



конференция
РусКрипто'2013

<http://www.ruscrypto.ru/conference/>

Learn. Connect.
Collaborate. *together.*

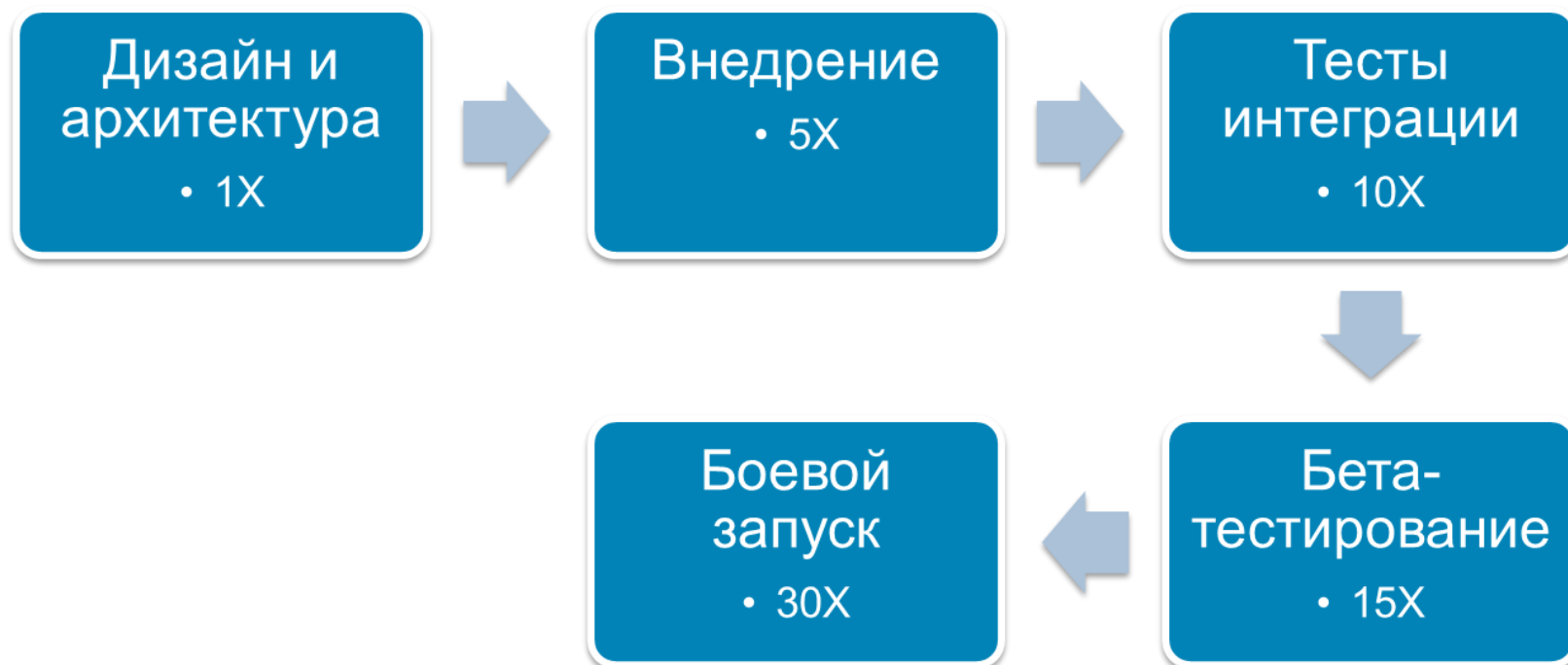
Анализ качества ПО с точки зрения безопасности: международный опыт

Лукацкий Алексей, консультант по безопасности

**ВЫГОДНО ЛИ ЗАНИМАТЬСЯ
АНАЛИЗОМ КАЧЕСТВА ПО?**



Почему выгодно заниматься анализом качества ПО?



Почему выгодно заниматься анализом качества ПО?


Этап	Найдено критических уязвимостей	Стоимость устранения 1 уязвимости	Стоимость устранения всех уязвимостей
Требования		\$139	
Дизайн		\$455	
Программирование		\$977	
Тестирование	50	\$7 136	\$356 800
Поддержка	150	\$14 102	\$2 115 300
Всего	200		\$2 472 100

Почему выгодно заниматься анализом качества ПО?

Этап	Найдено критических уязвимостей	Стоимость устранения 1 уязвимости	Стоимость устранения всех уязвимостей
Требования		\$139	
Дизайн		\$455	
Программирование	150	\$977	\$146 550
Тестирование	50	\$7 136	\$356 800
Поддержка		\$14 102	
Всего	200		\$503 350

- Данные расчеты применимы к крупным разработчикам ПО

**ЕСЛИ НЕ ДЕНЬГИ, ТО ЧТО
МОТИВИРУЕТ НА АНАЛИЗ
КАЧЕСТВА ПО?**



Что требует Министерство Обороны США?

