

УДК 681.5:004.22

Гріцкевич А.А.¹

¹ асп. НУ «Запорізька політехніка»

ВИЗНАЧЕННЯ АНОМАЛЬНОЇ ПОВЕДІНКИ СУБ'ЄКТІВ У ВЕЛИКИХ ІТ-СТРУКТУРАХ

В умовах стрімкого розвитку та масштабування ІТ-інфраструктур зростають ризики, пов'язані з кібербезпекою [1]. Особливо вразливими є великі ІТ-структури, що формувались протягом тривалого часу різними

командами розробників та архітекторів. Відсутність уніфікованого підходу до забезпечення безпеки та фрагментарність рішень створюють передумови для виникнення вразливостей у системах контролю доступу [2].

Традиційні методи забезпечення кібербезпеки, такі як впровадження комплексних систем керування доступом, часто стикаються з рядом обмежень: тривалі терміни впровадження, несумісність з існуючими політиками безпеки організацій, значні ресурсні витрати на інтеграцію. У цьому контексті особливої актуальності набуває розробка проміжних рішень, що дозволяють підвищити рівень захищеності IT-інфраструктури до моменту впровадження комплексної системи безпеки.

Одним із ключових факторів, що потребує постійного моніторингу, є аномальна поведінка користувачів системи, яка може свідчити про потенційні загрози безпеці [3]. Своєчасне виявлення таких аномалій дозволяє запобігти несанкціонованому доступу та мінімізувати можливі ризики.

Методи визначення аномальної поведінки базуються на комплексному аналізі активності користувачів інформаційних систем. Аномальність в поведінці суб'єкта виявляється шляхом налаштування тригерів на рівні операційної системи (ОС) користувача, без залучення сторонніх утиліт. Для відстеження певних подій застосовуються утиліти Auditd у Linux або Event Logging у Windows. Активація тригерів відбувається при виникненні подій запуску програми, зміни налаштувань системи, маніпулюванні критичними файлами, мережних підключеннях, передачі даних або підключенні зовнішніх пристроїв. Події реєструються автоматично після інсталяції в ОС та зберігаються в лог-файлах. Технічна реалізація досягається шляхом конфігурації Auditd із застосуванням правил для відстеження змін у файлах або мережних підключеннях, збереження цих подій у `/var/log/audit/audit.log`, а також через PowerShell-скрипти у Windows для моніторингу Event Logs і пересилання даних через захищений канал на зовнішній сервер.

Збір та пересилання журналів для централізованого аналізу реалізується за допомогою скриптів, що періодично сканують файли журналів на наявність необхідних даних, екстрагують їх і передають у стандартизованому форматі. Таким чином забезпечується автоматизована передача даних для подальшого аналізу та обробки.

Ефективність моніторингу значною мірою залежить від методики налаштування тригерів. Виявлення відхиленої поведінки можливе лише при відповідності дій користувача встановленим пороговим значенням правил. Надмірна кількість тригерів призводить до збільшення хибнопозитивних спрацьовувань, перевантаження системи нерелевантними даними і, як наслідок, ускладнення процесів аналізу.

Програмне забезпечення класу моніторингу активності користувачів (UAM) представляє готові рішення для спостереження за активністю

користувачів і виявлення аномальної поведінки. Системи UAM функціонують на рівні операційної системи, забезпечуючи контроль дій користувачів з метою забезпечення безпеки, запобігання витоку даних і підвищення ефективності роботи.

За замовчуванням UAM містить набір тригерів для відстеження специфічних подій: доступу до файлів, запуску програм із підвищеними правами, зміни налаштувань та мережевих підключень. Стандартний набір тригерів UAM системи включає:

- [Default] [Linux] User adding - an alert for detecting user creation;
- [Default] [Linux] Installation detection - an alert on installation events;
- [Default] [Linux] Mounting device - an alert on mounting storages.

Окрім стандартних тригерів, існує можливість створення та налаштування додаткових тригерів. UAM виконує автоматичну обробку згенерованих тригерів та аналіз рівня загрози відповідно до вбудованих алгоритмів. При виявленні потенційно небезпечного набору подій система формує оцінку ризику та генерує звіт для подальшого аналізу.

Застосування спеціалізованих систем моніторингу типу UAM забезпечує прискорене розгортання та налаштування через використання готових рішень. Це оптимізує часові витрати на впровадження для організацій, проте породжує питання довіри до стороннього програмного забезпечення з вбудованими алгоритмами оцінки.

Реєстрація даних реалізується за допомогою вбудованих засобів операційної системи з подальшою передачею в систему SIEM для поглибленого дослідження на основі попередньо визначених або налаштованих правил. Процес включає аналіз всіх подій за допомогою SIEM на предмет аномальної поведінки, зіставлення з відомими шаблонами, оцінку журналів за частотою, зв'язками з іншими подіями та рівнем ризику. Журнали надходять із серверів у систему SIEM, консолідуються в єдиний формат за допомогою інструментів Logstash, індексуються в Elasticsearch для фільтрації. Візуалізація даних здійснюється через Kibana з формуванням інформаційних панелей та звітів.

Для поглибленого аналізу аномалій у журналах застосовуються спеціальні правила запитів, засновані на пошуку специфічних комбінацій подій із використанням KQL або Lucene. Дані правила забезпечують пошук аномалій не за окремими тригерами, а за наборами подій, асоційованих з нетиповою поведінкою. На початковому етапі впровадження можливе генерування хибнопозитивних спрацьовувань до моменту навчання системи на типовому потоці журналу. Додатковим обмеженням виступає здатність системи лише фіксувати відхилення без точної класифікації подій як загроз.

Пропозиція оптимального методу базується на інтеграції різних підходів до моніторингу активності користувачів. Комбінація готових і

кастомних тригерів, агента UAM та інструментів аналізу журналів SIEM забезпечує створення комплексної системи виявлення аномальної поведінки. Запропонована модель поєднує різноманітні джерела даних і методи їх обробки, що дозволяє детектувати як явні загрози, так і приховані аномалії в поведінці користувачів.

Розгортання UAM-агентів на робочих станціях забезпечує формування мережі налаштованих тригерів з можливістю розширення додатковими правилами детектування. Взаємодія агента з операційною системою реалізується через системні виклики та функції, що включає роботу з реєстром, файловою системою, процесами та службами з використанням наданих при інсталяції привілеїв. Подальша передача логів до SIEM системи уможливило комплексний аналіз та формування звітів щодо виявлених тригерів, а також ідентифікацію прихованих загроз на основі аномальних записів в журналах ОС у випадках маскування зловмисником своїх дій під легітимні операції суб'єкта.

Наукова новизна запропонованого підходу полягає в інтеграції трьох взаємодоповнюючих методів виявлення аномалій:

- тригерного моніторингу на рівні ОС;
- спеціалізованих систем UAM;
- централізованого аналізу журналів через SIEM.

Перспективи розвитку комбінованого методу охоплюють розширення спектру контрольованих параметрів доступу. Аналіз частоти звернень до об'єктів інфраструктури (сервісів і серверів) реалізується через дослідження журналів, що акумулюються на серверах, системах моніторингу та мережевому обладнанні. За відсутності налаштованого логування впроваджується система реєстрації для забезпечення повноти аналізу використання об'єктів.

SIEM система забезпечує централізований збір журналів з різних компонентів інфраструктури з подальшою нормалізацією до уніфікованого формату. Збір статистики щодо кількісних показників та тривалості сеансів здійснюється незалежно. Реалізована можливість отримання журналів через API-інтерфейси у форматах JSON або XML. Після етапу фільтрації виконується обробка даних з подальшою візуалізацією в Kibana для формування аналітичних панелей моніторингу активності.

Подальший розвиток запропонованих рішень передбачає інтеграцію технологій машинного навчання та штучного інтелекту в систему контролю доступу. Аналіз напрацьованого архіву даних та оцінка ефективності застосованих методів створюють передумови для вдосконалення автоматизації моніторингу, що сприяє підвищенню точності виявлення аномалій та прогнозування потенційних загроз.

Розроблений комбінований підхід забезпечує оперативне виявлення аномальної поведінки та своєчасне реагування на потенційні загрози, дослідження якого відбулося за підтримки проекту "TELEMETRY" в рамках програми Horizon Europe. Інтеграція тригерного моніторингу на рівні ОС, UAM-агентів та централізованого аналізу через SIEM дозволяє досягти синергетичного ефекту в забезпеченні інформаційної безпеки. Запропоноване рішення демонструє високу ефективність для великих ІТ-структур, що не мають комплексних систем безпеки, а отримані результати можуть бути використані при розробці та адаптації комплексних рішень під специфічні потреби організацій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Anderson J.P. Computer Security Threat Monitoring and Surveillance. Technical Report, James P. Anderson Co., Fort Washington, Pennsylvania, 2020.
2. Garcia-Teodoro P., Diaz-Verdejo J., Maciá-Fernández G., Vázquez E. Anomaly-based network intrusion detection: Techniques, systems and challenges. *computers & security*, 28(1-2), 18-28, 2019.
3. Chandola V., Banerjee A., Kumar V. Anomaly detection: A survey. *ACM computing surveys (CSUR)*, 41(3), 1-58, 2021.