10 инструментов DevSecOps, которые необходимо знать разработчику или сисадмину

Описание

DevSecOps – это практика внедрения безопасности на каждом этапе жизненного цикла DevOps с помощью инструментов DevSecOps.

В разработке программного обеспечения DevOps – это сочетание конкретных действий по разработке с ИТ-операциями. Это сочетание направлено на повышение качества программного обеспечения и обеспечение непрерывной доставки. Если к DevOps добавить управление безопасностью, то получится DevSecOps: дисциплина, которая интегрирует безопасность как общую ответственность между миром ИТ и миром разработки программного обеспечения.

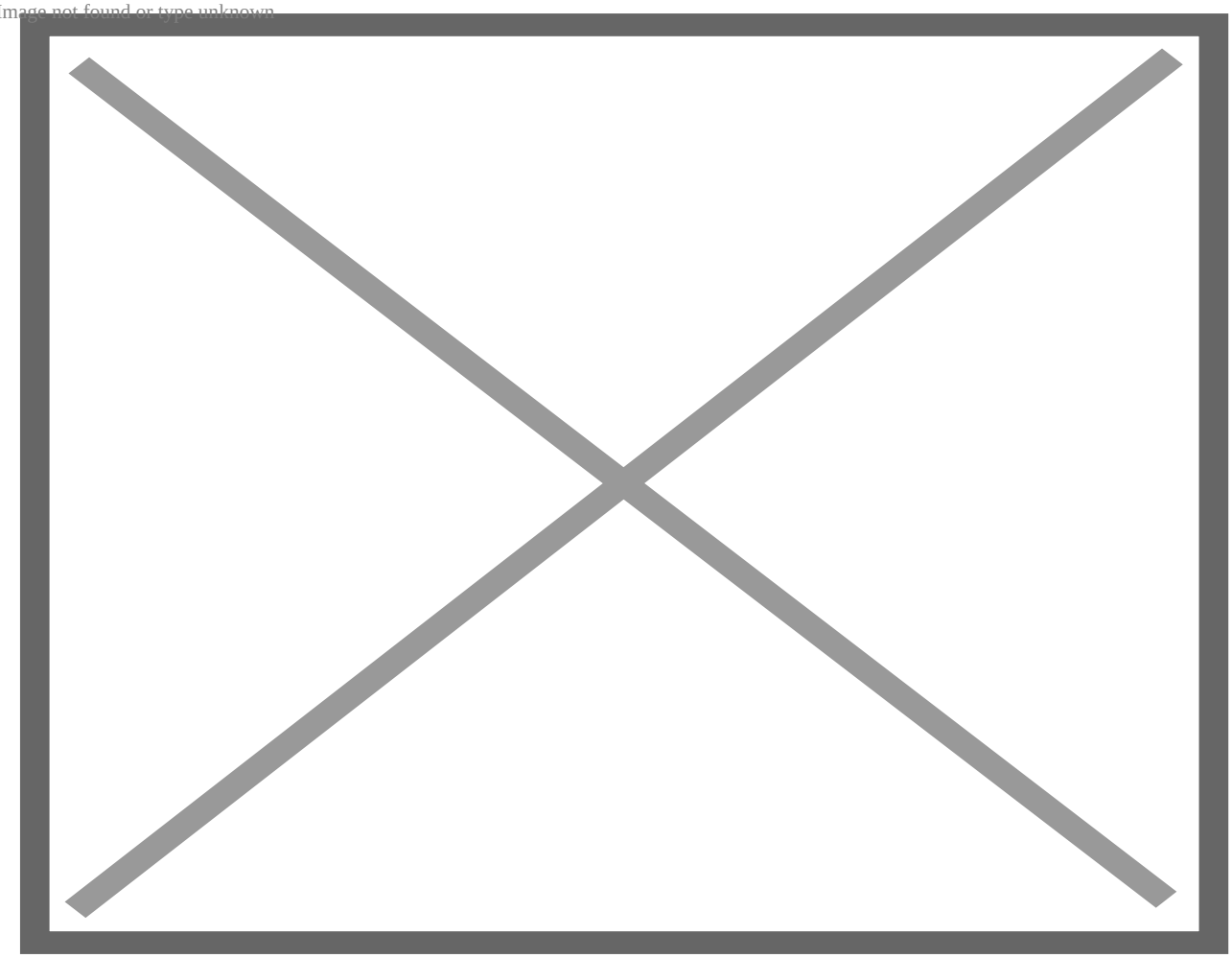
В прошлом безопасность была исключительной обязанностью специализированной команды, которая присоединялась к проектам на последних стадиях. Это хорошо работало в циклах разработки, которые длились месяцы или годы. Но при гибких циклах разработки, измеряемых неделями, методы обеспечения безопасности должны рассматриваться с самого начала и до конца проекта, а обязанности по обеспечению безопасности должны быть распределены между всеми командами разработчиков и ИТ-специалистов.

Чтобы DevSecOps работал, не нарушая парадигмы agile-методологий, его интеграция должна быть автоматизирована. Только так рабочий процесс DevOps не станет вялым при включении в него управления безопасностью. А для такой автоматизации необходимы соответствующие механизмы, которые интегрируют

средства разработки, такие как интегрированные среды разработки (IDE), с функциями безопасности.

Типы инструментов DevSecOps

Image not found or type unknown



Сочетание безопасности и DevOps может принимать различные формы. По этой причине существуют различные типы инструментов DevSecOps, которые можно обобщить следующим образом:

- **Сканирование уязвимостей в компонентах с открытым исходным кодом:** Они ищут возможные уязвимости в компонентах открытого кода и библиотеках, находящихся в анализируемой кодовой базе, вместе со всеми их зависимостями.
- **Статическое и динамическое тестирование безопасности приложений (SAST/DAST):** Статическое тестирование сканирует исходный код разработчиков на наличие небезопасного кода для выявления потенциальных

проблем безопасности. Динамическое тестирование выполняет тесты безопасности на работающих приложениях, не требуя доступа к исходному коду.

