LA TASSONOMIA CYBER DELL'ACN

Definizione della tassonomia cyber dell'Agenzia per la cybersicurezza nazionale

TLP:CLEAR

*Il presente documento ha un livello di condivisione **TLP:CLEAR.** Le informazioni possono essere distribuite senza restrizioni rispettando eventuali disposizioni sul copyright. Ulteriori dettagli sono disponibili sulla pagina dedicata del CSIRT Italia e sulla pagina dedicata del FIRST.*

AGENZIA PER LA CYBERSICUREZZA NAZIONALE

L'Agenzia per la cybersicurezza nazionale (ACN) è stata istituita dal Decreto-legge n.82 del 14 giugno 2021 che ha ridefinito l'architettura nazionale di cybersicurezza, con l'obiettivo di razionalizzare e semplificare il sistema di competenze esistenti a livello nazionale, anche attuando il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza, promuovendone azioni comuni.

L'Agenzia è l'Autorità nazionale per la cybersicurezza a tutela degli interessi nazionali nel campo della cybersicurezza. In tale veste ha il compito di tutelare la sicurezza e la resilienza nello spazio cibernetico del Paese promuovendo la realizzazione di azioni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese. A tal fine sviluppa anche capacità necessarie per proteggere dalle minacce informatiche reti, sistemi informativi e servizi informatici delle Pubbliche Amministrazioni e degli operatori di infrastrutture critiche nazionali, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico.

Siti web: **Agenzia per la Cybersicurezza Nazionale** **CSIRT Italia**

Contatti: **info@acn.gov.it**

Seguici sui nostri canali social:

Esclusione di responsabilità

Il presente documento fornisce, a titolo esemplificativo e non esaustivo, indicazioni di mero ausilio alle attività di sicurezza dell'Organizzazione e non solleva la stessa dall'onere di porre in essere, nel rispetto della normativa vigente in materia di cybersicurezza, tutte le azioni ritenute necessarie per la prevenzione e mitigazione del rischio nonché la risoluzione degli impatti derivanti dal verificarsi di eventi e incidenti informatici.

SOMMARIO

EXECUTIVE SUMMARY

La presente linea guida definisce la "**Tassonomia Cyber dell'Agenzia per la Cybersicurezza Nazionale**" **(TC-ACN)**, ossia il **linguaggio comune** per lo scambio delle informazioni relative a eventi e minacce di cybersicurezza.

Durante la redazione sono state opportunamente prese in esame le tassonomie preesistenti utilizzate in ambito internazionale e le norme in vigore riguardo alla notifica degli incidenti in carico ai soggetti appartenenti al Perimetro di Sicurezza Nazionale Cibernetica (PSNC), già effettuate in accordo a una "tassonomia degli incidenti".

La TC-ACN è redatta con lo scopo di fornire ai soggetti interessati gli strumenti per **caratterizzare un evento**, attraverso 144 attributi per specificarne la natura e fornirne una descrizione granulare durante gli scambi informativi.

1 INTRODUZIONE

Lo sviluppo tecnologico al quale si è assistito negli ultimi anni ha determinato la comparsa e l'evoluzione di rischi e minacce informatiche a danno dell'ecosistema cyber nazionale, così come esso è stato definito da documenti di policy dell'Agenzia quali le Relazioni Annuali e la Strategia Nazionale di Cybersicurezza 2022-2026, che persegue a livello strategico tre obiettivi brevemente descritti di seguito:

- **protezione** degli asset strategici nazionali attraverso un approccio sistemico orientato alla gestione e mitigazione del rischio, formato sia da un quadro normativo che da misure, strumenti e controlli che possono abilitare una transizione digitale resiliente del Paese;
- **risposta** alle minacce, agli incidenti e alle crisi cyber nazionali attraverso l'impiego di elevate capacità nazionali di monitoraggio, rilevamento, analisi e risposta e l'attivazione di processi che coinvolgano tutti gli attori facenti parte dell'ecosistema di cybersicurezza nazionale;
- **sviluppo** consapevole e sicuro delle tecnologie digitali, della ricerca e della competitività industriale, in grado di rispondere alle esigenze del mercato, funzione di cui l'ACN è responsabile, affrontando in maniera concreta i costanti cambiamenti del contesto cibernetico.

In linea con questi obiettivi, l'Agenzia si propone di condividere informazioni, conoscenze e analisi su rischi, minacce e incidenti informatici in maniera bidirezionale con il settore pubblico e privato, sviluppando le competenze e supportando la Pubblica Amministrazione e i settori produttivi nazionali nell'adattarsi a un panorama cyber in costante evoluzione.

In tale ottica l'Agenzia, attraverso la redazione della presente Linea Guida, si prefigge di definire una "tassonomia" che sia in grado di:

- **agevolare lo scambio di informazioni** a livello nazionale attraverso l'adozione di un lessico comune che rappresenti una base metodologica per la condivisione di informazioni riguardo agli eventi cyber;

- **identificare, definire e caratterizzare** gli eventi cyber attraverso un'unica tassonomia rilevante a livello nazionale;
- fornire ai soggetti interessati un documento che si **armonizzi con le tassonomie internazionali in materia di cybersecurity** e che sia al contempo adeguato al **contesto normativo nazionale**.

Il prosieguo del documento è strutturato come segue:

- **Capitolo 2 – Riferimenti**, in cui si forniscono i principali riferimenti e altre tassonomie cyber prese in considerazione nella definizione della tassonomia cyber.
- **Capitolo 3 – La tassonomia degli eventi cyber dell'ACN,** in cui si riporta la tassonomia degli eventi cyber costituita da un insieme di attributi che li caratterizzano.

In appendice si riporta in forma grafica di sintesi la Tassonomia Cyber dell'ACN.

2 RIFERIMENTI

In questo capitolo si riportano le principali **fonti normative** nazionali in tema di notifica di incidenti e i principali framework in tema di tassonomie cyber sviluppati da gruppi di lavoro internazionali.

2.1 FONTI NORMATIVE

Le fonti normative prese in considerazione sono quelle che designano il CSIRT Italia quale destinatario delle notifiche di incidenti che avvengono a danno di determinati soggetti, selezionati e individuati dalle leggi stesse.

Decreto Legislativo 7 marzo 2005, n. 82 "*Codice dell'Amministrazione Digitale – CAD*", che definisce i soggetti pubblici per i quali il CSIRT Italia coordina le iniziative di prevenzione e gestione degli incidenti informatici.

Decreto Legislativo 18 maggio 2018, n. 65 "*Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*", che istituisce e dettaglia compiti e funzioni del CSIRT nonché individua gli Operatori di Servizi Essenziali (OSE) ed i Fornitori di Servizi Digitali (FSD) quali soggetti con obblighi di notifica incidenti.

Decreto del Presidente del Consiglio dei Ministri 8 agosto 2019 "*Disposizioni sull'organizzazione e il funzionamento del Computer Security Incident Response Team – CSIRT italiano*", che definisce la costituzione, l'organizzazione ed il funzionamento del CSIRT italiano presso il Dipartimento delle informazioni per la sicurezza (DIS) – ora, a seguito delle modifiche introdotte dal **decreto-legge 14 giugno 2021, n. 82**, presso l'ACN assumendo la denominazione di CSIRT Italia. In tale quadro, i soggetti pubblici e privati, in caso di incidente cibernetico e/o di notifica di evento, hanno quale nuovo ed unico interlocutore il CSIRT Italia, che già riceve le notifiche obbligatorie e volontarie degli OSE e dei FSD, ai sensi del D.Lgs. n. 65/2018.

Decreto-legge 21 settembre 2019, n. 105, coordinato con la legge di conversione 18 novembre 2019, n. 133, "*Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica (e di disciplina dei poteri speciali nei settori di rilevanza strategica)*", e relativi provvedimenti attuativi, che mira ad assicurare, attraverso l'istituzione di un *Perimetro di Sicurezza Nazionale Cibernetica* (PSNC), un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, e la previsione di misure idonee a garantire i necessari standard di sicurezza volti a minimizzare i rischi consentendo, al contempo, la più estesa fruizione dei più avanzati strumenti offerti dalle tecnologie dell'informazione e della comunicazione.

Decreto del Presidente del Consiglio dei Ministri 30 luglio 2020, n. 131 "*Regolamento in materia di Perimetro di Sicurezza Nazionale Cibernetica, ai sensi dell'articolo 1, comma 2, del Decreto-Legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133*", che individua i soggetti pubblici e privati rientranti nel Perimetro.

Decreto del Presidente del Consiglio dei Ministri 14 aprile 2021, n. 81 "*Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del Decreto-Legge 21 settembre 2019, n.105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza*", che definisce le misure volte a garantire elevati livelli di sicurezza nonché le modalità di notifica al CSIRT Italia[1] degli incidenti aventi impatto sui beni ICT o sui beni contigui. In particolare, il decreto classifica tali tipologie di incidenti in categorie all'interno delle tabelle n. 1 e n. 2 dell'allegato A, e ne definisce le relative tempistiche di notifica. Al contempo, è possibile notificare, su base volontaria, anche i tipi di incidenti non elencati nel decreto.

Determina dell'Agenzia per la Cybersicurezza Nazionale 3 gennaio 2023, che ha rafforzato il PSNC estendendo l'ambito delle notifiche obbligatorie al CSIRT Italia ad ulteriori tipologie di incidenti informatici (categoria C di cui all'allegato A alla Determina). In tali casi il processo di notifica riguarda gli incidenti aventi impatto su reti, sistemi informativi e servizi informatici diversi

[1] La notifica di un incidente impattante i beni ICT o beni contigui effettuata allo CSIRT Italia costituisce anche adempimento dell'obbligo notifica ai sensi del decreto legislativo 18 maggio 2018, n. 65 (disciplina NIS), applicabile agli OSE e ai FSD.

dai beni ICT di pertinenza dei soggetti inclusi nel Perimetro.

Decreto Legislativo 1° agosto 2023, n. 259 "*Codice delle comunicazioni elettroniche*", così come modificato dal D.Lgs. n. 207/2021 e relativo "DM Telco", che impone obblighi di notifica ai soggetti imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico.

Legge 28 giugno 2024 n. 90 '*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*", che mira a potenziare la cybersicurezza nazionale e la resilienza delle istituzioni pubbliche e del settore finanziario in Italia. Impone obblighi di notifica degli incidenti informatici a Pubbliche Amministrazioni specifiche, con tempi definiti, e prevede sanzioni per la mancata adozione di interventi correttivi.

2.2 ALTRE TASSONOMIE CYBER

Il secondo gruppo di fonti prese in esame è rappresentato dai documenti prodotti da gruppi di lavoro internazionali che si sono dedicati alla razionalizzazione di termini e concetti inerenti alla sicurezza cibernetica. In particolare, sono state analizzate le produzioni sul tema di:

- ENISA e Trusted Introducer;
- MITRE Corporation;
- Unione Europea e NATO.

