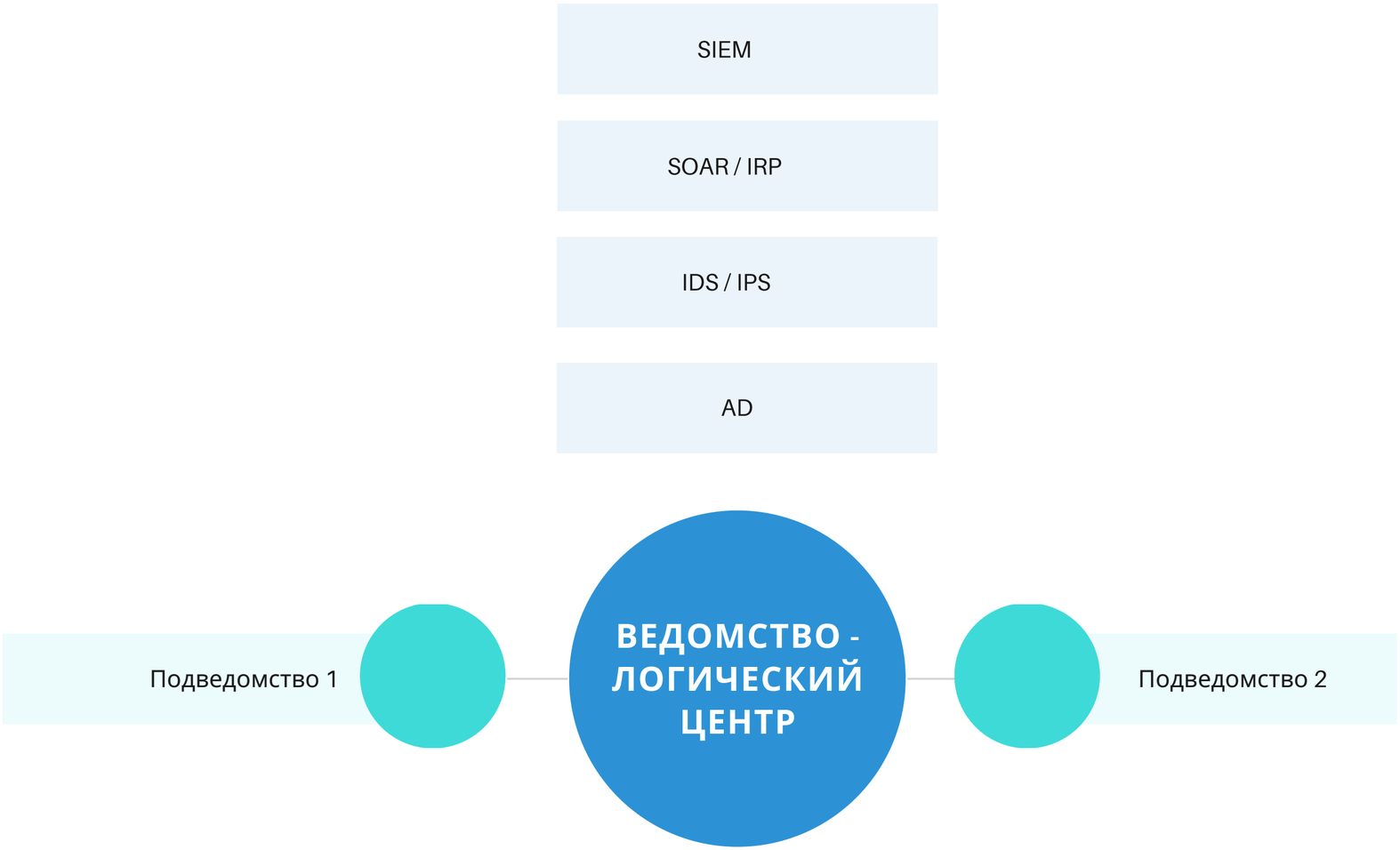
СЕВЕРО-ЗАПАДНЫЙ IT-ХАБ

Концепция **SOC** со сжатием текстовых логов

Карта сервисов



Security information and event management

IDS vs. IPS


IDS - инструменты
мониторинга и обнаружения
Эти инструменты
не действуют самостоятельно
Пользователь или сторонняя
система регулирует показатели IDS
Читает сетевые пакеты
Сличает с базами
известных угроз
IPS - управляющая система
Управляющая система
принимает или отвергает пакеты
руководствуясь правилами
Рекомендовано обновлять
базу данных IPS
списками новых угроз
строго регулярно

