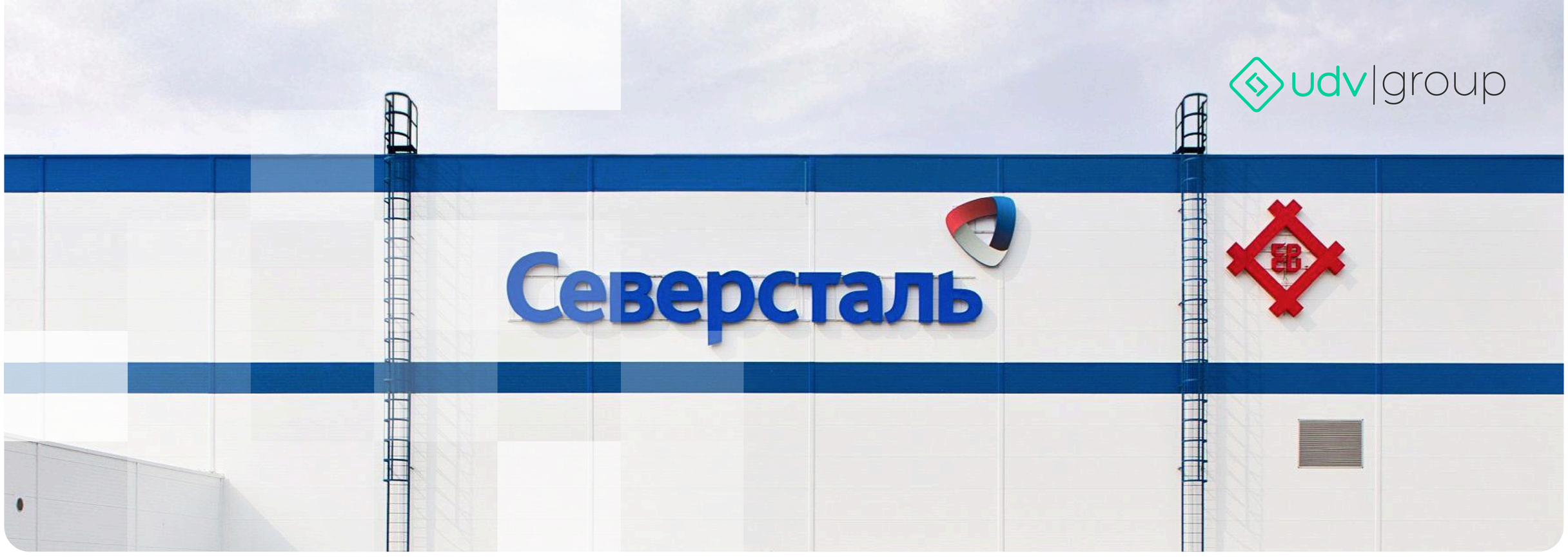


Система мониторинга ИБ для металлургической компании

Компания «Северсталь» — крупнейшее горно-металлургическое предприятие с крупными активами в разных странах. «Северсталь» производит десятки миллионов тонн различной металлопродукции — стали, чугуна, железной руды, осуществляя поставки в 69 стран мира.

ЦЕЛЬ ПРОЕКТА

Заказчику требовалось внедрить централизованную систему мониторинга информационной безопасности. Предыдущее решение представляло из себя разрозненную систему, которая не обеспечивала должного уровня защиты КИИ. Заказчик сталкивался с недостаточной видимостью конфигурации компонентов АСУ ТП, отсутствием гибкого механизма корреляции событий ИБ и медленной реакцией на инциденты, многие из которых были избыточными. Кроме того, на основании собственной экспертизы, сотрудники «Северстали» сформировали список инцидентов для отслеживания, под который было необходимо адаптировать внедряемое решение.

РЕЗУЛЬТАТЫ ВНЕДРЕНИЯ

- Правила корреляции событий ИБ были адаптированы под требования заказчика, что помогло сократить количество инцидентов и устранить «белый шум» из уведомлений
- Конфигурации АСУ ТП приведены к соответствию стандартам организации
- Автоматизировано выявление аномалий
- Автоматизирована отправка данных в корпоративную SIEM-систему заказчика для дальнейшей обработки специалистами по ИБ

В качестве решения был внедрен комплекс UDV DATAPK Industrial Kit, обеспечивающий:

- Сбор событий безопасности с компонентов АСУ ТП
- Непрерывный контроль неизменности конфигураций компонентов АСУ ТП

ОСОБЕННОСТИ ВНЕДРЕНИЯ

— Распределенная организационная структура

Независимые подразделения отвечают за свою часть информационной безопасности (ИБ АСУ ТП, настройка узлов АСУ ТП, настройка сетевого оборудования и т.д.), что создает необходимость консолидирования данных от каждого из них при сохранении автономности.

