СИСТЕМА ПОД КОНТРОЛЕМ

АВТОМАТИЗАЦИЯ КОНТРОЛЯ РАБОТОСПОСОБНОСТИ SIEM-СИСТЕМ

Иван ЛОПАТИН
технический эксперт
АО «ДиалогНаука»

Сейчас трудно представить себе отдел информационной безопасности, в арсенале которого нет SIEM-системы для выявления инцидентов информационной безопасности и оповещения.

В эпоху развивающейся эпидемии множество компаний стараются подключить к своим SIEM-системам как можно больше региональных источников — для контроля за всеми действиями пользователей в сети. Большинство крупных компаний переводят своих подчинённых на удалённую работу из дома, что неминуемо увеличивает нагрузку на коммуникационное оборудование и другие сервисы. Все эти действия неминуемо увеличивают поток событий, направленный на SIEM-системы, мощностные ресурсы которых не безграничны.

Для контроля за состоянием SIEM-системы необходимо иметь штат сотрудников, которые должны на постоянной основе снимать метрики и анализировать их изменения, чтобы увеличивающийся поток событий не вывел из строя всю систему. Сбор и анализ метрик является сложной и кропотливой работой, требующей определённых знаний пороговых значений, таких как: количество tcp-соединений с ОС, количество соединений с базой данных, состояние потоков в jvm, утилизация памяти правилами и многие другие, чтобы можно было в любое время получить реальную картину нагрузки всех компонентов SIEM-системы.

Системным администраторам и инженерам, ответственным за SIEM-систему, приходится вручную анализировать и делать выводы о её работоспособности. Зачастую по тем или иным проблемам приходится обращаться к производителю за поддержкой, где, проходя через ряд стандартных вопросов и действий, вендор предлагает ряд решений для стабилизации ситуации, которые не всегда приводят к моментальным результатам. Бывает и так, что специалисты вендора сильно загружены и не дают ответы на вопросы так быстро, как бы того хотелось.

Некоторые проблемы приводят даже к полной остановке сервиса или остановке приёма событий SIEM-системой. На рисунке 1 приведён пример, как SIEM система ArcSight была перегружена большим количеством tcp-соединений и её сетевой интерфейс был не готов принять такой объём сессий.

Для эффективного мониторинга своей SIEM-системы вы должны обратить внимание на мониторинг следующих метрик:

- метрики нагрузки на корреляционное ядро;
- метрики нагрузки на агрегационное ядро;
- метрики работы внутренних ресурсов базы данных;
- метрики работы базы данных;
- метрики поступающего потока событий;

- метрики состояния работы операционной системы;
- метрики состояния работы дисковых накопителей;
- метрики утилизации процессорного времени;
- и др.

Сейчас мы постараемся на примере SIEM-системы ArcSight показать, как те или иные метрики сказываются на её работе.

НАГРУЗКА НА КОРРЕЛЯЦИОННОЕ ЯДРО

Создание некорректных правил корреляции и их применение на большом потоке событий могут привести к ряду проблем, таких как:

- очереди в корреляционном ядре в части «застревающих» потоков (threadов), попавшие в статусы WAITING или SLEEP по той или иной причине;
- высокая утилизация памяти в базе данных CORR-E и JVM (java virtual machine);
- увеличение времени выборки событий из базы данных из-за переполнения буфера или превышения количества потоков к ней.

ОПРЕДЕЛЕНИЕ НАГРУЗКИ НА АГРЕГАЦИОННОЕ ЯДРО

Настройка агрегации событий является необходимой и обязательной процедурой для снижения нагрузки, но выставление неправильных значений ведёт к:

- недостижению порога событий или времени агрегации;
- превышению порога по поступлению событий или времени.

Неправильно настроенная агрегация также расходует ресурсы SIEM-системы или ее компонентов и в пиковых значениях нагрузки может привести к просадкам производительности.

ОПРЕДЕЛЕНИЕ РАБОТЫ ВНУТРЕННИХ РЕСУРСОВ БАЗЫ ДАННЫХ

Создавая внутренний контент (правила, фильтры, списки/листы), мы не задумываемся о нём, а иногда и вовсе забываем, что создавали. Неучтённый, забытый контент, а именно правила, листы и другие компоненты также потребляют ресурсы и способны пагубно отразиться на производительности

