Металлургический холдинг «Новосталь-М» выбрал «Лабораторию Касперского» своим основным поставщиком решений по кибербезопасности

Самым крупным металлургическим заводом холдинга «Новосталь-М» и центром компетенций по информационной безопасности является Абинский ЭлектроМеталлургический завод (АЭМЗ) — одно из самых современных и перспективных предприятий черной металлургии на юге России. Он выпускает проволоку, арматуру, катанку, стальную заготовку, кислород, азот, щебень шлаковый и другую продукцию.

kaspersky

Предыстория

01.

Завод был запущен в 2010 году, все этапы производственного цикла максимально цифровизированы. В процессе развития бизнеса, открытия новых цехов и роста цифровых активов встала задача по их защите.

Всеобъемлющую киберзащиту смогла обеспечить экосистема решений «Лаборатории Касперского», в основе которой лежат передовые технологии, аналитика об угрозах и многолетняя экспертиза.
Сотрудничество «Новосталь-М» и «Лаборатории Касперского» началось в 2018 году с построения защиты для корпоративного сегмента ключевого завода холдинга. В 2020 году перед предприятием встала задача провести категорирование объектов критической информационной инфраструктуры (КИИ) в соответствии с 187-ФЗ и осуществить полный аудит безопасности. После комплексного аудита, проведенного силами специалистов «Лаборатории Касперского», были выявлены наиболее уязвимые места и сформирована стратегия по развитию системы информационной безопасности завода. Усилен периметр безопасности как для корпоративной, так и для промышленной инфраструктуры.
Для динамично развивающегося производства, которое ежегодно наращивает свои обороты, было важно выбрать, во-первых, передовую защиту мирового класса, хорошо масштабируемую и сопровождаемую высококлассной экспертной поддержкой на всех этапах внедрения. Во-вторых, для предприятия, являющегося субъектом КИИ, эта защита должна обеспечиваться российским поставщиком. А «Лаборатория Касперского», будучи отечественным ИБ-разработчиком, давно заслужила признание в отрасли на международной арене и внедряет свои защитные решения по всему миру.

Абинский ЭлектроМеталлургический завод (АЭМЗ):

- **4000+ сотрудников;**
- **площадь завода — 120 га;**
- **мощность только одного сталеплавильного цеха — более 1 500 000 тонн в год;**
- **заслуженно считается одним из самых современных и развивающихся заводов отрасли;**
- **благодаря собственной транспортной инфраструктуре и непосредственной близости к морю продукция завода доставляется в максимально короткие сроки в любую точку планеты.**

Решение

02.

Совместная работа продуктов защиты для для корпоративной и промышленной инфраструктуры от одного вендора позволяет обеспечить комплексную безопасность предприятия на всех этапах производственного цикла. Кросс-платформенные сценарии взаимодействия дают возможность видеть полную картину происходящего в инфраструктуре и реагировать на инциденты централизованно.

Для обеспечения безопасности корпоративной среды мы выбрали концепцию XDR (Extended Detection and Response). Она включает все флагманские продукты вендора для защиты крупного бизнеса: защиту конечных точек Kaspersky Endpoint Security и Kaspersky EDR Expert, защиту сети Kaspersky Anti Targeted Attack с передовой песочницей и почтовый шлюз (Kaspersky Security для почтовых серверов), а также систему Kaspersky Unified Monitoring and Analysis Platform (KUMA) с полноценной Threat Intelligence-платформой Kaspersky CyberTrace.

