КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ОНЛАЙН

ОПЫТ РАБОТЫ С MCAFEE ESM: ФУНКЦИОНАЛ, ПЛЮСЫ И МИНУСЫ

Павел АРЛАНОВ
Руководитель отдела ИБ
Туту.ру

МОНИТОРИНГ СОБЫТИЙ БЕЗОПАСНОСТИ

18.00 МСК

29 - 30 ЯНВ'20

MCAFEE ESM – ЧЕРНАЯ ЛОШАДКА?

Архитектура и функциональные модули

1

Enterprise Security Manager
Платформа хранения данных и базовой корреляции.

2

Event Receiver
Платформа сбора и обработки / индексирования данных.

3

Enterprise Log Management
Платформа оптимизации хранения логов и журналов.

4

Advanced Correlation Engine
Усовершенствованный модуль корреляции со скоростью близкой к реальному времени и расширенными возможностями по совершению исторических запросов.

5

Enterprise Log Search
Усовершенствованный двигатель поиска

1-5

McAfee SIEM

6 причин любить mcafee esm

1

Легкость и понятность для оператора.
Все события обрабатываемые платформой легко нормализуются во внутреннем механизме ESM и принимают наиболее понятную и заранее заданную форму

2

Легкость администрирования.
Составление новых правил корреляции, обогащения и автообработки инцидентов

3

Встроенная тикет система.
Нет необходимости вести расследование постоянно заглядывая в текущие логи или пытаясь интегрироваться с внешними решениями

4

Легкая сборка дашбордов
Для сборки дашбордов не нужно знать какой либо внутренний язык запросов, все интуитивно и с выбором нужных переменных

5

API
Удобно и хорошо документировано

6

Унаследованный sub search
В случае если необходимо объединить 2 и более инцидентов в единый – есть корреляционный компонент

ЛЕГКОСТЬ И ПОНЯТНОСТЬ ДЛЯ ОПЕРАТОРА

В каждом событии оператор видит не только сырой лог целиком, но видит представление его, разбитое по именованным полям.

Например:
Antivirus – Trojan Attack
Source IP – 127.0.0.1
HostName – TestHost
Virus Type – Old Trojan

6 причин любить mcafee esm

1

Легкость и понятность для оператора.
Все события обрабатываемые платформой легко нормализуются во внутреннем механизме ESM и принимают наиболее понятную и заранее заданную форму

2

Легкость администрирования.
Составление новых правил корреляции, обогащения и автообработки инцидентов

3

Встроенная тикет система.
Нет необходимости вести расследование постоянно заглядывая в текущие логи или пытаясь интегрироваться с внешними решениями

4

Легкая сборка дашбордов
Для сборки дашбордов не нужно знать какой либо внутренний язык запросов, все интуитивно и с выбором нужных переменных