— Совмещение локального и централизованного управления

Новая система должна была учитывать интересы и приоритеты как филиалов, так и централизованной службы ИБ.

— Интеграция с корпоративным SOC

Необходимо было обеспечить совместимость с существующими ИБ-системами заказчика — в частности, отправку событий в SIEM.

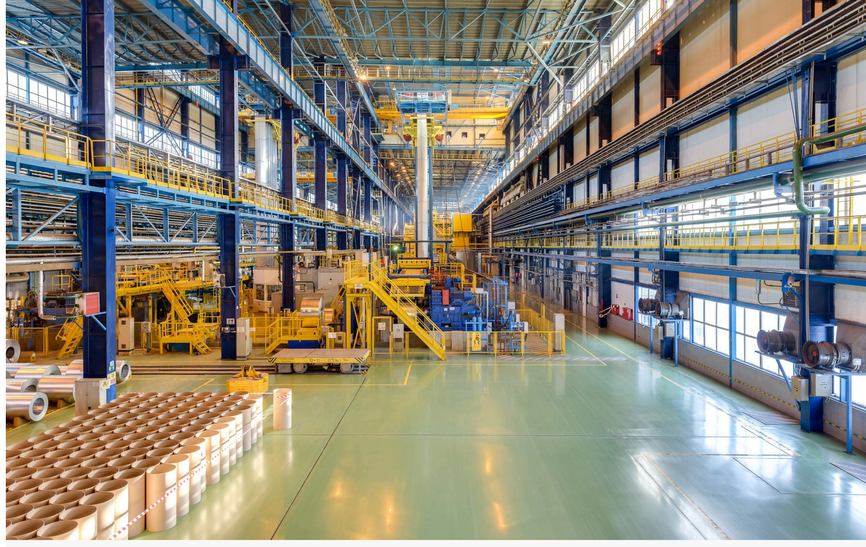
П

Представитель заказчика
Старший менеджер группы защиты производственных систем Управления информационной безопасностью АО «Северсталь Менеджмент»

«Для нас важно соблюдение баланса между функционалом создаваемой системы защиты КВО, удобством её обслуживания, обеспечиваемым уровнем безопасности и затратами. Внедряемое решение позволило достичь его, а активности в рамках совместного проекта — определить общий вектор развития систем защиты производств».

Виктор Колюжняк
Исполнительный директор UDV.Security, UDV Group

«Один из главных критериев нашей успешной работы — довольный заказчик, который продолжает использовать наше решение годы спустя. Совместно с коллегами из компании “Северсталь” нам удалось максимально эффективно осуществить внедрение продукта UDV DATAPK Industrial Kit в их систему информационной безопасности и в кратчайшие сроки доработать его под требуемые характеристики. Как итог — первое на территории России успешное промышленное внедрение решения класса оперативного мониторинга и контроля состояния защищенности ИБ АСУ ТП до сих пор функционирует и используется по назначению, а мы начинаем новую главу нашего сотрудничества с компанией “Северсталь”, работая над решением по контролю версий ПЛК — UDV DATAPK Version Control».



2018

Аудит

В рамках проекта был проведен аудит, цель которого — найти возможности и подобрать методики усиления защиты от внешних киберугроз и несанкционированного доступа к производственным системам.

2019

Внедрение на одном производстве

Внедрен комплекс UDV DATAPK Industrial Kit с полным функционалом: реализовано разделение сетей (выделение DMZ) для мониторинга событий, сбора конфигураций с сетевого оборудования и приема событий с узлов по протоколу Syslog.

2020

Внедрение комплекса UDV DATAPK Industrial Kit

На завершающем этапе были спроектированы и внедрены на нескольких производствах комплексы для массового контроля конфигураций с дашбордами на SIEM, а также проведена интеграция со смежным решением для сбора и анализа трафика из сети АСУ ТП.

В результате система защиты позволяет быстро и эффективно реагировать на инциденты информационной безопасности, обеспечивает стабильную работу автоматизированных систем и помогает снизить риски, которые могут угрожать жизни людей, окружающей среде и экономике.