Шитов Є.А., магістрант
Фальковський І. Г., ст. викладач
Державний університет «Житомирська політехніка»

АНАЛІЗ СИСТЕМИ РЕЄСТРАЦІЇ ПОДІЙ GRAYLOG ТА ЇЇ АНАЛОГІВ, А ТАКОЖ МЕТОДИ ЇХ ЗАСТОСУВАННЯ ДЛЯ ЗАХИСТУ ДОМЕННИХ КОНТРОЛЕРІВ AD

В умовах сучасних кіберзагроз доменні контролери (DC), що є ключовими компонентами інфраструктури Active Directory (AD), потребують ефективних рішень для моніторингу та виявлення атак. Системи реєстрації подій, такі як Graylog, Splunk, ELK Stack та Wazuh, забезпечують централізований збір, аналіз та кореляцію логів, що є важливим елементом кібербезпеки організації.

У ході дослідження проведено порівняльний аналіз Graylog, Splunk, ELK Stack та Wazuh за ключовими критеріями: тип ліцензії, продуктивність обробки логів, інструменти аналізу загроз, можливості інтеграції з SIEM/SOAR-рішеннями, гнучкість налаштувань та спрощеність розгортання. Graylog, як система з відкритим кодом, забезпечує хорошу продуктивність та можливість розширення через власні плагіни. Splunk, хоч і є комерційним продуктом, має розвинені механізми поведінкового аналізу та підтримку машинного навчання. ELK Stack надає високу продуктивність та потужну систему індексації даних завдяки Elasticsearch, а Wazuh спеціалізується на виявленні загроз із вбудованими механізмами SIEM.

Graylog є рішенням з відкритим вихідним кодом, що підтримує централізований збір логів через Windows Event Forwarding (WEF) та дозволяє створювати гнучкі конвеєри обробки даних (pipelines) для ефективного аналізу без значного навантаження на систему. Splunk, будучи комерційним продуктом, забезпечує потужний аналітичний інструментарій, включаючи засоби машинного навчання для виявлення аномалій та аналізу поведінки користувачів (UEBA). ELK Stack, завдяки Elasticsearch, оптимізований для швидкої обробки великих обсягів даних та підтримує інтеграцію з Logstash для складних схем обробки подій. Wazuh спеціалізується на безпеці, пропонуючи вбудовані механізми SIEM та IDS/IPS, що дозволяють оперативно виявляти загрози, зокрема атаки Pass-the-Hash, Golden Ticket та інші методи компрометації облікових записів AD. [1]

Дослідження показало, що застосування Graylog для захисту доменних контролерів Active Directory дозволяє оперативно виявляти спроби компрометації облікових записів, атаки типу Pass-the-Hash, Golden Ticket та інші методи зловмисників. Використання автоматизованих правил кореляції подій дає змогу швидко ідентифікувати аномальну активність, а інтеграція з системами реагування SOAR сприяє своєчасному нейтралізуванню загроз.

Аналіз ефективності систем реєстрації подій показав, що централізований моніторинг і аудит змін у критичних об’єктах AD значно знижує ризики несанкціонованого доступу. Впровадження Graylog дозволяє забезпечити відповідність міжнародним стандартам безпеки, зокрема ISO/IEC 27001, та підвищити рівень захисту корпоративних мереж.[2]

Окрім технічних аспектів, важливим фактором ефективного використання систем реєстрації подій є правильна організація політик безпеки та навчання персоналу. Недостатня обізнаність адміністраторів та операторів SOC щодо можливостей сучасних засобів моніторингу може призвести до пропуску критичних загроз. Тому доцільно розробляти стандартизовані сценарії реагування, регулярно оновлювати правила кореляції подій та проводити тренінги з аналізу інцидентів на основі отриманих журналів.[3]

Таким чином, результати дослідження підтверджують необхідність використання систем реєстрації подій для контролю безпеки доменних контролерів. Впровадження Graylog та аналогічних рішень дозволяє створити ефективну систему моніторингу та захисту від сучасних кіберзагроз.

Список використаних джерел:

1. What is Graylog?. [Електронний ресурс] /Graylog.org. – 2025. – Режим доступу до ресурсу: https://go2docs.graylog.org/current/what_is_graylog/what_is_graylog.htm
2. Тернистим шляхом до системи логування Graylog. [Електронний ресурс] / Євгеній Сафонов – 2019. – Режим доступу до ресурсу: https://dou.ua/lenta/articles/graylog-system/
3. Організація навчання працівників обізнаності з кібербезпеки [Електронний ресурс] / ITS CSAT. – 2025. – Режим доступу до ресурсу: https://my-itspecialist.com/organizing-employee-cybersecurity-awareness-with-its-csat