УДК 004

Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

К ВОПРОСУ О СОВЕРШЕНСТВОВАНИИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ

Аннотация. Статья посвящена сравнительному анализу функций Security Operation Center (SOC) и их использованию в современных организациях. Рассматриваются основные аспекты создания и управления SOC, включая процессы мониторинга, обнаружения и реагирования на киберугрозы. В рамках статьи, также обсуждают технологические инструменты и методы анализа данных, необходимые для обеспечения безопасности информационных систем. В статье представлены практические рекомендации по оптимизации работы SOC и повышению эффективности защиты от кибератак.

Ключевые слова: Security Operation Center (SOC), информационная безопасность, процессы, мониторинг, реагирование, инциденты.

Совершенствование системы защиты информации в организации нуждается в модернизации. Одним из перспективных направлений этой работы является использовании достижений науки и техники. Сравнительно новым в этой связи является создание специализированных структур обеспечения информационной безопасности. Такой структурой может стать Security Operations Center (SOC) – центр обеспечения информационной безопасности, структурное подразделение организации, отвечающее за контроль IT-среды и предотвращение киберинцидентов. SOC – это самостоятельное подразделение, обеспечивающее мониторинг, обнаружение, анализ, реагирование и управление информационной безопасностью в организации. SOC используется для защиты от киберугроз и инцидентов информационной безопасности. Основные функции SOC включают в себя наблюдение за событиями в реальном времени, анализ аномальных активностей, обнаружение инцидентов информационной безопасности, реагирование на угрозы, сбор данных о безопасности, управление уязвимостями и инцидентами, а также обеспечение объекта на соответствие требованиям по безопасности информации. SOC обычно сочетает в себе технологии, процессы и высококвалифицированный персонал для обеспечения надежной защиты от киберугроз. Основная триада SOC – это процессы, люди и инструменты, то есть благодаря этим элементам функционирует любой SOC. Если убрать хоть один из элементов, то есть людей, процессы или инструменты, то SOC работать не будет.

SOC включает в себя ряд процессов, направленных на обеспечение безопасности информационных систем [1]. Вот некоторые из них:

1. Мониторинг и анализ: SOC проводит непрерывный мониторинг информационной инфраструктуры с использованием специализированных инструментов и технологий. Аналитики SOC анализируют данные, чтобы выявлять подозрительную активность и потенциальные угрозы.

2. Обнаружение инцидентов: SOC занимается обнаружением инцидентов безопасности, таких как вторжения, вредоносные программы и несанкционированный доступ к данным. Это включает в себя идентификацию аномальных событий и поведения в сети.

3. Реагирование на инциденты: При обнаружении инцидентов SOC принимает меры по реагированию, в том числе изоляции уязвимых узлов, блокированию угроз и восстановлению системной безопасности.

4. Управление уязвимостями: SOC отслеживает уязвимости в информационной инфраструктуре и занимается их решением, чтобы предотвратить возможные атаки.

5. Исправление инцидентов и улучшение процессов: SOC анализирует каждый инцидент, чтобы предотвратить его повторение в будущем, и внедряет улучшения в процессы и системы безопасности.

Перечисленные процессы работают в совокупности, они взаимно дополняют друг друга, и обеспечивают надежную защиту информационных ресурсов организации. При этом SOC использует различные инструменты автоматизации этих процессов для обеспечения более эффективной работы в борьбе с киберугрозами [2]. Некоторые из ключевых инструментов включают в себя:

1. SIEM (Security Information and Event Management): SIEM-системы предоставляют возможность собирать, анализировать и отображать данные о безопасности из различных источников. Они способны обнаруживать аномальное поведение и предупреждать об угрозах.

2. IDS/IPS (Intrusion Detection System/Intrusion Prevention System): Системы обнаружения и предотвращения вторжений позволяют идентифицировать атаки и предотвращать их до того, как они нанесут урон системе.

3. Автоматизированные инструменты анализа угроз: Эти инструменты помогают SOC быстро обрабатывать и анализировать большие объемы данных, выявлять угрозы и классифицировать их по степени угроз безопасности.

4. Автоматизированные системы управления уязвимостями: Эти системы сканируют сети и приложения на наличие уязвимостей, устанавливают патчи и обеспечивают обновления безопасности.

5. SOAR (Security Orchestration, Automation and Response): Технология SOAR используется для автоматизации рутинных задач безопасности, ускорения реагирования на угрозы и упрощения согласования действий между различными системами безопасности.

Названные инструменты способствуют автоматизации многих операций SOC, повышению эффективности и улучшению способности защиты от киберугроз [3].

Другой важной задачей функционирования SOC является комплектование высококвалифицированными кадрами. В SOC требуются специалисты с профессиональными навыками и компетенциями для обеспечения надежной защиты информационной безопасности. Так, большинство обеспечивающих фугкций в SOC выполняют:

– аналитики безопасности (Security Analysts): Они отвечают за мониторинг и анализ данных безопасности для выявления аномальной активности и угроз;

– инцидент-менеджеры (Incident Managers): Эти специалисты занимаются реагированием на инциденты безопасности, осуществляют координацию действий и управление инцидентами;

– инженеры безопасности (Security Engineers): Они работают над проектированием, развертыванием и обслуживанием систем безопасности, а также проводят технические расследования инцидентов;

– специалисты по управлению уязвимостями (Vulnerability Management Specialists): Эти специалисты отвечают за идентификацию, классификацию и устранение уязвимостей в информационной инфраструктуре;

– аналитики угроз (Threat Intelligence Analysts): Они отслеживают и анализируют современные киберугрозы, оценивают потенциальные риски и предоставляют контекст для событий безопасности.

Кроме того, в SOC необходим дополнительный персонал по управлению проектами, командный состав и руководители с высокой степенью ответственности за проделанную работу. Персональную ответственность за обеспечение эффективного управления и координации работ несет руководитель SOC (SOC Manager) или директор-администратор информационной безопасности (Chief Information Security Officer).

В отличие от MSSP (Managed Security Service Provider), где совсем по-другому организована защита информации, SOC подходит для крупных организаций с достаточными ресурсами для создания выделенной инфраструктуры. MSSP больше подходит для малого и среднего бизнеса, у которого нет ресурсов для поддержания внутреннего SOC. Вот некоторые принципиальные отличия SOC (Security Operations Center) от MSSP (Managed Security Service Provider):

1. Собственность и управление. SOC – внутренняя функция, которая напрямую управляется компанией. MSSP – сторонний поставщик услуг безопасности, компании обращаются к нему для аутсорсинга некоторых или всех функций безопасности.

2. Сфера услуг. SOC в основном фокусируется на непрерывном мониторинге, обнаружении угроз и реагировании на инциденты. MSSP предлагает широкий спектр услуг, включая управление брандмауэрами,

обнаружение вторжений, управление уязвимостями и мониторинг событий безопасности.

3. Настройка. SOC обеспечивает индивидуальную защиту с учетом конкретных рисков организации. MSSP использует стандартизированные протоколы для управления общими рисками среди клиентов.

4. Затраты. SOC требует значительных первоначальных инвестиций в инфраструктуру, передовые технологии и квалифицированный персонал. MSSP работает по модели регулярных платежей, предлагая более доступное начальное решение с предсказуемыми затратами со временем.

5. Человеческие ресурсы и экспертиза. SOC включает высокоспециализированные внутренние команды, которые глубоко понимают конкретный контекст организации. MSSP полагается на экспертов с навыками работы в разных секторах, которые работают с несколькими клиентами и отраслями.

6. Подход к работе. SOC функционирует внутри инфраструктуры компании, что позволяет быстро реагировать и тесно сотрудничать с внутренними ИТ-командами. MSSP работает удаленно с использованием безопасных инструментов управления.

Таким образом, Security Operations Center (SOC) представляет собой важное подразделение в организации, ответственное за обеспечение безопасности информационных систем. Через сочетание высокотехнологичных инструментов и компетентного персонала SOC обеспечивает обнаружение, реагирование и предотвращение киберугроз. Ключевые процессы в SOC включают мониторинг и анализ, обнаружение инцидентов, управление уязвимостями и улучшение процессов обеспечения информационной безопасности. Для эффективного функционирования SOC требуется команда специалистов с различными навыками в области информационной безопасности. Автоматизированные инструменты играют важную роль в повышении эффективности работы SOC и борьбы с киберугрозами. В целом, SOC является неотъемлемым компонентом в обеспечении безопасности информационных активов и защите от современных киберугроз.

Список использованных источников:

1. Белоус А.И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения: учебник / А.И. Белоус. М.: Техносфера, 2021. 483 с. ISBN 978-5-94836-612-8.

2. Гришина Н.В. Информационная безопасность предприятия: учебное пособие / Н.В. Гришина. М.: Форум: ИНФРА-М, 2018. 238 с. ISBN 978-5-00091-545-5.

3. Заботина Н.Н. Проектирование информационных систем: учебное пособие. М.: ИНФРА-М, 2020. 331 с. ISBN 978-5-16-104187-1.

Yapparov R.M.
Ufa University of Science and Technology, Ufa

ON THE ISSUE OF IMPROVING THE INFORMATION SECURITY SYSTEM IN THE ORGANIZATION

Abstract. The article is devoted to a comparative analysis of Security Operation Center (SOC) functions and their use in modern organizations. The main aspects of SOC creation and management, including the processes of monitoring, detecting and responding to cyber threats, are considered. The article also discusses the technological tools and data analysis methods necessary to ensure the security of information systems. The article provides practical recommendations for optimizing the operation of SOC and improving the effectiveness of protection against cyber attacks.

Keywords: Security Operation Center (SOC), information security, processes, monitoring, response, incidents.