Обнаружение и предотвращение атак при помощи ViPNet EndPoint Protection.

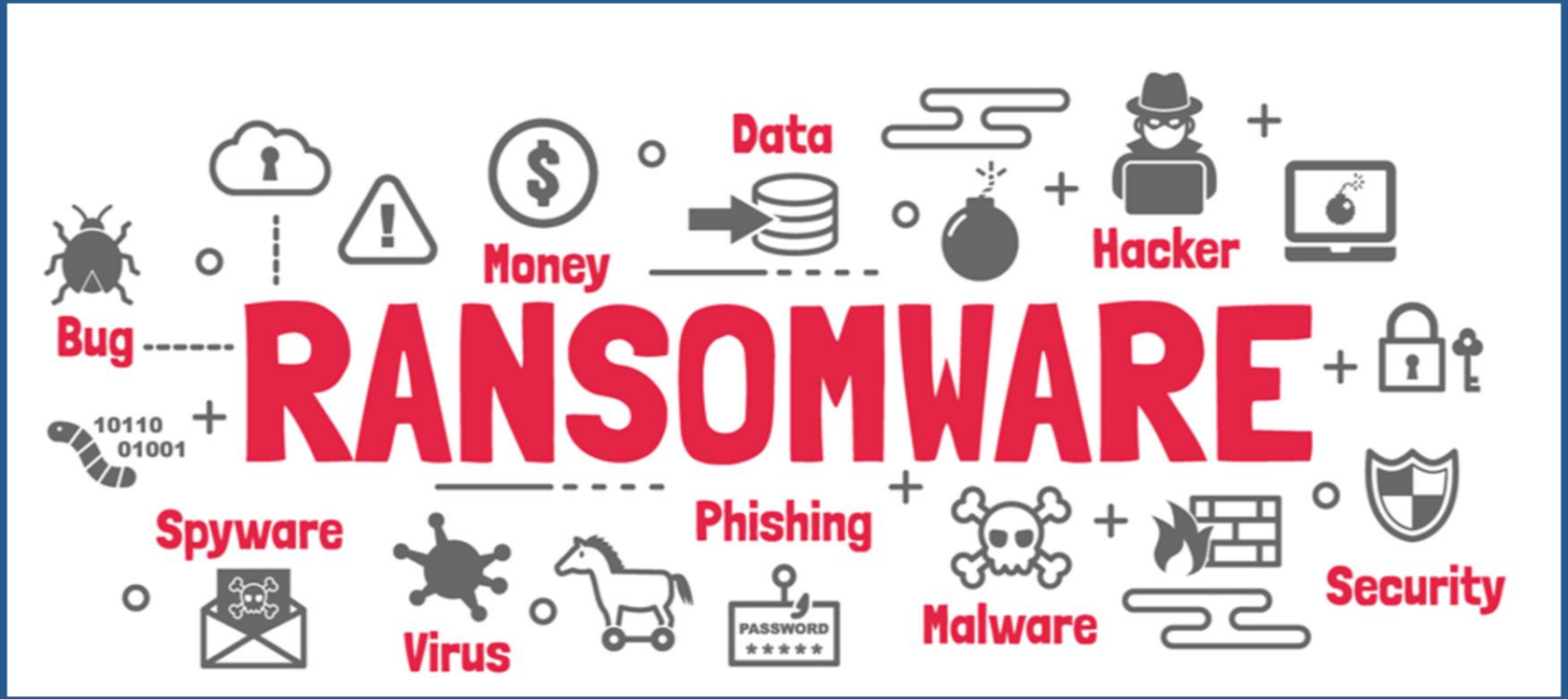
Разбор поведения злоумышленника по MITRE ATT&CK