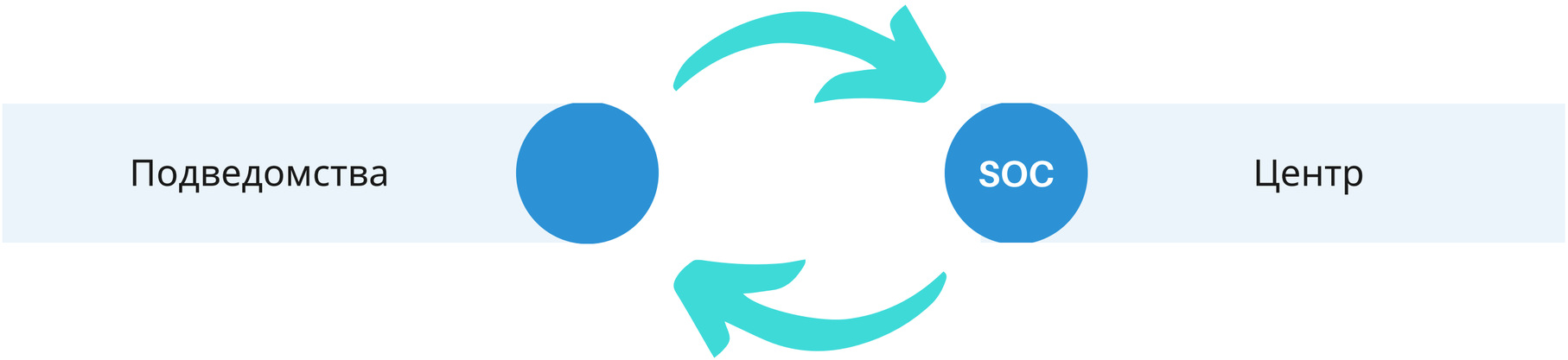
Чувствительная информация

- Личная переписка сотрудников
- Почта и почтовые вложения
- Документы на общих сетевых ресурсах
- Данные аутентификации
- Личные данные сотрудников
- И иные чувствительные данные...

