Come Migliorare la Sicurezza Informatica della Supply Chain

who am i

- **studi**

  laureato in ingegneria informatica (università la sapienza di roma)
  e sicurezza informatica (università di milano)
  specializzato in advanced cybersecurity (stanford university)
  certificato in cybersecurity engineering and software assurance
  e in digital forensics (carnegie mellon university)

- **esperienze**

  referente informatico e funzionario alla sicurezza cis
  (ministero dell'interno)
  professore a contratto di tecnologie per la sicurezza informatica

  consulente in sicurezza informatica e informatica forense
  relatore e autore sui temi della cybersecurity

LinkedIn vincenzocalabro

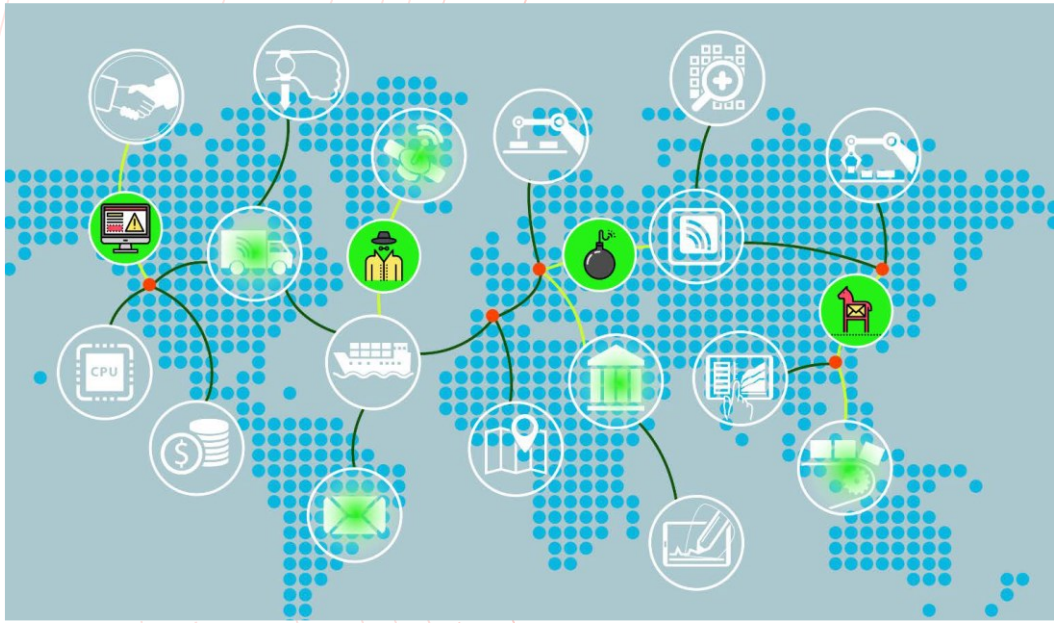
ICT Supply Chain

- Rappresenta l'insieme di risorse e processi che connette tra loro acquirenti, integratori e fornitori.
  Inizia con la progettazione dei prodotti e dei servizi ICT e si estende attraverso lo sviluppo, l'approvvigionamento, la produzione, la gestione e la consegna di prodotti e servizi ICT all'acquirente
- In altre parole è l'ecosistema distribuito e interconnesso di persone, processi, tecnologie, informazioni e risorse necessarie per creare e fornire un prodotto o servizio ICT

ICT Supply Chain Complexity

- Le catene di approvvigionamento di un'organizzazione spesso si **estendono su più paesi**
- Le catene di approvvigionamento ICT sono **dinamiche**, **multilivello** e **complesse**, il che rende difficile ad un'organizzazione visualizzare tutti i livelli della sua catena di approvvigionamento
- I componenti che finiscono in un prodotto ICT hanno le **proprie catene di approvvigionamento**
- La **mancanza di visibilità e tracciabilità** delle catene di approvvigionamento ICT può comportare rischi per la sicurezza

