Безопасность на первом месте: Интеграция проверок безопасности на всех этапах CI/CD

Михаил Синельников
Служба информационной безопасности
Отдел защиты ППО

'23 РАЗВИТИЕ СИЛА ХАРАКТЕР БУДУЩЕЕ

Руководитель направления ИБ в РСХБ-Интех

- DevSecOps TeamLead в РСХБ-Интех.
  В IT с 1999 года. Работал в качестве ведущего специалиста и руководителя направлений информационной безопасности в Эр-Телеком, Монета.ру, Ispring
- Занимаюсь контейнерной безопасностью и безопасностью kubernetes, развиваю и поддерживаю платформу ИБ

О чем доклад

- Можно ли платформу ИБ построить бесплатно и в кратчайшие сроки?

О чем доклад

- Можно ли платформу ИБ построить бесплатно и в кратчайшие сроки?
- Можно ли ASOC сделать понятным для бизнеса?

О чем доклад

- Можно ли платформу ИБ построить бесплатно и в кратчайшие сроки?
- Можно ли ASOC сделать понятным для бизнеса?
- Как оптимизировать процессы ИБ, сократив Time-to-Market до минимума?

О чем доклад

- Можно ли платформу ИБ построить бесплатно и в кратчайшие сроки?
- Можно ли ASOC сделать понятным для бизнеса?
- Как оптимизировать процессы ИБ, сократив Time-to-Market до минимума?
- Как оценить жизненный цикл уязвимости и эффективность работы специалистов ИБ?

О чем доклад

- Можно ли платформу ИБ построить бесплатно и в кратчайшие сроки?
- Можно ли ASOC сделать понятным для бизнеса?
- Как оптимизировать процессы ИБ, сократив Time-to-Market до минимума?
- Как оценить жизненный цикл уязвимости и эффективность работы специалистов ИБ?
- Как подготовиться к включению QG так, чтобы ни один из разработчиков не пострадал?

