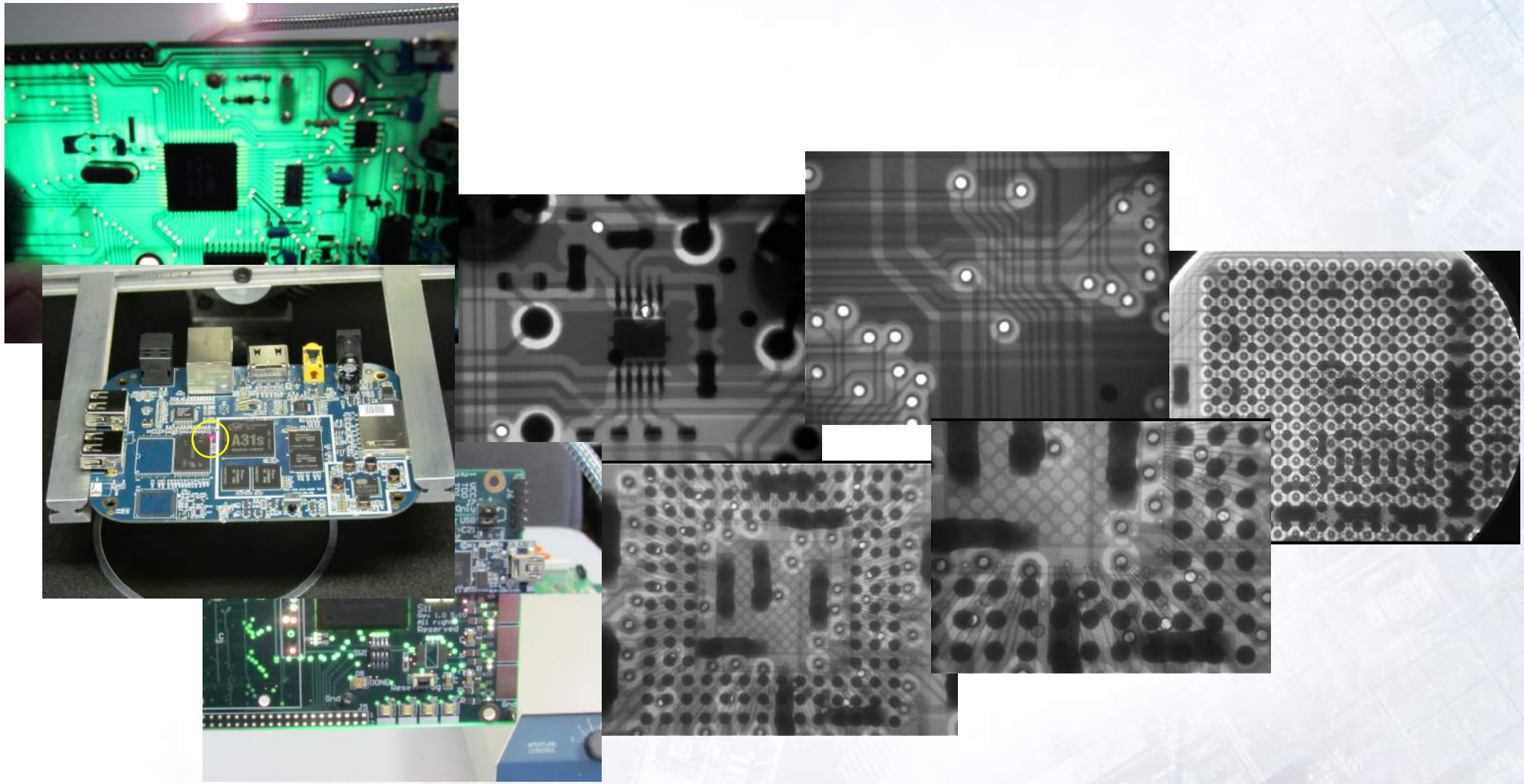
Проблемы безопасной разработки и поддержки импортных средств защиты информации

Алексей Лукацкий
Бизнес-консультант по безопасности

8 февраля 2017

Мы оставим за рамками вопросы железа



cisco

ГОСТ по безопасной разработке ПО

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56939—2016

Защита информации

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Общие требования

Издание официальное

Москва
Стандартинформ
2016

Дата введения – 1.06.2017

Устанавливает

общие требования к содержанию и порядку выполнения работ, связанных с созданием безопасного (защищенного) программного обеспечения и формированием (поддержанием) среды обеспечения оперативного устранения выявленных пользователями ошибок программного обеспечения и уязвимостей программы

Два набора мероприятий

Предотвращение

появления уязвимостей программного обеспечения

Устранение

выявленных пользователями уязвимостей программного обеспечения

Имеет свою специфику для импортных средств защиты информации в России

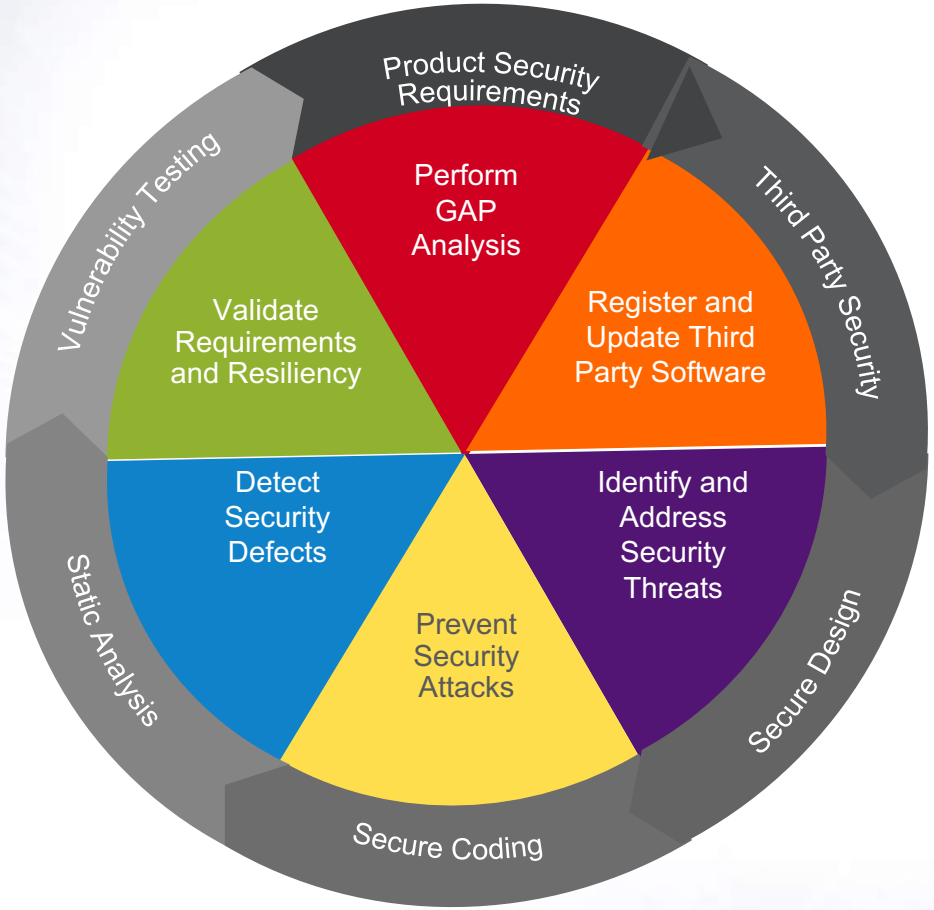
ГОСТ: Реализация ПО

4 процесса

- Анализ требований
- Проектирование архитектуры
- Конструирование
- Квалификационное тестирование

cisco

Cisco Secure Development Lifecycle



Обеспечение непрерывной безопасности продуктов через проверенные методы и технологии, позволяющие снизить количество и серьезность уязвимостей в программном обеспечении

Соответствует ISO 27034

Процесс разработки сертифицирован на соответствие ISO 27001

Для облаков все тоже самое

Product Security Baseline (PSB)

Определение требований к ПО

Архитектура PSB

- Administrative Access Security
- Application Security
- Authentication and Authorization
- Boot and System Integrity
- Cryptographic Support
- Development Process
- Hosted Services Hardening
- Logging and Auditing
- Operational Process
- Privacy and Data Security
- Session Management
- Threat Surface Reduction
- Traffic and Protocol Protection
- Vulnerability Management
- Web Security

Продукты третьих фирм

Минимизация воздействия за счет

- Обеспечение анализа требований
- Утверждение плана поддержки
- Проверка отсутствия НДВ
- Устранение известных уязвимостей до FCS

Управление алертами

- Регистрация компонентов в центральной БД
- Поддержка по контракту для критических дыр

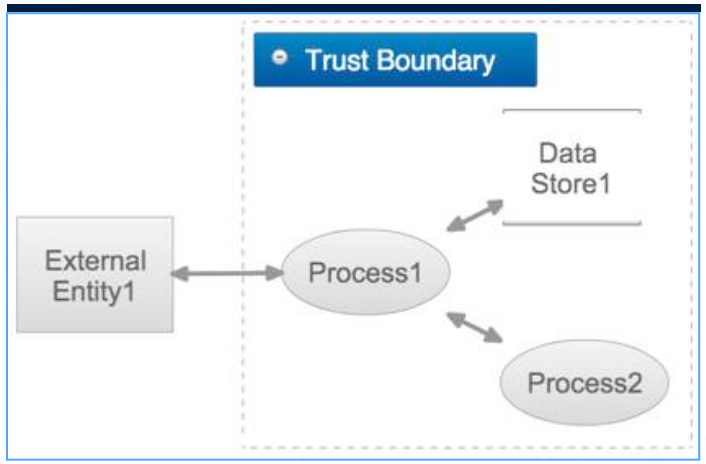
Реагирование на обнаруженные проблемы

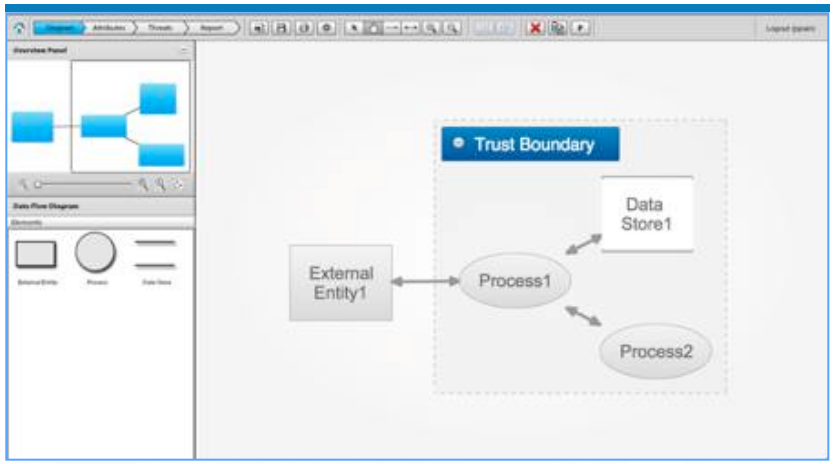
- Следовать установленному плану поддержки

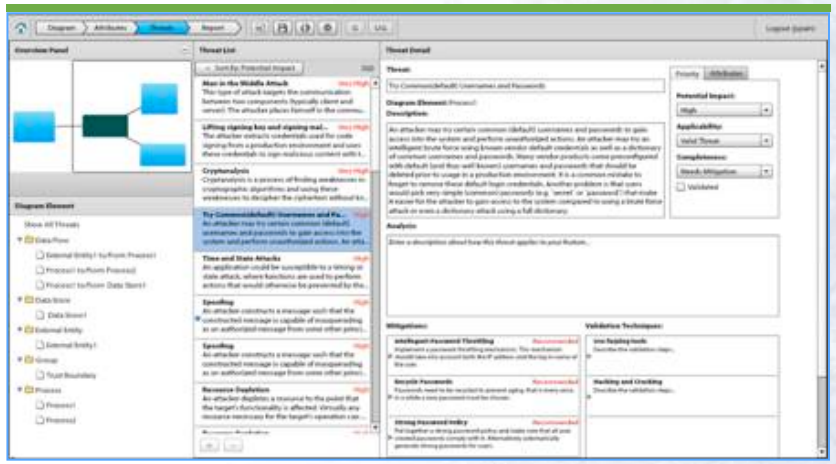
Защищенная архитектура

Моделирование угроз

Фокусировка на том, какие функции могут быть атакованы и как лучше всего нейтрализовать атаку

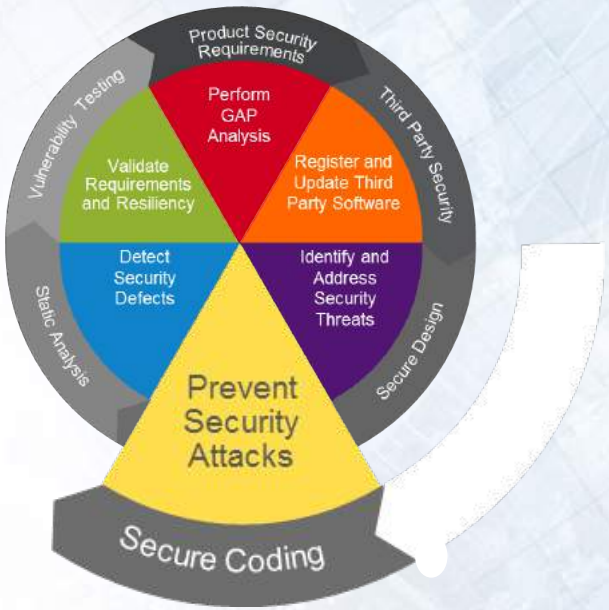






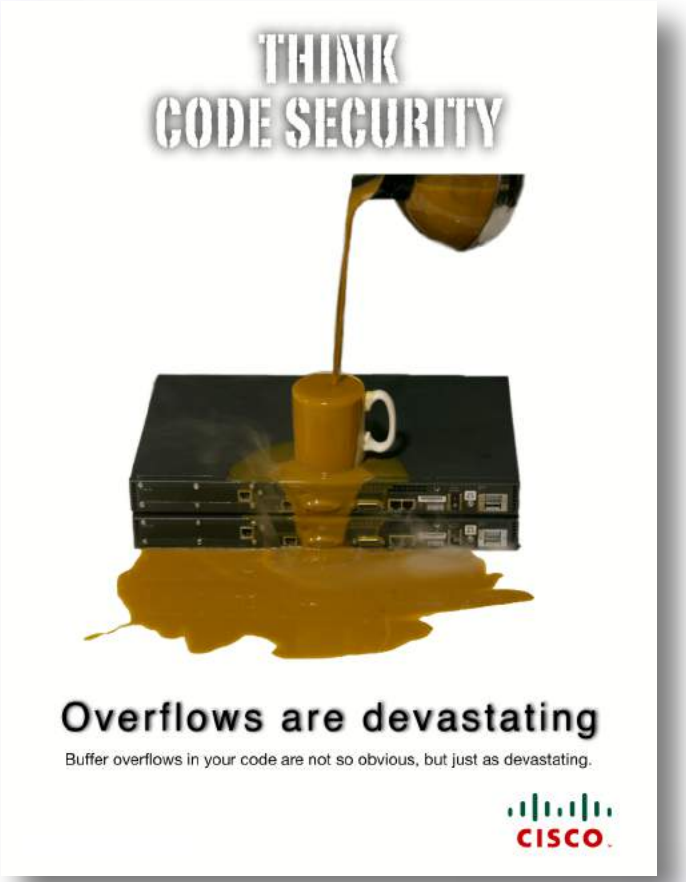
Cisco ThreatBuilder

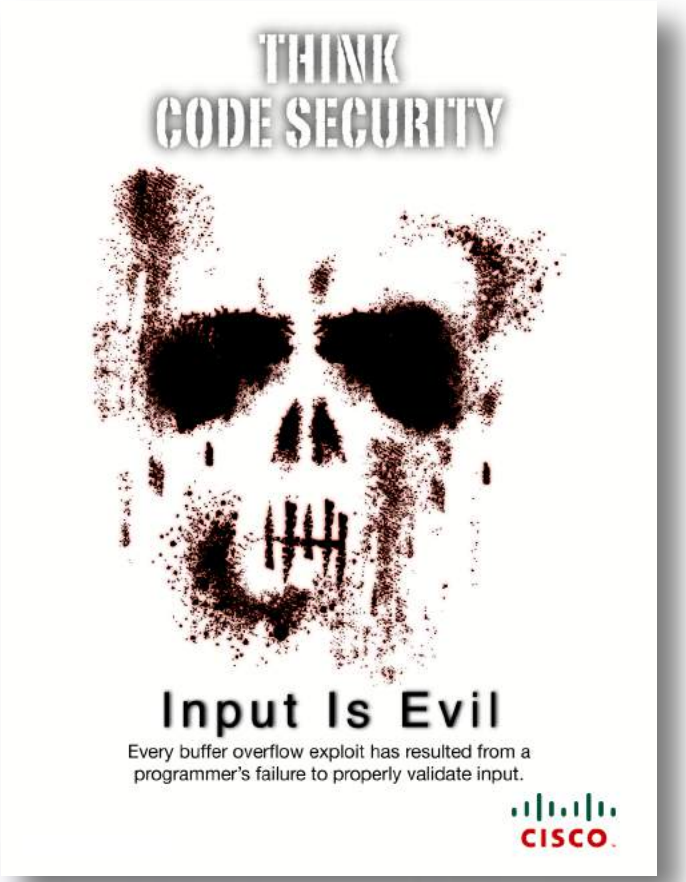
Безопасное программирование



- Контроль целостности в процессе загрузки и защита в процессе исполнения
  - ASLR
  - X-Space
  - OSC
- “Безопасные” библиотеки
- Проверка ввода
- Руководства и лучшие практики для каждой ОС
- Подписанные образы ПО

Плакаты в местах разработки

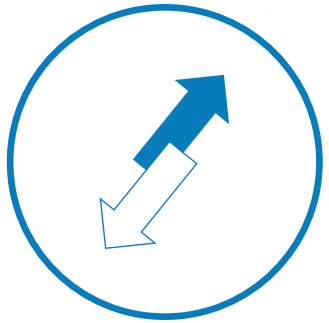




Статический анализ

Security Checkers ищут ключевые типы уязвимостей

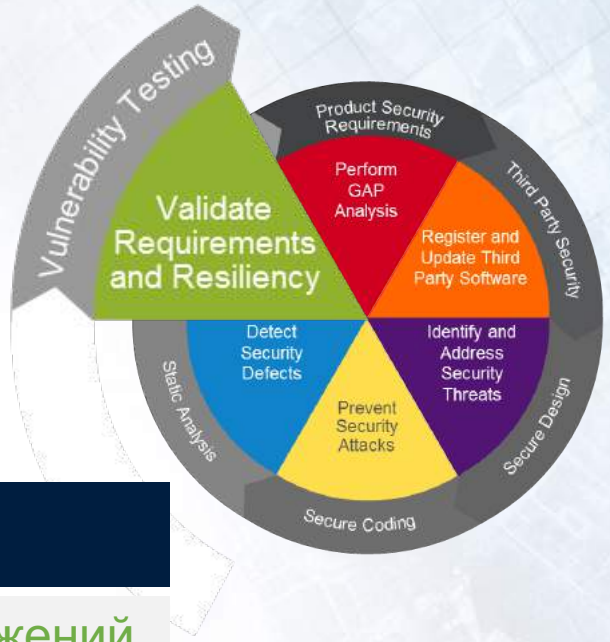
- Переполнение буфера
- Некорректный ввод
- Целочисленное переполнение



Уменьшение числа ложных срабатываний и максимизация эффективности

Тестирование на уязвимости

Проверка протоколов на прочность
Дублирование хакерских атак



Тестирование безопасности по CSDL

Тестирование сетевых устройств

Codenomicon Protocol Robustness

Наборы тестов для 50+ протоколов, включая: DNS, H.323, IKEv2, IPv4, IPv6, HTTP, SIP, SNMP, SSH, TLS и многие другие

Open Source “Hacker” Tools

20+ Open Source инструментов ИБ, включая: Amap, Curl, Dsniff, Hydra, Naptha, Nessus, Nikto, Nmap, Xprobe и многие другие

Тестирование приложений

IBM Rational AppScan

Семейство инструментов для тестирования и проверки атак на приложения, включая: анализ рисков, тестирование на соответствие стандартам, сканирования уязвимостей и многое другое

Наши инвестиции в безопасность

70,000+ сотрудников — подписали Code of Conduct

14, 230 — Политик ИБ и защиты данных, аудитов

150+ — Продуктовых линеек Cisco с Trustworthy Technologies

80+ Red Team
20 НИОКР в 5 странах

175+ — международных сертификаций

900+ — Security Advocates

100+ — Incident Responders

35K+ — Security Ninjas

- Обязательный Secure Development Lifecycle
- Программа Value Chain Security
- Программа защиты данных

Мы пришли к этому не сразу

1995-2003

Routers/Switches

- Login Credentials
- Access Lists
- Encryption

PSIRT

Common Criteria

FIPs

2003-2007

Anti-Counterfeiting Chip

Image Signing

Secure Functions Baseline

Security Testing

2008-2009

1st Product Security Baseline

Cisco Secure Development Lifecycle (CSDL) Released

1st SecCon

2010-2012

Threat Modeling

Secure Boot

3rd Party Security

1st Run Time Defenses (ASLR/XSpace/OSC)

Cisco NextGen Encryption

Hardware based Trust Anchor

Security Advocates

2013-2014

Security Ninja Training

Enrollment over Secure Transport

CSDL Mandate

Security Engagement Managers

2015 -

- Cyber Resilient System Architecture
- Cloud Tenant Hardening
- BIOS Protection
- JTAG Monitoring

И постоянно совершенствуемся

2015

2010

2005

2000

G1

Cisco 1800

Cisco 2800

Cisco 3800

ISR

Anti-Counterfeiting (ACT)
Common Criteria
FIPs

G2

800 Series

3900 Series

3900(E)

1900 Series

Anti-Counterfeiting (ACT)
39[24]5 PPC (XSPACE, ASLR)
MIPs based G2 – Partial ASLR
39[24]5e Intel (XSPACE)
Image Signing
Common Criteria + НДВ ФСТЭК
FIPs

G3

ISR 4451-X

CSDL
Trust Anchor Module
(SUDI, Secure Storage,
Entropy)
Secure Boot,
Image Signing,
XSPACE.
ASLR enabled IOSd
Cisco SSL
Common Criteria, FIPs

ГОСТ: Организационное обеспечение

2 процесса

- Менеджмент инфраструктуры среды разработки ПО
- Менеджмент персонала

- **Защита элементов конфигурации**
- **Резервное копирование элементов конфигурации**
- **Регистрация событий**

- **Периодическое обучение сотрудников**
- **Периодический анализ программы обучения**

