Атаки на на цифровую личность
Раннее выявление угроз и реагирование на инциденты

Сергей Золотухин

Ситуация с утечками персданных

По оценке экспертов:

100%	100%	50%	50%
Все плохо	Жить страшно	Будет еще хуже	Хуже не бывает

Пример: Утечки данных с госресурсов

40 000
учетных записей пользователей госресурсов

30
стран мира

52% **Италия**

22% **Саудовская Аравия**

5% **Португалия**

21% **Другие страны**

Государственные порталы:

- **Польша (gov.pl)**
- **Румыния (gov.ro)**
- **Швейцария (admin.ch)**
- **Болгария (government.bg)**

Сайты министерств и ведомств:

- **Министерство обороны Италии (difesa.it)**
- **Армия обороны Израиля (idf.il)**
- **Министерство финансов Грузии (mof.ge)**
- **Иммиграционная служба Норвегии (udi.no)**

Сайты госуслуг:

- **Франции (gouv.fr)**
- **Венгрии (gov.hu)**
- **Хорватии (gov.hr)**

Госслужащие
Военнослужащие
Пользователи госпорталов

Центр реагирования на инциденты информационной безопасности Group-IB оперативно предупредил уполномоченные государственные организации CERT в этих странах о потенциальной опасности.

> “
> Обмен данными системы Threat Intelligence с государственными центрами CERT других стран необходим для успешной совместной борьбы с мошенниками и хакерами. Для нас крайне важно сотрудничество с другими центрами CERT, так как это дает возможность не только вести оперативные мероприятия по реагированию (Incident Response) по всему миру, но и обогащать свою базу знаний о схемах и инструментах атак, индикаторах компрометации и аналитике о существующих или возможных угрозах. Киберпреступность не имеет государственных границ, поэтому и бороться с ней нужно не локально в одной стране, а объединив усилия с другими странами.

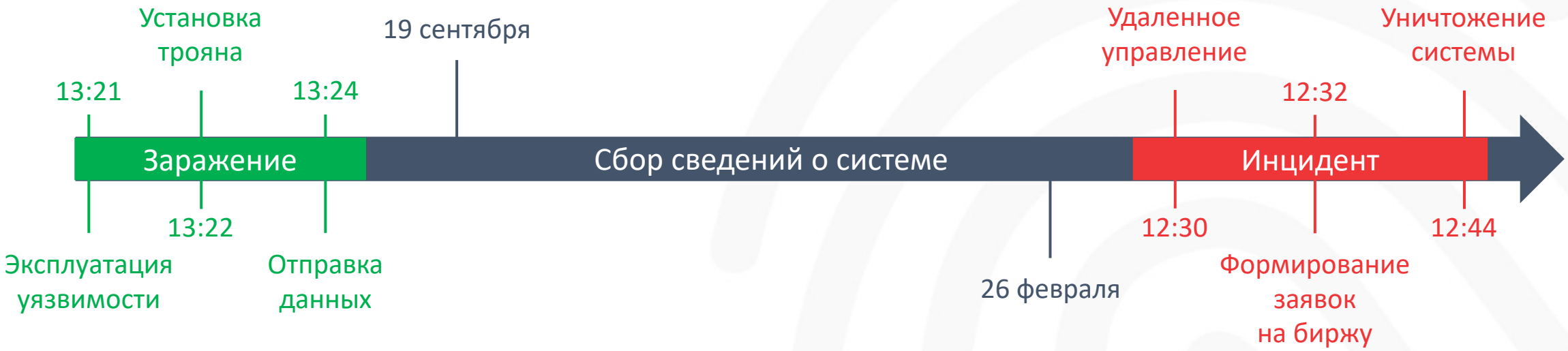
Александр Калинин
Руководитель отдела мониторинга и реагирования на инциденты информационной безопасно-сти (CERT-GIB)

Приватность vs цифровая личность
Что защищать в цифровом мире?

