SECURE NETWORK BV TECH

VICENZA

Non tutte le vulnerabilità sono uguali

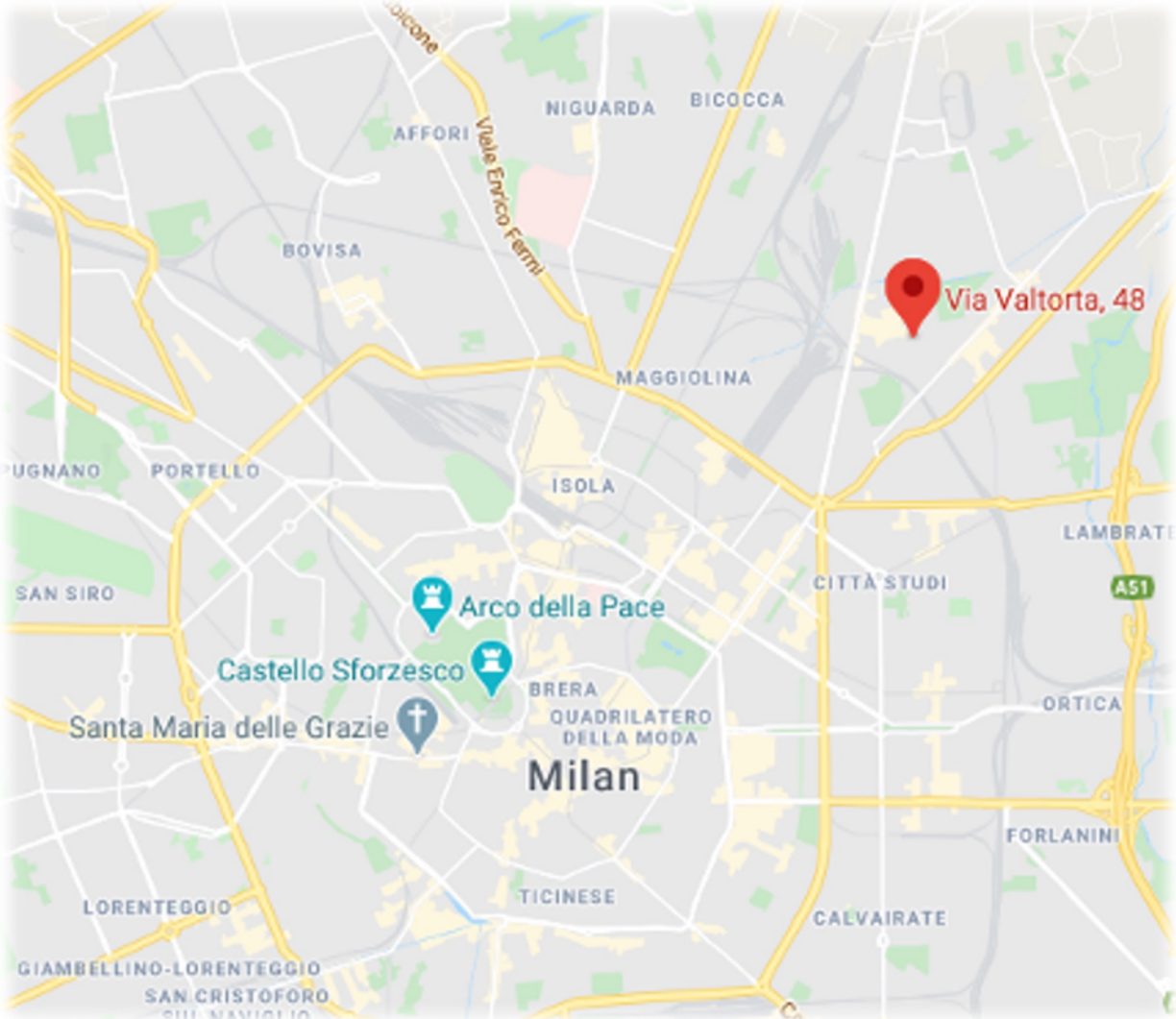
Eros Lever

Online, 01/02/2024

CHI SIAMO

- Servizi Professionali di Information Security
  - Security Assessment
  - Information Security Management
  - Security Training
  - Digital Forensics

- 2004 - Stefano Zanero & Alvise Biffi
- Via Valtorta 48 – Milano
- www.securenetwork.it



VICENZA

SECURE NETWORK BV TECH

$ WHOAMI

> Eros Lever

> Ingegneria Informatica @ Politecnico di Milano (2013)

> Sicurezza Informatica dal 2011
  Application Security
    Web app, web services, mobile apps
  Infrastructure Security
    External network, internal network, reti WiFi
  Firmware Testing & Reversing
    Prodotti IoT (Internet of Things)
  Penetration Test, vulnerability Assessment, Digital Forensics, etc…

> CTO @ Secure Network (2021)

VICENZA

SECURE NETWORK BV*TECH

AGENDA

Argomenti del giorno

- Introduzione ai concetti di vulnerabilità e rischio
- Metodologie di valutazione del rischio
- Ordine dal caos: classificazione di vulnerabilità ed attacchi
- Vulnerabilità note e contestualizzazione del rischio
- Monitoraggio e notifica di nuove vulnerabilità
- Tecniche per la riduzione dei rischi
- Security by Design e la sicurezza come processo continuo

SICUREZZA INFORMATICA

Requisiti fondamentali ("paradigma CIA"):

Confidentiality	Riservatezza
Integrity	Integrità
Availability	Disponibilità

*Il terzo requisito è in **diretto conflitto** con le soluzioni dei primi due*

BUG VS VULNERABILITÀ

- Bug = difetto funzionale
  - Risulta in un malfunzionamento
  - Può non avere impatti sulla sicurezza

- Il software dovrebbe rispettare determinate **specifiche**
  - Mancato rispetto di specifiche → bug
  - Mancato rispetto di specifiche di sicurezza → vulnerabilità

CONCETTI BASE

Vulnerabilità

Difetto nella protezione delle informazioni che permette di violare uno o più requisiti C, I, A

- Vulnerabilità di un software, un'infrastruttura, un processo, una struttura fisica, …

Exploit

Una specifica tecnica che permette di sfruttare una o più vulnerabilità

Attacco

Utilizzo intenzionale di uno o più exploit da parte di un attore esterno o interno

VULNERABILITÀ ED EXPLOIT PUBBLICI

- Alcune vulnerabilità sono pubbliche:
  - dettagli tecnici liberamente disponibili
  - probabilmente esiste una patch o un workaround per risolverla

- Per alcune vulnerabilità pubbliche, esistono exploit pubblici, disponibili online e all'interno di *framework* di testing
  - utilizzati per scopi sia malevoli che legittimi

Essere in grado di identificare vulnerabilità e sviluppare exploit è una parte essenziale delle abilità di un professionista della sicurezza informatica

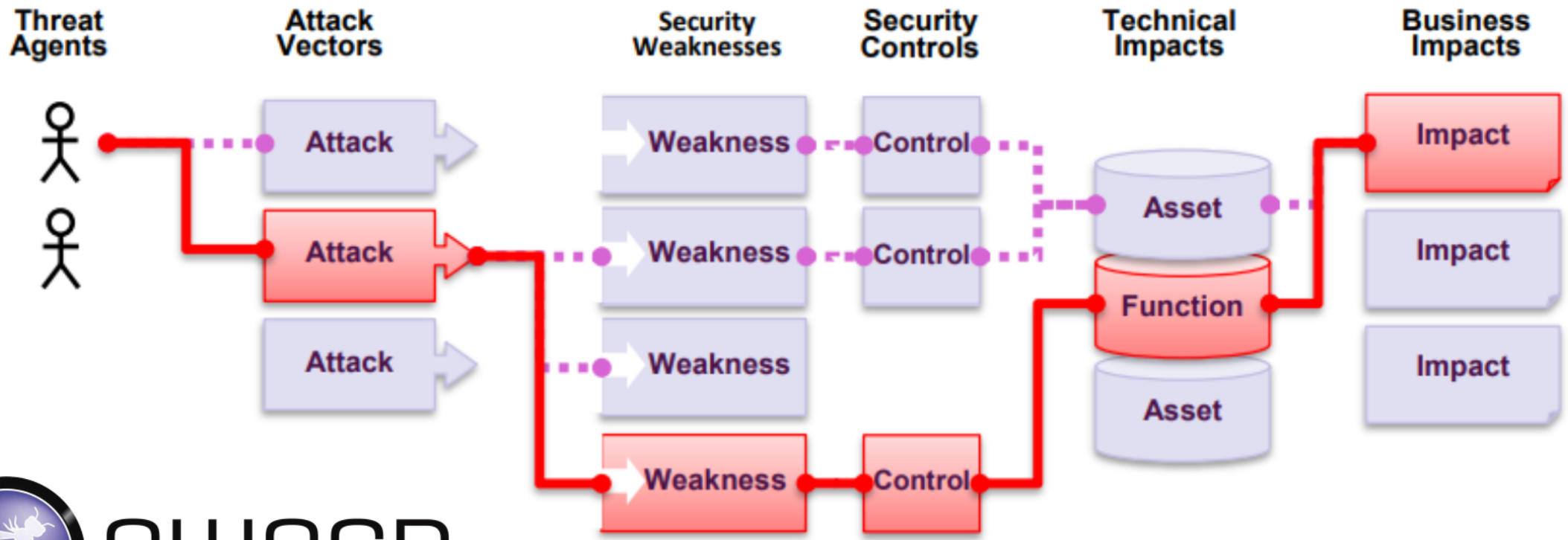
COME VALUTARE IL RISCHIO?

- È necessario individuare i fattori coinvolti
  - Danni subiti
    - Danni economici diretti
    - Perdita di clienti e danni d'immagine
    - Furto di informazioni
    - Sanzioni GDPR e violazioni
    - Costi di analisi, mitigazione o risoluzione
  - Danni potenziali
    - Come possiamo valutarli?

E IL RISCHIO POTENZIALE?

- Quanto è probabile che si verifichi un incidente/attacco?
- Quali asset verrebbero coinvolti?
- Quanto sono esposti/critici gli asset interessati?
- Sono presenti sistemi di sicurezza atti a mitigare i danni?

