Анализируй это: технические аспекты SIEM

IT-инфраструктура современных компаний весьма разнообразна. С развитием технологий основной проблемой построения защиты становится не отсутствие информации, а ее обработка. Число источников, обеспечивающих поступление актуальной информации по текущему состоянию защищенности, непрерывно растет. Из-за увеличения потока информации администраторам по информационной безопасности становится все сложнее отслеживать и анализировать возникающие угрозы. А если своевременно не предотвратить их, то любая система защиты окажется бесполезной. И здесь на помощь компаниям приходят системы класса Security Information and Event Management. На вопросы редакции по эксплуатации SIEM ответили эксперты:

Олег Бакшинский, *руководитель направления Security Intelligence, IBM Россия и СНГ*
Владимир Бенгин, *руководитель практики внедрения MaxPatrol SIEM, Positive Technologies*
Роман Ванерке, *руководитель отдела технических решений АО "ДиалогНаука"*
Тимур Ниязов, *менеджер по продвижению SOC и защиты баз данных Центра информационной безопасности компании "Инфосистемы Джет"*
Никита Цыганков, *главный специалист отдела технических решений АО "ДиалогНаука"*

– Почему большая часть внедрений SIEM не приносит ожидаемого результата?

Олег Бакшинский

– Не соглашусь с подобным утверждением – откуда такие данные? Практика показывает: там, где компании в достаточной степени понимают, что такое SIEM и не рассчитывают на "скатерть-самобранку", внедренное решение приносит пользу в размере даже большем, чем первичные ожидания.

Ожидания всегда связаны с какими-то предварительными условиями успеха того или иного внедрения. Результат внедрения SIEM как довольно сложной системы зависит от многих факторов. Часть из них безусловно относится к самому SIEM-решению от производителя и его функциональности, но довольно много факторов находятся и на стороне самого заказчика. Поэтому результат внедрения SIEM и его успешность будут во многом зависеть также и от уровня профессионализма администраторов SIEM и качества настройки интеграции с источниками.

Владимир Бенгин

– Согласно нашему опыту, эффективно работает одна из десяти SIEM-систем.

Почему так происходит? Во-первых, в традиционных SIEM-системах правила корреляции "ломаются" на второй же день, они не способны адаптироваться к изменениям. Правила приходится или бесконечно переписывать, или принять факт их нежизнеспособности и использовать SIEM как лог-коллектор. Дорогой лог-коллектор. Во-вторых, каждый специалист заказчика должен быть экспертом, способным проанализировать актуальные угрозы и выявить факторы компрометации, на основе которых можно разработать корреляционные правила. И в-третьих, начиная работать с SIEM, заказчик входит в бесконечный круговорот взаимодействия с интегратором по подключению новых источников логов и их адаптации в случае обновления продуктов.

В результате SIEM работают только в тех немногих компаниях, где есть десятки специалистов по безопасности. Далеко не все компании в России могут собрать команду высококвалифицированных ИБ-специалистов, а требовать так много от заказчика означает поставить крест на реальной работе SIEM-системы.

Роман Ванерке

– Использование любой системы – это в первую очередь персонал, затем процессы и уже потом сама система. Наличие системы без обученного персонала не даст особого эффекта. Эффекта не будет, если не использовать систему в рамках процессов обеспечения ИБ, например, если не реагировать на выявляемые инциденты, не вести соответствующий документооборот.

Зачастую при внедрении отталкиваются не от угроз и связанных с ним методов реализации угроз, а от – "подключите мне все источники, настройте мне все ваши правила, и я хочу получать уведомления по ним". На выходе тогда получится как в старой сказке про пастуха и волков, система будет заваливать инцидентами и на них никто не будет реагировать.

В компаниях, где внедряют подобные системы, как правило не знают, для чего им нужен SIEM, не понимают, какие сценарии хотят автоматизировать. Хорошим подспорьем в этом случае может быть накопленная база проведенных расследований – посмотреть, с какими инцидентами компания столкнулась за прошедший год-два и реализовать их выявление в создаваемой системе.

