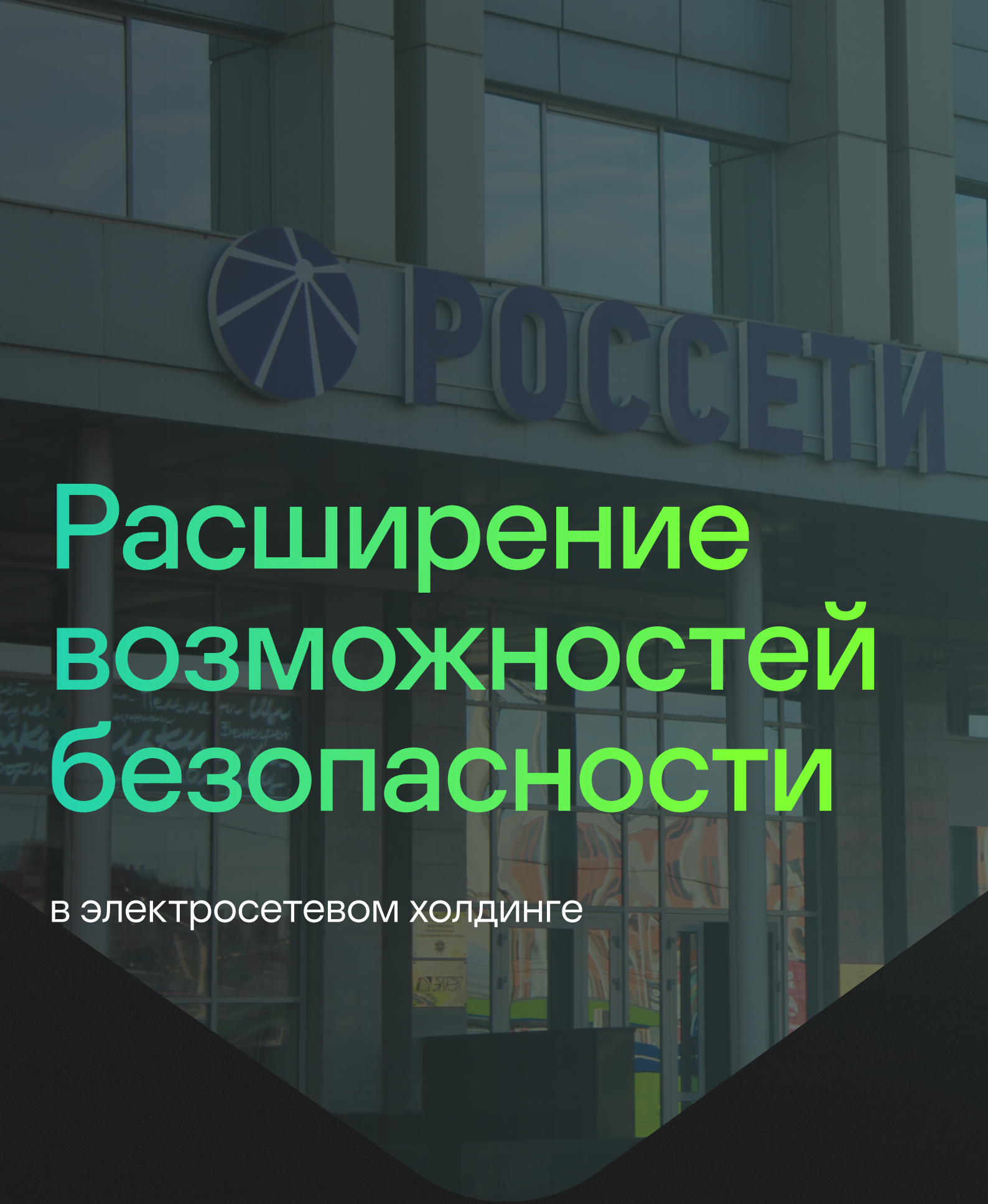

Расширение возможностей безопасности

в электросетевом холдинге

kaspersky активируй будущее

РОССЕТИ СЕВЕРО-ЗАПАД

1,4 млн км²

Территория обслуживания компании с населением около 5,8 млн человек

19 670 МВА

Составляет установленная мощность силовых трансформаторов подстанций

1 191 шт.

Количество подстанций 35 кВ и выше, состоящих на балансе

Задача «Россети Северо-Запад» — обеспечение эффективного управления распределительным сетевым комплексом семи территорий Северо-Западного федерального округа России

ПАО «Россети Северо-Запад»

Основной оператор, оказывающий услуги по передаче электроэнергии и присоединению к электросетям в Архангельской, Вологодской, Мурманской, Новгородской, Псковской областях, Республике Карелия и Республике Коми. 55,38% акционерного капитала компании принадлежит ПАО «Российские сети».

Виды деятельности компании:

1. Передача электроэнергии
2. Технологическое присоединение
3. Энергосбытовая деятельность
4. Дополнительные услуги

Развитие партнерства

«Россети Северо-Запад» сотрудничает с «Лабораторией Касперского» с 2015 года. Компания использует все флагманские продукты по защите корпоративной инфраструктуры на уровне хостов, веб- и почтового трафика, а также по защите промышленной сети. И продолжает расширять сотрудничество.

Бесспорный выбор

До внедрения SIEM-системы компания «Россети Северо-Запад» сталкивалась с проблемой отсутствия полной информации об ИБ-событиях в своей инфраструктуре, ей требовалось эффективное решение для интеграции в центр мониторинга информационной безопасности. Первоначально рассматривался продукт конкурентов, но такие факторы, как высокие требования к оборудованию и лицензирование по узлам, побудили руководство компании рассмотреть альтернативные варианты.

Выбором стало решение Kaspersky Unified Monitoring and Analysis Platform (KUMA) от «Лаборатории Касперского», лицензирование которого осуществляется по количеству EPS, что позволило сократить расходы на приобретение в несколько раз, а внедрение заняло всего два месяца. В качестве дополнительного преимущества в «Россети Северо-Запад» отметили возможность создания корреляционных правил в конструкторе системы, устраняющую необходимость написания их на языке программирования, как это распространено у других вендоров.

Удобство и эффективность

Выбирая отечественное SIEM-решение, в компании учитывали многолетний опыт и ведущую репутацию бренда для эффективной защиты своих критически важных систем и данных. Более 25 лет на рынке решений информационной безопасности и репутация надежного поставщика позволяют утверждать, что «Лаборатория Касперского» вселяет чувство уверенности и надежности в организациях, которые используют решения компании.

После интеграции Kaspersky Unified Monitoring and Analysis Platform в корпоративный сегмент «Россети Северо-Запад» осуществили трансформацию, избавившись от необходимости администрирования множества систем. Теперь все операции осуществляются через удобный веб-интерфейс KUMA, что значительно упрощает процессы и экономит время специалистов по информационной безопасности. В компании убедились в эффективности решения KUMA даже в условиях территориально-распределенной инсталляции и подключения к SIEM-системе более 10 000 устройств.

Благодаря успешному внедрению решения SIEM от «Лаборатории Касперского» «Россети Северо-Запад» выстроили ИБ-процессы, оптимизировав работу, повысив уровень защиты в организации и предоставив возможность специалистам по информационной безопасности работать более эффективно.

Следующим шагом после успешного внедрения и эксплуатации KUMA компания планирует усилить защиту инфраструктуры рабочих мест решением Kaspersky EDR Expert, обеспечить безопасность конечных точек в промышленной сети благодаря KICS for Nodes и KICS for Networks, а так же повысить уровень осведомленности об угрозах при помощи Kaspersky Automated Security Awareness Platform.

Кирилл Паничкин

Начальник отдела информационной безопасности и технической защиты информации, «Россети Северо-Запад»

Мы довольны выбором SIEM-системы от «Лаборатории Касперского» — высокая скорость реагирования на ИБ-запросы позволяет нам оперативно реагировать на киберинциденты, при этом низкие системные требования KUMA обеспечивают бесперебойную работу даже на бюджетном оборудовании. Кроме того, удобство интерфейса продукта, простота интеграции источников значительно повысили эффективность нашей работы. KUMA действительно превзошла наши ожидания, с ней приятно работать.

Анна Кулашова

управляющий директор «Лаборатории Касперского» в России и странах СНГ

«Лаборатория Касперского» ставит в приоритет потребности наших заказчиков и постоянно инвестирует в разработку решений, отвечающих их требованиям. Наша цель — предоставить компаниям удобные, надежные и эффективные средства кибербезопасности. Мы понимаем, с какими проблемами сталкиваются организации в условиях современного развивающегося ландшафта угроз, и стремимся предоставлять инновационные продукты, позволяющие нашим клиентам уверенно защищать свои цифровые активы.

Расширение сотрудничества

Компания «Россети Северо-Запад» выбрала Kaspersky EDR Expert в качестве защиты рабочих станций.

Решение представляет собой мощную систему, которая обеспечивает защиту от сложных и таргетированных атак, предоставляя специалистам ИБ прозрачную картину событий на рабочих местах.

Сбор, запись и централизованное хранение информации о событиях безопасности на всех рабочих местах обеспечивают оперативный доступ к ретроспективным данным при расследовании продолжительных атак даже в условиях недоступности рабочих мест, а также вредоносного шифрования или уничтожения данных злоумышленниками.

Используемые решения

Kaspersky Unified Monitoring and Analysis Platform

Высокопроизводительное решение класса SIEM, предназначенное для централизованного сбора, анализа и корреляции ИБ-событий из различных источников данных для выявления потенциальных киберинцидентов и их своевременной нейтрализации.

Преимущества KUMA:

Осуществляет централизованный сбор и анализ журналов регистрации, корреляцию событий ИБ в реальном времени и своевременное оповещение об инцидентах

Тесно интегрируется с богатым портфолио сервисов Kaspersky Threat Intelligence, что позволяет выявлять, приоритизировать угрозы и получать доступ к контекстной информации по новым атакам

Интегрируется с решениями класса EDR для реагирования на уровне хостов по результатам мониторинга

Современная микросервисная архитектура обеспечивает масштабируемость и отказоустойчивость

Встроенный модуль ГосСОПКА помогает соответствовать требованиям регуляторов

Высокая производительность и низкие системные требования снижают стоимость владения

Kaspersky Endpoint Detection and Response Expert

Мощный EDR-инструмент, разработанный для экспертов в области ИБ, SOC и команд реагирования на инциденты для продвинутого обнаружения, эффективного расследования, проактивного поиска угроз и устранения многоуровневых атак, направленных на инфраструктуру конечных устройств.

Преимущества KEDR Expert:

- Глубокая интеграция для комплексной защиты рабочих мест
- Эффективные выявление и анализ угроз
- Оперативное реагирование на киберинциденты
- Интеграция с Kaspersky Security Network (KSN)
- Доступ к аналитике угроз
- Входит в реестр Российского ПО и имеет сертификат ФСТЭК

Kaspersky Unified Monitoring and Analysis Platform

Подробнее

Kaspersky Endpoint Detection and Response Expert

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее