Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: *«Аналіз логів з використанням фаєрволу Watchguard»*

Виконав: студент (ка)

Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)

Волков А.В.
підпис (прізвище та ініціали)

Керівник *Загородна Н.В.*
підпис (прізвище та ініціали)

Нормоконтроль *Лобур Т.Б.*
підпис (прізвище та ініціали)

Завідувач кафедри *Загородна Н.В.*
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«19» __червня__ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Волкову Антону Вячеславовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Аналіз логів з використанням фаєрволу Watchguard

Керівник роботи Загородна Наталія Володимирівна, к.т.н. доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «03» 04 2023 року № 4/7-349

2. Термін подання студентом завершеної роботи 17.06.2023

3. Вихідні дані до роботи Фаєрвол Watchguard, персональний комп'ютер з ОС Windows, ELK Stack

4. Зміст роботи (перелік питань, які потрібно розробити)
Аналіз можливостей використання фаєрволів для захисту інформації
Огляд типів загроз і ризиків для інформації в інформаційно-комунікаційних мережах
Логи та інструменти для збору
Обґрунтування вибору фаєрволу Watchguard
Проектування системи захисту інформації за допомогою фаєрволу Watchguard
Аналіз структури логів
Аналіз інцидентів і логів фаєрволу Watchguard
Безпека життєдіяльності, основи охорони праці
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Пилипець.М.І., проф. кафедри МТ		

7. Дата видачі завдання 16.01.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	16.01 – 19.01	*Виконано*
2.	Підбір джерел про фаєрвол Watchguard та логи	20.01 – 05.02	*Виконано*
3.	Опрацювання джерел в галузі дослідження	06.02 – 10.03	*Виконано*
4.	Аналізування доцільності використання фаєрволу Watchguard для безпеки від зовнішніх загроз	11.03-05.04	*Виконано*
5.	Оформлення розділу «аналіз технічного завдання по використанню фаєрволу в системах захисту інформації»	06.04 – 17.04	*Виконано*
6.	Оформлення розділу «Теоретична частина»	18.04 – 29.04	*Виконано*
7.	Оформлення розділу «Практична частина»	30.04 – 13.05	*Виконано*
8.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи охорони праці»	14.05 – 21.05	*Виконано*
9.	Оформлення кваліфікаційної роботи	22.05 – 05.06	*Виконано*
10.	Нормоконтроль	06.06 – 11.06	*Виконано*
11.	Перевірка на плагіат	12.06 – 15.06	*Виконано*
12.	Попередній захист кваліфікаційної роботи	16.06 – 19.06	*Виконано*
13.	Захист кваліфікаційної роботи	20.06.2023	

Студент _____ *Волков А.В.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Загородна Н.В.*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Аналіз логів з використанням фаєрволу Watchguard // Кваліфікаційна робота ОР «Бакалавр» // Волков Антон Вячеславович// Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2023 // С. __ , рис. – , табл. – , кресл. – , додат. –

Ключові слова: БЕЗПЕКА, КОНФІДЕНЦІЙНІСТЬ, ЦІЛІСНІСТЬ, ФАЄРВОЛ, БРАНДМАУЕР, ЗАХИСТ, ВРАЗЛИВІСТЬ, ЛОГ, ПРИСТРІЙ, ЖУРНАЛ, МЕТОД, ОЦІНКА, АНАЛІЗ.

Інформація є найважливішим ресурсом підприємств та організацій, адже завдяки їй виконуються всі основні операції та здійснюються процеси, від яких залежить результативність господарської діяльності та прибуток підприємства. Особливо це стосується інформації про інноваційні та технологічні винаходи, конкурентні переваги, персональні дані працівників тощо. Тому питання розмежування доступу до інформації та убезпечення від втручань є актуальним.

Метою роботи є дослідження ефективності використання апаратних засобів кібербезпеки на прикладі фаєрволу Watchguard.

Згідно поставленої мети маємо наступні завдання дослідження:

- здійснити аналіз можливостей використання фаєрволів для захисту інформації;
- провести аналіз методів оцінки ефективності використання фаєрволів;
- здійснити обґрунтування вибору методики аналізу логів для оцінки ефективності роботи фаєрволів;

- дослідити можливості проектування системи захисту інформації за допомогою фаєрволу Watchguard;
- провести тестування апаратного мережевого екрану та зробити висновки щодо його ефективності.

Предмет дослідження – оцінка методів кібербезпеки підприємства шляхом аналізу засобів захисту фаєрволом.

Об’єкт дослідження – апаратний захист інформації за допомогою фаєрволів під час протидії зовнішнім загрозам.

Методологічна основа та методи дослідження: основою роботи є дослідження історичні, аналітичні, аналізу та синтезу. Теоретико-методологічна основа роботи послужили наукові концепції, які були розроблені науковцями зі всього світу, нормативно-правові акти у сфері захисту інформації та інформатизації. Для аналізу загроз та розробки засобів захисту використовано аналітичні методи. При визначенні рівня безпеки до та після формування алгоритму використання фаєрволу як засобу апаратного захисту в рамках оперативного реагування на інциденти в сфері кібербезпеки було застосовано метод порівняння.

Дослідження ґрунтується на наукових розробках, що охоплюють широкий спектр тем, таких як загальна теорія управління, моделювання складних систем, автоматизовані системи управління, захист інформації, інформаційна безпека, теорія прийняття рішень, менеджмент і т.д. Ці розробки складають основу інформаційної бази дослідження.

Структура роботи. Робота складається зі вступу, 4 основних розділів з підрозділами, висновків та переліку джерел посилань.

ABSTRACT

Log analysis using Watchguard firewall // Thesis of educational level "Bachelor" // Volkov Anton Vyacheslavovych // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, СБ-41 group // Ternopil, 2023 // P. ___ , fig. -____, table. - __ , chair. - ___ , added. -___.

Keywords: SECURITY, CONFIDENTIALITY, INTEGRITY, FIREWALL, BRANDMAUER, PROTECTION, VULNERABILITY, LOG, DEVICE, JOURNAL, METHOD, EVALUATION, ANALYSIS.

Information is the most valuable resource for enterprises and organizations, as it supports all essential operations and processes that determine the efficiency of business activities and the profitability of the enterprise. This particularly applies to information about innovative and technological inventions, competitive advantages, personal employee data, and so on. Therefore, the issue of access control and protection against intrusions is crucial.

The purpose of work is to study the effectiveness of using hardware security tools using the example of the Watchguard firewall.

In accordance with the set goal, the research tasks are as follows:

- Conduct an analysis of the possibilities of using firewalls for information protection.
- Perform an analysis of methods for evaluating the effectiveness of using firewalls.
- Substantiate the choice of log analysis methodology for evaluating the effectiveness of firewall operations.
- Investigate the possibilities of designing an information protection system using Watchguard firewall.

- Conduct testing of hardware network screens and draw conclusions about their effectiveness.

The subject of the research is the evaluation of enterprise cybersecurity methods through firewall protection analysis.

The object of the research is hardware information protection using firewalls in countering external threats.

The research was based on the application of historical, analytical, analysis, and synthesis methods. The theoretical and methodological foundation of the work consists of scientific concepts developed by researchers worldwide, as well as the regulatory and legal acts of Ukraine in the field of informatization and information security. Analytical methods were employed to analyze threats and the development of security measures. The comparative method was used to determine the level of security before and after the formulation of the firewall usage algorithm as a hardware protection measure within the framework of operational response to cyber security incidents.The information base of the research consists of scientific developments in general management theory, modeling complex systems, automated management systems, information protection, information security, decision theory, and management, among others.

The structure of the work: The paper consists of an introduction, 4 main chapters with subsections, conclusions, and a list of references.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ПК – персональний комп’ютер

ЕОМ – Електоронна обчислювальна машина

ІКС – Інформаційно-комунікаційна система

ПЗ – Програмне забезпечення

ОС – Операційна система

ІБ – Інформаційна безпека

VPN – Virtual Private Network

DOS – Denial-of-Service

TOR – The Onion Router

ВСТУП

Забезпечення інформаційної безпеки є однією з найважливіших пріоритетних справ для підприємств і організацій. Захист інформації від зовнішніх загроз та уникнення витоків стають все більш актуальними завданнями. В зв'язку з цим, розробка та впровадження систем захисту інформації, зокрема використання фаєрволів, набувають великого значення. Ця кваліфікаційна робота присвячена аналізу технічного завдання щодо використання фаєрволу в системах захисту інформації. Вона має на меті розглянути можливості використання фаєрволів для захисту інформації та провести огляд типів загроз і ризиків, які існують для інформації в інформаційно-комунікаційних мережах.

Далі у роботі розглядається теоретична частина, де детально розглядаються поняття про логи та їх важливість для забезпечення безпеки. Також обґрунтовується вибір фаєрволу Watchguard для впровадження і підтримки безпеки, а також проводиться проектування системи захисту інформації за допомогою даного фаєрволу.

У практичній частині роботи проводиться аналіз структури логів та інцидентів, пов'язаних з фаєрволом Watchguard. Це дозволяє з'ясувати ефективність його роботи та виявити можливі уразливості системи.

Нарешті, в розділі, присвяченому безпеці життєдіяльності та основам охорони праці, досліджується питання охорони праці на підприємстві, зокрема освітлення та мікроклімат. Також розглядається тема долікарської допомоги.

Загалом, ця кваліфікаційна робота спрямована на аналіз використання фаєрволу в системах захисту інформації та дослідження його ефективності. Результати дослідження можуть бути використані для покращення безпеки інформаційних систем та захисту конфіденційної інформації.

РОЗДІЛ 1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ ПО ВИКОРИСТАННЮ ФАЄРВОЛУ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Аналіз можливостей використання фаєрволів для захисту інформації

Фаєрвол (брандмауер, між мережевий екран) – це система безпеки мережі, яка відстежує та контролює вхідний і вихідний трафік на основі попередньо визначених правил безпеки. Фаєрвол зазвичай створює бар'єр між безпечною внутрішньою мережею та зовнішньою, незахищеною мережею. Його основне призначення – захист внутрішньої мережі або окремих її вузлів від несанкціонованого доступу. Фаєрвол контролює доступ до мережевих ресурсів за допомогою позитивної моделі управління (у внутрішню мережу надходить лише авторизований трафік, а весь інший трафік заборонено).

Типові функції фаєрволу:

- контроль доступу до вузлів мережі;
- фільтрація доступу до незахищених сервісів;
- контроль порядку доступу до мережі;
- запобігання спробам доступу із зовнішньої та внутрішньої мереж;
- запобігання витоку конфіденційної інформації з внутрішньої захищеної мережі.

Фаєрволи поділяються на 2 великі категорії:

- фаєрвол на рівні мережі – дозволяє або блокує трафік на основі вихідних IP-адрес або портів;
- фаєрвол на рівні програмного забезпечення – аналізує протоколи на рівні ПЗ, одночасно відстежуючи активність протоколу щодо певного профілю та дозволяючи або забороняючи трафік на основі відхилень профілю.

Деякі дослідники додають до цих типів третій – фаєрволи рівня підключення (з’єднання). У кожного з цих трьох типів існує власний підхід до забезпечення безпеки мережі. Фаєрвол на мережевому рівні може бути реалізований за допомогою екрануючого маршрутизатора, який контролює лише мережеві дані та інформацію на транспортному рівні пакетної служби. Однак, недоліком цих маршрутизаторів є те, що наступні п'ять рівнів залишаються поза контролем.

Адміністратори, що мають справу із екранованими маршрутизаторами, повинні знати, що більшість пристроїв фільтрації пакетів не мають механізмів аудиту та попередження. Тобто, роутер можна атакувати і відбивати їх велику кількість, не повідомляючи адміністраторів [1].

Фаєрволи прикладного, більш відомі як проксі-сервери. Завдяки фаєрволам прикладного рівня встановлюється фізичний розділ між локальною мережею та Інтернетом. Це дозволяє відповідати найвищим стандартам безпеки.

Проте, оскільки фаєрволи на рівні програмного забезпечення повинні аналізувати пакети та приймати рішення щодо контролю доступу до них, це незаперечно впливає на продуктивність мережі. Тому використовуються швидкі комп'ютери як проміжні сервери.

Фаєрвол рівня підключення також можна вважати проксі-сервером. Різниця лише в програмному забезпеченні. Для прикладного фаєрволу, для кожної мережевої служби, наприклад FTP або HTTP потрібне спеціальне програмне забезпечення. Фаєрволи рівня підключення у той же час, замість цього використовують протоколи [2].

Фаєрволи з фільтрацією пакетів вирішують, пересилати чи відхиляти пакет, дивлячись на IP-адреси, прапори або номер TCP-порту в заголовку пакета.

IP-адреса та номер порту є інформацією про мережевий і транспортний рівень відповідно, але фільтри пакетів також використовують інформацію про прикладний рівень, оскільки всі стандартні служби в TCP/IP прив’язані до певного номера порту [3].

Фаєрволи з серверами прикладного рівня використовують сервери певних служб – TELNET, FTP, які запускаються на брандмауері і пропускають через них весь трафік, пов'язаний з цією службою. Це створює два з’єднання типу: клієнт – брандмауер – місце призначення.

Для кожного фаєрвола, набір підтримуваних серверів є різним, але найпоширенішими серверами для таких служб є:

- термінали;
- передача файлів;
- електронна пошта;
- http;
- rsh;
- nntp.

Застосування серверів на прикладному рівні забезпечує конфіденційність структури локальної мережі від зовнішніх користувачів. Додатковою перевагою є можливість аутентифікації на рівні користувача. Аутентифікація - це процес підтвердження особи, і в даному випадку вона стосується підтвердження того, що користувач є тим, за кого себе видає. Детальніші відомості про аутентифікацію будуть надані нижче [20].

Параметрами опису правил доступу є: ім'я користувача, ім'я сервісу припустимий часовий проміжок для використання сервісу, дозволені комп'ютери для використання сервісу і схеми аутентифікації. Сервери на рівні застосунків забезпечують найвищий рівень захисту, оскільки вони взаємодіють зі зовнішнім світом за допомогою обмеженої кількості додатків, які здійснюють повний контроль вхідного і вихідного трафіку.

Сервер рівня підключення є транслятором підключення TCP. Користувач підключається до певного порту фаєрвола, після чого брандмауер підключається до пункту призначення з іншого боку фаєрвола. Цей інтерпретатор під час сеансу відтворює байти в обох напрямках, що призводить до його функціонування як

провідник. Зазвичай, призначений пункт визначається заздалегідь, тоді як джерела можуть бути декілька (з'єднання "один до багатьох"). Застосування різних портів дозволяє створювати різні конфігурації.

Завдяки цьому типу є можливість створювати транслятор для будь-якої визначеної користувачем служби на основі TCP, контролювати доступ до цієї служби та збирати статистику використання [22].

У телекомунікаційній галузі набули широкого поширення чотири типи фаєрволів:

- фаєрволи інформаційної безпеки є найпоширенішим типом брандмауерів у світі, що запобігає атакам на комп'ютери, сервери та веб-сайти;
- сигнальні фаєрволи – їхнє основне завдання – захист телекомунікаційних мереж від шахраїв, які користуються слабкими місцями мережі для отримання доступу до SMS-повідомлень, голосових дзвінків абонентів тощо;
- голосові фаєрволи – їх можна описати як розширені версії сигнальних брандмауерів із акцентом на захист користувачів від голосового шахрайства;
- фаєрволи SMS — це спеціалізовані брандмауери, призначені для захисту користувачів і телекомунікаційних компаній від шахрайства, утримуючи трафік A2P на монетизованих білих маршрутах і уникаючи незаконних сірих маршрутів Нижче наведено основні переваги та недоліки фільтрів пакетів і серверів на рівні програми.

До позитивних властивостей пакетних фільтрів можна віднести:

- відносно низька вартість;
- адаптація при встановленні правил фільтрації;
- низька затримка при пересиланні пакетів;

Недоліки брандмауера такого типу полягають у наступному:

- локальна мережа видима (маршрут) з Інтернету;

- для опису правил фільтрації пакетів потрібні хороші знання TCP/UDP;
- якщо фаєрвол вийде з ладу, всі комп'ютери стають повністю беззахисними або недоступними;
- автентифікація за допомогою IP-адреси може бути обманута за допомогою IP-спуфінгу (система-атака видає іншу IP-адресу);
- немає аутентифікації на рівні користувача.

Переваги серверів прикладного рівня включають:

- приватна мережа є невидимою ззовні;
- при виникненні несправності брандмауера, пакети перестають проходити через нього, тому немає загрози для захисту машин через нього;
- захист на рівні програми дозволяє проводити велику кількість додаткових перевірок, таким чином зменшуючи ймовірність злому за допомогою дірок у програмному забезпеченні;
- аутентифікація на призначеному користувачеві рівні може бути реалізована через систему негайного попередження про спробу злому.

