# ПОБУДОВА SIEM СИСТЕМИ ЗАХИСТУ ELASTICSEARCH

Гріненко Т.О., Федоров І.А., Калмиков Д.І.
Харківський національний університет радіоелектроніки, Харків, Україна
Нарєжній О.П.
Харківський національний університет імені В.Н. Каразіна, Харків, Україна

Вразливості в системах інформаційних технологій (IT), недосконале програмне забезпечення, людський фактор – можуть призвести до серйозних втрат з боку бізнесу, а саме, зламу системи IT, крадіжки персональних даних тощо. Для запобігання або упередження інцидентів інформаційної безпеки були розроблені SIEM системи (Security Information and Event Management, SIEM). Технологія SIEM забезпечує аналіз у реальному часі подій (загроз) безпеки, що виходять від мережевих пристроїв та додатків, і дозволяє реагувати на них, з метою запобігання або зменшення істотних збитків.

На жаль, дуже мало підприємств розуміють важливість та необхідність використання SIEM систем для впровадження, підтримки, контролю та постійного вдосконалення системи менеджменту інформаційної безпеки підприємства. SIEM система фіксує всі події (збирає дані), що відбуваються в мережі, і надає їх користувачу в максимально зручному для сприйняття вигляді. Для кожного конкретного випадку та цілей, SIEM система виглядатиме порізному [1].

Метою доповіді є побудова лабораторної мережі з SIEM системою Elasticsearch [2, 3], що відповідає вимогам стандарту ISO/IEC 27001 [4], і надає можливість отримати навички роботи з SIEM системою, а саме: аналіз логів, реагування на інциденти інформаційної безпеки, розробка та обґрунтування правил моніторингу системи для утиліти Sysmon, розслідування інцидентів інформаційної безпеки, документування інцидентів, документування даних для аналізу.

В доповіді наведені результати аналізу міжнародного стандарту ISO/IEC 27001, результати аналізу та дослідження SIEM системи Elasticsearch, надано рекомендації щодо ефективної роботи з SIEM системою Elasticsearch, а саме: рекомендації з оптимальної конфігурації утиліти моніторингу системи Sysmon, наданий детальний опис алгоритму підняття стеку ELK (elasticsearch, logstash, kibana), наводиться демонстрація обробки та пересилання системних логів Windows 10 на logstash та їх аналіз через kibana.

**Список літератури**

1. https://softlist.com.ua/articles/chto-takoe-siem-sistema
2. https://www.elastic.co/
3. https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elastic-stack-on-ubuntu-22-04
4. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements.