Обнаружение и предотвращение атак при помощи ViPNet EndPoint Protection.

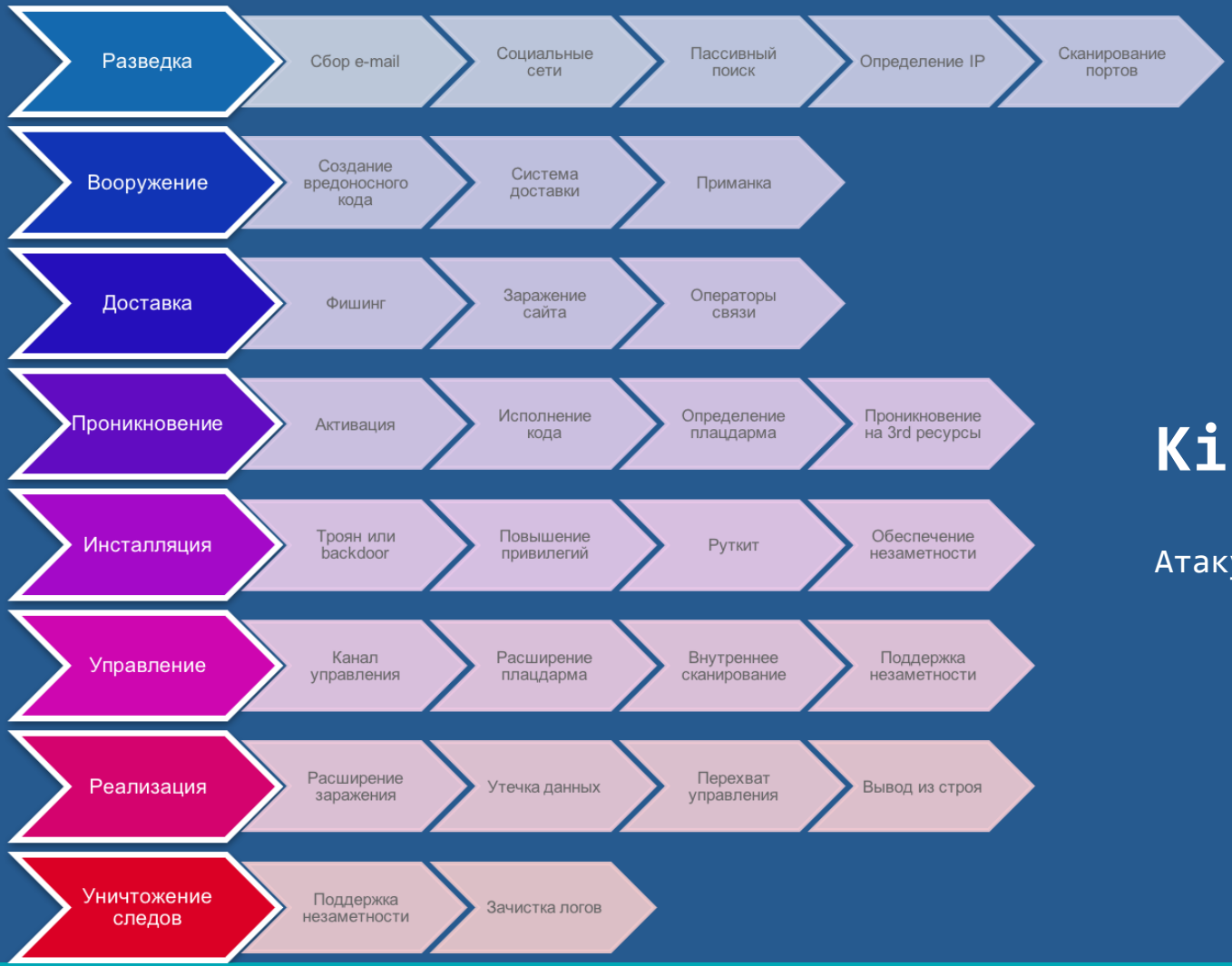
Разбор поведения злоумышленника по MITRE ATT&CK

Иван Кадыков

ТЕХНО 2021 infotecs ФЕСТ

О чём пойдёт речь?

«Болезни» последних 5-ти лет



ТЕХНО infotecs 2021 ФЕСТ

Kill Chain

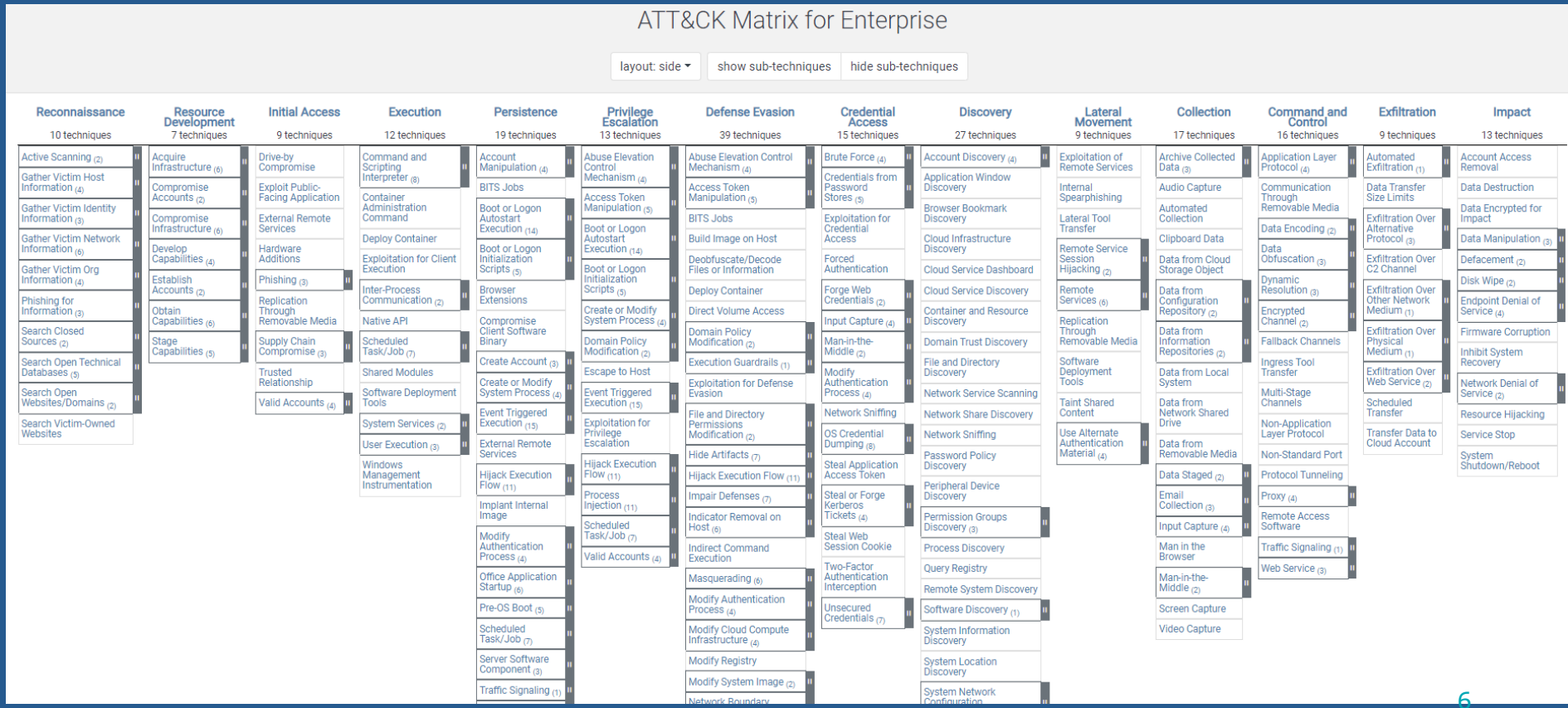
Атаку можно структурировать

Методология для специалистов ИБ

Adversary
Tactics
Techniques
&
Common
Knowledge

Техники — Тактики — Процедуры

ТЕХНО infotecs 2021 ФЕСТ

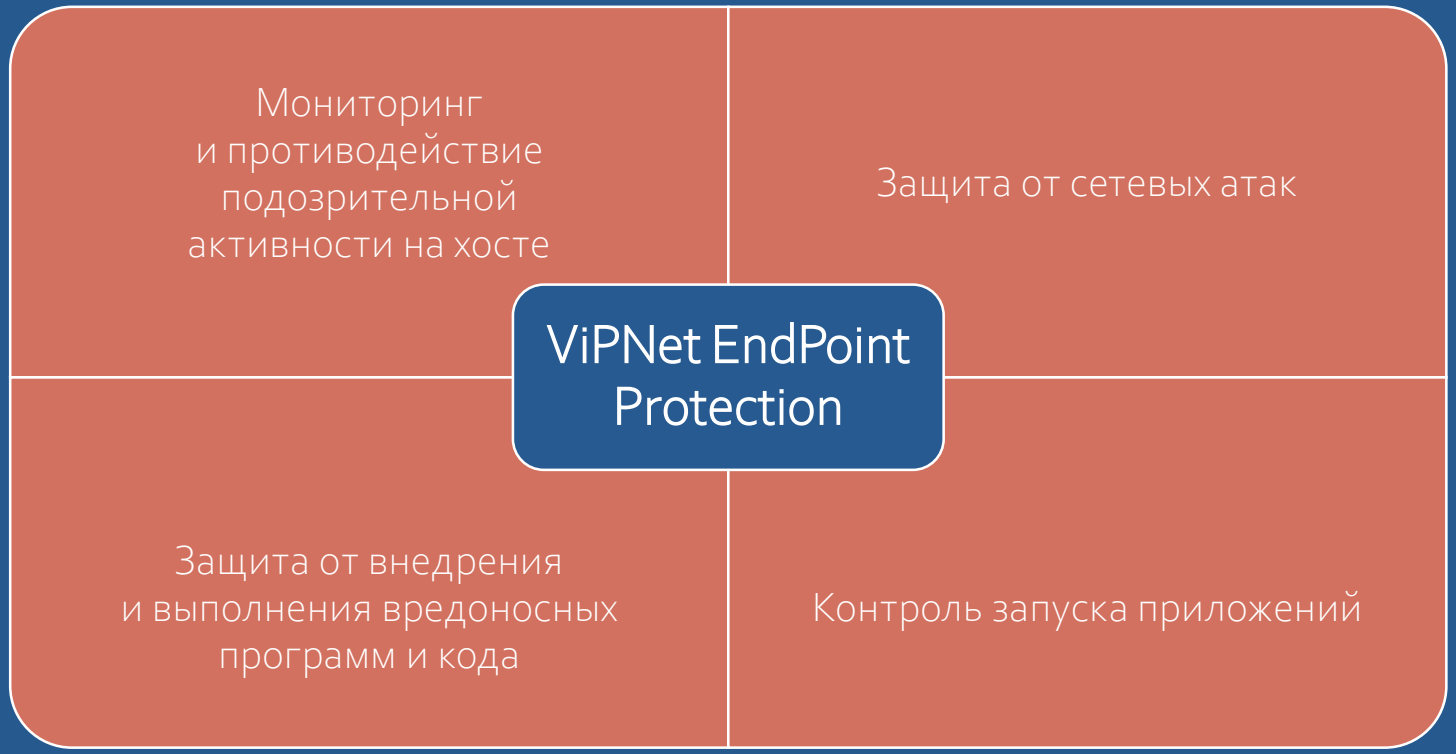


«Методика оценки угроз безопасности информации» — ФСТЭК России

ViPNet EndPoint Protection

Система комплексной защиты рабочих станций и серверов, предназначенная для предотвращения «файловых» и сетевых атак, обнаружения вредоносных действий и реакции на эти действия.

