https://doi.org/10.53360/2788-7995-2024-4(16)-7

МРНТИ: 81.93.29

Т.М. Мехдиев, А.К. Шайханова*, Г.Б. Бекешова
Евразийский национальный университет им. Л.Н. Гумилева
010000, Республика Казахстан, г. Астана, ул. Сатпаева, 2
*e-mail: shaikhanova_ak@enu.kz

АНАЛИЗ СИСТЕМ THREAT INTELLIGENCE

Аннотация. *Threat Intelligence (TI) – это информация о текущих или зарождающихся угрозах для информационной безопасности, которая используется для повышения защищенности организаций. Системы TI собирают и анализируют данные из различных источников, включая открытые источники, закрытые источники, а также данные, полученные от партнеров и клиентов. Анализ систем TI – это процесс оценки эффективности этих систем в сборе и анализе данных, а также в предоставлении полезной информации для принятия решений в области информационной безопасности. В современном цифровом мире, где угрозы информационной безопасности становятся все более сложными и утонченными, анализ систем Threat Intelligence (TI) приобретает ключевое значение для обеспечения безопасности информационных ресурсов. Threat Intelligence представляет собой процесс сбора, анализа и интерпретации данных об угрозах информационной безопасности, направленных на выявление угроз для информационной безопасности. В данном контексте анализ систем TI выступает важным инструментом для эффективного понимания угроз и принятия мер по их предотвращению. Эта статья посвящена рассмотрению особенностей, преимуществ и недостатков анализа систем Threat Intelligence. Например, анализ TI может быть использован для оценки эффективности системы обнаружения вторжений (IDS). Анализ может выявить, какие типы атак IDS может обнаруживать, а какие – нет. На основании результатов анализа можно принять решение о необходимости модернизации системы IDS или о добавлении дополнительных защитных мер.*

Ключевые слова: *Threat Intelligence, открытые источники, информационная безопасность, анализ информации, угрозы информационной безопасности*

Введение

Платформы Threat Intelligence – это коммерческие продукты, которые предоставляют организациям возможность централизованно и автоматически управлять данными об угрозах, анализировать их и действовать в соответствии с ними. Эти платформы обычно собирают и объединяют данные из нескольких источников, включая внутренние системы и потоки информации об угрозах, чтобы обеспечить всестороннее представление о текущих и возникающих угрозах безопасности [1, 2].

Каналы информации об угрозах (Threat Intelligence Feeds) – один из ключевых источников информации, на который эти платформы полагаются для предоставления точной и актуальной информации об угрозах. Эти каналы содержат структурированные и стандартизированные данные, содержащие информацию о текущих угрозах безопасности, в том числе сведения о методах, инструментах и тактиках, используемых злоумышленниками [3].

Коммерческие продукты Threat Intelligence могут варьироваться от простых инструментов анализа информации до более комплексных решений, включающих в себя функции управления угрозами, аналитики, интеллектуальной автоматизации и так далее. Threat Intelligence Feeds являются одним из источников информации, которые могут быть использованы для поддержания и обновления этих продуктов [**Ошибка! Источник ссылки не найден.**].

Целью данного исследования является – исследование и анализ существующих платформ Threat Intelligence с описанием их функционала.

Материалы и методы

Основная гипотеза исследования – реализация обзора, позволяющего выявить основные особенности каждой системы, преимущества и недостатки для эффективного реагирования на современные угрозы информационной безопасности и обеспечения безопасности информационных ресурсов.

Для реализации научного исследования применены методы изучения и анализа научно-методической литературы, информационный поиск по проблеме исследования, а также подходы, основанные на междисциплинарности.

Полученные результаты

Обзор основных продуктов Threat Intelligence. Прежде чем начать обзор продуктов, стоит выделить, что оценивать данные продукты будем по пятибалльной системе и сразу определим общие критерии оценивания данных систем. Из таких критериев были подобраны следующие:

1) Сбор данных: Способность собирать информацию из различных источников, таких как открытые источники, подземные форумы, базы данных угроз, даркнет и другие.

2) Агрегация и корреляция: способность объединять и агрегировать данные из различных источников для создания полной картины угроз. Корреляция данных для выявления связей между различными угрозами и инцидентами угроз информационной безопасности.

3) Анализ и оценка: экспертный анализ полученных данных для определения степени угрозы и ее потенциальных последствий. Возможность присвоения приоритетов угрозам информационной безопасности в зависимости от их серьезности и вероятности.

4) Интеграция с SIEM (система управления информационной безопасностью и событий): совместимость и интеграция с существующими системами безопасности для обеспечения согласованного реагирования на инциденты. Передача информации об угрозах в реальном времени для улучшения процессов обнаружения и реагирования.

5) Управление угрозами: инструменты и функциональности для управления жизненным циклом угроз, от обнаружения до реагирования и мониторинга. Средства для сотрудничества и обмена информацией с другими системами Threat Intelligence [**Ошибка! Источник ссылки не найден.**].

Каждую из систем Threat Intelligence будет очень тяжело оценить полностью, ведь могут быть единичные случаи, где одна система, которую мы оценим хуже, может показать результаты лучше в отдельных кейсах.

Обсуждение

В данной работе рассмотрены следующие системы: R-Vision TIP, Anomali Threat Intelligence Platform, Cisco Threat Intelligence Director, Your Everyday Threat Intelligence, Malware Information Sharing Platform.

R-Vision TIP – это централизованная платформа для работы с данными об угрозах информационной безопасности, которая предназначена для сбора, обработки, хранения и анализа данных об угрозах, а также для использования этой информации для выявления и блокировки угроз, реагирования на инциденты и проведения расследований. R-Vision TIP поддерживает работу с коммерческими и бесплатными источниками информации, а также с данными от ФинЦЕРТ. Продукт автоматически собирает данные из всех подключенных источников, нормализует и дедуплицирует их, приводит к единой модели представления для более удобного и эффективного анализа [**Ошибка! Источник ссылки не найден.**].

R-Vision TIP не только собирает индикаторы угроз, но также подгружает отчёты, информацию об уязвимостях и вредоносных программах, анализирует взаимосвязи между индикаторами, предоставляя полную картину угрозы. Продукт также интегрируется с внешними сервисами, такими как VirusTotal, Shodan, RiskIQ, Whois и другими, чтобы обогатить индикаторы дополнительным контекстом. Обработанные и отсортированные данные могут быть автоматически выгружены во внутренние средства защиты для быстрой блокировки угроз, поддерживая оборудование от производителей, таких как Cisco, Palo Alto Networks, Check Point и других. Кроме того, продукт обеспечивает мониторинг индикаторов в событиях SIEM (QRadar и ArcSight) для обеспечения текущего и ретроспективного анализа, и создания оповещений в случае обнаружения угроз. Наконец, в R-Vision TIP можно автоматизировать

все операции, связанные с индикаторами компрометации, от сбора до блокировки средствами защиты (рис. 1).

Названия	Оценка	Описание
Сбор данных	4	R-Vision TIP может работать с Kaspersky, Group-IB, IBM X-Force Exchange, AT&T Cybersecurity, ФинЦЕРТ (АСОИ либо email), В настоящий момент продукт поддерживает ограниченное число интеграций «из коробки».
Агрегация и корреляция	4	В блоке «Сводка», представлены объединенные сведения разного происхождения. Нет привычной для данного класса продуктов возможности построения графов взаимосвязей
Анализ и оценка	5	Возможность работы не только с индикаторами компрометации, но и с более полной картиной угроз — отчетами, вредоносным программным обеспечением, уязвимостями.
Интеграция с SIEM	4	R-Vision TIP с SIEM-системами QRadar и ArcSight, за счет которой осуществляется мониторинг индикаторов компрометации в событиях безопасности и формирование оповещений в случае обнаружения
Управление угрозами	4	Отсутствуют разграничения по уровням конфиденциальности данных (TLP), а также механизм обмена данными TI между участниками отраслевых или корпоративных сообществ.

Рисунок 1 – R-Vision TIP краткий итог

Anomali Threat Intelligence Platform является сервисом по поиску и обмену информацией об угрозах информационной безопасности. Основные два функционала данного сервиса – это Stream и Match.

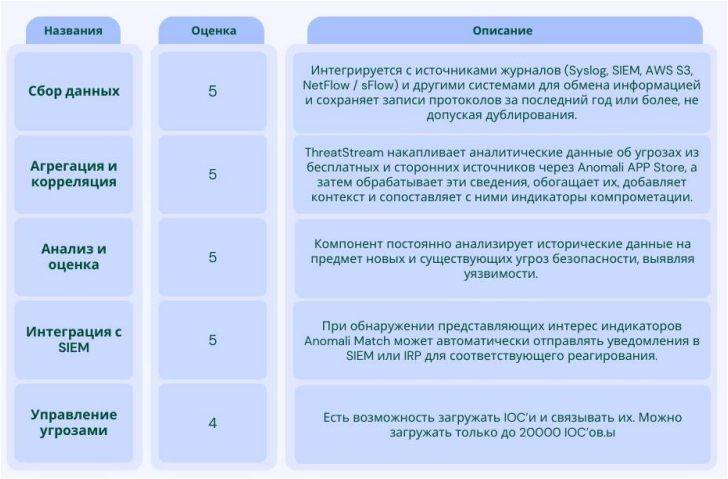
Stream – это функция в Anomali, которая помогает упростить процесс анализа угроз, предоставляя централизованную платформу для сбора, анализа и обмена информацией об угрозах. Платформа позволяет группам безопасности получать доступ и использовать широкий спектр источников информации об угрозах, включая информацию из открытых источников, каналы коммерческой информации и проприетарные источники информации.

Anomali Match – это функция платформы Anomali Threat Intelligence Platform, которая принимает данные от Stream, что позволяет организациям быстро и точно выявлять угрозы информационной безопасности и реагировать на них, также сопоставляя свою сетевую активность с всеобъемлющей и постоянно обновляемыми источниками данных индикаторов угроз. Платформа интегрируется с различными инструментами безопасности, включая брандмауэры, системы обнаружения вторжений и системы управления информацией и событиями безопасности (SIEM), для сбора данных о сети и безопасности в режиме реального времени. Затем собранные данные автоматически сопоставляются с индикаторами угроз в базе данных Anomali для выявления потенциальных угроз.

Anomali Match предоставляет организациям полезную информацию об угрозах, включая источник, тактику, методы и процедуры (TTP), используемые злоумышленником, что позволяет специалистам по безопасности быстро понять природу угрозы и принять соответствующие меры для ее устранения. Платформа также предоставляет возможность создавать настраиваемые каналы информации об угрозах и сотрудничать с другими организациями для обмена и получения информации об угрозах, что еще больше повышает точность и эффективность обнаружения угроз и реагирования на них [**Ошибка! Источник ссылки не найден.**].

Из вышеприведенной информации можно выделить следующие преимущества платформы Anomali Threat Intelligence Platform:

- Автоматизированный анализ и расставление приоритетов для угроз информационной безопасности;
- Настраиваемые информационные панели и отчеты для повышения прозрачности данных об угрозах;
- Функции совместной работы для обмена информацией об угрозах между командами и отделами (рис. 2).



Названия	Оценка	Описание
Сбор данных	5	Интегрируется с источниками журналов (Syslog, SIEM, AWS S3, NetFlow / sFlow) и другими системами для обмена информацией и сохраняет записи протоколов за последний год или более, не допуская дублирования.
Агрегация и корреляция	5	ThreatStream накапливает аналитические данные об угрозах из бесплатных и сторонних источников через Anomali APP Store, а затем обрабатывает эти сведения, обогащает их, добавляет контекст и сопоставляет с ними индикаторы компрометации.
Анализ и оценка	5	Компонент постоянно анализирует исторические данные на предмет новых и существующих угроз безопасности, выявляя уязвимости.
Интеграция с SIEM	5	При обнаружении представляющих интерес индикаторов Anomali Match может автоматически отправлять уведомления в SIEM или IRP для соответствующего реагирования.
Управление угрозами	4	Есть возможность загружать IOC'и и связывать их. Можно загружать только до 20000 IOC'ов.ы

Рисунок 2 – Anomali Threat Intelligence Platform краткий итог

EclecticIQ Threat Intelligence еще одна интересная зарубежная система Threat Intelligence. Платформа EclecticIQ Threat Intelligence разработана для содействия в кооперации между аналитиками информационной безопасности с помощью набора процессов в едином рабочем пространстве. Это позволяет командам по реагированию на инциденты (SOC, CERT и так далее) быстро получать полезную и релевантную информацию об угрозах, взаимодействовать с другими аналитиками, обновлять инструменты управления безопасностью и обмениваться информацией. Платформа включает в себя следующие компоненты: функциональный API для интеграции входящих и исходящих данных, систему оповещений на основе политик, расширенной логики поиска и матриц корреляции для сетевых графов, модули для создания различных отчетов, а также инструменты поиска и визуализации для обнаружения скрытых корреляций между большими наборами данных. Платформу можно реализовать в виде локальной инфраструктуры заказчика (on-premise), облачного решения или гибридной конфигурации [**Ошибка! Источник ссылки не найден.**].

