Версия документа: 002-2024

Функциональные возможности системы «ASPM Platform»

Москва, 2024

Содержание

1. Общие сведения

1.1 Назначение и краткая характеристика системы

ASPM Platform (далее – платформа, система) позволяет проводить комплексный анализ приложений для обеспечения безопасности и централизованного управления процессами обнаружения и устранения уязвимостей. Платформа обеспечивает взаимодействие между командами разработки и специалистами по безопасности, способствуя совместному выявлению и устранению уязвимостей на всех этапах жизненного цикла продукта.

Платформа поддерживает работу со следующими классами решений:

- SAST;
- IAC;
- OSA;
- SCA;
- DAST;
- API fuzzing;
- BCA.

Сканирование продукта включает в себя 4 ключевых этапа:

a) Настройка и запуск анализа. На этом этапе производится конфигурация инструментов и автоматический запуск анализа приложения.

b) Агрегация и корреляция данных. По результатам проведенного анализа данные централизованно собираются в едином репозитории для последующей обработки. Далее платформа осуществляет корреляцию уязвимостей, выявленных на разных уровнях анализа, что помогает определить взаимосвязи между ними и их совокупное влияние на безопасность приложения.

c) Оценка рисков и генерация рекомендаций. Платформа предоставляет интерфейс для обработки найденных уязвимостей, осуществляет замену исходных данных значениями, соответствующими заданным правилам из внутренней базы, обеспечивая единый механизм оценки и управления уязвимостями.

d) Создание отчетов и интеграция с другими системами. Платформа автоматически формирует отчеты о результатах проведенного анализа, выявленных уязвимостях и предложенных мерах по их устранению.

В результате система позволяет не допустить включения в состав разрабатываемых приложений уязвимых компонентов, исключить использование уязвимого функционала, определить ошибочную и вредоносную программную логику.

1.2 Глоссарий

В тексте настоящего документа представлены следующие термины и сокращения (см. Таблица 1).

Таблица 1 – Перечень терминов и сокращений

Сокращение/аббревиатура	**Значение**
API (Application programming interface)	Программный интерфейс приложения, описание и реализация способов взаимодействия программных продуктов
OSA (Open Source Analysis) и SCA (Software Composition Analysis)	Анализ библиотек и компонентов с открытым исходным кодом, которые входят в периметр разработки программного обеспечения
CI/CD (Continuous integration/continuous deployment,)	Системы для непрерывной интеграции и непрерывных поставок приложения
SAST (Static Application Security Testing)	Статический анализ исходного кода приложений с применением специальных инструментов
IAC (Infrastructure as Code)	Подход для управления и описания инфраструктуры через конфигурационные файлы
Fuzzing	Техника тестирования программного обеспечения, при которой осуществляется передача приложению на вход неправильных, неожиданных или случайных данных
Сканирование	Производимое с помощью платформы исследование
Severity	Оценка степени риска, влекомого уязвимостью, соответствующей дефекту в количественном

	представлении или представлении на шкале наименований
Quality Gate	Автоматические проверки качества, которые устанавливают пороговые значения для продвижения продукта по конвейеру разработки
DAST (Dynamic Application Security Testing)	Динамический анализ приложений с использованием специальных инструментов
BCA (Bytecode and Container Analysis)	Автоматический анализ скомпилированных артефактов сборки, дистрибутивов программного обеспечения и docker контейнеров с помощью определенных инструментов
Артефакт	Любой объект, который был задокументирован и сохранен в репозитории так, что его можно получить по запросу
Уязвимость	Сбой, изъян или слабое место в программном обеспечении, которое может быть использовано для нарушения функциональности или несанкционированного доступа к ресурсам приложения
Дефекты	Любое несоответствие исходного кода, конфигурационных, служебных и иных файлов проекта, а также документации требованиям безопасной разработки и безопасного программирования, повлекшее возникновение уязвимости

2. Функциональные возможности

В данном разделе описаны особенности реализации системы, ролевая модель, а также функциональные возможности платформы.

2.1 Особенности реализации системы

ASPM Platform реализована в виде веб-приложения, пользовательское взаимодействие осуществляются посредством работы с веб-браузером.

2.2 Ролевая модель

Платформа предполагает наличие следующих ролей:

- Администратор;
- Техническая поддержка;
- Руководитель;
- Старший аналитик;
- Аналитик;
- Разработчик.

Сведения о ролях с описанием доступных полномочий для каждой роли представлены в таблицах 2.1, 2.2, 2.3, 2.4.

Таблица 2.1 – Роли пользователей. Полномочия - 1

Разделы/Роли	Администратор	Тех. поддержка	Руководитель
1. Статистика	✓	✓	✓
2. Группы	✓	✓*	X
3. Репозитории	X	✓	X
4. Сканирования	✓	✓	✓
5. Дефекты	✓	✓	✓
6. DAST	✓	✓	✓
7. Компоненты	✓	✓	✓
8. Контейнеры	✓	✓	✓
9. Опубликованные ресурсы	✓	✓	✓
10. События	✓	✓	✓
11. Артефактории	✓	✓	✓
12. Распределение дефектов	X	X	X

✓* – за исключением прав на удаление

Таблица 2.2 – Роли пользователей. Полномочия - 2

Разделы/Роли	Старший аналитик	Аналитик	Разработчик
1. Статистика	✓	✓	✓
2. Группы	✓*	✓*	X
3. Репозитории	✓	✓	X
4. Сканирования	✓	✓	✓
5. Дефекты	✓	✓	✓
6. DAST	✓	✓	✓
7. Компоненты	✓	✓	✓
8. Контейнеры	✓	✓	✓
9. Опубликованные ресурсы	✓	✓	✓
10. События	✓	✓	✓

11. Артефактории	✓	✓	✓
12. Распределение дефектов	✓	X	X

✓* – за исключением прав на удаление

Таблица 2.3 – Роли пользователей. Доступ к настройкам платформы - 1

Разделы/Роли	Администратор	Тех. поддержка	Руководитель
1. Пользователи и роли	✓	X	X
2. API	✓	X	X
3. Почтовые уведомления	✓	X	X
4. Трекер задач	✓	✓	X
5. Аутентификация	✓	X	X
6. Хранилище кода	✓	X	X
7. Интеграции	✓	X	X
8. Пользовательские правила	✓	✓	X
9. Лицензии	✓	✓	X

Таблица 2.4 – Роли пользователей. Доступ к настройкам платформы - 2

Разделы/Роли	Старший аналитик	Аналитик	Разработчик
1. Пользователи и роли	X	X	X
2. API	X	X	X
3. Почтовые уведомления	X	X	X
4. Трекер задач	X	X	X
5. Аутентификация	X	X	X
6. Хранилище кода	X	X	X
7. Интеграции	X	X	X
8. Пользовательские правила	✓	✓	X
9. Лицензии	X	X	X

2.3 Аутентификация

ASPM Platform поддерживает интеграцию с корпоративными системами, такими как Active Directory, для централизованного управления доступом. При подключении сервера для синхронизации учетных записей происходит импорт данных в платформу, после чего администраторы могут назначать пользователям роли и распределять их по командам.

2.4 Взаимодействие с API

При работе с API платформы требуется генерация API-ключа для аутентификации запросов. API-ключ является обязательным атрибутом каждого запроса к серверу, обеспечивая защиту передаваемых данных.

2.5 Настройки сканирования репозитория

Каждое сканирование может иметь уникальные настройки, такие как:

- Задание таймаута job – установка таймаута для выполнения задач, связанных с CI/CD процессами.
- Настройки ветки – выбор контура сканирования для адаптации процессов сборки и тестирования в зависимости от стадии разработки или среды выполнения.
- Взаимодействие с Quality Gate – отслеживание количества уязвимостей, обнаруженных в конкретной ветке (отображение в виде числа уязвимостей для каждой группы severity).
- Сканирование tar.gz – опция сканирования архивов tar.gz для автоматизации проверок на наличие уязвимостей в файлах данного типа.

