SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

Опыт проведения киберучений

Роман Овчинников,
Руководитель отдела исполнения

Цели

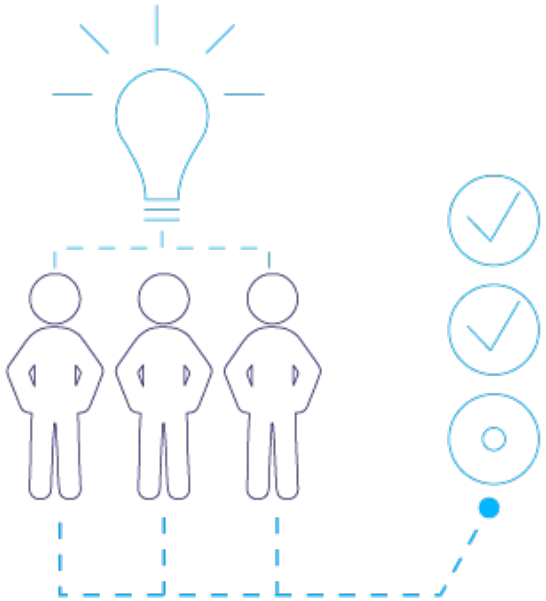
01 Получение практических навыков расследования инцидентов кибербезопасности

02 Повышение осведомленности в области актуальных угроз кибербезопасности

03 Знакомство с современными системами и средствами обеспечения кибербезопасности

