McAfee
Together is power.

# Corporate InfoSec Solutions

OWASP Cordoba, April 2017

Andres More | Product Architect

Nicolas Guini | Product Security Champion

McAfee External

# Corporate InfoSec Solutions

## Introduction

This 1-hour talk will review processes and tools we use to ensure the development of secure components at our corporate offerings, including roles, tasks and software we use in our daily work. The discussion is split between processes and also our CC/FIPS certification experience.

**Andres More** is a product architect at the Argentina Software Development Center. Andres holds a degree in CS from FaMAF and a MsC in High Performance Computing from UNLP. Andres started in security implementing Multi-Level Security at the Linux's kernel network stack and then working in several roles and products in the InfoSec topic. At the moment leads McAfee´s Threat Intelligence technical roadmap and collaborates on multiple corporate solutions on both protection and detection scenarios.

**Nicolás Guini** is a Software Engineer and Product Security Champion at the Argentina Software Development Center. Nicolás is System Engineer from IUA and is finishing the Information Security Specialization from the same institute. Nicolás has acquired certifications around Ethical Hacking (CPHE and CHEE) from Spain. Nicolás now is working in the Threat Intelligence Exchange project at McAfee as Software Developer and Security Specialist, leads the Security Research team on Malware Analysis and Binary Exploitation and is Virus Lab Owner.

