МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

ЛАУТА Роман Сергійович

Підвищення стійкості інформаційної безпеки з використанням siem системи wazuh/ Enhancing Information Security Resilience Using Wazuh SIEM System

спеціальність: 125 – Кібербезпека

освітньо-професійна програма –Кібербезпека

Кваліфікаційна робота

Виконав студент групи КБм -21
Р.С Лаута

_____

Науковий керівник
к.т.н., доцент С.В.Івасьєв

_____

Кваліфікаційну роботу допущено
до захисту:

«____» _____ ___2023 р.

Завідувач кафедри

_____ В.В.Яцків

ТЕРНОПІЛЬ – 2023

Факультет комп'ютерних інформаційних технологій

Кафедра кібербезпеки

Освітній ступінь «магістр»

спеціальність: 125 - Кібербезпека

освітньо-професійна програма –Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ В.В.Яцків

____" _____ 2023 року

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

ЛАУТА Роман Сергійович

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:
Підвищення стійкості інформаційної безпеки з використанням siem системи wazuh/Enhancing Information Security Resilience Using Wazuh SIEM System.

керівник роботи к.т.н., доцент Івасьєв С.В.

затверджені наказом по університету від 1 грудня 2022 року № 491

2. Строк подання студентом закінченої кваліфікаційної роботи 1 грудня 2023 р.

3. Вихідні дані до кваліфікаційної роботи: завдання на випускну кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити:

- Дослідити протокол Modbus для мереж та провести аналіз загроз безпеки для комп'ютерних мереж.
- Проаналізувати існуючі SIEM системи та їхні можливості.
- Налаштування системи виявлення вторгнень.
- Виконати аналіз системи запобігання вторгненням.
- Побудувати модель виявлення програм-вимагачів за допомогою Wazuh.
- Побудувати модель атаки на протокол DHCP за допомогою Suricata та Wazuh.
- Кібербезпека в контексті використання технологій MODBUS/TCP і системи Wazuh.

5. Перелік графічного матеріалу у роботі.

- Таблиця основних даних протоколу MODBUS

- Таблиця порівнянь основних IPS
- Складові частини клієнта Wazuh
- Схема виявлення атаки в клієнті Wazuh

6. Консультанти розділів кваліфікаційної роботи

	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 11 жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Аналіз загроз інформаційної безпеки	12.2023 р. – 03.2023 р.	
2	Системи запобігання вторгнень	03.2023 р. – 05.2023 р.	
3	Моделі загроз інформаційної безпеки	05.2023 р. – 11.2023 р.	

Студент _____ Р.С Лаута
(підпис)

Керівник роботи _____ к.т.н., доцент С.В. Івасьєв
(підпис)

АНОТАЦІЯ

Кваліфікаційна робота на тему: "Підвищення стійкості інформаційної безпеки з використанням SIEM-системи Wazuh" зі спеціальності 125 «Кібербезпека» освітньо-професійної програми «Кібербезпека» написана обсягом 70 сторінок і містить 19 ілюстрацій, 1 додаток та 14 джерел за переліком посилань.

Ця робота присвячена дослідженню та вдосконаленню стійкості інформаційної безпеки в організаціях шляхом впровадження системи управління подіями захисту інформації (SIEM) Wazuh. Зростання загроз та атак в сучасному цифровому середовищі наголошує на важливості ефективного захисту корпоративних мереж та даних. У цій роботі проведено аналіз сучасних загроз безпеці інформації, існуючих векторів атак та вразливостей. Досліджено основні принципи роботи та можливості SIEM-системи Wazuh у виявленні, моніторингу та реагуванні на події, пов'язані з потенційними загрозами безпеці. Визначено ключові переваги використання Wazuh у порівнянні з іншими системами моніторингу безпеки. Для досягнення цілей роботи розроблено та запропоновано стратегії підвищення стійкості інформаційної безпеки на основі впровадження Wazuh. Ці стратегії включають в себе оптимізацію конфігурації системи, підвищення ефективності аналізу подій, розробку проактивних заходів захисту та планування реагування на потенційні загрози.

Дослідження, проведене в цій роботі, підтверджує ефективність та важливість використання SIEM-системи Wazuh у підвищенні стійкості інформаційної безпеки. Рекомендації та результати дослідження можуть бути корисними для організацій, що прагнуть зміцнити свої заходи захисту даних та мережі в умовах постійно зростаючих кіберзагроз.

КЛЮЧОВІ СЛОВА: SIEM, MODBUS, IDS, IPS, SCADA, MODBUS/TSP, WAZUH, ЗАХИСТ МЕРЕЖІ, SURICATA.

ABSTRACT

The qualification work on the topic: "Enhancing Information Security Resilience Using Wazuh SIEM System" from the specialty 125 "Cyber Security" of the educational and professional program "Cyber Security" is written in the volume of 70 pages and contains 19 illustrations, 1 appendix and 14 sources according to the list of references.

This master's thesis is dedicated to exploring and improving the resilience of information security within organizations through the implementation of Security Information and Event Management (SIEM) using Wazuh. The escalating threats and attacks in today's digital environment underscore the importance of effective protection for corporate networks and data. The paper conducts an analysis of contemporary information security threats, existing attack vectors, and vulnerabilities. The study delves into the fundamental principles and capabilities of the Wazuh SIEM system in detecting, monitoring, and responding to security-threatening events. Key advantages of using Wazuh over other security monitoring systems are identified. To achieve the objectives of this research, strategies are developed and proposed to elevate information security resilience based on the implementation of Wazuh. These strategies encompass system configuration optimization, enhanced event analysis efficiency, proactive security measure development, and planning responses to potential threats.

The research conducted in this paper confirms the effectiveness and significance of employing the Wazuh SIEM system in bolstering information security resilience. The recommendations and research findings can be valuable for organizations aiming to fortify their data and network protection measures amid the continuously growing landscape of cyber threats.

KEY WORDS: SIEM, MODBUS, IDS, IPS, SCADA, MODBUS/TSP, WAZUH, NETWORK SECURITY, SURICATA.

ЗМІСТ

ВСТУП

Актуальність роботи. Зважаючи на постійно зростаючу складність кіберзагроз та їхні впливи на різні сфери сучасного життя, проблема забезпечення надійного захисту інформації та критичних систем стає надзвичайно актуальною. Аналізуючи сучасний стан безпеки інформації, стає очевидним, що загрози постійно еволюціонують та стають більш складними, використовуючи нові технології та методики. Розуміння цих загроз та їхньої актуальності є першочерговою задачею для розробки ефективних стратегій захисту. Поряд зі зростаючою загрозою виникає необхідність удосконалення систем та методів захисту, особливо коли йдеться про критичну інфраструктуру. Ця категорія включає в себе ключові системи, без яких функціонування суспільства, економіки та національної безпеки стає неможливим. Оскільки загрози з кіберпростору можуть мати серйозний вплив на ці критичні системи, розробка та впровадження надійних та ефективних методів захисту стає невідкладною необхідністю.

Практична реалізація стратегій та методів захисту критичної інфраструктури є важливим аспектом вирішення проблеми кібербезпеки. Інноваційні технології, впровадження систем моніторингу та захисту, а також аналіз результатів впровадження цих заходів стають ключовими етапами в забезпеченні надійності та ефективності захисту критичної інфраструктури від сучасних кіберзагроз.

Робота пропонує аналіз сучасних загроз, дослідження систем та методів захисту критичної інфраструктури та їхню практичну реалізацію з метою покращення стійкості та надійності захисту від кіберзагроз.

Мета роботи полягає в дослідженні можливостей SIEM системи Wazuh та розробці рекомендацій та методів налаштування :

Для досягнення даної мети ставились **наступні завдання**:

- Проаналізувати сучасний стан мережевих протоколів та обґрунтувати вибір теми та використання SIEM системи Wazuh у контексті підвищення безпеки.

- Дослідити протокол Modbus для мереж та провести аналіз загроз безпеки для комп'ютерних мереж.

- Проаналізувати існуючі SIEM системи та їхні можливості.

- Налаштування системи виявлення вторгнень.

- Виконати аналіз системи запобігання вторгненням.

- Побудувати модель виявлення програм-вимагачів за допомогою Wazuh.

- Побудувати модель атаки на протокол DHCP за допомогою Suricata та Wazuh.

- Кібербезпека в контексті використання технологій MODBUS/TCP і системи Wazuh.

Об'єкт дослідження – SIEM системи та загрози інформаційної безпеки. Предмет досліджень – практики налаштування Wazuh та моделі атак на інформаційну безпеку.

Методи дослідження базуються на методах та алгоритмах опрацювання пакетів стеку протоколів TCP/IP та моделі OSI.

Наукова новизна одержаних результатів визначається наступним чином:

Побудовано моделі загроз інформаційної безпеки для виявлення програм-вимагачів та протоколу DHCP.

Практична цінність одержаних результатів полягає в тому, що:

Розроблено практичні заходи щодо налаштування Wazuh для забезпечення інформаційної безпеки.

1. Лаута Р.С. Виявлення шкідливого програмного забезпечення за допомогою Wazuh. Збірник матеріалів проблемно-наукової міжгалузевої конференції «Автоматизація та комп'ютерно – інтегровані технології» (АКІТ - 2023), Тернопіль, 2023. С. 159 -161.

2. Лаута Р.С. Підвищення стійкості інформаційної безпеки з використанням SIEM Wazuh. Збірник матеріалів науково-практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно – інтегровані технології» (КБКІТ -2023), Тернопіль, 2023. С. 83-86.

1 АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Сучасний стан мережевих протоколів

Інформаційні технології увійшли в наше повсякденне життя. Зараз дуже важко назвати галузь людської діяльності, в якій вони не відігравали б суттєвої ролі. Звичайно, вони не оминули критичні компоненти критичної інфраструктури, для прикладу - енергетика, транспорт, водопостачання та інші. Загалом, ці скефективні системи мають поєднання технологічних і людських компонентів. Логіка розвитку інфраструктури підказувала необхідність удосконалення управління цими об’єктами, перш за все механізація процесу, потім автоматизація технологічних процесів, які задіяні в їх експлуатації. Стрімкий розвиток інформаційних технологій для комп’ютерів та інформаційних систем привів до створення єдиної системи, яка забезпечує роботу в реальному часі шляхом обробки, збору, зберігання та відображення інформації про контрольовані або керовані об’єкти – SCADA

Системи SCADA широко використовуються у всіх галузях економіки, де оператори потребують контролю технічних процесів у режимі реального часу. Системи SCADA складається з наступних компонентів:

– периферійні датчики;

– людино-машинний інтерфейс;

– логічна система контролю;

– база даних;

– генератор звіту.

– зовнішні інтерфейси;

– головна диспетчерська система (головний термінал)

– кінцевий пристрій (дистанційний термінал) (RTU);

– програмований логічний контролер (PLC);

– комунікаційна інфраструктура (англомовна комунікаційна система CS).

Ця складна система, яка складається з компонентів, які працюють у цифровому масштабі, може бути природним чином інтегрована в загальну систему управління та має ефект підвищення ефективності інфраструктури,

особливо критичної. Системи, які використовують ресурси енергетичного сектору, як правило, вимагають збору інформації через RTU, потім інформація надсилається назад у центральне розташування, виконується необхідний аналіз і інформація відображатиметься на HMI. Протокол SCADA для зв'язку є універсальним проектом, який представляє дані через канал, який базується на принципі "головний/підлеглий". DNP3 і IEC60870-5-104 є найпопулярнішими протоколами зв'язку в енергетиці. Іншим популярним протоколом для SCADA є Modbus. У багатьох галузях промисловості Modbus використовується як засіб зв’язку, включаючи водопостачання та каналізацію.

Для правильної роботи систем необхідно мати певний обмін даними. Як правило, інформація з SCADA передається або в базу даних, або в мережу, а потім долає комерційно-промисловий бар’єр у мережі. Шлях зв’язку може бути завалений атаками, особливо це стосується протоколів, які містять розширення, призначені для роботи через TCP/IP. Незважаючи на спільність специфікацій, такі як TCP/IP, які розширюють функціональність мереж, вони, тим не менш, вводять нові вразливості в системи SCADA, яких не було в попередніх конструкціях із використанням власних протоколів. Серйозність кібернебезпек ілюструє сумна статистика, яка накопичилася за останні роки. Важливо пам’ятати про комп’ютерні атаки 2015 року на системи управління трьох різних компаній, які постачають енергію в Україну, в результаті якої була виведена з ладу підстанція «Північна» компанії «Укренерго», що призвело до того, що споживачі пн. частина країни знеструмлена, а точніше, близько 230 тис. споживачів «Прикарпаттяобленерго».

Пізніший докладний аналіз показав, вразливість була в протокольному шлюзі, мініатюрним пристроєм, який полегшує важливу передачу інформації між датчиками, різними приводами та комп’ютерами, які керують електростанціями та системами розподілу. Зловмисники швидко отримали доступ до центру управління електромережею, а на підстанціях відключили шлюзи протоколу, встановивши пошкоджене ПЗ. Це призупинило всі спроби спеціалістів енергосистеми швидко відновити роботу, оскільки системи

управління не мали можливості передавати команди вимикачам, що призвело б до замикання кола.

Цей напад був похідним від вдосконаленої віруса трояна BlackEnergy, який обходив мережу енергетичної компанії через необережне використання документа Microsoft Word. Захист від цього типу кіберзагроз є системним, кожна організація повинна вжити тих самих попереджувальних заходів для захисту систем SCADA, як і для захисту інших внутрішніх мереж, включаючи надійні паролі та регулярні оновлення операційної системи. Однак ми вважаємо, що цього недостатньо. Система, яка виявляє, розпізнає та запобігає кібератакам, є обов'язковою. Цей тип системи має бути спеціалізованим SIEM, який спирається на надійні базові практики та порівняння трафіку в режимі реального часу з шаблонами, а також мати проактивну здатність протидіяти атакам нульового дня та негайно інформувати персонал критичної інфраструктури про потенційну загрозу.

Критична інфраструктура складається з виробництва, передачі та розподілу електроенергії разом з іншими критично важливими ресурсами. Це надзвичайно важливо для забезпечення належного функціонування сучасного економіки і суспільства.

Електростанції відіграють значну роль у всьому розподілі електроенергії. Передача даних між центрами керування електростанціями та розподільними центрами має вирішальне значення для регулювання, моніторингу та захисту розподілу системи електроенергії. Спочатку передача даних обмежувалася передачею керуючих сигналів між SCADA та компонентами електростанції.

SCADA — це промислова система управління та моніторингу, яка включає інфраструктуру, обладнання, виробничу або технологічну документацію. Системи SCADA використовуються для забезпечення, регулювання та оцінки щоденних зобов'язань сучасного суспільства. Наприклад, такі фізичні процеси, як процес передачі та транспортування газу, електроенергії, води та нафти. "Протоколи SCADA складаються з Conitel, Profibus, Modbus RTU і RP-570. Загальними протоколами є, перш за все, IEC 61850, DNP3 і IEC 6087-5-11 або 104". Дані протоколи є універсальними та

працюють на основі протоколу керування передачею/протоколу Інтернету (TCP/IP).

1.2 Обґрунтування вибору теми та значення використання SIEM системи Wazuh у контексті підвищення безпеки

З розвитком цифровізації та дедалі більшою залежністю від технологій потенційні ризики та наслідки кібератак стали серйознішими. У результаті ефективні заходи кібербезпеки необхідні для захисту конфіденційних даних, запобігання фінансовим втратам і підтримки безперервності бізнесу. Ось чому тема кібербезпеки є надь важливою для вивчення, а система Wazuh SIEM є важливим інструментом для підвищення безпеки. Ефективне управління безпекою необхідне для запобігання кібератакам і пом’якшення впливу, коли вони відбуваються. Одним із методів досягнення цього є використання системи управління інформацією про безпеку та подій (SIEM), яка забезпечує постійний моніторинг і аналіз сповіщень безпеки та подій. Wazuh SIEM — це централізована платформа, яка збирає та аналізує миттєво зібрані телеметричні дані з метою виявлення та відповідності. Це безкоштовна платформа безпеки з відкритим кодом, яка поєднує захист SiEm і XDR, щоб захистити кінцеву точку та хмару від зловмисної поведінки. Платформа Wazuh SIEM надає численні переваги, зокрема:

- Виявлення загроз у реальному часі.
- Керування відповідністю.
- Логістика.
- Реагування на інциденти.
- Виявлення вразливостей.

Після проведення порівняльного аналізу кількох систем SIEM з відкритим кодом Wazuh було обрано як кращий варіант. Wazuh є провідним рішенням SIEM, яке використовується багатьма підприємствами, у тому числі технологічними. Він пропонує низку функцій, які роблять його ефективним інструментом для підвищення безпеки, включаючи його здатність інтегруватися

з різними інструментами безпеки та його гнучкість у налаштуванні. Впроваджуючи систему Wazuh SIEM, організації можуть покращити свою безпеку та краще захистити від кіберзагроз.

Система Wazuh SIEM є потужним інструментом для підвищення безпеки в корпоративних умовах. Ця безкоштовна платформа з відкритим кодом об'єднує захист XDR і SIEM для кінцевих точок і хмарних робочих навантажень. Однією з ключових особливостей системи Wazuh SIEM є її здатність агрегувати й аналізувати телеметрію в режимі реального часу, забезпечуючи виявлення загроз і відповідність. Ця централізована платформа пропонує ряд переваг для організацій, які прагнуть посилити свої заходи безпеки.

Переваги використання системи Wazuh SIEM численні. Ця система може підвищити стабільність інформаційної безпеки на підприємстві, забезпечуючи централізований перегляд подій безпеки. Це може допомогти організаціям швидше й ефективніше виявляти загрози та реагувати на них, покращуючи загальну безпеку. Крім того, система Wazuh SIEM може забезпечити відповідність галузевим нормам і стандартам, таким як PCI-DSS, HIPAA та GDPR. Використовуючи систему Wazuh SIEM, організації можуть краще захистити свої конфіденційні дані та інтелектуальну власність. Є кілька прикладів успішного впровадження системи Wazuh SIEM на підприємствах. Wazuh – компанія, заснована в 2015 році, яка створила провідне рішення SIEM для багатьох підприємств, у тому числі технологічних компаній Fortune. Одним із прикладів успішного впровадження є інтеграція системи Wazuh SIEM із Snort, системою виявлення вторгнень. Ця інтеграція забезпечує додаткові переваги, такі як покращене виявлення загроз і час відповіді. Використовуючи систему Wazuh SIEM, організації можуть скористатися цілим рядом покращень безпеки та краще захистити свої активи та дані.

1.3 Виявлення загроз інформаційної безпеки

Поле, яке часто ігнорується під час планування або тестування кібербезпеки в комунальних підприємств – це критична інфраструктура для підключення або телеметрії. Це життєво важливі зв'язки, які зв'язують системи керування SCADA з різними частинами електромережі – генераторами, станціями передачі, підстанціями та споживачами. Підключення до мережі в комунальних компаніях включатиме як частини, які завжди підключені, так і сегменти, що періодично підключаються, які використовуються для передачі даних під час опитування або певної події.

Ці канали зв'язку – комутовані телефонні мережі загального користування (PSTN), оптичні волокна або безпровідні мережі, як-от Глобальна система мобільного зв'язку або Загальна служба пакетної радіопередачі (GSM/GPRS). Подібно до інших систем зв'язку, телеметрія системи живлення використовує загальні протоколи, зокрема:

– Modbus.

– IEC 870-5-10x.

– DNP3.

– Profibus/Profinet.

Незалежно від типу протоколу, більшість промислових протоколів керування дотримуються парадигми запит/відповідь, яка призначена для «головного» (наприклад, людино-машинного інтерфейсу), який запитує інформацію або записує «slaves», такі як RTU або PLA. Багато з тих протоколів не мають таких функцій безпеки, як автентифікація або шифрування. Як наслідок, вони сприйнятливі до зловмисних атак, які використовують той самий протокол/функцію для запиту та відповіді. Це дозволить нам потенційно скористатися цим і створити ситуацію, в якій «slaves» будуть:

(1) вимкнені;

(2) уникати сповіщень про тривоги або сповіщення, викликати помилкову тривогу, яка призведе до стирання або втрати важливої інформації.

Хоча загроза безпеки мережі очевидна, головною метою є захист мережі від атак, які можуть негативно вплинути на критичну інфраструктуру. Іншим аспектом безпеки, який слід розглянути, є потреба в додаткових заходах безпеки. Інтелектуальні мережі виробляють велику кількість даних про споживачів, їхні звички використовувати електроенергію, моделі споживання та іншу інформацію, яка дозволяє ідентифікувати особу. Зловживання цією інформацією може завдати шкоди. Розуміння звичок споживачів може допомогти продемонструвати, наприклад, чи перебуває людина вдома чи ні, якими пристроями вона користується.

1.4 Протокол Modbus для мережі.

Регулярне вивчення IP-трафіку добре задокументовано з точки зору його ефективності при виявленні хакерів у сфері інформаційної безпеки. Однак процес інтеграції звичайних IT (таких як мережі та служби) з промисловими комунікаційними технологіями призводить до нових середовищ із попередньо розробленими мережами та новими проблемами безпеки. У цьому випадку MODBUS TCP/IP є найпопулярнішим протоколом. Для цих мереж доступні комерційні продукти, які вміють аналізувати трафік, розпізнавати вторгнення та вживати необхідних заходів. Однак більшість із них мають власні апаратні та програмні компоненти, які не завжди легко зрозуміти або використовувати за призначенням. Крім того, їх вага може стати причиною того, що вони будуть непридатні для будь-якої місії.

Не так давно аналогові та індивідуальні системи зв'язку були поширені у великих компаніях, які використовували технології. Протягом 70-х років комунікаційні мережі використовувалися для безпосереднього керування цифровою інформацією. Протягом наступного десятиліття різні технології вдосконалювалися, і в 1979 році MODBUS вперше був випущений для широкого загалу. Modicon задумав цей протокол як засіб передачі вмісту регістру з aPLC (програмованого логічного контролера) в інше місце, на aPLC або комп’ютер.

MODBUS спочатку передбачався для роботи через послідовний порт, такий як RS-232 або RS-485. Однак він перетворився на протокол зв'язку клієнт/сервер, який реалізовано на рівні повідомлень програми. Через його архітектуру, яка виконує запити та відповіді, включення його в IP-пакети є природним прогресом, це зробить його доступним для різних комп'ютерів і мереж, які підключені один до одного.

Кадри протоколу, отримані від Modbus, мають код, який функціонує як поле даних. Код функції – це один байт, який має діапазон допустимих значень від 1 до 255. Код функції 0 є неправильним. Довжина поля даних залежить від коду функції та може не мати довжини (нульової довжини). Якщо помилок немає, відповідь сервера містить код функції (той самий, що й у запиті) і запитувану інформацію. Якщо помилка пов'язана із запитуваною функцією MODBUS, поле коду функції містить код функції, пов'язаний з помилкою. У цьому випадку поле даних містить код винятку.

Модель даних Modbus - це протокол передачі даних, який широко використовується в промислових мережах для збору даних з різних пристроїв. Цей протокол має свою власну структуру передачі даних, яка складається з функцій читання та запису даних. Функції читання та запису даних у моделі даних Modbus забезпечують взаємодію між пристроями та дозволяють читати та записувати дані з різних пристроїв. Функції читання даних використовуються для зчитування даних з пристроїв, таких як сенсори, контролери тощо. Функції запису даних використовуються для запису даних на пристрої.

Модель даних Modbus передбачає використання адресації в реєстрах, що дозволяє ідентифікувати окремі пристрої та зчитувати/записувати дані з/на конкретному адресі. Крім того, ця модель даних використовує дві форми адресування: адресування в режимі ASCII та адресування в режимі RTU. Модель даних Modbus підтримує різні типи даних, такі як біти, регістри, змінні типу float тощо. Це дозволяє передавати різні типи даних з різних пристроїв та взаємодіяти з ними. У моделі даних Modbus також існує можливість використовувати функції діагностики та контролю, які дозволяють виявляти

помилки та неполадки в промислових мережах. Загалом, модель даних Modbus є важливим елементом передачі даних у промисловості та дозволяє зчитувати та записувати дані з різних пристроїв, забезпечуючи ефективну роботу промислових процесів та точність збору та аналізу даних.

Модель даних MODBUS — це проста серія таблиць, які мають різні властивості. Основні дані протоколу MODBUS в Таблиця 1.1

Таблиця 1.1 - Основні дані протоколу MODBUS

Таблиця	Тип об’єкту	Тип	Характеристики
Дискретний вхід	Один біт інформації	Лише читання	Тип даних, отриманий із системи введення/виведення. Зазвичай це цифрові входи (напруга або контакт).
Котушки	Один біт інформації	Зчитується та записується	(Тип даних, які можуть бути змінені прикладною програмою, входи, виходи або проміжні змінні).
Вхідні регістри	Шістнадцяти бітне слово	Лише читання	для додаткових даних доступне через систему введення/виведення. Зазвичай аналогові входи.
Виконувані регістри.	Шістнадцяти бітне слово	Зчитується та записується	Цей тип даних може бути змінений за допомогою програми.

Загальноприйнято розуміти, що всі чотири таблиці розташовані поруч одна з одною. Для первинних таблиць протокол дозволяє вибрати 65 536 різних

компонентів даних. Однак, оскільки дані вважаються фактичним форматом фізичної пам’яті, це не обов’язково означає, що посилання на дані пов’язано з адресою пам’яті. Головна вимога до сервера MODBUS – пов’язати канал даних із фізичною адресою.

1.5 Аналіз сучасних трендів та викликів у сфері інформаційної безпеки

Штучний інтелект (AI) і машинне навчання (ML) є трендами, що стрімко розвиваються у сфері інформаційної безпеки. AI та ML можуть аналізувати багатофакторні дані та враховувати складні залежності, дозволяючи приймати об’єктивні та оптимальні рішення. Проте все більш широке використання ШІ в національній безпеці викликає занепокоєння з питань етики та безпеки. За допомогою автоматизованих засобів глибокого аналізу виявляються певні інформаційні тренди, відстежуються зміни в реакції користувача. Використання штучного інтелекту та ML в інформаційній безпеці потенційно може підвищити ефективність і точність виявлення загроз і реагування на них, але також вимагає ретельного розгляду етичних наслідків і наслідків для безпеки. Інтернет речей (IoT) — це ще одна тенденція в інформаційній безпеці із застосуванням у громадській безпеці та військових операціях. Поєднання AI та IoT може розширити доступну функціональність і сприяти цифровій трансформації. Однак широке використання пристроїв IoT також створює загрози безпеці, оскільки ці пристрої можуть бути вразливими до кібератак. Впровадження IoT в інформаційну безпеку вимагає комплексного підходу, який враховує потенційні ризики та вразливі місця, пов’язані з цими пристроями.

Хмарні обчислення — це ще одна тенденція в інформаційній безпеці, що дозволяє віддалене зберігання та доступ до даних. Хмарні обчислення можуть підвищити гнучкість і масштабованість систем інформаційної безпеки, але вони також викликають занепокоєння на рахунок конфіденційності даних та їх безпеки. Впровадження хмарних обчислень в інформаційну безпеку вимагає ретельного розгляду потенційних ризиків і вразливостей, пов’язаних із цією технологією. Крім того, відеоаналітика та біометричні системи контролю

доступу також є новими тенденціями в інформаційній безпеці. Впровадження цих технологій може підвищити точність та ефективність аналізу і виявлення загроз та реагування на них, але також вимагає ретельного розгляду етичних наслідків і наслідків для безпеки.

Однією з головних проблем у сфері інформаційної безпеки є збільшення частоти та серйозності кібератак і загроз. Зі швидким розвитком технологій кіберзлочинці стали більш досконалими у своїх методах, що ускладнює захист конфіденційних даних і систем. Ці загрози можуть надходити з різних джерел, зокрема:

- Хакери.
- Шкідливе ПЗ.
- Шахрайства звязані з фішингом.
- Внутрішні погрози.

Для боротьби з цими загрозами організації повинні запровадити надійні заходи безпеки, зокрема брандмауери, шифрування та регулярні перевірки безпеки. Однак навіть із застосуванням цих заходів ризик успішної кібератаки залишається постійною загрозою.

Ще одним викликом у сфері інформаційної безпеки є дефіцит кваліфікованих фахівців. Оскільки технології продовжують розвиватися, попит на кваліфікованих фахівців з кібербезпеки різко зріс, випереджаючи пропозицію кваліфікованих кандидатів. Ця нестача є особливо гострою в країнах, що розвиваються, де освітні та навчальні програми можуть бути обмеженими. Щоб вирішити цю проблему, організації та уряди повинні інвестувати в освітні та навчальні програми, щоб розвинути групу кваліфікованих фахівців з кібербезпеки.

Складність дотримання норм і правил є ще однією значною перешкодою у сфері інформаційної безпеки. Організації мають дотримуватися кількох законів і правил щодо конфіденційності, безпеки та контролю даних. Це можна вважати складним завданням, особливо для малих і середніх компаній, яким може не вистачати ресурсів, щоб орієнтуватися в складній законодавчій базі. Крім того, ландшафт регулювання постійно змінюється, що ускладнює

організаціям ознайомлення з найновішими вимогами. Щоб уникнути цієї проблеми, організації повинні виділяти ресурси для відповідності та нормативних знань, включаючи наймання відданих працівників або аутсорсинг цих працівників.

Головною з основних тактик вирішення проблем і не відставати від тенденцій інформаційної безпеки є постійне навчання та розвиток навичок. Оскільки розвиток технологій продовжує бути швидким, фахівцям з інформаційної безпеки важливо йти в ногу з останніми інноваціями та набувати нових здібностей, щоб ефективно протистояти небезпекам, що виникають. Це включає участь у навчальних програмах, відвідування конференцій, присвячених галузі, та участь у поточних ініціативах професійного розвитку. Слідкуючи за новою інформацією та оновлюючись, професіонали можуть покращити свою здатність розпізнавати потенційні загрози та реагувати на них, що зрештою призведе до підвищення загальної безпеки.

Іншим важливим підходом до вирішення сучасних проблем і викликів безпеки є впровадження передових технологій та інструментів. З розвитком Індустрії і все більшою поширеністю цифрових технологій у всіх сферах життя вкрай важливо використовувати передові методи та інструменти для збереження конфіденційної інформації та систем. Це може передбачати використання передових методів шифрування, алгоритмів машинного навчання, які використовуються для виявлення загроз, і інтеграцію географічних інформаційних систем (ГІС), які використовуються для покращення візуального представлення та аналізу інформації. Завдяки застосуванню цих технологій фахівці з безпеки можуть більш ефективно виявляти потенційні небезпеки та реагувати на них, що, у свою чергу, призведе до підвищення безпеки їхньої організації чи країни в цілому.

Обмін інформацією та співпраця також життєво важливі для ефективної інформаційної безпеки. Оскільки кількість загроз зростає та набуває глобального масштабу, фахівцям із безпеки важливо співпрацювати, щоб виявляти й усунути потенційні небезпеки.

1.6 Підвищення стійкості інформаційної безпеки

Із зростаючою залежністю від технологій у всіх аспектах життя, від особистого спілкування до критичної інфраструктури, потенційні наслідки порушення безпеки є серйозними. Необхідність захищати конфіденційну інформацію та підтримувати цілісність даних має першочергове значення, оскільки наслідки порушення можуть бути далекосяжними та руйнівними. Оскільки світ стає все більш цифровим, потреба в надійних і надійних заходах захисту інформації стає все більш гострою. Кількість кібератак зростає, і вони частішають та бувають все більш витонченими. Ця тенденція становить серйозну загрозу для окремих осіб, різних організацій та урядів. Витрати на забезпечення живучості є одночасно витратами на підвищення безпеки інформаційної структури. Потреба в надійних заходах захисту інформації є більш гострою, ніж будь-коли раніше, оскільки потенційні наслідки проникнення можуть бути доволі серйозними, зокрема: фінансові втрати, правові наслідки, нанесення збитків репутації, скомпрометована особиста інформація

Для вирішення цих проблем необхідні ефективні заходи захисту інформації. Держава повинна приділяти значну увагу засвоєнню основоположних принципів і завдань управління інформаційною безпекою, вивченню та аналізу правових і нормативних вимог до організацій щодо інформаційної безпеки. В інформаційній політиці держави першочерговою метою має стати розробка та впровадження ефективних методів захисту інформаційних систем, до яких, зокрема, слід віднести:

– Постійні перевірки та аудити безпеки.

– Надійне шифрування, а також контроль доступу.

– Програми навчання та підвищення обізнаності співробітників.

– Плани та відпрацювання реагування на інциденти.

Застосовуючи проактивний погляд до інформаційної безпеки, міжнародні організації та уряди можуть краще себе захистити від зростаючої загрози кібератак і забезпечити стабільність своїх інформаційних систем. Проблема

забезпечення стійкості інформаційної безпеки є актуальною зважаючи на стрімкий технічним прогресом та змінами у сфері інформаційних технологій. З розвитком технологій змінюються й методи та інструменти, які використовують кіберзлочинці для злому систем інформаційної безпеки. Природа технологій, що постійно розвивається, означає, що заходи безпеки необхідно постійно оновлювати та вдосконалювати, щоб не відставати від нових загроз. Невиконання цього може призвести до значних фінансових втрат, репутаційної шкоди та скомпрометованих даних.

Людські помилки та внутрішні загрози також є факторами, які в більшості впливають на стабільність інформаційної безпеки. Навіть із застосуванням найсучасніших заходів безпеки людська помилка може призвести до вразливості, якою можуть скористатися кіберзлочинці. Крім того,також є і внутрішні загрози, такі як незадоволені співробітники або підрядники, можуть становити значний ризик для інформаційної безпеки. Для пом’якшення цих внутрішніх загроз вкрай важливо мати належне навчання та протоколи.

Стратегії підвищення стійкості інформаційної безпеки.

Для підвищення стабільності безпеки інформації критично важливі регулярні оновлення та технічне обслуговування систем безпеки. Організаціям потрібно забезпечити регулярну перевірку своїх інформаційних систем на відповідність їх політикам і стандартам інформаційної безпеки. Ця практика допоможе виявити потенційні вразливості та пом’якшити їх, перш ніж ними зможуть скористатися кібер-зловмисники. Регулярні оновлення та технічне обслуговування також гарантують, що системи безпеки оновлюються та можуть ефективно захищати від нових і нових загроз. Іншою важливою стратегією для підвищення стабільності безпеки інформації є проведення програм навчання та підвищення обізнаності для співробітників. Співробітники часто є найслабшою ланкою в системі безпеки організації. Вони можуть ненавмисно клацати фішингові посилання, використовувати слабкі паролі або піддаватися тактиці яка використовує соціальну інженерію. Проводячи регулярні програми з навчання та підвищення обізнаності, організації можуть допомогти своїм співробітникам зрозуміти важливість безпеки інформації та те, як визначити

потенційні загрози та як правильно реагувати на них. Ці програми також допомагають співробітникам бути в курсі найновіших методів безпеки та технологій. Для боротьби зі зростаючою загрозою кібератак міжнародні організації та уряди повинні працювати разом над розробкою ефективних механізмів забезпечення міжнародної інформаційної безпеки. Дана співпраця в більшості випадків приймає різні форми, включаючи спільні ініціативи з боротьби з дезінформацією та кіберзлочинністю. Крім того, міжнародні організації, такі як НАТО, визнали важливість інформаційної безпеки та вжили заходів для вирішення цієї проблеми. Працюючи разом, міжнародні організації та уряди можуть обмінюватися інформацією та ресурсами для кращого захисту від кіберзагроз і забезпечення стабільності інформаційної безпеки в глобальному масштабі.

1.7 Аналіз можливостей SIEM та Wazuh

Інформаційна безпека є критично потрібним аспектом новітніх комп’ютерних і комунікаційних систем. Це передбачає захист інформації від несанкціонованого доступу, використання, розголошення, порушення, модифікації або навіть знищення. Важливість інформаційної безпеки не можна недооцінювати, оскільки втрата або пошкодження важливих даних може призвести до серйозних наслідків, зокрема фінансових втрат, шкоди репутації та юридичної відповідальності. У зв’язку з цим дуже важливо створювати та підтримувати ефективні практики та методи захисту інформації для збереження важливої інформації. Існує кілька небезпек і вразливостей, які можуть вплинути на безпеку інформаційних систем, зокрема зловмисне програмне забезпечення, фішинг, соціальна інженерія та внутрішні загрози. Зловмисне ПЗ — це зловмисне програмне забезпечення, яке призначене для шкоди чи збою в роботі комп’ютерів, тоді як фішинг — це практика отримання конфіденційної інформації обманним шляхом, видаючи себе за надійну. Соціальна інженерія передбачає маніпулювання особами з метою розголошення конфіденційної інформації, тоді як інсайдерські загрози передбачають зловмисну діяльність

окремих осіб в організації. Розуміння цих небезпек і недоліків має ключове значення для розробки ефективного захисту від ризику. Кілька різновидів атак можна використовувати для націлювання на інформаційні системи, включаючи атаки націлені на відмову в обслуговуванні (DoS), атаки типу "людина посередині" (MitM) і атаки з впровадженням SQL. Мета DoS-атаки – порушити доступність системи, перевантаживши її трафіком або запитами. Атака MitM відбувається, коли користувач взаємодіє з веб-програмою, яка має базу даних, доступ до якої здійснюється через код SQL, який є зловмисним. Дуже важливо розпізнавати ці типи нападів і вживати відповідних заходів безпеки, як-от брандмауери, системи виявлення вторгнень і системи безпеки та керування подіями (SIEM), як Wazuh. Системи SIEM збирають і ретельно перевіряють інформацію, пов’язану з безпекою, з численних джерел, ця інформація потім використовується для виявлення небезпек і ефективного реагування на них.

SIEM, який також відомий як Security Information Management і Event Management, — це комплексне рішення, яке поєднує інструменти захисту інформації з подіями безпеки. Це програмний продукт безпеки, який полегшує моніторинг у реальному часі, аналіз та реагування на інциденти, пов’язані з IT-інфраструктурою організації. Основною метою SIEM є значне підвищення безпеки інформаційної та телекомунікаційної інфраструктури. Система з функцією SIEM складається зі збору, зберігання та аналізу даних про ключові інциденти безпеки, ці події зазвичай генеруються та обробляються в реальному часі. Ключові компоненти системи Siem включають збір, нормалізацію, кореляцію та аналіз даних. Збір даних передбачає отримання інформації про інциденти безпеки з різних джерел, зокрема мережевих компонентів, серверів і програм. Нормалізація передбачає перетворення зібраних даних у загальний формат, який можна аналізувати. Кореляція передбачає виявлення шаблонів і зв’язків між подіями безпеки для виявлення атак або потенційних загроз. Аналіз передбачає оцінку даних і створення сповіщень або звітів для реагування персоналу, які відповідають за служби безпеки.

Переваги використання SIEM включають покращене виявлення загроз, швидшу реакцію на інциденти та покращену відповідність нормативним

вимогам. Забезпечуючи постійний моніторинг та аналіз подій безпеки, системи SIEM допомагають організаціям розпізнавати загрози безпеці та реагувати на них швидше та проактивніше. Окрім того, системи SIEM полегшує організаціям досягнення відповідності різноманітним вимогам законодавства, таким як HIPAA та PCI-DSS. Загалом SIEM зазвичай значно підвищує рівень безпеки організації та допомагає забезпечити конфіденційність, цілісність і доступність критично важливих даних і систем.

Wazuh — це безкоштовна платформа, яка має комплексні можливості моніторингу та виявлення як для фізичного, так і для віртуального середовища. Він покликаний допомогти організаціям розпізнавати ризики безпеці та реагувати на них у реальному часі, що призведе до підвищення загального стану інформаційної безпеки. Wazuh базується на основних принципах інформаційної безпеки, які включають цілісність, конфіденційність та доступність. Це потужний інструмент, який допомагає організаціям зберегти свої важливі дані та ресурси, дотримуючись галузевих норм. Однією з основних характеристик Wazuh є його здатність розпізнавати небезпеки та реагувати на них у режимі реального часу. Він комбінує аналіз журналів, перевірки файлів і виявлення вторгнень на основі хосту, щоб визначити потенційні загрози безпеці, а потім негайно повідомити про це команди безпеки. Даний підхід до безпеки допомагає організаціям мінімізувати вплив інцидентів безпеки та знизити ризик витоку даних. Крім того, Wazuh легко налаштовується, що дозволяє компаніям та організаціям адаптувати його до своїх конкретних потреб і вимог безпеки.

Wazuh можна поєднувати з іншими технологіями безпеки, включаючи системи SIEM, щоб забезпечити більш комплексне рішення інформаційної безпеки. Системи SIEM призначені для збору та аналізу даних, які пов’язані з безпекою, в IT-інфраструктурі організації, що забезпечує цілісне представлення про стан безпеки організації. Wazuh доповнює системи SIEM, надаючи можливості моніторингу безпеки кінцевих точок та хмар, які є ключовими компонентами комплексної стратегії безпеки. Завдяки інтеграції Wazuh із

системами SIEM організації можуть краще зрозуміти свою безпеку та ефективніше реагувати на інциденти загрози.

Системи SIEM збирають і ретельно перевіряють інформацію про безпеку які беруть з різних джерел, такі як: мережеве обладнання, сервери та програми, щоб отримати повну картину безпеки організації. Рішення Wazuh — це централізована платформа, яка збирає та аналізує телеметричну інформацію в реальному часі, щоб виявити та покращити відповідність. Ця платформа пропонує кілька функцій, які полегшують вирішення проблем і покращують безпеку даних та інформації. Рішення Wazuh забезпечує численні переваги, які роблять його вигідним рішенням для вирішення проблем безпеки даних та інформації. Одним із основних атрибутів цієї системи є її здатність розпізнавати загрози в реальному часі, за допомогою чого організація швидко реагувати на потенційні загрози безпеці. Іншим важливим атрибутом Wazuh є його здатність аналізувати криптографічно зашифрований трафік, це серйозна проблема для інших систем безпеки. Однак розповсюдження системи Wazuh може бути обмежено фізичною потужністю апаратного забезпечення, на якому розташований менеджер сервера. Незважаючи на обмеження, система Wazuh залишається життєздатним варіантом для організацій, які хочуть підвищити безпеку та захистити свої дані та інформаційні ресурси.

Безпека даних і важливої інформації є проблемою для кожної організації, незалежно від її розміру чи типу. У міру збільшення обсягу даних, які генеруються та зберігаються, захист цих ресурсів від різноманітних небезпек стає складнішим, включаючи кібератаки, розкриття даних і внутрішні загрози. Безпека даних та інформаційних ресурсів має першочергове значення, включаючи цілісність і доступність та конфіденційність. За для безпеки цих ресурсів, організації повинні усвідомлювати поточні небезпеки безпеки даних і тенденції. Сучасні виклики та тенденції у сфері безпеки даних включають все більшу поширеність хмарних сервісів, збільшення кількості підключених пристроїв і дедалі складніші кібератаки. Ці перешкоди змушують організації застосовувати передові рішення безпеки, які у реальному часі виявляють загрози та реагувати на них. Рішення безпеки та управління подіями (SIEM),

такі як Wazuh SIEM, допомагають організаціям подолати ці проблеми, надаючи централізовану платформу для агрегування та аналізу телеметрії в реальному часі для якнайшвидчому виявлення загроз і відповідності.

Система Wazuh надає численні переваги, які можуть допомогти організаціям вирішити поточні проблеми та тенденції, пов’язані з безпекою інформації та даних. Система виявляє та реагує на загрози у реального часі, керує дотриманням вимог і зберігає записи журналів. Він може збирати та аналізувати інформацію з кількох різних джерел, у тому числі кінцевих точок, хмарних робочих навантажень і мережевих пристроїв, що надасть організаціям повну картину їхньої безпеки. Система також використовує файли YAML і JSON для введення та виведення, що полегшує інтеграцію інших рішень безпеки. За допомогою Wazuh організації можуть посилити безпеку, розпізнавати небезпеки та реагувати на них у режимі реального часу, а також досягати відповідності законодавству.

Впровадження системи Wazuh SIEM має багато переваг у вирішенні проблем і тенденцій безпеки даних та інформації. Однією з головних переваг є розширена здатність розпізнавати ризики безпеці та реагувати на них. Рішення Wazuh надає централізовану платформу, яка збирає та аналізує дані в реальному часі для виявлення та усунення інцидентів безпеки. Ця здатність є важливою в сучасному середовищі кібератак, оскільки передбачає підвищення рівня складності та частоти. Ще одна перевага системи Wazuh полягає в тому, що вона підвищує відповідність нормативним вимогам і стандартам. Система підтримує кілька стандартів відповідності, включаючи PCI-DSS, HIPAA та GDPR, що гарантує, що організації відповідають необхідним вимогам безпеки та конфіденційності. Рішення Wazuh також містить докладний журнал перевірок, що полегшує перевірку відповідності та звітування за допомогою нормативних актів. Ця функція особливо важлива для організацій, які мають захистити конфіденційні дані.

Впровадження системи Wazuh SIEM також може призвести до зниження витрат і підвищення ефективності управління безпекою. Система автоматизує багато процесів безпеки, наприклад збір і аналіз журналів, зменшуючи потребу

в ручному втручанні та оптимізуючи операції безпеки. Крім того, Wazuh SIEM має відкритий вихідний код, що означає, що воно безкоштовне для використання та може бути налаштовано відповідно до конкретних потреб організації. Ця гнучкість призврдить до суттєвої економії коштів організації чи компанії, особливо для невеликих організацій з обмеженим бюджетом. Підсумовуючи, система Wazuh SIEM пропонує кілька переваг у вирішенні проблем і тенденцій у безпеці вашиї даних і інформаційних ресурсів. Покращуючи виявлення потенційних загроз і швидкого реагування на них, підвищуючи дотримання нормативно-правових вимог, а також зменшуючи витрати та підвищуючи ефективність управління безпекою, рішення Wazuh SIEM допомагає організаціям як найкраще захистити свої цінні дані та інформаційні ресурси.

2 СИСТЕМИ ЗАПОБІГАННЯ ВТОРГНЕНЬ

2.1 Загрози критичної інфраструктури

Для того щоб підвищити безпеку будь-якої системи та ефективно захистити її, надзвичайно важливо розуміти ризик, пов’язаний із потенційними збоями комп’ютера та зв’язку в її інфраструктурі. Експерти з кібербезпеки зазвичай поділяють на три типи помилок:

– Наприклад, порушення конфіденційності. неспроможність зберегти конфіденційність системної інформації, яка не авторизована.

– Втрата доступності, наприклад. відсутність можливості забезпечити доступ до інформаційної системи протягом тривалого періоду часу тим користувачам або машинам, які призначені одержувачами.

– Порушення цілісності, що є порушенням захисту даних системи від несанкціонованого доступу. Як наслідок, вигідним визначенням кіберризику є можливість виникнення будь-якого з цих режимів збою та їхні відповідні наслідки. У ICS, які контролюють фабрики, ці ефекти можуть проникати у фізичну сферу. Ризик є найбільш визнаним і, можливо, найбільш дослідженим прикладом у більшому класі показників кібербезпеки.

Повністю захищена комп’ютерна система не мала б слабких місць і не була б чутливою до будь-яких атак. Однак, як часто жартують з цього приводу експерти, система за своєю суттю ізольована від людей і ніким ніколи не використовується. Це демонструє значимість. Якщо всі небезпеки апаратного, програмного та мережевого забезпечення успішно уникнути, користувачі системи залишаються людьми та можуть виконувати заплановані чи незаплановані дії, які можуть негативно вплинути на роботу. Неможливо повністю уникнути внутрішньої загрози, пов’язаної з персональними комп’ютерами користувачів. Зважаючи на це, ми погоджуємося з концепцією, що справжня комп’ютерна система завжди вразлива до атак, незалежно від наявних технічних або фізичних перешкод.

Звичайно, це стосується комп’ютерів, які входять в частину ICS, ці комп’ютери використовуються для автоматизації та регулювання критичних

процесів у промислових умовах. Системи ICS в більшості випадків мають більш технічні та фізичні проблеми, ніж комп’ютери, просто тому, що сучасні комп’ютери зазвичай розроблені з урахуванням стандартів безпеки.

2.2 Аналіз можливостей систем виявлення вторгнень

Якщо комп’ютерна система вразлива, як її можна захистити? Ранні ідеї мали на меті спостереження за існуючими обліковими записами (для мейнфрейму IBM System Management Facility [SMF]) і проведення аналітичних тестів цієї інформації для виявлення незвичних закономірностей. Цей захід прийнято вважати першим IDS. Ідея полягає в тому, щоб поширювати інформацію про аномальні шаблони як засіб спостереження за безпекою людини, при цьому очікуючи, що більшість позначених шаблонів не будуть шкідливими. Деннінг (1987) пізніше розширив цю ідею, використовуючи більш складну модель і більший набір процесів, які були створені SRI International кількома роками раніше.

Дуже важливо визнати, що вразливі місця та небезпеки, пов’язані з цими ранніми комп’ютерами, відрізнялися від тих, які були пов’язані з іншими комп’ютерами в більшості систем ІКТ, які зараз використовуються. Знання технічних навичок користувача комп’ютера значно зросли. Графічний інтерфейс і комп'ютерні миші в цих пристроях не були поширені. Розважальна діяльність користувачів комп’ютерів (наприклад, серфінг в Інтернеті) була вкрай рідкісною або взагалі не існувала на той час, тому зовнішня небезпека через Інтернет не викликала великого занепокоєння. Крім того, небезпеки та можливі попередження, які потім були розглянуті.

- Спроба злому.
- Спроба маскування або успішний злом.
- Проникнення легітимним користувачем.
- Витік законним користувачем.
- Троян.
- Вірус.

- Відмова в обслуговуванні.

Сучасні моделі загроз майже ідентичні раннім моделям загроз, які використовувалися в цій системі, модель загроз була набагато простішою.

У зв'язку з ростом популярності IDS на основі ІКТ, стали використовувати додаткові методи для виявлення підозрілої активності. Багато з попереджень та загроз стосуються збереження конфіденційності приватних даних, які зберігаються на комп'ютерах чи у мережах. Поняття безпеки часто виражається через "тріаду" ЦРУ: конфіденційність, цілісність та доступність. При виявленні потенційної проблеми з безпекою в системі ІКТ першим кроком є оцінка того, чи були порушені конфіденційні дані, такі як банківська інформація, кредитні картки або особиста електронна пошта. Цілісність та доступність є ключовими аспектами для систем ІКТ, але в ініціативі IDS для ІКТ переважали питання конфіденційності. Мета більшості зловмисників, які атакують системи ІКТ, може відрізнятися від цілей тих, хто зламує системи ІКТ. Системи ICS, що контролюють процеси, мають за мету порушити саму процедуру, тобто доступність системи.

Перші домашні стаціонарні комп’ютери початку 80-х років мали незначний технічний або мережевий захист. Найефективніший спосіб захистити комп’ютери – це запровадити фізичну безпеку: запечатати кімнату, забрати жорсткий диск з ПК або навіть встановити фізичне блокування джерела живлення пов’язаної системи. Одні з перших користувачів ПК мали можливість використовувати пароль для автентифікації. Однак систему все одно виявилося легко зламати, якщо у вас був прямий доступ до комп’ютера, а використання ПК без прямого доступу було вкрай рідко. Фізична безпека була перш за все. ICS схожі на ці ранні комп’ютери. ICS зазвичай використовують обладнання, виготовлене у 80-х роках або раніше, і вважають фізичний захист основною формою захисту. Причина в тому, що старе обладнання все ще ефективне, а ICS першочергово турбується про доступність.

З тієї пори домашні комп’ютери стали складнішими та розширили пам’ять та обчислювальні можливості. Об’єднання в мережу персональних комп’ютерів і портативних пристроїв стало буденним явищем. Таким чином,

інформація легко доступна, і це можна зробити одним хаком. І навпаки, ICS не зазнав значних змін з 80-х років. Незважаючи на це, існує більше бажання підключити їх до інтернету та внутрішньої мережі, щоб дозволити менеджерам і операторам отримувати до них віддалений доступ. Після того як було встановлення віддаленого з'єднання з мережею з цими за своєю суттю незахищеними комп'ютерами фізична безпека мережі більше не викликає занепокоєння. Зломи найчастіше будуть відбуватися в глобальному Інтернеті, це зробить ICS (та їхні процедури) надзвичайно вразливими.

2.3 Система виявлення вторгнень

Система, яка має назву (IDS), відстежує мережевий трафік на шукає в ньому зловмисні транзакції і негайно надсилає сповіщення, коли це спостерігається. Дане програмне забезпечення, яке перевіряє мережу чи систему на наявність зловмисних дій або порушень політики. Кожна незаконна діяльність або порушення часто фіксується централізовано за допомогою системи SIEM або повідомляється адміністрації. IDS відстежує мережу чи систему на наявність зловмисної активності та захищає комп'ютерну мережу від несанкціонованого доступу користувачів, у тому числі, можливо, інсайдерів. Завдання навчання детектора вторгнень полягає в тому, щоб побудувати прогностичну модель (тобто класифікатор), здатну розрізняти «погані з'єднання» (intrusion/attacks) і «хороші (нормальні) з'єднання».

Роботу IDS можна розбити по пунктах:

- IDS (система виявлення вторгнень) відстежує весь мережевий трафік у мережі, з метою виявити будь-яку підозрілу активність.

- Він аналізує всі дані, які проходять через мережу, щоб знайти шаблони та ознаки ненормальної поведінки.

- IDS порівнює мережеву активність із набором правил і шаблонів, які були попередньо визначені, щоб визначити будь-яку активність, яка свідчить про атаку чи вторгнення.

- Якщо IDS виявляє щось, що відповідає одному з цих правил або шаблонів, вона надсилає сповіщення системному адміністратору.

- Після цього адміністратор системи може дослідити сповіщення та вжити заходів, щоб запобігти будь-якому пошкодженню чи подальшому вторгненню.

Класифікація систем виявлення вторгнень має декілька розділів. IDS поділяють на 5 типів:

1) Система виявлення вторгнень у мережу (NIDS): Системи виявлення вторгнень у мережу (NIDS) встановлюються в запланованій точці мережі для перевірки трафіку з усіх пристроїв у мережі. Він виконує спостереження за трафіком, що проходить у всій підмережі, і зіставляє трафік, який передається підмережами, із колекцією відомих атак. Після виявлення атаки або виявлення ненормальної поведінки сповіщення можна надіслати адміністратору. Прикладом NIDS є його встановлення в підмережі, де розташовані брандмауери, щоб побачити, чи хтось намагається зламати брандмауер. (Рисунок 2.1)

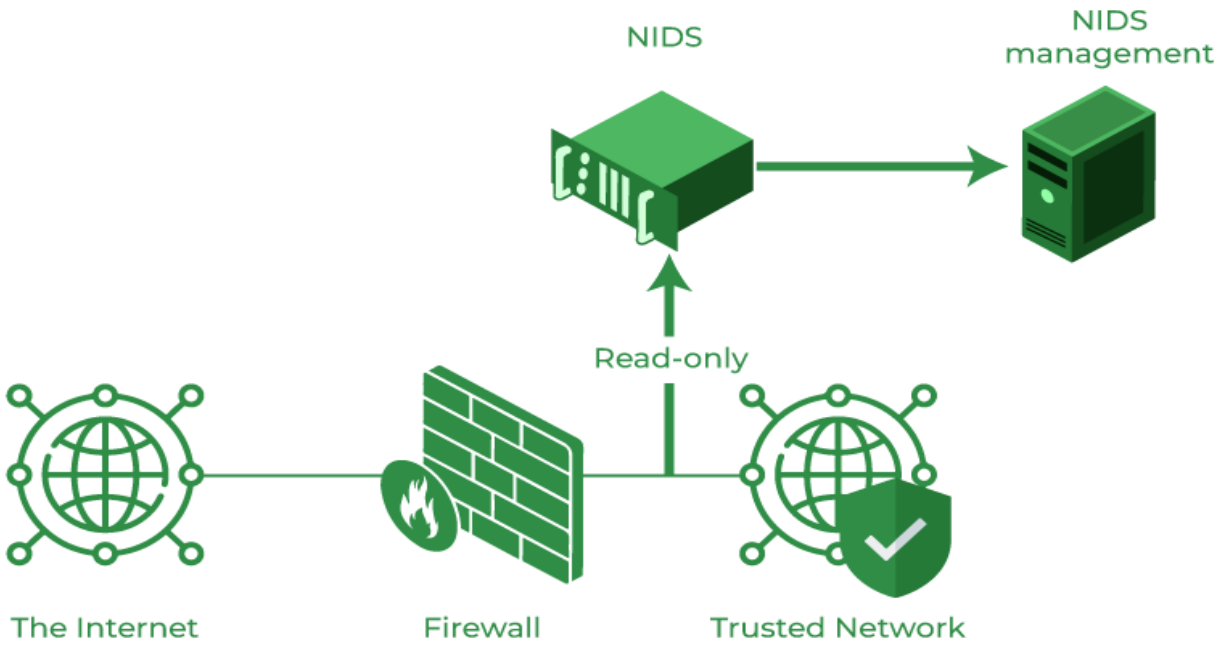


Рисунок 2.1 - Система виявлення вторгнень у мережу NIDS

2) Система виявлення вторгнень (HIDS), яка діє на окремих хостах або пристроях в мережі, спостерігає за вхідними та вихідними пакетами пристрою і повідомляє адміністратора, якщо вона помічає підозрілу чи зловмисну активність. HIDS робить знімок поточних системних файлів та порівнює їх з попереднім станом. У випадку редагування або видалення файлів системи, система надсилає сповіщення адміністратору для подальшого аналізу. Приклад використання HIDS можна побачити на критичних машинах, де не очікується зміна конфігурації (Рисунок 2.2).

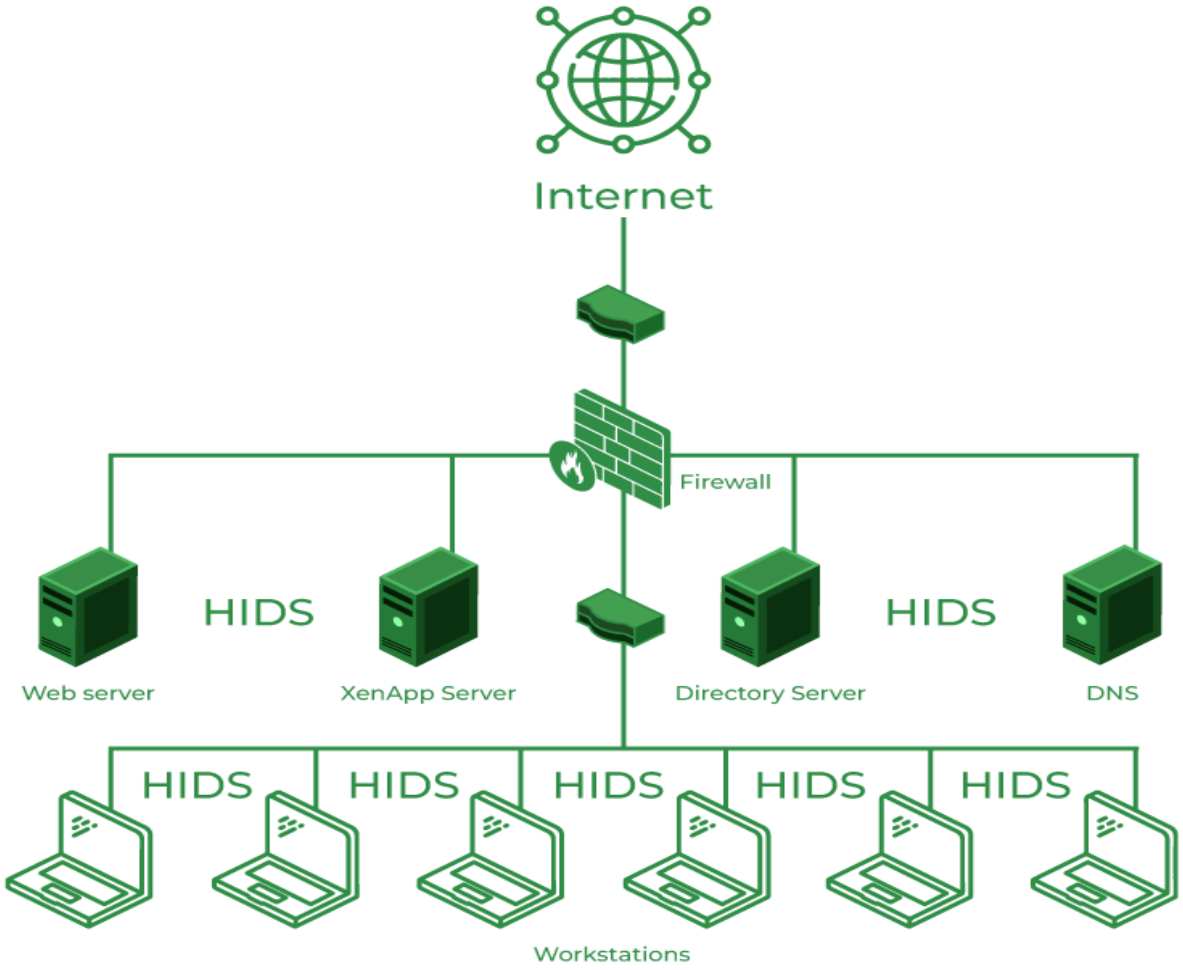


Рисунок 2.2 - Структура роботи HIDS

3) Система для виявлення вторгнень на основі протоколу (PIDS): Система виявлення вторгнення на основі протоколу (PIDS) складається з системи або агента, який постійно розміщується на передній частині сервера, контролюючи та інтерпретуючи протокол між користувачем/пристроєм і сервером. Він

намагається захистити веб-сервер, регулярно відстежуючи потік протоколу HTTPS і приймаючи відповідний протокол HTTP. Оскільки HTTPS не зашифрований і перед миттєвим переходом на рівень веб-презентації, ця система повинна знаходитися в цьому інтерфейсі між використанням HTTPS.

4) Система виявлення вторгнень на основі протоколу додатків (APIDS) - це система, що зазвичай розташована на серверах, спостерігає та аналізує комунікацію за протоколами, що стосуються окремих програм. Наприклад, вона може активно відслідковувати використання SQL-протоколу під час взаємодії програми з базою даних на веб-сервері.

5) Гібридна система виявлення вторгнень поєднує кілька підходів до виявлення вторгнень, об'єднуючи дані від агентів системи та мережеву інформацію для повнішого розуміння мережі. Цей підхід дозволяє створювати більш комплексне уявлення про систему порівняно з іншими системами виявлення вторгнень. Prelude є прикладом гібридної системи виявлення вторгнень.

Основні переваги IDS:

- Виявляє зловмисну активність: IDS може знайти будь-які підозрілі дії та попередити системного адміністратора до того, як буде завдано будь-якої значної шкоди.

- Покращує продуктивність мережі: IDS може виявляти різні проблеми з продуктивністю в мережі, які можна вирішити для покращення продуктивності мережі.

- Вимоги відповідності: IDS може допомогти виконати вимоги відповідності шляхом моніторингу активності мережі і створення звітів.

- Надає статистику: IDS створює цінну інформацію про мережевий трафік, яку використовують для того щоб знайти будь-якиі слабкиі місця і підвищення безпеки мережі.

2.4 Система запобігання вторгненням

Систему запобігання вторгненням також називають системою виявлення та запобігання вторгненням. Це програма безпеки для мереж, яка виявляє зловмисну активність. Основні функції систем запобігання вторгненням полягають у виявленні зловмисної активності, зборі інформації про цю діяльність, звіті про неї та спробі заблокувати або зупинити її. Системи запобігання вторгненням розглядаються як доповнення систем виявлення вторгнень (IDS), оскільки і IPS, і IDS керують мережевим трафіком і діяльністю системи для зловмисної діяльності.

IPS зазвичай записує інформацію, яка пов’язана з спостережуваними подіями, сповіщає адміністраторів безпеки про важливі спостережувані події та створює звіти. Багато IPS також можуть реагувати на виявлену загрозу, намагаючись запобігти її успіху.

Є два основних типи IPS:

- Мережевий IPS: мережевий IPS встановлюється на периметрі мережі та контролює весь трафік, який входить і виходить з мережі.

- IPS на основі хоста: IPS на основі хоста встановлюється на окремих хостах і відстежує трафік, який надходить і виходить із цього хосту.

IPS є важливим інструментом безпеки мережі. На це є декілька причин :

- Захист від відомих і невідомих загроз: IPS може блокувати відомі загрози, а також виявляти та блокувати невідомі загрози, яких раніше не було.

- Захист у реальному часі: IPS здатний виявляти та блокувати шкідливий трафік негайно, запобігаючи завданню шкоди в результаті атак.

- Вимоги до відповідності: у багатьох галузях є правила, які вимагають використання IPS для захисту вашої конфіденційної інформації та запобігання втрати даних.

- Економічно ефективний: IPS є доволі вигідно ефективним способом захисту вашої мережі порівняно з вартістю ліквідації наслідків взлому безпеки.

Система для запобігання вторгненням (IPS) класифікується на 4 типи:

1) Мережева система запобігання вторгненням (NIPS) .

вона контролює всю мережу на наявність підозрілого трафіку шляхом аналізу активності протоколу.

2) Система запобігання бездротовому вторгненню (WIPS).

вона відстежує бездротову мережу на наявність підозрілого трафіку шляхом аналізу протоколів бездротової мережі.

3) Аналіз мережі (NBA): виявляє аномальну поведінку трафіку, щоб визначити небезпеки, які спричиняють незвичайні потоки трафіку, такі як розподілені атаки відмови в обслуговуванні, певні типи зловмисного програмного забезпечення та насильницька політика.

4) Система запобігання вторгнень на основі хосту (HIPS). Це вбудований програмний пакет, який керує одним хостом на наявність сумнівної активності шляхом сканування подій, що відбуваються на цьому хості.

Нижче проведено порівняння технологій системи для запобігання вторгненням (Таблиця 2.1)

Таблиця 2.1 Порівняння IPS

Тип технології IPS	Виявлені типи шкідливих дій	Обсяг на датчик	Сильні сторони
Мережевий	Діяльність мережевого, транспортного та додаткового рівня TCP/IP	Кілька мережевих підмереж	Тільки IDPS, який може аналізувати найширший діапазон прикладних протоколів
Бездротови	Активність бездротового протоколу; несанкціонований бездротовий зв'язок використовуваня локальної мережі (WLAN)	Кілька мереж WLAN і групи бездротових клієнтів	Тільки IDPS може передбачити активність бездротового протоколу
NBA	Діяльність мережевого, транспортного та додаткового рівня TCP/IP	Кілька мережевих підмереж	ідентифікаційне розвідувальне сканування та DoS-атаки,
На основі хоста	Діяльність хост-програми та операційної системи(ОС); мережа, транспорт,	Індивідуальний хост	Може аналізувати діяльність, що було передано наскрізно, зашифровані комунікації

Метод виявлення системи запобігання вторгненням (IPS):

1) Метод виявлення на основі сигнатур:

IDS на основі сигнатур обробляє пакети в мережі та порівнює їх із заздалегідь створеними та визначеними шаблонами атак, відомими як сигнатури.

2) Статистичне виявлення аномалій:

IDS на основі аномалій відстежує трафік всієї мережі і зрівнює зі встановленим базовим рівнем. Базовий рівень визначає, що є нормальним для цієї мережі та які протоколи використовуються. Однак він може викликати тривогу, яка виявиться помилковою, якщо базові лінії не налаштовані розумно.

3) Метод виявлення аналізу протоколу з урахуванням стану IDS спостерігає за відмінностями у протоколах, порівнюючи події, які спостерігаються, з раніше створеними профілями нормальної активності.

Основна відмінність між системою запобігання вторгненням (IPS) та системами виявлення вторгнень (IDS) полягає в наступному:

- Системи IPS знаходяться на лінії та активно запобігають або блокують виявлені вторгнення.

- IPS може виконувати різні дії, такі як висилання тривог, видалення виявлених шкідливих пакетів, скидання з'єднань або блокування трафіку з неправильних IP-адрес.

- IPS також виправляє помилки у циклічній перевірці надлишковості (CRC), дефрагментувати потоки пакетів, лагодити проблеми послідовності TCP та очищати небажані параметри на рівні транспорту та мережі.

2.5 Додаткові методи виявлення вторгнень.

Сигнатура — це опис процедури або функції та параметрів, які з нею пов'язані. Сигнатура містить інформацію про аргументи, які передаються функції чи методу, їх типи та імена, а також інформацію про значення, що повертаються.

Під час написання оголошення функції підпис може мати такий склад:

- Ім'я функції;

- Різновидів і кількість параметрів.

Наприклад, підпис простої функції додавання в JavaScript буде таким:

```
////javascript
function add(x, y) {
return x + y;
}
////
```

Цей підпис має назву функції "add", два параметри, "x" і "y", і повернуте значення, яке є сумою двох параметрів.

Сигнатура функції в C++ зазвичай складається з таких компонентів:

```
////c++
void exchange(int* a, int* b) {
int temp = *a;
*a = *b;
*b = temp;
}
////
```

Сигнатура ідентична назві функції, яка переміщує два покажчики, «a» і «b», і змінює значення об’єктів, на які вказують ці покажчики.

Підпис є обов’язковим для розпізнавання визначення функції чи методу без необхідності його впровадження чи тестування. Це полегшує читання, розуміння та виправлення кодів, а також виявлення помилок коду під час розробки.

Одним з найпопулярніших інструментів безпеки, що використовують підписи, є Snort, створений Марті Решем у 1998 році та підтримується компанією Cisco. Інші методи виявлення, які базуються на сигнатурах, також відомі як експлойт-детектори або виявлення на основі знань. Ці методи

передбачають, що програмна загроза, яку вони розпізнають, вже відома. Багато антивірусних програм також використовують цей підхід у своїй технології. Snort часто використовується для виявлення шкідливого трафіку у мережі, але не впевнено розпізнає невідомий шкідливий код. Це може зробити методи, що базуються на підписах, менш надійними. Проте, вони досить точні у виявленні відомих випадків шкідливого коду, про які вже відомо. Якщо система видає тривогу про вторгнення, що вважається "позитивним", частота помилкових спрацьовувань для детекторів на основі сигнатур зазвичай досить низька.

Методи без підписів використовуються для ідентифікації користувача чи перевірки цілісності даних без специфічного підпису. Вони грають ключову роль у кібербезпеці, оскільки неможливо підробити або підписати певний знак, якщо його немає вихідного. Такі методи використовують альтернативні підходи, такі як шифрування та хешування, для перевірки достовірності та надійності даних. Важливість безпідписових методів у кібербезпеці полягає в їх здатності забезпечувати захист даних без необхідності використання підписів. Це особливо актуально у випадках, коли підпис може бути підробленим або заміненим, що може призвести до порушення безпеки даних. Наприклад, такі методи можуть застосовуватися для захисту від атак типу "людина посередині", де зловмисник намагається підробити підпис для доступу до даних.

Проте, впровадження непідписних методів може стикнутися з деякими проблемами. Наприклад, деякі методи можуть бути менш ефективними, ніж підписати, або потребувати більше ресурсів для реалізації. Крім того, використання непідписних методів може вимагати додаткової роботи для забезпечення даних безпеки та перевірки ідентифікації користувачів. Також не всі системи підтримують непідписні методи, які можуть створювати проблеми з їх використанням на практиці. Однак, із розвитком технологій та зростанням кількості кіберзлочинів, непідписні методи можуть стати все більш популярними в кібербезпеці.

Одним із типів методів, які не є похідними від сигнатур, є евристичний аналіз. Евристичний аналіз передбачає використання експертних знань і досвіду для виявлення потенційних загроз безпеці та вразливостей. Цей метод особливо

корисний у ситуаціях, коли немає відомих сигнатур або шаблонів кібератак. Покладаючись на людський досвід та інтуїцію, евристичний аналіз може виявити нові загрози, які неможливо виявити іншими методами.

Ще один метод аналізу загроз безпеці, який не ґрунтується на сигнатурах, — це аналіз поведінки. Цей підхід передбачає моніторинг поведінки користувачів і систем для виявлення аномальної активності, яка може свідчити про порушення безпеки. Аналізуючи моделі поведінки, такі як мережевий трафік або активність користувачів, аналіз на основі поведінки може виявляти нові та раніше невідомі загрози. Цей метод особливо корисний для виявлення розширених постійних загроз (APT), які часто використовують складні методи, щоб уникнути виявлення.

Штучний інтелект (AI) і машинне навчання (ML) також є методами, не заснованими на сигнатурах, які все частіше використовуються в кібербезпеці. Ці методи передбачають навчання алгоритмів для розпізнавання шаблонів і виявлення потенційних загроз на основі великих обсягів даних. На відміну від методів на основі сигнатур, AI і ML можуть виявляти нові та нові загрози, які ще не ідентифіковані. Це робить їх особливо корисними для виявлення атак нульового дня, які використовують уразливості, невідомі постачальнику програмного забезпечення. Завдяки постійному навчанню та адаптації штучний інтелект і машинне навчання можуть забезпечувати більш активний підхід до кібербезпеки, допомагаючи організаціям випереджати потенційні загрози, що розвиваються.

Використання методів, які не базуються на підписах, має свої переваги, зокрема, у гнучкості. Ці підходи не обмежені наявними шаблонами чи сигнатурами для виявлення потенційних загроз чи аномалій. Замість цього, вони проводять аналіз даних у реальному часі та виявляють будь-які відхилення від звичайної поведінки. Це забезпечує більшу адаптивність та здатність виявляти нові загрози, які можуть бути невідомі заздалегідь. Крім того, такі методи можна застосовувати в різних сферах, включаючи безпеку мережі, виявлення шахрайства та розпізнавання аномальних ситуацій.

Однак є також деякі недоліки використання методів, які не є похідними від підписів. Одним із таких недоліків є ймовірність помилкових спрацьовувань. Без попереднього підпису чи шаблону для порівняння ці методи можуть визначити нормальну поведінку як аномальну, що призведе до непотрібних сповіщень і збоїв. Крім того, ці методи можуть вимагати більше ресурсів і обчислювальної потужності для аналізу даних у режимі реального часу, що може стати проблемою для організацій з обмеженими ресурсами.

У порівнянні з методами, які базуються на підписах, переваги та недоліки використання методів, які не є похідними від підписів, стають більш очевидними. Методи на основі сигнатур покладаються на вже існуючі шаблони або сигнатури для виявлення потенційних загроз або аномалій. Хоча це може бути ефективним для виявлення відомих загроз, воно може бути не настільки ефективним для виявлення нових загроз, які не мають попереднього підпису. Крім того, методи на основі сигнатур можуть бути більш схильні до хибних негативів, оскільки вони можуть не ідентифікувати нові загрози, доки не буде розроблено сигнатуру. Зрештою, вибір методу залежатиме від конкретних потреб і ресурсів організації, а також від характеру загроз, які вони намагаються виявити.

Незважаючи на те, що поточні методи виявлення вторгнень перебувають на ранній стадії розвитку та класифікації, вони не охоплюють повну складність еволюції IDS. Основний ринок для IDS складають системи ІКТ, такі як мережеві комп’ютери у стилі настільного комп’ютера або серверні HIDS, які працюють на стандартних операційних системах на комп’ютерах, або NIDS, що прямо підключені до мереж ІКТ. У реальних умовах комерційні HIDS або NIDS зазвичай використовують різноманітні методи виявлення та запобігання вторгненням, такі як методи на основі сигнатур, аномальних та специфічних методів. Наприклад, армія США у своїй дослідницькій лабораторії розробила мережеву систему виявлення вторгнень Interrogator, яка використовує різноманітні методи виявлення в своїх мережевих сенсорах, а також має різноманітні аналітичні методи для передбачення загроз у центральній частині системи.

2.6 IDS зосередження на хостах у основній інфраструктурі.

Системи для виявлення вторгнень (IDS) є важливим компонентом для заходів безпеки будь-якої великої компанії або організації. IDS призначений для виявлення та запобігання несанкціонованому доступу до системи чи мережі. Однак IDS має певні обмеження, які можна вирішити шляхом впровадження IDS на основу хоста. IDS на основі хоста працює на окремих хостах у базовій інфраструктурі, а не відстежує лише мережевий трафік. Даний підхід може покращити виявлення вторгнень у базову інфраструктуру шляхом виявлення та блокування вторгнень на самому рівні хоста. У мережах IoT IDS можна розмістити на одному або кількох виділених хостах, що може допомогти у виявленні вторгнень. Ці виділені хости можуть відстежувати мережевий трафік і виявляти незвичайні дії, такі як спроби несанкціонованого доступу або незвичні шаблони передачі даних. Крім того, ці виділені хости також можуть використовувати алгоритми машинного навчання для виявлення шаблонів у даних, які можуть вказувати на потенційне вторгнення. Зосереджуючись на хостах базової інфраструктури, організації можуть покращити свою здатність виявляти та запобігати вторгненням, що, зрештою, може допомогти захистити їхні конфіденційні дані та критично важливі системи.

HIDS розроблено для використання на звичайних комп'ютерах та подібних пристроях, а також може бути використано на робочих станціях у мережі або на первинній шині. Важливо враховувати, що робота HIDS або центральної системи моніторингу мережі, яка збирає дані від HIDS через первинну комунікаційну шину, не має негативного впливу на доступність робочих станцій.

Зазвичай HIDS обмежені для використання на ПК або польових пристроях. По-перше, прошивка цих пристроїв не передбачена для виконання додаткового програмного забезпечення, а по-друге, їх процесори, пам'ять і канали зв'язку не призначені для додаткового навантаження. Використання HIDS на таких пристроях вимагає концептуальних змін та тестування всіх

польових пристроїв у середовищі ICS, що може призвести до значного опору у операційній системі.

Мережева IDS (NIDS) — це система IDS, яку легко інтегрувати в нові мережеві топології та вона не має значного впливу на роботу мережі. Вона відіграє важливу роль у захисті критично важливої інфраструктури, такої як транспортні системи, енергетичні та телекомунікаційні мережі, від кіберзагроз та атак. Виявляючи та сповіщаючи персонал служби безпеки про можливі вторгнення, IDS допомагає забезпечити цілісність і доступність критичної інфраструктури.

Для мереж та критичної інфраструктури існують різні типи IDS. Найпоширенішою класифікацією є системи IDS, що охоплюють від окремих комп'ютерів до обширних мереж. Passive IDS — це безпечне рішення, яке контролює трафік або мережу, не вживаючи жодних активних заходів проти вторгнень. З іншого боку, активна IDS займає активну позицію проти зловмисників, блокуючи або обмежуючи доступ до мережі. Крім того, існують IDS на основі хоста (HIDS), які відстежують діяльність на окремих комп’ютерах, і IDS на основі мережі (NIDS), які відстежують мережевий трафік. Використовуючи відповідний тип IDS, організації можуть ефективно виявляти потенційні загрози безпеці та реагувати на них.

IDS відіграє вирішальну роль у захисті критично важливої інфраструктури та мереж, тому дуже важливо мати комплексну стратегію безпеки. Тому наявність комплексної стратегії безпеки є критичною. Ця стратегія повинна включати використання IDS разом з іншими засобами безпеки, такими як брандмауери, антивірусне програмне забезпечення та системи управління інформацією та подіями безпеки (SIEM). SIEM надає консоль керування, що дозволяє персоналу займатися моніторингом стану мережі та встановленням параметрів IDS. Інтегруючи IDS у комплексну стратегію безпеки, організації забезпечують безпеку та надійність своєї критично важливої інфраструктури та мережі. Розгортання системи виявлення вторгнень (IDS) має доволі значне значення для захисту від проникнення критичної інфраструктури та мереж. Для ефективного розгортання IDS важливо

визначити пріоритетність критичних активів і даних. Критична інфраструктура відноситься до активів, систем і мереж, необхідних для підтримки безпеки, здоров'я та безпеки, а також соціального та економічного добробуту. Визначивши ці активи, організації можуть зосередити свої зусилля з безпеки на найважливіших компонентах своєї інфраструктури. Таке визначення пріоритетів може допомогти в більш ефективному розгортанні IDS, гарантуючи, що вони налаштовані для моніторингу та захисту найважливіших компонентів мережі та інфраструктури.

Після визначення критичних активів наступним кроком є налаштування IDS для мережі та критичної інфраструктури. IDS має бути налаштовано для виявлення та сповіщення про критичні вразливості, які перетинаються з цифровими активами. Систему IPS/IDS на основі штучного інтелекту можна використовувати для мереж 5G, які з'єднуватимуть критично важливу інфраструктуру, що вимагає більшої безпеки. IDS слід налаштувати для моніторингу мережевого трафіку, виявлення аномалій і сповіщення персоналу безпеки про потенційні загрози. Крім того, IDS слід налаштувати для реєстрації всіх подій і створення звітів для аналізу та дослідження.

Інтеграція IDS з іншими заходами безпеки дозволяє підвищити рівень безпеки та забезпечити повний захист критичної інфраструктури та мереж. Додаткові інструменти, наприклад, Nmap, можуть використовуватись для сканування мережі, виявлення хостів, служб та відкритих портів, що допомагає в аудиті безпеки. Важливо враховувати, що розгортання IDS для критичної інфраструктури потребує комплексного підходу, який включає ідентифікацію важливих активів, правильну настройку системи виявлення вторгнень та її інтеграцію з іншими заходами безпеки. Організація може зосередити свої зусилля на безпеці найважливіших компонентів інфраструктури, встановивши пріоритети для критично важливих активів. Настройка IDS для моніторингу мережевого трафіку, виявлення аномалій і сповіщення про потенційні загрози має вирішальне значення для забезпечення ефективної безпеки. Інтеграція системи виявлення вторгнень з іншими заходами безпеки може підвищити

рівень захисту організації та забезпечити повний захист критичної інфраструктури та мережі.

2.7 Початкове налаштування Wazuh

Wazuh - це безкоштовна платформа з відкритим вихідним кодом, яка спрямована на запобігання загрозам, виявлення їх та реагування на них. Ця система забезпечує захист робочих навантажень в різних середовищах, таких як локальні мережі, віртуальні оточення, контейнери та хмарні платформи. Wazuh користується популярністю серед різноманітних компаній, незалежно від їх розміру - від невеликих фірм до великих корпорацій. Основна мета Wazuh полягає у зборі, об'єднанні, індексації та аналізі безпекових даних, що допомагає підприємствам виявляти вторгнення, потенційні загрози та підозрілі дії.

Платформа Wazuh надає різноманітні можливості забезпечення безпеки для програм, що працюють у хмарних середовищах, контейнерах та серверних програмах. Вона включає в себе функції аналізу журналів, виявлення вторгнень та шкідливого програмного забезпечення, моніторинг цілісності файлів, оцінку конфігурацій, виявлення вразливостей та допомогу у дотриманні нормативних вимог. Архітектура Wazuh складається з трьох основних компонентів (Рисунок 2.3).

Агент Wazuh: надає можливості запобігання, виявлення та реагування, якщо встановлено на кінцевих точках, таких як ноутбуки, настільні комп’ютери, сервери, хмарні екземпляри або віртуальні машини. Він сумісний з Windows, Linux, macOS, HP-UX, Solaris і AIX.

Сервер Wazuh використовує дані, які надходять від агентів, оброблюючи їх за допомогою декодерів і правил. Він використовує ці дані для пошуку відомих ознак порушення безпеки (IOC). Якщо сервер Wazuh налаштований у вигляді кластера, один сервер може обробляти і оцінювати великий обсяг даних від сотень або тисяч агентів, що дозволяє масштабувати його роботу горизонтально.

Elastic Stack відповідає за індексацію та зберігання сповіщень від сервера Wazuh. Крім того, інтеграція між Wazuh та Kibana надає користувачам зручний інтерфейс для візуалізації та аналізу даних. Цей інтерфейс також контролює налаштування та статус сервера Wazuh, що спрощує управління та контроль за допомогою графічного інтерфейсу користувача.

Рисунок 2.3 - Компонента Wazuh

Платформа Wazuh може контролювати безагентні пристрої, такі як брандмауери, комутатори, маршрутизатори та мережеві IDS, серед іншого, на додаток до пристроїв на основі агентів. Наприклад, системи можуть використовувати Syslog для збору даних системного журналу, а його параметри можна контролювати, регулярно перевіряючи його дані. Компоненти Wazuh і потік даних показано на діаграмі нижче. Він представляє агент Wazuh, сервер Wazuh і Elastic Stack, які є трьома критичними компонентами рішення (Рисунок 2.4).

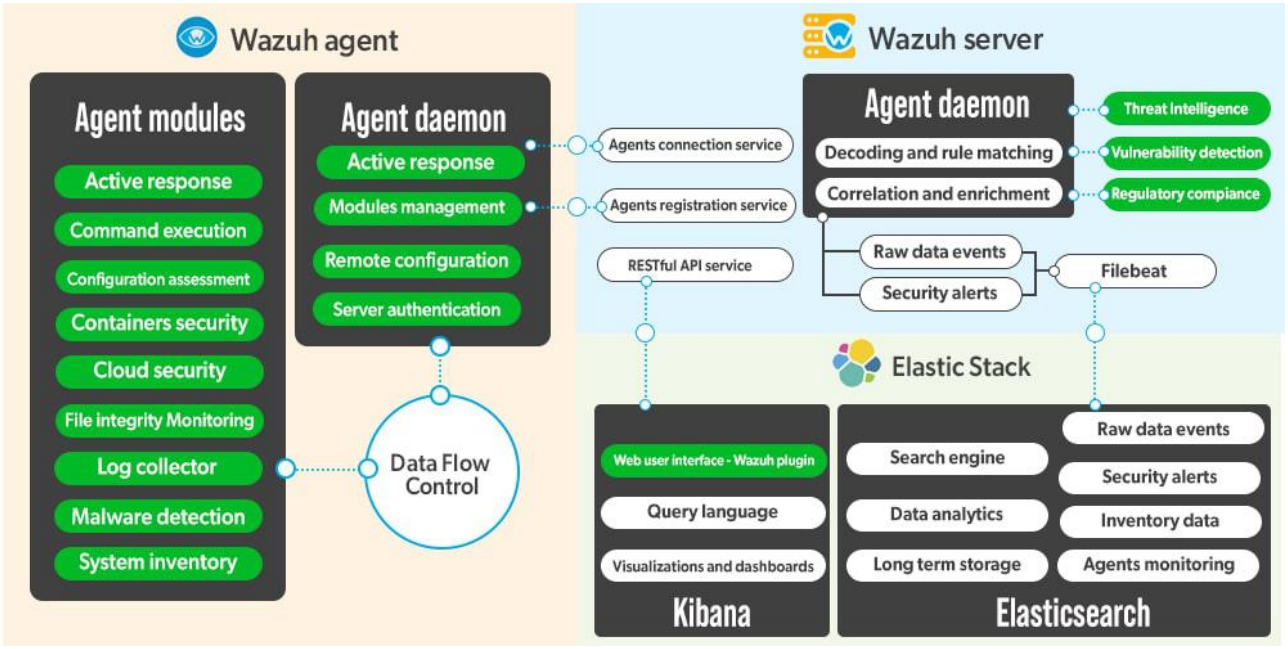


Рисунок 2.4 - більш детальні складові частини

Агенти Wazuh оцінюють безпеку систем, шукаючи зловмисне програмне забезпечення, руткіти та аномальну поведінку. Можна розпізнати приховані файли, та приховані процеси, мережеві слухачі без міток і відмінності у відповідях на системні виклики. Окрім можливостей агента, серверний компонент використовує підхід на основі сигнатур для виявлення вторгнення, аналізу записаних даних журналу та пошуку ознак компрометації за допомогою механізму регулярних виразів.

Нижче наведено деякі основні функції Wazuh:

- Виявлеє вторгнення
- Аналізує дані у журналі
- Перевіряє цілісності файлів
- Знаходить вразливості в системі
- Швидко реагує на інцидент
- Відповідає нормативним вимогам
- Моніторинг безпеки хмари та контейнера

Таким чином, Wazuh є чудовим вибором для Open Source SIEM, який є надійним, простим і може забезпечувати оперативний робочий процес безпеки для зміцнення стану безпеки.

3 МОДЕЛІ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Виявлення програм-вимагачів за допомогою Wazuh

Профілактичні дії для запобігання та виявлення атак програм-вимагачів мають вирішальне значення для безпеки системи. У цій роботі ми розглянемо, як Wazuh може допомогти у виявленні поточних атак програм-вимагачів за допомогою модуля моніторингу цілісності файлів. Останнім часом спостерігається збільшення кількості атак програм-вимагачів, націлених на різні сфери бізнесу. Ця конкретна форма зловмисного програмного забезпечення призначена для запобігання доступу до комп'ютерної системи або даних, шляхом шифрування їх до моменту здійснення викупу.

Програмне забезпечення-вимагач зазвичай передається через фішинг електронної пошти та спам (посилання на вразливі веб-сайти або зі шкідливими вкладеннями). Крім того, деякі сімейства програм-вимагачів, як-от сімейство WannaCry, використовують експлойти для зараження інших комп'ютерів у мережі, таким чином уникаючи допомоги людини для розповсюдження. Щоб уникнути зараження системи програмами-вимагачами, рекомендується оновлювати, регулярно створювати резервні копії даних і навчати кінцевих користувачів безпеці.

Модулі, які полегшують виявлення та запобігання програм-вимагачів:

- Виявлення вразливостей без опитування: ідентифікує вразливі системи та програми, пов'язуючи інформацію інвентаризації з добре відомими CVE.

- Оцінка конфігурації безпеки: використовується для оцінки погано налаштованих систем. Час від часу він перевіряє статус конфігурації щодо загальноприйнятих практик і стандартів, таких як CIS.

- Відстеження цілісності файлу: зміни файлової системи та використовуються для виявлення підозрілих файлів.

Під час нападу програма-вимагач здійснювала такі дії:

- Відкриття та аналіз даних файлів.

- Шифрує вміст і записує його в новий файл.

- Стирає вихідний файл

Оскільки моніторинг цілісності файлів Wazuh може спостерігати за додаванням, зміною та видаленням файлів у каталогах, Wazuh легко впізнає створення нового файлу та видалення вихідного файлу під час шифрування. Якщо ми отримуємо велику кількість сповіщень щодо створення та знищення файлів, ми можемо бути заражені програмою-вимагачем.

Давайте оцінимо ефективність системи моніторингу цілісності файлів Wazuh в дії. Щоб досягти цього, експерти компанії розробили скрипт на Python, який імітував би атаку програм-вимагачів. Вимоги до сценарію включають Python 3 і криптографічний пакет.

Пункт 1 Підготовка середовище тестування

1) Спочатку створимо каталог /home/vagrant/test:

-[root vagrant]# mkdir -p /home/vagrant/test

2) Далі пропишемо доручення агенту Wazuh стежити за цим каталогом:

<syscheck>

<directories check_all=”yes” whodata=”yes”>/home/vagrant/test</directories>

</syscheck>

3) За допомогою команди ми активували функцію Whodata. Це змусить агента Wazuh використовувати інтеграцію з ядром операційної системи, яка повідомлятиме про зміни файлів у режимі реального часу та надаватиме конкретну інформацію про те, хто та як ці зміни зробив.

4) Далі потрібно перезапустити агента, щоб застосувати зміни.

[root@agent01 vagrant]

5) Створюємо кілька файлів і підкаталогів у нашому боті. За замовчуванням сценарій створить 10 каталогів із 20 файлами розміром 1 КБ кожен.

-[root@agent01 vagrant]# Версія Python 3.8.1 підготовки wazuh-ransomware-poc.py.

6) Тепер ми можемо перерахувати каталоги та файли, які були створені (Рисунок 3.1).

```
drwxr-xr-x. 2 root root 4.0K Nov 28 14:27 Directory_00
drwxr-xr-x. 2 root root 4.0K Nov 28 14:27 Directory_01
drwxr-xr-x. 2 root root 4.0K Nov 28 14:27 Directory_02
drwxr-xr-x. 2 root root 4.0K Nov 28 14:27 Directory_03
drwxr-xr-x. 2 root root 4.0K Nov 28 14:27 Directory_04
drwxr-xr-x. 2 root root 4.0K Nov 28 14:27 Directory_05
drwxr-xr-x. 2 root root 4.0K Nov 28 14:27 Directory_06
drwxr-xr-x. 2 root root 4.0K Nov 28 14:27 Directory_07
drwxr-xr-x. 2 root root 4.0K Nov 28 14:27 Directory_08
drwxr-xr-x. 2 root root 4.0K Nov 28 14:27 Directory_09

/home/vagrant/test/Directory_00:
total 80K
-rw-r--r--. 1 root root 1.0K Nov 28 14:27 File_00.txt

-rw-r--r--. 1 root root 1.0K Nov 28 14:27 File_19.txt

/home/vagrant/test/Directory_01:
total 80K
-rw-r--r--. 1 root root 1.0K Nov 28 14:27 File_00.txt
```

Рисунок 3.1 - Створені каталоги та файли

В інтерфейсі Wazuh ми спостерігаємо появу нових файлів (Рисунок 3.2).

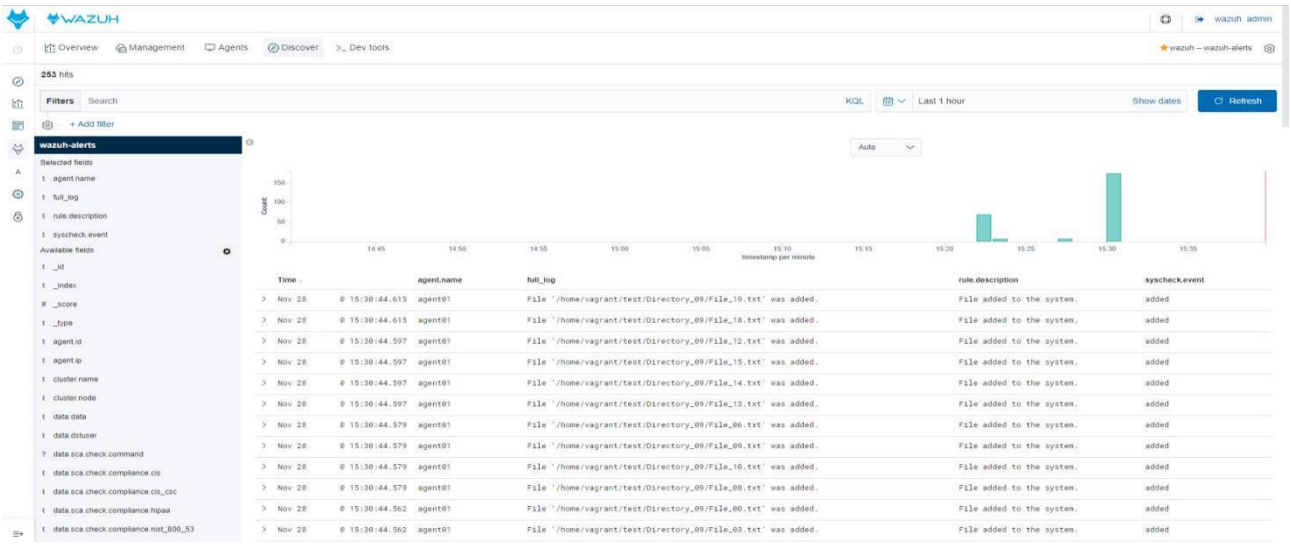


Рисунок 3.2 - каталог нових файлів в інтерфейсі Wazuh

Пункт 2: Спроба проведення атаки.

1) Почнемо нашу атаку програми-вимагача. Команда яка буде шифрувати кожен файл у /home/vagrant/test і видалить оригінальний вразі відмови від викупу:

–[root@agent01 vagrant]# python attack

2) В нашому інтерфейсі Wazuh ми спостерігаємо два сповіщення про моніторинг цілісності файлів:які були додані та видалені (Рисунок 3.3).

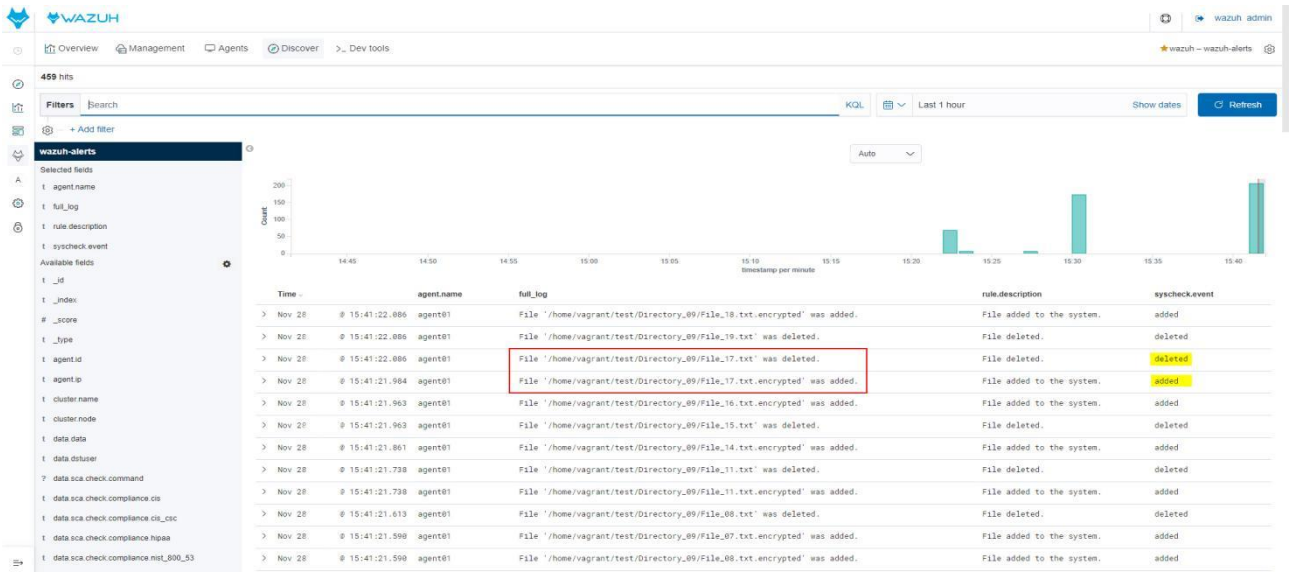


Рисунок 3.3 - Сповіщення про додавання та видалення файлів

Wazuh здатний розпізнавати атаки, викликані зараженням програмним вірусом-вимагачем, але людям які не достатньо володіють комп'ютером доволі важко розпізнати, коли відбувається атака. Щоб досягти цього, ви повинні автоматично ініціювати сповіщення, коли це відбувається. Краще використовати функцію сповіщень Open Distro (найкраща безкоштовна альтернатива Elastic Watchers із відкритим кодом).

Спочатку ми створимо інструмент, який відстежуватиме сповіщення про додавання нових файлів (фільтр: syscheck.event) (Рисунок 3.4).

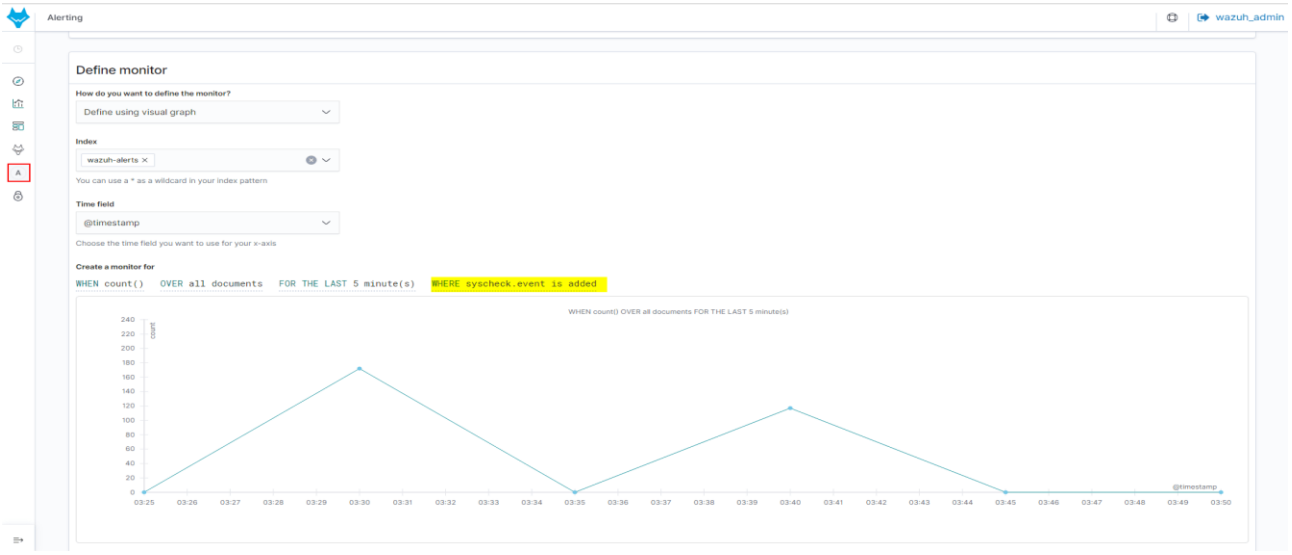


Рисунок 3.4 - Монітор сповіщень

Наступним кроком попереднього визначеного монітора ми створюємо тригер, встановлюючи умову (наприклад, понад 100) (Рисунок 3.5). Можете налаштувати даний параметр відповідно під власні потреби:

Рисунок 3.5 - Налаштування тригера сповіщення

Далі ми створюємо додатковий монітор, який буде сповіщає про видалення та зміну файлів (фільтр: виявлено подію видалення файлу) (Рисунок 3.6) і відповідний тригер. Наступного разу, коли Wazuh розпізнає цю підозрілу поведінку, на моніторах буде висвічуватись активний статус.

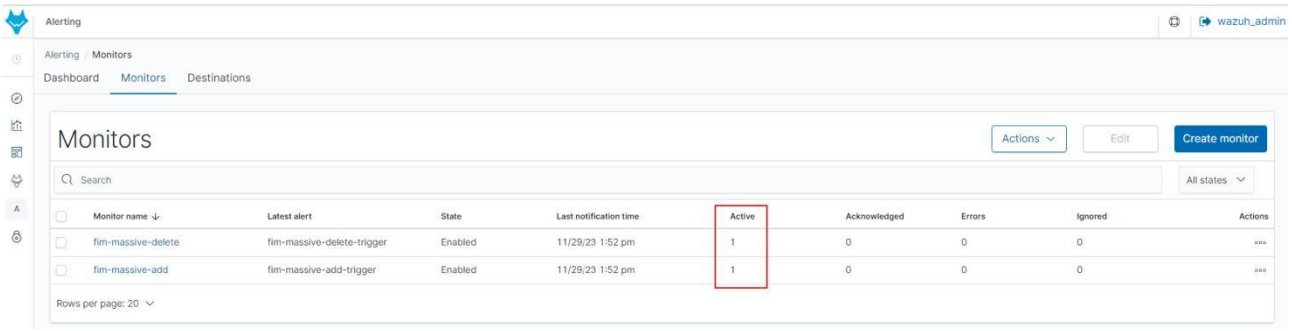


Рисунок 3.6 - Два активних монітори

3.2 Моніторинг “Голодної атаки” DHCP за допомогою Suricata та Wazuh

Вторгнення DHCP ініціюється зловмисником, який наповнює сервер DHCP великою кількістю пакетів DHCP DISCOVER, які є фальсифікованими MAC-адресами. Ця процедура вичерпує всі доступні адреси DHCP, які сервер DHCP може призначати клієнтам. Після успішного викрадення DHCP сервер DHCP не зможе надавати адреси своїм клієнтам. Динамічний DHCP-сервер характеризується пов’язаною з ним адресою, маскою, шлюзом за замовчуванням та іншою відповідною інформацією. Ця інформація призначається клієнтським пристроям. Клієнт DHCP, який зацікавлений в отриманні адреси через DHCP, робить це шляхом передачі пакетів із сервером DHCP (Рисунок 3.7). Пакети які в більшості випадків цікавлять зловмисника: Discover,Offer,Request,Acknowledgement (DORA).

Рисунок 3.7 - Процес DHCP DORA

Наступні кроки описують процедуру DHCP DORA:

1. Коли клієнт DHCP заходить у мережу, автоматично надсилається повідомлення DHCP DISCOVER, щоб знайти сервер DHCP. У повідомленні DHCP DISCOVER клієнт DHCP запитує адресу через DHCP від сервера DHCP.

2. З сервера DHCP приходить відповідь пакетом OFFER. У цьому пакеті OFFER сервер DHCP надає клієнту DHCP доступну IP-адресу.

3. Після того як клієнт DHCP отримує пакет OFFER від сервера DHCP, він в свою чергу передає DHCP-запит на сервер. У пакеті DHCP REQUEST клієнт DHCP розпізнає свій запит на призначену IP-адресу та просить DHCP-сервер надати її.

4. Зрештою сервер DHCP надсилає повідомлення ACK клієнту DHCP в мережі. Це повідомлення вказує на те, що сервер DHCP підтвердив запит клієнта DHCP на призначену адресу. Крім того, це гарантує, що клієнт має єдиний доступ до призначеної IP-адреси, і що інші клієнти не можуть зв’язатися з клієнтом DHCP через дану адресу.

Ми використовуємо Suricata та Wazuh, щоб розпізнати вторгнення DHCP на сервер DHCP.

Почнемо з установки сервера на Ubuntu.

1. Давайте встановимо клієнт DHCP на Ubuntu.

2. Потрібно змінити файл [/etc/dhcp/dhcpd.conf] і додамо конфігурації (Рисунок 3.8)

```
subnet 192.168.0.0 netmask 255.255.255.0 {
range 192.168.0.198 192.168.0.201;
option routers 192.168.0.230;
option subnet-mask 255.255.255.0;
default-lease-time 600;
max-lease-time 7200;
}
```

Рисунок 3.8 - Конфігурація

3. Далі потрібно знайти ім'я інтерфейсу Ubuntu за допомогою даного методу [$ ip a].

4. Змініть файл /etc/default/isc-dhcp-server, щоб вибрати інтерфейс, який розпізнає сервер DHCP (Рисунок 3.9).

```
# Additional options to start dhcpd with.
#       Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="<INTERFACE_NAME>"
INTERFACESv6=""
```

Рисунок 3.9 - Інтерфейс

5. Останнім кроком потрібно перезапустити DHCP.

Наступним що ми зробимо це встановимо Suricata:

1. Для спостереження за трафіком у мережі до сервера DHCP потрібно встановити Suricata ввівши наступні команд (Рисунок 3.10).

```
$ sudo add-apt-repository ppa:oisf/suricata-stable
$ sudo apt-get update
$ sudo apt-get install suricata
```

Рисунок 3.10 - Команди для вводу

2. Далі потрібно додати інтерфейс для моніторингу у конфігурацію Suricata (Рисунок 3.11)

```
af-packet:
  - interface: eth0
    # Number of receive threads. "auto" uses the number of cores
    #threads: auto
```

Рисунок 3.11 - Додавання інтерфейсу

3. Набір правил Emerging Threats Open додамо за допомогою команди: [sudo suricata-update]

4. Створимо файл /etc/suricata/ru1es/1oca1.ru1es і доповнимо ним таке правило:

[notify udp of any 68 > any 67]

5. Змінимо файл /etc/suricata/suricata.yam1 і додамо його до розділу правил. /etc/suricata/ru1es/1oca1.

6. Запускаємо Suricata.

7. Змінимо var/ossec/etc/ossec.conf у конфігурації агента Wazuh, потрібно додати наступну інформацію до блоку (Рисунок 3.12).

```
<!-- Configure Wazuh agent to collect and forward the Suricata logs to the Wazuh server for
<localfile>
  <log_format>json</log_format>
  <location>/var/log/suricata/eve.json</location>
</localfile>
```

Рисунок 3.12 - Зміна конфігурації файла Wazuh

8. Щоб зміни набули чинності - перезапустимо Wazuh

Щоб сервер Wazuh міг розпізнати атаку DHCP потрібно:

1. Зміни файл під назвою /var/ossec/etc/rules/local_rules.xml на сервері Wazuh і змінити конфігурацію на ту що нижче:

```
<group name="detect_dhcp_starvation_attack,">
  <rule id="100005" level="12">
    <if_sid>86601</if_sid>
    <match>Too many DHCP DISCOVER packets</match>
    <description> DHCP starvation attack detected.</description>
    <mitre>
      <id>T1498</id>
    </mitre>
  </rule>
</group>
```

2. Щоб зміни застосувались, перезапустіть Wazuh.

Щоб розпочати атаку на сервер DHCP в Kali прописуємо команду яка наведена нижче:

[sudo yersinia –G], повинен з’явитися інтерфейс (Рисунок 3.13).

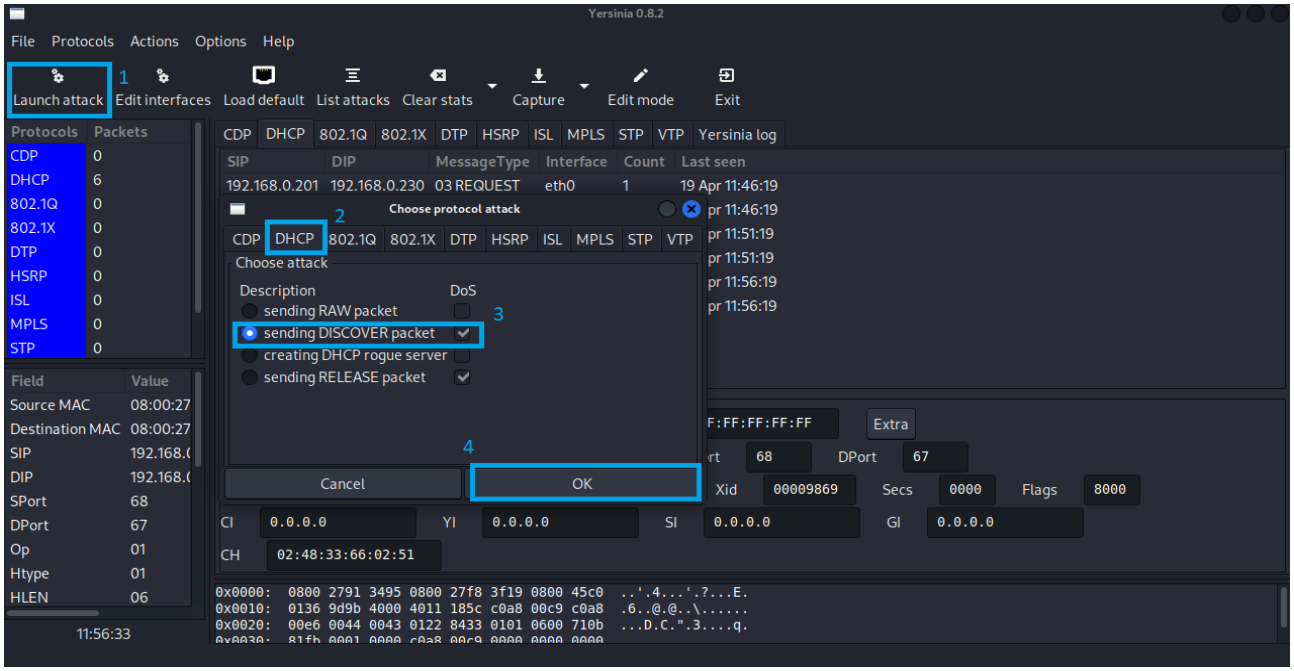


Рисунок 3.13 - Початок DHCP атаки на Yersinia

Щоб вивести сповіщення на панелі Wazuh, потрібно перейти до вкладки модулі, після чого вибрати події безпеки (Рисунок 3.14).

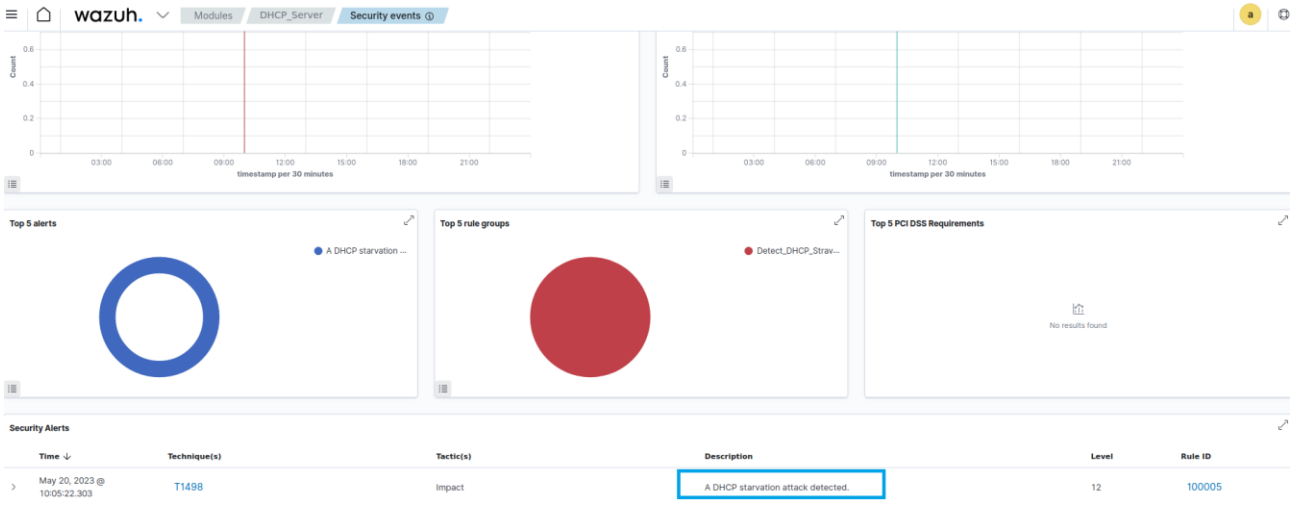


Рисунок 3.14 - Виявлення атаки DHCP

3.3 Модуль активної відповіді Wazuh.

Wazuh Active Response — це компонент, а якщо бути точніше модуль, який дозволяє групам безпеки автоматизувати відповіді на певні тригери, що

дає їм змогу ефективніше керувати інцидентами безпеки (Рисунок 3.15). Цей атрибут призначений для сприяння проактивному підходу до управління безпекою шляхом автоматичного реагування на потенційні небезпеки. За допомогою Active Response від Wazuh групи безпеки можуть визначати дії, які відбуватимуться, коли виконається певна подія, зокрема блокування певних IP-адрес або припинення процесів. Даний модуль є потужним компонентом, який допомагає організаціям покращити управління інцидентами та скоротити час реагування.

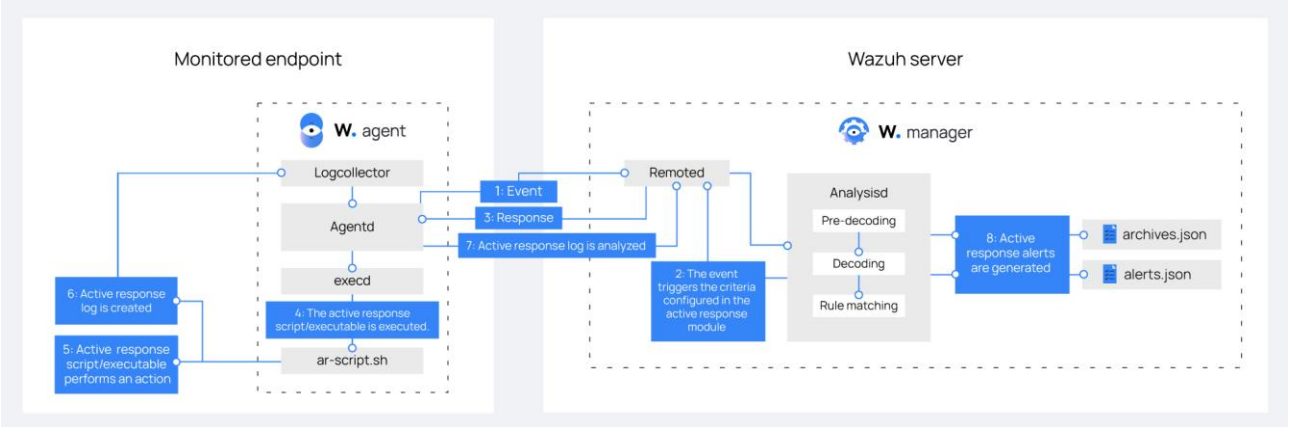


Рисунок 3.15 - Wazuh active responce

Wazuh Active Response призначений для спостереження за подіями, пов’язаними з безпекою, і вжиття попереджувальних дій, коли є певна індикація. Модуль створено за допомогою файлу ossec.conf, який описує дії, які необхідно виконати, коли відбувається конкретна подія, зв’язана з безпекою. Wazuh надає інструменти, готові до використання проти активних небезпек, таких як блокування IP-адрес або завершення процесів. Крім того, користувацькі виконувані файли можна включити в каталог активних відповідей на машинах Linux. Це підвищує гнучкість організацій у відповідь на дії та дозволяє їм конкретно реагувати на специфічні для них загрози.

Використання протоколу Wazuh Active Response має багато переваг для команд безпеки. Автоматизуючи реагування на інциденти, організації можуть скоротити час, необхідний для реагування, і покращити управління

інцидентами. Крім того, активна реакція Wazuh може допомогти зменшити наслідки інцидентів безпеки шляхом швидкого вирішення та пом’якшення небезпек. Це може сприяти зменшенню загальних витрат на інциденти та мінімальній шкоді репутації організації. Крім того, Active Response від Wazuh може сприяти більш проактивному підходу до управління безпекою, надаючи інформацію про те, як покращити безпеку. Загалом, використання Wazuh Active Response може мати значний вплив на безпеку організації та реагування на інциденти. Можна реалізувати превентивну відповідь, яка запобігає отриманню зловмисником адреси для відправки своїх атак, якщо він дотримується певного протоколу, який зберігається в Wazuh. Поговоримо для прикладу про систему вторгнення на основі SSH-Bruteforce. Беріть до уваги кількість невдалих логінів як форму спроби вторгнення. Під час цієї події активна політика «5712 – SSHD використовує грубу силу для доступу до системи». Таким чином здійснюється блокування IP-адреси.

Впровадження стратегії активного реагування Wazuh у ваш план кібербезпеки може значно підвищити здатність вашої організації розпізнавати загрози безпеці та реагувати на них своєчасно та відповідним чином. Однак перш ніж почати використовувати цей потужний ресурс, ви повинні переконатися, що ваше середовище належним чином підготовлено до його використання. Це передбачає встановлення та налаштування сервера та агентів Wazuh, а також потрібно переконатися, що архітектура вашої мережі сумісна з компонентом активної відповіді. Приділивши час правильному плануванню середовища, ви можете гарантувати, що функція Active Response Wazuh буде ефективною та матиме найбільший вплив на вашу організацію. Модуль активної відповіді можна запрограмувати на отримання конкретної відповіді на основі кількох критеріїв, включаючи ідентифікатор правила, рівень сповіщення або невелику підгрупу правил. Змінивши Active Response відповідно до конкретних вимог вашої організації, ви можете автоматизувати багато трудомістких і повторюваних завдань, пов’язаних із реагуванням на інциденти, звільняючи команду безпеки зосередитися на більш складних і важливих завданнях.

3.4 Налаштування систем моніторингу Wazuh

Минулого року від компанії Hostkey вимагали стежити за критичними файлами на сервері та їхню історією змін. Вони намагаємося знайти рішення, яке забезпечить узгоджену конфігурацію файлів на сервері та узгоджені сповіщення, коли ці файли було змінено. Вони вивчили кілька служб, які спеціалізуються на нагляді за файлами, і зрештою обрали Wazuh. Їх переконало кілька факторів:

1. Якість клієнта Wazuh. Частина яка зв’яана з клієнтом Wazuh є ресурсною та стабільною, але займає мінімум місця. Інструменти виявлення безпеки з відкритим кодом, перегляду та порівняння є важливими, але служать лише другорядною частиною програмного забезпечення. У результаті він не повинен давати велике навантаження на сервер. Якщо половина ресурсів вашого сервера спрямована на моніторинг, тоді щось працює не коректно.

2. Підтримка клієнтів. Він доступний для багатьох платформ, включаючи Windows і Linux.

3. Остаточний інтерфейс є похідним від Open Distro.

Спочатку вони хотіли знайти рішення для сімейства ОС Linux, але замість цього Wazuh став загальним підходом для всіх них.

Wazuh — це комплексна інформаційна система, ефективна на багатьох платформах. Wazuh полегшує виявлення поточних процесів, виявлення CVE, запис інцидентів тощо. Тепер ми розглянемо службу адміністрування Windows, зокрема те, як її можна підключити для спостереження за комп’ютерами з Windows. Уникнути агента Wazuh просто, все, що вам потрібно зробити, це позначити його як контролер домену. Надалі скрипт буде автоматично застосовуватися до всіх хостів. Є правила щодо Wazuh. Система Wazuh використовується для розпізнавання вторгнень, атак, помилок програмного забезпечення, проблем конфігурації, збоїв у додатках, зловмисного програмного забезпечення, руткітів і зловживань щодо безпеки чи політики. Набір правил містить зв'язок між PCI DSS v3.1 і відповідністю CIS.

Механізм моніторингу простий. Папки розташовані в різних місцях, наприклад: var/ossec/etc/shared, які потім розподіляються між хостами. Кожен файл описує процедури, які виконуються в операційних системах, є певні правила, яких необхідно дотримуватися для кожної ОС. На кожен хост переміщуються три різні документи.

Агент перевіряє файл windows.workstation.yml, який містить список значень і їх відповідні пояснення. Включаючи пропозиції щодо налаштування групових політик. Агенти полегшують перегляд конкретних даних, що стосуються перевірки. Дані перевірки розділені на три класи:

- pass – перевірка була правильною;
- fail - перевірити не вдалося;
- not applicable - не стосується.

Однією з значних проблем Wazuh була відсутність можливостей для аудиту системи Windows Server 2022. Вони вирішили цю проблему, змінивши файл sca_win_audit.yml для перевірки всіх комп'ютерів Windows. Вони змінили вміст файлу, щоб включити всі сканування, пов'язані з платформою Windows Server 2019. Коли вони вперше виконали сканування, організоване таким чином, отримали приблизно рівний розподіл класів:

- Pass – 62;
- Fail – 30;
- Not applicate – 161

Далі ми повинні вручну налаштувати політику для когорти комп'ютерів з операційною системою Windows Server 2022. Wazuh брав участь у розвитку, надаючи просте графічне представлення кожної невдалої перевірки, яка не вдалася, вони пропонували варіанти, які можна використати для вирішення проблеми, і рекомендували способи правильного виконання певної політики. Централізоване керування політикою є вигідним для адміністрування великого парку машин.

Не кожне повідомлення щодо реєстратора повинно викликати занепокоєння інженерів. Тому вони зосереджуються на моніторингу лише тих повідомлень із пріоритетом п’ять або вище. Приклад останніх подій:

Get /wazuh-alert-4.x-2022.03.15/_search&scroll-1029


```
{
 "query": {
  "bool": {
    "must":  {{
       "term":
         "rule.level":  6
        }
      }
      {
        "range": {
          "timestamp": {
            "gte": "now=6m"
         }
       }
     }
   }
  }
 }
```


Приклад відповіді:


```
{
 "_index": "wazuh-alerts-4.x-2023.12.11",
 "message": "\"An account login attempt was detected.\r\n\r\nSubject:\r\n\tSecurity ID:\t\tS-1-0-0\r\n\tAccount Name:\t\t-\r\n\tAccount Domain:\t\t-\r\n\tLogon
```

ID:\t\t0x0\r\n\r\nLogon Information:\r\n\tLogon Type:\t\t3\r\n\tRestricted Admin Mode:\t-\r\n\tVirtual Account:\t\tNo\r\n\tElevated Token:\t\tYes\r\n\r\nImpersonation Level:\t\tImpersonation\r\n\r\nNew Logon:\r\n\tSecurity ID:\t\tS-1-5-21-1234567890-1234567890-1234567890-1001\r\n\tAccount Name:\t\tUser1\r\n\tAccount Domain:\t\tEXAMPLE.COM\r\n\tLogon ID:\t\t0x1A2B3C4D\r\n\tLinked Logon ID:\t\t0x0\r\n\tNetwork Account Name:\t-\r\n\tNetwork Account Domain:\t-\r\n\tLogon GUID:\t\t{12345678-abcd-1234-efgh-1234567890ab}\r\n\r\nProcess Information:\r\n\tProcess ID:\t\t0x0\r\n\tProcess Name:\t\t-\r\n\r\nNetwork Information:\r\n\tWorkstation Name:\t-\r\n\tSource Network ... "
"version": "2"
}

Відповідь повна та має багато різної інформації, але все одно залишає відчуття дискомфорту при перегляді. Інформація, отримана з нього, повинна бути представлена в більш стислій формі та в зручному для читання форматі. Для цього розробники Wazuh створили засіб для комбінування інших продуктів. У нашому випадку це месенджер Rocket.

Журнал дій надає інформацію про події рівня підписки, які відбулися в Azure, ця інформація актуальна:

- Адміністративні дані: включають записи всіх створених, оновлених, видалених і активних ресурсів за допомогою менеджера ресурсів. Кожна дія, яку виконує користувач або програма за допомогою диспетчера ресурсів, вважається операцією над певним типом ресурсу. Такі операції, як запис, видалення або дії, передбачають запис початку та успіху чи невдачі операції в категорії «Адміністративні». Категорія «Адміністративні» включає будь-які рольові зміни інформації про підписку.

- Журнал даних сповіщень: містить журнал усіх активних сповіщень Azure. Наприклад, ми можемо отримати сповіщення, коли відсоток ЦП, який використовується однією з віртуальних машин в інфраструктурі, перевищує

певний поріг. Azure надає можливість створювати власні правила, які отримуватимуть сповіщення, коли подія відповідає правилу.

- Інформація про безпеку (або дані): ми перевіряємо журнал безпеки з центру безпеки Azure. Наприклад, журнал може включати виконання підозрілих файлів.

- Service HealthData: містить журнал усіх інцидентів працездатності служби, які сталися в Azure. Існує п’ять різних типів подій у сфері охорони здоров’я: "необхідна дія", "відновлення з допомогою", "інцидент задокументовано", "технічне обслуговування виконано", "інформація надана" або "застосовано безпеку", усі з яких записуються, коли подія відбувається на ресурсі підписки.

- Дані автомасштабування: реєструє пов’язану з подією інформацію про механізм автомасштабування відповідно до налаштувань, пов’язаних із вашою підпискою. Події автомасштабування, які відбуваються автоматично, а також успішні чи неуспішні події задокументовані в цій категорії.

- Рекомендовані дані: містить рекомендовані дії, які виконує порадник Azure.

Менеджеру Wazuh доручено реалізувати співпрацю з Microsoft Azure під час огляду служб інфраструктури. Щоб інтеграція працювала належним чином, потрібно встановити деякі компоненти.

Необхідні компоненти:

– Microsoft Azure

– Wazuh більше v3.7.0

– Python більше v2.7

– Pip

– pytz

– azure-storage-blob

Microsoft Azure. Інфраструктура Microsoft Azure є важливою. Щоб отримати доступ до інфраструктури, ми повинні мати доступ до облікових

даних, які відповідають модулям, які ми хочемо використовувати для отримання журналів.

– Wazuh v3.7.0 – інтеграція Microsoft Azure сумісна з Wazuh v.3.7.0. Якщо ви хочете оновити налаштування Wazuh, перегляньте вкладку оновлення.

– Python 2.7. Частину інтеграції було здійснено в Python, тому нам потрібно буде встановити принаймні версію 2.7 або новішу.

– Pip — це менеджер пакетів на основі Python, який інсталює всі необхідні бібліотеки та допоміжне програмне забезпечення для платформи Azure.

– Бібліотека pytz полегшує точні розрахунки часових поясів для конкретної платформи та додавання дат за місцевим часом.

– Бібліотека azure-storage-blob зменшує складність використання та доступу до вмісту Microsoft Azure Storage.

– Встановлення залежностей. Для правильного налаштування та конфігурації системи подій Microsoft Azure потрібні додаткові компоненти та модуль Wazuh.

3.5 Захист від загроз протоколу MODBUS/TCP за допомогою Wazuh-SIEM

Протокол MODBUS/TCP є популярним протоколом, який спочатку був розроблений як розширення протоколу MODBUS RTU. Це полегшує зв’язок між різними промисловими компонентами, такими як датчики, комп’ютери та виконавчі механізми в промислових умовах. Розуміння фундаментальних принципів протоколу MODBUS/TCP має важливе значення для професіоналів, які працюють у галузях, де є системи автоматизації та керування. Розуміючи фундаментальні принципи цього протоколу, професіонали можуть легко створювати та декодувати пакети MODBUS/TCP, а також ефективно керувати та контролювати промислові системи керування. Незважаючи на численні переваги протоколу MODBUS/TCP для промислових систем керування, він не

позбавлений потенційних небезпек. Деякі поширені атаки на MODBUS/TCP включають:

- Несанкціонований доступ до промислових пристроїв.

- Підробка даних або маніпуляції .

- Атаки на відмову в обслуговуванні (DoS).

Наслідки небезпеки MODBUS/TCP для промислових систем керування можуть бути серйозними, це може призвести до значних операційних проблем і дорогих простоїв. За допомогою рішень Wazuh-SIEM організації легше запобігти цим небезпекам і мінімізувати потенційні ризики для своїх систем управління. Wazuh-SIEM — це пристрій для перетворення протоколів, який перетворює ModBus RTU в Modbus TCP, він також функціонує як автономний сервер, який періодично зчитує важливу інформацію з промислових пристроїв. Це полегшує організаціям можливість ефективніше стежити за своїми промисловими системами управління та розпізнавати будь-який несанкціонований доступ, зміну даних або іншу зловмисну поведінку в режимі реального часу, це пом’якшить вплив протоколу MODBUS/TCP на їхні операції.

Будучи єдиним рішенням XDR і SIEM, Wazuh-SIEM забезпечує потужні функції захисту від атак, націлених на протокол MODBUS/TCP, цей протокол зазвичай використовується в промислових системах керування. Одним із основних атрибутів Wazuh-SIEM для захисту від загроз на основі MODBUS/TCP є його здатність відтворювати методи ATT&CK. Це полегшує організаціям розпізнавання методів, тактик і процедур (TTP), які використовують злочинці, щоб націлити свої атаки на їхні промислові комп’ютери. Деякі з головних переваг використання Wazuh-SIEM для безпеки MODBUS/TCP:

- Повна видимість подій безпеки: агрегуючи дані журналу з багатьох джерел, Wazuh-SIEM надає комплексне уявлення про вразливість організації до атак на безпеку, що дозволяє для більш ефективного виявлення та усунення потенційних загроз.

- Повна інтеграція з іншими рішеннями SIEM: Wazuh-SIEM можна поєднувати з іншими рішеннями, такими як Splunk, ArcSight і QRadar, що

дозволить організаціям скористатися наявною інфраструктурою безпеки для посилення захисту від атак. Використання протоколу Wazuh-SIEM для забезпечення безпеки протоколу MODBUS/TCP має численні переваги для організацій, які працюють у сфері промислових систем керування. Здатність платформи розпізнавати та досліджувати численні недоліки в конструкції протоколу MODBUS/TCP дозволяє групам безпеки завчасно запобігати атакам, які можуть негативно вплинути на їх критичну інфраструктуру. Крім того, повна видимість і бездоганний зв'язок з іншими рішеннями від Wazuh-SIEM дозволяють організаціям максимізувати безпеку, одночасно захищаючи свої системи керування через Інтернет.

Поєднання Wazuh-SIEM з іншими інструментами безпеки має важливе значення для комплексного підходу до захисту від загроз на основі MODBUS/TCP. Одним із прикладів такої інтеграції є додавання McAfee ePO до Wazuh-SIEM. Журнали McAfee ePO підтримують лише TCP і вимагають TLS як рівень протоколу. Іншим прикладом є інтеграція Zenarmor із Wazuh, яку можна здійснити за допомогою Syslog. Поєднуючи Wazuh-SIEM з іншими інструментами безпеки, ви можете розширити можливості вашої системи для виявлення загроз і моніторингу активності. Для того, щоб ефективно захистити протокол MODBUS/TCP за допомогою Wazuh-SIEM, слід застосовувати методи для всієї платформи. Інструмент під назвою SIEM надає повну картину будь-якого порушення безпеки шляхом поєднання інформації журналу. Деякі з найбільш ефективних методів використання Wazuh-SIEM для забезпечення безпеки в MODBUS/TCP включають:

-Постійні оновлення та оновлення платформи Wazuh-SIEM для підвищення безпеки

-Забезпечує належне налаштування та інтеграція інструментів безпеки.

-Постійно контролює та аналізує дані журналу, щоб розпізнати небезпеку.

-Реалізація ефективних політик і процедур безпеки на основі проаналізованої інформації.

-Навчання персоналу правильному використанню Wazuh-SIEM для максимізації його ефективності в захисті протоколу MODBUS/TCP

Дотримуючись цих найкращих практик, ви можете забезпечити оптимальний захист від загроз протоколу MODBUS/TCP за допомогою Wazuh-SIEM.

Переглянемо плюси та мінусипоєднання Wazuh-SIEM з MODBUS/TSP

Почнемо з плюсів:

– Підвищена безпека: Wazuh-SIEM забезпечує комплексну систему моніторингу безпеки, ефективну для запобігання атакам на основі протоколу MODBUS/TCP. Він може розпізнавати, спілкуватися та реагувати на інциденти безпеки, що підвищує безпеку промислових систем керування.

– Керування відповідністю: Wazuh-SIEM також допомагає керувати відповідністю, надаючи спеціальні звіти про інциденти, пов'язані з безпекою. Ці облікові записи можна використовувати для створення журналів аудиту, які відповідатимуть стандартам відповідності, які вимагаються різними галузевими правилами.

– Портативність: Wazuh-SIEM дуже портативний, що робить його придатним як для малих, так і для великих промислових систем. Це гарантує, що зі збільшенням розміру системи заходи безпеки можуть бути ефективно збільшені.

Мінуси:

– Продумане налаштування. Налаштування Wazuh-SIEM для захисту від загроз MODBUS/TCP є складним і трудомістким, особливо це стосується користувачів, які не мають попередніх знань про кібербезпеку.

– Інтенсивний: Wazuh-SIEM є інтенсивним, особливо для великих систем. Це може негативно вплинути на функціональність промислових комп'ютерів, які він призначений для захисту.

Загалом поєднання захисту від загроз на основі MODBUS/TCP і платформи Wazuh-SIEM забезпечує суттєву перевагу, як-от підвищення безпеки, нагляду та масштабованості. Однак його складне налаштування та високе споживання ресурсів можуть призвести до проблем. Ці проблеми можна подолати, звернувшись за професійною допомогою щодо налаштування та оптимізації системи для ефективної роботи. Як результат, рішення про використання Wazuh-SIEM має враховувати як переваги, так і проблеми.

ВИСНОВОК

В кваліфікованій роботі розглянуто аналіз сучасного стану мережевих протоколів, зосередженого на дослідженні протоколу Modbus та загроз безпеці, які його стосуються.

Обґрунтовано вибір теми через актуальність забезпечення безпеки в мережевому середовищі.

Виконано аналіз існуючих SIEM систем, чим обґрунтовано вибір системи Wazuh для підвищення рівня безпеки.

Детально розглянуто та досліджено процеси налаштування системи виявлення вторгнень та аналізу системи запобігання вторгненням.

Побудовано модель виявлення програм-вимагачів та модель атаки на протокол DHCP за допомогою систем Suricata та Wazuh.

Досліджено протокол Modbus для мереж та проведено аналіз загроз безпеки для комп’ютерних мереж. Проведено аналіз кібербезпеки в контексті використання технологій MODBUS/TCP і системи Wazuh.

Був проведений Моніторинг “Голодної атаки” DHCP за допомогою Suricata та Wazuh, де було продемонстровано саму атаку та сповіщення в клієнті Wazuh.

СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ

1. Nivethan J. Dynamic Rule Generation for SCADA Intrusion Detection / J. Nivethan, M. Papa. – 2016. – С. 6.
2. Langill J. T. Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems / Joel Thomas Langill., 2015. – 438 с.
3. Diaz J. Using SNORT® for intrusion detection in MODBUS TCP/IP communications / Javier Diaz., 2011. – 25 с.
4. Supervisory Control and Data Acquisition (SCADA) Systems : дис. канд. техн. наук / ., 2004. – 76 с.
5. SIEM for ICS/SCADA environments [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://resources.infosecinstitute.com/topic/siem-for-ics-scada-environments/.
6. Chokalingam A. SCADA Network Security Monitoring [Електронний ресурс] / Ashok Chokalingam. – 2017. – Режим доступу до ресурсу: https://logrhythm.com/blog/scada-network-security-monitoring/.
7. Gao Y. SIEM: Policy-based Monitoring of SCADA Systems / Y. Gao, X. Xie., 2016. – 12 с.
8. SCADA: Supervisory Control and Data Acquisition, 2009. – 204 с.
9. Knapp E. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid and SCADA / Eric D. Knapp., 2011. – 360 с.
10. Radvanovsky R. Handbook of SCADA/control Systems Security / R. Radvanovsky, J. Brodsky., 2016. – 432 с.
11. Industrial automation PLC, control panels, SCADA, engineering, 2012. – 100 с.
12. Wazuh Inc. Documentation Wazuh, User manual. URL: https://documentation.wazuh.com/current/user-manual/index.html
13. Wazuh Inc. Documentation Wazuh, Getting started, Components. URL: https://documentation.wazuh.com/current/getting-started/components/index.html
14. Wazuh Inc. Active Response. URL: https://documentation.wazuh.com/current/usermanual/capabilitiesresponse/index.html

ДОДАТОК А

Копії публікацій

ЗАХІДНОУКРАЇНСЬКИЙНАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТЕФАНИКА
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ
НАЦІОНАЛЬНИЙ ТРАНСПОРТНИЙ УНІВЕРСИТЕТ
НАДВІРНЯНСЬКИЙ КОЛЕДЖ НТУ
ГАЛИЦЬКИЙ КОЛЕДЖ ІМ. В. ЧОРНОВОЛА

Проблемно-наукова міжгалузева конференція

АВТОМАТИЗАЦІЯ ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ

(АКІТ – 2023)

23—25 лютого 2023 року

Тернопіль

АВТОМАТИЗАЦІЯ ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ

Збірник матеріалів проблемно-наукової міжгалузевої конференції «Автоматизація та комп'ютерно-інтегровані технології» (АКІТ - 2023), Тернопіль, 2023. -178 с.

Адреса редакції:
Західноукраїнський національний університет
кафедра спеціалізованих комп'ютерних систем
вул. Олени Теліги 8, м. Тернопіль 46003

Контактний телефон
тел. (0352) 50-17-87

УДК 004

Лаута Р.С

Західноукраїнський національний університет

ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗА ДОПОМОГОЮ WAZUH

Вступ. Шкідливе програмне забезпечення (ПЗ) є однією з найбільш серйозних загроз для користувачів і організацій у сучасному цифровому світі. Воно може викликати значні фінансові збитки, порушити приватність, викрасти чутливу інформацію або навіть спричинити великі системні відмови. Розповсюдження шкідливого ПЗ набуває все більшої складності і розмаїтості, тому необхідно розвивати ефективні методи його виявлення та захисту.

Мета: Дослідження та аналіз методу виявлення шкідливого ПЗ за допомогою системи Wazuh.

1. Існуючі методи виявлення шкідливого ПЗ

1.1 Шкідливе програмне забезпечення і методи його виявлення

Шкідливе програмне забезпечення (ПЗ) становить серйозну загрозу для безпеки і приватності користувачів і організацій. Воно може включати такі типи загроз, як віруси, черви, троянські коні, рекламне ПЗ, шпигунське ПЗ та інші. Існує багато методів виявлення шкідливого ПЗ, включаючи сигнатурний аналіз, аналіз поведінки, евристичний аналіз, машинне навчання та інші підходи [1].

1.2 Існуючі рішення для виявлення шкідливого ПЗ

На ринку існує багато рішень для виявлення шкідливого ПЗ, таких як антивірусні програми, файрволи, системи виявлення вторгнень (IDS) та системи виявлення вразливостей (VDS). Кожен з цих інструментів має свої переваги і обмеження. Антивірусні програми, наприклад, зазвичай використовують сигнатури для виявлення відомих шкідливих програм, але можуть бути неефективними проти нових атак. IDS та VDS спрямовані на виявлення аномальних дій у системі, але можуть вимагати складної настройки і потребувати великої кількості ресурсів [2].

1.3 Переваги використання системи Wazuh для виявлення шкідливого ПЗ

Система Wazuh [3] є потужним інструментом для виявлення шкідливого ПЗ. Вона комбінує різні методи виявлення, включаючи:

- сигнатурний аналіз;
- аналіз поведінки;
- машинне навчання

Ці методи дозволяють ефективно виявляти різні типи шкідливих програм. Основні переваги використання системи Wazuh включають:

- Відкритість та гнучкість: Wazuh є відкритою платформою, що дозволяє користувачам налаштовувати його під їхні потреби. Вона також підтримує інтеграцію з іншими інструментами безпеки, що розширює його функціональні можливості.
- Централізований моніторинг: Wazuh забезпечує централізований моніторинг безпеки в реальному часі. Він агрегує дані з різних джерел, таких як

лог-файли, системні події та мережевий трафік, для виявлення потенційних загроз.

- Аналіз поведінки: Wazuh використовує аналіз поведінки для виявлення аномальних дій у системі. Він аналізує активності процесів, з'єднань мережі та інших параметрів для ідентифікації потенційно шкідливих дій.
- Машинне навчання: Wazuh використовує методи машинного навчання для виявлення нових та невідомих загроз. Він навчається на основі історичних даних та виявляє залежності та шаблони, що можуть вказувати на наявність шкідливого ПЗ.

Окрім того, Wazuh містить більше 1000 правил детекції, що допоможуть виявити багато типів загроз, включаючи віруси, троянські програми, шпигунське ПЗ та інші. Крім того, Wazuh може стежити за конфігурацією пристроїв, щоб уникнути вразливостей, пов'язаних з неправильною настройкою.

Wazuh має інтуїтивно зрозумілий інтерфейс, який дозволяє легко переглядати та аналізувати дані. Крім того, використовуючи Wazuh, ви можете створювати власні правила детекції та налаштовувати сповіщення про потенційні загрози. Наприклад, ви можете налаштувати сповіщення про підозрілі дії на вашому сервері або сповіщення про зміни в конфігурації вашого пристрою.

У цьому розділі ми оглянули літературу щодо виявлення шкідливого ПЗ та існуючі рішення. Також були наведені переваги використання системи Wazuh для цієї мети. У наступних розділах ми більш детально розглянемо архітектуру та роботу Wazuh, а також проведемо експериментальну частину для оцінки його ефективності у виявленні шкідливого ПЗ.

2. **Архітектура та робота системи Wazuh**

2.1 Архітектура системи Wazuh

Система Wazuh має розподілену архітектуру, що дозволяє їй працювати ефективно в розподілених середовищах. Архітектура системи Wazuh наведена на рисунку 1.

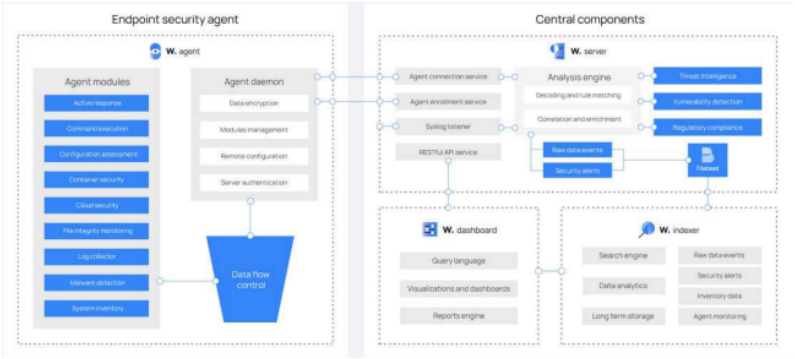


Рисунок 1 - Архітектура системи Wazuh

До основних компонентів системи включають:

- Wazuh Manager: Центральний компонент системи, який відповідає за керування, збір і аналіз даних безпеки. Wazuh Manager забезпечує централізоване керування всіма агентами та координацію роботи системи.
- Wazuh Agents: Агенти встановлюються на машинах, які підлягають

моніторингу. Вони забезпечують збір та надсилання даних безпеки до Wazuh Manager. Кожен агент відповідає за моніторинг своєї системи та надсилання зібраних даних.

- Wazuh Ruleset: Це набір правил, які використовуються для виявлення шкідливого ПЗ. Правила включають сигнатури, правила аналізу поведінки, використання машинного навчання та інші методи виявлення.
- Wazuh API: API (інтерфейс програмування додатків) дозволяє взаємодіяти з системою Wazuh та отримувати дані безпеки через програмні інтерфейси. Це дає можливість розширити функціональність системи або інтегрувати її з іншими інструментами.

2.2 Робота системи Wazuh

Після налаштування системи Wazuh і встановлення агентів на відповідних машинах, процес моніторингу безпеки розпочинається. Агенти починають збирати дані безпеки, такі як лог-файли, системні події, мережевий трафік та інші. Зібрані дані надсилаються до Wazuh Manager для подальшої обробки та аналізу.

Wazuh Manager отримує дані від агентів і застосовує правила з набору правил (Wazuh Ruleset) для виявлення потенційно шкідливих дій. Якщо будь-яка загроза виявляється, Wazuh Manager сповіщає про це відповідних операторів або адміністраторів безпеки через різні канали сповіщень, такі як електронна пошта, SMS-повідомлення або систему моніторингу подій.

Крім виявлення загроз, Wazuh також забезпечує можливості аналізу лог-файлів, аудиту системи, моніторингу цілісності файлів, виявлення вразливостей та багато іншого. Ці функції допомагають підтримувати безпеку системи на високому рівні та вчасно реагувати на потенційні загрози.

Висновок. У даній роботі були розглянуті існуючі методи виявлення шкідливого ПЗ і представлені різні підходи до виявлення таких загроз. Серед них сигнатурний аналіз, аналіз поведінки, евристичний аналіз та машинне навчання. Для виявлення шкідливого ПЗ було оглянуто різні рішення, такі як антивірусні програми, файрволи, системи виявлення вторгнень та системи виявлення вразливостей. Кожен з цих інструментів має свої переваги і обмеження.

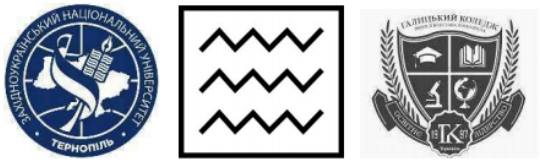
Особлива увага була приділена системі Wazuh, яка є потужним інструментом для виявлення шкідливого ПЗ. Вона комбінує різні методи виявлення, включаючи сигнатурний аналіз, аналіз поведінки та машинне навчання, що дозволяє ефективно виявляти різні типи шкідливих програм. Wazuh має такі переваги, як відкритість та гнучкість, централізований моніторинг, аналіз поведінки, машинне навчання та багато інших функціональних можливостей.

Перелік використаних джерел.

1. Козачок В.А., Гайдур Г.І., Гахов С.О., Хмелевський Р.М., Чумак Н.С. Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів – Київ: ДУТ ННІЗІ, 2020. – 167 с.

2. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с

3. Wazuh. Components.- [Електронний ркcурс].- Режим доступу: https://documentation.wazuh.com/current/getting-started/components/index.html



ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ
ГАЛИЦЬКИЙ ФАХОВИЙ КОЛЕДЖ ІМ. В. ЧОРНОВОЛА

КІБЕРБЕЗПЕКА ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ (КБКІТ – 2023)

науково-практична конференція
молодих вчених, аспірантів та студентів

29–31 серпня 2023
Тернопіль

Збірник матеріалів науково-практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ - 2023), Тернопіль, 2023. - 234 с.

Редактор коректор: Гуменний П.В.
Технічний редактор: Давлетова А.Я.

Адреса редакції:
Західноукраїнський національний університет, кафедра кібербезпеки,
вул. Олени Теліги 8, м. Тернопіль 46003
Контактний телефон: (0352) 50-17-87
e-mail: kb.tneu@gmail.com

УДК 004.056(477)

***Лаута Р.С.*[1]**

Західноукраїнський національний університет[1]

ПІДВИЩЕННЯ СТІЙКОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ З ВИКОРИСТАННЯМ SIEM СИСТЕМИ WAZUH

Вступ. Зростання загроз та атак в сучасному цифровому середовищі наголошує на важливості ефективного захисту корпоративних мереж та даних. У цій роботі проведено аналіз сучасних загроз безпеці інформації, існуючих векторів атак та вразливостей. Досліджено основні принципи роботи та можливості SIEM-системи Wazuh у виявленні, моніторингу та реагування на події, пов'язані з потенційними загрозами безпеці. Визначено ключові переваги використання Wazuh у порівнянні з іншими системами моніторингу безпеки. Для досягнення цілей роботи розроблено та запропоновано стратегії підвищення стійкості інформаційної безпеки на основі впровадження Wazuh. Ці стратегії включають в себе оптимізацію конфігурації системи, підвищення ефективності аналізу подій, розробку проактивних заходів захисту та планування реагування на потенційні загрози.

Мета: дослідження та вдосконалення стійкості інформаційної безпеки в організаціях шляхом впровадження системи управління подіями захисту інформації (SIEM) Wazuh. Зростання загроз та атак в сучасному цифровому середовищі наголошує на важливості ефективного захисту корпоративних мереж та даних.

1 Сучасний стан мережевих протоколів

Інформаційні технології увійшли в наше повсякденне життя. Зараз важко назвати галузь людської діяльності, в якій вони не відігравали б суттєвої ролі. Звичайно, вони не оминули критичні компоненти інфраструктури, такі як енергетика, водопостачання, транспорт та інші. Загалом, ці складні системи мають поєднання технологічних і людських компонентів. Логіка розвитку інфраструктури зумовила необхідність удосконалення управління її об'єктами, перш за все механізація процесу, потім автоматизація технологічних процесів, які лежать в основі функціонування об'єкта. Стрімкий розвиток інформаційних технологій, комп'ютерів та інформаційних систем призвів до створення єдиної системи забезпечення роботи в режимі реального часу шляхом збору, обробки, зберігання та відображення інформації про об'єкт контролю або управління – SCADA (Supervisory Control And Data).

Системи SCADA поширені у всіх галузях економіки, де необхідний операторський контроль за технологічними процесами в режимі реального часу. Система SCADA[1] складається з наступних компонентів:

- Периферійні датчики;
- Людино-машинний інтерфейс (HMI, англ. The English Human Machine Interface);
- Логічна система контролю;
- База даних реального часу;

- Генератор звіту.
- Зовнішні інтерфейси;
- Головна диспетчерська система (головний термінал) (MTU Master Terminal Unit);
- Абонентський кінцевий пристрій (дистанційний термінал) (RTU);
- Програмований логічний контролер (PLC);
- Комунікаційна інфраструктура (англомовна комунікаційна система CS)

Ця розвинута система, яка складається з компонентів, які працюють на цифровій основі, дозволяє природним чином інтегрувати систему в загальну систему управління та підвищує ефективність інфраструктури, особливо критичної. Системи, які використовують ресурси енергетичного сектору, передбачають збір інформації через RTU, надсилання її назад у центральне розташування, виконання необхідного аналізу та контролю, а потім відображення інформації на HMI. Протокол зв'язку SCADA є універсальним стандартом для представлення даних і передачі їх по каналу зв'язку на основі принципу «головний/підлеглий». IEC60870-5-104 і DNP3 є найпопулярнішими протоколами зв'язку в енергетиці. Іншим широко використовуваним протоколом для SCADA є Modbus. У багатьох галузях промисловості використовується Modbus, зокрема водопровідні та очисні споруди.

2. Критичність інфраструктури та рівень ризику, який вона несе.

Щоб підвищити безпеку будь-якої системи та ефективно захистити її, важливо розуміти ризик, пов'язаний із потенційними збоями комп'ютера та зв'язку в його інфраструктурі. Експерти з кібербезпеки часто класифікують три типи несправностей:

Порушення конфіденційності, тобто нездатність зберегти конфіденційну інформацію системи від несанкціонованого розголошення.

Втрата доступності, тобто нездатність забезпечити постійний доступ до системи інформацію тим користувачам або машинам, які є законними одержувачами.

Порушення цілісності, що є порушенням захисту даних системи від несанкціонованого доступу. Як наслідок, вигідним визначенням кіберризику є можливість виникнення будь-якого з цих режимів збою та їхні відповідні наслідки. У ICS, які контролюють фабрики, ці ефекти можуть проникати у фізичну сферу. Ризик є найбільш визнаним і, можливо, найбільш дослідженим прикладом у більшому класі показників кібербезпеки.

Повністю захищена комп'ютерна система не мала б слабких місць і взагалі не була б вразливою. Однак, як часто жартують з цього приводу експерти з безпеки, комп'ютерна система за своєю природою є ізольованою та ніким ніколи не використовується. Це демонструє важливість. Навіть якщо всі апаратні, програмні та мережеві небезпеки успішно запобігти, користувачі системи все ще залишаються людьми та можуть виконувати навмисні чи випадкові дії, які можуть руйнувати роботу. Внутрішня загроза, пов'язана з людьми, не може бути повністю усунена з жодної комп'ютерної системи з користувачами. Зважаючи на це, ми погоджуємося з передумовою, що реальна комп'ютерна система завжди піддається загрозі, незалежно від технічних або фізичних обмежень, які

розглядаються.

Це, звичайно, стосується комп'ютерів, які є частиною ICS, які використовуються для автоматизації та регулювання критичних процесів у промислових умовах. Насправді системи ICS зазвичай мають більше технічних і фізичних проблем, ніж комп'ютери, просто тому, що сучасні комп'ютери зазвичай розроблені з урахуванням безпеки.

3.Початок систем виявлення вторгнень

Якщо вразливість комп'ютерної системи, яку можна використовувати, завжди присутня, як забезпечити її безпеку? Ранні концепції були призначені для спостереження за обліковими записами, які вже існували (для мейнфрейму IBM System Management Facility [SMF]), і проведення аналітичних тестів цих даних для виявлення незвичайних моделей. Цю спробу часто вважають першим IDS. Концепція полягає в тому, щоб поширювати інформацію про аномальні шаблони як засіб моніторингу безпеки людини з розрахунком, що більшість позначених шаблонів не будуть шкідливою поведінкою. Пізніше Деннінг (1987) розширив цю ідею IDS, використовуючи більш складну модель і більший набір процесів (для того самого мейнфрейму IBM SMF), які були розроблені в SRI International кілька років тому.Важливо зазначити, що вразливі місця та небезпеки, пов'язані з цими ранніми комп'ютерами, значно відрізнялися від тих, які були пов'язані з іншими комп'ютерами більшості систем ІКТ, які зараз використовуються. Технічні навички користувача комп'ютера значно підвищилися. Графічний інтерфейс і комп'ютерна миша не були поширеними в цих пристроях.

Висновок: У цій роботі були досліджені та проаналізовані ключові аспекти сучасного стану мережевих протоколів, критичність інфраструктури та ризики, пов'язані з їхнім функціонуванням, а також етапи впровадження систем виявлення вторгнень для забезпечення безпеки цих систем. Аналіз сучасного стану мережевих протоколів відображає їхню еволюцію та важливість у сучасних інформаційних системах. Висвітлення основних протоколів, їхніх переваг та обмежень, дозволяє краще розуміти сучасні тенденції в мережевій безпеці та сприяє розвитку ефективних заходів захисту. Критичність інфраструктури в сучасному світі є важливою проблемою з точки зору безпеки. Оскільки багато сфер життєдіяльності підпорядковані цій інфраструктурі, виявлення, оцінка та управління ризиками стають надзвичайно важливими для забезпечення безперебійного функціонування систем.

Перелік використаних джерел:

1. Rajamäki J. A Redundant Communications Model for Critical Infrastructure Protection and Supervisory Control and Data Acquisition (SCADA) System / J. Rajamäki, J. Ahokas. – 2016. – С. 7.

2. Джинг Лю. Янг Сяо. «Огляд стандарту безпеки даних платіжних карток» // [Електронний ресурс] – Режим доступу: https://ieeexplore.ieee.org/document/5455788

3. «Що потрібно знати про відповідність стандартам PCI DSS: Витрати та контрольний список у Великобританії» // [Електронний ресурс] – Режим доступу: https://storekit.com/payments/pci-dss/