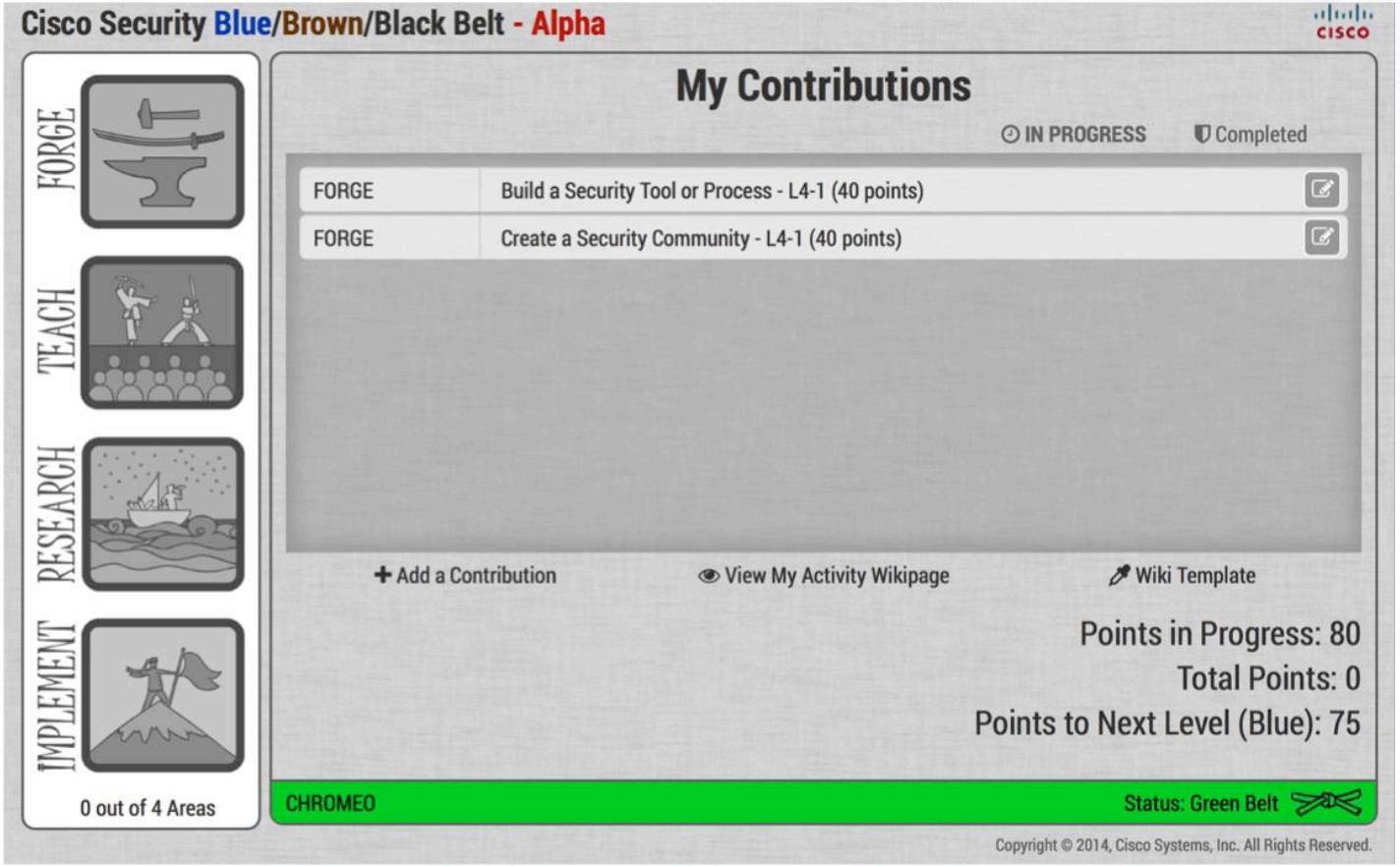
cisco

Внутренняя конференция Cisco SecCon

Программа Cisco Security Ninja

cisco

Программа Cisco Security Ninja



CISCO

ГОСТ: Поддержка ПО

2 процесса

- Менеджмент документации и конфигурации
- Решение проблем ПО в процессе эксплуатации

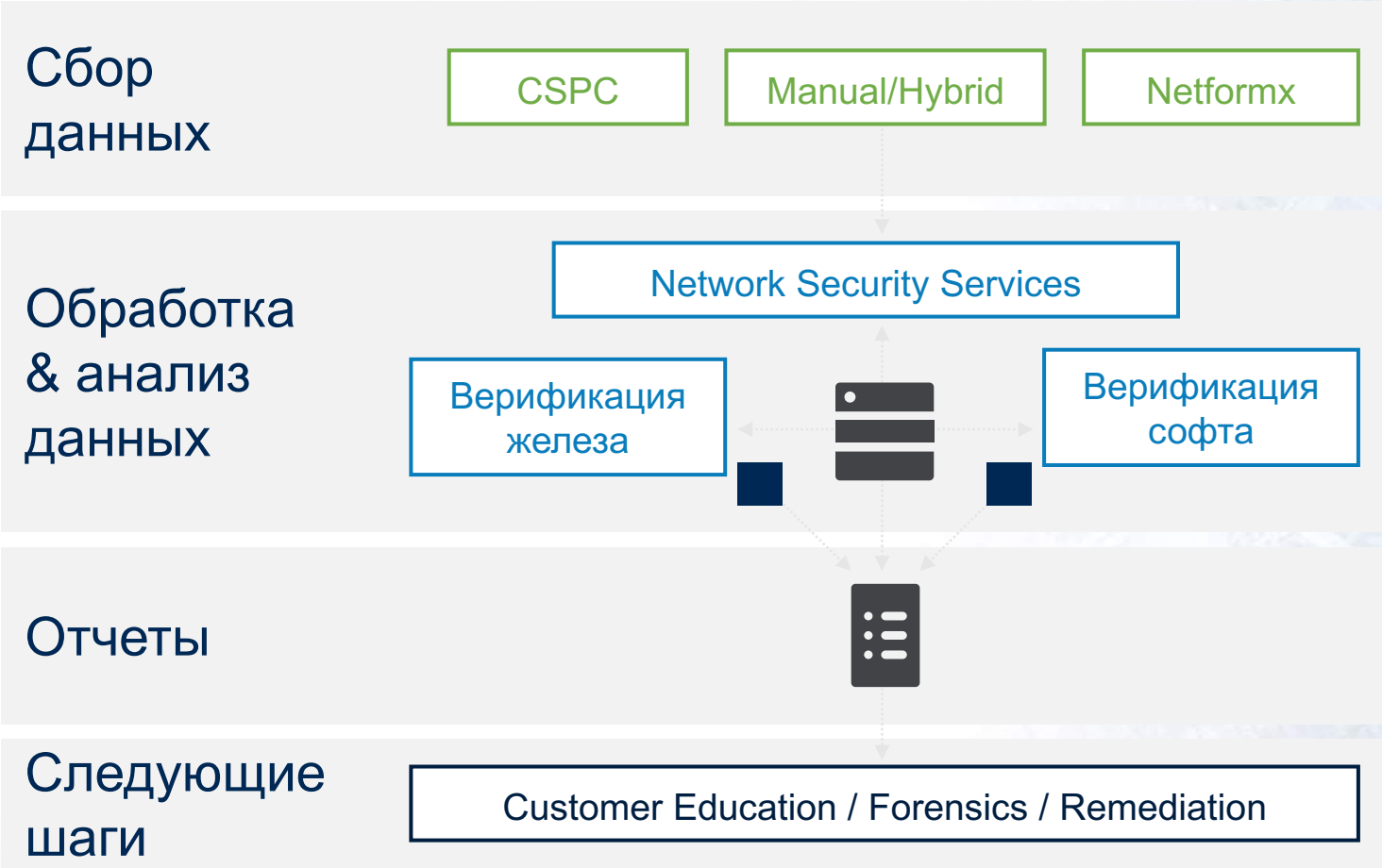
- **Маркировка каждой версии ПО**
- **Система управления конфигурацией**

- **Исправление обнаруженных уязвимостей**
- **Систематический поиск уязвимостей**

Удаленный мониторинг целостности устройств

Службы верификации целостности

Снижают риски, идентифицируя контрафактное оборудование, неавторизованные продукты и подмененное ПО на устройствах с Cisco IOS



А как выстроены процессы CSDL в России?

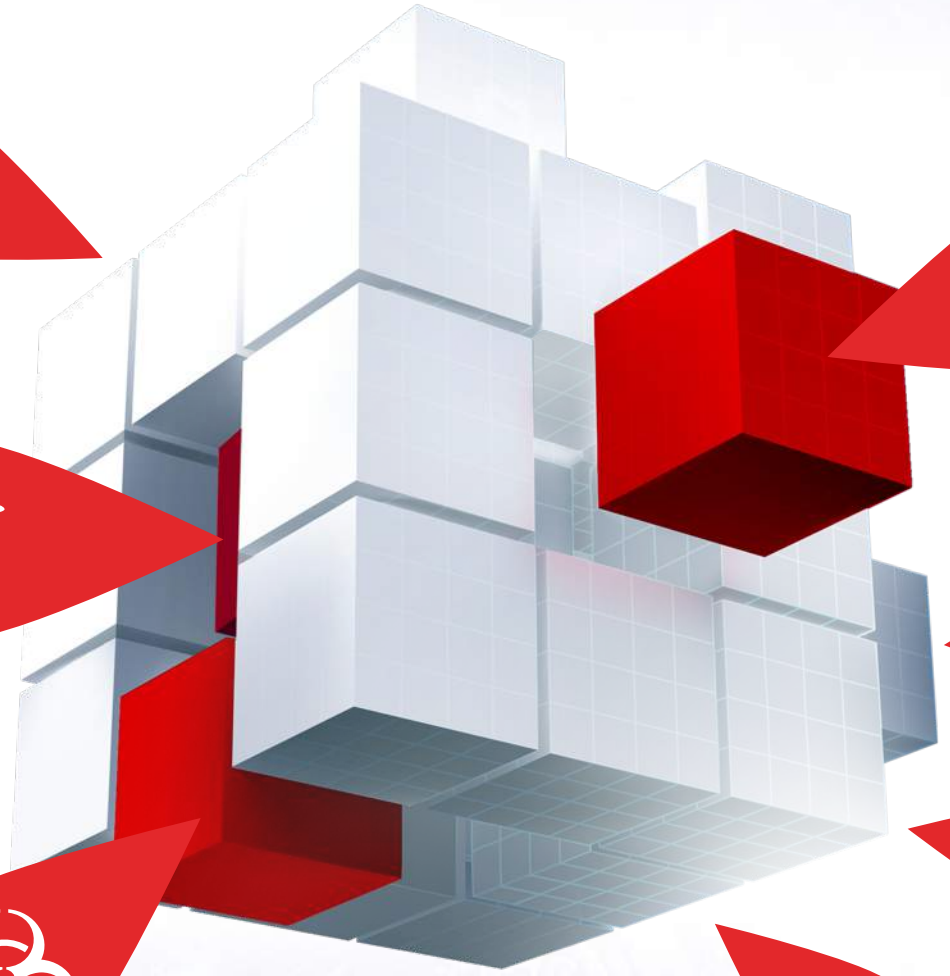
cisco

На этом можно было бы и закончить

«Их практика работы направлена на то, чтобы шантажировать заказчика и покупателя. Они вывешивают в открытом доступе систему своих уязвимостей и говорят — коллеги, если вы хотите, чтобы эти уязвимости не были использованы, заплатите нам за поддержку и мы их устраним»

Помощник президента России Игорь Щеголев

Что влияет на процессы CSDL в России?



Бизнес-процессы производителя

Законодательство о лицензировании

Российские исследователи

Требования к средствам защиты

Вассенаарские соглашения

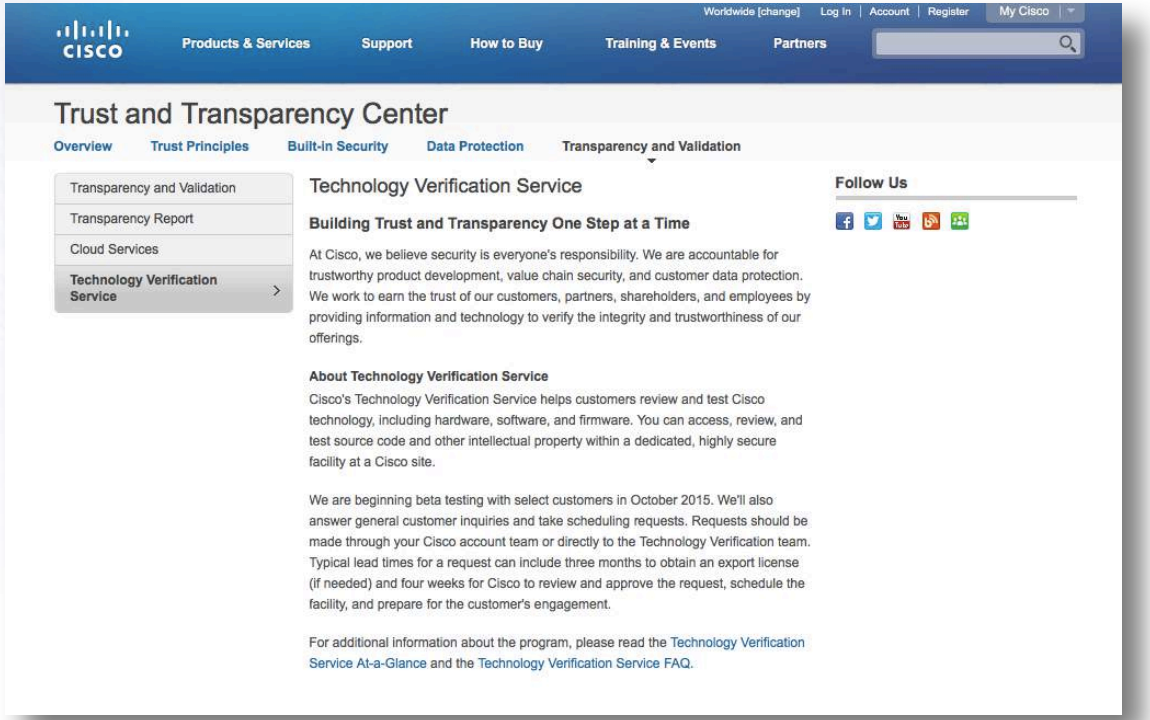
Требования отсутствия НДВ

Геополитика

Требования к заявителям

CISCO

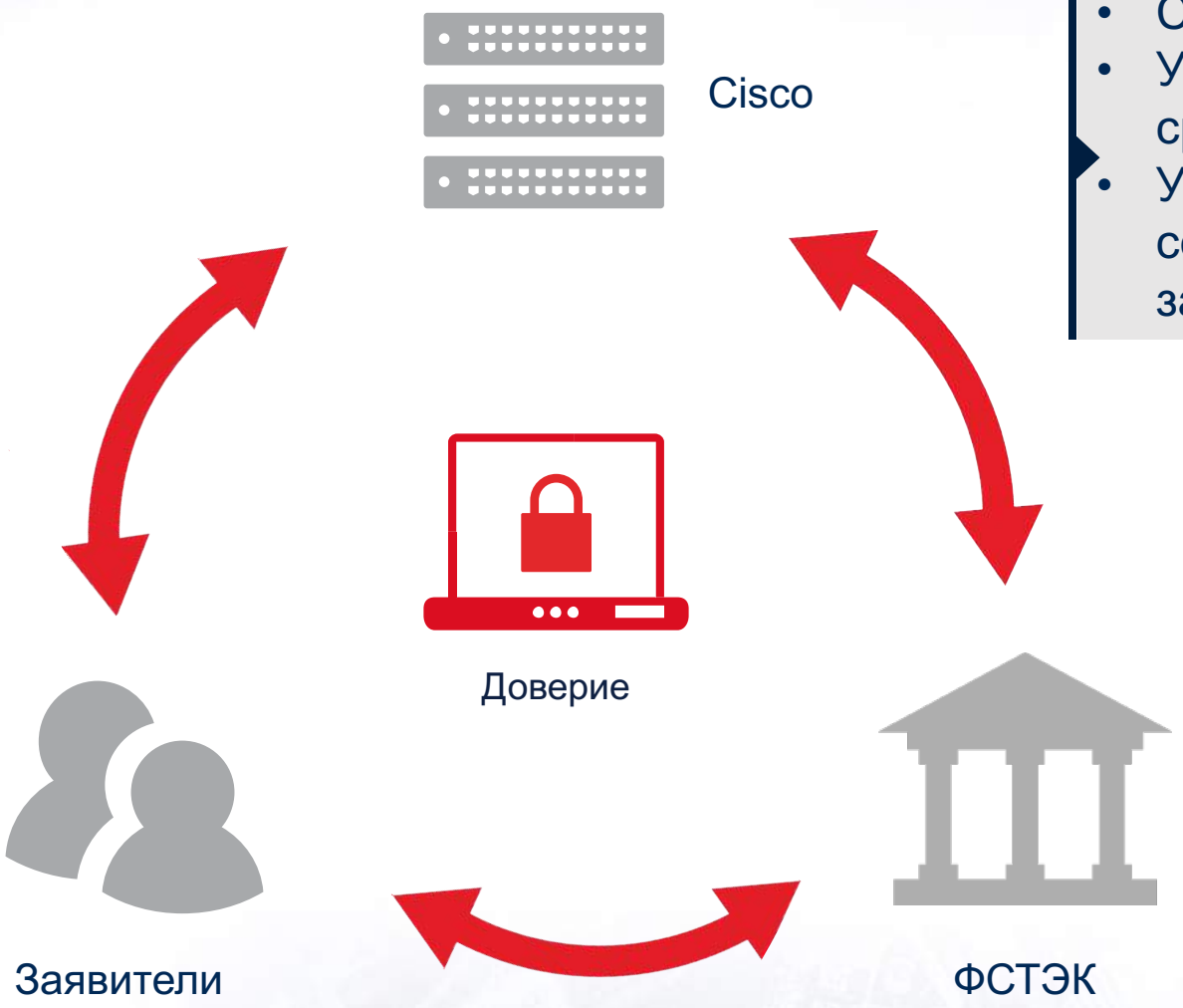
Cisco Technology Verification Service



Сервис, помогающий заказчикам проверять и тестировать технологии Cisco, включая железо и ПО

Запущен в октябре 2015 года

Что мы делаем в России?



- Сертификация средств защиты
- Устранение уязвимостей в средствах защиты
- Устранение уязвимостей в сертифицированных средствах защиты

Кто сертифицирует импортные средства защиты?

6 заявителей

САТЕЛ	С-ТЕРРА	ИТБ
АМТ	ЭЛВИС+	БИТК

ПО для сертификации публикуется на сайте Cisco для указанных учетных записей представителей заявителей

cisco

Требования Cisco к заявителям

- Наличие контактного лица/группы для получения уведомлений
- Наличие тестового оборудования при проведения тестирования ПО с исправленными уязвимостями
- Уведомление потребителей (пользователей) об обнаруженных уязвимостях и методах их устранений
- Согласованный процесс взаимодействия с испытательными лабораториями для оперативного проведения инспекционного контроля
- Согласованный процесс взаимодействия с ФСТЭК России для оперативного внесения уточнений в сертификаты после устранения уязвимости(ей)

cisco

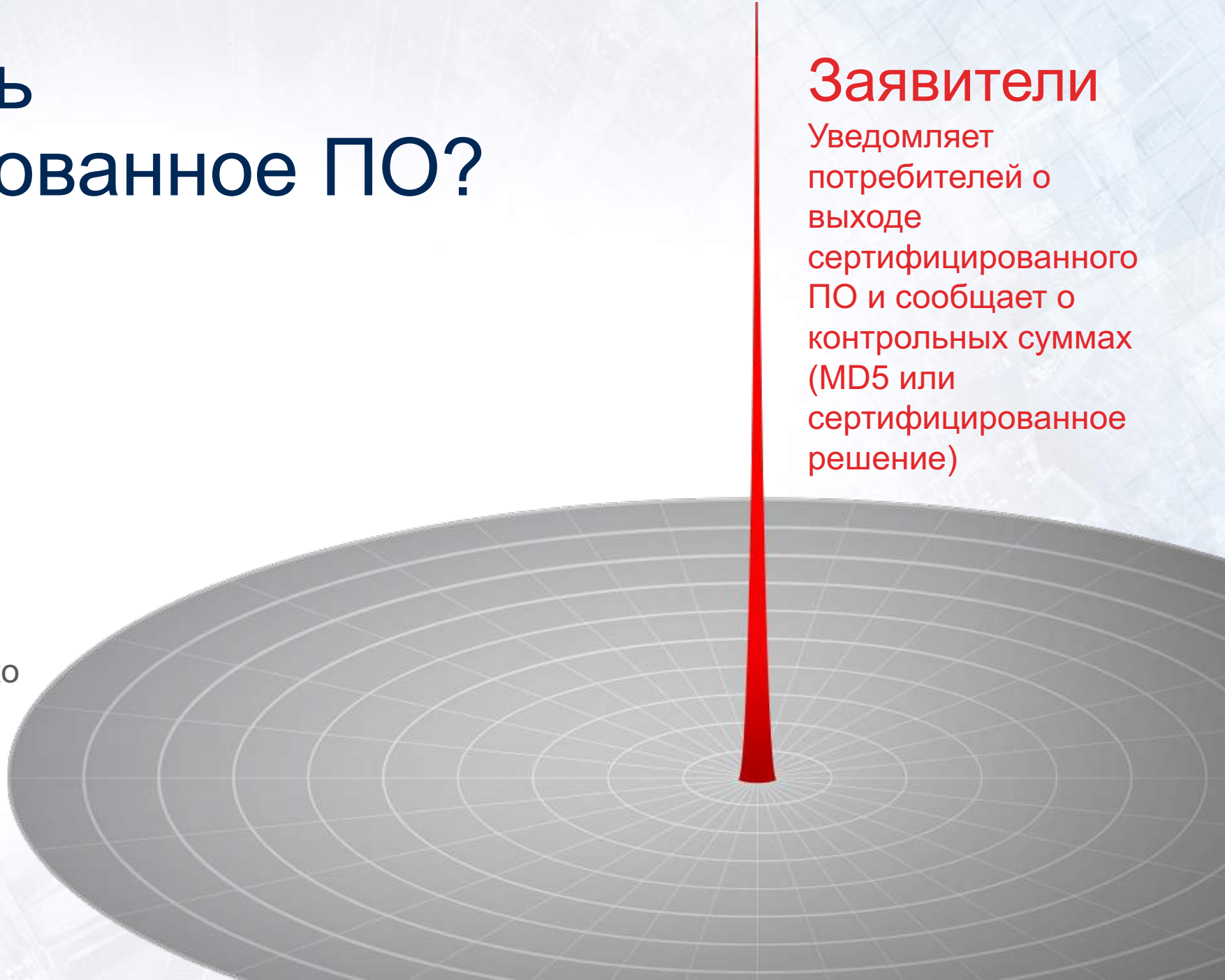
Откуда брать сертифицированное ПО?

Заявители

Уведомляет потребителей о выходе сертифицированного ПО и сообщает о контрольных суммах (MD5 или сертифицированное решение)

Cisco

Все ПО получается только с официального сайта компании Cisco



Другие вопросы

Сертификат за деньги?
Да. Деньги получает не Cisco, а заявитель/ испытательная лаборатория

Все релизы?
Мы сертифицируем не все релизы ПО (как правило, мажорные). Это не касается вопросов устранения уязвимостей

Что с НДВ?
Сертификат на маршрутизаторы Cisco ISR 2911R. В перспективе другие линейки

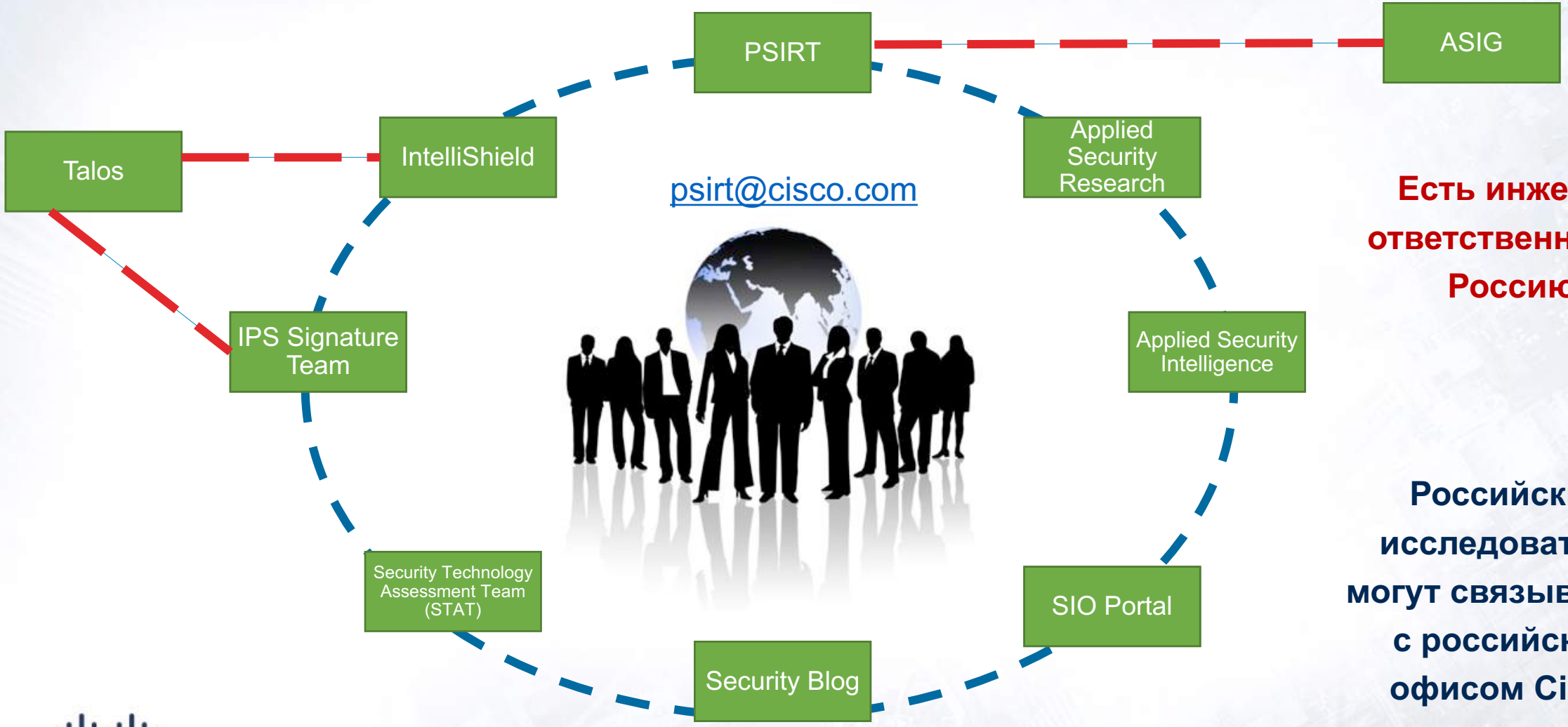
Обнаружение уязвимостей

Уязвимость обнаруживается российскими исследователями, например, ГНИИ ПТЗИ

Уязвимость обнаруживается Cisco или иными лицами за пределами России

cisco

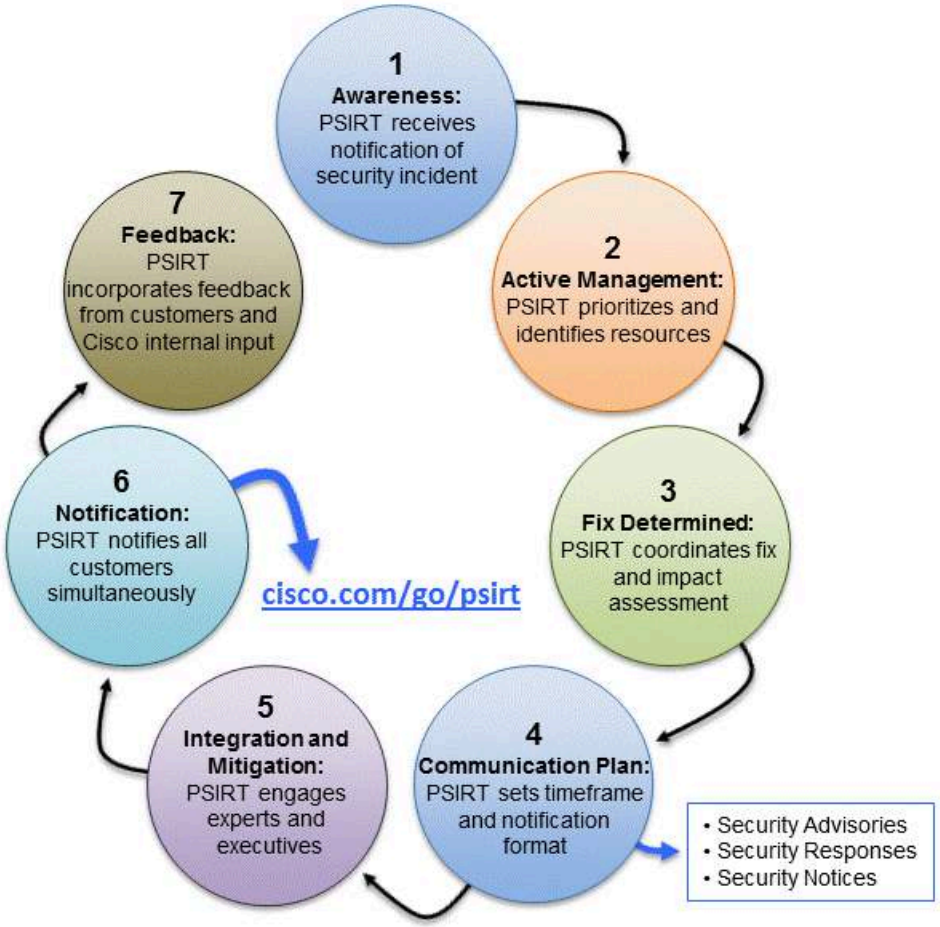
PSIRT – единая точка контакта



Есть инженер, ответственный за Россию!

Российские исследователи могут связываться с российским офисом Cisco

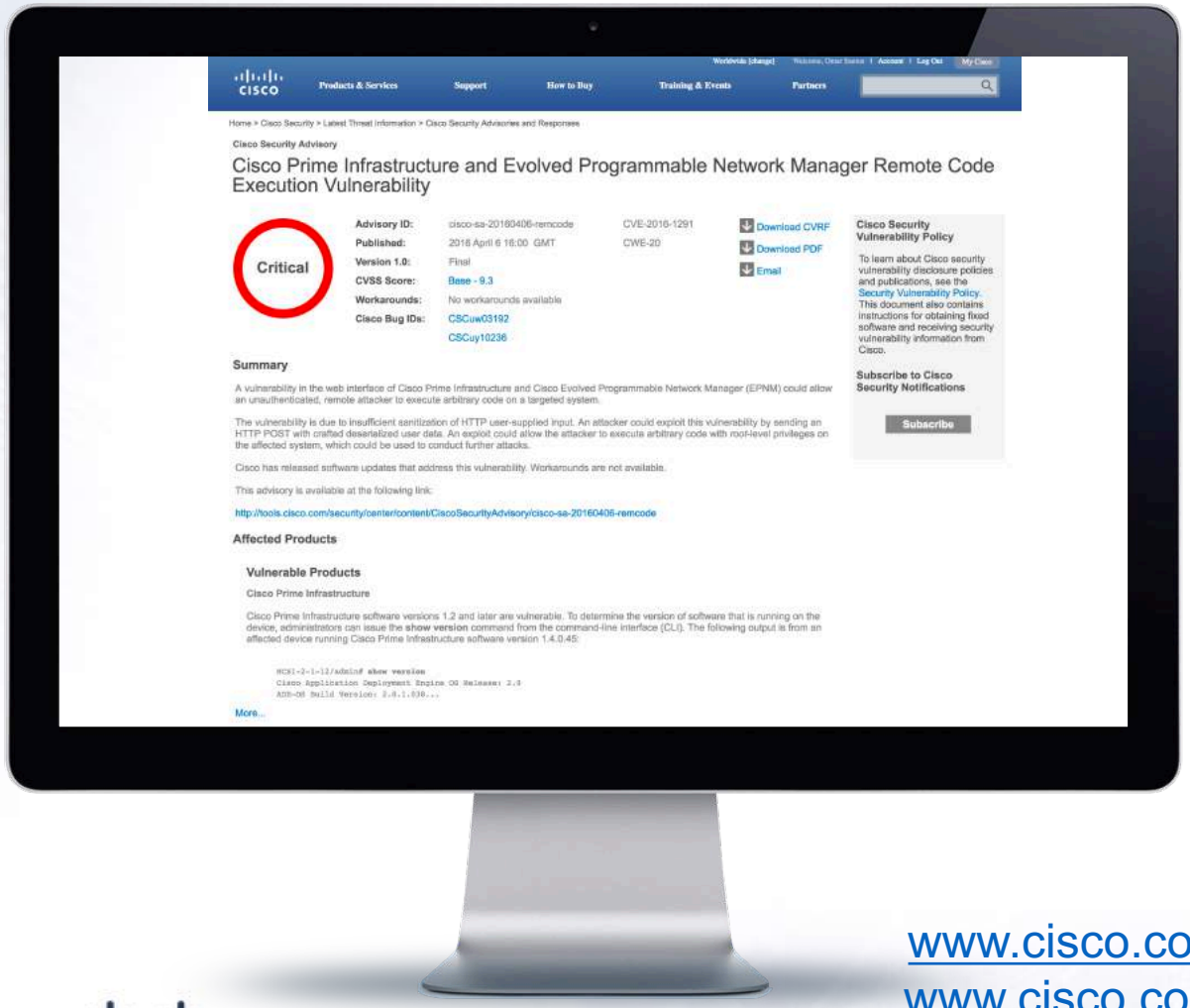
Cisco PSIRT



The incident handling process can take hours or months, depending on the scope.

- **Awareness**: PSIRT получает уведомление об инциденте или уязвимости
- **Active Management**: PSIRT приоритезирует уязвимости и выделяет ресурсы.
- **Fix Determined**: PSIRT координирует выпуск обновлений (или компенсирующих мер) и оценку воздействий.
- **Communication Plan**: PSIRT устанавливает временные ограничения и формат уведомлений.
- **Integration and Mitigation**: PSIRT вовлекает экспертов и руководство.
- **Notification**: PSIRT уведомляет всех потребителей одновременно.
- **Feedback**: PSIRT извлекает уроки по информации от заказчиков и внутренних подразделений Cisco.

Как узнать об уязвимости?



Заявители и потребители узнают об уязвимостях через:

- Почтовую рассылку от российского офиса компании Cisco (только для заявителей)
- RSS-фиды
- Автоматическая рассылка уведомлений
- Прикладной программный интерфейс openVuln для встраивания в приложения
- Через БДУ ФСТЭК

www.cisco.com/go/psirt
www.cisco.com/security

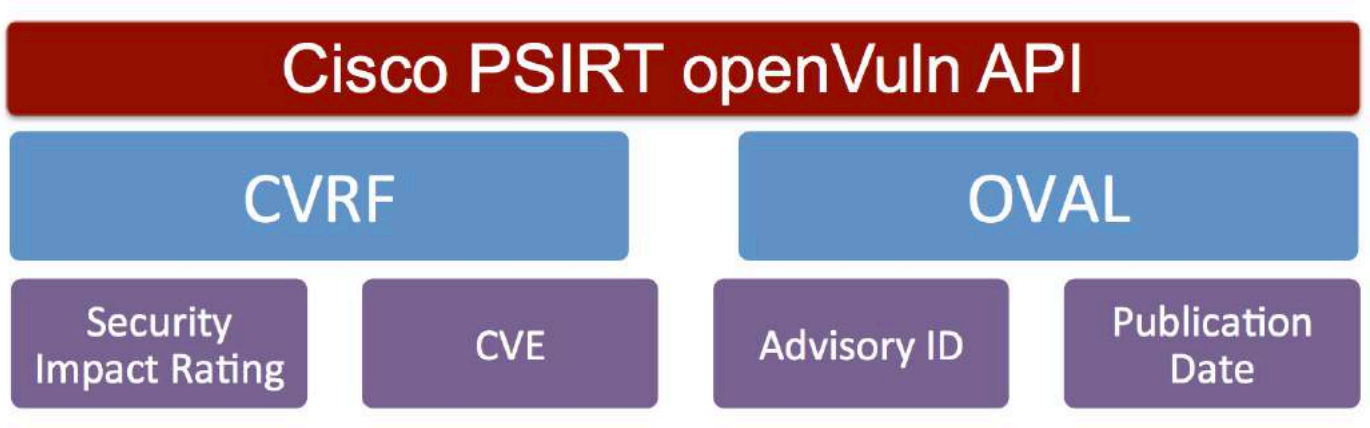
Варианты уведомления об уязвимостях

	Email	Security Portal	RSS	CNS	openVuln API	Bug Search Tool
Cisco Security Advisory - Critical and High Severity	Yes	Yes	Yes	Yes	Yes	Yes
Cisco Security Advisory - Medium Severity	No	Yes	Yes	No	Yes	Yes
Cisco Security Response	Yes	Yes	Yes	No	No	Yes
Cisco Event Response	No	Yes	Yes	No	No	No
Threat Outbreak Alert	No	Yes	Yes	No	No	No
Release Note Enclosure	No	No	No	No	No	Yes

http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

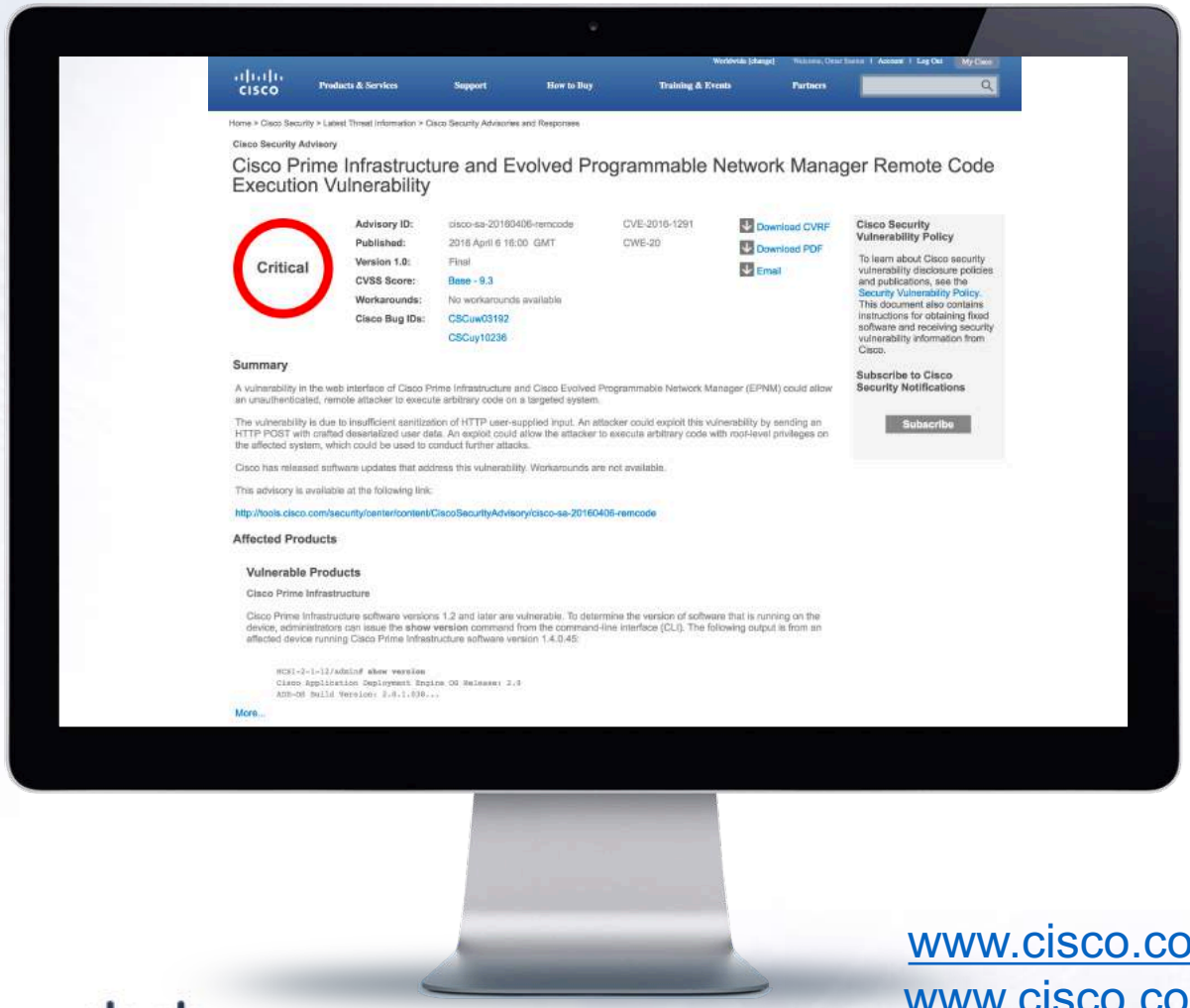
Сервис Cisco PSIRT openVuln API

- Бесплатный сервис Cisco PSIRT openVuln API позволяет получать в автоматическом режиме и машинно-читаемом формате информацию об уязвимостях в продукции Cisco в соответствии со стандартами CVE, CVSS, CVRF и OVAL



В январе 2017 мы перешли на CVSSv3

Как узнать об обновлении?



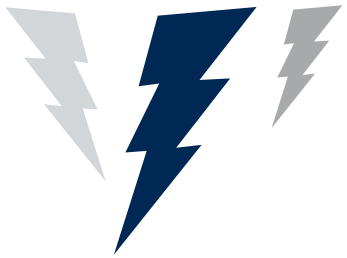
Потребители узнают об устранении уязвимостей в сертифицированном ПО от заявителей (в рамках программы поддержки сертифицированных изделий)

www.cisco.com/go/psirt
www.cisco.com/security

Другие вопросы

За деньги?
Получение обновления ПО с устраненной уязвимостью **бесплатно** через TAC (независимо от SMARTNET)

А что за деньги?
За деньги получается ПО с новым функционалом (в рамках контракта SMARTNET)



Какой тип обновления?
Тип 1 – устранение уязвимостей

А что с EOL?
Если продукт подошел к концу жизненного цикла, то увы…
Не стоит путать EOS и EOL, а также End of SW Maintenance

Спасибо!

alukatsk@cisco.com

CISCO