OWASP THREAT FACTORS



OWASP
Open Web Application Security Project

VICENZA

SECURE NETWORK BV*TECH

UNA FORMULA PER IL «RISCHIO»

- Valutazione statistica ed economica dell'esposizione ad un danno per la presenza di vulnerabilità e minacce

$$Rischio = \underbrace{Asset}_{\text{controllabili}} \; X \; \underbrace{Vulnerabilità}_{\text{variabile indipendente}} \; X \; Minacce$$

- Può essere difficile bilanciare
  - riduzione delle vulnerabilità
  - contenimento dei danni
  - costi implementativi/manutentivi (o anche solo di analisi)

OWASP RISK RATING

Rischio = Probabilità di accadimento * Impatto

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

OWASP
Open Web Application
Security Project

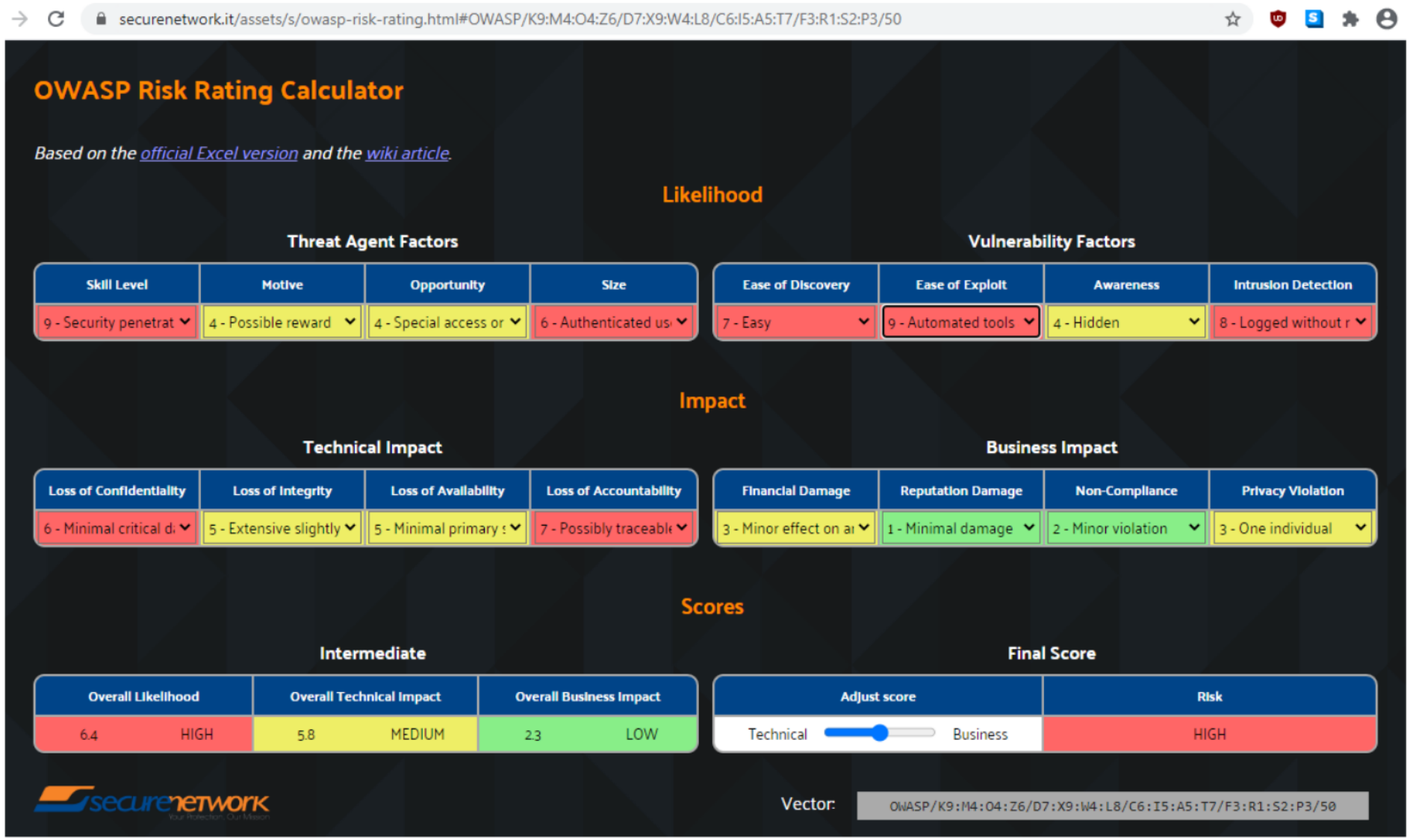
VICENZA

SECURE NETWORK BV TECH

CATEGORIZZAZIONE DEI FATTORI

- Threat Agent
  - Skill Level
  - Motive
  - Opportunity
  - Size
- Vulnerability
  - Ease of Discovery
  - Ease of Exploit
  - Awareness
  - Intrusion Detection
- Technical Impact
  - Confidentiality
  - Integrity
  - Availability
  - Accountability
- Business Impact
  - Financial Damage
  - Reputation Damage
  - Non-compliance
  - Privacy Violation

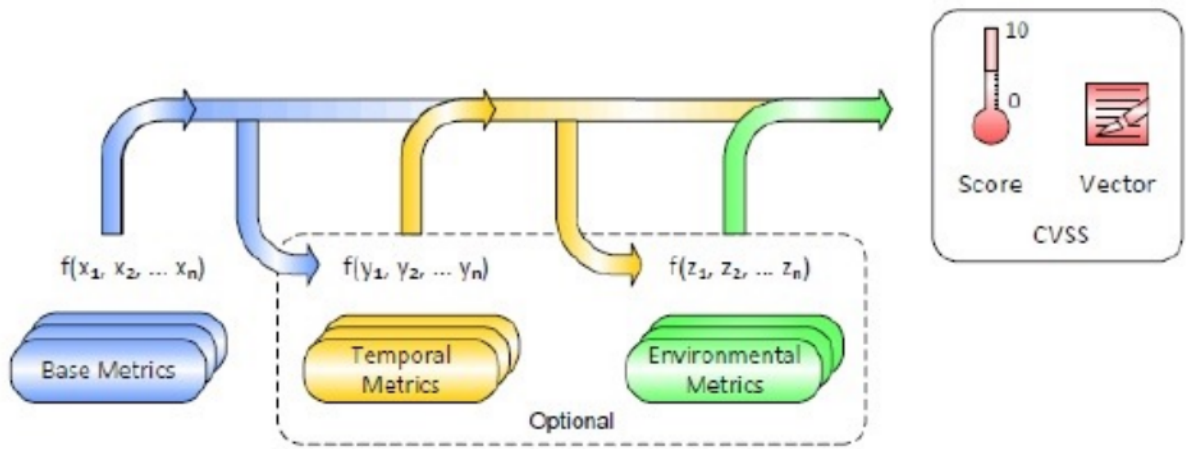
OWASP CALCULATOR



tinyurl.com/OwaspCalc

COMMON VULNERABILITY SCORING SYSTEM

- CVSS si basa su tre punteggi:
  - **Base score**: fattori fissi per singola vulnerabilità
  - **Temporal score**: possono variare nel tempo
  - **Environmental score**: varianti legate al contesto



CALCOLATORE CVSS

Base Score — 6.5 (Medium)

Attack Vector (AV)

Network (N) | Adjacent (A) | Local (L) | Physical (P)

Attack Complexity (AC)

Low (L) | High (H)

Privileges Required (PR)

None (N) | Low (L) | High (H)

User Interaction (UI)

None (N) | Required (R)

Scope (S)

Unchanged (U) | Changed (C)

Confidentiality (C)

None (N) | Low (L) | High (H)

Integrity (I)

Temporal Score — 5.9 (Medium)

Exploit Code Maturity (E)

Not Defined (X) | Unproven (U) | Proof-of-Concept (P) | Functional (F) | High (H)

Remediation Level (RL)

Not Defined (X) | Official Fix (O) | Temporary Fix (T) | Workaround (W) | Unavailable (U)

Report Confidence (RC)

Not Defined (X) | Unknown (U) | Reasonable (R) | Confirmed (C)

Environmental Score — 6.3 (Medium)

Confidentiality Requirement (CR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Integrity Requirement (IR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Availability Requirement (AR)

Not Defined (X) | Low (L) | Medium (M) | High (H)

Modified Attack Vector (MAV)

Not Defined (X) | Network | Adjacent Network | Local | Physical

Modified Attack Complexity (MAC)

Not Defined (X) | Low | High

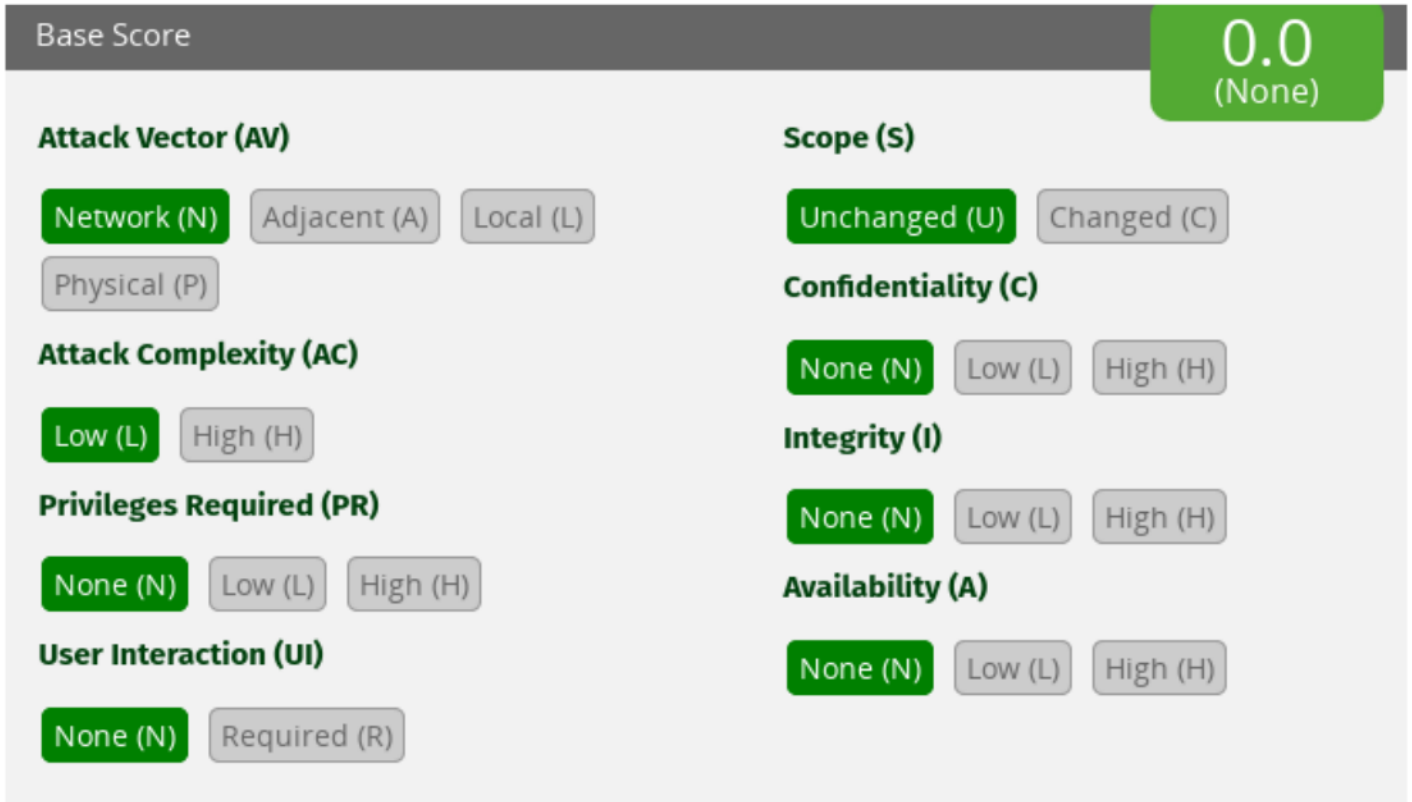
Modified Privileges Required (MPR)

Not Defined (X) | None | Low | High

http://first.org/cvss/calculator/3.1

CALCOLO DEL CVSS: BASE SCORE

- Caratteristiche intrinseche della problematica
  - Da dove può arrivare l'aggressore?
  - Quanto è difficile sfruttarla?
  - Quanti "danni" può fare?
- Rimane fisso nel tempo



CALCOLO DEL CVSS: TEMPORAL SCORE

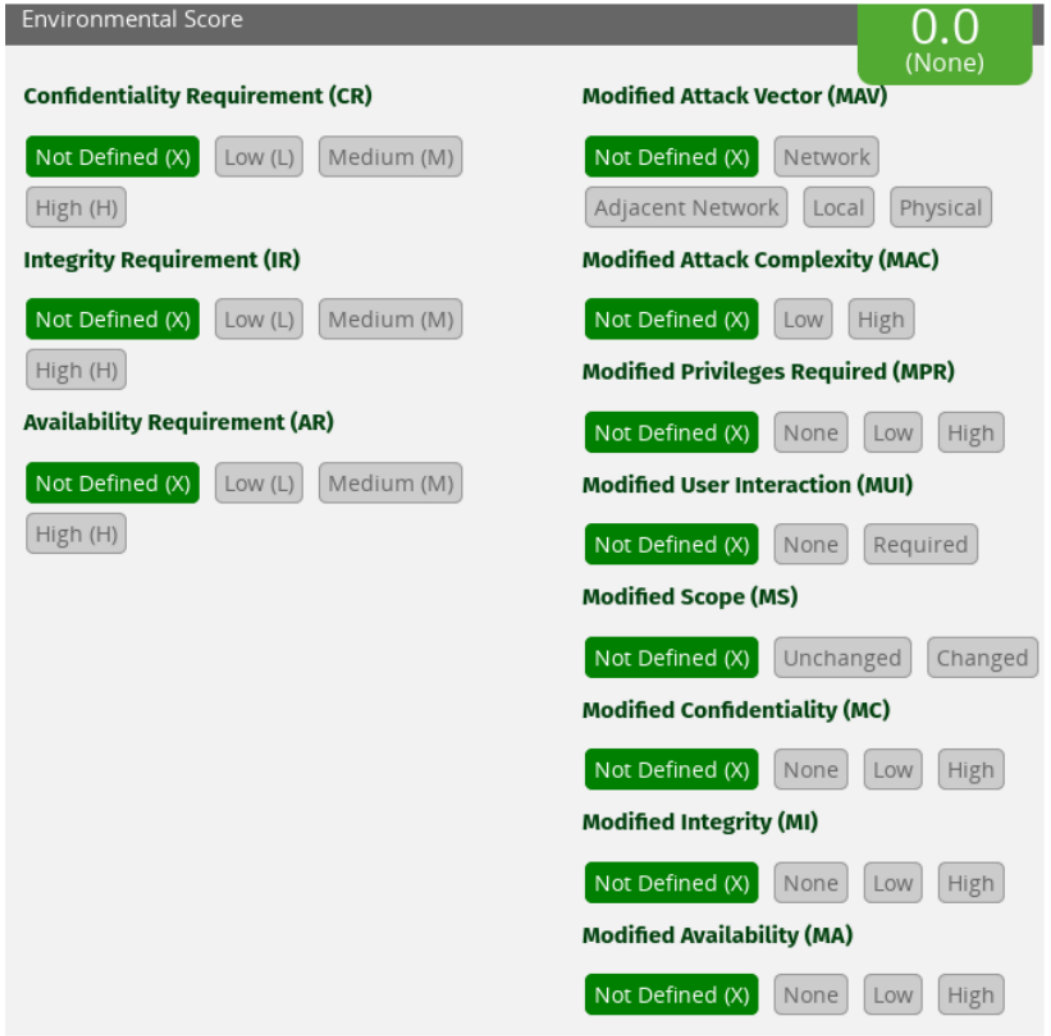
- Stato dell'arte degli exploit
  - Quanto è maturo l'exploit?
  - Posso rimediare?
  - Quanto sono sicuro che sia presente?
- Cambia nel tempo
  - Rilascio di nuovi exploit, più «affidabili» per sfruttare la stessa vulnerabilità
  - Rilascio di un aggiornamento risolutivo

VICENZA

SECURE NETWORK BV TECH

CALCOLO DEL CVSS: ENVIRONMENTAL SCORE

- Personalizzazione dello score
  - Quali sono i requisiti aziendali?
  - Quali controlli ci sono?
  - Quali mitigation ci sono?
- Diverse per ogni azienda
- Possono cambiare nel tempo



VICENZA

SECURE NETWORK BV TECH

VALUTAZIONE DEGLI IMPATTI: STRIDE

- Definito da Microsoft, non valuta direttamente il rischio ma aiuta a comprendere i possibili impatti:

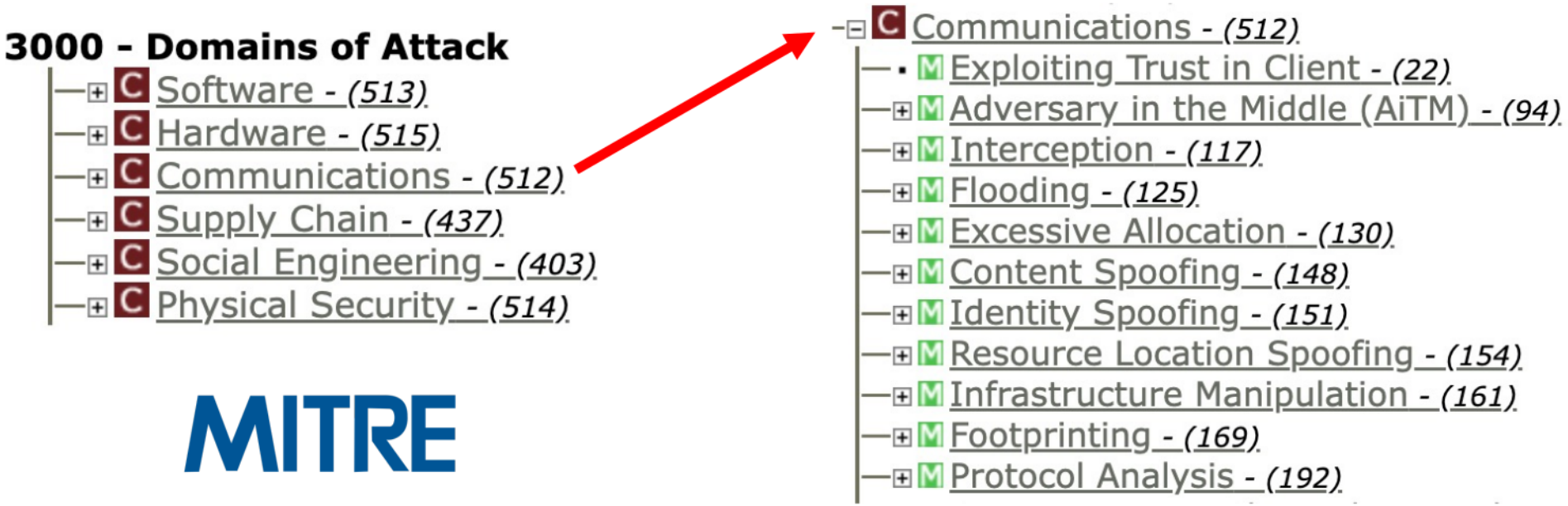
Threat	Property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiability
Information disclosure	Confidentiality
Denial of service	Availability
Elevation of privilege	Authorization

Microsoft

- Si usa in fase di design, o di analisi di un sistema, per verificare la resilienza a questi possibili impatti

VALUTAZIONE DEGLI ATTACCHI: CAPEC

- Definito da MITRE, categorizza famiglie di attacchi:
  - Common Attack Pattern Enumeration and Classification



- Si usa in fase di design, o di analisi di un sistema, per verificare la resilienza a questi possibili attacchi

CATEGORIE DI DIFETTI SOFTWARE: CWE

- **C**ommon **W**eakness **E**numeration: definito da MITRE
- Usato per *categorizzare* la natura delle vulnerabilità

699 - Software Development

- API / Function Errors - *(1228)*
- Audit / Logging Errors - *(1210)*
- Authentication Errors - *(1211)*
- Authorization Errors - *(1212)*
- Bad Coding Practices - *(1006)*
- Behavioral Problems - *(438)*
- Business Logic Errors - *(840)*
- Communication Channel Errors
- Complexity Issues - *(1226)*
- Concurrency Issues - *(557)*
- Credentials Management Errors
- Cryptographic Issues - *(310)*
- Key Management Errors - *(320)*
- Data Integrity Issues - *(1214)*
- Data Processing Errors - *(19)*
- Data Neutralization Issues - *(137*
- Documentation Issues - *(1225)*
- File Handling Issues - *(1219)*
- Encapsulation Issues - *(1227)*
- Error Conditions, Return Values,
- Expression Issues - *(569)*
- Handler Errors - *(429)*
- Information Management Errors
- Initialization and Cleanup Errors
- Data Validation Issues - *(1215)*
- Lockout Mechanism Errors - *(121*
- Memory Buffer Errors - *(1218)*
- Numeric Errors - *(189)*
- Permission Issues - *(275)*
- Pointer Issues - *(465)*
- Privilege Issues - *(265)*
- Random Number Issues - *(1213*
- Resource Locking Problems - *(4*
- Resource Management Errors -
- Signal Errors - *(387)*
- State Issues - *(371)*
- String Errors - *(133)*
- Type Errors - *(136)*
- User Interface Security Issues
- User Session Errors - *(1217)*

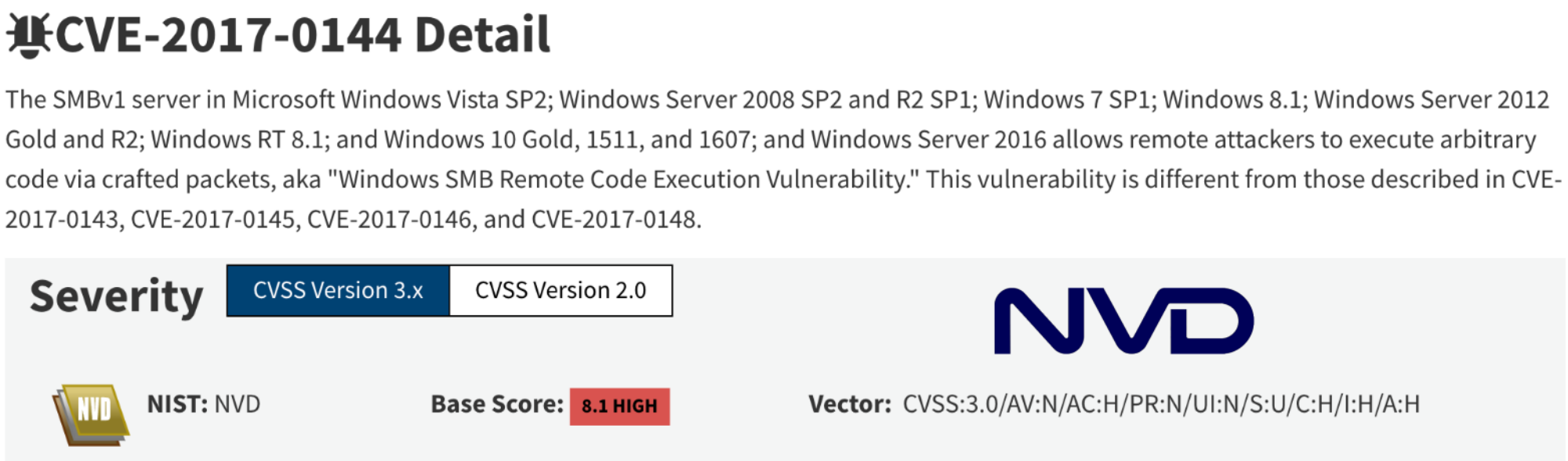
MITRE

VICENZA

SECURE NETWORK BV TECH

DATABASE DI VULNERABILITÀ PUBBLICHE: CVE

- **C**ommon **V**ulnerabilities and **E**xposures: definito da MITRE
  - Di fatto, «IL» database delle vulnerabilità note, usato dal NIST americano per il *National Vulnerability Database* (NVD)
  - Ogni vulnerabilità ha un ID univoco «*CVE-<YEAR>-<NUMBER>*»



LIMITI DELLE CVE

- Vengono tracciati solo i prodotti più diffusi
  - Microsoft Windows, Oracle Java, Apache HTTP Server…
- Spesso le descrizioni non sono chiare
  - Troppo generiche o perfino errate/imprecise

    «***Unspecified vulnerability*** *in the Core RDBMS component in Oracle Database Server 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, and 11.2.0.3 allows remote authenticated users to affect integrity via* ***unknown vectors*** *related to Privileged Account.»*
- La valutazione CVSS è spesso limitata al base-score
  - Non traspare la «sfruttabilità» reale, spesso richiede configurazioni custom
  - La presenza di exploit non è ben monitorata
- Non è chiaro il meccanismo di remediation/mitigation