Основные преимущества платформы включают расширение возможностей аналитиков информационной безопасности и улучшение их действий благодаря единому рабочему пространству, позволяющему анализировать угрозы в режиме реального времени, обмениваться информацией об угрозах между заинтересованными сторонами и существующими средствами безопасности через API, обмениваться данными между различными участниками Threat Intelligence на основе форматов STIX и TAXII, а также релевантную сортировку данных для фокусировки на наиболее актуальных угрозах [**Ошибка! Источник ссылки не найден.**]. Платформа также позволяет строить графы связей между индикаторами компрометации и внутренними артефактами, позволяющими просматривать связи между сущностями на основе их общих характеристик, что помогает поместить каждый фрагмент информации в правильный контекст (рис. 3).

Названия	Оценка	Описание
Сбор данных	4	С помощью API производится обмен информацией, связанной с угрозами, между существующими средствами защиты.
Агрегация и корреляция	3	Дает возможность связывать инциденты.
Анализ и оценка	5	расширение возможностей аналитиков информационной безопасности и повышение эффективности их действий за счёт единого рабочего пространства, позволяющего проводить анализ угроз в режиме реального времени
Интеграция с SIEM	5	Система отправляет запросы в режиме реального времени в SIEM
Управление угрозами	4	Поддерживается построение графов связей индикаторов компрометации и внутренних артефактов

Рисунок 3 – EclecticIQ Threat Intelligence краткий итог

Your Everyday Threat Intelligence (YETI) – это платформа анализа угроз с открытым исходным кодом, созданная Rapid7, ведущей компанией в области кибербезопасности. YETI был создан с целью предоставить организациям бесплатное решение с открытым исходным кодом для управления, анализа и обмена информацией об угрозах. Платформа позволяет организациям собирать, хранить и анализировать различные типы данных об угрозах из различных источников, включая каналы с открытым исходным кодом и коммерческие разведывательные данные, внутренние системы и отдельных экспертов. YETI предоставляет централизованный репозиторий данных об угрозах, упрощая организациям обмен информацией и совместную работу над угрозами безопасности. Платформа также оснащена мощным аналитическим механизмом, который может помочь организациям выявлять тенденции и закономерности в своих данных, предоставляя ценную информацию о потенциальных угрозах безопасности [**Ошибка! Источник ссылки не найден.**].

YETI поддерживает различные варианты интеграции, что позволяет легко интегрировать его с другими инструментами и платформами, используемыми организациями. Например, YETI интегрируется с системами управления информацией и событиями безопасности (SIEM), такими как ELK Stack, для предоставления аналитикам информации об угрозах в режиме реального времени. YETI также интегрируется с платформами аналитики угроз, такими как TheHive, чтобы обеспечить централизованное место для хранения и анализа данных аналитики угроз. Кроме того, YETI можно интегрировать с другими инструментами безопасности, такими как брандмауэры, системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS), для предоставления этим инструментам полезных данных об угрозах и повышения их общей безопасности [**Ошибка! Источник ссылки не найден.**].

Открытый исходный код YETI позволяет организациям настраивать платформу в соответствии со своими конкретными потребностями и интегрировать ее в существующую инфраструктуру безопасности. Это означает, что пользователи могут просматривать, изменять и даже расширять исходный код платформы, что делает ее более гибкой и подходящей для решения конкретных задач в рамках организации. Однако, открытый исходный код может представлять собой проблему для некоторых организаций, так как требует большего времени и усилий для поддержки и обновления.

Одним из преимуществ YETI является ее цена, так как это проект с открытым исходным кодом, он может быть бесплатным или стоить гораздо меньше, чем коммерческие платформы. Также YETI поддерживает множество форматов данных, включая STIX, TAXII и CybOX (рис. 4).

Названия	Оценка	Описание
Сбор данных	5	YETI предназначена для сбора, централизованного хранения и обогащения данных об угрозах и индикаторах компрометации из различных источников.
Агрегация и корреляция	3	Дает возможность связывать инциденты.
Анализ и оценка	1	Не производит анализ и оценку на уровне системы. Позволяет аналитикам информационной безопасности сосредоточиться на работе с инцидентами (реагирование, расследование и т.д.)
Интеграция с SIEM	1	Позволяет экспортировать данные в определяемые пользователем форматы для дальнейшей передачи другим инструментам наподобие SIEM.
Управление угрозами	4	Визуализация отношений между различными угрозами безопасности и индикаторами компрометации,

Рисунок 4 – Your Everyday Threat Intelligence краткий итог

Следующая платформа TI с открытым исходным кодом – Malware Information Sharing Platform (MISP), она разработана командой экспертов в области информационной безопасности в Европейском институте цифровых систем и прав (European Institute of

Computer Antivirus Research) в 2013 году. Она была разработана с целью улучшения обмена информацией об угрозах между участниками сообщества информационной безопасности.

MISP используется государственными и коммерческими организациями, а также агентствами по защите информации во всем мире. Она может интегрироваться с различными инструментами, такими как антивирусные программы, фаерволы, платформы SIEM и другие платформы обмена информацией об угрозах. Это позволяет организациям использовать информацию об угрозах, полученную от других участников сообщества, для улучшения своей защиты**.**

Malware Information Sharing Platform (MISP) имеет возможность интегрироваться с другими платформами, такими как:

- Open source системы обнаружения вторжений (IDS), такие как Suricata и Snort;
- Антивирусные программы, такие как ClamAV и McAfee;
- Системы контроля за соблюдением политик, такие как Palo Alto Networks и FortiGuard Labs;
- Системы контроля за безопасностью сети, такие как SIEM;
- Различные веб-службы, такие как аналитические службы, которые можно использовать вместе с MISP [**Ошибка! Источник ссылки не найден.**].

Интеграция с другими платформами позволяет обеспечить более глубокое и точное мониторинг сети и обеспечить быстрый и эффективный ответ на возможные угрозы (рис. 5).

Названия	Оценка	Описание
Сбор данных	4	Встроенные возможности совместного использования для упрощения обмена данными
Агрегация и корреляция	3	построение графа событий для создания и просмотра отношений между индикаторами компрометации и атрибутами
Анализ и оценка	1	Не производит анализ и оценку на уровне системы.
Интеграция с SIEM	3	Возможность автоматического обмена и синхронизации с другими сторонами
Управление угрозами	4	Построение графа событий для создания и просмотра отношений между индикаторами компрометации и атрибутами

Рисунок 5 – Malware Information Sharing Platform краткий итог

Заключение

В результате анализа различных систем Threat Intelligence, можно сделать вывод о том, что каждая из них имеет свои уникальные особенности, преимущества и недостатки. Каждая система предназначена для определенных сценариев использования, и правильный выбор зависит от конкретных потребностей и характеристик организации.

R-Vision TIP выделяется своей эффективностью в обнаружении угроз и интеграцией с различными средствами безопасности. Anomali Threat Intelligence Platform предоставляет широкий набор данных и акцентирует внимание на раннем обнаружении угроз. Cisco Threat Intelligence Director отличается высокой производительностью и надежностью, что делает его подходящим для критически важных систем.

EclecticIQ Threat Intelligence обеспечивает гибкость и масштабируемость, что делает его идеальным выбором для крупных организаций. Your Everyday Threat Intelligence, с фокусом на пользовательской дружелюбности, может быть предпочтителен для небольших предприятий. Malware Information Sharing Platform подчеркивает важность обмена информацией о вредоносных программах между сообществами.

В зависимости от конкретных потребностей организации, необходимо оценить интеграцию, совместимость, масштабируемость и производительность каждой системы. Рекомендуется также учитывать возможности адаптации к изменяющимся угрозам и будущим требованиям безопасности.

Исходя из данного анализа, рекомендуется принимать во внимание уникальные особенности каждой системы, чтобы обеспечить эффективное реагирование на современные

угрозы информационной безопасности и обеспечить безопасность информационных ресурсов.

Список литературы

1. M. Lee Cyber Threat Intelligence / M. Lee; Wiley, 2023. – 304 p.
2. Ozkaya E. Practical Cyber Threat Intelligence: Gather, Process, and Analyze Threat Actor Motives, Targets, and Attacks with Cyber Intelligence Practices / E. Ozkaya, 2022.
3. Moore R.O. III Cyber Intelligence-Driven Risk / R.O. Moore; Wiley, 2020. – 192 p.
4. Cyber A.R. Threat Intelligence / A.R. Cyber; Apress, 2021. – 207 p.
5. Hunting V.T. Cyber Criminals / V.T. Hunting; Wiley, 2020 . – 58 p.
6. Cloutier M. OSINT for Cybersecurity / M. Cloutier; Draft2digital, 2023.
7. Anomali Threat Intelligence Platform // URL: https://www.anti-malware.ru/products/anomali-threat-intelligence-platform (дата обращения: 04.03.2023).
8. Обзор рынка платформ и сервисов кибербразведки (Threat Intelligence) в России и в мире // URL: https://www.anti-malware.ru/analytics/Market_Analysis/Threat-Intelligence (дата обращения: 01.03.2023).
9. Краткий анализ рынка Threat Intelligence Platforms // URL: https://blog.volgablob.ru/?p=1842 (дата обращения: 08.12.2023).
10. Skillicorn D.B. Uwe Glässer Open Source Intelligence and Cyber Crime / D.B. Skillicorn, M.A. Tayebi; Springer International Publishing, 2020. – 251 p.
11. Martinez R. Incident Response with Threat Intelligence / R. Martinez; Packt Publishing, 2022. – 468 p.
12. Bou-Harb E. Cyber Threat Intelligence for the Internet of Things / E. Bou-Harb, N. Neshenko; Springer International Publishing, 2020. – 89 p.

References

1. M. Lee Cyber Threat Intelligence / M. Lee; Wiley, 2023. – 304 r. (In English).
2. Ozkaya E. Practical Cyber Threat Intelligence: Gather, Process, and Analyze Threat Actor Motives, Targets, and Attacks with Cyber Intelligence Practices / E. Ozkaya, 2022. (In English).
3. Moore R.O. III Cyber Intelligence-Driven Risk / R.O. Moore; Wiley, 2020. – 192 r. (In English).
4. Cyber A.R. Threat Intelligence / A.R. Cyber; Apress, 2021. – 207 r. (In English).
5. Hunting V.T. Cyber Criminals / V.T. Hunting; Wiley, 2020 . – 58 r. (In English).
6. Cloutier M. OSINT for Cybersecurity / M. Cloutier; Draft2digital, 2023. (In English).
7. Anomali Threat Intelligence Platform // URL: https://www.anti-malware.ru/products/anomali-threat-intelligence-platform (data obrashcheniya: 04.03.2023). (In Russian).
8. Obzor rynka platform i servisov kiberrazvedki (Threat Intelligence) v Rossii i v mire // URL: https://www.anti-malware.ru/analytics/Market_Analysis/Threat-Intelligence (data obrashcheniya: 01.03.2023). (In Russian).
9. Kratkii analiz rynka Threat Intelligence Platforms // URL: https://blog.volgablob.ru/?p=1842 (data obrashcheniya: 08.12.2023). (In Russian).
10. Skillicorn D.B. Uwe Glässer Open Source Intelligence and Cyber Crime / D.B. Skillicorn, M.A. Tayebi; Springer International Publishing, 2020. – 251 r. (In English).
11. Martinez R. Incident Response with Threat Intelligence / R. Martinez; Packt Publishing, 2022. – 468 r. (In English).
12. Bou-Harb E. Cyber Threat Intelligence for the Internet of Things / E. Bou-Harb, N. Neshenko; Springer International Publishing, 2020. – 89 r. (In English).

Т.М. Мехдиев, А.К. Шайханова*, Г.Б. Бекешова
Л.Н. Гумилёв атындағы Еуразия ұлттық университеті,
010000, Қазақстан Республикасы, Астана қаласы, Сәтпаев көшесі, 2
*e-mail: shaikhanova_ak@enu.kz

ҚАУІП-ҚАТЕРДІ БАРЛАУ ЖҮЙЕЛЕРІН ТАЛДАУ

Threat Intelligence (TI) – бұл ұйымдардың қауіпсіздігін арттыру үшін қолданылатын ақпараттық қауіпсіздікке төнетін немесе пайда болатын қауіптер туралы ақпарат. TI жүйелері

әртүрлі көздерден, соның ішінде ашық көздерден, жабық көздерден және серіктестер мен клиенттерден алынған деректерді жинайды және талдайды. Ті жүйелерін талдау-бұл жүйелердің деректерді жинау мен талдаудағы тиімділігін бағалау және ақпараттық қауіпсіздік шешімдерін қабылдау үшін пайдалы ақпарат беру процесі. Ақпараттық қауіпсіздікке төнетін қатерлер барған сайын күрделене түсетін қазіргі цифрлық әлемде Threat Intelligence (ti) жүйелерін талдау ақпараттық ресурстардың қауіпсіздігін қамтамасыз ету үшін маңызды болып табылады. Threat Intelligence-ақпараттық қауіпсіздікке төнетін қатерлерді анықтауға бағытталған ақпараттық қауіпсіздік қатерлері туралы деректерді жинау, талдау және түсіндіру процесі. Бұл тұрғыда ti жүйелерін талдау қауіптерді тиімді түсінудің және олардың алдын алу шараларын қабылдаудың маңызды құралы болып табылады.