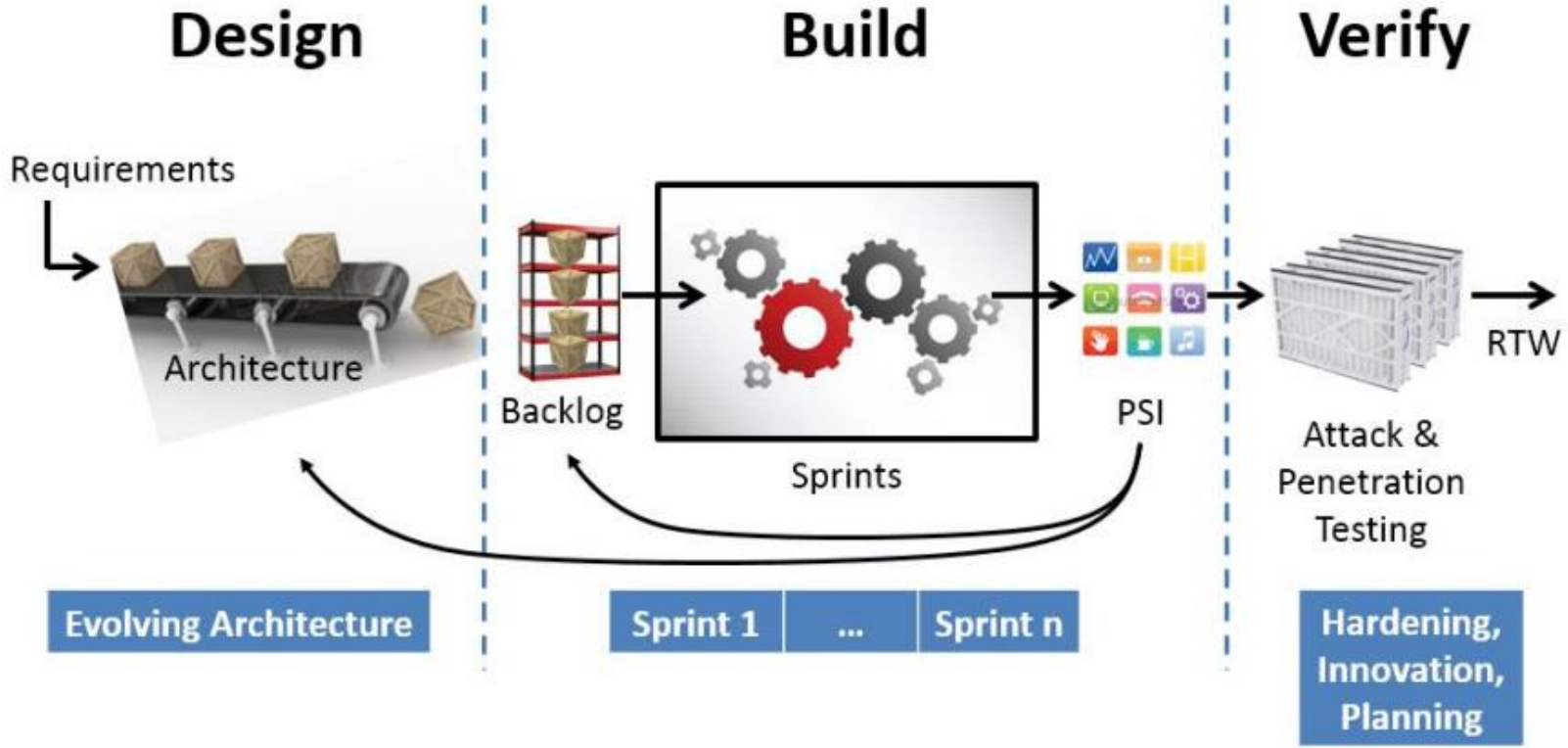
Source

# Secure Development Process

Introduction

# Corporate InfoSec Solutions

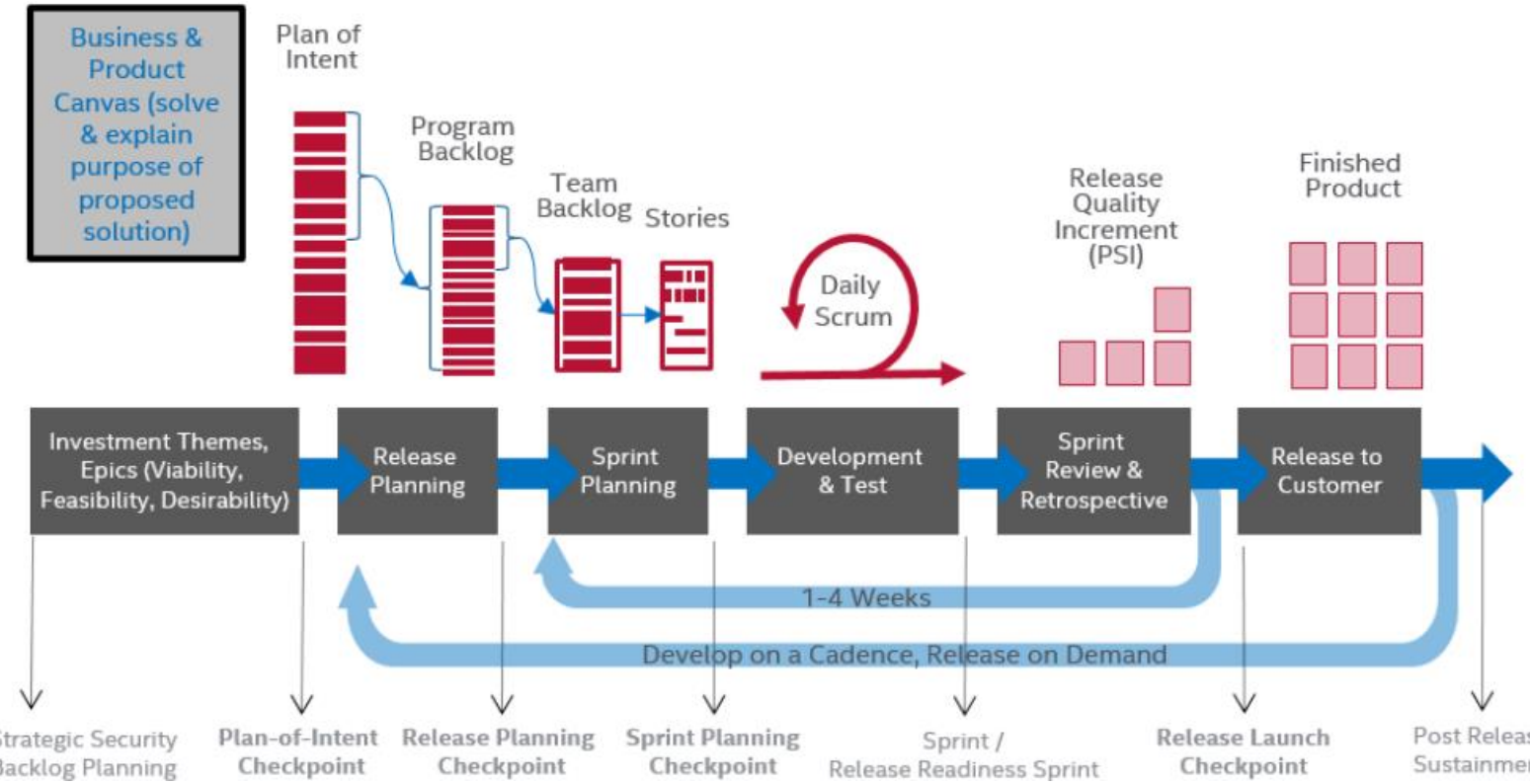
## High Level SDL




Source

# Corporate InfoSec Solutions

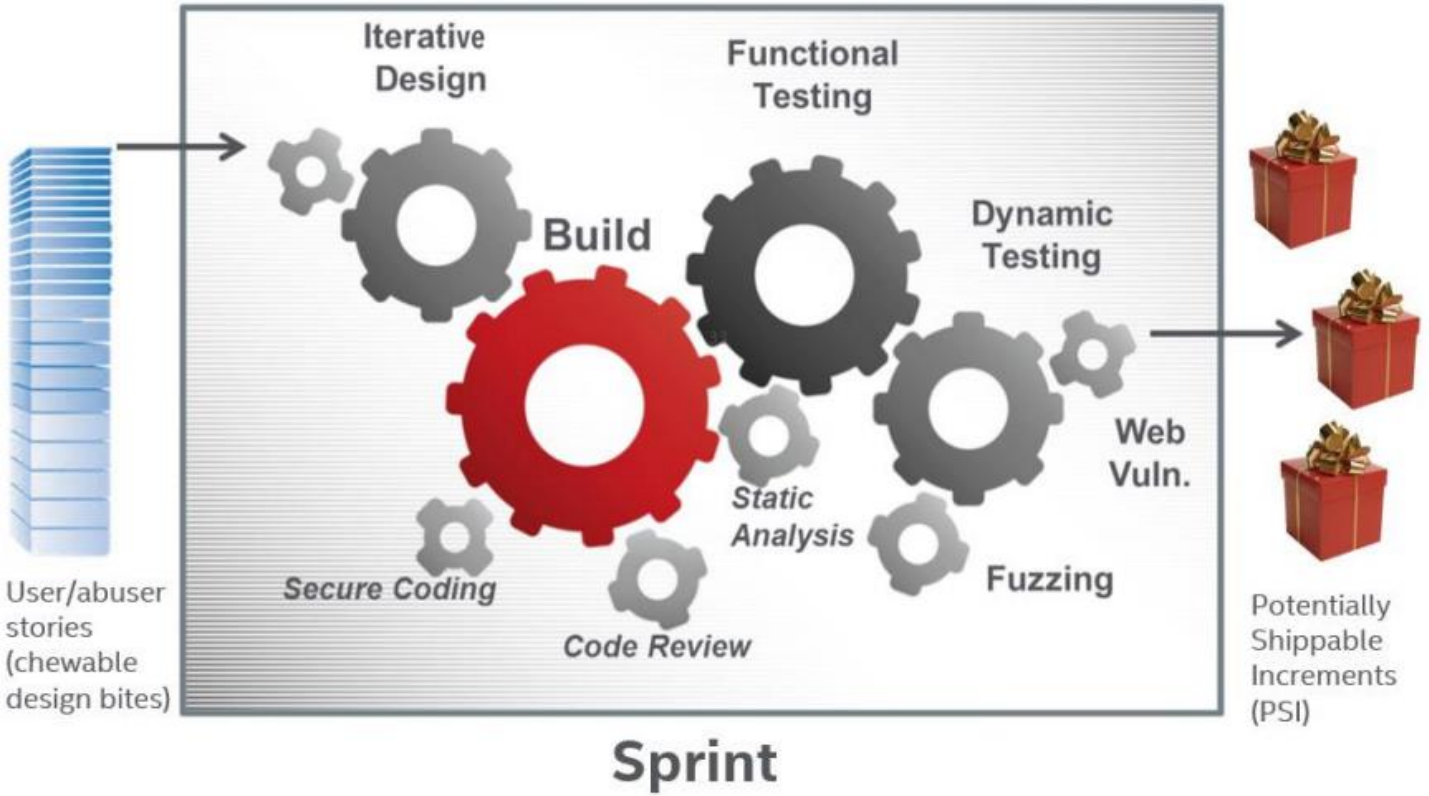
## Agile SDL




Source

# Corporate InfoSec Solutions

## Potentially Shippable Increments




Source

# Corporate InfoSec Solutions

## Software Development Lifecycle (SDLC) at McAfee

### Security Development Lifecycle (SDL)

- In line with industry standards such as ISO/IEC 27001/27002/27034, BSIMM, and SAFECode
- Our practices include designing for both privacy and security, in software and applications.
- We have rigorous product security policies and processes designed to find and remove software security defects, e.g. security vulnerabilities.
- We understand that our products must not only fulfill the stated function to help protect our customers, the software itself must also aim to protect itself from vulnerabilities and attackers.
- We strive to build software that demonstrates resilience against attacks.

Source

# Corporate InfoSec Solutions

## Product Security Maturity Model

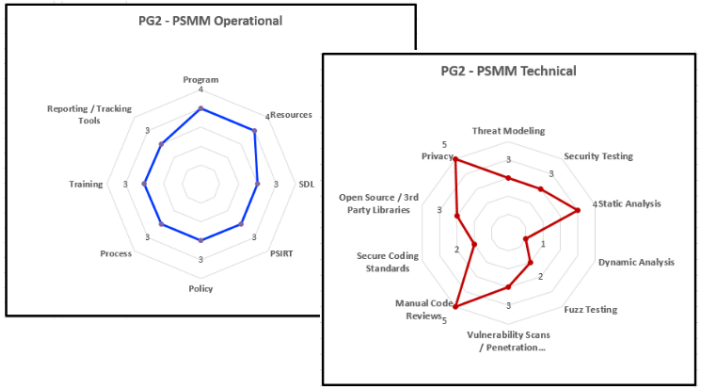
McAfee PSMM rates maturity on the execution of security practices, based on ISO 27034.

Indicates what needs to be done, but not how. Always process focused.

We use an internal model based on CMM with levels, our site got rated DFS 3 some years ago.

Initial, Repeatable, Defined, Managed, Optimized.

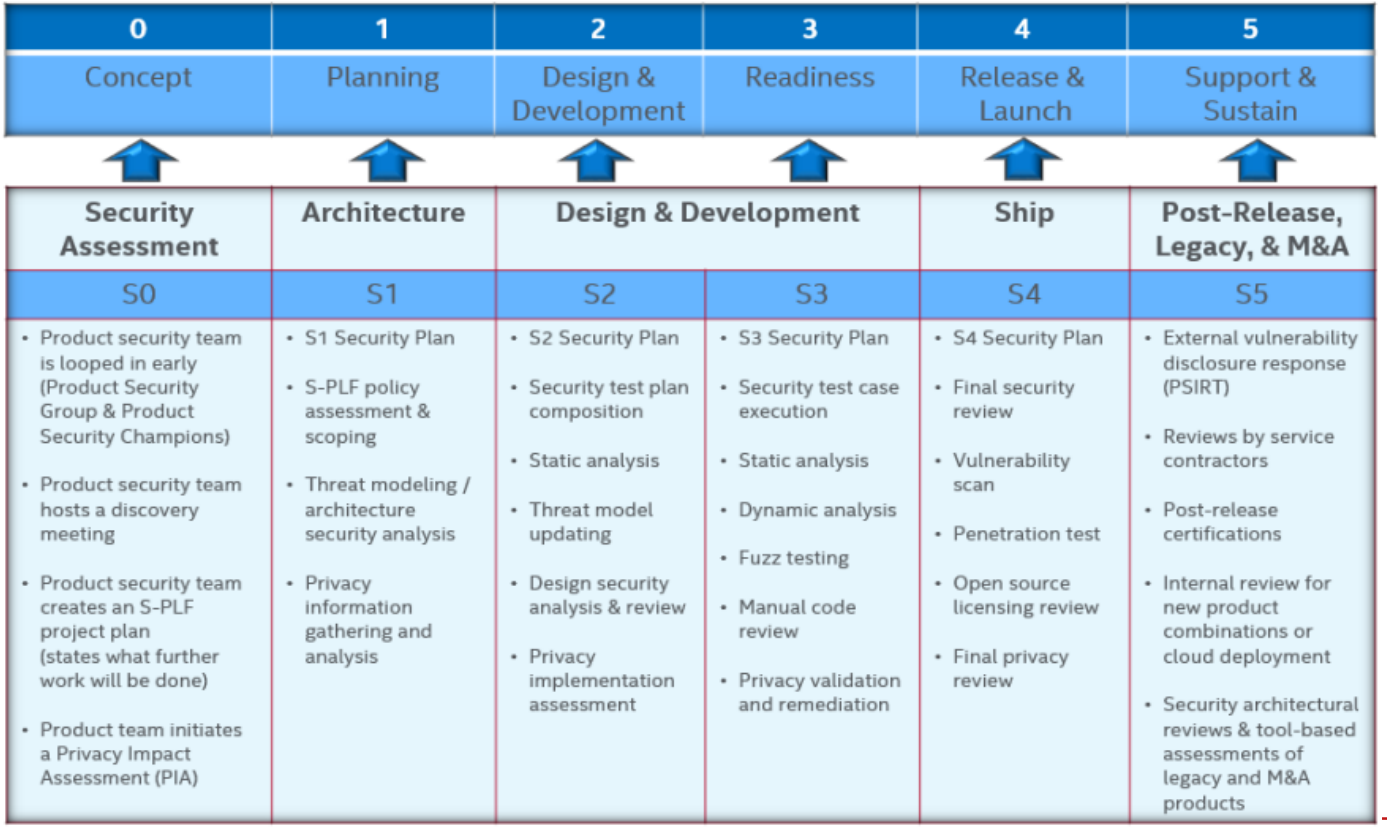
Product security can be split in operational and technical aspects.




Source

# Corporate InfoSec Solutions

## SDLC Phases




Source

# Corporate InfoSec Solutions

## Agile SDL Activities

### Design

SDL.T01 Security Definition of Done

SDL.T02 Security Architecture Review

SDL.T03 Security Design Review

SDL.T04 Threat Modeling

### Testing

SDL.T05 Security Testing

SDL.T06 Static Analysis

SDL.T07 Dynamic Analysis

SDL.T08 Fuzz Testing

SDL.T09 Vulnerability Scan

SDL.T10 Penetration Testing

### Peer Review

SDL.T11 Manual Code Review

SDL.T12 Security Coding Standards

### External

SDL.T13 Vendor Management

SDL.T14 Open Source / 3rd Party COTS Libraries

SDL.T15 Privacy

Source

# Corporate InfoSec Solutions

## Software Development Lifecycle (SDLC) at McAfee

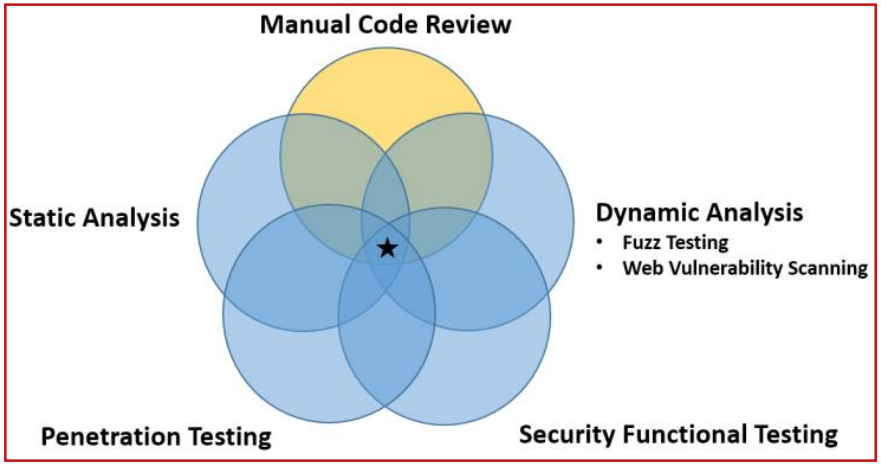
Product Security Champions and Evangelists: a.k.a. Security architects.

Trust and Verify: All new code is peer reviewed and goes thru automation layers.

Complimentary Independent Security Testing: Third party analysis.

External Policies: Transparent dialog.

