Современные тенденции развития SIEM-решений

SIEM-решения как один из ключевых элементов инфраструктуры безопасности корпоративных данных набирают популярность с каждым годом. В публикации дан обзор эволюции этих решений, а также приведен анализ тенденций и перспектив их развития.

Александр Кузнецов – руководитель отдела НТЦ "Вулкан".

Алексей Федоров – ведущий инженер НТЦ "Вулкан".

Введение: современный рынок SIEM

Термин "SIEM" (Security Information and Event Management) появился в 2005 г. благодаря сотрудникам аналитического агентства Gartner, которые наделили новой аббревиатурой симбиоз решений двух классов:

- *Security Information Management (SIM) – инструменты для работы с журналами событий и формирования ретроспективной отчетности;*
- *Security Event Management (SEM) – инструменты для мониторинга событий информационной безопасности в режиме, близком к реальному времени, а также для управления инцидентами ИБ.*

Источниками событий для SIM/SEM/SIEM являются компоненты информационно-телекоммуникационной инфраструктуры (активное сетевое оборудование, операционные системы серверов и рабочих станций, приложения, средства защиты информации, системы хранения данных, средства виртуализации и т.п.).

SIEM-решения уверенно занимают свое место в корпоративных системах обеспечения информационной безопасности (СОИБ), становятся ключевыми элементами центров управления ИБ (Security Operation Center, SOC). Вендоры и интеграторы активно продвигают на рынке десятки различных SIEM-продуктов, среди которых, безусловно, имеется своя когорта лидеров.

С момента своего появления решения класса SIEM активно развивались. Их развитие сопровождалось слияниями и поглощениями между игроками ИТ/ИБ-рынка и перспективными компаниями-разработчиками. В этом развитии каждый вендор старался идти в ногу с современными тенденциями рынка ИБ. В результате на выбор конечному потребителю представлено несколько десятков (по нашей оценке – более 80) различных SIEM-решений, но действительно лидерские позиции достались только нескольким крупным компаниям, среди которых такие гиганты, как: EMC (RSA), IBM, HP и Intel (McAfee).

Слияния и поглощения

Новости последнего десятилетия с рынка M&A в области ИТ и ИБ являются хорошей иллюстрацией к пониманию современной расстановки сил в квадранте лидеров Gartner для SIEM-решений.

В 2006 г. в результате продолжающегося "шопинг-тура" корпорация EMC приобретает компанию RSA Security и делает ее своей дочерней компанией, отвечающей за разработку решений в области ИБ. В том же, 2006 г., EMC приобретает компанию Network Intelligence и передает ее SIEM-решение enVision в RSA Security. Таким образом, на рынке появляется SIEM-решение RSA enVision, которое до 2009 г. будет занимать первое место в правом верхнем "магическом" квадранте Gartner и являться законодателем мод в данной области.

В 2010 г. компания HP покупает компанию ArcSight (имеющую к этому моменту за плечами обширную историю разработки и продвижения своего SIEM-решения). В этом же году HP ArcSight, по мнению Gartner, обгоняет решение RSA Security и занимает первое место в рейтинге экспертной организации, находясь и поныне там.

В 2011 г. компания IBM приобретает американского разработчика – компанию Q1 Labs. Вместе с рядом других продуктов Q1 Labs в портфель "голубого гиганта" переместилось решение QRadar, вышедшее на второе место в "Magic Quadrant for Security Information and Event Management".

В том же 2011 г. McAfee покупает компанию NitroSecurity. SIEM-решение этого альянса переместилось из правого нижнего в правый верхний квадрант Gartner и, по результатам исследования рынка за 2012 г., заняла третье место в мировом рейтинге SIEM.

Ретроспектива борьбы четырех лидирующих компаний за звание "чемпион среди производителей SIEM-решений" в рамках последней пятилетки показана на рис. 1.