- **Сканирование изображений:** Они ищут уязвимости в контейнерах Docker.
- **Автоматизация инфраструктуры:** Обнаруживают и устраняют различные проблемы конфигурации и уязвимости в конфигурации инфраструктуры, особенно в облачных средах.
- **Визуализация:** Обеспечение видимости KPI и тенденций для обнаружения увеличения или уменьшения количества уязвимостей с течением времени.
- **Моделирование угроз:** Обеспечение возможности принятия проактивных решений путем прогнозирования рисков угроз по всей поверхности атаки.
- **Оповещения:** Уведомление команды безопасности только тогда, когда аномальное событие было идентифицировано и приоритезировано как угроза, чтобы снизить уровень шума и избежать прерывания рабочих процессов DevSecOps.

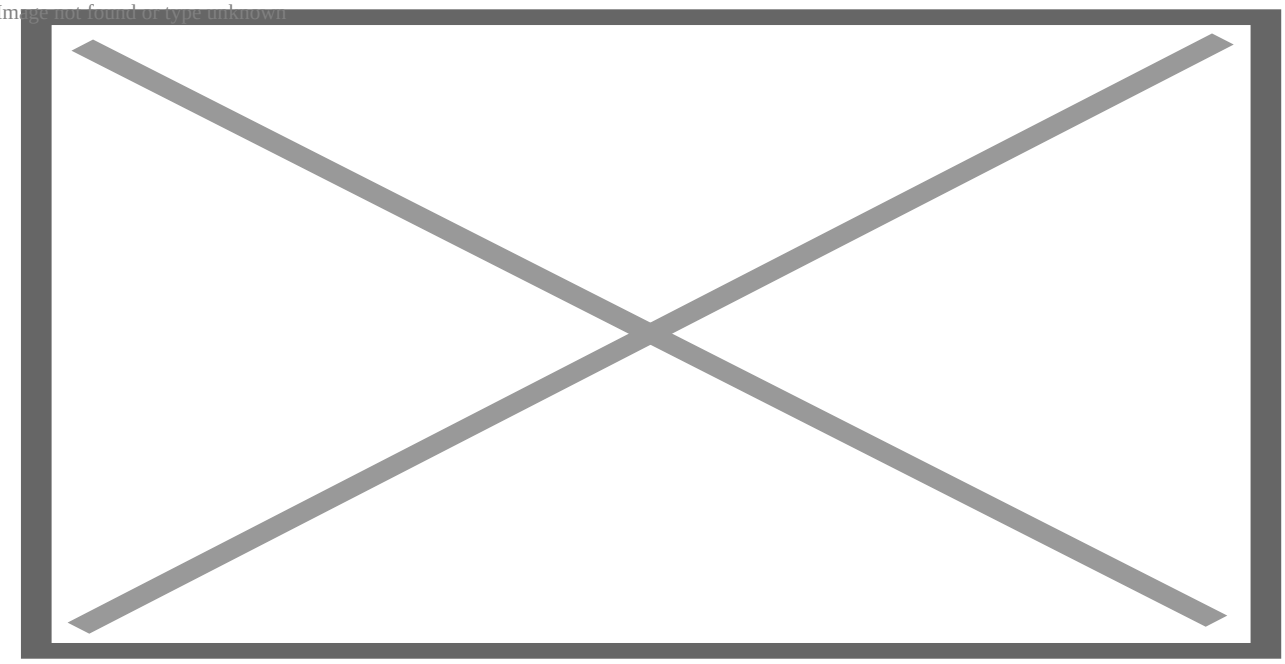
Ниже приведен список инструментов DevSecOps, на которые вы можете положиться, чтобы включить слово “Sec” в ваши рабочие процессы DevOps.

Invicti

Invicti – это инструмент, который вы можете интегрировать в SDLC для управления безопасностью ваших программных продуктов, сохраняя при этом гибкость процесса разработки.

Анализ, проводимый Invicti, является исчерпывающим, обеспечивая точность обнаружения проблем без ущерба для скорости управления SDLC.

Image not found or type unknown



Возможности автоматизации, предлагаемые Invicti, позволяют избежать вмешательства человека в выполнение задач по обеспечению безопасности, что обеспечивает экономию усилий вашей команды, которая может исчисляться сотнями часов в месяц.

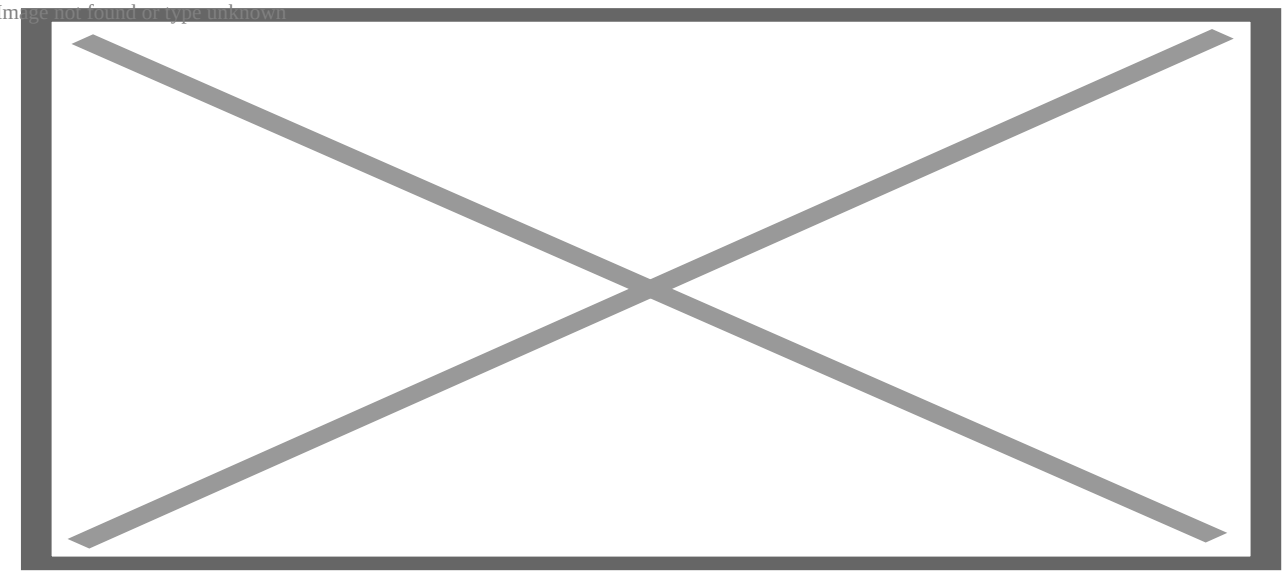
Эта экономия достигается за счет выявления уязвимостей, которые действительно имеют значение, и автоматического назначения их наиболее подходящим ресурсам для устранения.

Invicti также обеспечивает полную видимость уязвимостей в разрабатываемых приложениях и усилий, предпринимаемых для снижения риска.

SonarQube

SonarQube автоматически проверяет ваш код на наличие уязвимостей, выискивая в нем ошибки, которые могут стать угрозой. На момент написания статьи он поддерживает почти 30 различных языков программирования.

Image not found or type unknown



Уникальные QualityGates от SonarQube представляют собой простой способ остановить проблемы до того, как продукт выйдет в свет. Они также предоставляют команде разработчиков совместный взгляд на качество, позволяя всем знать стандарты и то, соответствуют ли им их разработки. SonarQube легко интегрируется в ваш конвейер DevSecOps, обеспечивая всем членам команды доступ к отчетам и отзывам, генерируемым инструментом.

Просто установив его, SonarQube четко показывает, чисты ли ваши коммиты и готовы ли ваши проекты к выпуску. Если что-то не так, инструмент немедленно сообщит вам, в чем проблема и каким может быть решение.

Aqua

Aqua позволяет визуализировать и пресекать угрозы на каждом этапе жизненного цикла ваших программных продуктов, от написания исходного кода до развертывания приложения в облаке. Работающий в качестве платформы защиты облачных приложений (CNAPP), инструмент предлагает проверку безопасности цепочки поставок программного обеспечения, сканирование рисков и уязвимостей, а также расширенную защиту от вредоносных программ.

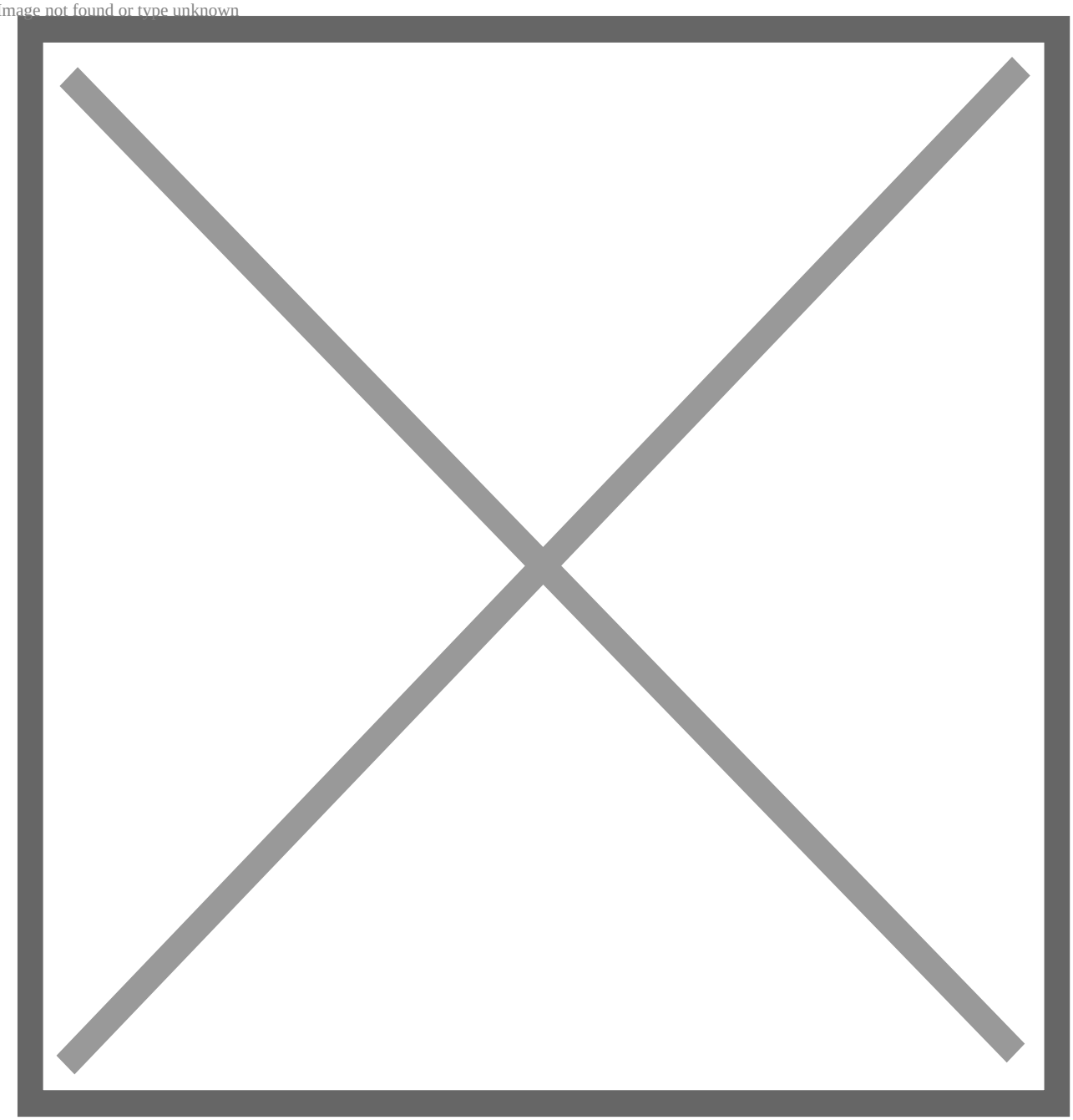
Возможности интеграции Aqua позволяют защищать приложения независимо от платформ и механизмов, используемых для разработки и развертывания, будь то облако, контейнеры, бессерверные системы, конвейеры CI/CD или оркестры. Она также интегрируется с платформами SIEM и аналитическими инструментами.

Отличительной особенностью Aqua является возможность контроля безопасности в контейнерах Kubernetes с помощью KSPM (Kubernetes Security Posture Management) и расширенной защиты во время выполнения Kubernetes. Использование встроенных функций K8s обеспечивает защиту на основе политик на протяжении всего жизненного цикла приложений, развернутых в контейнерах.

ProwlerPro

ProwlerPro – это инструмент с открытым исходным кодом, созданный специально для контроля безопасности в средах разработки Amazon Web Services (AWS).

Image not found or type unknown



ProwlerPro разработан таким образом, что вы можете создать учетную запись и начать выполнять сканирование конвейеров разработки в течение нескольких минут, обеспечивая целостное представление вашей инфраструктуры независимо

от региона, в котором вы находитесь. Его инструменты визуализации позволяют просматривать статус безопасности всех ваших служб AWS в одном окне.

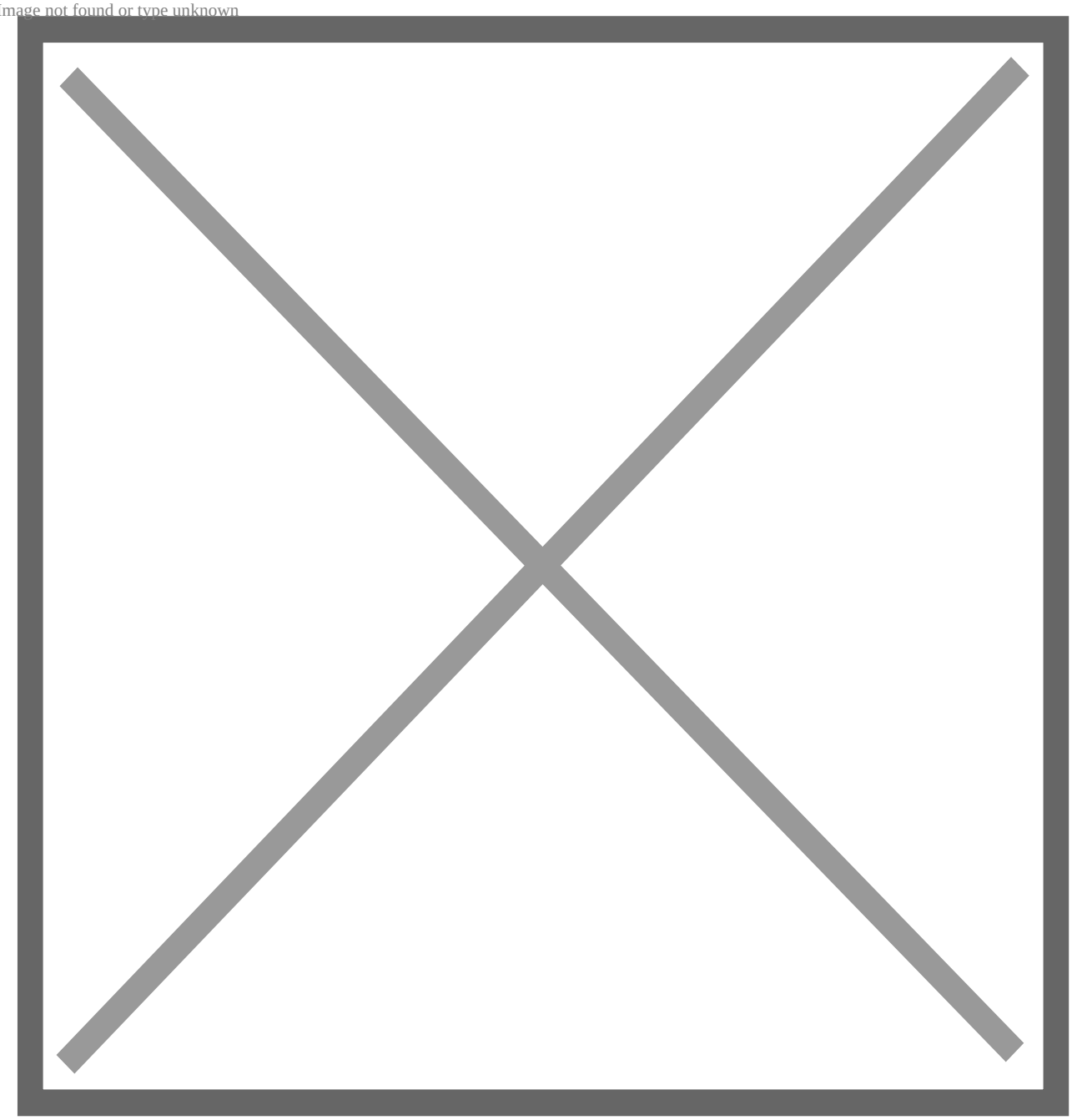
После создания учетной записи ProwlerPro и начала работы вы можете настроить систему на автоматический запуск серии рекомендуемых проверок каждые 24 часа. Сканирование с помощью ProwlerPro выполняется параллельно для повышения скорости, чтобы не замедлять рабочие процессы DevSecOps.

Результаты сканирования отображаются в серии предопределенных информационных панелей, которыми можно легко делиться и перемещаться по ним с помощью сверления для непосредственного изучения любого уровня детализации вашей системы безопасности.

Probely

Если у вас уже есть рабочий процесс DevOps и вы хотите интегрировать в него сканирование безопасности, Probely позволит вам сделать это в считанные минуты благодаря своим инструментам и API для сканирования уязвимостей веб-приложений.

Image not found or type unknown



Подход Probely основан на разработке по принципу API-first, что означает, что каждая новая функция инструмента сначала предлагается через API, а затем добавляется в интерфейс. Благодаря этой стратегии, если вам нужно интегрировать Probely с рабочими процессами или пользовательским программным обеспечением, вы всегда можете воспользоваться его API.

Вы также можете зарегистрировать webhooks, чтобы ваши приложения получали уведомления о каждом событии, которое генерирует Probely.

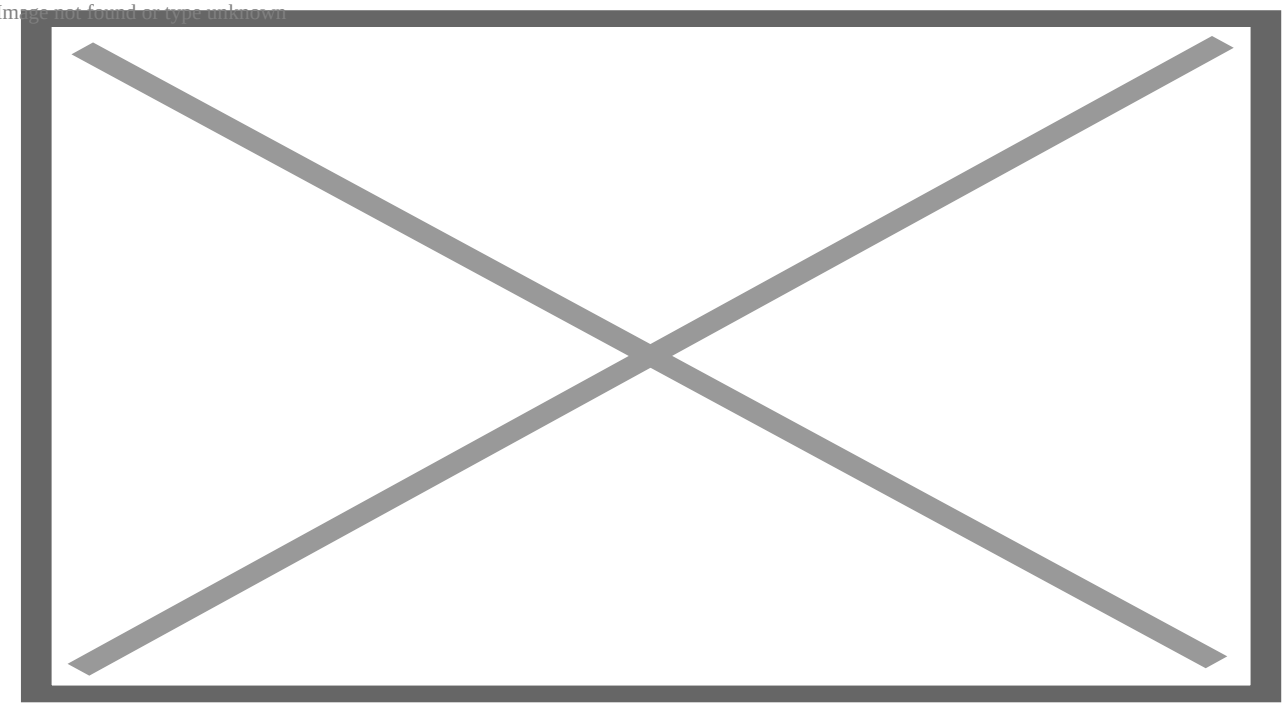
Поскольку Probely предлагает ряд готовых интеграций, есть вероятность, что вам не придется использовать его API для интеграции с вашими инструментами. Если вы уже используете Jira и Jenkins в своих рабочих процессах, интеграция будет мгновенной.

Probely будет автоматически инициировать сканирование в ваших CI/CD конвейерах и регистрировать найденные уязвимости как проблемы в Jira. Как только эти уязвимости будут устранены, он снова протестирует их и при необходимости снова откроет нерешенную проблему в Jira.

Checkov

Checkov сканирует конфигурации в облачных инфраструктурах с целью поиска недостатков конфигурации перед развертыванием программного продукта. Используя общий интерфейс командной строки, он сканирует результаты на различных платформах, таких как Kubernetes, Terraform, Helm, CloudFormation, ARM Templates и бессерверные фреймворки.

Image not found or type unknown



Благодаря схеме политик на основе атрибутов Checkov позволяет сканировать

облачные ресурсы на этапе компиляции, обнаруживая ошибки конфигурации в атрибутах с помощью простого Python-фреймворка policy-as-code. Помимо прочего, Checkov анализирует взаимосвязи между облачными ресурсами с помощью YAML-политик на основе графов.

Благодаря интеграции в конвейеры CI/CD и системы контроля версий Checkov выполняет, тестирует и изменяет параметры запуска в контексте целевого репозитория.

Благодаря расширяемому интерфейсу интеграции его архитектура может быть расширена для определения пользовательских политик, условий подавления и провайдеров. Интерфейс также позволяет интегрироваться с платформами поддержки, процессами сборки и пользовательскими системами выпуска.

Faraday

С помощью Faraday вы можете автоматизировать управление уязвимостями и действия по контролю, чтобы сосредоточить свое внимание на действительно важной работе. Его рабочие процессы позволяют запускать любые действия с помощью пользовательских событий, которые вы можете свободно разрабатывать, чтобы избежать повторения задач.

Faraday дает вам возможность стандартизировать и интегрировать инструменты безопасности в рабочие процессы, получая информацию об уязвимостях от более чем 80 инструментов сканирования. Используя агентов, сканеры автоматически интегрируются в ваши рабочие процессы для получения и нормализации данных с максимальной легкостью, генерируя результаты, которые можно просмотреть через веб-интерфейс.

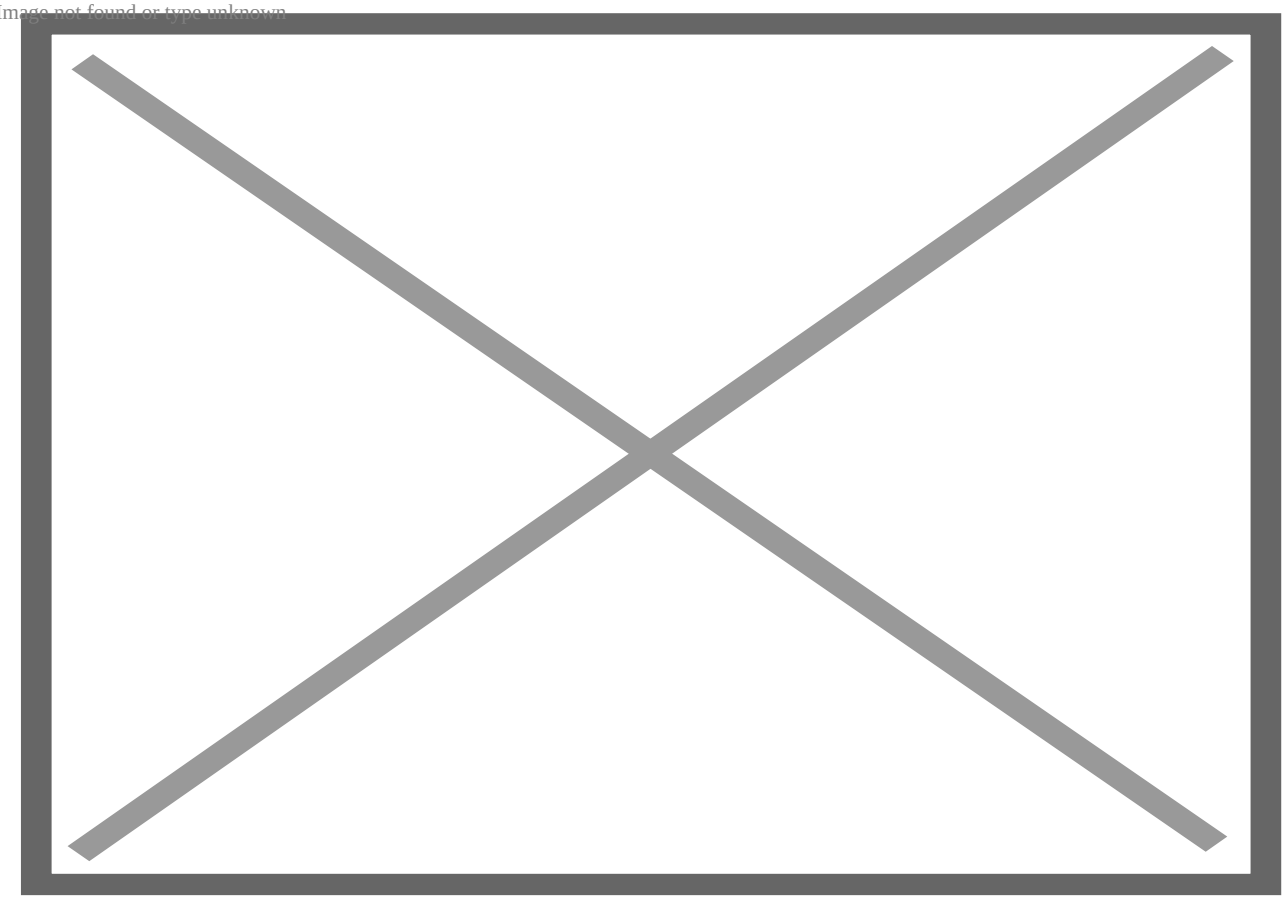
Примечательным и интересным аспектом Faraday является то, что он использует централизованный репозиторий для хранения информации о безопасности, которая может быть легко проанализирована и проверена различными членами команды DevSecOps.

Это дает дополнительное преимущество – возможность выявлять и объединять дубликаты проблем, о которых сообщают различные инструменты. Это снижает усилия членов команды, избавляя их от необходимости несколько раз обращать внимание на одну и ту же проблему, о которой сообщается более одного раза.

CircleCI

Чтобы интегрировать CircleCI с наиболее популярными инструментами безопасности DevOps, необходимо включить в конвейер разработки одного из его многочисленных партнеров. Партнеры CircleCI являются поставщиками решений в нескольких категориях, включая SAST, DAST, статический анализ контейнеров, применение политик, управление секретами и безопасность API.

Image not found or type unknown



Если вам нужно сделать что-то для обеспечения безопасности конвейера разработки, что вы не можете сделать ни с одной из доступных орбов, вы можете воспользоваться тем фактом, что орбы имеют открытый исходный код. По этой причине добавление функциональности в существующую сферу – это просто вопрос получения одобрения вашего PR и его слияния.

Даже если у вас есть сценарий использования, который, по вашему мнению, не входит в набор сфер, доступных в реестре CircleCI, вы можете создать его и внести свой вклад в сообщество. Компания публикует список лучших практик для создания автоматизированных конвейеров компиляции и тестирования орбов, чтобы

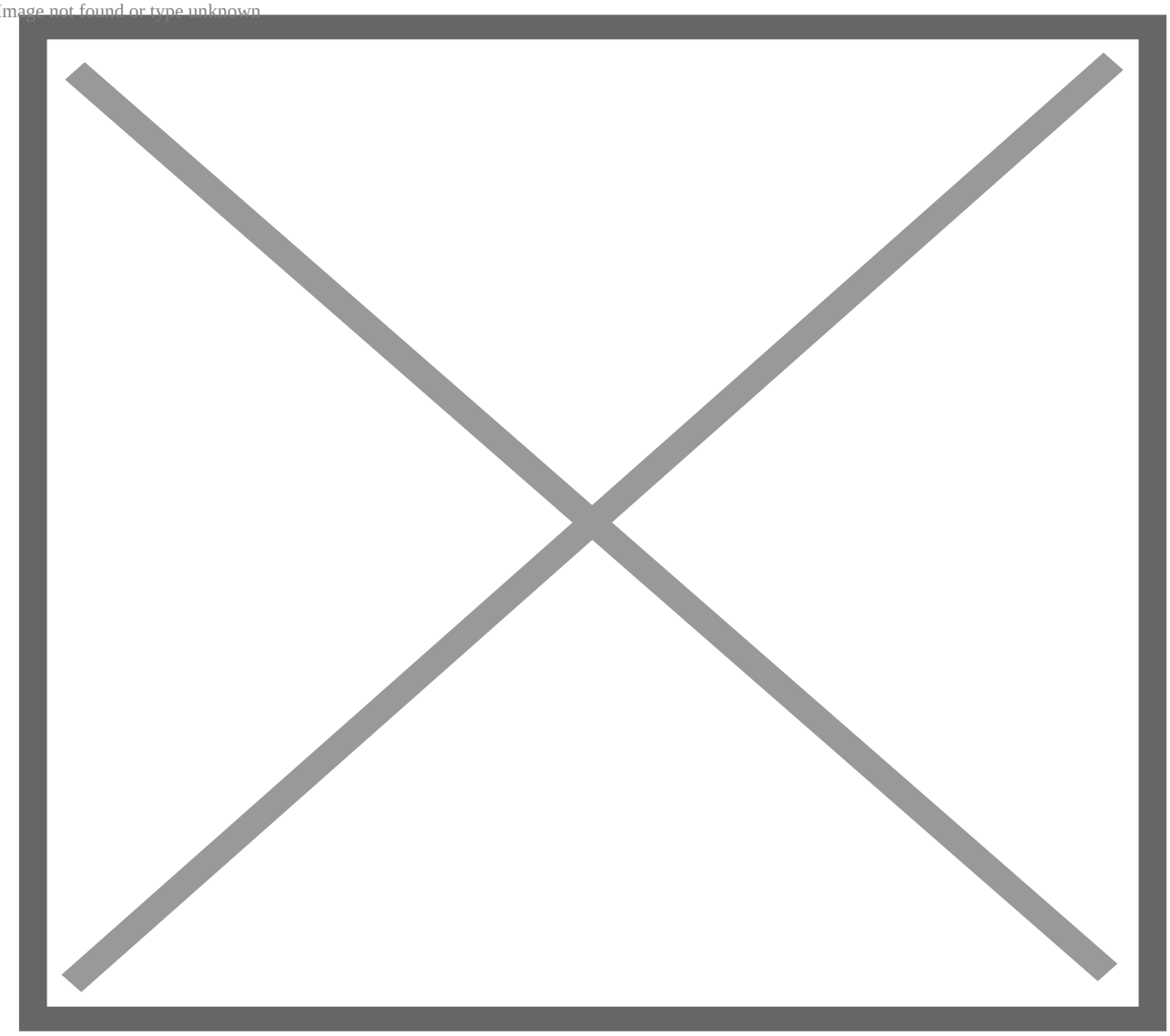
облегчить вам путь.

Чтобы обезопасить свой конвейер, устраните необходимость в собственной разработке и позвольте своей команде использовать услуги сторонних разработчиков. Используя CircleCI orbs, вашей команде нужно будет только знать, как использовать эти сервисы, без необходимости изучать их интеграцию или управление ими.

Trivy

Trivy – это инструмент безопасности с открытым исходным кодом, который имеет несколько сканеров, способных обнаружить проблемы безопасности, и различные цели, на которых он может найти такие проблемы. Среди целей, которые Trivy сканирует: файловая система, образы контейнеров, репозитории Git, образы виртуальных машин, Kubernetes и репозитории AWS.

Image not found or type unknown



Сканируя все эти возможные цели, Trivy может найти известные уязвимости, недостатки конфигурации, секреты или конфиденциальную информацию, а также лицензии на программное обеспечение и обнаружить проблемы в цепочке поставок программного обеспечения, включая зависимости от используемого программного обеспечения и пакетов операционной системы.

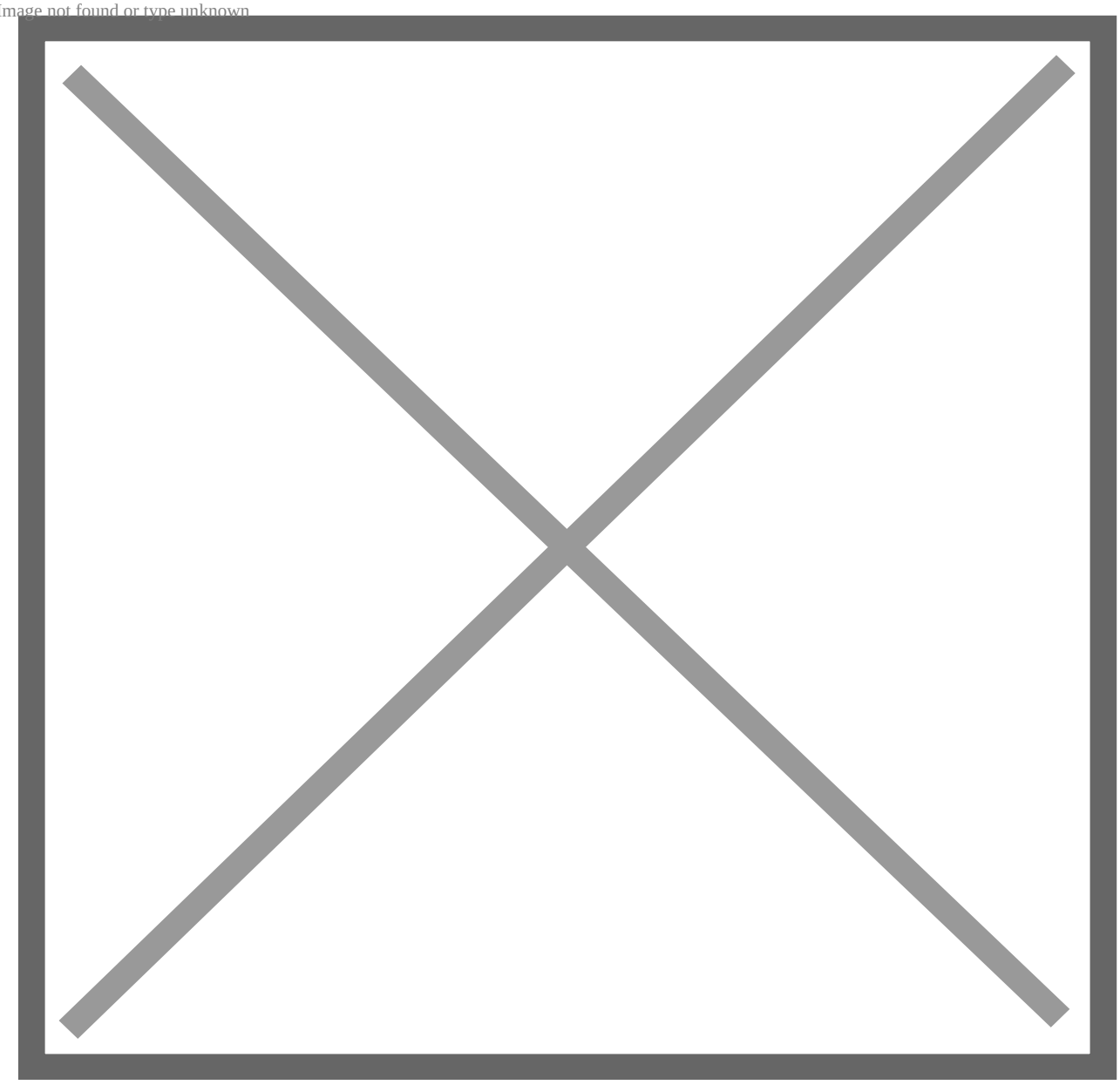
Платформы и приложения, с которыми Trivy может интегрироваться, можно найти на странице Ecosystem. Этот список включает самые популярные названия, такие как CircleCI, GitHub Actions, VS Code, Kubernetes или JetBrains.

Trivy доступен в apt, yum, brew и dockerhub. У него нет предварительных условий, таких как базы данных, среды развертывания или системные библиотеки, а его первое сканирование, по оценкам, завершается всего за 10 секунд.

GitLeaks

Gitleaks – это инструмент с открытым исходным кодом и интерфейсом командной строки, который может быть установлен с помощью Docker, Homebrew или Go. Он также доступен в виде бинарного исполняемого файла для наиболее популярных платформ и операционных систем. Вы также можете установить его непосредственно в свой репозиторий в качестве крючка предварительной коммисии или как общий ресурс GitHub с помощью Gitleaks-Action.

Image not found or type unknown



Его командный интерфейс прост и минималистичен. Он состоит всего из 5 команд для обнаружения секретов в коде, защиты секретов, генерации скриптов, получения справки или отображения версии инструмента. Команда detect позволяет сканировать репозитории, файлы и каталоги. Ее можно использовать как на машинах для разработки, так и в CI-средах.

Большая часть работы с GitLeaks выполняется с помощью команд detect и protect. Они работают с репозиториями Git, анализируя вывод команд git log или git diff и генерируя патчи, которые GitLeaks затем использует для обнаружения и защиты секретов.

Сохранять конкурентоспособность и безопасность

С одной стороны, маневренность и скорость ваших CI/CD конвейеров являются ключом к обеспечению быстрого выхода на рынок, что, в свою очередь, является ключом к сохранению конкурентоспособности разработчика программного обеспечения.

С другой стороны, включение средств обеспечения безопасности в процессы разработки является неоспоримой необходимостью. Чтобы включить средства обеспечения безопасности без негативного влияния на сроки SDLC, вам помогут инструменты DevSecOps.

Дата Создания
28.03.2023