ICT Supply Chain Risk



- I rischi possono derivare dalla perdita di riservatezza, integrità o disponibilità di informazioni o dei sistemi informativi
  e riflettono i potenziali impatti negativi sulle attività organizzative (incluse mission, funzioni, immagine o reputazione),
  sulle risorse organizzative, sugli individui,
  sugli altri stakeholders e sulla Nazione
- I rischi della ICT supply chain si realizzano quando le minacce sfruttano le vulnerabilità esistenti nella stessa catena
- Esempi:
  - Inserimento di elementi fraudolenti
  - Produzione non autorizzata
  - Manomissione
  - Furto di software, capacità di calcolo e dati
  - Inserimento di software e hardware dannosi (es. dispositivi di localizzazione GPS, chip per computer, ecc.)
  - Cattive pratiche di produzione e sviluppo nella catena di fornitura ICT

Tipologie di ICT Supply Chains

Hardware Supply Chains

- Concettualizzare, progettare, costruire e fornire hardware e sistemi
- Include le supply chains di produzione e integrazione

Service Supply Chains

- Fornire servizi agli acquirenti, inclusi elaborazione e hosting dei dati, servizi logistici e supporto per le funzioni amministrative

Software Supply Chains

- Produrre il software che gira su sistemi critici
- Comprendere la rete di stakeholders che contribuiscono al contenuto di un prodotto software o che hanno l'opportunità di modificarne il contenuto

Le vulnerabilità della sicurezza HW/SW sono in aumento

La vulnerabilità della sicurezza è una debolezza che consente ad un utente malintenzionato di aggirare i controlli di sicurezza.

Richiede tre elementi:

- **Debolezza o lacuna del sistema**
  - Milioni di righe di codice software che gestiscono una quantità sempre crescente di funzionalità
  - Migliaia di vulnerabilità del software
  - Maggiore dipendenza da software commerciale e open source
- **L'attaccante riesce ad accedere alla criticità**
  - Aumento della connettività collegando i sistemi ad altri sistemi e connettendosi a nuove tipologie di dispositivi (Internet of Things)
  - Maggiore capacità di comunicazione remota del sistema e del dispositivo
- **Capacità dell'attaccante di sfruttare la criticità**
  - Accesso agli stessi strumenti e tecniche utilizzati per creare software
  - Funzionalità di reverse engineering per commerciali e open source
  - Piattaforme e framework di malware e attacchi

Published on July 29, 2021

Perché un buon livello di sicurezza informatica non è sufficiente?

- Un'organizzazione potrebbe **essere vulnerabile** ad un attacco alla supply chain **anche quando le proprie difese sono abbastanza buone**.
- **Gli aggressori** esplorano nuove potenziali alternative per infiltrarsi nelle organizzazioni **prendendo di mira i loro fornitori**.
- Inoltre, a causa di un potenziale quasi illimitato dovuto all'impatto degli attacchi alla supply chain su numerosi clienti, **questi tipi di attacchi stanno diventando sempre più comuni**.

Le organizzazioni dovrebbero convalidare il codice e il software di terze parti prima di utilizzarli per assicurarsi che non siano stati manomessi o manipolati.

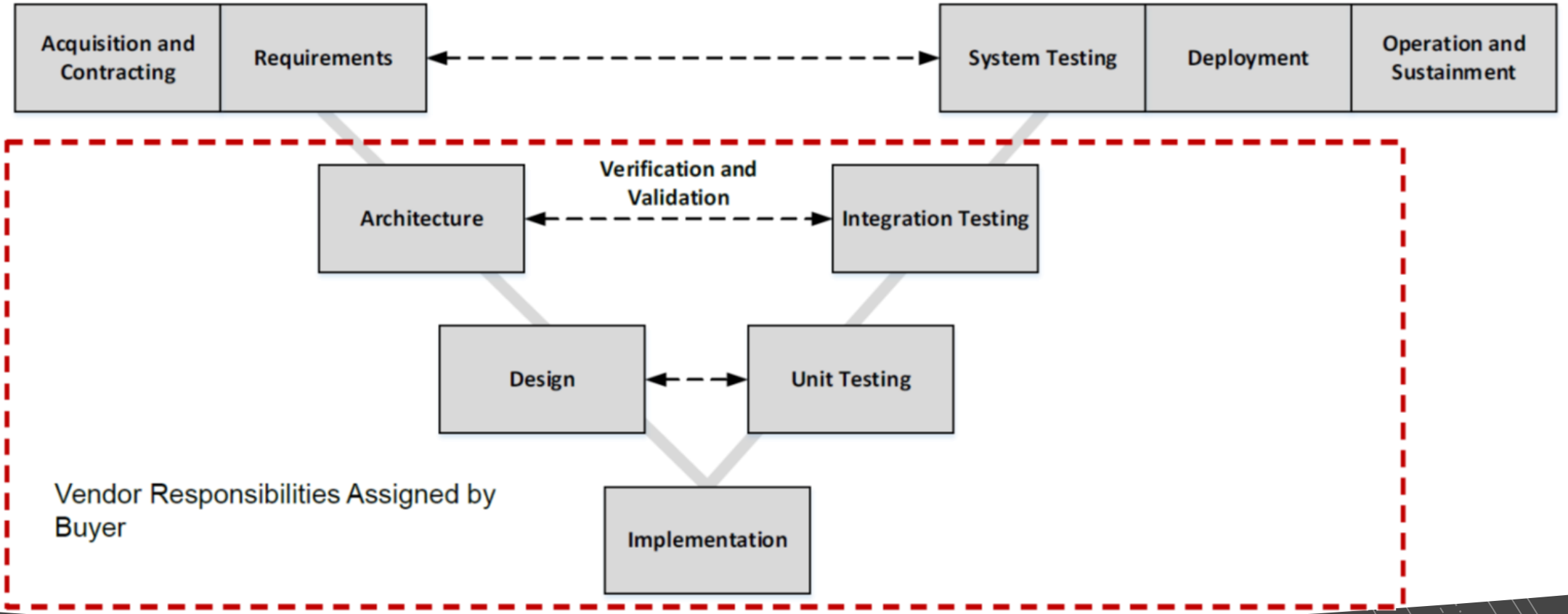
- La garanzia del software è definita come il livello di sicurezza che assicuri che il software funzioni come previsto e sia privo di vulnerabilità, progettate o inserite intenzionalmente o meno come parte del software, per tutto il ciclo di vita.
- La garanzia del software sta diventando sempre più importante per le organizzazioni di tutti i settori a causa della crescente influenza del software nei sistemi aziendali e mission-critical.

La strategia di acquisizione disegna la struttura della supply chain

Caso 1	L'organizzazione acquirente assume il tipico ruolo del cliente di un nuovo software, il fornitore decide i requisiti e sviluppa il prodotto.
Caso 2	L'organizzazione acquirente fornisce le specifiche dei requisiti al fornitore del nuovo software, il fornitore si occupa dello sviluppo.
Caso 3	L'organizzazione acquirente selezione e acquisisce direttamente componenti di tipo COTS - Commercial Off-The-Shelf, proprietary o open source, per integrarli con altri componenti oppure li personalizza in base alle proprie esigenze.

Caso 1 – Si concentra sul rapporto che si instaura tra acquirente e venditore

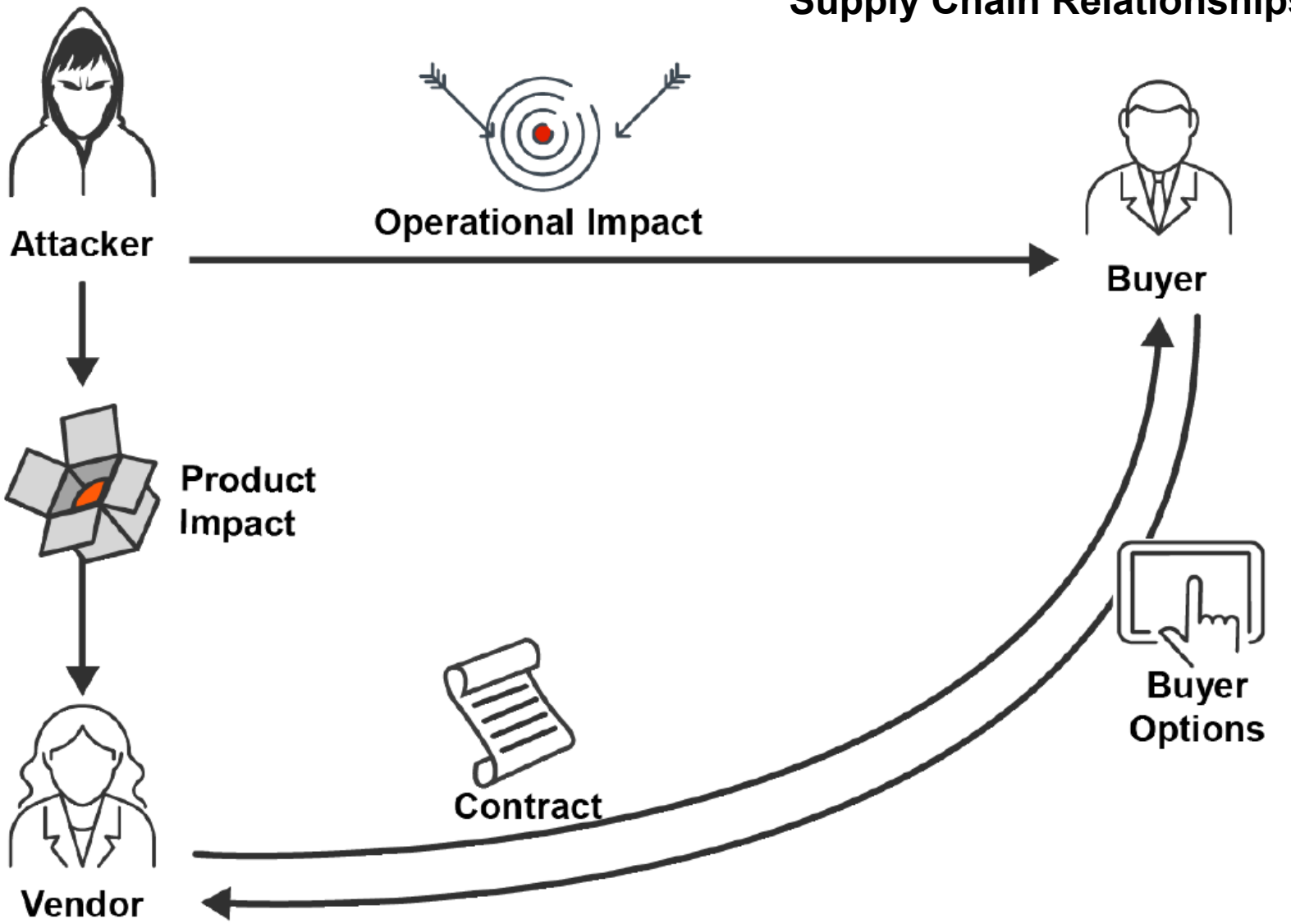
- Spesso i prodotti HW/SW sono il risultato di integrazioni di altri componenti diversi per natura, tipologia e responsabilità, per cui l'acquirente non è a conoscenza o visibilità dell'intera supply chain.

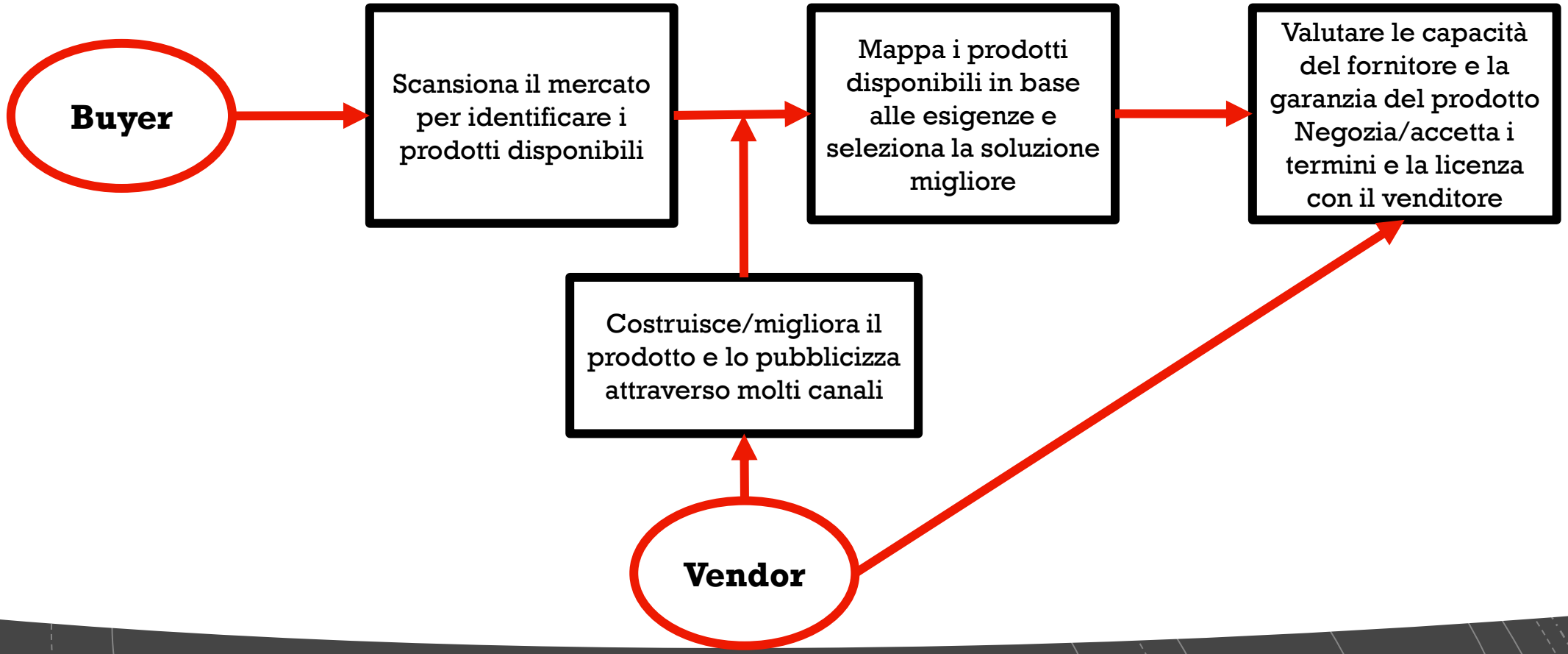


Caso 2 – L'acquirente partecipa alla fase iniziale e finale dello sviluppo del prodotto

- L'acquirente si concentra sulla definizione dei requisiti e il venditore fornisce un prodotto che soddisfi tali requisiti.
- L'acquirente verifica che il prodotto consegnato soddisfi i requisiti entro il costo e il programma contrattati.

