Как будут развиваться SIEM-системы в ближайшие три года

Алексей Андреев, *управляющий директор департамента исследований и разработки Positive Technologies*
Роман Ванерке, *технический директор АО "ДиалогНаука"*

Спрос на SIEM-системы[1] в мире остается достаточно высоким. По данным The Insight Partners, этот зрелый и высококонкурентный рынок, несомненно, продолжит свое развитие и вырастет с $2,597 млрд в 2018 г. до $6,24 млрд в 2027 г. В этой статье мы попробуем спрогнозировать, какими будут SIEM через три года, а также определим популярные технологические тренды, которые помогут таким системам лучше выявлять киберинциденты и предотвращать их последствия.

Развитие экспертизы

В числе факторов, влияющих на рынок SIEM, можно отметить развитие экспертизы в управлении системой. Последние 15 лет о SIEM принято говорить как о средстве для сбора логов с разных систем и корреляции событий. Для повышения качества мониторинга событий безопасности SIEM этого недостаточно: нужны правила нормализации, способы настройки источников, правила обнаружения угроз, инструкции по активации источников, описания правил детектирования, плейбуки.

Например, в 2018 г. в решении MaxPatrol SIEM[2] появилась возможность загружать пакеты экспертизы – набор тематических правил обнаружения угроз, а с 2019 г. пользователи ежемесячно получают новые пакеты экспертизы. Каждый пакет в интерфейсе сопровождается подробным описанием с рекомендациями по настройке правил и реагированию на инциденты (см. рис. 1).

По оценке экспертов Positive Technologies, в целом на мировом рынке каждый второй производитель развивает собственную экспертизу для дальнейшей ее передачи пользователям SIEM.

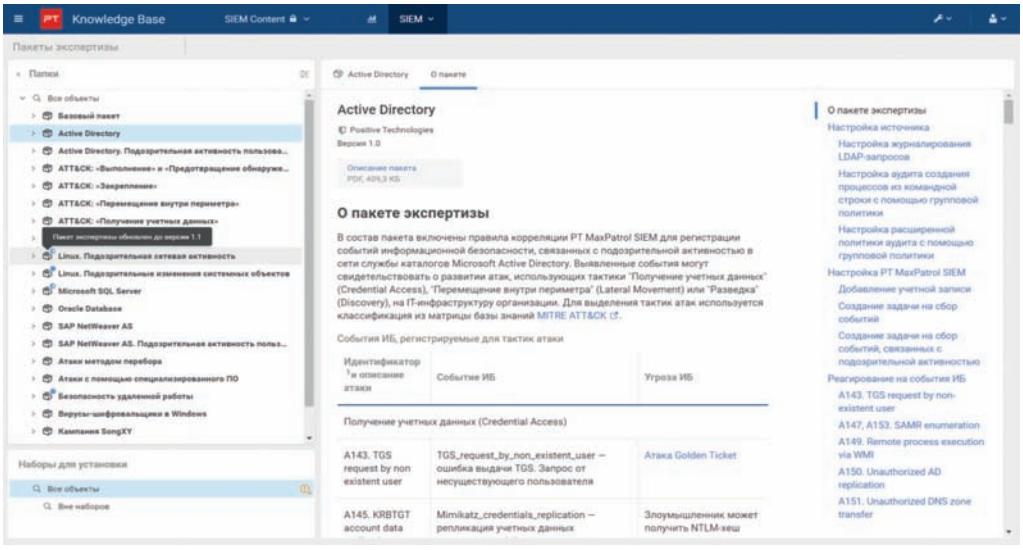

Рис. 1. Описание пакета экспертизы в базе знаний MaxPatrol SIEM

Автоматизация реагирования на инциденты

Согласно опросу[3], проведенному Positive Technologies, 25% специалистов по ИБ проводят в SIEM-системе от двух до четырех часов ежедневно. 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 информационной безопасности много времени отнимают настройка источников данных и отслеживание их работоспособности. Эти проблемы дают стимул для развития SIEM-систем в область продуктов другого класса – оркестрацию событий безопасности и автоматическое реагирование, или SOAR (Security Orchestration, Automation and Automated Response).

Развитие поведенческого анализа пользователей и сущностей

Стремление получить на одном экране единую картину происходящего в инфраструктуре будет способствовать добавлению к возможностям SIEM инструментов UEBA[4] – поведенческого анализа пользователей и сущностей (процессов, узлов сети, сетевых активностей).

Главное отличие SIEM от UEBA в том, что SIEM-система выступает в качестве своего

[1] *Security Information and Event Management (SIEM) – управление событиями информационной безопасности.*
[2] *https://www.ptsecurity.com/ru-ru/products/mpsiem/*
[3] *https://www.ptsecurity.com/ru-ru/research/analytics/siem-report-2019/*
[4] *User and Entity Behavioral Analytics (UEBA) – поведенческий анализ пользователей и сущностей.*

рода конструктора для сбора логов, а решение UEBA строит поведенческие модели. Алгоритмы поиска и обработки аномалий могут включать различные методы, а именно статистический анализ, машинное обучение, глубокое обучение (Deep Learning), которые подсказывают оператору, какие пользователи и сущности в сети стали вести себя нетипично и почему это поведение для них нетипично.

Облака

Согласно исследованию[5], проведенному Enterprise Strategy Group по заказу Dell Technologies и Intel, в 2019 г. примерно две трети предприятий планировали увеличить по сравнению с предшествующим годом расходы на публичные облачные платформы. Такой подход, с одной стороны, заставляет вендоров добавлять самые популярные облачные сервисы (AWS, Google Cloud Platform, Microsoft Azure) в список поддерживаемых SIEM-источников (за счет подключения коннекторов к облакам), а с другой стороны – научиться и самим предоставлять SIEM по модели As a Service посредством добавления специфичных для облачной инфраструктуры способов развертывания, конфигурирования и дирижирования SIEM (виртуальных, облачных аплайнсов[6]) (см. рис. 2).

Куда ведут эти тренды

Исходя из вышеизложенного, можно с уверенностью сказать, что все эти тренды уже заметны на рынке, а примерно через три года станут must-have для любой SIEM. Их развитие приведет к тому, что улучшится качество мониторинга и реагирования на инциденты и сократится объем ручной работы операторов, так как большая часть операций будет автоматизирована. ●

Рис. 2. Процент покрытия. Данные являются экспертной оценкой Positive Technologies. Тренды актуальны для лидеров рынка SIEM (в определении числа лидеров специалисты руководствовались данными IDC[7]).

АО "ДиалогНаука" выполнило НИР по созданию вертикально интегрированной системы взаимодействия Федерального фонда обязательного медицинского страхования с ГосСОПКА

Компания "ДиалогНаука", системный интегратор в области информационной безопасности, завершила научно-исследовательскую работу в сфере обязательного медицинского страхования для нужд Федерального фонда обязательного медицинского страхования (ФОМС) по разработке предложений по созданию вертикально интегрированной системы взаимодействия ФОМС и ТФОМС с ГосСОПКА.

ФОМС реализует государственную политику в области обязательного медицинского страхования граждан как составной части государственного социального страхования и является самостоятельным государственным некоммерческим финансово-кредитным учреждением.

Вопрос противодействия компьютерным атакам и реагирования на них для ФОМС является одним из значимых, поэтому было принято решение о реализации научно-исследовательской работы в сфере обязательного медицинского страхования "Проведение исследований и разработка научно обоснованных предложений по созданию вертикально интегрированной системы взаимодействия ФОМС и ТФОМС с ГосСОПКА".

Для достижения целей проекта специалистами АО "ДиалогНаука" были выполнены следующие работы:

- исследование предпосылок создания системы;
- проведение обследования ФОМС и ТФОМС с целью сбора информации о текущем уровне готовности фондов к созданию и дальнейшей эксплуатации системы;
- разработка научно обоснованных предложений по порядку и формам взаимодействия ФОМС и ТФОМС при создании и функционировании системы, а также при взаимодействии с ГосСОПКА;
- разработка научно и экономически обоснованных концептуальных предложений по созданию системы;
- проектирование системы;
- разработка дорожной карты реализации мероприятий по созданию системы;
- проведение экспертной апробации полученных научных результатов в ТФОМС.

В рамках НИР был осуществлен анализ нормативных правовых актов, устанавливающих полномочия и функции ФОМС по созданию системы, и анализ опыта создания аналогичных отраслевых, ведомственных и корпоративных систем управления и обеспечения информационной безопасности, а также проведено обследование текущего уровня обеспечения информационной безопасности ФОМС и ТФОМС и уровня готовности к эксплуатации вертикально интегрированной системы. Были сформированы предложения по вариантам построения системы с описанием ее функциональной и организационной структуры и разработан порядок и формы участия ФОМС и ТФОМС в создании и функционировании системы, которые легли в основу предложений по порядку создания и дальнейшему обеспечению функционирования системы.

По результатам работы над проектом специалистами АО "ДиалогНаука" был подготовлен научный отчет о выполнении НИР, в котором также содержится концепция создания системы, техническое задание и технический проект на создание системы.

"Результаты НИР послужат основой для дальнейшего формирования условий, позволяющих обеспечить высокий уровень информационной безопасности ФОМС путем построения взаимодействия с ГосСОПКА", – отметил Леонид Лобейко, начальник Управления информационной безопасности ФОМС. ●

[5] *https://www.tadviser.ru/index.php/Статья:Облачные_вычисления_(мировой_рынок)*

[6] *Виртуальное устройство – готовый образ виртуальной машины, предназначенный для работы в среде виртуализации (на облачной платформе).*

[7] *https://www.ptsecurity.com/upload/corporate/ru-ru/products/mpsiem/IDC-SIEM-research-rus.pdf*