Недоліками цього типу є:

- вартість вище, ніж у випадку з пакетними фільтрами;
- відсутність можливості використання протоколів RPC і UDP;
- ефективність нижча, ніж у пакетних фільтрів.

Також варто розглянути апаратні брандмауери від відомих і провідних компаній, які є лідерами в цій галузі. Одним із прикладів таких апаратних брандмауерів є рішення Cisco.

На відміну від традиційного програмного брандмауера, призначеного для захисту комп’ютера або сервера, «брандмауер як послуга» використовується для захисту кількох клієнтських IT-інфраструктур одночасно. Однак це не єдина відмінність такого підходу від традиційних апаратних і програмних рішень.

Традиційний брандмауер (його ще називають брандмауером або міжмережевим екраном) захищає лише пристрій, на якому він встановлений, від загроз з локальної мережі чи Інтернету. Це програмне забезпечення виконує базову фільтрацію мережевого трафіку, попереджаючи користувача про можливі загрози у разі небезпеки або блокуючи потенційно небезпечні з'єднання відповідно до певних правил.

«Брандмауер як послуга» (Firewall as a Service, FWaaS) працює на стороні провайдера і являє собою відмовостійкий кластер апаратних і програмних брандмауерів, ресурси якого надаються клієнтам відповідно до моделі обслуговування. FWaaS також виконує перевірки безпеки та діє як бар'єр між компонентами IT-інфраструктури клієнта та підключеними до нього системами та мережами.

Брандмауери можна умовно розділити на два види. Програмне забезпечення встановлюється на фізичних або віртуальних пристроях і використовується для відстеження вхідного та вихідного трафіку та блокування потенційних загроз. Це спеціалізоване програмне забезпечення можна встановити безпосередньо на комп'ютер або на сервер, який може виконувати роль програмного маршрутизатора. Ключовими перевагами програмних міжмережевих екранів можна вважати меншу вартість порівняно з апаратними засобами, можливість захисту окремих сегментів локальних мереж зсередини, а також можливість їх розгортання на комп'ютерах користувачів і існуючих серверах. Недоліки включають обмежену пропускну здатність порівняно з апаратними рішеннями та, у деяких випадках, досить трудомістке налаштування.

Апаратний брандмауер - це пристрій, призначений безпосередньо для обробки трафіку і працює під керуванням спеціального програмного забезпечення. Така система захищає підключену фізичну або віртуальну IT-інфраструктуру від мережевих атак.

До популярних брандмауерів належать такі рішення, як Cisco ASA, FortiGate, CheckPoint, SonicWALL і WatchGuard. Вони, як це буває у випадку з апаратними міжмережевими екранами, більш ефективні, ніж програмні рішення, характеризуються високою ефективністю, надійністю, а також простотою підключення та використання. Основним недоліком апаратного брандмауера є його висока вартість, що робить недоцільним використання його для індивідуального захисту.

Брандмауер, який пропонується в сервісній моделі, по суті, є апаратним забезпеченням. Це обладнання управляється спеціалізованим програмним забезпеченням, яке дозволяє створювати віртуальні домени - кожен з них буде обслуговувати конкретного клієнта і забезпечувати максимально можливу ізоляцію клієнтських навантажень один від одного. Віртуалізація працює за аналогічним принципом, де ізоляція віртуальних машин забезпечується гіпервізором.

По суті, в рамках послуги «мережевий екран як послуга» замовник отримує потужне та ефективне апаратне рішення для захисту будь-якої IT-інфраструктури: хмарної, фізичної чи гібридної. Цей підхід робить дорогі апаратні брандмауери доступнішими, оскільки вимагає використання потужного пристрою для захисту кількох клієнтських IT-інфраструктур. Насправді це той самий принцип, який лежить в основі популярної соціально-економічної моделі спільного використання, коли завдяки спільному використанню деякі цінні ресурси стають доступними для спільного одночасного використання.

Таким чином, ми оглянули основні різновиди фаєрволів та їх особливості в застосуванні під різні задачі захисту інформаційних мереж.

1.2 Огляд типів загроз і ризиків для інформації в інформаційно-комунікаційних мережах

Суб'єктами захисту інформації є:

- електронні документи;
- програмне забезпечення;
- ноу-хау;
- база даних;
- альтернативні матеріальні носії інформації.

Найважливіші типи інформації, на які впливає проблема інформаційної безпеки, включають:

- стратегічна інформація;
- політична інформація;
- соціально-економічна інформація;
- військова інформація;
- дослідницька інформація.

Предметом захисту є інформація, яка обробляється мережі банківської установи. Крім того, це можуть бути права власників цієї інформації, власників мережі і права користувача.

Всі дані, що містяться в локальній мережі, підлягають захисту відповідно до вимог власника цієї інформації або чинного законодавства.

Пов’язані з обробкою інформації суб’єкти це:

- власники інформації або уповноважені ними особи;
- власники мережі або уповноважені ними особи;
- користувачі інформації;
- користувачі локальної мережі.

Отримання доступу до інформації, яка зберігається, обробляється та передається в мережу, можливе лише відповідно до правил, що регулюють

розмежування доступу, встановлених власником інформації або уповноваженою ним особою. Винятком є передбачені чинним законодавством випадки.

Переваги використання програмного забезпечення моніторингу автоматизованої системи:

- визначення усіх випадків несанкціонованого доступу до інформації, яка є конфіденційною, із зазначенням точного часу та робочого місця в мережі, звідки була здійснена така спроба;
- локалізація всіх випадків зміни або знищення інформації;
- встановлення фактів несанкціонованого інсталювання ПЗ;
- контролювання можливості використання ПК у неробочий час;
- визначення всіх випадків несанкціонованого використання модемів у внутрішній мережі;
- виявлення випадків набору критичних слів і фраз з клавіатури, складання будь-яких критичних документів, розголошення яких третім особам призведе до матеріальних збитків;
- отримання достовірної інформації, на основі якої буде розроблено політику інформаційної безпеки компанії;
- контроль доступу до хостів і персональних комп'ютерів;
- проведення інформаційного аудиту;
- розслідування комп'ютерних інцидентів;
- проведення наукових досліджень, пов'язаних з визначенням точності, ефективності та адекватності реагування персоналу на зовнішню діяльність;
- визначити завантаженість АРМ ЕОМ;
- визначити навантаження на персонал підприємства;
- відновлення критичної інформації після збою комп'ютерної системи;
- забезпечення спостережуваності комп'ютерної системи. Саме ця властивість, залежно від якості її виконання, дозволяє більшою чи меншою

мірою контролювати дотримання працівниками компанії встановлених правил безпечної роботи на комп’ютері та політики безпеки [18, с. 102].

Для створення множини реальних загроз доцільно використовувати двоскладову структуру, де перша частина описуватиме дію небажаної події та предмет цієї дії, а друга частина описуватиме ситуацію, що характеризує причину ця акція відбулася (табл. 1.1).

Таблиця 1.1 - Процедури створення множини можливих загроз

Тип загрози	Об'єкти дії			
	Обладнання	Програми	Дані	Персонал
Витік інформації	Крадіжка медіа, підключення, несанкціоноване використання ресурсів	Несанкціоноване копіювання, перехоплення	Крадіжка, копіювання, перехоплення	Передача інформації про захист, розкриття
Порушення інформаційної цілісності	Підключення, модифікація, спеціальні доповнення, зміна режимів, несанкціоноване використання ресурсів	Введення «троянського коня» і «жуків»	Спотворення, модифікація	Вербування, підкуп персоналу
Порушення продуктивності системи	Зміна режимів, вимкнення, розорилися	Спотворення, видалення, заміна	Видалення, спотворення	Звільнення, фізичне вилучення

Системи виявлення можна поділити на системи виявлення аномалій і системи виявлення ознак. Головним недоліком систем виявлення особливостей є їх спрямованість на конкретні типи атак, які вважаються найнебезпечнішими на момент розробки системи. При зміні характеристик трафіку або нових атаках виникає потреба у перегляді і переосмисленні завдань системи виявлення. Різні припущення про функціонування системи використовуються в системах виявлень аномалій, такі як статистична однорідність трафіку. У результаті невеликі змінювання в моделях трафіку або наданих послугах можуть вимагати повторного навчання алгоритму виявлення. Одним з можливих виходів із цієї ситуації є використання комплексного підходу до побудови системи захисту від відмови в обслуговуванні, що включає моніторинг функціонування системи,

збереження історії транзакцій, ведення спеціального репозиторію для інтелектуального аналізу активності та дій зловмисників, та прийняття рішення про вибір стратегії протистояння. Пропонується побудувати систему захисту на основі таких елементів:

- агенти спостереження;
- засоби для попередньої обробки та зберігання;
- сховище для зберігання інформації про транзакції, що описують функціонування системи;
- репозиторій з аналітичними компонентами для виявлення загроз і ознак шкідливої діяльності;
- контратаки [1; с. 572].

Тому для того, щоб створити систему захисту об'єкта за допомогою фаєрвола, необхідно спочатку визначити рівень загроз. Аналіз факторів інформаційного ризику (FAIR) є одним із багатьох стандартних методів і технік для оцінки ефективності брандмауерів інформаційної безпеки [24]. Простіше кажучи, це модель кількісного аналізу ризику, яка описує, що таке ризик, як він працює та як його кількісно визначити. Розроблено Джеком А. Джонсом, сертифікованим спеціалістом з безпеки інформаційних систем (CISSP), сертифікованим менеджером з інформаційної безпеки (CISM), сертифікованим аудитором інформаційних систем (CISA). На відміну від стандартів оцінки ризиків, результати яких зосереджені на якісних кольорових діаграмах або числових зважених шкалах, модель кількісного аналізу ризиків FAIR спеціалізується на фінансових результатах, призначених для управління ризиками підприємства. Методика FAIR містить детальну класифікацію факторів, що призводять до виникнення загроз, визначає їх вплив один на одного та взаємозв’язки між ними. Це дозволяє адекватно оцінити частоту реалізації ризику та масштаб збитків.

Одним із стандартизованих методів є метод оцінки загроз IT-системам – Risk Assessment and Analysis Method (далі - RAM), яку запровадила асоціація аудиту і контролю інформаційних систем ISACA (Information Systems Audit and Control Association). Методологія розроблена, щоб допомогти організаціям визначити, оцінити та керувати ризиками, пов'язаними з їхніми інформаційними системами та технологічною інфраструктурою.

ISACA RAM надає організаціям структурований підхід до оцінки та вирішення ризиків, дотримуючись ряду кроків. Ці кроки зазвичай включають:

- встановлення контексту: розуміння цілей організації, середовища та стійкості до ризику;
- виявлення ризиків: визначення потенційних ризиків і вразливостей в IT-системах, процесах та інфраструктурі організації;
- оцінка ризику: оцінка ймовірності та потенційного впливу ідентифікованих ризиків для визначення їх значущості;
- реагування на ризики: створення планів для зниження ризиків і вибір відповідних засобів контролю для зниження виявлених ризиків до прийнятного рівня;
- впровадження контролю: впровадження вибраних засобів контролю та моніторинг їх ефективності;
- моніторинг ризиків та комунікація: неперервне відстеження ризиків та оцінка ефективності контрольних заходів та передача інформації, пов'язаної з ризиками, відповідним зацікавленим сторонам.

ISACA RAM узгоджується з міжнародно визнаними стандартами управління ризиками, такими як ISO 31000, і включає в себе різні системи контролю, включаючи COBIT (контрольні цілі для інформаційних і суміжних технологій), щоб забезпечити комплексний підхід до оцінки та управління ризиками в сфері IT [23].

Крім згаданих практичних методів, існують також академічні методи. Ці методи мають систематичний характер і використовують наукові інструменти оцінки ризику.

Одним із методів цього класу є метод, розроблений професорами В. О. Хорошко та В. В. Єрмошиним [13]. Автори використовують систематичний аналіз структури підприємства, встановлення межового рівня ризику для окремих підрозділів, оцінку інформаційної інфраструктури та організаційної структури підприємства з метою оцінки ризику інформаційної безпеки. Вони також враховують значення ризику автоматизованих систем, що використовуються підприємством, оцінюють активи підприємства та ймовірність загроз для його автоматизованих систем, а також ідентифікують ризики. Результатом цього процесу є ймовірність певного типу загрози на основі виявлених вразливостей, заходів захисту [19, с. 37].

До найбільш небезпечних явищ, які несуть загрозу інформації в ІКМ, відносяться: [21]:

- пошукова оптимізація (SEO). Зловмисники використовують це для поширення шкідливих програм, використовуючи уразливості в технологіях та програмному забезпеченні SEO. Вони розширюють можливості своїх раніше скомпрометованих веб-сайтів, щоб залучити користувачів шукати приманливі повідомлення у пошукових системах, отримувати результати і переходити за основними посиланнями на веб-сайти зловмисників. Це може призвести до комп'ютера, що стає компрометованим і потенційно шкідливим;
- вразливості стороннього ПЗ, наприклад т.зв нульова вразливість. Зловмисники все частіше використовують уразливості офісних програм, таких як офісний софт Mircosoft, а також мультимедійних програвачів, наприклад, iTunes разом із спеціальними інструментами для перегляду документів. Вони використовують ці уразливості для зупинки певних процесів;

- Spear Phishing. Використовується хакерами, щоб обманом змусити користувача зробити щось зловмисне, наприклад встановити зловмисне програмне забезпечення. Зловмисники надсилають чітко націлені повідомлення конкретним співробітникам компанії для переконання жертви, щоб вона відкрила зловмисне вкладення або перейшла на сторінку, що містить шкідливий фрагмент для використання вразливості;

- отримання контролю над браузером, за допомогою якого зловмисники розміщують на веб-сайтах контент, що містить шкідливі скрипти (скрипти). При відвідуванні такого сайту, запускаються відповідні шкідливі автоматизовані програми на своєму комп'ютері, що передає хакеру контроль над його браузером. Це дає зловмиснику можливість використовувати браузер користувача як платформу для подальших атак на інші системи, включаючи внутрішні ресурси та сервери компанії;

- масові SQL-ін’єкції. Зловмисники використовують їх для викрадення даних, які є конфіденційними з окремих веб-додатків і БД. Це також може призводити до змін у вмісті баз даних, що відображатимуться на веб-сайтах. Зловмисники можуть змінювати веб-вміст і вставляти шкідливі сценарії на веб-сайт, спрямовані на браузери відвідувачів, а також використовувати інші експлойти, що використовують уразливості безпеки на стороні користувача.

- атаки на адміністративні мережеві інтерфейси, які використовують хакери для управління певними системами чи інфраструктурою (ERP-системи, системи управління та контролю електроживлення та кондиціювання повітря тощо) шляхом захоплення контролю над браузером;

- атаки на соціальні мережі. Зловмисники використовують їх для отримання інформації про компанію, її робітників, роботодавців, діяльність організації та можливо навіть технології;

- хеш-атаки. Зловмисники використовують їх для отримання доступу до корпоративного домену шляхом використання інтегрованих пакетів атак у

Windows, наприклад, Nmap. В цьому випадку, зловмисники використовують вкрадені хеші для аутентифікації замість паролів, набуваючи незаконний доступ до системи;

- апаратний злом, який шляхом перехоплення інформації на шинах даних (прослуховування шини), злому, перемикання системного часу (збій годинника) та інших складних апаратних атак дозволяє зловмиснику обхід механізмів безпеки та отримання ключів шифрування [21].

Розглянемо детальніше види атак на інформацію, що здійснюються зловмисником за допомогою каналів зв'язку комп'ютерних мереж і засоби захисту від них. Основні категорії таких атак: атаки доступу; модифікаційні атаки; атаки типу «відмова в обслуговуванні»; атаки застереження [12; с. 63].

Атака на модифікацію спрямована на незаконну зміну інформації, порушуючи цілісність. На теперішній момент відомі наступні види атак:

- заміни;
- додаток;
- руйнування.

Атака підміни полягає в заміні цільової інформації іншою, не пов'язаною з цільовою. Атака додавання використовується для внесення нових, часто зайвих даних. Вона передбачає використання шкідливого ПЗ для викрадення інформації, яка доступна законному користувачеві до хакера. Атаки модифікації мають місце, якщо в ІКМ є вузькі (вразливі) місця. Цей вид атаки здійснюється в два етапи. Перший крок — перехоплення переданої інформації, другий — внесення змін до її відправки за призначенням.

Характерним проявом модифікаційної атаки є сфера фінансів. Наприклад, підмінна атака може проявлятися в тому, що змінюється заробітна плата працівника установи; додаткова атака проявляється коли на рахунок платника не надходять платіжні кошти; деструктивна атака робить запис банківської операції недійсним [9; с. 64].

