Kaspersky
Security Day
2021

Сервисы реагирования на инциденты ИБ

Константин Сапронов,
руководитель отдела оперативного решения инцидентов

kaspersky

Процесс реагирования на инцидент информационной безопасности

- Тренинги
- Проектирование SOC

- Обнаружение целевых атак
- MDR

- Сервисы расследования, реагирования и анализа вредоносного ПО

Сервисы реагирования «Лаборатории Касперского»

Мы предлагаем ряд сервисов, чтобы помочь организациям в реагировании на инциденты, расследовании инцидентов и анализе вредоносного ПО

Варианты обслуживания

- Подписка на реагирование на инциденты
- Экстренное реагирование по запросу

Анализ вредоносного ПО

Анализ вредоносного ПО

Файл

Хеш сумма

URL, IP адрес, домен

Отчет по анализу:

- Мета данные объекта
- Активность на файловой системе
- Сетевая активность
- Вредоносное поведение
- Создаваемые на системе артефакты
- Рекомендации по удалению и восстановлению

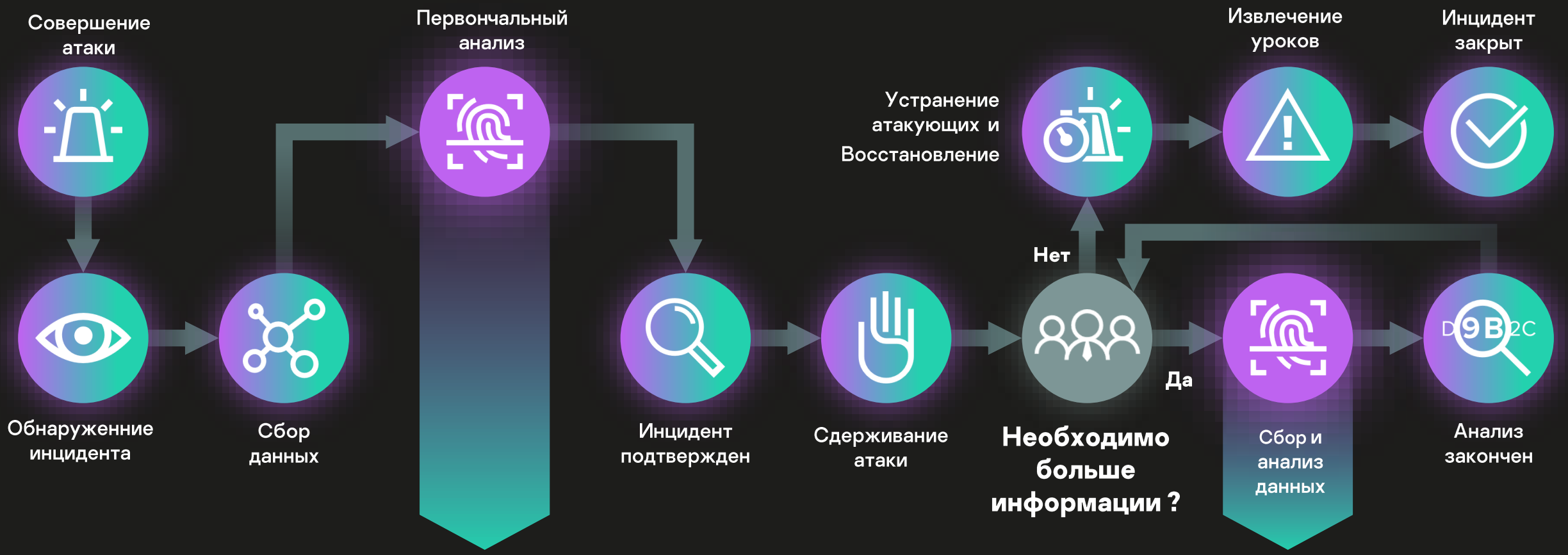
Вредоносный объект

Анализ

Отчет

Сервисы расследования и реагирования на инциденты

Этапы расследования



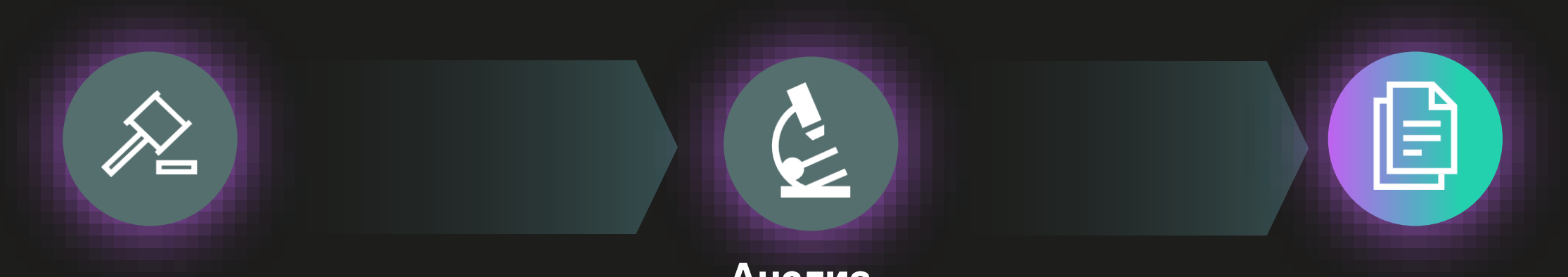
Первоначальный анализ:

- Начальные индикаторы атаки
- Оценка уровня угрозы
- Шаги по первоначальному реагированию
- Набор дополнительных данных на анализ

Полноценное расследование помогает установить полную картину атаки:

- Список скомпрометированных активов
- Вредоносная активность атакующих
- Первоначальная точка компрометации
- TTP атакующих

Детальный анализ улик



Сбор улик

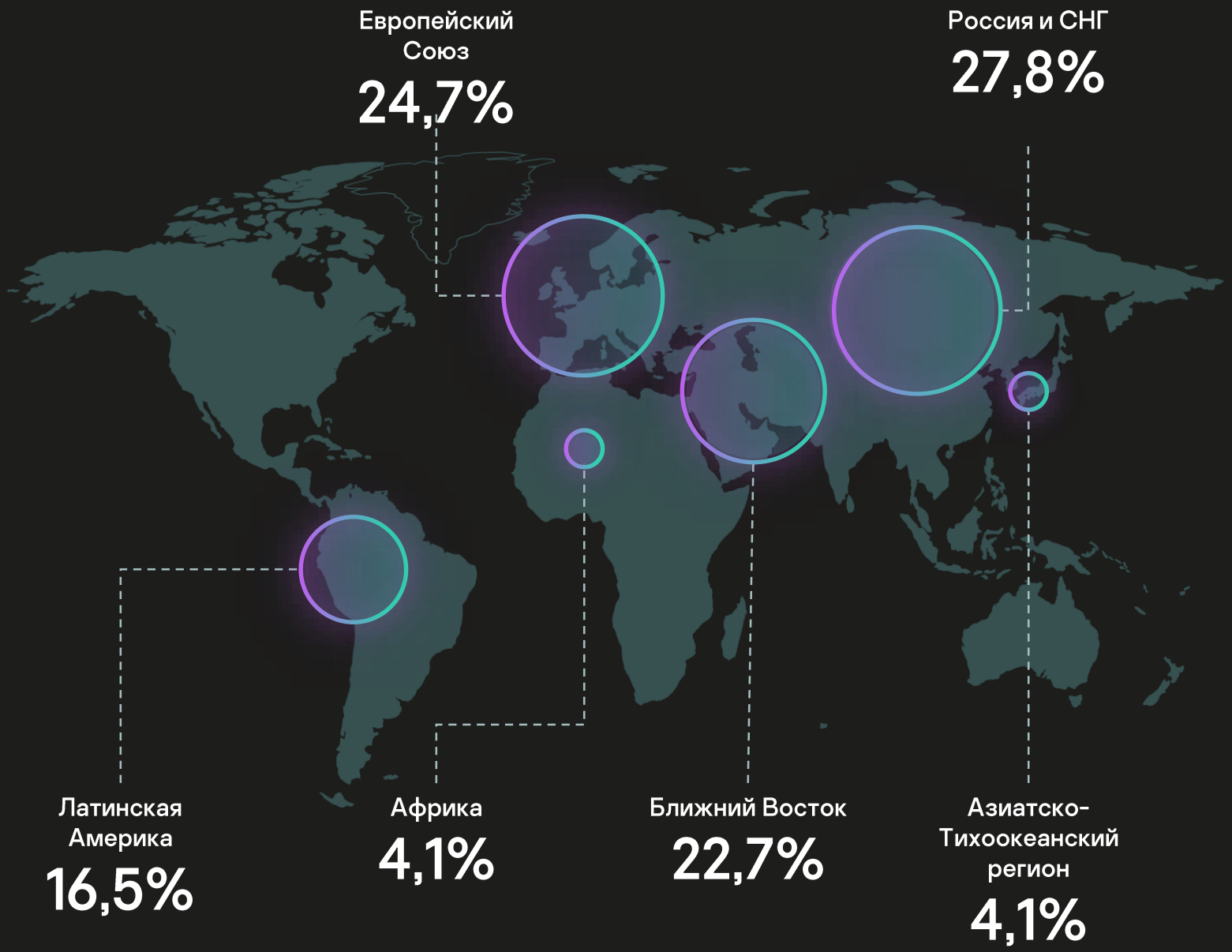
- HDD image
- Log files
- Network traffic
- Memory dump
- ...