SIEM – это в первую очередь "сигнатурный" подход к выявлению угроз – в системе настраиваются правила, которые описывают выявление известных на момент развертывания угроз. Эти "сигнатуры" необходимо создавать в процессе эксплуатации системы.

Также стоит отметить, что SIEM – это не коробочный продукт, с системой необходимо работать – реализовывать новые сценарии выявления ИБ, создавать новые правила, оптимизировать текущие, реагировать на выявляемые инциденты, выпускать отчеты.

Тимур Ниязов

– Причин отсутствия ожидаемого результата несколько.

Первая – внедрение "SIEM ради SIEM". Требования по мониторингу и управлению событиями встречаются все чаще в различных отраслевых стандартах, федеральных законах, законодательных актах и распоряжениях правительства. Нередко мы наблюдаем ситуации, когда организации внедряют SIEM не для того, чтобы извлечь реальную пользу от этого решения, а для того, чтобы пройти очередной аудит и получить заветный сертификат соответствия (например, PCI DSS или проверки РКН по защите ПДн).

Причина вторая – завышенные ожидания. Многие забывают, что SIEM – прежде всего является системой мониторинга и управления событиями ИБ. При этом от нее ждут, что она будет выступать в качестве DLP, системы обнаружения и предотвращения вторжений, систем противодействия мошенничеству, систем класса IDM и IAM. Но необходимо помнить, что систему все же необходимо использовать по ее прямому назначению (как пример: ни один смартфон не заменит полноценного зеркального фотоаппарата).

Третья причина – отсутствие должного внимания к системе. SIEM-система не является статичной. Все прекрасно понимают, что векторы атак и принципы их реализации постоянно меняются. В связи с этим логика, которая закладывается в SIEM-систему, должна адаптироваться к окружающей среде. Необходимо постоянно вносить изменения в правила корреляции событий для того, чтобы эффективно и своевременно обнаруживать новые виды инцидентов. Если этим не заниматься, SIEM превращается в черный ящик с большим количеством избыточных правил, потребляющих огромное количество аппаратных ресурсов (серверы, СХД и т.д.).

Никита Цыганков

– Потому что процесс развития SIEM, к сожалению, очень часто заканчивается в момент сдачи системы в промышленную эксплуатацию. Вендор или интегратор производит, по сути, базовую настройку системы с настройкой выявления высокоуровневых инцидентов, но для развития и работы SIEM на "полную мощность" этого недостаточно. Система должна развиваться постоянно, но зачастую мы сталкиваемся с ситуацией непонимания принципов работы и необходимости совершенствования SIEM в целом, что ведет к оставлению ее в первоначальном состоянии, и как результат – отсутствие ожидаемого результата от внедрения.

– Какие источники должна поддерживать SIEM в первую очередь? Существует ли некий "базовый набор" для SIEM?

Олег Бакшинский

– Базовый набор источников, конечно, существует. Без него было бы невозможно продавать SIEM. Однако этот базовый набор обычно очень условен и подходит для выявления базового же набора инцидентов. И этого базового набора скорее всего хватит для 80, а может, и 90% инцидентов. А вот остальные 10–20% потребуют большего внимания и настройки SIEM как в части правил корреляции, так и анализа логов с источников.

В качестве минимального базового набора можно привести следующий список: Endpoint, AV, FW, Proxy, DNS, User Logon (LDAP, Radius).

Владимир Бенгин

– Существует "золотой" набор источников, с которых мы обычно начинаем. Они абсолютно универсальны и не зависят от выбранной SIEM и масштаба инфраструктуры заказчика. В первую очередь это средства защиты информации, такие как антивирусы, межсетевые экраны, системы предотвращения вторжений. Подобные инструменты выявляют инциденты, аномалии и пишут множество логов, но в них, как правило, мало кто смотрит. Например, в IPS может быть тысячи срабатываний, но какие действительно важны? SIEM при правильном подходе отвечает на этот вопрос.

Но средства защиты – лишь верхушка айсберга. В базовый набор источников входит сетевое оборудование (коммутаторы, маршрутизаторы), а также операционные системы на серверах, в DMZ-сегментах, контроллерах доменов и на различных элементах критической инфраструктуры. В их логах содержится большая часть информации, которую нужно проанализировать в случае инцидента. Важно также подключать NetFlow.

Зачастую в базовый набор источников для SIEM включают собственную разработку заказчика, критически важную именно для него систему. Несанкционированные изменения в таких системах могут напрямую влиять на работу компании – например, если злоумышленник попал во внутреннюю сеть и подменил документ в системе документооборота.

Роман Ванерке

– Любая SIEM-система должна обеспечивать поддержку широкого набора источников событий, а также обеспечивать удобный, понятный и продвинутый способ подключения источников, не поддерживаемых производителем.

Наиболее часто подключаемые на первом этапе – это понятные для всех средства и системы защиты ИБ – периметр организации и, следовательно, все, что с этим связано – МЭ, IPS, VPN, прокси, а также традиционные источники – Active Directory, антивирус, системы защиты электронной почты, сетевое оборудование

Тимур Ниязов

– Я бы сказал, что существует минимум, в отсутствие которого нецелесообразно заниматься вопросом внедрения SIEM. К этому минимуму относятся: антивирус, периметровые средства защиты (межсетевые экраны, IDS/IPS), контроллер домена и средства анализа уязвимостей.

Никита Цыганков

– Очевидно, что SIEM должна поддерживать сбор информации с широко распространенного набора информационных систем, сетевого оборудования, антивирусных систем и средств защиты информации, например ОС Windows, *nix, Cisco, Symantec и т.д. Под "базовым набором" следует понимать тот состав систем, которые поддерживаются SIEM "из коробки".

– Должна ли SIEM иметь собственные механизмы сбора информации?

Олег Бакшинский

– Я считаю, что SIEM-решение не обязательно должно иметь собственные механизмы сбора. Однако для увеличения скорости обработки и выявления инцидентов в проактивной фазе близко к реальному времени это может быть полезно. Если же мы исследуем информацию постфактум, пытаясь выявлять инциденты по архиву, то можно использовать SIEM и без собственных механизмов сбора.

Владимир Бенгин

– Каждая система SIEM имеет широкий набор механизмов сбора, включая Syslog, SSH и др. Но задача SIEM – это не просто сбор логов, а выявление инцидентов ИБ. Мы давно поняли, что обычное накопление данных и попытка построить на этой основе корреляционные правила не работают. Современным системам такого класса требуются механизмы постоянного обогащения и актуализации ИТ-инфраструктуры. Наша система, к примеру, получает данные не только из подключенных внешних источников, но и задействует собственные технологии активного и пассивного аудита. Информация берется из анализа сетевого трафика на уровнях L2–L7, из операционных систем – о файловых событиях, о запуске процессов и сетевых соединениях и т.д. Другими словами, мы собираем данные, благодаря которым система видит полную картину состояния инфраструктуры на любой момент времени. Это принципиально новый подход к работе SIEM, который позволил нам заложить в продукт возможность создания правил корреляции, которые продолжают адекватно работать даже после изменений IP-адресов, MAC-адресов и других параметров сетевых узлов.

Роман Ванерке

– На сегодняшний момент многие решения ИБ поддерживают отправку событий по Syslog в форматах ведущих SIEM-решений, но остается много других источников, события с которых необходимо собирать с помощью самого SIEM. Для этого должны использоваться традиционные способы сбора – syslog, чтение файла/каталога, подключение к базе данных, SNMP, http и т.п.

Никита Цыганков

– Данная задача необязательна для SIEM, обязательным критерием выступает использование штатных механизмов сбора информации, поддерживаемых всеми источниками событий в организации, что делает SIEM более гибкой и удобной в процессе настройки и эксплуатации.

– Как много данных нужно собрать, чтобы гарантировать выявление инцидентов?

Олег Бакшинский

– Гарантировать 100%-ное выявление инцидентов невозможно! Можно гарантировать обратное – обязательно будут не выявленные с помощью SIEM инциденты.

Для более высокого процента выявления инцидентов лучше использовать множество данных из множества источников с применением множества технологий, не ограничиваясь возможностями только самих SIEM-решений, но дополняя их различными инструментами детектирования атак на рабочих станциях и серверах, в хранилищах данных, на периметре и внутри сети.