- Раздел 933 «IMPROVEMENTS IN ASSURANCE OF COMPUTER SOFTWARE PROCURED BY THE DEPARTMENT OF DEFENSE» закона «Defense National Defense Authorization Act of 2013»
 - Обязательный контроль качества ПО, приобретаемого Министерством Обороны США
- Задача достигается применением
 - автоматизированных сканеров безопасности,
 - тестированием,
 - анализом кода,
 - и т.д.



Требований у Министерства Обороны США немало

Cybersecurity-Related Policies and Issuances

Developed by the DoD CIO for Cybersecurity Last Updated: March 15, 2013 Send questions/suggestions to info@thesiac.com

IA GOAL 1: ORGANIZE					IA GOAL 2: ENABLE					IA GOAL 3: ANTICIPATE					IA GOAL 4: PREPARE					AUTHORITIES																								
1.1 Lead and Govern																																												
EO 13526: Improving Critical Infrastructure Cybersecurity					PD 21: Critical Infrastructure Security and Resilience					National Strategy for Information Sharing and Safeguarding					U.S. I&I Strategy for Cyberspace					25 Point Implementation Plan to Reform Federal IT Mgt.					Quadrennial Defense Review (QDR)					National Defense Strategy (NDS)					CNSS-24 Policy on Assured Info Sharing (AIS) for National Security Systems (NSS)					DoD 8500.01 Management of the DoD Information Enterprise				
DoD 8500.01E Information Assurance (IA)					DoD 8500.2 Information Assurance Implementation					DoD Strategy for Operating in Cyberspace					DoD Cyber, Identity & Information Assurance Strategic Plan					Guidance for Development of the Force (GDF) for 2010-2015					National Military Strategy Plan for the War on Terrorism					National Military Strategy (NMS)					National Military Strategy for Cyberspace Operations (NMS-CO)									
1.2 Design for the Fight					2.1 Secure Data in Transit					3.1 Understand the Battlespace					4.1 Develop and Maintain Trust...					OPERATIONAL																								
1.3 Develop the Workforce					2.2 Manage Access					3.2 Prevent and Delay Attackers... and 3.3 Prevent Attackers from Staying...					4.2 Strengthen Cyber Readiness																													
1.4 Partner for Strength					2.3 Assure Information Sharing					3.3 Prevent and Delay Attackers... and 3.3 Prevent Attackers from Staying...					4.3 Sustain Missions					SUBORDINATE POLICY																								
SP 800-119 Guidelines for the Secure Deployment of IPv6					FIPS 140-2 Security Requirements for Cryptographic Modules					FIPS 198 Standards for Security Categorization of Federal Info. and Info. Systems					CNSS-12 National Policy for Space Systems Used to Support NSS					Title 10 Armed Forces (32224, 30130, 30130S, 80130S) Title 32 National Guard (5100)																								
NISTSP-1 National Information Assurance Acquisition Policy					CNSS-17 National Policy for Safeguarding and Control of COMSEC Material					CNSS-29 Standards for Security Categorization of Federal Info. and Info. Systems					CNSS-21 National IA Policy on Enterprise Architecture for NSS					Title 40 Public Buildings, Property, and Works (211, 9611302, 11315, 11311)																								
DoD 8500.02 Interoperability and Supportability of IT and National Security Systems (NSS)					CNSS-17 National Information Assurance Policy on Wireless Capabilities					SP 800-80 R1 Guide for Managing the Risk of Info and Info Systems to Security Categories					NISTSP-1002 TEMPEST Glossary					Federal Information Security Management Act, 44 U.S.C. §3541 et seq.																								
DoD 7045.20 Capability Portfolio Management					CNSS-25 National Policy for PIR in National Security Systems					NISTIR 7893 Specification for Assent Identification 1.1					DoD 8100.10 Space Policy					DoD 8500.02 National Information Assurance (IA) Instruction for Computerized Information Systems																								
DoD 7000.02 Operation of the Defense Acquisition System					CNSS-2002 Communications Security (COMSEC) End Item Modification					DoD 8500.02 Counterintelligence (CI) Activities in Cyberspace					DoD 8100.12 ASD for Networks and Information Integratn/DoD CIO					DoD 8501.01 IA Policy for Space Systems Used by the DoD																								
DoD 7000.14 Financial Management Policy and Procedures (FMPC)					CNSS-5000 Communications Security (COMSEC) Guidelines for Voice Over Internet Protocol (VoIP), Confer, Telephony					FIP 200 Minimum Security Requirements for Federal Information Systems					DoD 8100.44 ASD for Networks and Information Integratn/DoD CIO					DoD 8501.01 IA Policy for Space Systems Used by the DoD																								
DoD IA Certification and Accreditation Process (DIACAP)					NACSS-001 Foreign Military Sales of COMSEC Article and Services to Foreign Countries and Users					NISTIR 800-123 Guide for Security-Forward Configuration Mgt of Info Systems					SP 800-128 R2 SCAP Ver. 1.2					Computer Fraud and Abuse Act Title 18 (5130)																								
DIACAP Knowledge Service					DoD 8501.01 Department of Defense Operations					CNSS-1-10.1 Reducing Risk of Removable Media in NS					DoD 8100.12 Computer Security Incident Handling Guide					Stored Communications Act Title 18 (51071 et seq.)																								
M&A between DoD CIO and DODI CIO Establishing Non-Centric Software Licensing Agreements					DoD 8501.01 Department of Defense Operations					DoD 8501.1 Support to Computer Network Defense (CND)					SP 800-18 R1 Guide for Developing Security Plans for Federal Information Systems					Foreign Intelligence Surveillance Act Title 50 (51801 et seq.)																								
DoDAR (Version 3.02) DoD Architecture Framework					DoD 8501.01 Department of Defense Operations					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					SP 800-19 Continuous Monitoring					Executive Order 13221 as Amended by EO 13289 - Critical Infrastructure Protection in the Info Age																								
DoD 8501.01 Net Ready Key Performance Parameter					DoD 8501.01 Department of Defense Operations					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					Executive Order 13526 Structural Reforms to Improve Classified Vets																								
Alignment Framework for the GIG IA Architecture (AFG) version 1.1					DoD 8501.01 Department of Defense Operations					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					Executive Order 13289 Structural Reforms to Improve Classified Vets																								
IAFP Version 3.1 Information Assurance Technical Processes					DoD 8501.01 Department of Defense Operations					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					Executive Order 13526 Structural Reforms to Improve Classified Vets																								
CNSS-000 Information Assurance (IA) Education, Training, and Awareness					DoD 8501.01 Department of Defense Operations					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					Executive Order 13289 Structural Reforms to Improve Classified Vets																								
COMSEC Equipment Maintenance and Maintenance Training					DoD 8501.01 Department of Defense Operations					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					Executive Order 13289 Structural Reforms to Improve Classified Vets																								
National IA Training Standard for Senior Systems Managers					DoD 8501.01 Department of Defense Operations					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					Executive Order 13289 Structural Reforms to Improve Classified Vets																								
National IA Training Standard for Information Systems Security Officers					DoD 8501.01 Department of Defense Operations					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					Executive Order 13289 Structural Reforms to Improve Classified Vets																								
National IA Training Standard for Risk Assessors					DoD 8501.01 Department of Defense Operations					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					Executive Order 13289 Structural Reforms to Improve Classified Vets																								
DoD 8501.01M Information Assurance Workforce Improvement Program					DoD 8501.01 Department of Defense Operations					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					Executive Order 13289 Structural Reforms to Improve Classified Vets																								
CNSS-1233 Security Categorization and Control Selection for National Security Systems					DoD 8501.01 Department of Defense Operations					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					Executive Order 13289 Structural Reforms to Improve Classified Vets																								
CNSS-4001 Communications Security (COMSEC) IAWP Program					DoD 8501.01 Department of Defense Operations					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					Executive Order 13289 Structural Reforms to Improve Classified Vets																								
DoD 8500.13 DoD 8500.13 Defense Industrial Base Cyber Security (IA) Activities					DoD 8501.01 Department of Defense Operations					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					Executive Order 13289 Structural Reforms to Improve Classified Vets																								
CNSS-14 National Policy for the Release of IA Products/Services					DoD 8501.01 Department of Defense Operations					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					Executive Order 13289 Structural Reforms to Improve Classified Vets																								
CNSS-1253 Security Categorization and Control Selection for National Security Systems					DoD 8501.01 Department of Defense Operations					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					Executive Order 13289 Structural Reforms to Improve Classified Vets																								
CNSS-4001 Communications Security (COMSEC) IAWP Program					DoD 8501.01 Department of Defense Operations					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					Executive Order 13289 Structural Reforms to Improve Classified Vets																								
DoD 8500.13 DoD 8500.13 Defense Industrial Base Cyber Security (IA) Activities					DoD 8501.01 Department of Defense Operations					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					Executive Order 13289 Structural Reforms to Improve Classified Vets																								
DoD 8501.01M Information Assurance Workforce Improvement Program					DoD 8501.01 Department of Defense Operations					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					DoD 8501.21 Use of Mobile Code Technologies in DoD Information Systems					Executive Order 13289 Structural Reforms to Improve Classified Vets																								

