# Профилирование активности пользователей для автоматизации выявления инцидентов ИБ

**Виктор Сердюк,** *генеральный директор АО "ДиалогНаука"*
**Евгений Афонин,** *ведущий архитектор решений по информационной безопасности HP ESP*

21 апреля этого года на конференции RSA Security было объявлено о появлении нового продукта в портфеле HP Enterprise Security – User Behavior Analytics (HP UBA), который является дополнительным модулем к системе HP ArcSight. Данный продукт позволяет автоматически обнаруживать инциденты информационной безопасности путем профилирования нормальных поведенческих паттернов активности пользователей.

## Описание

HP UBA позволяет решать следующие задачи:

- анализ любых событий пользовательской активности – доступ к базам данных, файловым каталогам, работа со съемными носителями, операции в корпоративных информационных системах (биллинг, платежи, документооборот, работа с персональными данными) и др.;
- использование готовых математических моделей по профилированию активности на основе полученных событий – группировка однотипных событий (Peer Group Analysis), выявление аномалий (Anomaly Detection), определение штатного профиля работы (Baseline Profiling), определение частоты возникновения событий (Event Rarity);
- применение результатов работы математических моделей к задачам информационной безопасности – выявление инсайдеров, контроль привилегированных пользователей, необычной активности в корпоративных системах: "спящие счета", "доступ к карточкам VIP-клиентов" и пр.

Фактически мы можем создать в системе универсальную карту пользователя, в которой будем автоматически поддерживать актуальными все его атрибуты – даты принятия на работу/увольнения, должность, подразделение, регион и пр. А также на отдельной вкладке вести журнал всех его учетных записей в наших информационных системах. Обладая этой информацией, можно выявлять целый ряд инцидентов безопасности, например:

- обнаружение значительного отличия в активности данного пользователя от рассчитанного профиля активности остальных сотрудников данного подразделения, данного региона, данной должности и т.д.;
- сумма проведенных транзакций по данному продукту превышает наблюдаемые нормально значения за рассчитанные временные промежутки (час дня, день недели, неделя, день месяца, месяц, выходные и пр.);
- ранее не наблюдаемая активность на данном АРМ по работе с административными транзакциями SAP.

## Работа с системой

Хорошо, события мы получили с помощью стандартных коннекторов HP ArcSight, настроили регулярную загрузку данных кадровой информации для формирования универсальной карты пользователя, импортировали и выполнили связывание учетных записей в информационных системах – что дальше?

Дальше система начнет обнаруживать инциденты по тем поведенческим профилям, которые она сформировала автоматически согласно нашим настройкам. Что делать с этим далее? Для сотрудника ИБ система предлагает встроенный интерфейс анализа и визуализации данных по инцидентам, а также она автоматически выполняет агрегацию выявленных инцидентов согласно их уровню риска. Таким образом, мы можем приоритизировать работу аналитика с инцидентами, а также проводить анализ по рискам согласно другим измерениям – пользователям, подразделениям, регионам и пр. Это чрезвычайно важно, поскольку в условиях постоянной нехватки времени в ИБ важно сконцентрироваться над расследованием наиболее важных инцидентов. По итогам расследования и при необходимости система позволяет вводить повышающие и понижающие коэффициенты расчета риска, чтобы адаптировать автоматическую работу системы согласно приоритетам ИБ.

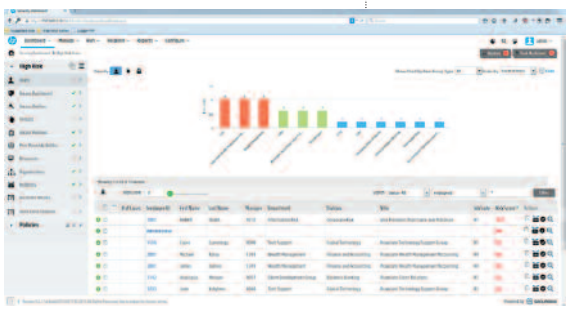
## Заключение

HP User Behavior Analytics стал важным элементом портфеля решений HP Enterprise Security Products, и мы видим к нему большой интерес как со стороны наших существующих клиентов, использующих HP ArcSight ESM, так и людей, которые только начинают знакомство с решениями HP. HP UBA дает возможность использовать инструменты поведенческого анализа, статистики и анализа Больших данных, которые раньше были уделом избранных специалистов.

С нашей точки зрения, использование решения HP User Behavior Analytics позволит существенно повысить уровень информационной безопасности компании за счет возможности выявления инцидентов, которые нельзя было обнаруживать существующими методами. ●

User Behavior Analytics позволяет дополнять события безопасности расширенным контекстом – информацией о пользователе, его рабочем окружении, организационных и других атрибутах. Таким образом, даже если в событии содержится только IP-адрес, мы все равно сможем вычислить ФИО пользователя, который стоял за этой активностью.

Само профилирование выполняется системой автоматически, после того как будут заданы исходные параметры для анализа. Поскольку математические модели универсальны, а использование для сбора событий коннекторов HP ArcSight позволяет привести эту информацию к единому виду, хрупкий баланс между простотой и функциональностью соблюден здесь на все 100%. Хотя часть аналитики и можно выполнить с помощью SIEM-системы, HP User Behavior Analytics позволяет это сделать быстрее, проще и с использованием некоторых функций, уникальных только для него.



Интерфейс HP UBA