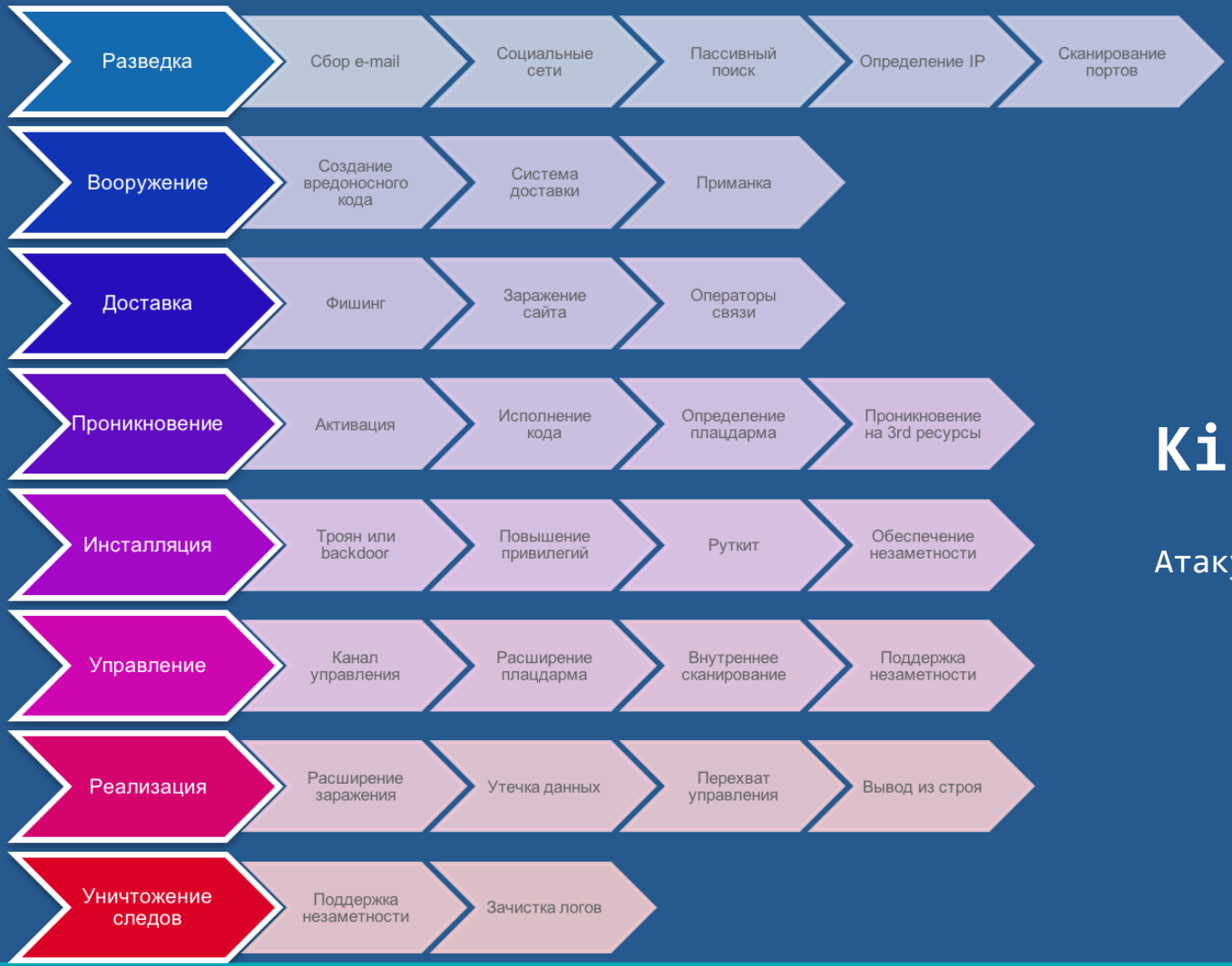
Кадыков Иван
Руководитель направления

ТЕХНО 2022 infotecs ФЕСТ

О чём пойдёт речь?

«Болезни» последних шести лет





Kill Chain

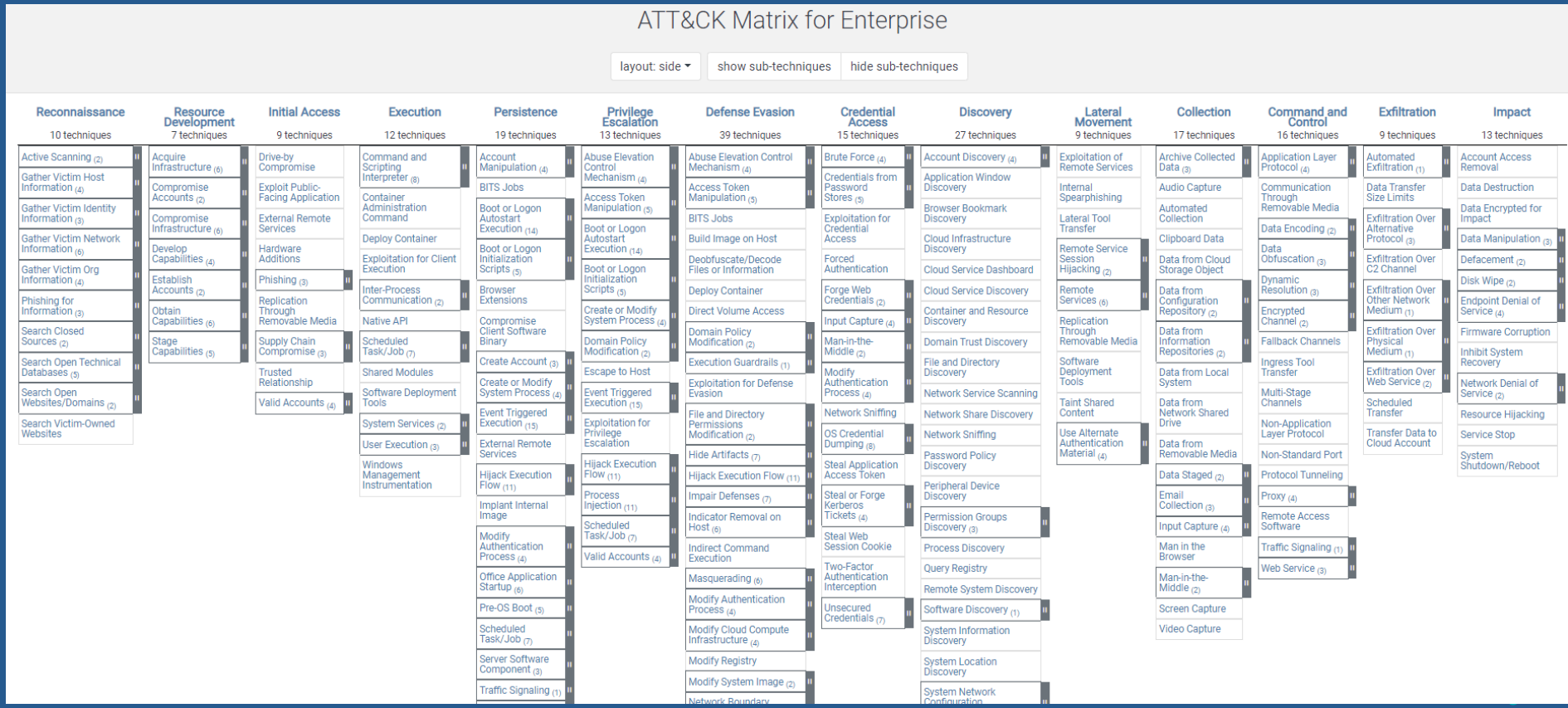
Атаку можно структурировать

Методология для специалистов ИБ

Adversary
Tactics
Techniques
&
Common
Knowledge

Техники — Тактики — Процедуры

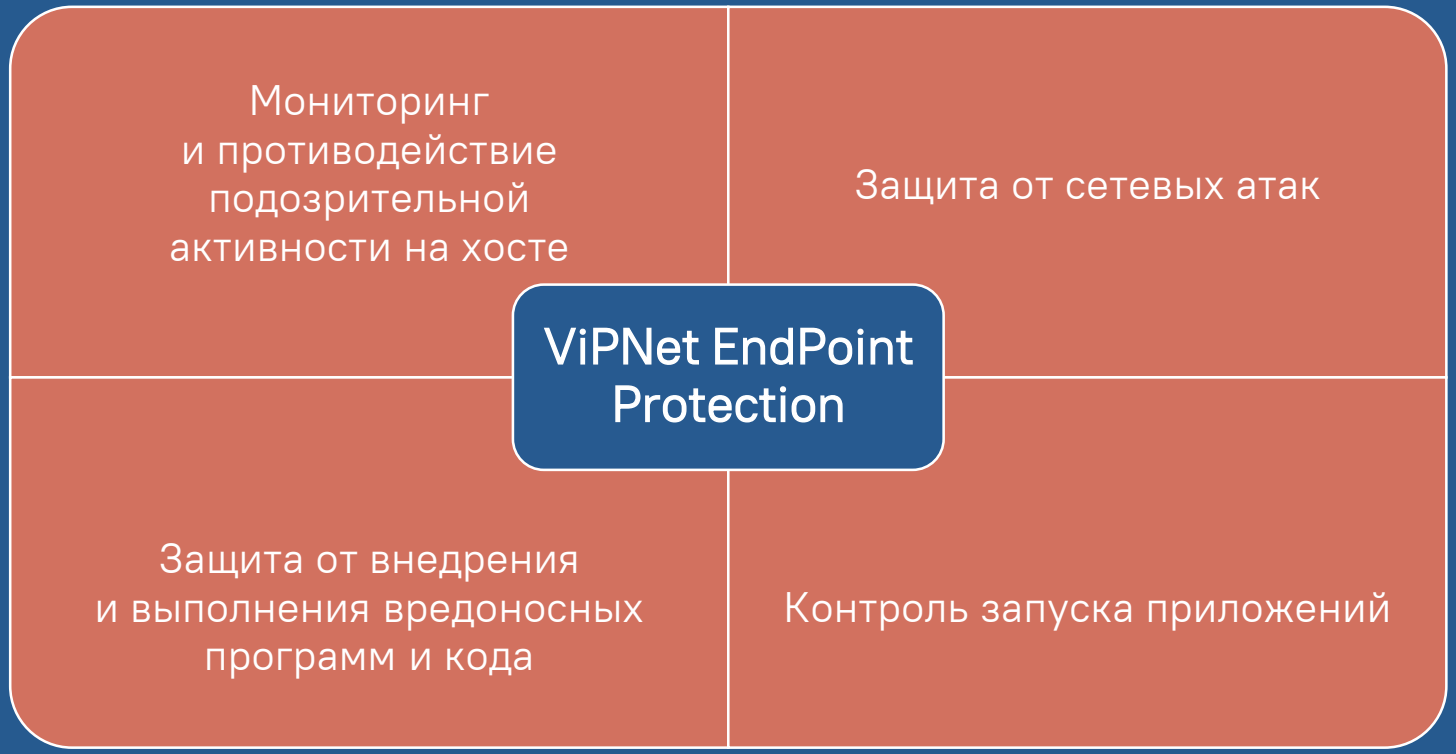
ТехноФест 2022 infotecs



«Методика оценки угроз безопасности информации». ФСТЭК России

ViPNet EndPoint Protection

Решаемые задачи



Давайте попрактикуемся

Продукт:

ViPNet EndPoint Protection

Знания:

MITRE ATT&CK

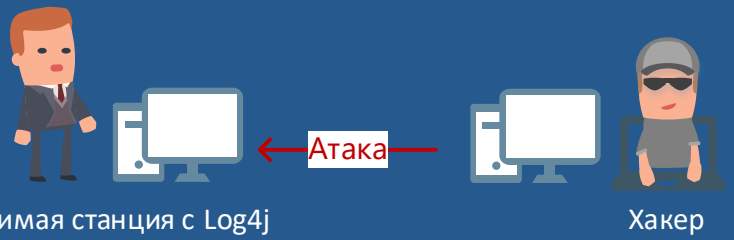
ВАЖНО!

- Мы не учим атаковать, мы показываем атаку и учим, как от нее защищаться!
- Все материалы по атакам взяты из открытых источников.
- Не стоит повторять атаки дома или на работе ☺
- А вот средства защиты использовать надо! ☺ ☺ ☺

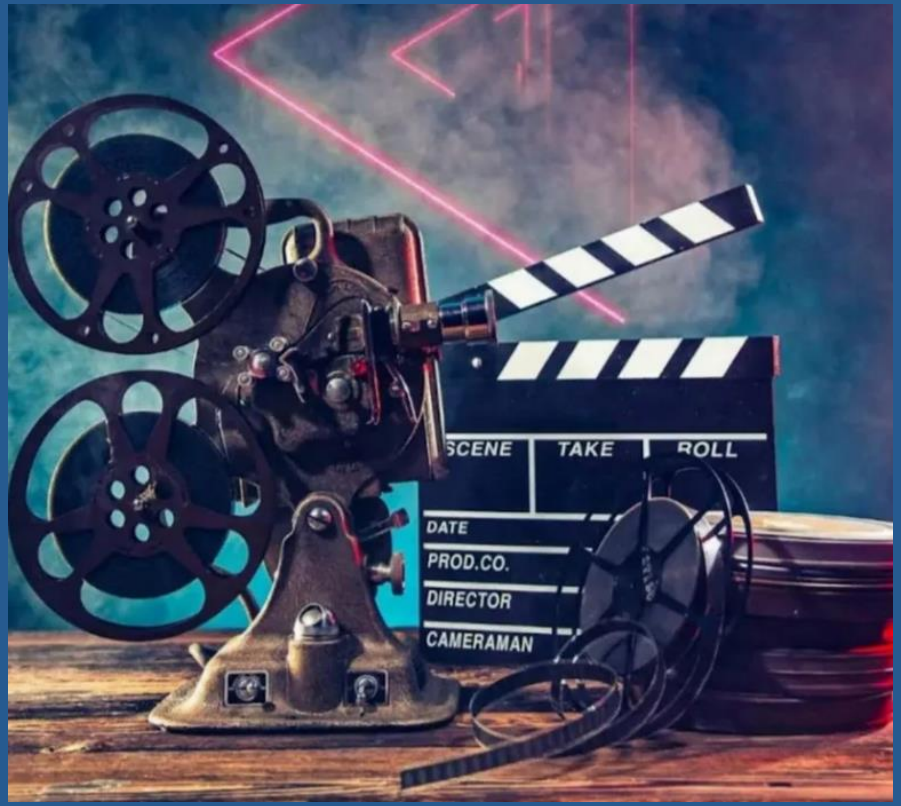
Сценарий 1.
Атака через уязвимость в Log4j. Запуск произвольного кода или приложения

Что за атака?

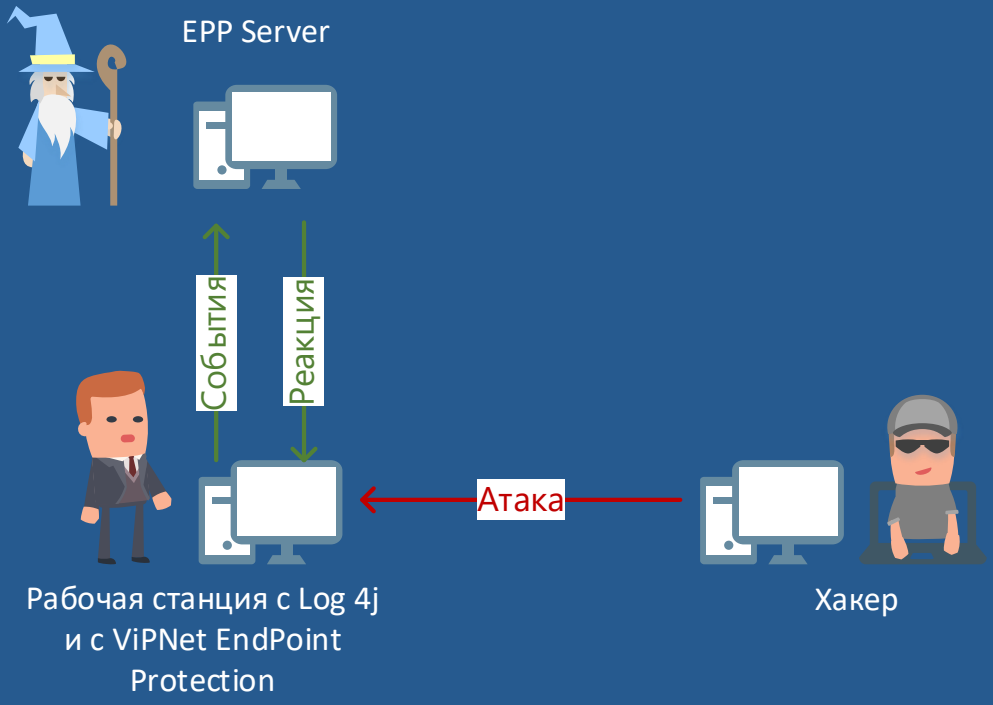
- Злоумышленник будет использовать известную уязвимость в Log4j, точнее **CVE-2021-44228.**
- Суть атаки – работающий Log4j позволяет запустить любую программу или команду на сервере, при помощи Java Naming and Directory Interface (JNDI).
- Запустим калькулятор через cmd.



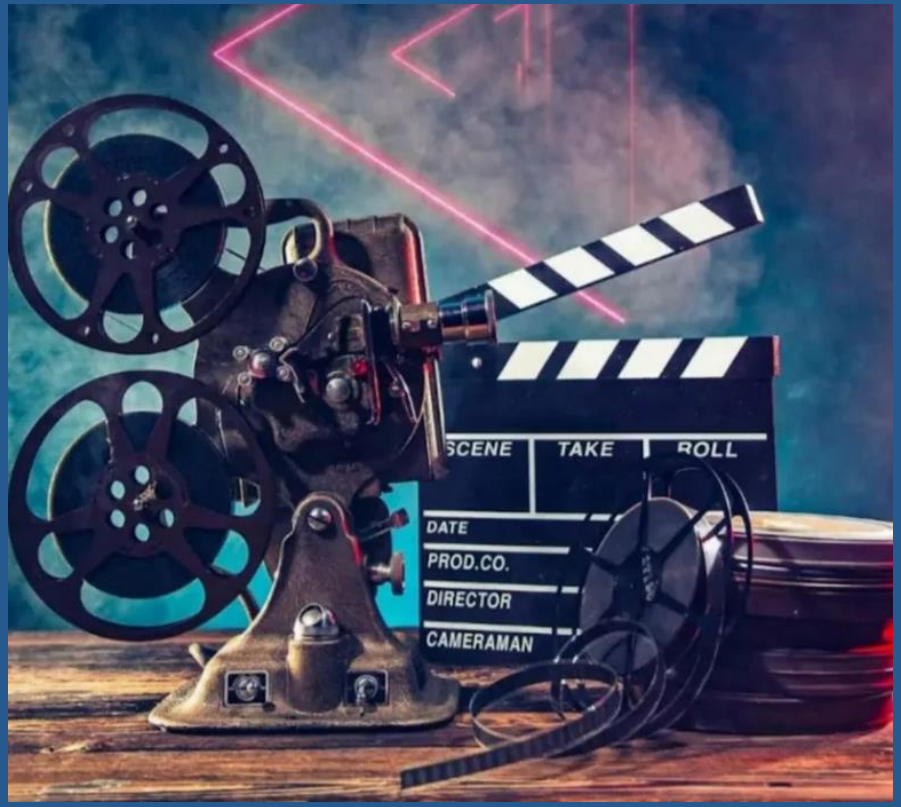
Демонстрируем атаку!



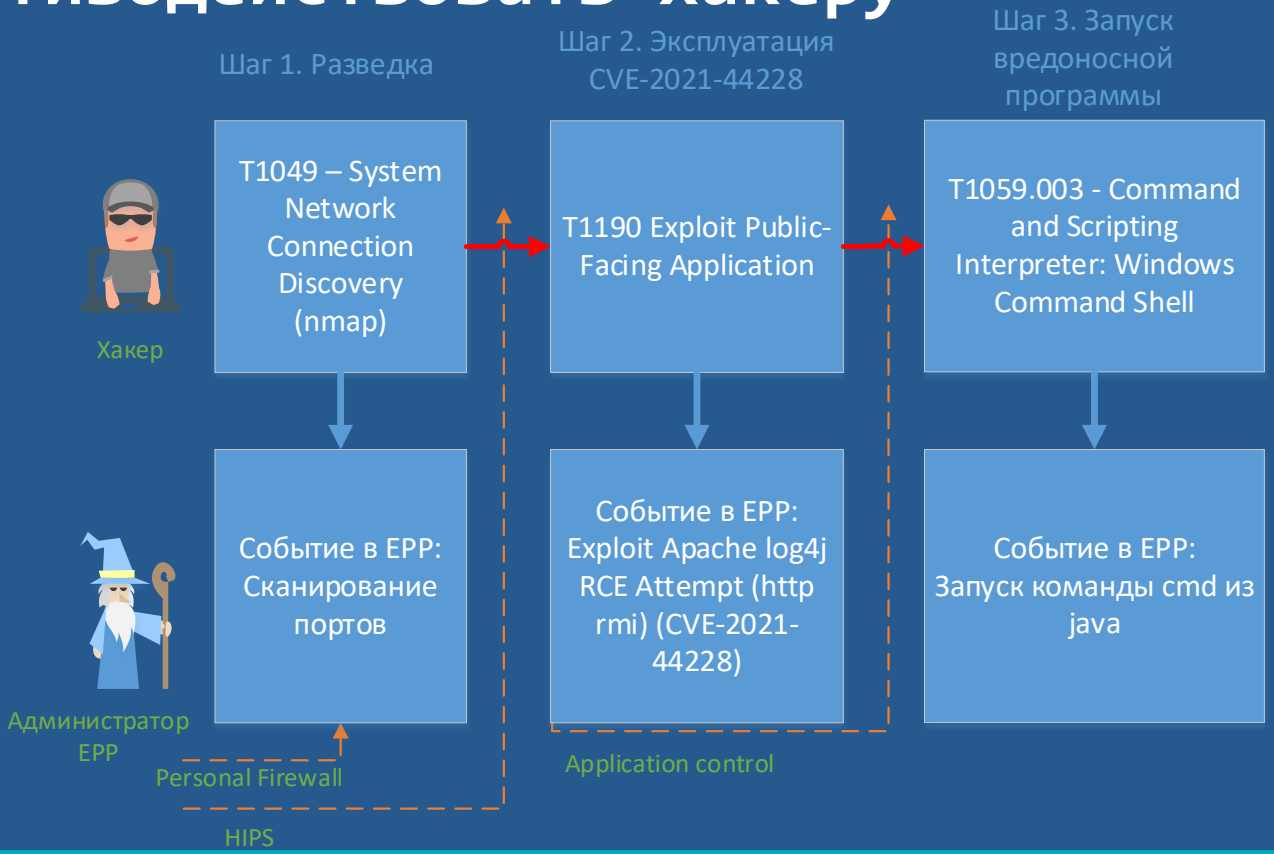
В инфраструктуре появился ViPNet EndPoint Protection



Повторно атакуем, с включенным ViPNet EndPoint Protection



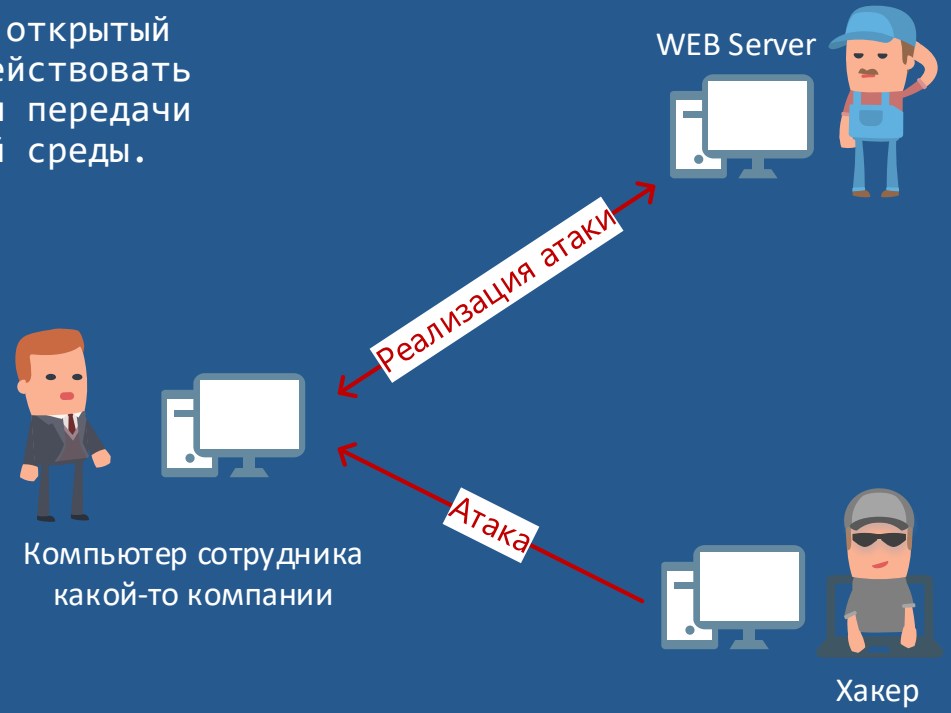
Пошаговый разбор. Как противодействовать хакеру



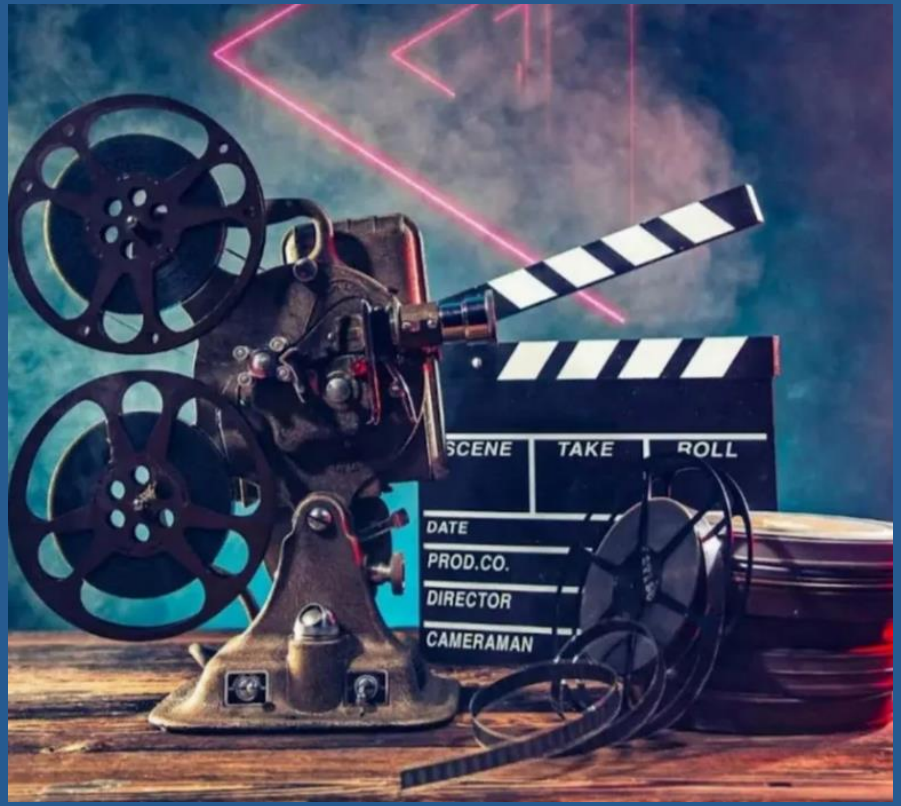
Сценарий 2. Загрузка вредоносной программы через открытый порт 22 (ssh) с использованием Resolve DNS.

Что за атака?

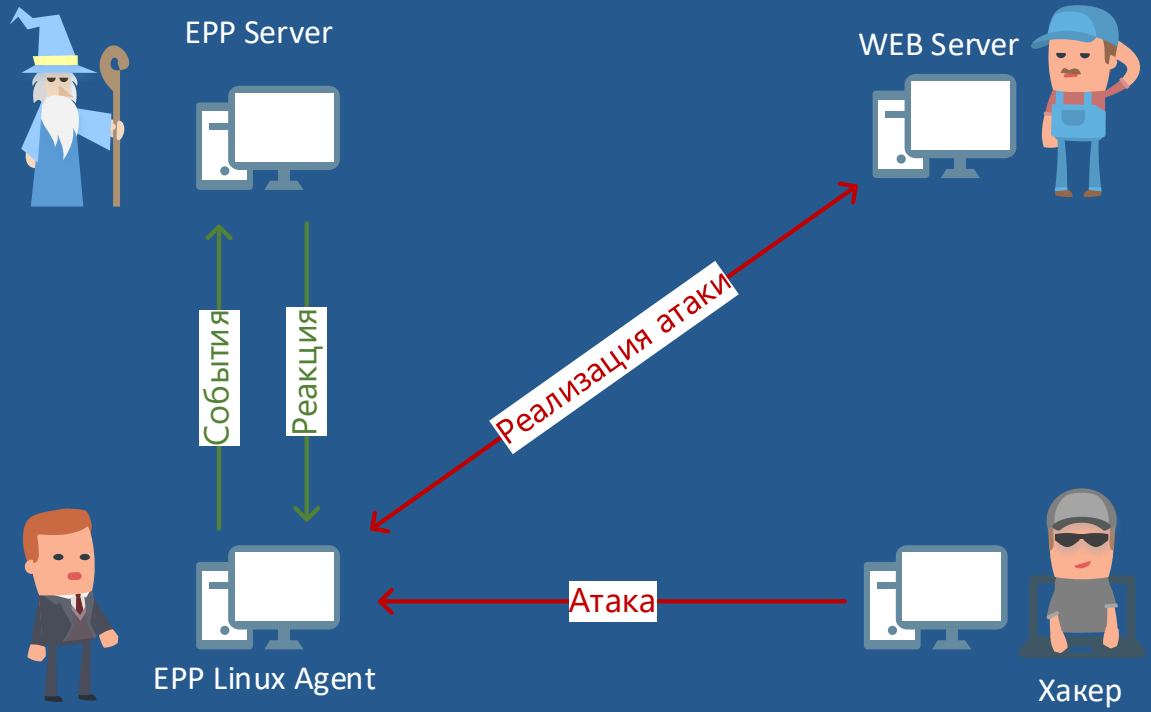
- Злоумышленник, используя открытый порт, будет пытаться задействовать легитимную веб-службу для передачи данных в/из корпоративной среды.



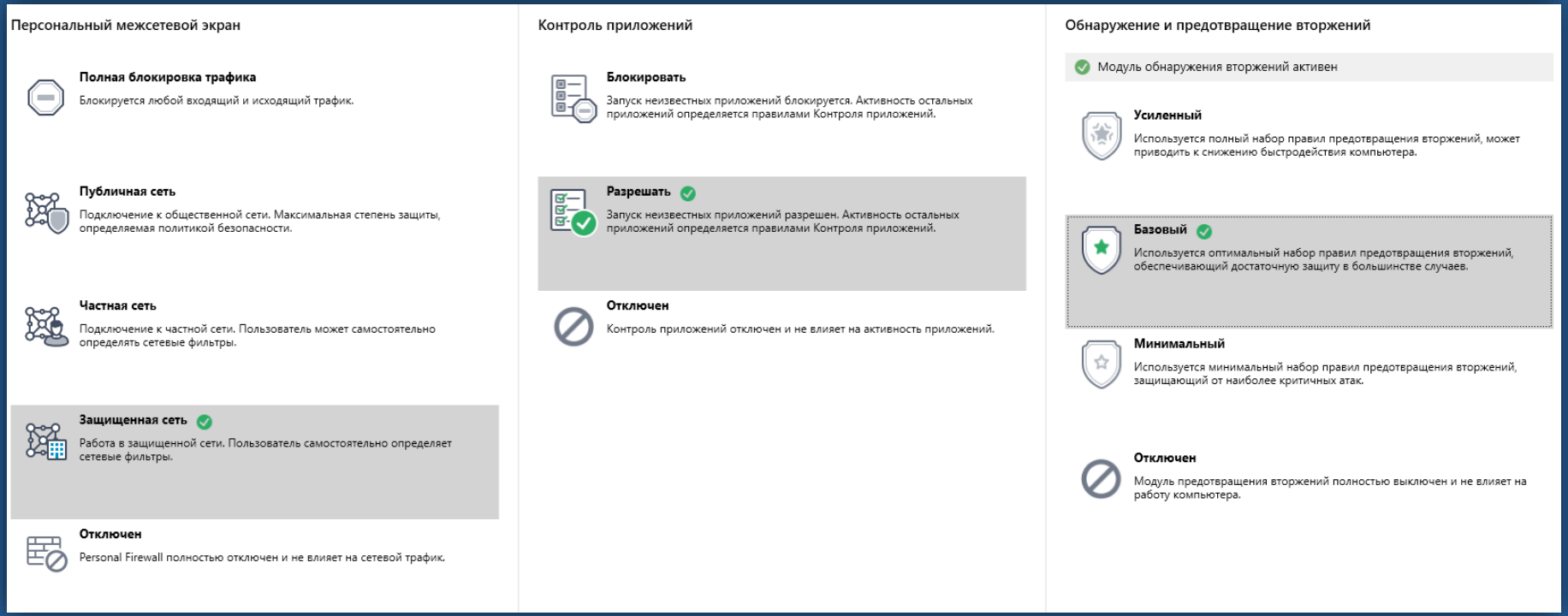
Демонстрируем атаку!



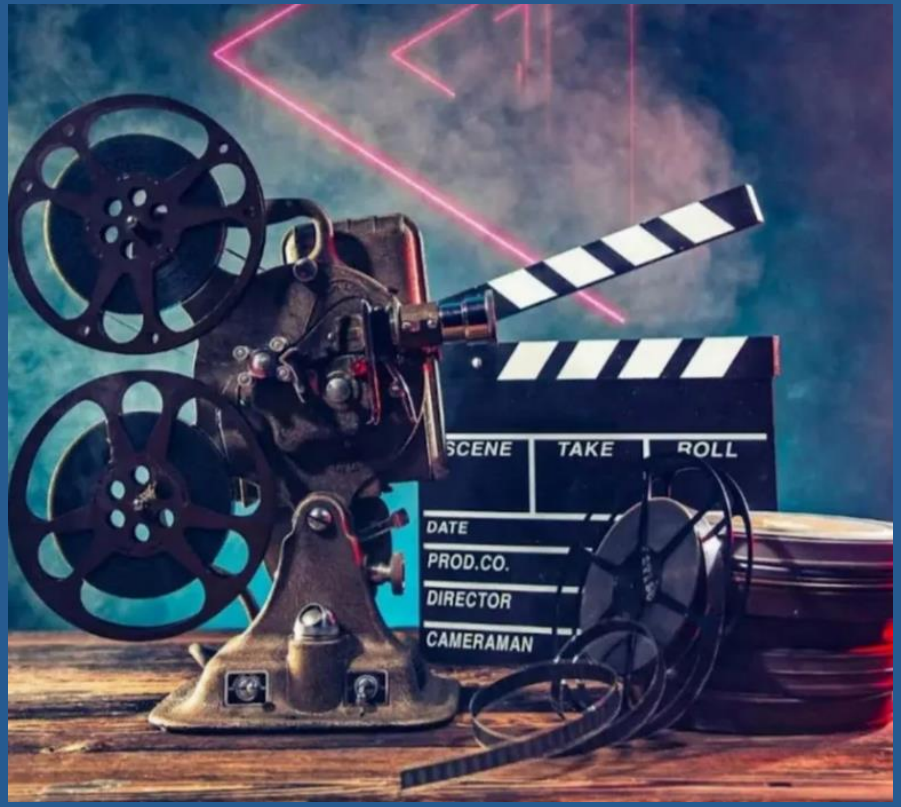
В инфраструктуре появился ViPNet EndPoint Protection



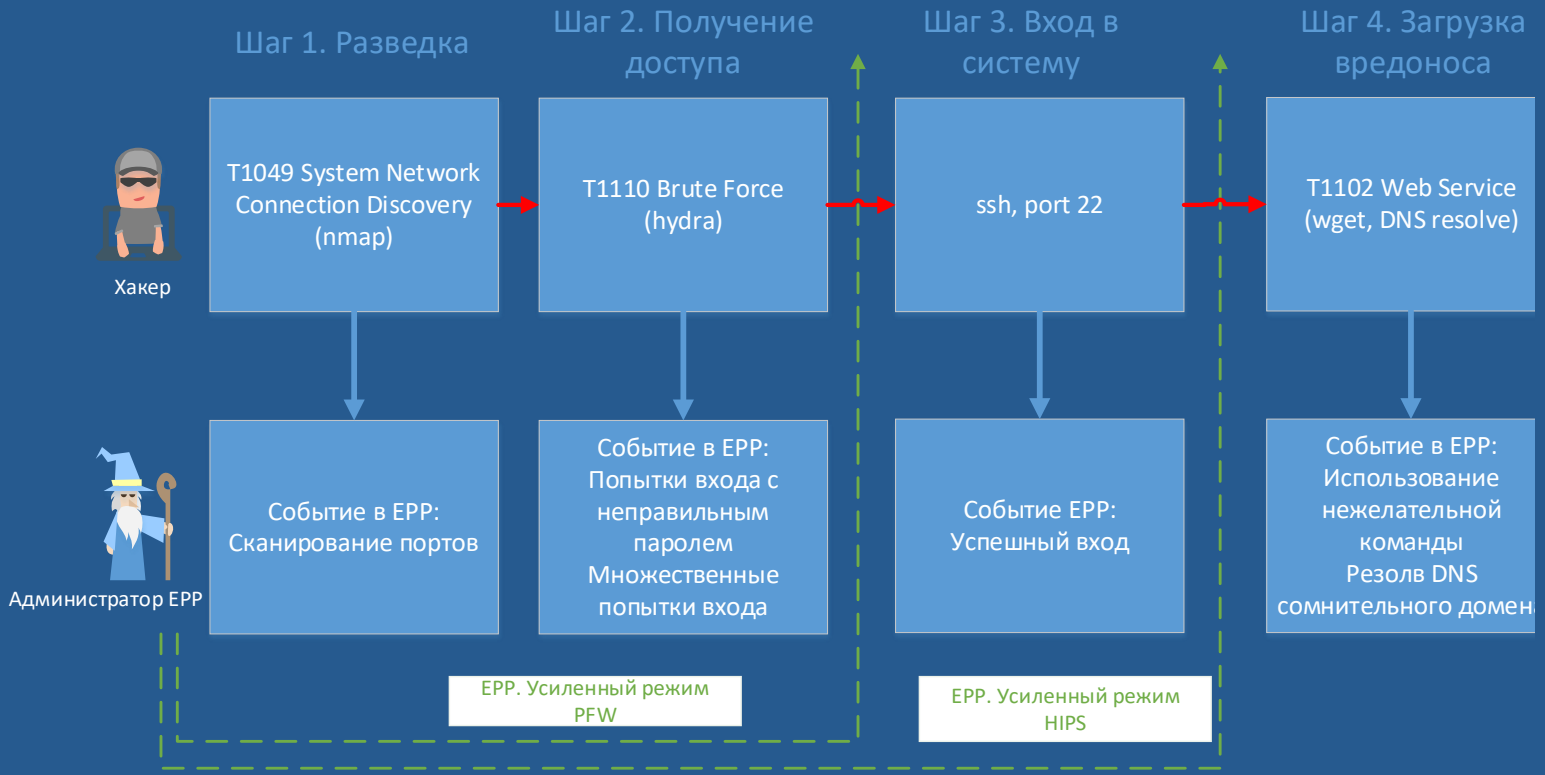
Что же должно быть включено в EPP?



Повторно атакуем, с включенным ViPNet EndPoint Protection



Пошаговый разбор. Как противодействовать хакеру



Акция «За безопасность!»

ТЕХНО infotecs 2022 ФЕСТ

Лицензии на перечисленные продукты предоставляются **на безвозмездной основе** на 6 месяцев!!!

Защита каналов связи	Системы управления и мониторинга	Защита рабочих станций и серверов	Обнаружение и предотвращение компьютерных атак
• ViPNet Coordinator VA • ViPNet xFirewall VA • ViPNet TLS Gateway VA • ViPNet PKI Client • ViPNet Client	• ViPNet Administrator • ViPNet Policy Manager	• ViPNet SafeBoot • ViPNet SafePoint • ViPNet IDS HS*	• ViPNet TIAS VA • ViPNet IDS MC VA • ViPNet IDS NS VA • ViPNet IDS HS*

Перевод отдела технической поддержки на усиленный режим работы и предоставление консультаций по подбору оптимальных решений для обеспечения информационной безопасности в рамках импортозамещения. Для получения консультации вы можете отправить электронное письмо с вопросами и контактными данными на адрес sos@infotecs.ru.

ТЕХНО 2022 infotecs ФЕСТ

Спасибо за внимание!

Подписывайтесь на наши соцсети

https://vk.com/infotecs_news

https://t.me/infotecs_news