УДК 004.421

Євген СЕГЕДА, Аліна ДАВЛЕТОВА

Західноукраїнський національний університет

КОМБІНОВАНА СИСТЕМА МОНІТОРИНГУ ТА ВИЯВЛЕННЯ MALWARE-ЗАГРОЗ

Вступ. На інформаційну інфраструктуру сучасних організацій постійний вплив мають складні та варіативні кіберзагрози. Традиційні методи захисту, що базуються на сигнатурному аналізі, не завжди забезпечують ефективне виявлення шкідливого програмного забезпечення (ШПЗ), яке може порушувати конфіденційність, цілісність та доступність корпоративних мереж і кінцевих вузлів. Для підвищення точності виявлення загроз необхідно застосовувати комплексні підходи, що інтегрують локальний контроль цілісності файлів, аналіз поведінки процесів та використання зовнішніх аналітичних джерел для верифікації та класифікації підозрілих артефактів.

Управління безпекою інформаційних систем передбачає не лише моніторинг подій, але й автоматизоване реагування на інциденти та мінімізацію ризиків компрометації активів. Для підвищення ефективності управління безпекою необхідна інтеграція локальних і віддалених джерел інформації, застосування алгоритмічних методів класифікації подій та механізмів автоматичного оновлення індикаторів компрометації, що дозволяє швидко і точно реагувати на загрози та підтримувати високий рівень захисту кінцевих вузлів.

Мета дослідження полягає у дослідженні та розробці комбінованої архітектури системи виявлення загроз що інтегрує локальні механізми моніторингу та аналізу кінцевих вузлів з віддаленим аналітичним сервісом для автоматизованого формування та оновлення індикаторів компрометації.

1. Дослідження інструментів виявлення загроз

Системи виявлення ШПЗ потребують використання сучасних інструментів, які забезпечують комплексний аналіз подій безпеки та контроль цілісності систем. Одним із таких інструментів є Wazuh [1]. Це платформа для моніторингу безпеки кінцевих вузлів та аналізу логів, що забезпечує виявлення загроз, контроль цілісності файлів, аудит конфігурацій та реагування на інциденти безпеки.

Платформа поєднує локальні засоби контролю з централізованим аналізом подій, що дозволяє ефективно управляти безпекою великих мережевих інфраструктур. Основні можливості Wazuh:

– File Integrity Monitoring (FIM) – контроль цілісності файлів та системних об'єктів;

– механізми створення правил;

– поведінковий аналіз процесів та активностей користувачів;

– YARA-сканування для виявлення відомих сигнатур Ш ПЗ;

– Active Response – автоматичне реагування на інциденти, напркилад, блокування, карантин, видалення загроз;

– централізований збір і аналіз логів з можливістю інтеграції з SIEM-системами.

Wazuh підтримує інтеграцію з різними операційними системами, Linux, Windows та macOS, та дозволяє налаштовувати правила і політики безпеки відповідно до потреб конкретної організації. Завдяки цьому Wazuh може виконувати багаторівневий аналіз подій безпеки, виявляючи як відомі загрози за сигнатурами, так і аномальні поведінкові патерни. Водночас, її ефективність обмежується здатністю самостійно виявляти нові, ще невідомі загрози, що потребує підключення зовнішніх аналітичних ресурсів.

Такою зовнішньою аналітичною системою є сервіс VirusTotal [2], який надає глобальну репутаційну інформацію про файли, URL-адреси, домени та IP-адреси. Основні можливості:

– аналіз файлів і URL-адрес понад 70 антивірусними движками;
– надання репутаційних даних про файли, домени та IP-Адреси;
– пошук індикаторів компрометації (IoC) для підозрілих об'єктів;
– API для інтеграції з локальними системами безпеки та автоматизації перевірок.

Сервіс має відкритий API, що дозволяє інтегрувати його з локальними системами моніторингу, автоматизуючи процес перевірки підозрілих файлів та об'єктів мережі. Основними обмеженнями VirusTotal є залежність від доступу до Інтернету та обмеження безкоштовної версії щодо кількості запитів, а також обмежена здатність виявляти абсолютно нові загрози, відсутні в базах репутаційних даних.

Інтеграція Wazuh та VirusTotal [3, 4] забезпечує багаторівневу модель виявлення ШПЗ, у якій локальне виявлення та реагування доповнюються глобальним репутаційним аналізом. Такий підхід підвищує точність і швидкість виявлення загроз, зменшує кількість хибнопозитивних спрацювань та створює передумови для автоматизованого доповнення індикаторів компрометації у процесі управління безпекою інформаційної інфраструктури.

2. Архітектура системи виявлення ШПЗ

Поєднання досліджених інструментів дозволить підвищити точність виявлення загроз, скоротити час реагування на інциденти та автоматизувати доповнення індикаторів компрометації, що, у свою чергу, забезпечує більш ефективний захист кінцевих вузлів мережі від відомих і потенційних загроз. Запропонована система складається з таких основних компонентів:

– Wazuh Agent - встановлюється на кінцеві вузли, здійснює моніторинг цілісності файлів, збір логів і виконання реакційних дій;
– Wazuh Manager - централізований сервер кореляції подій, аналізу правил та генерації сповіщень;
– Wazuh Integrator - модуль, що забезпечує обмін даними з зовнішніми API, зокрема з сервісом VirusTotal;
– VirusTotal API - онлайн-сервіс, який агрегує результати перевірки файлів антивірусними рушіями, для класифікації загроз та репутаційного аналізу.

Взаємодія компонентів може бути реалізована за схемою, що наведена на рисунку 1.

Active Response – механізм Wazuh, що автоматично реагує на загрози: карантин, ізоляція або видалення заражених файлів/процесів.

SIEM / SOC – система централізованого збору логів і управління інцидентами безпеки де відбувається логування подій та створення інцидентів для аналітики та реагування.

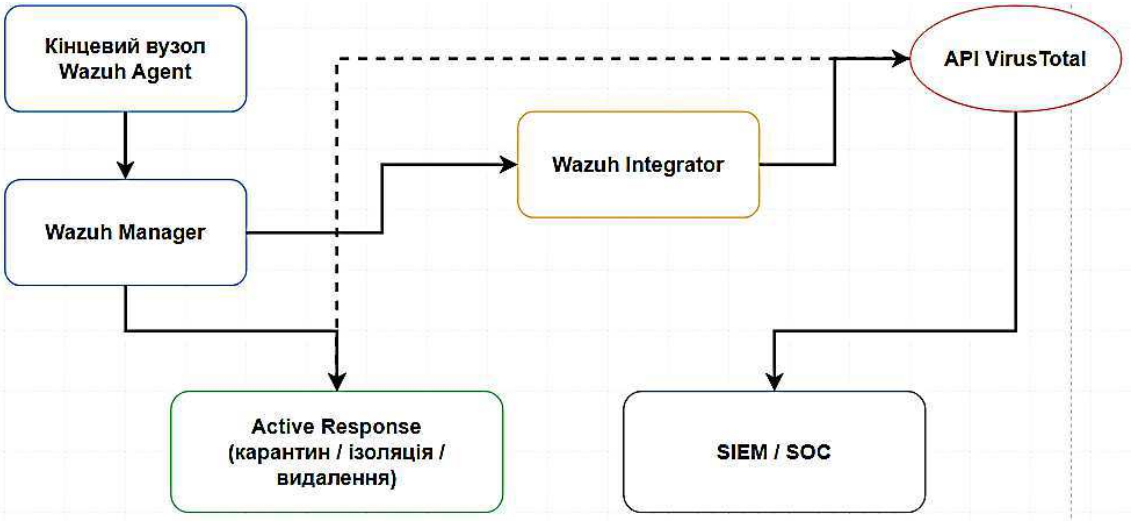

Рисунок 1 - Основні етапи обміну даними між компонентами системи виявлення ШПЗ на основі Wazuh та VirusTotal

На рисунку 1 пунктир позначає логічний зв'язок між результатом аналітики VirusTotal та активацією дій модуля Active Response, який реалізується через Wazuh Manager. Це означає, що інформація з VirusTotal може опосередковано впливати на активні дії, але не є прямою командою на реагування.

3. Алгоритм функціонування системи виявлення шкідливого ПЗ

1. Моніторинг змін. Wazuh Agent здійснює безперервне відстеження змін у системних і користувацьких каталогах. При появі нового або модифікованого файлу обчислюються його контрольні суми (MD5, SHA1, SHA256), які разом із метаданими (шлях, користувач, час, процес-ініціатор) передаються на Wazuh Manager.

2. Локальний аналіз. Змінені файли проходять попередню перевірку за допомогою Wazuh Manager, що містить сигнатури відомих загроз. Паралельно активуються поведінкові правила Wazuh, які виявляють аномальні дії, наприклад, спроби самозапуску, виконання коду з тимчасових каталогів чи звернення до підозрілих мережевих адрес.

3. Інтеграція з VirusTotal. Якщо локальний аналіз визначає файл як потенційно шкідливий, його хеш передається через Wazuh Integrator до VirusTotal API. Отримана відповідь містить оцінку кількості антивірусних рушіїв, що класифікували файл як шкідливий, тип виявленого сімейства та метадані попередніх перевірок.

4. Валідація та кореляція результатів.Wazuh Manager порівнює локальні результати із даними VirusTotal. Якщо кількість підтверджень шкідливості перевищує встановлений поріг (наприклад, 5 або 10 рушіїв), файл класифікується як загроза.

5. Автоматичне реагування (Active Response). Для підтверджених загроз реалізується шляхом виконання попередньо визначених дій, що можуть включати ізоляцію ураженого вузла, усунення шкідливого об'єкта та сповіщення

адміністратора або системи моніторингу.

Для реалізації інтеграції Wazuh із сервісом VirusTotal необхідно налаштувати відповідну секцію в конфігураційному файлі ossec.conf, зокрема вказати назву інтеграції, API-ключ доступу до VirusTotal, ідентифікатор правила Wazuh, при спрацюванні якого дані передаються на перевірку, а також формат повідомлень, наприклад, JSON:

```
<integration>
    <name>virustotal</name>
    <api_key>YOUR_API_KEY</api_key>
    <rule_id>554</rule_id>
    <alert_format>json</alert_format>
</integration>
```

Завдяки такій конфігурації підозрілі файли або їх хеші автоматично відправляються до VirusTotal для отримання репутаційної інформації.

Для мінімізації навантаження на мережу рекомендовано передавати тільки хеші файлів (SHA256 або MD5), а не повні їх копії. Важливим є регулярне оновлювлення правил Wazuh Manager для врахування нових загроз. При обробці результатів перевірки VirusTotal порогове значення підтвердження шкідливості визначається експериментально, щоб балансувати між чутливістю та кількістю хибних спрацювань. При використання публічного API VirusTotal важливо враховувати обмеження швидкості запитів (4 запити/хвилину). Для великих потоків подій рекомендується надсилати тільки критично важливі хеші або використовувати платну версію API з підвищеним лімітом запитів.

Висновок. Впровадження запропонованого підходу дозволить забезпечити підвищення точності виявлення відомого та модифікованого ШПЗ, зниження часу виявлення та реагування, інтеграцію процесів аналізу, підтвердження та нейтралізації в єдиній платформі. Поєднання механізмів Wazuh і VirusTotal формує гнучку, масштабовану та аналітично обґрунтовану систему моніторингу та виявлення ШПЗ, яка здатна підвищити рівень кіберзахисту.

Перелік використаних джерел.

1. Wazuh. Malware detection. [Електронний ресурс].- Режим доступу: https://documentation.wazuh.com/current/getting-started/use-cases/malware-detection.html

2. VirusTotal integration with Wazuh. [Електронний ресурс].- Режим доступу: https://medium.com/%40aravindraja150/virustotal-integration-with-wazuh-c79328d7543f

3. Wazuh. VirusTotal integration. [Електронний ресурс].- Режим доступу: https://documentation.wazuh.com/current/user-manual/capabilities/malware-detection/virus-total-integration.html

4. Detecting and removing malware using VirusTotal integration. [Електронний ресурс].- Режим доступу: https://documentation.wazuh.com/current/proof-of-concept-guide/detect-remove-malware-virustotal.html