Платформа
информационной безопасности
«Wazuh|BY версии 4»

Платформа информационной безопасности представляет собой локализованную и адаптированную под требования законодательства Республики Беларусь систему сбора и обработки событий информационной безопасности на базе международного open-source решения Wazuh.

Вследствие чего продукт обеспечивает комплексную защиту информационных систем, централизованный сбор и анализ событий безопасности, обнаружение угроз, мониторинг целостности и соответствие нормативным требованиям.

Благодаря использованию актуальных версий программного обеспечения и своевременной установке обновлений, система гарантирует надёжную защиту от новых угроз. Ограничение доступа к ключам и конфигурационным файлам средствами операционной системы, в свою очередь, предотвращает несанкционированное вмешательство.

Особое внимание уделено обнаружению угроз и вторжений (HIDS/NIDS) на основе анализа событий в реальном времени. Мониторинг целостности файлов (FIM) контролирует изменения в системных файлах, конфигурациях и реестре. Автоматическое сканирование на наличие уязвимостей, в свою очередь, позволяет своевременно выявлять и устранять слабые места в инфраструктуре.

В целях обеспечения соответствия нормативам система включает встроенные профили для проверки соответствия PCI DSS, GDPR. Единая консоль управления предоставляет наглядные дашборды, карты угроз и графики активности, что обеспечивает прозрачность и управляемость процессов безопасности.

Продукт успешно прошел аттестацию и имеет действующий Сертификат соответствия № BY/112 02.01. ТР027 036.01 00560 от 4 ноября 2022 г., выданный Оперативно-аналитическим центром при Президенте Республики Беларусь, что подтверждает его соответствие установленным требованиям в области информационной безопасности.