SafeCode 2024

Секреты в безопасности

Предотвращение утечек и компрометации в большой компании

Ольга Рачич

kaspersky

План доклада

- Предпосылки (зачем нужно защищать секреты)
- Почему нам понадобилось централизованное решение для контроля за секретами
- Концепт нашей системы для поиска секретов
- Проблемы, с которыми мы столкнулись и как их решили
- Процесс по борьбе с утечками секретов
- Локальные хуки и плагины для предотвращения компрометации секретов

Что киберпреступники используют для атак чаще всего?

Уязвимости 0-го дня?

Вредоносы?

Фишинг?

Скомпрометированные секреты!

Доменные креды

API ключи

Веб токены

Строки подключения к БД

Приватная часть ключей

Везде!

Репозитории

Базы знаний

Сетевые папки

Хранилища артефактов

Системы управления проектами

Системы логирования

Где потом это эксплуатируется?

Рабочие машины

Базы данных

Веб сервисы

Тестовые стенды

Сервера

Файловые хранилища

Облачные сервисы

Этапы зрелости

Глобальное требование (на всю компанию) о запрете хранения паролей в открытом виде

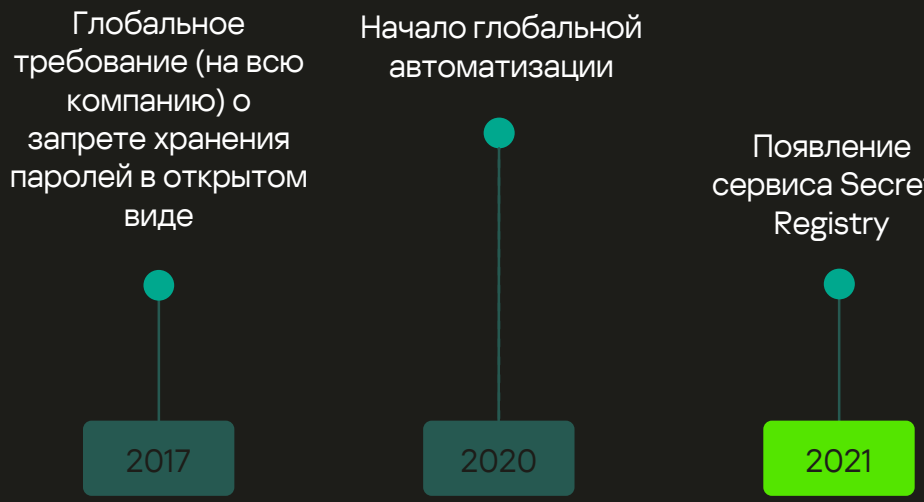
Формулировка требования ИБ:
Пароли и секреты не должны храниться в открытом виде в файлах, скриптах регистрации или командных файлах.

Этапы зрелости

Цели

- Обеспечить раннее обнаружение потенциальных утечек секретов
- Обеспечить контроль устранения рисков, возникающих в результате утечек секретов
- Соблюсти SLA по устранению выявленных секретов
- Предотвращать утечки секретов

