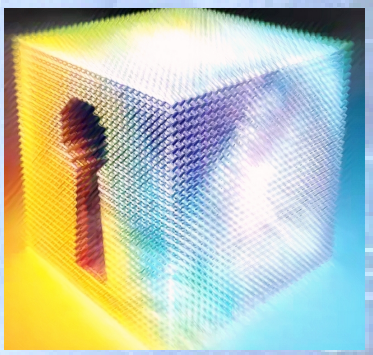
Seminario di Sicurezza Informatica

VALUTAZIONE DELLA SICUREZZA



Università degli Studi di Perugia

A.A. 2008/2009

Studente:
Manuela Ottobretti

Docente:
Stefano Bistarelli

INTRODUZIONE

1. Cos'è la valutazione della sicurezza?
2. Quadro per il confronto dei criteri di valutazione
3. Profilo storico
4. TCSEC - Orange Book
5. ITSEC
6. Federal Criteria
7. Common Criteria

Cosa si intende per Valutazione della sicurezza?

Processo di analisi tramite il confronto con criteri generali di funzionalità e di affidabilità.

Il risultato misura il livello di fiducia ovvero indica il grado con cui il sistema è conforme a particolari criteri.

I criteri utilizzati dipendono:

1. Obiettivi della valutazione
2. Metodologia di valutazione

VALUTAZIONE DELLA SICUREZZA INFORMATICA

Si occupa di:

- Decidere azioni/investimenti economici per ridurre esposizione a rischi
- Valutare opportunità di acquisire prodotti/servizi
- Sapere fino a che punto è possibile fidarsi di prodotti/sistemi/servizi
- Pubblicizzare caratteristiche di sicurezza di prodotti/servizi

CARATTERISTICHE GENERALI PER LA VALUTAZIONE

- **Imparzialità:** il Laboratorio per la Valutazione del Software (LVS) non deve avere interessi economici connessi con il risultato della valutazione
- **Ripetibilità:** un LVS deve ottenere lo stesso risultato ripetendo la valutazione
- **Riproducibilità:** un altro LVS deve ottenere lo stesso risultato ripetendo la valutazione
- **Obiettività:** il risultato della valutazione non deve essere determinato da giudizi soggettivi

QUADRO PER IL CONFRONTO DEI CRITERI

- Qual'è l'obiettivo della valutazione?
- Qual'è lo scopo della valutazione?

- Quali sono i metodi di valutazione?
- Qual'è la struttura organizzativa per il processo di valutazione?
- Qual'è la struttura dei criteri di valutazione?

- Quali sono i costi e i benifici della valutazione?

SCOPI E OBIETTIVI

La valutazione è rivolta a:

- **Prodotti**: componenti SW da utilizzare in un varietà di applicazioni e in ambienti con diversi gradi di sicurezza
- **Sistemi**: raccolta di prodotti assemblati per soddisfare specifiche esigenze

SCOPI E OBIETTIVI

La valutazione è rivolta a:

- **Prodotti**: componenti SW da utilizzare in un varietà di applicazioni e in ambienti con diversi gradi di sicurezza
- **Sistemi**: raccolta di prodotti assemblati per soddisfare specifiche esigenze

Gli scopi sono:

- **Valutazione**: valuta se il prodotto ha le proprietà di sicurezza richieste
- **Certificazione**: valuta l'idoneità di un prodotto (sistema) per un determinata applicazione
- **Accreditamento**: decidere di utilizzare un determinato prodotto

METODI DI VALUTAZIONE

1. **Orientata al prodotto:** si occupa di esaminare e testare il prodotto al meglio trovando eventuali problemi
2. **Orientata al processo:** verifica la documentazione relativa al processo di sviluppo del prodotto
   Meno costosa e ottiene risultati ripetibili

Ripetibilità e Riproducibilità sono proprietà desiderabili di una valutazione metodologica.

QUADRO ORGANIZZATIVO

- **Servizi Pubblici**: valutazione da parte di un'agenzia del governo (USA)
  - lenta
  - difficile trattenere personale qualificato

Quadro Organizzativo

- **Servizi Pubblici**: valutazione da parte di un'agenzia del governo (USA)
  - lenta
  - difficile trattenere personale qualificato
- **Servizi Privati**: valutazione da parte di un'agenzia di certificazione accreditata (Europa)
  - Come assicurarsi che la pressione del cliente non influenzi i risultati della valutazione?
  - **Interpretazione deriva - Criteria creep:** l'interpretazione dei criteri può variare nel tempo e si differenzia tra valutatori.

STRUTTURA DEI CRITERI DI VALUTAZIONE

Sicurezza e affidabilità dovrebbero essere legati ai concetti di:

1. **Funzionalità:** insieme delle caratteristiche riguardanti la sicurezza. Realizzazione: misure tecniche che contrastano le minacce
2. **Garanzia:** fiducia nella protezione offerta dalla funzionalità, a sua volta distinta in:
   1. **Efficacia:** grado in cui le misure tecniche contrastano le minacce da cui il prodotto/sistema si propone di difendersi. In relazione a un dato insieme di minacce (Es. valutare se meccanismi utilizzati sono adeguati "è sufficiente l'autenticazione con password?"...);
   2. **Correttezza:** grado di rispondenza dell'implementazione del prodotto/sistema ai requisiti espressi nelle funzionalità. Indipendente da efficacia e minacce. Strettamente dipendente alla qualità della realizzazione.

COSTI E BENEFICI

- **Costi diretti**: costi veri e propri della valutazione. Potenzialmente ripartiti su un gran numero di clienti.
- **Costi indiretti**:
  - tempo impegato
  - formazione valutatori
  - impatto sul processo di sviluppo

I costi andranno a pesare sul singolo cliente o proprietario.

COSTI E BENEFICI

- **Benefici**:
  La valutazione può essere necessaria
  - Ad es. contratti di governo, commercializzazione di prodotti...

  La valutazione può aiutare a creare un'immagine prestigiosa dell'azienda
  - maggiore credibilità
  - probabile incremento delle vendite

  Utile strumento per il confronto tra i diversi prodotti presenti sul mercato

PROSPETTIVA STORICA DEI METODI DI VALUTAZIONE

Istituzioni militari e governative creazione linee guida per valutazione sicurezza di prodotti/sistemi informatici inizio nel 1967(USA).

PROSPETTIVA STORICA DEI METODI DI VALUTAZIONE

Istituzioni militari e governative creazione linee guida per valutazione sicurezza di prodotti/sistemi informatici inizio nel 1967(USA).