Анализ данных

Отчет

- Хронология событий в течении атаки
- Описание инструментов атакующих, включая описание вредоснного ПО
- Список индикаторов компрометации
- Рекомендации по устранению последствий атаки и восстановлению инфраструктуры

География оказания сервисов по реагированию в 2020 году



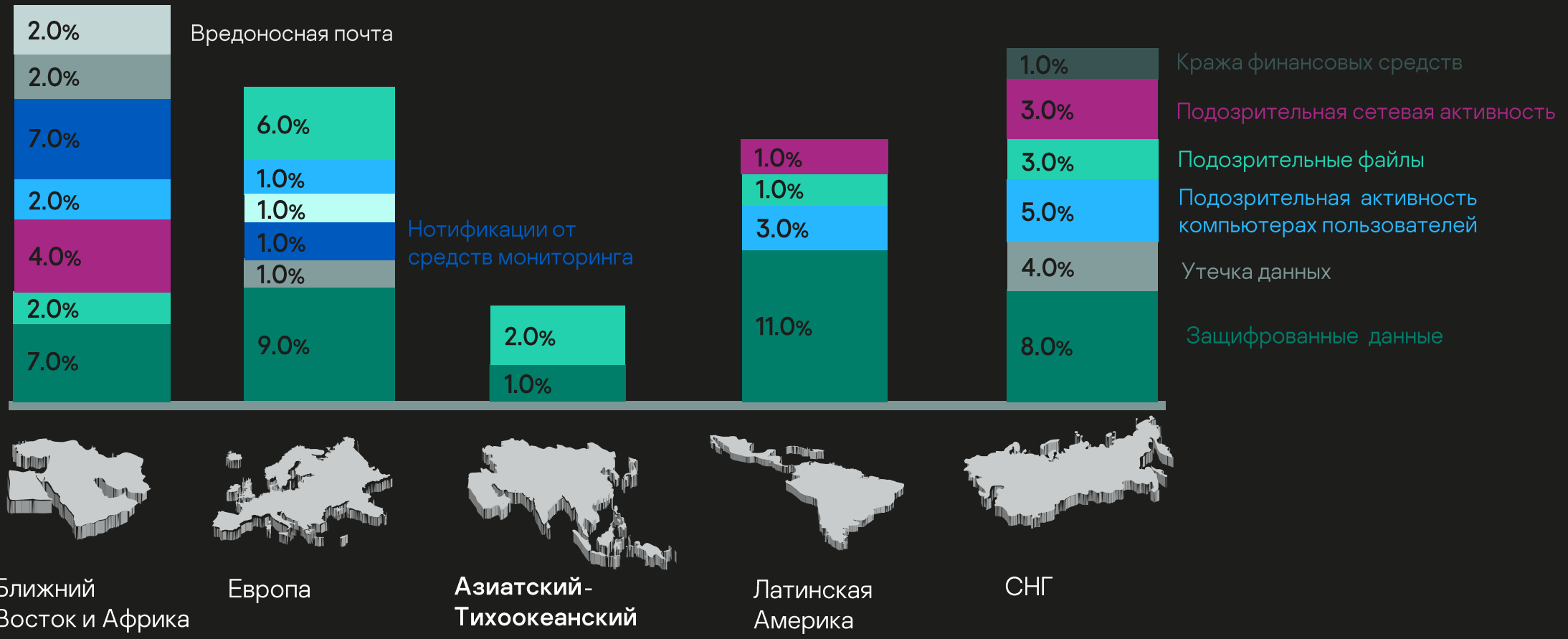
100+ инцидентов в 2020

97% удаленно

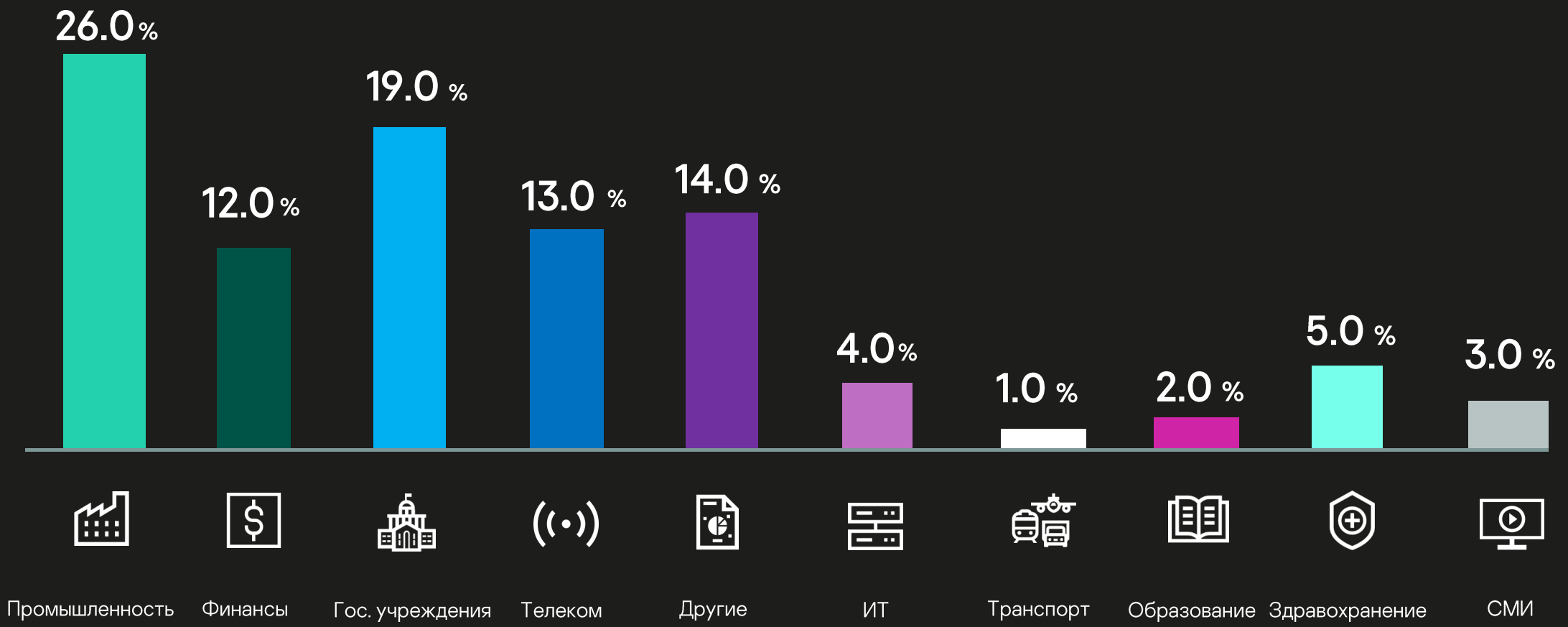
Международная группа экстренного реагирования на инциденты (GERT):