Мета атаки доступу – порушення конфіденційності інформації, що зберігається, обробляється та поширюється в системах інформаційно-комунікаційних технологій. Є всього два способи реалізувати атаки доступу. Спершу, це аналіз файлів, методом перегляду їх один за одним. Для його реалізації зловмисник повинен мати законний доступ до ІКТ-системи, бути в списку співробітників цієї організації або особою, яка отримала доступ, наприклад, через клієнта банку, а система захисту інформації не може накладати додаткові запити на аутентифікацію користувача, крім IP-адреси на основі ідентифікації користувача. Така атака називається інфрачервоною атакою. Виявлення IR-атаки спуфінгу вказує на підготовку зловмисника до типів атак, таких як DDoS [9; с. 63].

Одним з найважливіших завдань у галузі інформаційних послуг є забезпечення неперервної доступності та безперебійної роботи баз даних у будь-який час. При такому режимі роботи також потрібно забезпечити високий рівень надійності та стійкості системи навіть у стресових ситуаціях. Одним із серйозних та поширених видів атак є DDoS-атака (атака розподіленого відмови в обслуговуванні) [1; с. 230].

Розподілені атаки типу «відмова в обслуговуванні» є реальною загрозою для компаній у всьому світі. Атаки здійснюються великою кількістю програмних агентів, розташованих на хостах, які зловмисник раніше зламав. Здійснення цих атак призводить як до збою окремих серверів і сервісів, а й до повної зупинки мережі. Через критичність і нетривіальність цього класу атак побудова ефективного захисту від них є складною науково-технічною проблемою. На рівні маршрутизатора захист від DDoS-атак вже досить успішно реалізована Cisco Systems. Загалом, проблема DDoS-атак зараз, як і раніше, стоїть дуже гостро для більшості компаній [4; с. 6].

DoS-атаки — це певний вид зловмисних дій, метою яких є доведення комп’ютерної системи до стану, коли вона не може обслуговувати авторизованих

користувачів або належним чином виконувати покладені на неї функції. Стан «відмова в обслуговуванні» зазвичай спричинений помилками програмного забезпечення або надмірним навантаженням на мережевий канал або всю систему. У результаті програмне забезпечення або вся операційна система машини «зависає» або перебуває в «зациклюваному» стані. А це загрожує простоєм, втратою гостей/клієнтів і збитками. Основна мета DoS/DDoS-атак: приведення об’єкта в придатний для використання стан шляхом неотримання користувачем системи до спільних ресурсів або ускладнять цей доступ; заборонити доступ до популярного сайту; отримати конфіденційну інформацію, що зберігається в системі.

Основні загрози інформаційній безпеці в системі:

- несанкціонований доступ. В сучасному світі інформація практично не створюється та не обробляється без використання комп’ютера. Така інформація зазвичай передається по всьому підприємству або з кореспондентами (замовниками) через загальнодоступні телекомунікаційні системи зв'язку. Основні таблиці, які відносяться до цієї інформації є конфіденційними. Порівнюючи ризики несанкціонованого розголошення конфіденційної інформації в системах електронної обробки даних з системами, які є ручними, то напрошується висновок, що автоматизовані системи виділяє те, що набагато більше інформації можна перенести в зручнішу та технологічнішу форму, і це можливо зробити безслідно НСД, що мало місце. Чутливі місця: клеми; зброя; хости та сервери;

- відмова доступу. Вплив є особливо руйнівним для операцій з електронними кредитними переказами та платіжних систем, зокрема тих, які надають послугу гарантованого розрахунку в день показу, де одержувачі коштів залежать від отримання коштів для покриття своїх зобов’язань. Наслідки серйозного збою в системі можуть значно перевищувати вартість заміни

пошкодженого обладнання, даних або ПЗ. Уваги також потребують сервери та робочі станції, оскільки вони є потенційно уразливими елементами;

- кібератака. Наслідками, які кібератака може за собою понести є: спотворення/крадіжка, знищення інформації через неконтрольовану модифікацію IP-адреси, пошкодження інформації через неавторизований логічний доступ до інформації зовнішніми зловмисниками. Тут можливі як іміджеві, так і фінансові втрати, якщо особисті дані були викрадені/скопійовані або кошти були переведені в невідомому напрямку. Чутливі місця: термінали, банкомати, сервери та робочі станції.

Наразі слід розглянути можливі дії системи захисту інформації в різних випадках. Для цього розробимо алгоритм дій щодо оцінки ризиків і загроз для розподіленої інформаційної мережі та відповідного реагування (табл. 1.2).

Таблиця 1.2 - Алгоритм оцінки ризиків і загроз

№ з/п	Етап	Що оцінюється	Виявлення
1	Характеристики системи	- Обладнання - Програмне забезпечення - Системні інтерфейси - Дані та інформація - Люди - Призначення системи	- Межі системи - Системні функції - Критичність системи та даних - Чутливість системи та даних
2	Ідентифікація загроз	- Історія атак на систему - Дані служби безпеки, інформація державних органів, ЗМІ	Виявлені загрози
3	Ідентифікація вразливості	- Попередні звіти про оцінку ризиків - результати аудиту системи безпеки - Вимоги безпеки - Результати перевірки безпеки	Список потенційних вразливостей
4	Контрольний аналіз	- Поточні перевірки - Планові перевірки	Перелік поточних та планових перевірок

Таким чином, ми досліджували завдання та дії, які покладаються на систему захисту інформації. Відповідно до розроблених алгоритмів, система повинна регулярно аналізувати можливі загрози шляхом виявлення девіантної активності в будь-якому елементі розподіленої інформаційної мережі установи та належним чином виконувати заплановані алгоритмом дії для уникнення або мінімізації наслідків атаки. в інформаційній мережі. В результаті ефективних дій системи захисту інформації мінімізуються іміджеві та фінансові втрати установи, тому функціонування такої системи є обов’язковим елементом роботи кожної мережі.

РОЗДІЛ 2 ТЕОРЕТИЧНА ЧАСТИНА

2.1 Логи та інструменти для збору

Логи (logs) - це записи або журнали, які фіксують події, виникаючі в системі або програмі. Ці записи можуть містити різноманітну інформацію, таку як діагностичні повідомлення, помилки, виконані дії, стан системи тощо.

Вони дозволяють відстежувати, аналізувати та налагоджувати роботу системи або програми. Основною метою їх використання є виявлення помилок, відстеження виконання певних операцій, моніторингу стану системи, виявлення зловмисних дій, аналізу продуктивності та інших аспектів роботи програми чи системи.

Логи можуть містити різні типи інформації, такі як:

- діагностичні повідомлення: це повідомлення, які надають інформацію про поточний стан системи, програми або процесу. Наприклад, такі повідомлення можуть містити інформацію про початок або завершення певного процесу, статус виконання операцій, інформацію про конфігурацію системи тощо;
- повідомлення про помилки: ці повідомлення вказують на помилки, які виникли під час виконання системи або програми. Вони можуть містити детальну інформацію про помилку, включаючи стек викликів, код помилки, контекст виконання тощо. Повідомлення про помилки допомагають ідентифікувати та виправляти проблеми;
- історія виконання: це записи, які фіксують послідовність подій або операцій, виконаних в системі або програмі. Історія виконання дозволяє відстежувати послідовність дій та розуміти, як система або програма працюють в реальному часі;

- метри та статистика: логи можуть містити дані про продуктивність системи або програми, такі як час відповіді, обсяг використаної пам'яті, завантаження процесора та інші показники. Ці дані можуть бути використані для моніторингу та аналізу продуктивності, виявлення проблем та вдосконалення роботи системи.

Логи поділяються на декілька видів:

- системні логи – ті, які пов’язані із системними подіями;
- серверні логи – ті, що відповідають за звернення до сервера;
- логи баз даних – ті, які мають відношення до запитів баз даних;
- логи Cron – логи планувальника завдань;
- логи панелі управління хостингом – логи, які відносяться до хостингу, де розміщений сайт;
- лог основного файлу – лог, до прикладу, фаєрвола, DNS сервера тощо.

Логи знаходяться у різних місцях, залежно від того, яке ПЗ та ОС використовується. Зазвичай, найбільш частим місцем їх зберігання є шлях /var/log.

Додатковими загальними «технологічними» вимогами є підтримка різних форматів лог-файлів, низьке споживання ресурсів, зручний користувальницький інтерфейс і т. д. В теперішній час існує кілька комерційних засобів керування журналами для створення, організації, зберігання, пошуку та обробки лог-файлів. В першу чергу це LogParser, Logstash, WebLog Explorer [5; с. 62]. Ці засоби досить різні і далі будуть розглянуті детальніше.

LogParser (рис.2.1) – потужний інструмент , розроблений компанією Microsoft, який дозволяє запитувати, аналізувати та обробляти різноманітні типи лог-файлів. Він підтримує різні формати логів, такі як текстові файли, журнали подій Windows, журнали IIS та багато інших. LogParser має великий набір команд та запитів, які дозволяють виконувати розширені операції над лог-даними,

включаючи фільтрацію, агрегацію, злиття даних з різних джерел та багато іншого. Основною перевагою LogParser є його потужна мова запитів, яка дозволяє виконувати складні запити та аналізувати великі обсяги даних. Це означає, що ви можете створювати складні запити, які фільтрують дані на основі різних умов, агрегують дані для створення зведених таблиць чи підсумкових результатів, злити дані з різних джерел логів та виконувати інші операції для аналізу та вивчення лог-даних. Це надає користувачам зручність та гнучкість при роботі зі складними лог-файлами та дозволяє проводити детальний аналіз великих обсягів даних, що є досить важливим фактором для глибокого розбору подій та виконання складних запитів до лог-даних.

Недоліком LogParser є те, що він вимагає деякого рівня експертизи і знань SQL-подібного запитування для ефективного використання. Він також не має графічного інтерфейсу користувача та інтеграції з іншими інструментами аналізу даних.

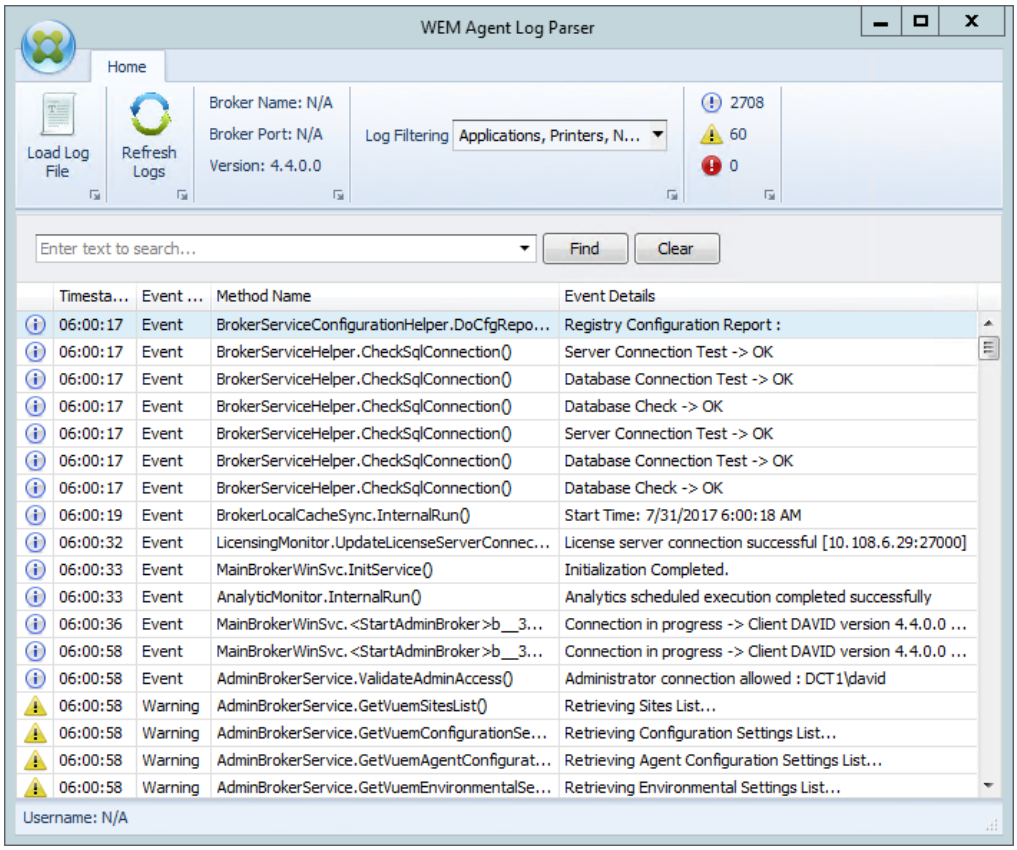


Рисунок 2.1 – Інтерфейс Log Parser

Logstash (рис.2.2) - це відкрите програмне забезпечення, що належить до стеку Elastic, яке використовується для збору, обробки та візуалізації лог-даних. Він може бути використаний для збору лог-файлів з різних джерел, їх обробки та направлення до різних призначень, таких як бази даних або інструменти аналізу. Logstash підтримує різні фільтри для обробки лог-даних, такі як розбиття на поля, регулярні вирази, географічне мапування тощо. Він також має гнучкість інтеграції з іншими компонентами стеку Elastic, такими як Elasticsearch для зберігання та пошуку даних, а також Kibana для візуалізації та аналізу. Logstash є простим в налаштуванні та використанні і позитивним фактором також є гнучкість обробки даних та можливість інтеграції з іншими компонентами стеку Elastic.

Недоліком може бути вимога до додаткових ресурсів для обробки великого обсягу даних та відносно складність управління та масштабування.

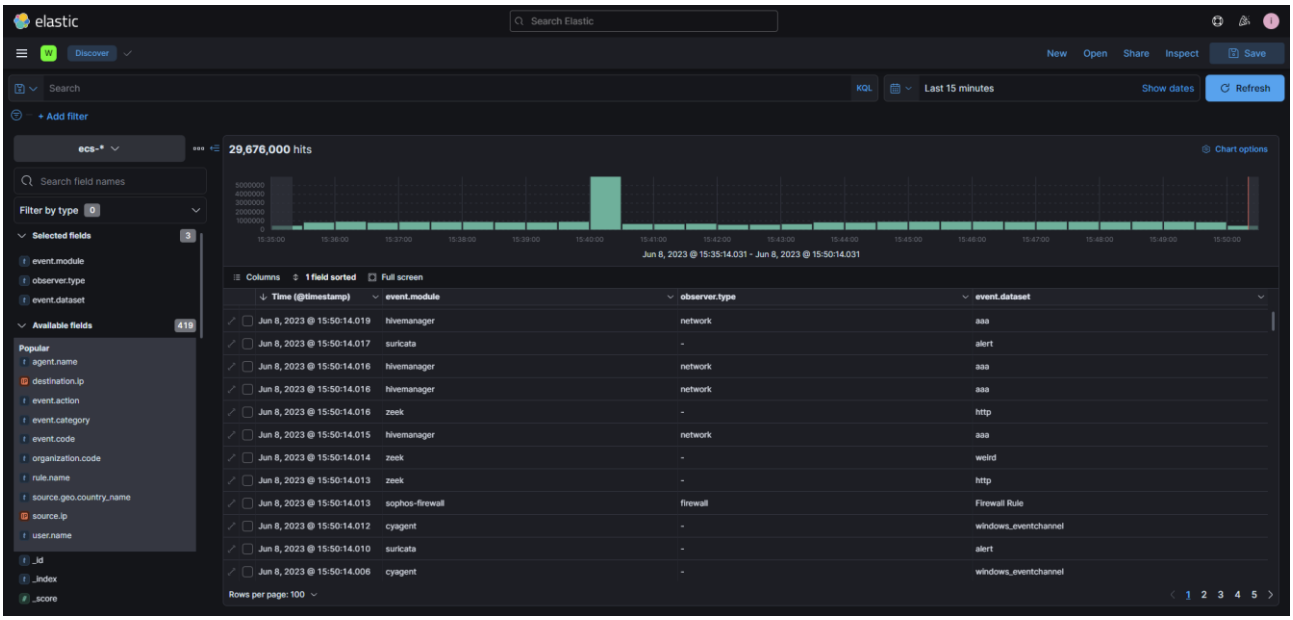


Рисунок 2.2 – Інтерфейс Logstash з візуалізатором Kibana

WebLog Explorer (рис.2.3) - це комерційний програмний продукт, який спеціалізується на аналізі лог-файлів веб-серверів, таких як Apache, Nginx, IIS та інші. Він надає зручний графічний інтерфейс користувача, який дозволяє

переглядати, фільтрувати та аналізувати лог-дані в зручному форматі. WebLog Explorer має вбудовані засоби візуалізації, такі як графіки та діаграми, для аналізу різних аспектів веб-трафіку. Він також надає різні функції звітності та експорту даних для подальшого аналізу. Основною перевагою WebLog Explorer є його спрощений процес аналізу лог-файлів веб-серверів та зручний інтерфейс користувача. Недоліком може бути обмежений функціонал, орієнтований переважно на аналіз лог-файлів веб-серверів, та відсутність гнучкості для аналізу інших типів лог-даних.