VARIABILITÀ DEL RISCHIO 1/2

- Anche impegnandosi a usare gli standard, le valutazioni possono differire a seconda delle informazioni disponibili e del metro di valutazione usato
- Esempio: CVE-2020-10627

> *"Il microinfusore per insulina Insulet Omnipod Insulin Management System, ID prodotto 19191 e 40160, è progettato per comunicare in modalità wireless RF con un dispositivo Personal Diabetes Manager prodotto da Insulet. Questo protocollo di comunicazione RF wireless non implementa correttamente l'autenticazione o l'autorizzazione. Un utente malintenzionato che abbia accesso a uno dei modelli di microinfusore per insulina interessati potrebbe essere in grado di modificare e/o intercettare i dati. Questa vulnerabilità potrebbe anche consentire agli aggressori di modificare le impostazioni del microinfusore e controllare la somministrazione di insulina."*

VARIABILITÀ DEL RISCHIO 2/2

CVSS 2.0 Severity and Metrics:

NIST: NVD **Base Score:** 4.8 MEDIUM **Vector:** (AV:A/AC:L/Au:N/C:P/I:P/A:N)

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 8.1 HIGH **Vector:** CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

CNA: ICS-CERT **Base Score:** 7.3 HIGH **Vector:** CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L

CVSS v4.0

Base	8.6 CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/S:P
Base + Environmental	9.7 CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/MSI:S/S:P

VICENZA

SECURE NETWORK BV TECH

CVSS 2 vs CVSS 3.1

- CVSS 2.0 (4.8)

Exploitability Metrics

Access Vector (AV)*

Local (AV:L)	**Adjacent Network (AV:A)**	Network (AV:N)

Access Complexity (AC)*

High (AC:H)	Medium (AC:M)	**Low (AC:L)**

Authentication (Au)*

Multiple (Au:M)	Single (Au:S)	**None (Au:N)**

Impact Metrics

Confidentiality Impact (C)*

None (C:N)	**Partial (C:P)**	Complete (C:C)

Integrity Impact (I)*

None (I:N)	**Partial (I:P)**	Complete (I:C)

Availability Impact (A)*

None (A:N)	Partial (A:P)	Complete (A:C)

- CVSS 3.1 (8.1)

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N)	**Adjacent Network (AV:A)**	Local (AV:L)	Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L)	High (AC:H)

Privileges Required (PR)*

None (PR:N)	Low (PR:L)	High (PR:H)

User Interaction (UI)*

None (UI:N)	Required (UI:R)

Scope (S)*

Unchanged (S:U)	Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N)	Low (C:L)	**High (C:H)**

Integrity Impact (I)*

None (I:N)	Low (I:L)	**High (I:H)**

Availability Impact (A)*

None (A:N)	Low (A:L)	High (A:H)

VICENZA

SECURE NETWORK BV*TECH

CVSS 3.1 – DIFFERENT AUTHORITY

- CVSS 3.1 (8.1 NIST)

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N)	**Adjacent Network (AV:A)**	Local (AV:L)	Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L)	High (AC:H)

Privileges Required (PR)*

None (PR:N)	Low (PR:L)	High (PR:H)

User Interaction (UI)*

None (UI:N)	Required (UI:R)

Scope (S)*

Unchanged (S:U)	Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N)	Low (C:L)	**High (C:H)**

Integrity Impact (I)*

None (I:N)	Low (I:L)	**High (I:H)**

Availability Impact (A)*

None (A:N)	Low (A:L)	High (A:H)

- CVSS 3.1 (7.3 ICS-CERT)

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N)	Adjacent Network (AV:A)	**Local (AV:L)**	Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L)	High (AC:H)

Privileges Required (PR)*

None (PR:N)	Low (PR:L)	High (PR:H)

User Interaction (UI)*

None (UI:N)	Required (UI:R)

Scope (S)*

Unchanged (S:U)	Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N)	**Low (C:L)**	High (C:H)

Integrity Impact (I)*

None (I:N)	Low (I:L)	**High (I:H)**

Availability Impact (A)*

None (A:N)	**Low (A:L)**	High (A:H)

VICENZA

SECURE NETWORK BV TECH

CVSS 3.1 vs CVSS 4.0

- CVSS 3.1 (8.1 NIST)

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N)	**Adjacent Network (AV:A)**	Local (AV:L)	Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L)	High (AC:H)

Privileges Required (PR)*

None (PR:N)	Low (PR:L)	High (PR:H)

User Interaction (UI)*

None (UI:N)	Required (UI:R)

Scope (S)*

Unchanged (S:U)	Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N)	Low (C:L)	**High (C:H)**

Integrity Impact (I)*

None (I:N)	Low (I:L)	**High (I:H)**

Availability Impact (A)*

None (A:N)	Low (A:L)	High (A:H)

- CVSS 4.0 (8.6 FIRST)

Attack Vector (AV):	Network (N)	**Adjacent (A)**	Local (L) / Physical (P)
Attack Complexity (AC):	**Low (L)**	High (H)	
Attack Requirements (AT):	**None (N)**	Present (P)	
Privileges Required (PR):	**None (N)**	Low (L)	High (H)
User Interaction (UI):	**None (N)**	Passive (P)	Active (A)
Confidentiality (VC):	**High (H)**	Low (L)	None (N)
Integrity (VI):	**High (H)**	Low (L)	None (N)

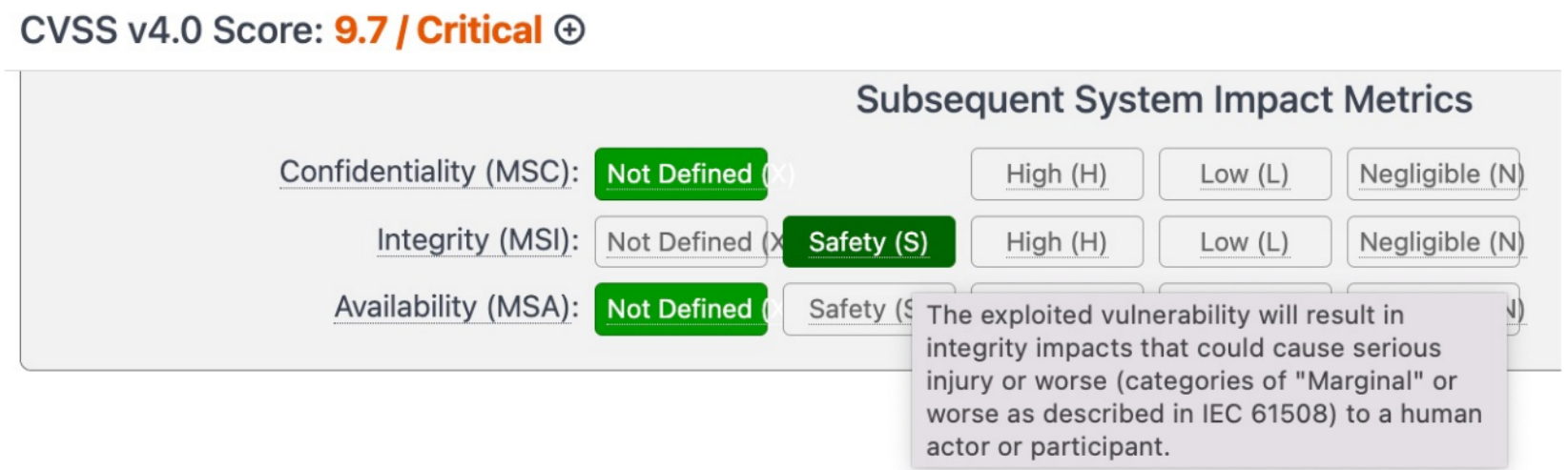
Availability (VA):	High (H)	Low (L)	**None (N)**
Confidentiality (SC):	High (H)	Low (L)	**None (N)**
Integrity (SI):	High (H)	Low (L)	**None (N)**
Availability (SA):	High (H)	Low (L)	**None (N)**
Safety (S):	Not Defined (X	Negligible (N)	**Present (P)**

VICENZA

SECURE NETWORK BV*TECH

ENVIRONMENTAL MODIFIER

- CVSS 4.0 (9.7 FIRST)



VICENZA

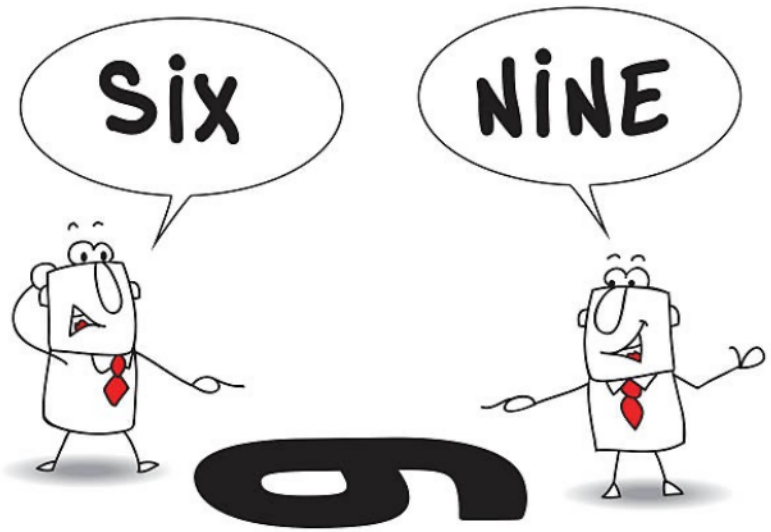
SECURE NETWORK BV'TECH

VARIABILITÀ DEL RISCHIO

- Non esiste uno score perfetto
- I parametri di valutazione possono variare

  "~~Beauty~~ Risk (?) is in the eye of the beholder"

- È importante mantenere una consistenza e una logica



APPLICABILITÀ DI UNA CVE

Nonostante esista una CVE, non è detto che la nostra installazione sia effettivamente vulnerabile.

Spesso sono necessarie particolari configurazioni o precondizioni

7. Cisco IOS Arbitrary Command Execution Vulnerability (CVE-2012-0384)

Vulnerability

Cisco IOS 12.2 through 12.4 and 15.0 through 15.2 and IOS XE 2.1.x through 2.6.x and 3.1.xS before 3.1.2S, 3.2.xS through 3.4.xS before 3.4.2S, 3.5.xS before 3.5.1S, and 3.1.xSG and 3.2.xSG before 3.2.2SG, when AAA authorization is enabled, allow remote authenticated users to bypass intended access restrictions and execute commands via a (1) HTTP or (2) HTTPS session, aka Bug ID CSCtr91106.

Attack

The vulnerability allows an attacker to bypass command authorization restrictions assigned to their specific user account and execute commands that are available to the Roll/Privilege level for which the user is assigned. For example, a user that is in a group that is assigned to Privilege level 15 (admin) but was restricted to executing a single command via AAA (RADIUS/TACACS) could exploit the vulnerability to execute any other command available to an unrestricted admin user at Privilege level 15.

OLTRE LE CVE

- È possibile monitorare il rilascio di nuove CVE?
  - A scopo difensivo: aggiornare installazioni vulnerabili
  - A scopo malevolo: sviluppare exploit per nuove vulnerabilità
- Il NIST offre una ricerca basata su "CPE"
  - CPE = < produttore, prodotto, versione >

Vendor	Product	Version
cpe:2.3:a:apache:http_server:2.4.55:*:*:*:*:*:*:* View CVEs		
apache	http_server	2.4.55

Search Parameters:

- Results Type: Overview
- Keyword (text search): cpe:2.3:a:apache:http_server:2.4.55:*:*:*:*:*:*:*
- CPE Name Search: true

There are **17** matching records.

Displaying matches **1** through **17**.

Vuln ID	Summary	CVSS Severity
CVE-2023-45802	When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection	*V3.1:* 5.9 MEDIUM *V2.0:*(not available)

VICENZA

SECURE NETWORK BV TECH

LIBRERIE, FRAMEWORK E PACCHETTI

- Oltre a specifici prodotti è possibile monitorare componenti software utilizzati
  - Dipendenze di un progetto (librerie di terze parti)
  - Pacchetti installati tramite repository (Ubuntu, RedHat)
- Esistono prodotti mirati:

SOFTWARE BILL OF MATERIALS

- Nuovi requisiti di sicurezza
  - 2021-05 "*US Executive Order on Improving the Nation's Cybersecurity*" introduce il tracciamento di una SBOM
  - Elenco <vendor, componente, versione, id, dipendenze, autore, timestamp>
- Necessità di nuovi standard
  - SPDX: Software Package Data Exchange (ISO/IEC 5692:2021)
  - CycloneDX: OWASP
  - SWID: **S**oft**w**are **Id**entification (ISO/IEC 19770-2:2015)

SOFTWARE BILL OF MATERIALS

- Nascita di nuovi strumenti (o funzionalità dedicate)
  - Synopsys Black Duck
  - CAST Highlight
  - Snyk
  - Anchore Syft
  - Aquasecurity Trivy

```
root@syft:~# syft alpine:latest
 ✔ Parsed image
 ✔ Cataloged packages      [14 packages]
NAME                    VERSION      TYPE
alpine-baselayout       3.2.0-r22    apk
alpine-baselayout-data  3.2.0-r22    apk
alpine-keys             2.4-r1       apk
apk-tools               2.12.9-r3    apk
busybox                 1.35.0-r17   apk
ca-certificates-bundle  20220614-r0  apk
libc-utils              0.7.2-r3     apk
libcrypto1.1            1.1.1q-r0    apk
libssl1.1               1.1.1q-r0    apk
musl                    1.2.3-r0     apk
musl-utils              1.2.3-r0     apk
scanelf                 1.3.4-r0     apk
ssl_client              1.35.0-r17   apk
zlib                    1.2.12-r3    apk
```

SBOM – AMBITO MEDICALE

- SBOM resa obbligatoria dalla FDA Americana

  In addition to the minimum elements identified by NTIA, for each software component contained within the SBOM, manufacturers should include in the premarket submission:

  - *The software level of support […] (e.g., the software is actively maintained, no longer maintained, abandoned);*
  - *The software component's end-of-support date;*
  - *A safety and security risk assessment of each known vulnerability (including device and system impacts);*
  - Details of applicable safety and security risk controls to address the vulnerability;

SBOM + VULNERABILITÀ

- Anchore Grype
  - Integra una SBOM (e.g., generate con Syft o Trivy) verificando se i componenti sono affetti da vulnerabilità note (usando un database locale)

```
❯ grype syft.cyclonedx
 ✔ Vulnerability DB        [no update available]
 ✔ Scanned image           [8 vulnerabilities]
NAME          INSTALLED  FIXED-IN    TYPE    VULNERABILITY         SEVERITY
busybox       1.35.0                 binary  CVE-2022-28391        High
busybox       1.35.0                 binary  CVE-2022-30065        High
certifi       2022.12.7  2022.12.07  python  GHSA-43fp-rhv2-5gv8   Medium
libcrypto3    3.0.7-r0   3.0.7-r2    apk     CVE-2022-3996         High
libssl3       3.0.7-r0   3.0.7-r2    apk     CVE-2022-3996         High
setuptools    65.5.0                 python  CVE-2022-40897        Medium
setuptools    65.5.0     65.5.1      python  GHSA-r9hx-vwmv-q579   High
sqlite-libs   3.40.0-r0              apk     CVE-2022-46908        High
```

MONITORAGGIO FORNITORI

- Oltre a singole vulnerabilità, prodotti e loro componenti, è sempre più importante monitorare la cybersecurity dei propri fornitori e della propria azienda
  - *Third-Party Cyber Risk Management*
- Esistono strumenti come SecurityScorecard

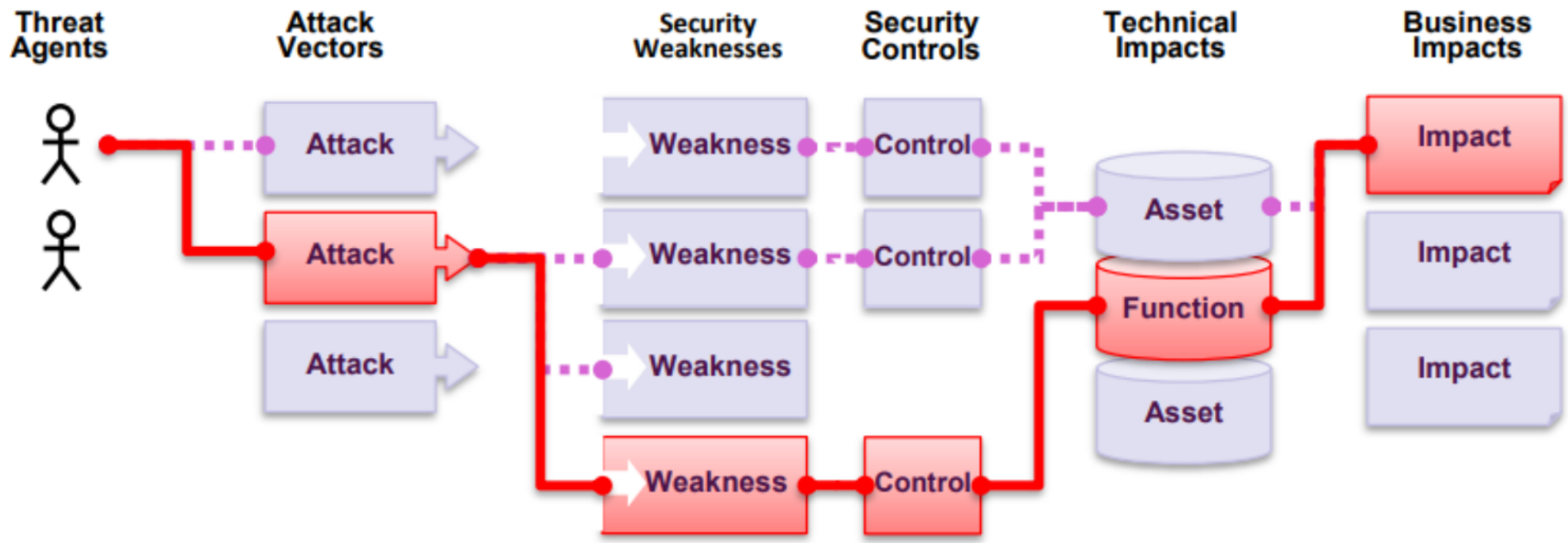
Third-Party Cyber Risk Management
Designed to put you in control

Automatic Vendor Detection
Know the unknown

Supply Chain Risk Intelligence
Prevent cyberattacks

Security Questionnaires
Automatically send and validate vendor questionnaires

RIDUZIONE DEL RISCHIO



- Ridurre l'esposizione dei sistemi agli attacchi
- Ridurre le problematiche presenti
- Introdurre nuovi controlli di sicurezza
- Valutare variazioni tecnologiche o di business

VICENZA

SECURE NETWORK BV*TECH

RIDUZIONE DELL'ESPOSIZIONE

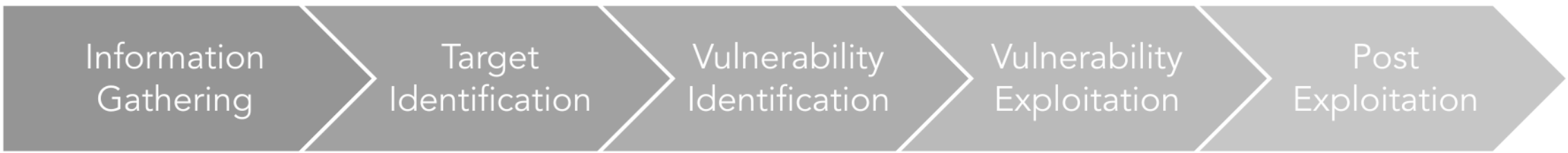
- È dapprima necessario conoscere la superficie esposta
  - Qualora non lo sia, è necessaria un'analisi
- Identificare flussi necessari, superflui o errati
  - È necessaria una conoscenza dei sistemi e delle tecnologie
- Chiusura/disattivazione di servizi non necessari
- Segregazione/isolamento dei servizi critici
  - Segregazione di rete in subnet e VLAN separate

RIDUZIONE DELLE PROBLEMATICHE NOTE

- Realizzazione di un inventario
  - Hardware (computer, server, appliance,…)
  - Software (installato localmente, erogato da fornitori, in cloud…)
  - Infrastrutturale e tecnologico (protocolli e prodotti utilizzati)
- Aggiornamento periodico e proattivo dei sistemi e software
  - Evitare la presenza di component affetti da CVE note
- Gestione delle “eccezioni”
  - Ciò che non può essere aggiornato
  - Ciò che non è attivamente mantenuto
  - Componenti meno diffusi, non tracciati da CVE

E LE PROBLEMATICHE (NON ANCORA) NOTE?

- Conduzione di analisi e test mirati volti a rilevarle
  - Revisione dei requisiti di sicurezza
  - Analisi del Threat Model
  - Vulnerability Scan (automatizzato)
  - Vulnerability Assessment
  - Penetration Test
  - Simulazione di scenari d'attacco
  - Security-oriented Code Review



INTRODUZIONE DI NUOVI CONTROLLI

- A livello di rete
  - Firewall, VLAN
  - NGFW, ZeroTrust
- Localmente e in maniera centralizzata
  - Endpoint protection (EDR/XDR)
  - Log Management, Alerting, SIEM, SOAR, SOC
- Hardening
  - Riduzione dei privilegi, irrobustimento autorizzativo

HARDENING DEI SISTEMI

- Non esiste una guida "universale", ogni prodotto ha le sue configurazioni e caratteristiche. Esistono però guide di riferimento per alcuni prodotti principali
  - DISA STIG (Security Technical Implementation Guides)
  - CIS (Center for Internet Security) Benchmarks

CIS CentOS Linux 8 Benchmark

v2.0.0 - 02-23-2022

5.5 Configure PAM 619

5.5.1 Ensure password creation requirements are configured (Automated) 620

5.5.2 Ensure lockout for failed password attempts is configured (Automated) .. 624

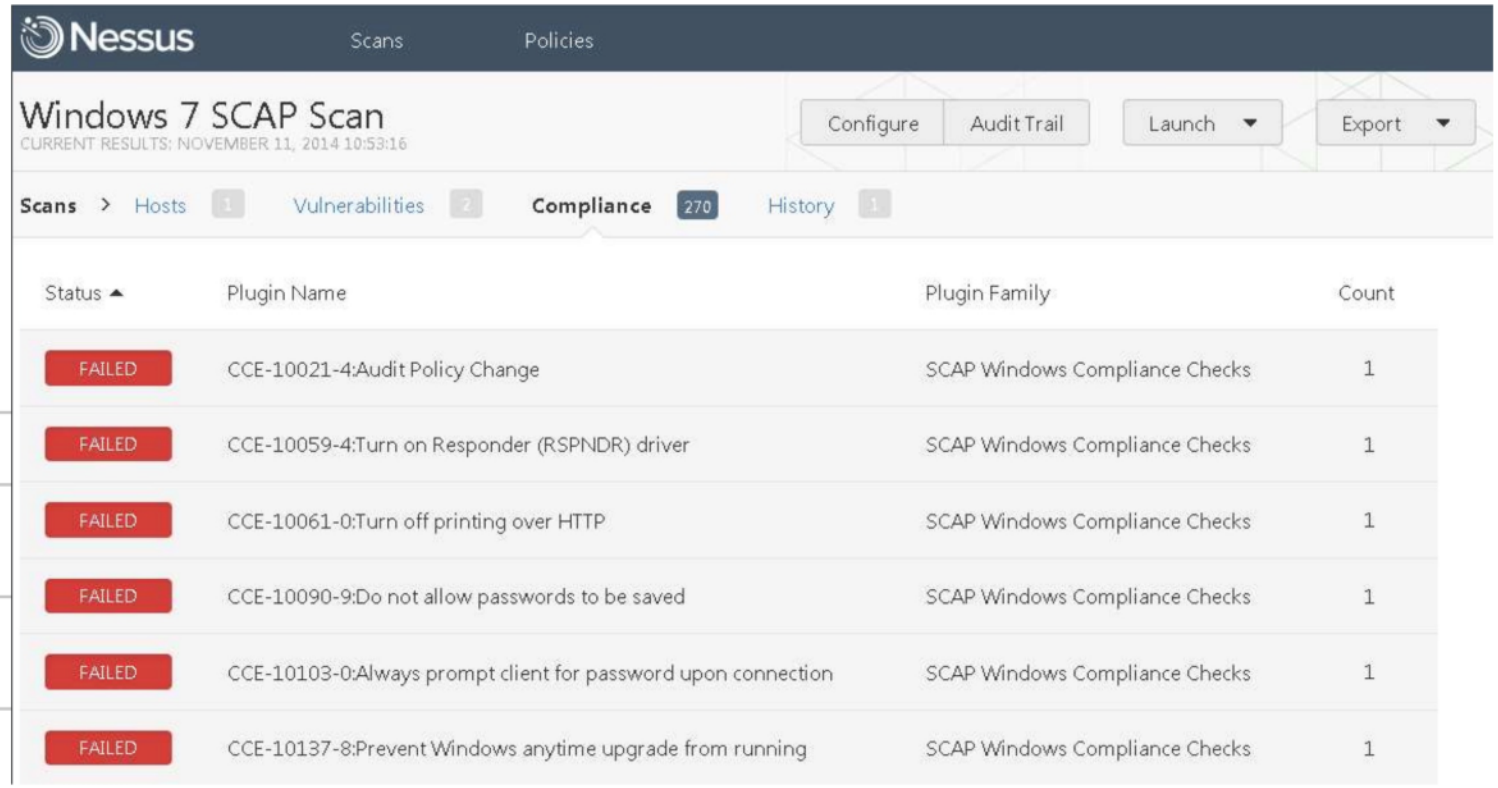
5.5.3 Ensure password reuse is limited (Automated) 628

5.5.4 Ensure password hashing algorithm is SHA-512 (Automated) 631

HARDENING DEI SISTEMI

- Esistono strumenti per la verifica dello stato di hardening (basati su CIS/STIG)
  - Tenable Nessus
  - OpenSCAP
  - Localtoast

Microsoft Windows 10 STIG Benchmark - Ver 2, Rel 9	104.35 KB	30 Oct 2023
Microsoft Windows 11 STIG Benchmark - Ver 1, Rel 3	96.95 KB	30 Oct 2023
Microsoft Windows Defender Firewall with Advanced Security STIG Benchmark - Ver 2, Rel 3	10.95 KB	30 Oct 2023
Microsoft Windows Server 2016 STIG Benchmark - Ver 2, Rel 5	93.06 KB	30 Oct 2023
Microsoft Windows Server 2019 STIG Benchmark - Ver 2, Rel 5	99.99 KB	30 Oct 2023
Microsoft Windows Server 2022 STIG Benchmark - Ver 1, Rel 3	93.73 KB	30 Oct 2023



VICENZA

SECURE NETWORK BV*TECH

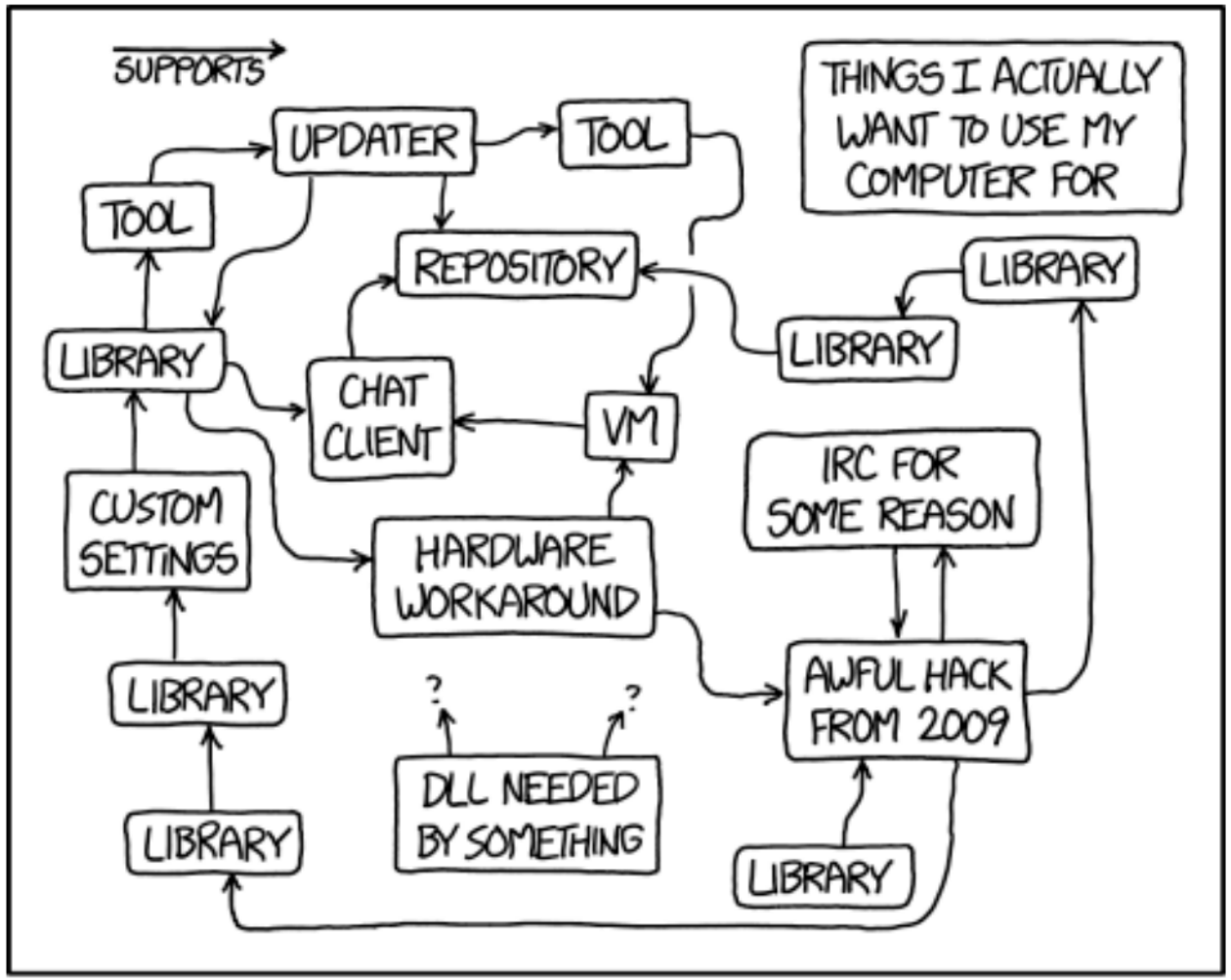
VARIAZIONI TECNOLOGICHE

- Qualora non risulti possibile aggiornare, mitigare o più in generale mettere in sicurezza il sistema:

- Sostituire i component problematici
- Mitigare il più possibile e valutare l'accettazione del rischio residuo
- Terminare il progetto prima di una eventuale compromissione

SECURITY BY DESIGN

- Messa in sicurezza di un sistema fin dalla sua progettazione
  - Meglio spendere X in fase di design e prototipazione che 100X per richiamare dispositivi vulnerabili, sostituire i componenti interessati, aggiornarli e resituirli ai client
  - Anche a livello implementativo e di manutenzione, è più semplice partire col piede giusto piuttosto che mettere una pezza sopra l'altra

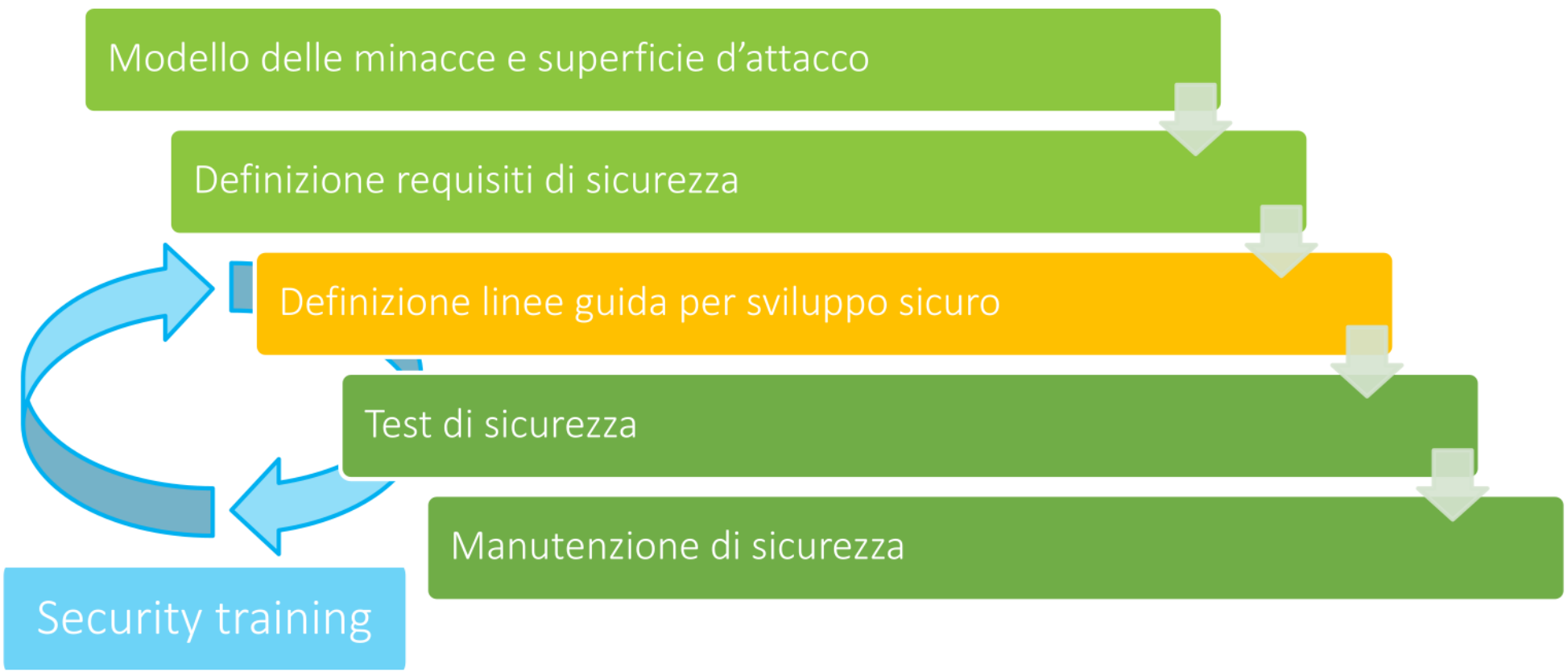


SECURITY BY DESIGN

- Per rendere il sistema informativo sicuro è necessario agire in più contesti in modo organizzato