- Америка
- Европа
- Ближний Восток
- Россия

Инциденты в регионах

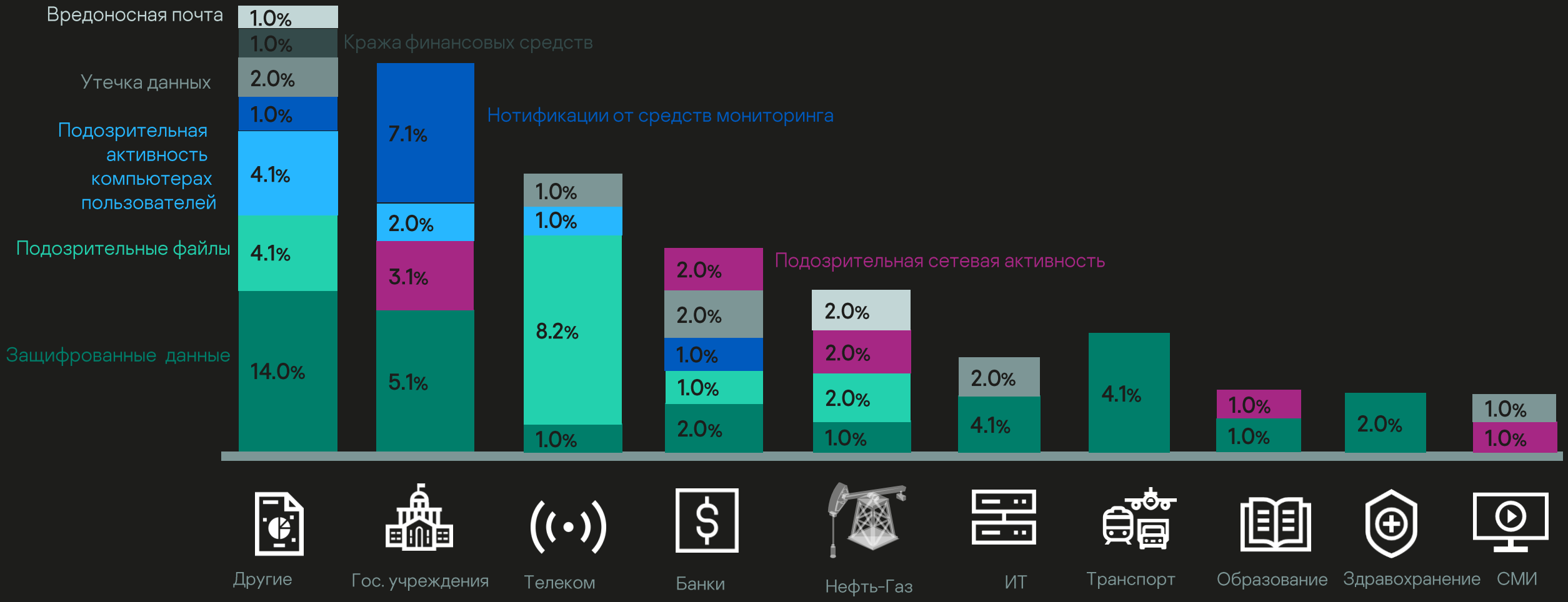


Сервисы реагирования «Лаборатории Касперского» по отраслям



Источник: отчет «Лаборатории Касперского» о реагировании на инциденты, 2020 г.

