Розроблено алгоритм об'єднання подій із гетерогенних джерел у єдиний нормалізований потік та механізм дедуплікації хмарних знахідок. Модель рушія детектування формалізує п'ять типів правил: порогове, паттерн, відсутність, кореляція, послідовність. Модель інциденту реалізовано як детермінований скінченний автомат $M = (Q, \Sigma, \delta, q_0, F)$ із шістьма станами та вбудованим контролем SLA.

Програмну реалізацію виконано у складі хмарно-нативної платформи uSafe. Основний модуль аналізу реалізовано у модулях alert_filters, alert_ingest та rule_engine. Також, модуль сканування хмарної безпеки, наприклад - AWS, охоплює 239 перевірок безпеки у 12 категоріях. Верифікацію алгоритмів проведено на синтетичних тестових наборах, що підтвердили коректність усіх стадій конвеєра.

Аналіз статистики FilterStats підтверджує ефективність розробленого конвеєра: pass rate складає ~14 %, тобто ~86 % подій відсіюється до їх запису в базу даних як події безпеки. Цей результат порівнянний із показниками ML-підходів (Carbon Filter: 82-84 % [3]) за суттєво вищої детермінованості та пояснюваності рішень. Розроблені методи впроваджено в продуктивному середовищі платформи uSafe та можуть бути застосовані у комерційних продуктах класу MSSP.

1. Illumio. The 2025 Global Cloud Detection and Response Report. URL: https://www.illumio.com/resource-center/2025-global-cloud-detection-and-response-report (дата звернення: 08.04.2026).
2. Tariq S., Chhetri M. B., Nepal S., Paris C. Alert Fatigue in Security Operations Centres: Research Challenges and Opportunities. ACM Computing Surveys. – 2025. – Vol. 57, No. 9. – DOI: 10.1145/3723158.
3. Yang L., Li Z., Chen H. Carbon Filter: Reducing False Positive Alerts in Security Operations Centers. IEEE Transactions on Information Forensics and Security. – 2022. – Vol. 17. – P. 2341–2354.

Виявлення несанкціонованого доступу та компрометації облікових записів завдяки SIEM системі

УДК 004.056

Степовенко Юрій[1], Ілля Фалендиш[2], Євгеній Юр'єв[3]

Тернопільський національний технічний університет імені Івана Пулюя,
[1]urastepovenko1@gmail.com, [2]illia.falendysh02@gmail.com, [3]yurev05@gmail.com

У сучасному світі важко переоцінити роль кібербезпеки. Враховуючи кількість існуючих вірусів, атак та загроз комп'ютерні системи вимагають особливої уваги до своєї активності. Саме тому сучасні компанії часто вводять в експлуатацію SIEM системи, які завдяки централізованому збору логів та евристичному аналізу здатні виявляти аномалії в активності системи та повідомляти про це IT команду. Головною проблемою подібних систем є велика кількість хибних спрацювань - поведінка як інтернет трафіку, так і користувачів рідко буває стабільною та передбачуваною, проте автоматизований алгоритм чи штучний інтелект не можуть відрізнити істинні спрацювання від хибних.

Метою цієї роботи було розглянути критичну ланку подібних аномалій, а саме проаналізувати, яким чином відрізнити несанкціонований вхід до системи від легітимного завдяки SIEM системі, а також проаналізувати сучасні техніки та атаки, завдяки яким зловмисники проникають у приватні сервіси.

Найпростіший та найефективніший метод, щоб заволодіти обліковими даними користувача, фішинг. Сучасні фішингові методи важко охарактеризувати певними спільними рисами, адже в залежності від підготовки зловмисника, посилання у фішинговому листі буває важко відрізнити навіть підготованому користувачу. Деякі системи здатні помічати перехід за подібними посиланнями, і коли аналітик проаналізує його в ізольованому середовищі, та співставить приблизний час натискання на посилання з підозрілим входом, стане зрозуміло, що акаунт скомпрометовано. Проте бувають випадки, коли переходи за подібними посиланнями не фіксуються системою. Це відбувається тому, що не всі системи клієнта можуть мати встановлені агенти, які відслідковують підозрілу активність, або ж взагалі користувач перейде за посиланням з власного, а не корпоративного пристрою. В таких випадках, вхід на перший погляд не відрізнятиметься від звичайного. По-перше, необхідно дослідити, з якого пристрою виконувався вхід. По-друге, необхідно порівняти ID сесії при звичайних входах та під час підозрілого. Зазвичай одна сесія видається користувачеві на доволі довгий період, близько кількох тижнів. Агент, тобто інформація про користувача при вході, його браузер, операційна система та рендер, доволі сталі для конкретного акаунту. Також IP адреса може дати цінну інформацію про користувача, насамперед тому, що завдяки вебсайту https://ip2proxy.com/ можна дослідити чи використовує користувач VPN, а завдяки https://www.abuseipdb.com/ – отримати інформацію про зловмисну діяльність тих чи інших IP-адрес.