ORANGE BOOK O TCSEC(TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA) - DOD (1983/85)

PROSPETTIVA STORICA DEI METODI DI VALUTAZIONE

RAINBOW SERIES

L'Orange Book è parte di una collezione di documenti sui requisiti, gestione e valutazione della sicurezza, pubblicati da NSA/NCSC (US National Security Agency/National Computer Security Center).

- Conosciuti grazie al colore della loro copertina come Rainbow Series.
- Concetti dell'Orange Book adattati a specifici aspetti:
  - Red Book: Computer Networks (Trusted Network Interpretation)
  - Purple Book: DBMS (Trusted Database Management System Interpretation)
  - ...

PROSPETTIVA STORICA DEI METODI DI VALUTAZIONE

Fine anni ’80 esigenza in Europa di sviluppare criteri di valutazione della sicurezza dei sistemi informatici.

- Memorandum Number 3 - Green Book (Regno Unito): a uso del governo ed elaborato dalle proposte del Dipartimento dell’Industria e Commercio;
- Ente per la sicurezza dell’informazione (Germania) - 1989: una prima versione dei propri criteri;
- Livre Bleu-blanc-rouge (Francia).

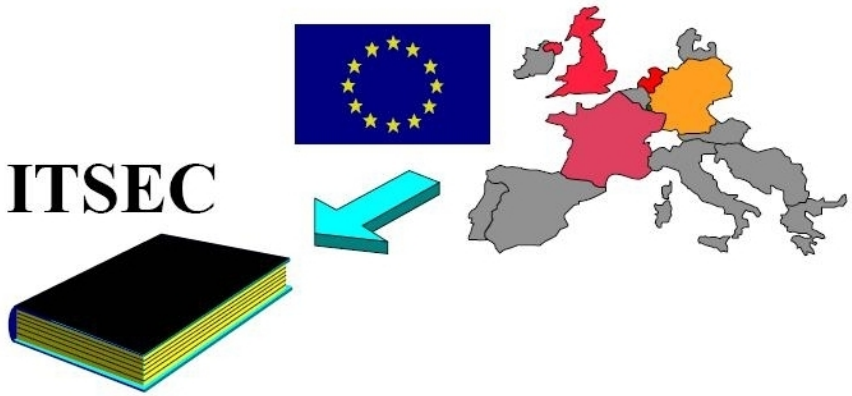
PROSPETTIVA STORICA DEI METODI DI VALUTAZIONE

Francia, Germania, Paesi Bassi e Regno Unito: armonizzazione dei criteri di sicurezza commissionata dalla CE.

PROSPETTIVA STORICA DEI METODI DI VALUTAZIONE

Francia, Germania, Paesi Bassi e Regno Unito: armonizzazione dei criteri di sicurezza commissionata dalla CE.

ITSEC (INFORMATION TECHNOLOGY SECURITY EVALUATION CRITERIA) - (1989/91)



- ITSEC ampiamente utilizzato (sostituito dai CC).
- ITSEM (Information Technology Security Evaluation Manual) - 1993 (CE).

PROSPETTIVA STORICA DEI METODI DI VALUTAZIONE

Nel 1989 anche il Canada rilasciò la prima versione del CTCPEC (Canadian Trusted Computer Product Evaluation Criteria)

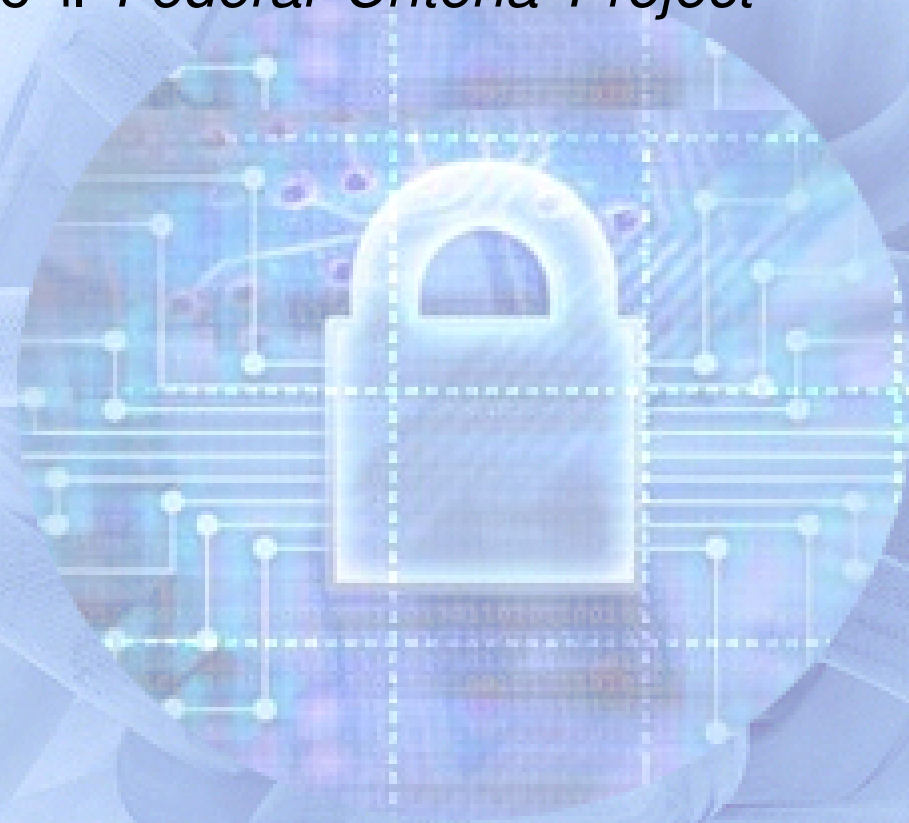
CSSC - Canadian System Security Center (1993).

CTCPEC fa affidamento al TCSEC, ma inserendo alcune nuove idee:

- separazione fra criteri funzionali e criteri per la valutazione dell'affidabilità del sistema.

PROSPETTIVA STORICA DEI METODI DI VALUTAZIONE

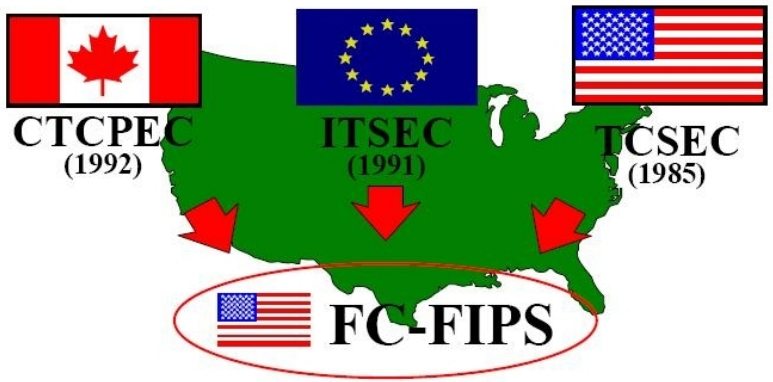
NIST (National Institute for Standard and Technology) e NSA (National Security Agency) avviano il *Federal Criteria Project* (1991).