Supply Chain Relationships per Caso 1 e 2

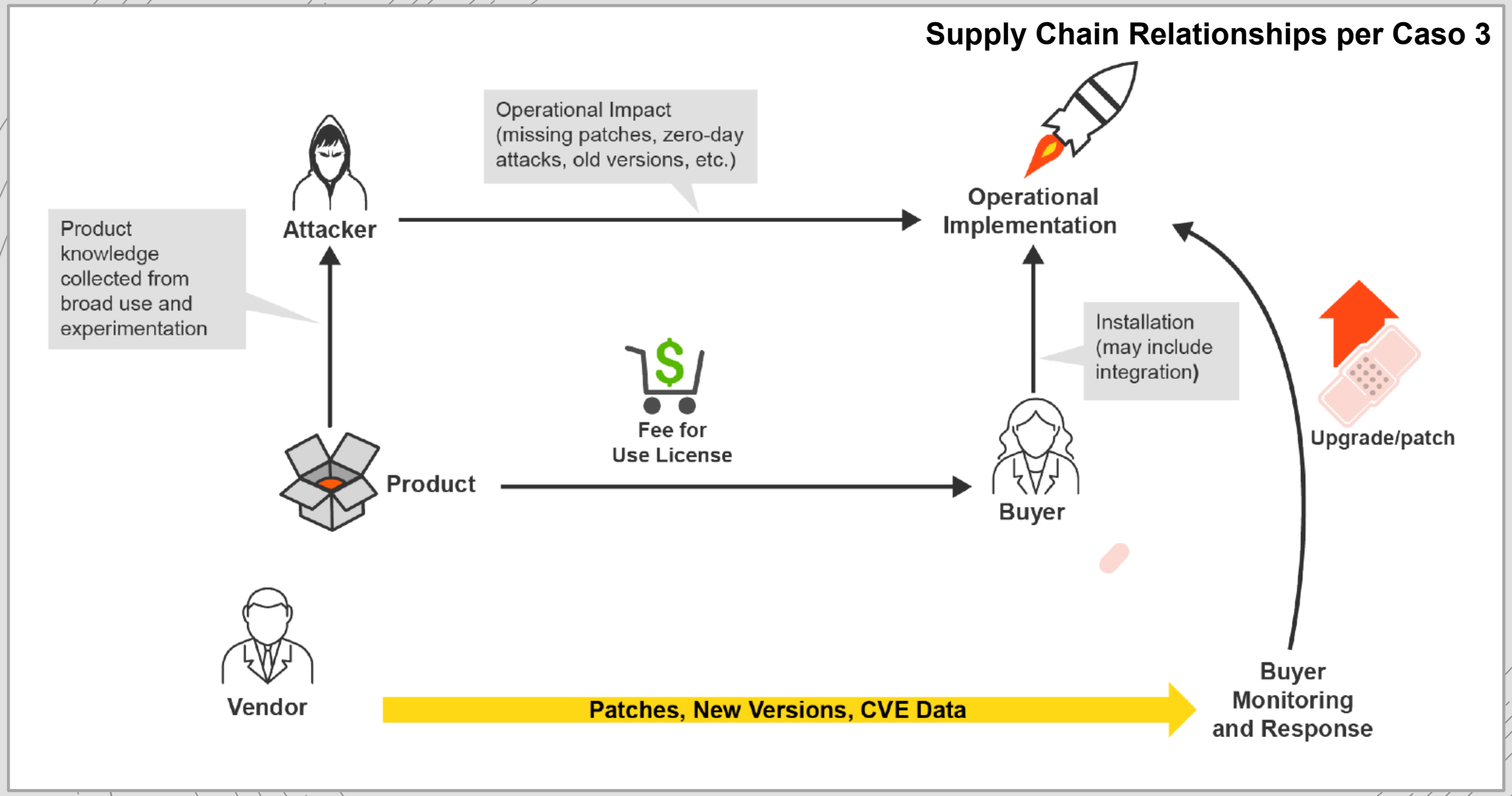




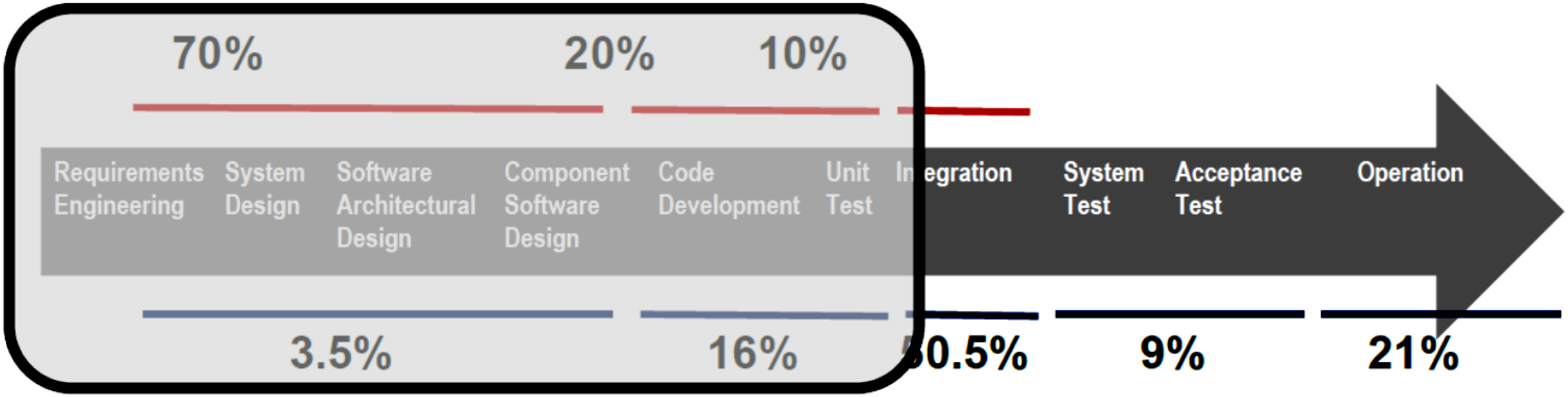
Caso 3 – L'acquirente si assume la responsabilità della scelta del prodotto

- Commercial Off the Shelf (COTS)
- Government Off the Shelf (GOTS)
- Open Source
- Web/AP store purchase
- Device or Service

Supply Chain Relationships per Caso 3



Dove vengono introdotti i difetti del software



Dove si trovano i difetti del software

In genere la visibilità, la comprensione e il controllo da parte dell'acquirente sono limitati in tutti i casi

ICT Supply Chain Risk Management

Come Migliorare la Sicurezza Informatica della Supply Chain

ICT Supply Chain Risk

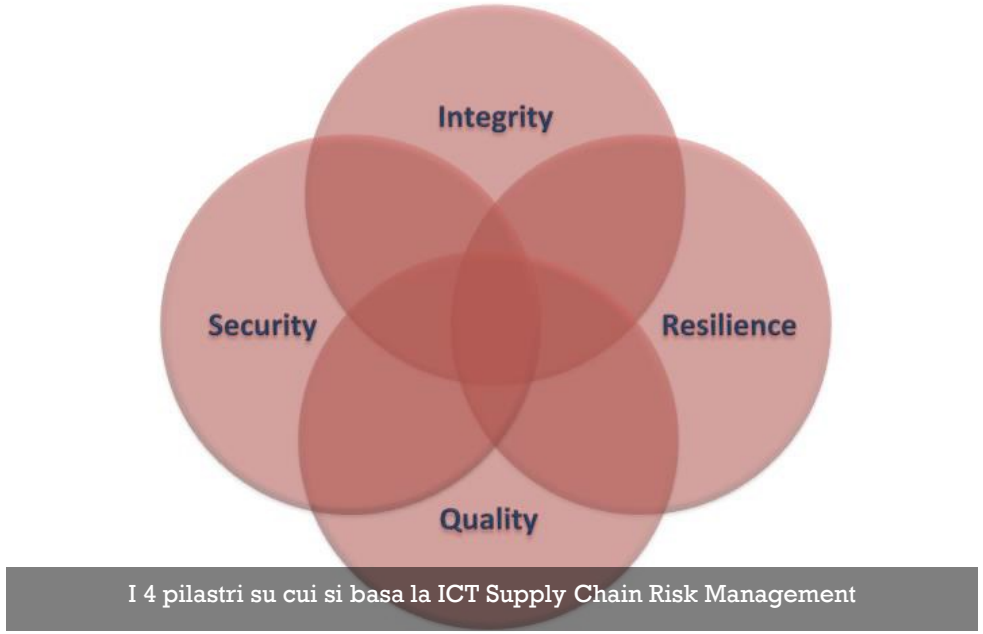
Threats / Minacce	Vulnerabilities / Vulnerabilità
Intenzionali: inserimento di contraffazioni, produzione non autorizzata, manomissione, furto, inserimento di sw e hw malevoli	**Esterne**: punti deboli della catena di approvvigionamento, controlli scarsi
Non intenzionali: utilizzo di pessime procedure per la produzione e lo sviluppo	**Interne**: sistemi informatici e componenti, politiche e processi organizzativi

Likelihood / Probabilità che una minaccia sfrutti una vulnerabilità	
Intenzionali: capacità e intenzione	**Non intenzionali:** occorrenze statistiche

Impact / grado del danno
Perdita, modifica o esfiltrazione dei dati
Guasti imprevisti o perdita della disponibilità del sistema
Riduzione della disponibilità dei componenti

Rischio

Lo scopo dell'ICT SCRM



I 4 pilastri su cui si basa la ICT Supply Chain Risk Management

Lo scopo dell'ICT SCRM è fornire uno strumento in grado di identificare, valutare e mitigare i rischi associati alla natura globale e distribuita delle catene di fornitura di prodotti e servizi ICT.

