Анализ критериев предоставления мандата на локализацию инцидента информационной безопасности

А.В. Кузнецов

Финансовый университет при Правительстве Российской Федерации

Аннотация: В статье представлены результаты анализа и оценки применимости различных критериев предоставления мандата на локализацию инцидента информационной безопасности в рамках реагирования. Мандат предоставляется средствам оркестрации или системам искусственного интеллекта для проведения локализации инцидента в автоматическом режиме, т. е. без участия сил групп реагирования. При проведении оценки применимости различных критериев предоставления мандата в отличие от известных оценивался уровень сложности определения значений для рассматриваемых критериев силами только групп реагирования. Предложены отдельные критерии и их значения, которые в отличие от известных выделяют область для локализации инцидентов информационной безопасности в автоматическом режиме, что позволяет сокращать время и силы, затрачиваемые группами реагирования на локализацию обнаруженных инцидентов.
Ключевые слова: группа реагирования, область реагирования, реагирование, автоматическая локализация, оркестрация, искусственный интеллект

Введение

Несмотря на все усилия специалистов по обеспечению информационной безопасности (ИБ), ежегодно количество инцидентов ИБ и размер ущерба от них только возрастают [1, 2]. Как следствие, актуальность тематики реагирования на возникающие инциденты ИБ остается высокой.

Стоит отметить, что в составе мероприятий непосредственно по реагированию на инциденты ИБ, т. е. активному противодействию нарушителю ИБ, можно выделить следующие действия [3, 4]:

- локализация (сдерживание) инцидента ИБ;
- устранение негативных последствий инцидента ИБ;
- восстановление нормальной работоспособности систем(ы) после инцидента ИБ.

Первичным действием по реагированию является локализация инцидента ИБ, т. е. создание условий для ограничения дальнейших действий

(продвижения) нарушителя ИБ и/или изоляции пораженной области информационной инфраструктуры.

Принимая во внимание, что силы групп реагирования на инциденты ИБ (ГРИИБ) всегда ограничены, особенно в территориально распределенных информационных инфраструктурах, охватывающих несколько часовых поясов, возникает необходимость использования средств оркестрации и/или систем искусственного интеллекта (далее – средств управления) [4, 5] для локализации обнаруживаемых инцидентов ИБ. Но, к сожалению, отсутствует работы, посвященные особенностям предоставления мандата на локализацию инцидента ИБ, в т. ч. используемым критериям предоставления мандата, удостоверяющего права и полномочия, выданные средствам управления на локализацию инцидентов ИБ.

Цель, задачи, материалы и методы исследования

Целью настоящего исследования является сокращение времени, затрачиваемого ГРИИБ на локализацию обнаруженных инцидентов ИБ, путем выдачи и использования мандата средствами управления в автоматическом режиме.

Для достижения поставленной цели предлагается:

1) Проанализировать и оценить существующие критерии предоставления мандата на локализацию инцидентов ИБ.

2) Установить значения для выбранных критериев, при которых возможна автоматическая локализация с использованием средств управления.

Материалами для настоящего исследования выступали научно-исследовательские статьи и тематические монографии.

В качестве методов исследования применялись анализ и синтез имеющихся общедоступных материалов и достижений, информация ограниченного доступа не использовалась.

За рамками настоящего исследования:

- вопросы обнаружения и подтверждения инцидентов ИБ (локализация осуществляется в отношении подтвержденных инцидентов ИБ);

- вопросы обеспечения ИБ самого мандата, в т. ч. его целостности,

а также не проводилось деление между понятиями инцидент ИБ, инцидент защиты информации и компьютерный инцидент.

Результаты анализа и оценки применимости критериев предоставления мандата

Первостепенно необходимо определить при каких условиях будет предоставляться мандат средствам управления. При этом стоит отметить, что средства реагирования (например: средства класса Endpoint Detection & Response или Network Detection & Response (ранее Network Traffic Analysis) [6]) не участвует в выдаче мандата, они только реализуют выбранное непосредственное техническое действие по локализации (например: блокируют использование определенных портов для протоколов TCP/UDP, завершают работу определенных процессов в операционной системы и т. п.) по команде от средства управления.

Поставщиком (провайдером) мандата будет выступать руководитель ГРИИБ, как ответственный за реализацию мероприятий по реагированию на инциденты ИБ в организации, в т. ч. за управление мандатами.

Мандаты могут быть представлены в различных форматах, но в рамках настоящего исследования будут рассматриваться в виде цифровых записей, содержащих идентификационную информацию, относящуюся к средству управления, его правам и полномочиям с учетом заданных критериев.

В таблице 1 приведены сведения о возможных вариантах критериев предоставления мандата и их значениях, а также экспертная качественная оценка уровня сложности их однозначного определения силами только ГРИИБ (по шкале: высокий, средний, низкий). Оценивался именно данный параметр, т. к. корректное и своевременное принятие решения по выдаче

(невыдаче) мандата является обязательным условием для перехода непосредственно к локализации инцидента ИБ. Ситуация аналогичная со своевременной и корректной классификацией инцидентов ИБ [7].

Экспертная оценка проводилась методом Дельфи [8, 9], в ней приняли участи шесть экспертов-архитекторов крупнейшего в России коммерческого центра мониторинга и реагирования на кибератаки «Ростелеком-Солар JSOC». Каждый участник обладал высшим образованием, действующим сертификатом от международной профессиональной ассоциации Information Systems Audit and Control Association (USA) или ведущих российских производителей средств реагирования (Лаборатории Касперского и/или Positive Technologies) и опытом в предметной области не менее 10 лет.

Таблица № 1

Сведения о возможных критериях предоставления мандата

№ п/п	Группа критериев	Формулировка критерия	Возможные значения критерия	Уровень сложности определения
1	По территории	Область реагирования ограничена площадкой (территорией)	Отдельная площадка	Средний (т. к. есть мобильные пользователи, подрядчики и/или иные удаленные подключения из любой точки)
			Все площадки	
2	По системам	Область реагирования ограничена системой	Отдельная система	Высокий (т. к. в организациях полноценно не ведутся/ актуализируются сведения о системах (не зона ответственности ГРИИБ))
			Отдельная категория систем (Mission critical, Business critical, Business operational или Office productivity)	
			Все системы	

№ п/п	Группа критериев	Формулировка критерия	Возможные значения критерия	Уровень сложности определения
3	По времени	Область реагирования ограничена временным диапазоном	Отдельные временные интервалы (рабочее время, нерабочее время и т. п.)	Низкий (т. к. в событиях безопасности всегда содержится время обнаружения)
			Любое время	
4	По реакции	Область реагирования ограничена вариантом действия по локализации	Отдельные действия	Низкий (т. к. перечень действий описан в эксплуатационной документации на средство реагирования)
			Любые действия	
5	По ложным срабатываниям	Область реагирования ограничена уровнем ложных срабатываний сценариев обнаружения инцидентов	Низкий уровень ложных срабатываний	Низкий (т. к. ГРИИБ ведется статистика по закрытию инцидентов (зона ответственности ГРИИБ))
			Средний уровень ложных срабатываний	
			Высокий уровень ложных срабатываний	
6	По риску компрометации	Область реагирования ограничена инцидентами, приводящими непосредственно к компрометации систем/данных	Низкий риск компрометации (разведка)	Низкий (т. к. ГРИИБ осуществляется классификация и приоритизация инцидентов (зона ответственности ГРИИБ))
			Средний риск компрометации (закрепление и расширение присутствия)	
			Высокий риск компрометации (нанесение ущерба)	
7	По влиянию реакции на бизнес-	Область реагирования ограничена	Низкое влияние (отсутствие или	Низкий (т. к. ГРИИБ формируются и

№ п/п	Группа критериев	Формулировка критерия	Возможные значения критерия	Уровень сложности определения
	деятельность	вариантами действий по локализации, не приводящими к блокировке бизнес-деятельности	незначительное ограничение бизнес-деятельности)	согласовывают планы реагирования (зона ответственности ГРИИБ))
			Среднее влияние (ограничение бизнес-деятельности)	
			Высокое влияние (блокировка бизнес-деятельности)	

Значения критериев предоставления мандата для автоматической локализации

По результатам проведенного анализа предлагается использовать критерии, получившие низкую оценку уровня сложности определения силами ГРИИБ, и следующие значения для них, характеризующие условия для локализации инцидента в автоматическом режиме:

- по ложным срабатываниям (*Fp*): низкий уровень ложных срабатываний;

- по риску компрометации (*R*): высокий риск компрометации (нанесение ущерба);

- по влиянию реакции на бизнес-деятельность (*I*): низкое влияние.

Данное предложение позволяет записать следующую функцию $M_{resp}(Fp, R, I)$. Опционально, дополнительно могут применяться критерии по времени и/или реакции.

Упрощенный вид целевой функции M_{resp}, характеризующей условия для локализации инцидентов ИБ средствами управления в автоматическом режиме, представлен на рис.1. На осях абсцисс и ординат используется

единая качественная шкала: от низкого к среднему и далее к высокому уровню. Глобальный максимум, выделенный желтым цветом, отражает область возможного применения автоматической локализации.

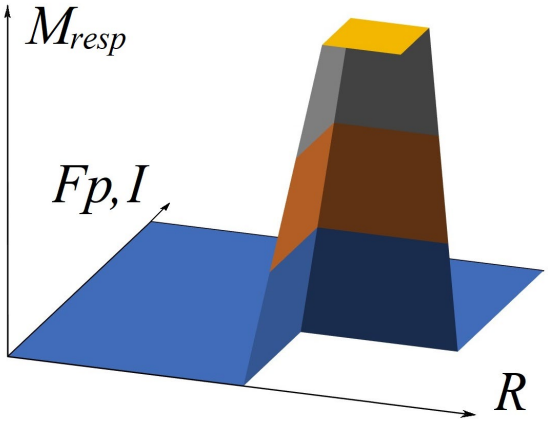

Рис. 1. – Упрощенный вид целевой функции M_{resp}

К примерам инцидентов ИБ, подлежащим автоматической локализации, можно отнести обнаружение запуска (применения) хакерских утилит (например: Cobalt Strike, Mimikatz, Metasploit, Hydra или других) или создания учетной записи локального администратора. Опционально можно учитывать, что обнаружение произошло в нерабочее время или в интервал времени, когда силы ГРИИБ не могут лично принять участие в реагировании.