PROSPETTIVA STORICA DEI METODI DI VALUTAZIONE

NIST (National Institute for Standard and Technology) e NSA (National Security Agency) avviano il *Federal Criteria Project* (1991).

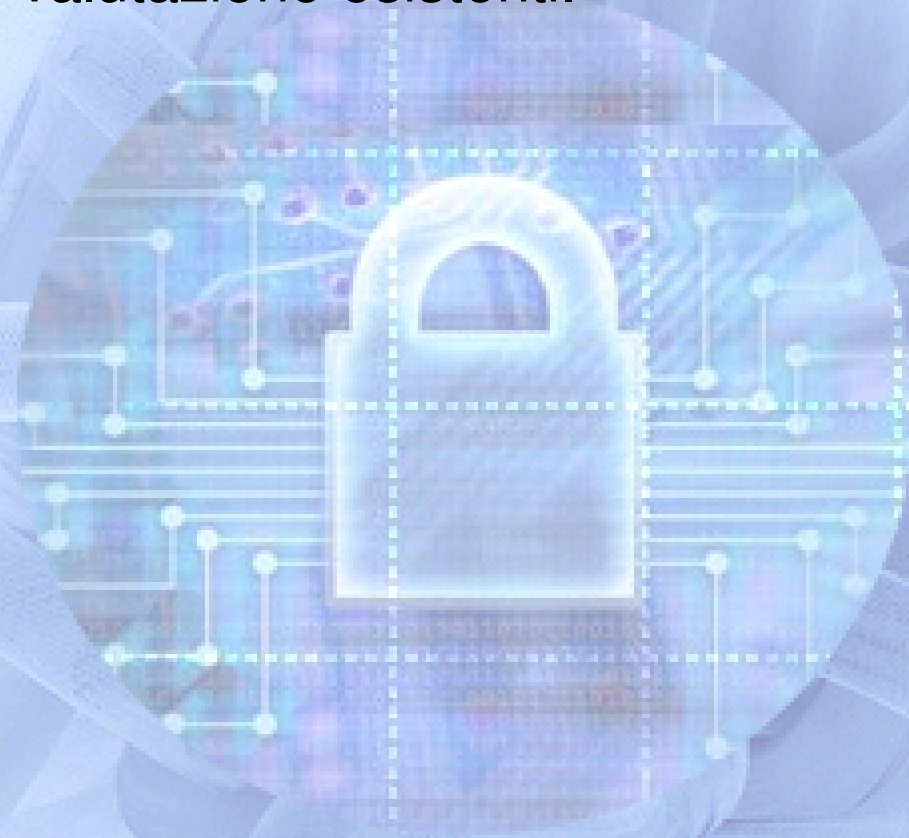
FEDERAL CRITERIA - FC (1992)



Mantiene forme di compatibilità con i TCSEC ma si basa su principi più simili a quelli dei criteri ITSEC e CTCPEC.

PROSPETTIVA STORICA DEI METODI DI VALUTAZIONE

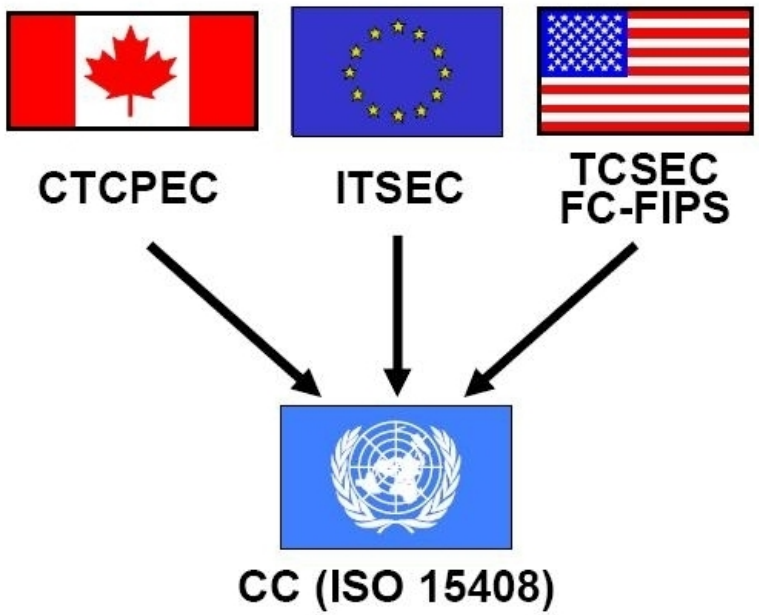
Common Criteria Editing Board (CCEB) producono i Common Criteria che allineano i vari criteri di valutazione esistenti.



PROSPETTIVA STORICA DEI METODI DI VALUTAZIONE

Common Criteria Editing Board (CCEB) producono i Common Criteria che allineano i vari criteri di valutazione esistenti.

COMMON CRITERIA - CC

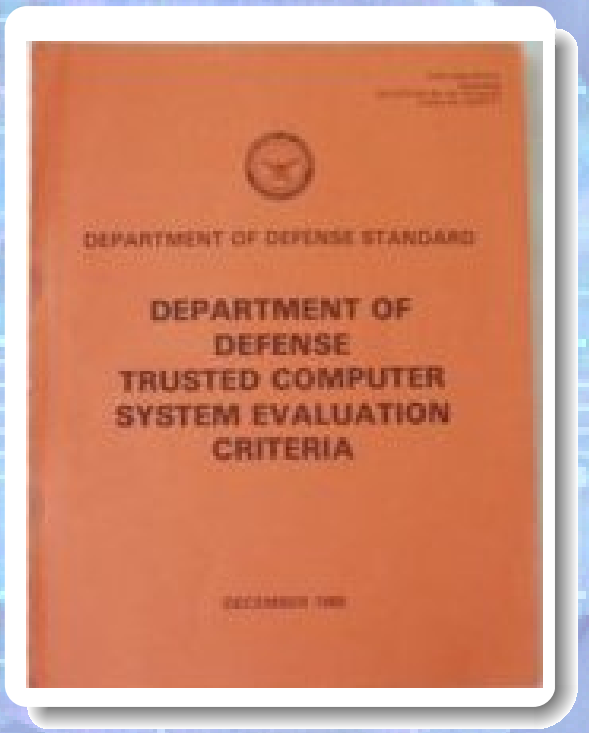


Nel 1999 i CC diventano uno standard internazionale: ISO 15048

TCSEC: ORANGE BOOK

Trusted Computer System Evaluation Criteria - DoD (1983/85)

- Prima metodologia completa per la valutazione della sicurezza
- Punto focale della Rainbow Series
- Non sicurezza ma livelli di fiducia
  - Un prodotto/sistema è fidato se è dotato di determinate protezioni
- Principalmente orientato alla valutazione di SO multiutente



OBIETTIVI DEI CRITERI TCSEC

Oltre a quello di protezione in ambito militare, richiesto dal DoD e per cui è nato.