Software Security Tools: Open Source, internal, commercial




Source

# Applying SDL

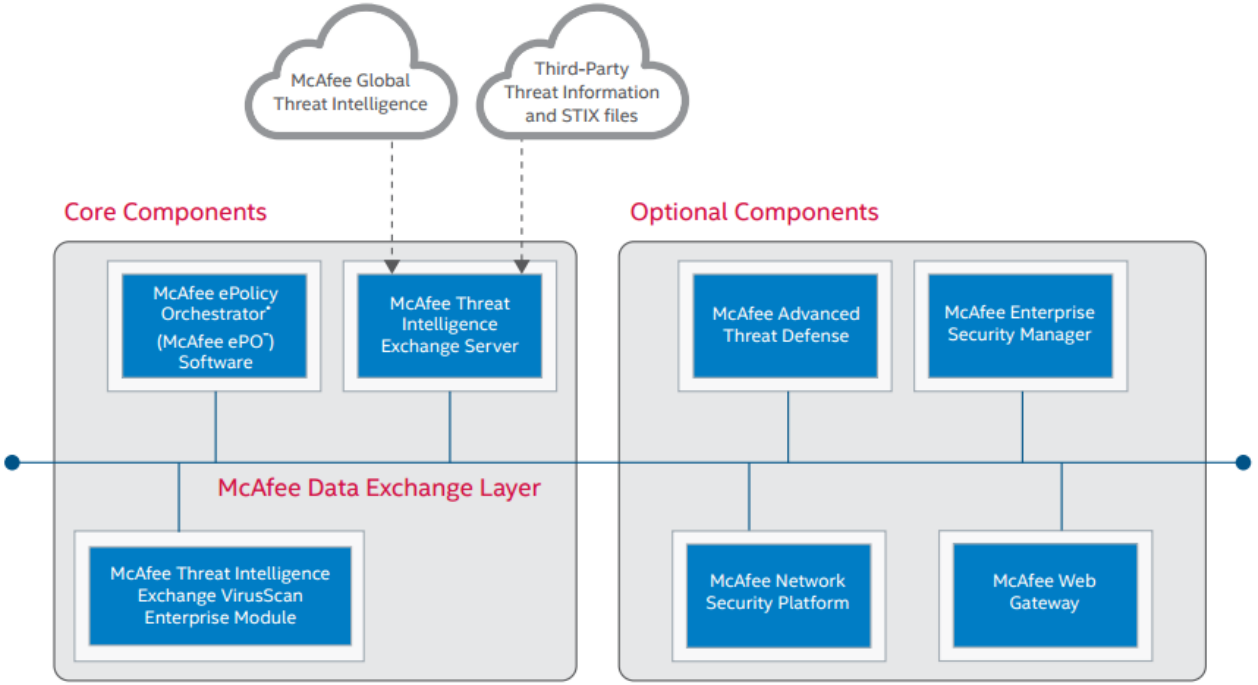
Case Study

# Corporate InfoSec Solutions

## Threat Intelligence Exchange

McAfee® Threat Intelligence Exchange enables adaptive threat detection and response by operationalizing intelligence across your endpoint, gateway, network, and data center security solutions in real time. Combining imported global threat information with locally collected intelligence and sharing it instantly, allows your security solutions to operate as one, exchanging and acting on shared intelligence.

[mcafee.com/tie](mcafee.com/tie)




