SDLC: практики и их применение в kaspersky

Дмитрий Шмойлов,

Руководитель отдела безопасности программных продуктов

Лаборатория Касперского

kaspersky

Обо мне

Опыт:

- 18 лет в ИТ сфере (из них 14 – ИБ)
- Ранее - CISO одной из финансовых компаний федерального уровня

Настоящее время в Kaspersky:

- Развитие SDLC
- Application Security
- Services Security
- Privacy (в т.ч. GDPR) в продуктах и внутренних сервисов

Agenda

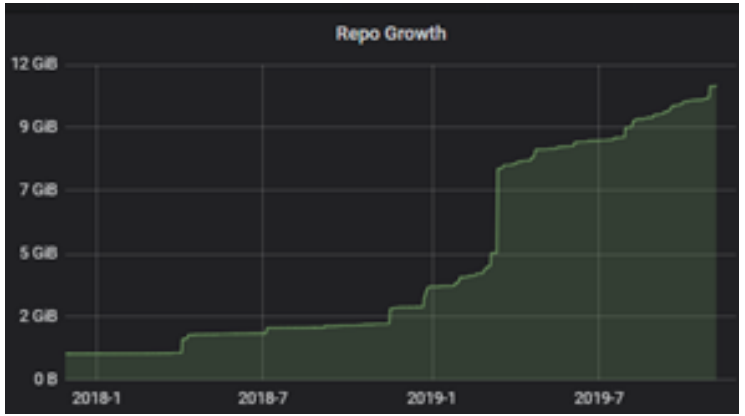
- Что есть безопасная разработка (SDL)
- Структура разработки в Kaspersky и с чего начался SDL
- Документы
- Роли
- Процессы и практики
- Инструментарий
- Несколько цифр из безопасной разработки

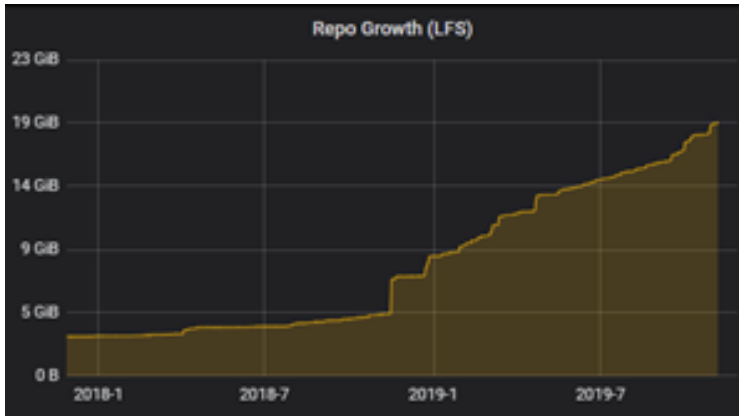
Q

Kaspersky: разработка в цифрах

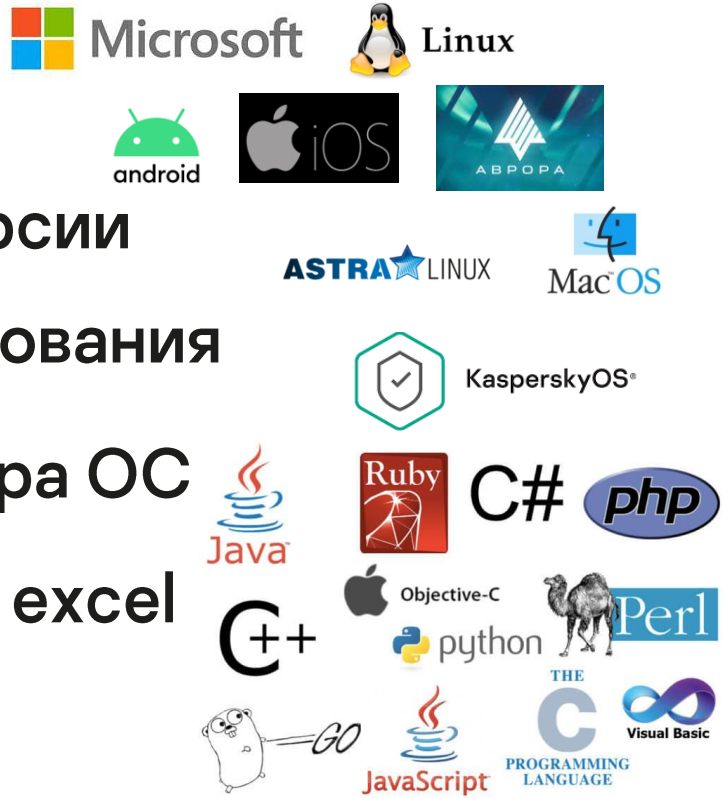
kaspersky

- ~750 разработчиков
- >200k строк кода меняется ежегодно
- ~70 продуктов (приложений) на поддержке
- 100+ крупных релизов продуктов ежегодно

