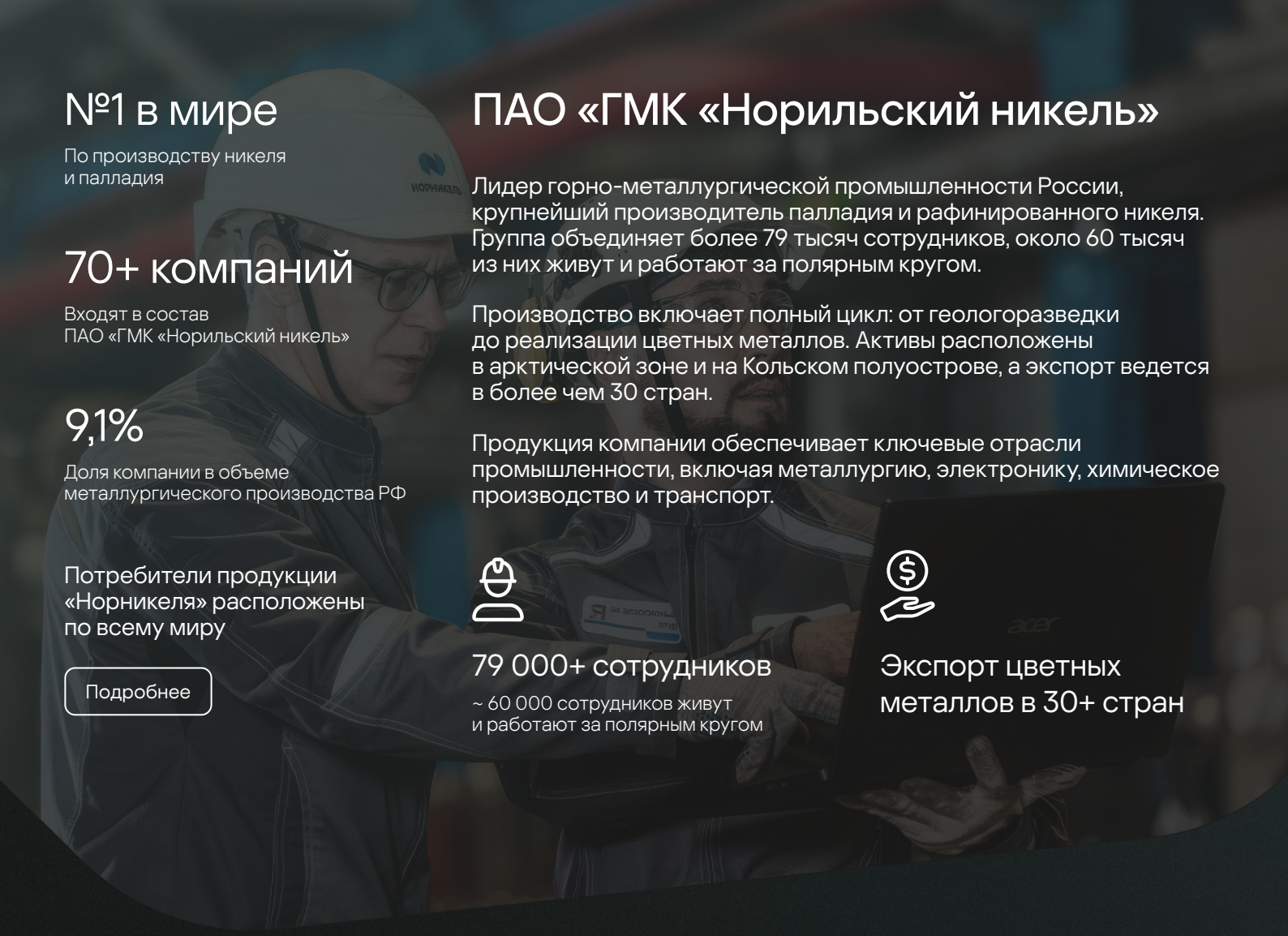
Развитие кибербезопасности: проактивная защита и снижение рисков

ПАО «ГМК «Норильский никель»

kaspersky активируй будущее

НОРНИКЕЛЬ



№1 в мире

По производству никеля
и палладия

70+ компаний

Входят в состав
ПАО «ГМК «Норильский никель»

9,1%

Доля компании в объеме
металлургического производства РФ

Потребители продукции
«Норникеля» расположены
по всему миру

Подробнее

ПАО «ГМК «Норильский никель»

Лидер горно-металлургической промышленности России, крупнейший производитель палладия и рафинированного никеля. Группа объединяет более 79 тысяч сотрудников, около 60 тысяч из них живут и работают за полярным кругом.

Производство включает полный цикл: от геологоразведки до реализации цветных металлов. Активы расположены в арктической зоне и на Кольском полуострове, а экспорт ведется в более чем 30 стран.

Продукция компании обеспечивает ключевые отрасли промышленности, включая металлургию, электронику, химическое производство и транспорт.

79 000+ сотрудников

~ 60 000 сотрудников живут
и работают за полярным кругом

Экспорт цветных металлов в 30+ стран

Многолетнее партнерство

В 2017 году «Норильский никель» и «Лаборатория Касперского» заключили стратегическое соглашение.

Проблематика

Современные кибервызовы требуют от компаний глубокого понимания того, что именно в цифровой среде им угрожает, кто за этим стоит, какими инструментами обладает злоумышленник и как с этим бороться. Стратегия информационной безопасности «Норникеля» предполагает развитие в том числе проактивных механизмов ИБ, позволяющих выявлять риски еще до того, как они перерастут в инциденты. Для этого необходимы решения, позволяющие определить и проанализировать актуальные для компании угрозы и принять меры по их предотвращению.

Для точного прогнозирования важно комплексно подходить к анализу: учитывать, какая именно информация о компании может быть использована злоумышленниками, какие векторы атак против российских компаний намечаются, есть ли адресные планы в отношении самой компании или ее подрядчиков и партнеров.

В построении системы ИБ компания придерживается бизнес-ориентированного подхода, планомерно выстраивает и развивает сервисную модель ИБ, которая позволяет оперативно реагировать на запросы бизнеса с учетом изменяющегося ландшафта угроз.

Поэтому для компании важно построить комплексную систему проактивного выявления, анализа и предотвращения киберугроз.

Александр Ардаков

Руководитель направления практической безопасности Департамента защиты информации и IT-инфраструктуры «Норникеля»

Мы часто слышим тезис о том, что злоумышленники всегда на шаг впереди защищающихся. Кибербразведка необходима для того, чтобы это расстояние между злоумышленниками и защитниками максимально сокращать.

Почему «Лаборатория Касперского»

«Норникель», как один из лидеров горно-металлургической промышленности стремится создать надежную систему киберустойчивости и активно сотрудничает с ведущими игроками российского рынка информационной безопасности (ИБ). «Лаборатория Касперского», будучи одним из стратегических партнеров, тесно взаимодействует с «Норникелем» в области защиты информации. Продукты ЛК входят в широкий портфель решений ИБ и используются «Норникелем» для комплексной защиты своих производственных активов.

Важную роль сыграла и гибкость вендора. Как отметил представитель заказчика: «Лаборатория Касперского видит в нас надежного партнера с высоким уровнем зрелости информационной безопасности и прислушивается к нашим пожеланиям по доработке функционала». Именно такой формат партнерства позволил интегрировать сервисы ЛК в общую систему проактивной безопасности «Норникеля».

Решение

«Норникель» развернул комплекс решений Kaspersky Threat Intelligence, чтобы получить полную видимость угроз на всех этапах их формирования.

Kaspersky Threat Intelligence

Kaspersky Threat intelligence — комплекс решений для кибербразведки, обеспечивающий раннее обнаружение угроз через анализ глобальных данных о киберпреступности.

Основные компоненты

Kaspersky Threat Intelligence Portal

Kaspersky Threat intelligence Portal — единый портал управления продуктами TI, предоставляющий администраторам доступ к безопасной среде для анализа вредоносных файлов, экспертным отчетам и ландшафту угроз для обогащения контекстом инцидентов.

Наличие исчерпывающей информации об обнаруженных угрозах помогает приоритизировать инциденты по их критичности и масштабу, установить атрибуцию к известным группировкам и предотвращать закрепление злоумышленников в инфраструктуре на ранних стадиях.

Kaspersky Digital Footprint Intelligence

Kaspersky Digital Footprint Intelligence — модульное решение, позволяющее управлять цифровым следом, обнаруживать утечки данных, а также следить за появлением в дарквебе информации о компании или ее сотрудниках.

Активный поиск уязвимостей в сетевых ресурсах и связывание данных о компании и ее сотрудниках с возможными векторами атак помогают управлять рисками и удалять из открытого доступа информацию, которая могла бы быть использована злоумышленниками.

Александр Ардаков

Руководитель направления практической безопасности Департамента защиты информации и IT-инфраструктуры «Норникеля»

Сервис Digital Footprint Intelligence позволяет четко понимать, какие данные о компании доступны злоумышленникам и как их можно использовать при построении атак.

Kaspersky Threat Data Feeds

Kaspersky Threat Data Feeds — постоянно обновляющиеся потоки данных, включающие в себя индикаторы компрометации для распознавания потенциальных угроз.

Kaspersky CyberTrace

Kaspersky CyberTrace — техническое решение для упрощения интеграции потоков данных в решения SIEM / NGFW / SOAR и быстрой интерпретации данных разных форматов.

Снижение числа ложных срабатываний детектирующих продуктов вместе с автоматической доставкой данных об угрозах по API позволяет уменьшать нагрузку на инженеров SOC и выделять больше ресурсов на активное противодействие угрозам.

Заключение

Управляемый и предсказуемый процесс работы с киберрисками в «Норникеле» удалось сформировать в том числе с помощью внедрения комплексного набора решений Kaspersky Threat Intelligence. Эти и другие решения для кибербразведки позволяют Компании оценивать существующие угрозы, адекватно выстраивать свою защиту и приоритизировать уязвимости по степени их значимости.

В результате появилась возможность эффективнее управлять ресурсами SOC-специалистов и глубже погрузиться в кибербразведку, тем самым снижая время реакции на атаки на самых ранних этапах.

Kaspersky Threat Intelligence

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее