Новинки

ArcSight Data Platform

Современные центры управления инцидентами информационной безопасности (ИБ) сталкиваются с постоянным ростом объёмов обрабатываемых данных и ограничениями доступа к ним. ArcSight Data Platform (ADP) предоставляет открытую платформу сбора и обработки событий, которая является ядром инфраструктуры выявления угроз информационной безопасности в масштабах предприятия. Обогащая собираемые события инфраструктуры компании контекстом ИБ в режиме реального времени, ADP предоставляет более полную информацию для аналитики угроз, а также возможности интеграции с Hadoop.

Новшества двух последних лет

- Шина передачи сообщений Event Broker на базе Apache Kafka позволяет непрерывно получать данные из **любого источника** и передавать их **в любую другую систему**
- **Окупаемость** аналитических систем, средств поиска угроз и систем на базе Hadoop **повышается** благодаря использованию структурированных данных, содержащих контекст безопасности
- **Затраты снижаются** за счет передачи только релевантных данных для их дальнейшей обработки системами информационной безопасности и различным ИТ-инструментарием
- Консоль с графическим интерфейсом **упрощает управление**
- **Добавление** новых источников данных **ускоряется** благодаря «мгновенному развертыванию коннекторов»

Это интересно!

- ArcSight Data Platform обрабатывает данные со скоростью **1 млн событий в секунду** — этого достаточно даже для очень крупных предприятий
- **Более 400 готовых коннекторов** ArcSight Data Platform помогут справиться с подключением разнообразных новых источников данных
- В 2017 году журнал SC Magazine отметил ArcSight Data Platform и ArcSight ESM как **«Лучшее SIEM-решение»** (Security Information and Event Management)
- **Обогащение данных в реальном времени** путем добавления в них контекста безопасности позволяет сразу же использовать их в системах аналитики и машинного обучения

1 IDC — «Цифровая Вселенная возможностей: насыщенные данные и растущая ценность Интернета вещей»

Ведущая американская финансовая компания

«ArcSight Data Platform и ArcSight Event Broker позволили нам интегрировать собираемые данные с открытыми (open source) системами… Это свидетельствует о понимании потребностей рынка и зрелости компании-разработчика… ArcSight отлично справляется со своими основными задачами, обеспечивая комплексную защиту и устранение угроз».

Руководитель крупного аэропорта, партнер по кибербезопасности.

«Объемы данных удваиваются ежегодно. К 2020 году они достигнут 44 Збайт»[1]