Kaspersky Unified Monitoring and Analysis Platform на страже цифровой трансформации Кыргызской Республики

Муниципальное предприятие «Центр цифровых технологий» мэрии города Бишкек усилило защиту своих цифровых систем с помощью решения SIEM «Лаборатории Касперского».

kaspersky

Предыстория

01.

Муниципальное предприятие «Центр цифровых технологий» — технический оператор всей цифровой инфраструктуры муниципалитета, созданный на базе мэрии города Бишкек – столицы Кыргызской Республики.

«Центр цифровых технологий» был создан в рамках реализации концепции глобальной цифровой трансформации Кыргызской Республики. Активный рост числа цифровых активов требует обеспечения комплексной защиты информационной инфраструктуры от возможных кибератак.
Для выполнения задач по комплексной защите инфраструктуры было предложено использовать решение класса SIEM. После проведения нескольких пилотов выбор остановился на решении Kaspersky Unified Monitoring and Analysis Platform (KUMA).
На итоговый выбор решения повлияла возможность быстрой интеграции KUMA с уже имеющимися продуктами «Лаборатории Касперского» в инфраструктуре компании и решениями других вендоров, а также легкость развертывания системы.
Интеграцию решения выполнил партнер «Лаборатории Касперского» — DAOGroup. Внедрение, пилотное тестирование и запуск в эксплуатацию были проведены всего за два месяца — это рекордный срок с учетом сложности задач и разветвленной IT-инфраструктуры.

Муниципальное предприятие «Центр цифровых технологий» мэрии города Бишкек:

- **создано в 2019 году;**
- **количество пользователей цифровой инфраструктуры — более 3000;**
- **обеспечивает электронное взаимодействие между государственными и муниципальными органами;**
- **поддерживает предоставление цифровых услуг учреждениям и предприятиям, юридическим и физическим лицам.**

Решение

02.

Kaspersky Unified Monitoring and Analysis Platform (KUMA) — решение класса SIEM, обеспечивающее комплексный подход к противодействию сложным угрозам и целевым атакам.

KUMA может объединять в единую экосистему как продукты «Лаборатории Касперского», так и решения других вендоров. Решение KUMA можно интегрировать с Kaspersky Threat Intelligence — сервисами информирования об угрозах. Это позволит аналитикам получать информацию об актуальных киберугрозах и производить более качественные расследования инцидентов безопасности.

Ключевые преимущества KUMA:

