ИССЛЕДОВАНИЕ МЕТОДОВ ФОРМИРОВАНИЯ ИНДИКАТОРОВ КОМПРОМЕТАЦИИ ОТ ВНУТРЕННИХ ИСТОЧНИКОВ ИНФОРМАЦИОННЫХ И КИБЕРФИЗИЧЕСКИХ СИСТЕМ

Мещеряков Р.В.[1], Исхаков С.Ю.[2]

Цель работы: *исследование методов формирования индикаторов компрометации внутри инфраструктуры для применения в системах защиты информационных и киберфизических систем.*

Метод исследования: *системный анализ открытых источников данных об индикаторах компрометации, способах их извлечения и методах применения при организации киберразведки внутри защищаемой инфраструктуры и систематизация знаний.*

Полученный результат: *сформулированы актуальные проблемы извлечения индикаторов компрометации от внутренних источников в информационных и киберфизических системах. Предложено алгоритмическое обеспечение для применения таких индикаторов в процессах киберразведки. Сформулированы базовые сценарии применения индикаторов компрометации от внутренних источников при обработке динамических потоков данных об угрозах в условиях изменяемых векторов атак.*

Установлено, что в отрасли киберразведки на сегодняшний день отсутствует унификация в части формирования индикаторов компрометации на основе данных защищаемых систем и дальнейшего обмена информацией между различными средствами защиты, но при этом имеют место ряд доминирующих форматов обмена подобными данными. В ходе исследования рассмотрены и структурированы задачи поиска и извлечения данных из внутренних источников для обогащения систем киберразведки и выявления целенаправленных методов атак на основе применения собственных наборов индикаторов компрометации и предложены методы их решения.

Научная новизна: *систематизированы методы формирования индикаторов компрометации внутри защищаемой инфраструктуры. Разработано алгоритмическое обеспечение применения индикаторов от внутренних источников и предложены базовые сценарии обработки таких данных для защиты киберфизических систем в условиях изменяемых векторов атак.*

Ключевые слова: *индикатор компрометации, киберразведка, контекст, киберфизическая система, система управления событиями безопасности, обогащение, ранжирование.*

DOI:10.21681/2311-3456-2023-6-35-49

Введение

Действительность сегодняшнего дня обуславливает постоянное изменение ландшафта киберугроз, поэтому в современном мире большинство компаний активно применяют системы обнаружения и предотвращения вторжений для защиты своей инфраструктуры. Системы подобного класса позволяют обнаруживать и сигнализировать о подозрительных действиях на периметре сети или на одном из внутренних хостов, однако зачастую обнаружение происходит лишь постфактум, когда уже зафиксированы последствия действий злоумышленников. Кроме того, во многих случаях атака может быть не зафиксирована, поскольку в системах защиты отсутствуют необходимые правила детектирования,

1 Мещеряков Роман Валерьевич, доктор технических наук, профессор, главный научный сотрудник ИПУ РАН, Москва, Россия. E-mail: mrv@ieee.org, ORCID: 0000-0002-1129-8434.

2 Исхаков Сергей Юнусович, кандидат технических наук, начальник отдела анализа и реагирования на компьютерные инциденты ПАО «Промсвязьбанк», Москва, Россия. E-mail: sergey@iskhakov.ru, ORCID: 0000-0003-3346-9262.

учитывающие актуальные изменения в ландшафте киберугроз.

Поэтому решение задачи обнаружения и предотвращения атак на современные информационные и киберфизические системы требует наличия механизмов, позволяющих выявлять ранее неизвестные методы и тактики действий злоумышленников. Применение классических средств защиты, например, средств антивирусной защиты или систем обнаружения вторжений на основе сигнатур, в данном случае весьма ограничено, поскольку подобные технологии не позволяют выявлять атаки с применением легитимного программного обеспечения и определять последовательность действий, способные привести к инцидентам. Кроме того, в современных системах число классических средств защиты информации (СЗИ) зачастую так велико, что генерируемые ими уведомления о возможных инцидентах требуют тщательного профилирования.

Для выявления передовых техник взлома на ранних стадиях атаки сегодня активно применяются механизмы кибербразведки (threat intelligence, TI) [1], включающие в себя сбор и анализ информации о злоумышленниках в части изучения техник, тактик и процедур, используемых при атаках. Одним из основных методов кибербразведки является использование индикаторов компрометации (indicator of compromise, IoC) [1,2] для обогащения СЗИ в информационных и киберфизических системах. IoC представляют собой технические данные, которые можно использовать для идентификации действий злоумышленников, отделяя их при этом от действий легитимных пользователей системы и штатных процессов ее функционирования. Индикаторы компрометации – один из результатов процесса кибербразведки по сбору информации об угрозах. Они могут применяться на операционном и тактическом уровнях кибербразведки [3] для выявления вредоносных объектов или действий и атрибуции их с известными угрозами. Проактивный подход позволяет обеспечить постоянное обновление знаний о киберугрозах и предотвращать атаки, сценарии которых еще не выявляются имеющимися СЗИ.

Поскольку эффективное применение индикаторов компрометации позволяет влиять на скорость реагирования на угрозы, то обсуждению данной проблемы и выдвижению различных подходов и методов посвящено множество исследований отечественных и зарубежных авторов, а также материалов профильных конференций. Активное обсуждение методов кибербразведки мировым научным сообществом отражает актуальность развития данной отрасли научного знания и формированию научно-методологической базы. Однако, результаты исследований, рассмотренные далее, свидетельствуют о том, что в отрасли кибербразведки отсутствуют комплексные решения по формированию индикаторов компрометации на основе данных, генерируемых внутри защищаемых инфраструктур. Большинство научных работ, а также коммерческих продуктов, ориентировано на работу с внешними источниками данных. С одной стороны, внутри инфраструктуры промышленных систем имеется множество источников данных, на основе которых можно организовать процесс формирования индикаторов компрометации. С другой стороны, на практике внутренняя кибербразведка сопряжена со значительными трудозатратами при низкой вероятности быстрого получения результатов. Помимо персонала, сопровождающего средства защиты и системы, необходимо нанимать в штат специалистов для анализа и практического применения подобной информации. К выстраиванию кибербразведки внутри инфраструктуры и работе с внутренними источниками приступают, когда основные процессы информационной безопасности уже находятся на высоком уровне зрелости.

В случае, если команда специалистов уже сформирована, то в инфраструктурах, где процессы уже ИБ выстроены, реальных инцидентов обычно немного, и они однотипны. Таким образом, в настоящее время в научной литературе практически не представлено методическое обеспечение по выстраиванию процессов кибербразведки внутри защищаемых инфраструктур. Настоящая статья посвящена исследованию проблем развития внутренней кибербразведки и вопросам формирования индикаторов компрометации на основе данных от внутренних источников.

1. Современные направления и методы кибербразведки

Интенсивное изменение ландшафта угроз и развитие инструментов автоматизации управления информационными и киберфизическими системами влечет за собой необходимость совершенствования методов кибербразведки. Современный подход к threat intelligence включает в себя выявление, анализ и описание индикаторов компрометации. Выполнение всех указанных действий позволяет получить действительно качественные данные кибербразведки, которые могут быть применены для реальной защиты объекта.