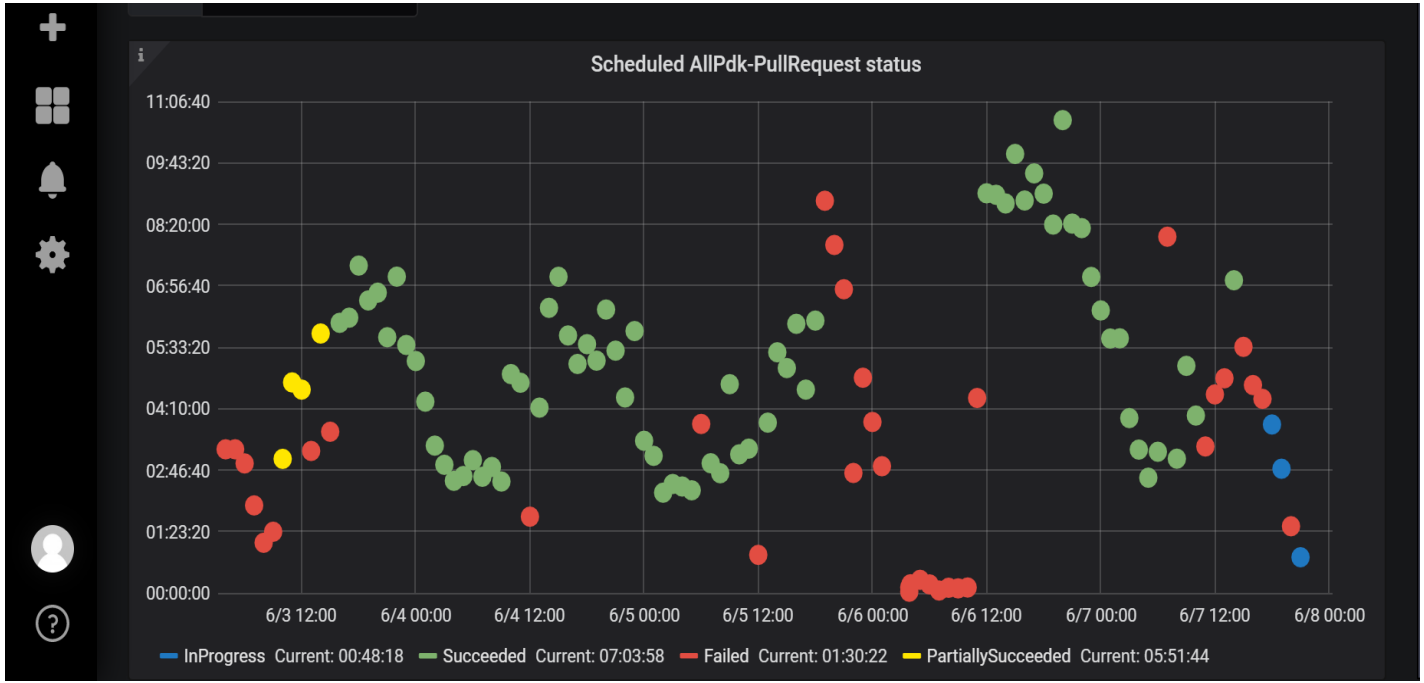




- Все платформы ОС (и даже специфические) и разные их версии
- Множество языков программирования
- Исполняемый код начиная от ядра ОС заканчивая Web или макросами excel



Разработка в ЛК: цифры



1070 релизов за последний год

Kaspersky: SDL внутри

kaspersky

Безопасное ПО: с чего начался SDL

1. Модели угроз и риски от вирусных аналитиков
2. Инициатива безопасности от команд и отдельных разработчиков
3. Зачатки процессов, которые поддерживались изнутри командами разработки
4. Тестирование
5. Процедура обработки обращений внешних исследователей

- Количество известных проблем безопасности на момент старта SDL ~ 115
- Проектная команда (частичное вовлечение) сотрудников ~ 7 чел

Безопасное ПО: с чего начался SDL

WikiLeaks Leaks News About Partners Search

Vault 7: CIA Hacking Tools Revealed

Kaspersky "heapgrd" DLL Inject

Overview

The Kaspersky AVP.EXE process references a DLL called WHEAPGRD.DLL.
by the PSP). Due to a UNICODE/ASCII processing mistake, the DLL name is
typicall installations, this causes Kaspersky to look for the DLL "CWHEAPGRD
process enables us to bypass Kaspersky's protections.

This vulnerability is limited to some of Kaspersky's previous releases (on both

Vunerable

1. KIS 7
2. KIS 8
3. WKSTN MP3

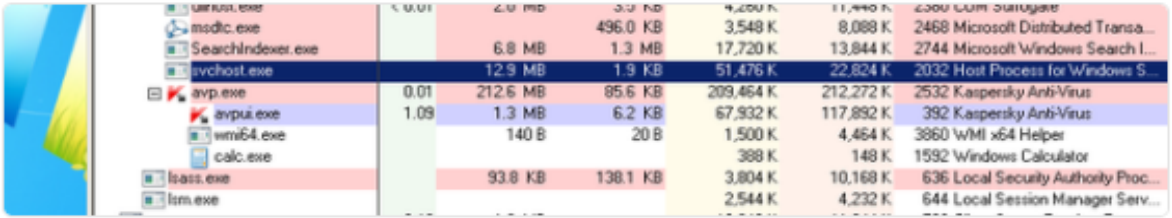
Not Vulnerable

1. KIS 9+
2. WKSTN MP4

Tavis Ormandy
@taviso

Follow

Okay, first Kaspersky exploit finished, works great on 15 and 16. Will mail report after dinner. /cc @ryanaraine



