ИСТОРИЯ УСПЕХА

Северсталь

Централизованная система управления событиями информационной безопасности

ПАО «Северсталь» – одна из крупнейших в мире вертикально интегрированных сталелитейных и горнодобывающих компаний с активами в России, Белоруссии, Украине, Казахстане, Латвии, Польше, Италии и Либерии.

Акции компании котируются на российской торговой площадке ММВБ-РТС, глобальные депозитарные расписки представлены на Лондонской фондовой бирже.

Компания обладает большой территориально распределенной ИТ-инфраструктурой и обширным арсеналом средств обеспечения информационной безопасности. Централизованная система управления событиями информационной безопасности (СУСИБ) позволила существенно повысить уровень ИБ компании. Система обеспечивает автоматизированный сбор, хранение и анализ порядка 5000 событий безопасности в секунду. К системе подключено более 400 различных источников, настроено более 100 специализированных правил.

На сегодня проект охватывает 5 географически распределенных площадок компании «Северсталь» в европейской части России.

«Мы получили единый инструмент мониторинга событий ИБ от большого количества разнородных систем, в том числе географически разнесенных. Общее количество инцидентов, которые служба ИБ может отслеживать в режиме, близком к реальному времени, увеличилось в 10 раз. Из этих событий, по статистике, несколько десятков оказываются инцидентами различных уровней критичности, и теперь мы можем своевременно на них реагировать, – говорит **Константин Иванов, менеджер управления обеспечения информационной безопасности компании "Северсталь"**. *– Нам также удалось свести к минимуму объем ручной обработки данных. Время, необходимое для сбора требуемой информации по инциденту, сократилось до нескольких минут. Теперь у нас есть возможность оперативно принимать решения на основе аналитики глубиной до полугода».*

БОЛЬШЕ ЧЕМ SIEM

Система управления событиями ИБ реализована на базе решения HP ArcSight ESM.

Проектирование и внедрение СУСИБ проводилось на основании данных об ИТ-инфраструктуре, предоставленных заказчиком, и с учетом существующих процессов управления ИБ. Ядро HP ArcSight развернуто в дата-центре «Северстали». На источниках событий установлены агенты (коннекторы), которые передают информацию в ядро напрямую или после предварительной обработки.

На первом этапе к системе были подключены базовые компоненты инфраструктуры ИБ – средства антивирусной и сетевой защиты, журналы операционных систем и СУБД, а также часть рабочих станций.

«В первую очередь к системе подключались средства защиты, которые наиболее информативны с точки зрения ИБ – антивирусы, МСЭ, IDS/IPS и т.п. Это позволило сразу начать проработку правил обработки инцидентов и адаптировать их к корпоративным политикам», – поясняет **Алексей Гришин**.

На втором этапе к системе управления событиями информационной безопасности был подключен ряд нестандартных источников, таких как SAP Business Objects, СКУД, портал ИТ-услуг и др. Для них специалисты компании «Инфосистемы Джет» разработали специальные коннекторы. Данные системы служат дополнительными источниками информации о действиях пользователей при формировании и последующем расследовании инцидентов.

Россия, 127015, Москва
ул. Б. Новодмитровская, д. 14, стр. 1
Тел.: +7 (495) 411-7601
Факс: +7 (495) 411-7602
E-mail: info@jet.msk.su
www.jet.msk.su

Специалисты компании «Инфосистемы Джет» разработали и внедрили в ИТ-инфраструктуру «Северстали» систему контроля защищенности и соответствия стандартам на базе решения MaxPatrol. По заданному расписанию в автоматическом режиме система инвентаризирует инфраструктуру предприятия – более 4000 единиц оборудования, включая рабочие станции и серверы под управлением ОС Microsoft Windows и Unix, сетевое оборудование, СУБД MS SQL и Oracle. Также MaxPatrol определяет уровень защищенности компонентов инфраструктуры, выявляет уязвимости информационных ресурсов и оповещает о них, формирует рекомендации по устранению уязвимостей в соответствии с настроенными политиками безопасности – корпоративными и отраслевыми. В результате ИБ-служба компании «Северсталь» получила возможность проактивно выявлять риски ИБ, связанные с эксплуатацией злоумышленниками уязвимостей базовых компонентов информационных систем, отсутствием обновлений или небезопасными настройками. Система контроля защищенности и соответствия стандартам интегрирована с СУСИБ, и информация о выявленных уязвимостях также учитывается при формировании инцидентов ИБ.

ПРИМЕРЫ ВОЗМОЖНОСТЕЙ СУСИБ

В системе реализована ролевая модель доступа пользователей, позволяющая разграничивать зоны ответственности и доступные инструментальные средства в соответствии с присвоенными пользователям правами (администратор или аналитик). Одновременно с системой могут работать до 10 человек, используя единую консоль или веб-интерфейс.

У службы безопасности «Северстали» появилась возможность в режиме близком к реальному времени фиксировать факты работы в сети аутсорсеров и удаленных пользователей, имеющих разные права доступа.

Интеграция с удостоверяющим центром позволяет автоматизировать процесс контроля жизненного цикла корпоративных сертификатов.

Благодаря интеграции с SAP сформированные в СУСИБ инциденты обогащаются информацией о сотрудниках, в том числе имеющих доступ к конфиденциальной информации. Интеграция со СКУД позволяет построить аналитику с использованием данных о наличии того или иного сотрудника на рабочем месте в момент наступления события информационной безопасности.

За счет подключения к системе контроллера Wi-Fi и решения Cisco ISE компания получила возможность контролировать наличие сторонних точек Wi-Fi на своей территории и работу в корпоративной беспроводной сети мобильных пользователей.

Функционал СУСИБ позволяет отправлять оповещения об инцидентах, анализировать оперативные данные из различных источников в режиме близком к реальному времени, также формировать отчеты с использованием накопленных данных. В системе предусмотрено оперативное хранение данных в течение 180 дней, информация старше этого периода выгружается в виде архивных файлов.

Дальнейшее развитие СУСИБ направлено на увеличение количества подключенных площадок и филиалов компании, источников и используемых правил, а также на оптимизацию архитектуры системы с целью повышения производительности и сокращения сроков подготовки отчетов и проведения расследований.

Алексей Гришин,
директор Центра информационной безопасности компании «Инфосистемы Джет»:

«Созданная система по своим параметрам шире, нежели классический SIEM. В типовой SIEM-системе первичная категоризация событий происходит на коннекторах. Затем события отправляются в ядро системы, где осуществляется их корреляция и визуализация. Мы доработали этот механизм с учетом особенностей процессов и ИТ-инфраструктуры компании “Северсталь”. Создаваемые системой инциденты обогащаются дополнительной информацией (например, о нарушениях парольных политик, нетипичном поведении пользователя в домене, аномальной сетевой активности и пр.) и связанными последовательностями событий. Это позволило уменьшить количество ложных срабатываний и упростить процесс расследования инцидентов».

Константин Иванов,
менеджер управления обеспечения информационной безопасности компании «Северсталь»:

«Спустя примерно год после старта проекта мы получили первые ощутимые результаты от внедрения системы. Сегодня при расследовании практически всех инцидентов ИБ так или иначе используется информация, получаемая из ArcSight SIEM. Скорость и качество расследования существенно увеличились».