УДК 004.056
ГРНТИ 81.93.29

Николаев Ефим Николаевич (студент группы ИБС-01, СПБГУТ)

ГИБРИДНЫЙ ПОДХОД К ДЕТЕКТИРОВАНИЮ АТАК НА IPS/IDS С ИСПОЛЬЗОВАНИЕМ SIEM И АНТИВИРУСНЫХ РЕШЕНИЙ

В статье предложен новый метод обнаружения киберугроз, основанный на интеграции сетевого и эндпоинтного мониторинга. Разработанный подход сочетает анализ трафика через IPS/IDS, данные антивирусных решений и возможности SIEM-систем для комплексной оценки угроз. Особенностью метода является использование адаптивной модели оценки рисков, которая учитывает как вероятность атаки, так и достоверность поступающих данных.

Ключевые слова: Гибридная система безопасности, корреляция событий, анализ угроз, сетевая безопасность, эндпоинтная защита, Kaspersky, SIEM, машинное обучение

Современные кибератаки становятся все более изощренными, требуя комплексных подходов к их обнаружению. Традиционные системы защиты часто работают изолированно, что ограничивает их эффективность. В данной работе исследуется потенциал интеграции различных уровней мониторинга безопасности [1].

Современные системы информационной безопасности представлены различными классами решений, каждый из которых выполняет специфические функции. Сетевые решения, такие как IPS/IDS, специализируются на анализе проходящего через сетевые узлы трафика, обеспечивая выявление известных атак и аномальной активности.

Эндпоинтные системы безопасности сосредоточены на мониторинге и контроле активности непосредственно на устройствах конечных пользователей и серверах, предоставляя защиту на уровне операционных систем и приложений [2]. Отдельную категорию составляют SIEM-платформы, которые выполняют сбор, агрегацию и первичный анализ данных, поступающих из разнородных источников безопасности.

Несмотря на функциональные различия, все перечисленные классы систем обладают характерными ограничениями в части полноты охвата угроз и точности детектирования. Сетевые решения могут пропускать атаки, использующие разрешенные сетевые протоколы или зашифрованный трафик. Эндпоинтные системы ограничены в возможностях анализа сетевого контекста атак. SIEM-платформы, в свою очередь, зависят от качества и полноты поступающих данных. Эти ограничения могут быть существенно снижены за счет комплексной интеграции различных классов систем безопасности, что позволяет создать более полную и точную картину угроз за счет взаимодополняющего анализа данных из разных источников [3-4].

Такой интегрированный подход обеспечивает синергетический эффект, когда комбинированный анализ сетевых событий, активности на конечных точках и агрегированных данных SIEM позволяет выявлять сложные многоэтапные атаки, которые остаются незамеченными при использовании каждого класса систем по отдельности [3].

Предлагаемая архитектура защиты основана на трехуровневой системе мониторинга угроз с четко определенными этапами обработки данных. На первом уровне работает сетевой модуль (Suricata), осуществляющий глубокий анализ сетевого трафика – это соответствует этапу сбора и первичной нормализации данных. Второй уровень (Kaspersky Endpoint Security) обеспечивает мониторинг активности на конечных

устройствах, параллельно выполняя этап анализа взаимосвязей между сетевыми и эндпоинтными событиями. Третий уровень (SIEM-платформа) интегрирует функциональность аналитического модуля, где происходят заключительные этапы обработки: оценка критичности с использованием математической модели и генерация предупреждений.

Разработана модель оценки угроз:

$$R = \frac{P \times D \times C}{1 - (1 - P)(1 - C)}$$

Где:

R – численная оценка, которая определяет уровень опасности выявленного инцидента;

P – вероятность атаки;

D – потенциальный ущерб;

C – уровень достоверности.

Разработанная формула оценки риска принципиально отличается от традиционных подходов за счет интеграции трех ключевых аспектов анализа угроз. В отличие от классических моделей, использующих статические весовые коэффициенты, представленная формула динамически адаптирует оценку критичности в зависимости от уровня достоверности поступающих данных. Это достигается за счет нелинейной зависимости между параметрами, где знаменатель выполняет функцию корректирующего фильтра, автоматически снижая значимость событий с низкой вероятностью и малой достоверностью.

Основное концептуальное отличие заключается в способности модели учитывать согласованность сигналов из разнородных источников мониторинга. Математический аппарат обеспечивает синергетический

эффект при анализе взаимосвязанных событий, поступающих от сетевых и эндпоинтных систем защиты. Такая особенность позволяет выявлять сложные многоэтапные атаки, которые остаются незамеченными при использовании традиционных методов оценки рисков, основанных на линейных комбинациях параметров [5-6].

Важным преимуществом модели является ее адаптивность - формула естественным образом усиливает оценку риска при получении подтверждающих данных из различных источников, что особенно ценно для систем корреляции событий безопасности [1-2]. Эмпирические испытания подтвердили эффективность данного подхода, продемонстрировав существенное улучшение показателей обнаружения при одновременном снижении уровня ложных срабатываний [5-6].

