ОБРПО. Лекция 6 Network Security Checklist

ТЮРИН КАЙ АНДРЕЕВИЧ

1. Политики

Acceptable Use Policy

Internet Access Policy

Email and Communications Policy

Network Security Policy

Remote Access Policy

BYOD Policy

Encryption Policy

Privacy Policy

2. Endpoint (конечные устройства)

Список серверов/рабочих машин

- Имя, цель, IP, время создания, время жизни, ОС, ответственный человек

Ответственный за каждый сервер/рабочую машину

- Человек или команда, которые знают, для чего нужен сервер, обновляют его и могут расследовать аномалии, с ним происходящие

Соглашение о наименовании

- Может помочь в критических ситуациях быстро опознать устройство

Корректная сетевая конфигурация

- DNS, DHCP,

IPAM (IP Address Management)

- Помогает понять, что за машина стоит за каждым IP адресом (даже Excel-таблица)

Endpoint (2)

Патчи
- Очень важно доставлять обновления безопасности

Антивирусы
- На всех машинах, с центральной консолью управления

Host Intrusion Prevention / Firewall
- Корректная конфигурация сетевых экранов и инструментов предотвращения вторжений

Удалённое управление
- Зафиксировать единый метод удалённого управления и придерживаться его

ИБП / Генераторы
- Для обеспечения целостности серверов

Endpoint (3)

Все машины помещать в домен

- Все машины внутренней сети должны быть в домене для централизованного управления

Переименовать аккаунт админа и установить сильный пароль

- Переименование – не самая надёжная защита, но с ним лучше, чем без него

Использовать группы пользователей по-максимуму

- И стараться избегать пользователей вне групп

Organizational Unit

- И Group Policy Object, GPO

Отчёты на единую консоль управления

- Проверять, что отправляются

Endpoint (4)

Выключать ненужные сервисы

- Сохраните память, CPU, электроэнергию и уменьшите поверхность атаки

Корректная конфигурация SNMP

- Проверять обязательно

Проверять, что все необходимые агенты установлены

- Бэкап-агенты, лог-агенты и т.д.

Бэкапы

- Если что-то стоит того, чтобы сделать, оно стоит того, чтобы сделать резервную копию

Восстановление из бэкапа

- Бэкапу нельзя доверять, если из него никогда не восстанавливались

Endpoint (5)

Сканирование уязвимостей

- Злоумышленник будет сканировать вашу сеть на наличие уязвимостей, так сделайте это раньше него

Проверка серверов перед выводом в продакшн

- В качестве обязательного пункта перед запуском

3. Сетевое оборудование

Список оборудования

- Имя, расположение, серийный номер, ответственный

Конфигурация

- Стандартная для каждого типа устройства для облегчения администрирования

IPAM

- Для расследования инцидентов

Патчинг

- Своевременное обновление

Удалённый доступ

- Как можно более защищённый протокол (SSH 2), обязательно выключить telnet и SSH 1. Использовать ключи или стойкие пароли

Сетевое оборудование (2)

Резервное копирование
- Конфигурации необходимо бэкапить

Сканирование на уязвимости
- Для своевременного обнаружения

VLANs
- Использовать VLAN’ы для разделения разных сегментов сети

Закрыть ненужные порты
- Все неиспользуемые порты должны быть закрыты

Firewalls
- Неявные запреты, явные разрешения: правильной политикой по умолчанию является «запретить всё»

Логи
- Журналировать всевозможные потенциальные нарушения безопасности

4. Сканирование на уязвимости

Регулярное сканирование

- Например, каждую неделю

Мониторинг изменений

- Каждое новое сканирование должно сравниваться с предыдущим

Сканирование не только внешнего периметра, но и внутреннего

- Внешнее сканирование – еженедельное, внутреннее – ежемесячное

5. Backups

Ротация

- Бэкапы не должны «съесть» всё место и перестать создаваться

Уничтожение старых хранилищ

- Для того, чтобы с них нельзя было восстановить информацию

Обеспечение физической безопасности для хранилищ

- В случае хранения и передачи

Шифрование

- В случае, если подразумевается передача хранилищ или доступ к ним извне

Регулярное восстановление

- Хотя бы раз в месяц

6. Удалённый доступ

Необходимо

1. Выбрать способ удалённого управления

2. Выдать разрешения тем, кому это необходимо

3. Убедиться, что другие способы запрещены

4. Настроить многофакторную аутентификацию

5. Регулярно проводить аудит (проверять наличие логинов ночью или тогда, когда их не должно быть)

6. Защитить соединение при помощи VPN

7. Беспроводная сеть

SSID

- SSID точки доступа следует скрывать и делать его неассоциируемым с организацией

Шифрование

- Как можно более сильное (желательно WPA2 Enterprise, ни в коем случае не WEP)

Аутентификация

- Рекомендуется использовать 802.1x, чтобы только доверенные устройства могли подключиться.

Создание гостевой сети

- Для подключения недоверенных устройств

BYOD

- Создайте политику “Bring Your Own Device".

8. Email

Установить средства анализа почты для:

1. Обнаружения спама

2. Обнаружения фишинговых писем

3. Обнаружения вредоносного ПО

Анализироваться должны как входящие, так и исходящие письма

9. Доступ к интернету

Шифрование

- Фильтровать незашифрованные соединения

Сканирование на предмет наличия вредоносного ПО

- Сканировать всё содержимое: загрузки, потоковые сервисы, содержимое страниц и т.д.

Блокирование портов

- Блокировать порты, которые могут позволить нарушить политику доступа к интернету (прокси, VPN и т.д.)

10. Общие файлохранилища

Убрать группы «everyone» и «authenticated users»

- Эти группы слишком широкие

Принцип наименьших привилегий

- Каждый пользователь должен иметь наименьшие привилегии, достаточные для работы

Группы

- Настраивать доступ не для конкретных пользователей, но для групп

11. Log correlation

В случае, если конечных устройств достаточно много, необходимо настроить сбор логов в единую систему для того, чтобы

1. получать к ним доступ из единого места и снизить вероятность что-то упустить

2. находить зависимые события в рамках некоторого инцидента

12. Время

Согласование времени на всех устройствах является важным для корректного мониторинга сети в целом.