Бұл мақалада Threat Intelligence жүйелерін талдаудың ерекшеліктері, артықшылықтары мен кемшіліктері қарастырылады. Мысалы, ТІ талдауын интрузияны анықтау жүйесінің (IDS) тиімділігін бағалау үшін пайдалануға болады. Талдау IDS шабуылдарының қандай түрлерін анықтай алатынын және қайсысын анықтай алмайтынын анықтай алады. Талдау нәтижелеріне сүйене отырып, IDS жүйесін жаңарту қажеттілігі немесе қосымша қорғаныс шараларын қосу туралы шешім қабылдауға болады.

***Түйін сөздер:** Қауіптер туралы, ашық көздер, ақпараттық қауіпсіздік, ақпаратты талдау, Ақпараттық қауіпсіздік қатерлері.*

T.M. Mekhdiev, A.K. Shaikhanova*, G.B. Bekeshova
L.N. Gumilyov Eurasian National University,
010000, Republic of Kazakhstan, Astana, Satpayev Str., 2
*e-mail: shaikhanova_ak@enu.kz

ANALYSIS OF THREAT INTELLIGENCE SYSTEMS

Threat Intelligence (TI) is information about current or emerging threats to information security that is used to enhance the protection of organizations. TI systems collect and analyze data from various sources, including open sources, closed sources, as well as data obtained from partners and clients. Analysis of TI systems is the process of evaluating the effectiveness of these systems in data collection and analysis, as well as in providing useful information for decision-making in the field of information security. In the modern digital world, where information security threats are becoming increasingly complex and sophisticated, the analysis of Threat Intelligence (TI) systems is becoming crucial for ensuring the security of information resources. Threat Intelligence is the process of collecting, analyzing, and interpreting data on information security threats aimed at identifying threats to information security. In this context, the analysis of TI systems serves as an important tool for effectively understanding threats and taking measures to prevent them. This article is dedicated to examining the features, advantages, and disadvantages of Threat Intelligence system analysis. For example, TI analysis can be used to evaluate the effectiveness of an intrusion detection system. (IDS). Analysis can identify which types of attacks an IDS can detect and which it cannot. Based on the analysis results, a decision can be made regarding the need to upgrade the IDS system or to add additional protective measures.

***Key words:** Threat Intelligence, open sources, information security, information analysis, information security threats.*

Сведения об авторах

Турадж Мехманоглы Мехдиев – магистрант 2-го курса; специальность информационной безопасности; Евразийский национальный университет имени Л.Н. Гумилева; Республика Казахстан; e-mail: mehdiev.t@gmail.com. ORCID: https://orcid.org/ 0009-0004-6771-1584.

Айгуль Кайрулаевна Шайханова – профессор кафедры информационной безопасности; Евразийский национальный университет имени Л.Н. Гумилева; Республика Казахстан; e-mail: shaikhanova_ak@enu.kz. ORCID: https://orcid.org/0000-0001-6006-4813.

Гульвира Бауржановна Бекешова – старший преподаватель кафедры информационной безопасности Евразийского национального университета имени Л.Н.Гумилева, Казахстан; e-mail: gulvirabauyrzhanovna@gmail.com. ORCID: https://orcid.org/0000-0002-1635-4693.

Авторлар туралы мәліметтер

Турадж Мехманоглы Мехдиев – 2 курс магистрант; ақпараттық қауіпсіздік мамандығы; Л.Н. Гумилёв атындағы Еуразия ұлттық университеті; Қазақстан Республикасы; e-mail: mehdiev.t@gmail.com. ORCID: https://orcid.org/ 0009-0004-6771-1584.

Айгуль Кайрулаевна Шайханова – ақпараттық қауіпсіздік кафедрасының профессор; Л.Н. Гумилёв атындағы Еуразия ұлттық университеті; Қазақстан Республикасы; e-mail: shaikhanova_ak@enu.kz. ORCID: https://orcid.org/0000-0001-6006-4813.

Гульвира Бауржановна Бекешова – Л.Н. Гумилев атындағы Еуразия ұлттық университетінің аға оқытушысы, Қазақстан; e-mail: gulvirabauyrzhanovna@gmail.com. ORCID: https://orcid.org/0000-0002-1635-4693.

Information about the authors

Turaj Mehmanogly Mehdiyev – 2st year master's degree; specialty of information security; Eurasian National University named after L.N. Gumilyov; The Republic of Kazakhstan; e-mail: mehdiev.t@gmail.com. ORCID: https://orcid.org/ 0009-0004-6771-1584.

Aigul Kairulayevna Shaykhanova – professor of the department of Information Security; Eurasian National University named after L.N. Gumilyov; Republic of Kazakhstan; e-mail: shaikhanova_ak@enu.kz. ORCID: https://orcid.org/0000-0001-6006-4813.

Gulvira Baurzhanovna Bekeshova – Senior Lecturer, L.N.Gumilev Eurasian National University, Kazakhstan; e-mail: gulvirabauyrzhanovna@gmail.com. ORCID: https://orcid.org/0000-0002-1635-4693.

Поступила в редакцию 17.10.2024
Поступила после доработки 21.10.2024
Принята к публикации 22.10.2024

https://doi.org/10.53360/2788-7995-2024-4(16)-8

МРНТИ: 81.93.29

А.Б. Какенова*, Б.К. Абдураимова, С.А. Сантеева
Л.Н. Гумилев атындағы Еуразия ұлттық университеті,
010008, Республика Казахстан, г. Астана, ул. Сатпаева, 2
*e-mail: akakenova1001@gmail.com

ЭЛЕКТРОНДЫҚ ПОШТА АРҚЫЛЫ ФИШИНГТІК ШАБУЫЛДАРДЫҢ АЛДЫН АЛУ ҮШІН ЖАСАНДЫ ИНТЕЛЛЕКТТІ ПАЙДАЛАНУ

Аңдатпа: *Бұл мақалада электрондық пошта арқылы фишингтік шабуылдардың қазіргі проблемалары мен жойқын әсерлері қарастырылады. Ұйымдарды деректердің бұзылуынан және ықтимал апатты салдардан қорғау үшін алдын алу шараларының маңыздылығы атап өтілді. Фишингтік шабуылдардың негізгі түрлері және тәуекелдерді тиімді азайту үшін жасанды интеллект (AI) негізіндегі шешімдерді енгізу қажеттілігі сипатталған. Жұмыста жасанды интеллект пен машиналық оқытуды қолдана отырып, фишингтің алғашқы белгілерін тану әдістері қолданылды. Әзірлеу үшін Python және Google Colab қолданылды, бұл деректерді тиімді талдауға және модельдерді оқытуға мүмкіндік берді. Ерекше әдістерді әзірлеуге және заманауи бағдарламалық жасақтаманы пайдалануға ерекше назар аударылды. Зерттеу нәтижесінде фишингтік шабуылдарды танудағы AI құралдарының жоғары тиімділігін растайтын деректер алынды. AI технологиялары фишингті анықтаудың дәлдігін едәуір арттырды және жаңа киберқауіптерге бейімделуді қолдады. Талдау көрсеткендей, AI қолдану шабуылдарды уақтылы анықтауға ғана емес, сонымен қатар алдын алу стратегияларын жасауға мүмкіндік береді. Нәтижелердің практикалық маңыздылығы-әзірленген әдістерді қолданыстағы қауіпсіздік жүйелеріне біріктіру мүмкіндігі. Жұмыс ақпаратты тұрақты қорғауды құру үшін технологиялық жетістіктер мен ұйымдастырушылық тәжірибелерді біріктіретін стратегиялық тәсілді ұсынады.*

Түйін сөздер: *спам, фишинг, ақпараттық қауіпсіздік, машиналық оқыту, сүзу, әдістер, қорғау, қиындықтар.*

Кіріспе

Электрондық пошта фишингі-бұл алаяқтық әдісі, онда жіберушілер өз хабарламаларын заңды сұраулар ретінде жасырады, олардың мақсаты алушылардың жеке мәліметтерін алу үшін алдау болып табылады. Жәбірленушілер қауіп-қатерден бейхабар болып, сақтандыру полистерін, банктік шоттар және әлеуметтік сақтандыру деректер сияқты құпия ақпаратты