

Алексей Жуков

Руководитель Департамента
сервисов и продуктов RT Protect

Как SOC-у увидеть всю инфраструктуру





Обо мне



- ✦ Руководитель экосистемы **RT Protect**
- ✦ Руководитель SOC для ГК Ростех
- ✦ Более **10 лет в ИБ**
- ✦ EX-pentester, C developer, threat analyst
- ✦ Более **7 лет** опыта развития продуктов EDR, XDR, NTA, SIEM, IPS, IRP

 @AK_Zhukov

Алексей Жуков

Руководитель Департамента
сервисов и продуктов RT Protect



Современные тенденции



✖ Существенное удешевление и ускорение разработки ВПО с помощью ИИ

✖ Всё более сложные социотехнические атаки, генерируемые при помощи ИИ, что кратно повышает требования к бдительности работников

- ✖ Эксплуатация уязвимостей:
- Microsoft Exchange (CVE-2024-49040 Server Spoofing)
 - Microsoft Outlook (CVE-2025-21298 Zero Click)
 - Microsoft Excel RCE : (CVE-2025-21381)
 - CVE-2022-41040+CVE-2022-41082 (MS Exchange RCE ProxyNotShell)
 - CVE-2024-49126(LSASS RCE)
 - CVE-2024-49112(LDAP RCE)

✖ Как следствие, повышение требований к объёму покрытия мониторингом ИТ-инфраструктур и качеству алертинга

Портрет злоумышленников



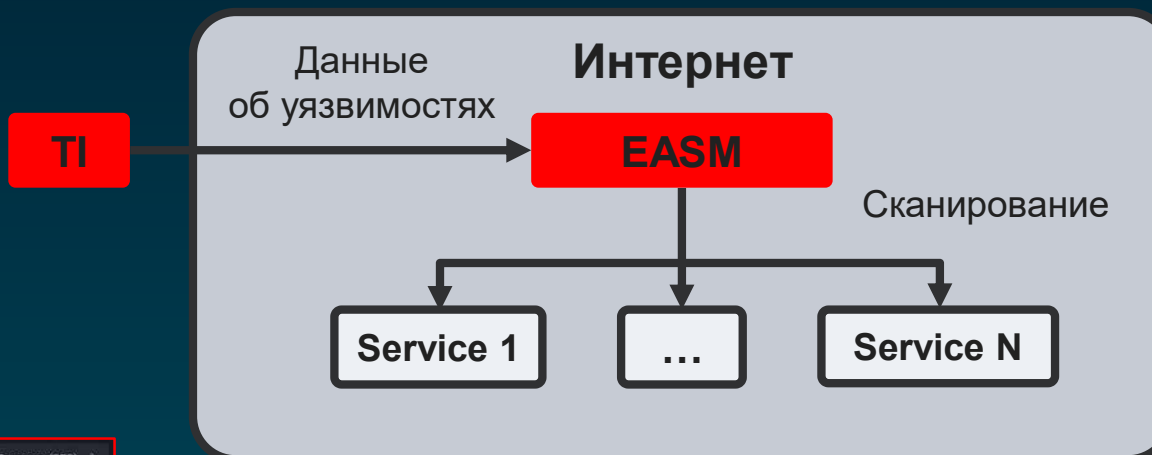
Как от них защититься



Как контролировать внешнюю инфраструктуру



- Решение класса EASM
- Регулярное сканирование внешних сервисов
- Контроль изменений внешней инфраструктуры



Трассировочные пути

Сканирования

Задача: ROS

Дата первого сканирования: 19.12.2023, 21:15:12

Дата второго сканирования: 20.12.2023, 21:15:14

Ввод идентификаторов сканирования

Применить

Активное сканирование (14) Поиск утечек (67) Пассивное сканирование (70) Сканирование веб-адресов (26) Брутфорс веб-адресов (0) Сертификаты (0)

