



Open Source в ИБ

OSSIM, OSSEC, ELK и кое-что еще.



Евгений Соколов

Руководитель Службы ИБ. ООО «Инбанк».

Причины использования Open Source

- ▶ Стоимость коммерческих систем явно превышает стоимость вероятного ущерба от злодейства.
Предполагается, что Open Source обойдется дешевле (спорный вопрос, но обсуждать его не будем).
- ▶ В компании вообще не выделяются никакие деньги на технические средства ИБ.
Денег нет, но вы держитесь тут.
- ▶ Open Source системы позволяют "обкатать" внутренние процессы ИБ, провести внедрение практик ИБ в компании, отладить встраивание в ИТ инфраструктуру и бизнес-процессы, проверить целесообразность и возможную эффективность технических мер ИБ, и правильность построения процессов ИБ.
Предполагается, что потом можно будет поговорить о внедрении коммерческих систем (вот научитесь нырять с вышки, тогда и воды в бассейн нальем).



ОСНОВНЫЕ СИСТЕМЫ

OSSIM, OSSEC, ELK



OSSIM (Open Source SIEM).

Преимущества

- ▶ Швейцарский нож ИБ. Полный набор типовых "контролей" ИБ. Кроме собственно SIEM содержит в том же флаконе Network IDS (Suricata), Host IDS (OSSEC), сборщик Netflow, сканер уязвимостей (OpenVAS) и даже некое средство трекинга обработки инцидентов. И всё это доступно из одной веб-консоли.
- ▶ Легко подключать источники событий, легко дорабатывать систему (python).
- ▶ Небольшой, но полезный набор правил корреляции событий и готовая "развесовка" событий Suricata и OSSEC по степени риска + встроенное взаимодействие с Open Threat Exchange (OTX).
- ▶ Лучший Open Source проект в классе SIEM.



OSSIM (Open Source SIEM).

Недостатки

- ▶ Чудовищный аппетит. Жрет ресурсы, сколько ни дай – всё мало.
- ▶ Из коробки признает только кодировку latin1. Это можно поправить конфигами, но в доках об этом нет ни слова.
- ▶ Нет возможности сохранять сколько-нибудь длительную историю событий, в реальной жизни - пять дней, поскольку при размере БД (MariaDB), более 10GB жутко тормозит. Это можно частично поправить прикручиванием внешнего логгера. Но придется написать несколько строк на питоне.
- ▶ Как всякий SIEM, "нормализует" события для хранения и последующей обработки, около дюжины полей для эффективного анализа. Для сравнения, в обычном eventlog Windows можно обнаружить более 750 различных полей. Соответственно, возможности агрегации, сортировки и автоматического анализа примитивные.



OSSEC (Open Source Host IDS).

Преимущества

- ▶ Очень простая, надежная и быстрая Host IDS. Не прожорлива.
- ▶ Довольно понятный способ описания правил обработки событий в текстовых (xml) файлах.
- ▶ Длительная и успешная история применения в реальной жизни.
- ▶ Небольшой, но вполне приличный набор готовых правил для контроля целостности ОС Windows/Linux и выявления подозрительных событий по логам ОС и веб-серверов.



OSSEC (Open Source Host IDS).

Недостатки

- ▶ Неудобно разворачивать агентов на большом количестве хостов, для каждого агента нужна индивидуальная инициализация с собственным ключом, который генерирует сервер.
- ▶ Никаких GUI/WEB консолей для операций "в один-два клика", только текстовый редактор и файлы xml.



ELK (Elasticsearch - Logstash - Kibana).

Преимущества

- ▶ Отличные возможности поиска, агрегации и визуализации данных.
- ▶ Высокая производительность, практически не зависящая от объема данных. Терабайт плохо структурированных данных - это мелочи.
- ▶ Позволяет очень быстро производить обзор и анализ событий из технических журналов серверов, рабочих станций, файрволлов, маршрутизаторов и коммутаторов. Нет необходимости в "нормализации" событий.
- ▶ Можно было бы сказать, что это отличный логгер, но благодаря Kibana и очень производительному поиску, это больше чем логгер, это отличный монитор реального времени с возможностью быстрого анализа истории событий.
- ▶ Возможно (и это очень просто) горизонтальное масштабирование системы.



ELK (Elasticsearch - Logstash - Kibana).

Недостатки

- ▶ Это голый движок. Никаких готовых визуализаций вы там не найдете, есть некоторые примеры, скорее для пояснения, как можно обрабатывать данные. Чтобы добиться от него толку, вы должны понимать, что вы хотите увидеть и где это надо искать.
- ▶ И это вообще никакой не SIEM и не IDS, "автоматически" он вас ни о чем не предупредит. Всё что вы можете увидеть – вы должны увидеть собственными глазами.
- ▶ Есть минимальные требования к производительности машины. Для нормальной работы необходимо не менее 8GB оперативной памяти и четырех ядер процессора (производительность ядер не важна). Однако, с этого порога до необходимости наращивать мощность системы очень далеко, можно и не добраться.