Индикаторы компрометации – это технические данные, применяемые СЗИ для обнаружения вре-

доносных объектов или процессов. Ключевым свойством индикатора являются определенные технические артефакты. При этом индикаторы, в описании которых имеется контекст, представляют наибольшую ценность. Контекст –дополнительное описание угрозы, с которой связан индикатор, позволяющее оценить возможность применения IoC в конкретном случае на защищаемом объекте. Наиболее простой способ описания контекста – текстовое поле, в котором в свободной форме представлена информация, имеющая отношение к индикатору. Например, время первого обнаружения, атрибуция к группировкам злоумышленников и др. В случае использования для описания контекста единого поля его обработка будет осложнена, поскольку для автоматизированного парсинга в таком случае необходимы четкие правила формирования текста. Иначе определить возможность применения и ценность отдельного индикатора для конкретной инфраструктуры можно будет только вручную. В [4] представлена классификация источников данных для индикаторов компрометации: внутренние источники, внешние модерируемые источники и внешние открытые источники.

Работы [5, 6] посвящены обзору рынка технологий передачи индикаторов и управления ими. При этом в [5] основной фокус нацелен на изучение влияния отношений между поставщиками данных кибрерразведки на механизмы обмена IoC, в то время как исследование [6] посвящено анализу непосредственно TI-платформ и протоколов обмена информацией об киберугрозах. Указанные работы свидетельствуют, что в отрасли threat intelligence до сих пор нет единых стандартов для представления и обмена индикаторами компрометации. При этом отмечается, что стандарты STIX и OpenIOC являются доминирующими на современном рынке кибербразведки.

В [7] рассмотрены инструменты для автоматизации извлечения индикаторов компрометации из публикаций в средствах массовой информации и различных отчетов, содержащих неструктурированные данные. Также представлен метод для сравнения таких инструментов. Однако, предлагаемые авторами механизмы ориентированы на внешние источники индикаторов и не могут быть применимы к источникам внутренним.

В [8] рассматривается фреймворк, позволяющий обрабатывать внешние источники кибербразведки, представленные в виде структурированных данных. Характерным отличием решения является возможность автоматизировать классификацию индикатора в соответствии с методологией матрицы Mitre ATT&CK [9]. Подобные механизмы в теории могут быть применимы и к индикаторам от внутренних источников, но только после того, как эти индикаторы уже извлечены и приведены к одному из форматов обмена данными кибербразведки [10].

В [11] затронута тема интеграции средств защиты при отражении DDoS-атак с помощью систем управления событиями безопасности (security information event management, SIEM). Предложенные авторами варианты парсинга событий СЗИ являются позволяют автоматизировать передачу между средствами защиты признаков, на основе которых необходимо корректировать набор контрмер, применяемых к атакующим. И хотя в данном исследовании не затронуты напрямую вопросы кибербразведки, такой подход может быть применен для извлечения индикаторов компрометации из внутренних источников.

Работа [12] посвящена классификации типов разведданных с точки зрения технических аспектов. Рассмотрены вопросы обмена IoC и определены факторы, при наличии которых производитель исследователь, получивший IoC, может отказаться от тиражирования и распространения конкретных индикаторов. Особое внимание уделено соотношению объема распространяемых фидов и качества содержащихся в них индикаторов компрометации. Указанная статья дополняет упомянутые выше публикации в вопросах проблем качества данных TI оценки возможности их применения для защиты конкретных информационных и киберфизических систем. Сформулированы возможные ограничения при обмене IoC между различными платформами, включая различия форматов данных и сложности их преобразования. Исследование

В [13] представлены результаты исследования способов публикации и обнародования данных threat intelligence, по результатам которого предложена классификация факторов, препятствующего подобным процессам. Помимо операционных, организационных, экономических и политических также рассмотрены факторы, влияющие на релевантность IoC, риск нарушения конфиденциальности при их публикации и затраты на создание инфраструктуры для формирования собственных фидов.

Исследование [14] посвящено проблемам эффективности используемых источников данных для кибербразведки, в том числе метрик индикаторов компрометации. Авторы формулируют проблемы разметки индикаторов и отсутствие объективных моделей ранжирования, кроме того, в статье наглядно представлена проблема длительного распространения

индикаторов компрометации в подготовленном структурированном формате, что нередко приводит к большому числу успешных «лавинообразных» атак, хотя при этом в неструктурированном виде индикаторы распространяются по Интернет достаточно быстро. Это несоответствие вполне объяснимо тем, что количество компаний, которые генерируют собственные индикаторы все еще невелико, число производителей коммерческих фидов весьма ограничено, а цены на их услуги высоки.

Таким образом, проведенный обзор научных исследований в области киберразведки свидетельствует, что большинство изысканий затрагивает автоматизацию обнаружения IoC из внешних источников, ранжирования полученных индикаторов и контроля их жизненного цикла применительно к задачам обогащения средств защиты. При этом вопросы развития киберразведки внутри защищаемых систем и формирования собственных индикаторов компрометации остаются нерассмотренными. В то же время рынок коммерческих индикаторов компрометации невозможен без решения задач по их формированию на основе данных защищаемых объектов. Вышеуказанные исследования, в своей совокупности отражают факт, что при обнаружении в работе защищаемого объекта даже небольшого числа IoC, атрибуты которых хотя бы частично совпадают с индикаторами с высоким рейтингом, может потенциально свидетельствовать о присутствии следов сложной целенаправленной атаки и требовать немедленных мер по реагированию.

Именно это и обуславливает затрагиваемую в данной статье проблему отсутствия методического обеспечения в части механизмов формирования индикаторов компрометации на основе данных внутренних источников киберразведки.

Таблица 1

Виды внутренних источников получения индикаторов компрометации

Источник киберразведки	Системы	Описание
Журналы регистрации событий	Все системы	Активность пользователей и служб, ошибки в работе программного обеспечения и события аудита безопасности
Сетевые события	Межсетевые экраны, маршрутизаторы, коммутаторы	Регистрация сетевых соединений, уведомления о срабатывании правил ограничения доступа, успешные и неуспешные попытки аутентификации
Профили сетевого трафика	Коммутаторы, маршрутизаторы, активное сетевое оборудование	Уведомления о превышении показателей по нагрузке, SNMP-трапы, метаданные траффика
Уведомления от периметральных средств защиты	Системы обнаружения и предотвращения вторжений, межсетевые экраны различного уровня	Уведомления и события обнаружения аномалий
Уведомления средств антивирусной защиты и системы обнаружения вторжений уровня хоста	Средства управления антивирусной защитой и системы защиты конечных точек	Уведомления об обнаружении вредоносного ПО и аномального использования системных утилит
Сотрудники	Все системы	Сообщения от пользователей и администраторов об аномальной работе систем
Внутренние расследования	Все системы	Индикаторы и артефакты, собранные в результате внутренних расследований инцидентов

2. Формирование индикаторов компрометации внутри защищаемой инфраструктуры

Данные киберразведки могут быть получены в результате мониторинга журналов событий СЗИ, а также самих защищаемых систем. При использовании внутренних источников речь в основном идет об IoC, поскольку формирование техник и тактик злоумышленников в этом случае возможно лишь в результате расследования инцидентов, которые не были предотвращены имеющимися средствами.