Що стосується методів протидії фішинговим атакам, то поряд з правилами цифрової гігієни, регулярної зміни пароля та аналізу листів на фішинг, безвідмовним способом захистити себе від несанкціонованого входу є впровадження двофакторної автентифікації. Проте все ще залишиться ризик перехоплення сесії та атак типу MITM, які не авторизуються до системи, а використовують вже існуючі сесії для обходу автентифікації. Якщо ж акаунт користувача вже скомпрометовано, необхідно розірвати з'єднання зі зловмисником. У деяких випадках компрометації, до акаунту входить лише один зловмисник з чистої IP адреси, що б замаскувати свій вхід. Інколи на акаунт "навалюються" десятки зловмисників, які виконують сканування, копіюють дані, встановлюють шкідливе ПЗ, і працюють на швидкість.

Проаналізуємо реальний інцидент безпеки, а саме несанкціонований вхід до SIEM системи. Імена скомпрометованих користувачів буде приховано, заради їх конфіденційності. У одному кейсі, було повідомлено про підозрілий вхід для певного користувача. Аналізуючи його активність, було помічено одну невдалу спробу входу через регіональну фільтрацію, з Британської IP адреси, проте сам користувач зазвичай має активність у Італії. Аналізуючи інші логіни з Італії, увагу привернув один неприродній вхід з нового девайсу. IP адреса у розглянутій моніторинговій системі позначалась як Італійська (рис. 1).

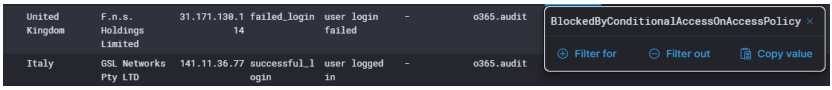

Рис. 1. Фіксація невдалого входу користувача

Проаналізувавши активність за допомогою IP2Proxy та AbuseIPDB було помічено, що насправді IP адреса є VPN, яка насправді походить з Німеччини, та має сумнівну репутацію (рис. 2).

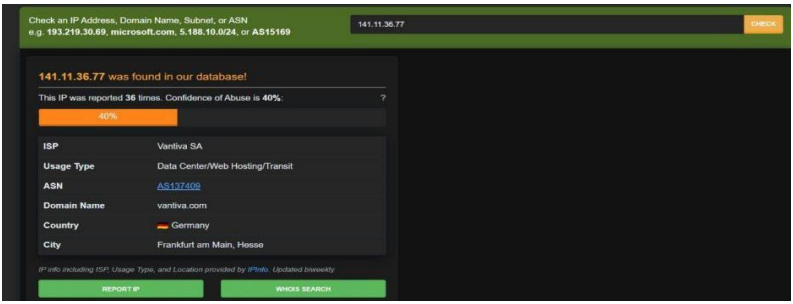

Рис. 2. Виявлена підозріла IP адреса

В результаті подальших перевірок було визначено, що користувач в результаті переходу за фішинговим посиланням ввів свої дані. Після виконання розриву сесій, зміни пароля та подальших перевірок атаку вдалось припинити.

Підбиваючи підсумки, навіть для такого простого процесу як авторизація можна використати десятки різних технік та атак, які дозволять обійти навіть найбільш досконалі системи захисту. Проте, якщо вчасно отримати повідомлення про підозрілі дії, можна виконати розрив сесії до виконання шкідливих дій. Тому актуальність використання моніторигових систем для аналізу стану безпеки зростатиме і надалі.

Розгортання системи моніторингу безпеки VPN-з'єднання на базі WireGuard

УДК 004.056

Каріна Крушельницька[1], Марина Деркач[2], Віталій Тимощук[3]

Тернопільський національний технічний університет імені Івана Пулюя,
[1]karina.kryshel@gmail.com, [2]m_derkach@tntu.edu.ua, [3]Tymoshchuk@tntu.edu.ua

У сучасних мережевих інфраструктурах VPN-з'єднання забезпечують створення захищених каналів передачі даних через Інтернет. У свою чергу, системи моніторингу дозволяють контролювати віддалений доступ до ресурсів, поєднуючи у єдину безпечну мережу територіально віддалені офіси, а також відстежувати підозрілу активність та своєчасно виявляти загрози.

Для реалізації такого підходу при розгортанні системи моніторингу безпеки використано систему виявлення вторгнень на основі мережі Suricata, яка демонструє широкі аналітичні можливості для моніторингу мережевого