???????? ??????? ? SIEM

Зона ответственности: Printum + Заказчик / Интегратор

> **Коротко:** Printum поддерживает передачу событий безопасности во внешние SIEM и системы мониторинга по протоколу Syslog, включая TCP, UDP и TCP с TLS. Передача выполняется только в исходящем направлении.

??????????

Система должна обеспечивать возможность передачи событий безопасности во внешние системы мониторинга, корреляции событий и расследования инцидентов.

Передаваемые события должны содержать достаточный объём информации для анализа событий безопасности и интеграции с корпоративным SOC или SIEM.

??? ??? ???????????? ? Printum

Printum поддерживает передачу событий безопасности во внешние системы мониторинга и управления событиями безопасности (SIEM).

Для передачи событий поддерживаются следующие механизмы:

- Syslog по UDP;
- Syslog по TCP;
- Syslog по TCP с TLS.

Для защищённого соединения может использоваться проверка сертификатов и TLS-шифрование канала связи.

Параметры подключения к внешней системе настраиваются через панель администратора Мониторинга, включая адрес назначения и используемый порт.

Передаваемые события могут фильтроваться по следующим параметрам:

- диапазон дат;
- типы событий;
- группы событий;

- результаты выполнения операций;
- уровень важности событий;
- локации.

Состав передаваемых событий соответствует атрибутному составу журнала информационной безопасности Printum и описан в статье «Атрибутный состав записи в журнале».

Для контроля передачи событий система ведёт учёт успешно и неуспешно переданных сообщений, а также отслеживает прогресс выгрузки событий.

При временной недоступности внешней системы события накапливаются и передаются после восстановления соединения.

Передача событий выполняется только в исходящем направлении. Приём данных через данный механизм не осуществляется.

??? ????????? ?? ????????????

Заказчик обеспечивает доступность и настройку внешней SIEM или иной системы мониторинга безопасности.

Для использования защищённого соединения по TLS должны быть настроены необходимые сертификаты и параметры доверия между системами.

Revision #1
Created 2026-06-08 19:39:00 UTC by DD
Updated 2026-06-08 19:39:01 UTC by DD