2.1 Источники индикаторов компрометации

В [4] представлена классификация индикаторов по источникам их получения, в которой выделяются хостовые, сетевые и поведенческие индикаторы. Согласно ей, к поведенческим индикаторам относятся данные из систем контроля и управления доступом и видеонаблюдения, поэтому их формирование требует привлечения человеческих ресурсов и ручного анализа. Данный тип источников не рассматривается в рамках текущей статьи. Таким образом, в случае КФС рассмотрению подлежат две группы – хостовые и сетевые индикаторы компрометации. Детектирование сетевых IoC в большинстве случае не является однозначным свидетельством компрометации системы и требует дополнительных процедуры проверки, тогда как хостовые индикаторы намного чаще сигнализируют об успешности атаки [15].

Ключевыми источниками данных внутри инфраструктуры являются СЗИ, защищающие периметр сети, средства контроля доступа между внутренними сегментами и хостовые средства защиты. Другие типы средств защиты тоже могут быть источниками данных киберразведки, но скорее для процессов обогащения обнаруженных индикаторов контекстом. При этом наблюдение таких событий во времени позволяет накапливать статистику и определять шаблоны штатной работы системы, чтобы в последствии выявлять инциденты на основе обнаруженных отклонений в поведении объектов. В таблице 1 представлены виды внутренних источников индикаторов компрометации.

Полученные в рамках одного оповещения об угрозе индикаторы целесообразно объединить в одну группу. Это позволит облегчить определение тип атаки, а также проверить потенциально скомпрометированную систему на предмет наличия других IoC.

При автоматизированном извлечении часто встречаются индикаторы, которые не позволяют однозначно говорить о компрометации системы. Например, IP адреса крупных хостинговых сервисов, хэш-суммы легитимных файлов и т.д. Для снижения количества ошибок первого рода необходимо предусмотреть механизм управления исключениями. Кроме того, при формировании собственного набора индикаторов на основе внутренних источников целесообразно устанавливать время жизни индикатора (time to live, TTL) [5, 16] больше, чем для IoC от внешних источников. В первую очередь, это актуально для хэш-сумм файлов. Эксплуатация систем часто подразумевает присоединение сегментов из смежных инфраструктур, и если в подключенном сегменте уже имелись следы присутствия злоумышленников, то увеличенное TTL позволит их обнаружить.

2.2 Методы извлечения индикаторов компрометации

Основными методами извлечения индикаторов компрометации из внутренних источников являются ручной анализ событий, трафика или его метаданных, а также автоматизированное извлечение из инцидентов. При этом автоматизированное извлечение возможно, как на стороне СЗИ, так и в системах, агрегирующих журналы событий, например, SIEM-системы. Также возможен подход, когда средства защиты генерируют индикаторы и направляют их в TI-платформу либо распространяют на другие СЗИ.

Ручной анализ. В первую очередь этот подход подразумевает работу аналитиков в консолях различных СЗИ. Суть подхода заключается в ручном выявлении аномалий, формировании и проверке гипотез и в случае их подтверждения формирования индикаторов в ходе реагирования на инцидент, а также формирование IoC, полученных в ходе расследования инцидентов.

Применение метода зачастую нецелесообразно выделять в отдельный процесс из-за высокого уровня трудозатрат. На практике такой подход активно используется в виде дополнительного этапа постинцидент анализа: IoC формируются после детального разбора инцидента и направляются в СЗИ для недопущения таких инцидентов. С одной стороны, индикаторы, полученные таким методом, имеют более высокий уровень достоверности, поскольку уже проведен тщательный анализ и криминалистические исследования. С другой стороны, указанные выше процессы занимают длительное время, IoC будут сформированы недостаточно оперативно, что может негативно сказаться на вероятности повторения подобных инцидентов. Также характерно использование широкого набора утилит и инструментов, перечень которых зависит от экспертов, проводящих исследование. Это

Таблица 2

Источники артефактов и инструменты извлечения хостовых IoC

Тип	Источник артефактов	Инструмент
Журналы удаленных подключений	C:\Windows\System32\winevt\Logs\Security.evtx	Windows Event Viewer Event Log Explorer
	C:\Windows\System32\winevt\Logs\Microsoft-Windows RemoteDesktopServicesRdpCoreTS%4Operational.evtx	
Аудит доступа к файлам	NTUSER.DAT|Software\Microsoft\Windows\ CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU	Registry Exlporer RegRipper
	C:\Users\%USERPROFILE%\AppData\Roaming\ Microsoft\ Windows\Recent\AutomaticDestinations	JLECMD.exe
Журналы браузеров	C:\Users\%USERNAME%\AppData\Local\ Microsoft\Edge\ User Data\Default\History	BrowsingHistoryView DB Browser for SQLite
	C:\Users\%USERPROFILE%\AppData\Roaming\ Mozilla\Firefo x\Profiles*.default*\places.sqlite	
Журналы запуска ПО	C:\Windows\Prefetch	PECMD.exe
Журналы доступа к USB	C:\Windows\appcompat\Programs\Amcache.hve	USB Detective
	C:\%USERPROFILE%\NTUSER.DAT	

может быть ПО для анализа реестра операционных систем, дампов трафика и оперативной памяти, а также извлечения данных журналов файловой системы, журналов интернет-браузеров и т.д. В таблице 2 представлены примеры источников артефактов и инструментов для извлечения из них хостовых индикаторов компрометации.

Автоматизированное извлечение. Поскольку объемы данных, генерируемых средствами защиты современных систем значительны, то извлечение индикаторов компрометации из них целесообразно автоматизировать. Кроме того, при наличии TI-платформы [6, 17] возможна реализация различных алгоритмов обработки таких IoC и использование их для автоматизированного обогащения средств защиты.

1. Извлечение индикаторов напрямую из СЗИ.

Современные СЗИ при срабатывании защитных механизмов делают записи в журналах событий, которые могут храниться, как на защищаемых объектах, так и в централизованном хранилище. При этом в большинстве СЗИ присутствует возможность удаленных запросов через API [18], которые позволяют получать в ответ искомые индикаторы. Например, данные о вредоносном объекте, полученные в результате эмуляции его работы в системе поведенческого анализа:

«file_info»: {
«file_uri»: «sha256:215a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f»,
«md5»: «44d88612fea8a7f36de82e1278abb02f»,
«mime_type»: «text/plain; charset=us-ascii»,
«sha1»: «3395856ce81f1b7382dee72602f798b642f14140»,
«sha256»: «275a021bbfb5489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f»,
«size»: 69
},

Стоит отметить, что распространенным является подход, при котором сбор IoC осуществляется с нескольких СЗИ в единое хранилище (например, TI-платформу) для последующей обработки.

2. Извлечение индикаторов компрометации из SIEM

При наличии в инфраструктуре SIEM-системы ее возможности часто используются для формирования собственных индикаторов компрометации. В SIEM агрегируются события со всей инфраструктуры, включая журналы аудита защищаемых объектов и СЗИ. При срабатывании правил корреляции часть данных из нормализованных событий записывается в отдель-

ные структуры (например, табличные списки), а потом доступна к извлечению посредством API-запросов или выгрузки в другие системы.