Di seguito si riporta una breve descrizione delle tassonomie prodotte dalle citate fonti:

ENISA e Trusted Introducer

Istituita nel 2004, ENISA è l'Agenzia dell'Unione Europea per la cybersicurezza, incaricata di creare le condizioni per un elevato livello comune di cybersicurezza in tutta Europa. Nel 2018 l'ENISA ha avviato il **Reference Security Incident Taxonomy Working Group** (RSIT WG), con lo scopo di lavorare alla definizione di una tassonomia unica per supportare gli CSIRT europei nel trattare di incidenti di cybersicurezza[2]. Il risultato è la "**Reference Incident Classification Taxonomy**"[3], che prende come riferimento la "Incident Classification / Incident Taxonomy

[2] https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force

[3] https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

according to eCSIRT.net" pubblicata nel 2012 da Trusted Introducer Service (anche noto come TI) e successivamente aggiornata nel 2015 sulla base della tassonomia degli incidenti elaborata dall'European CSIRT Network (eCSIRT).

La tassonomia così recepita da ENISA classifica gli incidenti in 11 categorie con 32 relativi "esempi di incidenti". Le categorie offerte da questa tassonomia sono generali e facilmente adattabili, per questo motivo sono state incluse nella TC-ACN (ad esempio Abusive content, Availability, Fraud, Infomation Gathering, etc). Tuttavia, prese separatamente, le tassonomie di ENISA e di Trusted Introducer non forniscono un livello di granularità sufficiente che è invece stato colmato con l'elaborazione della TC-ACN.

MITRE Corporation

La **MITRE Corporation** è un'organizzazione no-profit fondata nel 1958 allo scopo di guidare lo sviluppo di progetti che innalzino il livello generale di sicurezza in differenti aree di applicazione. Tra queste, MITRE si occupa di organizzare e creare team dedicati alla progettazione, sviluppo e supporto di soluzioni innovative nel campo della sicurezza informatica.

Il **MITRE ATT&CK** rappresenta un framework che fornisce una conoscenza dettagliata delle tattiche e delle tecniche utilizzate dagli avversari nel cyberspazio. Il progetto si compone di tre matrici di tattiche distinte per i domini Enterprise, Mobile e Industrial Control Systems (ICS), all'interno dei quali vengono definite le tecniche e le sotto tecniche associate all'attacco.

Le matrici del MITRE ATT&CK sono state opportunamente considerate e integrate dove necessario nella TC-ACN vista l'efficace granularità delle informazioni fornite. Tuttavia, la tassonomia del MITRE da sola non è stata ritenuta adatta a caratterizzare eventi e incidenti, data la sua specializzazione sull'analisi del comportamento degli attaccanti, le fasi di un attacco e gli strumenti da essi utilizzati.

Unione Europea e NATO

Nel 2011, l'Unione Europea e la NATO hanno avviato il **MISP Project**, un progetto con lo scopo di progettare, sviluppare, supportare e fornire strumenti open source per incentivare e permettere la condivisione delle informazioni di natura cyber.

Il MISP Project include innumerevoli iniziative, inclusa la "**MISP Taxonomies"**[4]**,** che ha lo scopo di fornire un insieme predefinito di linguaggi, standard e modelli di classificazione delle minacce

[4] https://www.misp-project.org/datamodels/#misp-taxonomies

informatiche che consentano lo scambio di informazioni in maniera efficace, efficiente e di valore tra più dispositivi in formato machine-readable. Tra questi, il "MISP Taxonomies" raccoglie anche le tassonomie elaborate da ENISA e dall'European CSIRT Network (eCSIRT), come analizzate nei paragrafi precedenti. Per questo motivo, le tassonomie incluse nel progetto sono state valutate e integrate ove ritenuto opportuno all'interno della TC-ACN.

3 LA TASSONOMIA DEGLI EVENTI CYBER DI ACN

Il presente Capitolo definisce la **Tassonomia Cyber dell'Agenzia per la Cybersicurezza Nazionale (TC-ACN).**

La TC-ACN è costituita da 144 "valori", ognuno appartenente a uno dei 22 "predicati", i quali sono organizzati in 4 "macrocategorie".

In particolare, si definisce:

- **macrocategoria,** un gruppo di predicati con caratteristiche affini;
- **predicato**, un lemma che ha lo scopo di raccogliere un sottoinsieme di valori in base alle loro proprietà e caratteristiche intrinseche;
- **valore**, ossia l'elemento granulare che specifica una determinata caratteristica di un evento cyber identificata dal predicato di riferimento.

In Figura 1 sono rappresentate le quattro macrocategorie.

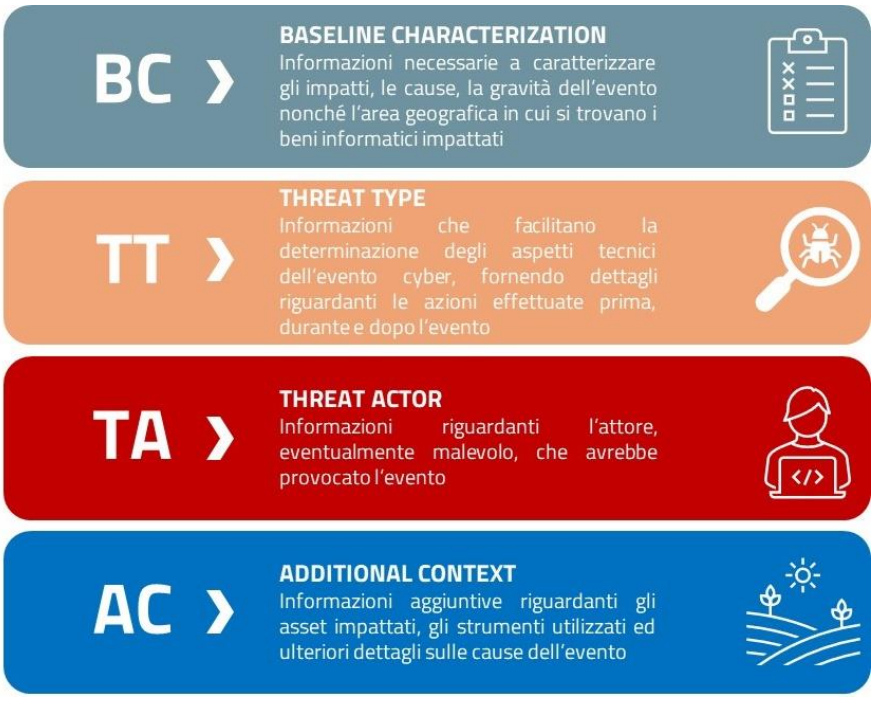

Figura 1: Struttura della tassonomia degli eventi cyber - Macrocategorie

In Figura 2 è invece riportata una rappresentazione della suddivisione dei predicati all'interno delle quattro macrocategorie.

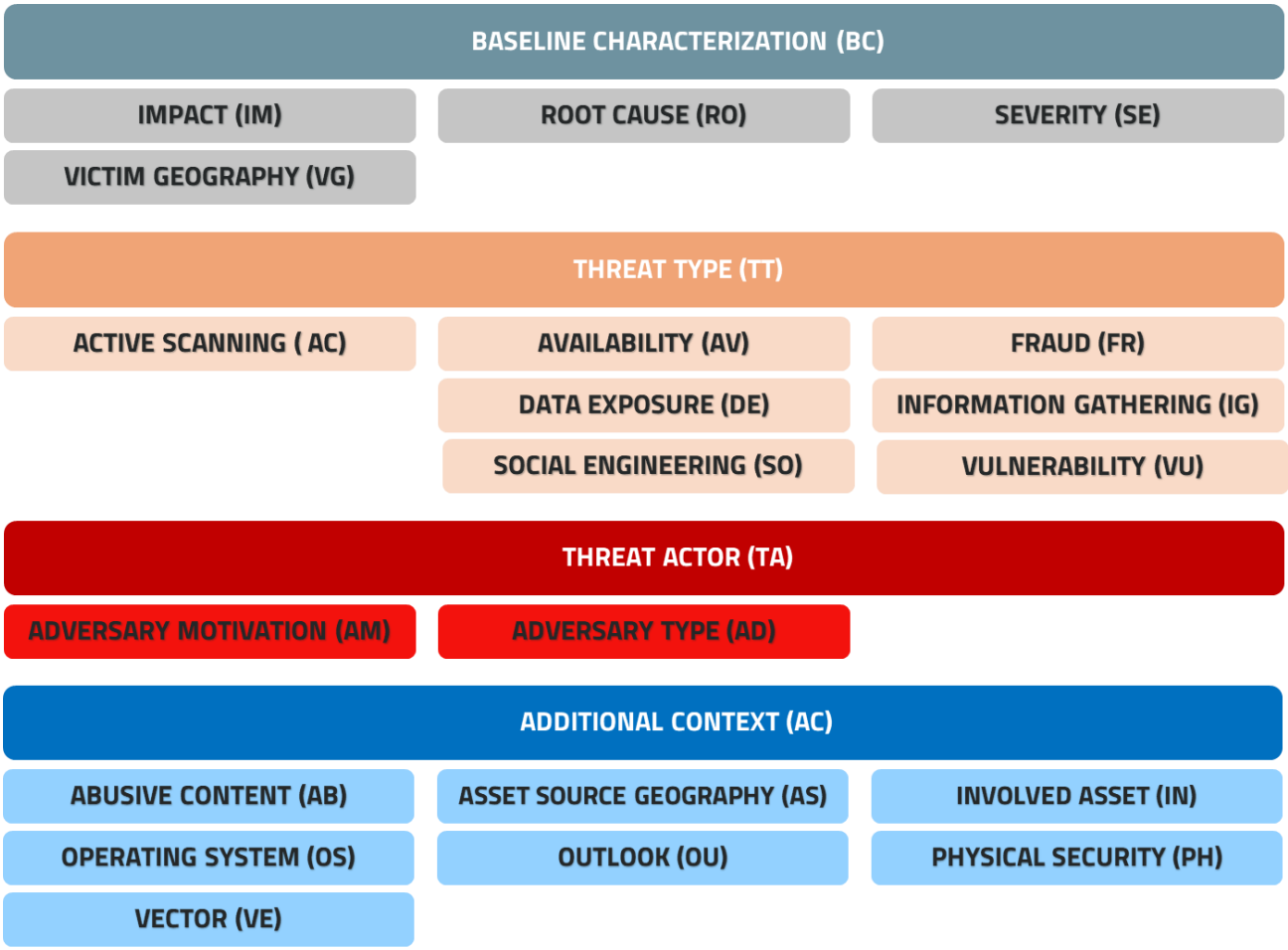

Figura 2: Struttura della tassonomia degli eventi cyber - Predicati

A titolo esemplificativo, consideriamo il caso di un *ransomware*, che è un malware. Pertanto, si avrà che il "***valore" ransomware*** ricadrà nel **predicato "malicious code"**, il quale, a sua volta, sarà ricompreso nella **macrocategoria "Threat Type"**.

Nelle successive sezioni vengono dettagliati tutti i 144 valori, organizzati per predicati e macrocategorie. L'elenco completo della TC-ACN è riportato in APPENDICE .

3.1 BASELINE CHARACTERIZATION (BC)

3.1.1 Predicato: Impact (IM)

Il predicato **Impact** si riferisce alla perturbazione causata da un evento cyber.

I valori associati a **Impact** identificati dall'Agenzia per la tassonomia degli eventi cyber sono elencati di seguito.

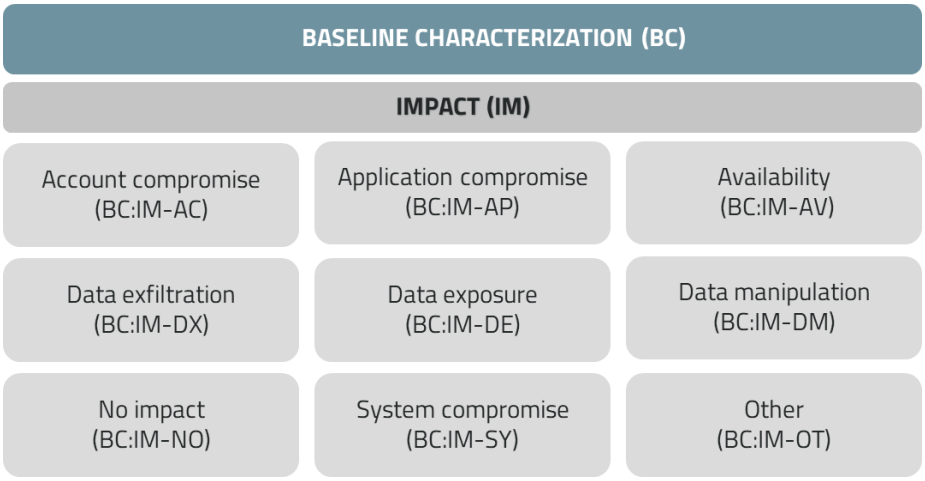

Figura 3: Predicato 'Impact' con i relativi valori

3.1.1.1 Account compromise (BC:IM-AC)

Account compromise identifica gli eventi cyber che hanno avuto come effetto la compromissione di un account utente o di servizio. È possibile specificare il tipo di account compromesso utilizzando il predicato Involved asset (§ 3.4.3).

3.1.1.2 Application compromise (BC:IM-AP)

Application compromise identifica gli eventi cyber che hanno avuto come effetto la compromissione di un'applicazione o di un servizio, incluse applicazioni Web, Mobile, Database, ecc. È possibile specificare il tipo di application compromise utilizzando il predicato Involved asset (§ 3.4.3).

3.1.1.3 Availability (BC:IM-AV)

Availability identifica gli eventi nei quali le attività malevole condotte da un attaccante hanno causato effetti sulla disponibilità del sistema o servizio erogato. Nel caso in cui un evento cyber venga classificato utilizzando tale valore, dovrà essere esplicitato anche il predicato Availability (§ 3.2.2).

3.1.1.4 Data exfiltration (BC:IM-DX)

Data exfiltration identifica gli eventi cyber in cui è stata riscontrata la compromissione della riservatezza delle informazioni presenti su un bene informatico. Tale perdita o fuga dei dati può avvenire a causa di attività malevole, ad esempio a seguito di una compromissione di un file server, oppure accidentalmente, nel caso di un database esposto su Internet senza un accurato processo di autenticazione.

3.1.1.5 Data exposure (BC:IM:DE)

Data exposure si riferisce alla divulgazione non autorizzata di dati sensibili o riservati, causata da vulnerabilità di sicurezza, errori di configurazione o pratiche inadeguate di gestione delle informazioni. Questo fenomeno può portare alla diffusione di informazioni personali, finanziarie

o aziendali aumentando il rischio di furti di identità, frodi o danni reputazionali per individui e organizzazioni.

3.1.1.6 Data manipulation (BC:IM-DM)

Data manipulation identifica gli eventi cyber in cui è stata riscontrata la compromissione dell'integrità delle informazioni presenti su un bene informatico. Tale valore include la modifica o la distruzione dei dati da parte di un attore malevolo.

3.1.1.7 No impact (BC:IM-NO)

No impact identifica un evento cyber che avrebbe potuto compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi, ma che è stato efficacemente evitato o non si è verificato. Un esempio è la ricezione di una e-mail di phishing riconosciuta come tale dall'utente e pertanto sostanzialmente priva di effetti.

3.1.1.8 System compromise (BC:IM-SY)

System compromise identifica gli eventi cyber che hanno avuto come effetto la compromissione di un bene informatico, ad esempio alterandone l'integrità.

3.1.1.9 Other (BC:IM-OT)

Other identifica gli eventi cyber relativi a Impact non identificabili con gli altri valori definiti nel sottoinsieme.

3.1.2 Predicato: Root cause (RO)

Il predicato **Root cause** categorizza le cause che hanno determinato uno specifico evento, sia di natura accidentale, sia deliberata.

I valori associati a **Root cause** identificati dall'Agenzia per la tassonomia degli eventi cyber sono elencati di seguito.

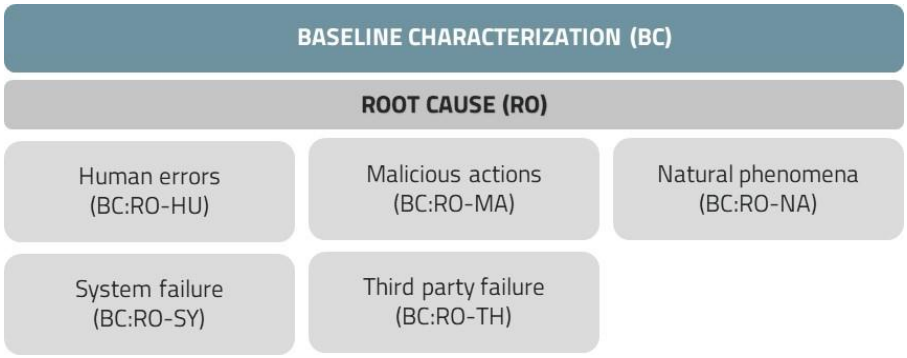

Figura 4: Predicato 'Root cause' con i relativi valori

3.1.2.1 Human errors (BC:RO-HU)

Human errors identifica gli eventi provocati da un errore umano non intenzionale. Un esempio è un'errata operazione che influisce sulla prevista funzionalità di un bene informatico.

3.1.2.2 Malicious actions (BC:RO-MA)

Malicious actions identifica qualsiasi tentativo di compromettere l'integrità, la confidenzialità o la disponibilità di un bene informatico.

3.1.2.3 Natural phenomena (BC:RO-NA)

Natural phenomena identifica gli eventi causati da un fenomeno naturale, come ad esempio, terremoti, valanghe ed esondazioni.

3.1.2.4 System failure (BC:RO-SY)

System failure identifica un evento non previsto, in cui un sistema cessa di funzionare secondo le specifiche progettuali previste, **comportando una perdita di servizio o una riduzione significativa della qualità del servizio fornito.**

3.1.2.5 Third party failure (BC:RO-TH)

Third party failure identifica l'interruzione o degradazione delle prestazioni di un sistema principale attribuibile a disfunzioni o guasti di servizi forniti da terze parti.

3.1.3 Predicato: Severity (SE)

Il predicato **Severity** ha lo scopo di indicare la gravità dell'impatto di un evento cyber. Questo predicato è associabile a quattro livelli, riferiti alla criticità dell'impatto subito.

I valori associati a **Severity** identificati dall'Agenzia per la tassonomia degli eventi cyber sono elencati di seguito.

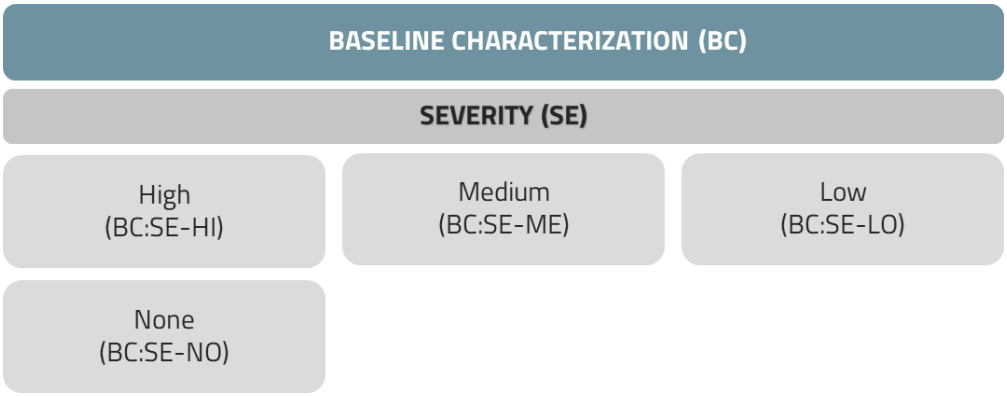

Figura 5: Predicato 'Severity' con i relativi valori

3.1.3.1 High (BC:SE-HI)

High identifica un evento cyber riferito ad una delle seguenti condizioni:

- l'organizzazione non è più in grado di fornire uno o più servizi essenziali agli utenti;
- dati/informazioni personali o proprietarie sono stati modificati, cancellati o esfiltrati;
- il ripristino dall'incidente non è possibile (ad esempio, dati sensibili esfiltrati e diffusi, non recuperabili a seguito di un evento ransomware).

3.1.3.2 Medium (BC:SE-ME)

Medium identifica un evento cyber riferito ad una delle seguenti condizioni:

- l'organizzazione è in grado di erogare un servizio essenziale solo ad una parte dell'utenza;
- è stato rilevato l'accesso e l'esfiltrazione a dati/informazioni personali o proprietarie;
- il ripristino è possibile con tempistiche non note in quanto, ad esempio, sono necessarie risorse aggiuntive o supporto esterno.

3.1.3.3 Low (BC:SE-LO)

Low identifica un evento cyber riferito ad una delle seguenti condizioni:

- l'organizzazione può ancora fornire tutti i servizi essenziali a tutti gli utenti, ma risultano non ottimali in termini di efficienza;
- è stato rilevato l'accesso a dati/informazioni sensibili o proprietarie;
- il ripristino è possibile con tempistiche note, anche tramite risorse aggiuntive.

3.1.3.4 None (BC:SE-NO)

None identifica un evento cyber riferito ad una delle seguenti condizioni:

- nessun effetto sulla capacità dell'organizzazione di erogare i servizi agli utenti;
- nessuna informazione è stata oggetto di accesso non autorizzato, esfiltrazione, modifica o cancellazione;
- il tempo necessario per il ripristino è prevedibile con le risorse esistenti.

3.1.4 Predicato: Victim geography (VG)

Il predicato **Victim geography** identifica l'area geografica in cui si trovano i beni informatici interessati dall'evento cyber.

I valori associati a **Victim geography** identificati dall'Agenzia per la tassonomia degli eventi cyber sono elencati di seguito.

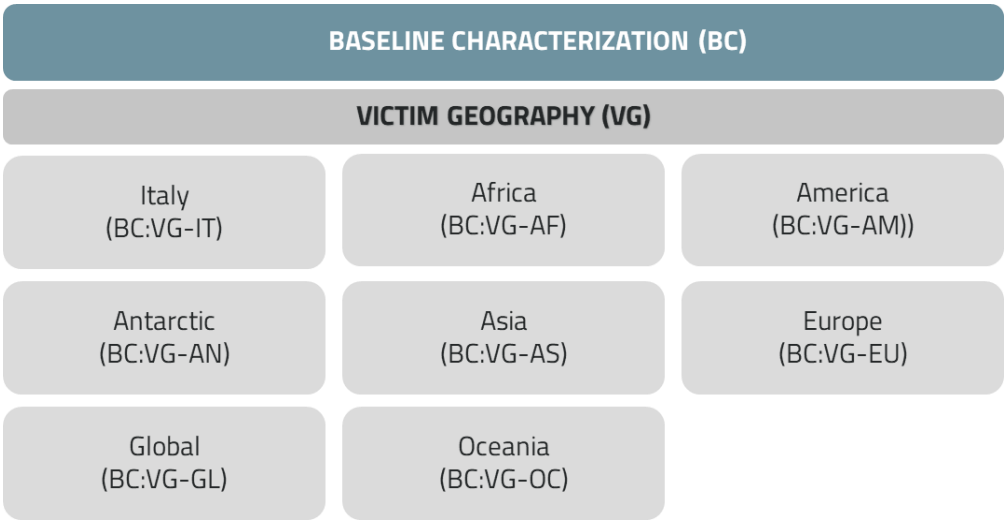

Figura 6: Predicato 'Victim geography' con i relativi valori

3.1.4.1 Italy (BC:VG-IT)

Italy indica che l'evento cyber ha avuto un impatto su beni informatici localizzati in Italia.

3.1.4.2 Africa (BC:VG-AF)

Africa indica che l'evento cyber ha avuto un impatto su beni informatici localizzati geograficamente sul continente africano.

3.1.4.3 America (BC:VG-AM)

America indica che l'evento cyber ha avuto un impatto su beni informatici localizzati geograficamente sul continente americano.

3.1.4.4 Antarctic (BC:VG-AN)

Antartica indica che l'evento cyber ha avuto un impatto su beni informatici localizzati geograficamente sul continente antartico.

3.1.4.5 Asia (BC:VG-AS)

Asia indica che l'evento cyber ha avuto un impatto su beni informatici localizzati geograficamente sul continente asiatico.

3.1.4.6 Europe (BC:VG-EU)

Europe indica che l'evento cyber ha avuto un impatto su beni informatici localizzati geograficamente sul continente europeo.

3.1.4.7 Global (BC:VG-GL)

Global indica che l'evento cyber ha avuto un impatto su beni informatici distribuiti in più paesi o ha un potenziale impatto globale.

3.1.4.8 Oceania (BC:VG-OC)

Oceania indica che l'evento cyber ha avuto un impatto su beni informatici localizzati nella zona continentale Oceania.

3.2 THREAT TYPE (TT)

3.2.1 Predicato: Active scanning (AC)

Il predicato **Active scanning** identifica tecniche utilizzate da attori malevoli che prevedono la scansione della rete attraverso un contatto diretto con il sistema o con la rete target. Gli attori malevoli effettuano scansioni attive per diverse finalità, come per esempio l'analisi e la rilevazione di vulnerabilità e falle di sicurezza o per l'enumerazione delle risorse disponibili all'interno di un sistema o di una rete.

I valori associati ad **Active scanning** identificati dall'Agenzia per la tassonomia degli eventi cyber sono elencati di seguito.

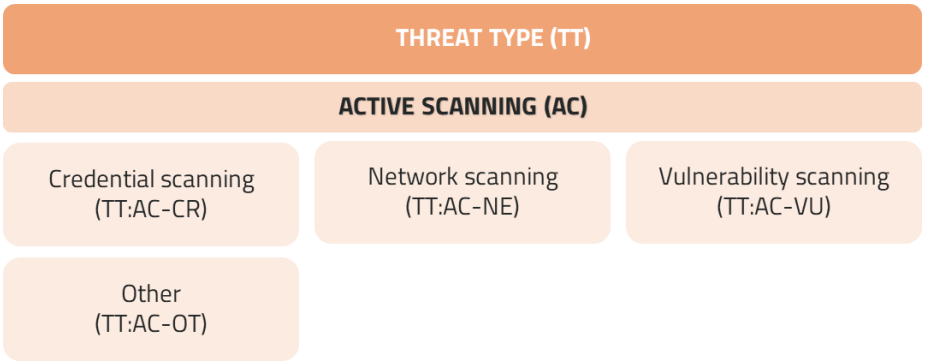

Figura 7: Predicato 'Active scanning' con i relativi valori

3.2.1.1 Credential scanning (TT:AC-CR)

Credential scanning identifica gli eventi cyber in cui un attore malevolo effettua una scansione attiva per rilevare credenziali di autenticazione deboli, impropriamente configurate oppure esposte su un bene informatico. Questo tipo di attività include diverse tipologie di eventi, quali gli attacchi a forza bruta, volti a individuare la password di uno o più account specifici, oppure attacchi di account discovery, mirati alla scoperta di account validi o realmente esistenti sul sistema target.

3.2.1.2 Network scanning (TT:AC-NE)

Network scanning identifica gli eventi cyber in cui un attore malevolo utilizza tecniche e procedure mirate a identificare la presenza di servizi in esecuzione su beni informatici remoti o connessi all'infrastruttura target. Questa categoria di evento comprende la scansione delle porte (port scan), la mappatura della rete (network mapping) e la rilevazione del sistema operativo (OS fingerprinting).

3.2.1.3 Vulnerability scanning (TT:AC-VU)

Vulnerability scanning identifica gli eventi cyber in cui un attore malevolo utilizza tecniche e procedure mirate in modo specifico all'individuazione di vulnerabilità presenti in un bene informatico al fine di mappare la superficie d'attacco.

3.2.1.4 Other (TT:AC-OT)

Other identifica gli eventi cyber relativi ad Active scanning non identificabili con gli altri valori definiti nel sottoinsieme.

3.2.2 Predicato: Availability (AV)

In ambito informatico, per **Availability** (Disponibilità) si intende la capacità di un sistema informativo di garantire agli utenti autorizzati un accesso e un uso tempestivo e sempre fruibile delle informazioni. Tale predicato è in uso per specificare la causa dell'impatto sulla disponibilità.

I valori associati a **Availability** identificati dall'Agenzia per la tassonomia degli eventi cyber sono elencati di seguito.

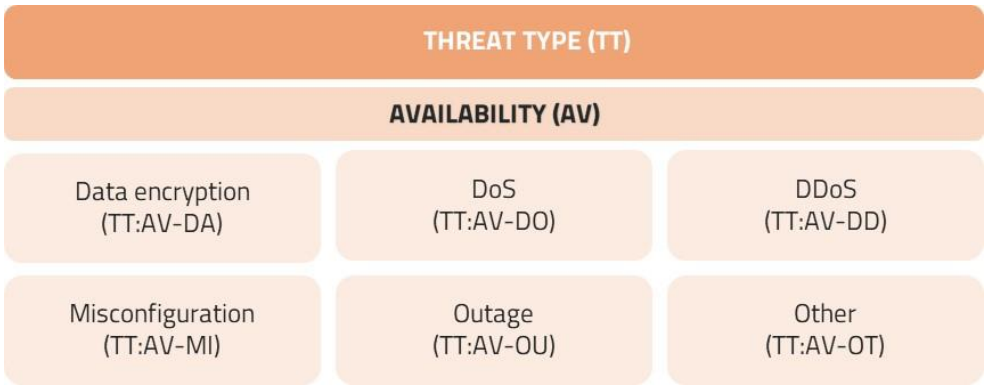

Figura 8: Predicato 'Availability' con i relativi valori

3.2.2.1 Data encryption (TT:AV-DA)

Data encryption identifica gli eventi cyber in cui un attore malevolo applica algoritmi di cifratura ai dati custoditi in un sistema informatico compromesso, senza il consenso del proprietario, al fine di renderli inaccessibili. Tale attività comporta principalmente un impatto sulla disponibilità dei dati presenti sul bene informatico e sull'erogazione dei servizi. Un esempio di tale evento è la cifratura dei dati di un sistema informatico a seguito dell'esecuzione di un ransomware.

3.2.2.2 DoS (TT:AV-DO)

Denial of Service (DoS) identifica gli eventi cyber in cui un attore malevolo effettua un attacco che mira a compromettere la disponibilità di un bene informatico o di un servizio mediante esaurimento delle sue risorse di rete, di elaborazione o di memoria.

3.2.2.3 DDoS (TT:AV-DD)

Distributed Denial of Service (DDoS) identifica gli eventi cyber in cui un attore malevolo effettua un attacco, da sorgenti multiple e distribuite, che mira a compromettere la disponibilità di un bene informatico o un di servizio mediante esaurimento delle sue risorse di rete, di elaborazione o di memoria.

3.2.2.4 Misconfiguration (TT:AV-MI)

Misconfiguration identifica gli eventi cyber non malevoli in cui una configurazione errata o non ottimale di un bene informatico o di una sua componente ha compromesso la disponibilità di un servizio. Un caso d'esempio è un'errata configurazione di un componente di rete che potrebbe causare la perdita totale o parziale di erogazione di un servizio. È importante evidenziare che la disponibilità è stata compromessa a causa di un'azione non intenzionale e quindi non malevola, pertanto, tale predicato è comunemente associato al valore Human errors (§ 3.1.2.1) del predicato Root cause (§ 3.1.2).

3.2.2.5 Outage (TT:AV-OU)

Outage identifica gli eventi cyber non malevoli in cui si è riscontrata la perdita totale o parziale della disponibilità di un bene informatico a causa di eventi naturali o causati dall'uomo. Possibili cause di un evento di indisponibilità possono essere l'avvenimento di un disastro naturale, il mancato funzionamento dei sistemi di refrigerazione di un datacenter oppure un guasto elettrico. È importante evidenziare che la disponibilità è stata compromessa a causa di un'azione non intenzionale e quindi non malevola.

3.2.2.6 Other (TT:AV-OT)

Other identifica gli eventi cyber nei quali si riscontra una perdita di disponibilità di un bene informatico o di un applicativo per una causa che non rientra in quelle indicate negli altri valori associabili al predicato Availability (§ 3.2.2).

3.2.3 Predicato: Fraud (FR)

Il predicato **Fraud** identifica un'azione o una serie di azioni deliberatamente compiute con l'intento di ottenere un vantaggio economico o di altro tipo, attraverso l'inganno o la manipolazione.

I valori associati a **Fraud** identificati dall'Agenzia per la tassonomia degli eventi cyber sono elencati di seguito.

