# Развитие централизованной киберзащиты с помощью Kaspersky EDR Expert

kaspersky

МАГНИТОГОРСКИЙ МЕТАЛЛУРГИЧЕСКИЙ КОМБИНАТ

№1 поставщик
стали на российский рынок

11,8 млн тонн
продажи металлопродукции

$8,83 млн
инвестиции в НИОКР и цифровизацию

# Магнитогорский металлургический комбинат

ПАО «Магнитогорский металлургический комбинат» (ММК) — один из мировых лидеров по производству стали и ведущее предприятие российской черной металлургии. Производственные мощности компании в России — это крупный металлургический комплекс с полным производственным циклом, начиная с подготовки железорудного сырья и заканчивая глубокой переработкой черных металлов. ММК производит широкий сортамент металлопродукции с преобладающей долей инновационной продукции.

# Эволюция систем защиты конечных точек в группе ПАО «ММК»

С 2010 года компания выстраивает централизованный подход к кибербезопасности. Однако с развитием ИТ-инфраструктуры, ростом числа цифровых сервисов и эволюцией киберугроз стало очевидно, что традиционных инструментов защиты уже недостаточно для обеспечения необходимого уровня киберустойчивости и оперативного реагирования на современные атаки.

Специалисты информационной безопасности (ИБ) ММК отмечали следующие вызовы:

- ограниченная видимость угроз при использовании только антивирусной защиты;
- недостаточный объем контекста для расследования инцидентов;
- длительное время реагирования;
- отсутствие взаимосвязи между событиями безопасности.

В ответ на эти вызовы компания приняла решение о внедрении передовых инструментов защиты от актуальных угроз.

Распределенная инфраструктура компании предъявляет дополнительные требования к средствам защиты. Для ММК критически важно обеспечить централизованное управление и мониторинг событий безопасности, сохранить стабильность работы масштабной инфраструктуры и минимизировать риски, связанные с возможными сбоями или нарушением функционирования систем защиты.

## Возможности Kaspersky Endpoint Detection and Response Expert

- Непрерывный мониторинг событий безопасности
- Проактивный поиск угроз и централизованное реагирование
- Сбор данных компьютерной криминалистики для расследования инцидента
- Доступ к платформе киберразведки и открытой библиотеке хантов

# Решение

В рамках развития комплексного подхода к кибербезопасности и повышения уровня выявления и реагирования на инциденты ММК внедрил Kaspersky EDR Expert, входящий в состав линейки Symphony EDR.

Kaspersky EDR Expert обеспечивает защиту рабочих станций и серверов компании, позволяя обнаруживать и нейтрализовать самые сложные угрозы, включая целевые атаки. Архитектура построена на едином агенте KES/KEDR, что упрощает развёртывание и администрирование, а также обеспечивает централизованное управление средствами защиты.

Kaspersky EDR Expert позволил ММК выстроить комплексный процесс предотвращения сложных угроз, обеспечить полную видимость событий на конечных точках и предоставить специалистам инструменты для глубокого расследования инцидентов.

Особенно важным преимуществом стала возможность интеграции решения в существующие процессы SOC, это позволило сократить время реагирования на инциденты.

## Ключевые достижения после внедрения

- Быстрое внедрение благодаря использованию единого агента на базе KES
- Выявление новых типов инцидентов и расширение сценариев реагирования на них
- Повышение скорости и качества расследований инцидентов
- Легкое горизонтальное и вертикальное масштабирование

# Измеримые результаты

Использование Kaspersky EDR Expert позволило ММК значительно повысить эффективность процессов мониторинга и расследования событий ИБ.

**78%**
Сокращение среднего времени обнаружения атак

**50%**
Рост объема детектируемой вредоносной активности

**75%**
Сокращение времени обработки инцидентов высокой критичности

**68%**
Увеличение общей скорости реагирования

**Вадим Феоктистов**

Главный специалист
по информационным технологиям
ПАО «ММК»

Внедрение Kaspersky EDR Expert стало важным этапом развития кибербезопасности нашей компании. Решение позволило повысить уровень контроля над инфраструктурой конечных устройств, улучшить качество расследований и обеспечить более эффективное противодействие современным киберугрозам. При выборе решения мы учитывали не только функциональные возможности, но и стратегические факторы: развитие отечественной экспертизы и технологическую независимость. Kaspersky EDR Expert полностью соответствовал этим требованиям.

**Марина Усова**

Коммерческий директор
«Лаборатории Касперского» в России

Мы наблюдаем устойчивый рост количества целевых атак, в том числе с применением автоматизации и технологий искусственного интеллекта. В таких условиях компаниям необходимы инструменты, которые позволяют не только предотвращать угрозы, но и видеть полную цепочку развития атаки. Мы рады, что Магнитогорский металлургический комбинат оценил функциональные возможности решения и выбрал Kaspersky EDR Expert для повышения уровня кибербезопасности.

# Преимущества Kaspersky EDR Expert

Единый агент объединяет антивирусную защиту и EDR-функциональность на базе Kaspersky Endpoint Security

Kaspersky EDR Expert покрывает более 460 тактик, техник и процедур матрицы MITRE ATT&CK. 2100+ уникальных правил IoA от центра экспертизы Лаборатории Касперского

Интеграция с облачной репутационной базой Kaspersky Security Network: проверка репутации файлов и URL-адресов в реальном времени

Доступ к аналитике угроз: получение расширенного контекста по обнаруженным индикаторам компрометации (IOC) при обращении аналитика в онлайн базу знаний Kaspersky Threat Lookup

Открытая библиотека хантов с прозрачной логикой, привязанной к реальным группировкам и угрозам, кросс-корреляция с отраслевым ландшафтом угроз

Соответствие требованиям регуляторов: входит в реестр Российского ПО и имеет сертификаты ФСТЭК, ФСБ и Минобороны

# Kaspersky Endpoint Detection and Response Expert

Подробнее

www.kaspersky.ru



#kaspersky
#активируйбудущее