Цифровая борьба без правил

1. Противник мотивирован и знает о нас всё
2. Противник применяет современное оружие
3. Главное правило хакеров - «к черту любые правила»

Скрытая атака на организацию



ЧАСТЬ 1

Выявление угроз

Аудит ИБ: Знать свою сеть лучше чем хакер

- Системы ДБО и приложений мобильного банкинга
- Профилактика DoS / DDoS-атак, проведение нагрузочного тестирования
- Корректность коммутации сигнальных сетей операторов связи
- Веб-ресурсы в том числе корп./гос. порталы, e-commerce площадки
- Социотехнические тесты (социальная инженерия)
- Поиск уязвимостей сетевых инфраструктур
- Программное обеспечение, в том числе iOS, Android, Windows Phone
- Исследование защищенности POS, mPOS-терминалов
- Системы защиты коммерческой тайны и персональных данных
- Программное обеспечение АСУ ТП и систем SCADA

Аудит информационной безопасности от Group-IB:

- Анализируем уязвимости более 10 лет
- Глубоко погружаемся во внутреннюю логику работы ваших систем.
- видим риски, ускользающие из поля зрения других
- каждый отчёт содержит как краткое резюме для принимающих решения, так и подробное описание и конкретные рекомендации для специалистов

Виды аудита в ИБ:

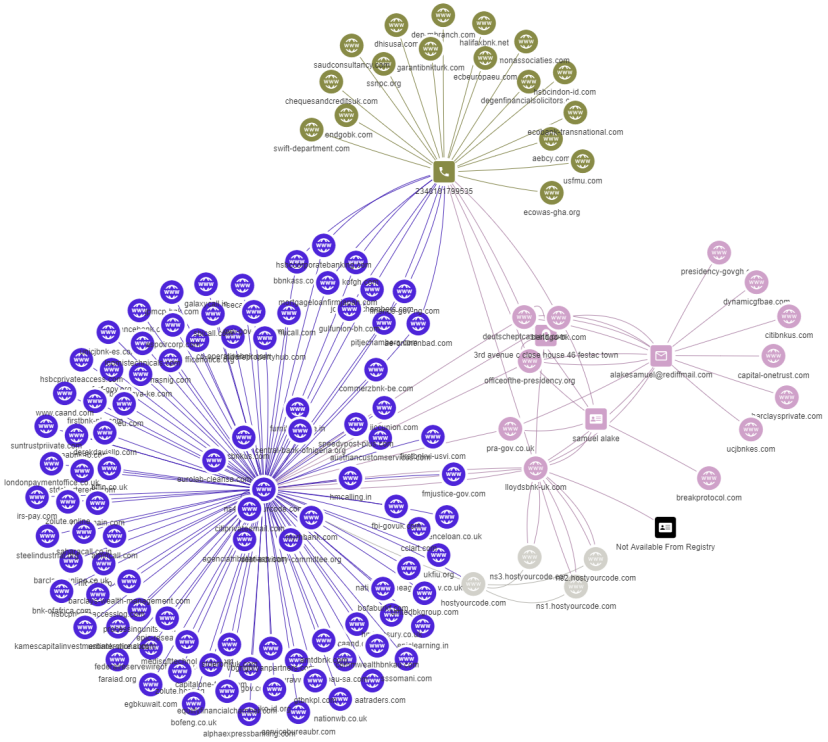
Анализ защищенности

Пентест

Red Teaming

Compromise Assessment

Знать хакера лучше чем он сам: Кибербразведка



Threat Intelligence

Знаем врага “в лицо”:

- **Тактику и инструменты**
- **Уникальные поведенческие характеристики атакующих**
- **Анатомию сложных целевых атак**

4,2 млрд

IP-адресов - ежедневное сканирование всего диапазона IPv4

650 МЛН

доменов и архивные данные за 15 лет

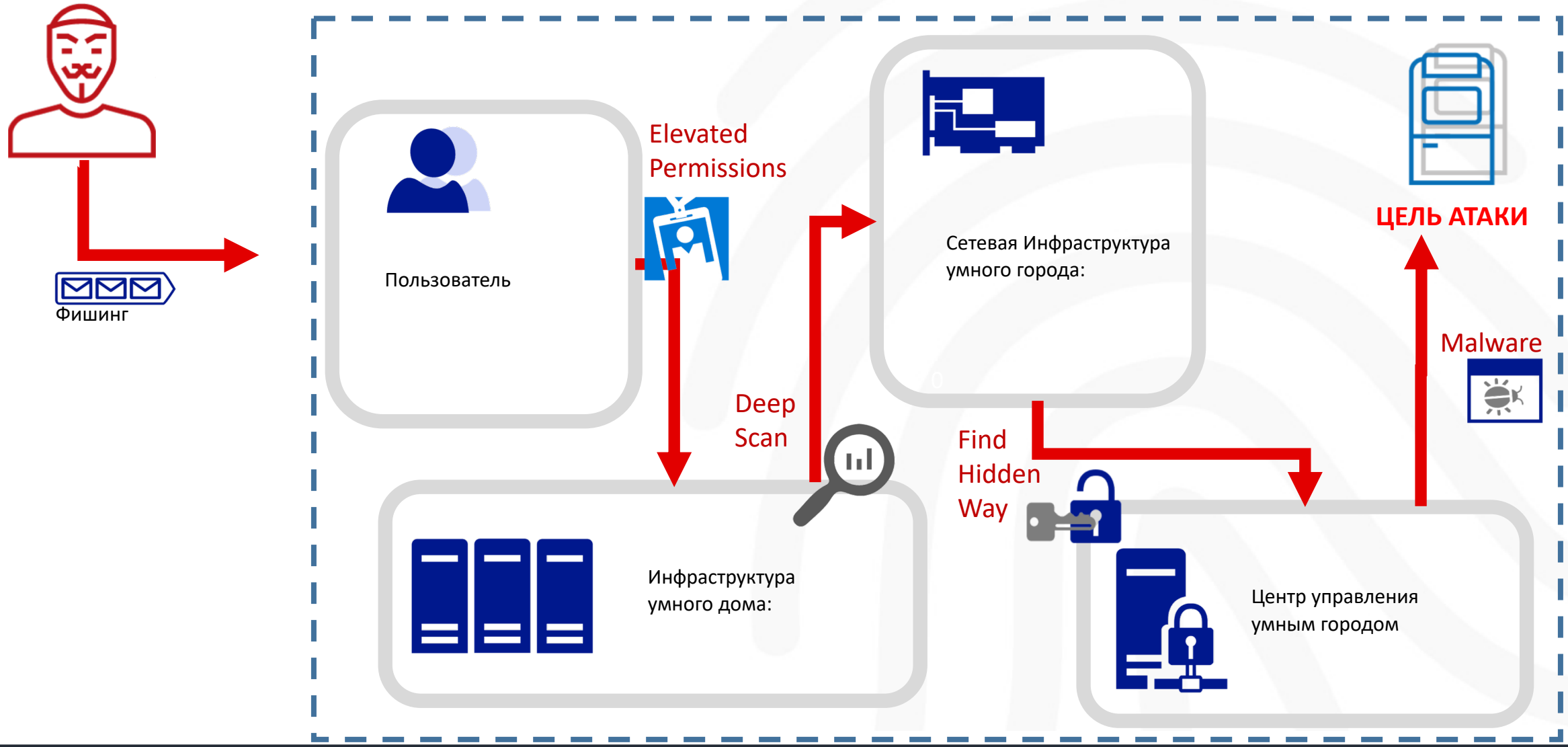
145 МЛН

ключей SSH

689 МЛН

SSL-сертификатов

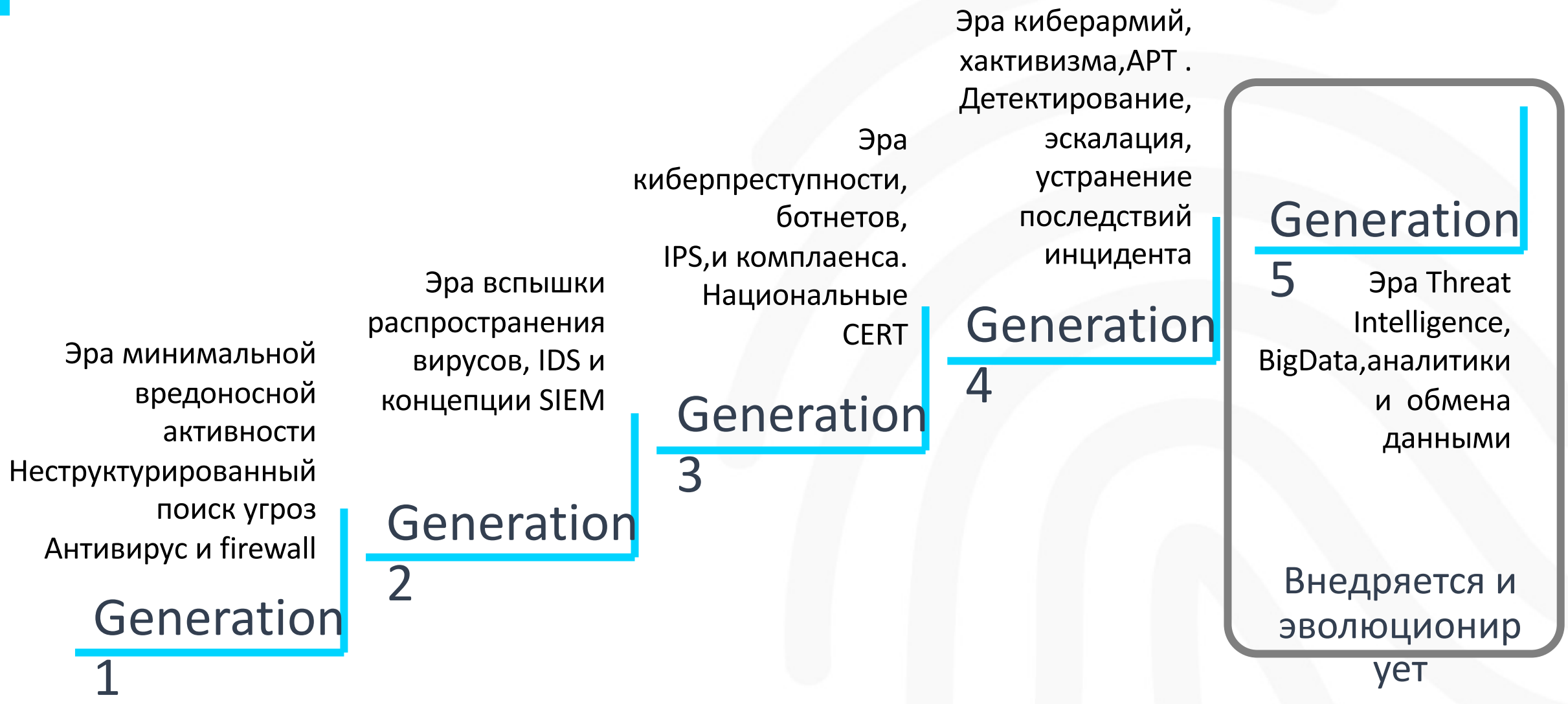
Пример: Получение доступа к инфраструктуре