Инциденты в секторах экономики

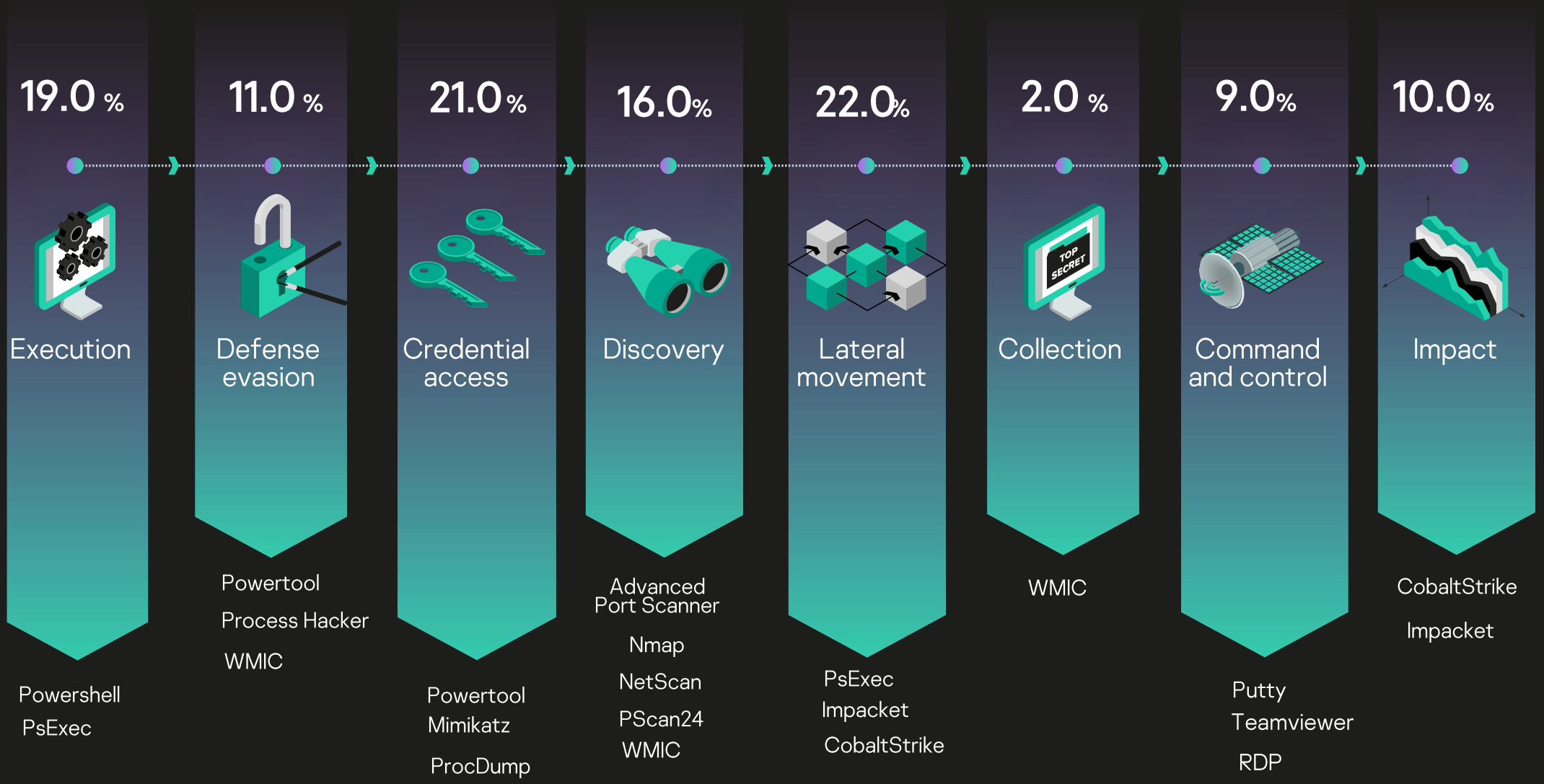


Начальный вектор атаки

Самый популярный начальный вектор атаки – вредоносная электронная почта

cve-2019-11510
cve-2020-0796
cve-2018-8453
cve-2017-0144
cve-2017-11317
cve-2020-0787
cve-2017-8464
cve-2019-0604

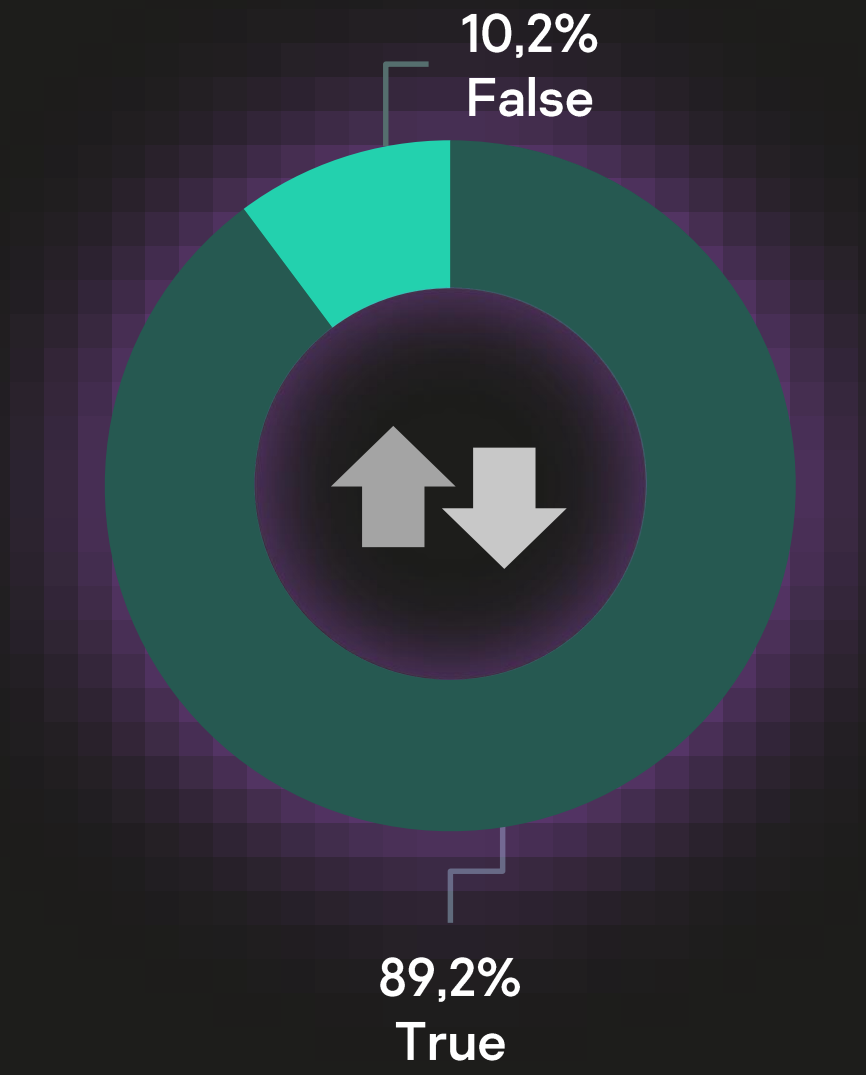
Использование легального ПО в тактиках по классификации MITRE



Ложные срабатывания

Обнаруженные инциденты

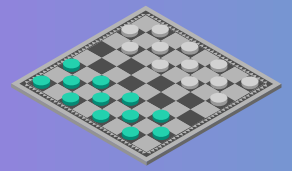
Защифрованные файлы
32.7 %
Подозрительные файлы
19.1 %
Подозрительная сетевая активность,
Подозрительная активность на машинах пользователей
12.7 %
Нотификация от систем мониторинга 8.2 %
Утечки данных , 6.4 %
Неизвестные причины 6.1%
Вредоносные e-mail, 4.5 %
Кража финансовых средств, 1.8%