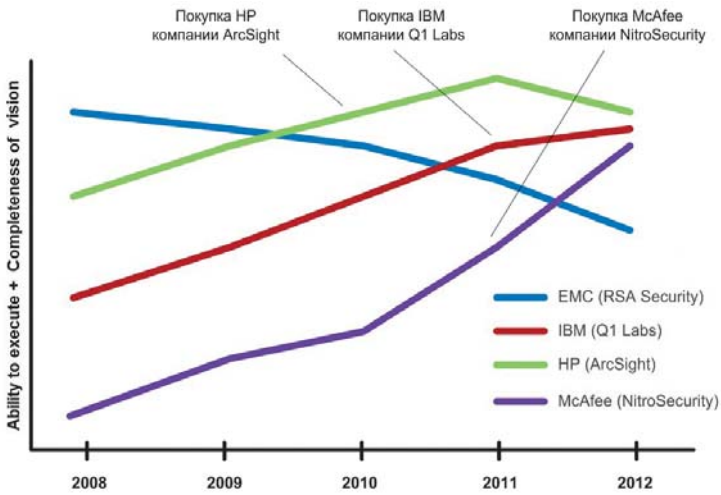

Рис. 1. Динамика положения лидеров рынка SIEM – "Magic Quadrant for Security Information and Event Management" по мнению Gartner.

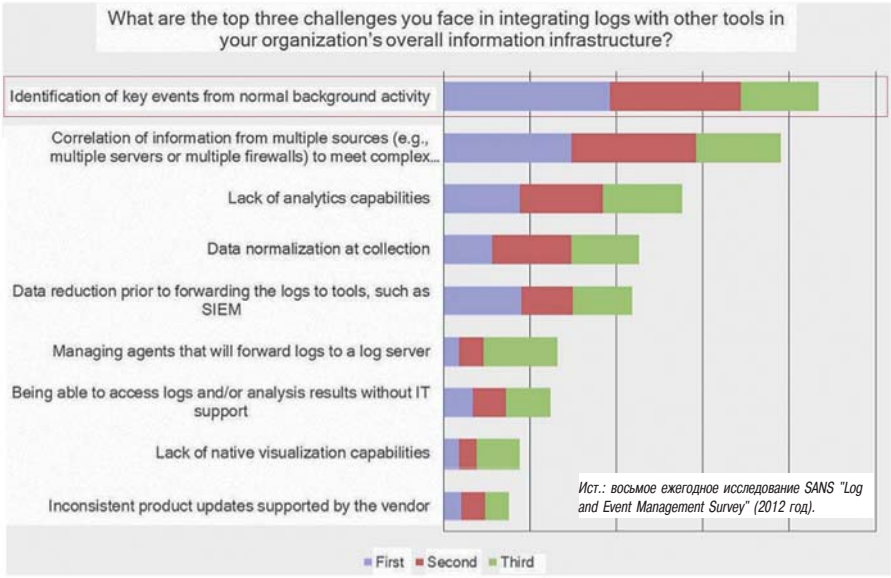

Рис. 2. Организации, занимающиеся лог-менеджментом, не способны отделить обычные или штатные данные от действительно важных или подозрительных, на которые следует обращать внимание.

В целом, нынешний рынок SIEM-решений сформировался в 2011 г., когда корпорациями IBM и McAfee были приобретены динамично развивающиеся компании Q1 Labs и Nitro Security, соответственно. Эти компании и сегодня показывают рост на рынке SIEM-решений, и захваченное HP лидерство может пошатнуться уже в 2013 г.

В России рынок SIEM-решений отличается от мировых усредненных значений. Ключевым отличием являются резкое доминирование HP ArcSight и относительно невысокая доля McAfee и IBM. Впрочем, ситуации на рынке свойственно меняться, и некоторые сдвиги уже замечены экспертами. Кроме того, следует учитывать, российский рынок ИБ традиционно является менее прозрачным, чем западный, и в этих условиях аналитика специалистов не претендует на высочайшую точность.

Быстрее, выше, сильнее

Продукты класса SIEM – явно не дешевые средства, и ключевые игроки продолжают войну за кошельки своих клиентов.

SIEM-решения должны развиваться с опережением потребностей рынка, чтобы оставаться на лидирующих позициях и быть востребованными. В настоящее время классическое SIEM-решение, сочетающие в себе только инструменты по работе с журналами событий, поступающих от компонентов ИТ-инфраструктуры (сбор, хранение, корреляция, проверка на соответствие требованиям, уведомление), является "устаревшим" и не может удовлетворить всех потребностей зрелой компании.