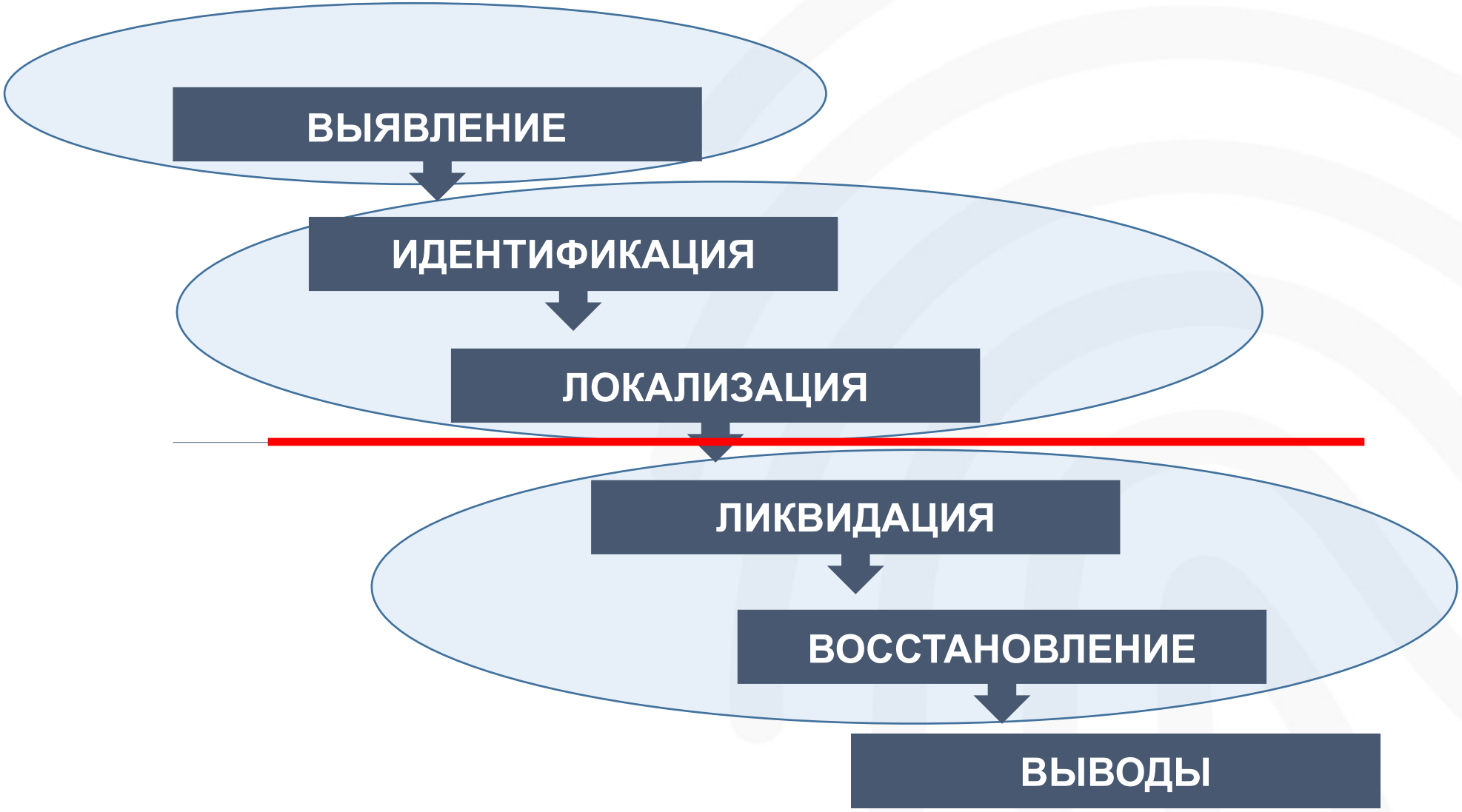
ЧАСТЬ 2

Реагирование на атаку

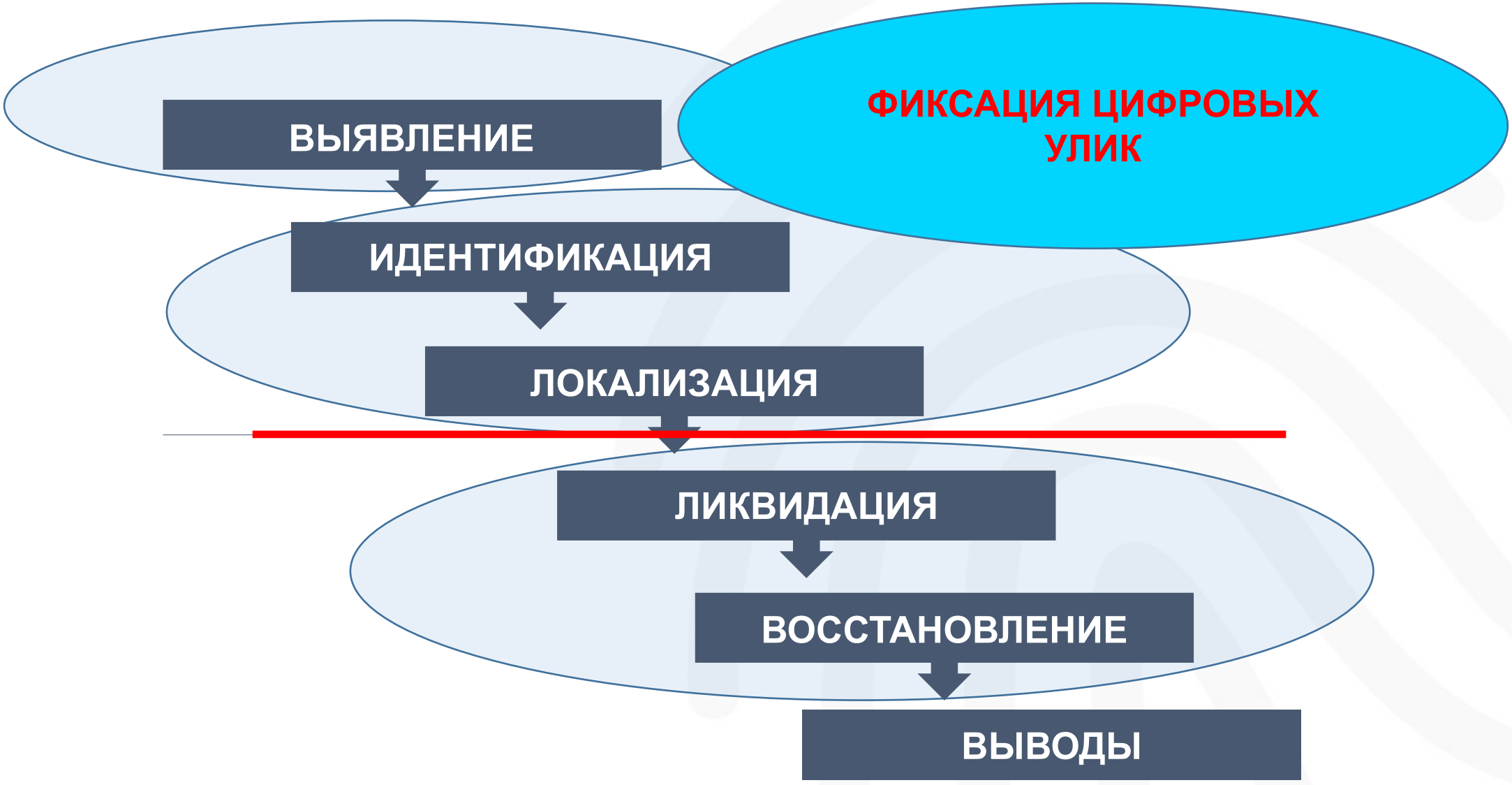
Мониторинг угроз и реагирование на инцидент



Стадии реагирования на инцидент



