сессий
- Карта сети
- Имя пользователя
- Процесс / путь + сессия



☐	Ст...	Пр...	Пр...	Тек...	Ср...	Все...	На...	П...	Кол...	Ст...
☐	Активна	TCP	SSH	0 бит/с	3 кбит/с	11 КБ	27.07...	27.07...	105	10.65.5...
☐	Активна	TCP	SSH	0 бит/с	936 би...	3.3 КБ	27.07...	27.07...	13	10.65.5...
☐	Завершена	TCP	HTTPS	0 бит/с	391 кб...	10 МБ	27.07...	27.07...	12072	10.16.4...
☒	Завершена	TCP	SSH	0 бит/с	6.3 кби...	130 КБ	27.07...	27.07...	926	10.65.5...
☐	Завершена	TCP	TCP	0 бит/с	72 кби...	8.9 КБ	27.07...	27.07...	18	10.65.5...
☐	Завершена	TCP	TCP	0 бит/с	72 кби...	8.9 КБ	27.07...	27.07...	18	10.65.5...
☐	Завершена	TCP	TCP	0 бит/с	72 кби...	8.9 КБ	27.07...	27.07...	18	10.65.5...
☐	Завершена	TCP	TCP	0 бит/с	1.3 кби...	30 КБ	27.07...	27.07...	48	10.65.5...
☐	Завершена	TCP	TCP	0 бит/с	35 кби...	4.3 КБ	27.07...	27.07...	15	10.65.5...
☐	Завершена	TCP	TCP	0 бит/с	72 кби...	8.9 КБ	27.07...	27.07...	18	10.65.5...
☐	Завершена	TCP	TCP	0 бит/с	72 кби...	8.9 КБ	27.07...	27.07...	18	10.65.5...
☐	Завершена	TCP	TCP	0 бит/с	72 кби...	8.9 КБ	27.07...	27.07...	18	10.65.5...
☐	Завершена	TCP	TCP	0 бит/с	72 кби...	8.9 КБ	27.07...	27.07...	18	10.65.5...
☐	Завершена	TCP	TCP	0 бит/с	72 кби...	8.9 КБ	27.07...	27.07...	18	10.65.5...

Протокол приложений SSH

Текущая скорость 0 бит/с

Средняя скорость 802 бит/с

Начало 27.07.2023 13:14:28

Последнее взаимодействие 27.07.2023 13:17:14

Всего передано 130 КБ

Сторона 1

Устройство

ft2-server-kea

Адрес

10.65.50.200

Порт

59588

Приложение

ssh.exe (OpenSSH_7.7p1 for Windows)