Distribution Statement A: Approved for Public Release. Distribution is unlimited.

Что требуется в госорганах США?

- 5.02.2013 NIST опубликовал 4-ю версию SP800-53 «Security and Privacy Control for Federal Information Systems and Organizations»
 - Обязателен для государственных органов США
 - Группа защитных мер «Systems and Service Acquisition»
 - Абсолютно новый блок SA-11 «Developer Security Testing and Evaluation»
- 7 защитных мер (на выбор)
 - Средства анализа кода
 - Анализ уязвимостей и угроз
 - Независимая оценка плана анализа защищенности
 - Ручной анализ кода
 - Пентесты
 - Моделирование угроз
 - Проверка области тестирования/анализа

Что требуется в госорганах США?

- В NIST SP800-53 также введен новый блок защитных мер SA-12 по контролю цепочек поставок компонентов информационных систем
 - Вы уверены, что в приобретенном вами коде нет случайных или намеренных закладок?
 - Оценка **ДО** выбора системы, **ДО** ее использования и **ДО** ее обновления
- Механизмы реализации SA-12
 - Статический и динамический анализ
 - Симуляция
 - Тестирование в режиме «белого»/«серого»/«черного» ящика
 - Пентесты
 - Fuzz testing
 - Криптографические хэши
 - И т.д.