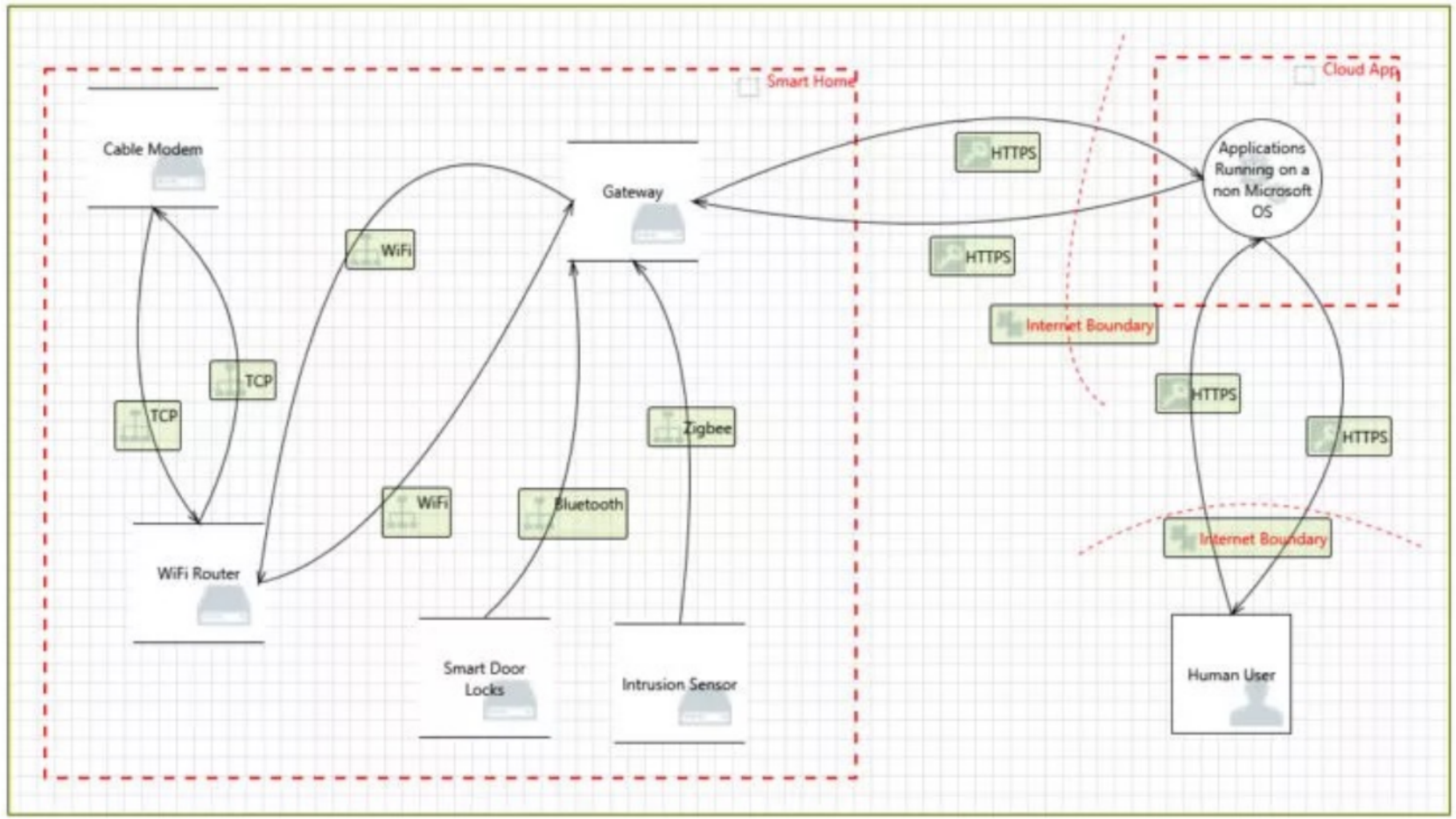
  - **Livello di policy aziendale**: analisi dei rischi e definizione dei processi per la gestione delle informazioni
  - **Livello infrastrutturale**: processo di aggiornamento, mantenimento e monitoraggio dei sistemi
  - **Livello applicativo**: introduzione della sicurezza in tutte le fasi di progetto, dal design allo sviluppo
  - **Livello umano**: formazione tecnica e sensibilizzazione del personale

SECURITY BY DESIGN



THREAT MODEL

- Esempio realizzato con Microsoft Threat Modeling Tool



Source: threatmodeler.com

THREAT MODEL

Code	Vulnerability	Components						Threat Actor				
		Device X	Service Y	Service Z	Application A	Application B	Application C	3rd Party Infrastructure Provider	Company Employee	Customer Employee	Internet User	Competitor
OTG-AUTHN-001	Credentials Transported over an Encrypted Channel	Applicable		Applicable	Applicable	Applicable			Applicable	Applicable	Applicable	Applicable
OTG-AUTHN-002	Default credentials	Applicable			Applicable	Applicable			Applicable	Applicable	Applicable	Applicable
OTG-AUTHN-003	Weak lock out mechanism	Applicable			Applicable	Applicable			Applicable	Applicable	Applicable	Applicable
OTG-AUTHN-004	Authentication Schema Bypass	Applicable			Applicable	Applicable			Applicable	Applicable	Applicable	Applicable
OTG-AUTHN-005	Vulnerable Remember Password	Applicable			Applicable	Applicable			Applicable	Applicable	Applicable	Applicable
OTG-AUTHN-006	Browser cache weakness	Applicable			Applicable	Applicable			Applicable	Applicable	Applicable	Applicable
OTG-AUTHN-007	Weak password policy	Applicable			Applicable	Applicable			Applicable	Applicable	Applicable	Applicable
OTG-AUTHN-008	Weak security question/answer											
OTG-AUTHN-009	weak password change or reset	Applicable			Applicable	Applicable			Applicable	Applicable	Applicable	Applicable
OTG-AUTHN-010	Weaker authentication in alternative channel					Applicable	Applicable		Applicable	Applicable	Applicable	Applicable

VICENZA

SECURE NETWORK BV·TECH

SECURITY REQUIREMENTS

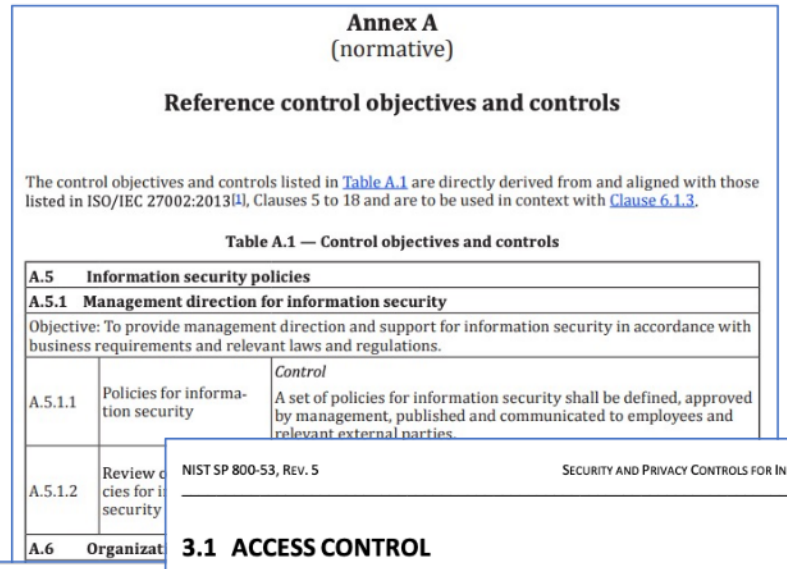
Security Requirements

Category	Requirement ID	Security Requirement	IoT	Web		Mobile	Infrastructure		Risk / Priority	Likelihood	Impact	Solution
				Web Application	Rest API	Mobile Application		Managed DNS				
	SEC-CONF-12	HTTP Strict Transport Security shall be implemented by all HTTPS services		•	•		•		Medium	Medium	Medium	Implent HTTP Strict Transport Security by adding the HTTP Header "Strict-Transport-Security: max-age=31536000; inclu traffic shall be allowed
	SEC-CONF-13	Applications and services shall be configured with least minimum privileges	•	•	•				Medium	Medium	Medium	Restrict access to the file system by applying the *least minimum privilege* criteria
Identity Management Security	SEC-ID-01	A Role Base Access Control (RBAC) system shall be used in order to assign users different privileges based on their own role	•	•	•				Critical	High	High	Use a RBAC system to define roles and related privileges in order to map each user/entity to the corresponding role
	SEC-ID-02	If implemented, the sign up process shall implement validation steps to confirm user-supplied information		•	•	•			High	High	Medium	Validate the supplied email address by sending a random generated and not-guessable one-time token
	SEC-ID-03	If 2FA is implemented, one-time tokens must be valid for a limited time and they can be used only once		•					Critical	High	High	Set the time validity of one-time tokens to a fixed value (e.g., 30 minutes) and validate the time when it is received from stored in the database
	SEC-ID-04	Only authorized users and entities shall be able to provision other accounts or invite external users	•	•					Critical	High	High	Restrict the possibilty to provision or invite users to specific roles
Authentication Security	SEC-AUTH-01	All information shall be transmitted over a secure communication channel	•	•	•	•			High	Medium	High	If supported, all protocols must use TLS v1.2 or v1.3
	SEC-AUTH-02	Any default credential must be removed or replaced with strong and unguessable secrets	•	•	•				Critical	High	High	Configure all services to use custom credentials, which strength must be compliant to the best-practice
	SEC-AUTH-03	Web application shall mitigate the risk of brute-forcing attacks	•	•	•				Medium	Medium	Medium	Web application shall rely on CAPTCHA to mitigate the risk of brute forcing attacks.
	SEC-AUTH-04	All non-public resources shall be accessible prior authentication. In case a service is exposed via different channels, the same	•	•	•				Critical	High	High	Enforce authentication for all non-public resources. Use the same authentication schema for all alternative channels

VICENZA

SECURE NETWORK BV TECH

ESEMPI DA CUI PRENDERE SPUNTO



Annex A
(normative)

Reference control objectives and controls

The control objectives and controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2013[1], Clauses 5 to 18 and are to be used in context with Clause 6.1.3.