Инструменты до 2022 года

nexus firewall

Checkmarx

APPSECHUB

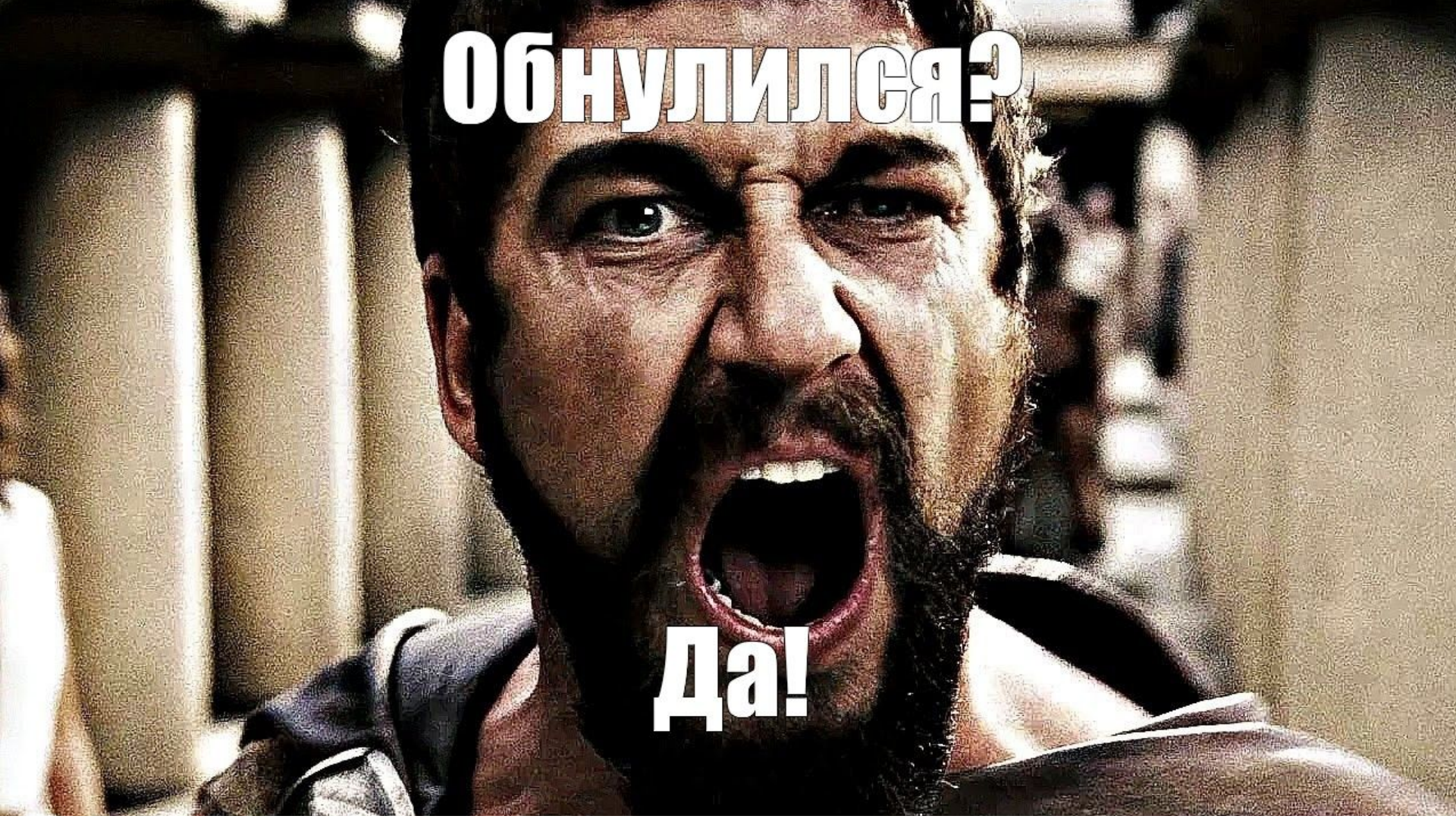
Netsparker by Invicti

CI/CD

Инструменты на май 2022 года

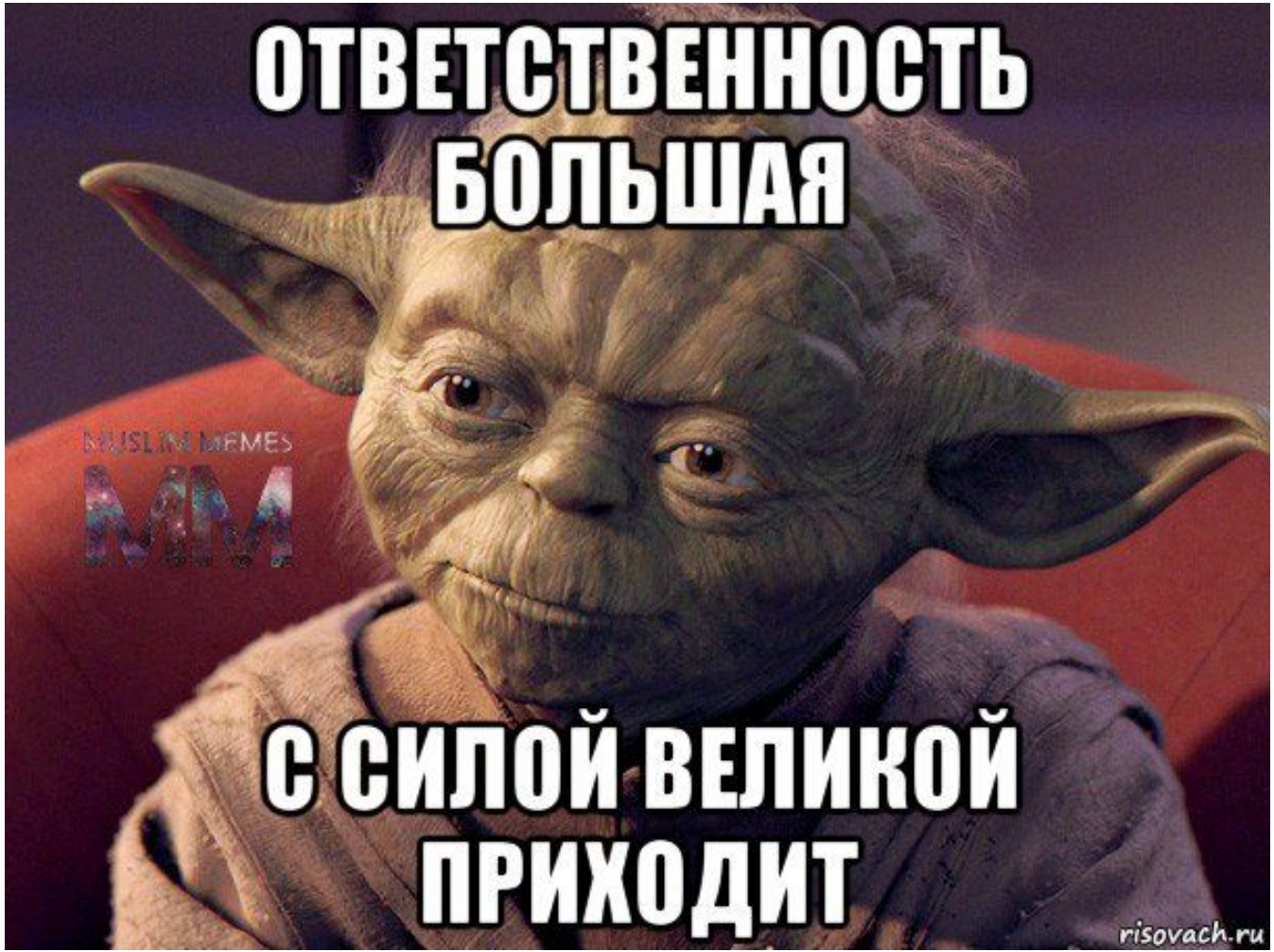
APPSECHUB

CI/CD


Обнулился?
Да!

Техдолг растет?

Да!


ОТВЕТСТВЕННОСТЬ
БОЛЬШАЯ
MUSLIM MEMES
MM
С СИЛОЙ ВЕЛИКОЙ
ПРИХОДИТ
risovach.ru

Проблематика. Почему мы это делаем?

- Резервирование ИБ
- Прозрачность
- Гибкость и настраиваемость
- Экономия
- Быстрое обновление

Что выбрать из ASOC?

APPSECHUB

Nessus
vulnerability scanner

DEFECT DOJO

tenable
Security Center

WIZ

SentinelOne™

Локальная установка

APPSECHUB

Nessus vulnerability scanner

DEFECT DOJO

tenable Security Center

WIZ

SentinelOne™

Локальная установка + “закрытый контур”

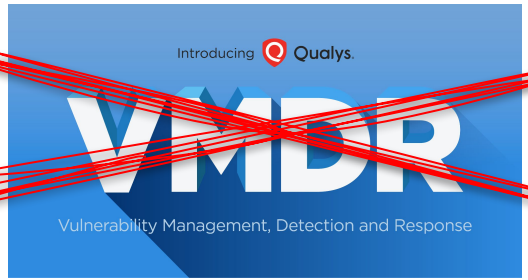
APPSECHUB

Nessus vulnerability scanner

DEFECT DOJO

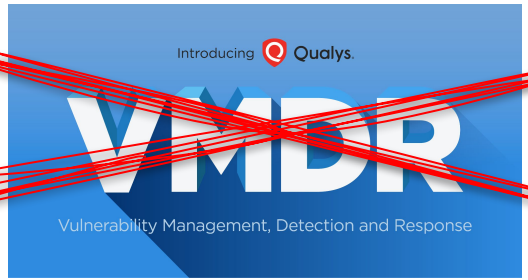
tenable Security Center

WIZ



SentinelOne™

Локальная установка + “закрытый контур” + SARIF + Opensource



System	Open Source	Self-hosted	On-premise	SARIF support
DefectDojo				
Tenable Nessus				
Wiz Security				
Tenable Security Center				
SentinelOne Singularity				
Qualys VMDR				
AppSecHub				

Наш стек


GO


Java


JavaScript
JS


TS


Kotlin


python

Dart


{json}


Swift


BASH
&
Shell Scripts


XML


HTML


YAML


Ruby


C#

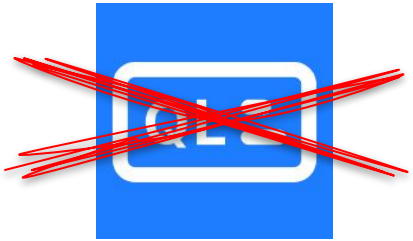
Что выбрать из SAST?

Бесплатный + Opensource

Flawfinder
Finds vulnerabilities in C/C++ source code

Бесплатный + Opensource + стек

Бесплатный + Opensource + стек + быстрый



Инструмент	Скорость сканирования	Поддерживаемые языки	Платный/бесплатный	Open Source
SonarQube	Средняя	20+	Бесплатный и платный	
CodeQL	Средняя	35+		
Flawfinder	Быстрая	C/C++		
Bandit	Быстрая	Python		
SpotBugs	Средняя	Java		
Brakeman	Средняя	Ruby		
Semgrep	Быстрая	40+		
Horusec	Быстрая	40+	Бесплатный и платный	

Что выбрать из SCA/OSA?

DEPENDENCY-CHECK

nexus
IQ server

snyk

dependency track

Стек

DEPENDENCY-CHECK

nexus
IQ server

snyk

dependency track

Стек + бесплатный + Opensource + быстрый

DEPENDENCY-CHECK

nexus
IQ server

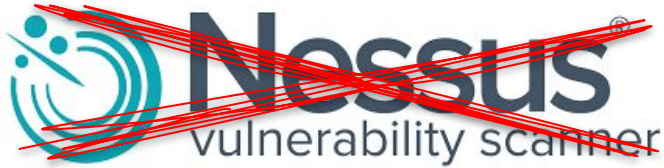
snyk

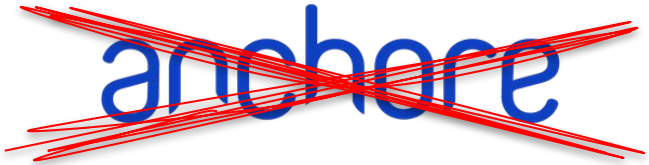
dependency track

Инструмент	Скорость сканирования	Поддерживаемые языки	Платный/ бесплатный	Open Source
OWASP Dependency-Check		Множество		
Snyk		Множество		
Sonatype Nexus IQ Server		Множество		
Retire.js		JavaScript		
Dependency-Track		Множество		

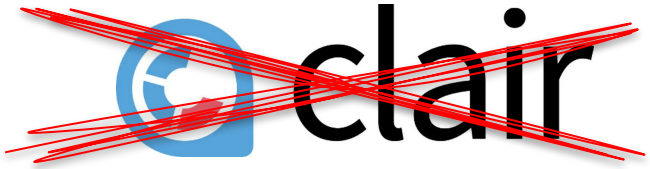
Что выбрать из BCA?

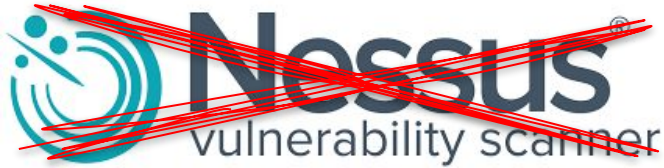
Бесплатный + opensource

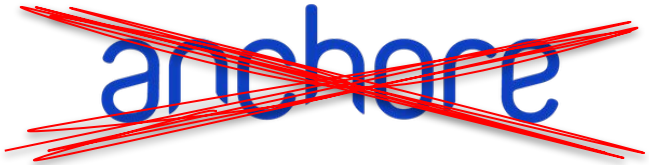




Бесплатный + opensource + стек + быстрый





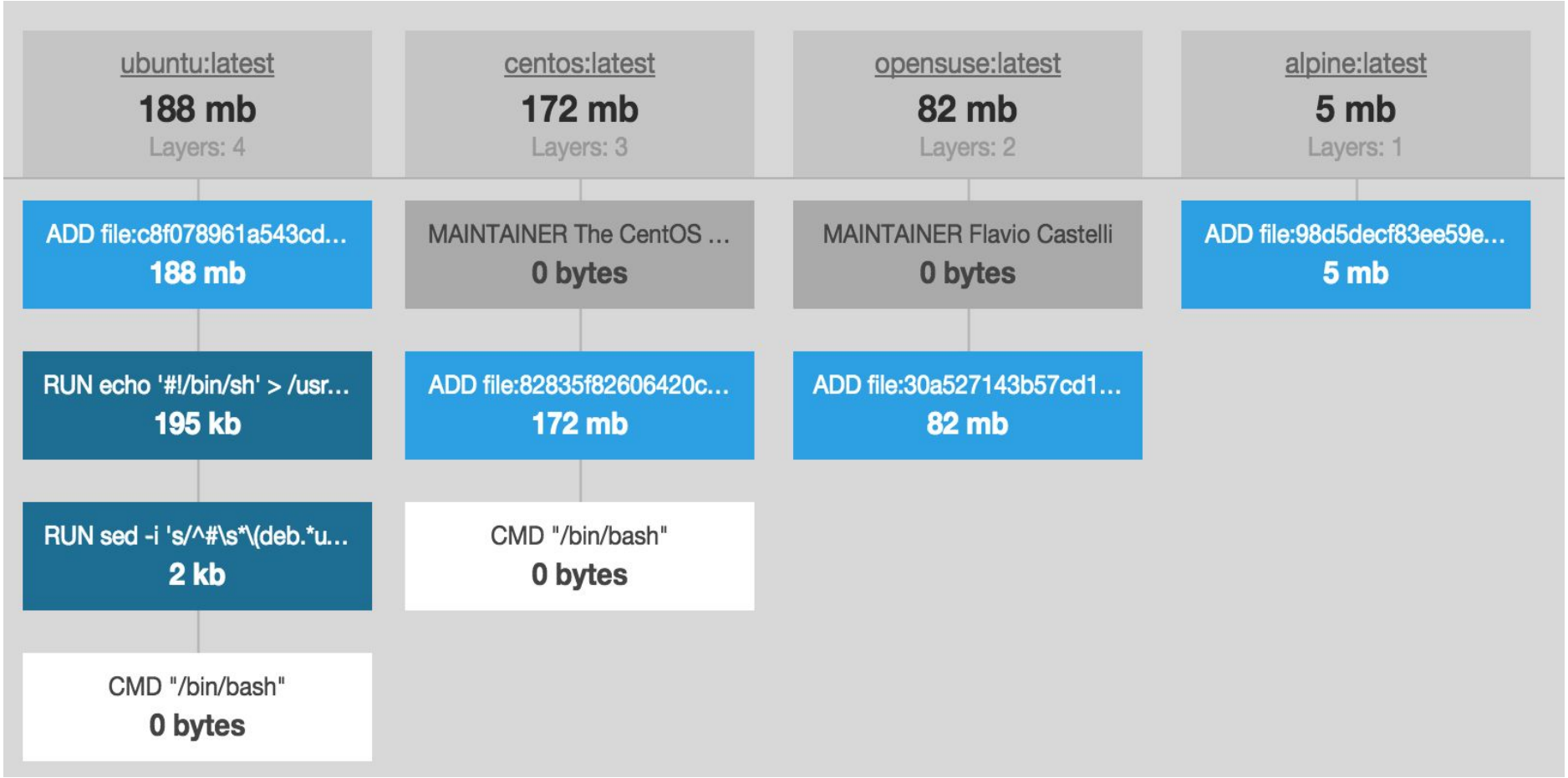


Инструмент	Скорость сканирования	Количество языков	Платный/ бесплатный	Open source
Clair				
Anchore				
Nessus				
Aqua Security				
Trivy				

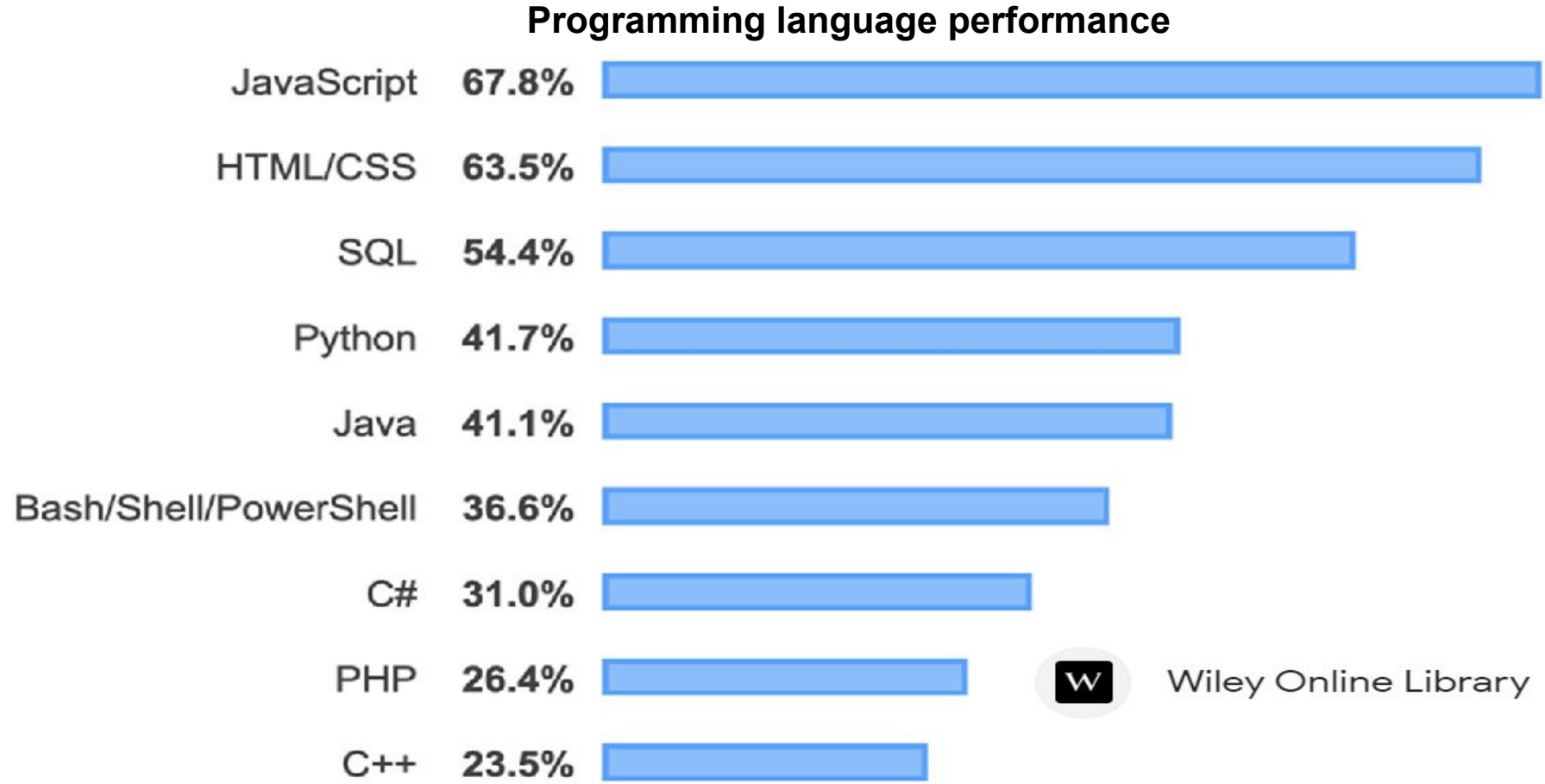
Защита ASOC

- Аутентификация и авторизация
- Защита flow от отключения проверок ИБ
- Шифрование данных, защита от CSRF-атак, валидация входных данных
- Ограничение запросов
- Мониторинг и журналирование
- Обновление и патчи
- Сегментация сети
- Безопасность хранилища, бэкапы
- Аудит

