PS CLOUD SERVICES 20

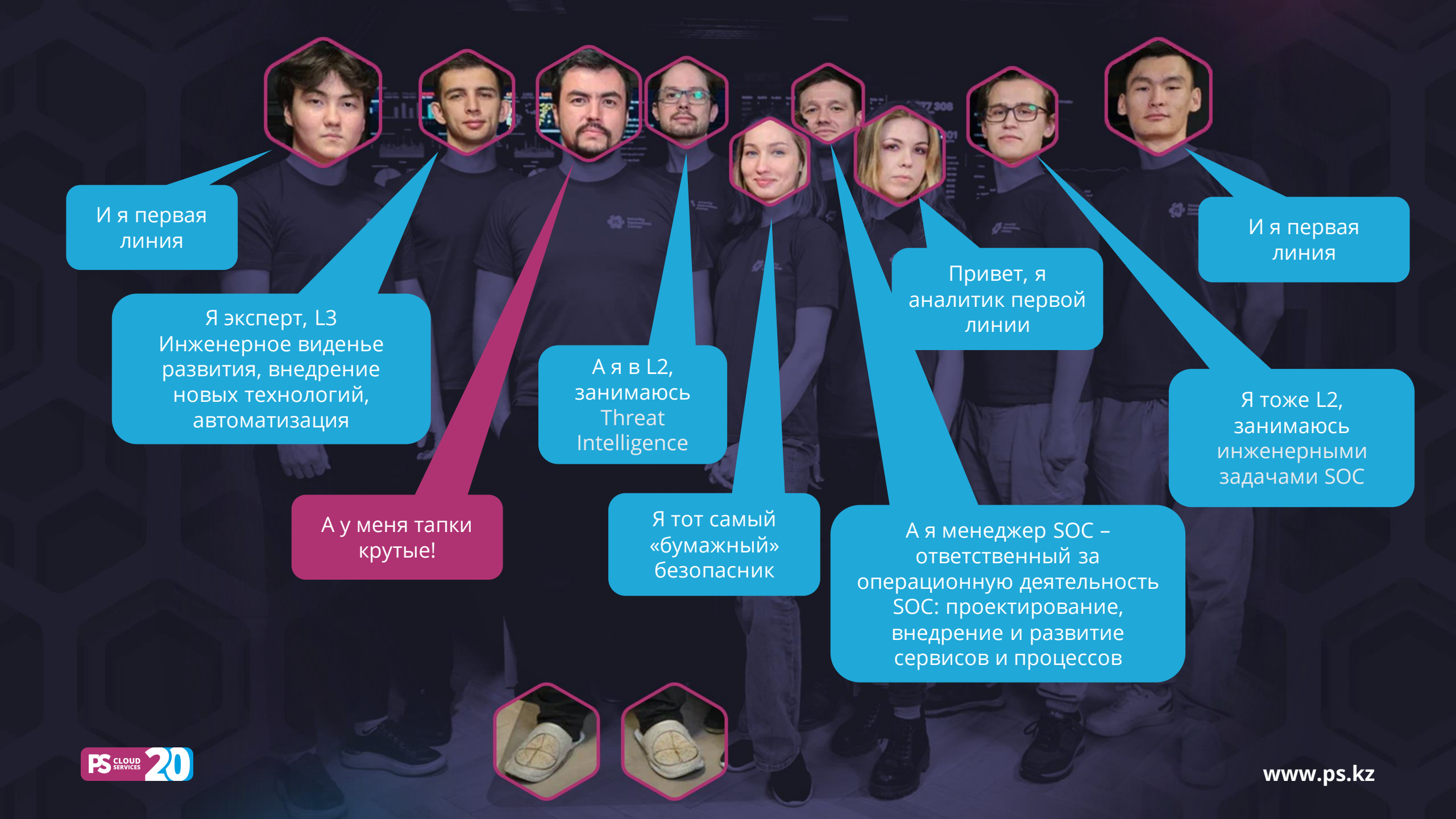
КАК МЫ СТРОИМ ЛУЧШИЙ SOC

Александр Пушкин
CISO PS Cloud Services

#whoami

- RedTeam – 15 лет
- BlueTeam – 3 года
- CISO
- Bareboat Skipper
- Гелий, миллиампер, плебей, фиточай

Security Operations Center


И я первая линия
Я эксперт, L3 Инженерное виденье развития, внедрение новых технологий, автоматизация
А у меня тапки крутые!
А я в L2, занимаюсь Threat Intelligence
Я тот самый «бумажный» безопасник
Привет, я аналитик первой линии
А я менеджер SOC – ответственный за операционную деятельность SOC: проектирование, внедрение и развитие сервисов и процессов
И я первая линия
Я тоже L2, занимаюсь инженерными задачами SOC

КАКОЙ МОТИВ У ЗАКАЗЧИКОВ?

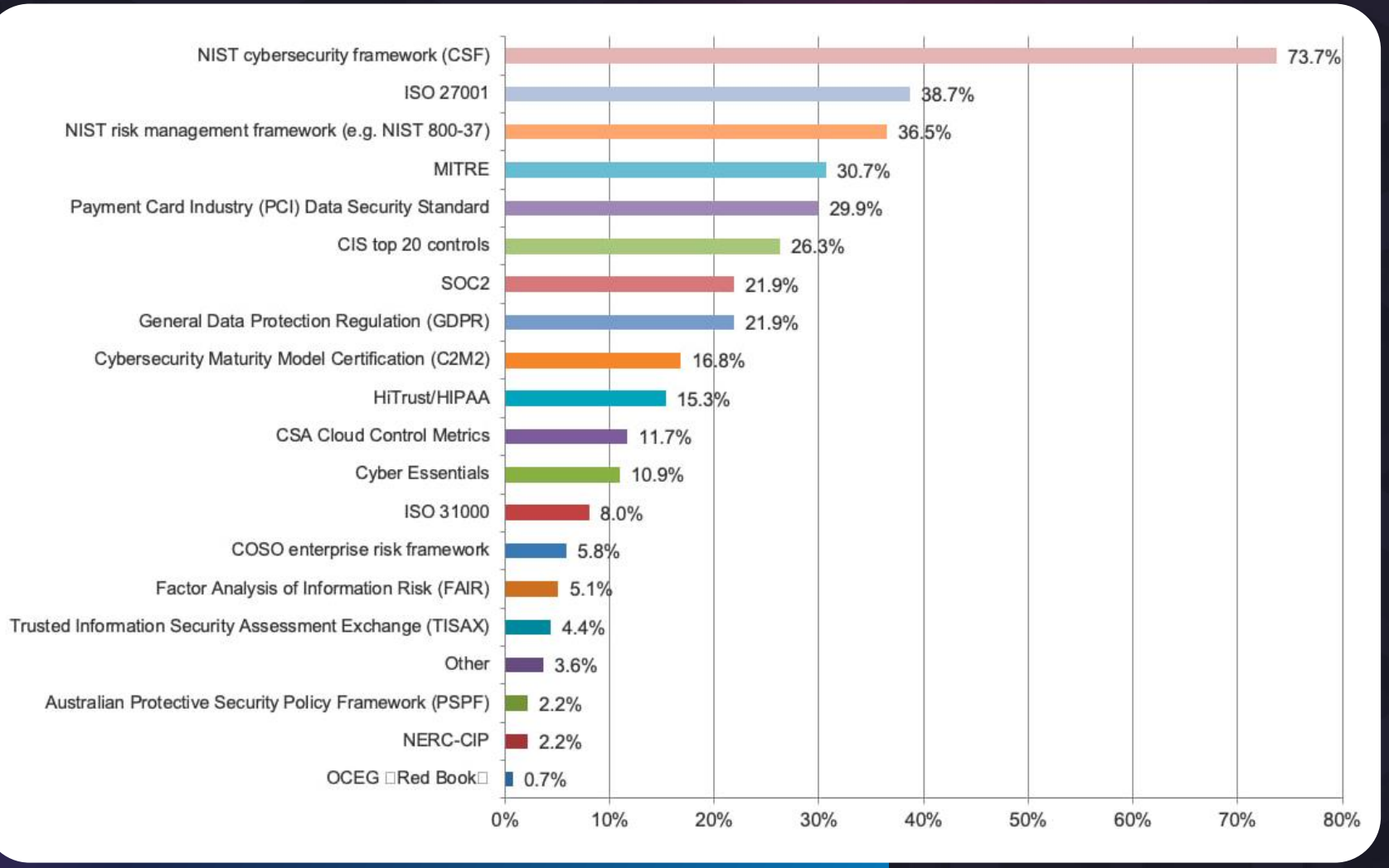
~~Пройти испытания ИБ~~

Только 10% успешных кибератак выявляются жертвами самостоятельно

об остальных 90% они узнают из внешних источников

НА КОГО РАВНЯТЬСЯ?

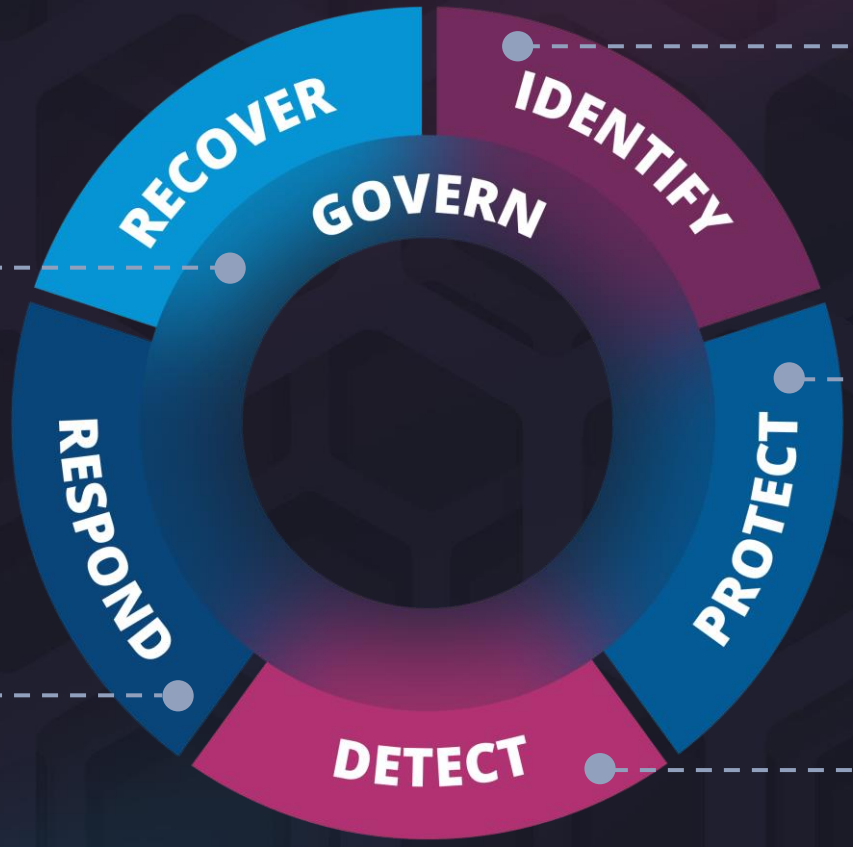
С помощью какого фреймворка/стандарта компании вы оцениваете эффективность/зрелость своей программы ИБ?



ПРИНЦИПЫ ВЫСТРАИВАНИЯ ДЕЯТЕЛЬНОСТИ SOC

Системный подход в управлении процессами SOC

Оперативное реагирование на инциденты ИБ



Инвентаризация активов и киберугроз

Контроль за состоянием защищенности

Мониторинг информационной безопасности

КЛЮЧЕВЫЕ СЕРВИСЫ SOC

Security Monitoring

Мониторинг событий ИБ

Круглосуточное отслеживание событий, потенциально связанных с реализацией угроз ИБ, опираясь на индивидуальную модель угроз защищаемой инфраструктуры

15 охватываемых категорий требований NIST CSF

Security Incident Management

Управление инцидентами ИБ

Системный процесс оперативной отработки инцидентов ИБ, включающий оповещение ответственных лиц и их экспертную поддержку

15 охватываемых категорий требований NIST CSF

Vulnerability Management

Управление уязвимостями

Системный процесс отслеживания состояния защищенности инфраструктуры, в т.ч. посредством имитации действий злоумышленников

10 охватываемых категорий требований NIST CSF

ЭКСПЕРТНЫЕ СЕРВИСЫ SOC

Threat Intelligence

Кибербразведка в отношении объекта защиты, в т.ч. OSINT

6 охватываемых категорий требований NIST CSF

Security Analysis & Forensics

Глубокая аналитика инцидентов и событий ИБ, компьютерная криминалистика

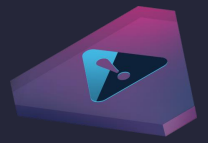
9 охватываемых категорий требований NIST CSF

Threat Hunting

Поиск экспертами угроз, недетектируемых стандартными средствами защиты информации

6 охватываемых категорий требований NIST CSF

Мониторинг событий ИБ



Управление инцидентами ИБ

Управление уязвимостями

ФАКАПЫ И ПРОБЛЕМЫ, ПОКА МЫ ПРОДАВАЛИ САМИ СЕБЕ

ЛЮДИ

1. Отпуск/больничный
2. Соблюдение рабочего графика

КЛИЕНТЫ

1. Нам только бумажечку

ПРОЦЕССЫ

1. Регламенты/плейбуки
2. Состав услуг. Текущий и целевой
3. Кто наш клиент?
4. Процесс разработки правил
5. ~~А не х**ю ли я делаю?~~

А как оценить?

ТЕХНОЛОГИИ

1. Стек технологий
2. DevOps
3. Электроэнергия, провайдеры интернет

ЧТО МЫ СДЕЛАЛИ И ПРОДОЛЖАЕМ ДЕЛАТЬ?

ЛЮДИ

1. Сделали 4+1
   (по состоянию на 2023Q4)
2. Планируем расширение

КЛИЕНТЫ

1. Awareness

ПРОЦЕССЫ

1. Регламенты появились
2. Определили целевой состав услуги
3. Появился процесс разработки правил
4. Профиль клиента
5. SOC CMM

ТЕХНОЛОГИИ

1. Выбрали новый стек
2. DevOps отдали на аутсорс
3. Гарантированная автономность

КАНАЛ С ДАЙДЖЕСТАМИ ИБ И АНАЛИТИКОЙ:

https://t.me/pssoc

PS CLOUD SERVICES 20

www.ps.kz

СПАСИБО

ЗА ВНИМАНИЕ!

Александр Пушкин
CISO PS Cloud Services

Telegram: @alex_bezopasnikov
Email: alexandr.pushkin@ps.kz

PS CLOUD SERVICES 20

www.ps.kz