Заключение

По результатам исследования:

1) Проведен анализ и экспертная оценка существующих критериев, которая в отличие от известных учитывала (оценивала) уровень сложности определения значений для критериев силами только ГРИИБ;

2) Предложены критерии и их значения, которые в отличие от известных выделяют область для локализации инцидентов ИБ в автоматическом режиме, что позволяет сокращать время и силы, затрачиваемые ГРИИБ на локализацию обнаруженных инцидентов ИБ.

Применение результатов настоящего исследования дает положительный эффект в области технических наук (методы и системы защиты информации, ИБ) и представляет наибольший интерес для ГРИИБ, обслуживающих территориально распределенные информационные инфраструктуры, в т. ч. по сервисной модели [10], а также для центров Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) и координационных центров групп реагирования на компьютерные инциденты (Computer Emergency Response Team Coordination Center (CERT CC)).

Направлением развития данного исследования является расширение рассматриваемых мероприятий по реагированию на инциденты ИБ помимо действий по локализации (сдерживанию) [3, 4].

Литература

1. Кушко Е.А., Паротькин Н.Ю., Золотарев В.В. Организация защищенного обмена данными внутри программно-управляемой локальной сети // Вестник СибГУТИ. Том 17. 2023. №4. С. 62-73. DOI: 10.55648/1998-6920-2023-17-4-62-73.

2. Ермаков А.С. Цифровая война: понятие, генезис, проблемы защиты национальных интересов государств // Вестник НГУЭУ. 2023. №1. С. 206-221. DOI: 10.34020/2073-6495-2023-1-206-221.

3. Benjamin Kovacevic. Security Orchestration, Automation, and Response for Security Analysts. UK: Packt Publishing, 2023. 338 p.

4. Кузнецов А.В. Эволюция реагирования на инциденты информационной безопасности // Защита информации. Инсайд. 2024. №5(119). С. 14-20.

5. Беспалова Н.В., Корчагин С.А., Сердечный Д.В., Селиверстов В.В. Анализ зарубежного опыта применения интеллектуальных методов в задачах защиты объектов критической информационной инфраструктуры

финансового сектора // Инженерный вестник Дона. 2024. №5. URL: ivdon.ru/ru/magazine/archive/n5y2024/9196.

6. Barros A., Chuvakin A., Belak A. Applying Network-Centric Approaches for Threat Detection and Response // Gartner, Inc. URL: gartner.com/en/documents/3904768.

7. Кузнецов А.В. Особенности классификации компьютерных инцидентов // Журнал высоких гуманитарных технологий. 2024. №4(7). С. 6-11.

8. Стончюте К.Э., Гурбо А.А., Пузыревская А.А. Методы экспертных оценок: метод Дельфи // Научное знание современности. 2021. №5(53). С. 16-19.

9. Кумалагова Е.А. Особенности использования метода Дельфи // Учет и контроль. 2023. Т.2. №11. С. 28-32.

10. Берёза Н.В. Современные тенденции развития мирового и российского рынка информационных услуг // Инженерный вестник Дона. 2012. № 2. URL: ivdon.ru/ru/magazine/archive/n2y2012/758.

References

1. Kushko E.A., Parot'kin N.Yu, Zolotarev V.V. Vestnik SibGUTI. Tom 17. 2023. №4. pp. 62-73. DOI: 10.55648/1998-6920-2023-17-4-62-73.

2. Ermakov A.S. Vestnik NGUEU. 2023. №1. pp. 206-221. DOI: 10.34020/2073-6495-2023-1-206-221.

3. Benjamin Kovacevic. Security Orchestration, Automation, and Response for Security Analysts. UK: Packt Publishing, 2023. 338 p.

4. Kuznetsov A.V. Zaŝita informacii. Inside. 2024. №5 (119). pp. 14-20.

5. Bespalova N.V., Korchagin S.A., Serdechnyy D.V., Seliverstov V.V. Inzhenernyj vestnik Dona. 2024. №5. URL: ivdon.ru/ru/magazine/archive/n5y2024/9196.

6. Barros A., Chuvakin A., Belak A. Applying Network-Centric Approaches for Threat Detection and Response. Gartner, Inc. URL: gartner.com/en/documents/3904768.

7. Kuznetsov A.V. Zhurnal vysokikh gumanitarnykh tekhnologiy. 2024. №4 (7). pp. 6-11.

8. Stonchyute K.E., Gurbo A.A., Puzyrevskaya A.A. Nauchnoe znanie sovremennosti. 2021. №5 (53). pp. 16-19.

9. Kumalagova E.A. Uchet i kontrol'. 2023. T.2. №11. pp. 28-32.

10. Bereza N.V. Inzhenernyj vestnik Dona. 2012. № 2. URL: ivdon.ru/ru/magazine/archive/n2y2012/758.

Дата поступления: 13.01.2025

Дата публикации: 25.02.2025