При этом сами потребности рынка ИБ постоянно растут, процессы защиты информации требуют новых механизмов и технологий, которые способны выявлять, предотвращать и разрешать все более и более сложные инциденты ИБ. Рост данных потребностей, в первую очередь, обусловлен внешними факторами, а именно: резким увеличением количества методов реализации угроз ИБ, в том числе появлением "постоянных угроз повышенной сложности" (Advanced Persistent Threat), формированием рынка купли-продажи "уязвимостей нулевого дня" (0-days), а также популяризацией "Хактивизма" (Hacktivism) и активизацией правительств различных стран в области кибер-войн.

В складывающихся условиях выявить несанкционированную и/или злонамеренную активность по отдельным признакам становится практически невозможно, т.к. она очень качественно "завуалирована" под санкционированную или легальную деятельность. Это же подтверждается институтом SANS, в рамках восьмого ежегодного исследования "Log and Event Management Survey" (2012 г.): "Организации, занимающиеся лог-менеджментом, не способны отделить обычные или штатные данные от действительно важных или подозрительных, на которые следует обращать внимание" (рис. 2).

Не упрощает ситуацию и непрерывный рост объема данных, обрабатываемых в информационных системах и циркулирующих в корпоративных сетях; увеличение количества событий, генерируемых компонентами ИТ-инфраструктуры, и уровень их детализации.

В связи с этим ИБ-специалистам требуется комплексный ретроспективный анализ больших объемов данных, учитывающий поведенческий характер пользователей и различных процессов, проходящих в информационных системах и сети, для выявления аномалий и локализации проблем (Network Behavior & Anomaly Detection). А для этого необходимы высокопроизводительные и масштабируемые решения, интернирующиеся с большими хранилищами. При этом используемые "классическими" SIEM-решениями технологии и механизмы остались на уровне 2000-х годов.

Что предлагают лидеры рынка SIEM сегодня?

В настоящее время само понятие SIEM стало гораздо шире. Сейчас от SIEM-решений требуются новые функции и механизмы, способные более быстро и точно (качественно) выявлять и предотвращать инциденты ИБ, при этом не ограничиваясь анализом данных только из журналов событий. По сути, SIEM-решения нового поколения становится "интеллектуальной платформой обеспечения информационной безопасности" (Security Intelligence Platform).

SIEM-решение нового поколения тяготеет к тому, чтобы сочетать в себе "традиционный" SIEM, а также функции анализа сетевого трафика и управления рисками. По существу, такой "комбайн" уже выходит за рамки классического определения SIEM-решения. Примером может служить история с приобретением в 2011 г. корпорацией EMC американской компании NetWitness, специализирующейся на анализе сетевого трафика. Спустя два года на свет появился новый продукт RSA Security Analytics, который сочетает в себе функции SIEM-системы RSA enVision и технологии платформы для сбора и анализа сетевого трафика NetWitness.

SIEM-решения нового поколения способны не только осуществлять сбор и анализ событий из регистрационных журналов (log-файлов), но и коррелировать их с сетевым трафиком (используя потоки типа NetFlow, sFlow и др.), выполняя функции "глубокого анализа пакетов" (Deep Packet Inspection, DPI). Некоторые SIEM-решения способны записывать все сетевые соединения и переданные в них данные для последующего корреляционного анализа. Таким образом, к функциям SIEM-решения нового поколения добавляются сетевая безопасность и управление большими объемами данных.

Возросший объем обрабатываемых в процессе работы SIEM-решений данных заставил разработчиков полностью отказаться от использования в качестве хранилищ собранных данных реляционных СУБД в пользу нереляционных решений, что позволило получить прирост скорости выполнения обращений к данным, а также в разы сократить объемы дискового пространства, требуемого для хранения данных.

