Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту
Кафедра управління інформаційною безпекою

«Допущено до захисту»
Начальник кафедри УІБ
д.т.н. доц. Ткачук Р.Л.
_____
“____” _____2021 року

ДИПЛОМНА РОБОТА БАКАЛАВРА

на тему Дослідження та порівняльна характеристика сучасних SIEM-систем

Виконав:
студент 4 курсу,
групи КБ-41, спеціальності 125
«Кібербезпека»
(шифр і назва спеціальності)
Володимир ВЕРГУН
(прізвище, ім’я, по батькові)

Керівник Орест ПОЛОТАЙ
(прізвище та ініціали)

Рецензент Богдан МІЗЮК
(прізвище та ініціали)

Львів – 2021 року

АНОТАЦІЯ

Володимир Вергун «Дослідження та порівняльна характеристика сучасних SIEM-систем». Дипломна робота за спеціальністю 125 «Кібербезпека» складається з текстової частини, що містить 3 розділи, 52 с., 15 рис., 24 джерел.

Об'єктом дослідження є SIEM - системи управління інформаційною безпекою та подіями інформаційної безпеки.

Мета роботи – дослідження та аналіз роботи систем управління інформаційною безпекою та подіями інформаційної безпеки, тобто SIEM-системи.

Методи дослідження – вивчення наукової літератури з теми дослідження, нормативно-правової бази, аналітичний і порівняльний методи, методи системного аналізу, індукції.

У першому розділі розглядаються основні поняття та особливості використання сучасних SIEM-системи. Досліджуються особливості роботи та сфери застосування сучасних SIEM -системи. В другому розділі відбувається порівняння сучасних SIEM-систем за такими елементами: обробка подій в сучасних SIEM рішеннях, збір інцидентів в сучасних SIEM-інструментах, методи кореляції подій в сучасних SIEM-системах, візуалізація та інтерфейс сучасних SIEM-рішень, глобальні параметри та вбудований функціонал SIEM-інструментів. У третьому розділі досліджено SIEM системи Splunk.

SIEM-СИСТЕМИ, ІНФОРМАЦІЙНА БЕЗПЕКА, SPLUNK

ABSTRACT

Volodymyr Vergun "Research and comparative characteristics of modern SIEM-systems". Thesis in the specialty of 125 "Cybersecurity" consists of textual part that contains 3 sections, 52 pages, 15 figures, 24 sources.

The object of research is SIEM - information security management systems and information security events.

The purpose of the work - research and analysis of information security management systems and information security events, ie SIEM-system.

Research methods - the study of scientific literature on the research topic, regulatory framework, analytical and comparative methods, methods of systems analysis, induction.

The first section discusses the basic concepts and features of modern SIEM - systems. Peculiarities of work and scope of application of modern SIEM systems are investigated. The second section compares modern SIEM-systems by the following elements: event handling in modern SIEM-solutions, incident collection in modern SIEM-tools, methods of event correlation in modern SIEM-systems, visualization and interface of modern SIEM-solutions, global parameters and built-in functionality SIEM tools. The third section examines the SIEM of the Splunk system.

SIEM SYSTEMS, INFORMATION SECURITY, SPLUNK

Зміст

ЗАГАЛЬНІ ВИСНОВКИ

У роботі проведено аналіз характеристик, особливостей роботи та джерел інформацій, з якими працює SIEM-систем. Досліджено SIEM-системи в якості додаткового і дуже важливого елемента захисту від цілеспрямованих атак, при яких система виявляє вторгнення.

Сучасні системи безпеки та управління подіями аналізують дані, які отримали з логу реєстру, ґрунтуються на двох різних принципах: використання правил кореляції та побудова моделей користувачів та активів.

Перетворюючи багато різних типів повідомлень логу з багатьох різнотипних систем у загальну мову , платформа SIEM може порівнювати подібні, а потім співставляти дані, які в іншому випадку не могли бути відносними.

