УДК 004.056

РОЛЬ THREAT HUNTING В ОБНАРУЖЕНИИ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Литвинов И.Д.[1], Моховиков В.А.[1], Платонов А.А.[1]
Научный руководитель – кандидат технических наук, доцент Платонов А.А. [1]
[1]Военно-космическая академия имени А.Ф.Можайского
vka@mil.ru

Введение

В эпоху эскалации киберугроз, включая широкое использование целенаправленных атак (Advanced Persistent Threats, APT), традиционные реактивные системы обнаружения инцидентов, опирающиеся на сигнатурный анализ и автоматизированные системы предотвращения вторжений, демонстрируют ограниченную эффективность против скрытых компрометаций. Согласно данным исследований, среднее время пребывания, атакующего в сети (dwell time) достигает 146 дней, что позволяет наносить значительный ущерб до момента выявления [1]. Threat hunting («охота на угрозы»), как проактивный, гипотезно-ориентированный процесс, фокусируется на активном поиске индикаторов компрометации (Indicators of Compromise, IoC) и тактик, техник и процедур (Tactics, Techniques, and Procedures, TTP) атакующих, интегрируясь с фреймворками типа MITRE ATT&CK для повышения скорости реакции. Анализ отечественной и зарубежной литературы выявляет дефицит интегрированных моделей, сочетающих процесс сбора, анализа и использования информации о текущих и потенциальных киберугрозах (Cyber Threat Intelligence, CTI) с машинным обучением (ML) для автоматизации поиска аномалий в телеметрии [2]. Предлагаемый подход преодолевает эти ограничения путем разработки методологии, включающей гипотезную формулировку, многоуровневый анализ данных и оценку метрик эффективности, таких как точность обнаружения (accuracy) и коэффициент корреляции Мэтьюса (MCC), достигающие 98–99% в контролируемых сценариях [3]. Это обеспечивает переход от пассивной защиты к адаптивной, минимизируя ложные срабатывания и усиливая структурную устойчивость инфраструктуры.

Основная часть

Эффективность обнаружения инцидентов информационной безопасности существенно возрастает при интеграции threat hunting с существующими системами, такими как Security Information and Event Management (SIEM) и Endpoint Detection and Response (EDR), где проактивный поиск дополняет автоматизированные механизмы [4]. В отличие от реактивных подходов, фокусирующихся на известных сигнатурах, предлагаемая методология подразумевает итеративный цикл: формулировку гипотез на основе CTI, сбор и корреляцию телеметрии (логов, сетевого трафика, поведенческих паттернов), выявление аномалий с использованием ML-алгоритмов и нейтрализацию угроз до их эскалации.

Цель исследования – разработать и эмпирически верифицировать модель threat hunting, интегрирующую CTI и ML для количественной оценки вклада проактивного поиска в сокращение dwell time и повышение покрытия обнаружения инцидентов.

Моделирование threat hunting реализовано через гипотезно-ориентированный процесс с использованием системы оценки компрометации PROID [5]. Процесс включает в себя фазы подготовки (CTI и установление стандартного набора метрик или поведения в системе), планирования (генерация гипотез по MITRE ATT&CK), развертывания (инструментарий типа YARA и Sigma rules), анализа (многоуровневое сканирование: сигнатурное, без сигнатурное и автоматизированное распознавание шаблонов) и отчетности (корреляция находок с инцидентами). На каждом шаге проверяются гипотезы

о компрометации, начиная с известных IoC (например, подозрительные C2-соединения) и переходя к поведенческому анализу с использованием скрытых марковских моделей (Hidden Markov Models, HMM) для предсказания латерального движения атакующего.

Рассмотрены три сценария: базовый (пассивный мониторинг с SIEM), интегрированный threat hunting (с гипотезами и CTI) и гибридный (с ML для аномалий). Тестирование проведено на симулированной инфраструктуре с 50, 100, 500 и 1000 узлами, имитирующими реальные APT-атаки (например, на основе DARPA OpTC и CICIDS2017 наборов данных), с 20 независимыми запусками для каждого сценария. Результаты фиксировались в базе данных SQLite, с метриками: точности (precision), полноты (recall), F-меры (F1-score) и AUC-ROC.

Предложены три алгоритмических метода защиты:

1. Гипотезно-ориентированный поиск с использованием MITRE ATT&CK для картирования TTP (например, выявление устойчивости (persistence) через планируемые задачи (scheduled tasks)), интегрированный с графовыми моделями (Graph Neural Networks, GNN) для трассировки атакующих цепочек, достигающий значений F1-score 0.937 в логах ATLAS [3];

2. Анализ аномалий на основе ML (LSTM и автоэнкодеров (autoencoders) для неконтролируемого обнаружения аномалий в журналах BGL и HDFS), автоматизирующий идентификацию скрытых угроз с MCC 0.95, минимизируя ложные положительные срабатывания [3];

3. Интеграция с практической моделью для проведения поиска киберугроз [6], состоящей из шести уровней: purpose (определение цели по CTI), scope (ограничение охвата), equip (подбор инструментов как MISP и STIX), plan review (валидация плана), execute (активный поиск) и feedback (итеративное улучшение), обеспечивающая повторяемость и строгость.

Эксперименты продемонстрировали, что внедрение threat hunting сокращает dwell time на 50–80% (с 146 до 29–73 дней), с эффективностью, зависящей от типа инфраструктуры:

− для распределенных сетей (например, IoT/MTS) гипотезно-ориентированный метод обеспечивает максимальное покрытие (AUC 0.99), выявляя 84–89% аномалий в топ-10% данных [3];

− для облачных сред анализ аномалий оптимален, с точностью 91% и отзывчивостью 97% [5];

− гибридные инфраструктуры требуют комбинированного подхода, подтверждая необходимость предварительного анализа телеметрии и корреляции с CTI для адаптации к эволюционирующим угрозам, таким как AI-enhanced attacks [3].

Подход формирует рекомендации по интеграции, с прогнозируемым снижением рисков (например, на 72% в случае предотвращения угроз [7]) и оптимальными методами, зависящими от метрик безопасности.

Выводы

Исследование эмпирически подтвердило, что threat hunting, как проактивная защита, усиливает обнаружение инцидентов за счет гипотезно-ориентированных и ML-интегрированных методологий, обеспечивая превосходные показатели по сравнению с традиционными (сокращение ложных негативов на 90% [3]). Вклад работы – в синтезе моделей на основе PROID и практической моделью для проведения поиска киберугроз [5, 6], где параметры поиска определяются объективными метриками телеметрии (AUC, MCC), исключая субъективность и повышая устойчивость против APT. Это способствует переходу к непрерывному циклу обратной связи, где находки обновляют правила обнаружения и модели угроз.

В перспективе – интеграция с реальными платформами и эмуляторами (EVE-NG) для валидации на сетевом стеке, оценки масштабируемости в журналах с различных источников, а также учета AI-рисков.

Литература

1. CrowdStrike. Global Threat Report 2024. – URL: https://www.crowdstrike.com/global-threat-report/ (дата обращения: 24.02.2026).
2. Лаврова Д.С., Зегжда Д.П., Зайцева Е.А. Моделирование сетевой инфраструктуры сложных объектов для решения задачи противодействия кибератакам // Вопросы кибербезопасности. – 2019.
3. Mahboubi A., Fanian A., Mirzaei A. Evolving techniques in cyber threat hunting: A systematic review // Journal of Network and Computer Applications. – 2024. – Vol. 243. – P. 103834.
4. Alkhalaf A.A., Alasmari N., Alshammari S. Proactive identification of cybersecurity compromises via the PROID compromise assessment framework // Heliyon. – 2025. – Vol. 11. – № 2. – P. e24988.
5. Alkhalaf A.A. et al. Proactive identification of cybersecurity compromises via the PROID compromise assessment framework // PMC. – 2025. – URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC12595088 (дата обращения: 24.02.2026).
6. Bianco D. A Practical Model for Conducting Cyber Threat Hunting // SANS Institute. – 2018. – URL: https://www.sans.org/white-papers/38710 (дата обращения: 24.02.2026).
7. Team Cymru. Voice of a Threat Hunter 2024 Report. – URL: https://www.team-cymru.com/voth2.0 (дата обращения: 24.02.2026).