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

Зона ответственности: Printum + Заказчик / Интегратор

Коротко: Printum обеспечивает регистрацию событий безопасности и их передачу во внешние системы мониторинга. Обнаружение, корреляция и анализ инцидентов информационной безопасности выполняются средствами SIEM или SOC заказчика.

??????????

Система должна обеспечивать возможность мониторинга событий безопасности, анализа действий пользователей и расследования инцидентов информационной безопасности.

Для обнаружения инцидентов необходимо получать сведения о событиях безопасности, произошедших в системе, а также обеспечивать возможность их последующего анализа и корреляции.

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

Printum ведёт журнал информационной безопасности и регистрирует события, связанные с аутентификацией пользователей, изменением настроек системы, управлением учётными записями, изменением ролей и другими действиями, влияющими на безопасность системы.

Для каждого события сохраняется набор атрибутов, достаточный для анализа и расследования инцидентов. Состав записи журнала описан в статье «Атрибутный состав записи в журнале».

Printum поддерживает передачу событий безопасности во внешние системы мониторинга и управления событиями безопасности (SIEM). Подробная информация приведена в статье «Передача событий в SIEM».

Средства корреляции событий, автоматического обнаружения инцидентов, управления инцидентами и автоматизированного реагирования в состав Printum не входят.

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

Обнаружение, идентификация и корреляция инцидентов информационной безопасности выполняются средствами SIEM, SOC или других систем мониторинга безопасности, используемых заказчиком.

Для повышения эффективности мониторинга рекомендуется разрабатывать правила корреляции и сценарии реагирования с учётом перечня регистрируемых событий безопасности и требований службы информационной безопасности организации.

Revision #1
Created 2026-06-08 19:38:58 UTC by DD
Updated 2026-06-08 19:38:58 UTC by DD