04 Практический опыт взаимодействия с CERT

05 Работа в команде



Задачи

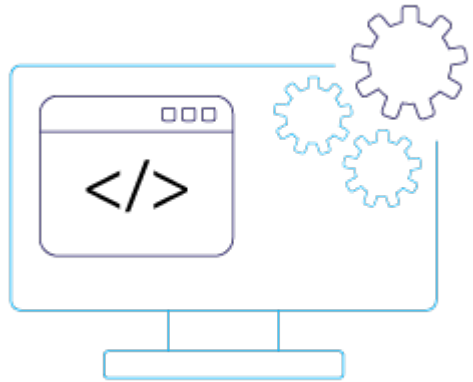
01 Разработка сценария учений и атак

02 Техническая реализация сценариев атак

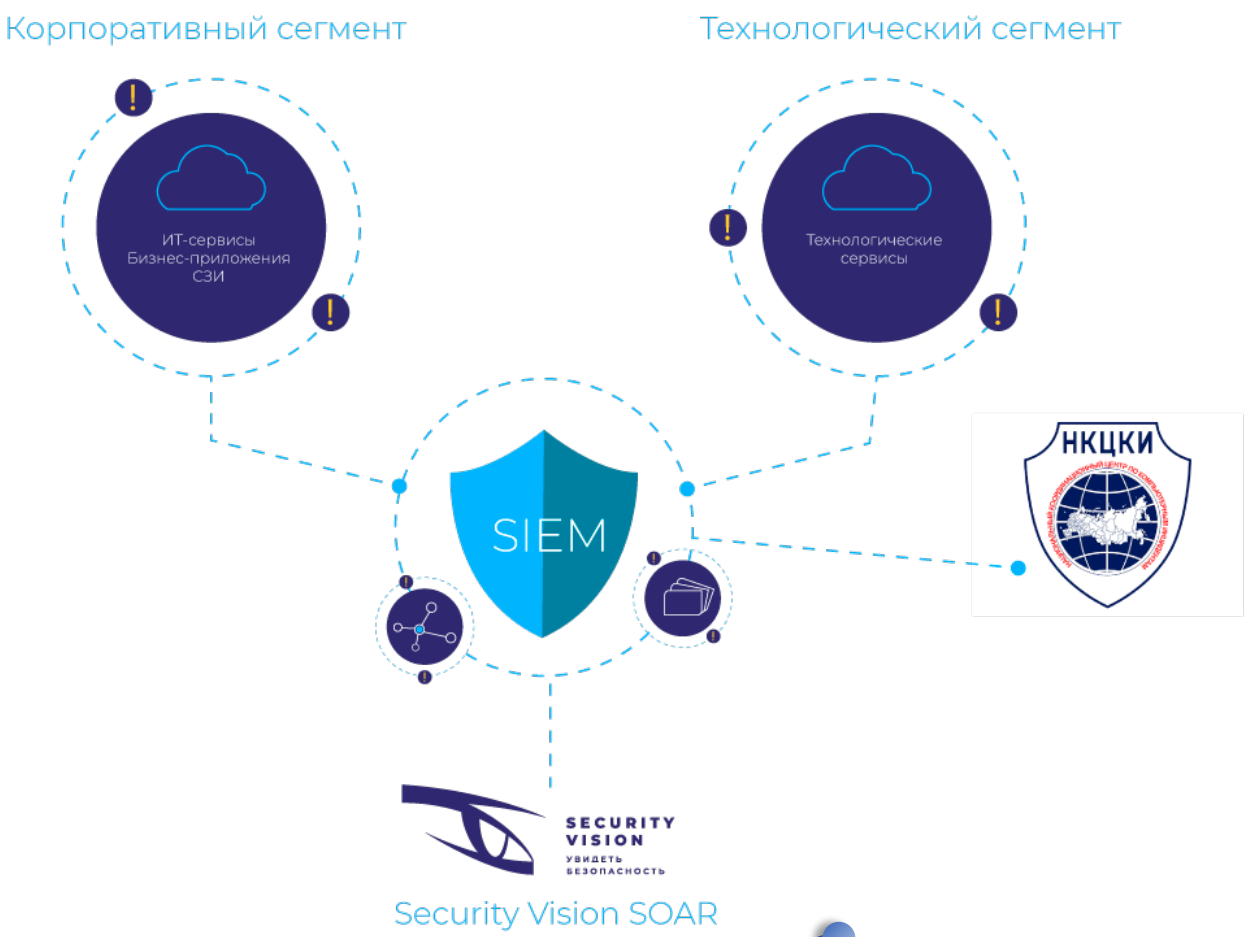
03 Настройка система защиты информации

04 Настройка инструментария SOAR

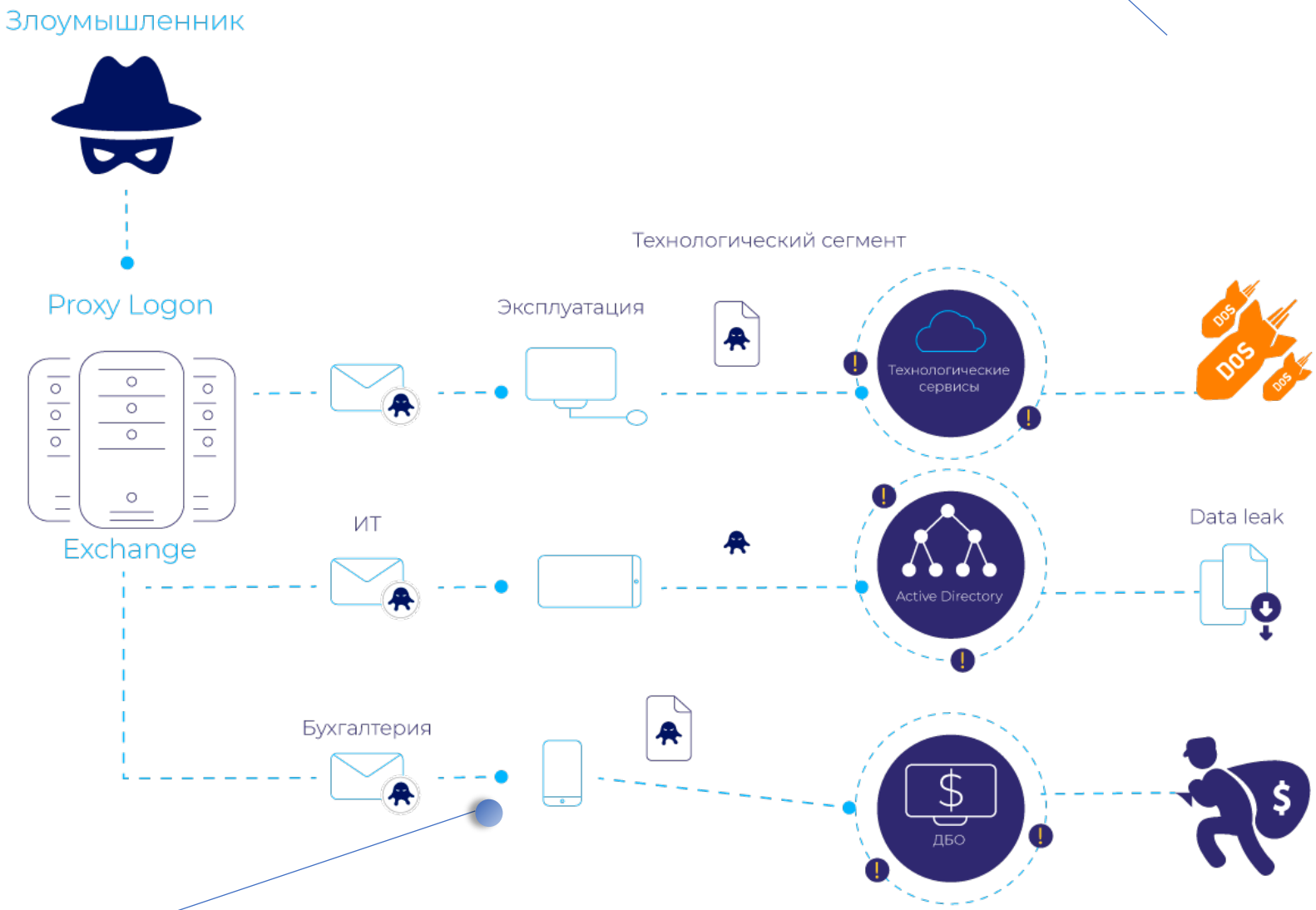
05 Построение двустороннего взаимодействия с CERT



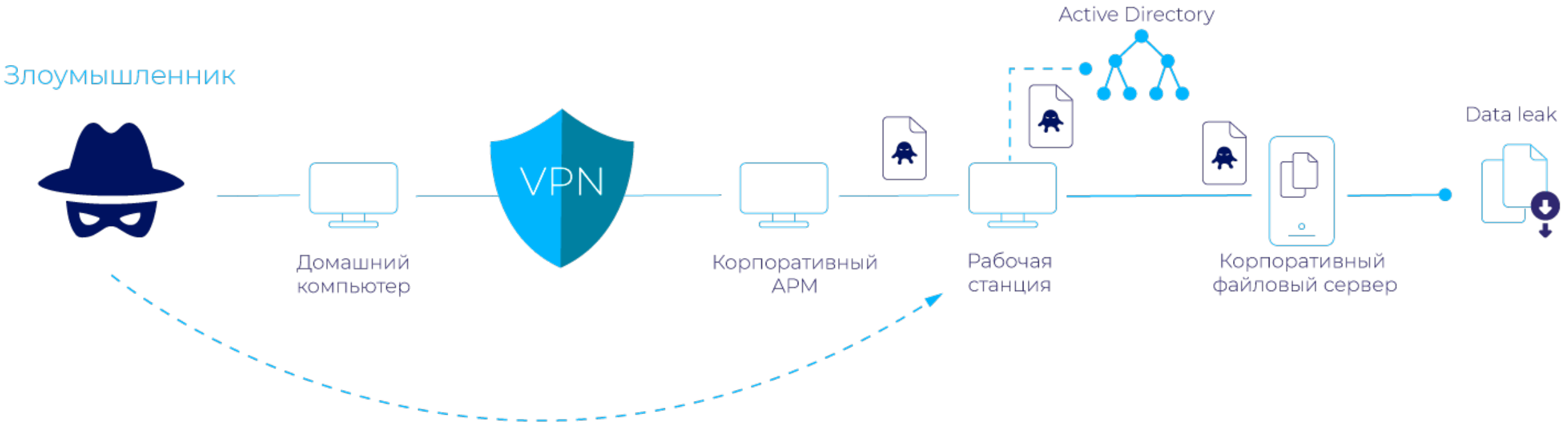
Инфраструктура



Сценарий 1


Злоумышленник
Proxy Logon
Exchange
Технологический сегмент
Эксплуатация
Технологические сервисы
DOS
ИТ
Active Directory
Data leak
Бухгалтерия
ДБО
$

Сценарий 2


Active Directory
Злоумышленник
VPN
Data leak
Домашний компьютер
Корпоративный АРМ
Рабочая станция
Корпоративный файловый сервер

Инструментарий нарушителя

01 Metasploit

02 dcsync

03 impacket

04 uacme

05 Powershell empire

SOAR


Анализ и репутация
ALIEN VAULT
OPSWAT.
MetaDefender
VirusTotal
Поиск схожих инцидентов
Активы
SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ
SIEM
Процессы
Службы
Файловая система
Сетевые соединения
Журналы событий
Планировщик задач
НКЦКИ
Active Directory
Exchange

Итоги

01 Участники успешно провели расследование и «раскрутили» цепочки атак

02 Осуществлено взаимодействие с CERT, по итогам которого разработан бюллетень безопасности для других участников

03 Получен новый опыт – как участниками, так и организаторами

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

СПАСИБО ЗА ВНИМАНИЕ