ЛУЧШИЕ ПРАКТИКИ



Что такое защищенный код?

- 10% функций защиты
 - МСЭ
 - ACL
 - криптография
- 90% защищенных функций
 - Защита от переполнения
 - Проверка входных данных
 - Контроль выходных данных
- Требуется непрерывный процесс обеспечения и повышения качества ПО, включающий решение различных задач



Лучшие практики по обеспечению качества ПО

- Включает не только анализ качества ПО, но и также
- Правила защищенного программирования
- Регулярные тренинги и программы повышения осведомленности
- Моделирование угроз
- Тестирование
- И т.д.



Cisco Security Ninja: все начинается с тренингов и повышения осведомленности



- Стимулирование изучения CSDL широким спектром сотрудников Cisco
- Система распознавания и мотивации сотрудников
- Применение практик CSDL в работе



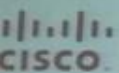


SecCon 2012

Security Briefings & Training



Is your code a bomb?...



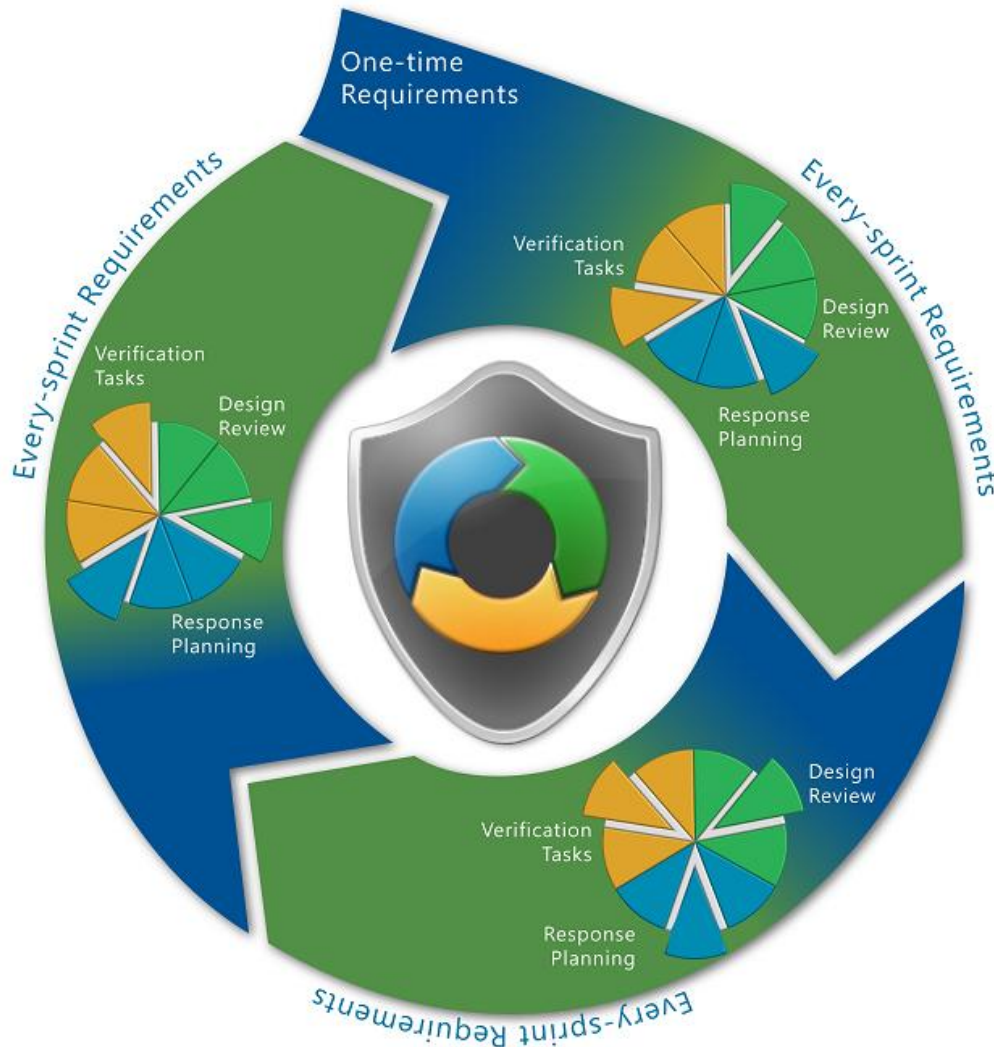
Microsoft Security Development Lifecycle (SDL) и Agile

- Цикл защиты
различные за
 - Тренинги
 - Анализ ри



- Моделирс
- Механизм
- Реагирова
- И т.д.