↓

Сторона 2

Устройство

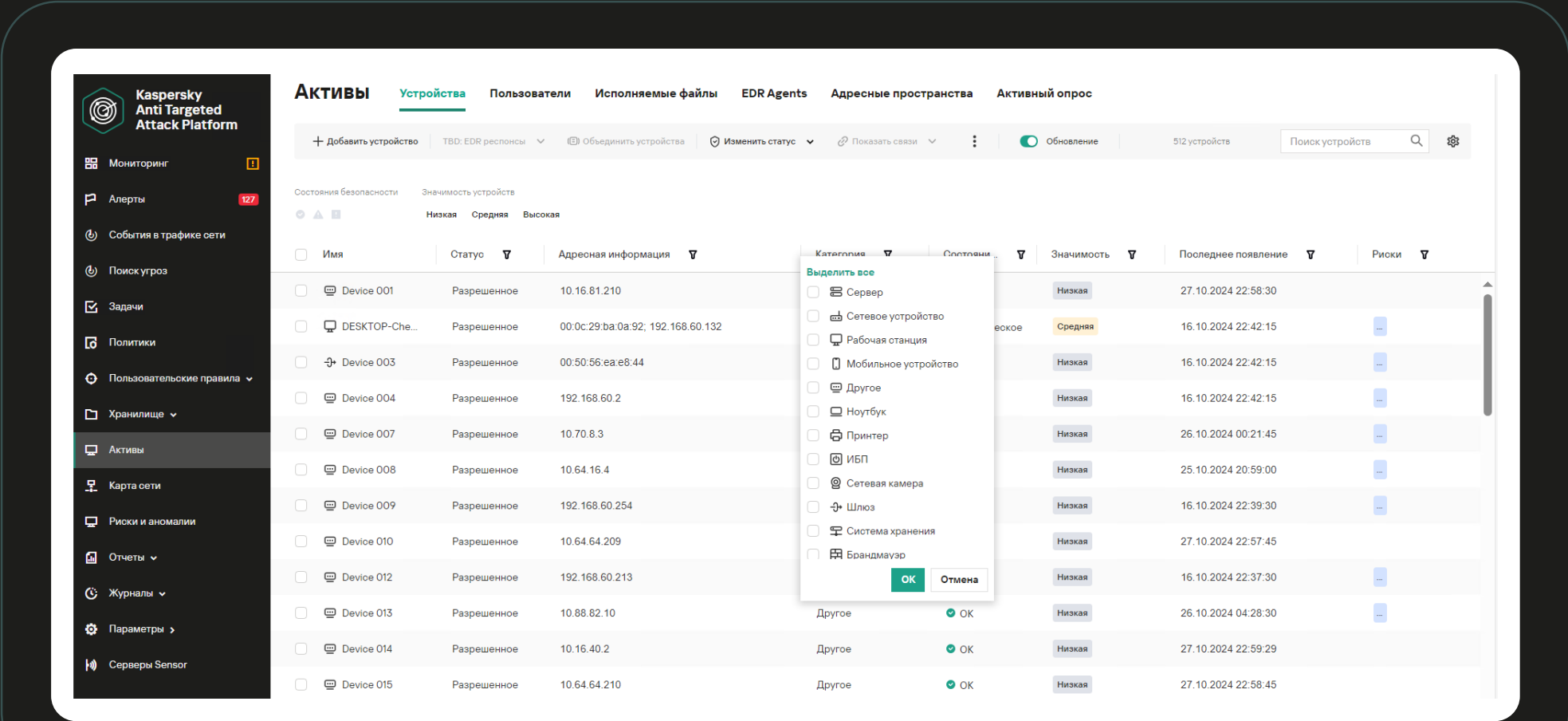
Устройство 003

Адрес

10.65.51.225

Порт

22



Риски и аномалии

Изменить статус

Показать связи

Экспорт

Источники уязвимостей

Период обнаружения

Последние 30 дней

Категории

Уязвимость

Конфигурация

Архитектура

Оценки

0 — 10

Статусы

Актуальный

Принят

Устранен

Фильтр

Категория	Оценка	Устройство
☐ Проблемы конфигурации	10	* (1)
☐ Проблемы конфигурации	10	DK10.sales.lab
☐ Проблемы конфигурации	10	KESS
☐ Проблемы конфигурации	10	KSCDK
☐ Проблемы конфигурации	10	PC-2
☐ Проблемы конфигурации	10	PC-4
☐ Проблемы конфигурации	10	PC-5
☒ Проблемы конфигурации	10	WORKSTATION
☐ Небезопасная архитектура сети	5	
☐ Небезопасная архитектура сети	5	

10 Устаревшая ОС на устройстве

Изменить

Изменить статус

Показать связи

Экспорт

Категория	Проблемы конфигурации	ID риска	13
Статус	Актуальный	Тип риска	5000005034
Устройство	WORKSTATION		

Описание

На устройстве установлена устаревшая о

Возможные последствия

- Устаревшая ОС содержит уязвимос
- исправлений от производителя ОС
- Открыты возможности для наруше

Меры по устранению угроз

- Обновить операционную систему.

