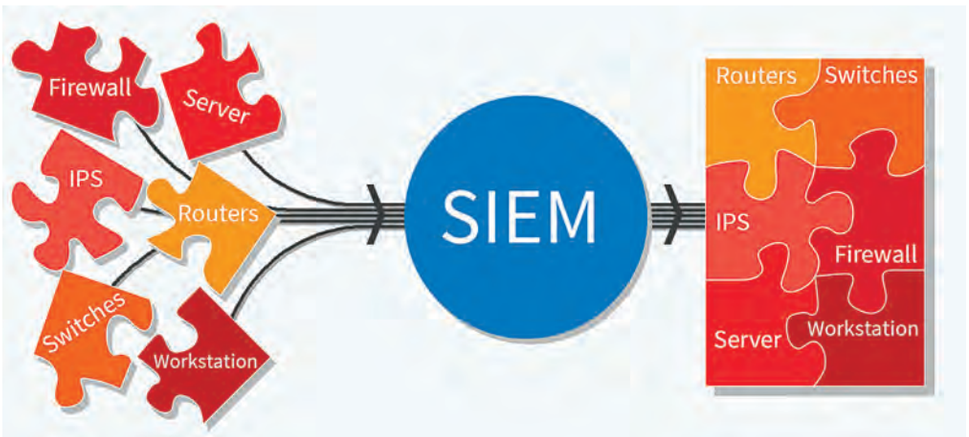
Найти и уничтожить:
SIEM — охотник за киберугрозами



Поскольку кибератак происходит все больше, на подмогу защитникам приходят изощренные средства аналитики на основе искусственного интеллекта и машинного обучения.

Системы Security Information and Event Management (управление информацией и событиями безопасности), или сокращенно SIEM, являются центральным элементом центра управления кибербезопасностью (SOC), и вообще — любой развитой системы защиты предприятия или государственной организации. Они собирают данные об инцидентах от разрозненных систем защиты, таких как межсетевые экраны, IPS и антивирусы, позволяют обнаруживать подозрительные и потенциально опасные ситуации. Кроме того, эти системы сокращают затраты на ИБ и риски угроз безопасности, уменьшают время их выявления. «СиБ» разобрался, как работает SIEM, в какую сторону развиваются технологии и в чем особенности решений разных производителей.

Для чего это нужно

Первые SIEM-решения возникли около десяти лет назад, эволюционировав из систем управления журналами событий. Потребность в таких решениях обусловлена лавинообразным ростом количества угроз, их усложнением и появлением целенаправленных атак, в том числе с использованием разных векторов проникновения. SIEM может быть реализована либо аппаратно, либо в виде программного обеспечения (виртуальное устройство), а размещаться — как на территории заказчика, так и в облаке. Система объединяет в себе две функции: SIM (ведение журналов, анализ и составление отчетов) и SEM (мониторинг и извещение персонала в реальном времени об инцидентах безопасности, связанных как с подозрительной активностью в сети, так и с действиями пользователей, работой приложений). Схема работы SIEM представлена на рисунке.

SIEM собирает данные от всех узлов сети и разрозненных устройств защиты (межсетевые экраны, системы обнаружения и предотвращения вторжений, антивирусы на рабочих станциях и т.д.), в реальном времени проводит их корреляцию и оповещает сотрудников в случае выявления несоответствия установленным правилам. Эти правила можно настроить в зависимости от потребностей организации по приоритезации угроз и сокращения ложных срабатываний. Например, таким образом, чтобы система выдавала приоритетный сигнал тревоги в случае предупреждения от системы IDS, сопровождаемого установлением сессии связи со стороны зараженного компьютера или попыткой создания новой учетной записи Windows.

Ценность SIEM в том, что она собирает разрозненную информацию воедино, выдает в доступном виде и позволяет выявлять тренды. Также система хранит данные обо всех событиях в сети (например, успешный или неуспешный ввод пароля, активность вирусов и т.д.) для расследования инцидентов. Например, только SIEM способна эффективно обнаружить комплексную долговременную атаку (APT), при которой вредоносный код может присутствовать в системе многие месяцы перед активацией. Благодаря анализу накопленных данных SIEM позволяет определить, произошел ли инцидент впервые или подобные атаки были и в прошлом.