- Традиционн



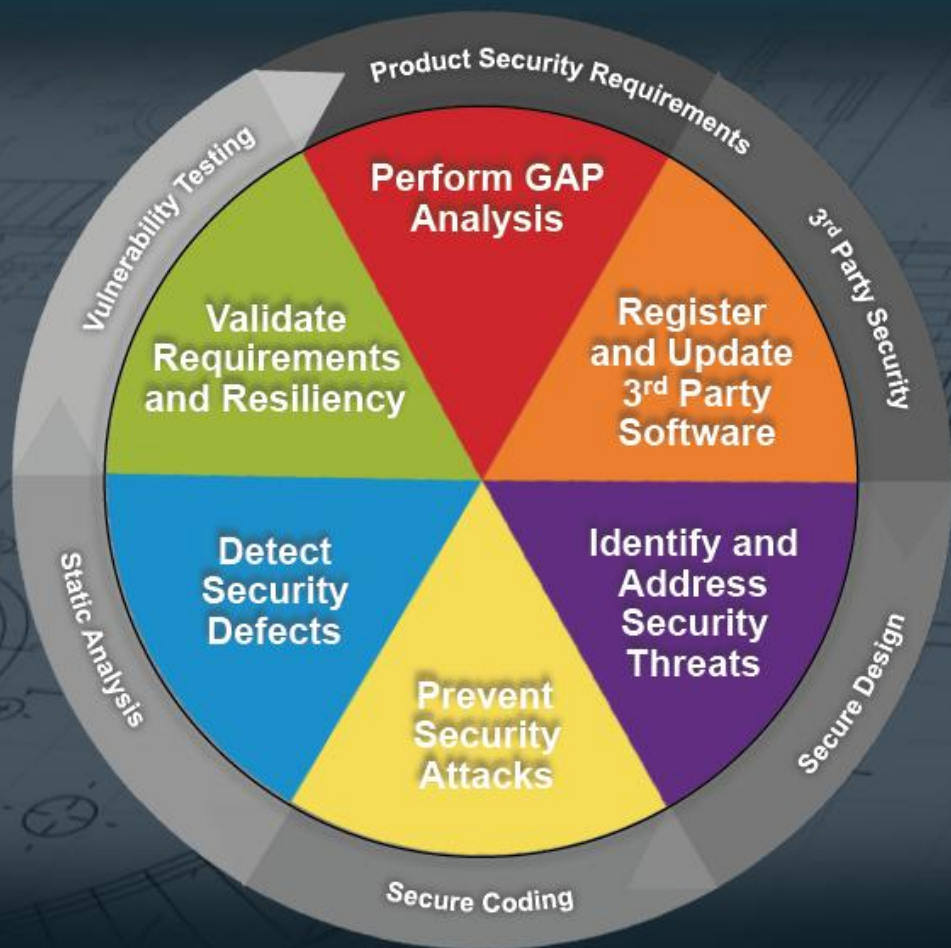
т в себя



ого)



Cisco Secure Development Lifecycle (CSDL)



EMC SDL

<i>SDL Standard</i>	<ul style="list-style-type: none">✓ <i>Training</i>✓ <i>Requirements</i>✓ <i>Threat modeling</i>	<ul style="list-style-type: none">✓ <i>Code scanning</i>✓ <i>Security testing</i>✓ <i>Documentation</i>	<ul style="list-style-type: none">✓ <i>Code signing</i>✓ <i>Assessment</i>✓ <i>Response</i>
---------------------	--	---	---

PRODUCT SECURITY POLICY

Secure Design

- ✓ *Authentication & access control*
- ✓ *Logging*
- ✓ *Network security*
- ✓ *Cryptography and key management*
- ✓ *Serviceability*
- ✓ *Secure design principles*