Также эта тенденция "заставила" вендоров вспомнить и о технологии Big Data. Первым SIEM-решением, шагнувшим в сторону технологии Big Data, стало RSA Security Analytics. Сочетание технологии по обработке больших данных с аналитическими методами в области ИБ существенно повышает значимость продукта на рынке SIEM и поможет компании EMC отыграть потерянные лидирующие места в обозримом будущем. Однако технология Big Data в связке с SIEM-решением не является прерогативой только RSA Security Analytics, движение в этом направлении замечено также и у компании IBM, которая недавно представила решение IBM Security Intelligence with Big Data, объединяющее SIEM-решение QRadar с функциями IBM InfoSphere BigInsights. Стоит отметить, что и остальные лидеры рынка SIEM не оставили данную технологию без внимания.

Отдельного внимания требует процесс выбора варианта поставки SIEM-решений, который на сегодняшний день практически всегда включает в себя расчет требуемого дискового пространства или

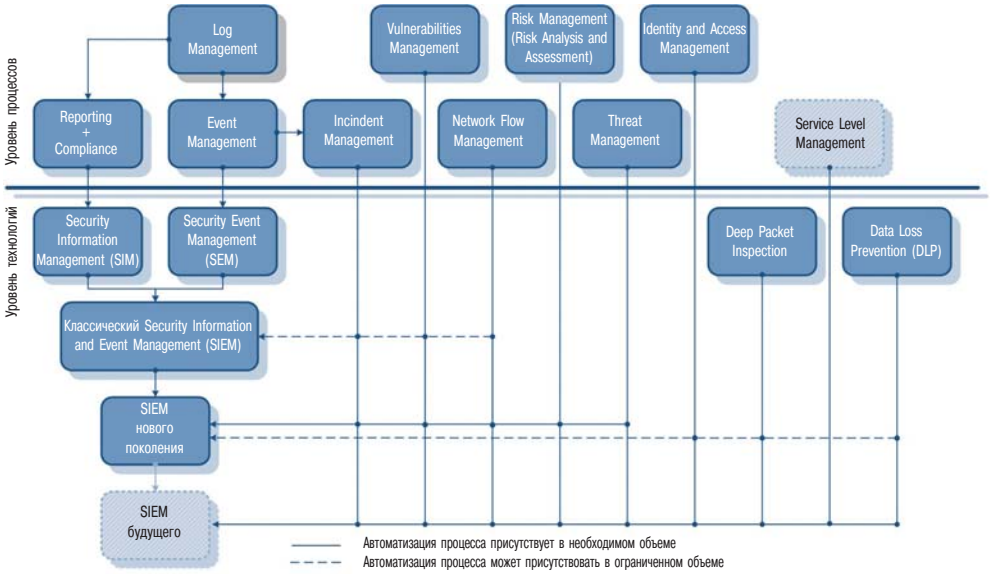

Рис. 3. Тенденции развития SIEM.

вопрос интеграции с СХД. Здесь попрежнему камнем преткновения остаются вопросы приоритезации хранения собранной информации, а именно, обеспечение полного жизненного цикла данных (Data Life Cycle). В данной области от производителей ожидаются не просто рекомендации (например, важные данные храним 1 год, менее важные – 3 месяца; или в ROW-формате храним 1 месяц, в сокращенном – 6 месяцев), а готовые "шаблоны", учитывающие сектор рынка, в котором применяются SIEM-решения (например, кредитно-финансовые учреждения, телекоммуникационные компании и т.д.), и действующие в данном секторе "правила игры". Плюс к этому, рано или поздно должна произойти стандартизация форматов хранения собранной информации, которая позволит, на фоне общей глобализации и интеграции, упростить и унифицировать процессы Управления событиями (Event Managment) в различных организациях, а также применять различные SIEM-решения, используя единую платформу для хранения данных. Мы надеемся, что упомянутые выше сложности, связанные с хранением данных, в ближайшем будущем будут решены производителями.

Не исключено, что в обозримом будущем SIEM-решения обретут элементы и механизмы DLP и IPS-систем, во всяком случае, тенденция к появлению модуля, функционально похожего на DLP и IPS, замечена у многих лидеров рынка.

