DOI 10.36622/1682-7813.2024.27.1.011
УДК 004.056

ПОРЯДОК ОЦЕНКИ УРОВНЯ ЭФФЕКТИВНОСТИ СИСТЕМЫ НЕПРЕРЫВНОГО ПРОТИВОДЕЙСТВИЯ ИНЦИДЕНТАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОБЪЕКТЕ

М.Ю. Рытов, О.М. Голембиовская, Е.В. Кондрашова, М.М. Голембиовский, К.Е. Шинаков

Статистика нарушений информационной безопасности различных объектов имеет стабильную тенденцию к росту, преимущественно за счет появления большого количества уязвимостей прикладного и системного ПО, которые активно используют злоумышленники, проводя кибератаки. В рамках статьи описаны основные условия формирования эффективной системы непрерывного противодействия инцидентам информационной безопасности на объекте, а также порядок оценки уровня ее эффективности. Приведен порядок организации работы первой линии реагирования на инциденты информационной безопасности, схема встраивания технологии мониторинга сетевых событий в инфраструктуру объекта, общий порядок действий, по оценке истинности срабатывания мониторинговых систем, особенности классификации и атрибуции кибератак, шаблон заполнения сведений о первичном реагировании на инцидент ИБ и анкета оценки непрерывного противодействия инцидентам ИБ на объекте.

Ключевые слова: инцидент, информационная безопасность, противодействие, непрерывность.

Противодействие инцидентам информационной безопасности одно из самых приоритетных направлений в сфере защиты информации. Статистика нарушений ИБ различных объектов имеет стабильную тенденцию к росту, преимущественно за счет появления большого количества уязвимостей прикладного и системного ПО, которые активно используют злоумышленники, проводя кибератаки.

По данным НКЦКИ ежедневно более 170 кибератак направлено на российские компании. В первом полугодии 2023 года участились координированные целевые атаки одновременно с «фоновым шумом» в виде массовых поверхностных атак, с целью отвлечения внимания. С середины года хакеры действуют «точечно», используя данные, полученные в результате утечек [1]. Предотвратить реализацию кибератак на объекте, а также нейтрализовать или же минимизировать возможные последствия можно посредством построения на объекте системы противодействия инцидентам ИБ.

Она позволяет пресечь кибератаку на начальных этапах ее реализации и своевременно применить методы предотвращения возможных потерь.

Основой эффективного противодействия инцидентам ИБ является непрерывный мониторинг сетевых событий и оперативное выстраивание наиболее действенного плана локализации инцидента ИБ.

Команда, отвечающая за реагирование на инциденты ИБ, как правило, состоит из двух линий реагирования. Первая линия отвечает за стремительные активные действия, вторая – за углубленное расследование.

Ключевое значение имеет качество работы первой линии реагирования. Она ведет круглосуточный мониторинг алертов (оповещений систем мониторинга), производит анализ инцидентов и атрибуцию кибератак на основе общедоступных и собственных данных о техниках злоумышленников, вплоть до информации о конкретной преступной группе или конкретном злоумышленнике. При помощи данной информации аналитики первой линии определяют масштаб и выстраивают наиболее подходящий и эффективный план локализации инцидента. Иными словами, первая линия должна ответить на вопрос кто реализовал инцидент (если это возможно, то назвать группировку, если нет – вид нарушителя (преступная группировка, отдельный хакер, внутренний сотрудник),

если и это не представляется возможным – с какой целью реализован инцидент) и что конкретно было сделано. Именно данная информация позволяет составить оптимальный план и получить ответ на вопрос что делать дальше для локализации инцидента.

Основным помощником в реагировании на инциденты ИБ являются системы мониторинга сетевых событий. Они позволяют в автоматическом режиме обнаружить аномалии, происходящие в рамках инфраструктуры. Если аномальное событие обнаружено, система выдает алерт – оповещение о том, что информационная система и сеть подвергаются атаке или находятся в опасности вследствие аварии, сбоя или человеческой ошибки.

В настоящее время наиболее удобной технологией мониторинга являются SIEM-системы (MP SIEM, IBM QRadar, Wazuh), а также совмещение SIEM-систем и систем EDR (есть варианты готовых решений SIEM + EDR, например Kaspersky Smart II). SIEM-система собирает информацию из систем аутентификации и системы контроля и управления доступом, антивирусных средств, межсетевых экранов, систем обнаружения/предотвращения вторжений, систем проксирования доступа в интернет и веб-фильтрации (проксирование – перенаправление трафика, использование прокси-сервера в качестве посредника между пользователем и целевым сервером). системных журналов событий ИБ серверов и рабочих станций. EDR же анализирует сетевые события на конечных рабочих станциях.

Общая схема встраивания технологии мониторинга сетевых событий в инфраструктуру объекта представлена на рис. 1.

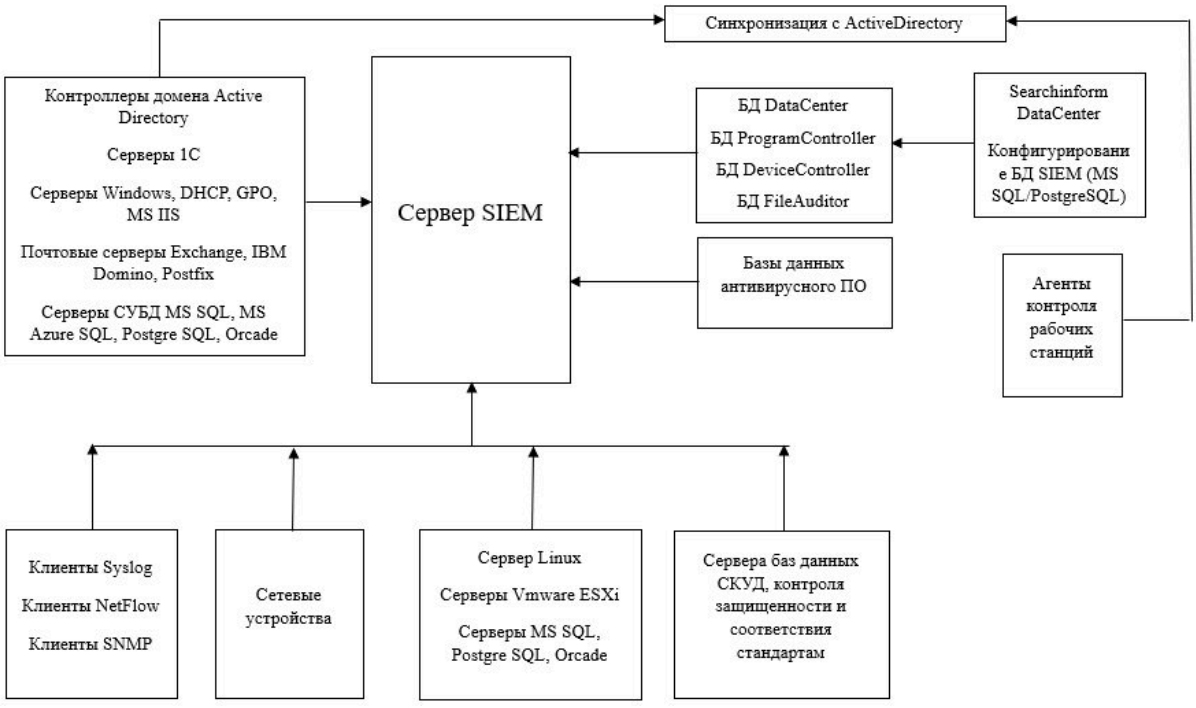

Рис. 1. Схема встраивания технологии мониторинга сетевых событий в инфраструктуру объекта

Данные системы функционируют на основе правил корреляции, в рамках которых прописывается информация о том какие признаки активности в системе говорят об ее аномальности. В случае если система обнаруживает событие, подходящее под правило, она выдает предупреждение (алерт).