Общие сведения

Последнее изменение статуса

04.12.2024 12:34:10

Обнаружен

04.12.2024 12:34:10

Базовая оценка

9.8

Группа устройств

—

Типы рисков

30 типов рисков

Поиск типов рисков

Базовые оценки

0 — 10

Категории

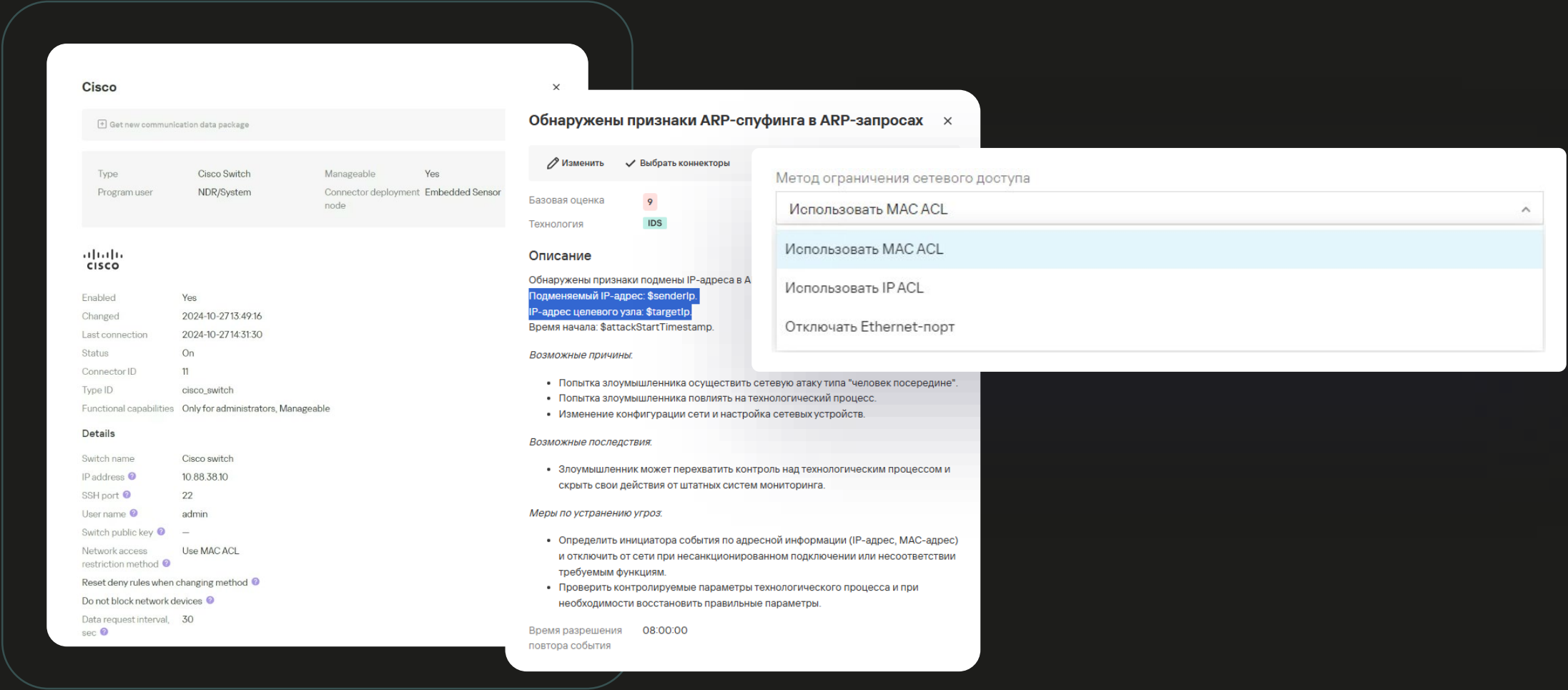
Уязвимость

Конфигурация

Архитектура

Фильтр по умолчанию

Название	Категория	Базовая оценка
Недостаточная защита учетных данных	Проблемы конфигурации	6
Взаимодействия с внешними сетями	Небезопасная архитектура сети	6.5
Подключение по протоколу SMB доступно из нулевого сванса	Проблемы конфигурации	6.5
FTP-сервер доступен из внешних сетей	Небезопасная архитектура сети	6.5
Нет защиты с помощью EPP-приложения на устройстве	Проблемы конфигурации	8.1
Использование VNC для удаленного доступа	Небезопасная архитектура сети	8.8
Использование TeamViewer для удаленного доступа	Небезопасная архитектура сети	8.8
Использование RDP для удаленного доступа	Небезопасная архитектура сети	8.8
Использование Radmin для удаленного доступа	Небезопасная архитектура сети	8.8
Использование AnyDesk для удаленного доступа	Небезопасная архитектура сети	8.8
Использование Remote Utilities для удаленного доступа	Небезопасная архитектура сети	8.8
Использование AnyMy Admin для удаленного доступа	Небезопасная архитектура сети	8.8
Использование AeroAdmin для удаленного доступа	Небезопасная архитектура сети	8.8
Использование служб удаленного доступа	Небезопасная архитектура сети	8.8
Устаревшая ОС на устройстве	Проблемы конфигурации	9.8



Спасибо!