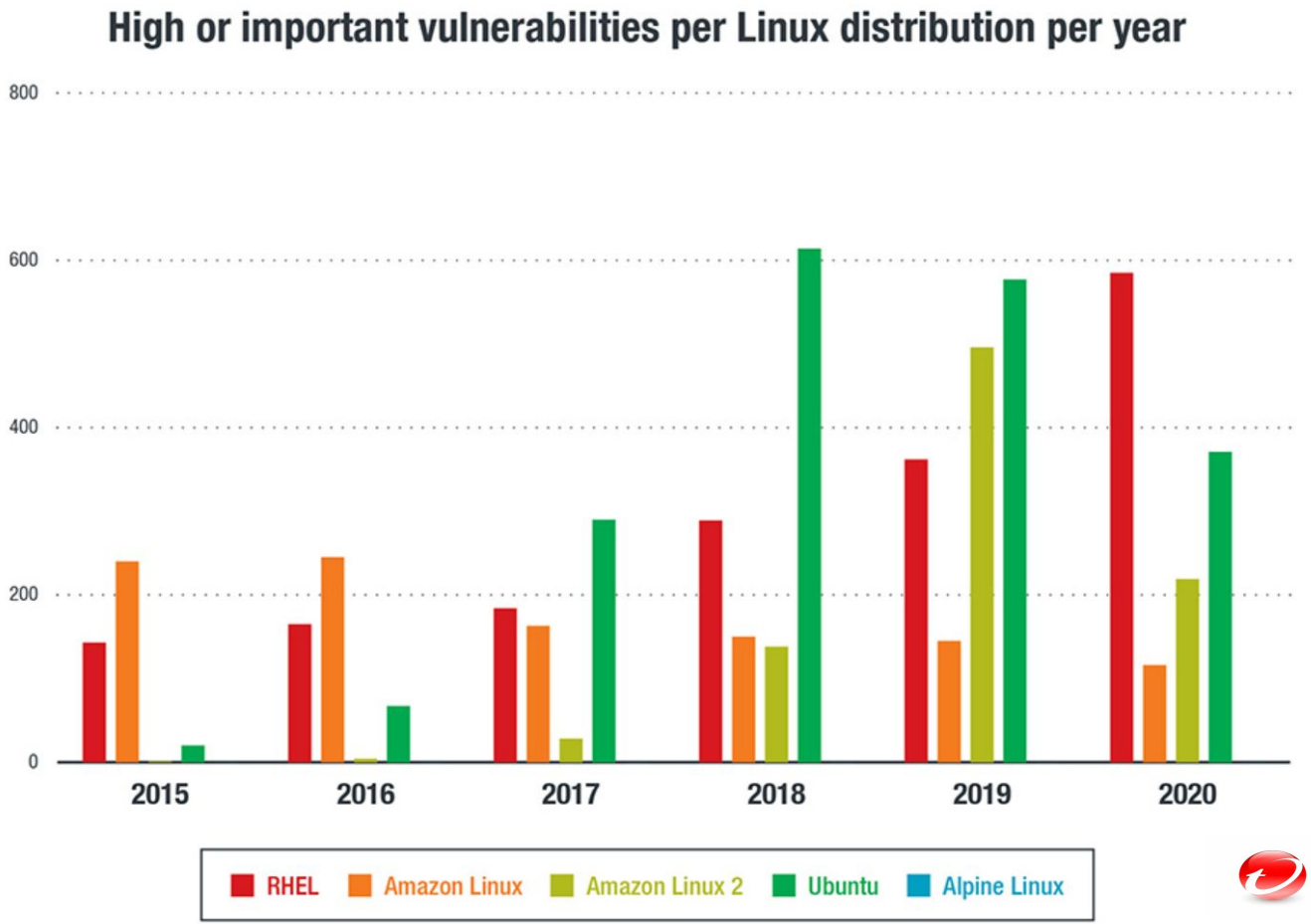
Выбор OS для сканеров уязвимостей



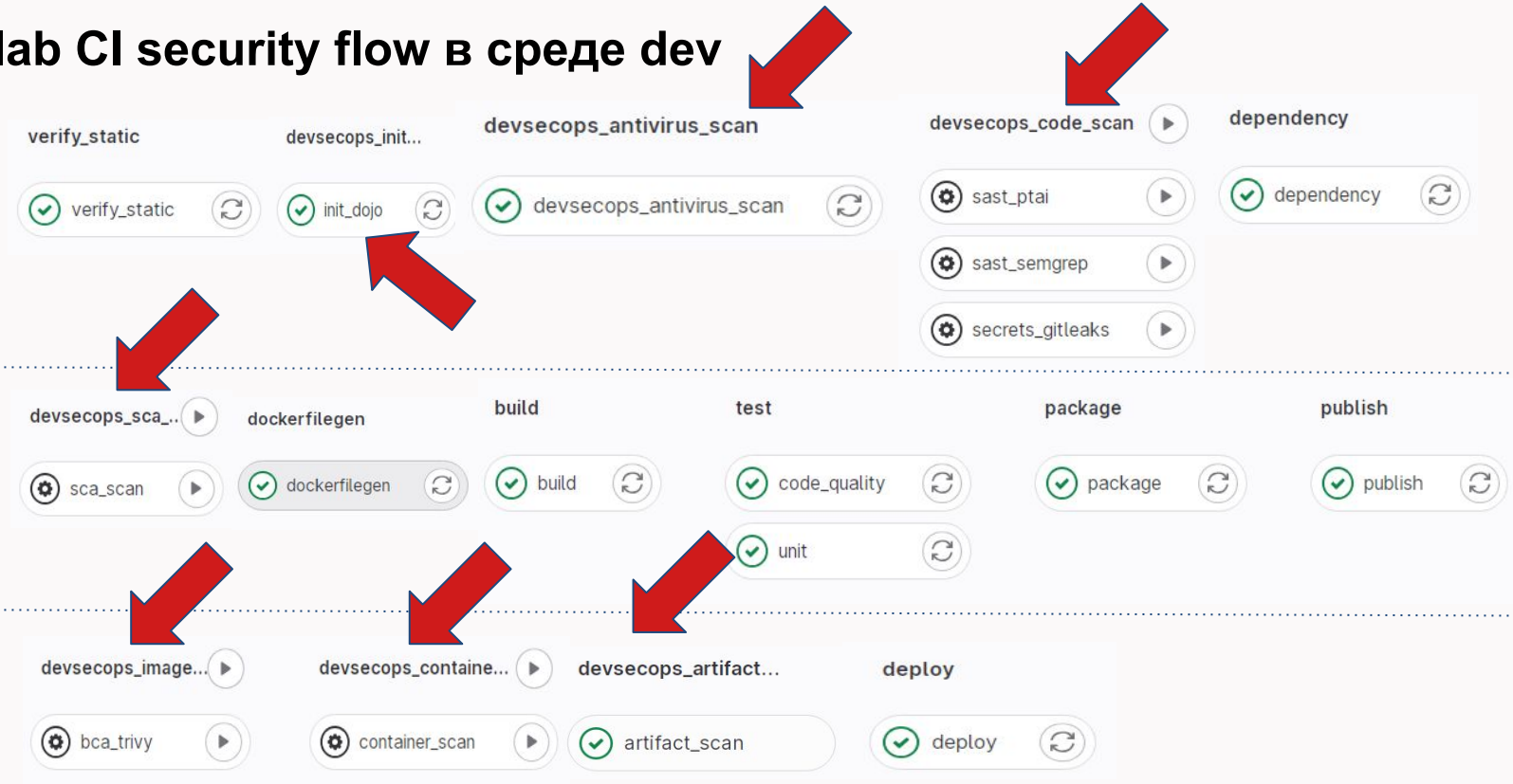
Выбор OS для сканеров уязвимостей



Выбор OS для сканеров уязвимостей



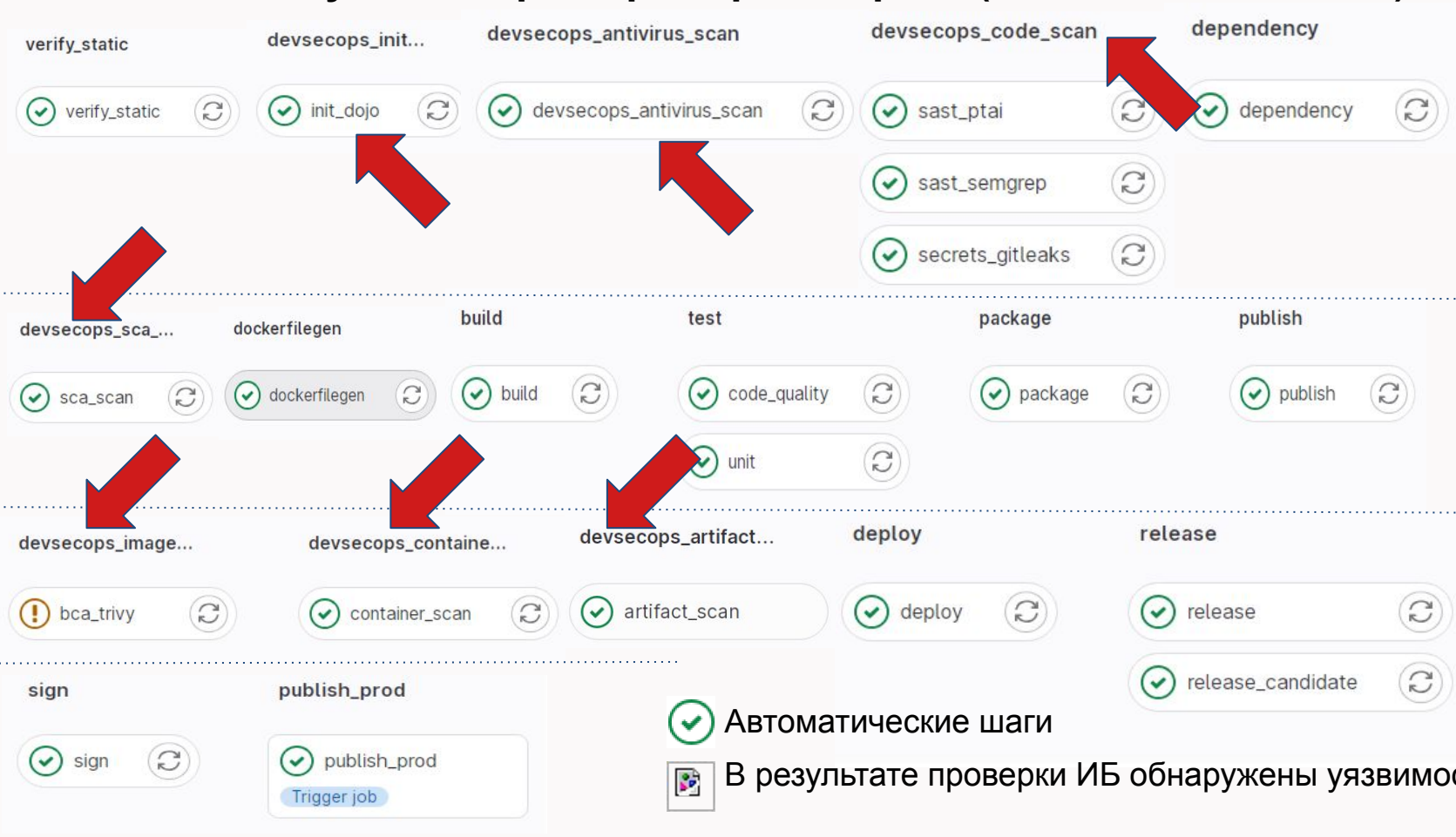
Gitlab CI security flow в среде dev



Автоматические шаги

Проверки запускаемые вручную

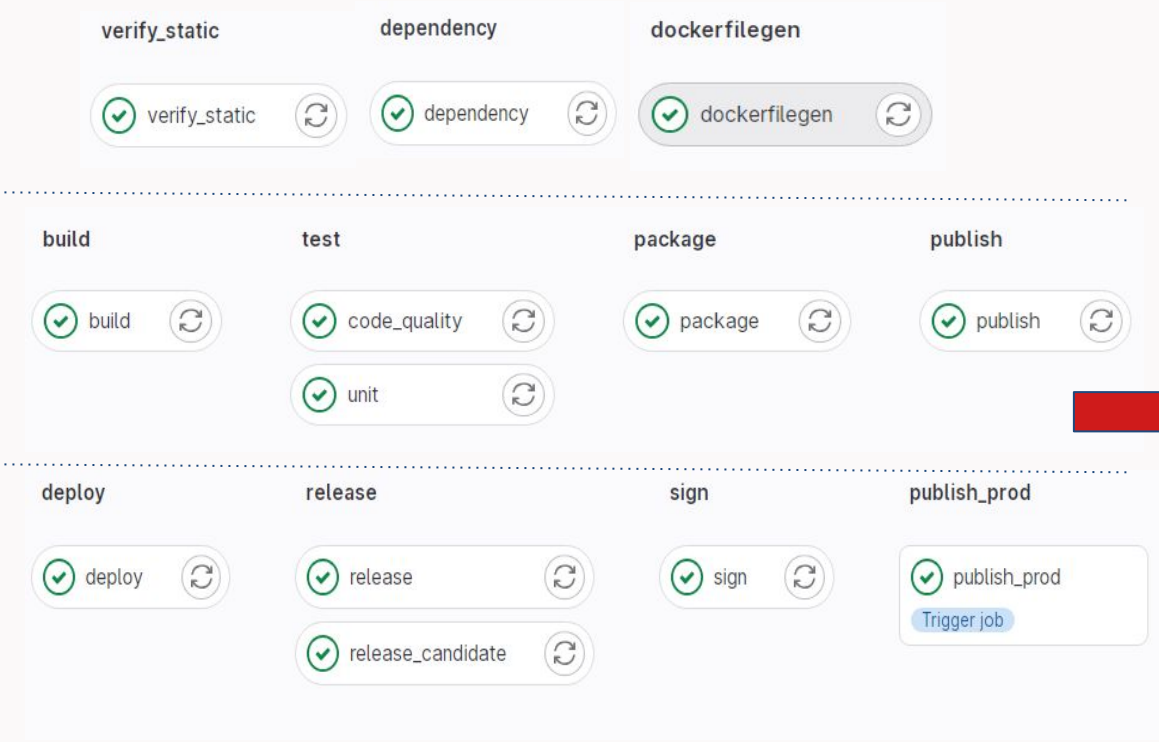
Gitlab CI security flow в среде pred-prod и prod (последовательные)