Владимир Бенгин

– Производители SIEM-систем могут уверять заказчика, что данных много не бывает и собирать надо все. Но в больших компаниях за день могут аккумулироваться несколько терабайт данных. Для подобных задач нужны быстрые хранилища, а это означает космическую стоимость. Каждый заказчик должен определить приоритеты: контролировать выполнение внутренних политик безопасности, отслеживать взаимодействие с теми или иными ИТ-системами и др. Например, у государственных учреждений много разработок, сделанных на субподряде. Зачастую в них невозможно выявить виновника инцидента, нет информации о пользователях и времени их входа. Сбор информации с критичных систем, обслуживаемых на аутсорсинге, является крайне важным в таких инфраструктурах.

Тимур Ниязов

– На мой взгляд, большой объем собираемых SIEM данных абсолютно не гарантирует выявление нужных инцидентов. При внедрении SIEM необходимо учитывать другой фактор: чем больше критичных источников и средств защиты подключено, тем больше вероятность выявить реальный инцидент. В то же время большое количество источников не всегда влечет за собой большой объем данных. Не все типы событий в журнале могут быть полезны и информативны – это зависит от источника.

Никита Цыганков

– Это зависит от постановки задач на выявление инцидентов. Например, если политикой компании определено, что неактивные учетные записи должны блокироваться по истечении 90 дней, то очевидно что для выявления инцидента нарушения политики необходимо собирать данные все эти 90 дней. В любом случае более остро стоит вопрос не столько количества собранных данных, сколько корректности настройки аудита источников данных, уровня журналирования и применения расширенных параметров аудита.

– Кто должен писать правила корреляции: вендор, заказчик, интегратор?

Олег Бакшинский

– Выполнением задачи должен заниматься тот, кто умеет это делать. При использовании вендорского решения лучшими знаниями самого продукта обладает вендор. Интегратор при определенной вовлеченности в процесс и обучении может также поднять свой уровень знаний о продукте довольно высоко. Но ни вендор, ни интегратор не знают все потребности заказчика, как устроена инфраструктура заказчика во всех деталях. Кстати, и сам заказчик это не всегда знает. Поэтому логичным кажется ответ: писать правила корреляции лучше вендору или опытному интегратору по поручению и под руководством заказчика.

Владимир Бенгин

– Сегодня на рынке производителей систем SIEM сложилось мнение, что вендор должен предоставить богатый функционал, а написание правил корреляции является работой интегратора и заказчика. В результате каждый заказчик вынужден проходить очень длинный, долгий и дорогой путь, что в большинстве случаев приводит к неработоспособности внедренных систем SIEM.

Мы хотим такую практику поменять. Разумеется, для вендора и интегратора лучше уметь писать правила корреляции. Но правила корреляции и информация о необходимости подключения определенных источников также должны приходить из коробки, как обновление сигнатур IDS или обновление базы антивирусов.

Ежегодно наши эксперты проводят сотни тестирований на проникновение, что позволяет накапливать огромную базу знаний о способах взлома самых специфических систем. Кроме того, наш экспертный центр безопасности PT ESC дает понимание актуальных техник поиска и выявления инцидентов. Поэтому в базовый набор источников у нас всегда включен антивирус. Антивирусы

так или иначе, не сразу, но ловят инструменты APT-групп и даже именуют у себя их как семплы. Это не очень длинный список с персонифицированным инструментарием. Знание техник и тактик дает возможность правильно приоритизировать поток событий от антивирусных средств и своевременно реагировать на APT-атаки. Когда мы начали подключать к SIEM антивирусы, за один месяц совместно с коллегами из PT ESC мы выявили семь таких доказанных инцидентов. Хакерские группы сидели там годами, несмотря на наличие дорогих анти-APT-решений. Именно поэтому мы спорим с тем, что вендор может давать только функционал. Производитель SIEM может и должен давать экспертизу.

Тимур Ниязов

– Правила корреляции должен писать, прежде всего, квалифицированный специалист. При отсутствии такого человека в штате заказчик всегда может обратиться за помощью как к интегратору, так и к вендору.