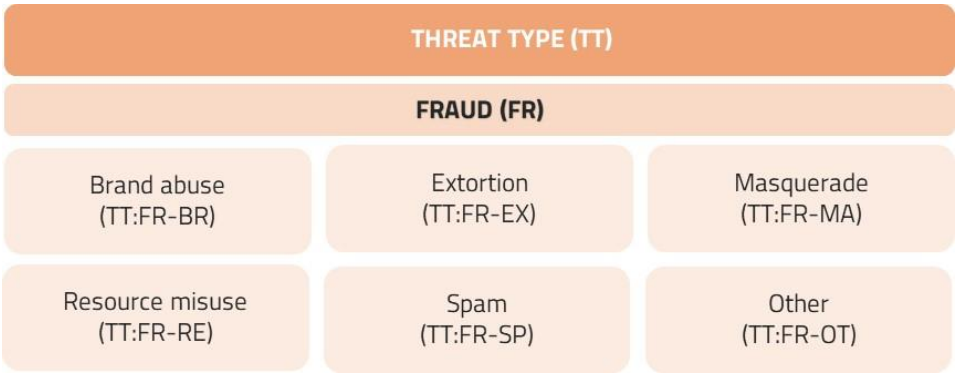

Figura 9: Predicato 'Fraud' con i relativi valori

3.2.3.1 Brand abuse (TT:FR-BR)

Brand abuse identifica un'attività fraudolenta in cui un attore malevolo sfrutta la notorietà di un'organizzazione per creare falsi siti web, false campagne pubblicitarie o false partnership con il proposito di danneggiarne la reputazione o di condurre attività di criminalità informatica. Tra gli esempi rientrano: la creazione di profili o gruppi falsi sui social media che sfruttano illecitamente il brand o il logo di un'azienda, la creazione di applicazioni mobili ingannevoli o la distribuzione di pubblicità non autorizzate.

3.2.3.2 Extortion (TT:FR-EX)

Extortion identifica, nel contesto della sicurezza informatica, l'attività criminale in cui un aggressore esercita coercizione su un individuo o un'organizzazione per ottenere benefici finanziari o altre forme di compensazione. La condotta viene attuata tramite l'esercizio della minaccia di causare danni o di divulgare informazioni sensibili. Un esempio di questa pratica è il ransomware, un tipo di malware che cifra i dati della vittima rendendoli inaccessibili, utilizzato per costringere la vittima a pagare un riscatto, di solito in criptovalute, in cambio della chiave di decifratura. Altre forme di estorsione possono includere la minaccia di diffusione di dati personali o aziendali, qualora non vengano soddisfatte le richieste dell'aggressore.

3.2.3.3 Masquerade (TT:FR-MA)

Masquerade indica un'attività fraudolenta in cui un attore malevolo assume l'identità di un altro utente, dispositivo o entità all'interno di una rete o sistema informatico, al fine di eludere i meccanismi di sicurezza e acquisire accessi non autorizzati a risorse o beni informatici.

Tale attacco implica l'utilizzo fraudolento di credenziali, indirizzi di rete, token di autenticazione o altri dati identificativi utili per impersonare una fonte autorizzativa fidata. Un tipico caso è rappresentato da un attaccante che invia un'e-mail a un dipendente aziendale fingendo di essere il CEO dell'azienda e richiede con urgenza un trasferimento di fondi per una transazione aziendale critica o la divulgazione di informazioni riservate, come dati finanziari o dati dei clienti.

3.2.3.4 Resource misuse (TT:FR-RE)

Resource misuse identifica gli eventi cyber in cui un attore malevolo ha sfruttato in maniera non autorizzata le risorse di un computer o di una rete per scopi illeciti. Un tipico esempio è rappresentato da un dipendente che sfrutta il suo accesso ai sistemi aziendali per eseguire programmi che estraggono criptovalute (mining) oppure per effettuare attacchi informatici ai danni di soggetti terzi.

3.2.3.5 Spam (TT:FR-SP)

Spam identifica gli eventi cyber in cui un attore malevolo invia messaggi pubblicitari indesiderati o non richiesti, generalmente di carattere commerciale. I messaggi di spam possono essere inviati attraverso qualunque sistema di comunicazione, tra cui messaggi di posta elettronica, SMS, chat, forum e social media.

3.2.3.6 Other (TT:FR-OT)

Other identifica gli eventi cyber relativi al predicato Fraud (§ 3.2.3) non identificabili con gli altri valori definiti nel sottoinsieme.

3.2.4 Predicato: Brand abuse (BA)

Un'azione o una serie di azioni intenzionali che sfruttano il valore o la reputazione di un marchio per scopi malevoli, phishing, cybersquatting, typosquatting. Il **Brand abuse** può includere l'imitazione di siti web, l'uso non autorizzato di loghi o di marchi e la creazione di contenuti apparentamenti legittimi destinati a trarre in inganno gli utenti.

I valori associati per **Brand abuse** identificati dall'Agenzia per la tassonomia degli eventi cyber sono elencati di seguito.

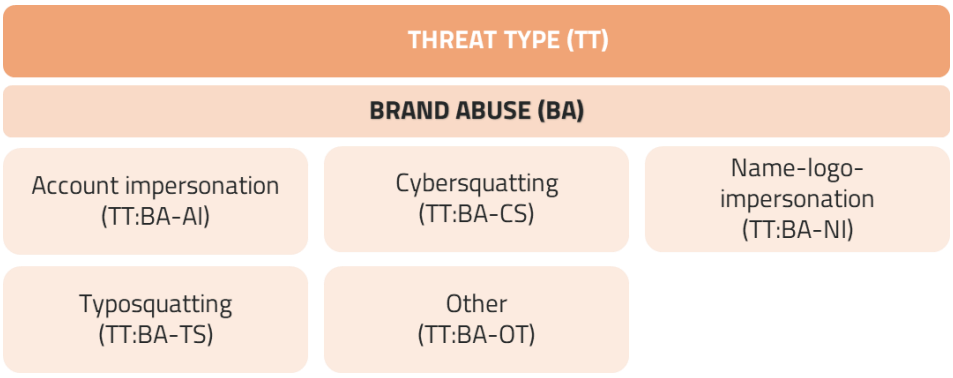

Figura 10: Predicato 'Brand abuse' con i relativi valori

3.2.4.1 Account impersonation (TT:BA-AI)

Account impersonation si riferisce all'attività in cui un attore malevolo si finge un'altra persona, sistema o organizzazione per ingannare la vittima e ottenere l'accesso non autorizzato a informazioni sensibili. Questa attività può includere sia la compromissione di un account

esistente, sia la creazione di un nuovo profilo affine.

3.2.4.2 Cybersquatting (TT:BA-CS)

Cybersquatting si riferisce alla pratica di registrare e utilizzare abusivamente un nome di dominio Internet identico o simile a marchi registrati, nomi di servizi, nomi personali o aziendali, con l'intento malevolo di deviare il traffico verso altri siti per ricavarne un profitto economico, diffondere malware o rubare proprietà intellettuale.

3.2.4.3 Name-logo-impersonation (TT:BA-NI)

Name-logo-impersonation si riferisce all'atto deliberato di replicare o imitare in modo fraudolento il nome e il logo di un'entità riconosciuta, come un'organizzazione rinomata o un servizio noto, nell'intento di trarre in inganno la vittima. Questa tecnica è impiegata prevalentemente nelle strategie di phishing o in altri schemi di ingegneria sociale.

3.2.4.4 Typosquatting (TT:BA-TS)

Typosquatting, conosciuto anche come "URL hijacking", è una pratica fraudolenta nell'ambito della sicurezza informatica che si verifica quando un attore malevolo registra deliberatamente nomi di dominio che imitano siti web esistenti con lievi variazioni ortografiche. Questo fenomeno sfrutta gli errori di digitazione che gli utenti commettono durante la battitura degli indirizzi web nel browser. Questa pratica può essere utilizzata per una serie di attività fraudolente, tra cui deviare il traffico verso altri siti, phishing o la diffusione di malware.

3.2.4.5 Other (TT:BA-OT)

Other identifica gli eventi cyber relativi a Brand abuse non identificabili con gli altri valori definiti nel sottoinsieme.

3.2.5 Predicato: Data exposure (DE)

Il predicato **Data exposure** identifica gli eventi cyber in cui è occorsa una violazione di sicurezza dei dati/informazioni personali o proprietarie. L'evento si riferisce alla divulgazione involontaria o non autorizzata di dati sensibili, compromettendo la riservatezza e la sicurezza delle informazioni.

I valori associati a **Data exposure** identificati dall'Agenzia per la tassonomia degli eventi cyber sono elencati di seguito.

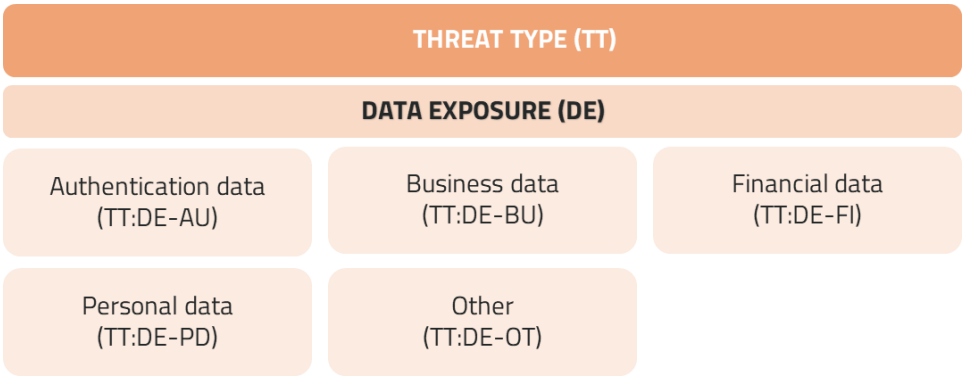

Figura 11: Predicato 'Data exposure' con i relativi valori

3.2.5.1 Authentication data (TT:ID-AU)

Authentication data identifica gli eventi cyber nei quali è stata identificata una violazione di sicurezza dei dati relativi all'autenticazione degli utenti del bene informatico impattato, come username e password.

3.2.5.2 Business data (TT:ID-BU)

Business data identifica gli eventi cyber nei quali è stata identificata una violazione di sicurezza dei dati relativi all'azienda, quali dati sulle sue attività, sui suoi contratti, sulla proprietà intellettuale, ecc.

3.2.5.3 Financial data (TT:ID-FI)

Financial data identifica gli eventi cyber nei quali è stata identificata una violazione di sicurezza dei dati relativi alla sfera finanziaria dell'azienda, come entrate, uscite, dati di transazioni finanziarie, dati relativi a carte di credito, ecc.

3.2.5.4 Personal data (TT:ID-PD)

Personal data identifica gli eventi cyber nei quali si è verificata una violazione di sicurezza dei personali, ovvero delle informazioni che identificano o rendono identificabile, **direttamente o indirettamente**, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc.