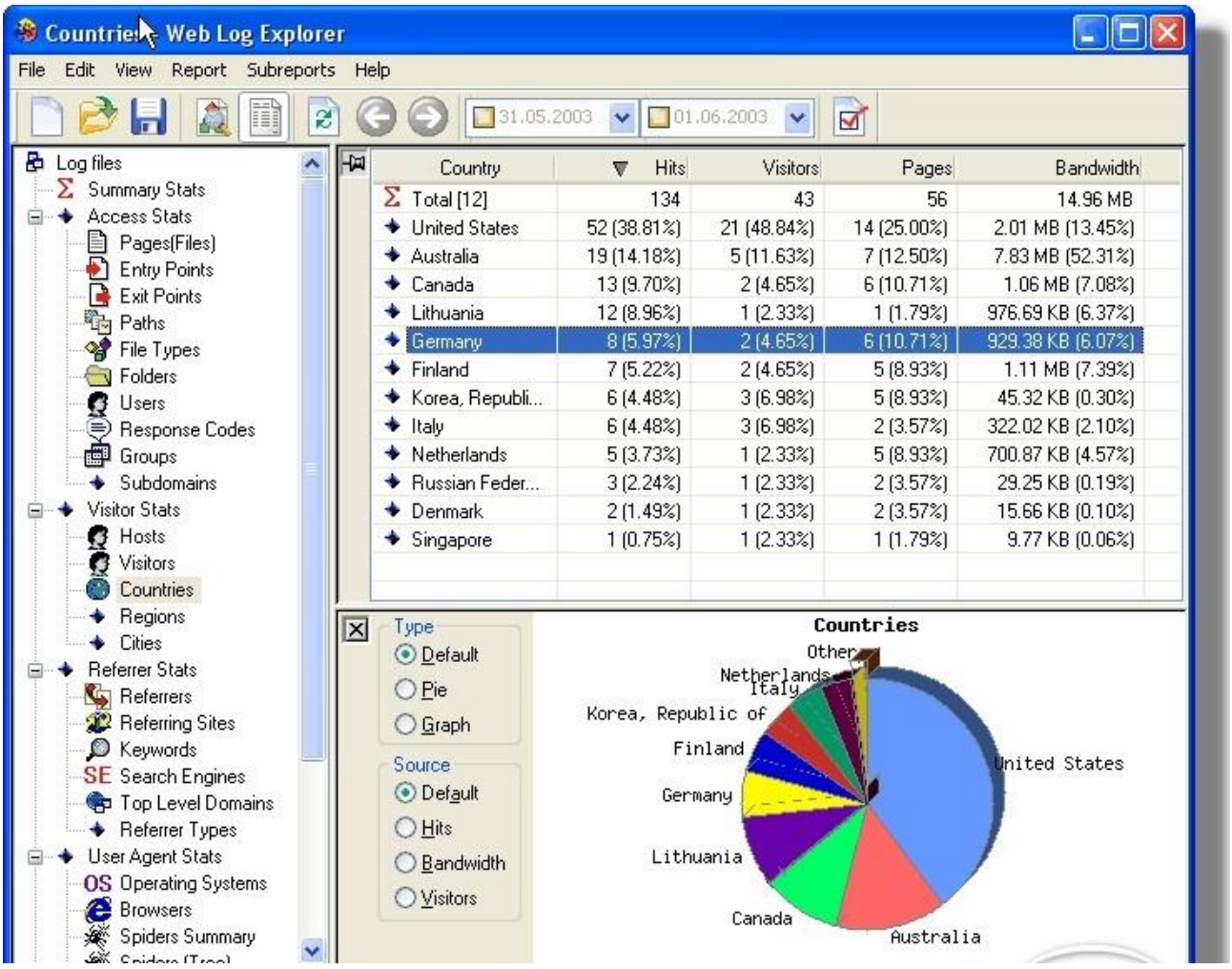


Рисунок 2.3 – Інтерфейс Web Log Explorer

Спроба атак на сервер може призвести до кодів статусу як успіху, так і помилки. Індикатори стану в журналах сервера — це тризначні коди стану, які сервер надсилає назад клієнту. Ця інформація має велику цінність, оскільки вона

дає змогу визначити, чи був запит успішним (коди, що починаються з 2), чи було перенаправлення (коди, що починаються з 3), чи сталися помилки, спричинені клієнтом (коди, що починаються з 4), або помилки сервера (коди, що починаються з 5). Під час атаки зловмисник часто зіткнеться з послідовністю помилок, перш ніж знайде правильну комбінацію, що призведе до успіху. Таким чином, ми можемо аналізувати IP-адреси, які спричиняють найбільше помилок. Велика кількість помилок сама по собі не є доказом атаки, але це може бути початковою точкою для подальшого дослідження. Крім аспектів безпеки, такий аналіз також може допомогти виявити проблеми, з якими користувачі стикаються при використанні системи, а також ідентифікувати IP-адреси, які створюють найбільше навантаження на систему.

Іншим методом аналізу є виявлення IP-адрес з максимальною кількістю запитів, які виявились невдалими. Проаналізувавши наші журнали, ми можемо визначити відсоток невдалих запитів відносно загальної кількості запитів. Найвищий відсоток невдалих запитів буде спостерігатись, коли клієнти здійснили лише кілька запитів або навіть один. Зазвичай ці записи не є проблемою. Однак, якщо ми помітимо значну кількість таких запитів протягом короткого періоду часу, це може вказувати на розподілену DoS-атаку, коли боти надсилають запити доступу з великої кількості різних IP-адрес.

Під час аналізу ми можемо виділити IP-адреси з найбільшою кількістю невдалих запитів на день або місяць. Якщо в певний день з будь-якої IP-адреси вузла надходить дуже велика кількість запитів, це може означати спробу атаки, таку як атака DoS. У цьому випадку ви бачите, що IP-адреси з найбільшою кількістю невдалих запитів на день є тими самими адресами, які зазвичай генерують найбільшу кількість запитів.

Найпростіший спосіб виявити спроби атаки в журналах сервера – пошук у полі «запит». У цьому полі відображається інформація про запит користувача до сервера, тому багато атак залишають у цьому полі сліди, які нам потрібно знайти.

Тому аналіз лог-файлів спрямований на виявлення загроз та їх подальшу локалізацію.

2.2 Обґрунтування вибору фаєрволу Watchguard для впровадження і підтримки безпеки

WatchGuard Firewall - це комплексна система безпеки мережі, розроблена компанією WatchGuard Technologies. Основна функція фаєрволу WatchGuard - контроль трафіку, що проходить через мережу. Він діє як "воротар" або фільтр між зовнішнім і внутрішнім мережевими середовищами, аналізуючи пакети даних та приймаючи рішення щодо їхнього подальшого руху на основі заданих правил і політик безпеки.

У фаєрвола WatchGuard є різні функції, з яких можна відмітити наступне:

- SPI (Stateful Packet Inspection) - це технологія, яка використовується для аналізу трафіку мережі на основі стану з'єднання. Вона дозволяє виявляти і контролювати вхідний і вихідний мережевий трафік, забезпечуючи високий рівень безпеки. Основний принцип роботи SPI полягає в тому, що фаєрвол відстежує стан кожного з'єднання, перехоплює пакети даних і аналізує їх заголовки. Він зберігає інформацію про стан з'єднання, таку як IP-адреси, порти, стан пакетів тощо, у своїй пам'яті. При проходженні кожного нового пакету даних фаєрвол порівнює його збережений стан з правилами безпеки, які задані адміністратором мережі. Ці правила можуть визначати, які типи трафіку є безпечними і повинні бути пропущеними, а які - потенційно небезпечними і мають бути заблоковані або перенаправлені. SPI дозволяє встановлювати контекст для кожного з'єднання і вести стеження за його станом в реальному часі. Наприклад, якщо відкривається з'єднання з певним зовнішнім IP-адресом і портом, фаєрвол зберігає цю інформацію і знає, що після цього потрібно

дозволяти пакетам з цього з'єднання проходити через нього. Однією з переваг SPI є його здатність виявляти й блокувати певні типи атак, які можуть проникнути через простий пакетний фільтр. Він може розпізнавати аномальний або небезпечний трафік, який не відповідає стандартним сценаріям комунікації. Крім того, SPI дозволяє підтримувати стан з'єднання, що спрощує аналіз і фільтрацію трафіку. Це дозволяє фаєрволу бути більш ефективним та пропускати лише дозволений трафік, ігноруючи непотрібні пакети;

- DPI (Deep Packet Inspection) - це технологія, яка використовується для детального аналізу пакетів даних, що проходять через мережу. Вона дозволяє отримати більш глибоке розуміння вмісту та структури пакетів, а також виявити потенційно шкідливі віруси, загрози або аномалії. Основний принцип роботи DPI полягає в тому, що фаєрвол аналізує не лише заголовки пакетів даних, але й їхні внутрішній вміст. Він розібирає пакети на рівні протоколів мережі і додатково аналізує дані, що містяться всередині пакетів. Це дозволяє виявляти конкретні типи даних, виконувати перевірку на відповідність стандартам протоколів, а також знаходити загрози та шкідливі програми, які можуть бути приховані в пакетах. Серед можливостей DPI можна відмітити виявлення шкідливих загроз, фільтрацію вмісту, контроль протоколів та додатків й аналіз трафіку. Однією з головних переваг DPI є його здатність забезпечувати більш глибокий та точний рівень аналізу трафіку, що дозволяє виявити ширший спектр загроз та застосувати більш детальні політики безпеки. Однак, слід зауважити, що DPI може вимагати більше обчислювальних ресурсів і призводити до збільшення затримки обробки пакетів в порівнянні з іншими методами інспекції пакетів;

- IPS (Intrusion Prevention System) - є однією з ключових функцій у фаєрволі безпеки і відіграє важливу роль у захисті мережі від вторгнень і атак. Він працює в режимі реального часу і спрямований на виявлення та блокування потенційно шкідливого трафіку та атак на мережу. Основними функціями є

виявлення вторгнень, блокування шкідливого трафіку, оновлення баз даних загроз, кореляція подій та проактивний захист;

- VPN-підтримка дозволяє безпечно з'єднувати локальні мережі чи віддалених користувачів з приватною мережею за допомогою шифрованого тунелю. Ця функція дозволяє забезпечити захищений обмін даними через незахищені мережі, такі як Інтернет. Основними її можливостями є підтримка IPsec (Internet Protocol Security), що є стандартним протоколом для забезпечення безпеки мережевих з'єднань через Інтернет. IPsec використовує механізми шифрування та аутентифікації для створення захищеного тунелю між мережами або віддаленими користувачами. Крім IPSec, WatchGuard також підтримує VPN на основі протоколу SSL/TLS (Secure Sockets Layer/Transport Layer Security). Цей тип VPN забезпечує безпечне з'єднання через веб-браузер, що дозволяє віддаленим користувачам отримувати доступ до ресурсів мережі без необхідності встановлювати спеціальне. Також, WatchGuard дозволяє налаштовувати мультисайтові VPN, що дозволяє з'єднувати багато локальних мереж між собою. Це дозволяє побудувати захищену мережу з багатьма розташованими географічно об'єктами або філіями. Врешті-решт VPN-підтримка впроваджує автентифікацію й авторизацію, захист від загроз і моніторинг та аналітику;

- блокування загроз і антивірусний захист – ідентифікування, блокування та вирішування потенційно шкідливих загроз для мережі. Аспектами цього є: інтелектуальне виявлення загроз, блокування шкідливого трафіку, оновлення бази даних загроз, виявлення невідомих загроз, антивірусний сканер, інтеграція з додатковими захисними рішеннями;

- журналювання та аналіз дозволяють збирати, зберігати і аналізувати дані про активність мережі з метою забезпечення безпеки та виявлення потенційних проблем. Основні аспекти включають журнали подій, аналіз

мережевого трафіку, інтеграцію з системами моніторингу, попередження та сповіщення й аналітику безпеки;

- веб-фільтрація – функція, яка дозволяє контролювати доступ до Інтернету та фільтрувати веб-зміст для захисту мережі від небажаного, шкідливого або небезпечного вмісту. Основною метою веб-фільтрації є обмеження доступу користувачів до певних категорій веб-сайтів і контенту, а також захист мережі від загроз, пов’язаних з веб-джерелами. Основними можливостями є функції категоризації веб-сайтів, білий та чорний список, контроль за додатковими протоколами, фільтрація на основі ключових слів, SSL-інспекція тощо.

Фаєрволи WatchGuard мають свої плюси та мінуси, які варто враховувати при розгляді їх як рішення для захисту мережі. Ось кілька плюсів і мінусів фаєрволу WatchGuard:

Плюси:

- Комплексний захист: як вказано вище, WatchGuard пропонує широкий спектр функцій безпеки, таких як фірмовий брандмауер, блокування загроз, антивірусний захист, VPN-підтримка та інші. Це забезпечує комплексний захист мережі від різних видів загроз;
- легкість використання: фаєрволи WatchGuard мають інтуїтивний і легкий у використанні інтерфейс, що дозволяє адміністраторам легко налаштовувати та керувати параметрами безпеки мережі;
- журналювання та аналіз: WatchGuard надає розширені можливості журналювання та аналізу, що дозволяють збирати дані про активність мережі та проводити комплексний аналіз для виявлення загроз та вразливостей;
- масштабованість: WatchGuard пропонує рішення для малого, середнього і великого бізнесу, які можуть масштабуватись під зростаючі потреби мережі;

Мінуси:

- вартість: фаєрволи WatchGuard можуть мати високу вартість, особливо для підприємств з обмеженим бюджетом. Вони можуть вимагати інвестицій у придбання обладнання та підписки на оновлення програмного забезпечення;
- складність конфігурування: для встановлення і налаштування фаєрволу WatchGuard може знадобитися технічна експертиза або допомога фахівців. Вони можуть бути складними для конфігурування, особливо для користувачів без досвіду роботи зі схожими системами;
- потреба у підтримці: фаєрволи WatchGuard вимагають регулярного оновлення програмного забезпечення, баз даних загроз та виконання інших процедур підтримки. Це може займати багато часу та ресурсів.

Нижче проведемо коротке порівняння фаєрволів Fortinet і WatchGuard.

Fortinet і WatchGuard – це найпопулярніші мережеві брандмауери, що використовуються сьогодні. Вони забезпечують неперевершену ефективність безпеки на основі штучного інтелекту, аналіз загроз, повну видимість і захищену мережеву конвергенцію.

Fortinet – найкраще використовувати для компаній, які шукають багаторівневу вдосконалену безпеку зі зниженою складністю.

Watchguard – найкраще використовувати для компаній, які шукають економічно ефективні рішення для брандмауера.

Нижче (табл.2.2) порівняно декілька аспектів цих двох фаєрволів.

Таблиця 2.2 - Порівняльна характеристика фаєрволів Watchguard і Fortinet

	Watchguard	Fortinet
Найкращі основні функції	Зручна панель керування трафіком, захист від зловмисного програмного забезпечення на основі штучного інтелекту та покращена видимість мережі	Інноваційна технологія механізму безпеки, неявна функція проксі, централізована консоль автоматизованого керування
Зручності використання	Просте налаштування завдяки потужному клієнтському інтерфейсу	Початкове налаштування без зусиль
Найкраще для точності, надійності та масштабованості	Конфігурація мережі для кількох клієнтів, працює з мінімальним наглядом	Моніторинг інформації в режимі реального часу та однакові, відповідні, скоординовані відповіді на загрози в мережах
Підтримка	Необмежена підтримка 24 години на добу 7 днів на тиждень з підтримкою дзвінків у режимі реального часу	Цілеспрямована глобальна підтримка 24 години на добу 7 днів на тиждень
Прайсинг	Стартує від $100-$200/рік	Стартує від $250/рік

2.3 Проектування системи захисту інформації за допомогою фаєрволу Watchguard

Система захисту інформації може включати в себе апаратні мережеві пристрої для забезпечення безпечного обігу інформації в мережі. Аналітики IDC ввели термін Unified Threat Management (UTM). UTM — це клас універсальних мережевих пристроїв, які виконують три основні завдання: фільтрацію мережевого трафіку, захист від вірусів, а також виявлення та запобігання атакам. По суті, ці комплекси в одній будівлі захищають весь корпоративний периметр - дуже цікаві і складні машини. Досить сказати, що вони повинні працювати на всіх рівнях моделі OSI, аж до прикладного рівня (UTM може аналізувати

протоколи на прикладному рівні), що вимагає досить серйозних обчислювальних ресурсів і складної мікропрограми. Вартість такого «комбайна» значно нижча за вартість рішення, складеного з окремих компонентів, і UTM затребуваний малими та середніми компаніями.

Для зазначених цілей варто розглянути WatchGuard XTM 505 – наймолодшу модель в лінійці пристроїв серії XTM 5, призначену для комплексного захисту мереж малого та середнього бізнесу. Функціональність пристрою включає брандмауер, антивірус, контроль додатків, веб-фільтрацію, а також запобігання вторгненням, захист від спаму та комплексну систему захисту від загроз на основі репутації ресурсу. WatchGuard XTM 505 призначений для підприємств з локальною мережею до 300 активних користувачів одночасно (старіші моделі лінійки підходять для дата-центрів і великих компаній, де працюють до 1500 осіб) і забезпечує пропускну здатність екрану мережі до 1,5 Гбіт / с, а також VPN - до 210 Мбіт/с

WatchGuard XTM 505 (як і інші пристрої п'ятої серії) виконано в корпусі, пристосованому для монтажування в шафу типу стойки 1U. Пристрої відрізняє впізнаваний фірмовий дизайн і яскраво-червона (майже помаранчева) колірна гамма. Усі інтерфейси (Ethernet 10/100 Мбіт/с, Ethernet 10/100/1000 Мбіт/с, 2 порти USB і послідовний порт) знаходяться на панелі спереду девайсу. Також є невеликий рідкокристалічний екран і кнопки керування. Задню панель творці оснастили роз'ємом живлення (один блок живлення), сітки декількох вентиляторів охолодження, які не мають можливості гарячої заміни і вимикач.

Типова конфігурація для цього класу пристроїв однакова для всіх моделей лінійки. Вимоги до живлення та споживання електроенергії також стандартні: 100-240 В і 50-171 Вт (мінімум і максимум). Важлива відмінність: кожну модель клієнт може оновити за допомогою програмного ключа до старішої моделі в лінійці, надаючи можливість масштабування рішення без дорогої заміни обладнання.

Пристрої серії WatchGuard XTM 5 забезпечують пропускну здатність мережі до 2,6 Гбіт/с (1,5 Гбіт/с на моделі XTM 505) з пропускною здатністю VPN до 750 Мбіт/с (XTM 505 - 210 Мбіт/с), а також можливість аналізувати HTTPS, SIP і H .323. Аналіз контенту на рівні додатків дозволяє ідентифікувати та блокувати загрози, які не можуть бути виявлені брандмауером із пам'яттю стану пакетів. За допомогою фільтрів для протоколів HTTP/HTTPS, TCP/UDP, DNS, POP3, FTP забезпечується широкий захист мережі.

Також варто відзначити наявність вбудованого SSL VPN. Адміністрування пристрою здійснюється з підтримкою скриптів за допомогою інтерфейсу командного рядка, веб-інтерфейсу та спеціального додатку для персональних комп'ютерів.

Пристрої WatchGuard XTM Series 5 постачаються з ОС Fireware XTM, яка оновляється ліцензійних ключем до Fireware XTM Professional. Розширену версію системи відрізняє підтримка великої кількості одночасних SSL тунелів клієнт-сервер (у простій версії доступний один тунель), можливість розподілу навантаження між серверами та між кількома WAN-каналами. Забезпечує можливість створення відмовостійкого кластера шляхом об'єднання пристроїв «Активний/Активний» або «Активний/Пасивний». До того ж, Fireware XTM Professional має ширшу підтримку протоколів маршрутизації - до статичної та RIP-маршрутизації також додано динамічну маршрутизацію (BGP4, OSPF, RIP v1/2), а також можливості маршрутизації на основі політики (Policy Base Routing).

У короткому огляді важко розповісти про всі можливості XTM 505. Більше немає інтерактивного моніторингу та звітності в режимі реального часу, рольового контролю доступу (RBAC), внутрішнього зв'язку VPN із функцією перетягування, безпеки VoIP та різних типів VPN для гнучкості віддаленого доступу, режиму прозорого мосту, трансляції каналів VPN і не тільки .

Детальні технічні характеристики XTM 505:

- пропускна здатність екрану мережі - до 1,5 Гбіт/с;
- пропускна здатність VPN - до 210 Мбіт/с;
- сумарна пропускна здатність XTM - до 330 Мбіт/с;
- один інтерфейс Ethernet - 10/100 Мбіт/с;
- 6 інтерфейсів Ethernet - 10/100/1000 Мбіт/с;
- інтерфейси введення/виведення - 1 послідовний і 2 USB;
- кількість підтримуваних вузлів (LAN IP) не обмежена;
- 40 000 одночасних двосторонніх (двосторонніх) сеансів;
- 75 VLAN (мости, тегування, режим маршрутизації);
- до 500 аутентифікованих локальних облікових записів в базі користувачів;
- до 65 VPN-тунелів у відділеннях;
- 5/75 Mobile VPN IPSec тунелів (базова доставка / максимум);
- 1/65 SSL Mobile VPN тунелі;
- екран мережі: перевірка пакетів із зазначенням стану, глибока перевірка пакетів, брандмауер проксі;
- проксі-сервер прикладного рівня: HTTP, HTTPS, SMTP, FTP, DNS, TCP/UDP, POP3;
- захист від загроз: блокування шпигунського ПЗ, DoS/DDoS-атаки, фрагментовані пакети, неправильно сформовані пакети, змішані загрози та багато іншого;
- VoIP: H.323, фільтри проксі SIP;
- підписки безпеки: Application Control, Intrusion Prevention Service, spamBlocker, Gateway AntiVirus, WebBlocker, RED;
- IPSec: спільний ключ IKE, сертифікат третьої сторони, SHA-1, MD5,;
- VPN відмова;
- SSL: тонкий клієнт, інтернет-обмін;
- PPTP: сервер і переадресація;

- єдиний вхід: Прозора автентифікація Active Directory;
- зовнішня аутентифікація: Windows Active Directory, RADIUS;
- інші типи аутентифікації: SecurID, VASCO, локальна;
- 4 включені ліцензії WSM;
- сповіщення: SNMP v2/v3, електронна пошта, оповіщення системи управління;
- підтримка серверів: журналювання та звітування про стан справності сервера, карантин, WebBlocker, управління;
- веб-інтерфейс: підтримка ОС Linux, MAC, Windows і Solaris;
- командний рядок: прямий доступ і підтримка сценаріїв;
- призначення IP-адрес: DynDNS, Static, DHCP , PPPoE (сервер, клієнт, реле);
- охорона праці: НРТЛ/С, КБ;
- вміст небезпечних речовин: REACH, WEEE, RoHS.

Поставка машин серії виконується за схемою «на вимогу» – оновлення пристрою до старшої моделі лінійки здійснюється за допомогою ліцензійного ключа (точна специфікація кожної моделі доступна на сайті виробника).

Такий підхід дозволяє ефективно збільшити продуктивність UTM і пропускну здатність каналу, необхідні для цього, без необхідності витрачати кошти на заміну дороговартісного обладнання. Масштабування Watchguard є його одним з переваг – XTM 5 добре працює з пристроями серії XCS. Таким чином рівень безпеки контенту та електронної комунікації значно підвищується.

Отже, для побудови системи захисту інформації доцільно більш детально дослідити ефективність мережевих пристроїв типу WatchGuard для визначення потрібної моделі та достатності її для задач, які стоять перед системою на конкретному підприємстві.

РОЗДІЛ 3 ПРАКТИЧНА ЧАСТИНА

3.1 Аналіз структури логів

За допомогою таких інструментів як Logstash, логи отримуються, обробляються і «сирими» відправляються у візуалізатор Kibana, де вони структуруються в поля, які є легшими для розуміння аналітику. Розділення логів на окремі поля зазвичай відбувається шляхом використання логувальних бібліотек або інструментів, які підтримують структурований формат логів. Багато мов програмування мають спеціальні бібліотеки для логування, які дозволяють створювати структуровані логи. Ці бібліотеки часто надають методи або функції для реєстрації рівня журналювання, встановлення часової мітки, вказівки на компонент або модуль, додавання повідомлення та контекстних даних. Бібліотеки можуть автоматично форматувати логи у вигляді структурованих полів або використовувати певний формат, такий як JSON. Деякі системи логування дозволяють використовувати спеціальні формати логів, такі як JSON або XML. У таких форматах кожен елемент логу може бути представлений як поле з відповідним значенням. Логувальний інструмент чи бібліотека може відповідно форматувати логи у вигляді структурованого формату. Розробники можуть створити свою власну логіку для розділення логів на окремі поля. Це може бути реалізовано шляхом створення власних об'єктів або структур даних, які містять різні поля для рівня журналювання, часової мітки, повідомлення та інших контекстних даних. Логувальний код може заповнювати ці поля і формувати логи з використанням створеної структури.

Деякі загальні поля, які можуть бути використані для структурування логів, включають:

- Timestamp (рис.3.1) – включення точного часу, для встановлення послідовності подій та аналізу часової залежності.

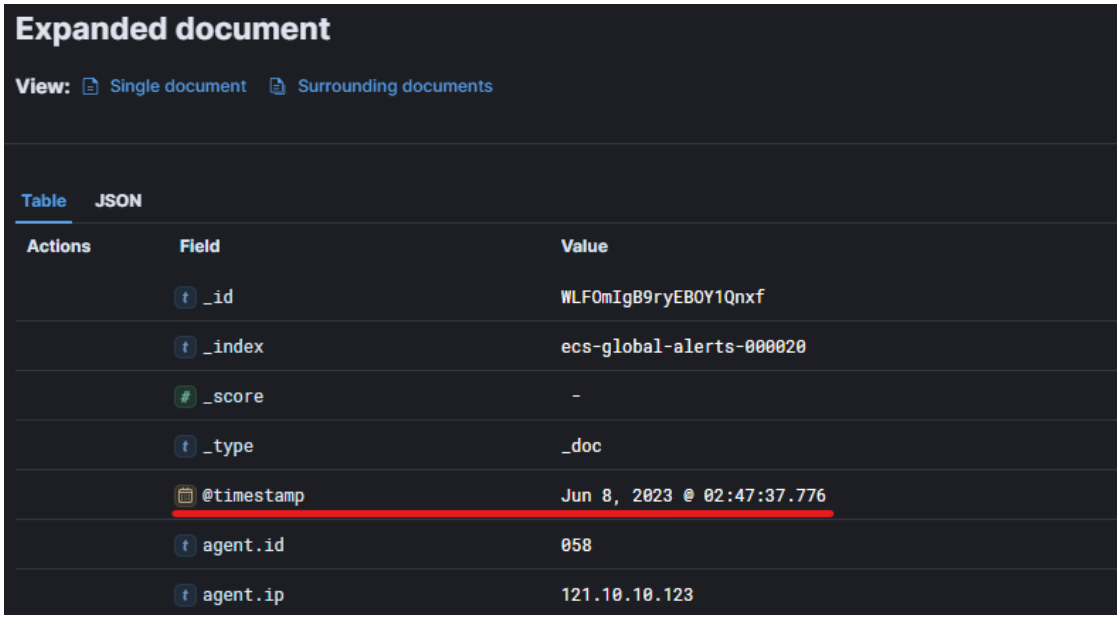


Рисунок 3.1 – Лог з візуалізацією Timestamp

- Log Level (рис.3.2) – вказує на важливість або серйозність події. Це може бути поле, яке містить значення, такі як "DEBUG", "INFO", "WARNING", "ERROR" тощо.

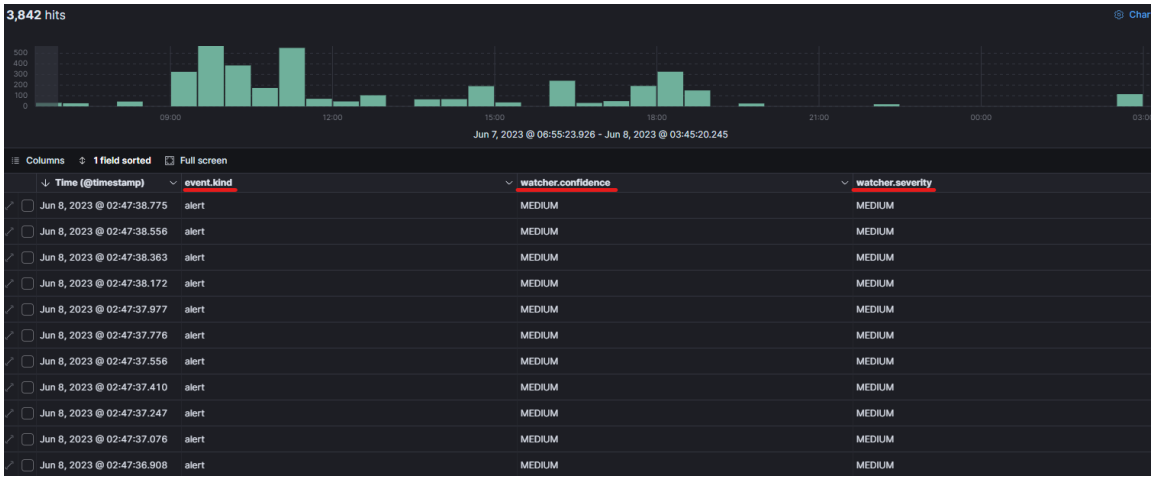


Рисунок 3.2 – Поля, які відносяться до Log Level

- Module (рис.3.3) – вказує на конкретний компонент або модуль системи, який створив лог. Це поле може допомогти в ідентифікації джерела проблеми або відстеженні пов'язаних подій.

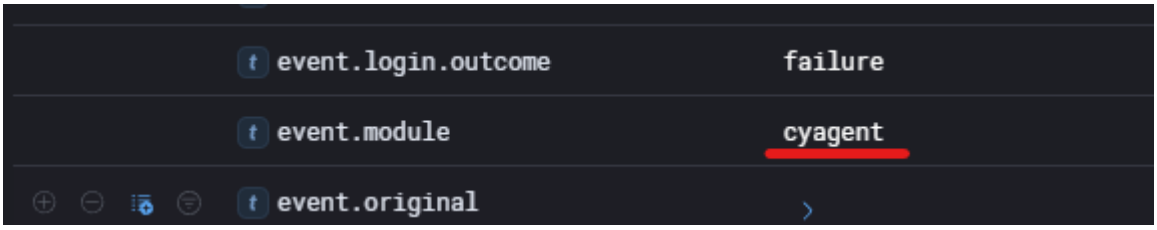


Рисунок 3.3 – поле, яке вказує на модуль системи

- Message (рис.3.4) – це той самий «сирий» лог без структуризації, який буває корисним в окремих випадках.

