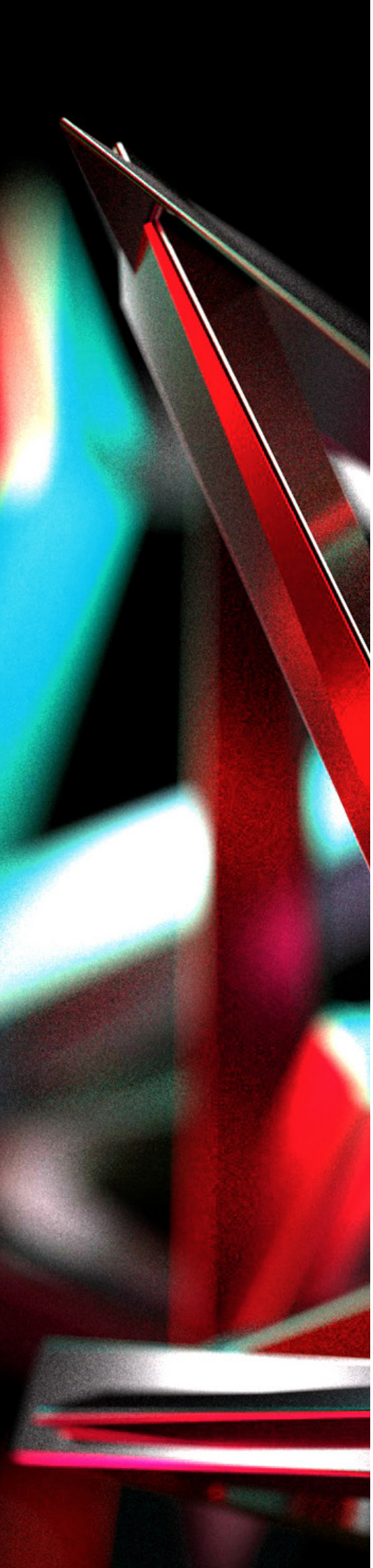
Positive Tech Press Club

Мониторинг событий ИБ: рынок SIEM и технологические тренды

ptsecurity.com



Топ-5 технологических трендов рынка SIEM на ближайшие три года[1]

Алексей Андреев, управляющий директор департамента исследований и разработки Positive Technologies

Опыт, накопленный более чем за пять лет разработки продукта класса security information and event management (SIEM), анализа мировых технологических трендов и реальных потребностей компаний из различных отраслей в обеспечении ИБ, позволяет экспертам Positive Technologies прогнозировать рост значимости ряда технологий SIEM. В частности, особенно актуальными станут пять направлений:

- обогащение экспертизы в части управления системой,
- автоматизация реагирования на инциденты,
- расширение возможностей SIEM-систем за счет инструментов, свойственных другим классам средств защиты (анализа трафика, анализа происходящего на конечных узлах, анализа поведения пользователей и сущностей),
- использование облаков как источника данных для мониторинга ИБ и формата предоставления SIEM as a service.

Часть этих трендов уже выражены в той или иной степени, часть приобретет актуальность на горизонте 1-3 лет[2]. Упомянутые технологии подчеркивают и ведущие аналитические агентства. Так, согласно оценкам Gartner, отсутствие поддержки анализа трафика, инструментов оркестрации, поведенческого анализа пользователей и сущностей, облачных инфраструктур считается недостатком современных SIEM-решений. А IDC рекомендует организациям, планирующим внедрение SIEM, ориентироваться на тех поставщиков, у которых есть своя экспертиза в области безопасности и которые предлагают возможности автоматизации и оркестрации управления инцидентами.

1 Экспертная оценка Positive Technologies. Тренды актуальны для лидеров рынка SIEM (при определении лидеров мы руководствовались данными IDC).

2 Более точные оценки реализованности каждого тренда см. в разделах «Доля покрытия технологии», «Качество реализации технологии». Оба параметра являются результатом экспертной оценки специалистов Positive Technologies.

Тренд № 1. Развитие экспертизы в области управления системой

Доля покрытия

50–60%

Качество реализации

3

Этот технологический тренд нацелен на получение максимальных результатов от мониторинга событий безопасности. Уже 15 лет принято говорить о SIEM-системах как о средстве для сбора логов с разных систем и средств корреляций, а анализ собранных массивов данных ограничивается маппингом правил корреляции по матрице MITRE ATT&CK[4]. Но сегодня этого недостаточно: от них требуется все больше экспертных возможностей и параметров (нужны правила нормализации, способы настройки источников, пакеты с правилами обнаружения угроз, инструкции по активации источников, описания правил детектирования, рекомендации о том, что делать, если правило сработало). Благодаря этим данным операторы систем смогут качественнее реагировать на инциденты и понимать глубину покрытия определенных рисков: это дает всегда актуальную экспертизу в том, какие угрозы сейчас наиболее значимы, какие техники и тактики стоят за конкретными угрозами, а следовательно — на что обращать особое внимание при мониторинге.

