УДК 004.056

Кондратюк Т.Г.
Кирилащук А.В.

Метод зниження рівня хибних спрацювань (False Positives) при моніторингу технік Living off the Land у корпоративних мережах

Вінницький національний технічний університет

Анотація

У роботі досліджується проблема критичного перевантаження центрів моніторингу безпеки (SOC) хибними спрацюваннями (False Positives), що виникають під час спроб виявлення атак типу «Living off the Land» (LotL). Оскільки зловмисники використовують легітимні системні інструменти (PowerShell, WMI, PsExec), класичні сигнатурні правила SIEM-систем не здатні відрізнити шкідливу активність від рутинної роботи системних адміністраторів. Це призводить до явища «втоми від тривог» (Alert Fatigue) та пропуску реальних інцидентів. Для вирішення цієї проблеми запропоновано метод контекстного збагачення даних безпеки, який інтегрує технічні події з організаційними метаданими (роль користувача, профіль поведінки, критичність активу). Застосування методу дозволяє автоматизувати фільтрацію легітимної активності та суттєво знизити рівень інформаційного шуму.

Ключові слова: *False Positives, Living off the Land (LotL), SIEM, SOC, Alert Fatigue, контекстно-орієнтований аналіз, інформаційна безпека.*

Abstract

The paper investigates the critical problem of Security Operations Centers (SOC) being overloaded with false positives during attempts to detect "Living off the Land" (LotL) attacks. Since attackers utilize legitimate system tools (PowerShell, WMI, PsExec), classic signature-based SIEM rules cannot distinguish malicious activity from the routine work of system administrators. This leads to the phenomenon of "alert fatigue" and the missing of actual incidents. To address this issue, a method of contextual security data enrichment is proposed, which integrates technical events with organizational metadata (user role, behavioral profile, asset criticality). The application of this method automates the filtering of legitimate activity and significantly reduces the level of information noise.

Keywords: False Positives, Living off the Land (LotL), SIEM, SOC, Alert Fatigue, context-aware analysis, information security.

Вступ

Сучасний ландшафт кіберзагроз характеризується поступовою відмовою зловмисників від використання спеціалізованого шкідливого програмного забезпечення (Malware) на користь технік «Living off the Land» (LotL). Використання вбудованих унікальних інструментів операційних систем дозволяє атакуючим залишатися непоміченими для традиційних засобів захисту.

У спробах виявити таку активність, інженери з кібербезпеки створюють правила кореляції в SIEM-системах, що реагують на запуск стандартних утиліт адміністрування. Проте такий підхід генерує неприйнятну кількість хибних спрацювань (False Positives), оскільки IT-персонал використовує ті самі інструменти для легітимного обслуговування інфраструктури. Наслідком цього стає деградація ефективності роботи аналітиків SOC, які змушені витрачати більшість робочого часу на обробку нерелевантних тривог. Метою даної роботи є розробка методу оптимізації процесу моніторингу, що дозволить знизити відсоток хибних спрацювань без втрати видимості реальних загроз.

Результати дослідження

1. Еволюція атак та марність класичних індикаторів компрометації (IoC)

Доведено, що покладання виключно на статичні індикатори компрометації (IoC), такі як хеші файлів, статичні IP-адреси чи доменні імена командних центрів (C2), остаточно втратило свою практичну цінність при протидії атакам типу «Living off the Land». Традиційна парадигма захисту, побудована на пошуку "відомого зла" (Known Bad), зазнає краху, коли зловмисник свідомо відмовляється від розробки та використання кастомного шкідливого ПЗ. Згідно з концепцією «Піраміди болю» (Pyramid of Pain), статичні індикатори знаходяться на найнижчому рівні ефективності захисту: атакуючий може автоматизовано змінювати хеші корисного навантаження при кожній

компіляції, проте зміна самої тактики (використання легітимного інструментарію) вимагає від нього значних ресурсів.

Сучасні APT – угруповання використовують вбудовані утиліти операційної системи (LOLBins – Living off the Land Binaries). Коли зловмисник отримує доступ до валідних облікових даних та ініціює запуск утиліт на кшталт powershell.exe, wmic.exe, certutil.exe або vssadmin.exe для розвідки домену, дампа пам'яті чи горизонтального переміщення, він не залишає на диску жодних класичних шкідливих артефактів. Більше того, виконання шкідливого коду часто відбувається виключно в оперативній пам'яті (Fileless атаки). У таких умовах система моніторингу фіксує запуск процесу, який є технічно бездоганним: він легітимний, розташований у системній директорії та підписаний дійсним цифровим сертифікатом розробника ОС.

