МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

«МИРЭА – Российский технологический университет»

**РТУ МИРЭА**

Институт Искусственного Интеллекта

Кафедра «Информационная безопасность» (БК №252)

# КУРСОВАЯ РАБОТА

по дисциплине «Предупреждение, выявление и установление причин и условий компьютерных инцидентов»

**Тема курсовой работы:** «Проведение сравнительного анализа средств, реализующих технологию Threat Intelligence»

Студент группы ККСО-01-19: *Филиппов Д.В.*

Руководитель работы: *Гончаренко В.Е.*

Работа представлена к защите: «_____»
декабрь 2023 года

Оценка: «_____»

Москва 2023

# Оглавление

# Введение

На сегодняшний день наше общество находится на этапе активного и глубокого развития информационных технологий, что несомненно порождает как свои преимущества, так и свои недостатки. Одни из главных недостатков является угроза целостности, доступности и конфиденциальность информации. В отдельно конкретном случае под информацией могут пониматься различные моменты, например персональные данные пользователей некоторой социальной сети или же коммерческая тайна о разработке некоего продукта какой-то компании. Основной задачей социальной сети или компании обеспечить безопасность. Одним из инструментов обеспечения безопасности в современном мире является использование технологии Threat Intelligence.

Threat Intelligence – информация об актуальных угрозах и группировках киберпреступников, которая позволяет организациям изучить цели, тактику и инструменты злоумышленников и выстроить эффективную стратегию защиты от атак. Использование данной технологии сильно облегчит работу всем отделам компании связанных с обеспечением безопасности, а также позволит создать новые или укрепить старые инструменты превентивной безопасности. Все это необходимо для более точно детектирования угроз и атак, так как современный мир киберпреступников тоже не стоит на месте, придумываются различные технологии, шаги для обхода защиты, маскируются известные вирусные ПО.

В рамках текущей курсовой работы будут рассматриваться технологии, использующие совместно с Threat Intelligence, теоретические и практические моменты работы технологии, перспективы дальнейшего развития.

# Глава 1. Анализ текущего состояния в области построения технологий и систем Threat Intelligence

Область построения систем Threat Intelligence является достаточно перспективным направлением в современной информационной безопасности и соответственно очень активно развивается. В данном направлении появляются различные новые решения и технологии с ним связанные. Происходит тенденция к стандартизации данной области, потому что на текущей момент каких-то стандартов не существует, например для передачи отчетности или ее формирования.

На текущей момент уже существуют системы с использование технологии Threat Intelligence как зарубежные, так и отечественные. Ярким примером отечественных решений в данной области является Kaspersky Threat Intelligence, который включает в себя различные сервисы, отвечающие за решение задач, которые в свою очередь являются фундаментальными для самой технологии. Список задач, которые решает технология Threat Intelligence:

- Наблюдение за эволюцией кибератак;
- Сбор данных об угрозах;
- Анализ полученных данных;
- Структурирование и хранение данных;
- Формирование отчетов по угрозам;
- Оповещение об угрозах;
- Первоначальное реагирование.

## 1.1 Исследование процесса составления отчета об угрозах на основе использования технологии Threat Intelligence

Отчет об угрозах является главным элементом исследуемой технологии, так как центру, отвечающему за информационную безопасность или лицу, принимающему решение в данной области, необходимо понимать, с каким

типом атаки они столкнулись, чтобы принять соответствующие меры по противодействию. Ниже рассмотрим подробнее этот процесс.

### 1.1.1 Анализ структуры составления отчета об угрозах с использованием Threat Intelligence

Процесс составления отчета многогранен и включает в себя несколько этапов.

Этап подготовки собственной базы данных об угрозах является подготовительным, разведывательным, так как без него все-таки использование технологии Threat Intelligence будет неполным. Суть данного этапа заключается в сборе и обработке данных как из открытых источников и источников партнеров, так и использование собственного опыта устранения угроз. Сбор данных состоит из следующих действий:

- Сбор IP-адресов зараженных веб-ресурсов;
- Сбор хэшей файлов;
- Сбор меток времени;
- Сбор имен угроз.

Обработка данных стоит из следующих действий:

- Использование песочниц для анализа;
- Проверка аналитиком полученных данных;
- Использование статистических критериев;
- Использование инструментов для определения сходства.

Данный этап является достаточно важным, так как он экономит драгоценное время в случае возникновения угрозы безопасности.

Следующим этапом является формирование отчета на основе полученных данных из систем, детектирующих угрозы. Данный этап частично похож на предыдущий, так как представляет собой поиск данных и их обработку. В поиск данных входит обращение к своей базе данных угроз и

обращение к открытым источникам. Основными действиями является глубокий анализ идентификаторов угроз и поиск соответствующих зависимостей. К обработке данных относится их структурирование и фильтрация. Структурирование происходит при использование различных форматов, например STIX и MISP. Фильтрация данных подразумевает выставление приоритетов и удаление дублирующей информации из собранных данных.

*Таблица 1. Структура составления отчета с использованием Threat Intelligence*

| **Этап** | **Процесс** | **Процедура** | **Действие** |
|---|---|---|---|
| Подготовка собственной базы данных об угрозах | Сбор данных | Обращение к собственному опыту устранения угроз | Сбор IP-адресов зараженных веб-ресурсов |
| | | | Сбор хэшей файлов |
| | | | Сбор меток времени |
| | | | Сбор имен угроз |
| | | Обращение к стороннему опыту устранения угроз или к любым открытым источникам в сети Интернет | Сбор IP-адресов зараженных веб-ресурсов |
| | | | Сбор хэшей файлов |
| | | | Сбор меток времени |
| | | | Сбор имен угроз |
| | Обработка данных | Проверка собранных данных | Использование песочниц для анализа |

| | | | |
|---|---|---|---|
| | | | собранных данных |
| | | | Проверка аналитиком полученных данных |
| | | Фильтрация собранных данных | Использование статистических критериев |
| | | | Использование инструментов для определения сходства |
| Формирование отчета | Поиск данных | Обращение к собственной базе угроз | Глубокий анализ идентификаторов угроз |
| | | | Поиск соответствующих зависимостей |
| | | Обращение к сторонней базе угроз или к любым открытым источникам в сети Интернет | Глубокий анализ идентификаторов угроз |
| | | | Поиск соответствующих зависимостей |
| | Обработка данных | Структурирование данных | Использование формата STIX |
| | | | Использование формата MISP |

| | | | |
|---|---|---|---|
| | | Фильтрация данных | Удаление дублирующейся информации |
| | | | Установка приоритета угрозе |

### 1.1.2 Исследование методологической основы составления отчета об угрозах с использованием Threat Intelligence

*Таблица 2. Методологическая основа составления отчета с использованием Threat Intelligence*

| Этап | Процесс | Процедура | Действие | М. О. |
|---|---|---|---|---|
| Подготовка собственной базы данных об угрозах | Сбор данных | Обращение к собственному опыту устранения угроз | Сбор IP-адресов зараженных веб-ресурсов | RFC 791 |
| | | | Сбор хэшей файлов | RFC 1321 |
| | | | Сбор меток времени | RFC 8877 |
| | | | Сбор имен угроз | Name, hostname, domain |
| | | Обращение к стороннему опыту устранения угроз или к любым | Сбор IP-адресов зараженных веб-ресурсов | RFC 791 |
| | | | Сбор хэшей файлов | RFC 1321 |

| | | | | |
|---|---|---|---|---|
| | | открытым источникам в сети Интернет | Сбор меток времени | RFC 8877 |
| | | | Сбор имен угроз | Name, hostname, domain |
| | Обработка данных | Проверка собранных данных | Использование песочниц для анализа собранных данных | |
| | | | Проверка аналитиком полученных данных | Использование ГОСТов и внутренней документации |
| | | Фильтрация собранных данных | Использование статистических критериев | Использование математической статистики |
| | | | Использование инструментов для определения сходства | Использование отчетов, ранее полученных в ходе разведки либо аналитики |
| Формирование отчета | Поиск данных | Обращение к собственной базе угроз | Глубокий анализ идентификаторов угроз | |

| | | | | |
|---|---|---|---|---|
| | | | Поиск соответствующих зависимостей | |
| | | Обращение к сторонней базе угроз или к любым открытым источникам в сети Интернет | Глубокий анализ идентификаторов угроз | |
| | | | Поиск соответствующих зависимостей | |
| | Обработка данных | Структурирование данных | Использование формата STIX | Использование документации [1] |
| | | | Использование формата MISP | Использование документации [2] |
| | | Фильтрация данных | Удаление дублирующейся информации | |
| | | | Установка приоритета угрозе | Использование внутренней документации и ориентирован |

[1] https://oasis-open.github.io/cti-documentation/resources#stix-21-specification
[2] https://www.misp-project.org/documentation/

| | | | | |
|---|---|---|---|---|
| | | | | ие на OWASP 10 |

### 1.1.3 Построение структурно-функциональной схемы систем и средств. Исследование существующих систем, комплексов и средств, реализующих составления отчета об угрозах с использованием Threat Intelligence

Построим схему создания отчета об угрозах с использованием Threat Intelligence:

