БАНК САНКТ-ПЕТЕРБУРГ

Банк высокой культуры

Практический подход к построению процесса управления угрозами

Как было раньше

Отбили атаку и хорошо?

- Примерно несколько сотен группировок
- Ограниченное количество тактик
- Количество объектов для атаки превышает количество атакующих на несколько порядков

Обязательно необходимо выяснить, кто атаковал и зачем.

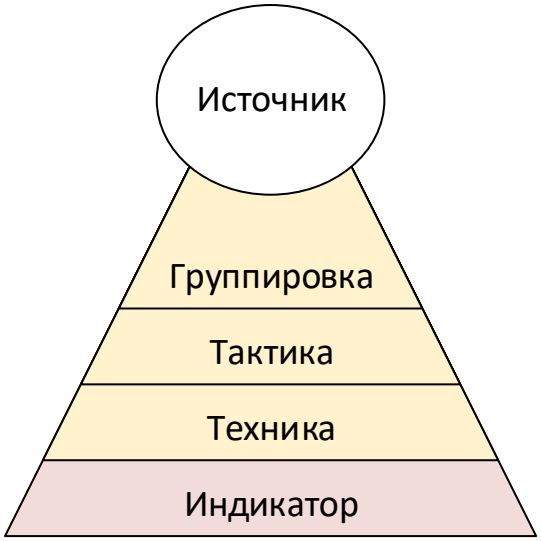
Описание угрозы

База сигнатур

Индикаторы компрометации

TI

Что такое атрибуция

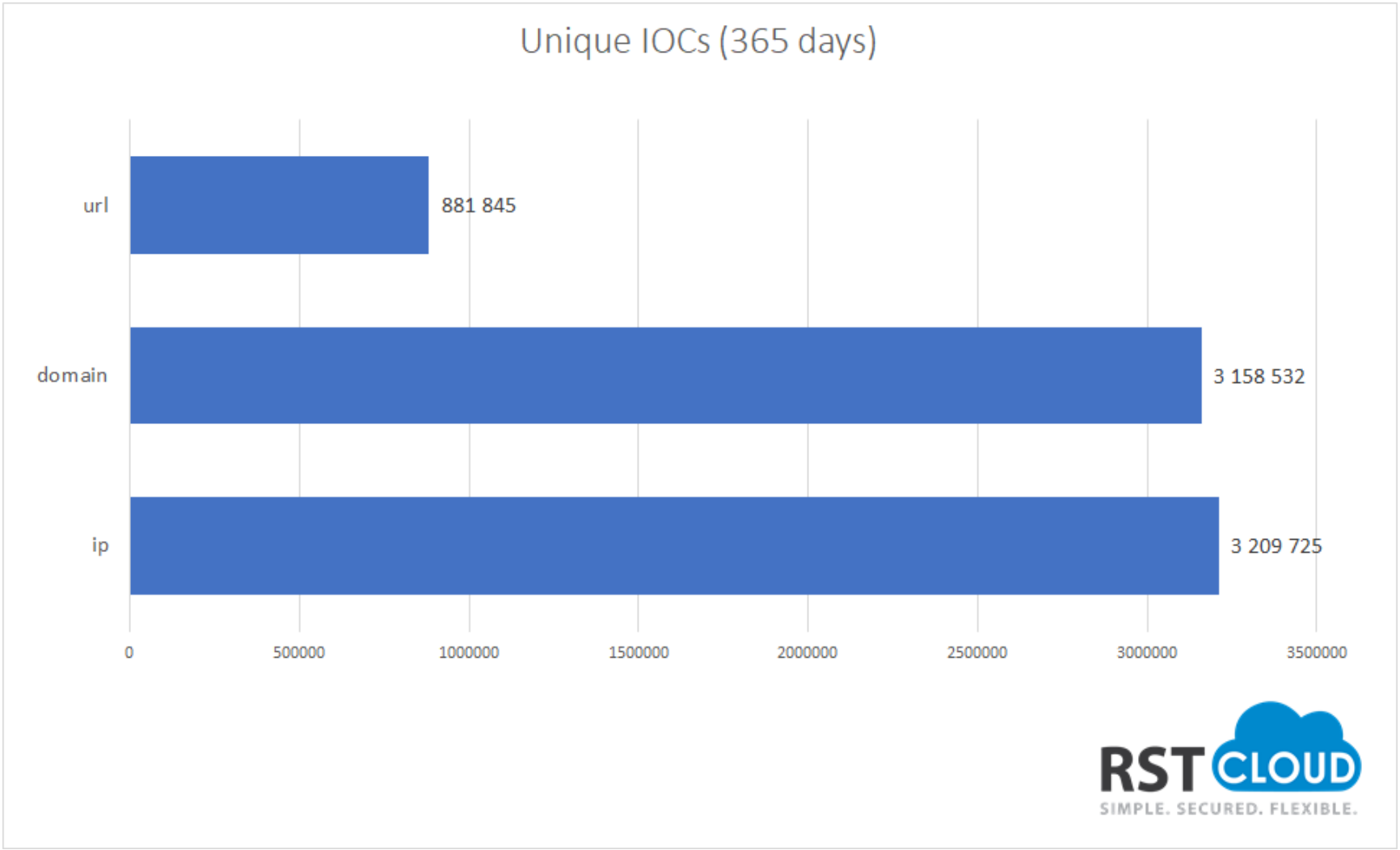


Контекст — дополнительная информация для анализа индикаторов компрометации, которая позволяет ответить на вопросы, кто как и зачем использовал какую-то технику, на которую указывает данный индикатор.

Индикатор компрометации — базовый технический признак атаки. Например, IP-адрес, с которого была зафиксирована рассылка управляющих команд в ботнет-сеть, или хеш-сумма файла вируса-вымогателя.