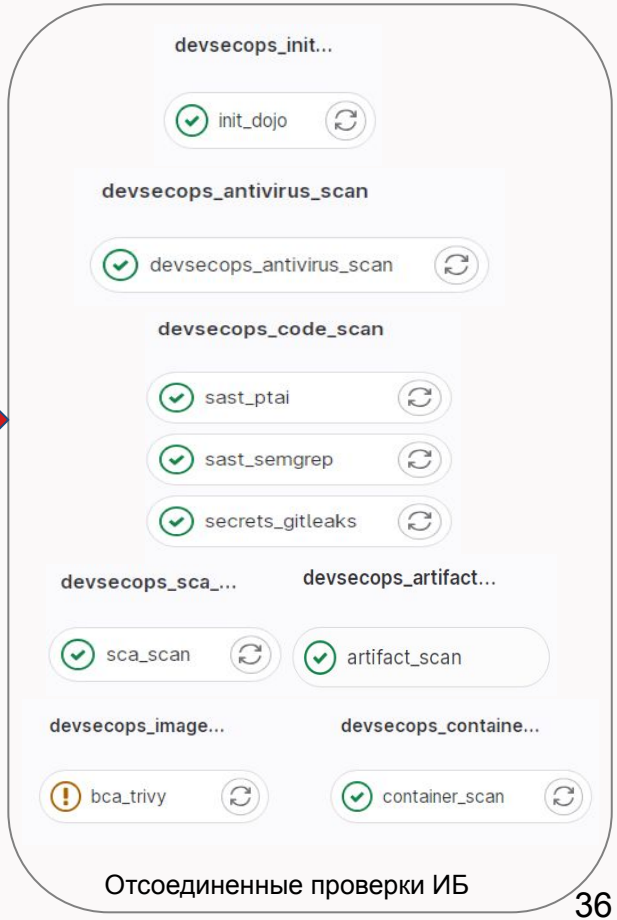


Автоматические шаги

В результате проверки ИБ обнаружены уязвимости

Gitlab CI security flow в среде pred-prod и prod (пареллельно-открепленные)





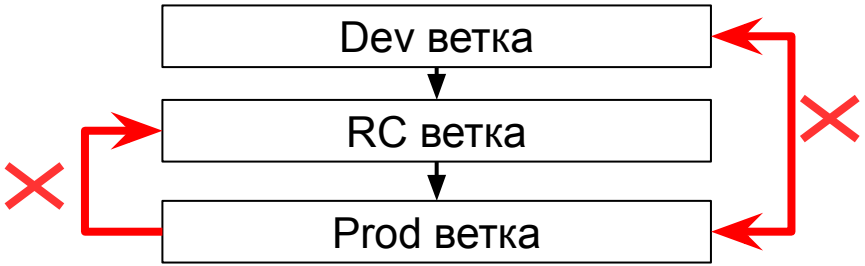
Автоматические шаги

В результате проверки ИБ обнаружены уязвимости

Особенности построения gitlab CI flow для проверок ИБ

- Принцип Shift-Left.
- Фоновые проверки ИБ
- Дедупликация
- Отчеты для разработчиков в среде разработки
- Код не покидает контура
- Единый пайплайн для всего
- Формат результатов сканирований понятнен разработчику и специалисту ИБ

Устранение дубликатов обнаруженных уязвимостей



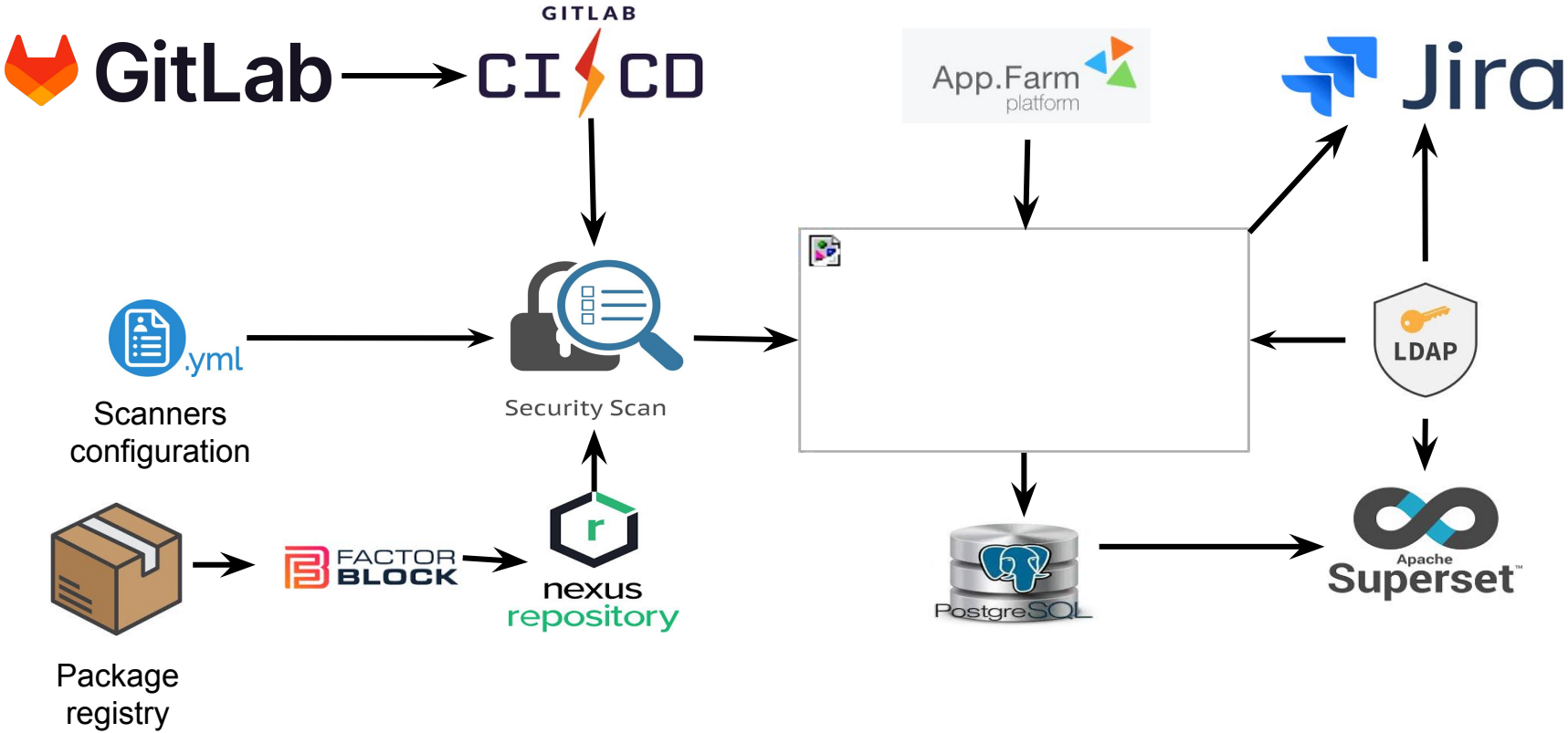
$Vuln_{total}=Vuln_{dev}+Vuln_{rc}+Vuln_{prod}$

$Vuln_{total}=Vuln_{rc}+Vuln_{prod}$

$Vuln_{total}=Vuln_{prod}$

Antivirus	Secrets	OSA	SAST	BCA	SCA	DAST
Нет дублей	Нет дублей	Нет дублей	Выкл. secrets	Выкл. lang-pkgs	Дедупликация SCA	Нет дублей

Схема платформы ИБ



Темплейт задачи в Jira на устранение дефекта

Детали задачи:

Статус: Готово

Приоритет: Высокий

Компоненты: SECOPS

Метки: #secopsops #defectdojo #CVE-2023-0401 #alpine #os-pkgs #Справочники(ID_17173)

Темплейт задачи в Jira на устранение дефекта

Детали задачи:

Статус: Готово

Приоритет: Высокий

Компоненты: SECOPS

Метки: #secopsops #defectdojo #CVE-2023-0401 #alpine #os-pkgs

#Справочники(ID_17173)

Темплейт задачи в Jira на устранение дефекта

Детали задачи:

Статус: Готово

Приоритет: Высокий

Компоненты: SECOPS

Метки: #secopsops #defectdojo #CVE-2023-0401 #alpine #os-pkgs

#Справочники(ID_17173)

Темплейт задачи в Jira на устранение дефекта

Детали задачи:

Статус: Готово

Приоритет: Высокий

Компоненты: SECOPS

Метки: #secopsops #defectdojo #CVE-2023-0401 #alpine #os-pkgs #Справочники(ID_17173)

Темплейт задачи в Jira на устранение дефекта

Описание:

Information system: IPS

Technical Contact: Михаил Синельников

Title: CVE-2023-0401 Libssl3 3.0.7-r0

GitLab link: https://gitlab.xxx.ru/rshbintech/it-invest/ckips/ips/frm/dictionary

Defect Dojo link: https://defect-dojo.xxx.ru/finding/488783

Severity: High

Due Date: Dec. 23, 2022

CWE: CWE-476

CVE: CVE-2023-0401

CVSSv3 Score: 7.5

Темплейт задачи в Jira на устранение дефекта

Описание:

Information system: IPS

Technical Contact: Михаил Синельников

Title: CVE-2023-0401 Libssl3 3.0.7-r0

GitLab link: https://gitlab.xxx.ru/rshbintech/it-invest/ckips/ips/frm/dictionary

Defect Dojo link: https://defect-dojo.xxx.ru/finding/488783

Severity: High

Due Date: Dec. 23, 2022

CWE: CWE-476

CVE: CVE-2023-0401

CVSSv3 Score: 7.5

Темплейт задачи в Jira на устранение дефекта

Описание:

Information system: IPS

Technical Contact: Михаил Синельников

Title: CVE-2023-0401 Libssl3 3.0.7-r0

GitLab link: https://gitlab.xxx.ru/rshbintech/it-invest/ckips/ips/frm/dictionary

Defect Dojo link: https://defect-dojo.xxx.ru/finding/488783

Severity: High

Due Date: Dec. 23, 2022

CWE: CWE-476

CVE: CVE-2023-0401

CVSSv3 Score: 7.5

Темплейт задачи в Jira на устранение дефекта

Описание:

Information system: IPS

Technical Contact: Михаил Синельников

Title: CVE-2023-0401 Libssl3 3.0.7-r0

GitLab link: https://gitlab.xxx.ru/rshbintech/it-invest/ckips/ips/frm/dictionary

Defect Dojo link: https://defect-dojo.xxx.ru/finding/488783

Severity: High

Due Date: Dec. 23, 2022

CWE: CWE-476

CVE: CVE-2023-0401

CVSSv3 Score: 7.5

Темплейт задачи в Jira на устранение дефекта

Описание:

Information system: IPS

Technical Contact: Михаил Синельников

Title: CVE-2023-0401 Libssl3 3.0.7-r0

GitLab link: https://gitlab.xxx.ru/rshbintech/it-invest/ckips/ips/frm/dictionary

Defect Dojo link: https://defect-dojo.xxx.ru/finding/488783

Severity: High

Due Date: Dec. 23, 2022

CWE: CWE-476

CVE: CVE-2023-0401

CVSSv3 Score: 7.5

Темплейт задачи в Jira на устранение дефекта

Описание:

Product/Engagement/Test: Справочники (ID 17173) / Олег Проскоряков <p@xx.ru> (ID 435124) / Trivy Scan

BuildID: 435124

Commit hash: 6baf3d7e

Vulnerable Component: libssl3 - 3.0.7-r0

Description:

openssl: NULL dereference during PKCS7 data verification

Target: registry.xxx.ru/rshbintech/frm/dictionary:1.0.0-RC1 (alpine 3.17.0)

Type: alpine

Fixed version: 3.0.8-r0

Темплейт задачи в Jira на устранение дефекта

Описание:

Product/Engagement/Test: Справочники (ID 17173) / Олег Проскоряков <p@xx.ru> (ID 435124) / Trivy Scan

BuildID: 435124

Commit hash: 6baf3d7e

Vulnerable Component: libssl3 - 3.0.7-r0

Description:

openssl: NULL dereference during PKCS7 data verification

Target: registry.xxx.ru/rshbintech/frm/dictionary:1.0.0-RC1 (alpine 3.17.0)

Type: alpine

Fixed version: 3.0.8-r0

Темплейт задачи в Jira на устранение дефекта

Описание:

Product/Engagement/Test: Справочники (ID 17173) / Олег Проскоряков <p@xx.ru> (ID 435124) / Trivy Scan

BuildID: 435124

Commit hash: 6baf3d7e

Vulnerable Component: libssl3 - 3.0.7-r0

Description:

openssl: NULL dereference during PKCS7 data verification

Target: registry.xxx.ru/rshbintech/frm/dictionary:1.0.0-RC1 (alpine 3.17.0)

Type: alpine

Fixed version: 3.0.8-r0

Темплейт задачи в Jira на устранение дефекта

Описание:

Mitigation:

Done

References:

https://access.redhat.com/errata/RHSA-2023:0946

https://access.redhat.com/security/cve/CVE-2023-0217

Эффективность платформы ИБ

50

750

Large stack

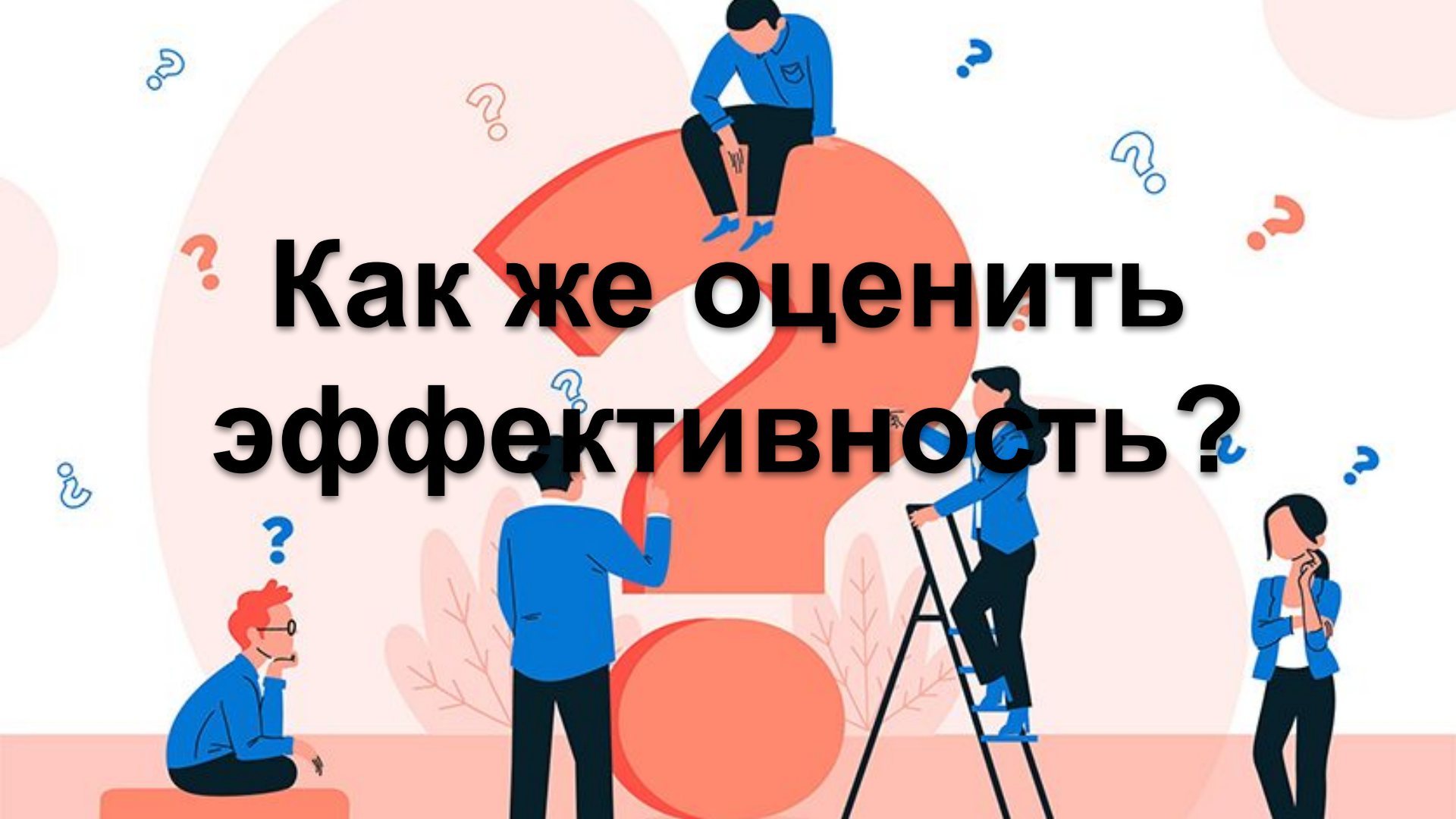
Dev, pred-prod, prod

~300 MR / day

CRITICAL+HIGH ~ 70 in day

70% duplicates

5 AppSec + 2 SecOps


Как же оценить эффективность?

Аналитика по обнаружению/устранению уязвимостей

Аналитика по уязвимостям в информационных системах

Статистика по уязвимостям в ИС

Search 7 records...

Наименование ИС	Найденных	Critical	High	Открытых	Закрытых	Дубликатов	Открытых (%)	Закрытых (%)
АУСН	59,967	943	12,390	43	4,721	57,817	0.9%	99.1%
Скрининг ПС	31,018	429	978	113	2,903	28,945	3.7%	96.3%
Кибербразведка	28,000	395	4,610	115	4,560	24,501	2.5%	97.5%
МЗ ККР ФЛ	20,463	111	277	325	13,931	7,146	2.3%	97.7%
Виртуальный помощник	16,853	76	3,147	85	4,312	14,139	1.9%	98.1%
RTF	14,467	109	323	28	2,357	12,420	1.2%	98.8%
Система управления контентом Wildless-CMS	376	32	232	9	299	325	2.9%	97.1%
Totals	**171,144**	**2,095**	**21,957**	**718**	**33,083**	**145,293**	**2.1%**	**97.9%**

Аналитика по уязвимостям в микросервисах

Статистика по уязвимостям в микросервисах

Show 10 entries

Search 820 records...

Наименование микросервиса	Найденных	Critical	High	Открытых	Закрытых	Дубликатов	Открытых(%)	Закрытых(%)
Базовые образа	151,955	18,739	133,216	0	1,713	150,242	0.0%	100.0%
Сервис Retail Admin Ui App (ID 1531)	889	76	183	1	760	685	0.1%	99.9%
Сервис нечеткого поиска - fuzzy (ID 1553)	6,135	71	52	3	935	5,777	0.3%	99.7%
ККРФЛ М3 ltg (ID 22667)	14,027	36	70	40	12,394	2,043	0.3%	99.7%
Сервис управления котировками (ID 15923)	1,638	14	31	1	308	1,423	0.3%	99.7%
Центр поддержки (ID 4771)	3,260	51	625	1	280	3,095	0.4%	99.6%
Сервис Веб Бот (ID 4393)	3,477	15	532	3	831	3,070	0.4%	99.6%
Сервис загрузки данных (ID 12927)	1,323	10	30	1	219	1,103	0.5%	99.5%
Тестовый внутренний kotlin сервис 23092225393028 (ID 28506)	206	9	18	1	205	0	0.5%	99.5%
Сборщик событий (ID 16820)	2,521	37	311	4	801	2,176	0.5%	99.5%

Аналитика по практикам и критичности уязвимостей

Аналитика по работе специалистов ИБ

Закрепление ИС за работниками СИБ

			metric	Микросервисов	Открытых	Закрытых	Найденных
⊟ Специалист DevSecOps	⊟ Наименование ИС	Наименование микросервиса					
⊟ kuznetsova	**Subtotal**			**6**	**26**	**433**	**890**
	⊟ SSO	**Subtotal**		**3**	**17**	**242**	**464**
		Интеграционный сервис (ID 12952)		1	1	37	112
		Отправитель сообщений (ID 7649)		1	13	161	193
		Сервис интеграции Keycloak с системой АСУП (ID 22743)		1	3	44	159
	⊟ qa-invest	**Subtotal**		**3**	**9**	**191**	**426**
		Terra (ID 14097)		1	7	83	235
		Выгрузка тест-планов TestIT + Jira (ID 13575)		1	1	56	126
		Тестовый клиент сервиса mdm (ID 16036)		1	1	52	65
			Total (Sum)	**6**	**26**	**433**	**890**

Выводы и рекомендации

Выводы и рекомендации

- Выбор инструментов безопасности — ответственный момент. От него зависит эффективность и качество защиты систем от угроз и уязвимостей

Выводы и рекомендации

- Выбор инструментов безопасности — ответственный момент. От него зависит эффективность и качество защиты систем от угроз и уязвимостей

- Оптимизация процессов безопасности — ключевой фактор для повышения эффективности и эффективной защиты систем

Выводы и рекомендации

- Выбор инструментов безопасности — ответственный момент. От него зависит эффективность и качество защиты систем от угроз и уязвимостей
- Оптимизация процессов безопасности — ключевой фактор для повышения эффективности и эффективной защиты систем
- Грамотно построенный пайплайн ускоряет процесс проверки

Выводы и рекомендации

- Выбор инструментов безопасности — ответственный момент. От него зависит эффективность и качество защиты систем от угроз и уязвимостей
- Оптимизация процессов безопасности — ключевой фактор для повышения эффективности и эффективной защиты систем
- Грамотно построенный пайплайн ускоряет процесс проверки
- Недостаточно просто создать систему — ее нужно правильно защищать

Выводы и рекомендации

- Выбор инструментов безопасности — ответственный момент. От него зависит эффективность и качество защиты систем от угроз и уязвимостей
- Оптимизация процессов безопасности — ключевой фактор для повышения эффективности и эффективной защиты систем
- Грамотно построенный пайплайн ускоряет процесс проверки
- Недостаточно просто создать систему — ее нужно правильно защищать
- Хорошая система ИБ — это информативная и понятная система для бизнеса, разработчиков и специалистов ИБ

Выводы и рекомендации

- Выбор инструментов безопасности — ответственный момент. От него зависит эффективность и качество защиты систем от угроз и уязвимостей
- Оптимизация процессов безопасности — ключевой фактор для повышения эффективности и эффективной защиты систем
- Грамотно построенный пайплайн ускоряет процесс проверки
- Недостаточно просто создать систему — ее нужно правильно защищать
- Хорошая система ИБ — это информативная и понятная система для бизнеса, разработчиков и специалистов ИБ
- Правильно построенная система ИБ может быть запущена в кратчайшие сроки и обслуживаться небольшой командой инженеров

Спасибо!

/23 РАЗВИТИЕ
СИЛА
ХАРАКТЕР
БУДУЩЕЕ