Тип события	Сетевой адрес	Порт	Протокол	Сервис	Версия	SSL	Описание
Новая запись	81.1	80	http	Microsoft HTTPAPI HTTPd	2.0	Выкл	SSDP/UPnP
Новая запись	81.1	443	https	Microsoft HTTPAPI HTTPd	2.0	Вкл	SSDP/UPnP
Новая запись	188.128	80	http	nginx	нет данных	Выкл	нет данных
Новая запись	188.128	443	https	nginx	нет данных	Вкл	нет данных
Новая запись	185.22	80	http	nginx	нет данных	Выкл	нет данных
Новая запись	78.155	80	http	nginx	нет данных	Выкл	нет данных

Легенда (258)

Исключить

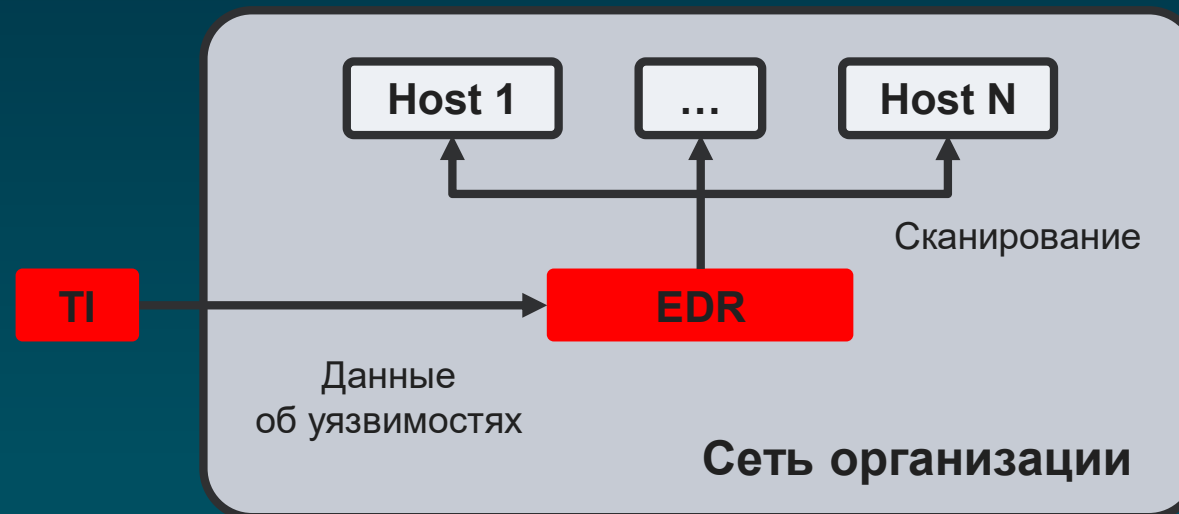
- 10.1
- 10.1
- 10.10
- 105.201
- 192.108
- 195.83
- 85.112
- 87.220
- 180.254
- 83.188
- 87.198
- 212.33
- 170.49
- 195.216
- 79.104

Как контролировать внутреннюю инфраструктуру



- Решение класса EDR
- Агентская инфраструктура
- Сбор данных об установленных программах
- Регулярное сканирование

Установленное ПО ☒ Только уязвимые	 6	Имя: Google Chrome Издатель: Google LLC Версия: 120.0.6099.225	 3
		Имя: Intel(R) Chipset Device Software Издатель: Intel Corporation Версия: 10.1.18836.8283	 1
		Имя: Intel(R) Chipset Device Software Издатель: Intel(R) Corporation Версия: 10.1.18836.8283	 1
		Показать все (6)	



Как получить сводную статистику?

- Решение класса IRP
- Получение данных от EDR, EASM, NTA
- Сводная информация о состоянии инфраструктуры через AI помощника



Как бороться с Shadow IT?