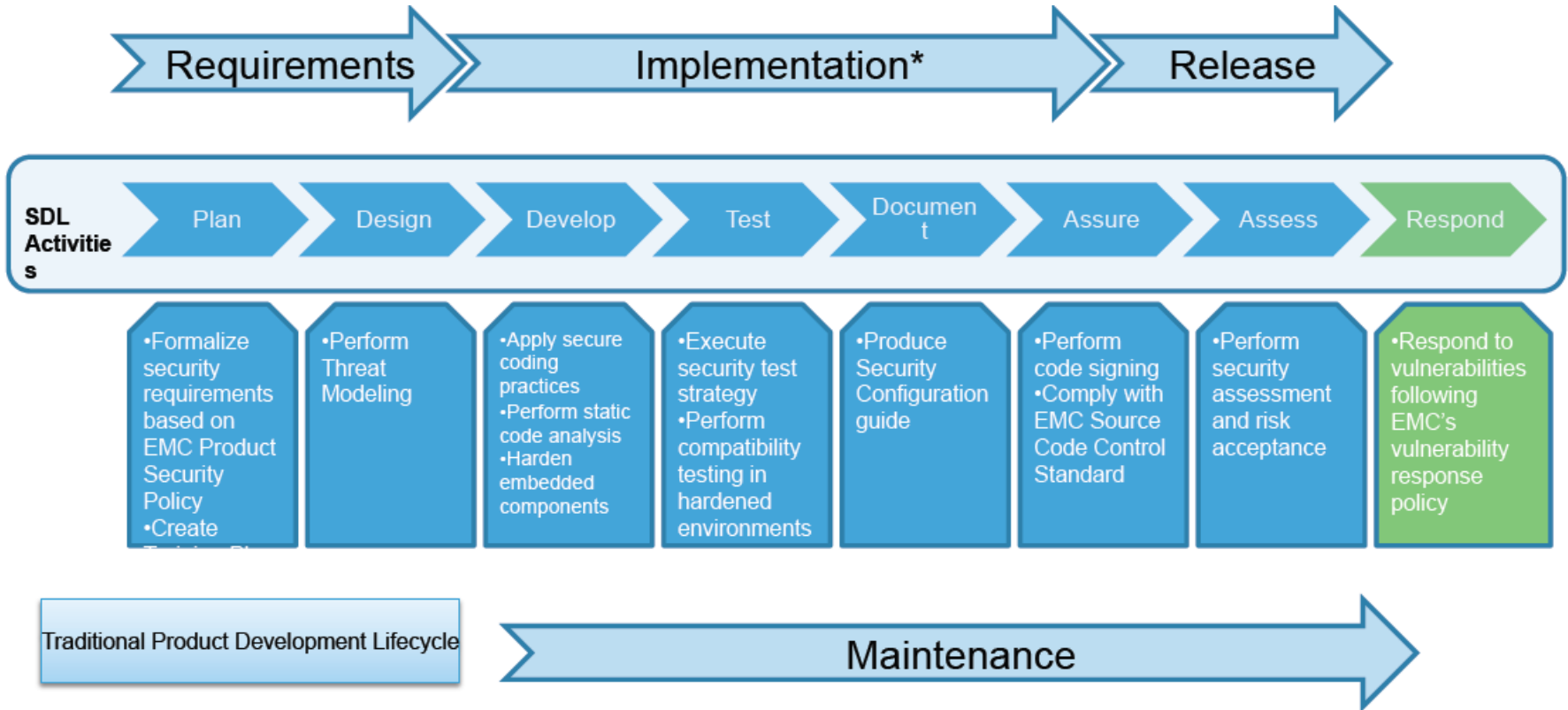
Secure Implementation

- ✓ *Input validation*
- ✓ *Injection protection*
- ✓ *Directory traversal protection*
- ✓ *Web and C/ C++ coding standards*
- ✓ *Code Signing*
- ✓ *Handling secrets*

Security Development Lifecycle



SDL разных компаний похожи между собой



Библиотека угроз при разработке ПО ускоряет время разработки

DFD element	Characteristic	Threat
User or administrator	Unauthenticated user	User impersonation
User or administrator	Privileged	Privilege abuse
Dataflow	Unauthenticated server	Server spoofing
Dataflow	Unauthenticated client	Client spoofing
Dataflow	Plaintext transmission of sensitive data over a network	Network sniffing
Dataflow	Transmission of authentication credentials	Replay attacks
Dataflow	Transmission of session identifiers or tokens	Session hijacking
Process	Generates password or encryption key	Predictable password or encryption key
Process	Uses cryptography	Attacks on cryptography
Process	Is written in C/C++	Buffer overflow
Process	Is written in C/C++ or perl	Uncontrolled format string
Process	Executes SQL queries using input data	SQL injection
Process	Executes LDAP queries using input data	LDAP injection
Process	Executes operating system commands (e.g. system(), exec(), open()) using input data	OS command injection
Process	Exposes a user web interface	Cross-site scripting
Process	Exposes a user web interface	Cross-site request forgery

Оценка рисков для каждой угрозы позволяет учесть приоритеты

Impact	
Does the attack allow unauthorized access to private or confidential information?	No
Can the attack be used to cause unauthorized changes to the system or external systems?	Yes
Can the attack be used to cause unauthenticated changes to the system or its data?	No
Can the attack be used to cause a permanent* denial of service?	Yes
Exploitability	
Can the attack be conducted through an unauthenticated interface?	Yes
Does the attack require a highly privileged** access role?	No
Can the attack be conducted remotely?	Yes
Does the attack require custom exploit code?	No
Does the attack require a special condition (e.g. an uncommon deployment or configuration, a race condition with a very limited window of exposure, etc)?	No
Does the attack require first compromising other components or external systems (e.g. DNS, routing, etc)?	Yes

CVSS score: 8.8
Risk: **CRITICAL**

Рекомендации по защищенному программированию

Security Development Lifecycle: Develop: **Secure Coding Reference**



This page contains links to detailed guidance to help software developers comply with

- Perform adequate input validation
- Prevent common injection issues
 - Preventing SQL injection
 - Preventing LDAP injection
 - Preventing command injection
 - XML injection
- Preventing directory traversal
- Web coding standards
 - Preventing cross site scripting (XSS)
 - Preventing HTTP response splitting
 - Cross-site request forgery (XSRF)
 - Clickjacking
 - Preventing session fixation
 - Securing cookies
 - Securing sensitive web data
- C/C++ coding
 - Preventing buffer overflows
 - Avoiding unsafe functions
 - Safely using Printf/scanf
 - Compiler settings
- Memory hardening (see [compiler settings](#))
- Embedded components
 - Embedded component patching
 - Embedded component hardening
- Handling sensitive data

There are a few simple ways to limit the risk of security vulnerabilities in source code susceptible to Buffer Overflows.