Если ведение подобных списков оказывается ресурозатратным (например, поток событий слишком большой, а извлекающие их правила корреляции используются не для реагирования, а только для получения набора IoC), применяется метод, когда к SIEM периодически выполняется внешний запрос на поиск событий за определенный период времени, в условиях которого задан возврат наиболее часто встречающихся индикаторов (например, 20 самых часто блокируемых URL за последние 24 часа). Формирование и отправка индикаторов компрометации непосредственно СЗИ и их распространение.

Некоторые СЗИ способны самостоятельно направлять данные в другие средства защиты или публиковать их на общих ресурсах для последующего использования другими СЗИ. Например, во многих межсетевых экранах для веб-приложений (Web Application Firewall, WAF) [19] есть функционал выгрузки списка наиболее часто атакующих IP-адресов. Например, Positive Technologies Application Firewall при API-запросе вида

GET https://waf.local/api/ptaf/v4/config/global_lists/045af7b7 -bc30-4a50-97ae-ea914eb06039/file

возвращает файл подобного содержания:

HTTP/1.1 200 OK

Content-Type: text/plain

Content-Disposition: attachment; filename=»DDoS list.txt»

Content-Encoding: gzip

198.51.100.1

198.51.100.5

198.51.100.238

Такой список может быть размещен на сетевом ресурсе для последующего импорта в средства защиты от DDoS-атак [20] на уровне L3-L4 модели OSI [15, 21] или передаваться на оборудование провайдеров для полной блокировки любого трафика с таких источников.

3. Алгоритмы применения индикаторов от внутренних источников

В зависимости от выбранного метода формирования собственного фида на основе индикаторов компрометации от внутренних источников возможно построение различных алгоритмов их применения. Предположим, что в составе средств защиты имеется система, обеспечивающая возможность агрегации и ранжирования индикаторов компрометации на основе некоторых правил и методов threat intelligence [5, 22].

3.1 Использование индикаторов непосредственно от источников

В случае извлечения IoC напрямую от средств защиты, каждое СЗИ выступает отдельным источником и к поступившим от него данным применяются вышеуказанные правила и методы. Если TI-платформа допускает применение различных правил агрегации и ранжирования для нескольких групп источников, то в случае наличия внешних потоков данных об угрозах и внутренних индикаторов их целесообразно разделить. Таким образом, собирая данные с нескольких СЗИ внутри защищаемого объекта можно сформировать

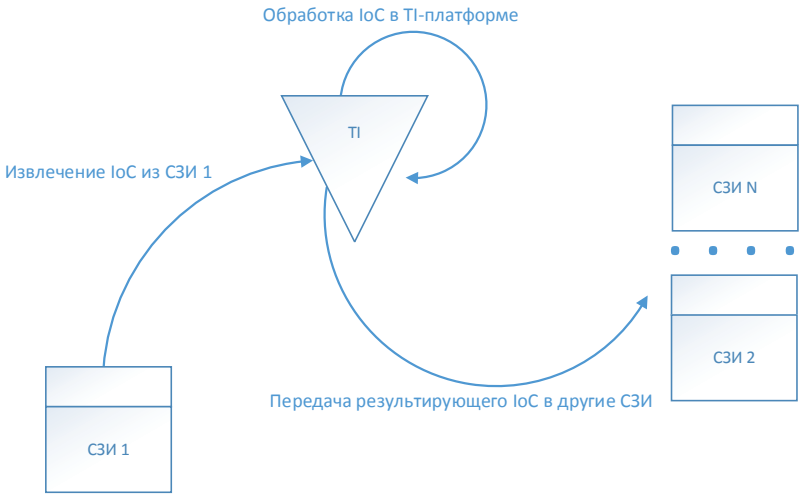

Рис. 1. Схема потоков данных при использовании IoC непосредственно от источников

собственный набор индикаторов для дальнейшего применения (кастомный фид).

Полученный фид может быть направлен в конкретные СЗИ для принятия превентивных мер, автоматизированного реагирования и предотвращения возможных инцидентов. Например, предположим, что в системе используется несколько антивирусных решений – в зависимости от защищаемых контуров. С одного из них получены данные о множественных попытках подключения к вредоносному сайту. Полученные данные направлены и обработаны в TI-платформе. Сформированный на их основе фид направлен в корпоративный прокси-сервер для блокировки обнаруженного URL. Это позволит обеспечить превентивную меру реагирования и исключит возможность подключения к данному ресурсу с хостов, где по какой-то причине еще не обновились базы антивирусов. Схема потоков данных для данного примера представлена на рис. 1, а блок-схема алгоритма применения метода представлена на рис. 4а.

3.2 Извлечение индикаторов через нормализацию событий

Если TI платформа поддерживает возможность приема событий из SIEM, то на основе фильтров часть данных дублируется и отправляется для анализа в TI. В этом случае извлечение индикаторов полностью производится на стороне системы, агрегирующей IoC. Это позволяет снизить нагрузку на SIEM и тратить ресурсы коррелятора на непрофильную задачу, особенно если события, из которых извлекаются данные, не участвуют в правилах детектирования угроз. В то же время возникает необходимость дублировать данные между двумя системами и при больших потоках данных существенно нагружать сетевое оборудование. Дублирование может быть частично исключено, если на стороне SIEM существует возможность управлять очередями событий и реализовать отправку в TI их усеченной копии, в которой точно будут содержаться IoC. После обработки полученных из SIEM событий TI извлекает IoC и также обеспечивает формирование собственного фида. Этот фид может быть направлен напрямую в СЗИ, как в случае с получением IoC от СЗИ. Также фид может быть использован вместе со внешними потоками данных и включен в механизм ранжирования. При этом целесообразно повысить значение параметра, отвечающего за уровень опасности индикатора, поскольку он уже получен от внутренних источников и на защищаемом объекте имеются следы взаимодействия с ним.

Затем набор таких индикаторов может быть направлен в СЗИ для принятия мер по блокировке и при этом обратно в SIEM для обновления табличных списков и использования в правилах корреляции. Такой подход позволяет оставить за SIEM-системой механизм выявления инцидентов на основе IoC, но при этом снизить нагрузку на подсистему корреляции за счет проверки и ранжирования индикаторов в другой системе. Схема потоков данных для данного варианта представлена на рис. 2, а блок-схема алгоритма применения метода представлен на рис. 4б.

Рис. 2. Схема потоков данных при извлечении IoC через нормализацию событий в SIEM

3.3 Применение корреляции для обработки индикаторов

Если же в TI платформе нет механизма получения событий из SIEM, используется подход, основанный на извлечении индикаторов с помощью коррелятора. В случае срабатывания правил корреляции реализуется обновление динамических или табличных списков, куда помещаются уже извлеченные IoC. Эти списки передаются в TI платформу, где происходит их агрегация и ранжирование. При таком подходе основным инструментом извлечения IoC остается SIEM, но при этом работа в части агрегации, ранжирования и отправки индикаторов в СЗИ происходит на стороне TI. Схема потоков данных такого решения представлена на рис.3, а блок-схема алгоритма применения метода на рис. 4в.

3.4 Интеграция средств защиты через собственные наборы индикаторов

Поскольку многие средства защиты имеют собственные механизмы формирования индикаторов и могут быть интегрированы с другими СЗИ, то нередко формирование собственного фида осуществляется этими средствами. Например, системы поведенческого анализа («песочницы») зачастую обеспечивают возможность повторных проверок – при обновлении базы знаний в выборочном порядке производится анализ объектов, проверенных ранее. В случае выявления фактов, что вредоносный объект был пропущен, «песочница» формирует набор IoC, например, хеш-суммы файлов. Этот набор может быть передан через API в систему защиты конечных точек (Endpoint Detection and Response, EDR) [15] для автоматического поиска и блокировки таких файлов на всех хостах в сети. Поскольку данный метод предполагает точечные интеграции между средствами защиты, которые могут быть выполнены с использованием различных механизмов, то типового алгоритма в этом случае не существует. Наборы интеграций и механизмы реализации уникальны для каждого объекта.

В то же время для случаев, перечисленных в пунктах 3.1 – 3.3, в результате исследований авторами были выделены основные этапы и разработаны алгоритмы применения индикаторов компрометации для обогащения СЗИ (рисунок 4).

4. Сценарии применения индикаторов компрометации для защиты киберфизических систем

Сценарий 1. В одном из сетевых СЗИ, например, системе класса IDS [23] или NTA [23], обнаружена подозрительная сетевая активность. В качестве IoC в большинстве подобных случаев будут выступать IP-адреса источника или назначения. Эти индикаторы необходимо передать в TI платформу для обработки и дальнейшего принятия решения. Если передача IoC происходит через SIEM, то они могут быть обогащены контекстом (поиск хоста, с которого идет вредоносный трафик, затем идентификация процесса, связанного с этим сетевым соединением). На стороне TI происходит обработка индикаторов – ранжирование с другими потоками данных об угрозах, определение критичности и времени жизни.

Сценарий 2. В одном из средств защиты на хосте (антивирусное ПО или EDR агент [4, 22]) быстрее обновились базы и была зафиксирована потенциальная

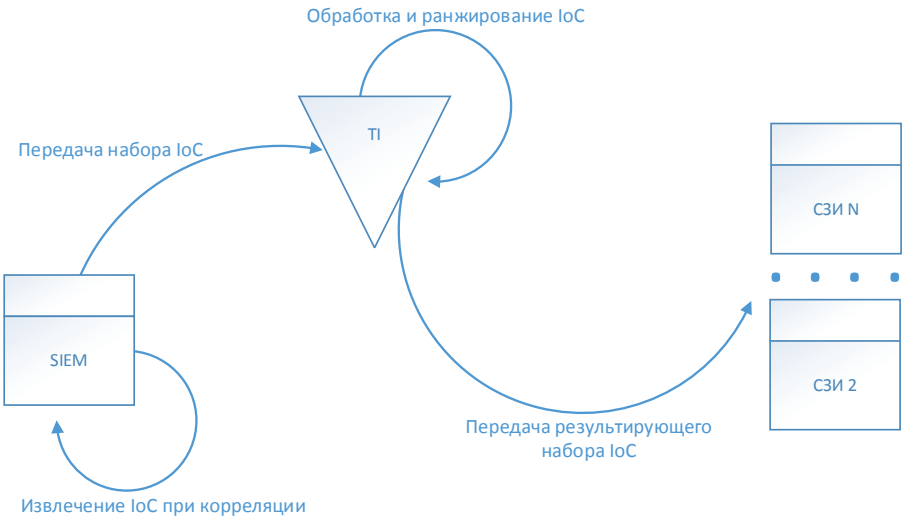

Рис. 3. Схема потоков данных при извлечении IoC через корреляцию в SIEM

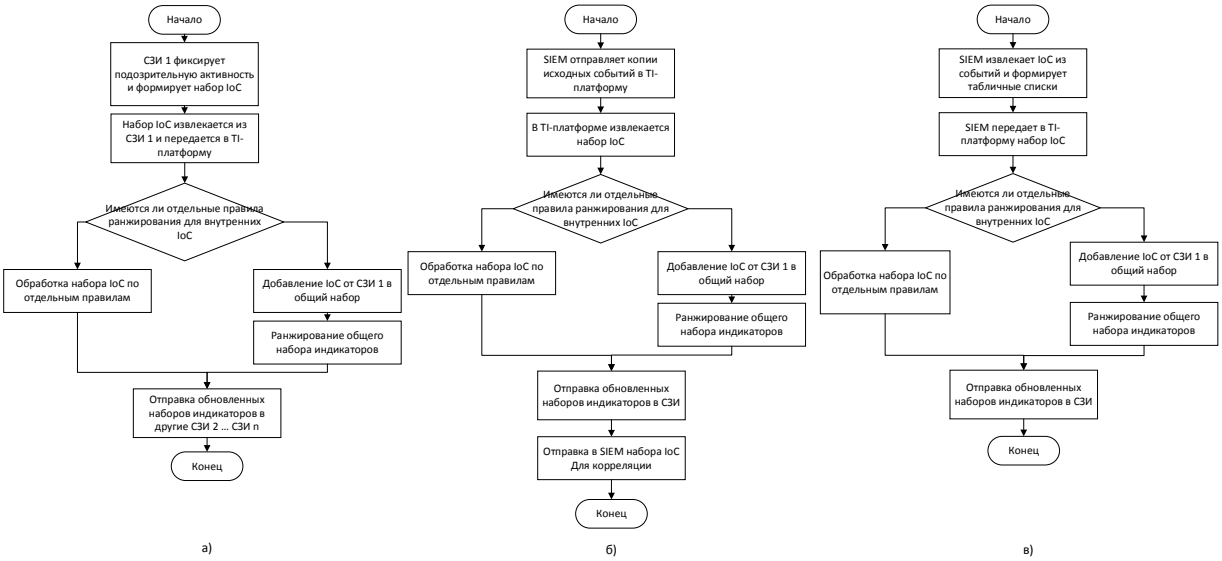

Рис. 4. Алгоритмы применения индикаторов от внутренних источников

вредоносная активность, события об этом направлены в SIEM. Далее в зависимости от алгоритма и механизма интеграции в TI платформу направляются данные события или извлеченные из них индикаторы. В зависимости от реализации данного алгоритма дублирование может быть исключено частично, если на стороне SIEM существует возможность управлять очередями событий и реализовать отправку в TI их усеченной копии, в которой будут содержаться IoC. В этой платформе они проходят обработку в рамках обновленного собственного фида распространяются на все другие хосты. Кроме того, полученные и обогащенные индикаторы направляются обратно в SIEM для использования в правилах корреляции. Подобный сценарий позволяет реализовать прообраз самообучения системы защиты – СЗИ выявляют угрозы на конечных хостах, эти данные обогащаются через TI и автоматически добавляются в условия правил корреляции в случае высокого скоринга по результатам ранжирования с другими потоками данных.

Сценарий 3. Рассмотрим случаи применения индикаторов от внутренних источников без применения TI платформ. Например, часть сервисов КФС доступна через веб-интерфейс и защищена WAF. Помимо этого, на периметре сети расположен межсетевой экран класса NGFW [20] с функциями IDS и IPS. Предположим, что WAF обнаруживает признаки DDoS-атаки на уровне L7 и начинает блокировать запросы с наиболее активных адресов атакующих. В случае наличия у злоумышленников значительных мощностей для проведения атаки нагрузка как WAF, так и защищаемое приложение может стремительно возрасти до критического уровня. Здесь целесообразным является подключение механизма IPS и сброс пакетов от наиболее активных атакующих. WAF формирует списки IP-адресов атакующих, которые перенаправляются в периметровый NGFW, например через запросы к API или выгрузку на общий ресурс текстового файла. При этом возможно создание нескольких типов списков с различным временем жизни индикатора (TTL). Это необходимо, чтобы обеспечить возможность снижения количества ошибок первого рода и блокировки легитимных пользователей.

Сценарий 4. Данный сценарий относится не столько к извлечению IoC из внутренних источников, сколько к дополнительной обработке данных, поступающих с них, с целью проверки взаимосвязей с индикаторами из внешних источников. Большинство целенаправленных атак осуществляются без использования вредоносного ПО и активных действий по сканированию сети или передачи большого объема данных. Поэтому зачастую СЗИ не позволяют определить является ли запуск задачи или создание сервиса легитимным.

Для решения этой задачи часто используют SIEM, создавая правила корреляции на определенные последовательности событий или значения конкретных параметров. Такие «пакеты правил» сложно поддаются оперативной корректировки, особенно в части детектирования новых техник и тактик злоумышленников. При наличии внешних источников IoC актуальным является следующий сценарий. С помощью SIEM агрегируются события с внутренних источников, из них извлекаются данные о параметрах запуска процессов, создания сервисов и других легитимных дей-

Таблица 3

Примеры собираемых данных от внутренних источников

Тип индикатора	Наблюдаемое значение из событий	Индекс источника
windows_path	.\powershell	32
url	http://c2cdomain/malicious-picrure-1.jpg’	39
windows_path	.\pOWErS^H^EIL^.eX^e^	41
md5_hash	81ed03caf6901e444c72ac67d192fb9c	54
url	http://evilserver/pwnme»	46
windows_path	.\reg query add mscfile\\\\open	59
windows_path	\system\CurrentControlSet\Control\Terminal	63
ipv4	1.2.3.4	79
ipv4	127.0.0.1	114

ствиях. Это данные передаются в TI платформу, где сверяются с регулярно обновляемыми внешними потоками данных об угрозах. При этом сравнение происходит на основе полей, относящихся к контекстной составляющей индикаторов. В случае обнаружения совпадений данные о хостах, где зафиксирована такая активность, возвращаются в SIEM в виде обновляемых табличных списков. Эти списки используются для правил корреляции и накопления статистики, глубину которой можно регулировать временем жизни таких списков.

Таким образом, на защищаемых хостах фиксируется определенный набор легитимных действий (пример событий с извлеченными данными представлен в таблице 3). Эти события проверяются на основе внешних IoC и в случаях совпадения объекты, где зафиксирована активность, ставятся на усиленный контроль. При срабатывании других правил корреляции с такими хостами повышается приоритет инцидентов, кроме того обеспечивается возможность построения длительных цепочек событий и обнаружения целенаправленных атак.

5. Анализ источников данных киберразведки

Получение индикаторов компрометации из внутренних источников в большинстве случаев относится к проприеритарным технологиями, что обуславливает характерную особенность такого вида источников – отсутствие какой-либо типизации при определении контекста. В одних случаях дополнительную информацию можно извлечь из специальных полей события, в других требуется дополнительно обогащать данные из справочников или анализировать запросы внутри сессий, а в некоторых случаях контекст отсутствует. Кроме того, во многих источниках имеются схожие базы знаний и извлеченные индикаторы многократно дублируются. Особенно это характерно для IP-адресов, dns-записей и URL. Например, попытки подключения к вредоносному веб-ресурсу могут зафиксироваться в событиях прокси-сервера, антивируса, периметрального NGFW и т.д. При этом часть извлеченных IoC будет дублирована и подлежит обработке и ранжированию.

В части определения контекста наиболее часто наблюдались проблемы при извлечении URL. В большинстве внутренних источников отсутствует какая-либо подробная информация и детальное описание. Изредка в событиях блокировки доступа к таким ресурсам отмечается принадлежность к некоторой категории согласно классификации вендора данного СЗИ. На практике это является одним из ограничивающих факторов применения таких данных для киберразведки. В то же время некоторые поставщики IoC предоставляют достаточно полное описание контекста подобным индикаторам. Поэтому в большинстве случаев обработка контекста индикаторов компрометации внутренних источников требует ручного процесса для преобразования данных в машиночитаемый формат или автоматизации ранжирования и обогащения с потоками данных от внешних источников. Тем не менее эти данные не могут быть полностью игнорированы как источник информации о киберразведке, поскольку именно в них может содержаться ценная информация для выявления и реагирования на инцидент.

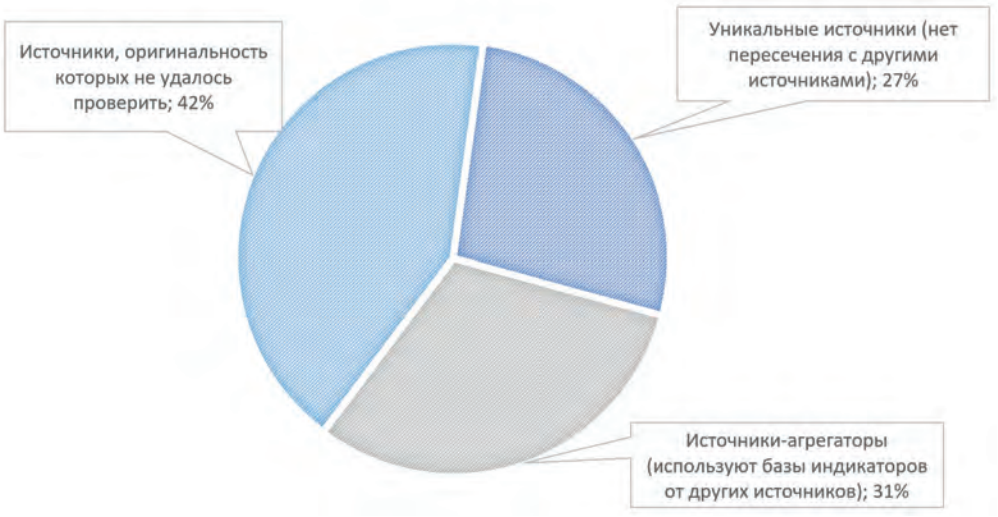

Рис. 5. Анализ оригинальности индикаторов в внутренних источниках TI

Анализ исследуемых внутренних TI-источников выявил, что многие из них являются ретрансляторами данных, получаемых из внешних потоков данных об угрозах. Это обусловлено тем, что многие производители СЗИ используют внешние обновляемые базы знаний, что часто приводит к дублированию информации. В большей степени это относится к источникам, поставляющим IoC в более сложных форматах. На рис. 5 представлены результаты анализа исследуемых источников на предмет оригинальности. Следует отметить, что в некоторых случаях реализовать достоверную проверку на предмет оригинальности было невозможно из-за преобразования информации при ее ретрансляции.

Было обнаружено, что при агрегации и ретрансляции индикаторов некоторые данные могут быть потеряны или изменены. В основном, это связано с ошибками форматирования данных, искажением дат обнаружения, дублированием или агрегацией нескольких индикаторов. Подобные трансформации существенно снижают качество данных кибербразведки и повышают вероятность ошибок первого рода при работе с ними.

Заключение

Обеспечение надлежащего уровня защищенности является одной из ключевых задач при эксплуатации информационных и киберфизических систем, в том числе относящихся к категории критической инфраструктуры. При этом одним из трендов в решении этой задачи является развитие методов кибербразведки и оркестрации работы множества средств защиты. Стремительно развиваются направления проактивного поиска угроз и опережения действий злоумышленников с использованием методов кибербразведки, среди которых наиболее распространено применение индикаторов компрометации для обогащения средств защиты киберфизических систем. Их использование позволяет проводить действия, направленные на выявление новых, ранее неизвестных угроз и обеспечивать защиту подобных объектов на качественно новом уровне, оперируя тактиками и процедурами и предугадывая действия злоумышленников.

В настоящей статье рассмотрены и структурированы задачи поиска и извлечения данных из внутренних источников для обогащения систем кибербразведки и выявления целенаправленных методов атак на основе применения собственных наборов индикаторов компрометации и предложены методы их решения. Установлено, что в отрасли кибербразведки отсутствует унификация в части формирования индикаторов компрометации на основе данных защищаемых систем и дальнейшего обмена информацией между различными средствами защиты, но при этом имеют место ряд доминирующих форматов обмена подобными данными. Разработано алгоритмическое обеспечение применения индикаторов от внутренних источников и предложены базовые сценарии обработки таких данных для защиты киберфизических систем в условиях изменяемых векторов атак. Кроме того, при работе с внутренними источниками кибербразведки в рамках данного исследования был выявлен ряд проблем эффективной обработки таких данных, поскольку решение каждой из них обуславливает несколько отдельных задач, их рассмотрение будет проведено и представлено на дальнейших этапах исследования.

Работа выполнена при финансовой поддержке гранта РНФ № 22-21-00846.

Литература

1. Abu M.S.; Selamat S.R., Ariffin A., Yusof R. Cyber Threat Intelligence – Issue and Challenges. Indones // Indonesian Journal of Electrical Engineering and Computer Science. – 2018. Vol. 10, no. 1. – P. 371–379.
2. Sauerwein C., Pekaric I., Felderer M., Breu R. An analysis and classification of public information security data sources used in research and practice // Computers & Security. – 2019. – Vol. 82. – P. 140-155.
3. Pala A., Zhuang J. Information sharing in cybersecurity: A review // Decision Analysis. – 2019. – Vol. 16, no. 3. – P. 172-196.
4. Мещеряков Р.В., Исхаков С.Ю. Исследование индикаторов компрометации для средств защиты информационных и киберфизических систем // Вопросы кибербезопасности. – 2022. – № 5 (51). – С. 82-99. DOI: 10.21681/2311-3456-2022-5-82-89
5. Sauerwein C., Sillaber C., Mussmann A., Breu R. Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives // Wirtschaftsinformatik und Angewandte Informatik. – 2017. – P. 837-851.
6. Zrahia A. Threat intelligence sharing between cybersecurity vendors: Network, dyadic, and agent views // Journal of Cybersecurity. – 2018. – Vol. 4, issue 1. – P. 1–16.
7. Caballero J., Gomez G., Matic S., Sanchez G., Sebastian S., Villacanas A. The Rise of GoodFATR: A Novel Accuracy Comparison Methodology for Indicator Extraction Tools // Future Generation Computer Systems. – 2023. – Vol. 144. – P. 74-89.
8. Alam M., Bhusal D., Park Y., Rastogi N. Looking Beyond IoCs: Automatically Extracting Attack Patterns from External [Электронный ресурс]. – 2022. –URL: https://arxiv.org/abs/2211.01753 (дата обращения 19.09.2023).
9. Allegretta M., Siracusano G., Gonzalez R., Gramaglia M. Are crowd-sourced CTI datasets ready for supporting anti-cybercrime intelligence? // Computer Networks. – 2023. – Vol. 234. – P. 109920.
10. Liu R., Zhao Z., Sun C., Yang X., Gong X., Zhang J. A Research and Analysis Method of Open Source Threat Intelligence Data // Communications in Computer and Information Science (CCIS). – 2017. – Vol. 727. – P. 352–363.
11. Тергеуов О.С., Маликова Ф.У. Обнаружение и устранение DDoS-атаки IoT-ботнетов на основе SIEM // Universum: технические науки. – 2022. – №4-1 (97). – С. 54-63.
12. Tounsi W., Rais H. A survey on technical threat intelligence in the age of sophisticated cyber attacks // Computer Security. – 2018. – Vol. 72. – P. 212–233.
13. Zibak A., Simpson A. Cyber threat information sharing: Perceived benefits and barriers // Proceedings of the 14th International Conference on Availability, Reliability and Security. – Canterbury, UK, 26–29 August 2019. – P. 1–9.
14. Guo Li V., Dunn M., Pearce P., McCoy D., Voelker G., Savage S, Levchenko K. Reading the tea leaves: a comparative analysis of threat intelligence // Proceedings of the 28th USENIX Conference on Security Symposium (SEC'19). – Santa Clara, USA, 14-16 August 2019. – P. 851-867.
15. Schaberreiter T., Kupfersberger V., Rantos K., Spyros A., Papanikolaou A., Ilioudis C., Quirchmayr G. A quantitative evaluation of trust in the quality of cyber threat intelligence sources // Proceedings of the 14th International Conference on Availability, Reliability and Security. – 2019. – P. 1-10.
16. Brown S., Gommers J., Serrano O. From Cyber Security Information Sharing to Threat Management // Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security. – Denver, CO, USA, 12–16 October 2015. – P. 43–49.
17. Wagner C., Dulaunoy A., Wagener G., Iklody A. MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform // Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security. – Vienna, Austria, 24 October 2016. – P. 49-56.
18. Wei Y., Bo L., Sun X., Li B., Zhang T., Tao C. Automated event extraction of CVE descriptions // Information and Software Technology. – 2023. – Vol. 158. – P. 107178.
19. Calva M., Beltran M. A Model for risk-Based adaptive security controls // Computers & Security. – 2022. – Vol. 115. – P. 102612.
20. Skopik F. Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at National Level. – CRC Press: Boca Raton, FL, USA, 2018. – 446 p.
21. Lavrova D.S. An approach to developing the SIEM system for the Internet of Things // Automatic Control and Computer Sciences. – 2016. – Vol. 50. – P. 673-681.
22. Bryant B., Saiedian H. Improving SIEM Alert Metadata Aggregation with a Novel Kill-Chain Based Classification Model // Computers & Security. – 2020. – Vol. 94. – P. 101817.
23. Mavroeidis V., Bromander S. Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence // Proceedings of the 2017 European Intelligence and Security Informatics Conference (EISIC). – Athens, Greece: IEEE, 2017. – P. 91–98.

RESEARCH OF METHODS FOR FORMING INDICATORS OF COMPROMETATION FROM INTERNAL SOURCES OF INFORMATION AND CYBERPHYSICAL SYSTEMS

Meshcheryakov R.V.[3], Iskhakov S.Yu.[4]

Purpose of work: *research of methods for generating indicators of compromise within the infrastructure for use in systems for protecting information and cyber-physical systems.*

Research method: *system analysis of open sources of data on indicators of compromise, methods of extracting them and methods of application when organizing cyber reconnaissance within the protected infrastructure.*

The result obtained: current problems of extracting indicators of compromise from internal sources in information and cyber-physical systems are formulated. Algorithmic support for the use of such indicators in cyber intelligence processes is proposed. Basic scenarios for using indicators of compromise from internal sources when processing dynamic streams of threat data in the context of changing attack vectors are formulated.

It was found that the cyberintelligence industry currently lacks unification in terms of forming compromise indicators based on data from protected systems and further exchange of information between different defenses, but there are a number of dominant formats for the exchange of such data. In the course of the research, the tasks of searching and extracting data from internal sources to enrich cyberintelligence systems and identify targeted attack methods based on the use of proprietary sets of compromise indicators are considered and structured, and methods for their solution are proposed.

Scientific novelty: *methods for generating indicators of compromise within the protected infrastructure have been reviewed and systematized. Algorithmic support for the use of indicators from internal sources has been developed and basic scenarios for processing such data have been proposed to protect cyber-physical systems in the face of variable attack vectors.*

Keywords: *indicator of compromise, cyber-intelligence, context, cyber-physical system, security information event management, enrichment, ranking.*

References

1. Abu M.S.; Selamat S.R., Ariffin A., Yusof R. Cyber Threat Intelligence – Issue and Challenges. Indones // Indonesian Journal of Electrical Engineering and Computer Science. – 2018. Vol. 10, no. 1. – P. 371–379.
2. Sauerwein C., Pekaric I., Felderer M., Breu R. An analysis and classification of public information security data sources used in research and practice // Computers & Security. – 2019. – Vol. 82. – P. 140-155.
3. Pala A., Zhuang J. Information sharing in cybersecurity: A review // Decision Analysis. – 2019. – Vol. 16, no. 3. – P. 172-196.
4. Meshherjakov R.V., Ishakov S.Ju. Issledovanie indikatorov kompрometacii dlja sredstv zashhity informacionnyh i kiberfizicheskih sistem // Voprosy kiberbezopasnosti. – 2022. – № 5 (51). – S. 82-99. DOI: 10.21681/2311-3456-2022-5-82-89
5. Sauerwein C., Sillaber C., Mussmann A., Breu R. Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives // Wirtschaftsinformatik und Angewandte Informatik. – 2017. – P. 837-851.
6. Zrahia A. Threat intelligence sharing between cybersecurity vendors: Network, dyadic, and agent views // Journal of Cybersecurity. – 2018. – Vol. 4, issue 1. – P. 1–16.
7. Caballero J., Gomez G., Matic S., Sanchez G., Sebastian S., Villacanas A. The Rise of GoodFATR: A Novel Accuracy Comparison Methodology for Indicator Extraction Tools // Future Generation Computer Systems. – 2023. – Vol. 144. – P. 74-89.
8. Alam M., Bhusal D., Park Y., Rastogi N. Looking Beyond IoCs: Automatically Extracting Attack Patterns from External [Jelektronnyj resurs]. – 2022. –URL: https://arxiv.org/abs/2211.01753 (data obrashhenija 19.09.2023).
9. Allegretta M., Siracusano G., Gonzalez R., Gramaglia M. Are crowd-sourced CTI datasets ready for supporting anti-cybercrime intelligence? // Computer Networks. – 2023. – Vol. 234. – P. 109920.
10. Liu R., Zhao Z., Sun C., Yang X., Gong X., Zhang J. A Research and Analysis Method of Open Source Threat Intelligence Data // Communications in Computer and Information Science (CCIS). – 2017. – Vol. 727. – P. 352–363.

3 Roman V. Meshcheryakov, Dr. Sc. (Technology), Professor, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. E-mail: mrv@ieee.org, ORCID: ORCID: 0000-0002-1129-8434.

4 Sergey Yu. Iskhakov, Ph.D. (Technology), Promsvyazbank, Moscow, Russia. E-mail: sergey@iskhakov.ru, ORCID: 0000-0003-3346-9262.

11. Tergeuov O.S., Malikova F.U. Obnaruzhenie i ustranenie DDoS-ataki IoT-botnetov na osnove SIEM // Universum: tehnicheskie nauki. – 2022. – №4-1 (97). – S. 54-63.
12. Tounsi W., Rais H. A survey on technical threat intelligence in the age of sophisticated cyber attacks // Computer Security. – 2018. – Vol. 72. – P. 212–233.
13. Zibak A., Simpson A. Cyber threat information sharing: Perceived benefits and barriers // Proceedings of the 14th International Conference on Availability, Reliability and Security. – Canterbury, UK, 26–29 August 2019. – P. 1–9.
14. Guo Li V., Dunn M., Pearce P., McCoy D., Voelker G., Savage S, Levchenko K. Reading the tea leaves: a comparative analysis of threat intelligence // Proceedings of the 28th USENIX Conference on Security Symposium (SEC'19). – Santa Clara, USA, 14-16 August 2019. – P. 851-867.
15. Schaberreiter T., Kupfersberger V., Rantos K., Spyros A., Papanikolaou A., Ilioudis C., Quirchmayr G. A quantitative evaluation of trust in the quality of cyber threat intelligence sources // Proceedings of the 14th International Conference on Availability, Reliability and Security. – 2019. – P. 1-10.
16. Brown S., Gommers J., Serrano O. From Cyber Security Information Sharing to Threat Management // Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security. – Denver, CO, USA, 12–16 October 2015. – P. 43–49.
17. Wagner C., Dulaunoy A., Wagener G., Iklody A. MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform // Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security. – Vienna, Austria, 24 October 2016. – P. 49-56.
18. Wei Y., Bo L., Sun X., Li B., Zhang T., Tao C. Automated event extraction of CVE descriptions // Information and Software Technology. – 2023. – Vol. 158. – P. 107178.
19. Calva M., Beltran M. A Model for risk-Based adaptive security controls // Computers & Security. – 2022. – Vol. 115. – P. 102612.
20. Skopik F. Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at National Level. – CRC Press: Boca Raton, FL, USA, 2018. – 446 p.
21. Lavrova D.S. An approach to developing the SIEM system for the Internet of Things // Automatic Control and Computer Sciences. – 2016. – Vol. 50. – P. 673-681.
22. Bryant B., Saiedian H. Improving SIEM Alert Metadata Aggregation with a Novel Kill-Chain Based Classification Model // Computers & Security. – 2020. – Vol. 94. – P. 101817.
23. Mavroeidis V., Bromander S. Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence // Proceedings of the 2017 European Intelligence and Security Informatics Conference (EISIC). – Athens, Greece: IEEE, 2017. – P. 91–98.