Чем более изощренными становятся атаки, тем больше потребность в усовершенствовании механизмов их распознавания. Важно и не пропустить угрозу, и ограничить число ложных срабатываний, что непросто в силу самого объема накапливаемой информации. Как отметил во время проходившего в Киеве форума Cyber Defense Congress эксперт ***GlobalLogic*** Александр Адамов, в крупной компании SIEM собирает в день до 100 ТБ

информации и генерирует более 100 оповещений, к тому же разрозненные устройства защиты выдают данные в разных форматах.

Поэтому разработчики внедряют различные технологии автоматизации обработки оповещений, которые позволяют уменьшить количество персонала и нагрузку на него: машинное обучение, искусственный интеллект. Агентство Forrester отмечает, что за последние годы эволюционное развитие привело к появлению систем анализа безопасности (SA). Эволюция состоит в том, что данные системы не только отслеживают атаки извне, но и включают в себя дополнительные функции, а именно: анализ и контроль работы сети, анализ поведения пользователей и средства обработки больших данных. В частности, искусственный интеллект научится выявлять закономерности, а также будет способен на то, что называется «предиктивным восстановлением»: инструмент мониторинга сможет сам предлагать корректирующие меры, а в будущем – принимать их самостоятельно.

Добавим, что хотя SIEM является ядром SOC, эти термины не равнозначны. В частности, как отметил на том же Cyber Defense Congress директор компании ***InfoSafe*** Виктор Жора, в SOC обязательно должны быть: персонал, который следит за ситуацией и реагирует на оповещения; корреляция данных SIEM с информацией из центров аналитики угроз (Threat Intelligence); платформа для эмуляции угроз для их исследования и анализа.

Также аналитики обращают внимание на то, что даже установив у себя SIEM, не все организации смогут сполна воспользоваться ее возможностями. Прежде всего, специалисты должны обладать достаточным опытом для качественного управления и поддержки SIEM. Как отметил эксперт Forrester Роб Страуд в интервью сайту ***CSOonline***, во многих организациях специалисты-безопасники поначалу реагируют на все «ложные срабатывания», но по мере лучшего понимания ситуации настраивают систему таким образом, чтобы отсеивать то, что является нормой. Другие

Общая схема работы SIEM (на основе данных eSecurity Planet)

такой настройки не проводят и просто игнорируют «ложные срабатывания», тем самым рискуя пропустить реальные атаки, объяснил Страуд.

CSOonline также приводит оценку аналитика компании ***451 Research*** Эрика Огрена, который говорит, что большинство компаний используют SIEM в основном для расследования инцидентов. «Если компанию взломают и правление спросит, что случилось, никакой президент не захочет, чтобы только оставалось ответить: «Почем я знаю?», — прокомментировал аналитик. В то же время компании все чаще интересует быстрое обнаружение и расследование в сроки, приближенные к реальному времени.

SIEM в мире

Существует множество международных рейтингов производителей SIEM. Самый известный из них, конечно, — «магический квадрант» ***Gartner***. В своем отчете Magic Quadrant for Security Information and Event Management, опубликованном в декабре прошлого года, агентство относит к лидерам четыре компании: ***IBM***, ***Splunk***, ***LogRythm*** и ***McAfee***. Gartner, напомним, группирует исследуемых производителей на основе отзывов заказчиков по двум категориям параметров: полноте видения и возможностям компании.

Еще одно сопоставление можно посмотреть в отчете ***Forrester*** Wave: Security Analytics Platforms, которому, правда, уже больше года. Forrester оценивает производителей по возможностям текущего предложения, стратегии развития продукта и рыночному присутствию — лидерами названы IBM, LogRhytm и RSA (компания, приобретенная Dell Technologies в 2016 году). Как отмечалось выше Forrester использует собственную терминологию — «платформы анализа безопасности».

Также в этом году рейтинг SIEM-решений представила компания ***IT Central Station***. Он составлен на основе оценок посетителей и общего количества просмотров, отзывов и сравнений продуктов между собой. По средним оценкам производители были проранжированы следующим образом: на первом месте ***Splunk***, далее ***LogRhytm***, ***AlienVault***, ***IBM*** (QRadar) и ***Micro Focus*** (ArcSight).