Этапы зрелости

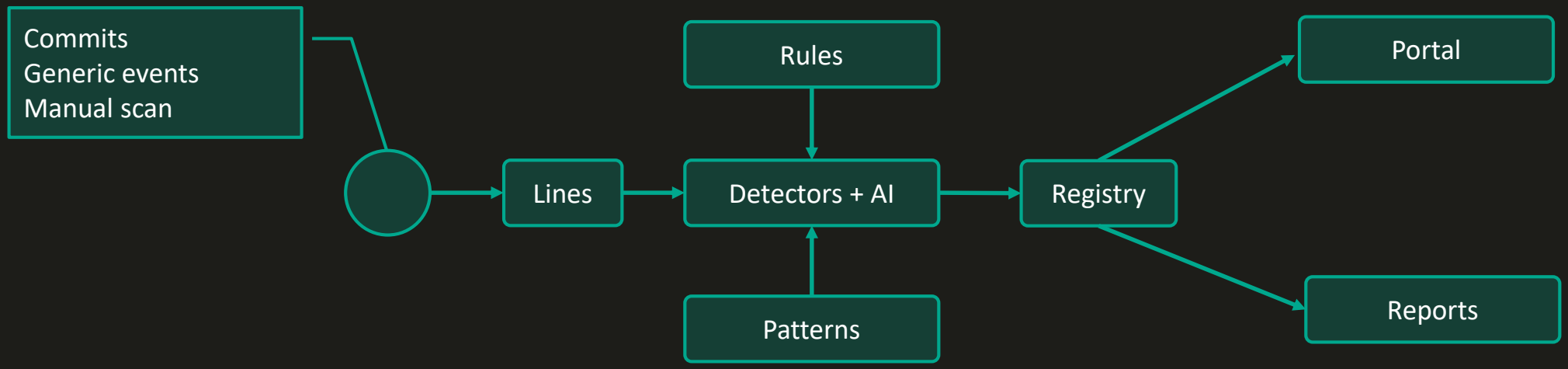


Почему мы не использовали open-source решения

Gitleaks

git-secret

Концепт Secrets Registry



Состояние на начало 2021 года

Проблемы, с которыми столкнулись

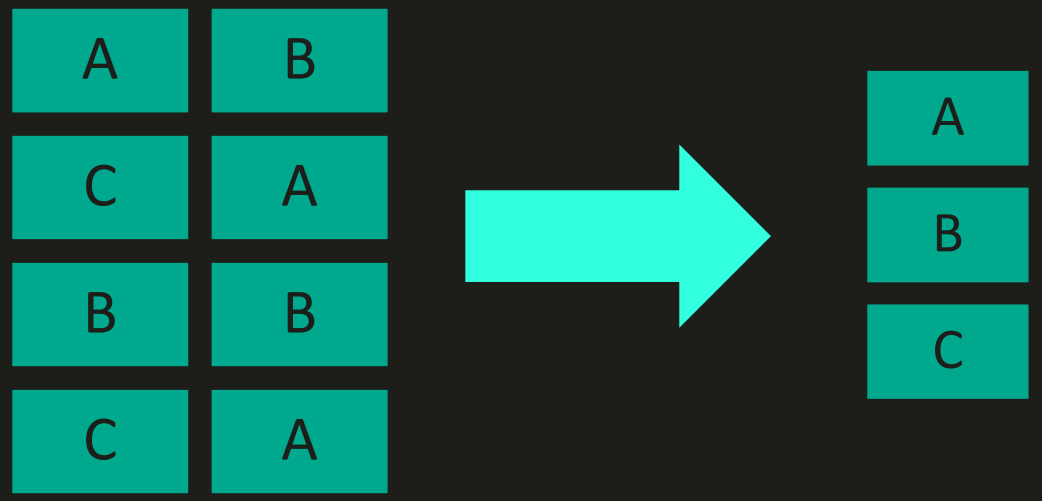
- Массовые False Detect-ы
- Тестовые секреты
- Дублирующиеся секреты

Этапы зрелости

ЭТАП 1. Поиск и схлопывание секретов в файле

ЭТАП 2. Дедупликация:

- в файлах с совпадающим хешем
- кредов
- в скопированных рабочих элементах
- сертификатов с совпадающим хешем



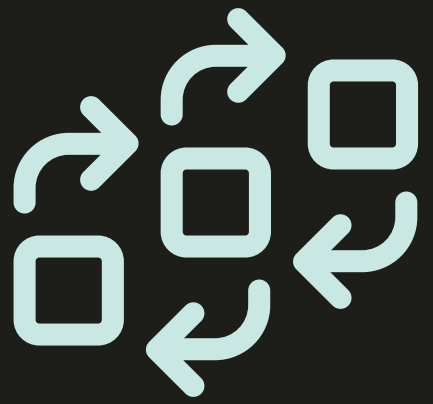
Количество детектов, закрытых как дубликаты

