RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Your Product is Made WHERE?

SESSION ID: GRC-W03

David Doughty

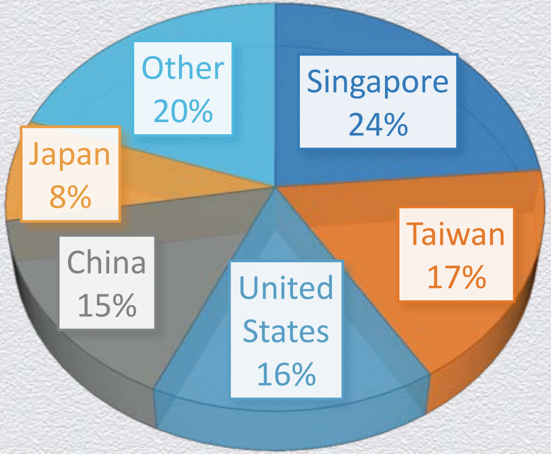
Director Product Security Engineering
Intel Corporation

intel Security

Intel Corporation

- 2012 revenue of $53B USD
- Global commercial off the shelf products and services for varied applications
- Worldwide development and manufacturing facilities
- Diverse workforce representing global nature of our business

INTEL REVENUE BY COUNTRY 2012



Source: Intel 2012 Annual Report

Trust *noun*

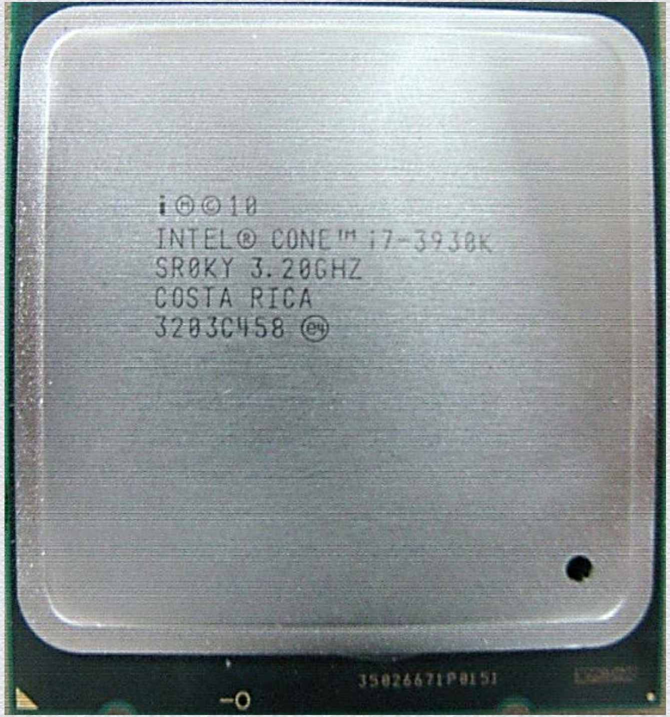
Firm belief in the reliability, truth, or ability of someone or something

Source: Oxford English Dictionary

Should You Trust This Product?

- Considerations:
  - What's the usage?
  - What's the source?
  - How has it been handled?
  - How has it been qualified?

What About This Product?



- Additional Info:
  - Intel has seen counterfeit CPU, they have been authentic Intel products that where remarked
- Considerations:
  - What’s the usage?
  - What’s the source?
  - How has it been handled?
  - How has it been qualified?

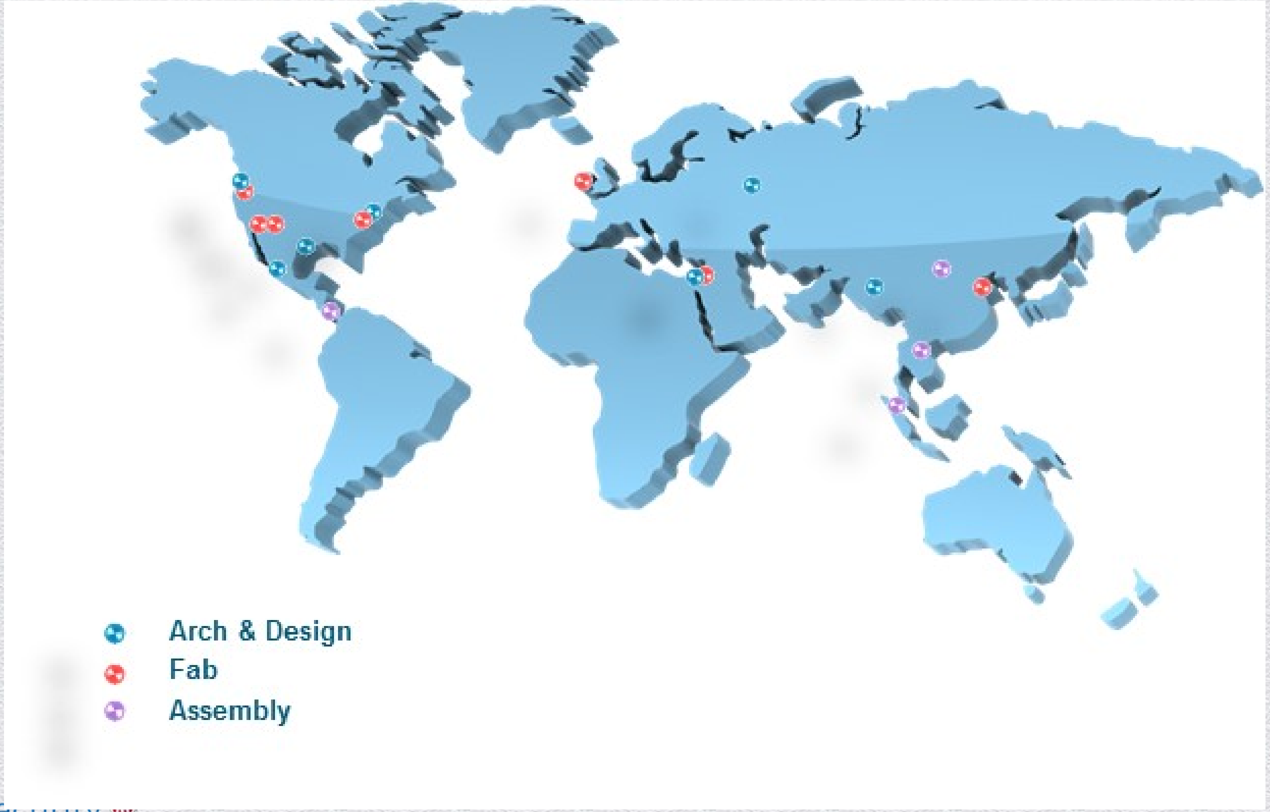
CLAIM

Security of a Product is Based on Where it is “Made In”

Made in <Country of Origin>

- Country of Origin **IS**
  - Based on where final assembly & test is performed
- Country of Origin **IS NOT**
  - An indication of where design, development or manufacturing was performed

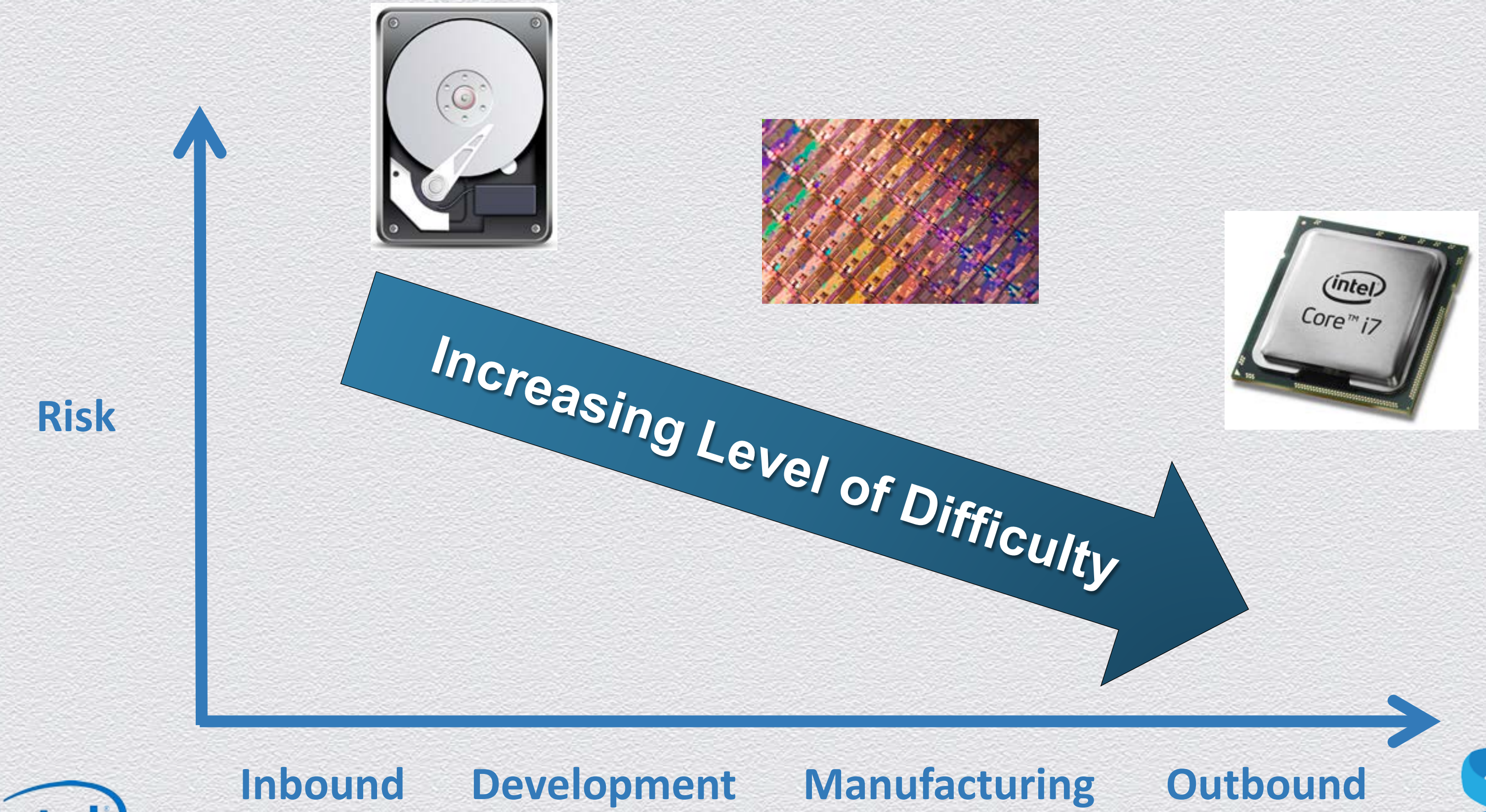
Intel Hardware Development & Manufacturing



Intel Hardware Product Country of Origin

	Product A	Product B
Definition	USA	India
Architecture	USA	India
Design	USA	India
Validation	USA	India, USA, Mexico
Mask	USA	USA
Fabrication	USA	USA
Assembly	China	Costa Rica
Test	China	Costa Rica
Country of Origin or “Made In”	China	Costa Rica

Risk of Vulnerability Being Introduced

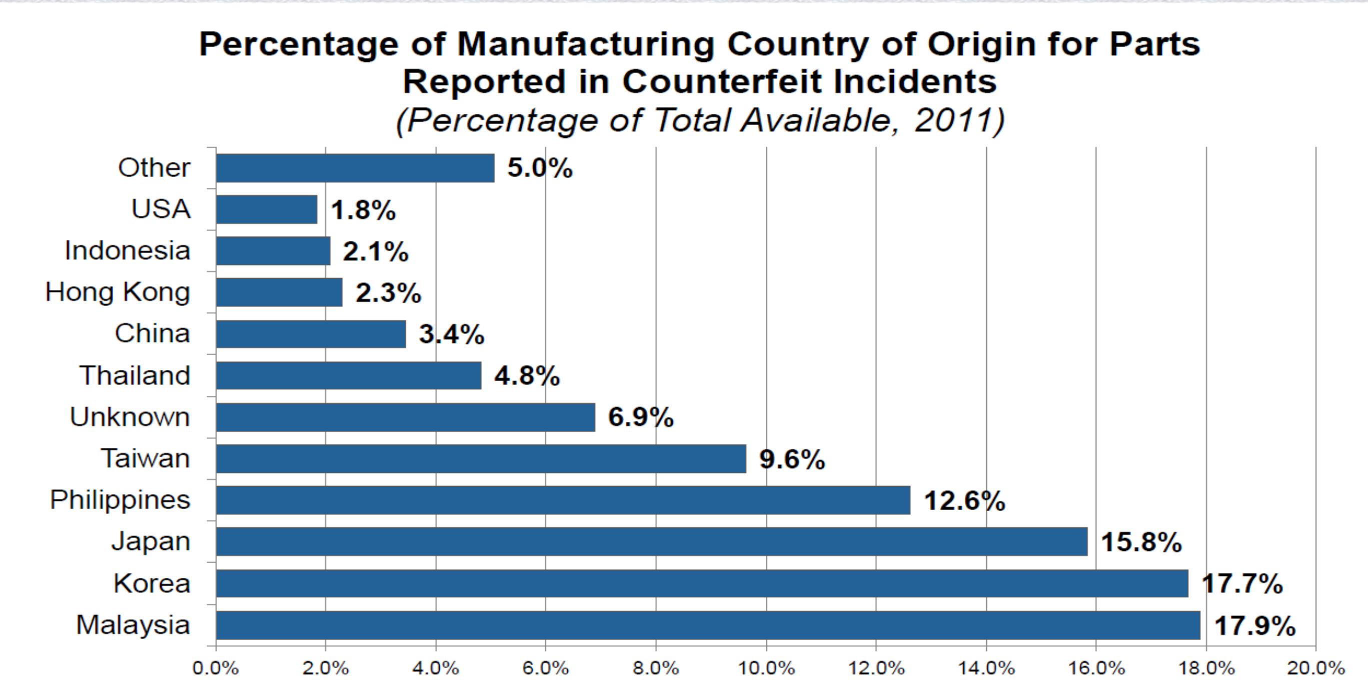


Risk

Increasing Level of Difficulty

Inbound Development Manufacturing Outbound

Where Counterfeit ICs Come From



Source: Counterfeit Analysis: An In-Depth Look at Counterfeits from a Statistical Perspective, Rory King IHS, Mike Snider ERAI, May '12

Assessment: Pants on Fire

- Country of Origin is a poor indicator of product security

- The source of counterfeit ICs will likely be in countries where ICs are "Made In"

CLAIM

Security of a Product is Based on Who it is Purchased From

Counterfeit Products

Sikorsky SH-60 Sea Hawk

Lockheed C-130 Hercules

“We do not want a $12 million missile defense interceptor’s reliability compromised by a $2 counterfeit part.”

General Patrick O’Reilly, Director Missile Defense Agency, 2011

Source: Inquiry Into Counterfeit Electronics Parts in the DoD Supply Chain, May ‘12

Top Reasons Counterfeits Enter Supply Chain

1	Less Stringent Inventory Management by Parts Brokers
2	Greater Reliance on Gray Market Parts by Brokers
3	Greater Reliance on Gray Market Parts by Independent Distributors
4	Insufficient Chain of Accountability
5	Less Stringent Inventory Management by Independent Distributors
6	Insufficient Buying Procedures
7	Inadequate Purchase Planning by OEMs
8	Purchase of Excess Inventory on Gray Market
9	Greater Reliance on Gray Market by Contract Manufacturers
10	Inadequate Production by OCM

Source: US Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, May 2009

Assessment: True

- Purchasing from authorized sources helps to ensure authenticity and proper handling

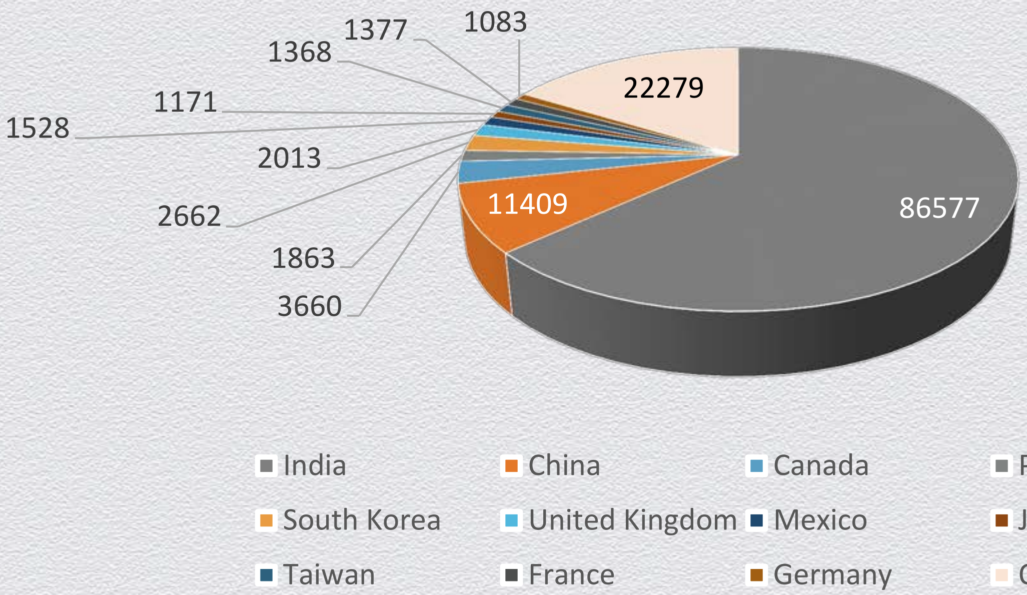
- Purchasing from unauthorized sources or by price, risks counterfeit products

CLAIM

Security of a Product is Based on Who Made it

Global Company = Global Workforce

USA H-1B Petitions Approved by Country of Birth



61% of H-1B petitions approved in FY 2012 were for workers in computer related occupations

Source: Characteristics of H1B Specialty Occupation Workers: Fiscal Year 2012 Annual Report to Congress

US Citizens "Gone Rogue"

Edward Snowden
NSA contractor wanted for release of classified documents

Robert Hanssen
FBI agent convicted of spying

Aldrich Ames
CIA officer/analyst convicted of spying

Insider Threat Motivations

Well Meaning

- Actions unknowingly or unintentionally lead to issues

Disgruntled

- Intentional actions lead to issues

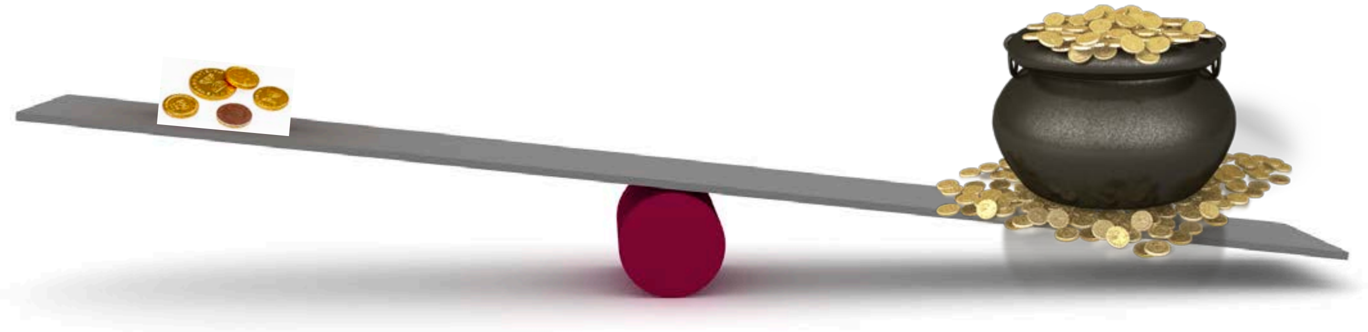
Compromised

- Corrupted of influenced to take actions leading to issues

State Actor

- Nationalistic pride or influence cause to take actions

All Vulnerabilities are Important



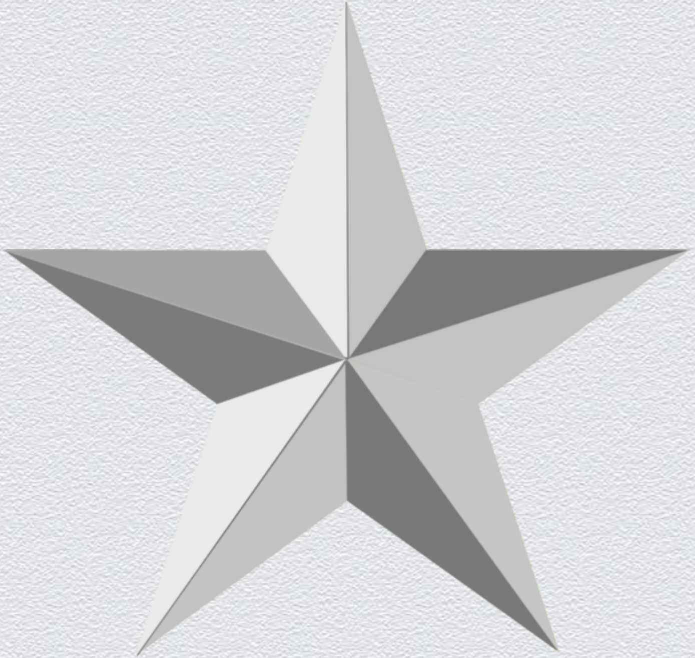
Intentional Actions

Unintentional Actions

Assessment: Partial Truth

- The knowledge and skills of those involved in product development contributes to security

- Focusing on who or where people are from misses the fact that vast majority of vulnerabilities are unintentional



CLAIM

Security of a Product is Based on How it was Made and Handled

Potential Threats

Inbound:
- Vulnerable Intellectual Property
- Ineffective Design Tools
- Out of Specification Packages

Development:
- Architectural/Design Vulnerability
- Unintentional/Intentional Changes
- Compromised Secrets

Enterprise:
- Network/System Vulnerability
- Unauthorized Facility Access
- Business Continuity

Outbound:
- Remarked Products
- Substitute Products
- Functionally Modified Products

Manufacturing:
- Facility Availability
- Die/Wafer Changes
- Improper Fusing
- Incomplete Testing

Security Objectives

Authentic

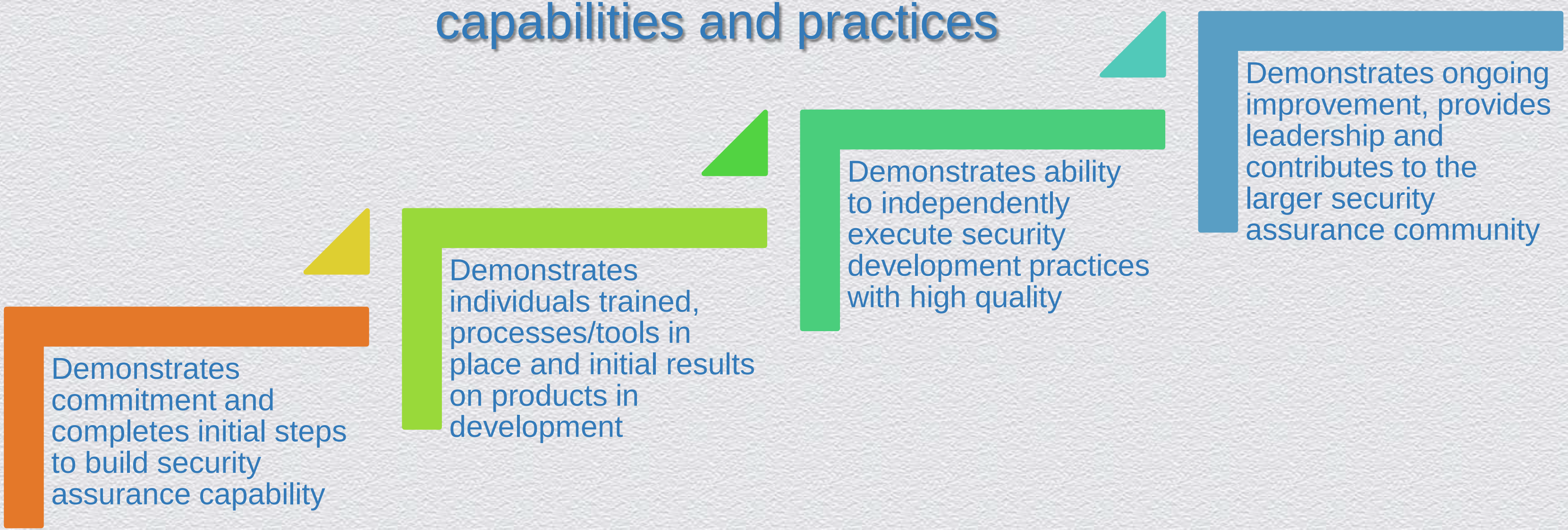
- An official product of the expected company
- Robust supply chain with no changes made since release

Trustworthy

- Features are present that enhance security
- Development followed security best practices
- Active support to address issues that may arise

Building the Capability

Maturity model that guides and measures security development capabilities and practices



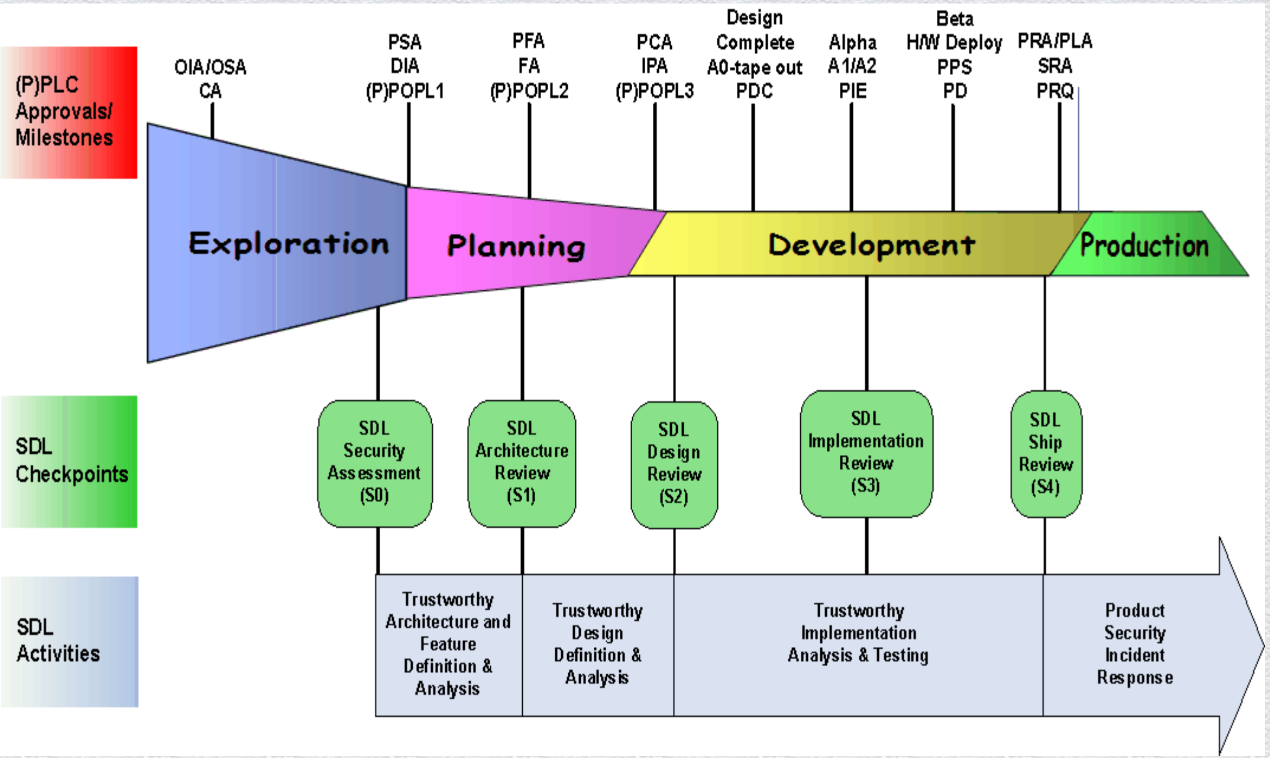
Demonstrates commitment and completes initial steps to build security assurance capability

Demonstrates individuals trained, processes/tools in place and initial results on products in development

Demonstrates ability to independently execute security development practices with high quality

Demonstrates ongoing improvement, provides leadership and contributes to the larger security assurance community

Following the Practices



(P)PLC Approvals/ Milestones

OIA/OSA CA

PSA DIA (P)POPL1

PFA FA (P)POPL2

PCA IPA (P)POPL3

Design Complete A0-tape out PDC

Alpha A1/A2 PIE

Beta H/W Deploy PPS PD

PRA/PLA SRA PRQ

Exploration

Planning

Development

Production

SDL Checkpoints

SDL Security Assessment (S0)

SDL Architecture Review (S1)

SDL Design Review (S2)

SDL Implementation Review (S3)

SDL Ship Review (S4)

SDL Activities

Trustworthy Architecture and Feature Definition & Analysis

Trustworthy Design Definition & Analysis

Trustworthy Implementation Analysis & Testing

Product Security Incident Response

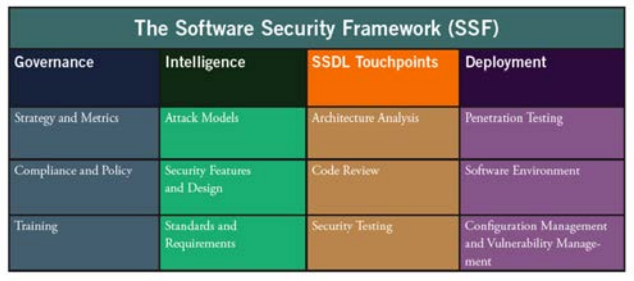
Benchmarking Practices

ISO/IEC 27034-1

- Internationally recognized standard used to:
  - Standard for describing security management processes
  - Supporting acquirer's need to for information across suppliers
  - Supporting suppliers need for standard response
  - Specific, rigorous and flexible to support diverse engineering approaches

Building Security In Maturity Model

- Empirical Measurement Model used to:
  - Assist organization understanding maturity of security practice
  - Plan tactical and strategic changes that will mature practices



The Software Security Framework (SSF)

Governance	Intelligence	SSDL Touchpoints	Deployment
Strategy and Metrics	Attack Models	Architecture Analysis	Penetration Testing
Compliance and Policy	Security Features and Design	Code Review	Software Environment
Training	Standards and Requirements	Security Testing	Configuration Management and Vulnerability Management

Assessment: True

- Following a robust Security Development Lifecycle is the single most important determining factor of a products security assurance level

Summary

Summary

- Global companies building commercial products should:
  - Follow a robust Security Development Lifecycle to build-in security at each stage from concept through product delivery
  - Regularly evaluate practices against international standards and industry best practices
  - Employ a risk based approach to prioritize actions to address current and emerging threats
  - Continuously improve practices to eradicate exploitable vulnerabilities prior to release regardless of the source

RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Q&A