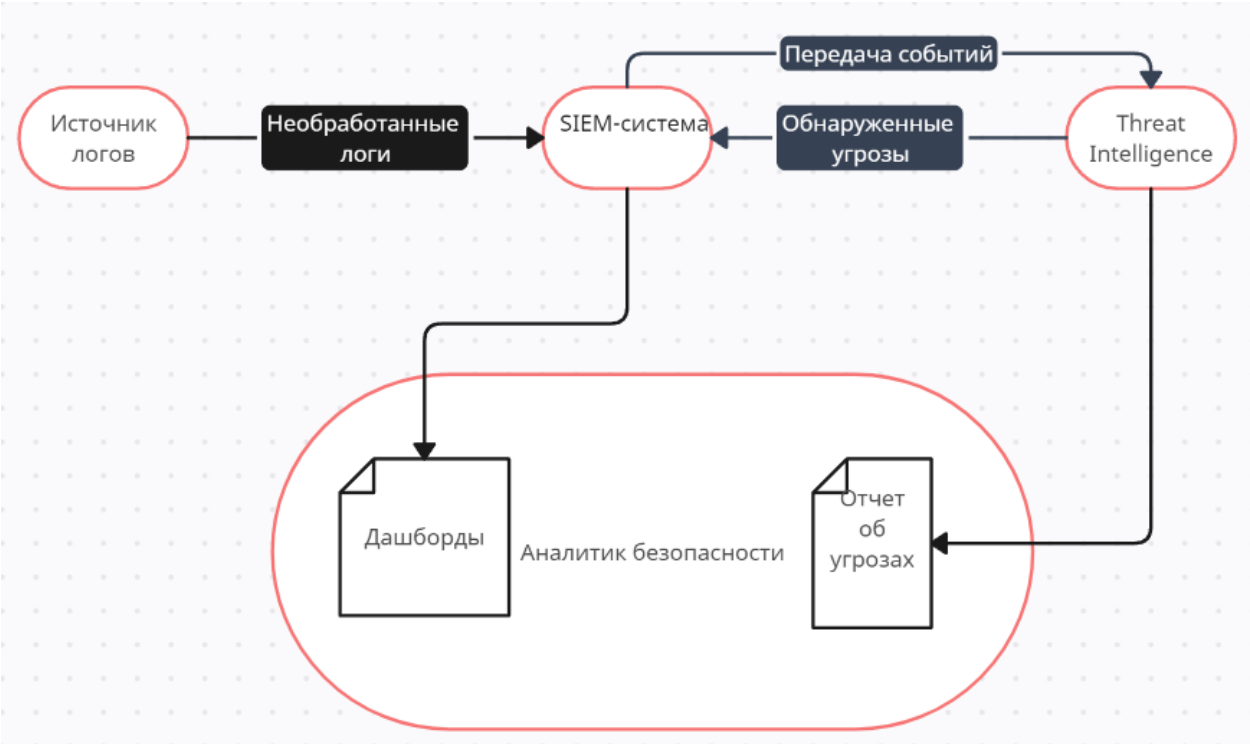


*Рисунок 1. Схема создания отчета об угрозах*

## 1.2 Анализ состава задач в области составления отчета об угрозах с использованием Threat Intelligence. Анализ предмета исследований – исследование составления отчета об угрозах с использованием Threat Intelligence

Прикладными технологиями являются технологии реализующиеся в Threat Intelligence.

### 1.2.1. Анализ структуры построения существующих прикладных технологий Threat Intelligence и их составляющих

В прошлых пунктах была рассмотрена теоретическая структура составления отчетности об угрозах с использованием Threat Intelligence. Прикладная структура никак не отличается от теоретической, все этапы ровно следуют теории описанной в таблице 1.

### 1.2.2. Исследование теоретических аспектов построения прикладных технологий Threat Intelligence, определение сценариев применения теоретической основы построения существующих прикладных технологий

Сбор имен угроз, меток времени, установленные IP-адреса зараженных веб-ресурсов, хэши представление собой исследование открытых ресурсов в сети Интернет или использование баз данных об угрозах партнеров.

Использование песочницы — это мощный инструмент, который позволяет исследовать исходные образцы файлов, находить индикаторы компрометации на основании поведенческого анализа и обнаруживать вредоносные объекты, которые не встречались ранее. Принятие аналитического решения на основе поведения файла при одновременном анализе памяти процессов, сетевой активности и прочих показателей – это оптимальный подход к пониманию современных комплексных целевых и APT-угроз.

Использование различных фильтрующих действий позволяет отсеивать менее значимую или дублирующую информацию в потоке данных, что значительно повышает эффективность обнаружение необходимой угрозы в критический момент.

Использование форматов для структурирования информации позволяет хранить и передавать данных об угрозах в удобном для компании формате, а также для более эффективной работы сервисов связанных с передачей данных,

так как если нет определенного стандарта по передаче и хранении данных, может повлечь за собой сбой.

# Заключение

# Список литературы

**Текущий документ не содержит источников.**