Решаемые задачи



Давайте попрактикуемся

Продукт:

ViPNet EndPoint Protection

Знания:

MITRE ATT&CK

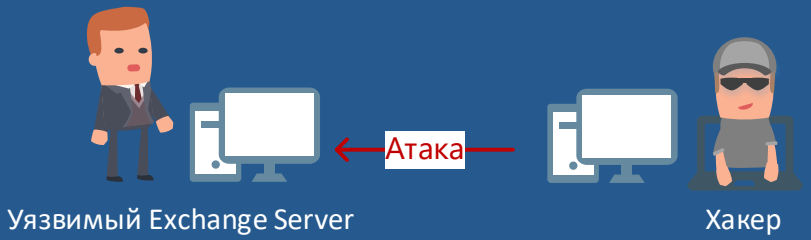
ВАЖНО!

- 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! ☺ ☺ ☺

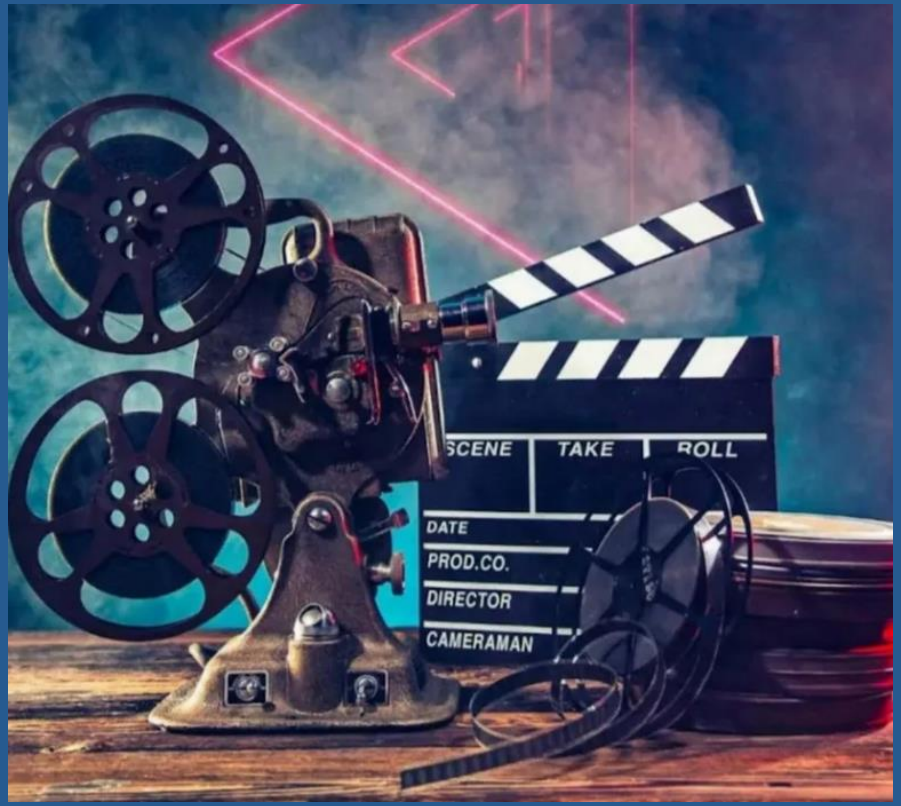
Сценарий 1. Атака уязвимого Exchange-сервера. Получение хэша пароля администратора

Что за атака?

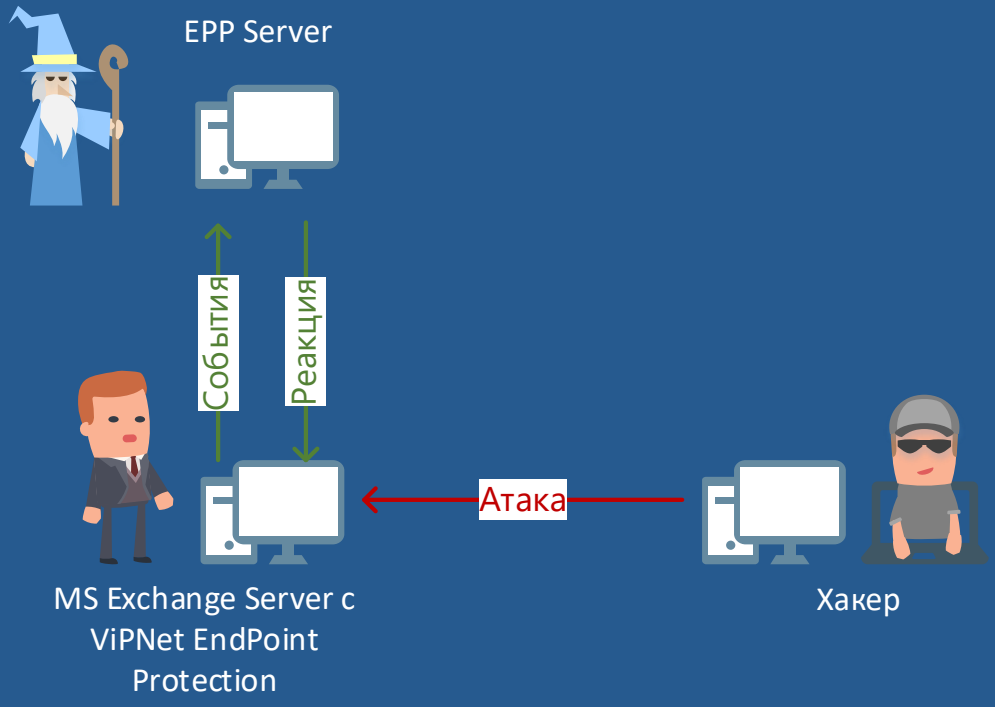
- Злоумышленник будет использовать известную уязвимость ProxyLogon, точнее **CVE-2021-26857** (2 марта 2021 года Microsoft выпустила обновления безопасности, чтобы закрыть эти уязвимости).
- Суть атаки – отправка HTTP-запроса для обхода механизма аутентификации, с дальнейшим проникновением в систему и закрепление.



