РЕШЕНИЯ ДЛЯ ЗАДАЧ УПРАВЛЕНИЯ И МОНИТОРИНГА СОБЫТИЙ ИБ

Роман Ванерке
Руководитель отдела технических решений
АО «ДиалогНаука»

ДиалогНаука

infosecurity RUSSIA

Содержание

- Что такое мониторинг и какие есть варианты мониторинга
- Что такое LM и SIEM, какие функции должны выполнять?
- Общая архитектура комплексной системы мониторинга
- Вариант построения системы на базе продуктов ArcSight

Что такое мониторинг?

- «**Мониторинг** — систематический сбор и обработка информации, которая может быть использована для улучшения процесса принятия решения, а также, косвенно, для информирования общественности или прямо как инструмент обратной связи в целях осуществления проектов, оценки программ или выработки политики.

  *https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D0%BD%D0%B8%D1%82%D0%BE%D1%80%D0%B8%D0%BD%D0%B3

Что обычно под этим понимают?

- Системный мониторинг (ИТшный) – контроль работоспособности:
  - Пинги
  - Snmp, счетчики
  - Nagios/Cacti/MRTG…
  - Продвинутые системы мониторинга (HPE Operations Bridge)
- ИБ – контроль выполнения требований политики ИБ:
  - Анализ логов (руками, скриптами)
  - Syslog-ng
  - ArcSight
  - Аналитика

По статистике Verizon в **82%** случаях взломов доказательства были в логах…

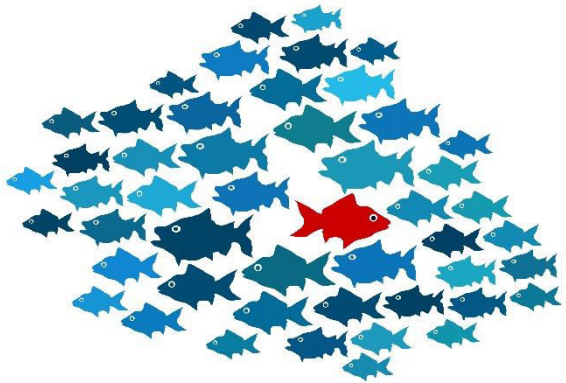
Варианты мониторинга

- Отсутствие мониторинга
- Просмотр событий на самих устройствах\системах
- Примитивный сбор логов (syslog, копирование файлов в сетевую папку, события хранятся с исходном виде) – rsyslog, ftp, cifs
- Централизованный сбор (индексация событий +нормализация событий +соответствие требованиям) – arcsight logger, splunk, log stash
- Выявление нарушений и инцидентов (корреляция событий, интеграция со сторонними системами) – arcsight esm\express
- Поиск аномалий (профилирование, поиск отклонений в поведении, сравнение с группой) – arcsight user behavior analytics
- Проактивный контроль (ручной или автоматизированный поиск нарушений) – различные инструменты hunt team

Что такое LM и SIEM?

- LM = Log Management – Управление журналами
  - Централизованный **сбор**
  - Долговременное хранение, **архив**
  - Поиск, анализ, расследование
  - Отчетность

- SIEM = Security Information and Event Management – Управление событиями ИБ и контекстом ИБ
  - **Корреляция**, отчетность и т.п.
  - Управление инцидентами
  - Интеграция



Must-have функции «правильных» LM\SIEM

LM

SIEM

Возможность сбора событий со всего, что генерирует логи
- Разработка кастомных коннекторов в разумные сроки
- Единый формат, возможность предобработки данных

Хранение
- Настройка политики хранения в зависимости от источника
- Сжатие >> возможность хранения онлайн и оффлайн большого количества событий
- Кластер

Поиск… быстрый поиск

Корреляция
- Использование списков, переменных для манипуляции данными
- Обогащение данных

Контекст (активы, уязвимости, приоритеты, пользователи и прочее)

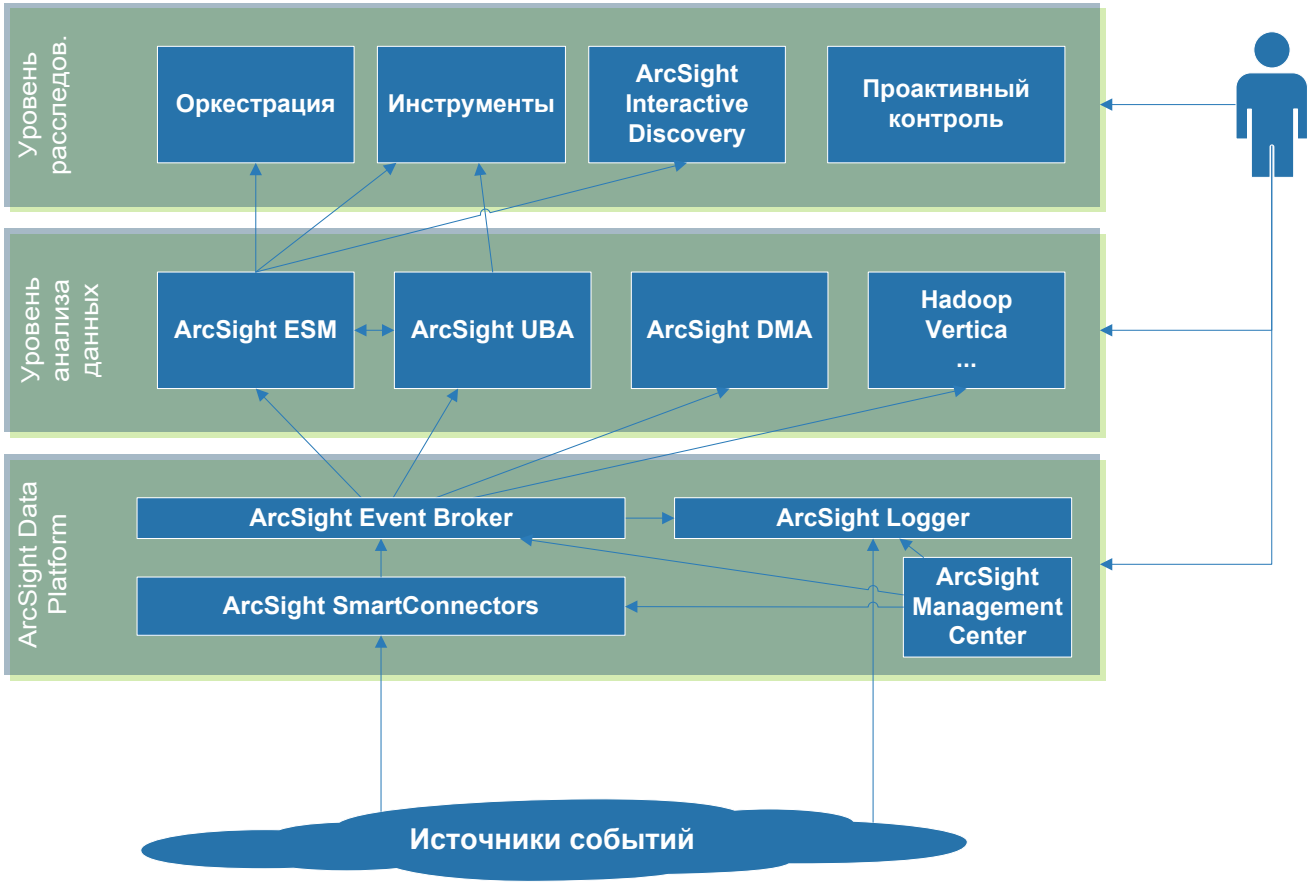
Управление инцидентами и многое другое

Общая архитектура системы мониторинга

Преимущества HP ArcSight

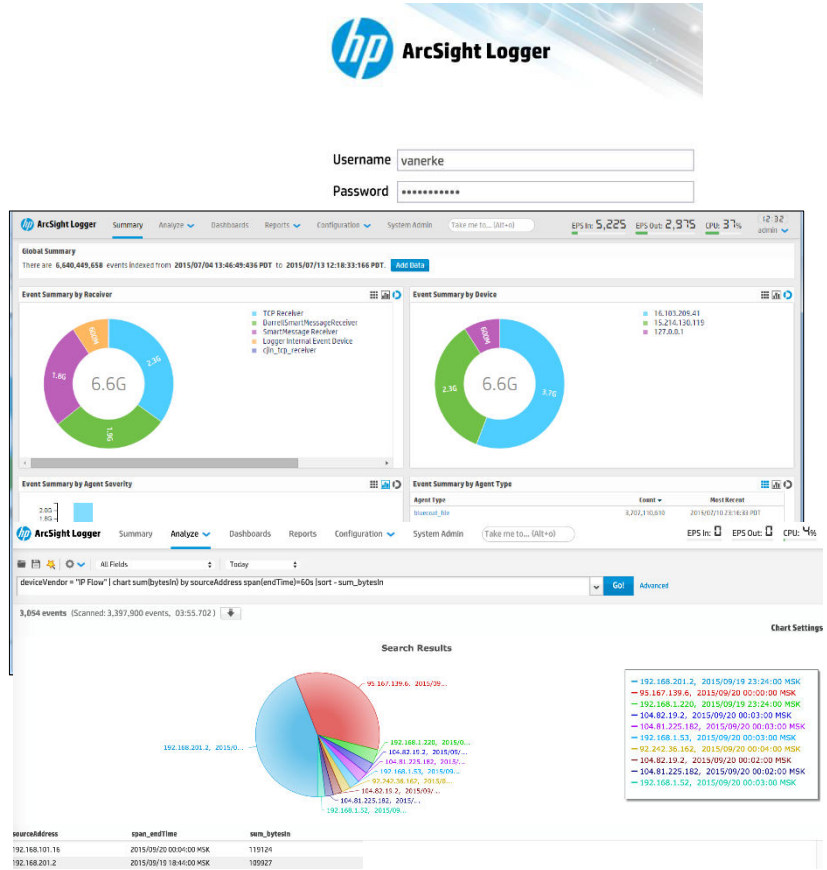
Функция		Преимущество
Сбор		Сбор логов с любого устройства, источника, и любого формата на высокой скорости
Обогащение		События приводятся к единому формату через нормализацию и категоризацию
Поиск		Простой и удобный поиск по логам и событиям
Хранение		Архив за многие годы обеспечивается высоким уровнем сжатия данных
Корреляция		Автоматизация анализа, отчетности и оповещения для ИБ, ИТ и IT GRC

Продуктовая линейка HP ArcSight



ArcSight Data Platform

- Включает в себя:
  - ArcSight Logger – как система централизованного сбора и хранения событий
  - ArcSight Management Center – управление коннекторами, логерами
  - ArcSight SmartConnector\FlexConnector
  - ArcSight Event Broker – доставка событий между несколькими получателями (логеры, ESM, Hadoop и т.п.)
- Возможности ArcSight Logger:
  - Веб-интерфейс
  - Быстрый поиск
  - Кратное увеличение скорости поиска при добавлении нод в кластере
  - Высокая степень сжатия данных
  - Работа со данными в списках
- Поставляется в виде ПАК или ПО



HP ArcSight Express

- Настоящий All-in-one программно-аппаратный комплекс
  - Лицензируется только по количеству событий
  - Без ограничений по пользователям или источникам
- Высокая производительность
- ПАК базируется на HP DL380 Gen9 (2x12-core CPU, 196GB, 8*600 GB)
- Использует последний движок CORR-E (ESM 6.9c)
- Хранение до 2.5 Тб
- Web-консоль ArcSight Command Center
  - Поиск событий (как в Logger и ESM) через веб полнотекстовый поиск
  - Active Channel

Результаты

- Централизованный сбор, хранение и обработка событий ИБ
- Мониторинг, анализ и корреляции событий информационной безопасности в режиме реального времени
- Использование средств визуализации и детализации инцидента
- Позволяет решить самые разнообразные задачи
- Интеграция с различными средствами и системами защиты информации
- Снижение времени расследования и реагирования на инциденты
- Снижение рисков информационной безопасности за счет своевременного обнаружения и обработки инцидентов информационной безопасности

Вопросы?

Роман Ванерке

rv@dialognauka.ru
+7 (495) 980-67-76, доб. 162

http://www.DialogNauka.ru