Source

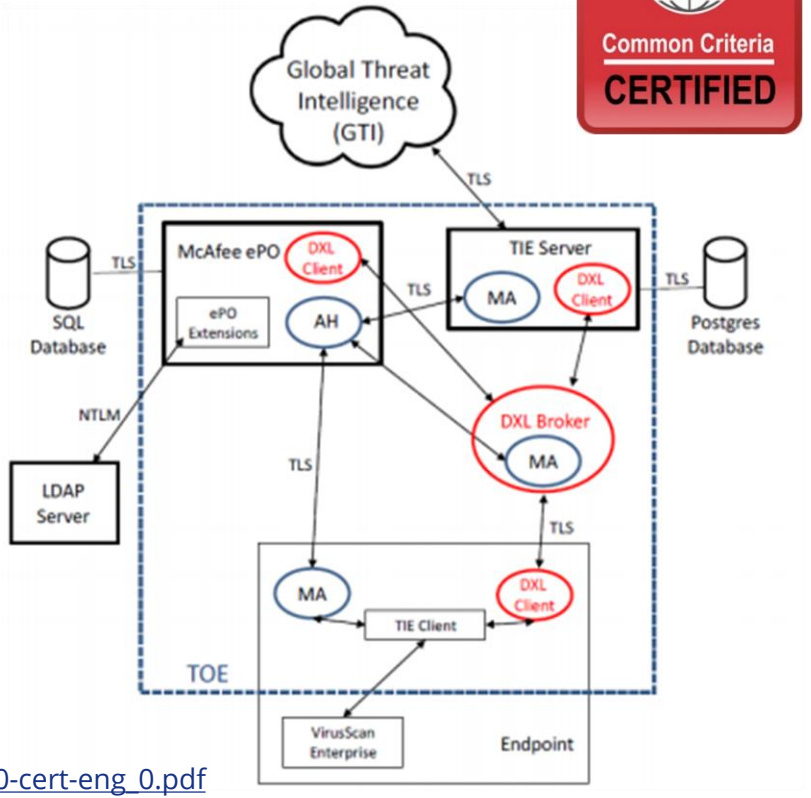
# Corporate InfoSec Solutions

## Common Criteria

We underwent CC EAL 2+ certification recently.

Process:

1. We documented the solution thread model
2. Identified potential attacks and ensured mitigations where in place for them
3. We secured every communication channel
4. Performed several penetration testing exercises closing all identified gaps
5. We automated the upgrade from the Beta release into the hardened version without manual steps




https://www.cse-cst.gc.ca/en/system/files/pdf_documents/mcafee-threat-200-cert-eng_0.pdf

Source

# Corporate InfoSec Solutions

## Federal Information Processing Standard (FIPS)

We underwent FIPS-140-2 Level 2 certification successfully recently for our 2.0 release.

Process:

1. We met with federal-sector experts and reviewed the whole process.
2. We reviewed all our components to ensure they were using compliant algorithms and key sizes.
3. Then worked with a contractor for the paperwork of the solution: how it works, its communication channels, which libraries where used, how we configure them, etc.
4. At last, we provided support for an independent lab to setup an environment to gather specific evidence of secure communication.



Source

# Corporate InfoSec Solutions

## Supporting Tools

Management console is a web interface for easier remote management.

Our continuous deployment tooling run integration builds that include security tools

We use Coverity, OpenVAS, MVM, Nessus, nmap, OWASP dependency-check, Defensics, codecollab.





Source

# Corporate InfoSec Solutions

## Product Security Incident Response Team

We formally answer customer requests on vulnerabilities or security-related concerns such as independent penetration testing as required for PCI-compliance and similar.

Some of our products have their own CVEs, but usually we patch our appliance components.

| | |
|---|---|
| **Impact of Vulnerability:** | Permissions, Privileges, and Access Control (CWE-264)<br>Improper Access Control (CWE-284) |
| **CVE Numbers:** | CVE-2015-7238 |
| **Severity Rating:** | Low |
| **Base / Overall CVSS v3 Scores:** | 3.7 / 3.5 |
| **Base / Overall CVSS v2 Scores:** | 3.0 / 2.6 |
| **Recommendations:** | Upgrade to TIE 1.2.0 |
| **Security Bulletin Replacement:** | None |
| **Affected Software:** | Threat Intelligence Exchange (TIE) 1.1.1 and earlier |
| **Location of Updated Software:** | http://www.mcafee.com/us/downloads/downloads.aspx |

Source

No computer system can be absolutely secure. McAfee makes no warranty with respect to any malfunctions or other errors in its hardware products or software products caused by viruses, infections, worms, or similar malicious code not developed or introduced by McAfee. McAfee makes no warranty that any hardware products or software products will protect against all possible security threats, including intentional misconduct by third parties. McAfee is not liable for any downtime or service interruption, for any lost or stolen data or systems, or for any other damages arising out of or relating to any such actions or intrusions.

Additional information on security and privacy is available at http://www.intel.com/content/www/us/en/policy/policy-securityprivacy.html?wapkw=security+and+privacy


McAfee, the McAfee logo and [insert <other relevant McAfee Names>] are trademarks or registered trademarks of McAfee LLC or its subsidiaries in the U.S. and/or other countries.
Other names and brands may be claimed as the property of others.
Copyright © 2017 McAfee LLC.