Одной из черт SIEM-решения нового поколения может стать "подъем" с сетевого уровня модели OSI, т.е. переход от "мышления" в терминологии IP-адресов к "пользовательскому" уровню. При этом в анализе событий на первое место выходят не узлы сети, а пользовательские учетные данные, от имени которых совершаются действия. Такой подход уже демонстрируется отдельными вендорами (в частности, речь идет об HP).

Еще одним нововведением в SIEM-решениях нового поколения становятся центры (сервисы) компетенции (это область Управления угрозами – Threat Management), которые позволяют компании всегда "держать руку на пульсе". В задачу таких сервисов, например, McAfee Global Threat Intelligence (GTI) или RSA Live/RSA FirstWatch, могут входить функции отслеживания вредоносных веб-сайтов, почтовых отправлений, использование аппарата репутации для сетевых узлов Интернет. По сути, в автоматическом режиме с помощью корреляции событий в масштабах сети Интернет такими центрами выявляются злонамеренные активности и новые способы реализации угроз. Эта информация может оперативно транслироваться в SIEM-решения в виде новых правил и/или информационных бюллетеней. Такие центры компетенции, или глобальные сервисы уже становятся неотъемлемой частью SIEM-решений нового поколения. Аналогом такого центра компетенции уже внутри самой компании может стать модуль управления рисками (Risk Management) в составе SIEM-решения, который позволит описать внутреннюю структуру сети, выставить репутационные оценки или уровни критичности компонентам ИТ-инфраструктуры и в последующем коррелировать их с поступающими в SIEM-решение событиями и данными о сетевом трафике.

В целом обобщенные тенденции развития SIEM-решений представлены на рис. 3.

В табл. 1 приведен краткий сравнительный анализ современных SIEM-решений, исходя из описанных выше тенденций развития.

Как видно из таблицы выше, все лидирующие SIEM-решения способны решать примерно схожие задачи. Выделить явного лидера на данный момент достаточно сложно, выбор зависит от ИТ-инфраструктуры заказчика, целей внедрения SIEM и бюджета.

Нельзя сказать, что для владельцев "классических" SIEM-решений описанные выше функциональные возможности недосягаемы. При желании заказчика и умении интегратора к SIEM можно всегда подключить такие системы, как DLP, NetFlow-коллектор или GRC-решение. Однако, как правило, это требует больших затрат и не всегда доводится до логического завершения по различным причинам, в том числе и из-за слабой возможности интеграции и последующей корреляции полученных событий между системами.

В завершении данной части отдельно хочется выделить проект "Management of Security information and events in Service Infrastructures (MASSIF)", разрабатываемый в рамках European Commission's FP7 ICT Work Programme 2009 (FP7-ICT-2009-5) с октября 2010 г., целью которого является создание инновационной технологи, способной предпринять действия по нейтрализации еще не выявленных инцидентов ИБ. Проект использует принцип обработки сложных событий (Complex Event Processing, CEP), суть которого заключается в обработке множества событий на всех уровнях организации с целью выявления наиболее существенных. Такой подход выходит за рамки ИТ/ИБ-инфраструктуры, и позволяет SIEM-решению "захватить" новые рубежи.

Светлое будущее

Что изменится для конечного пользователя с внедрением SIEM-решения нового поколения?

Во-первых, SIEM-решение нового поколения это не просто платформа, на которой необходимо произвести тысячи манипу-