Никита Цыганков

– Идеальная ситуация – когда правила корреляции пишутся всеми. Вендор предоставляет базовый набор правил, который подходит для большинства заказчиков. Интегратор создает и настраивает правила корреляции под конкретные нужды заказчика, учитывая пожелания и особенности функционирования систем и средств. Заказчик же должен совершенствовать созданные правила для минимизации ложных срабатываний, а также для создания более низкоуровневых правил корреляции на основе расследования инцидентов.

– Как снизить количество ложных срабатываний на SIEM?

Олег Бакшинский

– Путем тщательной настройки правил срабатываний. Другого способа пока никто не придумал. Однако с развитием платформ реагирования на инциденты (IRP) и машинного обучения у нас появилась возможность анализировать более детально ложные срабатывания и делать выводы, помогая перенастраивать правила срабатываний на SIEM. В этой связи стоит отметить, что компания IBM – одна из первых на рынке, кто предлагает интегрированные решения SIEM и IRP с наличием такой возможности.

Владимир Бенгин

– В большинстве систем SIEM проблема ложных срабатываний решается с помощью персонализации тех или иных типовых правил корреляции и назначением огромного листа исключений. Такой подход приводит к тому, что правила из коробки никогда не работают: заказчик или интегратор вынужден переписывать все сам. Например, использование обычного ПК несколькими пользователями одновременно может вызвать подозрение на инцидент (во многих SIEM-системах есть такое правило корреляции из коробки). Но если SIEM не знает, что перед ним терминальный сервер, то это вызовет миллион ложных срабатываний.

Роман Ванерке

– Если идти от методов реализации угроз и связанных с ними сценариев, то количество ложных срабатываний будет не столь велико. Но ключевым фактором является реагирование на инциденты, проведение расследований и тюнинг правил по их результатам.

Тимур Ниязов

– Как я говорил ранее, SIEM – это не статичная система. Правила корреляции необходимо постоянно "тюнинговать". Хорошей практикой является проведение тестов на проникновение для внесения корректировок в правила корреляции и более раннего обнаружения нарушителя.

Никита Цыганков

– Необходимо производить постоянный мониторинг работы правил корреляции с целью задания исключений или изменения логики работы правил в случае необходимости.

– Должны ли производители SIEM предоставлять какой-то обязательный набор сервисов своим заказчикам?

Олег Бакшинский

– Каждый производитель имеет желание и возможность предоставлять набор сервисов по внедрению и сопровождению своих SIEM-решений, но не все производители имеют локальные ресурсы для таких сервисов. До недавнего времени и сами заказчики не хотели тратить на них бюджеты. Однако в последний год мы замечаем изменение этой тенденции в позитивную сторону. Похоже, что качество работы посредников и принципы разумной экономии не позволяют больше покупать задорого некачественные сервисы, и заказчики все больше внимания обращают на сервисы самих производителей.

Владимир Бенгин

– Да. Прежде чем выявлять связи между событиями, необходимо собрать логи. Процесс лог-менеджмента весьма сложен, и его нельзя перепрыгнуть. Необходимо настроить источники и ротацию, понять, какой объем информации мы готовы обрабатывать и поддерживать, согласовать все с ИТ и т.д. После этого нужно сделать данные логи читаемыми. Десятки различных систем по-разному логируют: кто-то пишет в файл, кто-то в базу данных, информация может быть структурирована и не очень. Далее эти операции зацикливаются: заказчик переводит свои ИТ-системы на новые версии, интегратор снова и снова адаптирует логи. Мы решили помочь и заказчикам, и интеграторам и рамках технической поддержки осуществлять подключение всех источников силами наших экспертов. Например, при переходе заказчика на новую версию SAP подключаются наши эксперты по SAP. Иногда к взаимодействию подключается разработчик бизнес-системы, иногда мы берем ее как черный ящик и исследуем самостоятельно.

Роман Ванерке

– Назрела потребность в получении обновлений по готовым правилам, которые могут быть применены для широкого круга компаний. Примером может служить выявление актуальных угроз (WannaCry, Petya) по ключевым IOC – URL, md5 суммы, IP-адреса.

