Анализируй это...

Виктор Сердюк, *генеральный директор АО "ДиалогНаука"*
Роман Ванерке, *технический директор АО "ДиалогНаука"*

Человеческий фактор в информационной безопасности является одним из ключевых. С одной стороны, он источник возможных угроз информационной безопасности, а с другой – именно мониторинг поведения легитимных пользователей в информационной системе позволяет выявить возможные несанкционированные действия. Так, например, можно сделать вывод о том, что в случае сильного изменения поведения пользователя его учетные данные могут быть скомпрометированы и от его имени работает кто-то посторонний. Такое изменение поведения также может указывать и на нарушения, связанные с умышленными действиями сотрудника. Именно возможности профилирования и анализа активности пользователей и объектов ИТ-инфраструктуры реализованы в относительно новом сегменте рынка систем защиты, который получил название "средства поведенческого анализа пользователей и сущностей" – UEBA (User and Entity Behavioral Analytics).

Место аналитики

С точки зрения архитектуры механизмы UEBA похожи на решения, предназначенные для мониторинга событий информационной безопасности (SIEM), и даже некоторые производители называют их NGSIEM (Next Generation SIEM). Они состоят из агентов, которые собирают информацию о действиях пользователей, единого хранилища, куда эти сведения собираются из всех источников, и аналитического модуля, который выполняет анализ событий, возможно, в реальном времени и с реакцией на наиболее опасные действия по заранее заданным правилам. Иногда в качестве агента и даже хранилища сведений о действиях пользователей могут выступать сторонние системы, такие как DLP, IDM, SIEM или др. Таким образом, достаточно часто анализ поведения пользователей – это модуль, который использует инфраструктуру другого приложения для получения данных, но дает ему сигналы о выявленной подозрительной активности.

UEBA-решения могут быть реализованы в виде отдельных продуктов либо в виде расширений для уже существующих систем.

Необходимо отметить, что сейчас методики обнаружения подозрительного поведения активно развиваются в связи с появлением доступных технологий машинного обучения и искусственного интеллекта, которые могут самостоятельно, без предварительного обучения выявлять аномальное поведение пользователей и резкое изменение стиля их работы, что вызывает подозрение в компрометации пароля или же попытке доступа к критическим ресурсам без необходимых для этого полномочий. Тем не менее в ряде случаев результаты подобного анализа требуют ручной проверки аналитиком для подтверждения или опровержения гипотезы, выдвинутой системой UEBA. В частности, в составе SOC логично иметь подобный модуль, который давал бы операторам центра реагирования дополнительную информацию о подозрительных действиях пользователей и привлекал их внимание к определенным цепочкам событий.

UEBA-решения

UEBA-решения могут быть реализованы в виде отдельных продуктов либо в виде расширений для уже существующих систем, например SIEM, DLP или PAM (Privileged Access Management) и др. С практической точки зрения служба информационной безопасности может с помощью инструментария UEBA решать следующие задачи:

- выявление скомпрометированных учетных записей. Анализ поведения пользователей может устанавливать, в какой именно момент пользователь начинает вести себя подозрительно, проявляя активность в тех направлениях, которые ранее ему свойственны не были. К сожалению, система UEBA не сможет ответить на вопрос, что послужило причиной

необычного поведения – утечка паролей учетных данных, троянская программа или просто изменение должностных инструкций. Ответить на эти вопросы должен уже администратор безопасности, но привлечь его внимание к подозрительной активности с, казалось бы, легальной учетной записью аналитическая система способна. В первую очередь объектом контроля здесь являются учетные записи привилегированных пользователей, а также тех сотрудников, которые имеют доступ к критическим информационным активам;

- выявление внутренних нарушителей. Собственно, это часть функционала UEBA, которая дополняет возможности DLP-решений, которые сейчас являются основными для поиска так называемых инсайдеров. Конечно, отличить инсайдера-человека от троянской программы, проникшей на компьютер, достаточно сложно, поэтому классические DLP такую задачу решить не могут. Но именно аналитика поведения пользователей может более точно отличить сотрудника, который по глупости установил троянскую программу, от реального злоумышленника, целенаправленно получившего легальные учетные данные в системе и пытающегося добраться до ценной информации;
- мониторинг прав доступа сотрудников. Одной из наиболее сложных задач обеспечения безопасности является минимизация прав легальных пользователей – их права должны обеспечить им доступ ко всем необходимым для них информационным системам и блокировать – ко всем остальным. Обычно достигнуть такого идеального состояния сложно – у пользователей всегда есть некоторые избыточные права доступа. Система анализа поведения пользователя может выявить действительно необходимые пользователю права и обнаружить явно избыточные назначения;
- обнаружение целенаправленных атак. В этом случае именно необычное поведение пользователей или устанавливаемых ими приложений позволит выявить действия хакеров, причем как с помощью вредоносных программ, так и за счет компрометации учетных данных с использованием уже установленных на предприятии приложений.

Служба информационной безопасности может с помощью инструментария UEBA решать следующие задачи:

- **выявление скомпрометированных учетных записей;**
- **выявление внутренних нарушителей;**
- **мониторинг прав доступа сотрудников;**
- **обнаружение целенаправленных атак.**

Современные технологии в составе UEBA

Для решения всех указанных выше проблем современные средства UEBA используют технологии анализа больших данных и те или иные механизмы искусственного интеллекта, которые предназначены для поиска аномалий, профилирования работы пользователя и обнаружения злоупотреблений правами доступа. Для этого они строят модели поведения пользователей и групп, куда эти пользователи входят, и сравнивают их с эталонными для выявления отклонений и нарушений. Причем чем больший массив данных о поведении пользователей анализируется, тем точнее будет построена модель поведения, что позволит более точно предсказать отклонения от нормы и выявить подозрительное поведение пользователей. При этом решения класса UEBA позволяют строить профили не только пользователей, но и объектов ИТ-инфраструктуры – телекоммуникационного оборудования, серверов, приложений, сетевого трафика и др. Это позволяет выявлять атаки не только на основе выявления аномалий в работе пользователей, но и ИТ-систем.

По каждому аномальному поведению пользователя решение класса UEBA увеличивает значение риска по нему и при достижении определенного порога начинает сигнализировать администратору безопасности о наиболее "подозрительных" пользователях. Такой подход позволяет, с одной стороны, создавать инциденты по наиболее вероятным нарушениям, а с другой стороны – минимизировать количество ложных срабатываний.

К сожалению, UEBA-системы не являются "коробочными" и для их внедрения необходимо выполнить большой объем работ по настройке этих средств.

Модули UEBA уже достаточно давно появились в SIEM-решениях, таких как IBM QRadar, ArcSight и Splunk. Однако есть и решения, где аналитика поведения пользователей является основным конкурентным преимуществом, например решение Exabeam. Российские производители также ведут разработки систем подобного класса.

Заключение

На сегодняшний день существует большое количество угроз информационной безопасности, которые можно выявить только за счет поведенческого анализа событий, регистрируемых в локальной сети компании. Использование для этих задач решений класса UEBA позволит предоставить администраторам безопасности эффективный инструмент для выявления атак злоумышленников. ●

С точки зрения архитектуры механизмы UEBA похожи на решения, предназначенные для мониторинга событий информационной безопасности (SIEM), и даже некоторые производители называют их NGSIEM (Next Generation SIEM). Они состоят из агентов, которые собирают информацию о действиях пользователей, единого хранилища, куда эти сведения собираются из всех источников, и аналитического модуля, который выполняет анализ событий, возможно, в реальном времени и с реакцией на наиболее опасные действия по заранее заданным правилам.