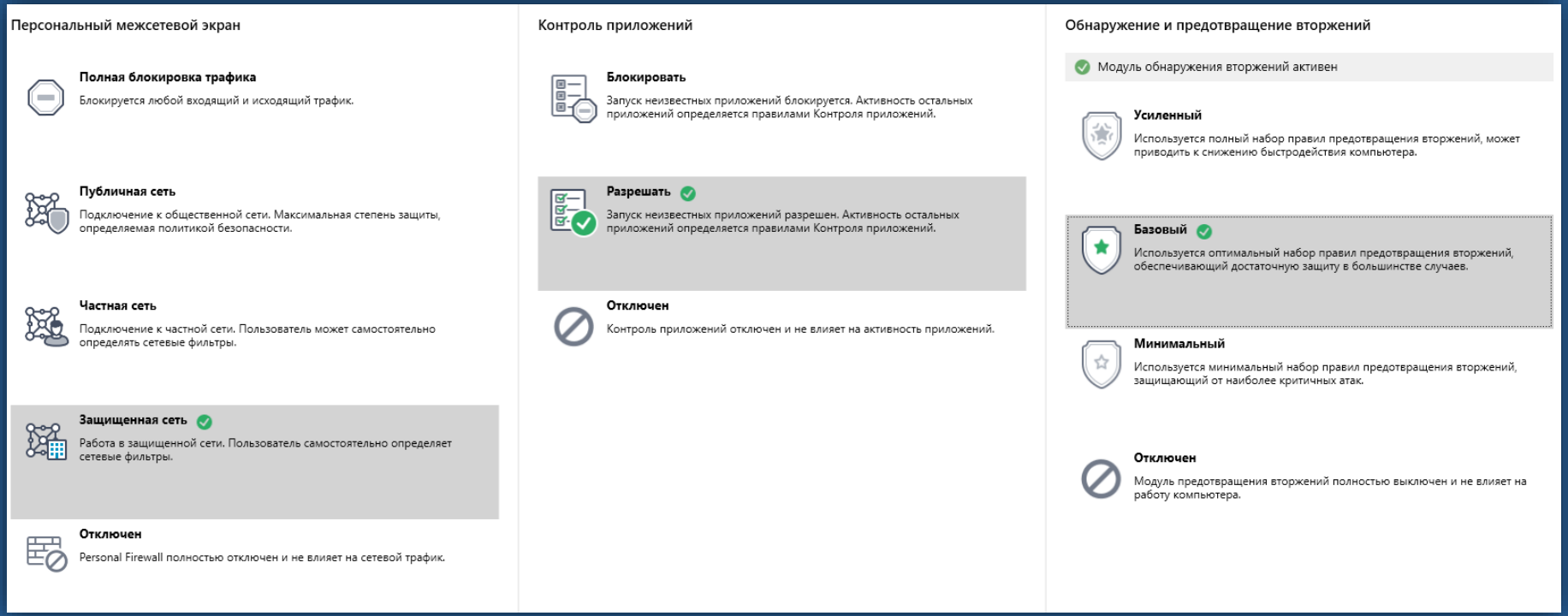
Демонстрируем атаку!



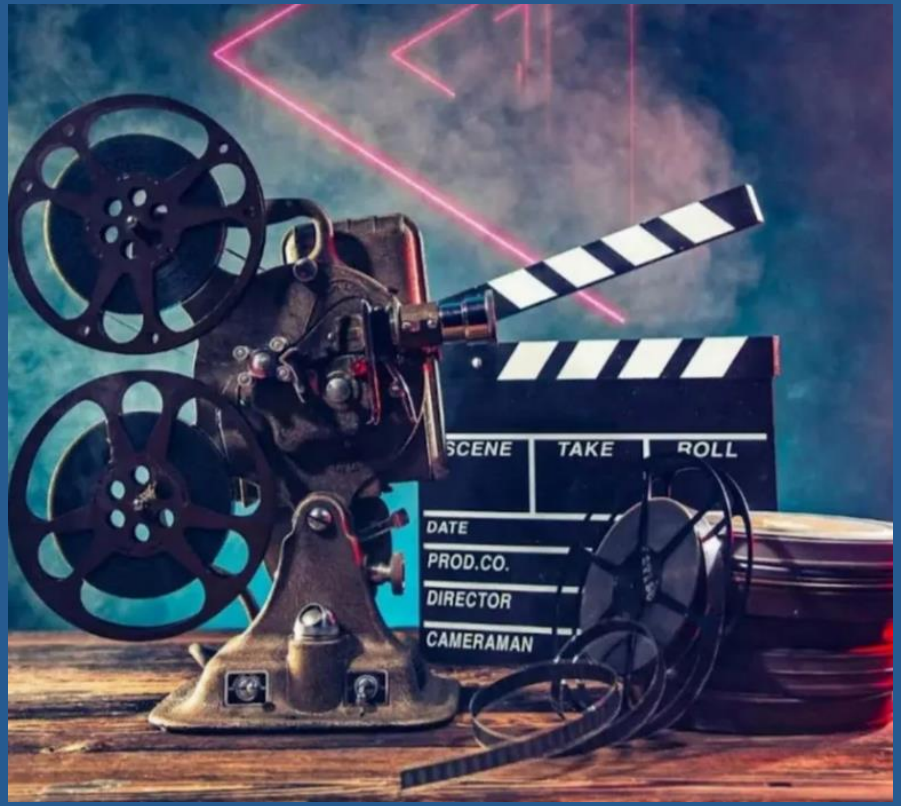
В инфраструктуре появился ViPNet EndPoint Protection



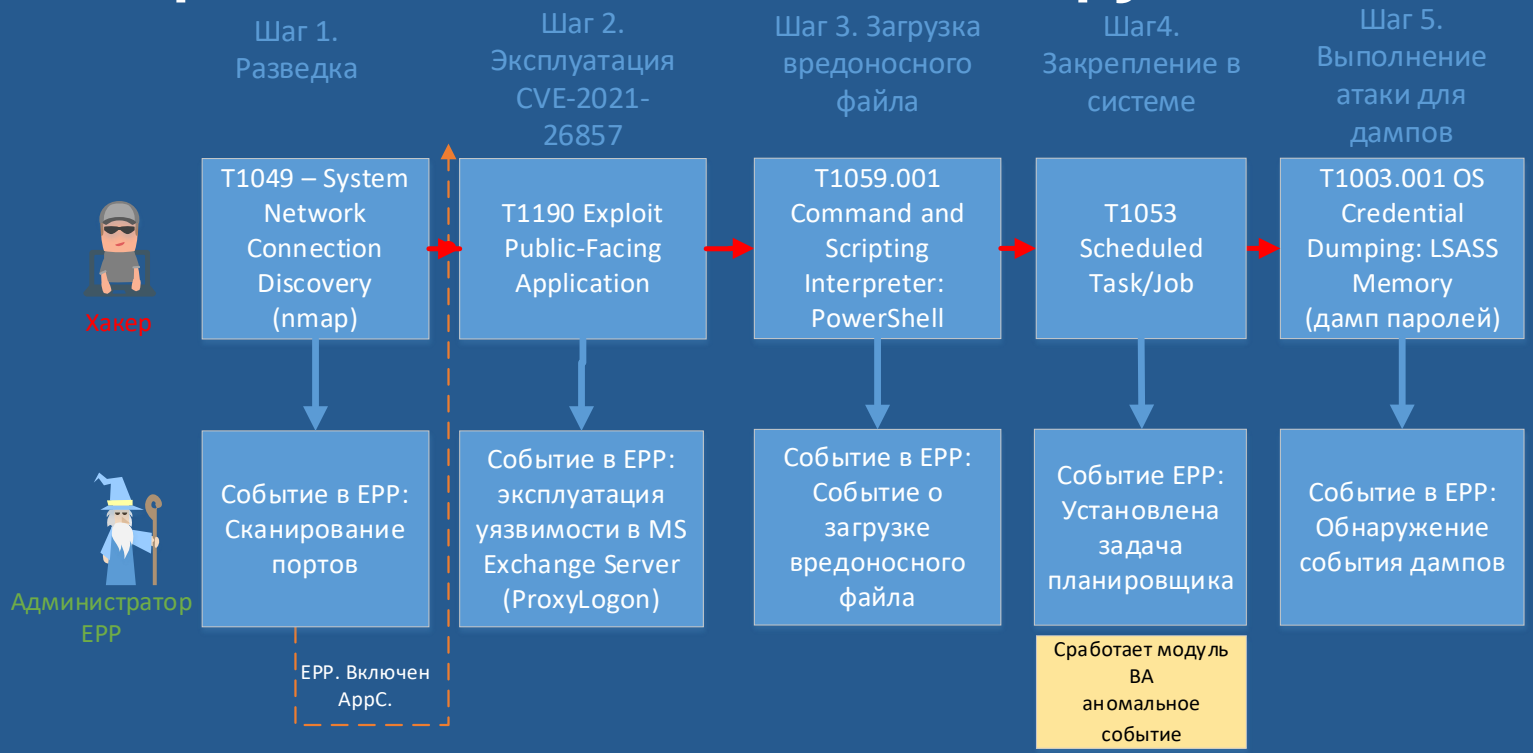
Что же должно быть включено в EPP?