Le evidenze dell'ICT SCRM

Per realizzare un ICT SCRM efficace ed efficiente, in grado di ridurre i rischi ad un livello accettabile, è necessario che l'organizzazione disponga di evidenze che gli consentano di verificare:

- Sicurezza sulla **competenza del fornitore**
- Sicurezza sulle **caratteristiche del prodotto**
- **Metodo di distribuzione** del prodotto
- **Controllo operativo** del prodotto

Prove di sicurezza sulla **competenza del fornitore**

I dipendenti sono formati sulle practices dell'ingegneria della sicurezza

- Documentazione della formazione di ciascun ingegnere
- Date di revisione per i materiali della formazione
- Elenchi delle credenziali accettate per gli istruttori
- Nomi degli istruttori e delle loro credenziali

Il fornitore segue adeguate pratiche di progettazione della sicurezza

- Documentate linee guida di progettazione
- Fornisce prove che sono state risolte le debolezze di progettazione e codifica che possono influenzare la sicurezza (Common Weakness Enumeration [CWE])
- Ha analizzato i modelli di attacco appropriati alla progettazione, come quelli inclusi in Common Attack Pattern Enumeration and Classification (CAPEC)

Prove di sicurezza sulle **caratteristiche del prodotto**

Quali caratteristiche del prodotto riducono al minimo le opportunità di inserire e modificare le proprietà di sicurezza del prodotto?

- Valutazione della superficie di attacco: le funzionalità sfruttabili sono state identificate ed eliminate ove possibile
- Controlli di accesso
- Canali di input/output
- Applicazioni che abilitano gli attacchi: e-mail, Web
- Targets
- Sono stati identificati e mitigati i punti deboli di progettazione e codifica associati alle funzionalità sfruttabili (CWE)
- Convalida e verifica indipendenti della resistenza alle minacce

Prove sul **metodo di distribuzione** del prodotto

Il prodotto è sicuro alla consegna o ci sono misure che l'acquirente deve intraprendere per renderlo sicuro?

Il venditore ha fornito istruzioni per rendere il prodotto effettivamente sicuro?

I meccanismi di distribuzione sono appropriati per mantenere la sicurezza del prodotto? Il venditore

- Richiede buone pratiche di sicurezza da parte dei loro fornitori
- Valuta la sicurezza dei prodotti consegnati
- Affronta i rischi aggiuntivi associati all'utilizzo del prodotto nel loro contesto

Le patch e gli aggiornamenti sono forniti in modo tempestivo e sicuro?

Prove sul **controllo operativo** del prodotto

Chi si assume la responsabilità di preservare la resistenza agli attacchi del prodotto durante la sua implementazione?

- Patch e aggiornamenti di versione
- Estensione della distribuzione di utilizzo
- Estensione dell'integrazione

L'uso modifica la superficie di attacco e i potenziali attacchi al prodotto

- Cambiamento nell'utilizzo delle funzioni o dei rischi associati
- Le mitigazioni del rischio fornite dal fornitore sono adeguate per l'utilizzo desiderato?
- Effetti di aggiornamenti/patch del fornitore e modifiche alla configurazione locale
- Effetti dell'integrazione nelle operazioni (sistema di sistemi)

Conclusioni

Per valutare correttamente i rischi legati alla ICT supply chain occorre contemplare:

- i Rischi del fornitore
- i Rischi del prodotto
- i Rischi del metodo di distribuzione
- i Rischi operativi

Ricordarsi che i rischi di un processo aziendale possono passare attraverso la ICT supply chain

Pertanto, è necessario integrare i controlli dell'ICT Supply Chain Risk Management nel Framework di Security Risk Management

Approfondimenti

- **National Institute of Standards and Technology**
  Cyber Supply Chain Risk Management Program
  https://csrc.nist.gov/projects/cyber-supply-chain-risk-management
- **Software Engineering Institute**
  Carnegie Mellon University
  Supply Chain Risk Management Program
  https://www.sei.cmu.edu/
- **The Open Group, Open Trusted Technology Provider Standard (O-TTPS),** Version 1.0, Mitigating Maliciously Tainted and Counterfeit Products, 2013,
  https://www2.opengroup.org/ogsys/catalog/c139
- **ISO/IEC 27036-2:2014**, Information technology -- Security techniques -- Information security for supplier relationships