Пресс-релиз
16 октября 2015 г.

ПАО «Северсталь»
Управление коммуникаций
+7 (495) 926-77-66
news@severstal.com
www.severstal.com

Компания «Инфосистемы Джет»
Отдел PR
+7 (495) 411-76-01
pr@jet.msk.su
www.jet.msk.su
www.facebook.com/jetinfosystems.online

Компания «Инфосистемы Джет» развернула централизованную систему управления событиями информационной безопасности для компании «Северсталь»

16 октября 2015 г., г. Москва – Компании «Северсталь» и «Инфосистемы Джет» запустили в работу единый инструмент управления событиями информационной безопасности (ИБ), автоматизирующий процесс их сбора, хранения и анализа. В результате существенно возрос общий уровень ИБ компании: система обрабатывает порядка 5000 входящих событий безопасности в секунду; общее число инцидентов, которые ИБ-служба может обрабатывать в режиме, близком к real-time, возросло в 10 раз, время, требуемое для сбора необходимой информации по инциденту, сократилось до нескольких минут.

«Мы получили единую консоль мониторинга событий ИБ от большого количества разнородных систем. Из этих событий, по статистике, несколько десятков оказываются инцидентами с различным уровнем критичности, – рассказывает **Константин Иванов, менеджер управления обеспечения информационной безопасности компании "Северсталь"**. – *Нам также удалось свести к минимуму объем ручной обработки данных, и теперь у нас есть возможность оперативно принимать решения на основе аналитики глубиной до полугода».*

Система управления событиями ИБ реализована на базе решения HP ArcSight ESM. Проект охватил 3 географически распределенные площадки компании «Северсталь» в европейской части России.

Эксперты компании «Инфосистемы Джет», используя данные по ИТ-инфраструктуре компании «Северсталь» и существующим процессам обеспечения и управления ИБ, спроектировали и внедрили систему управления событиями. Сегодня к ней подключено более 400 различных источников (в том числе журналы ОС, СУБД, средств антивирусной защиты, сетевой защиты и пр.), настроено более 100 специализированных правил. С целью информационного обогащения была проведена интеграция с рядом нетиповых систем, для которых были разработаны дополнительные коннекторы (порядка 10 шт.): SAP Business Objects, СКУД, портал ИТ-услуг и др.

Выполнена интеграция с системой контроля защищенности и соответствия стандартам (MaxPatrol), предварительно внедренной в ИТ-инфраструктуру компании «Северсталь» (всего более 4000 единиц оборудования, включая рабочие станции и серверы под управлением ОС Microsoft Windows и Unix, сетевое оборудование, СУБД MS SQL и Oracle). Созданный на базе данной системы инструмент в автоматическом режиме по заданному расписанию осуществляет инвентаризацию всей инфраструктуры, определяет уровень защищенности ее компонентов, заблаговременно выявляет уязвимости информационных ресурсов и оповещает о них, формирует рекомендации по их устранению в соответствии с настроенными политиками безопасности (корпоративными и отраслевыми). В результате ИБ-служба компании «Северсталь» получила возможность проактивно выявлять инциденты ИБ, связанные с эксплуатацией злоумышленниками уязвимостей базовых компонентов информационных систем, отсутствием обновлений или небезопасными настройками.

«Созданная система по своим параметрам шире, нежели классический SIEM, – поясняет **Евгений Акимов, директор по развитию бизнеса Центра информационной безопасности компании "Инфосистемы Джет"**. *– За счет более глубокой проработки правил с учетом особенностей процессов и ИТ-инфраструктуры компании (например, по нарушениям парольных политик, нетипичному пользовательскому поведению в домене, аномальной сетевой активности и пр.) система создает инциденты, обогащенные дополнительной информацией и связанными последовательностями событий, что на порядок упрощает и ускоряет процесс расследования».*

В системе реализована ролевая модель доступа пользователей, позволяющая разграничивать зоны ответственности и набор доступных к использованию инструментальных средств в соответствии с присвоенными им правами (администратор или аналитик). Одновременно с системой могут работать до 10 человек, используя единую консоль или web-интерфейс.

Богатый функционал SIEM ArcSight позволяет отправлять оповещения об инцидентах, анализировать оперативные данные из различных источников в online-режиме, а также формировать отчеты с использованием накопленных данных. Система предусматривает оперативное хранение данных в течение 180 дней, информация старше этого периода выгружается в виде архивных файлов.

Дальнейшее развитие системы нацелено на увеличение числа подключенных к ней площадок и филиалов компании, источников и используемых правил, а также на оптимизацию ее архитектуры с учетом возросших требований по производительности, сокращение времени на подготовку отчетов и проведение расследований.

****