KSD 2022
Kaspersky Security Day

Построение SOC на базе решений Kaspersky

Докладчик: Владимир Ли
email: li-vladimir@outlook.com
mobile: +7 705 290 5260

Microsoft: MCP, MCSA, MCSE, MCT
Kaspersky: KCP, KCSE (level 1-2), KDSS, KCSE, KCT

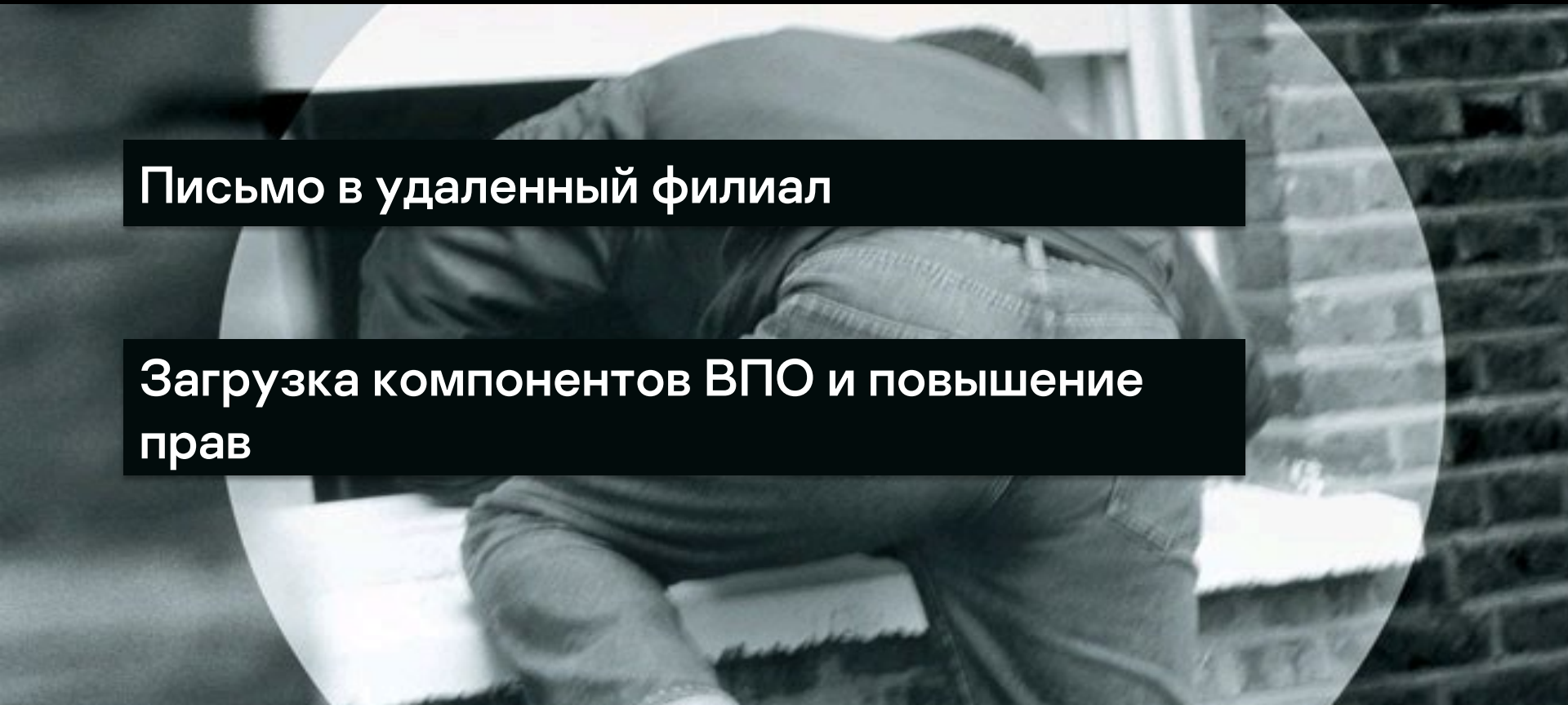
kaspersky 25 лет

Краткий план презентации

1. Проблематика
2. Мой SOC
3. Увлекательные истории

Проблематика

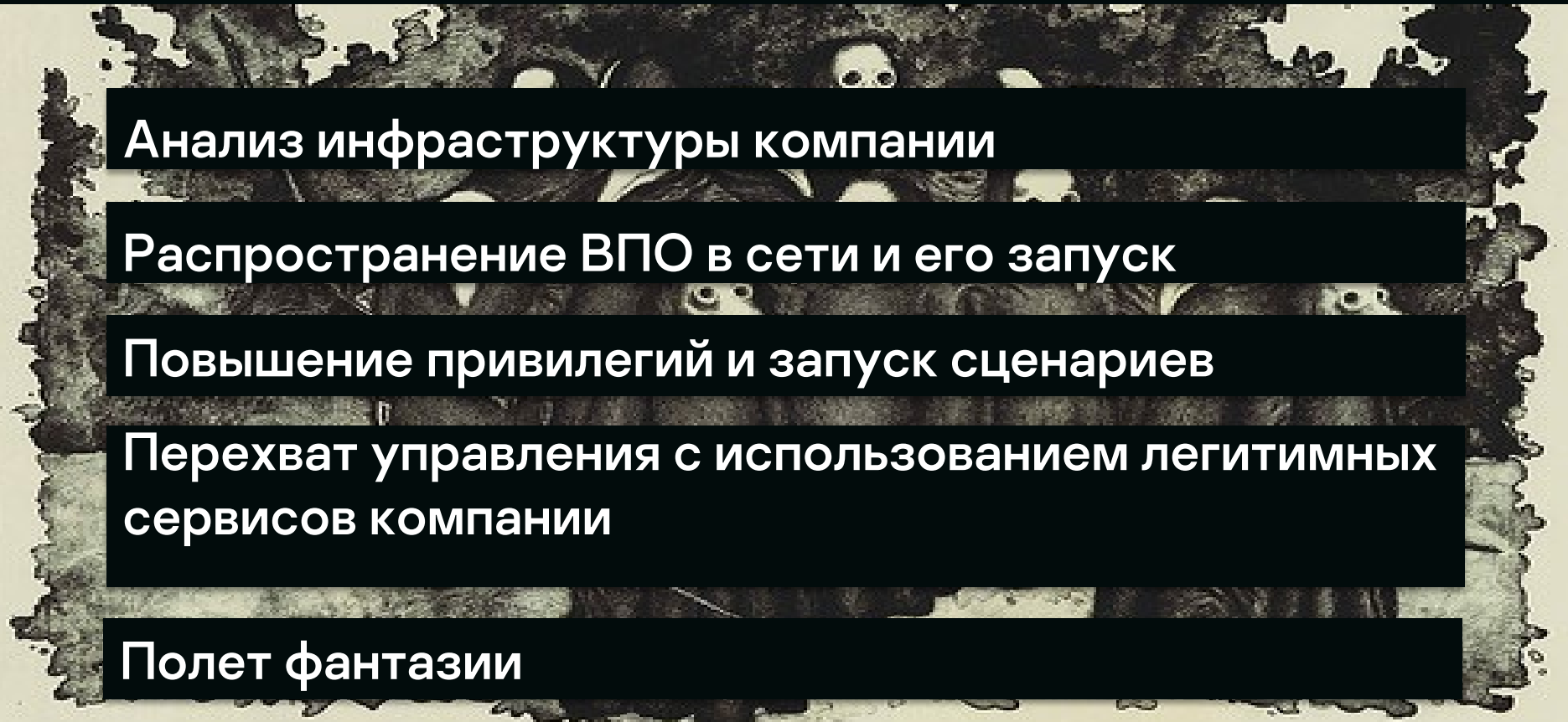
Проникновение



Письмо в удаленный филиал

Загрузка компонентов ВПО и повышение прав

Распространение и закрепление



Анализ инфраструктуры компании

Распространение ВПО в сети и его запуск

Повышение привилегий и запуск сценариев

Перехват управления с использованием легитимных сервисов компании