Модули сканирования активов LASM



Решения NTA для обнаружения аномалий и определения ИТ-активов по команде от различных систем

Модули уязвимостей и контроль утечек (VM, EASM)



ИИ-анализаторы и настроенные правила определения различных устройств

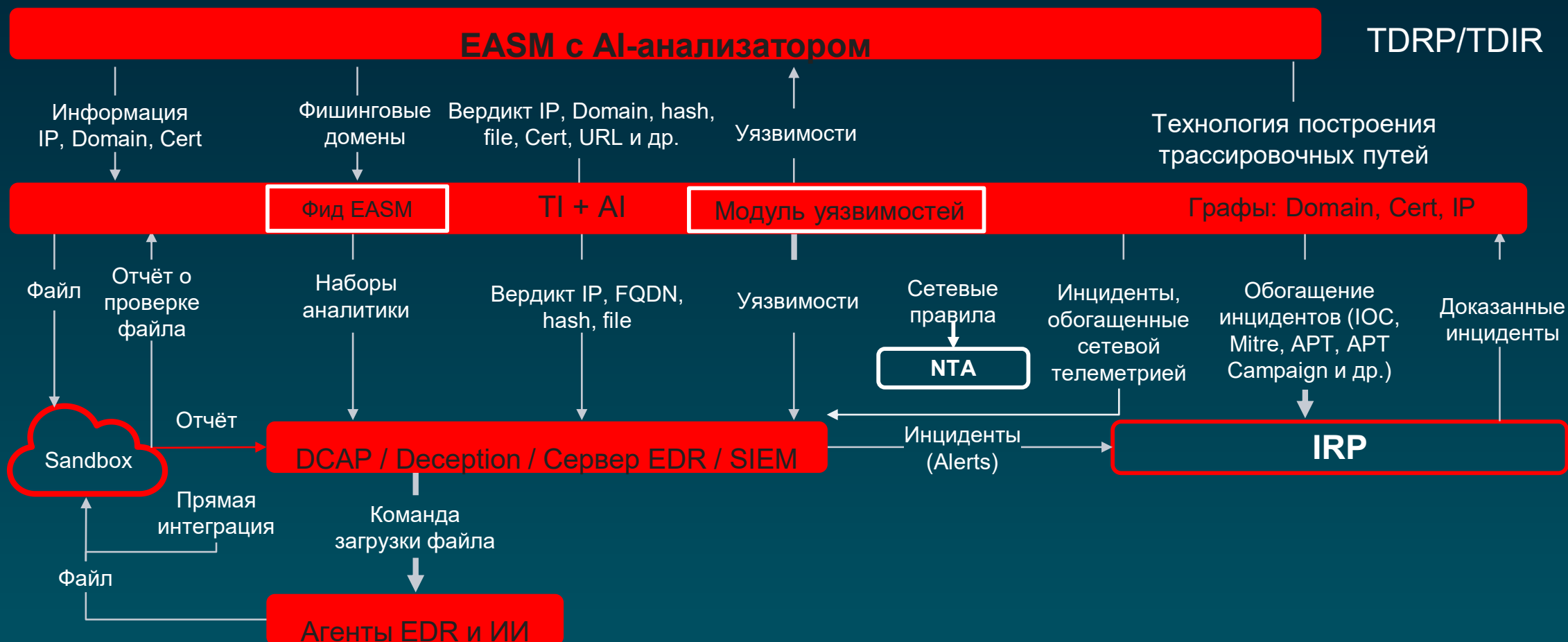
ВЫВОДЫ



- Увидеть всю инфраструктуру почти **невозможно одним решением** или утилитой
- Покрыть все конечные точки необходимыми СЗИ **редко** кому удастся
- Поэтому требуется **комплекс средств**, который при этом помогает специалисту



Нужна взаимосвязанная система продуктов



Telegram канал



@RTINFOBEZ

Контакты



Нам доверяют



Адрес: 117587, г.
Москва, Варшавское
шоссе, дом 118, корпус 1
Tel.: +7 (499) 390-79-05
E-mail: info@rt-ib.ru
Сайт: rt-ib.ru

**ТЕХНОЛОГИИ
В ТВОИХ
РУКАХ**

phdX pt

Спасибо!