Источник

Complete Network Security Checklist

https://www.titanhq.com/complete-network-security-checklist

Итого

Инвентаризация

Резервное копирование

Своевременное обновление

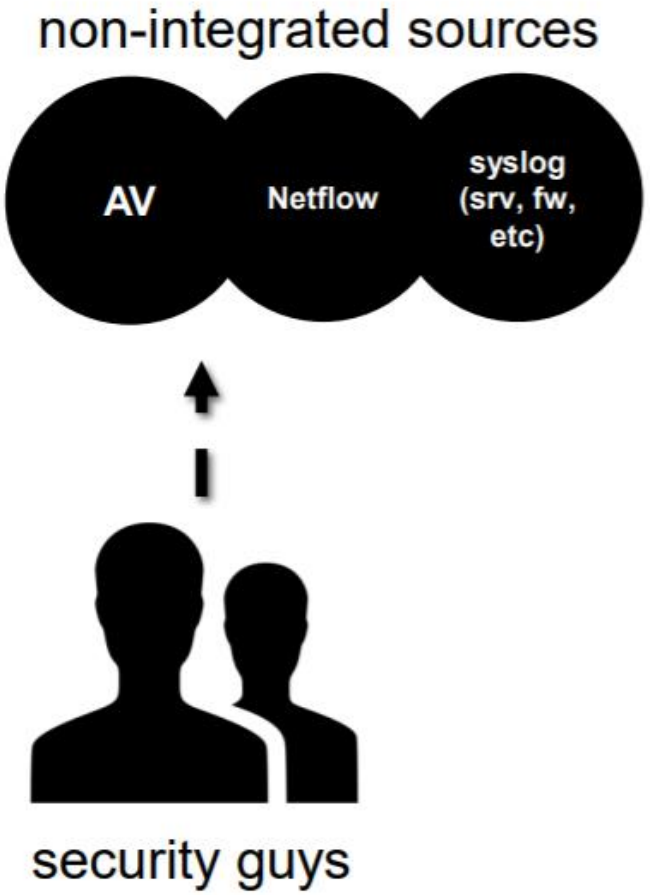
Разграничение прав с запретом по умолчанию

Регулярный мониторинг

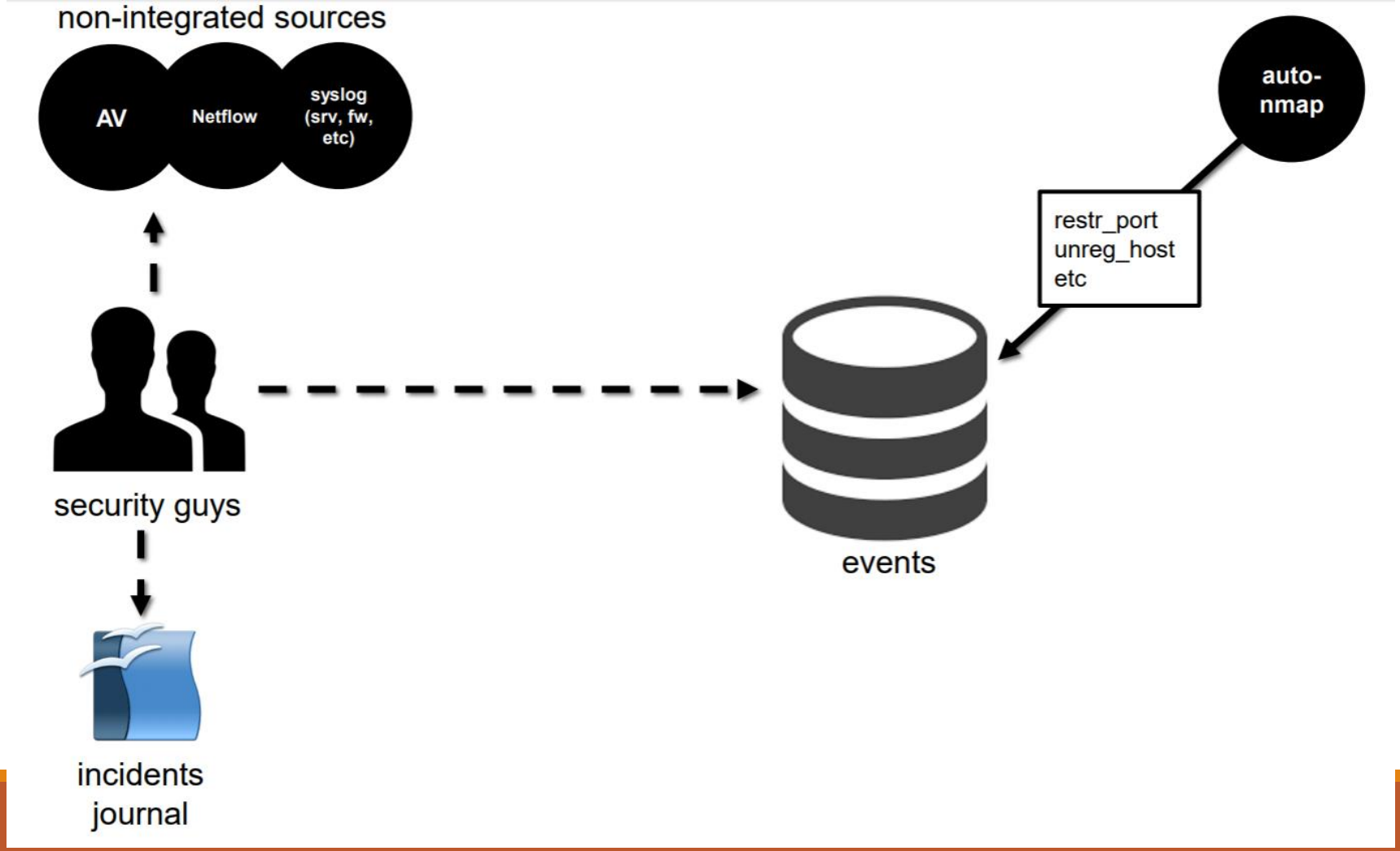
Один из ключевых принципов сегодня

Пытаемся не только предотвратить инцидент, но и **быстро отреагировать на его происхождение.**

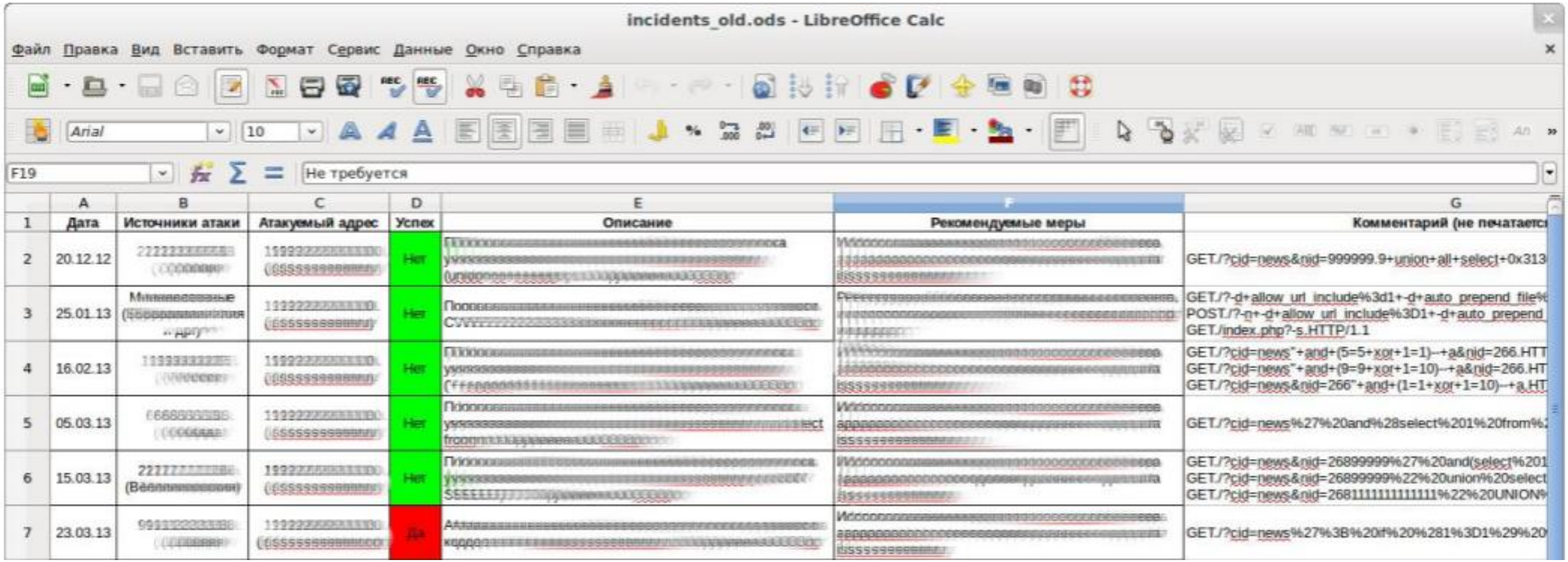
Как это обычно происходит в жизни?