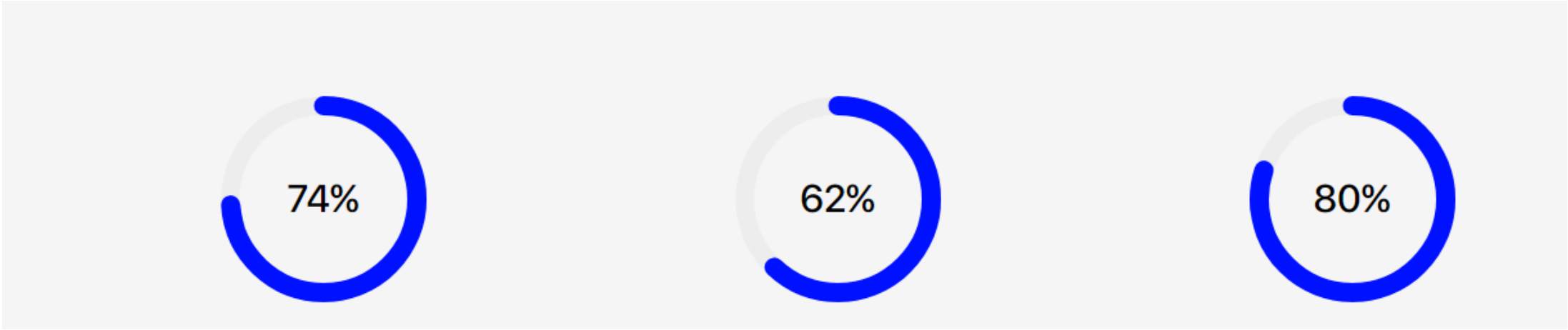
Стадии реагирования на инцидент



Стадии реагирования на инцидент

Подготовка к инциденту

Готовность инфраструктуры
Наличие инструментов
Квалификация персонала
Отлаженность процессов



не были готовы к реагированию на инцидент

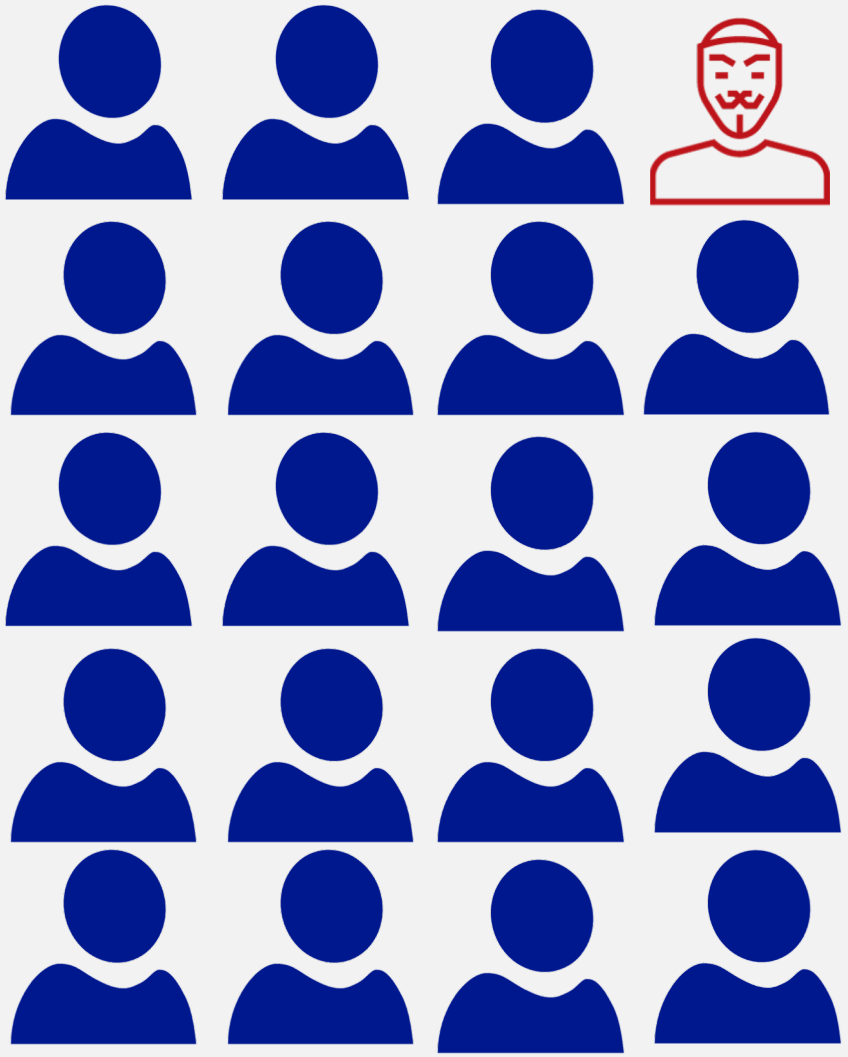
не способны централизованно управлять сетью

не имели достаточной глубины журналирования

ЧАСТЬ 3

Дискуссионные вопросы защиты цифровой личности

Как не навредить легитимным пользователям?



Атаки мошенников

<1%

>99%

Активность легитимных пользователей

Что мешает построению системы реагирования?

Отсутствие компетентного персонала	**57,7%**
Слишком много разрозненных инструментов	**43,0%**
Проблемы в процессах и playbook реагирования	**36,8%**
Проблемы взаимодействия команд	**30,2%**
Высокие требования у сотрудников	**25,0%**
Регуляторы и прочие правовые вопросы	**9,2%**

Международный характер угроз

На пресс-конференции в Джакарте было объявлено о том, что операция Night Fury успешно завершена: киберполиция Индонезии совместно с Интерполом и Group-IB объявили о задержании участников преступной группы, заразивших JavaScript-снифферами сотни онлайн-магазинов в Австралии, Бразилии, Великобритании, Германии, Индонезии, США и других странах мира.

Кто защитит цифровую личность?

Ваше мнение имеет значение!

Сергей Золотухин

Zolotukhin@group-ib.com

+7 906 093 3517