Це створює патову ситуацію для центрів моніторингу (SOC). З одного боку, базовий сигнатурний аналіз виявляється абсолютно сліпим до таких загроз, оскільки антивірусні рішення та класичні SIEM-правила не можуть блокувати системні компоненти без руйнування бізнес-процесів самої організації. З іншого боку, спроби інженерів написати детектуючу логіку "в лоб" (наприклад, створення алертів на кожен мережевий запит від PowerShell або використання параметрів ExecutionPolicy Bypass) змушують систему безперервно кричати про небезпеку.

2. Проблема «інформаційного шуму» та Alert Fatigue у роботі SOC

Аналіз рутинної роботи центрів моніторингу (SOC) безжально демонструє, що гучні обіцянки вендорів безпекових рішень розбиваються об сувору реальність: понад 70-80% згенерованих SIEM-системою інцидентів є відвертим інформаційним сміттям та хибними спрацюваннями (False Positives). Це неминуче призводить до глибокого психологічного вигоряння та професійної деформації аналітиків першої лінії (L1) – явища, відомого як «втома від тривог» (Alert Fatigue). Коли система безперервно, 24/7, генерує тисячі критичних попереджень на абсолютно нормальну поведінку мережі (наприклад, щоденне резервне копіювання баз даних або масовий запуск PowerShell-скриптів оновлення), людський мозок адаптується через блокування подразника. Аналітик починає несвідомо ігнорувати важливі деталі у логах, а згодом переходить до масового закриття інцидентів за шаблоном, просто щоб виконати формальні KPI та очистити чергу до кінця зміни. Ця рутина перетворює високооплачуваних фахівців з кібербезпеки на звичайних операторів кліків, створюючи ідеальне вікно можливостей для зловмисника, який буквально ховається на видноті.

Більше того, така ілюзія контролю створює парадоксальну ситуацію: компанії інвестують величезні бюджети у розгортання SIEM, але не отримують жодного практичного захисту від цілеспрямованих атак. Поки керівництво заспокоює себе зеленими дашбордами та звітами про тисячі "оброблених" подій, реальний середній час виявлення інциденту (MTTD – Mean Time to Detect) залишається катастрофічно високим. Професійні атакуючі чудово усвідомлюють цю вразливість сучасних SOC. Вони розуміють, що їм не обов'язково бути невидимими – достатньо просто злитися з загальним хаосом легітимних процесів. Використовуючи техніки LotL, хакери генерують події, які губляться у нескінченному потоці False Positives, цілком обґрунтовано розраховуючи на те, що втомлений аналітик на іншому кінці екрану просто натисне кнопку «Resolve», аби швидше піти додому. У результаті, замість проактивного полювання на загрози (Threat Hunting), діяльність SOC зводиться до безглуздого обслуговування недосконалих алгоритмів системи.

3. Архітектура методу контекстного збагачення даних (Context Enrichment) та подолання «сліпоти» логування

Для реального рівня False Positives, базової логіки SIEM критично мало. «Сирі» логи самі по собі є абсолютно безглуздим набором технічних фактів, які не несуть жодної цінності без розуміння середовища. Замість того, щоб згодовувати кореляційному рушію мільйони ізольованих подій, запропоновано архітектуру попереднього збагачення (Context Enrichment). Вона примусово інтегрує організаційні метадані до логів ще до того, як спрацює будь-яке правило, перетворюючи «сліпий» запис на осмислений індикатор. Архітектура базується на трьох обов'язкових рівнях контексту:

– Ідентифікаційний контекст (Identity-Awareness): Глибока перевірка ролі та реальних (а не номінальних) повноважень користувача через безперервну інтеграцію з Active Directory та HR-системами. У реальному корпоративному середовищі AD найчастіше нагадує звалище історичних привілеїв, де звичайний бухгалтер може роками зберігати права локального адміністратора через чиюсь лінь або тимчасову необхідність у 2018 році.

– Контекст активу (Asset Criticality): Динамічне визначення бізнес-цінності, мережевого сегмента та призначення конкретного вузла на основі актуальної бази CMDB (Configuration Management

Database). Традиційні SIEM-системи часто налаштовані так, ніби всі комп'ютери в мережі однаково важливі, що є фатальною помилкою. Контекст активу дозволяє системі кардинально по-різному оцінювати одну й ту саму технічну дію.