Добавление автосканирования

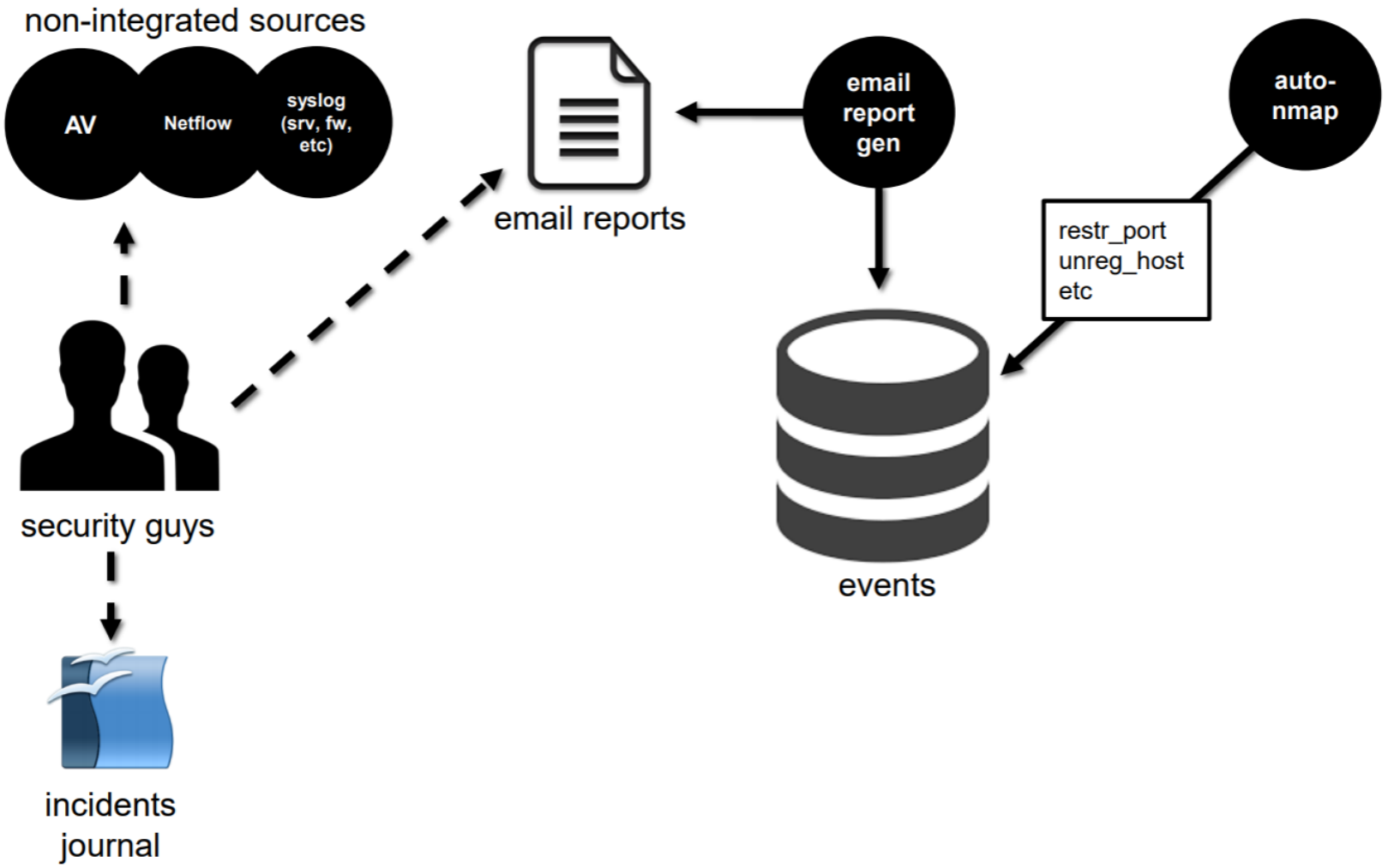


Вид журнала инцидентов

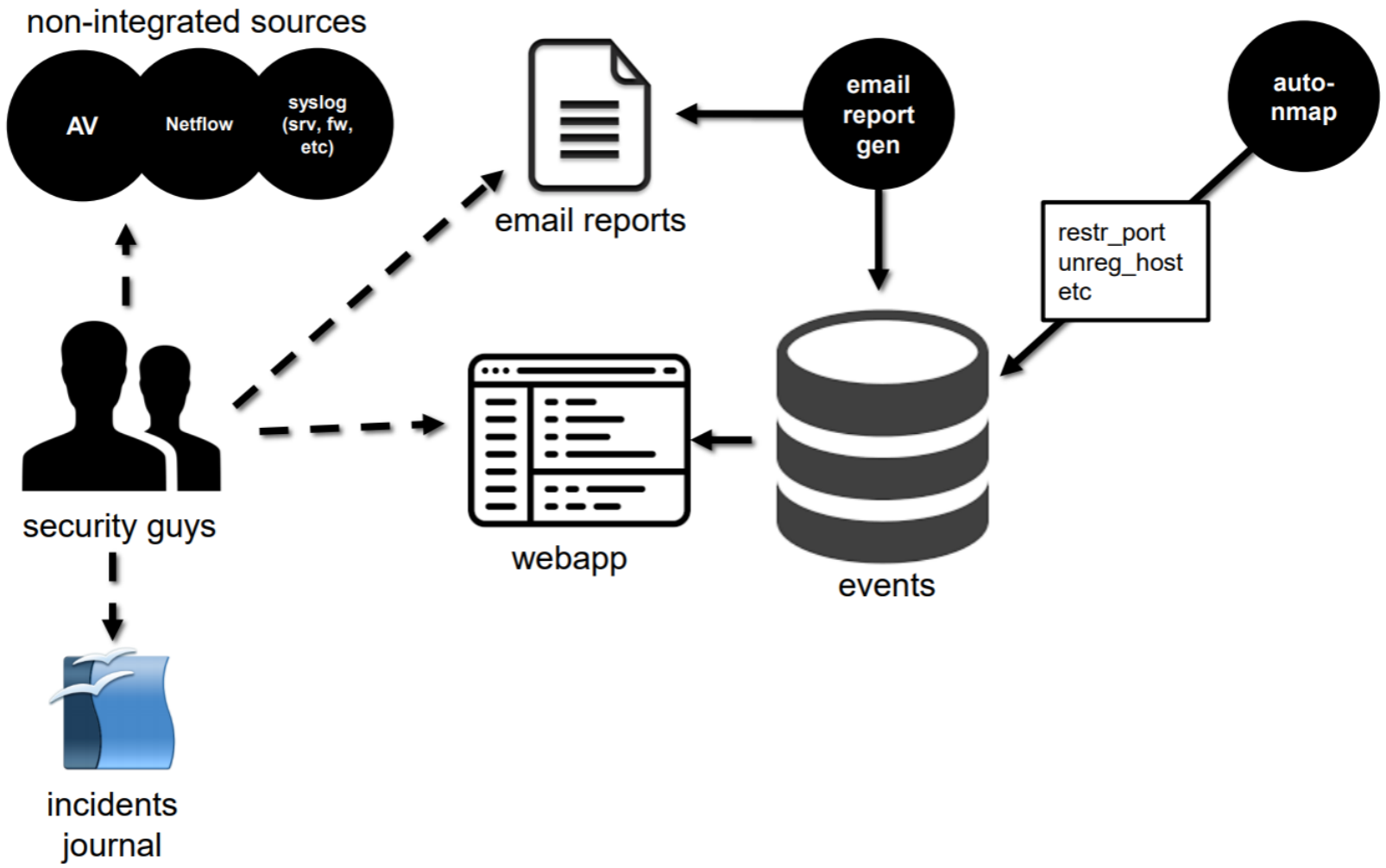


	A	B	C	D	E	F	G
1	Дата	Источники атаки	Атакуемый адрес	Успех	Описание	Рекомендуемые меры	Комментарий (не печатается)
2	20.12.12	[illegible]	[illegible]	Нет	[illegible]	[illegible]	GET /?cid=news&nid=999999.9+union+all+select+0x313
3	25.01.13	[illegible]	[illegible]	Нет	[illegible]	[illegible]	GET /?-d+allow_url_include%3d1+-d+auto_prepend_file% POST /?-n+-d+allow_url_include%3D1+-d+auto_prepend_ GET /index.php?-s HTTP/1.1
4	16.02.13	[illegible]	[illegible]	Нет	[illegible]	[illegible]	GET /?cid=news"+and+(5=5+xor+1=1)--+a&nid=266 HTT GET /?cid=news"+and+(9=9+xor+1=10)--+a&nid=266 HT GET /?cid=news&nid=266"+and+(1=1+xor+1=10)--+a HT
5	05.03.13	[illegible]	[illegible]	Нет	[illegible]	[illegible]	GET /?cid=news%27%20and%28select%201%20from%2
6	15.03.13	[illegible]	[illegible]	Нет	[illegible]	[illegible]	GET /?cid=news&nid=26899999%27%20and(select%201 GET /?cid=news&nid=26899999%22%20union%20select GET /?cid=news&nid=2681111111111111%22%20UNION%
7	23.03.13	[illegible]	[illegible]	Да	[illegible]	[illegible]	GET /?cid=news%27%3B%20if%20%281%3D1%29%20

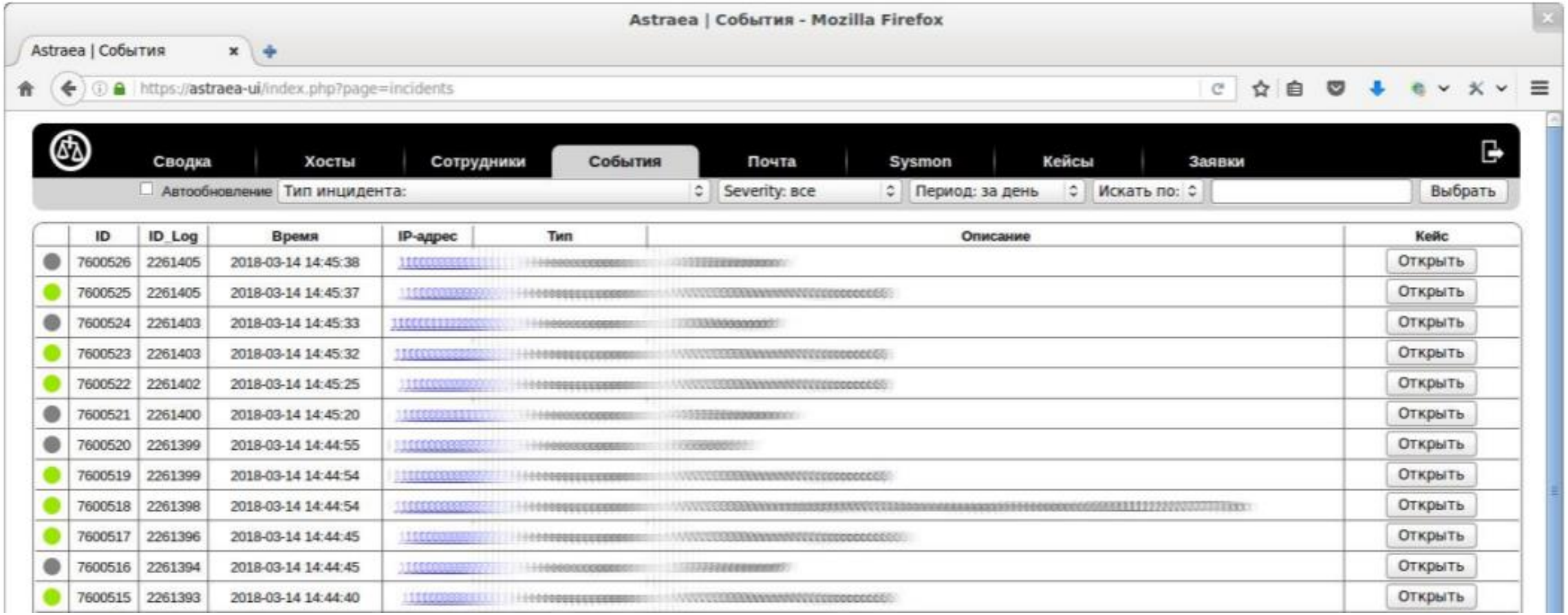
Добавление оповещения



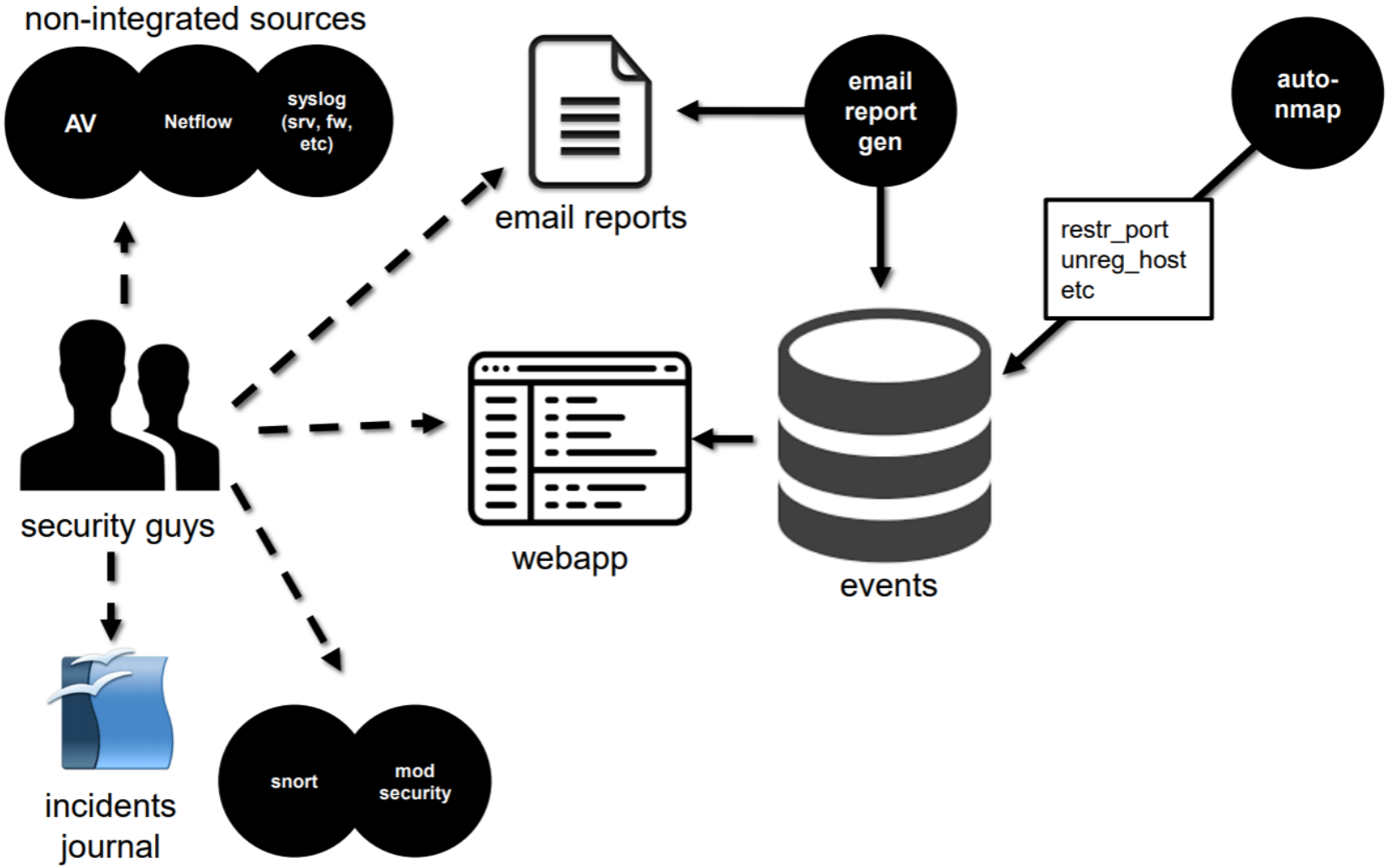
Добавление интерфейса



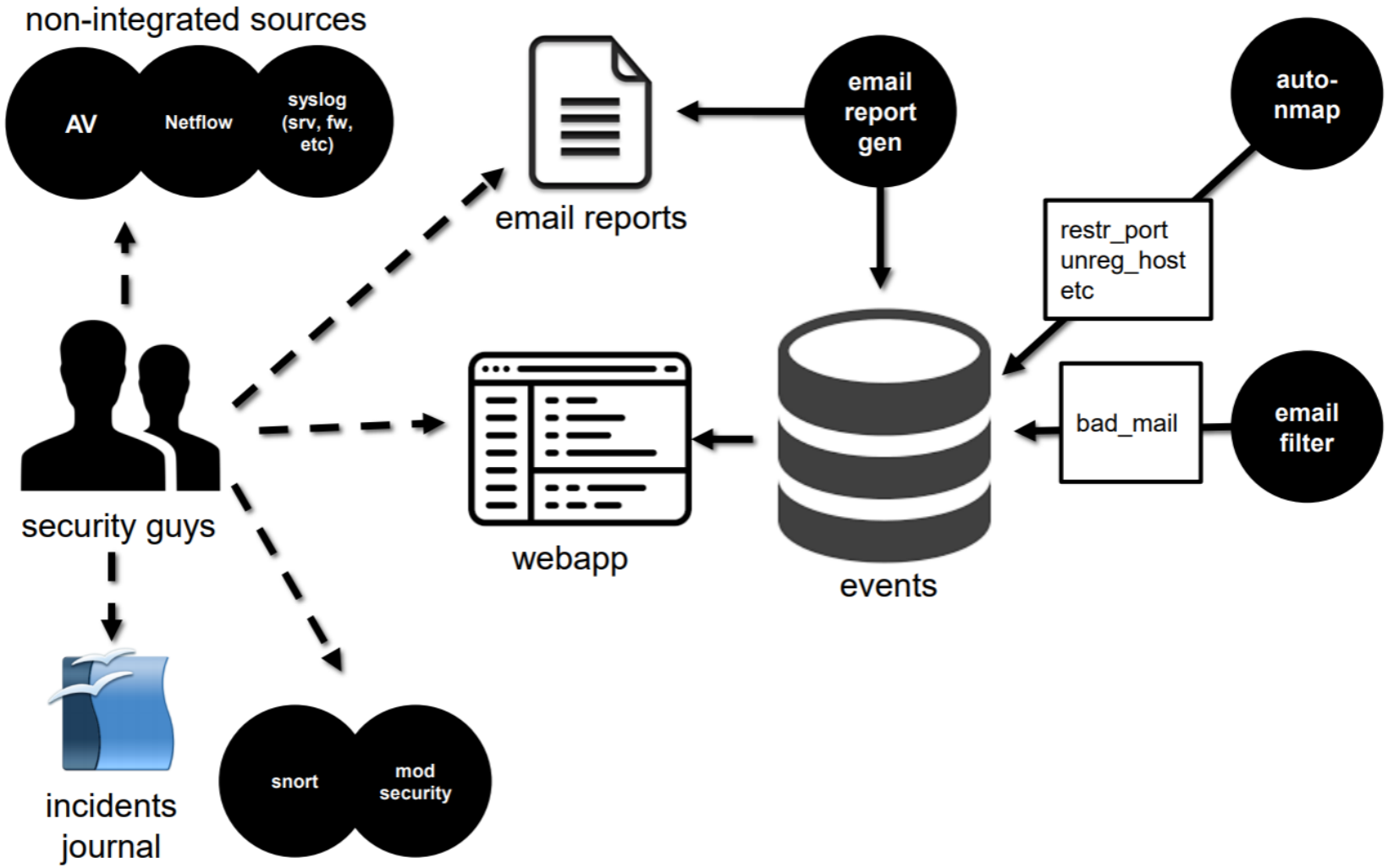
Веб-интерфейс с событиями



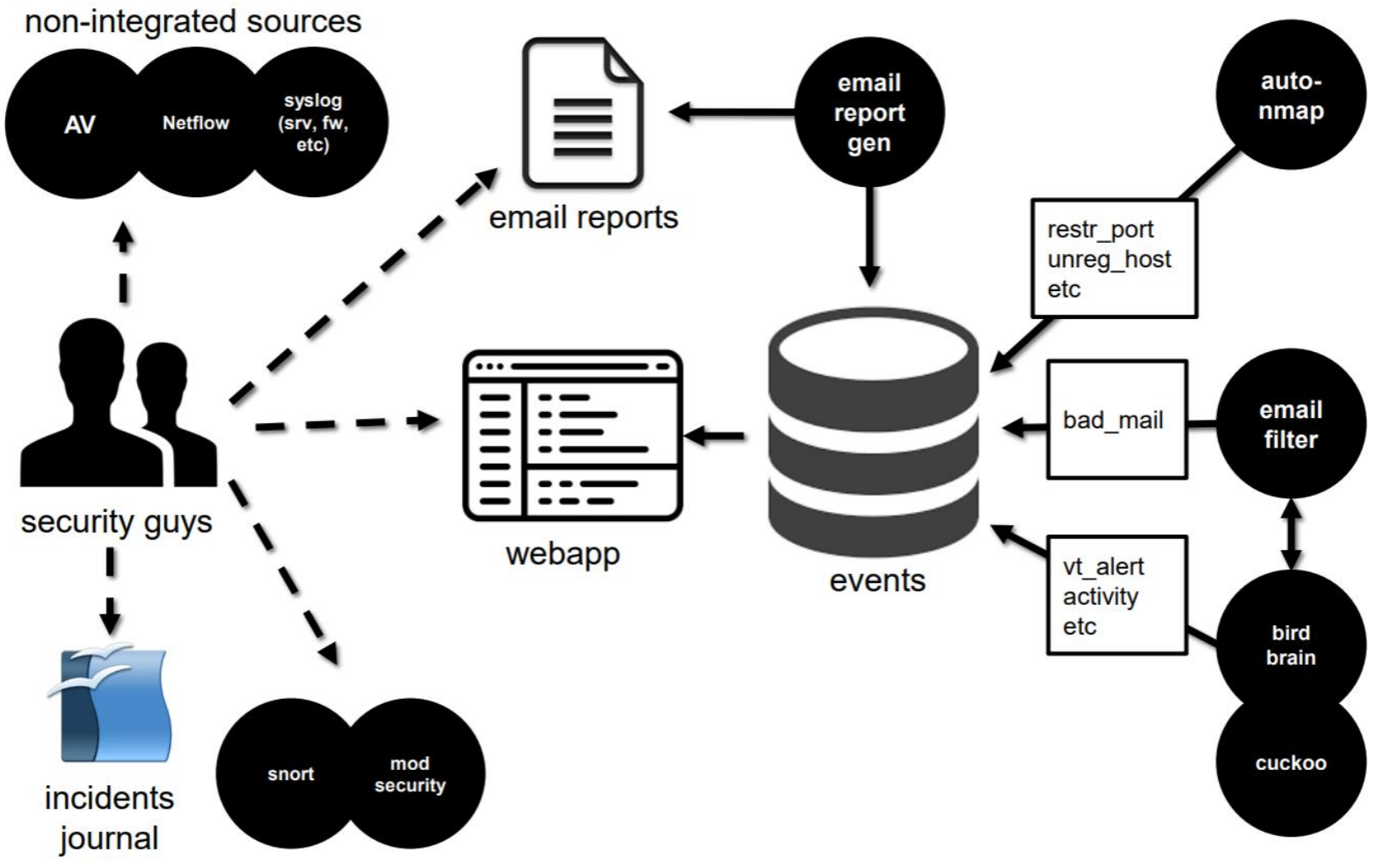
Добавление IDS и Firewall



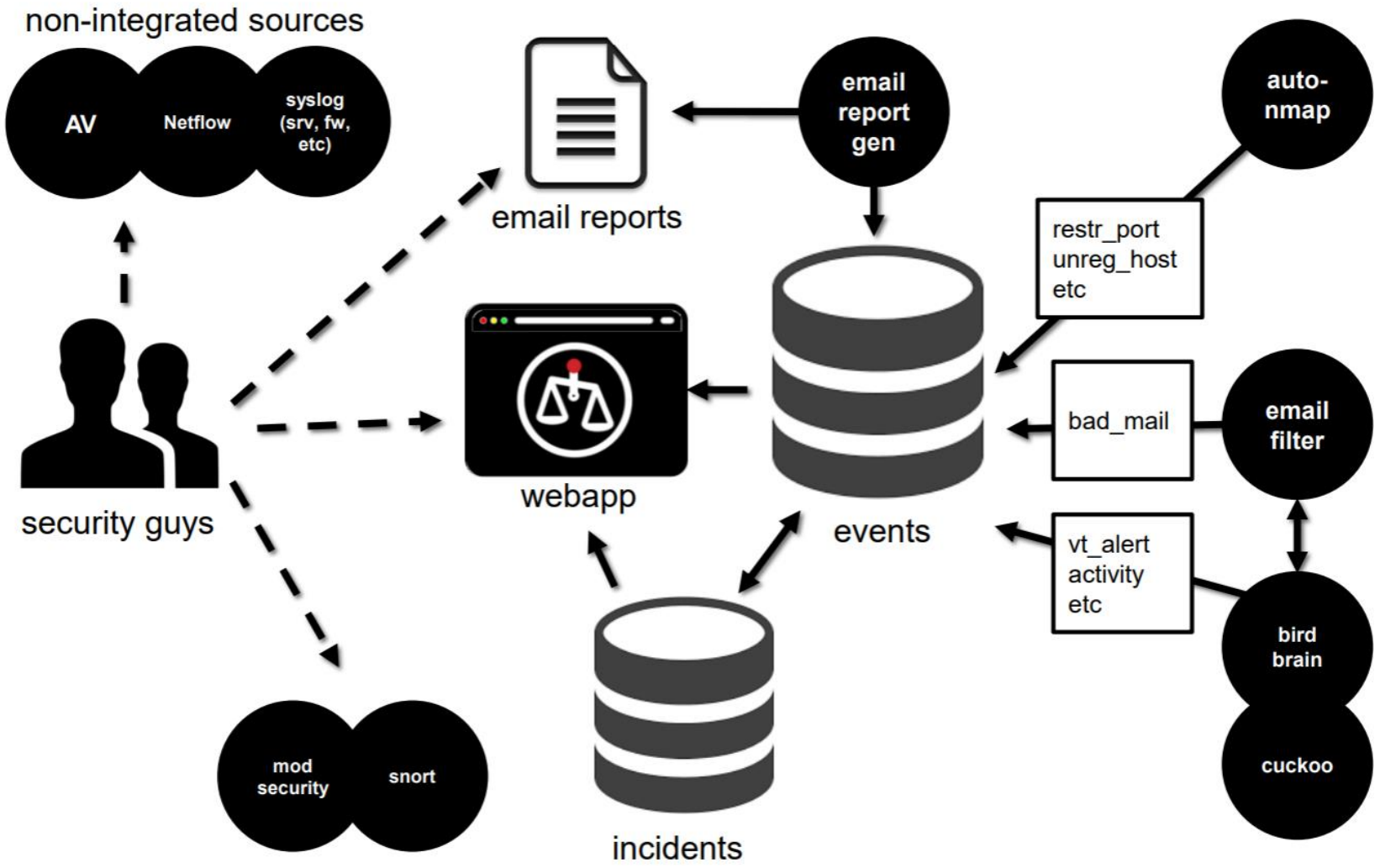
Новые источники: анализ почты