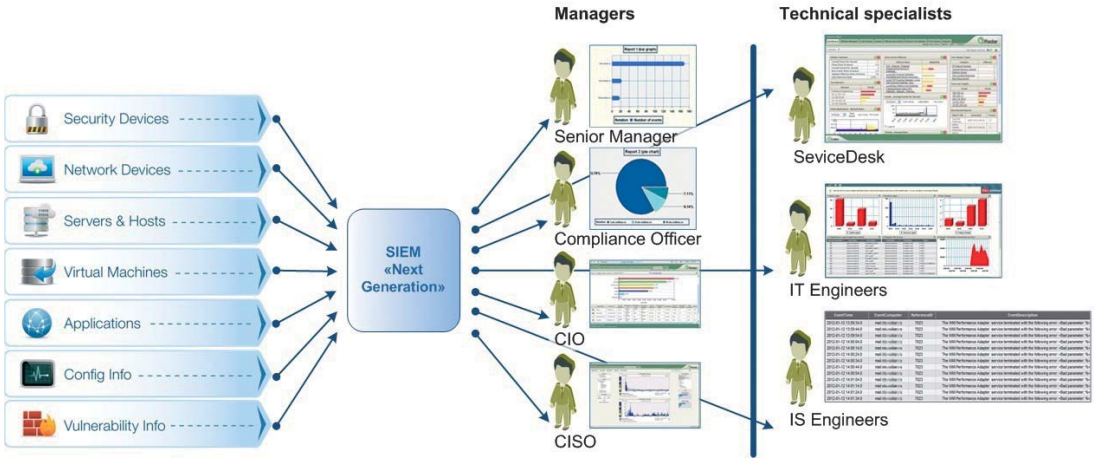

Рис. 4. Современный интерфейс SIEM-решений за счет множества вариаций представлений и наглядности обрабатываемой информации позволяет не только быть на передовой в SOC, но и выступать источником информации для менеджеров, порой далеких от технических тонкостей.

Табл. 1. Краткий сравнительный анализ современных SIEM-решений

Параметр	RSA SecurityAnalytics	IBM QRadar	HP ArcSight	McAfee ESM
Функции классического SIEM-решения	Да	Да	Да	Да
Работа с сетевыми потоками (NetFlow и др.)	Да	Да	Да	Да
Технология Big Data	Да	Да (в связке с IBM InfoSphere Big Insights)	Да (в связке с HP Autonomy IDOL)	Да
Компонент, отвечающий за управление угрозами (Threat Management)	RSA Live/RSA FirstWatch	IBM X-Force	HP ArcSight Threat Detection	McAfee GTI
Реализация риск-ориентированного подхода (Risk-based)	Да (отдельный модуль)	Да (отдельный модуль)	Да	Да (отдельный модуль)
Функции DPI/DLP/IPS или схожие	Да	Да (отдельный модуль)	Да (отдельный модуль)	Да (отдельный модуль)

ляций, чтобы добиться видимого результата. SIEM-решение становится продуктом, который "out-of-box" имеет предустановленные корреляционные правила и репутационные оценки, а также обновляет их на постоянной основе, опираясь на результаты работы различных центров компетенции и/или сообществ. По мере поступления событий и сетевого трафика с компонентов ИТ-инфраструктуры происходит обучение и адаптация SIEM под конкретную ИТ-инфраструктуру.

Во-вторых, SIEM-решения нового поколения отличает хорошая масштабируемость. Все решения имеют гибкие модели внедрений и состоят из модулей (компонентов), которые позволяют начать с небольшого участка сети и/или не полного функционала, а в последующем вырасти до масштаба Enterprise. Такая модель хорошо зарекомендовала себя в классических SIEM-решениях и является выгодной как для компаний-заказчиков, так и для вендоров.

В-третьих, это современный интерфейс, который не привязывается к определенному веб-браузеру или ОС (что зачастую осложняло работу с "классическими" SIEM-решениями). Современный интерфейс многофункционален и быстр, он содержит такие функции и операции, как гиперссылки (hyperlink) и "погружения" (drilldown), способен выводить данные одновременно в графическом и табличном видах. Множество вариаций представлений и наглядности обрабатываемой в SIEM-решениях информации позволяет им не только быть на передовой в SOC, но и выступать источником информации для менеджеров, порой далеких от технических тонкостей (рис. 4). Вообще стоит отметить, что тенденции по управлению ИБ-инфраструктурой стремятся к "единой консоли", возможно, в будущем SEIM-решение и станет той "единой консолью" SOC, которая позволит всем уровням пользователей (от специалиста ИТ/ИБ до CIO/CISO) получать требуемую информацию по состоянию защищенности компании. На этом фоне не исключено полноценное слияние SIEM-решений с системами класса GRC.

В-четвертых, стоит отметить, что SIEM-решения стали более "локализованные". Если раньше вендор смотрел только на программные продукты и языковую поддержку западных стран, то сейчас стоит отметить "дружелюбную" тенденцию в нашу сторону. Конечно, не приходится надеяться на локализацию интерфейса, да и не нужно это современным специалистам, а вот всесторонняя поддержка кириллицы и программных продуктов российского производства может очень положительно сказаться на росте популярности SIEM-решений в регионе EMEA, немалую долю которого составляет Россия и страны бывшего СНГ.