Тренд № 2. Автоматизация реагирования на инциденты

Доля покрытия

60–70%

Качество реализации

3

В ближайшие годы автоматизация в SIEM-системах распространится на процесс выявления инцидентов и реагирования на них. Чтобы этот процесс был организован четко, к функциональным возможностям SIEM-систем должны добавиться инструменты, которые автоматизируют процессы подключения источников, обеспечения мониторинга, сведения к минимуму ложных срабатываний, генерации алертов (предупреждений об инцидентах), и реакции на них. Потребность компаний в такой автоматизации подтверждают результаты проведенного нами опроса: 25% специалистов по ИБ проводят в SIEM-системе от двух до четырех часов ежедневно, 22% специалистов — более 4 часов. К наиболее трудоемким задачам участники опроса отнесли работу с ложными срабатываниями (донастройку правил корреляции) и разбор инцидентов: их отметили 58% и 52% респондентов соответственно. У 30% специалистов по ИБ много времени отнимают настройка источников данных и отслеживание их работоспособности (рис. 1). Этот тренд даст толчок развитию SIEM-систем в область другого класса продуктов — security orchestration and automated response (оркестрация событий безопасности и автоматическое реагирование, SOAR). Вендоры, лидирующие на рынке SIEM, будут добавлять к привычным возможностям SIEM-систем модули, позволяющие выстроить удобный процесс реагирования на события ИБ за счет автоматизации этих операций. Таким образом, в ближайшее время мы увидим, как стираются границы между функциональными возможностями SIEM- и SOAR-решений. При этом автоматизация реагирования на инциденты невозможна без другого тренда — автоматизации внедрения SIEM, который сегодня вполне можно отнести к незаслуженно забытым, без четко отлаженных процессов внедрения невозможно качественное реагирование на инциденты.

---

3 Качество реализации оценивается экспертами Positive Technologies по шкале от 1 до 5, где 1 — плохо реализовано, 2 — качество реализации ниже среднего, 3 — среднее качество реализации, 4 — качество реализации выше среднего, 5 — хорошо реализовано.

4 Общедоступная база знаний, разработанная и поддерживаемая корпорацией MITRE на основе анализа реальных APT-атак. Она представляет собой структурированный набор тактик и техник, используемых злоумышленниками, и позволяет специалистам по ИБ со всего мира разговаривать на одном языке. База постоянно расширяется и дополняется.

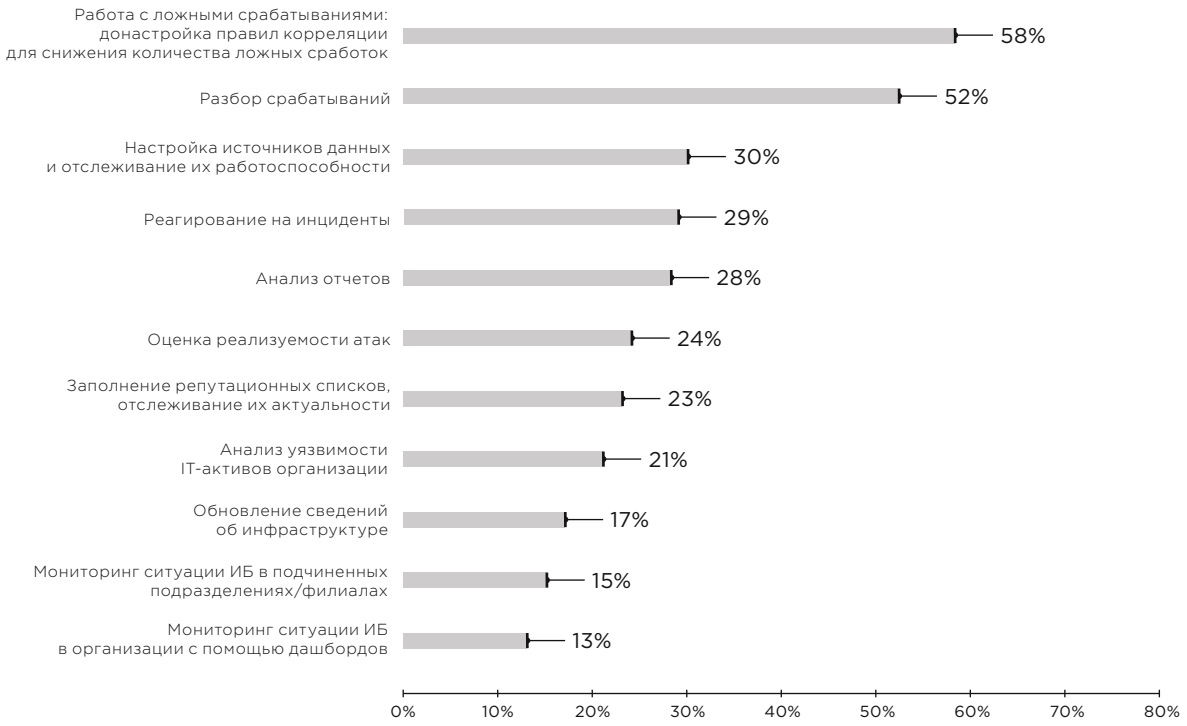


Рисунок 1. Результаты опроса Positive Technologies «Трудозатраты специалистов по ИБ на работу с SIEM-системами»

Тренд № 3. Конвергенция технологий анализа трафика, логов и происходящего на конечных узлах.

Доля покрытия

60–70%

Качество реализации

2

Современные подходы к ИБ подразумевают интеграцию возможностей по анализу логов (область классических SIEM-систем), по анализу сети и сетевого трафика (область network traffic analysis, NTA), а также детектированию событий на конечных узлах пользователей и серверах (область endpoint detection response, EDR). Без глубокого анализа сети и возможностей EDR мониторинг не будет полным, при этом, по нашим оценкам, анализ трафика будет рассматриваться как обязательное условие будущего SIEM, а анализ событий на конечных узлах — как дополняющая функциональная возможность. Благодаря интеграции этих технологий оператор SIEM-системы сможет работать с единой исчерпывающей картиной происходящего в инфраструктуре — для более качественного реагирования на инциденты и threat hunting (проактивного поиска угроз). Тенденция к росту числа таких запросов со стороны пользователей приведет к тому, что немало вендоров SIEM-систем либо добавят в свое портфолио технологии NTA и EDR, либо приобретут их у сторонних компаний, либо подпишут OEM-соглашения с соответствующими разработчиками. По данным Gartner, NTA есть у 9 из 16 игроков рынка, один из которых купил NTA у другого разработчика, а EDR — у 10 из 16 игроков, один из них заключил партнерское соглашение со сторонним вендором.

Тренд № 4. Анализ поведения пользователей и сущностей

Доля покрытия

70–80%

Качество реализации

4

Стремление получить на одном экране единую картину происходящего в инфраструктуре будет способствовать добавлению к возможностям SIEM-систем инструментов user and entity behavioral analytics (UEBA) — поведенческого анализа пользователей и сущностей (процессов, узлов сети, сетевых активностей). Главное отличие SIEM от UEBA в том, что SIEM-система выступает в качестве своего рода конструктора для сбора логов, а решение UEBA строит поведенческие модели. Алгоритмы поиска и обработки аномалий могут включать различные методы: статистический анализ, машинное обучение (machine learning), глубокое обучение (deep learning) и др., которые подсказывают оператору, что в сети стало вести себя нетипично и почему это поведение нетипично для такой сущности или пользователя. Вендоры решений UEBA сами перешли в сегмент SIEM-решений, и наоборот, игроки SIEM-рынка добавили в свои продуктовые портфели UEBA, разработав их или, что встречается чаще, приобретя у других компаний. Несмотря на положительную динамику тренда, главной проблемой для UEBA-решений все еще остаются высокое количество ложных срабатываний и отсутствие понятных для операторов алгоритмов интерпретации этих результатов.

Тренд № 5. Облака как источник данных для мониторинга ИБ и формат предоставления SIEM as a service

Доля покрытия

60–70%

Качество реализации

3

Если говорить о внедрении SIEM-систем, то нельзя обойти вниманием факт миграции инфраструктур компаний в облака. Согласно исследованию, проведенному Enterprise Strategy Group по заказу Dell Technologies и Intel, в 2019 году примерно две трети (64%) предприятий планировали увеличить расходы на публичные облачные платформы по сравнению с предшествующим годом. Такой подход, с одной стороны, заставляет вендоров, добавлять самые популярные облачные сервисы (AWS, Google Cloud Platform, Microsoft Azure) в список поддерживаемых SIEM-системой источников — за счет добавления коннекторов к облакам, а с другой, научиться и самим предоставлять SIEM по модели as a service — посредством добавления специфичных для облачной инфраструктуры способов разворачивания, конфигурирования и дирижирования SIEM (виртуальные, облачные аплайнсы[5]). Это дает толчок к тому, что многие разработчики начинают поддерживать различные гетерогенные, приватные и публичные облака. Выбор предпочтительной модели — облачного или классического SIEM — зависит от отрасли, в которой работает компания, от размеров бизнеса, политики хранения корпоративных данных (в облаке или в локальной инфраструктуре) и других факторов.

Представленные технологические тренды в конечном итоге служат двум стратегическим целям современных SIEM-систем — повышению качества работы с SIEM и сокращению объема ручной работы операторов при мониторинге и реагировании на инциденты.

5 Виртуальный аплайнс, (виртуальное устройство, virtual appliance) — готовый образ виртуальной машины, предназначенный для работы в среде виртуализации (облачной платформе).

О компании

Positive Technologies уже 18 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».

Следите за нами в соцсетях (Facebook, ВКонтакте, Twitter), а также в разделе «Новости» на сайте ptsecurity.com.

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

PT-SIEM_6.0_Information Security Monitoring_A4.RUS.0001.01