«Лаборатория Касперского» защищает «Азиатский Газопровод» от таргетированных кибератак с Kaspersky Anti Targeted Attack

ТОО «Азиатский Газопровод» выбрало в качестве защиты от сложных направленных атак комплекс продуктов «Лаборатории Касперского» — Kaspersky Anti Targeted Attack для выявления вредоносной активности в сети и Kaspersky EDR Expert для расследования инцидентов и реагирования на них.

kaspersky

Предыстория

01.

«Азиатский Газопровод» оперирует огромной инфраструктурой и уделяет особое внимание ее защите и обеспечению информационной безопасности в целом. Высочайшая квалификация экспертов, многолетний опыт успешных внедрений и технологически продвинутые решения «Лаборатории Касперского» соответствуют уровню требований оператора по защите критической информационной инфраструктуры.

«Азиатский Газопровод» — это:

- Оператор проекта строительства газовой магистрали Казахстан — Китай, которая входит в состав газопровода Туркменистан — Узбекистан — Казахстан — Китай.
- Маршрут от нефтегазовых месторождений Туркменистана до конечной точки в южных провинциях Китая.
- Общая протяжённость газопровода — более 7,5 тысячи километров.
- Проектная мощность магистрали Казахстан — Китай — 55 млрд куб. м в год.
- Три параллельные нити: проектная мощность нитей «А» и «Б» — 30 млрд куб. м в год, «С» — 25 млрд куб. м в год.

Решение

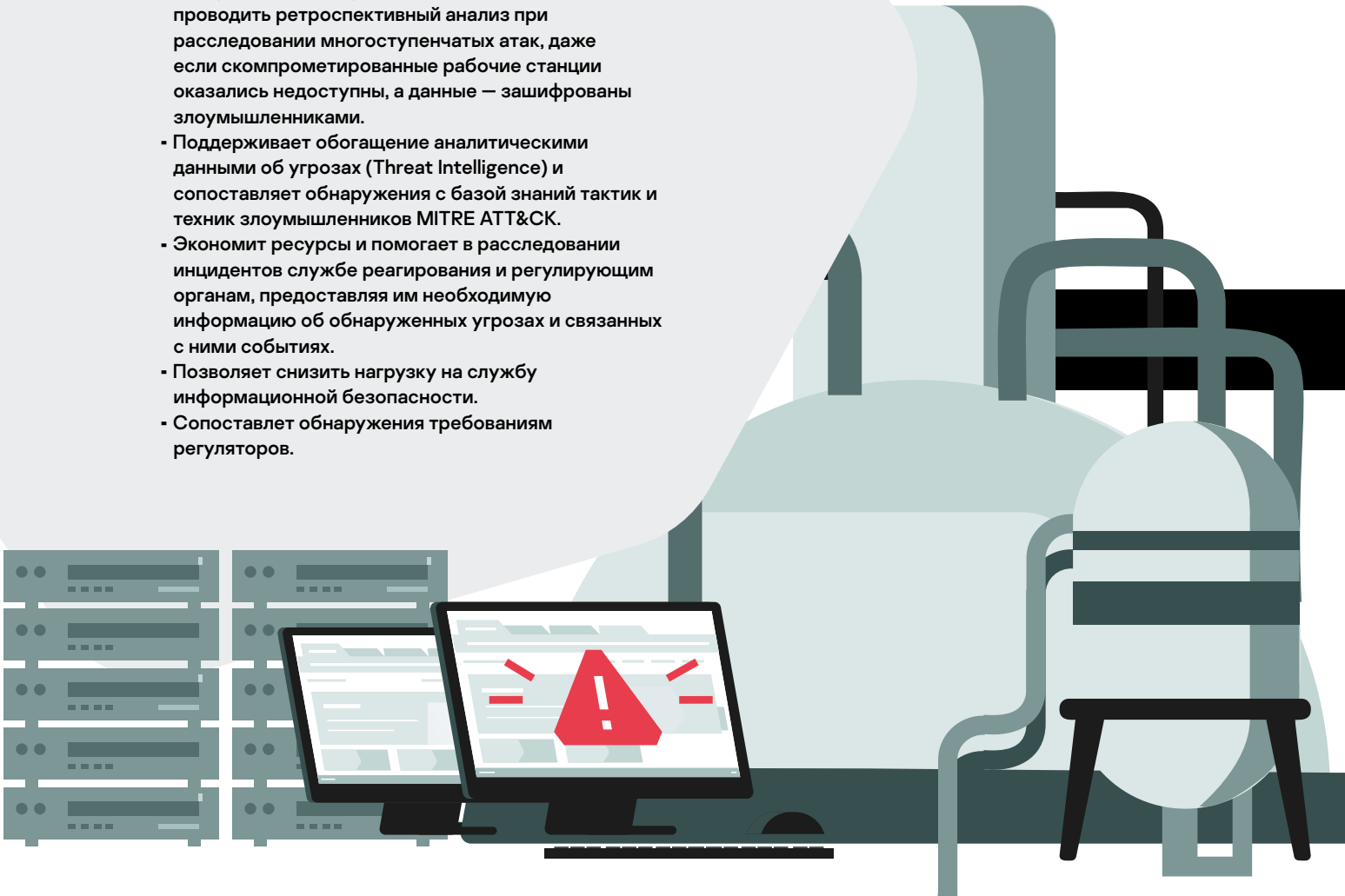
02.

