

Программное обеспечение «Система сбора и обработки событий информационной безопасности SL] SIEM версии 1»



Программный комплекс представляет собой систему централизованного сбора, обработки и хранения событий информационной безопасности из различных элементов ИТ-инфраструктуры. Таким образом, продукт позволяет эффективно выявлять угрозы, своевременно реагировать и расследовать инциденты.

Решение интегрируется с различными типами источников событий, включая Syslog и Webhooks, Kubernetes, Windows-агенты и macOS-агенты, что обеспечивает гибкую работу в инфраструктурах любого масштаба. Благодаря готовым правилам нормализации и корреляции система позволяет быстро развернуть мониторинг без дополнительной настройки.

Особое внимание уделено безопасности Kubernetes-сред. В частности, система обрабатывает события Kubernetes (Pods, Nodes, API Server), выявляет атаки на кластеры, включая повышение привилегий и латеральное перемещение, а также обнаруживает аномалии в работе контейнерной оркестрации.

Конструктор правил корреляции, в свою очередь, позволяет наглядно и быстро создавать собственные сценарии обнаружения без написания кода. Наряду с этим, обогащение контекстом и данными Threat Intelligence связывает внутренние события с внешней информацией об угрозах для автоматического выявления индикаторов компрометации.

Встроенный мониторинг обеспечивает непрерывное наблюдение за ключевыми показателями безопасности, а именно: активностью источников, работой корреляционного движка, динамикой инцидентов и стабильностью потока Syslog-логов.

Управление агентами Windows и macOS, в свою очередь, осуществляется через единый веб-интерфейс, включая настройку политик сбора, мониторинг потребления ресурсов и контроль статуса в реальном времени.

Продукт успешно прошел аттестацию и имеет действующий Сертификат соответствия № ВУ/112 02.01. ТР027 036.01 02565 от 17 марта 2026 г., выданный Оперативно-аналитическим центром при Президенте Республики Беларусь, что подтверждает его соответствие установленным требованиям в области информационной безопасности.