5

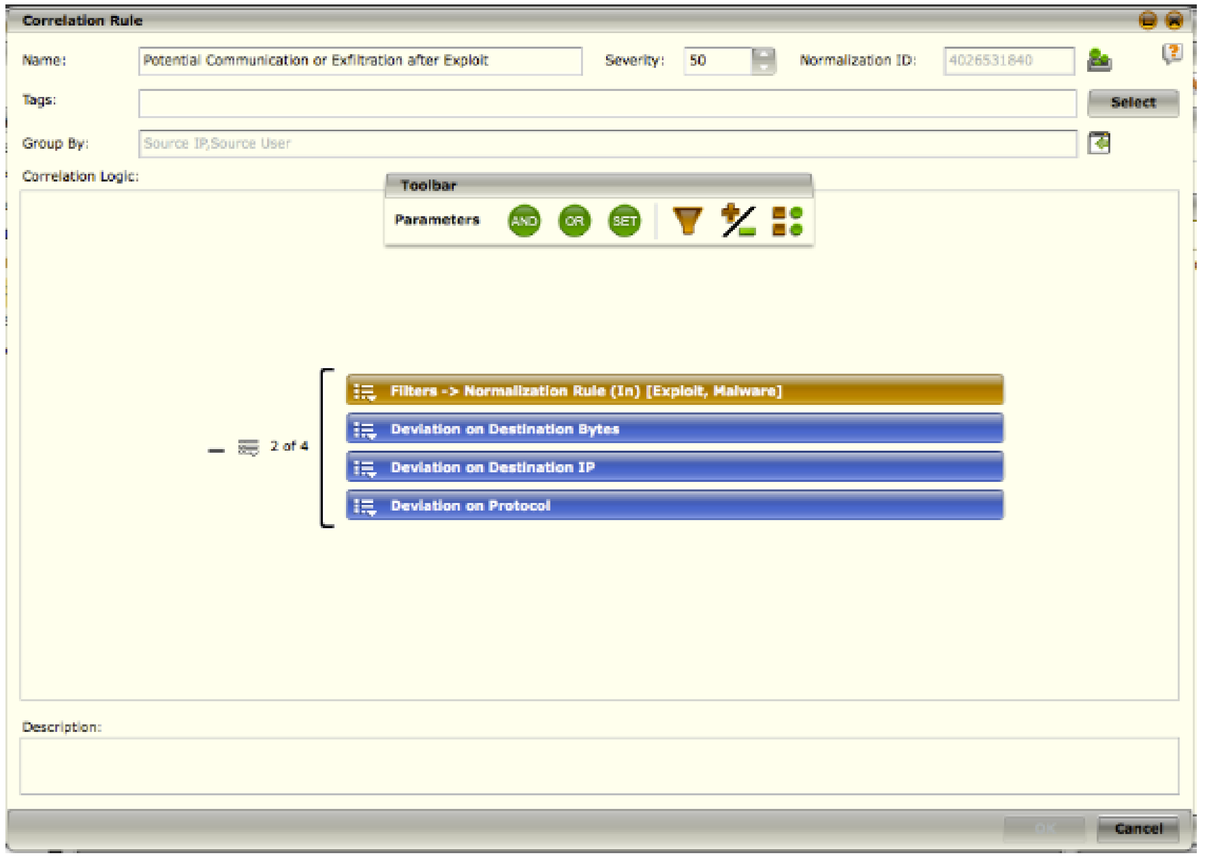
Легкий процесс получения триала
Нужно просто зайти на сайт макафи и заполнить форму, не нужно что либо просить у интегратора

6

Унаследованный sub search
В случае если необходимо объединить 2 и более инцидентов в единый – есть корреляционный компонент

ЛЕГКОСТЬ АДМИНИСТРИРОВАНИЯ

Абсолютно все правила могут быть созданы при помощи нескольких опциональных полей обозначающих ограничения для значений внутри инцидента или логических операторов



6 причин любить mcafee esm

1

Легкость и понятность для оператора.
Все события обрабатываемые платформой легко нормализуются во внутреннем механизме ESM и принимают наиболее понятную и заранее заданную форму

2

Легкость администрирования.
Составление новых правил корреляции, обогащения и автообработки инцидентов

3

Встроенная тикет система.
Нет необходимости вести расследование постоянно заглядывая в текущие логи или пытаясь интегрироваться с внешними решениями

4

Легкая сборка дашбордов
Для сборки дашбордов не нужно знать какой либо внутренний язык запросов, все интуитивно и с выбором нужных переменных

5

Легкий процесс получения триала
Нужно просто зайти на сайт макафи и заполнить форму, не нужно что либо просить у интегратора

6

Унаследованный sub search
В случае если необходимо объединить 2 и более инцидентов в единый – есть корреляционный компонент

3 причины не любить mcafee esm

1

Отсутствии верификации pcre выражений
Если парсер корректен, но может отправить Reciever в бесконечный цикл – он это сделает.

2

Работа с JSON
Если JSON имеет много повторяющихся полей – будет найдено только одно из них.

3

8 опциональных полей
Нет необходимости вести расследование постоянно заглядывая в текущие логи или пытаясь интегрироваться с внешними решениями

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ

Павел Арланов
arlanov@tutu.tech
@TeErevia