Платформа для управления уязвимостями и обеспечения безопасности в процессах разработки и DevSecOps "Tron ASOC v.0.5"

Руководство администратора

Июнь 2024

Содержание

Термины и определения	3
Общие сведения	4
Начало работы в системе	6
Настройка правил авторизации	6
Управление пользователями и ролями	7
Роли	7
Добавление роли	7
Изменение роли	8
Пользователи	8
Добавление пользователя	9
Редактирование профиля пользователя	10
Изменение пароля пользователя	11
Настройка интеграций с инструментами	11
Инструменты безопасности	11
Подключение инструментов безопасности	11
Редактирование инструмента	13
Удаление инструмента	13
Источники сканирования	14
Подключение источника сканирования	14
Редактирование источника сканирования	15
Удаление источника сканирования	16

Термины и определения

БДУ	Банк данных угроз безопасности информации
по	Программное обеспечение
Уязвимость (Vulnerability)	Уязвимость программного обеспечения — это сбой, изъян или слабое место в программном обеспечении, которое может быть использовано для нарушения функциональности или несанкционированного доступа к ресурсам приложения
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ASOC (Application Security Orchestration and Correlation)	платформы или решения, предназначенные для управления и координации безопасностью приложений. ASOC позволяет автоматизировать процессы обнаружения, анализа и реагирования на угрозы безопасности, связанные с приложениями.
CI/CD	комбинация непрерывной интеграции (continuous integration) и непрерывного развертывания (continuous delivery или continuous deployment) программного обеспечения в процессе разработки. CI/CD объединяет разработку, тестирование и развертывание приложения.
CVE	Common Vulnerabilities and Exposures - база данных общеизвестных уязвимостей информационной безопасности. Каждой уязвимости присваивается идентификационный номер вида CVE-год-номер, описание и ряд общедоступных ссылок с описанием.
DevSecOps	методология разработки программного обеспечения, которая интегрирует практики безопасности (Sec) в процессы разработки и поставки программного обеспечения (DevOps).
NVD	National Vulnerability Database - национальная база данных уязвимостей. Американский правительственный репозиторий данных управления уязвимостями на основе стандартов, представленных с использованием протокола автоматизации содержимого безопасности.

PCI SSC Pipeline	PCI Security Standards Council - открытое глобальное сообщество, задачи которого включают непрерывное развитие, совершенствование, хранение, распространение и внедрение стандартов безопасности для защиты данных платежных карт. сочетание заданий для непрерывной доставки программного обеспечения, состоит из нескольких состояний или этапов,
SAST (Static Application Security Testing)	это процесс тестирования приложения на наличие ошибок и уязвимостей в исходном коде с применением статического анализа. Статический анализ может применяться для поиска кода, потенциально содержащего уязвимости
Проект	это сущность, которая создается авторизованным пользователем, чтобы логически объединить весь набор связанных приложений или компонентов, которые разрабатываются или поддерживаются в рамках одной команды или организации, и который нужно проверять на соответствие политикам безопасности компании и качество.

Общие сведения

«TRON.ASOC» - программный продукт для обнаружения и управления уязвимостями, а также обеспечения безопасности в процессах разработки и DevSecOps.

«TRON.ASOC» позволяет осуществлять всесторонний контроль безопасности разрабатываемых проектов, обеспечивая надежную защиту на всех этапах разработки.

«TRON.ASOC» интегрируется с репозиторием Gitlab, реестром образов Nexus и различными инструментами анализа безопасности разрабатываемых продуктов, такими как статический анализатор исходного кода РТ Application Inspector и анализатор безопасности контейнеров KCS. Программа управляет проверками исходного кода и образов контейнеров на уязвимости и помогает управлять результатами этих проверок. Интеграция с этими инструментами позволяет настроить сканирование, запускать проверки и консолидировать результаты.

«TRON.ASOC» упрощает работу с найденными при помощи инструментов AST проблемами и уязвимостями, проводя их анализ и группировку для более эффективного управления.

«TRON.ASOC» осуществляет консолидацию и визуализацию данных, предоставляя пользователям наглядную информацию о состоянии безопасности их проектов.

«TRON.ASOC» предлагает удобный пользовательский интерфейс, доступный в современных браузерах на движке Chromium (Google Chrome, Яндекс Браузер, Edge, Safari и т.д.) и Firefox.

«TRON.ASOC» предоставляет возможности для управления сканированиями, включая настройку параметров сканирования, планирование запусков и мониторинг выполнения сканирований.

«TRON.ASOC» позволяет выгружать отчеты по результатам сканирований в формате JSON, что обеспечивает удобство интеграции с другими системами и инструментами анализа данных.

Начало работы в системе

В браузере перейдите по адресу URL платформы ASOC. На странице авторизации (Рис.1) обязательные поля отмечены звездочкой. Есть возможность переключения между русским и английским языками. Для входа введите имя и пароль учетной записи и нажмите кнопку Войти.

TRON ASOC	Joop noxanosatsi: Ku v Hun nonsoosatenni* Begute wun nonsoosatenni Begute wun nonsoosatenni Imagonation Raponation Imagonation Bookm Badumu naponation Bookm Badumu naponation Innyvarte Gonazie wuhopmaajuur o Tron ASOO (2)

Рис.1

Настройка правил авторизации

На вкладке Аутентификация (Рис.2) можно задать параметры требований к паролю, максимальной продолжительности сеанса, время выхода из системы после периода неактивности, количество попыток ввода пароля до временной блокировки, длительность временной блокировки.

	Аутентификация	
Аутентификация	Требования к паролю	Сохранить
Управление доступом		
Проекты	2 Пароль должен содержать хотя бы одну прописную и одну строчную букау.	
Интеграции 🗸	🕑 Пароль должон содержать хотя бы один специальный символ .	
Инструмент безопасности	Минимальная длина пароля (символов): 8	
Источники сканирования		
Виртуальные помощники	Аутентификация	
	Максимальная продолжительность севноа	
	Выход из сиютемы после неактивнооти 5 мин. О	
	Количество попыток ввода пароля до временного бана 3	
	Период временного запрета	
≗ admin@admin.com >		

Управление пользователями и ролями

Управление пользователями и ролями происходит в разделе Управление доступом. Переход к разделу осуществляется из левого сайд-бар меню.

Роли

Информация о ролях в системе отображается в разделе Управление доступом на вкладке Роли (рис.3). Здесь также доступен поиск по роли, возможность просмотреть количество пользователей с определенной ролью, сортировка ролей по идентификатору, имени роли и количеству пользователей.

	Управление доступом				
Аутонтификация	Пользователи Роли				
Управление доступом Проекты	Добавить роль				Поиск Q
Интеграции ~	Идентификатор роли 三	Название роли ~	Fpynna Active Directory	Пользователи ч	
Инструмент безопасности	dev	Developer		1	Û
О программе	lsadm	IS Administrator		1	Û
	isaud	IS Auditor		0	Û
	isoff	IS Officer		0	Û
	Bcero 4				< 1 > По/страница ч

Рис.3

Добавление роли

Добавление роли (Рис.4) производится из раздела Управление доступом, вкладка Роли. Для создания новой роли нажмите кнопку Добавить роль.

На странице создания роли заполните общую информацию: идентификатор роли имя роли, описание. Обязательные для заполнения поля отмечены звездочкой. Отметьте доступные роли разрешения на просмотр или управление разделами системы. Чекбокс Управление для назначения прав на управление разделом становится активным только после выбора чекбокса Просмотр на право просмотра соответствующего раздела.

	Управление дост	упом › Добавить роль			
Аутентификация	Общая информация			Отмена	Создать
Управление доступом	Идентификатор роли*				
Проекты					
Интеграции 🗸	Только латичские букво без пробелов и специ симеолов	алонох			
Инструмент безопасности	Название роли*				
Источники сканирования					
Опрограмме	Описание				
	Разрешения				
	Поиск	Q			
	Настройки аутентификации	Просмотр и управление			
	Роли	Просмотр	Управление		
	Пользователи	Просмотр	Управление		
	Проекты	Просмотр	Управление		
	Инструменты безопасности	Просмотр и управление			
	Источники сканирования	Просмотр и управление			
	Проверки безопасности	Просмотр и управление			
	Конвейеры безопасности	Просмотр и управление			

Рис.4

Изменение роли

Чтобы отредактировать роль, нажмите на идентификатор роли в списке ролей на вкладке Роли. Форма редактирования аналогична форме создания роли, за исключением поля Идентификатор роли, которое является недоступным для редактирования.

	Управление дост	тупом > Develope	er		
Аутентификация	Общая информация			Отмена	Cox
	Идентификатор роли*				
Проекты	dev				
Интеграции ~	Только латичские бухам без пробелов и спец симеолов	prentereox			
Инструмент безопасности	Название роли*				
Источники сканирования	Developer				
О программе	Описание				
	Разряшения Польователи Настройки вутентификации Роли Польователи Инструменти безопасности Инструменти безопасности Истремения сканорования Проверки безопасности	Decuerop u repasteure Peccuerop Peccuerop Peccuerop Peccuerop Peccuerop Peccuerop Peccuerop u repasteure Peccuerop u repasteure Peccuerop u repasteure Peccuerop u repasteure	 Vippanove Vippanove Vippanove 		

Рис.5

Пользователи

Информация о пользователях системы отображается в разделе Управление доступом на вкладке Пользователи (Рис. 5). Здесь также доступен поиск, возможность просмотреть назначенные пользователю роли, назначение принудительной смены пароля и удаление пользователя

	Управление доступом				
Аутентификация	Пользователи Роли				
Управление доступом	Добавить пользователя Сброс пароля 📋 Удалить			Поиок	Q
Проекты					
Интеграции у	Имя пользователя Е	Отображаемое имя ~	Назначенные роли	Сброс пароля	
Инструмент безопасности	admin	admin	Isadm	No	
Источники сканирования	C testuser	Test User	dev	No	8
U Igo passo	Боего 2 / Выбрано 0			¢ 🛛	1 > (10/orpawuja v)

Рис.6

Добавление пользователя

Чтобы создать нового пользователя, нажмите на кнопку Добавить пользователя на вкладке Пользователи. На странице создания пользователя заполните общую информацию: имя пользователя, отображаемое имя, электронную почту, а также введите и подтвердите пароль доступа.Обязательные для заполнения поля отмечены звездочкой. Опционально можно выбрать чекбокс принудительной смены пароля, чтобы пользователь сменил пароль при следующем входе в систему. Выберите как минимум одну роль для назначения пользователю и нажмите кнопку Создать.

	Управление доступом > Добавить поль	зователя	
Аутентификация	Общая информация		Отмена Создать
Управление доступом	Имя пользователя*		
Проекты			
Интеграции ~	Отображаемое имя		
Инструмент безопасности			
Источники сканирования	Электронная почта		
Виртуальные помощники			
Опрограмме	Новый пароль*		
	Введите новый пароль 🔹		
	Проти заляни гозарнилі, •••••••••••••••• •••••••••••••••• ••••••••••••••••••••••••••••••••••••		
	ACTIVEROLE ACTIVEUSER arragent generFour argentget		

Рис.6

Редактирование профиля пользователя

Чтобы отредактировать данные пользователя, нажмите на Имя пользователя в списке пользователей на вкладке Пользователи. Форма редактирования аналогична форме создания пользователя, за исключением поля Имя пользователя, которое является недоступным для редактирования.

	Управление доступом	ı → admin	
Аутентификация	Общая информация	Отмена Сокрыти	ь
Управление доступом	Имя пользователя*		
Проекты	admin		
Интеграции ~	Отображаемое имя		
Инструмент безопасности	admin		
Источники сканирования	Электронная почта		
Виртуальные помощники	admin@admin.com		
Опрограмме	Новый пароль		
	Введите новый пароль 👁		
	Пароль должен содержаль: Не измечая В сликанова Хлят бы саши измеру Поллискую букау Слоточную букау Хлят бы саши сликаниный сликаол Подтвердите пароль Подтвердите пароль Подтвердите пароль Подложается должен соменить пароль грои следуучицем входе в систему		
	Роли для назначения*		
	Поиск Q		
	ACTIVEROLE		
	ACTIVEUSER		
	arangent -		
	_ argunt of		

Рис.7

Изменение пароля пользователя и профиль пользователя

Администратор может отметить чекбокс принудительной смены пароля. Пользователь при своем следующем входе получает форму для смены пароля. Смена пароля может производиться пользователем в профиле.

	Мой профиль	
Антонтификация	Общая информация	
Managen	оощия информация	
травление доступом	Имя пользователя admin	
Проекты	Отображаемое имя admin	
Интеграции ~	Электронная почта admin(Qadmin.com
Инструмент безопасности	Роли ISADM	A
Источники сканирования	Изменить пароль	
О программе		
	Токен АРІ	
	П Копировать Обновить ток	xeu
	Разрешения	
	Разрешения Настройки аутентификации Просм	хотр и управление
	Разрешения Настройки аутентификации Просм Польаователи Просм	xorg » yrigaatswore org, Yrogaatswore
	Разрешения Настройки аутонтификации Просм Пользователи Просм Роли Просм	лотр и управление опотр. Управление опотр. Управление
	Разрешения Настройки зутентификации Порсом Пользователии Просм Роли Проекти Просм	когр и управление отду, Управление когду, Правление
	Разрешения Настройки аутонтификации Просм Попъзователи Просм Роли Просмти Ороекти Просм Инструменти безопасности Просм	NOT pi vyťpasteve NOT p. Vypasteve NOT p. Vypasteve NOT p. Vypasteve
	Разрешения Настройки кутентификации Просм Пользователи Просм Рол Проекти Просм Инструненти безопасности Проем Источники сканирования Просм	котр и управление котр, Управление котр, Управление котр управление котр и управление
	Разрешения Настройки аутектичикали Просм Пользователи Просм Поронт Просм Мострументи безопасност Проск Иструменти безопасност Просм Проверки безопасност Просм	котр и управление котр. управление котр. управление котр и управление котр и управление
	Разрешения Настройки вутектериками Просе Пользаятели Просе Роли Проекта Просе Проекта Проект Инструменти безопасности Проек Конзейнери безопасности Проек	NOTO IN YIDERIAANIA NOTO, YIDERIAANIA NOTO, YIDERIAANIA NOTO, YIDERIAANIA NOTO IN YIDERIAANIA
	Разрешения Настройка утистификации Просек Пользователи Просек Рола Просем Просети Просек Источника ссанарования Просек Коливийери безопасности Просек Коливийери безопасности Просек	оотр. управление мотр. Управление мотр. управление мотр. и управление мотр и управление
	Разрешения Настройка зуткитификации Проси Пользоватили Проси Роля Проси Проекти Проси Проекти Проси Инструменти безопасности Проси Конгейкри безопасности Проси Конгейкри безопасности Проси	котр и управление котр. Управление котр. управление котр и управление котр и управление
	Разрешения Рекес Настойна иргинсфикации Рекес Голозантами Рекес Рабо Просм. Порона Рекес Порона Просм.	ото у управление мото, Управление мото, Управление мото у управление мото и управление
	Разрешения Кексеноналии Кексеноналии Настоянатом Поска Поска Рака Прека Прека Констринентом Поска Прека Исстринентом Поска Прека Исстринентом Поска Прека Исстринентом Поска Прека Коливание Поска Прека	котр и управление котр, Управление котр, управление котр и управление котр и управление
	Разрешения Ресес Настовни участнения Ресес Гользантам Ресес	котр и управление котр. Управление котр. и управление котр и управление котр и управление

Рис.8

Настройка интеграций с инструментами

Инструменты безопасности

Просмотр всех доступных подключенных инструментов безопасности производится в разделе Интеграции - Инструмент безопасности. Здесь можно увидеть название инструмента, описание (с возможностью сортировки по этим полям), а также перейти к удалению и редактированию инструмента.

	Инструмент безопасности		
Аутентификация Управление доступом	Побавить инструмент безопасности		Novex Q
Проекты	Инструмент Е.	Описание ~	
Интограции 🗸	Kaspersky Container Security	KCS	8
Инструмент безопасности Источники сканирования	PT Application Inspector	PTAI	Θ
Опрограмме	Boero 2		< 1 > ПО/страница ч

Рис. 9

Подключение инструментов безопасности

Чтобы добавить новый Инструмент безопасности, перейдите в раздел Интеграции - Инструменты безопасности и нажмите кнопку Добавить инструмент безопасности.



Рис.10

В форме добавления инструмента (Рис.10) в раскрывающемся меню поля Инструмент безопасности выберите инструмент (для выбора доступны: PT Application Inspector, Kaspersky Container Security), добавьте описание инструмента и URL, выберите язык результатов сканирования. Выбор метода аутентификации на этом шаге не является обязательным, но без заполнения метода аутентификации нельзя проверить соединение с инструментом. Поля для заполнения далее могут отличаться в зависимости от выбора метода аутентификации. Если метод указан и выбрана аутентификация по API -токену, нужно заполнить поле Токен API, если выбран метод аутентификации по логину и паролю, нужно заполнить поля Логин/Пароль. Чтобы сделать проверку соединения, нажмите Проверить соединение. Система отправит запрос на соединение с инструментом и в верхнем правом углу пользовательского интерфейса отобразится соответствующее уведомление.

Для завершения добавления инструмента нажмите кнопку Создать.

Редактирование инструмента

Редактирование инструмента производится по клику на Инструмент в списке Инструментов безопасности. Форма редактирования аналогична форме добавления, но имеет все поля предзаполненными.

	Инструмент безопасности Kaspersky Container Security			
Аутонтификация	Редактирование инструмента безопасности	Отмена	Сохранить	
Управление доступом	Hactpymout*			
Проекты	Kaspersky Container Sacurity v			
Интеграции ч	Onucave			
Инструмент безопасности	KCS			
Источники сканирования				
Опрограмме				
	https://sci.int.sim.group/api/v1			
	Язык рекультатов сканирования*			
	English V			
	Merca ayrenrydoxauni			
	Toxee API			
	Toxes AP*			
	kos,érőő221xahaág27igatóh			
	Descentry: Sciences and			
	-			

Рис.10

Удаление инструмента

Удаление инструмента сканирования производится на странице списка Инструменты безопасности по нажатию на иконку действий в конце строки у инструмента, который нужно удалить.

Источники сканирования

Просмотр всех доступных подключенных источников сканирования производится в разделе Интеграции - Источники сканирования. Можно отсортировать по названию, типу источника, описанию, перейти к редактированию или удалению.

	Источники сканирования			
Аутснтификация	Добавить источних сканирования		Поиск	
Управление доступом				
Проекты	Название Е.	Источник ~	Описание ~	
Интеграции ~	Git1	Git	Команда 1	•
Инструмент безопасности	Gittab_tron_core	Git	Gitlab_tron_core	8
Источники сканирования О программе	Gittab_tron_front	Git	Gitlab_tron_front	Θ
	NEXU5	Nexus	Nexus	8
	Ren 4			< 1 > 10/eppendar v

Рис.11

Подключение источника сканирования

Чтобы подключить источник сканирования, перейдите в раздел Интеграции-Источники сканирования и нажмите кнопку Add Scan source. В форме добавления источника сканирования (Рис.12) задайте имя инструмента, описание, в раскрывающемся меню поля Источник выберите источник сканирования (доступные: Gitlab, Nexus Repository).

	Источники сканирования 🚿	Іобавить новый		
Аутентификация	Добавить новый источник сканирования			Отмена Создять
Управление востуром				
D	Имя*			
Проекты	Название источника			
	Описание			
Инструмент безопасности	Описание			
О программе	L. A			
	Источник*			
	Git v			
	Мы ожилаем успешный воступ к /арі/уб/* по			
	этому URL			
	URL лаборатории Git			
	Название ветки*			
	Введите название			
	Метод аутентификации			
	Логин/Пароль 🗸			
	Погин*			
	Пароль*			
	•			
	Проверить соединение			

Рис.12

После выбора типа инструмента появятся дополнительные поля, специфичные выбранному на предыдущем шаге инструменту. Заполните URL инструмента. Заполнение поля Метод аутентификации на этом этапе не является

обязательным, но без него нельзя будет осуществить проверку соединения с источником сканирования. Поля для заполнения далее могут отличаться в зависимости от выбора метода аутентификации. Если метод указан и выбрана аутентификация по API - токену, нужно заполнить поле Токен API, если выбран метод аутентификации по логину и паролю, нужно заполнить поля Логин/Пароль. Чтобы сделать проверку соединения, нажмите Проверить соединение. Система отправит запрос на соединение с источником и в верхнем правом углу пользовательского интерфейса отобразится соответствующее уведомление.

Редактирование источника сканирования

Редактирование источника производится по клику на название источника в списке Источников сканирования. Форма редактирования аналогична форме добавления, но имеет все поля предзаполненными.

	Источники сканирования > Gitlab_tron_core	
Аутентификация	Изменение источника сканирования	Отмена Сохранить
Управление доступом	More -	
Проекты	Gitab_tron_core	
Интограции ч	Orncave	
Инструмент безопасности	Gitab_tron_core	
Источники сканирования		
О программе	Methoda and a second and a se	
	Μι σικερασιν χροιευμού χροτη π. (./po) (nd) " no " πατουγ UR.	
	They (Julian Development of the Construction o	
	Hasawee settor*	
	Core	
	Merca, ayrenndynxaant	
	Totetei API ♥	
	Torsen API*	
	gluar-txtpgTanyTotYPEmHUNtrf	
	I poop in cogereare	
	l l l l l l l l l l l l l l l l l l l	

Рис. 13

Удаление источника сканирования

Чтобы удалить источник сканирования, перейдите в раздел Интеграции - Источники сканирования и нажмите на иконку удаления в конце строки источника, который нужно удалить.