Оценка за поведение

Роман ВАНЕРКЕ,
технический директор, АО «ДиалогНаука»

Хакеры часто выдают себя за легальных пользователей: либо перехватывают учетные данные, либо заставляют программы легальных пользователей выполнять опасные команды от их имени. Для системы пассивного контроля такие действия являются разрешенными, поскольку они не всегда могут оценить опасность действий пользователей. Именно поэтому в последнее время начали появляться решения, которые позволяют по действиям пользователей и активности узлов выявлять хакерские «вставки» и подмены. Эти системы получили название «системы анализа действий пользователей и узлов» (User & Entity Behavior Analysis – UEBA).

Контроль и досмотр

Понятно, что для выявления вредоносного поведения необходимо фиксировать все действия пользователя в системе – тогда можно обнаружить аномальные действия, если они случатся. Фиксировать можно как действия пользователя на устройстве – запуск программ, обращение к файлам, попытки удаленного подключения, так и сетевое взаимодействие – загрузка файлов, обращение к веб-ресурсам (особенно если доступ вовне заблокирован), DNS-запросы и многое другое. В первом случае данные можно получить от операционной системы, во втором – от сетевого оборудования. Причем желательно иметь представление об эталонном поведении пользователей и узлов, чтобы точнее выявлять аномалии. Подобная информация накапливается в системных журналах и хранилище системы обработки событий SIEM, однако в самом ядре обработки событий зачастую проблематично строить модели поведения пользователей и узлов сети и выявлять отклонения и аномалии.

Перед службами информационной безопасности часто возникают задачи по анализу поведения конкретных пользователей или узлов, потому и появился целый набор специализированных систем, которые решают прикладные задачи по изучению подозрительной активности пользователей, выявлению инсайдерских действий, обнаружению скомпрометированных учетных записей, некорректно работающих сервисов и проведению расследований. На наш взгляд, для этих задач отлично подходят специализированные решения UEBA.

Системы UEBA могут решать следующие задачи:

- изучение подозрительной активности сервисных, редко используемых и вовремя не заблокированных аккаунтов. К этому же классу задач можно отнести и выявление учетных записей, созданных самими хакерами для закрепления в системе, или совместно используемых аккаунтов. Последний вариант неприемлем для правильно построенной системы защиты, но недобросовестные сотрудники иногда прибегают к подобным упрощениям. Выявление аномалий в активности таких аккаунтов становится поводом для дальнейшего расследования, поскольку опасные действия от их имени очень часто являются результатами взломов;
- выявление инсайдеров и скомпрометированных аккаунтов. Если учетная запись используется часто, но иногда ее владелец совершает опасные аномальные действия, то этому могут быть две причины: он является инсайдером и в определенные моменты осознанно выполняет вредоносные действия либо его учетные данные были украдены хакерами. UEBA позволяет разделить эти ситуации и принять адекватные меры защиты – локализовать инсайдера или просто заменить данные скомпрометированного аккаунта;
- захват привилегированных пользователей. К этому классу можно отнести наиболее сложный для расследования случай заражения вредоносной программой привилегированного компьютера, т. е. рабочего места высшего руководителя или системного администратора. Компрометация их аккаунтов также чрезвычайно опасна. Расследование затрудняется тем, что привилегированные пользователи могут сопротивляться расследованию, и не всегда

потому, что они сами являются злоумышленниками, – просто не хотят, чтобы служба безопасности им мешала. Поэтому изучение поведения таких пользователей является весьма деликатной задачей, которую сложно решить без интеллектуальной системы аналитики поведения пользователей;

- расследование инцидентов. Этот класс задач связан с той неприятной ситуацией, когда обнаружены взлом или утечка данных. В подобных случаях необходимо быстро определить учетные записи, которые получали доступ к скомпрометированным ресурсам, и провести изучение возможных путей проникновения злоумышленников в систему и вывода из нее ценной информации. Это необходимо как для закрытия дыр в защите, так и для наказания виновных.

Детективы и детекторы

Технологически UEBA основаны на принципах глубокого машинного обучения и других методах искусственного интеллекта, которые нацелены на выявление аномальной активности. Для этого в модулях анализа поведения пользователей применяются технологии больших данных, помогающие обработать исторические записи из SIEM и строить максимально точные модели поведения конкретного пользователя, групп пользователей или узла, причем с привязкой к зафиксированным ранее действиям. Это позволяет проводить максимально подробные расследования и обнаруживать не только аномальную активность, но и ее причину.

Собирая данные как из SIEM, так и непосредственно с источников событий, UEBA строит модели поведения и по пользователям, и по группам, членами которых являются пользователи. Например, решение позволяет сравнивать поведение сотрудников, которые имеют одинаковые роли в компании, или подчинены одному руководителю, или находятся в одном офисе. Кроме того, система строит модель поведения узла сети – это могут быть как рабочие станции пользователей, так и, например, серверы. Очевидно, что чем больше будет подано на вход информации об активности пользователей и узлов, тем детальнее будет картина. Например, кроме событий входа и выхода имеет смысл собирать следующие данные: полученные веб-запросы, посылаемые почтовые сообщения, сведения о доступе к периферийным портам ввода-вывода, журналы запуска процессов на узлах, команды по управлению учетными записями, обращение к файлам, вердикты антивирусов и т. д.

Один из примеров решения класса UEBA – Exabeam [1]. В отличие от SIEM-системы, где в качестве единицы измерения используется событие, в решении Exabeam Advanced Analytics используется понятие «сессия», и уже в рамках сессии пользователя или узла система фиксирует происходящие события и, если событие несет в себе угрозу и является отклонением (например, запуск процесса, который до этого ни разу не запускался в сети предприятия), повышает уровень риска для пользователя или узла. При достижении порогового значения система выделяет таких пользователей, чтобы офицер безопасности смог сфокусироваться в первую очередь на них. Чтобы минимизировать ложные срабатывания, необходимо сначала дать системе обучиться – от двух недель до нескольких месяцев.

В результате работы подобных решений формируется план-график (timeline) деятельности пользователя или узла, на котором выделяются наиболее подозрительные моменты его активности. Построенный график является удобным инструментом для изучения поведения пользователей и узлов и расследования инцидентов с возможностью обнаружения взаимосвязей с другими пользователями и узлами на предприятии. При помощи таких графиков служба безопасности может составить максимально подробное представление о процессах, происходящих в информационных системах компании.

Решение такого класса удобно тем, что может поставляться в виде самостоятельного продукта, модуля для корпоративного SOC, программного комплекса или виртуальной машины. Наиболее продвинутые решения способны даже в начальной конфигурации решать достаточно много задач из приведенного выше списка. Например, Exabeam Advanced Analytics позволяет «из коробки» решить до 80% задач, связанных с анализом поведения пользователей и узлов.

Заключение

Следует отметить, что UEBA являются контрольными модулями и не предназначены для защиты информационных ресурсов. Они позволяют обнаружить наиболее сложные атаки, но не предотвратить их или отразить. В то же время UEBA – средство не только обеспечения кибербезопасности, т. е. выявления действий хакеров, но и обнаружения инсайдерских действий корпоративных пользователей. Графики пользовательской активности можно применять в качестве доказательной базы для выявления собственных нечистоплотных сотрудников.

Таким образом, анализ поведения пользователей и сервисов UEBA может стать важным элементом системы корпоративной информационной защиты предприятия, который необходимо правильно использовать для выявления хакерской и инсайдерской активности, скомпрометированных и посторонних учетных записей, контроля соблюдения политик безопасности, принятых на предприятии, для расследования инцидентов и совершенствования всей системы информационной безопасности в целом. ■