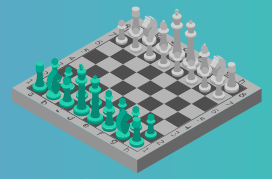


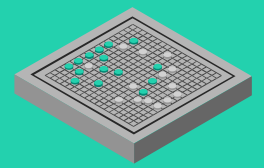
Ложные срабатывания

Подозрительная сетевая активность
33.3%
Подозрительная активность на машинах пользователей
25.5 %
Нотификация от систем мониторинга
16.7 %
Подозрительные файлы
16.7 %
Утечка данных
8.3 %

Длительность атак

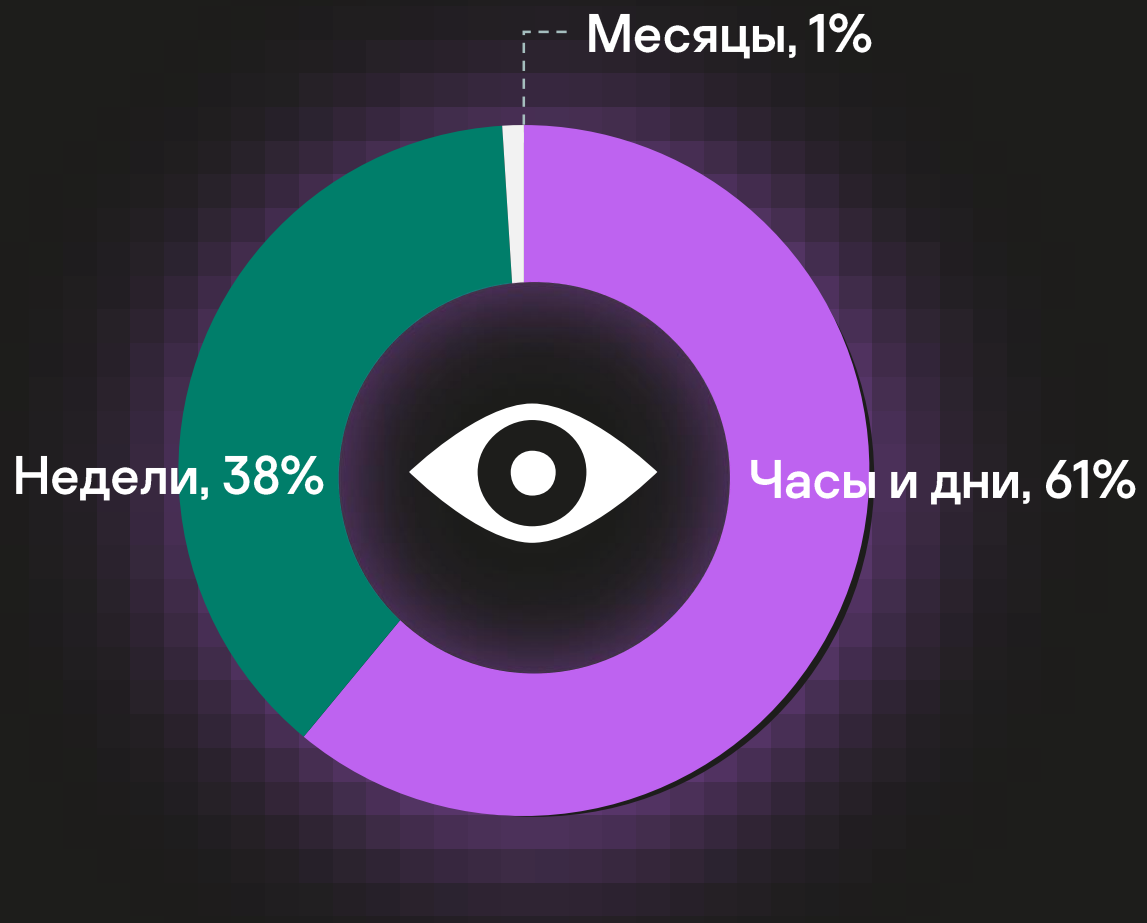

Часы и дни


Недели

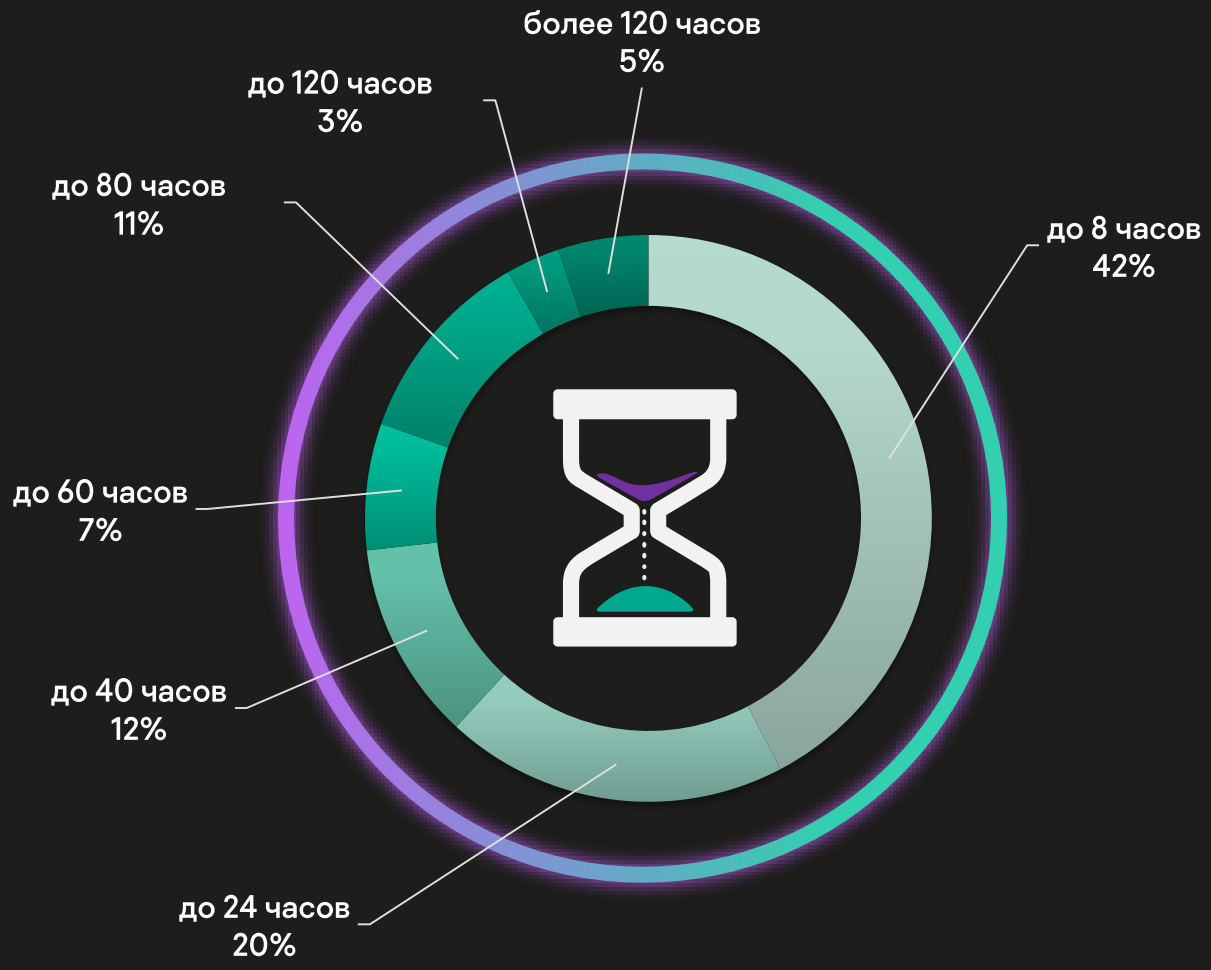

Месяцы и больше

Тип атаки	Быстрые атаки	Атаки средней длительности	Длительные атаки
Угрозы	Заражение шифровальщиком	Кража финансовых средств	Кибер шпионаж и кража данных
Длительность атаки	62%	16%	22%
Длительность проведения расследования	Часы и дни 61 %	Недели 38 %	Месяцы 1 %

Сроки и время на проведение расследований



Сроки проведения
расследования и реагирования



Время затраченное на расследование

Заключение и рекомендации

- Каждый инцидент должен быть полностью расследован, приступать к устранению последствий можно только после определения начального вектора атаки
- Неправильное применение средств мониторинга ведет к увеличению ложных срабатываний, увеличению потока событий и как следсвие пропуску событий о реальной атаке
- Отсутствие практик по своевременной установке обновлений безопасности ведет к увеличению рисков ИБ
- Политики аудита должны обеспечивать возможность выявления инцидентов и их расследований

Спасибо!

kaspersky