3.2.5.5 Other (TT:ID-OT)

Other identifica gli eventi cyber relativi a **Information disclosure** non identificabili con gli altri valori definiti nel sottoinsieme.

3.2.6 Predicato: Information gathering (IG)

Per **Information gathering** si intendono le tecniche, tattiche o procedure che possono essere utilizzate da criminali informatici al fine di raccogliere quante più informazioni possibili su un

determinato obiettivo, sia esso un utente, un'applicazione, un sistema o una rete.

I valori associati a **Information gathering** identificati dall'Agenzia per la tassonomia degli eventi cyber sono elencati di seguito.

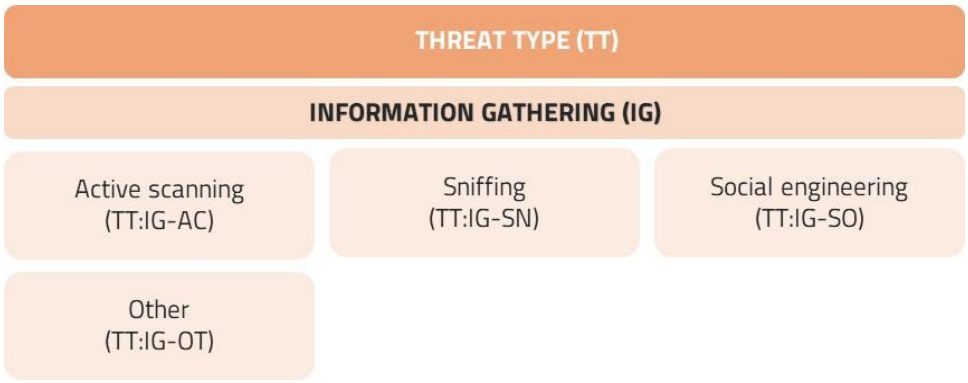

Figura 12: Predicato 'Information gathering' con i relativi valori

3.2.6.1 Active scanning (TT:IG-AC)

Active scanning identifica gli eventi cyber in cui un attore malevolo cerca di raccogliere informazioni mediante una scansione attiva, ossia attraverso contatti diretti con il bene informatico target. Per specificare i dettagli sulla tipologia di scansione attiva si utilizza il predicato Active scanning (§ 3.2.1).

3.2.6.2 Sniffing (TT:IG-SN)

Sniffing identifica gli eventi cyber in cui un attore non autorizzato utilizza tecniche o strumenti atti ad acquisire pacchetti di rete con il fine di rubare dati, monitorare attività di rete e raccogliere informazioni. Un esempio di eventi identificabili con tale valore è l'osservazione non autorizzata di informazioni d'interesse come ad esempio, header, credenziali o token di accesso non cifrati inviati in rete.

3.2.6.3 Social engineering (TT:IG-SO)

Social engineering identifica gli eventi cyber in cui un attore malevolo utilizza un insieme di tecniche e tattiche per persuadere un individuo a compiere determinate azioni per diverse finalità, tra le quali si evidenziano le seguenti:

- ottenere informazioni personali;
- ottenere credenziali di accesso;
- indurre l'utente a compiere azioni come, ad esempio, installare malware.

Attività di social engineering fanno leva sulla componente psicologica ed emotiva della vittima per ottenere gli obiettivi prefissati.

3.2.6.4 Other (TT:IG-OT)

Other identifica gli eventi cyber relativi a Information gathering non identificabili con gli altri valori

definiti nel sottoinsieme.

3.2.7 Predicato: Malicious code (MA)

Per **Malicious code** si intende un software o una porzione di codice potenzialmente dannosa, spesso inquadrabile come malware, che, una volta eseguito su un sistema, ha l'obiettivo di prenderne il controllo e/o comprometterne potenzialmente la riservatezza, l'integrità e la disponibilità.

I valori associati a **Malicious code** identificati dall'Agenzia per la tassonomia degli eventi cyber sono elencati di seguito.

THREAT TYPE (TT)		
MALICIOUS CODE (MA)		
Backdoor (TT:MA-BA)	Banker (TT:MA-BK)	Bot (TT:MA-BO)
Coin miner (TT:MA-CO)	Exploit kit (TT:MA-EX)	Hacking tool (TT:MA-HA)
Information stealer (TT:MA-IN)	Loader (TT:MA-LO)	Potentially Unwanted Program (TT:MA-PO)
Ransomware (TT:MA-RA)	Remote Access Tool (TT:MA-RE)	Rootkit (TT:MA-RO)
Trojan (TT:MA-TR)	Unknown (TT:MA-UN)	Virus (TT:MA-VI)
Webshell (TT:MA-WE)	Wiper (TT:MA-WI)	Worm (TT:MA-WO)

Figura 13: Predicato 'Malicious code' con i relativi valori

3.2.7.1 Backdoor (TT:MA-BA)

Una **Backdoor** è una tipologia di malware che garantisce un accesso secondario a un bene informatico compromesso, consentendo all'attaccante di accedervi da remoto ed eseguire azioni arbitrarie, come il trasferimento di file o l'esecuzione di comandi.

3.2.7.2 Banker (TT:MA-BK)

Un **Banker**, anche noto come banking trojan, è una tipologia di malware che tenta di sottrarre illecitamente le credenziali dei clienti di istituti bancari o di ottenere l'accesso alle loro informazioni finanziarie, tipicamente intercettando le comunicazioni del browser.

3.2.7.3 Bot (TT:MA-BO)

Un **Bot** è un programma informatico progettato per adempiere ad un preciso scopo, sia esso lecito o dannoso. In questo secondo caso, si parla di **bot malware**, ovvero strumenti utilizzati da criminali informatici per creare una rete di computer zombie, nota come *botnet*, ed effettuare un insieme di attività malevole di diversa natura. Spesso i bot vengono installati sulle macchine target a insaputa dell'utente.

3.2.7.4 Coin miner (TT:MA-CO)

Un **Coin miner** è una tipologia di malware che sfrutta la potenza di calcolo del bene informatico target per estrarre criptovalute a insaputa dell'utente.

3.2.7.5 Exploit kit (TT:MA-EX)

Un **Exploit kit** è un insieme di strumenti software progettati per sfruttare le vulnerabilità presenti in una rete, in un sistema o in un'applicazione. In sicurezza informatica, questi strumenti sono utilizzati dagli attaccanti per eseguire e automatizzare numerose tecniche e procedure di attacco al fine di accedere, infettare e danneggiare i beni informatici.

3.2.7.6 Hacking tool (TT:MA-HA)

Un **Hacking tool** è un programma progettato per violare le misure di sicurezza di un bene informatico. È utilizzato sia per attività di natura legittima (ad esempio per valutare la sicurezza di un bene informatico in un'attività di tipo red team) sia in contesti non autorizzati o per scopi illeciti. Alcuni esempi sono PsExec, Mimikatz, Cobalt Strike e LOIC.

3.2.7.7 Information stealer (TT:MA-IN)

Un **Information stealer** è una tipologia di malware che ha lo scopo di raccogliere informazioni su un bene informatico in maniera illegittima. Queste informazioni possono includere credenziali di accesso, dati personali e informazioni finanziarie. I malware noti come **keylogger** o **spyware** rientrano in questa classificazione.

3.2.7.8 Loader (TT:MA-LO)

Un **Loader** è una tipologia di malware che permette di scaricare ed eseguire malware aggiuntivi sul bene informatico compromesso. I malware noti come **dropper** e **downloader** rientrano in questa classificazione.

3.2.7.9 Potentially Unwanted Program (TT:MA-PO)

Un **Potentially Unwanted Program**, noto anche come PUP o PUA (Potentially Unwanted Application), può essere considerato come un software indesiderato secondo le preferenze dell'utente. Sebbene questa classificazione non indichi la presenza di un malware, i PUP possono rappresentare una minaccia per la privacy e la sicurezza del sistema e dell'utente.

3.2.7.10 Ransomware (TT:MA-RA)

Il **Ransomware** è una tipologia di minaccia che ha lo scopo di cifrare i dati del bene informatico target in modo da comprometterne la disponibilità e l'integrità. Inoltre, in questa tipologia di minaccia spesso l'attaccante crea dei file, detti *ransom notes*, tramite i quali viene richiesto alla vittima un riscatto in cambio dell'accesso ai propri dati. In alcuni casi i dati, prima di essere cifrati, vengono esfiltrati in modo da offrire all'attaccante uno strumento in più di ricatto nei confronti della vittima.

3.2.7.11 Remote Access Tool (TT:MA-RE)

Un **RAT**, acronimo di Remote Access Tool, è una tipologia di malware che consente all'attaccante di controllare un bene informatico target da remoto. Questa tipologia di codice malevolo permette di eseguire varie azioni non autorizzate, come l'acquisizione di dati, il trasferimento di file e l'esecuzione di comandi arbitrari.

3.2.7.12 Rootkit (TT:MA-RO)

Un **Rootkit** è una tipologia di malware tipicamente sofisticato progettato per infiltrarsi all'interno di un sistema operativo o di un'applicazione, mascherando la sua presenza e ottenendo privilegi di accesso elevati. Un rootkit ha la caratteristica di infettare e modificare le funzioni del sistema operativo e le sue strutture dati. In sicurezza informatica, le caratteristiche del rootkit permettono di evadere i controlli dell'antivirus e di garantire persistenza a lungo termine sui sistema target.

3.2.7.13 Trojan (TT:MA-TR)

Un **Trojan** è una tipologia di software che si presenta all'utente sotto forma di programma legittimo o comunque non dannoso, ma che una volta eseguito ha lo scopo di scaricare e avviare sul bene informatico target un ulteriore software malevolo. I trojan sono progettati per ingannare gli utenti e possono svolgere una vasta gamma di funzioni malevole, come il furto di informazioni, il controllo remoto del sistema, l'installazione di altri malware o la creazione di backdoor per consentire l'accesso non autorizzato.

3.2.7.14 Unknown (TT:MA-UN)

Unknown identifica una tipologia di codice malevolo per cui non si hanno informazioni sufficienti a indicarne la natura. Tale valore si utilizza in eventi cyber in cui è stata riscontrata la l'esecuzione di codice malevolo o malware ma non è ancora in grado di stabilirne la tipologia.

3.2.7.15 Virus (TT:MA-VI)

Un **Virus** è un software potenzialmente dannoso che, quando eseguito su un bene informatico, ha l'obiettivo di autoreplicarsi modificando (infettando) i programmi in esecuzione e alterandone (injection) il funzionamento. Utilizzando un virus, un attaccante potrebbe eliminare i dati e/o i programmi presenti su un bene informatico, bloccarne l'accesso o attuare tecniche di

compromissione avanzate per garantirsi persistenza sul sistema e permetterne la raggiungibilità da remoto (i.e. installando una backdoor).

3.2.7.16 Webshell (TT:MA-WE)

Una **Webshell** è una tipologia di script o programma che viene installato su un server web compromesso al fine di ottenere un accesso non autorizzato e persistente sul bene informatico.