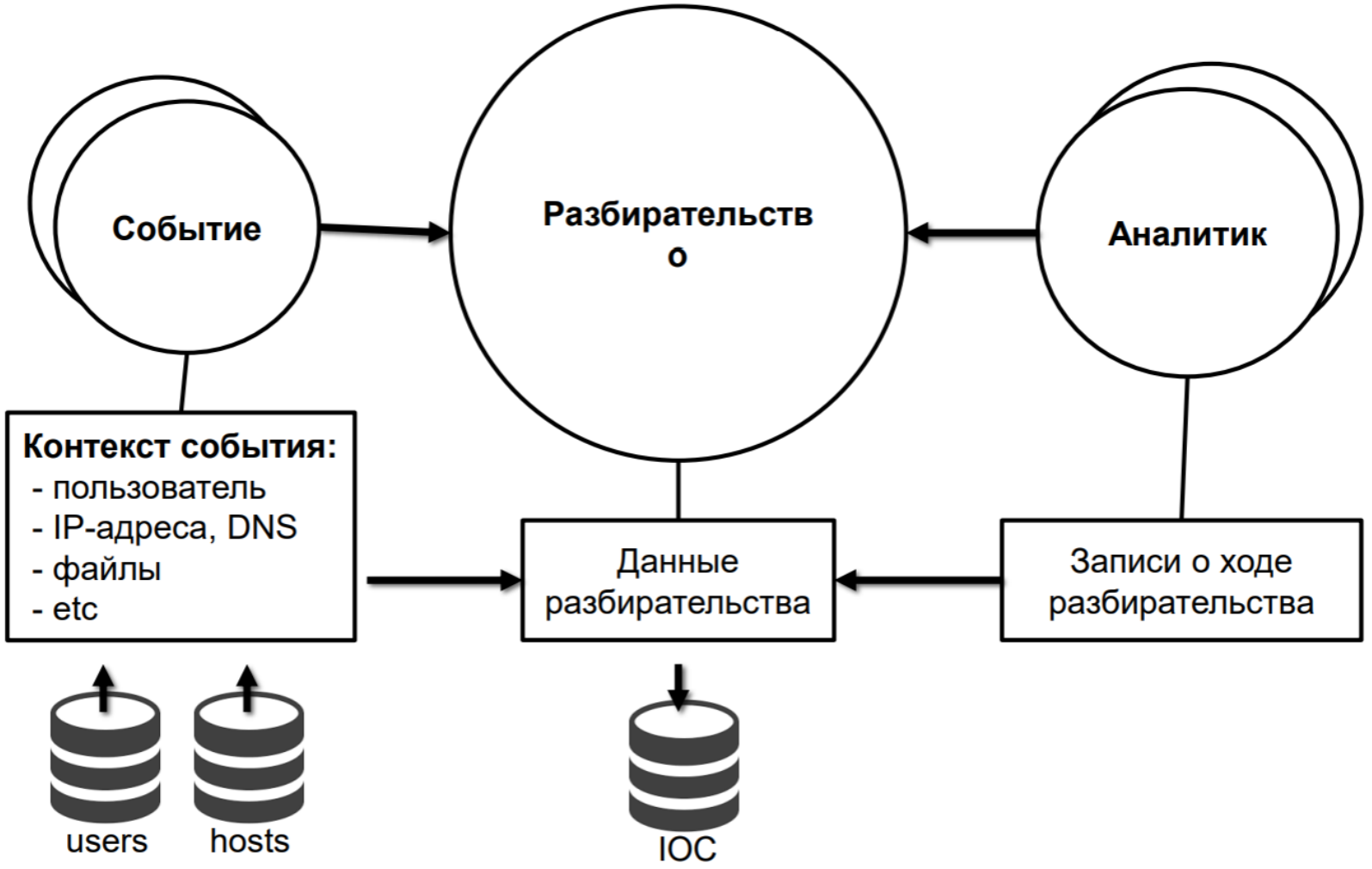
Новые источники: песочницы



Переход от инцидентов к разбирательтсвам

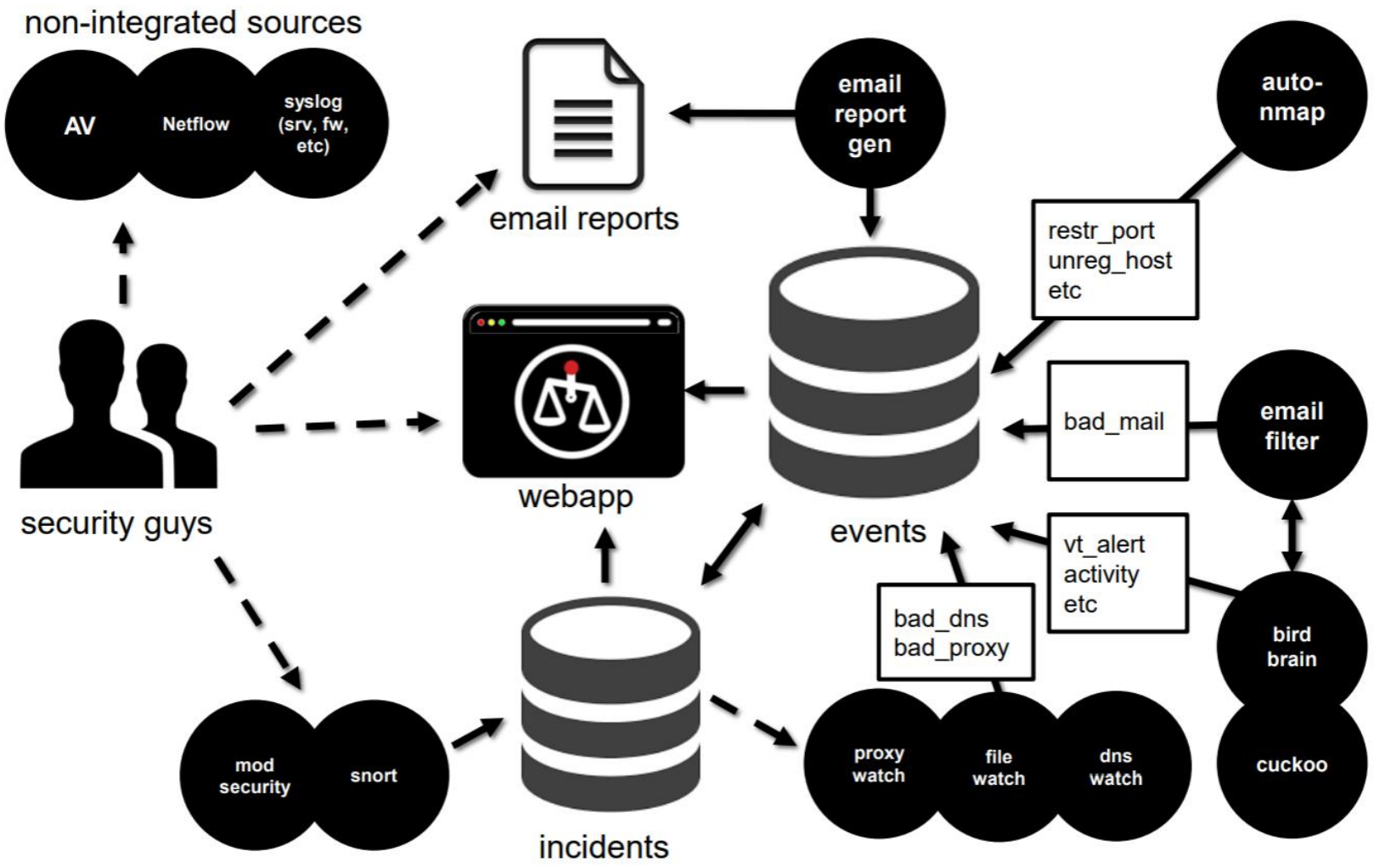


Структура разбирательтсва