1. Fornire agli utenti un metro con cui valutare il grado di fiducia che può essere immesso nei sistemi informatici;
2. Fornire una base per decretare i requisiti di sicurezza nelle specifiche di acquisizione;
3. Fornire una guida per sviluppatori e costruttori di sistemi per la realizzazione delle caratteristiche di sicurezza.

REQUISITI DI SICUREZZA DEL TCSEC 1

L'assegnazione di un sistema ad una delle classi avviene sulla base di 7 requisiti fondamentali di sicurezza:

REQUISITI DI SICUREZZA DEL TCSEC 1

L'assegnazione di un sistema ad una delle classi avviene sulla base di 7 requisiti fondamentali di sicurezza:

- **Security policy:**
  - politiche di sicurezza precise e ben definite
  - DAC/MAC
- **Marking of objects:** si assegna a ciascun oggetto un livello di criticità
  - **Etichetta** (non richiesta fino alla classe B1)
- **Identification of subject:** ogni soggetto deve essere identificato e autenticato

REQUISITI DI SICUREZZA DEL TCSEC 2

- **Accountability:** capacità del sistema di tenere traccia delle attività delle varie entità
  - log mantenuti e protetti
  - audit
  - Trusted Path
- **TCB - Trusted Computing Base:** insieme di componenti HW e SW definiti e conosciuti come fidati. Deve tener traccia attraverso registri di controllo di eventi rilevanti sulla sicurezza (login, operazioni sugli oggetti, logout)
- **Assurance:**
  - meccanismi affidabili
  - verifica indipendente delle componenti

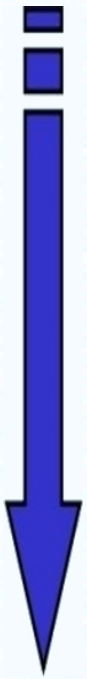
  Si articola in: affidabilità delle operazioni, del processo di sviluppo e documentazione

REQUISITI DI SICUREZZA DEL TCSEC 3

- **Documentation:** gestori e utenti di un sistema necessitano di una guida per installare e utilizzare tutte le proprietà di sicurezza; valutatori necessitano di documentazioni sulla progettazione per effettuare test.
  - Guida utente sulle caratteristiche di sicurezza (SFUG)
  - Guida amministratore: Trusted Facility Manual (TFM)
  - Documentazione di test: piani, procedure, prove e risultati dei test
- **Continuos protection:** accessi ad oggetti con importanza rilevante per quanto concerne la sicurezza devono essere continuamente monitorati; i meccanismi di sicurezza non dovrebbero essere manomessi.

SCALA TCSEC: CATEGORIE DI SICUREZZA

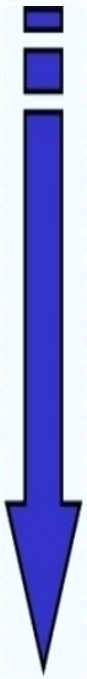
Quattro categorie di sicurezza:



- D – Minimal Protection: sistemi valutati che non soddisfano requisiti per nessuna classe.
  No sistemi in questa classe - valutazione costosa.

SCALA TCSEC: CATEGORIE DI SICUREZZA

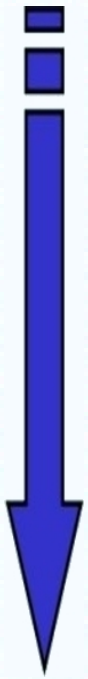
Quattro categorie di sicurezza:



- D – Minimal Protection: sistemi valutati che non soddisfano requisiti per nessuna classe.
  No sistemi in questa classe - valutazione costosa.
- C – Discretionary Protection: responsabilità dei soggetti sulle azioni che intendono avviare attraverso l'inclusione di capacità di controllo.
  Politiche DAC e per il riuso degli oggetti.

SCALA TCSEC: CATEGORIE DI SICUREZZA

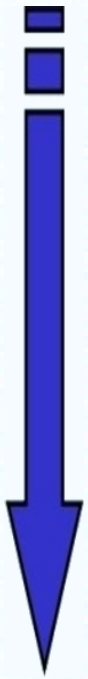
Quattro categorie di sicurezza:



- D – Minimal Protection: sistemi valutati che non soddisfano requisiti per nessuna classe.
  No sistemi in questa classe - valutazione costosa.
- C – Discretionary Protection: responsabilità dei soggetti sulle azioni che intendono avviare attraverso l'inclusione di capacità di controllo.
  Politiche DAC e per il riuso degli oggetti.
- B – Mandatory Protection: politica MAC, necessari meccanismi per etichettare criticità dei dati.

SCALA TCSEC: CATEGORIE DI SICUREZZA

Quattro categorie di sicurezza:



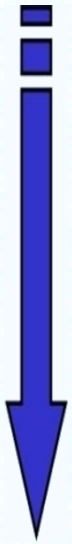
- D – Minimal Protection: sistemi valutati che non soddisfano requisiti per nessuna classe.
  No sistemi in questa classe - valutazione costosa.
- C – Discretionary Protection: responsabilità dei soggetti sulle azioni che intendono avviare attraverso l'inclusione di capacità di controllo.
  Politiche DAC e per il riuso degli oggetti.
- B – Mandatory Protection: politica MAC, necessari meccanismi per etichettare criticità dei dati.
- A – Verified Protection: metodi di verifica formali.

SCALA TCSEC: CLASSI DI SICUREZZA

Categoria D

- Non ha classi

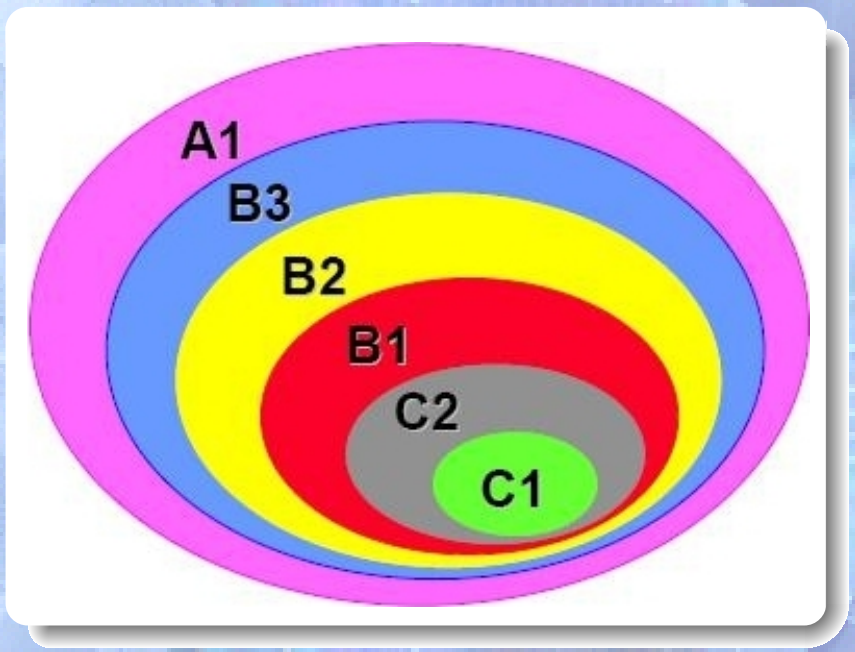
Categorie C, B e A suddivise in classi gerarchiche:



- C – Discretionary Protection
  - C1 - Discretionary Security Protection
  - C2 - Controlled Access Protection
- B – Mandatory Protection
  - B1 - Labelled Security Protection
  - B2 - Structured Protection
  - B3 - Security Domain
- A – Verified Protection
  - A1 - Verified Protection

SCALA TCSEC: CLASSI DI SICUREZZA

- Classi di sicurezza definite in modo incrementale
  - Requisiti di una classe inclusi nelle classi superiori
- Prodotti in classi superiori forniscono maggiori meccanismi di sicurezza e una maggiore garanzia attraverso una più rigorosa analisi



C1: Discretionary Security Protection

- Sistema composto da una serie di processi, utenti e dati che cooperano allo stello livello di integrità
- Requisiti funzionali minimi solo per identificazione e autenticazione: obbligo di autenticazione degli utenti; DAC sulla base di singoli utenti o gruppi
- Test per i soli difetti evidenti
- Documentazione:
  - Guida utente
  - Trusted Facility Manual (per l'amministratore di sistema)
  - Documentazione di test e di progettazione
- Non offre particolari strumenti di sicurezza, adatto ad ambienti di tipo non professionale

C2: Controlled Access Protection

- C1 + riuso degli oggetti e auditing
- Controllo più rigido sugli accessi a oggetti da parte di soggetti autenticati: DAC a granularità dei singoli utenti
- Obbligo di tenere traccia delle operazioni rilevanti per la sicurezza
- Test per i soli difetti evidenti
- ECMA(1993): C2 più ragionevole classe per applicazioni commerciali. Molti SO e DBMS appartengono a questa classe, nonostante i sistemi C2 risultino deboli
- Prevedono strumenti in grado di guidare installazione e configurazione dei prodotti secondo specifiche C2

B1: Labelled Security Protection

- MAC su insieme ridotto di oggetti (politiche di sicurezza conformi al modello Bell-LaPadula)
- Soggetti e oggetti vengono etichettati
- Problema: come considerare un'etichetta quando l'oggetto viene esportato in un sistema esterno?
  - comunicazione multilevel: oggetti mantengono propria etichetta
  - comunicazione single-level: dato valutato dal TCB e da utenti autorizzati e ri-etichettato
- Contenuto più approfondito della documentazione
- Test sia a livello di prodotto sia a livello di codice sorgente
- Sistemi gestione sicurezza a più livelli ambiente Unix: V/MLS (AT&T), SO: Hewlett Packard, DEC e Unisys. DBMS: Trusted Oracle 7, INFORMIX-Online/Secure, Secure SQL Server.

B2: Structured Protection

- Nuovi vincoli alla fase di progettazione del sistema:
  - Meccanismi di protezione della memoria
- MAC per tutti gli oggetti
- Comunicazioni fra entità differenti protette e monitorate
- Trusted Path per login e autenticazione iniziale
- Descrizione politiche sicurezza DTLS attraverso un modello formale, ad es. Bell-LaPadula
- Test puntano alla difesa da attacchi esterni
- TCB prevede indirizzo spazi distinti per isolare i processi
- Eventi che possono potenzialmente creare un canale nascosto devono essere controllati
- TCB è relativamente resistente alla penetrazione
- B2 è il livello valutato per il sistema operativo Trusted Xenix

B3: Security Domain

- Implementa un Reference Monitor
- Elevata resistenza ad attacchi provenienti dall'esterno
- Nuovi requisiti in materia di gestione della sicurezza:
  - amministratore politiche di sicurezza
  - meccanismi di controllo monitorano eventi rilevanti per la sicurezza e rilasciano avvertimenti in situazioni sospette
- Trusted Recovery, dopo un guasto del sistema
- Più sforzi per l'ingegneria di sistema per ridurre al minimo la complessità del TCB ed escludere moduli non adeguati alla sicurezza
- Coerenza tra modello formale della politica e DTLS
- Valutazione B3 per le versioni di sistema operativo Wang's XTS-300 (e XTS-200) multilevel OS, che gira in macchine Wang con HW di base x86

A1: Verified Design

- Funzionalmente equivalente alla B3 + analisi covert channel e verifica “formale” progetto
- Più alto livello di garanzia attraverso metodi formali
- Formal Top Level Specification (FTLS), che include definizioni astratte delle funzioni del TCB;
- Prove di coerenza tra il modello e FTLS (formali)
- Analisi formale canali nascosti: eventuale esistenza di canali nascosti va giustificata, larghezza di banda può essere limitata
- Obbligo di controllo per accertare che la versione installata all’utente sia la stessa della Master Copy valutata
- Valutazione A1 per le componenti di rete: LAN MLS (da Boeing) e Gemini Trusted Network Processor SO-SCOMP

LIMITI DEL TCSEC

1. Campo di applicazione limitato (protezione per elaboratori non connessi in rete)

LIMITI DEL TCSEC

1. Campo di applicazione limitato (protezione per elaboratori non connessi in rete)
2. Valutazioni del TCSEC riconosciute solo negli USA

LIMITI DEL TCSEC

1. Campo di applicazione limitato (protezione per elaboratori non connessi in rete)
2. Valutazioni del TCSEC riconosciute solo negli USA
3. No flessibilità nella modalità di valutazione: complessità proporzionale al livello di sicurezza

LIMITI DEL TCSEC

1. Campo di applicazione limitato (protezione per elaboratori non connessi in rete)
2. Valutazioni del TCSEC riconosciute solo negli USA
3. No flessibilità nella modalità di valutazione: complessità proporzionale al livello di sicurezza
4. Pochi livelli per cui quasi tutti i prodotti valutati con livello medio-alto (C2)

LIMITI DEL TCSEC

1. Campo di applicazione limitato (protezione per elaboratori non connessi in rete)
2. Valutazioni del TCSEC riconosciute solo negli USA
3. No flessibilità nella modalità di valutazione: complessità proporzionale al livello di sicurezza
4. Pochi livelli per cui quasi tutti i prodotti valutati con livello medio-alto (C2)
5. Processo di valutazione costoso

SPECIFICAZIONI NCSC PER UNIX

"Unix non è stato progettato per essere sicuro ma è stato concepito con le necessarie caratteristiche per rendere la sicurezza funzionale"

Dennis Ritchie

SPECIFICAZIONI NCSC PER UNIX

> "Unix non è stato progettato per essere sicuro ma è stato concepito con le necessarie caratteristiche per rendere la sicurezza funzionale"
>
> Dennis Ritchie

- Dal punto di vista dello NCSC tutte le versioni tradizionali di UNIX appartengono alla **classe C1**
- Il Governo USA ha richiesto che entro il 1992 tutti i sistemi UNIX da esso impiegati raggiungssero almeno livello **C2**
- Dal 1992, il Pentagono acquista solamente sistemi **B2**, cioè sistemi molto affidabili.

Specificazioni NCSC per Unix

Esempi singole versioni di UNIX:

- **C2:** UNIX SCO versione 3.2;
- **B2:** UNIX System V 4.1 versione ES (Enhanced Security, SVR4.1 ES), supportando anche caratteristiche della classe **B3**;
- **C2:** ULTRIX versione 4.0;
- UNICOS può essere installato nella versione chiamata “UNICOS secure” che spinge molto a fondo i criteri di sicurezza.

La notevole espansione di UNIX in ambienti militare, giudiziario, bancario, ecc. ha portato al proliferare di diversi UNIX “secure” per cui non è più fondata la cattiva fama di UNIX come sistema insicuro.

DAL TCSEC ALL'ITSEC

Information Technology Security Evaluation Criteria - Armonizzazione criteri Europei CE(1991)

- **TCSEC** è uno standard US.
- In TCSEC si classificano i sistemi secondo una gerarchia in cui per ciascuna classe sono specificati i requisiti di funzionalità a garanzia.
- **ITSEC** è uno standard Europeo.
- ITSEC è più flessibile: applica una scelta arbitraria delle funzioni di sicurezza, adattabile a sistemi con funzionalità non previste.

STANDARD EUROPEO ITSEC

Netta separazione tra requisiti funzionali e quelli di garanzia

Prevista possibilità di *upgrade* delle classi funzionali

Lo *sponsor* è colui che richiede la valutazione

STANDARD EUROPEO ITSEC

Netta separazione tra requisiti funzionali e quelli di garanzia

Prevista possibilità di *upgrade* delle classi funzionali

Lo *sponsor* è colui che richiede la valutazione

Concetti ITSEC:

- **TOE** - (Target Of Evaluation): oggetto della valutazione
- **ST** - (Security Target): obiettivo di sicurezza
- **EAL** - (Evaluation Assurance Level): livelli di severità della valutazione

VALUTAZIONE ITSEC

Valutazione effettuata prendendo a riferimento il **TS**, documento che deve contenere:

- System Security Policy o Product Rationale:
  - obiettivi di sicurezza
  - minacce
  - organizzazione e procedure
  - misure sul personale
- Security Enforcing Functions - **SEF**: specifica delle funzioni di sicurezza per conseguimeto obiettivi specificati
- Strength of mechanisms: livello di robustezza dei meccanismi dichiarato
- Evaluation level: livello di valutazione desiderato

SEF sono le contromisure raggruppate secondo un certo numero di categorie: **Generic Headings**

STANDARD EUROPEO ITSEC

Valutazione basata sul concetto di Assurance offerta dal sistema che si caratterizza per:

- Correctness: modo di concretizzare le funzioni di sicurezza e dei relativi meccanismi d'attuazione.
  Fiducia nella correttezza espressa utilizzando una scala a sette livelli (da E0 ad E6)
- Effectiveness: mira a stabilire se le funzioni di sicurezza adottate sono idonee agli scopi specificati nel ST per cui sono state scelte e se i meccanismi che realizzano tali funzioni sono in grado di contrastare attacchi diretti

GRADI DI ROBUSTEZZA DELL'ITSEC

Efficacia misurata sulla base della **robustezza dei meccanismi** (strenght of mechanisms):

- **BASE** se al minimo fornisce protezione contro eventi sovversivi casuali, benché possa essere violata da alcuni aggressori;
- **MEDIA** se al minimo fornisce protezione contro aggressioni caratterizzate da limitate opportunità o risorse;
- **ALTA** se può essere superata solo da aggressioni caratterizzate da un alto livello di esperienza, opportunità e risorse, con attacchi portati con successo al di sopra della normale praticabilità.

DETERMINAZIONE DEL GRADO DI ROBUSTEZZA

Documento ITSEM - Annex 6.C definisce modalità di determinazione del grado di robustezza del meccanismo basate su:

- tempo necessario per violare il meccanismo (min, gg)
- complicità necessaria (senza o utente o responsabile)
- esperienza tecnica necessaria (diffusa, professionale, esperto)
- tipo di attrezzatura da utilizzare (nessuna, apparecchiatura normale o particolare)

TIPOLOGIE INDICATE DA ITSEC 1

Singole funzioni di sicurezza raggruppate in **Generic Headings**. ITSEC prospetta otto tipologie di funzioni di sicurezza che comunque possono essere integrate da nuove tipologie, con l'evoluzione delle tecnologie e delle tipologie d'attacco.

- **Identificazione ed Autentificazione:** Stabiliscono e verificano l'identità che dichiara un utente che intende accedere al sistema informatico.
- **Controllo degli accessi:** Garantiscono che un utente possa espletare le sole operazioni di propria competenza.
- **Autorizzazioni:** Registrano gli accessi alle varie risorse del sistema in modo da riconoscere chi ha operato.