Тимур Ниязов

– У каждого из представленных на российском рынке производителей SIEM есть ряд сервисов, которые они предлагают заказчикам. Это и Threat Intelligence, и различные консалтинговые услуги (оценка уровня зрелости SOC, аудит инсталляции и проверка корректности настроек), и инженерные ресурсы (привлечение специалистов вендора на стадии внедрения системы). Безусловно, набор сервисов должен быть, и он есть.

Никита Цыганков

– Безусловно, как минимум это доступ на порталы загрузки актуального программного обеспечения, документации, порталы технической поддержки и лицензирования. Несомненным плюсом является наличие портала, на котором можно задать вопрос специалистам со всего мира, получить доступ к лучшим практикам, а также разработанным наборам готовых правил корреляции.

– Какими компетенциями и навыками должен обладать пользователь SIEM?

Олег Бакшинский

– Пользователь администратору рознь. Но постараюсь ответить просто. Если вы понимаете, как расшифровывается аббревиатура SIEM и можете по каждой букве дать компетентное подтверждение своих навыков, то вы сможете быть хорошим пользователем SIEM. Навыки работы администратором, знание регулярных выражений, понимание инцидентов, векторов атак, анализ рисков и многое другое, как ни странно, неплохо умещается в эти четыре буквы.

Владимир Бенгин

– Эффективно использовать настроенную систему SIEM может человек даже с невысокой квалификацией в области ИТ. Задача подобных систем и состоит в том, чтобы обработать множество событий и перевести их в понятные сообщения. Если же человек захочет настроить систему самостоятельно (писать правила корреляции, подключать источники), то это, разумеется, потребует специализированных знаний.

Тимур Ниязов

– Формальные требования к пользователям SIEM выглядят следующим образом:

- высшее техническое образование;
- опыт администрирования Linux/UNIX-систем, сетевого оборудования (коммутаторы, маршрутизаторы), Web-серверов, межсетевых экранов;
- опыт работы с FOSS IDS/IPS, знание протоколов и аналитических утилит (Snort, Suricata, tcpdump, WireShark);
- наличие знаний протоколов стэка TCP/IP и модели OSI;
- опыт работы с решениями Vulnerability Assesment;
- наличие знаний основ программирования и скриптов;
- аналитический склад ума;
- стрессоустойчивость.

Но по сути каждый пользователь SIEM должен пройти вендорский курс и получить базовые навыки работы с системой. ●

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

UEBA, или поведенческая аналитика

Базовая функция всех систем безопасности будущего

Сергей Добрушский, *руководитель направления защиты баз данных и Web-приложений, "МФИ Софт"*

С легкой подачи Gartner термин UEBA (User and Entity Behavior Analytics), или поведенческий анализ пользователей и сущностей как процесс кибербезопасности для детектирования внутренних угроз, атак или мошенничества, обрел популярность среди вендоров и специалистов в сфере информационной безопасности. Давайте попробуем разобраться, что же такое UEBA. Новый класс решений? Новый модуль в существующих решениях? Какие задачи возлагаются на UEBA-системы? Какие цели преследуются? И как эти возможности реализуются на практике?

Основные цели UEBA – оптимизация расследования инцидентов за счет сокращения как времени расследования, так и числа сотрудников, в нем задействованных. Еще одна цель – повышение качества выявления инцидентов, по сути, предотвращение инцидентов, которые могут произойти в компании. И отсюда следует еще одна цель – прогнозирование, или управление рисками информационной безопасности.

Новая технология для проверки легитимного поведения

Причиной популярности технологии UEBA стал рост количества данных, с которыми приходится ежедневно работать офицерам ИБ. Развиваются технологии больших данных, причем не только как часть систем информационной безопасности, но и как часть защищаемых систем. В то же время растет компетенция злоумышленников, увеличивается сложность атак с целью хищения критичной информации или ее модификации в информационных системах. Их становится крайне сложно отличить от штатного, легитимного поведения пользователей. Все это потребовало новых решений по защите информации и предотвращению инцидентов, которыми отчасти и стали технологии UEBA.

Новый модуль в старых системах, а не новый класс решений

Одни эксперты говорят, что UEBA – это отдельная интеллектуальная SIEM-система, в которую включена логика