ТИТУЛЬНЫЙ ЛИСТ

Проведение сравнительного анализа средств, реализующих технологию Threat Intelligence.

РЕФЕРАТ

Расчетно-пояснительная записка содержит 39 страниц, 8 рисунков, 3 таблицы, 25 источников.

THREAT INTELLIGENCE, СРАВНИТЕЛЬНЫЙ АНАЛИЗ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ.

Объектом исследования являются технологии Threat Intelligence.

Предметом исследования является сравнение различных подходов исполнения технологии Threat Intelligence в целях обеспечения информационной безопасности вычислительных устройств коммерческих организаций и государственных предприятий.

Цель курсовой работы заключается в проведении сравнительного анализа TI-технологий с последующим выявлением фундаментальных свойств и отличий различных подходов исполнения киберразведки в области Threat Intelligence.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

В настоящем отчете о курсовой работе применяют следующие сокращения и обозначения:

TI	–	**T**hreat **I**ntelligence
SOC	–	**S**ecurity **O**peration **C**enter
SIEM	–	**S**ecurity **I**nformation and **E**vent **M**anagement
IoC	–	**I**ndicator **o**f **C**ompromise
SOAR	–	**S**ecurity **O**rchestration, **A**utomation, **R**esponse
MRTI	–	**M**achine **R**eadable **T**hreat **I**ntelligence
ИБ	–	Информационная безопасность
ПДн	–	Персональные данные
ПО	–	Программное обеспечение
ИСПДн	–	Информационная система [обработки] персональных данных

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем отчете о курсовой работе применяют следующие термины с соответствующими определениями:

TI — (Threat Intelligence, Данные о киберугрозах) информация об актуальных угрозах и группировках киберпреступников, позволяющая предприятиям изучить цели, тактику и инструменты злоумышленников для построения эффективной стратегии защиты от потенциальных и нежелательных атак [1].

SOC – (Security Operation Center, Центр мониторинга информационной безопасности) является структурным подразделением предприятия, отвечающее за своевременный и оперативный мониторинг IT-среды с целью предотвращения появления возможных киберинцидентов [2].

SIEM — система решений, объединяющая в себе два класса: **SEM** (**S**ecurity **E**vent **M**anagement, Управление событиями безопасности, управление событиями ИБ в режиме реального времени) и **SIM** (**S**ecurity **I**nformation **M**anagement, Управление информацией о безопасности, долгосрочное хранение и анализ данных) [3].

IoC – (**I**ndicator **o**f **C**ompromise) индикатор компрометации, под которым понимают наблюдаемый в сети или на конкретном устройстве объект/активность, с большой долей вероятности указывающий на несанкционированный доступ к системе. Индикаторы используются для обнаружения вредоносной активности на ранней стадии с целью предотвращения известных угроз ИБ [4].

ВВЕДЕНИЕ

С увеличением числа успешно проводимых компьютерных атак на объекты информационной инфраструктуры с последующими регулярными утечками как персональных данных пользователей, так и конфиденциальной и критической информации ограниченного доступа, среди специалистов в области информационной безопасности возрос предметный интерес к технологиям Threat Intelligence, направленным на своевременное выявление потенциальных угроз опережающего характера.

По данным аналитического портала [5], к четвертому кварталу 2033 года предсказывается рост инвестиций и суммарного капитала технической сферы TI до 55 млрд долларов. Представленный факт подтверждает предположение о все более возрастающей роли перспективной технологии в области информационной безопасности вычислительных систем и устройств. В связи с этим, данная курсовая работа будет посвящена углубленному изучению существующих на настоящий момент технологий Threat Intelligence с дальнейшим проведением сравнительного анализа имеющихся решений на рынке ИБ.

Новизна постановки исследовательского вопроса заключается в отсутствии в открытом доступе систематизированных материалов по структурированному изложению возможных характеристик и функциональных особенностей имеющихся в расположении технических отделов крупных предприятий и государственных учреждений инструментов технологии Threat Intelligence.

Актуальность выбранной темы обусловлена тем, что в настоящее время все больше возрастает потребность в применении обособленных средств программного и/или программно-аппаратного характера по сбору, анализу и превентивному применению информации об угрозах безопасности в автоматическом режиме без вмешательства сторонних лиц, привносящих в представленную систему вытекающие свойства включения человеческого фактора.

Более того, компания NTT DATA Americans, ежегодно публикующая аналитические сводки под названием «Global Threat Intelligence Report» [11], утверждает, что за последние несколько лет количество атак на ключевые сферы информатизации увеличилось на 30% (Рис. 1).

Рис. 1. Динамика количества проведения атак с 2021 по 2022 года [11].

Рост несанкционированных действий со стороны злоумышленников закономерно увеличивает спрос на Threat Intelligence решения, способные противостоять появляющимся угрозам.

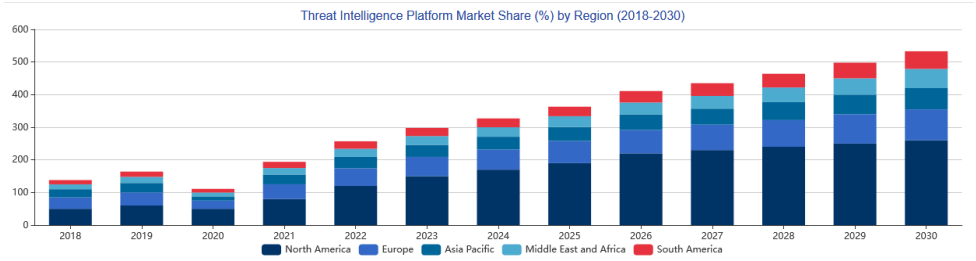

Рис. 2. Уровень роста коммерческих решений Threat Intelligence [12].

Приведенные выше аналитические данные и статистические расчеты подтверждают актуальность и своевременность проводимого исследования по выполнению сравнительного анализа TI-технологий.

Степень научной разработанности проблемы исследования

Одним из основных трудов по технологиям Threat Intelligence и смежной с ними области SIEM является книга «Security Information and Event Management (SIEM) Implementation» [6]. Авторы, являющиеся специалистами в области информационной безопасности, подготовили представленный научный труд в интересах всех технических специалистов, регулирующих информационные потоки в рамках закрытого контура собственных

предприятий с применением автоматического журналирования событий. Исследователи не обошли стороной и Threat Intelligence технологии, подробно описав и предложив пути по их практическому применению в работающих системах ИБ.

Начиная с 2020 года рассматриваемая область знаний стала привлекать все большее число кадров с богатым научно-исследовательским потенциалом, в результате чего стали появляться работы по технологиям TI. Среди таких исследований следует отметить статью команды Cyber Proof Research [7], которая в 2020 году опубликовала свое превью к вопросу совместного использования Искусственного Интеллекта и процесса сбора и разведки данных об угрозах и уязвимостях. Авторы твердо убеждены, что в настоящий момент стремительно приближается то время, когда человеческие возможности обработки информации достигнут своего физического предела, в результате чего инструментом решения предельных ограничений, возникающих в подобных ситуациях, является внедрение средств машинного обучения в Threat Intelligence и SIEM технологии.

Совместная работа 2020 года ученых из Греции и Великобритании [8] предлагает изучение в ознакомительном формате источников, способов и технических приемов по организации технологии Threat Intelligence, что послужило отправной точкой для последующего написания норвежскими исследователями статьи 2023 года «Модель анализа киберугроз: Таксономия, стандарты, онтология технологии Threat Intelligence» [9]. Обе научно-исследовательские работы содержат детальное описание ключевых методов и технологий исполнения Threat Intelligence в пространстве и сфере информационной безопасности.

Научная значимость и практическая ценность исследования заключается в систематизации накопленных знаний и опыта в зоне ответственности TI-технологий на актуальный момент выполнения научного исследования. Все полученные результаты могут быть успешно использованы для формирования детального представления об уровне технического

состояния Threat Intelligence по всему миру, что может послужить серьезным подспорьем для последующего анализа и принятия решений о выборе способов и средств исполнения современной технологии обнаружения и предсказания компьютерных инцидентов, атак и уязвимостей.

Объектом исследования являются технологии Threat Intelligence.

Предметом исследования является сравнение различных подходов исполнения технологии Threat Intelligence в целях обеспечения информационной безопасности вычислительных устройств коммерческих организаций и государственных предприятий.

Цель курсовой работы заключается в проведении сравнительного анализа TI-технологий с последующим выявлением фундаментальных свойств и отличий различных подходов исполнения кибербразведки в области Threat Intelligence.

Структура курсовой работы разбита на несколько логических частей:

– В вводной части курсовой работы определена актуальность темы, сформулированы цель и задачи исследования, выявлен объект и предмет исследования, обоснована научная новизна и практическая значимость работы, а также описана структура работы;

– Первая глава курсовой работы содержит исследование в области определения основных свойств, функциональных особенностей и назначения технологии Threat Intelligence, а также сведения о структурно-функциональных схемах средств и систем TI;

– Вторая глава содержит анализ ограничений существующих прикладных TI-технологий, а также требования по разработке современных Threat Intelligence технологий;

– Третья глава отражает основные направления дальнейших перспективных исследований предметной области научной работы;

– В заключении подводятся итоги исследования, обобщаются полученные результаты, а также сформулированы рекомендации для дальнейших исследований в предметной области.

1 Анализ текущего состояния в области построения TI-технологий и систем

Перед тем, как переходить к непосредственному предмету исследований, следует установить, какие сектора экономики относятся к ключевым потребителям технологии Threat Intelligence.

К главным корпоративным потребителям, имеющих непосредственный интерес во внедрении рассматриваемой технологии в собственную систему безопасности, можно отнести пять секторов экономики.

Малый и средний бизнес. Данная группа может включить Threat Intelligence в свою систему защиты информации с целью обеспечения защиты конфиденциальных сведений пользователей, обработка которых зачастую является одним из основных направлений предпринимательской деятельности компаний. Однако, как правило, из-за отсутствия высокой степени масштабирования подобные организации нередко не имеют собственной службы, обеспечивающей ИБ. В таком случае целесообразно использовании услуг отечественных центров SOC или создание внутреннего отдела защиты информации.

Международный бизнес. По предприятиям, сеть офисов которых распространена пор всему миру следует сделать отдельное замечание, связанное с тем, что компании, имеющие представительства на территории Российской Федерации в одностороннем порядке были отключены от иностранных поставщиков услуг обеспечения защиты данных. Более того, за последние два года количество атак, направленных на российские информационно-аналитические системы, достиг беспрецедентного уровня. Представленный факт служит неоспоримым аргументом в пользу использования и применения решений отечественных разработчиков по запуску и наладке технологии Threat Intelligence.

Субъекты КИИ. Организации, подпадающие под действие Федерального закона №187-ФЗ «О критической информационной структуре

РФ», в обязательном порядке необходимо иметь в собственной системе безопасности технологии TI. При отсутствии соответствующих технических мер по обеспечению информационной защиты ответственные лица предприятия подлежат юридическому преследованию в соответствии с законодательством РФ. В настоящее время крупнейшим сервисом данной защиты является «ГосСОПКА» (Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак) [15].

Организации, обрабатывающие персональные данные пользователей. Данные предприятия имеют в своей структуре ИСПДн, что автоматически накладывает на соответствующие компании обязательства по соблюдению и исполнению Федерального закона №152-ФЗ «О защите персональных данных граждан РФ». В соответствии с изменениями от 2022 года, все предприятия обязаны передавать в сервис «ГосСОПКА» сведения об инцидентах информационной безопасности, выявленных во внутренней информационно инфраструктуре. Данный факт предполагает наличие собственных технологий Threat Intelligence, без которых своевременное реагирование на киберугрозы не представляется возможным.

Главным катализатором развития системы защиты информации, в том числе при использовании таких технологий, как Threat Intelligence и SIEM, является Государство, которое из года в год вносит изменения в действующее законодательство, ужесточая контроль за методами и способами защиты конфиденциальных сведений граждан и иных физических и юридических лиц в соответствии с актуальными киберугрозами, развитие которых происходит с регулярной периодичностью.

В результате ухода иностранных компаний, предлагающих TI решения коммерческим и государственным предприятиям, произошло распределение и переформатирование существующего рынка на территории Российской Федерации, что положительно сказалось на развитии отечественных продуктов обеспечения киберразведки.

При проведении анализа текущего состояния в области построения TI-технологий и систем, важно определить, какие предприятия, специализирующиеся на создании и поддержании средств Threat Intelligence для массового сегмента, предлагают собственные решения в исследуемой области.

Выявление ключевых игроков данного сектора наглядно демонстрирует степень актуальности, востребованности и проработанности сферы TI, что может быть подтверждено их ролью и авторитетом на рынке коммерческих услуг, количеством предлагаемых решений, а также влиянием рассматриваемых предприятий на общее состояние информационной безопасности IT-компаний. Автор убежден, что авторитет перечисляемых ниже знаковых производителей ИБ-продуктов не подлежит сомнению, что напрямую демонстрирует высокую вовлеченность существующих современных технических специалистов в область построения TI-технологий.

Главными игроками предоставления рассматриваемых услуг считаются шесть компаний.

Kaspersky Threat Intelligence (KTI). Данный сервис является продолжением продукта Kaspersky Security Network, помимо выполнения основных задач TI позволяющий собирать данные о вредоносной активности в сети Интернет, что генерирует актуальные TI-фиды в режиме реального времени. Уровень исполнения кибербразведки KTI получил международное признание, в результате чего данный продукт был включен в список ведущих мировых лидеров в области Threat Intelligence [12], куда также вошли сервисы США, Японии и Израиля.

BI.Zone ThreatVision. Основное направление деятельности – подготовка индивидуальных стратегий нетривиальных проектов по противодействию злоумышленникам. Существует собственный центр реагирования на киберугрозы.

Group-IB (ныне F.A.C.C.T.) Threat Intelligence. Компания всегда специализировалась на расследовании инцидентов в банковской сфере. На

основе полученного опыта за годы работы в данной области было разработано собственное решение по созданию сервиса предупреждению компьютерных атак.

PT Cybersecurity Intelligence. TI-сервис компании Positive Technologies был разработан на основе результатов длительной разработки инструментов по оценке систем защищенности предприятий, после чего весь накопленный опыт был использован для разработки технологии Threat Intelligence на основе открытых и коммерческих TI-фидов в «связке» с собственными данными.

R-Vision Threat Intelligence Platform (TIP). Компания поддерживает программно-аппаратный продукт по являющийся сублимацией TI-фидов сторонних коммерческих организаций и открытых источников, в совокупности с данными отраслевого центра реагирования FinCERT (Центр реагирования кредитно-финансового сектора).

Securtiy Vision Threat Intelligence Platform (TIP). Поддерживает широкий функционал, осуществляя полный и детализированный цикл выявления и предупреждения киберугроз, что подробно рассматривается в пункте 1.2 представленного научного исследования.

1.1 Определение объекта исследований, анализ состава задач предметной области объекта исследований

В первую очередь, Threat Intelligence – это процесс сбора, анализа и применения информации об угрозах безопасности. Согласно аналитическому порталу [10], визуально TI-технологию в упрощенном виде можно представить так, как это показано на Рис. 3.

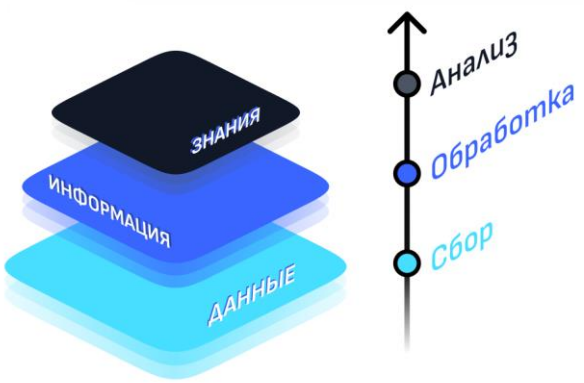

Рис. 3. Визуальное представление Threat Intelligence [10]

Под *данными* понимаются необработанные сведения с набором статистики. *Информация* – подготовленные к отчету данные. *Знания* являются результатом работы технологии Threat Intelligence и представляют из себя результат анализа данных и информации, сформированных на первых двух этапах обработки получаемых сведений.

Существует несколько тематических направлений развития технологии Threat Intelligence, которые могут быть применены сотрудниками отделов безопасности на предприятиях. Самым универсальным решением является использование *Threat Intelligence Platform* (TIP), что позволяет хранить, использовать и распространять сведения об актуальных угрозах в режиме реального времени с большого числа прикладных источников информации.

Другой, более узконаправленный подход исполнения методов киберразведки делится на четыре тематических класса (рис. 4).

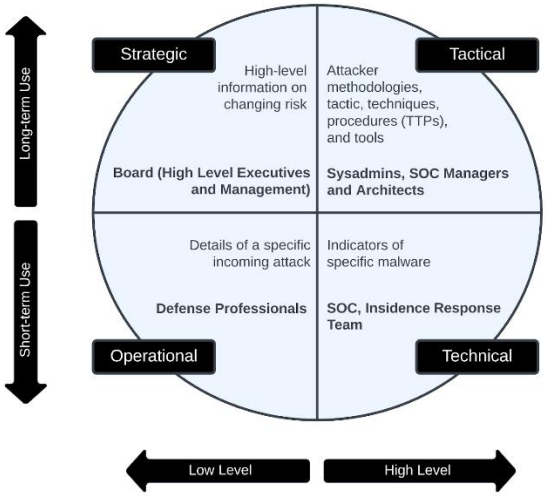

Рис. 4. Типы Threat Intelligence [17].

– *Technical* – основной задачей является контроль, мониторинг и совершенствование технологии защиты средствами взаимообмена значительных объемов предварительно необработанных машиночитаемых данных.

Техническая информация о киберугрозах относится к конкретным, пригодным для принятия мер сведениям об угрозах, фокусируясь на индикаторах компрометации (IOCS), таких как вредоносные IP-адреса, URL-адреса URL-адресов или хэш-значения вредоносных программ. Он включает в себя сложные детали киберугрозы, такие как характеристики используемого вредоносного ПО и тактика, применяемая злоумышленниками. Эта информация жизненно важна для Центров управления безопасностью (SOC) и групп реагирования на инциденты, помогая им понять ландшафт угроз, расставить приоритеты предупреждений и разработать эффективные стратегии защиты.

Ценность технической информации о киберугрозах заключается в ее своевременном распространении, поскольку IoCs могут быстро устаревать. При эффективном внедрении в системы безопасности техническая информация о киберугрозах может ускорить процессы обнаружения, обеспечивая раннее выявление атак. Это также помогает идентифицировать подозрительный сетевой трафик или IP-адреса, связанные с распространением вредоносных программ и спама.

– *Tactical* – ключевым объектом анализа является так называемое «Tactics, Technics & Procedures» (TTP) (информация о деятельности несанкционированных пользователях, нарушителях, хакерах). Нередко используется в Threat Hunting.

Тактическая разведка угроз сосредоточена на анализе цепочки кибератак злоумышленников, предлагая глубокое понимание их методов и стратегий, таких как индикаторы компрометации (IoCs), сигнатуры вредоносных программ и схемы трафика. Кроме того, подробно описываются IP-адреса с плохой репутацией, вредоносные URL-адреса и данные,

полученные из файловых журналов, скомпрометированные учетные данные, связанные с расширенными постоянными угрозами (APT), программами-вымогателями и фишинговыми кампаниями.

– *Strategic* – тонкая настройка, предписание и контроль исполнения организационных вопросов управления и распределения персонала организации с последующей оценкой потенциальных рисков, на основании чего строится политика информационной безопасности. Стратегическая аналитика угроз предоставляет всестороннюю информацию о кибербезопасности, акцентируя внимание на потенциальных угрозах и затратах, связанных с кибердеятельностью. Как правило, данный подход используют руководители высшего звена.

В получаемой аналитической информации используется подход, основанный на оценке риска, с вниманием на последствиях риска и возможностях, что может послужить основой для принятия решений относительно распределения бюджета или укомплектования персонала для защиты критически важных активов.

– *Operational* – непосредственное расследование киберинцидентов, ежедневный поиск и анализ функционирующей инфраструктуры. Оперативная разведка угроз раскрывает, как противники планируют, проводят и поддерживают свои кампании, предоставляя более четкую картину всего ландшафта угроз.

Оперативная разведка угроз – стратегическое использование данных для понимания того, "кто", "почему" и "как" стоит за каждой кибератакой. "Кто" относится к атрибуции, выявлению вовлеченных в угрозу субъектов или групп. Вопрос "почему" направлен на определение их мотивации или намерений, таких как финансовая выгода, политические потрясения или промышленный шпионаж. Раздел "Как" углубляется в тактику, методы и процедуры (TTP), которые субъекты угроз используют для выполнения своих атак.

1.2 Анализ структуры построения существующих TI-технологий

Идея Threat Intelligence заключается в регулярном обновлении текущей информации о существующих угрозах информационной инфраструктуре замкнутого контура отдельно взятого предприятия посредством анализа данных широкого спектра тематических блоков аналитических сведений. В процессе сбора и анализа информации технология Threat Intelligence опирается на такие сведения, как:

– Общедоступные TI-фиды;
– Социальные сети;
– log-файлы;
– База данных УБИ;
– Платформу дампов malware;
– Тематические сообщества.

На основе получаемых данных, после их обработки, принимаются решения по методике дальнейшей настройки и эксплуатации действующей политики информационной безопасности. Представленный список не является исчерпывающим, однако встречается в большинстве сервисов, специализирующихся на выявлении компьютерных угроз.

Если рассматривать технологию TI более широко, то можно разбить процесс ее функционирования на четыре этапа, предложенных в соответствии с методологией CREST (Табл. 1).

Таблица 1. Структура Threat Intelligence технологий

Этап	Процесс	Процедура	Действие
Планирование и направление	Подготовка тактико-технического задания	Технические мероприятия	Выбор или определение имеющегося оборудования (коммутаторы, роутеры…)
			Формирование представления об IoC, протоколах и технических средствах
		Организационные мероприятия	Определение типа разведывательной информации, подлежащей сбору
			Налаживание взаимодействие между конечными подразделениями с CTI отделом
		Отслеживание актуальных источников угроз	Мониторинг MITRE, УБИ ФСТЭК, официальных источников
			Контроль информации в dark web
		Составление тепловой карты	Выявление возможных векторов проведения атак

		ATT&CK MITRE Navigator	Формирование Дорожной карты инструментов и методов кибератак
Сбор данных	Сбор внутренних источников	Исследование отчетов об уязвимостях и инцидентах ИБ	Анализ имеющейся Базы уязвимостей и инцидентов
			Журналирование и протоколирование событий ИБ
		Контроль сетевых журналов, host-журналов	Применение Syslog, WEF
			Использование технологии SIEM; Настройка и сбор TI-фидов
	Сбор внешних источников	Разведка на основе открытых источников (OSINT)	Автоматический мониторинг соц. сетей
			Использование инструментальных возможностей WHOIS, Catalog CVE…
		Анализ вредоносного ПО	Проведение статического анализа
			Проведение динамического анализа
Анализ информации	Нормализация и обработка данных	Группировка тематических IoC, набор контекстов	Обработка ACL (Access Control List)
			Исследование log-файлов и данных Дампы malware
		Разбор	Выявление наблюдаемых аномалий и событий, MRTI
			Группировка артефактов и разведданных после срабатывания событий
	Анализ данных	Анализ информации с пограничных устройств	Сбор данных с IDS/IPS
			Контроль Firewall, WAF; Проверка локализации атаки
		Анализ и контроль трафика	Сбор и анализ статистики SNMP, NetFlow
			Исследование RMON – Remote Monitoring
Распространение разведданных и обратная связь	Распространение разведданных	Координация действий с внутренними отделами ИБ и организациями TI	Отчетность перед SOC, Incident Response, Red Team
			Оповещение внутренних служб безопасности и конечных потребителей
		Рассылка информации	Отправка отчетов, файлов STIX/MISP
			Распространение IoC, служебных сообщений, TTPs
	Сбор обратной связи	Фиксирование отчетных материалов	Журналирование и архивирование полученных данных
			Внесение изменений в соответствии с рекомендациями и отчетами об уязвимостях
		Переход на этап Планирование и направление	Корректировка ТТЗ с учетом полученного опыта; Перенастройка политики ИБ
			Старт очередного цикла технологии Threat Intelligence

Некоторые информационные порталы расширяют четыре этапа до шести:

1. Requirements (Требования). Масштабирование и расширение Threat Intelligence.
2. Collection (Сбор [данных]). Сбор необработанных данных о потенциальных угрозах.
3. Processing (Обработка [данных]). Обработка данных, полученных на втором этапе. Ключевыми параметрами являются IoC, SIEM, SOAR.
4. Analysis (Анализ). Анализ и интерпретация обработанных данных.
5. Dissemination (Распространение). Этап распространения сведений об угрозах и возможных векторах проведения атак.
6. Feedback (Обратная связь). Сбор сведений и результатов кибербразведки от участников информационного обмена.

1.2.1 Исследование методологической основы построения базовых TI-технологий

Вопрос методологии настройки, организации и проведения технологии Threat Intelligence представляет собой весьма нетривиальную и в то же время критически важную область знаний, так как от верного выбора структурной модели кибербразведки зависит результат обеспечения информационной безопасности защищаемых критических объектов информационной инфраструктуры.

На сегодняшний день существует два подхода к определению методологии обеспечения Threat Intelligence.

Модель Detection Maturity Model (DML – Степень готовности обнаружения киберугрозы) была сформулирована и предложена исследователем Райаном Стиллсоном через четыре года после резкого роста рынка TI – в 2014 году [22]. DML хорошо применима в случаях определения

уровня готовности конкретной компании противодействовать имеющимся киберугрозам в соответствии с разведданными об их применимости в рассматриваемой инфраструктуре.

Данная модель имеет 10 тематических уровней, на основании которых формируется итоговая оценка информационной системы (Рис. 5).

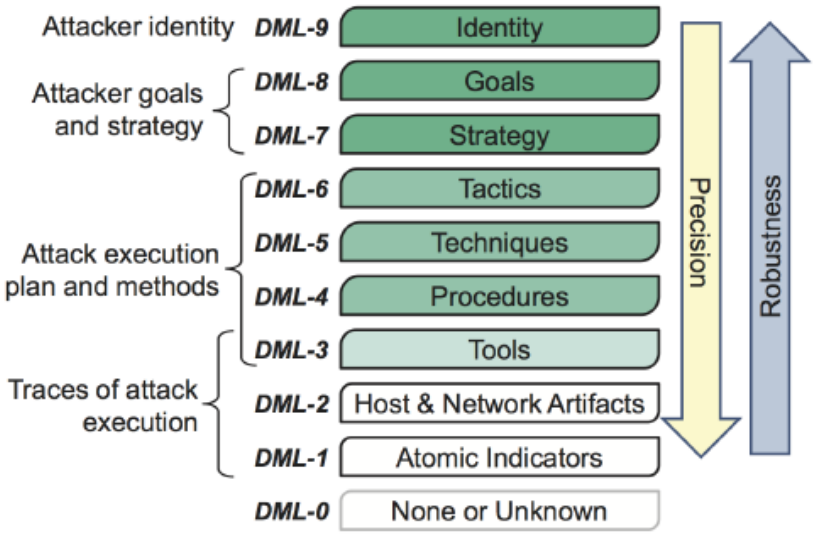

Рис. 5. Методология TI: уровни модели DML.

Из представленного рисунка видно, что по мере того, как растет надежность системы (синяя стрелка, направленная вверх), снижается точность представления киберугроз (желтая стрелка, направленна вниз). Чем выше уровень DML (в направлении от ‘0’ до ‘9’), тем более уверенно можно утверждать, что исследуемая организация имеет высокий уровень готовности по противодействию потенциальному появлению внешних угроз, что находит незамедлительное отражение в количестве и качестве обрабатываемых аналитических данных.

На основе методологии DML группа норвежских исследователей предложила усовершенствованную модель по определению векторов атак, нашедшую свое отражение в работе «Cyber threat Intelligence Model», опубликованной в 2023 году [9]. Схематичное отображение результатов работы ученых представлено на рис. 6 в виде структурной схемы модели Cyber Threat Intelligence Model.

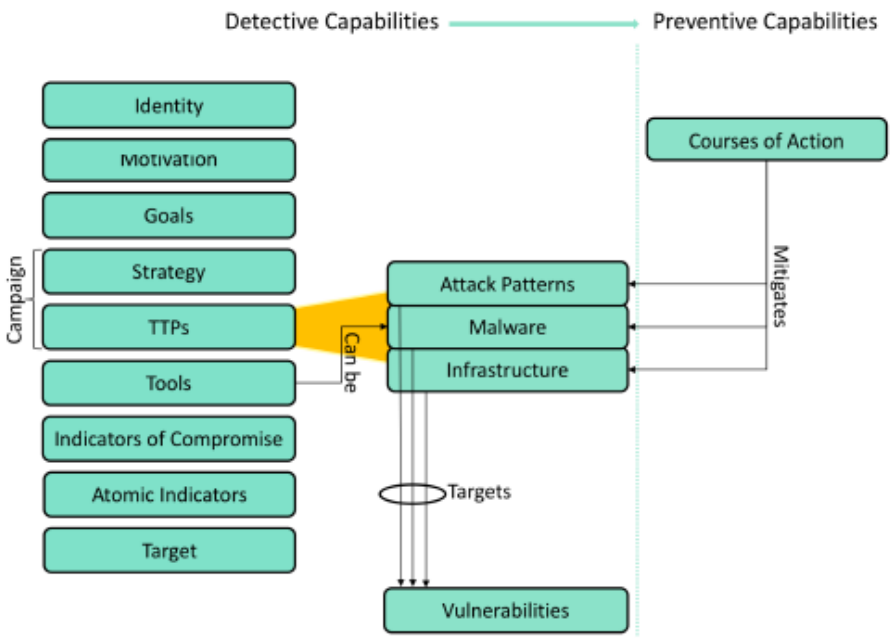

Рис. 6. Методология TI: Модель CTIM.

Identity (Идентификация нарушителя). Первичные сведения о злоумышленнике могут быть как установленными данными о физическом лице, так и юридическая информация об организации, филиалах групп хакеров или отдельных стран. Собранные сведения позволяют идентифицировать поведенческие характеристики субъекта, мотивации, цели и технические возможности.

Motivation (Мотивация нарушителя). Мотивация определяет движущую силу, которая определяет действиям атакующего. В процессе атаки цели злоумышленника могут меняться, но мотивация в большинстве случаев остается прежней. Знание мотивации субъекта угрозы позволяет сузить круг целей, на которых может быть сосредоточена основные технологические мощности киберпреступника, что помогает специалистам информационной безопасности сосредоточить свои ограниченные защитные ресурсы на наиболее вероятных сценариях нападения.

Goals[1] (Задачи, цели). В зависимости от того, как организована атака, изначально конечная цель может быть неизвестна. Зачастую на первых этапах

[1] Цель – это когнитивное представление желаемой конечной точки, которое влияет на оценки, эмоции и поведение [23].

атаки отделы ИБ могут лишь определить направление и стратегию поведения нарушителя. Сама же цель может быть сформулирована как кортеж из двух понятий – «Действие–Объект». К числу общераспространенных целей относят хищение интеллектуальной собственности, повреждение инфраструктуры, компрометация конкурентов.

Strategy (Стратегия). Стратегия – это нетехническое высокоуровневое описание планируемой атаки. Так как в арсенале злоумышленника имеется целый набор методов и техник по достижению поставленных перед ним задач, наибольшее, чего можно ожидать от параметра стратегия – предварительное представление о том, какой именно подход может использовать источник угрозы.

TTPs (Tactics, Technics and procedures). Блок «Тактика, техника и процедуры» характеризует поведение противника с точки зрения того, как он планирует достичь своих целей.

Attack Pattern (Схема атаки). Описывает поведение злоумышленников, которое они используют для осуществления своих атак.

Malware (Вредоносные программы, ПО). Характеризует программное обеспечение, внедряемое в защищаемую систему с целью подвергнуть под угрозу цель атаки с точки зрения конфиденциальности, целостности или доступности обрабатываемой информации.

Infrastructure (Инфраструктура). Уровень описывает систему, программную службу и любой иной связанный физический или виртуальный ресурс, предназначенный для поддержки технических операций, таких как использование приобретенных доменов для поддержки управления и контроля вектора атаки, доставки вредоносного ПО в целевую информационную среду, функционирование фишинговых сайтов.

Tools (Инструменты). Инструменты включают в себя как специальное программное обеспечение (СПО) из арсенала нарушителя, так и общедоступное программное обеспечение, предназначенное для станадртных задач мониторинга систем безопасности, но используемое для злонамеренных

целей (к примеру, сканирование уязвимостей и сети, удаленное выполнение процессов, PowerShell).

IoC (Индикаторы компрометации). Элементы защиты, используемые инструментами кибербезопасности для обнаружения несанкционированных вторжений. IoC служат вспомогательными артефактами к системам защиты и предоставляют контекстную информацию в дополнение к поведенческим данным.

Atomic Indicators (Атомарные индикаторы). Атомарные индикаторы имеют ограниченный контекст и короткий срок хранения информации, из-за чего являются скорее дополнением к основным механизмам защиты, нежели самостоятельной единицей обеспечения защиты информации. Индикаторы могут включать адреса электронной почты, доменные имена и IP-адреса.

Target (Цель). Представляет собой объект, на который направлена атака.

Course of Action (Направление атаки). Характеризует меры, принимаемые для реагирования и предотвращения атак.

1.2.2 Построение структурно-функциональной схемы Threat Intelligence

Говоря об общей схеме работы технологии Threat Intelligence, можно выявить фундаментальную последовательность действий при выполнении задачи киберразведки (Рис. 7).

Предлагаемая схема опирается на десятилетний опыт планомерного развития индустрии TI-технологий, а также научные работы по подходам к построению методологической базы построения Threat Intelligence.

На этапе детектирования угрозы происходит обработка больших массивов информации с целью поиска и выявления аномального поведения информационной системы, либо определения присутствия зловредных

приложений в инфраструктуре сети. Зачастую TI используется в паре с SIEM-технологиями для повышения вероятности обнаружения киберугрозы.

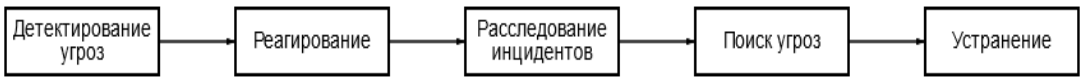

Рис. 7. Схема отдельно взятой итерации работы TI-технологии [14].

В процессе постоянного мониторинга при нахождении критических IoC, происходит реагирование на событие с дальнейшим расследованием зафиксированного инцидента. На этом шаге происходит определение отдельно взятых угроз и анализ новых, ранее не документированных уязвимостей, с активным использованием операционных и тактических данных.

После осуществляется «Threat Hunting» (поиск угроз), где осуществляется построение маршрутов и векторов потенциальных атак злоумышленников, формируется методологическая база потенциальной деятельности несанкционированных пользователей, обновляются индикаторы компрометации.

На заключительном этапе применяются меры организационно-технического характера по устранению уязвимостей и нивелированию всех выявленных и неблагоприятных возможных вариантов дальнейшего развития событий с функционированием в системе разрушающего программного воздействия извне.

1.3 Анализ состава задач стандартизации в области построения TI-технологий

В связи с тем, что сфера Threat Intelligence является широкой областью знаний в пространстве информационной безопасности, для регулирования деятельности специалистов в области ИБ с применением элементов TI-технологий существует ряд стандартов, владение которыми позволяет

унифицировать существующие подходы по использованию инструментов киберразведки.

Основополагающей базой знаний является классификация MITRE ATT&CK Framework (Adversarial Tactics, Techniques and Common Knowledge). Данная система представляет собой матрицу тактик, техник и процедур, активно применяемые злоумышленниками. Для корректной настройки системы безопасности и TI-технологии следует составить тепловую карту потенциальных направлений атак предприятия для получения минимальной вероятности компрометации всей системы со стороны атакующих группировок и отдельных хакеров. Аналогичные сведения рекомендательного и ознакомительного характера содержит База Угроз безопасности информации (УБИ) ФСТЭК.

В более широком смысле все имеющиеся стандарты, к которым обращаются специалисты ИБ, делятся на 3 категории:

– Enumerations (дословно – перечисления, список).

– Scoring Systems (Рейтинговая система).

– Sharing Standards (Стандарты совместного использования/применения).

Enumerations.

Threat Agent Library, TAL (Библиотека угроз) представляет собой набор стандартизированных определений и описаний для отображения ключевых представителей угроз. Библиотека не отображает отдельных субъектов угроз, однако, активно используется для идентификации физических лиц или процессов расследования реальных событий, связанных с инцидентами безопасности. Целью TAL является поддержка управления рисками с конкретным выявлением угроз. Используя данный набор данных, специалисты по безопасности имеют возможность заранее выстраивать защиту от известных угроз.

В 2015 году Тим Кейси представил авторскую таксономию определения мотивации нарушителей [24]. Результаты теоретического исследования

определяет движущие силы, которые вынуждают субъектов угроз совершать незаконные и противоправные действия. Знание этих факторов способно указать на характер ожидаемых стратегий кибервоздействия.

Common Vulnerabilities and Exposures, CVE (Распространенные уязвимости и угрозы) – список записей общеизвестных уязвимостей информационной безопасности в пакетах свободно распространяемого программного обеспечения.

National Vulnerability Database, NVD (Национальная база данных уязвимостей) – хранилище данных управления уязвимостями, сформированное на основе стандартов, представленных с использованием протокола автоматизации контента безопасности (SCAP, Security Content Automation Protocol). NVD выполняет анализ CVE, опубликованных в имеющейся базе знаний. Результатом этого анализа являются получение показателей серьезности (Common Vulnerability Scoring System — CVSS), связи с типами уязвимостей (Common Weakness Enumeration — CWE) и заявления о применимости (Common Platform Enumeration — CPE), а также другие ценные метаданные, представляющие интерес для аналитиков киберугроз.

Common Platform Enumeration, CPE (Список платформ) – спецификация классов программного и программно-аппаратного обеспечения, применяемого в критической информационной инфраструктуре.

Common Weakness Enumeration, CWE (Список распространенных уязвимостей) – библиотека распространенных уязвимых мест программного и аппаратного обеспечения.

Common Attack Patterns Enumerations and Characteristics, CAPEC (Список общих шаблонов атак) – ориентирован на обеспечение безопасности приложений. CAPEC описывает общие атрибуты и методы, используемые злоумышленниками для эксплуатации изветных слабых мест.

Adversarial Tactics, Techniques and Common Knowledge, ATT&CK (Матрица атак ATT&CK). Матрица атак ориентирована на описание сетевой

защиты и описывает этапы жизненного цикла противника «до» и «после» кибератаки. Стандарт способствует предсказанию поведения злоумышленников, поведенческого анализа, обогащения информации о киберугрозах, оценке слабых мест в защите, оценке зрелости SOC.

Scoring Systems.

Common Vulnerability Scoring System, CVSS (Система оценки уязвимостей) – стандарт, целью которого является оценка уязвимостей на основе уровня их опасности. CVSS полезен при определении приоритета предпринимаемых действий, необходимых по устранению уязвимостей.

Common Weakness Scoring System, CWSS (Система оценки слабых мест КИИ). Является частью проекта CWE и включает в свой состав механизм оценки и определения приоритетности слабых мест ПО с использованием двух десятков различных факторов.

Разница между CVSS и CWSS заключается в том, что первый оценивает конкретные уязвимости программного обеспечения (уязвимость уже обнаружена и проверена), тогда как второй стандарт ориентирован на оценку слабых мест программного обеспечения, исходя из имеющейся неполной информации.

Sharing Standards.

Structured Threat Information eXpression (STIX) является одним из самых актуальных и востребованных исследований существующих инициатив по обмену информацией об угрозах в сфере Threat Intelligence технологий. В первую очередь STIX – это гибкий и расширяемый язык представления, используемый для передачи всей информации об известных на текущий момент угрозах. Архитектура STIX включает в себя индикаторы, инциденты, тактики противника, методы и процедуры злоумышленников, стратегии, наборы инструментов вторжений, субъекты угроз, цели и способы противодействия.

OpenIOC, разработанный компанией Mandiant, является расширяемой схемой XML, которая описывает технические характеристики,

идентифицирующие известные угрозы и методологии злоумышленника совокупно с иными видами доказательств компрометации. Все данные набора OpenIOC получены из атомарных индикаторов низкого уровня и индикаторов компрометации.

2 Анализ ограничений существующих прикладных TI-технологий, проведение их классификации. Формирование требований по разработке современной TI-технологии, их классификация и обоснование.

В рамках проведенного детального и углубленного исследования основ TI-технологии был определен объект Threat Intelligence, проведен анализ состава задач и область применения кибербразведки, а также анализ структуры построения технологии Threat Intelligence. Все предварительные научные наработки послужат отправной точкой для анализа ограничений существующих прикладных технологий с их классификацией, для чего текущие подходы по практическому исполнению Threat Intelligence будут систематизированы по имеющимся и применяемым стандартам построения TI-систем в контексте DML методологии.

Таблица 2 отражает пересечения уровней реагирования на возникающие угрозы среди наиболее распространенных стандартов Threat Intelligence.

Табл. 2. Анализ стандартов TI по уровням реагирования на угрозы.

Стандарты	Identity	Motivation	Goal	Strategy	TTP	Tool	IoC	Atomic Indicator	Target	COA
STIX 1 [18]	Θ	Θ	Θ	Θ	Θ	Θ	Θ	Θ	Θ	Θ
STIX 2 [19]	Θ	Θ	Θ	Θ	Θ	Θ	Θ	Θ	Θ	Θ
MAEC [20]							Θ			
OpenIoC [21]					Θ	Θ	Θ	Θ		

Из полученных данных следует, что практиками, обладающими наиболее широким покрытием возникающих потребностей в предоставлении подробной информации о потенциальных векторах атаки, являются стандарты STIX 1 и его более актуальная версия STIX 2. Более того, в соответствии с анализом [25], такие стандарты, как MAEC – являются узкопрофильными и в действительности встречаются реже. Однако, следует учитывать, что применение каждого набора определенных практик и методов выявления

злонамеренных воздействий строится исходя из задач, преследуемых заказчиком, в виду чего использование MAEC и OpenIoC может найти самостоятельное применение, либо использоваться в кооперации с более фундаментальными и устоявшимися STIX версий 1 и 2.

Давая некоторую характеристику стандарту STIX, стоит отметить, что его развитие длится уже более десяти лет, а новые регулярно выпускаемые редакции с нововведениями актуальных атак и угроз выполняется под контролем организации OASIS, чья структура включает в себя более 50 компаний, входящих в комитет по «Cyber Threat Intelligence».

Инструментарий STIX включает в себя мощные технические возможности по описанию существующих угроз, ее взаимосвязи и технические артефакты. Главные принципы стандарта:

– Выразительность;
– Расширяемость;
– Гибкость;
– Читаемость;
– Автоматизируемость.

Формат данных, собираемый и интерпретируемый вычислительными устройствами, предоставляется в виде «.txt» или «.csv», в виду простоты и наглядности отображения информации (данная практика была перенята другими стандартами). Сведения об угрозах описываются в виде связного графа, узлами которого являются STIX Domain Objects (SDO), а ребрами – STIX Relation Objects. Выражаясь более лаконично, отметим, что SDO – это сущности, отображенные в таблице 2, по которым происходит сравнительный анализ сформированных стандартов.

Минус стандартов STIX – высокий уровень вхождения в предметную область для технических специалистов, только начинающих погружаться в сферу Thread Intelligence.

Отдельно стоит отметить набор техник и методов киберразведки – MISP. Этот стандарт является open-source платформой, на данный момент – не является межотраслевым стандартом, однако, предпринимаются предпосылки по переходу в статус RFC стандарта.

В таблице отсутствует MISP по причине собственных и немногочисленных сущностей, не пересекающихся напрямую со своими аналогами из смежных стандартов:

Event (Событие). Инцидент или аналитический отчет.

Event attributes (Атрибуты события). Своеобразные индикаторы компрометации IoC, отражающие свойства конкретной киберугрозы.

Object (Объект). Объединяет атрибуты по заранее согласованному признаку.

Tag (Тег). Метка классификации. Настраиваются пользователем, либо определяются сформировавшимися техническими документами.

Sighting (Обнаружение). Сведения о времени, месте и сопутствующих условиях обнаружения отдельно взятого атрибута.

Galaxy (Дословно: Галактика). Описывает взаимосвязь объектов или атрибутов с подробным описанием атрибутов (их контекстом).

Наравне с обособленными сущностями, не коррелирующих в явном виде с распространенными уровнями реагирования на угрозы в других стандартах, к минусам MISP относят слабую детерминированность и неполную типизированность взаимосвязей и правил их использования.

Следующая таблица содержит сравнительный анализ устоявшихся классификаций угроз в соответствии с уровнями реагирования DML.

Табл. 3. Анализ классификации угроз по уровню реагирования.

Таксономия	**Identity**	**Motivation**	**Goal**	**Strategy**	**TTP**	**Tool**	**IoC**	**Atomic Indicator**	**Target**	**COA**
TAL	Θ									
TAM	Θ	Θ								
CVE								Θ		
NVD								Θ		
CPE								Θ		
CWE					Θ			Θ		Θ
CAPEC					Θ		Θ			Θ
ATT&CK	Θ				Θ	Θ				
CVSS								Θ		
CWSS								Θ		

Из полученных результатов можно сделать закономерный вывод, что все десять этапов позволяют выявить значительное количество угроз, которые относятся к основным существующим уязвимостям, которые отслеживаются и контролируются сообществом технических специалистов по всему миру.

Так же можно заключить, что поверхностное отношение к настройке технологии Thread Intelligence хотя бы на одном из представленных этапов грозит серьезными последствиями, так как б*о*льшая часть киберугроз может быть выявлена исключительно на одном промежутке законченного цикла выявления и отслеживания несанкционированного воздействия на защищаемые информационные инфраструктуры.

В ходе проведения сравнительного анализа ограничений существующих прикладных технологий Threat Intelligence, была выполнена окончательная классификация существующих стандартов и методов обеспечения превентивной защиты предприятий. Также были установлены ограничения существующих методик и практик по организации технической составляющей кибербразведки. Данные ограничения были наглядно отображены в таблицах, где отображаются возможности тех или иных техник по проведению кибербразведки исходя из классификации широко распространённых угроз.

На основе полученных выводов ответственным лицам в сфере обеспечения информационной безопасности следует формировать соответствующие требования по настройке Threat Intelligence на предприятиях, а также учитывать применяемые стандарты в контексте тех возможностей, которые они предоставляют для превентивного выявления атак и своевременного реагирования на их последствия.

3 Определение перспективных направлений исследований в данной предметной области

Технологии Threat Intelligence насчитывают более десяти лет развития прикладных инструментов и действенных методов выявления и реагирования на возникающие киберугрозы. За прошедшее время методики и тактики противодействия злоумышленникам были доведены до максимального уровня, стандарты регулярно обновляются в соответствии с вновь публикуемыми уязвимостями, однако, остается открытым вопрос одного из самых слабых мест, на первый взгляд, казалось бы, автоматизированной системы Threat Intelligence – человеческий фактор.

Учитывая регулярно возрастающие объемы обрабатываемой информации становится очевидно, что даже целые ИБ отделы с высококвалифицированными специалистами не в состоянии своевременно выявлять и реагировать на индикаторы компрометации и другие факторы, характеризующие вероятность эксплуатирования уязвимостей нарушителями. Более того, существующие вычислительные устройства, без сомнения превосходно справляющиеся со своими задачами по кибербразведке, обладают ограниченным потенциалом, что сказывается на скорости и качестве реагирования на оценку текущей обстановки в ИТ инфраструктуре.

Одним из путей устранения сложившихся преград на пути к созданию наиболее результативной технологии Threat Intelligence, является применение возможностей машинного обучения. Искусственный интеллект способен не только оперативно выявлять отклонения от штатной работы систем защиты, но и строить предсказательные модели поведения злоумышленников, на основании чего в дальнейшем могут приниматься ключевые решения по изменению средств защиты информации, что нераздельно связано с политикой построения бюджета организации, а это в свою очередь является

очень чувствительным фактором для всех коммерческих и государственных предприятий.

Анализ угроз на основе искусственного интеллекта относится к использованию искусственного интеллекта, в частности больших языковых моделей (Large Language Models, LLM), для решения таких проблем, как «перегрузка» вновь возникающими угрозами, сложные функциональные прикладные инструменты и нехватка узкопрофильных специалистов в области кибербезопасности. LLM могут обрабатывать огромные объемы данных, расширяя охват отслеживания цифровых угроз и обеспечивая более глубокое представление актуальной ситуации за счет объединения данных из нескольких источников.

По мнению многочисленных аналитиков, такое привлечение высокотехнологичной области в сферу обеспечения защиты информации средствами Threat Intelligence видится в обозримом будущем – в интервале 5-10 лет. Помимо искусственного интеллекта ожидается внедрения ряда других технологий и организационно-технических мер и решений, отображенных на графике на Рис.8.

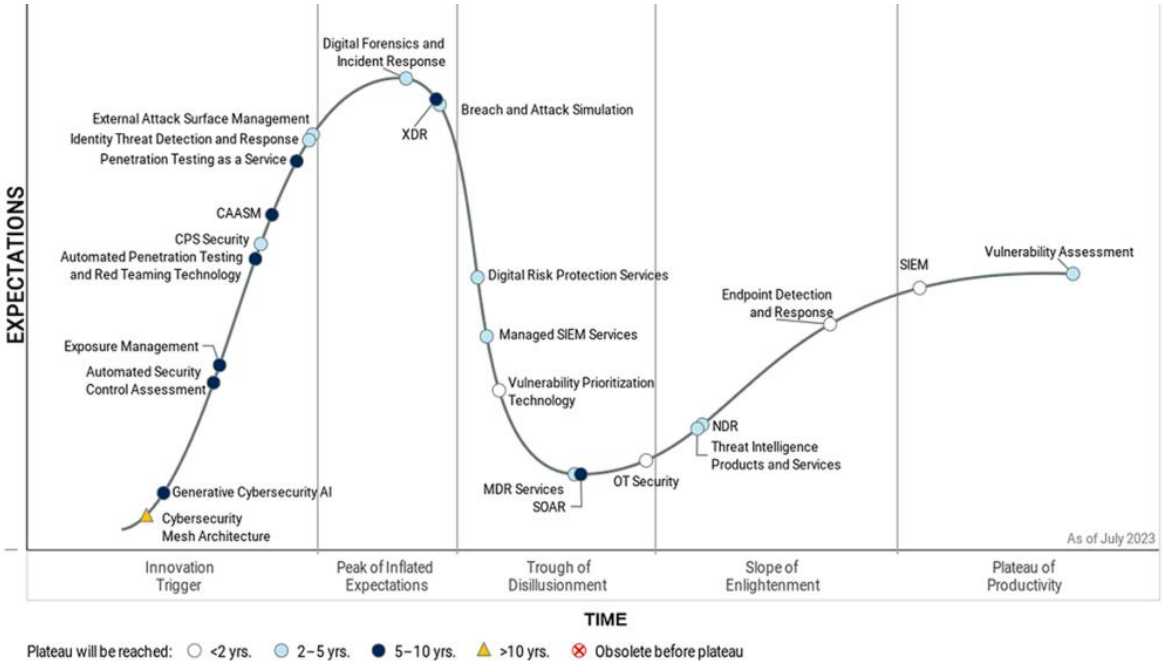

Рис. 8. График развития интереса к высокотехнологичным областям обеспечения Информационной безопасности (на 07.2023) [13].

Помимо повсеместного внедрения технологий Threat Intelligence автору также видится необходимость в комплексном и междисциплинарном взаимодействии между предприятиями критической инфраструктуры по обмену информацией и опытом по обнаружению и отражению атак. Так, в качестве примера подобного взаимодействия может послужить опыт CERT – Computer Emergency Response Team, имеющий налаженный обмен данными между финансовым и государственным секторами.

Наравне с Threat Intelligence следует использовать возможности SIEM-технологии, которые не столько заменяют, сколько дополняют друг друга. Следует уделять больше внимания предварительной настройке систем для получения максимально релевантной информации, что также достигается при помощи фокуса поиска данных на конкретной стране или регионе.

Важным следствием ухода иностранных TI решений с российского рынка является снижение конкуренции среди отечественных разработок. На первый взгляд, при недобросовестном отношении со стороны вендоров такое явление может привести к ухудшению качества и эффективности проведения кибербразведки. Однако, в последние годы наблюдается тенденция в ужесточении контроля за исполнением отечественными разработчиками требований регуляторов и государства, а также привлечение высококвалифицированных специалистов и расширение количества и зоны покрытия распределительных центров реагирования на компьютерные инциденты, что неизменно приведет сферу защиты информации на новый этап развития по превентивные противодействия угрозам, направленным на подрыв национальных интересов страны.

ЗАКЛЮЧЕНИЕ

В представленной курсовой работе была определена актуальность темы исследования, обоснована научная новизна и практическая значимость выполняемой работы. Автор определил основные свойства и функциональные возможности технологии Threat Intelligence, а также систематизировал обобщенную информацию с помощью структурно-функциональной схемы средств и систем TI.

Был проведен анализ ограничений существующих прикладных TI-технологий, а также определены требования по разработке современных технологий Threat Intelligence. Наконец, были отражены основные направления дальнейших перспективных исследований в рассматриваемой предметной области научной работы.

Цель курсовой работы была полностью достигнута, был успешно проведен сравнительный анализ TI-технологий с последующим выявлением фундаментальных свойств и отличий различных подходов исполнения киберразведки в области Threat Intelligence.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Threat intelligence: Данные о киберугрозах // Kaspersky. Encyclopedia. URL: https://encyclopedia.kaspersky.ru/glossary/threat-intelligence/ (дата обращения: 17.09.2023).
2. Центр мониторинга информационной безопасности (Security Operations Center, SOC) // Kaspersky. Encyclopedia. URL: https://encyclopedia.kaspersky.ru/glossary/security-operations-center-soc/ (дата обращения: 18.09.2023).
3. SIEM (Security information and event management) // Kaspersky. Encyclopedia. URL: https://encyclopedia.kaspersky.ru/glossary/siem/ (дата обращения: 20.09.2023).
4. Индикатор компрометации (Indicator of Compromise, IoC) // Kaspersky. Encyclopedia. URL: https://encyclopedia.kaspersky.ru/glossary/indicator-of-compromise-ioc/ (дата обращения: 20.09.2023).
5. Threat Intelligence Market Snapshot 2023 to 2023 // Threat Intelligence Market. URL: https://www.futuremarketinsights.com/reports/threat-intelligence-market (дата обращения: 20.09.2023).
6. D. Miller, S. Harris, S. Vandyke. "Security Information and Event Management (SIEM) implementation". McGrawHill (2011): 496.
7. Cyber Proof Research Team. Artifcial Intelligence and Threat Intelligence: Better Together. 2020.
8. A. Ramsdale, S. Shiaeles, N. Kolokotronis. A Comparative Analysis of Cyber-Threat Intelligence Sources, Formats and Languages. // MDPI Electronics, 2020, Vol.9, p. 824.
9. V. Mavroeidis, S. Bromander. Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence. // EISIC, 2023. DOI: 10.1109/EISIC.2017.20.
10. Threat Intelligence // Информационно-техническое издание Xaker. URL: https://xakep.ru/2023/07/04/threat-intelligence/?ysclid=lowrjxitzw341207025 (дата обращения: 17.10.2023).

11. Global Threat Intelligence Report // NTT DATA. URL: https://us.nttdata.com/en/insights/global-threat-intelligence-report (дата обращения: 17.10.2023).
12. Threat Intelligence Platform Market Report 2023 (Global Edition) // Qnitive Market Research. URL: https://www.cognitivemarketresearch.com/threat-intelligence-platform-market-report (дата обращения: 17.10.2023).
13. The Hype Cycle for Security Operations // Gartner Report. URL: https://www.exabeam.com/library/gartner-report-hype-cycle-for-security-operations-2023/ (дата обращения: 17.10.2023).
14. Threat Intelligence: применение на практике. // Security Vision. URL: https://safe.cnews.ru/articles/2022-09-18_threat_intelligence_chto_eto_takoe_i_kak_primenit (дата обращения: 17.10.2023).
15. ГосСОПКА. Официальный сайт. URL: https://g-sopka.ru/ (дата обращения: 17.10.2023).
16. MITRE ATT&CK. Positive technologieas. URL: https://mitre.ptsecurity.com/ru-RU/techniques/product/pt-nad?utm_source=habr&utm_medium=article&utm_campaign=matrixPTNAD (дата обращения: 17.10.2023).
17. Cyber Threat Intelligence. // PICUS. URL: https://www.picussecurity.com/resource/glossary/what-is-cyber-threat-intelligence (дата обращения: 17.10.2023).
18. S. Barnum, “Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX ™),” MITRE Corporation, vol. 11, 2012.
19. OASIS CTI TC, «Structured Threat Information Expression (STIX) 2.0» // URL: https://oasis-open.github.io/cti-documentation/, 2017. (дата обращения: 17.10.2023).
20. Mitre, «Malware Attribute Enumeration and Characterization» // URL: https://maec.mitre.org (дата обращения: 17.10.2023).

21. Mandiant Corporation, «Sophisticated Indicators for the Modern Threat Landscape: An Introduction to Open IOC» // URL: http://www.openioc.org/resources/An_Introduction_to_OpenIOC.pdf, 2013. (дата обращения: 17.10.2023).
22. S. Bromander, A. Jøsang, and M. Eian. «Semantic Cyberthreat Modelling» in STIDS, 2016, pp. 74–78.
23. A. Fishbach and M. J. Ferguson. «The goal construct in social psychology». 2007.
24. T. Casey. «Understanding cyber threat motivations to improve defense». Intel White Paper, 2015.
25. Threat Intelligence: стандарты обмена данными. // URL: https://habr.com/ru/companies/rvision/articles/553534/ (дата обращения: 21.10.2023).