TIPOLOGIE INDICATE DA ITSEC 2

- **Ispezioni:** indagano su eventi anomali.
- **Riutilizzo degli oggetti:** garantiscono il riutilizzo di spazi di memoria, impedendo che ciò costituisca minaccia alla sicurezza.
- **Accuratezza:** garantiscono integrità di SW e dati.
- **Ripristino del servizio:** garantisce che le risorse siano accessibili ed utilizzabili su richiesta di qualunque utente abilitato, entro i tempi prefissati.
- **Scambio di dati:** assicura disponibilità, riservatezza ed integrità delle trasmissioni.

LIVELLI DI FIDUCIA ITSEC 1

- **E0** utilizzato per prodotti che non soddisfano altri livelli.
- **E1**
  - richiede ST per valutare il prodotto/sistema
  - descrizione informale dell'architettura del prodotto/sistema
  - prodotto/sistema deve dimostrare che il suo ST è soddisfatto
- **E2**
  - descrizione informale di progettazione del prodotto/sistema del TOE
  - controllo di configurazione e processo di controllo della distribuzione
- **E3**
  - requisiti più severi sui dettagli di progettazione
  - necessaria corrispondenza tra codice sorgente e requisiti di sicurezza

LIVELLI DI FIDUCIA ITSEC 2

- **E4**
  - richiede modello formale della politica di sicurezza
  - analisi di vulnerabilità a livello di progettazione
- **E5**
  - richiede corrispondenza tra il progetto e codice sorgente
  - analisi di vulnerabilità a livello di codice sorgente
- **E6**
  - ampio uso di metodi formali
  - mappatura parziale del codice eseguibile per il codice sorgente

Anche per l'ITSEC i livelli elencati dal più basso al più alto. Ogni livello include i requisiti del precedente livello.

FEDERAL CRITERIA

Federal Criteria Project NIST/NSA - USA (1992)

Mantiene forme di compatibilità con i TCSEC ma si basa su principi più simili a quelli dei criteri ITSEC e CTCPEC.

- Prevedono requisiti funzionali e qualitativi separati
- Possibilità di *upgrade* sia dei requisiti funzionali sia di quelli qualitativi
- Cerca di superare la rigida struttura dell'Orange Book attraverso l'introduzione dei **Protection profiles**.

PROTECTION PROFILES

Un PP ha cinque sezioni:

1. Descriptive Elements: 'nome' del PP e descrizione del problema da risolvere
2. Rationale: motivazione del PP
   - minaccia
   - ambiente
   - ipotesi di utilizzo
3. Functional Requirements: stabilisce il limite di protezione che deve essere fornita dal prodotto
4. Development Assurance Requirements: requisiti per tutte le fasi di sviluppo
5. Evaluation Assurance Requirements: specifica il tipo e l'intensità della valutazione

DALL'ITSEC AI COMMON CRITERIA (CC)

ITSEC 

- **ITSEC** è uno standard europeo.
- In ITSEC gli elementi che qualificano la valutazione sono scelti dal committente se non si leggono i documenti della valutazione non si hanno informazioni sulle caratteristiche di sicurezza.

- **Common Criteria** sono uno standard internazionale.
- Nei Common Criteria è possibile fare riferimento a profili di protezione predefiniti e certificati (Protection profile) relativi a tipologie omogenee di prodotti.

SIGNIFICATO CC

Un apparato è sicuro solo se si specifica:

- **Obiettivi di sicurezza**: sicuro per fare cosa
- **Ambiente di sicurezza**: sicuro in quale contesto
- **Soddisfacimento requisiti di assurance**: sicuro a fronte di quali verifiche eseguite

In altri termini: la valutazione della sicurezza secondo i CC ha lo scopo di offrire garanzie (assurances), che è possibile graduare, sulla capacità del TOE di soddisfare i propri obiettivi di sicurezza nell'ambiente di sicurezza per esso ipotizzato.

COMMON CRITERIA

Abbandonata stretta separazione fra classi funzionali e livelli di garanzia (ITSEC) per seguire i FC nell'uso dei Protection Profiles, in modo da predefinire classi di protezione.

Concetti dei CC:

- **TOE - Target of Evaluation:** criteri per la valutazione della sicurezza di prodotti/sistemi. Costituisce l'oggetto della valutazione.
- **PP - Protection Profile:** serie (riutilizzabile) di requisiti di sicurezza, compresa una EAL; deve essere sviluppato da un gruppo di utenti per catturare tipiche esigenze di protezione.

COMMON CRITERIA

- **ST - Security Target:** esprime i requisiti di sicurezza per uno specifico TOE (beni, minacce, ipotesi, ambiente operativo). E' suddiviso generalmente in:
  - Obiettivi di sicurezza
  - Requisiti funzionali relativi alla sicurezza
  - Requisiti di sicurezza informatica
  - Assunzioni
  - Rationale
- **EAL - Evalutation Assurance Level:** definisce cosa deve essere fatto in una valutazione, ci sono sette ordini gerarchici gli EALs.

LIVELLI DI SICUREZZA DEI CC 1

Rappresentano una misura della garanzia che il TOE raggiunga i suoi obiettivi di sicurezza rispetto al proprio ST

- **EAL1** - functionally tested
  - tester riceve ST, esamina documentazione ed esegue test per confermare le funzionalità documentate
  - valutazione non richiede alcuna assistenza da parte degli sviluppatori
  - esborso per la valutazione minimo
- **EAL2** - structurally tested
  - sviluppatore fornisce documentazione e risultati dei test
  - valutatore controlla documentazioni di recensione e ripete alcuni test
  - esborso limitato per lo sviluppatore

LIVELLI DI SICUREZZA DEI CC 2

- **EAL3** - methodically tested and checked
  - sviluppatore utilizza gestione della configurazione, documenti in materia di sicurezza per lo sviluppo e prevede progettazione di documentazione ad alto livello e di documentazione sui test di copertura per il riesame
  - EAL3 destinato a sviluppatori che hanno già seguito una buona prassi di sviluppo, ma che non vogliono attuare ulteriori modifiche alle loro pratiche
- **EAL4** - methodically designed, tested, and reviewed
  - sviluppatore fornisce un basso livello di progettazione e codice sorgente per la valutazione di un sottoinsieme di funzioni di sicurezza del TCB
  - garantisce la consegna delle procedure
  - valutatore svolge analisi indipendente della vulnerabilità
  - EAL4 più alto livello che economicamente fattibile per una linea di prodotti esistenti