Преимущества и особенности предлагаемого решения

Система совершенствования политик

Отчеты работы систем мониторинга подведомств

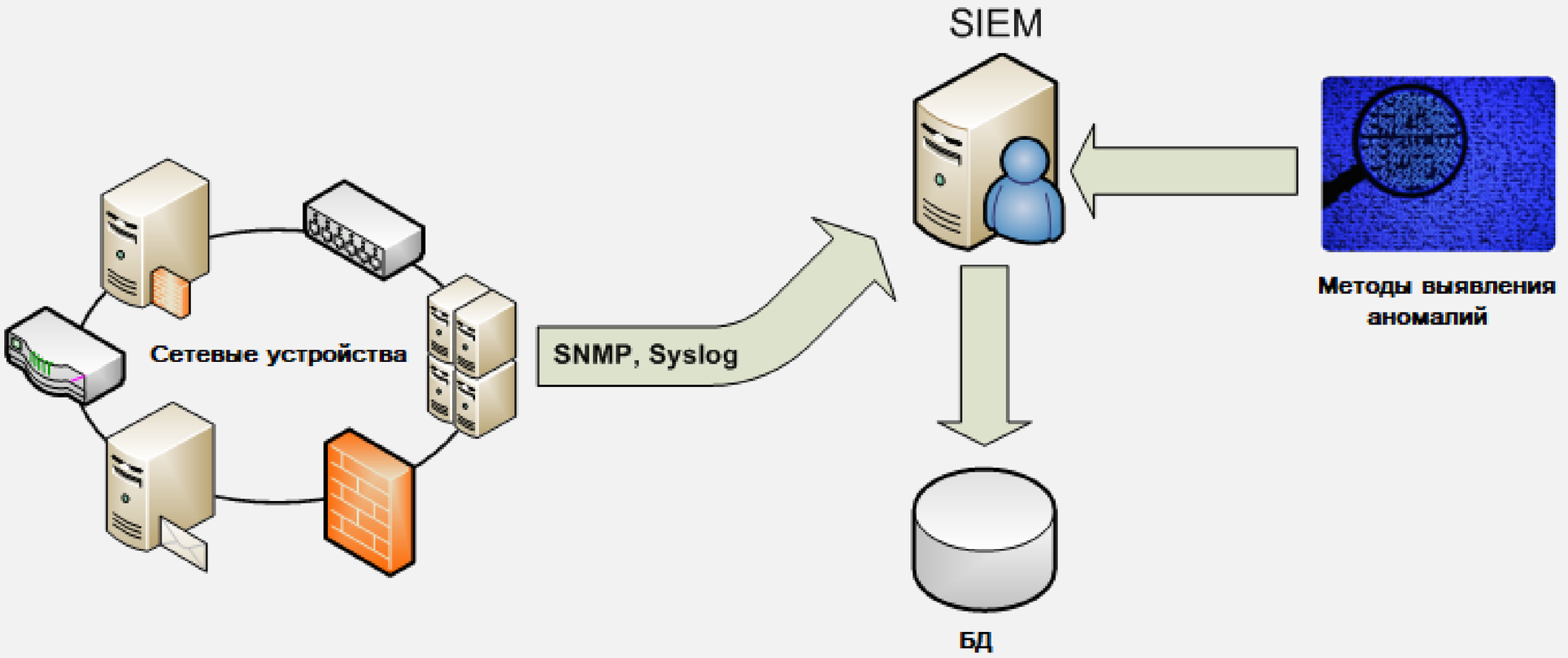


Усовершенствованные политики на основе отчетов SIEM

IRP


Регистрация инцидента
Первоочередные действия
Расследование и восстановление
Эскалация и уведомления
Блокирование угрозы
Проверка системы
Сбор свидетельств
Востановление из резервной копии
Директор по ИБ
Руководитель подразделения
Выключение хоста
Проверка запущенных процессов
Сбор списка уязвимостей на хосте
Подготовка справки по инциденту

Анализ логов



Сжатие логов

```
6c 6f 67 33 44 FF 48 38 F3 55 66 34 A5 73 C3
6c 6f 67 56 78 FF 48 38 F3 34 6g 34 A5 73 C3
6c 6f 67 36 76 FF 48 38 F3 23 87 34 A5 73 C3
6c 6f 67 33 44 FF 48 38 F3 55 66 34 A5 73 C3
6c 6f 67 56 78 FF 48 38 F3 34 6g 34 A5 73 C3
6c 6f 67 36 76 FF 48 38 F3 23 87 34 A5 73 C3
6c 6f 67 33 44 FF 48 38 F3 55 66 34 A5 73 C3
6c 6f 67 56 78 FF 48 38 F3 34 6g 34 A5 73 C3
6c 6f 67 36 76 FF 48 38 F3 23 87 34 A5 73 C3
6c 6f 67 33 44 FF 48 38 F3 55 66 34 A5 73 C3
6c 6f 67 56 78 FF 48 38 F3 34 6g 34 A5 73 C3
6c 6f 67 36 76 FF 48 38 F3 23 87 34 A5 73 C3
6c 6f 67 33 44 FF 48 38 F3 55 66 34 A5 73 C3
6c 6f 67 56 78 FF 48 38 F3 34 6g 34 A5 73 C3
6c 6f 67 36 76 FF 48 38 F3 23 87 34 A5 73 C3
6c 6f 67 33 44 FF 48 38 F3 55 66 34 A5 73 C3
6c 6f 67 56 78 FF 48 38 F3 34 6g 34 A5 73 C3
6c 6f 67 36 76 FF 48 38 F3 23 87 34 A5 73 C3
```

```
6c 6f 67 2f 0 2f 3 2f 2a
FF 48 38 F3 2f 5 2f 4 2f 2a
34 A5 73 C3 2f B 2f 4 2f 25 0 2D 14
44 D4 38 99 2f B 2f 4 2f 25 15 2D 30
33 44 55 66
56 78 34 6g
36 76 23 87
33 44 55 66
56 78 34 6g
36 76 23 87
33 44 55 66
56 78 34 6g
36 76 23 87
33 44 55 66
56 78 34 6g
36 76 23 87
33 44 55 66
56 78 34 6g
```

Сжатие логов

2206 Б ----> 752 Б

Файл уменьшился в
2,9 раза

Алгоритм не подвержен статистической трактовке при обратной операции

Алгоритм не подвержен переполнению словаря алгоритма Лемпеля — Зива — Велча

Экономический эффект от внедрения

Сокращение издержек на разнообразие конфигураций.

Сокращение расходов на обучение новых ИТ-сотрудников.

Сокращение издержек при информационных потерях.

- Сетевые технологии позволяют расширить область действия системы на всю территорию действия Российского законодательства.
- Количество узлов системы ограничивается только мощностями пропускных линий связи.
- Адаптируемость под задачи различных ведомств а так же под задачибизнеса различногоуровня развития.

Информация о реализации

- Сроки: *примерно год*
- Стоимость: *стандартная стоимость программы внедрения ПО*
- Порядок внедрения: *закупка необходимого оборудования и ПО, введение пользователей в AD, настройка ПО и выстраивание правил и политик, корректировка политик на основе первого времени работы - повторить на оставшихся подведомствах, наладить коммуникацию между удаленными подразлелениями и центром*

Команда

- **Анастасия Коновалова**
- pochtaplay2013@gmail.com
- *https://t.me/Eimay*

- **Илья Макаренко**
- nikolsson.elias@yandex.ru
- *https://t.me/Elias*

- **Лев Мирзагалямов**
- liev.03@mail.ru
- *https://t.me/NIIIIAUU*

Источники:

https://www.anti-malware.ru/analytics/Market_Analysis/incident-response-platforms-irp-in-russia

https://www.anti-malware.ru/practice/methods/SIEM-and-IRP-systems-with-repeated-cyber-incidents

https://www.varonis.com/blog/?p=11421