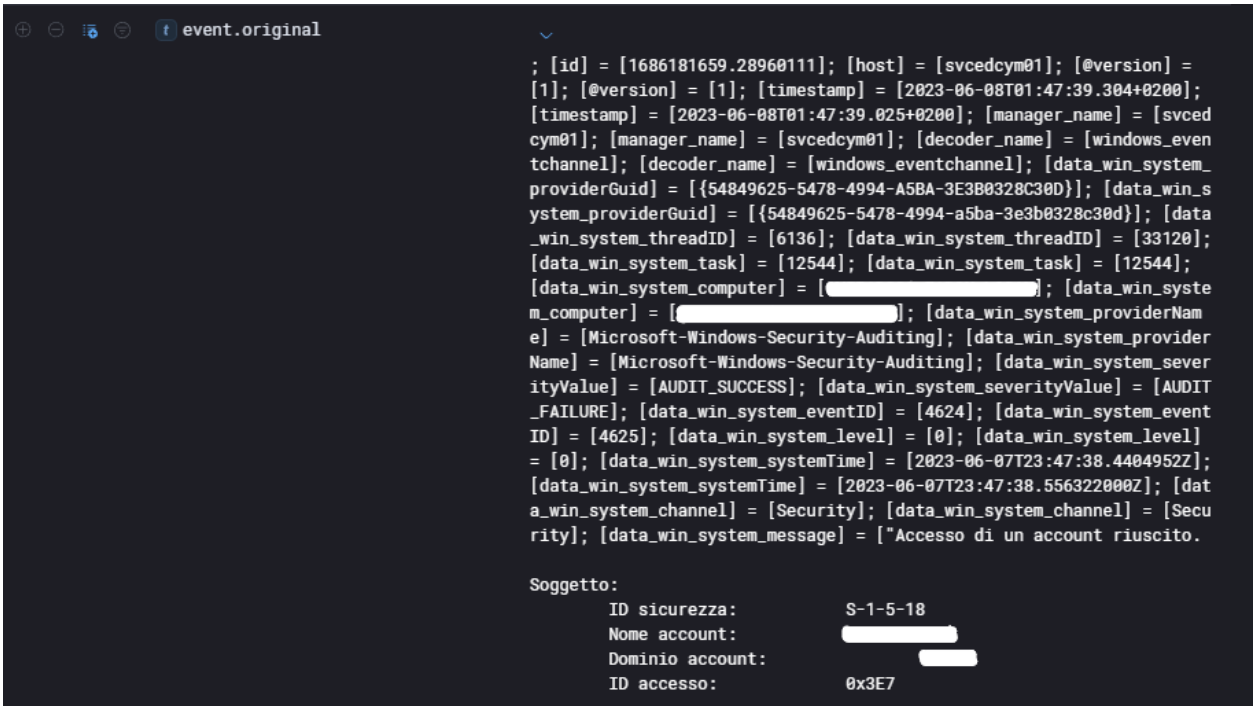
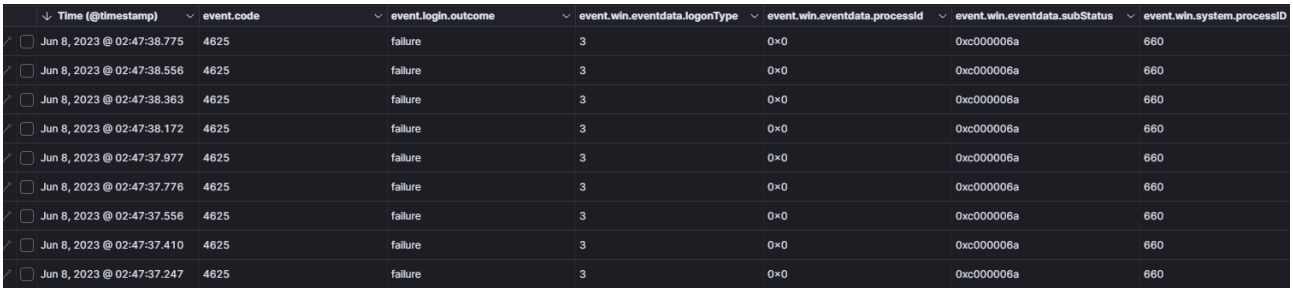


Рисунок 3.4 – Оригінальний необроблений лог

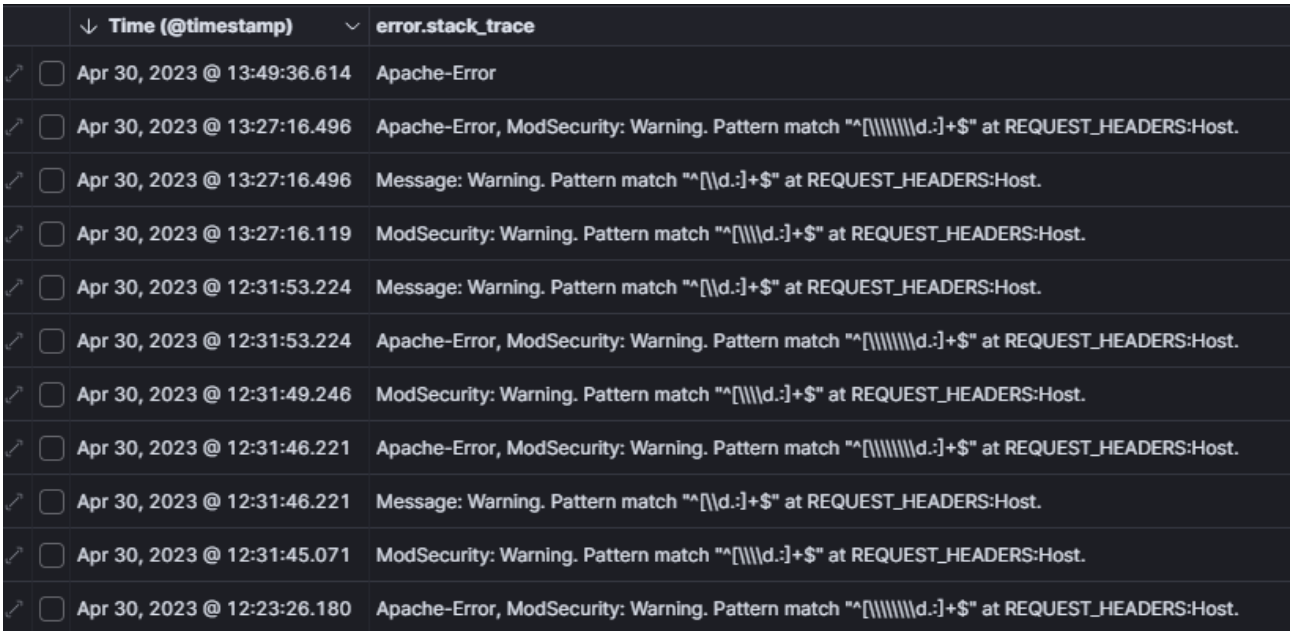
- Contextual Data (рис.3.5) – додаткові параметри, дані або властивості, які можуть бути корисними для розуміння контексту події. Наприклад, це можуть бути ідентифікатори, вхідні параметри, статуси, коди помилок тощо.



Time (@timestamp)	event.code	event.login.outcome	event.win.eventdata.logonType	event.win.eventdata.processId	event.win.eventdata.subStatus	event.win.system.processID
Jun 8, 2023 @ 02:47:38.775	4625	failure	3	0×0	0xc000006a	660
Jun 8, 2023 @ 02:47:38.556	4625	failure	3	0×0	0xc000006a	660
Jun 8, 2023 @ 02:47:38.363	4625	failure	3	0×0	0xc000006a	660
Jun 8, 2023 @ 02:47:38.172	4625	failure	3	0×0	0xc000006a	660
Jun 8, 2023 @ 02:47:37.977	4625	failure	3	0×0	0xc000006a	660
Jun 8, 2023 @ 02:47:37.776	4625	failure	3	0×0	0xc000006a	660
Jun 8, 2023 @ 02:47:37.556	4625	failure	3	0×0	0xc000006a	660
Jun 8, 2023 @ 02:47:37.410	4625	failure	3	0×0	0xc000006a	660
Jun 8, 2023 @ 02:47:37.247	4625	failure	3	0×0	0xc000006a	660

Рисунок 3.5 – Контекстні дані

- Stack Trace (рис.3.6) – якщо лог пов'язаний з помилкою або виключенням, то включення стеку викликів може допомогти виявити місце, де сталася помилка та послідовність функцій, що привела до неї.



Time (@timestamp)	error.stack_trace
Apr 30, 2023 @ 13:49:36.614	Apache-Error
Apr 30, 2023 @ 13:27:16.496	Apache-Error, ModSecurity: Warning. Pattern match "^[\\\\\\\\d.:]+$" at REQUEST_HEADERS:Host.
Apr 30, 2023 @ 13:27:16.496	Message: Warning. Pattern match "^[\\d.:]+$" at REQUEST_HEADERS:Host.
Apr 30, 2023 @ 13:27:16.119	ModSecurity: Warning. Pattern match "^[\\\\d.:]+$" at REQUEST_HEADERS:Host.
Apr 30, 2023 @ 12:31:53.224	Message: Warning. Pattern match "^[\\d.:]+$" at REQUEST_HEADERS:Host.
Apr 30, 2023 @ 12:31:53.224	Apache-Error, ModSecurity: Warning. Pattern match "^[\\\\\\\\d.:]+$" at REQUEST_HEADERS:Host.
Apr 30, 2023 @ 12:31:49.246	ModSecurity: Warning. Pattern match "^[\\\\d.:]+$" at REQUEST_HEADERS:Host.
Apr 30, 2023 @ 12:31:46.221	Apache-Error, ModSecurity: Warning. Pattern match "^[\\\\\\\\d.:]+$" at REQUEST_HEADERS:Host.
Apr 30, 2023 @ 12:31:46.221	Message: Warning. Pattern match "^[\\d.:]+$" at REQUEST_HEADERS:Host.
Apr 30, 2023 @ 12:31:45.071	ModSecurity: Warning. Pattern match "^[\\\\d.:]+$" at REQUEST_HEADERS:Host.
Apr 30, 2023 @ 12:23:26.180	Apache-Error, ModSecurity: Warning. Pattern match "^[\\\\\\\\d.:]+$" at REQUEST_HEADERS:Host.

Рисунок 3.6 – Stack Trace логи

У цьому розділі було розглянуто процес структурування логів за допомогою інструментів, таких як Logstash, і їх подальша візуалізація у Kibana. Структуровані логи полегшують аналіз та моніторинг системи, оскільки їх можна легко фільтрувати, пошуково аналізувати та візуалізувати за допомогою інструментів, таких як Kibana. Це допомагає розробникам швидко знаходити проблеми, виявляти залежності та здійснювати відповідні кроки для покращення системи.

3.2 Аналіз інцидентів і логів фаєрволу Watchguard

TOR Connections – це сигналізація (рис.3.7), яка надсилається у випадку підключень, створених через мережу TOR. Це досягається шляхом шифрування та маршрутизації інтернет-трафіку через серію серверів. Це зазвичай означає, що фаєрвол виявив або позначив мережевий трафік, що надходить із мережі TOR або призначений для неї. Цей тривога може спрацьовувати в певних ситуаціях, коли використання TOR вважається підозрілим або потенційно ризикованим. У деяких організаціях або мережевих середовищах наявність з'єднань TOR може суперечити політикам або правилам безпеки. Таким чином, сигнали тривоги, пов'язані з підключеннями TOR, можуть означати потенційні ризики безпеці, вимагаючи подальшого розслідування, щоб визначити характер і наміри трафіку TOR.

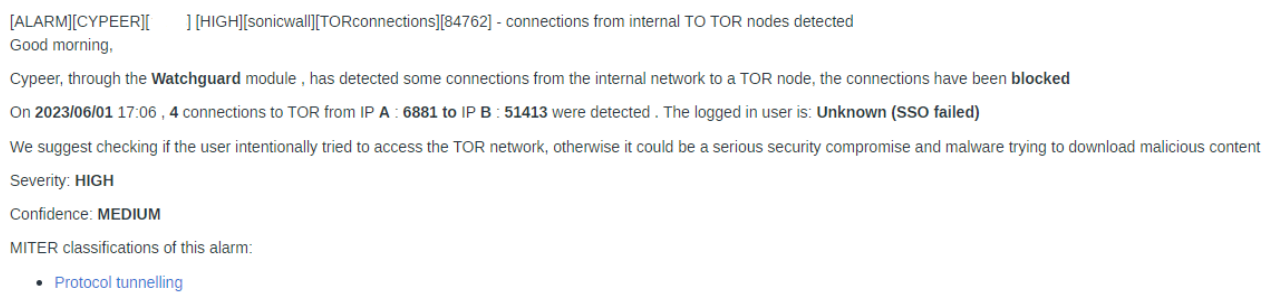
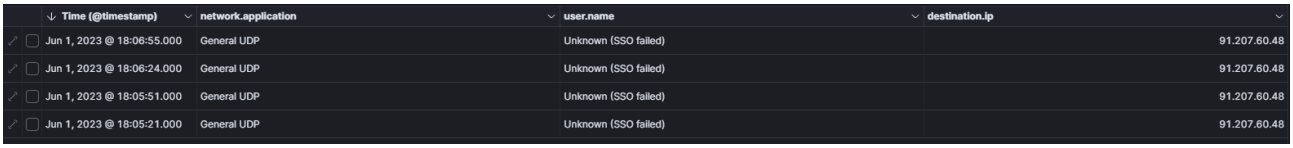

[ALARM][CYPEER][ ] [HIGH][sonicwall][TORconnections][84762] - connections from internal TO TOR nodes detected
Good morning,
Cypeer, through the **Watchguard** module , has detected some connections from the internal network to a TOR node, the connections have been **blocked**
On **2023/06/01** 17:06 , **4** connections to TOR from IP **A** : **6881 to** IP **B** : **51413** were detected . The logged in user is: **Unknown (SSO failed)**
We suggest checking if the user intentionally tried to access the TOR network, otherwise it could be a serious security compromise and malware trying to download malicious content
Severity: **HIGH**
Confidence: **MEDIUM**
MITER classifications of this alarm:
- Protocol tunnelling

Рисунок 3.7 – згенерована фаєрволом сигналізація TOR Connections

Ця сигналізація дає нам знати, що фаєрвол watchguard виявив 4 підключення до мережі TOR з IP-адреси A до IP-адреси B і заблокував його. Користувача, який входив визначає як Unknown (SSO failed).

Після ретельного аналізу (рис.3.8) було виявлено, що поле network.application, яке посилається на назву програми, пов'язану з підключенням, дорівнює "General UDP". Це зазвичай вказує на те, що підключення використовує UDP, який є протоколом без встановлення з'єднання,

який зазвичай використовується для програм реального часу, таких як потокове медіа, онлайн-ігри та VoIP.



Time (@timestamp)	network.application	user.name	destination.ip
Jun 1, 2023 @ 18:06:55.000	General UDP	Unknown (SSO failed)	91.207.60.48
Jun 1, 2023 @ 18:06:24.000	General UDP	Unknown (SSO failed)	91.207.60.48
Jun 1, 2023 @ 18:05:51.000	General UDP	Unknown (SSO failed)	91.207.60.48
Jun 1, 2023 @ 18:05:21.000	General UDP	Unknown (SSO failed)	91.207.60.48

Рисунок 3.8 – Логи інциденту з виставленими фільтрами

Також варто зазначити, що поле user.name = “Unknown (SSO failed)”. Це вказує на те, що користувач, пов’язаний із підключенням, невідомий через невдалу автентифікацію за системою єдиного входу (Single Sign-On). SSO — це механізм, який дозволяє користувачам пройти автентифікацію один раз і отримати доступ до кількох систем без необхідності повторної автентифікації. У цьому випадку процес єдиного входу не вдався, в результаті чого користувача було ідентифіковано як «Невідомий».

Врешті-решт, було звернуто увагу на destination.ip. Це один з найважливіших факторів виявлення неправомірної діяльності не тільки для TOR Connections. Провівши детальніший аналіз IP-адреси, було виявлено, що вона дійсно відноситься до IP-адрес TOR exit node. Тим паче, 8485 користувачів повідомили про неї, як про шкідливу і що вона використовувалась для різних категорій атак. (рис.3.9)

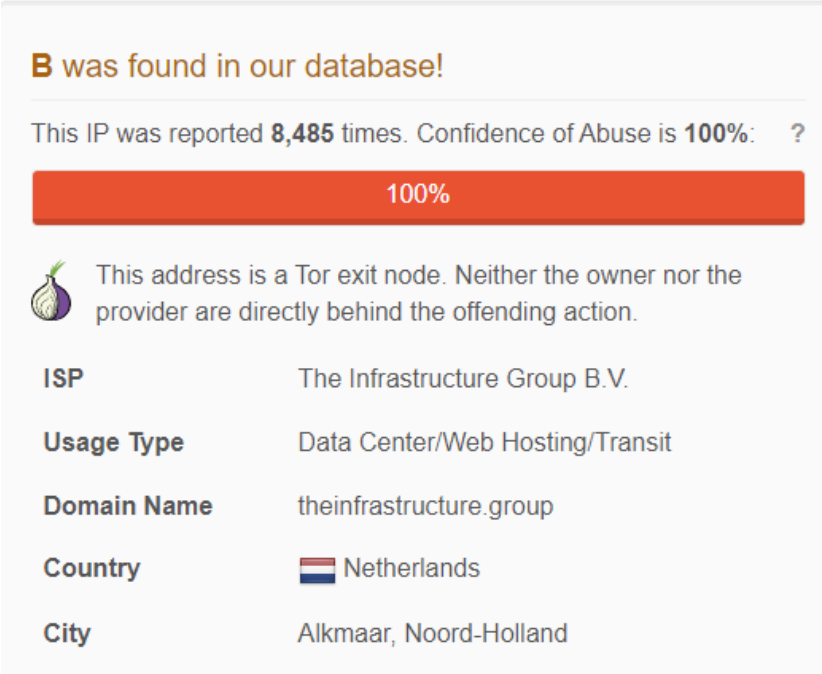
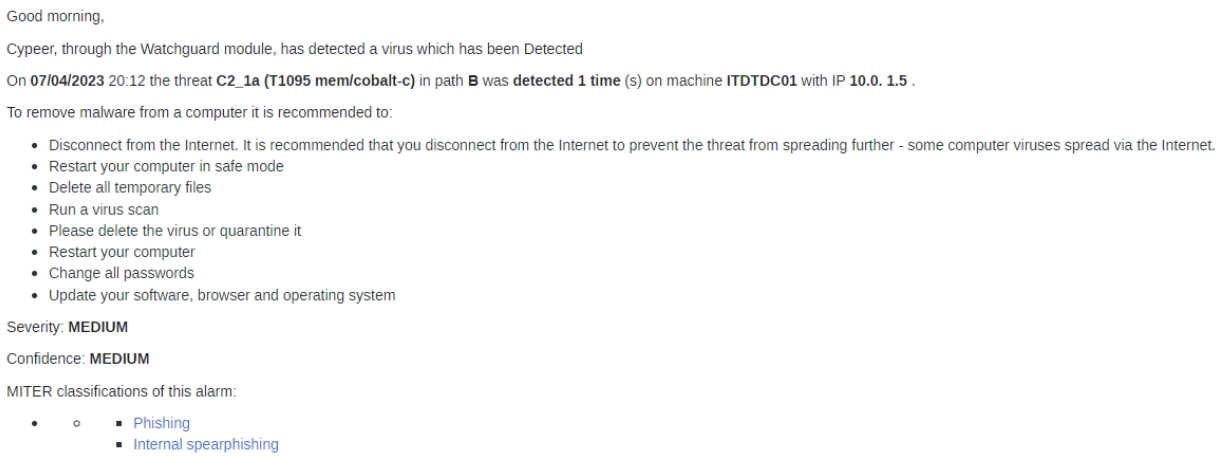


Рисунок 3.9 – Репутація IP-адреси B

Таким чином, поєднавши всі фактори разом, до рекомендації було надано блокування цієї IP-адреси у фаєрволі, щоб уникнути пагубних наслідків.