Повторно атакуем, с включенным ViPNet EndPoint Protection



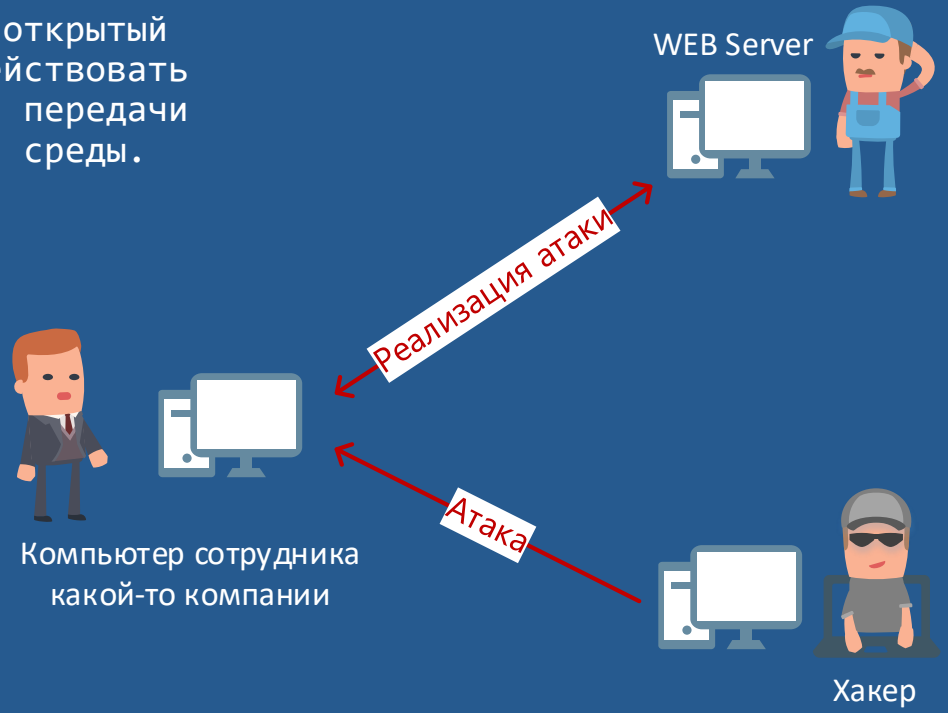
Пошаговый разбор.
Как противодействовать хакеру



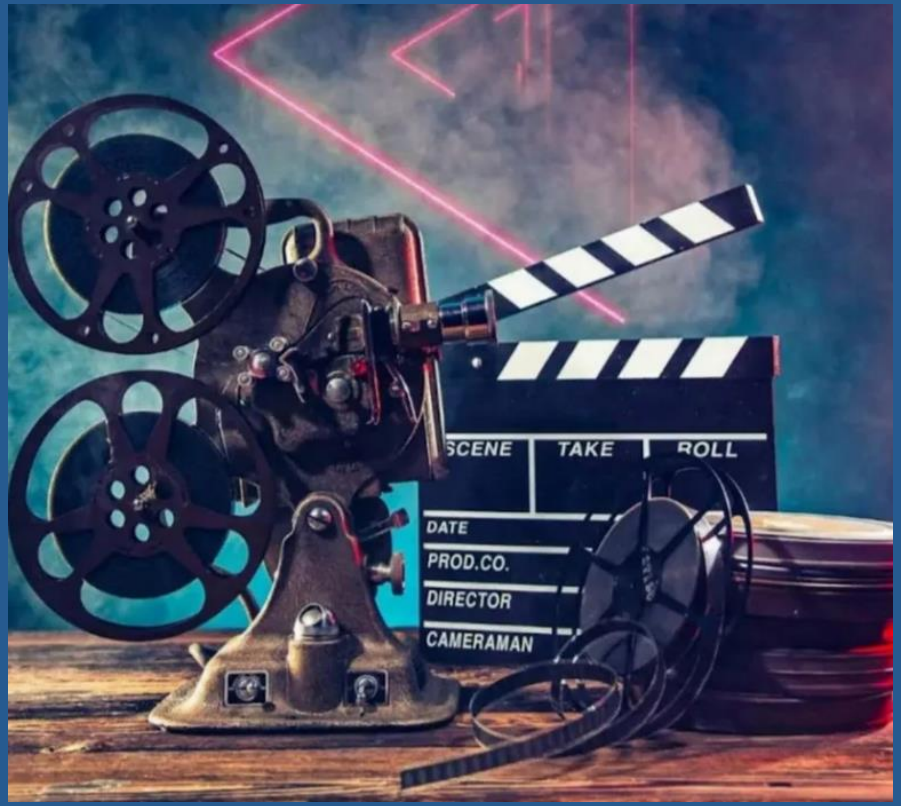
Сценарий 2. Загрузка вредоносной программы через открытый порт 22 (ssh), используя Resolve DNS.

Что за атака?

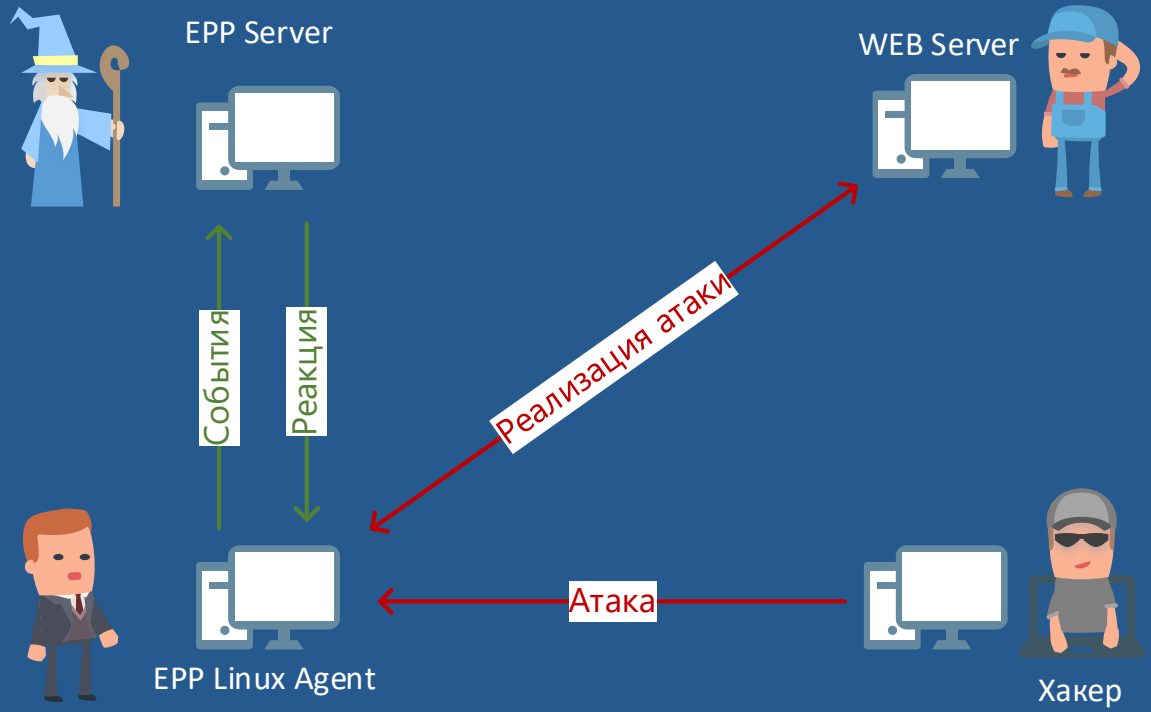
- Злоумышленник, используя открытый порт, будет пытаться задействовать легитимную веб службу для передачи данных в/из корпоративной среды.



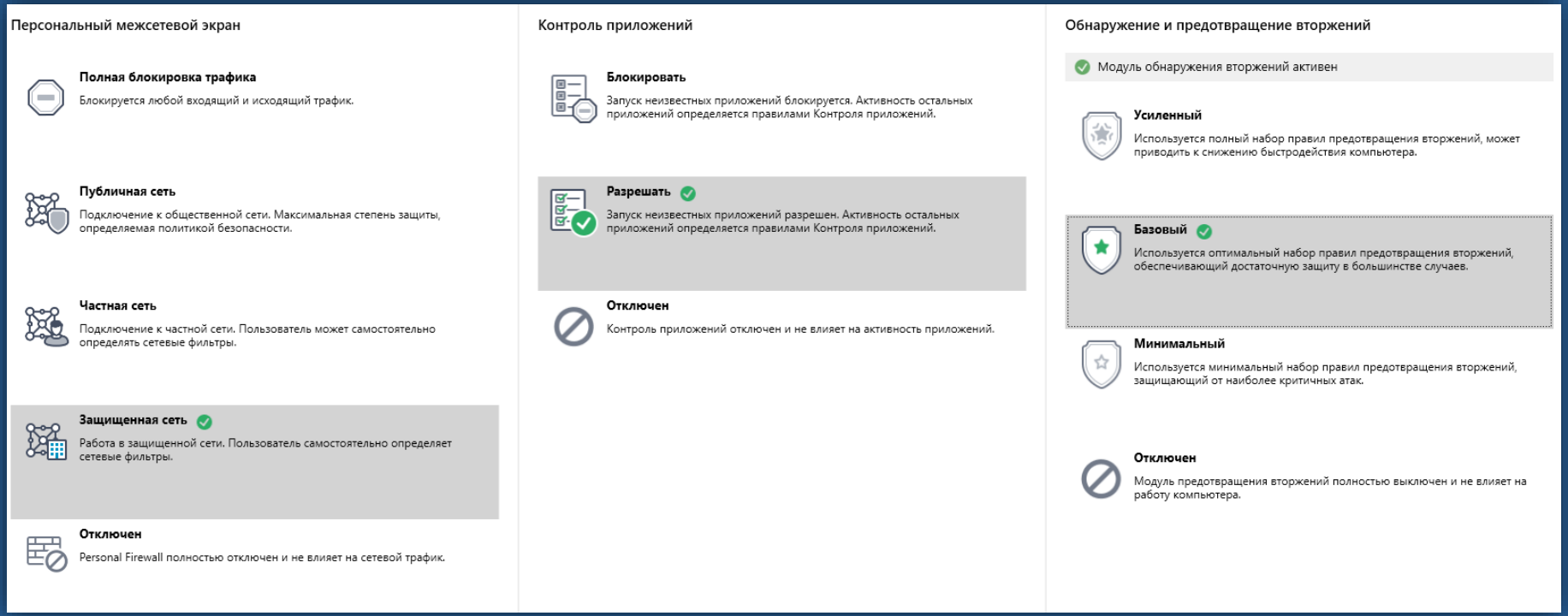
Демонстрируем атаку!



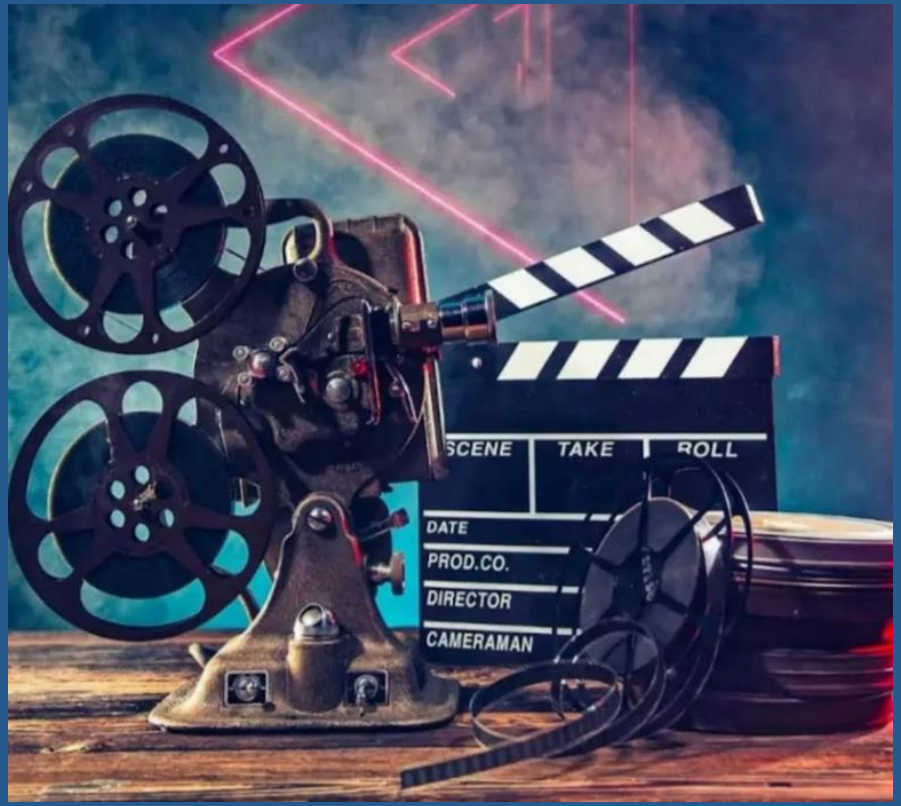
В инфраструктуре появился ViPNet EndPoint Protection



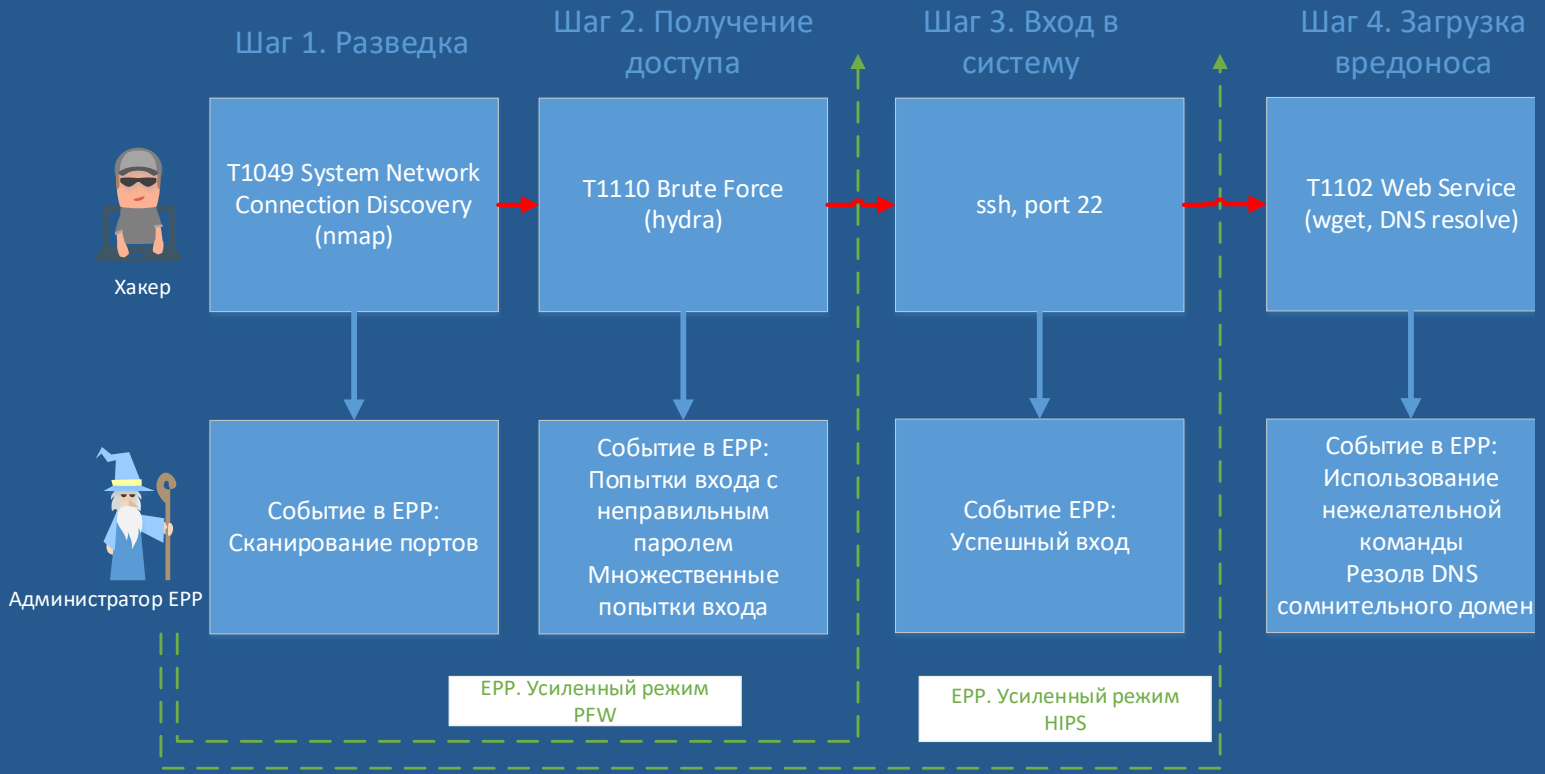
Что же должно быть включено в EPP?



Повторно атакуем, с включенным ViPNet EndPoint Protection



Пошаговый разбор.
Как противодействовать хакеру



ТЕХНО infotecs 2021 Фест

Спасибо за внимание!

Подписывайтесь на наши соцсети

@infotecs.ru

@vpninfotecs

@InfoTeCS_Moscow