Contents [hide]	
1	What is a Buffer Overflow?
2	Preventing or limiting buffer overflows
2.1	BEST: Avoid unchecked buffers
2.1.1	Proper bounds checking
2.1.2	Use safe functions and data structures
3	See Also

What is a Buffer Overflow?

A Buffer Overflow occurs when an application defines a buffer of a fixed or loosely-controlled length, and data is copied in the program's address space at the buffer location in memory, potentially overwriting critical data, registers, and if the application crash), code or command injection, and arbitrary code execution. The severity of a buffer overflow attack may SYSTEM or root contains an exploitable buffer overflow, then an attacker may gain control of the host by injecting shellcode [more details...](#)

Preventing or limiting buffer overflows

BEST: Avoid unchecked buffers

The most effective method for limiting the effectiveness and risk from buffer overflows is to avoid them altogether by ensuring steps are taken to ensure data being written does not overflow the buffer.

Proper bounds checking

- Make sure that buffer writes are limited to the length of the buffer by checking the incoming data carefully. Understand and set defaults accordingly. For example, if you are writing code to read file names, be aware of the file system limit multi-byte characters (and remember to double or triple all upper bounds accordingly).

Use safe functions and data structures

- Avoid allocating fixed-length buffers. Instead, if the language supports them, consider using self-sizing array types or

Рекомендации по тестированию ПО

Using the Security Test Library

The Security Test Library is a resource to assist product testing engineers to identify and specify security test cases that are required to ensure products do not ship with vulnerabilities. The Security Test Library (STL) should be used in the following manner:

1. Understand and document the architecture of the product under test. The PSO can assist in this activity, and is working on making tools available to make this easier.
2. (Optional, but highly recommended) Use the architecture information to create a **Threat Model**, which highlights risk in the product based on certain functionality.
3. Using the architectural information and/or Threat Model, identify the test procedures from the lists below that apply to the product.
4. Use the identified security test procedures to create security test cases to execute during the product testing cycle.

A couple of things to keep in mind:

- Each test procedure below describes recommended and generic methods for testing for each vulnerability type. Certain test procedures may suggest other testing methods beyond the scope of the particular test procedure.
- Test procedures are designed to be repeatable for like inputs. For example, the test procedure for **malware scanning** indicates the test should be run "for each product module" and should be created, each following the same procedure for each module in the product.

STEP 0 - Known Vulnerability Detection

Product Characteristics (for Test Applicability)	Test Procedure
Product ships binary packages (on any media or downloadable)	Testing for malware (Binary Image)
Product embeds an appliance system image	Testing for malware (Appliance Image)
Product or components the product embeds open network services	Security vulnerability scanning
Product has a web interface and/or embeds a web server	Security vulnerability scanning
Product will be deployed in a US/non-US government facility	Testing in hardened environments

STEP 1 - Basic Security Testing

Product Characteristics (for Test Applicability)	Test Procedure
Product performs database operations and allows externally-controlled input, or embeds a database server	Testing for SQL injection
Product performs user authentication using LDAP or AD	Testing for LDAP injection
Product contains CLIs, or executes system-level commands and allows externally-controlled input	Testing for command injection
Product uses XML-based communication protocols or accesses XML-encoded data (from files or the network, etc)	Testing for XML injection
Product uses a web interface (HTML, Javascript, Flash) and/or embeds a web server serving static or dynamic content	Web security
Product uses a web interface (HTML, Javascript, Flash) and/or embeds a web server serving static or dynamic content	Testing for cross site scripting (XSS)

Как тестировать?



Чем проверять: десятки различных инструментов

- Статический анализ
 - FxCop
 - CAT.NET
 - PReFast
- Динамический анализ
 - Различные fuzzer'ы
 - AppVerifier
- Библиотеки для защищенного программирования
 - StrSafe
 - SafeInt
 - AntiXss



Как оценить результаты тестирования ПО?

TEST CASE: Testing for Malware (Appliance Image) [\[edit\]](#)

Test Characteristics [\[edit\]](#)

- Applicable PSP (v3.0): 1.2.3.3
- Applicable CWE(s): CWE-506 Embedded Malicious Code
- STEP: 0 - Known vulnerability detection
- Objective: Perform a scan of a running master system image for an appliance to identify malware (spyware, trojan horses, backdoors, rootkits, or viruses).
- Long description: Using platform-appropriate malware scanning tools, identify if a system image for an EMC product, before being released to manufacturing or customers (and then duplicated to customer environments) contains malware such as viruses, trojan horses, worms, rootkits, or spyware.
- Test Applicability: This test case applies to any product that is released to customers (internal or external). This test case applies to each product appliance system images.

Architectural Representation/DFD [\[edit\]](#)

Not Applicable

Testing Procedure [\[edit\]](#)

Step	Action	Outcome
Pre-test Setup	Install the product system image under test in a lab environment.	[SUCCESS] The product is installed and configured in a lab environment.
Pre-test Setup	Configure the product system image under test to match an appropriate customer-targeted release configuration.	[SUCCESS] The product is configured as a customer may install and operate it.
Pre-test Setup	Select and download appropriate malware scanning tool(s), selected from the tools below (see Resources). Install each tool in the test system image. Update malware definition rules.	[SUCCESS] The malware and rootkit scanning tools are installed on the system image, with latest malware definitions available.
1	Run the malware scanning tool on the system image using the most aggressive settings possible (with hueristics to find new malware, etc) and with all logging enabled. Cleaning any infections are not required at this time.	[SUCCESS] Malware scanner identifies 0 infections on the system image. [FAILURE] Malware scanner detects one or more infections. Note the infected files and which malware infected them for follow up.
2	Run the rootkit scanning tool on the system image using the most aggressive settings possible (with hueristics to find new malware, etc) and with all logging enabled. Cleaning any infections are not required at this time.	[SUCCESS] Rootkit scanner identifies 0 infections on the system image. [FAILURE] Rootkit scanner detects one or more infections. Note the rootkit names and locations for follow up.
Post-Test Data Gathering	For each malware infection finding collect infected file names and the malware that infected them, or for rootkits the name and location of the rootkit.	[SUCCESS] List of infections and rootkits identified, if any.
Reporting Defects	If a defect is discovered using the above Procedure, file a defect ticket that includes the Title of the test case and/or Case ID and the list of infections as noted above. File the defect ticket with Critical/Must-fix severity.	[SUCCESS] Any identified defect is recorded and classified appropriately.

Уровни зрелости обеспечения качества ПО

Активности в зависимости от уровня зрелости	Реактивный	Проактивный	Интегрированный	Оптимальный
Identify Product Security liaisons	+	+	+	+
Pre-GA Risk Assessment		+	+	+
Security Alert Tracking		+	+	+
Vulnerability Scanning		+	+	+
Full Engineering training			+	+
Threat Modeling @ Design			+	+
Source Code Analysis			+	+
Security Testing against Product Security Standard			+	+
Supply Chain Protection				+
Independent Penetration Testing				+

А ЧТО В РОССИИ?



Российские требования по анализу качества кода: финансовые организации

- Также документация на разрабатываемые АБС или приобретаемые готовые АБС и их компоненты должна содержать описание реализованных защитных мер, принятых разработчиком относительно безопасности разработки и безопасности поставки
 - 7.3.5 СТО БР ИББС 1.0
- Разделы 6.3, 6.5 и 6.6 PCI DSS, посвященные проверке качества кода, безопасной разработке и регулярному тестированию ПО на предмет требований стандарта PCI DSS и других лучших практик
- Стандарт PA DSS полностью посвящен вопросам разработки платежных приложений
 - Особенно раздел 5
- РС «Требования к банковским приложениям и разработчикам банковских приложений» (**план**)

Постановление Правительства №1119

- Угрозы 1-го типа актуальны для информационной системы персональных данных, если для нее, в том числе, актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в **системном** программном обеспечении, используемом в составе информационной системы персональных данных
- Угрозы 2-го типа актуальны для информационной системы персональных данных, если для нее, в том числе, актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в **прикладном** программном обеспечении, используемом в составе информационной системы персональных данных
- Угрозы 3-го типа актуальны для информационной системы персональных данных, если для нее не актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в составе информационной системы персональных

данных

Российские требования по анализу качества кода: персональные данные

- В случае определения в качестве актуальных угроз безопасности персональных данных 1-го и 2-го типов дополнительно к мерам по обеспечению безопасности персональных данных могут применяться следующие меры
 - Проверка системного и (или) прикладного программного обеспечения, включая программный код, на отсутствие недеklarированных возможностей с использованием автоматизированных средств и (или) без использования таковых;
 - Тестирование информационной системы на проникновения
 - Использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования



Дополнительная информация

- «Build Security In»
 - <https://buildsecurityin.us-cert.gov/>
- Институт Карнеги-Меллона
 - <https://www.cert.org/secure-coding/>
- Software Assurance Marketplace (SWAMP)
 - <http://swamp.cosalab.org/index.html>



The screenshot shows the homepage of the Build Security In website. At the top left is the Homeland Security logo with the text "Homeland Security" and "Privacy and Use" below it. To the right is the site title "Build Security In" with the tagline "Setting a higher standard for software assurance" and "Sponsored by DHS Office of Cybersecurity and Communications". A search bar is located in the top right corner. Below the header is a navigation menu with "Actions" and "Navigational Links". The main content area is divided into three columns. The left column contains a "Home" section with links to "Mission", "Articles [by Content Area]", "Events", "About Us", "FAQs", "Secure Coding Sites", "Additional Resources", "DHS SwA Web Site", "DHS Software Assurance Resources", "RSS Feeds", and "Contact Us". The middle column features "Build Security In Home" and "What is Build Security In?", which describes the collaborative effort and provides links to "Introduction to Software Security" and "The Software Assurance Curriculum Project". The right column highlights "Improve Security and Software Assurance: Tackle the CWE Top 25 Most Dangerous Software Errors" and "What's New", including information about the Spring 2013 Software Assurance Forum and the Winter 2012 Software Assurance Working Group Sessions.

security-request@cisco.com

Благодарю вас
за внимание