Полет фантазии

Полет фантазии

Другие возможные сценарии:

Банкоматы отдают деньги жуликам
Деньги утекают через swift
Уничтожение данных
Производство останавливается
Газ не идет по трубам
Электричества нет
Больницы не работают

Всё плохо

Если сработал антивирус?

Старт активной фазы атаки

Мой SOC

Продуктовое наполнение:

KTS

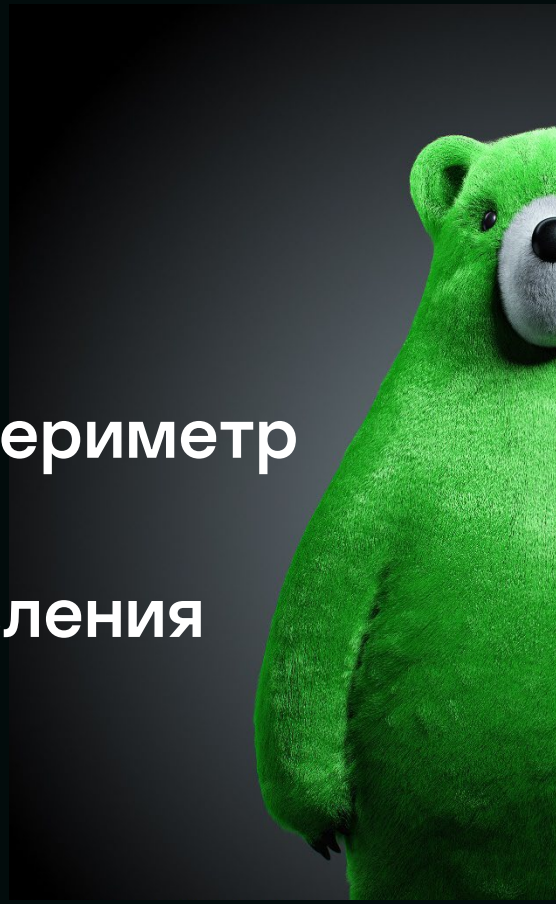
KATA

KEDR

KUMA (пилотируем)

Почему Kaspersky?

- Лучшее покрытие в регионе
- Интеграция всех решений в один периметр
- Единая точка мониторинга и управления



Увлекательная история №1

О шифровальщиках

Увлекательная история №2

Маркетинг и песочницы

Увлекательная история №3

Земля или облако?

Спасибо!