Заключение

Подводя итог, можно с уверенностью сказать, что SEIM-решения за последние годы серьезно эволюционировали. В стандартный перечень задач SIEM-решений нового поколения вошли функции, выполнение которых ранее отдавалось на откуп другим средствам и системам защиты информации. Существуют явные лидеры рынка, однако конкуренция между всеми участниками очень высока, и тот, кто отстанет в развитии своего продукта, может многое потерять.

В России и странах бывшего СНГ SIEM-решения распространяются медленнее, чем за рубежом, хотя потенциал таких систем у нас значителен. В последнее время в этом направлении наметилась положительная динамика. Практически все SIEM-решения нового поколения поддерживают популярные российские антивирусные решения, некоторые шагнули дальше и интегрировали поддержку российских сканеров безопасности. Также не стоит забывать, что в SIEM-решениях есть механизмы по подключению штатно неподдерживаемых компонентов ИТ-инфраструктуры.

Наконец, SIEM-решения, как никакие другие средства защиты информации, чутко реагируют на новые тенденции в области обработки данных. И это неудивительно, ведь аналитика на больших данных способна придать новое качество результатам обработки. А если учесть потребности в анализе классических событий совместно с анализом сетевого трафика, становится очевидным, что скоро технологии Big Data прочно займут свое место в SIEM-решениях, ориентированных на рынок Enterprise.

Александр Кузнецов,
Алексей Федоров,
НТЦ "Вулкан".

Dell SharePlex 8.0: интеграция данных в реальном времени

Май 2013 г. – Корпорация Dell объявила о выпуске новой версии SharePlex™, ведущего решения для репликации данных. Новая версия поддерживает интеграцию данных практически в режиме реального времени, что упрощает создание бизнес-аналитических решений и позволяет повысить эффективность хранения данных. Продолжая линейку решений для репликации данных формата Oracle-to-Oracle, SharePlex 8.0 позволяет заказчикам извлекать информацию из СУБД Oracle 10g/11g и перемещать их в разнообразные структурированные и неструктурированные базы данных.

В современных информационных средах одновременно используются оба представления данных – в структурированном и неструктурированном виде, что усложняет управление информацией, заставляя искать более эффективные методы работы с гетерогенными средами. Учитывая эту тенденцию, специалисты программного подразделения корпорации Dell Software вывели возможности SharePlex за пределы стандартной функции репликации Oracle-to-Oracle. Обновленное решение поможет заказчикам Dell легко справляться с усложняющимися средами хранения информации.

SharePlex 8.0 позволяет при помощи технологии Change Data Capture (CDC) реплицировать данные Oracle в другие базы данных, включая ведущие структурированные базы данных SQL Server, DB2, Sybase, Netezza и Teradata, а также новые неструктурированные базы Hadoop и Greenplum. Технология CDC заменяет традиционный метод извлечения данных: переносу подлежат только те данные, которые были изменены.

В современных условиях данные должны быть доступны 24 часа в сутки 7 дней в неделю и всегда находиться в актуальном состоянии. Новое решение SharePlex создано с учетом этой потребности. Благодаря значительному сокращению числа операций CDC ускоряет процесс обработки информации, что крайне важно для соответствия современным стандартам. Кроме того, это повышает эффективность работы решений бизнес-аналитики, так как анализу подлежит только наиболее актуальная и релевантная информация.

Оставаясь ведущим решением для работы с базами данных Oracle, SharePlex предлагает поддержку новых функций защиты и оптимизации Oracle, включая Transparent Data Encryption (TDE) и Hybrid Columnar Compression (HCC). Функция TDE позволяет организациям защищать важные данные с помощью шифрования, а технология HCC обеспечивает дополнительное сжатие данных на платформах Oracle Exadata, что в свою очередь позволяет разместить больше данных на накопителях с высокой производительностью, увеличить скорость работы и в целом снизить расходы на хранение данных в системах Exadata.