Для киберзащиты «Азиатского Газопровода» были выбраны продукты Kaspersky Anti Targeted Attack и Kaspersky EDR Expert. Они дополняют друг друга и превращаются в мощное комплексное решение для защиты от продвинутых кибератак.

Платформа Kaspersky Anti Targeted Attack совместно с Kaspersky EDR Expert — это решение класса XDR (Extended Detection and Response) нативного типа. Оно защищает многочисленные точки входа потенциальной угрозы в сети и на рабочих местах и предоставляет детализированный обзор всего, что происходит в IT-инфраструктуре. Это даёт ИБ-подразделению и специалистам возможности по многоуровневому обнаружению атак, проведению глубинных расследований, проактивному поиску угроз и централизованному реагированию на сложные инциденты. Кроме того, такое решение помогает организациям соответствовать требованиям российского законодательства.

Преимущества решения:

- Анализирует сетевой трафик и телеметрию с рабочих мест, может эмулировать угрозы с помощью песочницы и использует большой набор современных детектирующих технологий.
- Автоматизирует сбор данных и вердиктов и централизованно хранит их. Это позволяет проводить ретроспективный анализ при расследовании многоступенчатых атак, даже если скомпрометированные рабочие станции оказались недоступны, а данные — зашифрованы злоумышленниками.
- Поддерживает обогащение аналитическими данными об угрозах (Threat Intelligence) и сопоставляет обнаружения с базой знаний тактик и техник злоумышленников MITRE ATT&CK.
- Экономит ресурсы и помогает в расследовании инцидентов службе реагирования и регулирующим органам, предоставляя им необходимую информацию об обнаруженных угрозах и связанных с ними событиях.
- Позволяет снизить нагрузку на службу информационной безопасности.
- Сопоставлет обнаружения требованиям регуляторов.



Результат и отзывы

03.

Одним из требований «Азиатского Газопровода» к продукту для обеспечения информационной безопасности была защита от сложных таргетированных атак. На первом этапе организация приняла решение запустить пилотный проект на основе Kaspersky Anti Targeted Attack. По итогам этого проекта защиту решили дополнить, и организация внедрила Kaspersky EDR Expert — систему для расследования инцидентов и реагирования на них на уровне конечных устройств, а также защиту конечных устройств в промышленной сети.

«Для эффективной защиты "Азиатского Газопровода" нужны продвинутые компетенции и технологии. Всё это есть в наших продуктах, и мы рады, что теперь столь важный объект находится под нашей защитой», — отметил Валерий Зубанов, коммерческий директор «Лаборатории Касперского» в Казахстане, Средней Азии и Монголии.

«Платформа Kaspersky Anti Targeted Attack предоставляет возможность выполнить все требования к созданию и защите систем безопасности значимых объектов критической информационной инфраструктуры. Решение использует множество механизмов детектирования. Например, встроенная песочница позволяет выявить те угрозы, для обнаружения которых недостаточно традиционных превентивных средств защиты. Это позволяет выстроить современную, эффективную, эшелонированную защиту от сложных и целевых атак», — рассказал Станислав Соловьёв, заместитель директора департамента телекоммуникаций и информационных технологий ТОО «Азиатский Газопровод».