Host Malware – аларм який означає, що на хост-системі (комп'ютері або сервері) виявлено або підозрюється наявність шкідливого програмного забезпечення. Цей аларм вказує на те, що система може бути компрометована або інфікована шкідливим кодом. Аларм "Host Malware" (рис.3.10) може відображатися в результаті виявлення таких шкідливих програм, як віруси, троянські програми, рекламне програмне забезпечення (adware), черв'яки, шпигунське програмне забезпечення (spyware) або інші види зловмисного коду. Такі програми можуть бути приховані на хост-системі і виконувати дії, що можуть бути шкідливими для пристрою, даних користувачів або мережі.



Good morning,

Cypeer, through the Watchguard module, has detected a virus which has been Detected

On **07/04/2023** 20:12 the threat **C2_1a (T1095 mem/cobalt-c)** in path **B** was **detected 1 time** (s) on machine **ITDTDC01** with IP **10.0. 1.5** .

To remove malware from a computer it is recommended to:

- Disconnect from the Internet. It is recommended that you disconnect from the Internet to prevent the threat from spreading further - some computer viruses spread via the Internet.
- Restart your computer in safe mode
- Delete all temporary files
- Run a virus scan
- Please delete the virus or quarantine it
- Restart your computer
- Change all passwords
- Update your software, browser and operating system

Severity: **MEDIUM**

Confidence: **MEDIUM**

MITER classifications of this alarm:

- Phishing
- Internal spearphishing

Рисунок 3.10 – Згенерована фаєрволом сигналізація Host Malware

Ця сигналізація повідомляє про те, що фаєрвол виявив потенційний вірус на хості ITDTDC01 за шляхом B. Назва загрози, яку виявив брандмауер - C2_1a (T1095 mem/cobalt-c).

Проаналізувавши, було зазначено, що C2_1a (T1095 mem/cobalt-c) – це ім’я, яке ідентифікує певний тип зловмисного програмного забезпечення, зловмисної програми, призначеної для проникнення в комп’ютери та спричинення пошкоджень або викрадення інформації. Зокрема, C2_1a — це троян, тип зловмисного програмного забезпечення, яке виглядає як законне або нешкідливе програмне забезпечення, але насправді має приховані функції, які можуть завдати шкоди системі або викрасти інформацію. Також, подіями користувача, який відноситься до цього хоста є Creds_4h (T1003.002). Це термін, який визначає певний тип кібератаки, відомий як «скид облікових даних». Ця атака полягає у відновленні облікових даних (ім’я користувача та пароля) для доступу до операційної системи або програми, як правило, шляхом використання вразливості або діри в безпеці. По суті, коли фаєрвол виявляє наявність Threat.name Creds_4h (T1003.002), це вказує на те, що були спроби здійснити дампінг облікових даних для отримання облікових даних для входу в систему та програму, і що ви повинні вжити заходів безпеки, щоб запобігти

несанкціонованому доступу до конфіденційної інформації. Для цього аналізу, потрібно було знайти лог і правильно підібрати поля (рис.3.11).

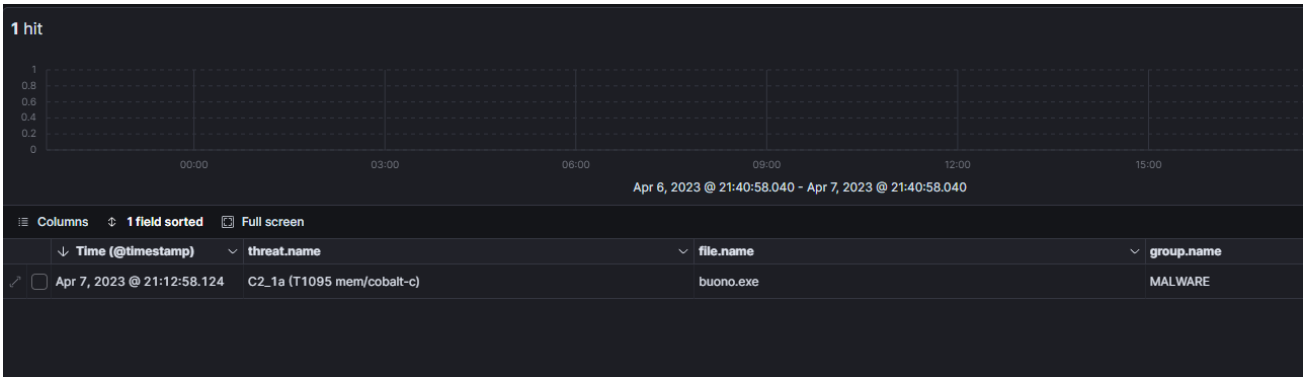


Рисунок 3.11 – Лог з відокремленими полями для інциденту Host Malware

Таким чином, в цій ситуації файл buono.exe, який було позначено як небезпечний, рекомендовано видалити й слідувати інструкціям Watchguard.

Network Exploit – це аларм, який означає виявлення або підозру на використання експлойта в мережі. Експлойт - це зловмисний код або техніка, що використовується зловмисниками для вразливостей або слабких місць у мережевих протоколах, програмах або операційних системах. Аларм "Network Exploit" повідомляє про можливу атаку на систему або мережу, коли використовуються експлойти для отримання несанкціонованого доступу, виконання коду або використання інших зловмисних дій. Цей аларм може спрацьовувати, коли виявляються підозрілі мережеві активності, що вказують на можливе використання експлойтів, наприклад: спроби вразити відомі вразливості, аномальний мережевий трафік, відправка зловмисних пакетів.

Good morning,

Through the Watchguard module, Cypeer has detected software, data or a set of commands that exploit a bug or vulnerability to cause unexpected or unpredictable behavior on computer software or hardware. it was **allowed** by the firewall

On **09/03/2023** 16:47 **Traceroute** threat was **allowed 2 times** from source IP address **192.168.150.102 to** destination IP address **13.107.22.200**

On **09/03/2023** 16:47 **Traceroute** threat was **allowed 2 times** from source IP address **192.168.150.92 to** destination IP address **93.184.221.240**

On **09/03/2023** 16:42 **Traceroute** threat was **allowed 2 times** from source IP address **192.168.150.106 to** destination IP address **93.184.221.240**

On **09/03/2023** 16:41 **Traceroute** threat was **allowed 2 times** from source IP address **192.168.150.96** to destination IP **address 13.107.21.200**

On **09/03/2023** 16:37 the threat **TCP.Overlapping.Fragments** was **allowed 1 times** from source IP address **192.168.150.103 to** destination IP address **52.109.88.85**

On **09/03/2023** 16:40 **Traceroute** threat was **allowed 2 times** from source IP address **192.168.150.93** to destination IP **address 93.184.221.240**

On **09/03/2023** 16:42 **Traceroute** threat was **allowed 2 times** from source IP address **192.168.150.95 to** destination IP address **209.197.3.8**

Severity: **MEDIUM**

Confidence: **MEDIUM**

MITER classifications of this alarm:

- Phishing
- Internal spearphishing

Рисунок 3.12 - Згенерована фаєрволом сигналізація Network Exploit

Ця сигналізація вказує на виявлення подібності до атаки трасування маршруту. Атака трасування маршруту є одним з методів виявлення інформації про мережу та її інфраструктуру. У цьому випадку, атака трасування маршруту була спробою відправити ICMP пакети типу PING від джерела з IP-адресою 192.168.150.93 до призначення з різними IP-адресами. Після перевірки IP-адрес виявлено, що усі з них повідомлялись про неправомірну діяльність (рис.3.13).

13.107.22.200 was found in our database!

This IP was reported **21** times. Confidence of Abuse is **0%**: ?

0%

ISP	Microsoft Corporation
Usage Type	Data Center/Web Hosting/Transit
Domain Name	microsoft.com
Country	United Kingdom of Great Britain and Northern Ireland
City	London, England

Рисунок 3.13 – Репутація одної з IP-адрес

У цьому випадку, було рекомендовано встановити правило блокування трафіку такого типу безпосередньо у фаєрволі Watchguard та оновити систему IPS.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Охорона праці на підприємстві. Освітлення, мікроклімат.

Відповідно до ст. 3 Конституції України і Закону «Про охорону праці» основним принципом державної політики є пріоритет життя і здоров'я робітників відносно будь-яких результатів виробничої діяльності, а державна політика в галузі охорони безпосередньо спрямована на створення належних, безпечних і здорових умов праці, запобігання нещасним випадкам та професійним захворюванням.

Виходячи із загальних завдань охорони праці, мета розділу полягає у розробці ефективних заходів покращання умов праці комп'ютерного відділу компанії на основі аналізу шкідливих та небезпечних виробничих факторів, що мають місце при виконанні робочих обов'язків.

Очікуваними результатами роботи є створення оптимальних умов праці для організації ефективної роботи комп'ютерного відділу.

Об'єктом дослідження в цьому розділі є умови праці в комп'ютерному відділі, який відповідає за захист інформації в комп'ютерних мережах.

Предметом дослідження – є формування системи охорони праці на підприємстві.

Діяльність підприємства повинна відбуватися в межах чинного законодавства України. Складовою частиною управління підприємством є система управління охороною праці.

Управління охороною праці – це підготовка, прийняття та реалізація рішень по здійсненню організаційних, технічних, санітарно-гігієнічних та лікувально-профілактичних заходів, спрямованих на забезпечення безпеки, збереження здоров'я та працездатності людини у процесі праці.

Проведений аналіз дозволить визначити ті основні законодавчі та нормативно-правові документи, що мають регулювати управління охороною праці на підприємстві; визначити права, обов’язки та відповідальність керівника за додержання законодавства про охорону праці.

Нормативні акти про охорону праці на підприємстві – це правила стандарти, норми, положення, інструкції, та інші документи, яким надано чинність правових норм обов’язкових для виконання. Особливістю законодавства України про охорону праці є регулювання значної частини питань з охорони праці документами, прийнятими на підприємстві. Нормативно-законодавча база з охорони праці складається з документів, які діляться на 4 типи: документи зовнішнього походження, галузеві документи й стандарти, внутрішні документи підприємства (накази, розпорядження, положення), інші документи (інструкції, журнали інструктажів). До першого типу відносяться такі документи як: Кодекс законів про працю України, Закон України «Про охорону праці», Закон України «Про загальнообов'язкове державне соціальне страхування» тощо. До галузевих документів й стандартів відносяться: НПАОП 0.00-4.15-98 «Положення про розробку інструкцій з охорони праці», ДБН В.2.5-28:2018 «Природне і штучне освітлення», ДСН 3.3.6.037-99 Санітарні норми виробничого шуму, ультразвуку та інфразвуку. До третього типу (внутрішні документи) відносяться: Положення про систему управління охороною праці на даному підприємстві, Положення про організацію первинного і періодичних медичних оглядів працівників певних категорій. До інших документів можна віднести: Інструкції з охорони праці для керівника департаменту, керівника відділення; Інструкція з охорони праці для бухгалтера, касира; Журнал реєстрації інструктажів з техніки безпеки.

Нормативно-правова документація з охорони праці на підприємстві має чотири рівні:

- закони України, що регулюють питання, пов’язані з охороною праці;

- галузеві нормативи та стандарти;
- накази та розпорядження керівника підприємства;
- інструкції з охорони праці та техніки безпеки.

Мікроклімат виробничих приміщень – це умови внутрішнього середовища у виробничому приміщенні, що впливають на тепловий обмін працюючих з середовищем шляхом конвекції, кондукції, теплового випромінювання та випаровування вологи і діють на людину в процесі праці на його робочому місці, у робочій зоні.

Параметри мікроклімату: 1) температура повітря T, oC; 2) відносна вологість Y, %; 3) швидкість руху повітря V, м/с; 4) інтенсивність теплового(інфрачервоного) опромінення; 5) температура поверхонь устаткування.

Основним нормативним документом, що регламентує параметри мікроклімату виробничих приміщень є ДСН 3.3.6.042-99. Ці параметри нормуються для робочої зони − визначеного простору, в якому знаходяться робочі місця постійного або непостійного (тимчасового) перебування працівників.

Температуру вимірюють ртутними чи спиртовими термометрами. У приміщеннях зі значними тепловими випромінюваннями використовують парний термометр, що складається з двох термометрів (із зачорненим та посрібленим резервуаром). Для неперервної реєстрації температури навколишнього повітряного середовища застосовують самозаписувальні прилади − термографи. Температуру повітря вимірюють у кількох точках робочої зони, як правило, на рівні 1,3-1,5 м від підлоги в різний час. На тих робочих місцях, де температура повітря біля підлоги помітно відрізняється від температури повітря верхньої зони приміщення, вона вимірюється й на рівні ніг (0,2-0,3 м від підлоги). Відносна вологість повітря (відношення фактичного вмісту маси водяних парів, що містяться в даний час в $м^3$ повітря, до максимально можливого їх вмісту при даній температурі) визначається психрометром Августа,

аспіраційним психрометром, гігрометром та гігрографом. Для вимірювання швидкості руху повітря використовують крильчасті (0,3-0,5 м/с) та чашкові (1-20 м/с) анемометри, а для визначення малих швидкостей руху повітря (менше 0,5 м/с) − термоанемометри та кататермометри. Температура нагрітих поверхонь вимірюється за допомогою електротермометрів, термопар та інших контактних приладів. Для вимірювання інтенсивності теплового опромінення використовують актинометри, термостовбці, спеціальні радіометри.

Значні коливання параметрів мікроклімату можуть призвести до порушення терморегуляції організму (здатності утримувати постійну температуру), загальної слабкості та інших негативних проявів [7, с. 81].

Відповідно до обраної технології та матеріально-технічного забезпечення можуть спостерігатися такі чинники небезпек:

Таблиця 4.1 – Основні НВФ/ШВФ на робочих місцях цеху

Дільниця	Діючий небезпечний і шкідливий виробничий фактор	
	група	Вид
Комп’ютерний відділ	фізичні	підвищене значення напруги в електричному ланцюзі, підвищений рівень електромагнітного випромінювання, підвищений рівень статичної електрики
	психофізіологічні	статичні та динамічні перевантаження, перенапруження зорового аналізатора

Необхідними заходами зменшення впливу цих факторів є: інсталяція систем загально-обмінної та локальної вентиляції, запобіжників електричної мережі, нанесення акустичних покриттів; механізми дистанційного контролю і оповіщення.

Основні параметри мікроклімату наведемо в табл. 4.2-4.3

Таблиця 4.2 – Основні параметри мікроклімату

Категорія робіт	Дільниця	Температура, ^{O}C			Відносна вологість, %		Швидкість руху, м/с	
		оптимальна	допустимі границі		оптимальна	допустима на	оптимальна,	допустима
			постійне робоче місце	не постійне робоче місце		робочих місцях постійних і непостійних, не більше	не більше	на робочих місцях постійних і непостійних
		холодний період року						
Легка-Іа	Комп'ютерний відділ	22-24	21-25	18-26	40-60	75	0,1	не > 0,1
		теплий період року						
		23-25	22-28	20-30	40-60	55 (при 28^{O}C)	0,1	0,1-0,2

Таблиця 4.3 – Рівні іонізації повітря приміщень при роботі на ПК

Рівні	Кількість іонів в 1 см3 повітря	
	+п	–п
Мінімально необхідні	400	600
Оптимальні	1500 – 3000	3000 – 5000
Максимально допустимі	50000	50000

Визначимо норми і якісні показники освітлення для окремих приміщень.

Таблиця 4.4 – Норми освітлення

№ з/п	Приміщення	Системи освітлення	Норми освітлення	
			Штучне, лк	Природне (коеф.), %
1	2	3	4	5
1	Комп'ютерний відділ	Комбіноване	300	1,8

Таблиця 4.5 – Якісні показники освітлення

Виробнича дільниця, робоче місце	Площина (г-горизонтальна, в-вертикальна) нормування, висота площини над підлогою, м	Розряд та підрозряд зорових робіт	Штучне освітлення			Природне освітлення КПО, %		Тип лампи
			Освітленість робочих поверхонь, лк	Показник дискомфорту, не більше, од	Коефіцієнт пульсації освітленості, %, не більше	При верхньому чи бічному освітленні	При бічному освітленні	
Робота з ПК		IIг		40	10		—	
рукопис, клавіатура	Г-0,8		400				—	ЛБ
поверхня екрану	В-1,0		300				1,5	ЛБ

На підприємстві обладнане природне та штучне освітлення згідно з ДБН В.2.5-28:2018. Природне освітлення забезпечується через вікна в стінах, а штучне – комбіноване (загальне + місцеве). Розрахуємо штучне освітлення в приміщенні адміністратора комп'ютерного відділу. Площа приміщення А = 4,8 м, В = 2,74. Робоча поверхня, на якій нормується освітленість, – горизонтальна. Фон – середній. Розряд зорової роботи – III в. Освітлення комбіноване (загальне + місцеве). Показник освітлюваності не більше 40. Оскільки робота не пов`язана з розпізнаванням кольорів, вибираємо люмінесцентні лампи ЛБ номінальною потужністю 80 Вт, закріплені по дві штуки у світильнику.

Визначаємо віддаль $H_0 = h + h_c$ від стелі до робочої поверхні: $H_0 = h - h_p$, $h_c = 0,2H_0 = 0,2\ (H-h_p)$.

Висота світильника над робочою поверхнею

$h = H_0 - h_c = H - h_p - 0,2\ (H - h_p) = (H - h_p)$ x 0,8.

Відстань між рядами світильників $L = \alpha h$, де $\alpha = 0,9$, $H = 0,9h$.

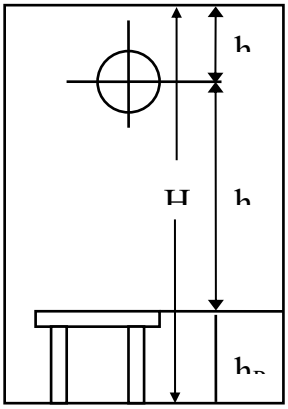


Рисунок 4.1 – Положення світильників відносно робочої зони

При люмінесцентному освітленні відомий світовий потік лампи Фл (для ЛБ80 Фл = 5220 лм), тому розраховується необхідна кількість світильників N для забезпечення нормованої освітленості Е: $N = \frac{EK_3 S_z}{n\Phi_л \eta}$,

де $К_3$ – коефіцієнт запасу;

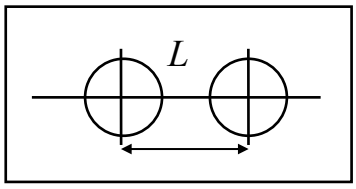
S – освітлювана площа;

z – коефіцієнт нерівномірності (z =1,1...1,2);

η – коефіцієнт використання світового потоку;

n – кількість ламп у світильнику (приймаємо 2 лампи).

Попередньо визначаємо індекс приміщення



$$i = \frac{A \cdot B}{h(A+B)} = \frac{4{,}80 \cdot 2{,}74}{0{,}8(4{,}2-0{,}8)\cdot(4{,}80+2{,}74)} = 1{,}41.$$

Висота робочого приміщення Н = 2,35 м; h_p = 0,8 м, тоді η = 45 %;

$$N = \frac{350 \cdot 1{,}3 \cdot 1{,}15 \cdot 4{,}8 \cdot 2{,}74}{2 \cdot 5220 \cdot 0{,}45} = 1{,}46 \approx 2$$

Світильники розміщуються у один ряд на відстані від стін l = 1,4 м із подальшою відстанню між світильниками 1,5 метри.

4.2 Долікарська допомога при ранах

Робота в сучасному підприємницькому середовищі неможлива без використання комп'ютерів, які є необхідними інструментами для багатьох видів діяльності. Проте, разом з безперечними перевагами комп'ютерів, існують й певні ризики, пов'язані зі здоров'ям працівників.

Однією з найпоширеніших проблем, яка може виникнути при роботі з комп'ютерами, є отримання ран. Це може бути спричинено кількома чинниками, включаючи неправильну організацію робочого місця, незручне розташування обладнання, некваліфіковане використання або обслуговування комп'ютерних пристроїв. При роботі з комп'ютерами існує ризик отримання різного типу травм. Наприклад, довготривале сидіння перед монітором може призводити до напруги м'язів спини, шиї і рук, а також сприяти розвитку синдрому карпального каналу. Використання некомфортного клавіатурного або мишкового пристрою може призвести до болю в зап'ястях і плечах. Крім того, незабезпечення належної ергономіки робочого місця може призвести до появи ран, таких як подряпини, порізи або опіки.

Говорячи про ризики отримання травм, ран на підприємстві, набагато краще зробити все для того, щоб їх попередити і максимально унеможливити допуск таких ситуацій. При роботі з комп’ютерами варто дотримуватись наступного:

- організація робочого місця: правильна організація робочого місця включає належну розстановку комп'ютерного обладнання, таку як монітор, клавіатура, мишка, щоб забезпечити комфортну позицію для працівника. Регулюйте стільці та стіл так, щоб підтримувати правильну позицію тіла;
- комфортна робоча позиція: забезпечте, щоб робоча позиція була комфортною. Налаштуйте висоту стільця та монітора, щоб уникнути надмірного

навантаження на шию, спину та очі. Використовуйте підставки для зап'ястя, щоб уникнути напруження рук та зап'ястя;

- паузи та вправи: важливо виконувати перерви та фізичні вправи для розслаблення м'язів та попередження надмірного напруження. Регулярні перерви допоможуть покращити кровообіг та запобігти м'язовому напруженню.

У випадку, якщо все ж таки сталась ситуація, що у когось появилась рана – потрібно діяти негайно. Існують декілька типів ран, тому одразу потрібно визначити тип, щоб правильно надати першу долікарську допомогу.

Поріз – це найімовірніший випадок на підприємстві. Це різкі, проникаючі рани, які зазвичай виникають внаслідок контакту з гострими предметами, наприклад ножами, склом або лезами. Порізи можуть бути поверхневими або глибокими і потребують належної обробки та захисту від інфекцій. При порізі потрібно зупинити кровотечу, притиснувши чисту стерильну серветку до моменту зупинки кровотечі. Потім, потрібно очистити рану і нанести антисептик, щоб знезаразити поріз. Врешті-решт, потрібно прикрити рану, для того, щоб запобігти потраплянню туди бруду, мікробів.

Опіки – це ушкодження шкіри, яке виникає внаслідок контакту з високою температурою, хімічними речовинами, сонцем або електричним струмом. Опіки потребують в першу чергу, якнайшвидшого охолодження місця опіка, щоб запобігти подальшому ушкодженню шкіри. Згодом, можна нанести охолоджуючий гель та накрити місце опіку.

Забої – це травма шкірного покриву без порушення його цілісності. Її можна отримати при падінні, ударах тупим предметом, дії ударної хвилі при вибухах снарядів, мін, авіабомб. При забої потрібно зробити наступне: накласти на місце травми тугу пов’язку та підняти уражену ділянку тіла; прикласти до травмованого місця щось холодне; обробити дезінфікуючим засобом місце забою, якщо на ньому є подряпини; забезпечити пошкодженій ділянці тіла спокій.

ВИСНОВКИ

Роботу присвячено питанням забезпечення кібербезпеки шляхом використання фаєрволів в системах захисту інформації. В роботі було поставлено і виконано наступні завдання:

- здійснено аналіз можливостей використання фаєрволів для захисту інформації. Ми оглянули основні різновиди фаєрволів та їх особливості в застосуванні під різні задачі захисту інформаційних мереж;

- проведено аналіз методів оцінки ефективності використання фаєрволів. Зроблено висновки, що оцінка ефективності фаєрволів відбувається за допомогою аналізу кількості відхилених загроз, а також їх співвідношення з кількістю інцидентів, наявності вразливостей, засобів додаткового захисту тощо. Тому існує потреба в більш детальному дослідженні окремих фаєрволів та можливості і доцільності їх використання для захисту інформаційної системи;

- здійснено обґрунтування вибору методики аналізу логів для оцінки ефективності роботи фаєрволів. Досліджено деякі програми роботи з лог-файлами та сутність аналізу логів для виявлення загроз та їх локалізації;

- досліджено можливості проектування системи захисту інформації за допомогою фаєрволу Watchguard. Розглянуто окремі моделі фаєрволив даної групи і визначено їх технічні характеристики та можливості по захисту мережі від несанкціонованого доступу;

- проведено тестування апаратного мережевого екрану та зроблено висновки щодо його ефективності.

Таким чином, в роботі було розглянуто наступні питання і сформовано відповідні висновки:

- визначено сутність безпеки інформації, її основні характеристики та основні складові. Безпека інформації включає в себе комплекс заходів з забезпечення збереження інформації від несанкціонованого доступу, а також

знищення чи викривлення її. Також до безпеки інформації включається поняття надання безперервного доступу легітимним користувачам, тобто якщо задекларовано доступ до серверу чи сайту 24/7, то адміністратори та власники ресурсу повинні забезпечити доступність вузлу та даних на ньому в зазначеному періоді;

- розглянуто концепцію розробки системи захисту від зовнішніх загроз в контексті безпеки інформаційних ресурсів. Дана концепція включає в себе заходи технічної, фізичної та кадрової безпеки, тобто створення комплексу заходів щодо захисту інформації від пошкодження, витоку, викривлення, знищення, утруднення доступу тощо. В залежності від рівня інформаційної системи, в якій знаходиться інформація, її важливості тощо різними є загрози, а відповідно й заходи протидії їм;
- досліджено фактори, що впливають на безпеку електронної інформації та роль технічних і програмних засобів в ній. На безпеку інформації в системі впливає ряд чинників зовнішнього та внутрішнього походження, отже, перед розпорядником інформаційної бази даних стоїть задача забезпечити весь комплекс заходів по забезпеченню інформаційної безпеки. З цією метою організовуються захищені приміщення для розташування серверів, залучається фізична охорона приміщень та об’єктів, а також встановлюється ряд програмних засобів по захисту інформації;
- досліджено методи та ефективність боротьби з атаками на комп’ютерні мережі на сучасному етапі. Розглянуто основні типи атак та їх особливості, а також існуючі засоби протидії окремим типам атак. Проте заздалегідь неможливо визначити, якого типу атаку буде проведено, тому окремі методи, які є ефективними проти одного типу атаки, можуть видатися безсилими проти іншого типу. Тому доцільно розглянути існуючі методики та виробити комплекс заходів, адекватний рівню загрози та важливості інформації в окремо взятій інформаційно-комунікаційній системі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Андон П. І., Ігнатенко О.П. Протидія атакам на відмову в мережі інтернет: концепція підходу. *Проблеми програмування*. 2018. № 2-3. С. 564-574.

2. Антонюк П. Є. Класифікація ймовірних способів вчинення атак на інформацію як напрям протидії комп'ютерній злочинності [Електронний ресурс] / П. Є. Антонюк. – 2011. – Режим доступу : http://www.nbuv.gov.ua/portal/Soc_Gum/bozk/19text/g1927.htm.

3. Бабенко Т. В. Дослідження ентропії мережевого трафіка як індикатора DDoS-атак / Т. В. Бабенко // Науковий вісник НГУ. – 2013. – № 2. – С. 86-89.

4. Багнюк Н. В. Види DDoS-атак та алгоритм виявлення DDoS-атак типу Flood-атак / Н. В. Багнюк, В. М. Мельник, О. В. Клеха // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. – 2015. – № 18. – С. 6-12.

5. Брацький В.О., М'якшило О.М., Литвинов В.А. Діагностична система аналізу log-файлів із віддалених вузлів обробки даних. *Математичні машини і системи.* 2022. № 1. С. 62-70.

6. Воронов М. П. Інформаційне забезпечення діяльності місцевих органів державної влади та органів місцевого самоврядування / М. П. Воронов // Збірник наукових праць. – Х., 2001. – Вип. 2, ч. 2: Державне управління та місцеве самоврядування. – С. 106–108.

7. Гаман Т. В. Вдосконалення організаційно-правового механізму інформаційної діяльності місцевих державних адміністрацій : дис. ... канд. наук з держ. упр.: 25.00.02 / Тетяна Василівна Гаман. – Л., 2006. – 246 с.

8. Гарасимчук О. І. Оцінка ефективності систем захисту інформації / О. І. Гарасимчук, Ю. М. Костів // Вісник КНУ імені Михайла Остроградського. – 2016. – № 1. – С. 16–20.

9. Гвозденко М. В. Технічні та програмні засоби виявлення джерела DDoS-атаки / М. В. Гвозденко, Я. В. Чобу // GLOBAL SCIENTIFIC UNITY 2014. – С. 106-115.

10. Гнатюк С. Є. Математичні моделі оцінки та прогнозування надійності програмно-керованих засобів захисту інформації в системі урядового зв'язку / С. Є. Гнатюк // Ukrainian Information Security Research Journal. – 2016. – № 2. – С. 150-156.

11. Голенищев Э. П. Информационное обеспечение систем управления : учеб. пособие. / Э. П. Голенищев, И. В. Клименко. – Ростов-на-Дону : Феникс, 2003. – 351 с.

12. Грищук Р. В. Атаки на інформацію в інформаційно-комунікаційних системах / Р. В. Грищук // Сучасна спеціальна техніка. – 2011. – № 1(24).– С. 61-66.

13. Єрмошин В. В. Методика оцінки інформаційних ризиків системи управління інформаційною безпекою / В. В. Єрмошин, В. О. Хорошко, М. В. Капустян // Сучасний захист інформації. – 2010. – №3. – С. 95–104.

14. Менеджмент інформаційної безпеки: підруч.: у 2 ч. / А. К. Гринь, О. Д. Довгань, В. І. Журавель та ін.; за заг. ред. Є. Д. Скулиша. – К. : Наук.–вид. Центр НА СБ України, 2013. – Ч.1. – 456 с.; Ч.2. – 604 с.

15. Невойт Я. В. Метод оцінювання стану захищеності інформаційних ресурсів на основі дослідження джерел загроз інформаційній безпеці : дис. канд. техн. наук. спец. 21.05.01/ Я. В. Невойт ; К. – ДУТ, 2016. – 110 с.

16. Перевалова Л. В. Захист конфіденційної інформації: проблеми та шляхи вирішення / Л. В. Перевалова, С. В. Кваша / Вісник Національного тех.-нічного університету «Харківський політехнічний інститут». Збірник науко-вих. праць. Тематичний випуск: Актуальні проблеми розвитку українського суспільства. – Харків : НТУ «ХПІ», 2011. – № 30. – 179 с.

17. Практика ИБ \ SANS: топ 20 наиболее критичных защитных мер и средств [Електронний ресурс].— Режим доступу: https://www.sugarsync.com/pf/D6870693_7400982_60553

18. Пронченко А.А., Коломицев М.В. Виявлення загроз на основі аналізу лог-файлів Apache. Системи та технології кібернетичної безпеки. С. 193-194.

19. Шпінталь М. Я. Методи захисту робочих станцій від DDoS-атак / М. Я. Шпінталь, Н. М. Орловський // ACIT'2014. – Тернопіль, 16-17 травня 2014. – С. 230-231.

20. Abdelsayed S., Glimsholt D., Leckie C., Ryan S., Shami S. An efficient filter for denial-ofservice bandwidth attacks // In Proceedings of the 46th IEEE Global Telecommunications Conference (GLOBECOM'03). – P. 1353–1357.

21. Basseville M. Detection of Abrupt Changes: Theory and Application / M. Basseville, I. V. Nikiforov (Prentice Hall, 1993).

22. Biskup J. Security in computing systems: challenges, approaches and solutions: monogr. / J. Biskup. – Berlin : Springer, 2009. – 694 p.

23. Borgnat P. Extracting Hidden Anomalies using Sketch and Non-Gaussian Multiresolution Statistical Detection Procedures / P. Borgnat // LSAD'07. – Kyoto, Japan, 2007.

24. Factor Analysis of Information Risk (FAIR) [Електронний ресурс]. – Режим доступу : http://www.riskmanagementinsight.com/.

25. NIST SpecialPublication 800-30 Risk Management Guide for Information Technology Systems [Електронний ресурс]. – Режим доступу : http://www.nist.gov.