Что для чего?



OSSIM

- ▶ Это скорее учебно-тренировочная система, которую очень полезно использовать в проектах по внедрению технических средств ИБ и разработке способов применения этих средств в конкретной инфраструктуре, для создания и наладки внутренних процессов ИБ.
- ▶ Как «боевой» SIEM он не годится, поскольку для SIEM главное качественный набор правил корреляции событий и правильная развесовка рисков. Вот этого ни в одной Open Source системе нет и никогда не будет, поскольку это огромная работа, которую никто не сделает бесплатно. А выполнить эту работу собственными силами не получится, у вас нет достаточного объема экспериментальных данных.



OSSEC

- ▶ Очень хорош для "промышленных" систем, там, где ограниченный набор функций и неизменная программная среда: банкоматы, платежные терминалы, веб-сервера.
- ▶ В этих системах он прекрасно решает задачи контроля целостности среды, отслеживания доступа привилегированных пользователей.




ELK

- ▶ Отличная система для организации мониторинга ИБ в небольших и средних компаниях.
- ▶ Казалось бы, здесь нет вообще никаких правил автоматизации. Почему я считаю его хорошей «боевой» системой, а тот же OSSIM негодной?
- ▶ ELK позволяет проводить мониторинг и анализ событий собственными глазами и головой, что компенсирует отсутствие "наборов правил". В небольшой компании этого вполне достаточно.
- ▶ Это как раз тот случай, когда затраты на коммерческие системы не оправданы, а работать как-то надо.



Почему Open Source продукты
редко применяются в ИБ?



Нет знаний и нет возможности «отладки»

- ▶ Как ни странно, для специалистов ИБ такие слова, как Java, Python, JSON, Syslog, SQL, TCP/IP - китайская грамота. Не для всех, конечно, но для большинства. Они хотят видеть что-то с одной кнопкой и большим раскрашенным экраном. Это удивительно. По крайней мере в части компьютерной безопасности, совершенно невозможно делать что-то разумное, если вы не представляете себе, как эти самые компьютеры работают.
- ▶ Для систем класса IDS/IPS, SIEM нужны "экспериментальные данные", которых нет у сотрудника ИБ предприятия. Это всё равно, что писать антивирус, не имея доступа к вирусам.

LittleBeat

- ▶ Все же специалистам ИБ следует внимательно смотреть на Open Source продукты по причинам, изложенным в начале этой презентации. И, по возможности, следует помогать коллегам в освоении таких систем.
- ▶ Я вот нашел время и силы, чтобы сделать на основе ELK некий готовый аплаенс, ориентированный в первую очередь на сбор и анализ журналов событий Windows. И основанный на собственной практике. Я назвал его LittleBeat и раздаю со своего OneDrive в виде образа iso. Можно забрать по этой ссылке <https://1drv.ms/u/s!Al6nQoPiJAEjgYG5cWmTFRa0asxGV84> а исходники лежат на гитхабе <https://github.com/ESGuardian/LittleBeat>



И другие ...

Кое что еще вы можете найти в моем блоге:
<https://esguardian.ru/>



iTop

- ▶ Это система управления конфигурациями, инцидентами, и, вообще, система поддержки ITSM. Причем здесь ИБ?
- ▶ Самая главная проблема компьютерной безопасности — отсутствие достоверной информации о конфигурации инфраструктуры, которые вы намерены обезопасить.
- ▶ iTop – инструмент, помогающий решить эту проблему.
- ▶ А еще я сделал для iTop собственный модуль управления чек-листами. С его помощью можно привязывать к элементам инфраструктуры правила проверки соответствия требованиям ИБ, например, правила PCI DSS, и отмечать выполнены они или нет.
- ▶ И еще сделал модуль управления ролями пользователей с возможностью задания несовместимых ролей и автоматическим контролем наличия пользователей с несовместимыми ролями.



Cuckoo Sandbox

- ▶ Это антивирусная песочница. Работать с ней сложно, но можно.
- ▶ Что такое антивирусная песочница всем понятно.
- ▶ Я работаю с форком Бреда Шпенглера (Brad Spengler), который можно найти здесь:
<https://github.com/spender-sandbox/cuckoo-modified>

Вопросы?

<https://esguardian.ru/>

<https://www.facebook.com/esguardian/>

<https://github.com/ESGuardian>

esguardian@outlook.com

skype: esokolov.ru