Код	Рабочие элементы	Сетевые папки
64500	3600	1023600

ЭТАП 6. Закрытие шифрованных PEM

ЭТАП 7. Закрытие просроченных JWT

ЭТАП 8. Закрытие по Name Convention (секреты, помеченные пользователем определённым тегом закрываются автоматом)



1. Проверка найденного секрета на энтропию
2. Проверка на длину
3. «Вайтлист» непаролей

Будут задетекчены:
89&^598
ILoveMyCatLordStewart
IoaBMW,wa5782p

Не будут задетекчены:
123
Password
Complicated
Qwerty
Пароль

1. ML выставляет рейтинг от 0 до 1 обнаруженному детекту
2. Детекты выше определенного порога помечаем как «секреты»
3. По мере поступления новых секретов переобучаем модель
4. Размер обучающей выборки на текущий момент >200 000 записей

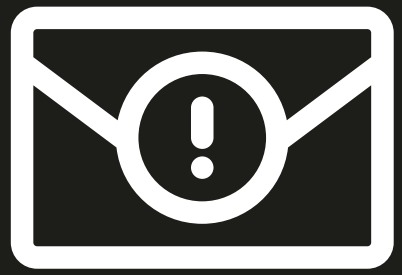
Количество фолсы уменьшилось в 18 раз за счёт переобучения модели

Доступ к секрету предоставляется:

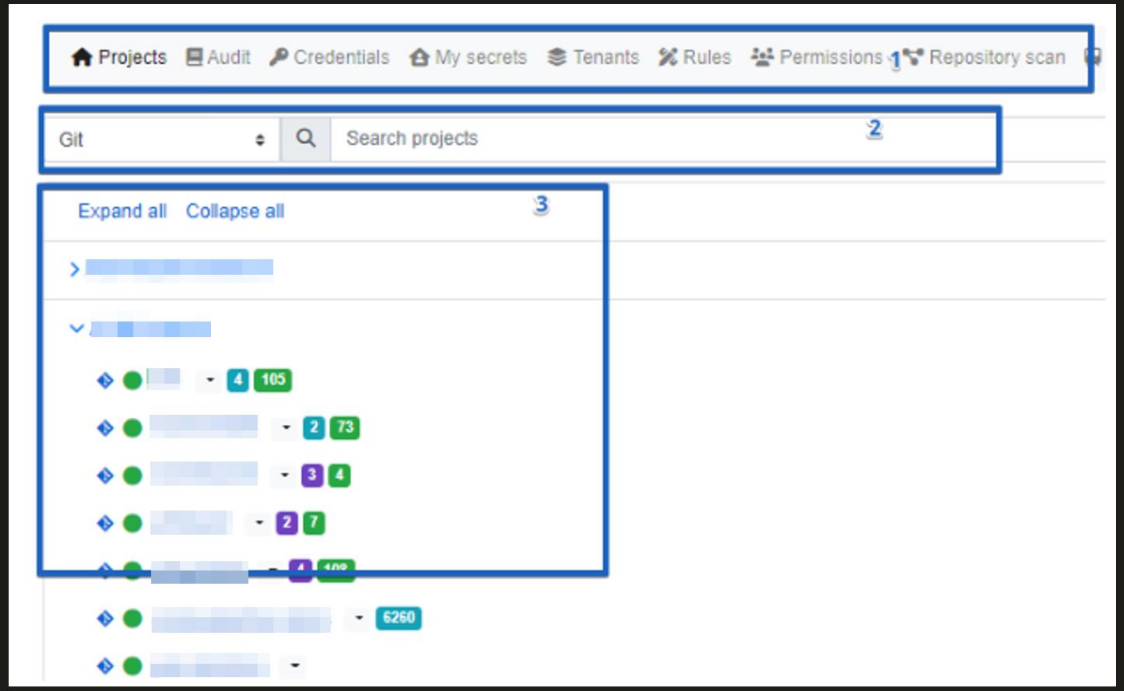
- По умолчанию — владельцу информационного ресурса/кода;
- Тому, кто закомитил секрет
- При делегировании — тому, на кого был назначен секрет (Assigned to)