LIVELLI DI SICUREZZA DEI CC 3

- **EAL5** - semiformally designed and tested
  - sviluppatore fornisce modello formale delle politiche di sicurezza, semi-formale alto livello di progettazione, specifiche funzionali e l'intero codice sorgente delle funzioni di sicurezza
  - canale nascosto di analisi
  - valutatore esegue test di penetrazione
  - TOE deve essere stato progettato e sviluppato con l'intento di raggiungere il livello EAL5 di garanzia;
    ulteriori costi di valutazione non devono essere esosi

LIVELLI DI SICUREZZA DEI CC 4

- **EAL6** - semiformally verified design and tested
  - richiede codice sorgente ben strutturato
  - Reference monitor con bassa complessità
  - valutatore effettua intensivi test di penetrazione
  - costo della valutazione aumenta
- **EAL7** - formally verified design and tested
  - sviluppatore fornisce elevato livello di progettazione
  - dimostra corrispondenza tra tutte le rappresentazioni di funzioni di sicurezza
  - EAL7 tipicamente realizzato solo con un TOE che ha una ben precisa funzionalità di sicurezza e si prestano ad ampie analisi formali

CORRISPONDENZA DEI LIVELLI DI FIDUCIA

La tabella seguente dà corrispondenza dei livelli di fiducia delle diverse metodologie.

TCSEC	ITSEC	CC
D	E0	-
-	-	EAL1
C1	E1	EAL2
C2	E2	EAL3
B1	E3	EAL4
B2	E4	EAL5
B3	E5	EAL6
A1	E6	EAL7

CC offre un livello inferiore a qualsiasi livello precedentemente offerto.

ESEMPI DI VALUTAZIONE DI SO COI CC

- EAL4:
  - Sun Solaris (TM) 8 Operating Environment
  - HP-UX (11i) Version 11.11
  - B1/EST-X Version 2.0.1 with AIX, Version 4.3.1
- EAL4+:
  - AIX 5L for POWER V5.2 Programm Number 5765-E62
  - Windows 2000 Professional, Server, and Advanced Server with SP3 and Q326886 Hotfix
- EAL3:
  - SGI Trusted IRIX/CMW Version 6.5.13

UN PRODOTTO CERTIFICATO CC È SICURO?

Ogni vulnerabilità che possa compromettere il prodotto nella configurazione di valutazione, dovrebbe comportare:

- cancellazione volontaria da parte del produttore della propria certificazione
- rivalutazione del prodotto per includere l'applicazione delle patch per fissare le vulnerabilità nella configurazione di valutazione
- certificazione dovrebbe essere sospesa o cancellata dall'ente che l'ha emessa

UN PRODOTTO CERTIFICATO CC È SICURO? ESEMPIO

Microsoft Windows 2000 è un prodotto certificato EAL4+, ma sono ancora pubblicate regolarmente da Microsoft patch di sicurezza per vulnerabilità.

- Certificazione EAL4+ di Microsoft Windows 2000, deve essere considerata sicura solo nella configurazione specificata da Microsoft stesso.

La valutazione di Microsoft Windows 2000 resta EAL4+ solo se non si applica di nessuna patch.

METODOLOGIE DI VALUTAZIONE

- CEM - Common Evaluation Methodology: specifica le misure che devono essere seguite per convalidare i requisiti di garanzia di sicurezza in un ST.
- CCRA - Common Criteria Recognition Agreement: prevede il riconoscimento delle valutazioni effettuate in altri paesi.
  - Livelli di garanzia indirizzabili da EAL1 a EAL4, ivelli più elevati ammessi solo all'interno di un unico paese.
- CCEVS - Common Criteria Evaluation and Validation Scheme: programma nazionale statunitense per l'esecuzione di valutazioni di sicurezza secondo i CC.

STANDARDS DI QUALITÀ

Come valutare il modo in cui un prodotto è sviluppato, senza riferimenti al prodotto stesso?
Società denominate - *'certified producer of secure systems'*.

Approccio diffuso per quanto riguarda il controllo della qualità: Standard **ISO 9000** - raccomanda attuare gestione qualità interna e affidabilità qualità esterna per attestare qualità prodotti.

- miglior argomento di vendita rispetto a un certificato di sicurezza
- costi della valutazione molto ridotti

ECMA(1993) suggerisce Standard di qualità ISO 9000 come alternativa alla valutazione.

CONCLUSIONI: UNO SFORZO BEN SPESO?

- La valutazione della sicurezza in accordo con i CC è richiesta in alcuni paesi dai clienti del settore pubblico
- I maggiori venditori di SO e DBMS offrono prodotti valutati

In verità, al di fuori del settore pubblico vi è stato poco entusiasmo per la valutazione dei prodotti

Una eccezione corrente sono i SW per le **smart card**

CONCLUSIONI: UNO SFORZO BEN SPESO?

Valutazione della sicurezza criticata per i suoi costi eccessivi

- Costo valutazione varia fra 10%-40% dei costi di sviluppo

Problemi persistenti:

- ambiguità di interpretazione dei criteri

CONCLUSIONI: UNO SFORZO BEN SPESO?

Valutazione della sicurezza criticata per i suoi costi eccessivi

- Costo valutazione varia fra 10%-40% dei costi di sviluppo

Problemi persistenti:

- ambiguità di interpretazione dei criteri
- segretezza dei processi di valutazione

CONCLUSIONI: UNO SFORZO BEN SPESO?

Valutazione della sicurezza criticata per i suoi costi eccessivi

- Costo valutazione varia fra 10%-40% dei costi di sviluppo

Problemi persistenti:

- ambiguità di interpretazione dei criteri
- segretezza dei processi di valutazione
- costi della ri-valutazione di nuove versioni di prodotti

Conclusioni: Uno sforzo ben speso?

Valutazione della sicurezza criticata per i suoi costi eccessivi

- Costo valutazione varia fra 10%-40% dei costi di sviluppo

Problemi persistenti:

- ambiguità di interpretazione dei criteri
- segretezza dei processi di valutazione
- costi della ri-valutazione di nuove versioni di prodotti

CONCLUSIONI: UNO SFORZO BEN SPESO?

Valutazione della sicurezza criticata per i suoi costi eccessivi

- Costo valutazione varia fra 10%-40% dei costi di sviluppo

Problemi persistenti:

- ambiguità di interpretazione dei criteri
- segretezza dei processi di valutazione
- costi della ri-valutazione di nuove versioni di prodotti

Certificati riferiti a specifica versione o particolare configurazione del prodotto
Sistemi/prodotti si evolvono e rispettiva valutazione si riferisce a una versione non più in uso pertanto non offre garanzie di sicurezza


FINE