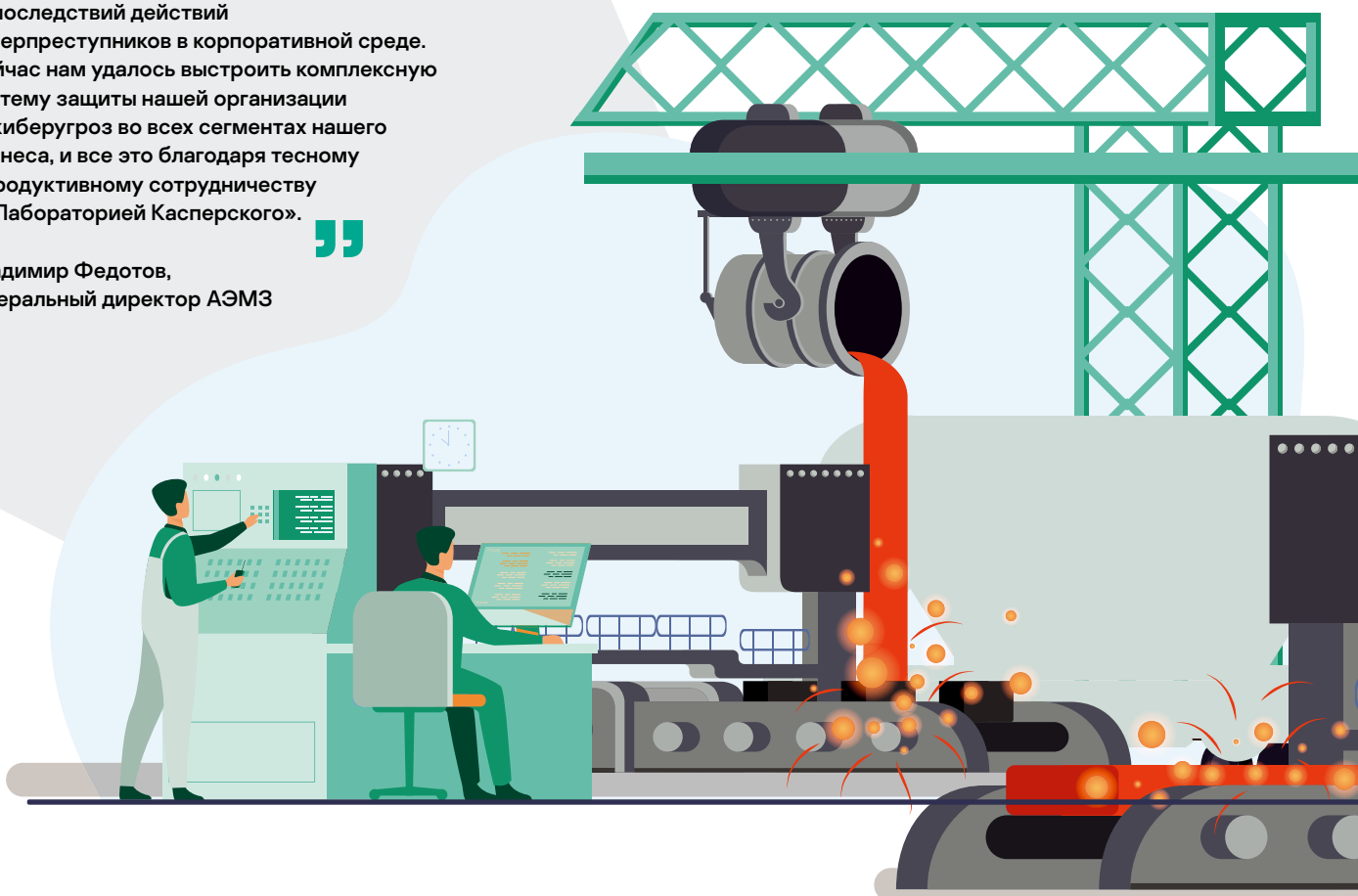
Платформа XDR позволяет вести постоянный мониторинг IT-инфраструктуры, обеспечивает обнаружение кибератак, их детальное расследование и реагирование на них.

Для безопасности технологических процессов была внедрена промышленная XDR-платформа Kaspersky Industrial CyberSecurity (KICS), взаимосвязанными элементами которой являются решение Kaspersky Industrial CyberSecurity for Nodes, предназначенное для защиты промышленных панелей оператора, рабочих станций и серверов, и Kaspersky Industrial CyberSecurity for Networks для мониторинга безопасности промышленной сети. Эти два продукта благодаря нативной интеграции позволяют реализовать базовые сценарии XDR. KICS for Nodes передает телеметрию с конечных точек в сторону KICS for Networks, обогащая данные об инвентаризации узлов и о событиях информационной безопасности.

Обе платформы XDR образуют единое целое в вопросе комплексной киберзащиты всего предприятия, взаимодействуют между собой, позволяя контролировать все, что происходит на наиболее уязвимом пересечении двух сред (корпоративной и промышленной).

«Киберугрозы способны нанести огромный ущерб предприятию. Речь идет как о репутационных и экономических потерях, вызванных сбоем технологического процесса, так и о возможном ущербе от последствий действий киберпреступников в корпоративной среде. Сейчас нам удалось выстроить комплексную систему защиты нашей организации от киберугроз во всех сегментах нашего бизнеса, и все это благодаря тесному и продуктивному сотрудничеству с «Лабораторией Касперского».

Владимир Федотов,
генеральный директор АЭМЗ



Результат и отзывы

03.

Внедрение решений для обеспечения безопасности как в промышленной, так и в корпоративной средах от одного вендора позволило обеспечить комплексную защиту завода и реализовать единую концепцию кибербезопасности.

Благодаря легкой масштабируемости, простоте внедрения решений и поддержке «Лаборатории Касперского» в ближайших планах — внедрение аналогичной экосистемы информационной безопасности на других предприятиях холдинга «Новосталь-М».

«В условиях сегодняшних реалий российские компании, конечно, могут продолжать использовать иностранные решения для обеспечения информационной безопасности, но стоит учитывать, что, даже если это ПО продолжает работать, получение актуальных обновлений уже становится невозможным и влияет на эффективность его работы. Сейчас отечественные разработчики могут предложить не менее качественные решения, например «Лаборатория Касперского». Эта компания предоставляет своим клиентам надежную киберзащиту, включающую передовые технологии, актуальные аналитические данные об угрозах и экспертные сервисы. Использование двух взаимосвязанных линеек решений для корпоративного и промышленного сегмента от одного вендора позволило нам получить синергетический эффект в укреплении безопасности и в простоте управления», — комментирует Артем Садовский, начальник управления информационной безопасности ООО «Новосталь-М».

Kaspersky OT CyberSecurity

Kaspersky Unified Monitoring and Analysis Platform

«Ландшафт киберугроз становится все более сложным, особенно в случаях целевых атак на предприятие. Злоумышленники все чаще применяют комплексные средства для проникновения в инфраструктуру. Чтобы обеспечить по-настоящему надежную защиту, подход к построению системы ИБ тоже должен быть комплексным. В случае с АЭМЗ использование экосистемы защитных решений «Лаборатории Касперского» для промышленного и корпоративного сегментов позволило обеспечить максимальный уровень защищенности предприятия от современных вызовов в киберпространстве», — говорит Антон Иванов, директор по исследованиям и разработке «Лаборатории Касперского».