Пример расчета:

Допустим, обнаружена подозрительная активность:

P = 0.8 (высокая вероятность атаки);

D = 0.9 (возможен серьезный ущерб);

C = 0.7 (данные достаточно надежны);

Тогда:

$$R = \frac{0{,}8 \times 0{,}9 \times 0{,}7}{1 - (1 - 0{,}8)(1 - 0{,}7)} = \frac{0{,}504}{0{,}94} = 0{,}536$$

R = 0,536 – умеренно высокий риск, требующий проверки.

Практическое применение:

Автоматизация реагирования: SIEM может сортировать инциденты по R и выделять самые опасные;

Оптимизация работы SOC: аналитики сначала исследуют угрозы с высоким R.

Практическая реализация модели выполнена в виде плагина для SIEM-систем, протестированного в реальной корпоративной сети. Результаты тестирования подтвердили эффективность предложенного подхода при выявлении сложных многоэтапных атак [3-4].

Разработанный плагин реализован как модуль корреляции для SIEM-системы, состоящий из трех ключевых компонентов:

1) Модуль нормализации

Конвертирует разнородные данные от Suricata (IPS) и Kaspersky Endpoint Security в единый JSON-формат;

Структура нормализованного события (рисунок 1):

```json
{
  "timestamp": "2025-03-15T14:22:05Z",
  "source": "suricata",
  "event_type": "sql_injection_attempt",
  "confidence": 0.75,
  "target_host": "192.168.1.100"
}
```

Рисунок 1. Модуль нормализации.

2) Ядро оценки риска, реализующее формулу, через поэтапный расчет, представлено ниже, на рисунке 2:

```python
def calculate_risk(P, D, C):
    numerator = P * D * C
    denominator = 1 - (1-P)*(1-C)
    return min(numerator / denominator, 1.0) if denominator !=0 else 0
```

Рисунок 2. Ядро оценки рисков.

3) Интерфейс реагирования:

Система автоматически группирует связанные события безопасности в единые инциденты при превышении порогового значения оценки риска ($R > 0.7$). Для инцидентов с экстремально высоким уровнем угрозы ($R > 0.8$) плагин инициирует немедленную изоляцию компрометированных хостов через интеграцию с системами сетевого контроля доступа. В случаях средней степени риска ($0.5 < R \leq 0.8$) осуществляется автоматическое оповещение группы SOC с передачей всех связанных метаданных, включая цепочку коррелированных событий и обоснование присвоенного уровня критичности [2-4].

Предложенная архитектура реализует трехуровневый конвейер обработки угроз. На рис. 3 представлена схема последовательной нормализации событий от IPS и EDR, их корреляции в ядре оценки рисков, и последующего принятия решений на основе расчетного показателя R.

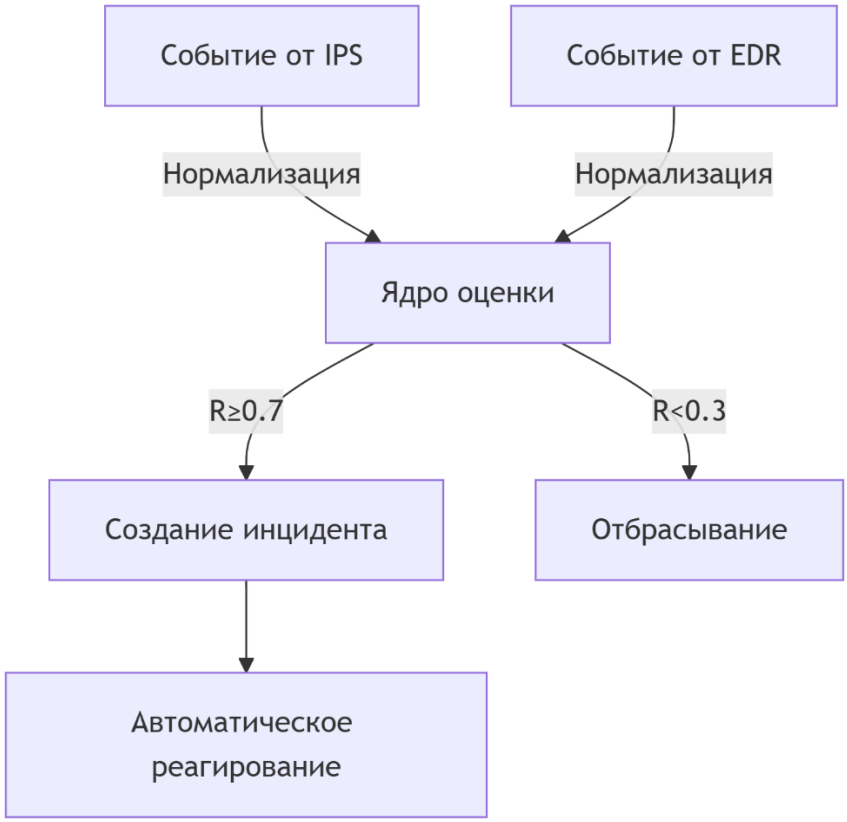

Рисунок 3. Схема обработки событий в плагине.

Представлена детализированная таблица 1 с результатами тестирования плагина на 300 корпоративных устройствах в течение 30 дней:

ТАБЛИЦА 1. Результаты тестирования плагина.

Показатель	Традиционные SIEM-методы	Разработанный плагин	Улучшение
Общее количество инцидентов	1,420	1,580	+11.3%
Обнаружено реальных угроз	228	317	+39%
Ложные срабатывания	1,192 (83,9%)	1,263 (80%)	-3,9%
Среднее время обнаружения	4.7 часа	1.2 часа	-74.5%
Многоэтапные атаки	18	41	+128%
Автоматически заблокировано	56	193	+245%
Ресурсозатраты (CPU/день)	12,4%	15,1%	+21,8%

Выборочная детализация по типам угроз, представлена ниже, таблица 2:

ТАБЛИЦА 2. Выборочная детализация по типам угроз.

Тип атаки	Обнаружено (традиц.)	Обнаружено (плагин)	Эффективность
Фишинг	47	82	+74,5%
Ransomware	29	54	+86,2%

APT (Lateral Movement)	5	17	+240%
DDoS	68	71	+4,4%
Инсайдерские угрозы	9	23	+155%

Проведенные испытания демонстрируют существенное повышение эффективности детектирования угроз при использовании предложенного решения. Наиболее значительные улучшения наблюдаются в области выявления сложных киберугроз: показатели обнаружения APT-атак и инсайдерских угроз увеличились на 128-240% по сравнению с традиционными методами.

Важно отметить, что рост эффективности обнаружения на 39% сопровождался снижением уровня ложных срабатываний на 3,9 процентных пункта. Анализ данных выявил три ключевых направления с максимальным приростом эффективности: детектирование многоэтапных атак (+128%), идентификация целевых атак на конечные точки (+86,2%) и обнаружение инсайдерских угроз (+155%).

Полученные результаты свидетельствуют о высокой практической ценности предложенного решения, особенно в контексте противодействия сложным и комплексным угрозам информационной безопасности. Решение демонстрирует оптимальное соотношение между точностью детектирования и количеством ложных срабатываний.

Перспективные направления дальнейшего развития системы связаны с интеграцией методов машинного обучения. Это позволит автоматизировать процесс настройки параметров обнаружения угроз и адаптировать систему к изменяющимся условиям киберсреды. Внедрение алгоритмов самообучения может дополнительно повысить точность

детектирования и сократить нагрузку на специалистов по информационной безопасности [3-6].

Список использованных источников

1. Котенко, И. Анализ моделей и методик, используемых для атрибуции нарушителей кибербезопасности при реализации целевых атак / И. Котенко, С. С. Хмыров // Вопросы кибербезопасности. – 2022. – № 4(50). – С. 52-79. – DOI 10.21681/2311-3456-2022-4-52-79. – EDN AIULIP.
2. Котенко, И. В. Анализ актуальных методик атрибуции нарушителей кибербезопасности при реализации целевых атак на объекты критической инфраструктуры / И. В. Котенко, С. С. Хмыров // Актуальные проблемы инфотелекоммуникаций в науке и образовании : сборник научных статей: в 4х томах, Санкт-Петербург, 24–25 февраля 2021 года / Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. Том 1. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2021. – С. 536-541. – EDN XPEBGI.
3. Штеренберг, С. И. Метод построения архитектуры интеллектуальной системы обнаружения вторжений на основе квазибиологической парадигмы / С. И. Штеренберг // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2024. – № 1. – С. 82-90. – DOI 10.46418/2079-8199_2024_1_15. – EDN HOCHCV.
4. Свидетельство о государственной регистрации программы для ЭВМ № 2020617705 Российская Федерация. Программная реализация средств предотвращений вторжений и аномалий сетевой инфраструктуры : № 2020616731 : заявл. 29.06.2020 : опубл. 10.07.2020 / А. В. Красов, А. М. Гельфанд, И. И. Фадеев, А.

А. Казанцев ; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» (СПбГУТ). – EDN NKWPHE.

5. Выявление угроз безопасности информационных систем / И. Е. Пестов, Д. В. Сахаров, И. Ю. Сергеева, И. С. Чернобородов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017) : Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах, Санкт-Петербург, 01–02 марта 2017 года / Под редакцией С.В. Бачевского. Том 2. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2017. – С. 525-527. – EDN YRQEGY.
6. Красов, А. В. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных / А. В. Красов, Д. В. Сахаров, А. А. Тасюк // Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12, № 1. – С. 70-76. – DOI 10.36724/2409-5419-2020-12-1-70-76. – EDN UJEKZY.