MITRE ATT&CK

Немного статистики



Еще немного статистики от RVision

Источник: CIRCL (www.circl.lu) Данные за 2020 и 2021

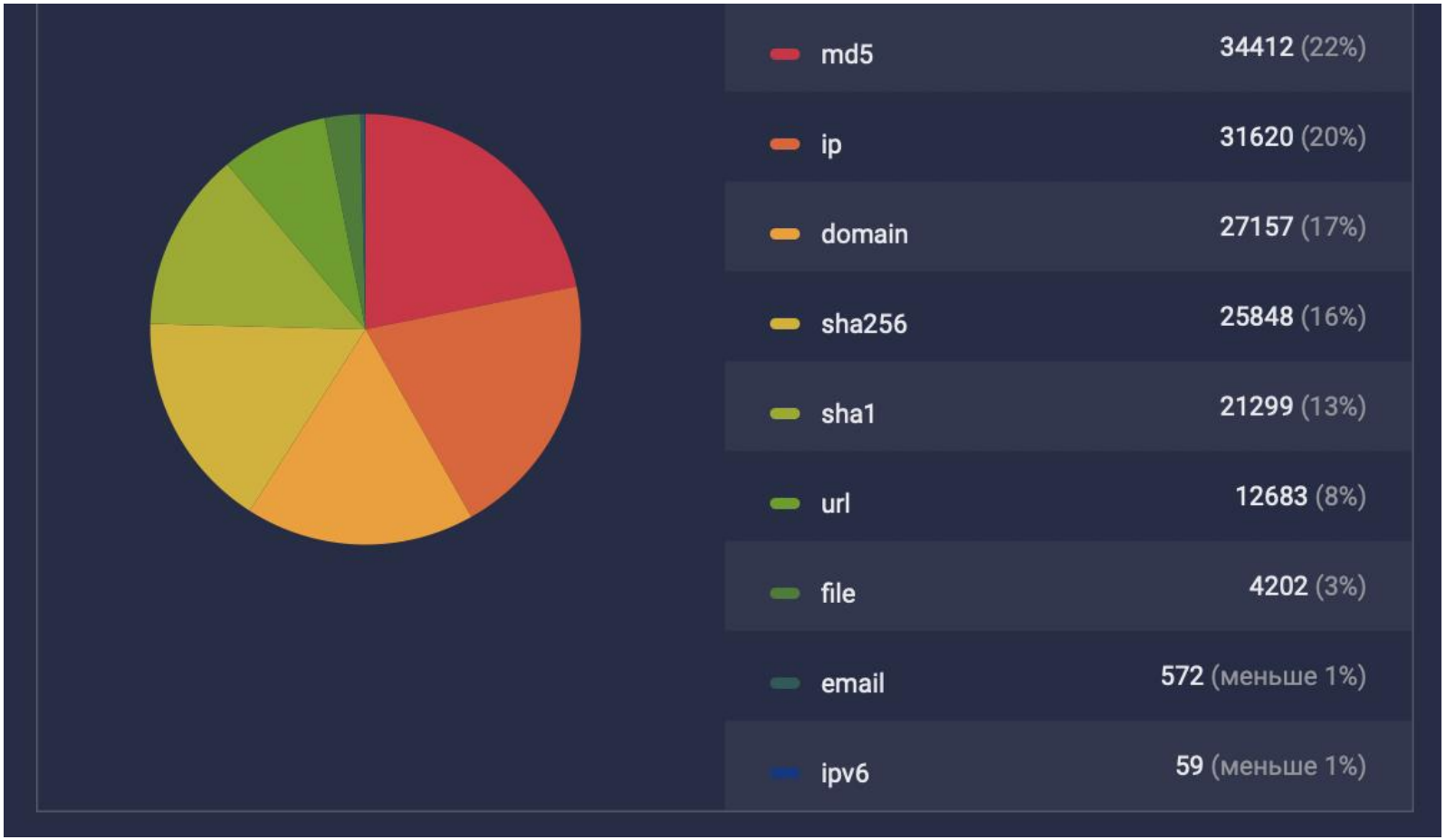
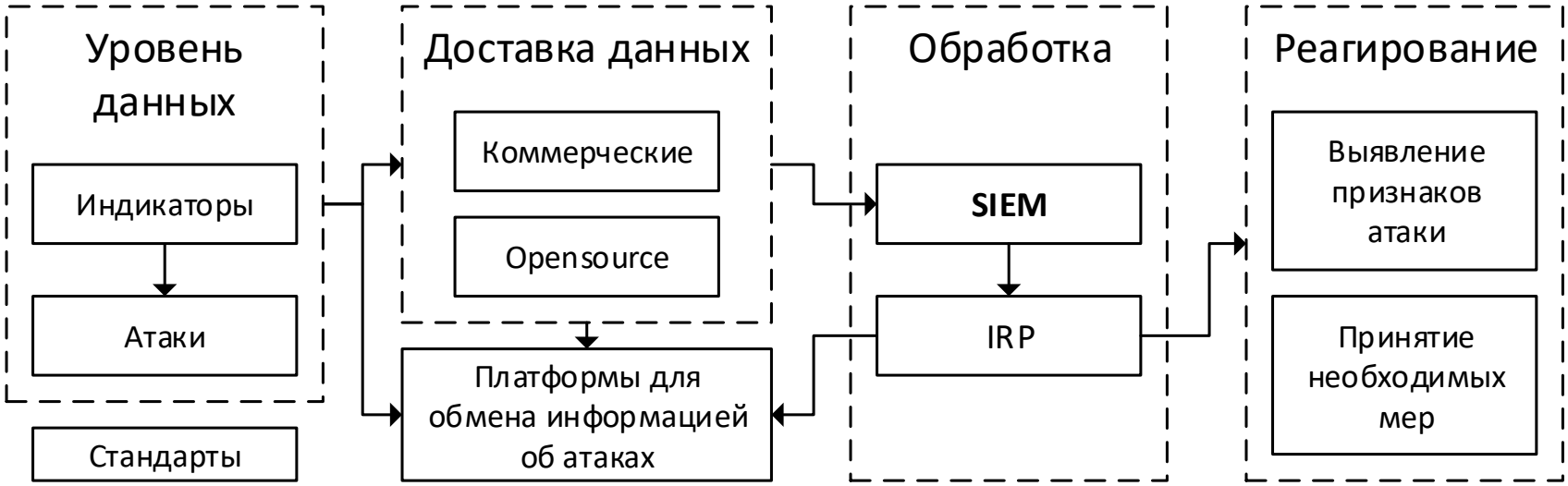


Схема доставки данных

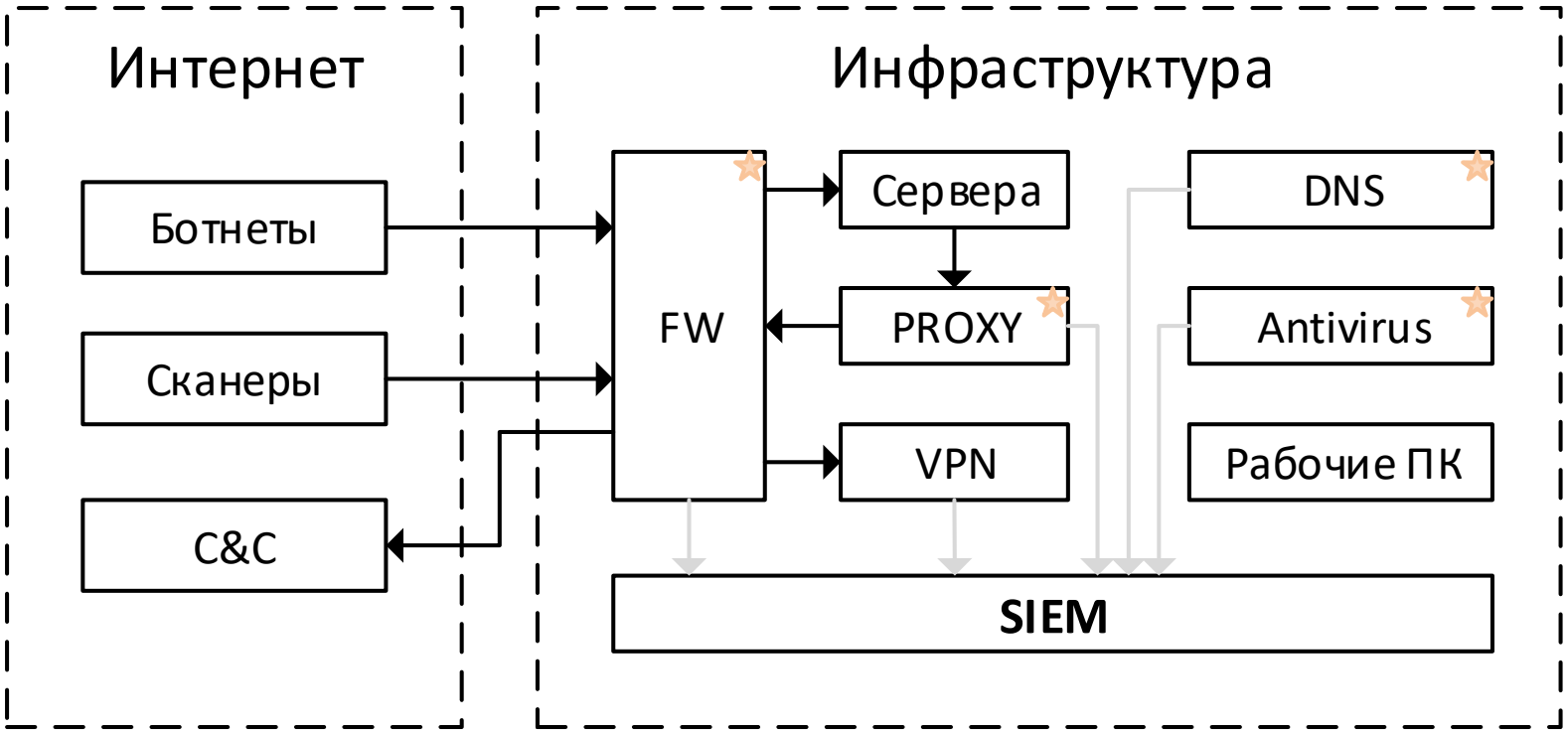


Преимущества	Недостатки
1. Экономия на ресурсах 2. Единое окно для аналитиков	Проблема форматов – ваша проблема. + поддержка интеграций

Источники данных об угрозах

Наименование	Обоснование
Коммерческий источник	Достаточный объем индикаторов с приемлемым качеством
Локальный CERT (ФинЦЕРТ)	Небольшое количество специфических индикаторов с высоки качеством
MISP	Платформа активно развивается
Фиды от ИБ компаний и экспертов	Для понимания общей статистики по угрозам (техникам и тактикам)
Бесплатные фиды	Если есть свободное время на анализ ☺

Обязательные точки контроля



Сценарии использования данных TI

Индикатор	Источник	Сценарий
IP	FW	Сканирование периметра
IP	FW	Атака ботнета
IP, DNS	FW, DNS, PROXY	Заражение внутреннего хоста
Hash	Antivirus	Заражение внутреннего хоста
Hash	Песочница	Рассылка вредоносного ПО

Преимущества дополнительного анализа

№	Преимущество
1	Приоритизация инцидентов.
2	Обогащение инцидентов дополнительной информацией
3	Выявление новых техник и тактик проведения атак. Повышение осведомленности об актуальных угрозах
4	Выявление известных типов атак на ранних стадиях

Существующие сложности

№	Преимущество
1	Отсутствие единой глобальной платформы для обмена информацией об атаках.
2	Малое количество компаний обменивается данными об атаках.
3	Не все используют единые словари для описания атак
4	Несколько форматов данных для описания индикатора с атрибуцией

БАНК
САНКТ-ПЕТЕРБУРГ

Банк высокой культуры

Беляков И.А.
bia@bspb.ru

Спасибо за внимание!