Table A.1 — Control objectives and controls

A.5	**Information security policies**	
A.5.1	**Management direction for information security**	
Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.		
A.5.1.1	Policies for information security	*Control* A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.
A.5.1.2	Review c… cies for i… security	
A.6	**Organizat…**	

NIST SP 800-53, REV. 5 SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS

3.1 ACCESS CONTROL

Quick link to Access Control Summary Table

AC-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] access control policy that:

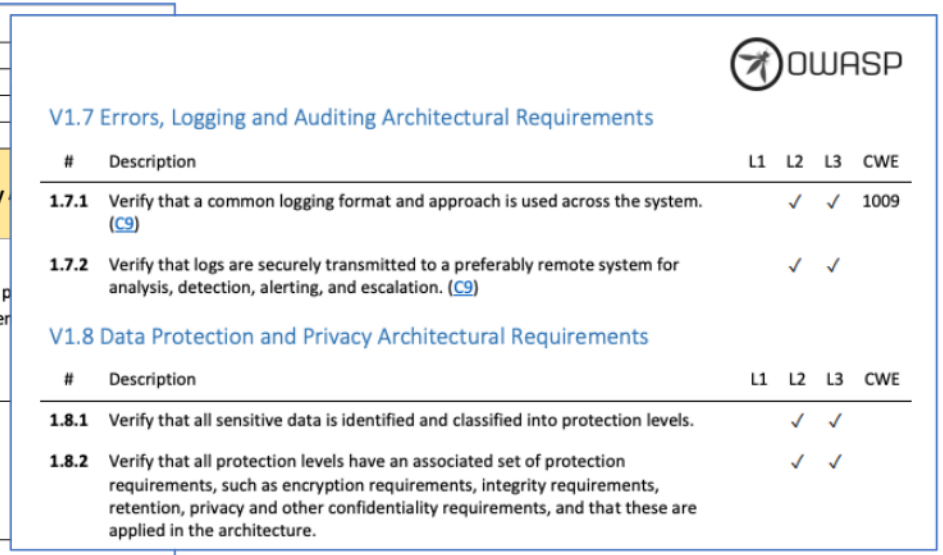
(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the access control policy and the associated access controls;

…pliance Template

NIST 800-171 Control Number				Responsible Party
3.12.3	**Securit…**			System security monitoring in p… reivewed regularly for effectiver… when necessary.
3.13.1	**Systen… Communications Protection**	routers, firewalls, VPNs; organizational DMZs; and restricting external web traffic to only designated servers.	ITS	IT Policies
3.13.2	**System and Communications Protection**	Outline organizational information security policies, to include standards for architectural design, software development, and system engineering principles designed to promote information security	ITS	IT Policies



OWASP

V1.7 Errors, Logging and Auditing Architectural Requirements

#	Description	L1	L2	L3	CWE
1.7.1	Verify that a common logging format and approach is used across the system. (C9)		✓	✓	1009
1.7.2	Verify that logs are securely transmitted to a preferably remote system for analysis, detection, alerting, and escalation. (C9)		✓	✓	

V1.8 Data Protection and Privacy Architectural Requirements

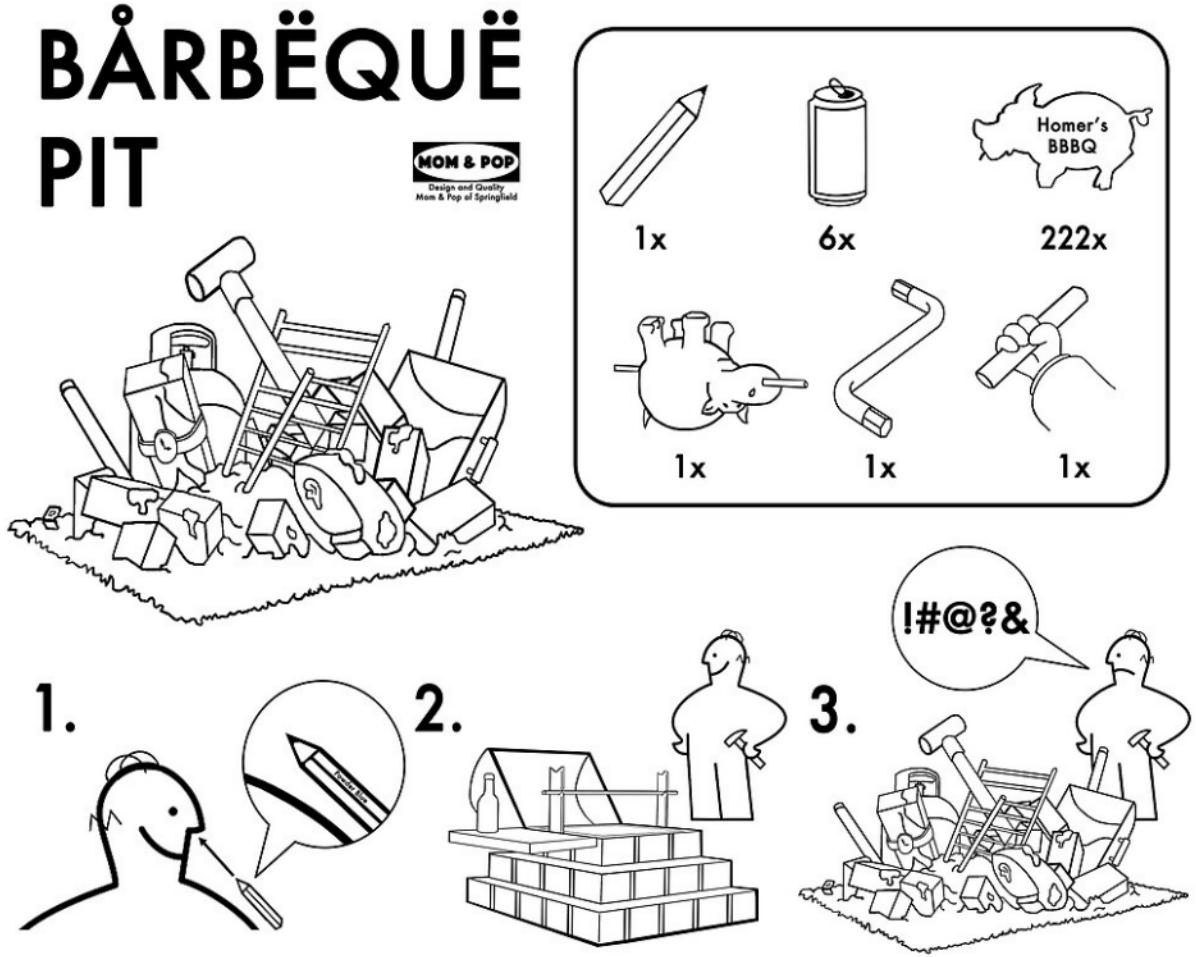
#	Description	L1	L2	L3	CWE
1.8.1	Verify that all sensitive data is identified and classified into protection levels.		✓	✓	
1.8.2	Verify that all protection levels have an associated set of protection requirements, such as encryption requirements, integrity requirements, retention, privacy and other confidentiality requirements, and that these are applied in the architecture.		✓	✓	

- ISO 27001 Annex A
- NIST 800-53 & 800-171
- IEC 62443, NIST 800-82, NERC & ENISA DSP
- CIS Benchmarks & COBIT PAM
- OWASP ASVS & Top 10 Risks
- CWE & CAPEC (problematiche ed attacchi)

SECURE NETWORK BV·TECH

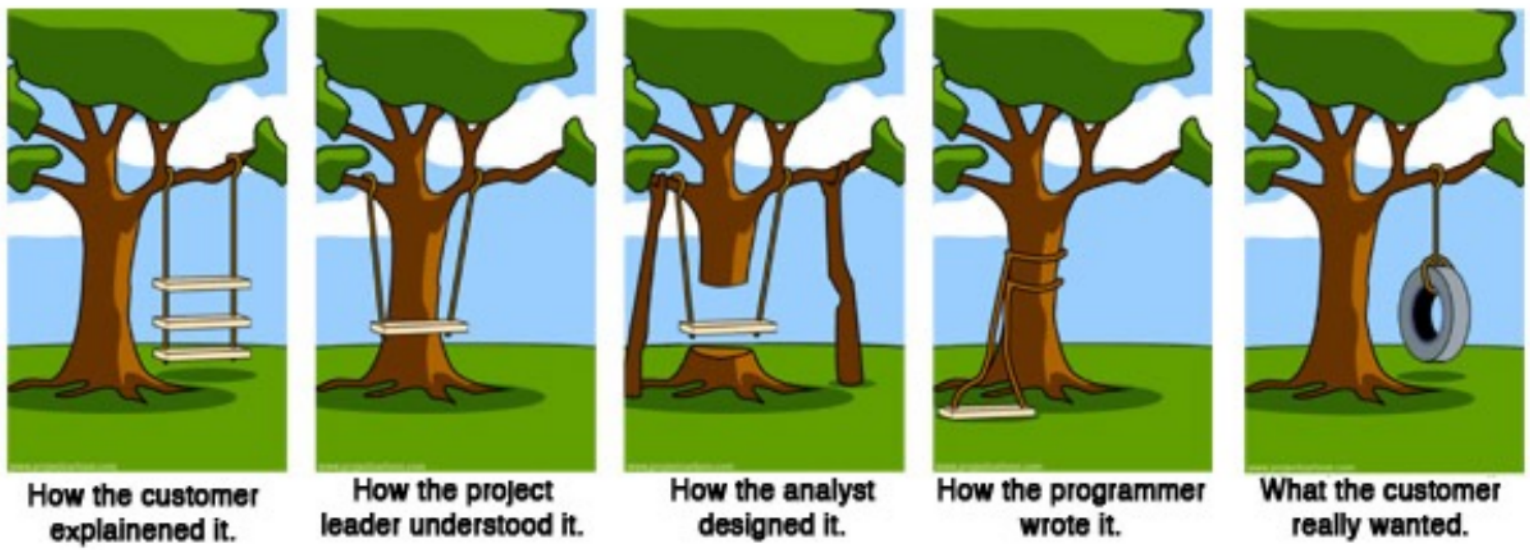
SECURE DEVELOPMENT

- Erano davvero chiari i requisiti?
- L'architettura ipotizzata è realizzabile?
- Abbiamo le competenze necessarie?
- Abbiamo gli strumenti adatti?



SECURE DEVELOPMENT

- Sviluppo interno o delegato a fornitore esterno?
- Infrastruttura on-premises, data-center o cloud?
- Rete locale managed o infrastuttura virtualizzata VDI?
- Quali linguaggi di programmazione e framework scegliere?
- Il team di sviluppo è allineato rispetto agli altri team?



SECURITY TRAINING

- Processo formale per educare progettisti e sviluppatori a ideare e produrre prodotti sicuri:
  - Diminuisce le inaccuratezze durante l'identificazione dei requisiti di sicurezza
  - Riduce la probabilità di errori logici nel design concettuale
  - Evita l'introduzione di vulnerabilità date da pratiche di sviluppo inadatte
  - Riduce gli errori in fase di manutenzione o aggiornamento
  - Favorisce la volontà di stilare delle Security Policies

E' un processo in continua evoluzione, per via di modifiche ai requisiti di sicurezza dovute a condizioni dall'esterno.

SOFTWARE TESTING

- Esistono diversi tipi di test in fase di sviluppo:
  - Unit test: focus su un singolo componente;
  - Integration test: controlla l'interazione tra componenti;
  - Functional test: verifica una specifica funzionalità;
  - Regression test: a seguito di modifiche, verifica il corretto funzionamento del resto
  - End-to-end test: focus sul corretto funzionamento dal punto di vista dell'utente;
  - User-acceptance test: semplicità di utilizzo, ma potrebbe evidenziare dubbi di sicurezza che potrebbe avere un utente (perché mi viene chiesta un'informazione personale?)
  - Performance/stress test: verifica i tempi di computazione, permette di rilevare bottle-neck e favorire la disponibilità del sistema.
- E ovviamente test di sicurezza più mirati

SECURITY TESTING

- **Vulnerability Scan**: analisi automatizzata con strumenti specialistici
- **Vulnerability Assessment**: estensivo, svolto da specialisti in sicurezza
- **Penetration Test**: mirato, verifica la possibilità di attacchi reali
- **Protocol Fuzzing**: identifica input malformato che evidenzia i bug
- **Reverse Engineering**: verifica la resistenza ad analisi esterne
- **Social Engineering**: testa l'anello debole della catena, l'essere umano

La fase di test può essere ortogonale, a diversi livelli di profondità ed estensività.

SECURITY MAINTENANCE

- Supporto e rilascio di correzioni post-rilascio
- Critico per prodotti IoT o industriali
- I test in laboratorio potrebbero non rilevare problematiche evidenti sul campo in contesti specifici
- …tuttavia attivare sistemi di monitoraggio on-board potrebbe interferire con il funzionamento del prodotto oppure andare contro leggi vigenti
- L'aggiornamento del prodotto potrebbe non essere eseguibile da remoto, ma potrebbe richiedere costosi richiami o interventi in sede

La manutenzione di un prodotto deve essere tenuta in considerazione e pianificata fin dalla fase di design del prodotto.

SECURE NETWORK

BV TECH

VICENZA

Non tutte le vulnerabilità sono uguali

Eros Lever

Online, 01/02/2024