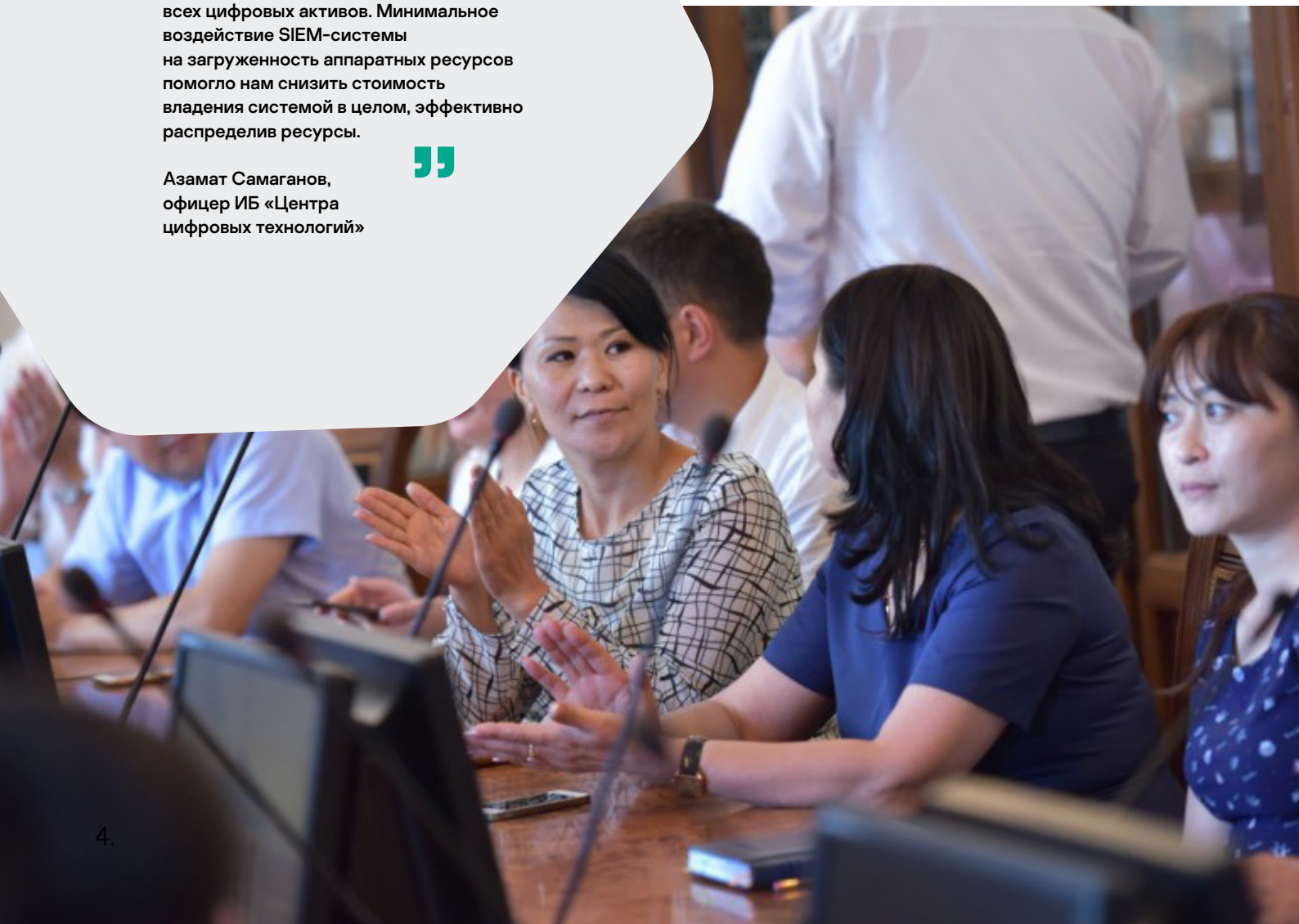
- простая интеграция с продуктами «Лаборатории Касперского» и решениями других производителей;
- тесное взаимодействие с Kaspersky Threat Intelligence;
- высокая производительность;
- готовые правила корреляции событий ИБ;
- масштабируемая архитектура и низкие системные требования;
- управление инцидентами безопасности из единой консоли;
- помощь в реагировании на инциденты;
- гибкое лицензирование.

Результат и отзывы

03.

Решение Kaspersky Unified Monitoring and Analysis Platform стало ядром комплексной системы информационной безопасности «Центра цифровых технологий». Оно позволяет анализировать все события в сети, поступающие от большого количества подключенных источников.

Быстрое внедрение осуществлено благодаря слаженной и профессиональной работе «Лаборатории Касперского» и DAOGroup, что в конечном итоге способствовало бесперебойной и безопасной деятельности информационной инфраструктуры столичного муниципалитета. «Цифровая трансформация — глобальный тренд, который требует быстрых и точных решений по защите быстрорастущей цифровой инфраструктуры. В переходный момент критически важно обеспечить надежную защиту систем от всех видов цифровых угроз. Kaspersky Unified and Analysis Platform предоставляет ИБ-специалистам максимальные возможности по обнаружению и нейтрализации киберинцидентов любого уровня сложности», — отмечает Валерий Зубанов, коммерческий директор офиса «Лаборатории Касперского» в Казахстане, Центральной Азии и Монголии.

Узнать подробнее о SIEM-системе Kaspersky Unified Monitoring and Analysis Platform →

> **Kaspersky KUMA позволила нам выстроить комплексную и централизованную систему защиты всех цифровых активов. Минимальное воздействие SIEM-системы на загруженность аппаратных ресурсов помогло нам снизить стоимость владения системой в целом, эффективно распределив ресурсы.**
>
> **Азамат Самаганов, офицер ИБ «Центра цифровых технологий»**