– Часовий та ситуаційний контекст (Temporal & Behavioral Baseline): Порівняння поточної активності з типовим робочим графіком співробітника та його історичним профілем поведінки (Baseline). Сучасні зловмисники чудово знають розклад роботи корпорацій і часто планують маневри на вихідні або нічний час, коли пильність SOC найнижча. Проте жорсткі часові правила на кшталт «тривога після 18:00» не працюють у реальному IT-світі, де адміністратори регулярно лагодять критичні системи о третій ночі.

4. Динамічна оцінка ризиків (Risk Scoring) як математичний критерій фільтрації

Класична бінарна логіка кореляції в SIEM – це утопія, яка життєздатна лише в стерильних презентаціях вендорів. У реальному корпоративному середовищі, де панує перманентний хаос із легасі-систем, тимчасових скриптів-«милиць» та непередбачуваної поведінки IT-відділу, такий жорсткий детермінований підхід гарантовано призводить до колапсу SOC. Щоб система не захлинулася у власних тривогах при спробах виявити атаки типу LotL, необхідна повна відмова від прямолінійних тригерів на користь алгоритмічної моделі зваженого ризику (Risk Scoring). Суть цього підходу полягає в тому, що кожна потенційно небезпечна подія спочатку проходить через скоринговий рушій. Замість того, щоб сліпо генерувати алерт на сам факт запуску умовної утиліти розвідки чи адміністрування, система бере базову технічну небезпеку цієї дії та пропускає її через систему понижуючих або підвищуючих коефіцієнтів, отриманих на етапі контекстного збагачення.

На практиці це працює як автоматизований фільтр адекватності, що виключає фактор людської втоми. Наприклад, якщо масові віддалені WMI-запити ініціюються застарілим скриптом інвентаризації від імені сервісного акаунту в узгоджене нічне вікно обслуговування, алгоритм штучно деградує рівень загрози. Система розуміє, що це рутина, і просто залишає "тихий" лог, не відволікаючи аналітика на сміттєвий алерт. Проте, якщо абсолютно ідентичний системний запит ініціює обліковий запис рядового HR-менеджера у бік критичного сервера баз даних, профіль ризику експоненціально зростає. Навіть використовуючи повністю легітимний системний інструментарій, зловмисник неминуче діє поза межами нормального бізнес-контексту скомпрометованого користувача. Це дозволяє миттєво підняти пріоритет такого інциденту до критичного рівня, фокусуючи увагу команди безпеки виключно на математично підтверджених аномаліях, а не на щоденній роботі власних системних адміністраторів.

Висновки

У ході дослідження доведено, що критично високий рівень хибних спрацювань (False Positives) при виявленні атак типу «Living off the Land» є прямим наслідком структурної недосконалості класичних правил SIEM-систем. Сліпе покладання на детерміновану логіку та сигнатурний аналіз, що повністю ігнорує організаційний бізнес-контекст подій, перетворює дорогі системи безпеки на генератори марного інформаційного сміття.

Запропонований у роботі метод контекстного збагачення логів (перевірка ролі користувача, критичності активу, часових рамок) у поєднанні з алгоритмами динамічної оцінки ризиків дозволяє автоматизовано відрізняти хаотичну, але легітимну рутину IT-адміністраторів від прихованих маневрів зловмисників. Це зміщує фокус системи з пошуку міфічних шкідливих артефактів на виявлення реальних поведінкових аномалій.

Застосування такого ризик-орієнтованого підходу вирішує фундаментальну проблему «інформаційного шуму» та ліквідує руйнівний ефект Alert Fatigue (втоми від тривог) серед аналітиків SOC. Трансформація процесу моніторингу з пасивного збору логів на інтелектуальну фільтрацію значно підвищує точність і швидкість реагування на цілеспрямовані кіберзагрози, не дозволяючи їм безкарно розчинитися у повсякденній корпоративній метушні.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Lateral Movement, Tactic TA0008 - Enterprise | MITRE ATT&CK®. *MITRE ATT&CK®*. URL: https://attack.mitre.org/tactics/TA0008/ (дата звернення: 02.03.2026).
2. SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations | CSRC. *NIST Computer Security Resource Center | CSRC*. URL: https://csrc.nist.gov/pubs/sp/800/137/final (дата звернення: 02.03.2026).

3. Rapid7. *Rapid7*. URL: https://www.rapid7.com/fundamentals/living-off-the-land-attack/ (дата звернення: 02.03.2026).

Артем Вячеславович Кондратюк – студент групи 2КІТС-24б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: pashapugach2@gmail.com;

Науковий керівник: Тетяна Геннадіївна Кирилащук – асистент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця.

Artem V. Kondratiuk – student of group 2KITS-24b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: pashapugach2@gmail.com;

Supervisor: Tatyana G. Kyrylashchuk – Assistant Professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia.