Столыпинский вестник

Научная статья
Original article
УДК 004.424

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ БЕЗОПАСНОСТИ И СОБЫТИЯМИ (SIEM)

SECURITY INCIDENT AND EVENT MANAGEMENT (SIEM)

Цымбал Федор Алексеевич студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), tsybal007@rambler.ru

Tsymbal Fedor Alekseevich bachelor student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), tsybal007@rambler.ru

Аннотация: Решения SIEM позволяют получать и сопоставлять информацию из разных систем. Эта агрегация данных позволяет командам более эффективно обнаруживать угрозы, более эффективно управлять предупреждениями и предоставлять лучший контекст для расследований. Решения SIEM также полезны для регистрации событий, происходящих в системе, или создания отчетов о событиях и производительности. Затем вы можете использовать эту информацию для подтверждения соответствия или для оптимизации конфигураций.

Abstract: SIEM solutions allow you to receive and compare information from different systems. This data aggregation allows teams to more effectively

detect threats, manage alerts more effectively, and provide better context for investigations. SIEM solutions are also useful for logging events that occur in the system or generating event and performance reports. You can then use this information to validate compliance or to optimize configurations.

Ключевые слова: информационная безопасность, SIEM, конфигурации системы, управление

Keywords: information security, SIEM, system configurations, management

Защита от потери данных (DLP)

Стратегии защиты от потери данных включают инструменты и методы, которые защищают данные от потери или изменения. Это включает в себя категоризацию данных, резервное копирование данных и мониторинг того, как данные распространяются внутри организации и за ее пределами. Например, вы можете использовать решения DLP для сканирования исходящих электронных писем, чтобы определить, не передается ли конфиденциальная информация ненадлежащим образом.

Система обнаружения вторжений (IDS)

IDS-решения — это инструменты для мониторинга входящего трафика и обнаружения угроз. Эти инструменты оценивают трафик и предупреждают обо всех экземплярах, которые кажутся подозрительными или вредоносными.

Система предотвращения вторжений (IPS)

Решения безопасности IPS аналогичны решениям IDS, и они часто используются вместе. Эти решения реагируют на трафик, который определяется как подозрительный или вредоносный, блокируя запросы или завершая сеансы пользователей. Вы можете использовать решения IPS для управления сетевым трафиком в соответствии с определенными политиками безопасности.

Поведенческая аналитика пользователей (UBA)

Решения UBA собирают информацию о действиях пользователей и сопоставляют это поведение с базовым уровнем. Затем решения используют этот базовый уровень в качестве сравнения с новым поведением для выявления несоответствий. Затем решение помечает эти несоответствия как потенциальные угрозы. Например, вы можете использовать решения UBA для мониторинга действий пользователей и определения того, начинает ли пользователь экспортировать большие объемы данных, что указывает на внутреннюю угрозу.

Кибербезопасность блокчейна

Кибербезопасность блокчейна — это технология, основанная на неизменных транзакционных событиях. В технологиях блокчейна распределенные сети пользователей проверяют подлинность транзакций и обеспечивают сохранение целостности. Хотя эти технологии еще не получили широкого распространения, некоторые компании начинают включать блокчейн в большее количество решений.

Обнаружение конечных точек и ответ (EDR)

Решения EDR для кибербезопасности позволяют отслеживать активность конечных точек, выявлять подозрительные действия и автоматически реагировать на угрозы. Эти решения предназначены для улучшения видимости оконечных устройств и могут использоваться для предотвращения проникновения угроз в ваши сети или утечки информации. Решения EDR основаны на непрерывном сборе данных конечных точек, механизмах обнаружения и регистрации событий .

Управление состоянием облачной безопасности (CSPM)

CSPM — это набор методов и технологий, которые вы можете использовать для оценки безопасности ваших облачных ресурсов. Эти технологии позволяют сканировать конфигурации, сравнивать средства защиты с эталонными показателями и обеспечивать единообразное применение политик безопасности. Часто решения CSPM предоставляют

рекомендации или рекомендации по исправлению, которые можно использовать для повышения уровня безопасности.

Удаленный доступ через VPN и SASE

Виртуальная частная сеть удаленного доступа (VPN) позволяет организациям предоставлять безопасный удаленный доступ к данным и приложениям, находящимся в корпоративной сети. VPN создает туннель между сетью и удаленным пользователем. Он защищает трафик, проходящий через туннель, путем его шифрования.

Удаленный доступ через VPN подключает одного пользователя к локальным ресурсам, но не обеспечивает видимость облачных ресурсов. Secure Access Service Edge (SASE) устанавливает безопасность в гибридной среде, обеспечивая видимость всех ресурсов. SASE — это облачная служба, которая не использует VPN или автономные прокси-серверы. Вместо этого он предоставляет различные инструменты сетевой безопасности в виде облачной службы.

BYOD

Принесите свое собственное устройство (BYOD) — это подход, который позволяет сотрудникам использовать свои личные устройства, такие как ноутбуки, планшеты, смартфоны, USB-накопители и ПК, в рабочих целях. Это означает, что сотрудники могут использовать свои устройства для подключения к корпоративной сети и доступа к важным системам и конфиденциальным данным.

BYOD может улучшить взаимодействие с пользователем, позволяя сотрудникам работать на знакомых устройствах из любого места. Это позволяет сотрудникам использовать свои устройства для удаленной работы из дома или во время путешествий. Однако BYOD часто приводит к теневой ИТ, поскольку ИТ-персонал плохо видит (если вообще видит) эти конечные точки и не может должным образом внедрить и поддерживать меры безопасности.

Организации могут защититься от угроз BYOD, используя виртуализацию приложений и решения для обеспечения безопасности конечных точек, чтобы улучшить видимость и получить комплексные средства управления безопасностью и управлением.

Примеры информационной безопасности в реальном мире

Существует много способов реализовать информационную безопасность в вашей организации, в зависимости от вашего размера, доступных ресурсов и типа информации, которую необходимо защитить. Ниже приведены три примера того, как организации реализовали информационную безопасность для удовлетворения своих потребностей.

DLP в Berkshire Bank

Berkshire Bank — пример компании, которая решила реструктурировать свою стратегию DLP. Компания хотела получить доступ к более подробным отчетам о событиях. Их старая система предоставляла общую информацию только тогда, когда угрозы были предотвращены, но компания хотела знать подробности о каждом событии.

Чтобы внести это изменение, Berkshire Bank внедрил решения Exabeam для обеспечения управляемого покрытия DLP. Это покрытие включало улучшенную видимость событий и централизованную информацию DLP в единой временной шкале для большей доступности. Благодаря этой расширенной информации команда безопасности Berkshire может лучше расследовать события и принимать значимые превентивные меры.

SOC в Грант Торнтон

Grant Thornton — это организация, которая сотрудничает с Exabeam для улучшения SOC. Компания стремилась улучшить свои возможности по защите системной информации и более эффективно достигать целей безопасности. В рамках партнерства Грант Торнтон создал озеро данных, служащее центральным хранилищем их данных и инструментов.

Такая централизация повысила эффективность их операций и уменьшила количество интерфейсов, к которым необходимо было получить

доступ аналитикам. Централизация также позволила компании использовать расширенную аналитику, включив свои новые агрегированные данные.

Реагирование на инциденты в WSU

Для защиты от растущего числа продвинутых злоумышленников Государственный университет Райта (WSU) внедрил решения Exabeam для реагирования на инциденты. Они предприняли это действие, чтобы быстрее обнаруживать инциденты, более тщательно расследовать действия и более эффективно реагировать на угрозы.

Принятый WSU инструментарий включает в себя решение для организации безопасности, автоматизации и реагирования (SOAR), а также решение для анализа поведения пользователей и объектов (UEBA). Эти инструменты позволяют WSU обнаруживать более широкий спектр угроз, включая динамические или неизвестные угрозы, и автоматически реагировать на эти угрозы. Эти инструменты предоставляют важную контекстную информацию и своевременные предупреждения об угрозах, с которыми решения не могут справиться автоматически, чтобы вы могли быстро принять меры и свести к минимуму ущерб.

Сертификаты информационной безопасности

Еще одним важным аспектом при реализации стратегий информационной безопасности является обеспечение надлежащей подготовки ваших сотрудников для защиты вашей информации. Одним из распространенных методов является сертификация информационной безопасности. Эти сертификаты гарантируют, что профессионалы соответствуют определенному стандарту знаний и осведомлены о передовом опыте.

Доступны многочисленные сертификаты как от некоммерческих организаций, так и от поставщиков. Двумя наиболее востребованными сертификатами являются:

- **CompTIA Security+** — обеспечивает базовый уровень обучения кибербезопасности. Он охватывает основные знания, связанные с ИТ-

безопасностью , и предназначен для профессионалов начального уровня, таких как младшие аудиторы или тестировщики на проникновение . Эта сертификация предлагается через Ассоциацию индустрии вычислительных технологий.

– **Сертифицированный специалист по безопасности информационных систем (CISSP)** — гарантирует знание восьми областей информационной безопасности, включая связь, оценку и тестирование, а также управление рисками. Он предназначен для специалистов высокого уровня, таких как менеджеры по безопасности. Эту сертификацию можно получить в Международном консорциуме по сертификации безопасности информационных систем (ISC)².

Литература

1. Бабаш, А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2019. - 432 с.
2. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.
3. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2017. - 400 с.
4. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2017. - 476 с.
5. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 с.
6. Баранова, Е.К. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Е.К. Баранова, А.В. Бабаш, Д.А. Ларин. - М.: Риор, 2008. - 400 с.
7. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013. - 474 с.
8. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с.

9. Глинская, Е.В. Информационная безопасность конструкций ЭВМ и систем: Учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: Инфра-М, 2018. - 64 с.

References

1. Babash, A.V. Information security: Laboratory workshop / A.V. Babash, E.K. Baranova, Yu.N. Melnikov. - M.: KnoRus, 2019. - 432 p.
2. Babash, A.V. Information Security. Laboratory workshop: Textbook / A.V. Babash, E.K. Baranova, Yu.N. Melnikov. - M.: KnoRus, 2013. - 136 p.
3. Baranova E.K. Information security and information protection: Textbook / E.K. Baranova, A.V. Babash. - M.: Rior, 2017. - 400 p.
4. Baranova E.K. Information security and information protection: Textbook / E.K. Baranova, A.V. Babash. - M.: Rior, 2017. - 476 p.
5. Baranova E.K. Information security and information protection: Textbook / E.K. Baranova, A.V. Babash. - M.: Rior, 2018. - 400 p.
6. Baranova E.K. Information Security. History of special methods of cryptographic activity: Textbook / E.K. Baranova, A.V. Babash, D.A. Larin. - M.: Rior, 2008. - 400 p.
7. Biryukov, A.A. Information security: protection and attack / A.A. Biryukov. - M.: DMK Press, 2013. - 474 p.
8. Gafner, V.V. Information Security: Textbook / V.V. Gafner. - Rn / D: Phoenix, 2010. - 324 p.
9. Glinskaya E.V. Information security of computer structures and systems: Textbook / E.V. Glinskaya, N.V. Chichvarin. - M.: Infra-M, 2018. - 64 p.

Для цитирования: Цымбал Ф.А. Управление инцидентами безопасности и событиями (SIEM)// *Научный сетевой журнал «Столыпинский вестник» №4/2022.*