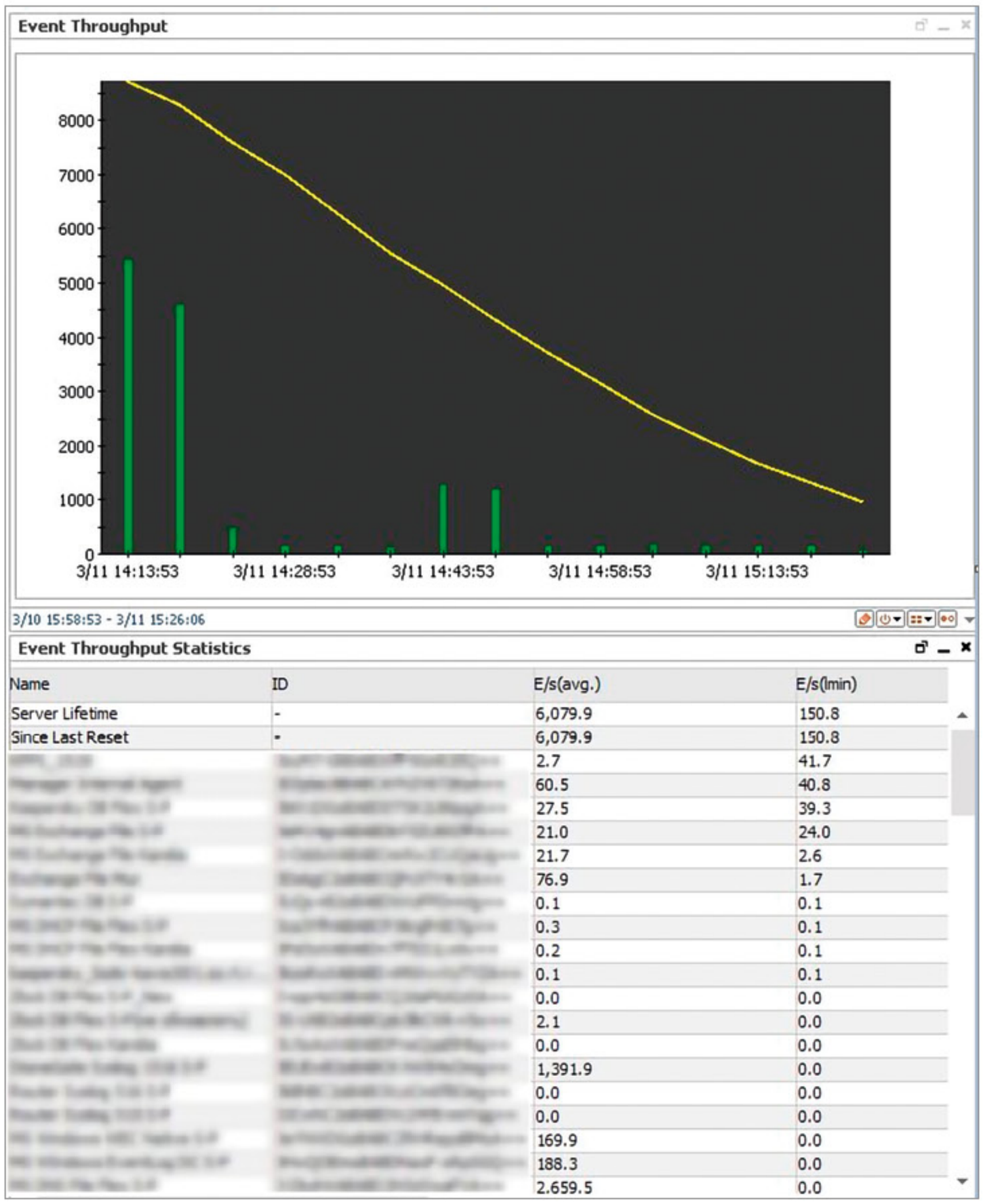

Рисунок 1. Перегрузка SIEM-системы ArcSight большим количеством tcp-соединений

SIEM-системы. Мы приведём два примера, которые снижают производительность SIEM системы ArcSight:

1. Переполненные активные листы — это происходит в случае указания неправильного TTL (time to live — время жизни событий) в активных листах при количестве поступающих записей в лист больше, чем освобождающихся событий по истечении времени.

2. Правила корреляции с большим показателем «Partial Matches» — говорит о необходимости пересмотра правила корреляции.

Все описанные выше метрики и параметры подтолкнули нас к созданию программного комплекса по анализу работоспособности SIEM-систем для увеличения скорости реакции на изменившиеся метрики и снижения собственных трудозатрат.

КОРОТКО О НАШЕЙ СИСТЕМЕ

Система анализа работоспособности SIEM состоит из набора компонентов, которые позволяют ей эффективно контролировать метрики и события:

- модуль сбора событий — обладает механизмами сбора событий и метрик, как в агентском режиме, так и без него;
- модуль обработки и обогащения событий — обладает механизмом парсинга событий SIEM-систем и обогащения их необходимой информацией для дальнейшего реагирования;
- база данных — необходима для хранения и анализа метрик, а также

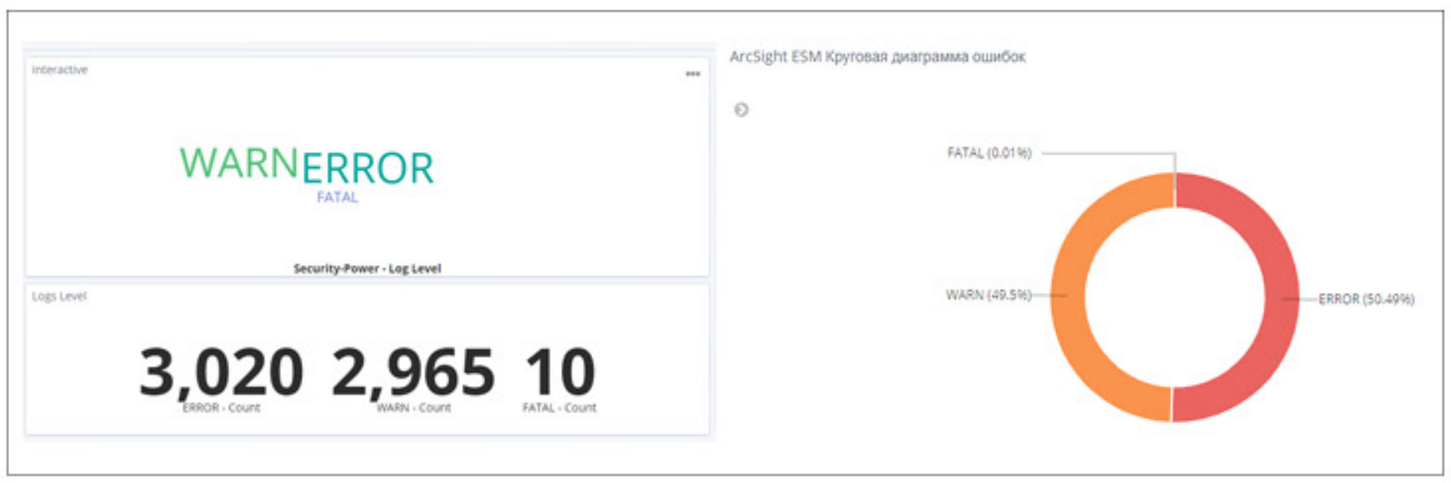

Рисунок 2. Визуализация количества ошибок

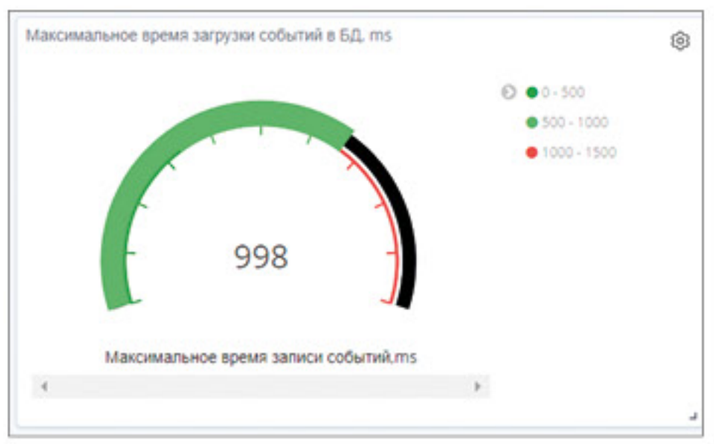

Рисунок 3. Визуализация скорости записи в базу данных событий ИБ

оперативной оценки состояния архитектуры. База данных включает в себя визуализацию метрик и критичных событий, а также итоговый дашборд, который займёт достойное место в SOC;

- визуализация:
  - визуализация всех ошибок с возможностью поиска по каждой из ней (рис. 2);
  - визуализация скорости записи в базу данных событий информационной безопасности (рис. 3);
  - компановка метрик на одном дашборде (рис. 4);
- работа с оповещениями:
  - регистрация поступающих оповещений в отдельный интерфейс (рис. 5);
  - рекомендации по решению выявленных проблем (рис. 6).

Необходимость в мониторинге сервисов всегда стояла не на последнем месте, а в непростое эпидемиологическое время только возрастает. Необходимость контролировать работоспособность систем из любой точки планеты и реагировать на инциденты — основная задача любого руководителя IT или ИБ направления.