3.2.7.17 Wiper (TT:MA-WI)

Il **Wiper** è una tipologia di malware il cui obiettivo principale è quello di eliminare in modo irreversibile dati e file presenti su un bene informatico compromesso. A differenza di altri tipi di malware che cercano di rubare informazioni o estorcere denaro, il wiper ha come obiettivo principale l'eliminazione dei dati, spesso con l'intento di causare danni irreparabili o di sabotare le attività di un'organizzazione.

3.2.7.18 Worm (TT:MA-WO)

Il **Worm** è un software potenzialmente dannoso che l'attaccante può sfruttare per replicare un malware all'interno di un bene informatico per comprometterne le funzionalità. La caratteristica principale del worm è la capacità di autoreplicarsi su una rete, senza richiedere l'interazione diretta dell'utente. I worm, a differenza di altri tipi di malware come i virus, possono propagarsi in modo indipendente e autonomo, ad esempio sfruttando le vulnerabilità dei beni informatici o le funzionalità di condivisione di file e risorse di rete.

3.2.8 Predicato: Social engineering (SO)

Il predicato **Social engineering** identifica un evento di sicurezza informatica in cui un attore malevolo sfrutta un insieme di tecniche e tattiche per persuadere un individuo a compiere azioni che hanno conseguenze sul dominio cyber quali, ad esempio, il download di malware e la condivisione di informazioni personali o sensibili. Attività di Social Engineering fanno leva sulla componente psicologica ed emotiva della vittima per ottenere gli obiettivi prefissati.

I valori associati a **Social engineering** identificati dall'Agenzia per la tassonomia degli eventi cyber sono elencati di seguito.

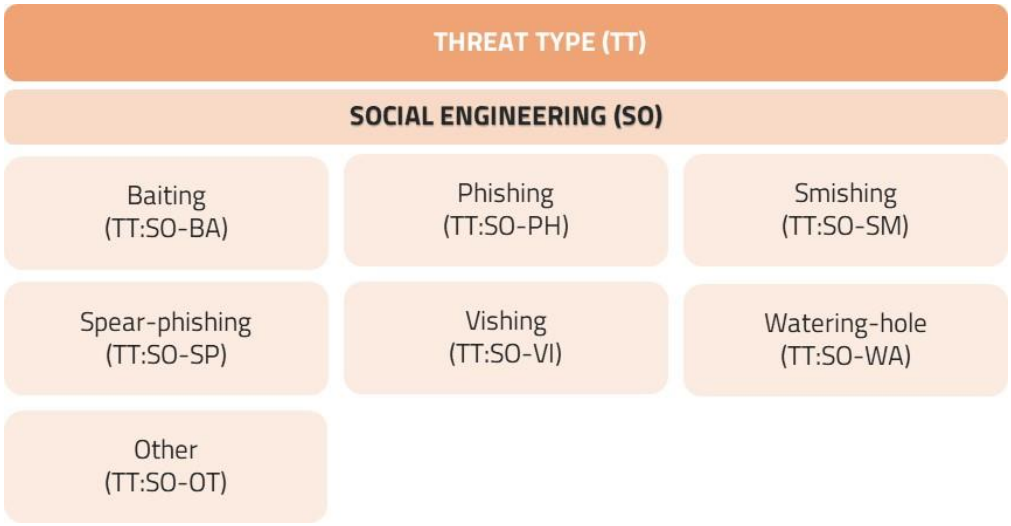

Figura 14: Predicato 'Social engineering' con i relativi valori

3.2.8.1 Baiting (TT:SO-BA)

Baiting identifica attività fraudolente in cui un attore malevolo attira la vittima mediante un'esca, come la promessa della ricezione di un bene o l'ottenimento di un vantaggio. La superficie di attacco comprende sia il mondo online sia la vita reale. In questi casi, l'attaccante tenta di sfruttare la curiosità umana per convincere la vittima ad effettuare azioni quali, ad esempio, l'inserimento di dati personali su falsi servizi online, il download di malware occultato da applicazioni e contenuti leciti, oppure tramite dispositivi USB utilizzati come esca.

3.2.8.2 Phishing (TT:SO-PH)

Phishing identifica gli eventi cyber in cui un utente viene contattato, tramite e-mail o altri strumenti di messaggistica, da un attore malevolo allo scopo di condurre la vittima all'esecuzione di codice malevolo o a visitare risorse artefatte con lo scopo di carpire dati personali, bancari o credenziali di accesso, trasferire somme di denaro. Gli eventi di phishing possono anche essere il preludio o una componente di attacchi informatici più ampi e complessi.

3.2.8.3 Smishing (TT:SO-SM)

Smishing identifica gli eventi cyber in cui un utente viene contattato, tramite l'invio di brevi messaggi di testo (SMS), da un attore malevolo allo scopo di condurre la vittima all'esecuzione di codice malevolo come false applicazioni *mobile* o a visitare risorse artefatte con lo scopo di carpire dati personali, bancari o credenziali di accesso, trasferire somme di denaro. Gli eventi di smishing possono anche essere il preludio o una componente di attacchi informatici più ampi e complessi.

3.2.8.4 Spear-phishing (TT:SO-SP)

Spear-phishing è una tipologia di phishing contro target di specifico interesse che prevede l'invio di un messaggio altamente personalizzato da un account di posta elettronica apparentemente noto alla vittima, con l'intento di carpire informazioni sensibili, ovvero indurla ad aprire/scaricare

allegati o link malevoli. Allo spear-phishing possono essere associate tecniche di ingegneria sociale, tra cui il monitoraggio delle relazioni e delle abitudini sui social media del soggetto d'interesse.

3.2.8.5 Vishing (TT:SO-VI)

Vishing identifica gli eventi cyber in cui un utente viene contattato, tramite sistemi di comunicazione vocale, da un attore criminale allo scopo di condurre la vittima all'esecuzione di codice malevolo o di carpire dati aziendali, personali, bancari o credenziali di accesso, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

3.2.8.6 Watering-hole (TT:SO-WA)

Watering-hole identifica gli eventi cyber nel quale un attaccante mira a compromettere un gruppo specifico di utenti attraverso l'infezione di siti web che sono noti per essere regolarmente visitati da tale gruppo. L'obiettivo di questa tipologia di attacchi è quello di colpire la vittima in modo indiretto tramite la compromissione dell'applicazione Web interessata.

3.2.8.7 Other (TT:SO-OT)

Other identifica gli eventi cyber relativi a Social engineering non identificabili con gli altri valori definiti nel sottoinsieme.

3.2.9 Predicato: Vulnerability (VU)

Il predicato **Vulnerability** identifica quale tipologia di vulnerabilità interessa un determinato prodotto o servizio o è connessa ad uno specifico evento cyber.

I valori associati a **Vulnerability** identificati dall'Agenzia per la tassonomia degli eventi cyber sono elencati di seguito.

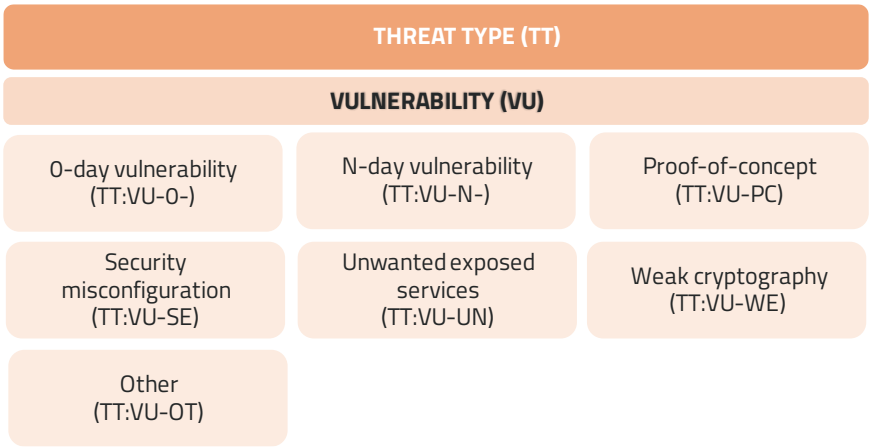

Figura 15: Predicato 'Vulnerability' con i relativi valori

3.2.9.1 0-day vulnerability (TT:VU-0-)

0-day vulnerability identifica che un determinato bene informatico è affetto da una vulnerabilità

non nota pubblicamente, che quindi potrebbe essere sfruttata da un attaccante per compromettere un sistema informativo e minarne l'integrità, la riservatezza e la disponibilità.

3.2.9.2 N-day vulnerability (TT:VU-N-)

N-day vulnerability identifica una vulnerabilità 0-day che è stata resa pubblica da più di un giorno, indipendentemente dal rilascio del software correttivo. Generalmente, in questi casi, anche successivamente alla pubblicazione della falla di sicurezza un attaccante potrebbe sfruttare la vulnerabilità per compromettere i beni informatici affetti prima che venga attuata la risoluzione tramite il relativo aggiornamento o l'eventuale workaround.

3.2.9.3 Proof-of-concept (TT:VU-PC)

Proof-of-concept identifica, nel contesto della sicurezza informatica, la disponibilità di una dimostrazione tecnica realizzata per validare la presenza di una vulnerabilità teorica, dimostrando come essa possa essere sfruttata in un software o in un sistema informatico.

3.2.9.4 Security misconfiguration (TT:VU-SE)

Security misconfiguration indica che la configurazione errata di un bene informatico può portare a rischi di sicurezza e provocare falle che possono essere facilmente sfruttate da un criminale informatico per compromettere un sistema. Alcuni esempi di Security misconfiguration sono il mancato hardening dei sistemi, un'errata gestione dei permessi o l'installazione e abilitazione di funzionalità non adeguatamente protette.

3.2.9.5 Unwanted exposed services (TT:VU-UN)

Unwanted exposed services indica che il bene informatico coinvolto nell'evento di sicurezza espone servizi di rete generalmente non raccomandati in quanto in grado di ampliare la superficie di attacco e, se non adeguatamente protetti, possono inficiare sulla postura di sicurezza. Si tratta di servizi sfruttabili da attori malevoli per penetrare all'interno della rete delle vittime o tali da agevolare, ad esempio, attacchi di tipo DDoS reflection.

3.2.9.6 Weak cryptography (TT:VU-WE)

Weak cryptography identifica gli eventi cyber relativi all'utilizzo improprio o non corretto dei meccanismi di sicurezza legati alla crittografia. Tecniche di cifratura che impiegano algoritmi di crittografia deboli possono fornire una sicurezza inadeguata contro gli attacchi informatici tali da comportare l'esposizione di dati sensibili, la perdita di chiavi, l'interruzione dell'autenticazione, sessioni non sicure e facilitare attacchi di spoofing.

3.2.9.7 Other (TT:VU-OT)

Other identifica gli eventi cyber relativi a Vulnerability non identificabili con gli altri valori definiti nel sottoinsieme.

3.3 THREAT ACTOR (TA)

3.3.1 Predicato: Adversary motivation (AM)

Adversary motivation identifica, se note al momento della condivisione, le motivazioni che hanno mosso l'attore malevolo nel compiere l'attività illecita o malevola.