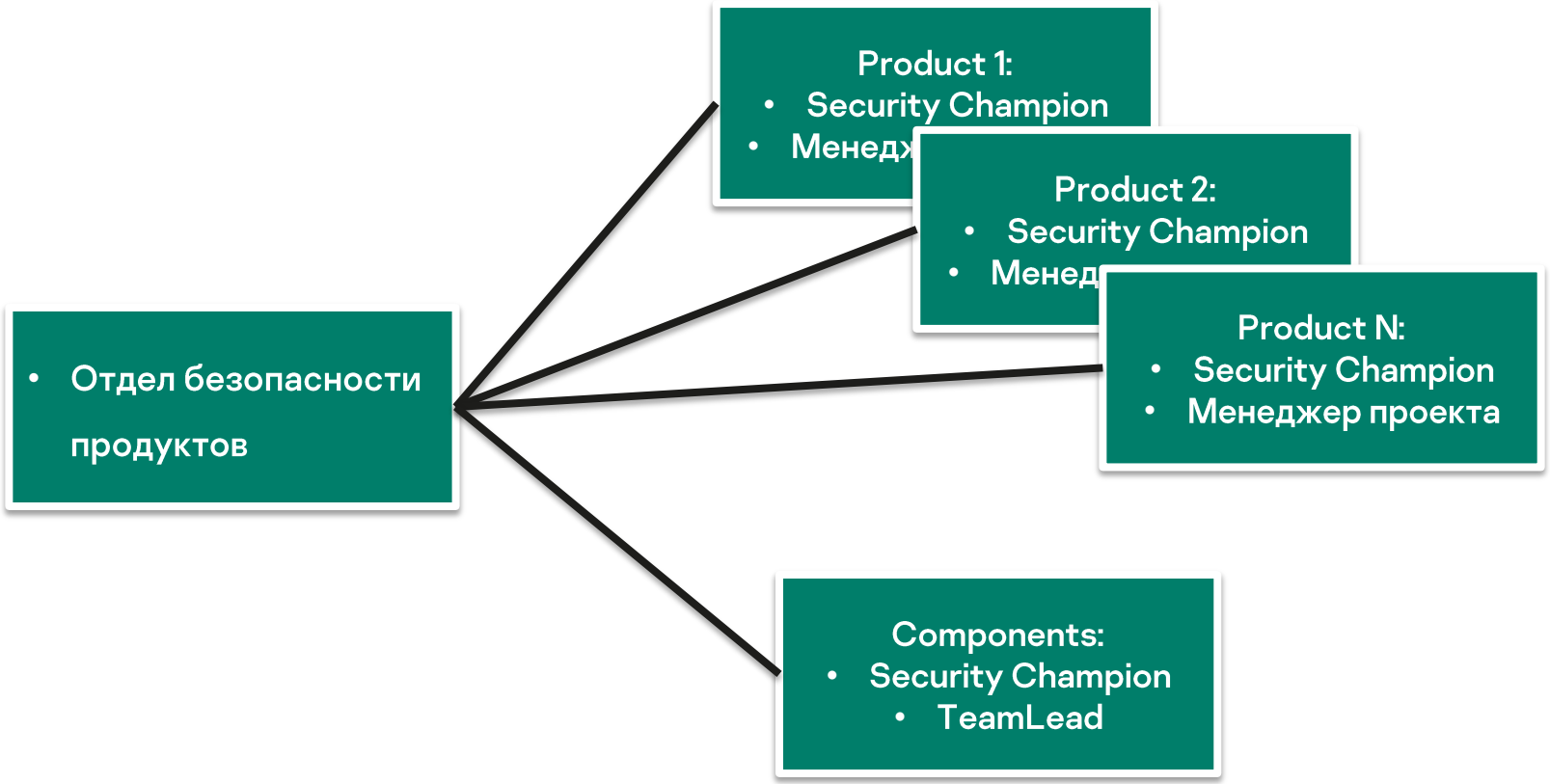
7:43 PM - 4 Sep 2015

SDL. Документы

Название документа
Правила проведения тестирования на проникновение
Процесс Secure code review
Secure coding guideline (checklist)
Процесс моделирования угроз
Инструкция для Security Champion по процессу моделирования угроз
Процесс фаззинг тестирования
Процесс управления уязвимостями
Руководство по разработке безопасного программного обеспечения
Процесс статического анализа кода
Процесс динамического анализа кода
Процесс использования сторонних библиотек

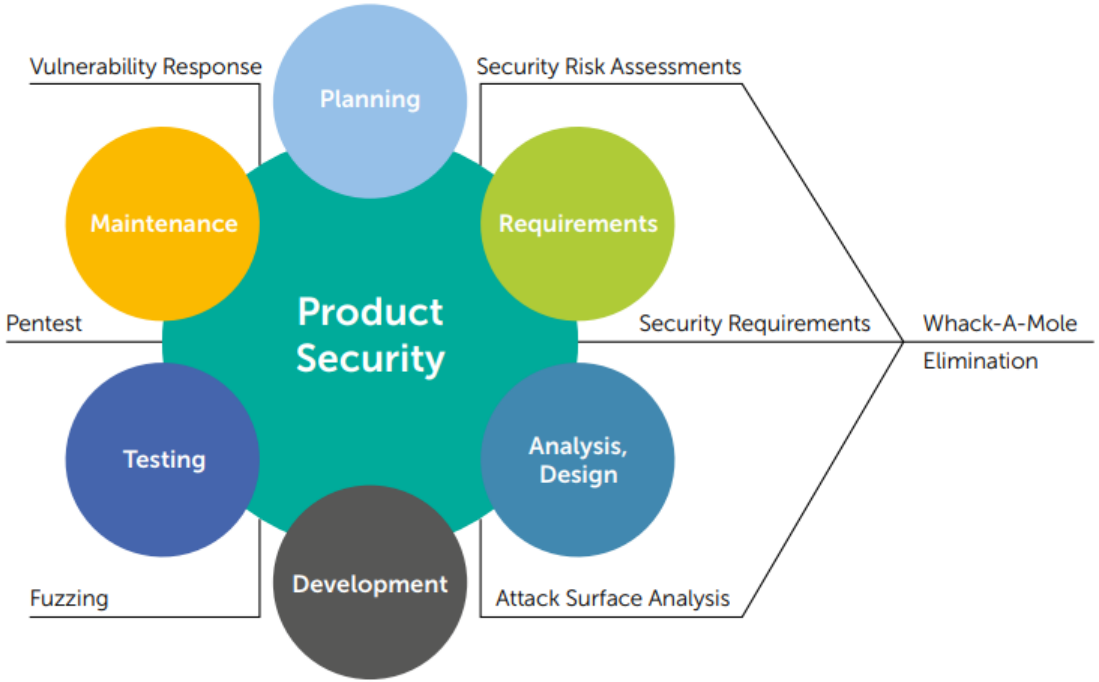
- Команда разработки
- Security чемпион
- Менеджеры продуктов
- Команда сертификации
- QA (контроль качества)
- Отдел безопасности продуктов

SDL. Люди и роли



- **Security чемпион:**
  - Находится внутри команды
    - Как правило архитектор или ведущий разработчик
  - Знает об изменениях
  - Проводит предварительный security анализ
  - Привлекает Application Security

Отдел безопасности ПО



- Требования по безопасности
- Модели угроз на основании сценариев
- Стратегия митигаций рисков
- Проверка закрытия рисков
- Фаззинг и тестирование на проникновение
- Автоматизация тестирования требований
- Автоматизация фаззинга

SDL. Обучение

Наименование	Участники
SDL. Вводный курс	Все
Безопасная разработка C/C++	Разработчики, Руководители команд, Архитекторы
Моделирование угроз	Руководители команд, Архитекторы, Security чемпионы
Fuzzing	Руководители команд, Архитекторы, Security чемпионы
Безопасность Web приложений	Все
Безопасность мобильных приложений	Разработчики, Руководители команд, Архитекторы
Криптография	Разработчики, Руководители команд, Архитекторы

SDL. VULN. Общие требования

Training | Require-ments | Design | Implemen-tation | Verificati on | Release | Response

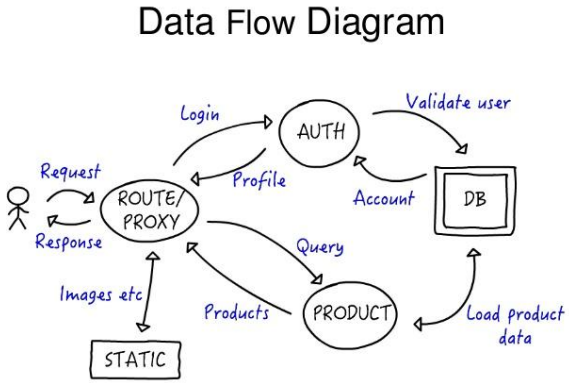
Требование
Up-to-date third party software
Perform static analysis
Prevent local privilege escalation
Mitigate network vulnerabilities (incl OWASP's Top 10)
Mitigate risks of sensitive data disclosure
SDL
Basic security requirements
Secure communication with KL infrastructure