* * *

Наша команда более 10 лет занимается исследовательской работой по минимизации трудозатрат для анализа работоспособности SIEM-систем. Нами была разработана отечественная система анализа работоспособности SIEM-систем, которая переросла в продукт, который мы можем предложить нашим клиентам и заказчикам. Наше решение позволит сократить время реакции на инциденты работоспособности и повысить производительность SIEM.

Рисунок 4. Компоновка метрик на одном дашборде

Рисунок 5. Перечень поступающих оповещений

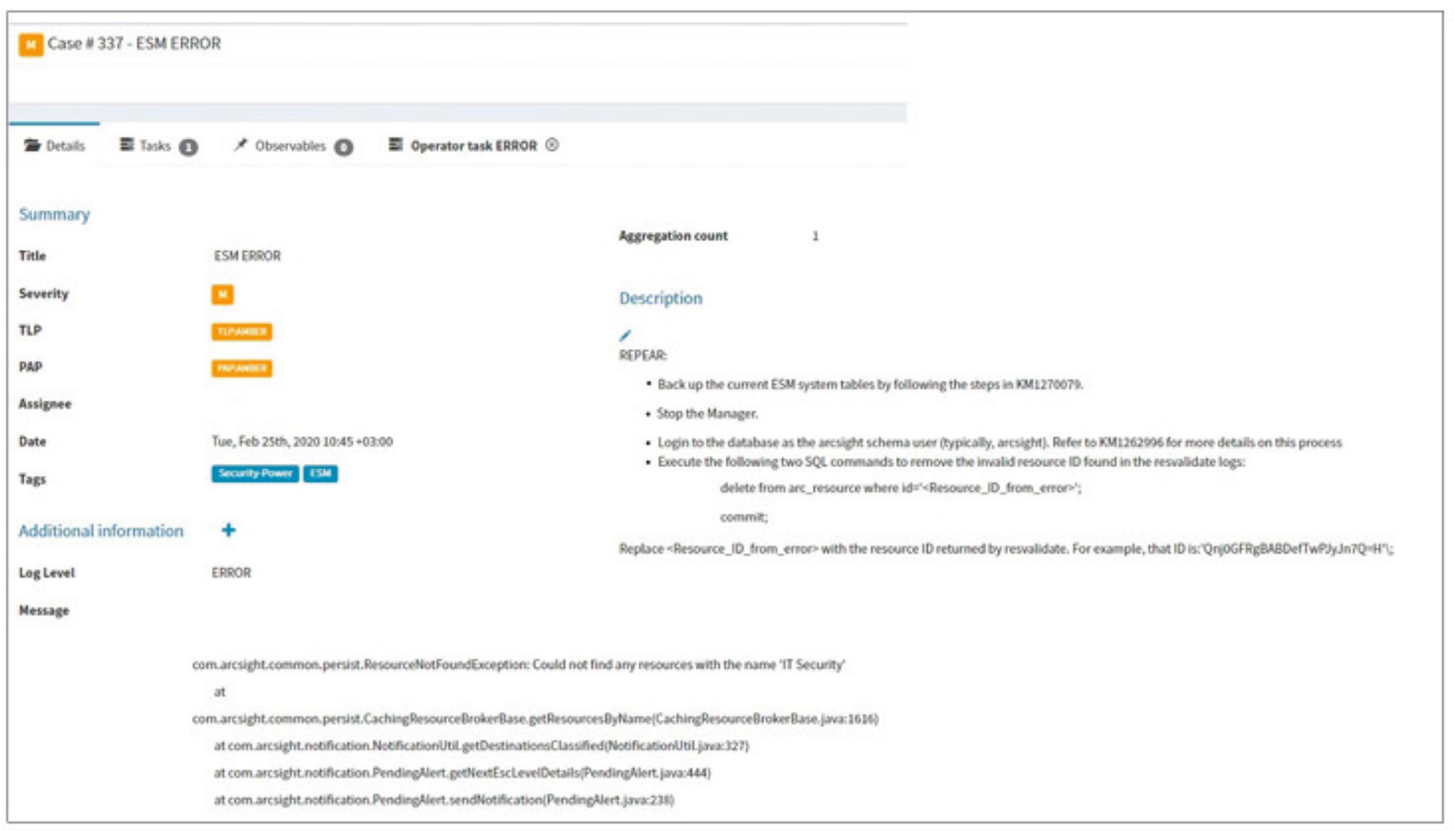

Рисунок 6. Визуализация оповещения и пути его решения