Что касается оценок рынка, то, согласно отчету агентства ***Techavio***, который был опубликован в январе прошлого года, к 2021 году объем сегмента должен достигнуть $5,93 млрд при годовом росте 12%. Наиболее крупными заказчиками SIEM выступают государственные организации, финансовый сектор и телекоммуникационные компании, а в географическом разрезе основным потребителем этих решений является Северная Америка. Gartner оценивает мировые расходы на SIEM в 2017 году в $2,4 млрд и прогнозирует более скромный рост: $2,6 млрд в 2018-м и $3,4 млрд в 2021-м.

Аналитики отмечают, что SIEM-системы используют в основном крупные компании и государственные организации, что в том числе связано с регуляторными требованиями. Малые и средние компании не могут позволить себе ни само решение, ни ИТ-специалистов для его поддержки, хотя некоторые пользуются SIEM по модели SaaS (QRadar on Cloud, Splunk Cloud и другие). Крупные компании предпочитают разворачивать SIEM на месте, не желая передавать данные о своей инфраструктуре через Интернет, хотя некоторые эксперты полагают, что с развитием технологий автоматизации производители будут предлагать «гибридные» решения, потому что у них будет больше возможностей для обработки и просеивания данных, чем у заказчика.

Что предлагают производители

Теперь рассмотрим некоторые системы SIEM, которые предлагают ведущие мировые производители. Как правило, они состоят из некоего ядра, реализующего основные функции сбора данных, анализа и отчетности, а также внешних приложений, обеспечивающих расширенные возможности обнаружения угроз и расследования инцидентов.

Например, платформа ***IBM QRadar*** включает в себя собственно SIEM и целый ряд дополнительных компонентов, таких как Log Manager (средство хранения данных о событиях и составления отчетности), Network Insights (анализ данных в сети, в том числе с возможностью отследить их аномальное перемещение), QFlow Collector (сбор информации о потоках сетевых данных, относящихся к сеансу связи), Incident Forensics (расследование действий злоумышленников), Vulnerability Manager (выявляет уязвимости и определяет действия по их устранению), Risk Manager (мониторинг конфигураций устройств, определение рисков и вероятности их использования злоумышленниками), User Behavior Analytics (приложение для анализа поведения пользователей и выявления взломанных систем), а также другие программные средства.

В прошлом году семейство QRadar пополнилось еще несколькими решениями. Среди них — приложение когнитивного анализа Advisor with Watson, которое осуществляет поиск по неструктурированным пользовательским данным (таким как блоги, веб-сайты, исследовательские отчеты) и сопоставляет эти сведения с информацией от SIEM. Это облегчает работу аналитиков, значительно ускоряя расследование инцидентов (как рассказал на Cyber Defense Congress Андрей Кузьменко из IBM, за несколько минут может быть найдена как причина происшествия, так и скрытые угрозы).

QRadar доступен в аппаратном или программном исполнении либо как облачная услуга, также возможен гибридный вариант, когда оборудование на территории заказчика дополняется SaaS-решением из облака IBM Cloud. Дополнительно IBM может взять на себя удаленный мониторинг из своего операционного центра. Есть и бесплатная версия QRadar.

Splunk — американская компания, которая специализируется на программах для сбора, анализа и визуализации данных. Ее семейство продуктов Security Intelligence Platform включает в себя базовое решение Splunk Enterprise, которое обеспечивает сбор, анализ и визуализацию данных, причем не только для

целей информационной безопасности, но и для мониторинга производительности сети и приложений, бизнес-аналитики и т.д. Функции безопасности реализованы в других продуктах: Enterprise Security (поиск угроз, визуализация, реагирование) и UBA (анализ поведения пользователей).

Из новой функциональности стоит отметить приложение Machine Learning Toolkit (MLTK), с помощью которого пользователи могут создавать свои алгоритмы анализа на основе машинного обучения. Уже в этом году Splunk выпустила для MLTK экспериментальный интерфейс управления, который позволяет лучше контролировать ход опытов по машинному обучению, а также включает в себя новые алгоритмы выявления закономерностей.

Платформа Splunk может быть развернута как локально, так и в облаке (Splunk Cloud) или по гибридной модели.

Платформа ***ArcSight*** в 2017 году перешла от ***HPE*** к компании ***Micro Focus***. ArcSight доступна в двух вариантах: Enterprise Security Manager (ESM) для крупных предприятий и ArcSight Express для небольших компаний. Оба могут быть реализованы как аппаратно, так и программно. К достоинствам ArcSight эксперты относят быстроту работы (до 75 тыс. событий в секунду), а также возможность получения данных из множества источников и интеграции в различные среды SOC.

В 2017 году ArcSight перешла на открытую архитектуру безопасности и представила решение Event Broker, которое предоставляет данные об угрозах для сторонних аналитиков и механизмов машинного обучения. В релизе ESM 7.0 реализована распределенная корреляция событий, что позволяет в реальном времени анализировать большие массивы информации и сразу использовать их для идентификации событий. Также весной 2018 года компания представила решение ArcSight Investigate, предназначенное для поиска и нейтрализации неизвестных угроз.

Добавим, что у Micro Focus есть еще одно SIEM-решение под названием ***Sentinel***. Это разработка ***NetIQ*** — еще одной компании, принадлежащей Micro Focus. Она более простая, чем ArcSight, и среди ее достоинств Gartner называет интеграцию с другими продуктами Micro Focus — в частности, с системой управления учетными данными.

LogRythm — это компания, которая специализируется на SIEM. Ее решение Threat Lifecycle Management Platform состоит из нескольких интегрированных программных модулей, которые могут работать как на одном устройстве, так и распределенно. В их числе — AI Engine (непрерывный анализ всех наблюдаемых действий), Detection (обнаруживает целенаправленные атаки, в том числе через «уязвимости нулевого дня»), Network Visibility (мониторинг трафика с возможностью перехвата пакетов для целей расследования) LogRythm поддерживает разные модели развертывания, в том числе мультиарендную (Multitenancy), но эксперты обращают внимание на недостаточную интеграцию платформы с продуктами сторонних производителей.

У ***McAfee***, которая в прошлом году снова выделилась в отдельную компанию после нескольких лет пребывания в составе Intel, SIEM-система носит название Enterprise Security Manager (ESM). Здесь эксперты отмечают, что решению пока не хватает развитых средств машинного обучения, но на его основе можно построить интегрированную инфраструктуру безопасности, которая обеспечивает мощную защиту и мониторинг промышленных систем. Среди ее компонентов можно выделить Advanced Correlation Engine (анализ в реальном времени с использованием четырех корреляционных подходов — на основе шаблонов поведения, рисков, статистики и истории); Global Threat Intelligence (собственная служба аналитики угроз McAfee); Application Data Monitor (декодирование и анализ трафика на прикладном уровне); Database Event Monitor (мониторинг баз данных на уровне транзакций).

Быстрее, еще быстрее

В завершение добавим, что существуют и решения, которые могут рассматриваться как альтернативы SIEM, один из вариантов — системы автоматизации и оркестровки (Security Automation and Orchestration — SAO). Их цель — автоматизация реагирования на инциденты и уменьшение нагрузки на персонал, отвечающий за безопасность. Если инцидент относится к понятным и изученным, SAO может самостоятельно предпринимать действия по заранее прописанным сценариям. SAO обеспечивает отправку данных на анализ в центр Threat Intelligence, вложения электронных писем направляются в «песочницу» для проверки, зараженные устройства попадают в карантин (а пользователи получают уведомление о выявленной угрозе).

В качестве примера можно назвать решение ***LogRythm SmartResponse***, которое получает данные об выявленных угрозах от SIEM-платформы и может либо сразу принимать меры для их локализации и устранения (например, блокировать учетные записи), либо запрашивать разрешение у персонала. Еще один пример — разработки для реагирования на инциденты безопасности от компании ***Resilent Systems***, которую IBM приобрела в 2016 году и которая специализируется на подобных решениях. Основным продуктом Resilent является система Incident Response Platform (IRP), нынешней весной дополненная инструментом оркестровки Intelligent Orchestration. Оба решения обеспечивают автоматизацию процессов реагирования.

Как видно, SIEM и SAO вполне могут работать вместе, дополняя друг друга. SAO и другие средства автоматизации, от которых все больше зависит работа SIEM, в будущем сделают революцию в информационной безопасности хотя бы за счет сокращения человеко-часов, на которые приходится значительная доля расходов SOC. Возможно, в будущем от киберугроз нас будут защищать одни роботы.

Василий ТКАЧЕНКО, **СиБ**