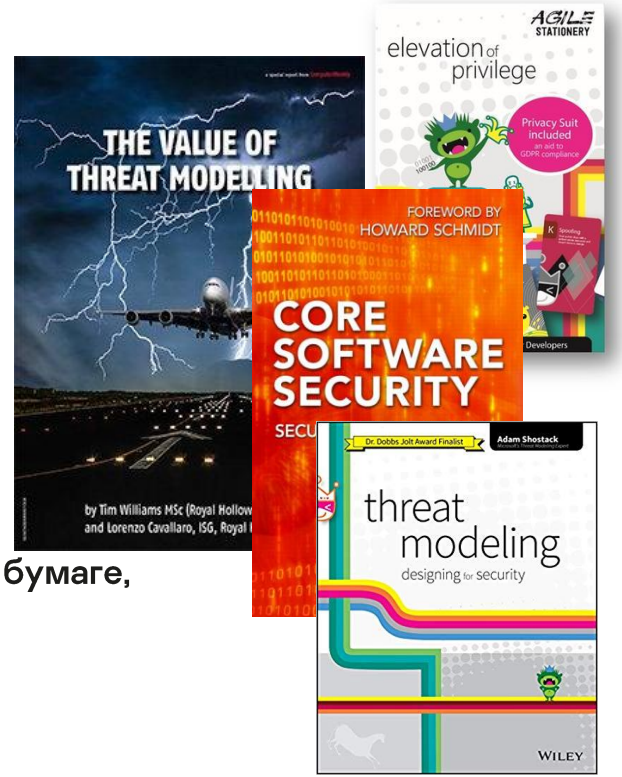
SDL. Моделирование угроз

Training | Require-ments | Design | Implemen-tation | Verificati on | Release | Response

Методология:

1. STRIDE
2. DREAD
3. PASTA
4. Kill Chain
5. OWASP
6. ..... mixed?





Рекомендации гуру:

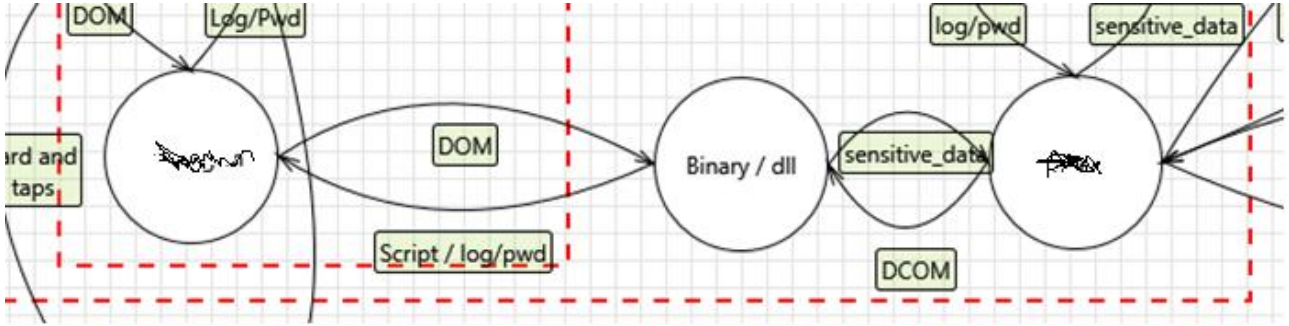
1. Концентрироваться на важных продуктах/модулях
2. Описывать и обсуждать изменения
3. Рисовать диаграммы, схемы, идеально – архитектуру (на доске, бумаге, где удобнее)
1. Задавать вопросы «а что если»
2. Идентифицировать риски без привязки к реализации

SDL. Моделирование угроз

Training | Require-ments | **Design** | Impleme n-tation | Verificat ion | Release | Respons e

Основные сценарии приложения, влияющие на безопасность:

1. **Предоставление интерфейса** – поверхность атаки
2. **Парсинг данных** – удаленные атаки с выполнением кода
3. **Сетевое взаимодействие** – раскрытие данных, перехват управления
4. **Изменение окружения** – локальное повышение привилегий
5. **Хранение данных** – раскрытие данных



SDL. Анализ исходного кода

Training | Require-ments | Design | Implemen-tation | Verificati on | Release | Response

Централизованный отчет по покрытию CodeReview

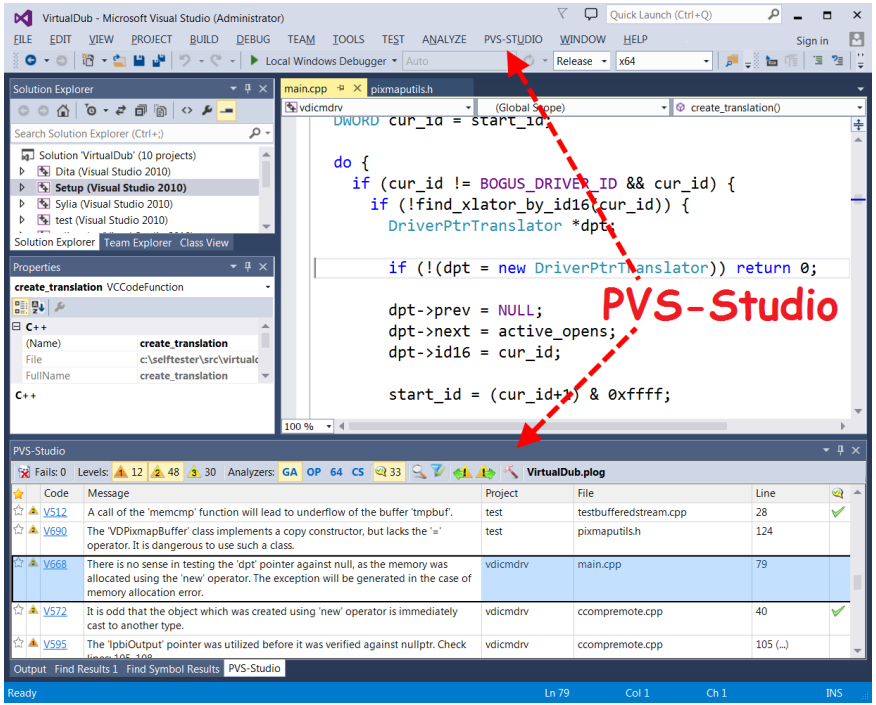
Сбор артефактов и построение отчетов роботами

Training | Require-ments | Design | Implemen-tation | Verificati on | Release | Response

Инструменты:

- PVS Studio
- Clang
- Svace
- PMD (android)
- Lint (android)

Статический анализатор должен использоваться в **блокирующем режиме**



SDL. 3-rd party библиотеки

Training | Require-ments | Design | Implemen-tation | Verificati on | Release | Response

Процессы:

1. проверка публичных уязвимостей
2. Приоритезация
3. Передача запросов на исправления в продукты и компоненты

open source

Common Vulnerabilities and Exposures

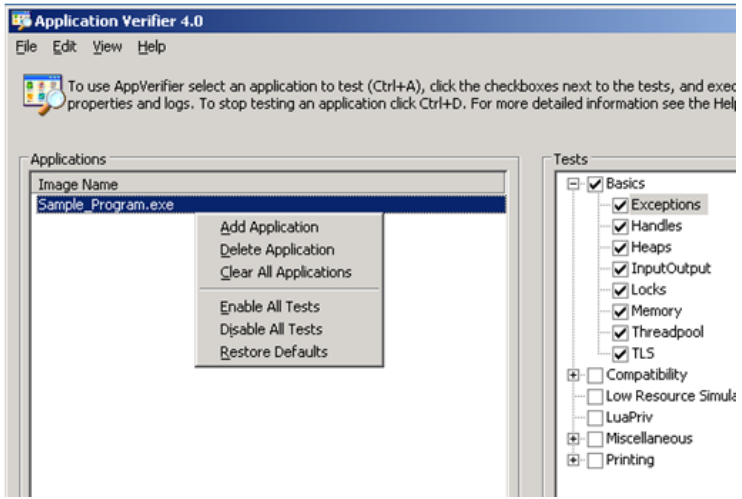
Продукты, компоненты, сервисы:

1. Устранение уязвимостей

Training | Require-ments | Design | Implemen-tation | Verificati on | Release | Response

Инструменты:

- Application Verifier
- Driver Verifier
- Dr.Memory/compiler specific
- * - sanitizer (address-, memory-, etc.)
- Valgrind



SDL. Динамический анализ

Training | Require-ments | Design | Implemen-tation | Verification | Release | Response

Product Security Requirement Verifier

DLL Hijacking:

- DLL is loaded by short or invalid path
- DLL is loaded by unsafe path
- Resource is accessed by path with weak ACL

Data corruption:

- Write to external folder under priveleged user

Проверка заголовка исполняемого файла:

- DLL does not support DEP
- DLL does not support ASLR
- DLL does not support isolation
- DLL does not support GS

Прочее:

- Write & Execute memory detected
- Using insecure protocol detected
- In process loaded unsigned module

SDL. Fuzzing

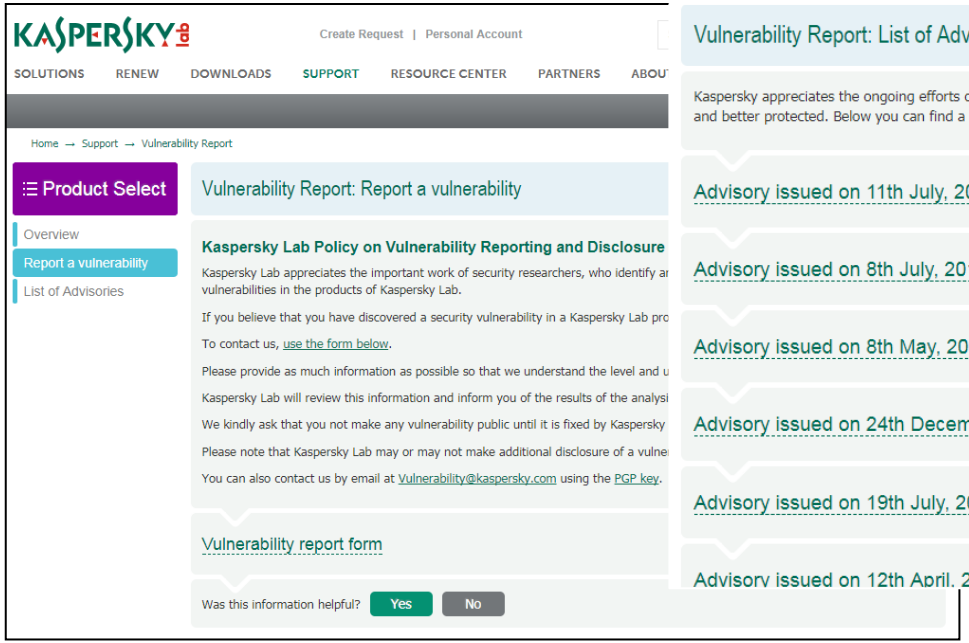
Training | Require-ments | Design | Implemen-tation | Verificati on | Release | Response