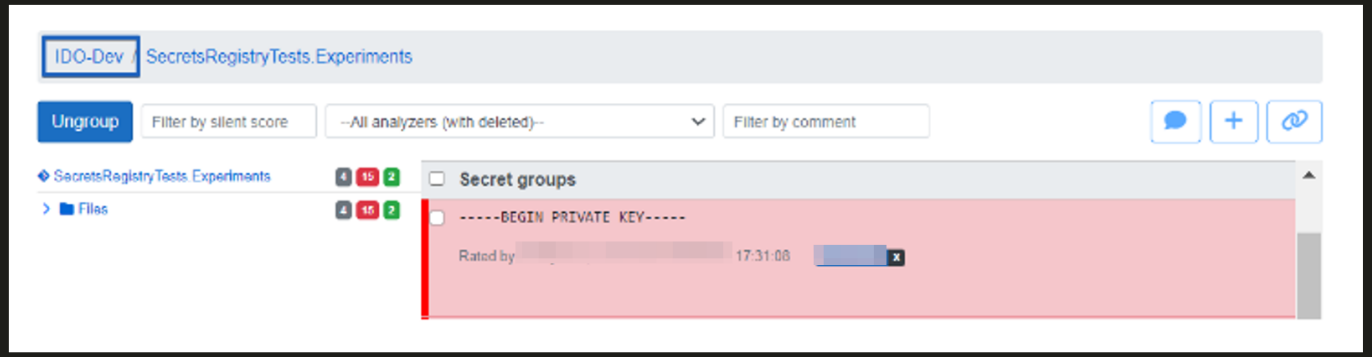
При обнаружении секретов, SR уведомляет ответственного с помощью нотификаций:

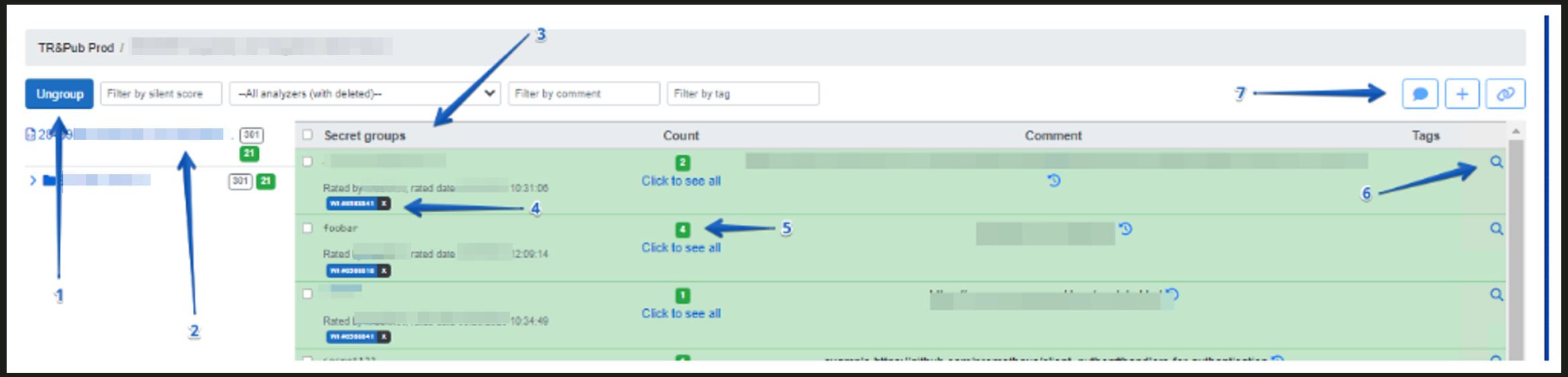
1. Реактивные
2. Еженедельные
3. Предупреждающие о приближении SLA
4. Assigned To



Интерфейсы

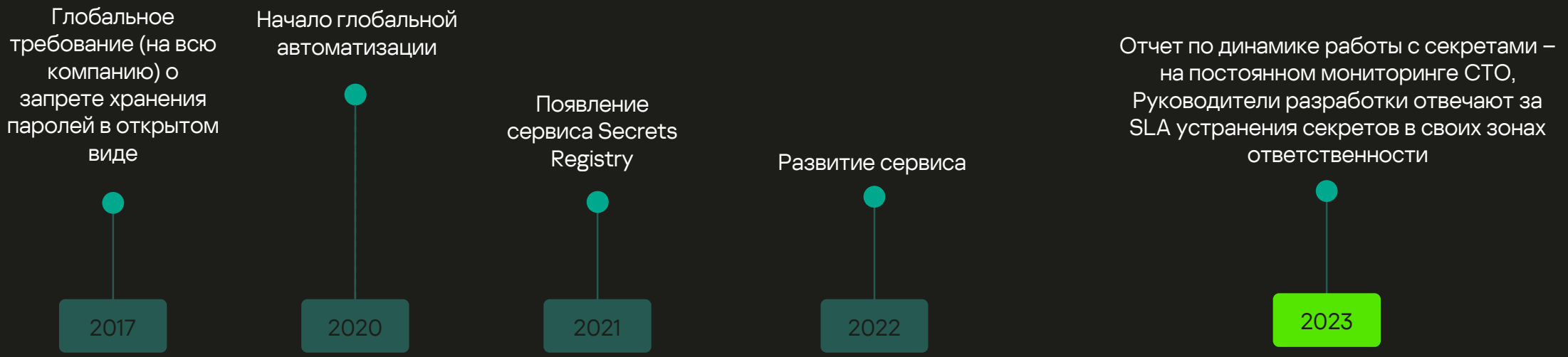

Projects
Audit
Credentials
My secrets
Tenants
Rules
Permissions
Repository scan
1
Git
Search projects
2
Expand all
Collapse all
3
4
105
2
73
3
4
2
7
6260


IDO-Dev
SecretsRegistryTests.Experiments
Ungroup
Filter by silent score
--All analyzers (with deleted)--
Filter by comment
SecretsRegistryTests.Experiments
Files
Secret groups
-----BEGIN PRIVATE KEY-----
Rated by
17:31:08

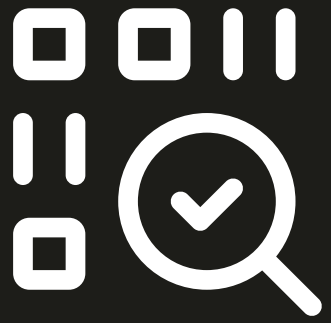

TR&Pub Prod /
Ungroup
Filter by silent score
--All analyzers (with deleted)--
Filter by comment
Filter by tag
Secret groups
Count
Comment
Tags
Click to see all
foobar
1
2
3
4
5
6
7


Secret List
51
10
65
316
Кнопка для обработки секрета
Toggle All
Show duplicates
--All analyzers (with deleted)--
What should I do
Update Status
Repository
Work Item
Field
Revision
Line
Type
Score
Status
Reason
Rated by
Work Items
Owner
Assigned to
Comment
Dates
Silent
Secret Keyword
0.19
Security risk secret
Not fixed
1
Detected: 16.09.22
Committed: 2
2.04.14
0.96

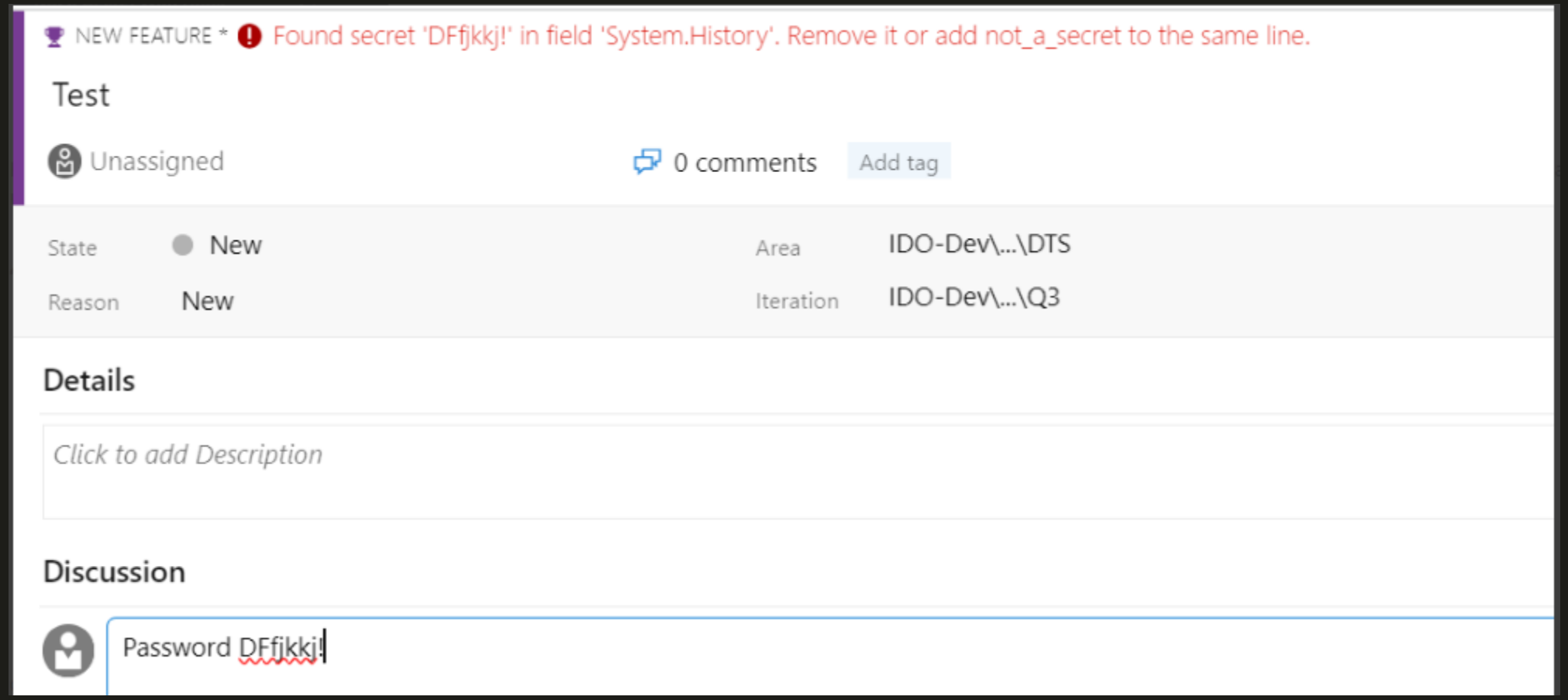
Этапы зрелости



- Блокирующая проверка на секреты в PR-ах
- Проверка всех публикуемых файлов на наличие секретов перед их публикацией
- Проверка дистрибутивов с распаковкой во время приемки тех. релиза



Предотвращение компрометации секретов: плагин для TFS



Отчет содержит:

- Общее кол-во актуальных (непоправленнных) секретов на текущий момент в компании
- Кол-во исправленных секретов за временной интервал
- Метрики по среднему времени фикса секретов
- Разбивку по подразделениям и менеджерам
- Метрики по установке и работе локального хука

Заключение

- Классификация
- Нотификации
- Интеграция с Azure DevOps
- Standalone Shell
- Аудит
- Поиск во всех типах информационных ресурсов
- Аналитика
- Локальный хук

- разобрали все потенциальные секреты, которые копились с момента появления компании (с 1997 года)
- **154.795.850** просканированных файлов
- **6.394.734** просканированных воркайтемов
- **23.556.891** просканированных комитов

Thank you!

Telegram chat:
https://t.me/+JGFaSXsRbglwY2Vi