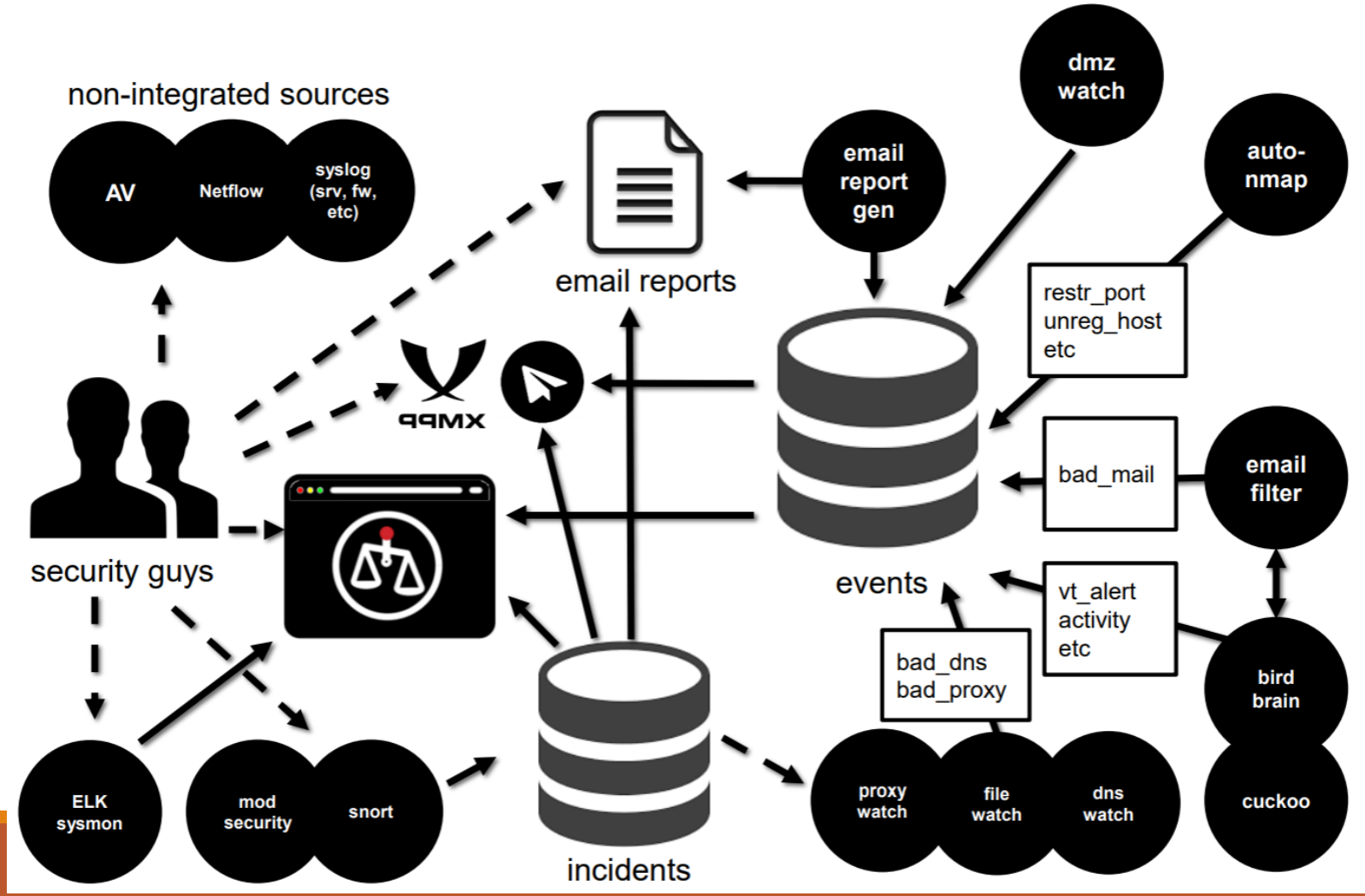


Процесс разбирательства

Добавление анализа IoC (Indicator of Compromise)



Пример конечного вида системы



Источник

Positive Hack Days 2018

Своими руками: корпоративная безопасность «на коленке»

Данил Бородавкин

https://youtu.be/wgvn0TilIi0

http://2018.phdays.com/ru/program/reports/svoimi-rukami-korporativnaya-bezopasnost-na-kolenke/