- Web API для передачи тестов на тестирование
- Автоматический запуск нового фазинг-теста на ферме

Fuzzing with AFL

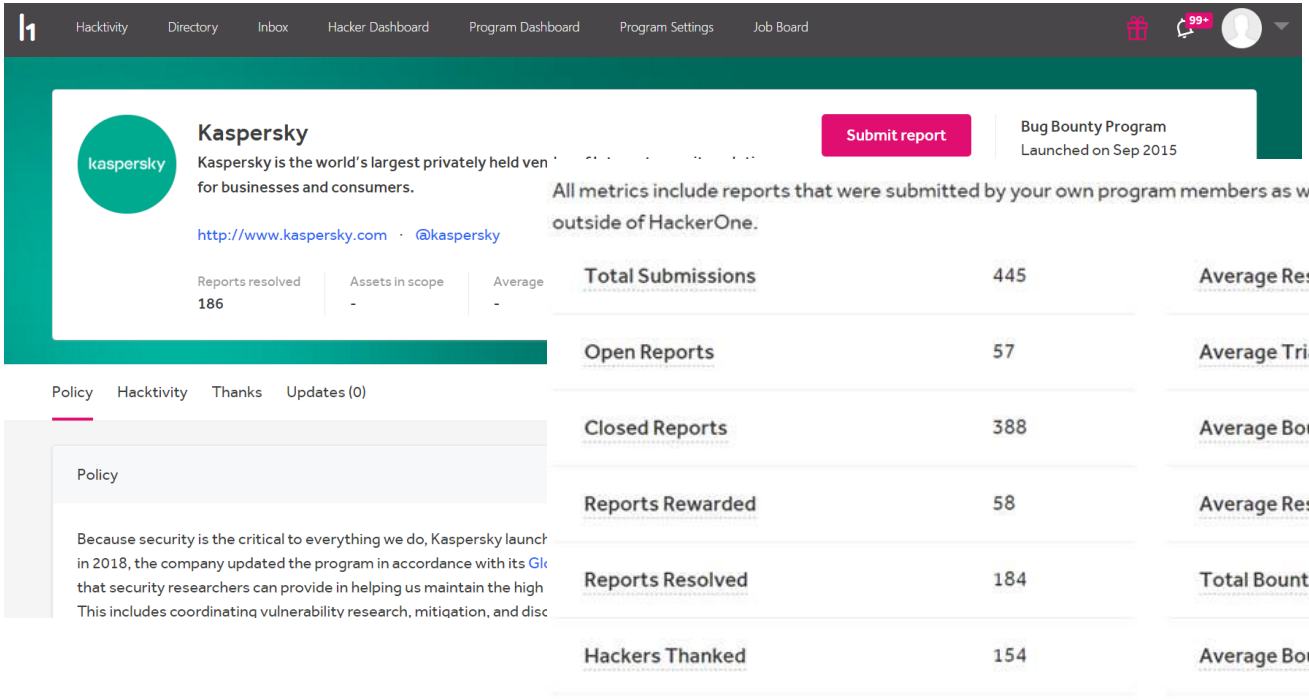
SDL. Публичные уязвимости

Training | Require-ments | Design | Implemen-tation | Verificati on | Release | Response



SDL. Публичные уязвимости

Training | Require-ments | Design | Implemen-tation | Verificati on | Release | Response



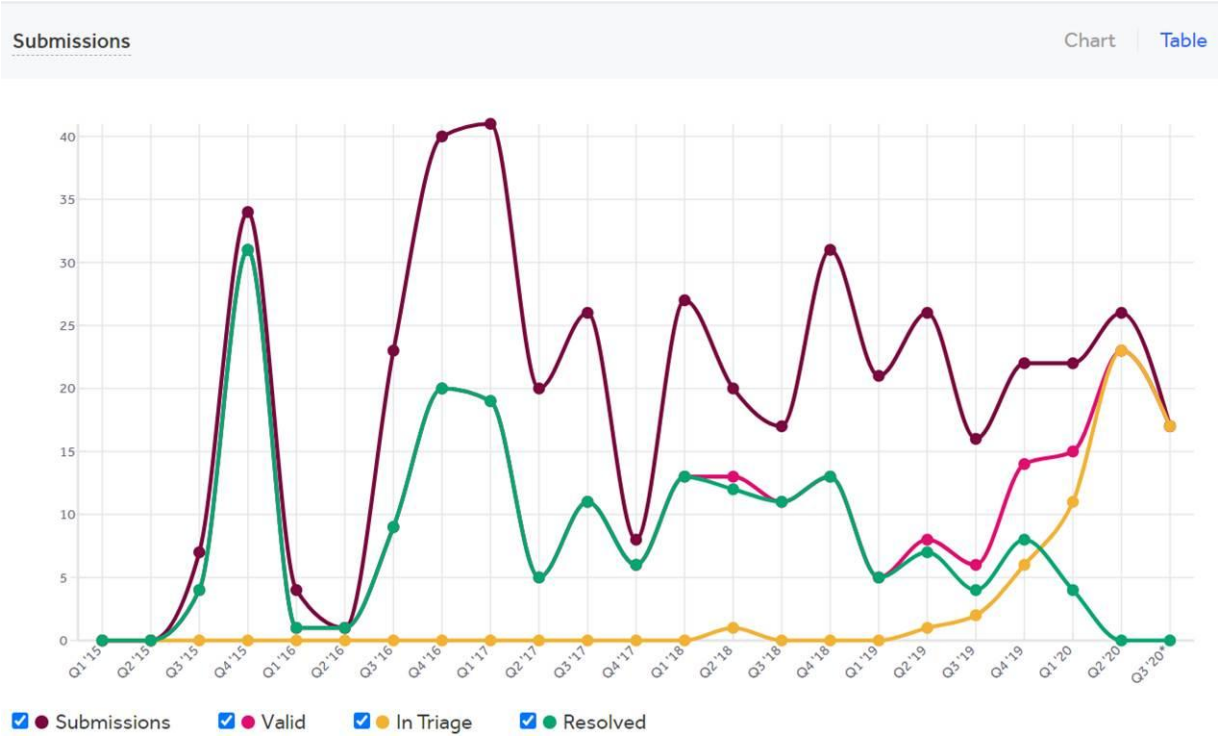
All metrics include reports that were submitted by your own program members as well as external reports that were submitted outside of HackerOne.

Total Submissions	445	Average Response Time	6 days
Open Reports	57	Average Triage Time	a month
Closed Reports	388	Average Bounty Time	15 days
Reports Rewarded	58	Average Resolution Time	4 months
Reports Resolved	184	Total Bounties	$64,050
Hackers Thanked	154	Average Bounty	$1,104

- BugBounty программа
- Платформа Hackerone
- До $100 000 вознаграждение

SDL. Публичные уязвимости

Training | Require-ments | Design | Implemen-tation | Verificati on | Release | Response



- BugBounty программа
- Платформа Hackerone
- До $100 000 вознаграждение

SDL. Сертификация безопасности

СЕРТИФИКАТ

TÜV AUSTRIA

ZERTIFIKAT | CERTIFICATE | CERTIFICAT | CERTIFICADO | СЕРТИФИКАТ | شهادة | 证书 | 인증서

соответствия системы менеджмента требованиям стандарта
ISO/IEC 27001:2013

В соответствии с процедурами TÜV AUSTRIA Deutschland настоящим подтверждается, что

АО «Лаборатория Касперского»
Ленинградское шоссе, д.39А/2
125212, г. Москва
Российская Федерация

Применяет систему менеджмента, соответствующую вышеназванному стандарту в следующих областях:

Доставка вредоносных и подозрительных файлов с помощью инфраструктуры Kaspersky Security Network (KSN), их безопасное хранение в Kaspersky Lab Distributed File System (KLDFS) и обеспечение доступа.

Действующее заявление о применимости: V2.0, 16.09.2019

Регистрационный номер сертификата: TAD ISMS 19924

Действительно с: 2019-12-13
Действителен до: 2022-12-12

Орган по сертификации
TÜV AUSTRIA Deutschland GmbH

Фильдерштадт, 2019-12-13

Данная сертификация была проведена в соответствии с процедурами аудитирования и сертификации TÜV AUSTRIA Deutschland GmbH и подлежит регулярным надзорным аудитам.
TÜV AUSTRIA Deutschland GmbH Kurze Straße 40 D-70794 Filderstadt www.tuv-ad.de

DAkkS

TÜV AUSTRIA

CERTIFICATE

ZERTIFIKAT | CERTIFICATE | CERTIFICAT | CERTIFICADO | СЕРТИФИКАТ | شهادة | 证书 | 인증서

Certification according to IEC 62443
Security for industrial automation and control systems
Part 4-1: Secure product development lifecycle requirements (IEC 62443-4-1:2018)

In accordance with TÜV AUSTRIA SERVICES procedures, it is hereby certified that

Kaspersky Lab JSC
Leningradskoe sh. 39A bld.2
125212 Moscow
Russian Federation

applies a secure product development lifecycle in line with the above standard **at a maturity level of 3** for the following scope

Kaspersky Industrial Cybersecurity for Networks

Based on inspection report: AU-20042706
Initial certification 2020-09-01
Valid until 2023-08-31

Certification Body
at TÜV AUSTRIA SERVICES GMBH

Vienna, 2020-09-01

This certification was conducted in accordance with TÜV AUSTRIA SERVICES auditing and certification procedures and is subject to regular surveillance audits.

TÜV AUSTRIA SERVICES GMBH Deutschstraße 10 A-1230 Wien www.tuv.at

Вопросы?

Дмитрий Шмойлов

Руководитель отдела безопасности
программных продуктов

kaspersky