УДК 004.056

В. О. Фененко
І. С. Зоря

ОПТИМІЗАЦІЯ РОЗМІЩЕННЯ СЕНСОРІВ СИСТЕМИ ЗБОРУ ТЕЛЕМЕТРІЇ (SYSLOG) ДЛЯ МОНІТОРИНГУ БЕЗПЕКИ МЕДИЧНОЇ УСТАНОВИ

Вінницький національний технічний університет

Анотація

У роботі розглянуто підходи до оптимізації моніторингу подій інформаційної безпеки в медичних установах. Проаналізовано специфіку об'єкта дослідження, запропоновано ієрархічну модель розміщення сенсорів збору телеметрії за протоколом Syslog та визначено критерії ефективності такої системи.

Ключові слова: кібербезпека, Syslog, моніторинг безпеки, медична інформаційна система, телеметрія, ієрархічна модель, Open Source.

Abstract

The paper examines approaches to optimizing the monitoring of information security events in medical institutions. The specifics of the research object are analyzed, a hierarchical model for placing telemetry sensors using the Syslog protocol is proposed, and the effectiveness criteria of such a system are determined.

Keywords: cybersecurity, Syslog, security monitoring, medical information system, telemetry, hierarchical model, Open Source.

Вступ

Сучасний етап розвитку галузі охорони здоров'я характеризується стрімкою цифровізацією та впровадженням комплексних інформаційно-комунікаційних систем [1] . Перехід на електронні медичні картки та використання систем архівації зображень PACS створюють єдиний цифровий простір, який водночас стає вразливим до кіберзагроз.

Головною проблемою для ефективного моніторингу безпеки є висока гетерогенність мережевого середовища та обмеженість ресурсів медичних закладів. Використання протоколу Syslog дозволяє забезпечити аудит подій, проте без належної оптимізації це призводить до надмірного навантаження на канали зв'язку та накопичення значного обсягу малоінформативних даних.

Аналіз об'єкта дослідження

Медична установа є складною територіально-розподіленою системою з високою гетерогенністю обладнання. Об'єкт дослідження включає різнорідні кінцеві точки: від адміністративних робочих станцій до діагностичних комплексів із обмеженими можливостями встановлення засобів захисту.

Специфіка закладу вимагає доступності сервісів у режимі 24/7, що унеможливлює агресивне сканування мережі. Тому основна увага приділяється пасивним методам збору телеметрії, які забезпечують моніторинг без впливу на стабільність життєво важливого обладнання [2].

Сегментація мережі медичної установи

Для ефективного логування мережу доцільно розділити на три сегменти з різними профілями ризику. Публічна зона (реєстратура, термінали) потребує контролю фізичного доступу та підключень. Діагностична зона (МРТ, КТ) через застарілі ОС потребує моніторингу на рівні шлюзів для виявлення аномальних потоків. Адміністративна зона (сервери МІС, бази даних) вимагає деталізованого аудиту доступу. Така модель дозволяє реалізувати диференційований підхід до безпеки в кожному сегменті.

Ієрархічна модель збору телеметрії та критерії оптимізації розміщення сенсорів

Замість централізованої схеми запропоновано багаторівневу ієрархічну модель із використанням Syslog-релеїв. Це дозволяє локалізувати трафік у відділеннях [3], запобігаючи перевантаженню магістральних каналів. Проміжні вузли здійснюють дедуплікацію та нормалізацію даних до їх надходження в центр обробки. Такий підхід знижує навантаження на ядро системи та забезпечує відмовостійкість через можливість локального накопичення повідомлень у разі розриву зв'язку.

Запропонована стратегія оптимізації базується на трикритеріальній моделі прийняття рішень. По-перше, це максимізація охоплення критичних активів (шлюзи сегментів, сервери СКБД), що обробляють конфіденційну медичну інформацію. По-друге, мінімізація часових затримок (Latency Optimization) при передачі критичних алертів, що є вирішальним для оперативного реагування на інциденти в умовах роботи закладу 24/7. По-третє, впровадження механізмів адаптивної диференціації трафіку за рівнями важливості (Severity Levels [4]), що дозволяє відсіювати "інформаційний шум" на рівні периферійних вузлів. Таке наукове обґрунтування точок розміщення сенсорів дозволяє досягти раціонального компромісу між глибиною аудиту безпеки та обчислювальною потужністю IT-інфраструктури лікарні.

Практична реалізація на базі Open Source рішень та очікувані результати

Реалізація орієнтована на програмне забезпечення з відкритим кодом. Для аналізу та візуалізації доцільно використовувати стеки ELK або Graylog, а для збору та фільтрації «інформаційного шуму» на джерелах – агенти rsyslog або syslog-ng [5]. Така архітектура гарантує масштабованість системи: додавання нових корпусів потребує лише встановлення локальних релеїв без зміни конфігурації центрального вузла.

Впровадження методики дозволяє виявляти до 99% аномалій на ранніх стадіях атак. Попередня фільтрація даних на рівні локальних сегментів зменшує мережеве навантаження на 30–40%. Створення захищеного сховища логів забезпечує надійну базу для ретроспективного аналізу інцидентів та оперативного реагування на загрози в реальному часі.

Висновок

Оптимізація розміщення сенсорів Syslog є ключовим фактором стійкості IT-інфраструктури лікарні. Ієрархічна модель збору телеметрії ефективно вирішує проблему «інформаційного шуму» та підвищує рівень відповідності закладу вимогам законодавства щодо захисту персональних даних. Це гарантує цілісність медичної інформації та безперервність надання послуг в умовах кіберзагроз..

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Захист персональних даних пацієнта при роботі з інформаційно-комунікаційними системами електронної охорони здоров'я. Міністерство охорони здоров'я України. URL: https://moz.gov.ua/uk/zahist-personalnih-danih-paciyenta-pri-roboti-z-informacijno-komunikacijnimi-sistemami-elektronnoyi-ohoroni-zdorov-ya (дата звернення 29.03.2026)
2. Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури. Держспецзв'язку України. URL: https://zakon.rada.gov.ua/rada/show/v0773519-23#Text (дата звернення 29.03.2026)
3. Rainer Gerhards and Others. System Architecture. rsyslog documentation. URL: https://docs.rsyslog.com/doc/development/architecture.html (дата звернення: 29.03.2026).
4. Guide to Computer Security Log Management. Special Publication 800-92. National Institute of Standards and Technology (NIST). URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf (дата звернення 29.03.2026)
5. Elastic Docs | Elastic. Elastic – The Search AI Company | Elastic. URL: https://www.elastic.co/guide/index.html (дата звернення: 29.03.2026).

Фененко Владислав Олександрович **–** студент групи КІТС-25м, факультет менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: energetic040406@gmail.com

Науковий керівник: ***Зоря Ірина Сергіївна*** **–** ас. каф. Менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: ira.zoria@vntu.edu.ua

Fenenko Vladyslav O. **–** student of group KITS-25m, Faculty of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: energetic040406@gmail.com

Supervisor: ***Zoria Iryna S.*** **–** assistant of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: ira.zoria@vntu.edu.ua