Далее представлены примеры алертов SIEM-систем.

Алерт SIEM-системы 1: сброс учетных данных: SAM (Security Account Manager, который управляет всеми учетными записями пользователей и их паролями)

INC 292901 – статус.

Remote_SAM_Dump_Windows.

Опасность – высокая.

На узле DC-01.INF.RU обнаружена попытка удаленного дампа учетных данных из базы SAM пользователем infuser-buh.

Статус – закрыт (ложное срабатывание).

Создан на основе 1 срабатывания правил кореляции Remote_SAM_Dump_Windows.

Категория – не определена.

Источник инцидента – скрипт SIEM.

Тип – не определен.

Расположение – Unmanaged hosts.

Алерт SIEM-системы 2: очищение истории ввода команд bash_history (атакующий может использовать данную технику для того, чтобы уничтожить историю вводимых команд).

INC 276079 – статус.

Clear_Command_History

Опасность – средняя.

2023-12-12T14 03:52 0000000Z на хосте 10.3.132.126 зафиксирована попытка очистить историю вводимых команд пользователем bitrix-admin Листинг команды-‘bash -c echo”>/root/.bash_history’.

Статус – закрыт (ложное срабатывание).

Создан на основе 1 срабатывания правил кореляции Clear_Command_History.

Категория – не определена.

Источник инцидента – скрипт SIEM.

Тип – не определен.

Расположение – Unmanaged hosts.

После получения алерта специалисты первой линии должны определить истинное это срабатывание или ложное.

На рис. 2 представлен общий порядок действий, по оценке истинности срабатывания мониторинговых систем.

Рис. 2. Общий порядок действий по оценке истинности срабатывания мониторинговых систем

После того как алерт проверен на достоверность, первая линия реагирования проводит процедуру атрибуции, для того чтобы выстраиваемый в последствии план локализации инцидента был максимально действенным.

Атрибуцией называют процесс установления злоумышленника или преступной группировки, стоящей за кибератакой или вредоносной кампанией при помощи организационных мероприятий и технических средств.

В настоящее время набирают развитие APT-атаки. Это целевые атаки на отдельную инфраструктуру, как правило они хорошо спланированы, сильно распределены во времени (от нескольких дней до нескольких лет) и включают несколько этапов, сочетая в себе комбинацию различных методов реализации (социальная инженерия, эксплуатация уязвимостей, вредоносное ПО и т.д.). Знание или предположение того, какая группировка стоит за проводимой атакой может помочь подобрать более точечные меры противодействия.

Основной особенностью атрибуции в России является отсутствие ее веса в правовом поле. Как правило, доказать правдивость выводов аналитика, проводящего атрибуцию кибератаки невозможно, потому что вывод делается на основе косвенных признаков. Исключением являются три случая:

- злоумышленник пойман с поличным;
- злоумышленник признался в совершении кибератаки сам (однако важно учитывать наличие ситуаций, когда кто-то один берет на себя всю вину);
- произошла утечка информации (если это не направленная дезинформация).

Таким образом, в настоящий момент целью атрибуции является вынесение предположения о том, кто стоит за реализацией атаки, какие цели он преследует и какими инструментами пользуется, для того чтобы минимизировать возможные последствия от продвижения злоумышленника вглубь инфраструктуры и не допустить реализации подобной атаки в будущем. Исследователь должен быть ориентирован на поиск ляпов, ошибок, отличительных особенностей, которые в дальнейшем могут быть полезны в вопросах противодействия. Далее представлены примеры классификации и атрибуции кибератак

Пример атаки: атака на энергетическую компанию госсектора [2].

Программы: модификации трояна Decoy Dog.

Цели: организации на территории Российской Федерации.

Источник: аккаунт с именем пользователя @lahat.

Технические приемы: предварительный доступ к хосту, помещение файла в загрузчик.

Группа: Hellhounds.

Пример атаки: атаки на организации различных сфер и масштабов в России и Сербии [3]

Программы: ВПО ShadowPad, бэкдор Deed RAT, ВПО Voidoor, публично доступные утилиты для продвижения по сети.

Цели: шпионаж и кража конфиденциальной информации.

Технические приемы: переиспользование старых адресов сайтов, с помощью создания на них доменов более высокого уровня, внедрение ВПО, использование уязвимостей, разведка при помощи Acunetix и использование слабых мест.

Группа: Space Pirates.

Пример атаки: атаки на правительственный сектор России, Белоруссии, Азербайджана, Турции, Словении [4]

Уязвимость: уязвимость в редакторе уравнений из пакета Microsoft Office CVE-2017-11882.

Программы: полезная нагрузка ВПО.

Цели: шпионаж и кража конфиденциальной информации.

Источник: фишинговое письмо с вредоносным вложением - документ (как формата .doc, так и .docx), реализующий атаку типа Template Injection.

Технические приемы: целенаправленные рассылки, основанные на профессиональной сфере атакуемых.

Группа: Cloud Atlas.

Основой для проведения процедуры атрибуции также могут быть данные, полученные из публичных исследований. Например, отчеты PT ESC Threat Intelligence [5], отчеты Лаборатории Касперского об аналитике APT-атак [6].

Таким образом, системы мониторинга, атрибуция и квалифицированные

специалисты-аналитики обеспечивают эффективный первичный мониторинг, однако важно также учитывать задачу по обеспечению непрерывности реагирования на инцидент ИБ и обеспечение взаимосвязи со второй линией реагирования.

В рамках работы второй линии реагирования наиболее ценной информацией являются сведения о порядке локализации инцидента, а также данные, которые удалось получить в ходе атрибуции. Они используются при реализации активного реагирования на инцидент ИБ и проактивного поиска угроз, а также при обучении сотрудников и обмене опытом.

Для передачи информации второй линии реагирования предлагается использовать шаблон заполнения сведений о первичном реагировании (табл. 1).

Таблица 1

Шаблон заполнения сведений о первичном реагировании на инцидент ИБ

Критерий	Сведения об инциденте (пример заполнения)
Общее описание инцидента	В 14.48 в SIEM-систему пришло оповещение об аномальном событии. В ходе проверки подтверждена подлинность срабатывания. Сотрудник отдела продаж загрузил вредоносный файл на свою машину, ВПО сформировало коммуникационный пакет, который был отправлен серверу с целью установки соединения. Данный пакет содержал информацию о зараженной машине и, скорее всего, предназначен для идентификации целей злоумышленника.
Инструменты проведения атаки	Целенаправленная рассылка, неустановленное ВПО
Источник	Фишинговое письмо
Цель	Кража конфиденциальной информации
Данные проверки программных ресурсов (уязвимости, артефакты и пр.)	Обнаружена уязвимость CVE-2017-11882, требующая устранения
Данные о субъектах атаки (название группы/имя /принадлежность субъекта, мотивация, поведенческие особенности атаки)	Предположительно Cloud Atlas
Иная информация (аналитика возможных причин, провокации и пр.)	Провокация и кража конфиденциальной информации в связи с участием в тендере
Предложения по локализации инцидента	Изолировать зараженные устройства от сети, сменить аутентификационную информацию, запустить проверку антивирусным ПО и удалить обнаруженное ВПО, проверить инфраструктуру на наличие аномальной активности, устранить обнаруженные уязвимости

Данная карточка позволит зафиксировать первичную информацию, полученную аналитиками и упростить ее применение при реализации других компонентов.

Для оценки эффективности системы непрерывного противодействия инцидентам

ИБ на объекте предлагается оценочная анкета (табл. 2), ответив на вопросы, которые также можно составить план рекомендаций, которые следует внедрить на объекте для улучшения показателей.

Таблица 2

Анкета оценки непрерывного противодействия инцидентам ИБ на объекте

№	Вопрос / ответы	Балл
$К_{1.1}$	На объекте установлены системы автоматического мониторинга сетевых событий? (SIEM, EDR+SIEM, SOAR)?	
	Да, установлена система мониторинга EDR+SIEM	1
	Да, установлена одна из указанных систем мониторинга	0,7
	Нет	0
$К_{1.2}$	На объекте сформирована группа, отвечающая за мониторинг оповещений мониторинговых систем и выстраивание наиболее эффективного плана локализации инцидента ИБ?	
	Да	1
	Нет	0
$К_{1.3}$	На объекте обеспечен круглосуточный мониторинг оповещений систем мониторинга?	
	Да	1
	Нет	0
$К_{1.4}$	Производится ли периодическое обогащение систем мониторинга новыми правилами реагирования?	
	Да, специалисты регулярно мониторят новые уязвимости и вносят правила в систему	1
	Да, обновление производится в случае критических событий	0,4
	Нет	0
$К_{1.5}$	Закреплен ли на объекте порядок оценки оповещений мониторинговых систем на предмет ложносрабатываний?	
	Да, такой же или аналогичный представленному в рамках статьи	1
	Да, но иной по структуре	0,7
	Нет	0
$К_{1.6}$	Проводится ли для аналитиков первой линии обучение и конференции по обмену опытом для накапливания собственной базы знаний, проведения более качественной атрибуции и составления плана реагирования?	
	Да, регулярно при наличии новой информации /курсов/ конференций	1
	Да, с заданной временной периодичностью не чаще чем раз в полгода	0,5
	Да, с заданной временной периодичностью не чаще чем раз в год	0,3
	Нет	0
$К_{1.7}$	Закреплена ли на объекте единая форма заполнения сведений о первичном реагировании на инцидент ИБ?	
	Да, такая же или аналогичная представленной в рамках статьи	1
	Да, но иная по структуре	0,7
	Нет	0

Оценка эффективности системы непрерывного противодействия инцидентам ИБ на объекте рассчитывается по следующей формуле:

$$K = \frac{K_{1.1} + K_{1.2} + ... + K_{1.i}}{i},$$

где K – показатель оценки эффективности системы непрерывного противодействия инцидентам ИБ на объекте, $K_{1.i}$ – балл по каждому вопросу анкеты, i – количество вопросов анкеты.

Результат интерпретируется по шкале, основанной на шкале Харрингтона. Числовые значения данной шкалы получены на основе статистического анализа большого массива данных, она может использоваться для оценки различных показателей качественного характера. В рамках собственной шкалы числовые значения шкалы Харрингтона объединены из пяти в три параметра, путем слияния уровней «очень высокий» и «высокий», а также «очень низкий» и «низкий».

0,64 - 1,0 – уровень эффективности системы непрерывного противодействия инцидентам ИБ на объекте высокий, внедрение дополнительных мер и средств не требуется;

0,38 - 0,63 – уровень эффективности системы непрерывного противодействия инцидентам ИБ на объекте средний, требуется внедрение дополнительных мер и средств для повышения показателя;

0 - 0,37 – уровень эффективности системы непрерывного противодействия инцидентам ИБ на объекте низкий, требуется внедрение дополнительных мер и средств для повышения показателя.

В случае если уровень эффективности системы непрерывного противодействия инцидентам ИБ на объекте не высокий, следует внедрить описанные в рамках оценочной анкеты (табл. 2) меры и средства на объекте.

Таким образом, представленные условия формирования эффективной системы непрерывного противодействия инцидентам ИБ на объекте, а также порядок оценки уровня ее эффективности позволяют понять насколько системно и действенно осуществляется противодействие инцидентам ИБ на объекте, а также внедрить недостающие подходы, меры и средства для улучшения данного показателя.

Список литературы

1. Positive Technologies: какие уязвимости будут главными угрозами в 2023 году // URL: https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/apt-cloud-atlas-unbroken-threat/ (дата обращения: 30.12.2023)

2. Hellhounds: операция Lahat [// URL: https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/hellhounds-operaciya-lahat/ (дата обращения: 30.12.2023).

3. Space Pirates // URL: https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/space-pirates-exploring-non-standard-techniques-new-attack-vectors-and-grouping-tools/ (дата обращения: 30.12.2023).

4. APT Cloud Atlas: Unbroken Threat // URL: https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/apt-cloud-atlas-unbroken-threat/ (дата обращения: 30.12.2023).

5. PT ESC Threat Intelligence // URL: https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/ (дата обращения: 30.01.2023).

6. Отчеты APT // URL: https://securelist.com/category/apt-reports/ (дата обращения: 30.12.2023).

Брянский государственный технический университет
Bryansk State Technical University

Поступила в редакцию 06.02.2024

Информация об авторах

Рытов Михаил Юрьевич – канд. техн. наук, профессор, зав. кафедрой «Системы информационной безопасности», Брянский государственный технический университет, e-mail: ozikts@yandex.ru

Голембиовская Оксана Михайловна – канд. техн. наук, доцент кафедры «Системы информационной безопасности», Брянский государственный технический университет, e-mail: bryansk-tu@yandex.ru

Кондрашова Екатерина Владимировна – специалист отдела маркетинга и связей с общественностью, Брянский государственный технический университет, e-mail: kondrashova_katerina@bk.ru
Голембиовский Максим Михайлович – ассистент кафедры «Системы информационной безопасности», Брянский государственный технический университет, e-mail: proverka-bstu32@yandex.ru
Шинаков Кирилл Евгеньевич – канд. техн. наук, доцент кафедры «Системы информационной безопасности», Брянский государственный технический университет, e-mail: uprproject-bstu32@yandex.ru

THE PROCEDURE FOR ASSESSING THE LEVEL OF EFFECTIVENESS OF THE SYSTEM OF CONTINUOUS COUNTERACTION TO INFORMATION SECURITY INCIDENTS AT THE FACILITY

M.Y. Rytov, O.M. Golembiovskaya, E.V. Kondrashova, M.M. Golembiovsky, K.E. Shinakov

The statistics of information security violations of various objects has a stable upward trend, mainly due to the appearance of a large number of vulnerabilities in application and system software, which are actively used by hackers conducting cyber attacks. The article describes the basic conditions for the formation of an effective system of continuous counteraction to information security incidents at the facility, as well as the procedure for assessing the level of its effectiveness. The procedure for organizing the work of the first line of response to information security incidents, a scheme for embedding network event monitoring technology into the facility's infrastructure, a general procedure for evaluating the validity of monitoring systems, features of classification and attribution of cyber attacks, a template for filling in information about the initial response to an information security incident and an assessment questionnaire for continuous counteraction to information security incidents at the facility.

Keywords: incident, information security, counteraction, continuity.

Submitted 06.02.2024

Information about the authors
Rytov Mikhail Yuryevich – Cand. Sc. (Technical), Professor, Head of the Department of Information Security Systems, Bryansk State Technical University, e-mail: ozikts@yandex.ru
Golembiovskaya Oksana Mikhailovna – Cand. Sc (Technical), Associate Professor of the Department of Information Security Systems, Bryansk State Technical University, e-mail: bryansk-tu@yandex.ru
Kondrashova Ekaterina Vladimirovna – specialist of the Marketing and public Relations Department, Bryansk State Technical University, e-mail: kondrashova_katerina@bk.ru
Golembiovsky Maxim Mikhailovich – Assistant of the Department of Information Security Systems, Bryansk State Technical University, e-mail: proverka-bstu32@yandex.ru
Shinakov Kirill Evgenevich – Cand. Sc. (Technical), Associate Professor of the Department of Information Security Systems, Bryansk State Technical University, e-mail: uprproject-bstu32@yandex.ru