SIEM в основному застосовується в HIPAA, PCI, GDPR, внутрішні загрози, зловживання привілейованим доступом, полювання на загрозу та для загальної безпеки.

Також досліджено збір даних та опрацювання подій в сучасних SIEM-системах та їх порівняльна характеристика за такими критеріями: кореляція подій, візуалізація, глобальні параметри, функціонал та особливості.

Вибір правильного інструменту SIEM залежить від ряду факторів, включаючи бюджет організації та позицію безпеки.

Однак компанії повинні шукати інструменти SIEM, які пропонують такі можливості:

- звітність про відповідність;
- реагування на інциденти та криміналістику;
- моніторинг доступу до бази даних та сервера;
- виявлення внутрішньої та зовнішньої загрози;
- моніторинг, кореляція та аналіз загроз у реальному часі для різних програм та систем;
- система виявлення вторгнень (IDS), IPS, брандмауер, журнал додатків подій та інші інтеграції програм та систем;
- розвідка про загрозу ;
- моніторинг активності користувачів (UAM).

На прикладі сучасної SIEM-системи Splunk було досліджено, спроби отримати несанкціонований доступ до інформації. Було показано звіти та статистки всіх подій, які відбулись в системі. Далі за допомогою кореляції залишаються тільки найбільш небезпечні логи.

Це дало чітке розуміння роботи та для чого потрібна SIEM для організацій. Варто пам’ятати, що з розвитком технологій також розвивається і кіберзлочинність. Кожного дня зловмисники намагаються підкорювати найновіші системи. Пробують запустити зловмисне програмне забезпечення, віруси або дістати несанкціонований доступ до інформації. Для будь-якої компанії це понесе великі збитки, а то й може призвести до закриття. Компанія повинна мати окремий відділ зі захисту інформації та робочу SIEM-систему.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бурнашов С. В. Проектування та розроблення відкритих wifi-мереж з функцією збирання інформації про пристрої / С. В. Бурнашов, Ящук В. І. // Інформаційна безпека та Інформаційні технології: збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 27 листопада 2020 року. Львів, ЛДУ БЖД, 2020, 249 с. (С.121-124).

2. Грайворонський М. В. Безпека інформаційно-комунікаційних систем: підруч. для студ. вищ. навч. закл., які навчаються за напрямами "Безпека інформаційних і комунікаційних систем", "Системи технічного захисту інформації", "Управління інформаційною безпекою" / М. В. Грайворонський, О. М. Новіков. – К. : Вид-во BHV, 2009. – 608 с.

3. Захарова М.В. Синтез механізмів захисту інформаційних ресурсів від кібератак. Автореф. Канд. Техн. Наук. ДСК

4. Иванов О. Что такое SIEM-системы и для чего они нужны? [Електронний ресурс] /Олег Иванов // Anti-Malware.ru. – 2017. – Режим доступу до ресурсу:https://www.anti-malware.ru/analytics/Technology_Analysis/Popular-SIEM-Starter-Use-Cases.

5. Полотай О., Довганик С. SIEM-системи, як елемент аналізу та управління подіями CSOC. Автоматизація та комп’ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції. – Черкаси, 2020. - С.60-61.

6. Полотай О., Довганик С. Системи збору інформації про безпеку та управління подіями. Захист інформації в інформаційно-комунікаційних системах : зб. тез. ІІІ Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів. Львів, ЛДУ БЖД. – 2019. С. 7-9.

7. Ящук В. І. Онтологія наукових досліджень та методологія наукового пізнання / В.І. Ящук // Економіка в контексті глобальних змін суспільства:

матеріали Міжнародної науково-практичної конференції (м. Дніпро, 18 липня 2020 р.). – Дніпро: НО «Перспектива», 2020. – 140 с. (С.100-104).

8. Bumgarner V. Implementing Splunk: Big Data Reporting and Development for Operational Intelligence / Vincent Bumgarner. – Birmingham, 2013. – 417 c. – (Packt Publishing). – (978-1-84969-328-8).

9. Carasso D. Exploring Splunk / David Carasso. – New York, 2012. – 156 c. – (Splunk). – (978-0-9825506-7-0).

10. IBM QRadar : Architecture and Deployment Guide. // International Business Machines Corporation. – 2019. – С. 56.

11. Jacobs J. ata-Driven Security: Analysis, Visualization and Dashboards / J. Jacobs, B. Rudis. – Canada, 2014. – 321 c. – (John Wiley&Sons). – (978-1-118-79372-5).

12. Lentz R. Definitive Guide to Security Intelligence and Analytics / Robert Lentz. – Annapolis, 2019. – 61 c. – (CyberEdge Gourp). – (978-0-9961827-4-4).

13. Melone M. Think Like a Hacker: A Sysadmin’s Guide to Cybersecurity / M. Melone, D. Zinck., 2017. – 85 c. – (Michael J. Melone). – (0692865217).

14. O.Polotai, O. Belej, N. Nestor. Developing a local positioning algorithm based on the identification of objects in a wireless Wi-Fi network of the mall. IEEE 16th International Conference on the Perspective Technologies and Methods in MEMS Design, MEMSTECH 2020 - Proceedings, 2020, pp. 53-58.

15. O.Polotai, O. Belej., N. Nestor, S. Panchak Developing a Model of Cloud Computing Protection System for the Internet of Things. 2020 IEEE 16th International Conference on the Perspective Technologies and Methods in MEMS Design, MEMSTECH 2020 - Proceedings, 2020, pp. 53-58.

16. O.Polotai, O.Belej, K.Kolesnyk Application of neural networks in intrusion monitoring system for wireless sensor networks. Conference on computer science and information technologies. CSIT 2020: advances in intelligent systems and computing, vol 1293, Springer, Cham. – pp.1101-1115.

17. PETTERS J. What is SIEM? A Beginner’s Guide [Електронний ресурс] / JEFF PETTERS // Varonis. – 2020. – Режим доступу до ресурсу: https://www.varonis.com/blog/what-is-siem/.

18. Preimesberger C. Splunk vs. LogRhythm: SIEM Head-to-Head [Електронний ресурс] / Chris Preimesberger // eWEEK. – 2019. – Режим доступу до ресурсу: https://www.eweek.com/security/splunk-vs-logrhythm-siem-head-to-head.

19. Sanders C. Applied Network Security Monitoring: Collection, Detection, and Analysis / C. Sanders, J. Smith. – 225 Wyman Street, Waltham, MA 02451, USA, 2014. – 467 c. – (Elsevier). – (978-0-12-417208-1).

20. Savaram R. IBM QRadar Tutorial [Електронний ресурс] / Ravindra Savaram // MindMajix. – 2019. – Режим доступу до ресурсу: https://mindmajix.com/ibm-qradar-tutorial.

21. SIEM – Security Information and Event Management [Електронний ресурс] // Amica – Режим доступу до ресурсу: https://amica.ua/siem-security-information-and-event-management/.

22. Top SIEM Use Cases for Correlation and SIEM Alerts Best Practices [Електронний ресурс] // DNSstuff. – 2020. – Режим доступу до ресурсу: https://www.dnsstuff.com/common-siem-alerts .

23. Vault A. 4 SIEM Use Cases That Will Dramatically Improve Your Enterprise Security [Електронний ресурс] / Alien Vault // Infocorp Security&Networking – Режим доступу до ресурсу: https://www.infocorp.cl/ver-mas-articulos/145-4-siem-use-cases-that-will-dramatically-improve-your-enterprise-security.

24. WHAT IS SIEM? (PART 3): HOW DOES SIEM WORK? [Електронний ресурс] // Comtact SOC, Cyber Security. – 2018. – Режим доступу до ресурсу: https://www.comtact.co.uk/blog/what-is-siem-part-3-how-does-siem-work.