- Настройка сканирования динамического анализа – возможность включения динамического анализа.

2.6 Интеграция сканеров безопасности

ASPM Platform поддерживает работу с широким спектром инструментов сканирования и объединяет результаты анализа в единую систему. Интеграция обеспечивает более точное выявление уязвимостей, полученных с помощью различных инструментов, каждый из которых может быть настроен на выявление проблем определенного типа.

2.7 Корреляция и объединение результатов

Путем корреляции уязвимостей, найденных разными сканерами, платформа объединяет схожие проблемы в единые записи, уменьшая избыточность информации и упрощая последующий анализ.

2.8 Распределение дефектов

Распределение дефектов включает в себя назначение ответственных лиц для всех выявленных дефектов. Также предусматривается возможность фильтрации по ответственным лицам, что позволяет отслеживать статус каждого дефекта и контролировать процесс его обработки.

2.9 Трекер задач

Для эффективного управления задачами платформа поддерживает интеграцию с трекерами задач, такими как Jira. Настройка интеграции позволяет синхронизировать задачи и дефекты между платформой и трекером,

обеспечивая непосредственное взаимодействие между разработчиками и специалистами по безопасности.

2.10 Поддержка языков и экосистем

Платформа поддерживает анализ приложений для следующих языков программирования:

- Apex;
- Bash;
- C;
- C#;
- C++;
- Cairo;
- Clojure;
- Dart;
- Elixir;
- Go;
- HTML;
- Java;
- JavaScript;
- JSON;
- JSX;
- Julia;
- Kotlin;
- Lisp;
- Lua;
- Ocaml;
- PHP;
- Python;
- R;
- Ruby;
- Rust;
- Scala;
- Solidity;
- Swift;
- TypeScript;
- XML;
- YAML.

Система поддерживает OSA и анализ компонентов приложений, включая как исходный код, так и бинарные файлы. Функциональность платформы предусматривает построение графа зависимостей, позволяющего визуализировать связи между компонентами и выявлять потенциальные уязвимости.

Платформа может работать со следующими форматами файлов:

- Образы Docker;
- APB;
- APK;
- DMG;
- EXE;
- IPA.

В рамках интеграции с DAST-решениями реализована возможность динамического анализа и тестирования конечных точек для выявления уязвимостей в API и других компонентах системы. Платформа также поддерживает фаззинг-тестирование API, осуществляя проверку различных сценариев.

Дополнительно осуществляется анализ инфраструктурного кода, включая Terraform, Ansible, что позволяет определять уязвимости и потенциальные риски на уровне конфигурации и развертывания.

2.11 Артефактории

Функция сканирования артефакториев в платформе предоставляет возможность проводить комплексный анализ артефактов, хранящихся в JFrog Artifactory/Sonatype Nexus Repository. В процессе сканирования платформа идентифицирует все доступные артефакты и выводит детализированный список компонентов, включая их версии, типы и другие метаданные.

2.12 Аналитика и визуализация

ASPM Platform предоставляет инструменты для визуализации аналитических данных, в частности графики для интерактивного исследования. Графики обновляются в реальном времени и показывают изменения в системе, отражая актуальную информацию для анализа.

2.13 Отчеты и уведомления

ASPM Platform формирует детализированный отчет, в котором уязвимости классифицируются по уровню критичности. Отчеты содержат описание и рекомендации по устранению выявленных проблем, а также включают визуализации, такие как графики и диаграммы, ссылки на соответствующую документацию и базы данных уязвимостей. Отчеты интегрируются с существующими системами управления безопасностью и смежными платформами, обеспечивая обмен данными.

В случае обнаружения новых уязвимостей в приложениях в продуктивном контуре или контуре разработки система отправляет соответствующее уведомление командам разработки и безопасности.