I valori associati ad **Adversary motivation** identificati dall'Agenzia per la tassonomia degli eventi sono elencati di seguito.

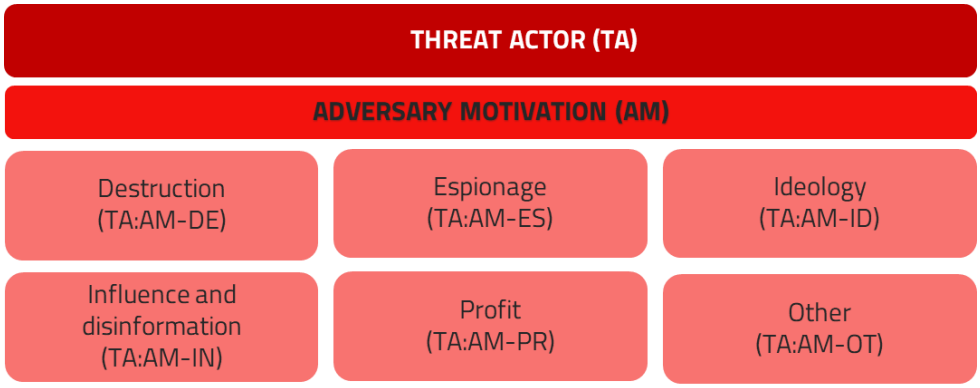

Figura 16: Predicato 'Adversary motivation' con i relativi valori

3.3.1.1 Destruction (TA:AM-DE)

Destruction identifica gli eventi cyber nei quali un attaccante ha condotto attività malevole o illecite volte a danneggiare un bene informatico, al fine di comprometterne il funzionamento, di interrompere l'erogazione totale o parziale dei servizi forniti o di impedirne l'accesso al personale autorizzato. Un esempio di evento cyber dimostrativo per queste caratteristiche è rappresentato dagli attacchi che prevedono l'utilizzo di malware di tipo wiper (§ 3.2.7.17).

È importante evidenziare che gli eventi ransomware non possono essere identificati con questo valore poiché in tali casi, solitamente, l'avversario è mosso da interessi economici (§ 3.3.1.5) e pertanto non è interessato al mero danneggiamento.

3.3.1.2 Espionage (TA:AM-ES)

Espionage identifica gli eventi cyber nei quali un attaccante ha condotto un'attività indebita finalizzata all'acquisizione di dati/informazioni sensibili, proprietarie o classificate al fine di conseguire un guadagno economico, un vantaggio competitivo o per ragioni politiche. In questa categoria rientrano, ad esempio, la sottrazione di segreti industriali, di informazioni classificate o di proprietà intellettuale.

3.3.1.3 Ideology (TA:AM-ID)

Ideology identifica gli eventi cyber nei quali un attaccante ha condotto attività malevole o illecite per diffondere un messaggio di natura ideologica all'organizzazione colpita, ai fruitori del servizio

impattato o a qualunque terza parte anche non direttamente coinvolta nell'illecito. Gli eventi cyber che appartengono a questa categoria vengono spesso compiuti dai cosiddetti hacktivisti. A tal proposito di rimanda al valore Hacktivist (§ 3.3.2.2) del predicato Adversary type (§ 3.3.2).

3.3.1.4 Influence and disinformation (TA:AM-IN)

Influence and disinformation identifica gli eventi cyber nei quali avviene diffusione intenzionale di notizie o informazioni inesatte o distorte allo scopo di influenzare le azioni e le scelte di qualcuno.

3.3.1.5 Profit (TA:AM-PR)

Profit identifica gli eventi cyber in cui un attaccante o un gruppo effettua azioni malevole o illecite al fine di ottenerne in modo diretto o indiretto un profitto. Alcuni esempi:

- richiesta di riscatto in denaro in caso di ransomware;
- richiesta di riscatto in denaro in caso di sextortion;
- phishing finalizzato alla sottrazione di dati bancari;
- infezione con malware di tipo trojan bancari.

3.3.1.6 Other (TA:AM-OT)

Other identifica gli eventi cyber relativi ad Adversary motivation non identificabili con gli altri valori definiti nel sottoinsieme.

3.3.2 Predicato: Adversary type (AD)

Il predicato **Adversary type** identifica, se nota al momento della condivisione, la tipologia di attaccante o gruppo che ha perpetrato le azioni malevole o illecite. Questo predicato non indica le motivazioni che hanno mosso l'avversario, per le quali è invece prevista la categoria Adversary motivation (§ 3.3.1).

I valori associati ad **Adversary type** identificati dall'Agenzia per la tassonomia degli eventi cyber sono elencati di seguito.

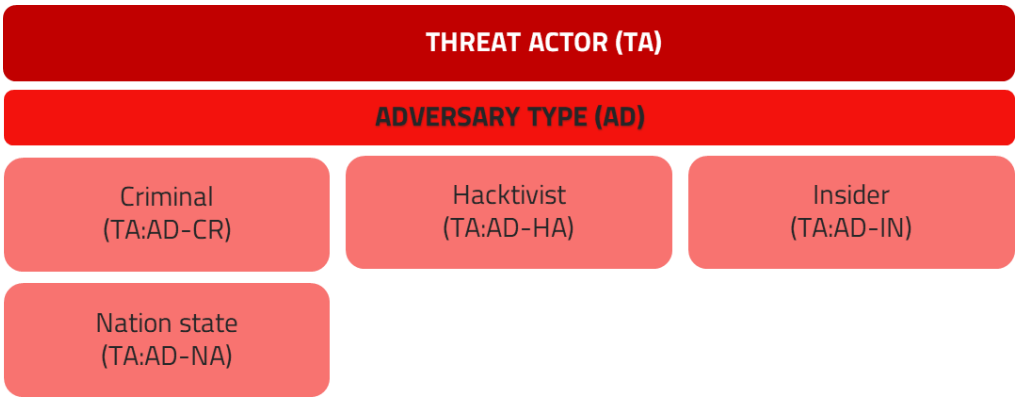

Figura 17: Predicato 'Adversary type' con i relativi valori

3.3.2.1 Criminal (TA:AD-CR)

Criminal identifica gli eventi cyber in cui l'attaccante o il gruppo che ha causato l'evento può essere categorizzato nella tipologia più generica di "criminale" i cui scopi tendono a generare un profitto dalle azioni svolte.

3.3.2.2 Hacktivist (TA:AD-HA)

Hacktivist identifica gli eventi cyber in cui è previsto l'uso sovversivo di strumenti digitali al fine di promuovere un'agenda politica o principi di connotazione sociale. Questi gruppi utilizzano tecniche di hacking ad esempio per:

- attaccare siti web per compromettere l'erogazione di servizi o alterarne i contenuti per diffondere messaggi di natura politica o ideologica;
- pubblicare dati governativi classificati per denunciare la mancanza di protezione dei dati da parte delle autorità;
- reindirizzare gli utenti su siti gestiti dagli attivisti digitali per diffondere la propria ideologia.

3.3.2.3 Insider (TA:AD-IN)

Insider identifica gli eventi cyber in cui un attaccante utilizza le proprie autorizzazioni o le conoscenze acquisite durante le consuete attività lavorative per compiere un attacco informatico dall'interno della rete dalla quale opera. L'obiettivo di un insider può essere ad esempio il furto di informazioni sensibili, il danneggiamento di un sistema, il sabotaggio dell'azienda o la vendita delle informazioni trafugate.

3.3.2.4 Nation state (TA:AD-NA)

Nation state identifica gli eventi cyber condotti da entità o gruppi statuali o sponsorizzati dallo Stato, ossia gruppi che conducono operazioni cibernetiche avanzate per conto di un governo o di uno Stato sovrano. Questi attori sono sostenuti o autorizzati dal governo del loro paese per perseguire obiettivi di interesse nazionale attraverso attività di hacking, spionaggio o guerra cibernetica. Questa tipologia di avversario dispone solitamente di risorse significative, tra cui personale altamente qualificato, budget cospicui e accesso a strumenti e tecnologie avanzate.

3.4 ADDITIONAL CONTEXT (AC)

3.4.1 Predicato: Abusive content (AB)

Nell'ambito di un evento di sicurezza informatica, il predicato **Abusive content** identifica la presenza di materiale offensivo, illegale o non voluto inviato ad un utente con finalità di ferirne la sensibilità o la dignità. La diffusione di tale materiale può avvenire in maniera diretta, ad esempio tramite e-mail o sms, o in maniera indiretta, ad esempio tramite popup o pubblicità su Internet.

I valori associati a **Abusive content** identificati dall'Agenzia per la tassonomia degli eventi cyber sono elencati di seguito.

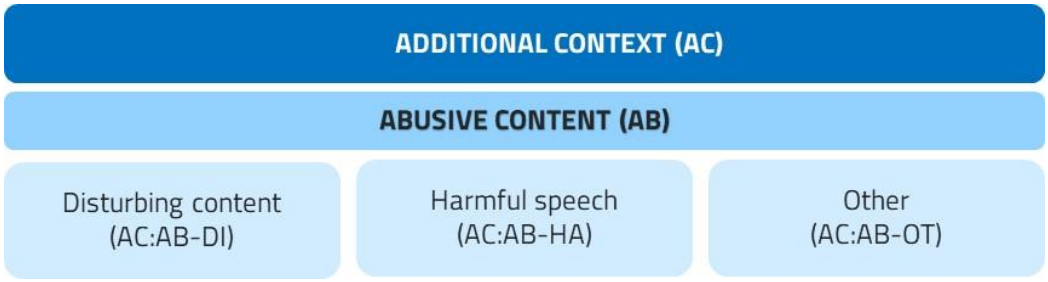

Figura 18: Predicato 'Abusive content' con i relativi valori

3.4.1.1 Disturbing content (AC:AB-DI)

Disturbing content identifica qualsiasi tipo di materiale o informazione diffusa tramite sistemi informatici che può essere considerato offensivo, inappropriato, dannoso o che possa provocare disagio psicologico o emotivo.

3.4.1.2 Harmful speech (AC:AB-HA)

Harmful speech identifica eventi qualsiasi forma di comunicazione espressa tramite piattaforme digitali che può causare danno, disagio o discriminazione a individui o gruppi. Tra questi, discorsi corredati da argomenti offensivi quali bullismo, molestie, mobbing, diffamazione o discriminazione contro uno o più soggetti, con il possibile intento di discreditare e/o diffamare pubblicamente la vittima.

3.4.1.3 Other (AC:AB-OT)

Other identifica gli eventi cyber relativi ad Abusive content non identificabili con gli altri valori definiti nel sottoinsieme.

3.4.2 Predicato: Asset source geography (AS)

Il predicato **Asset source geography** identifica la localizzazione geografica di beni informatici coinvolti in eventi cyber che sono stati identificati come "sorgenti" di attività malevole o illecite.

I valori associati ad **Asset source geography** identificati dall'Agenzia per la tassonomia degli eventi cyber sono elencati di seguito.

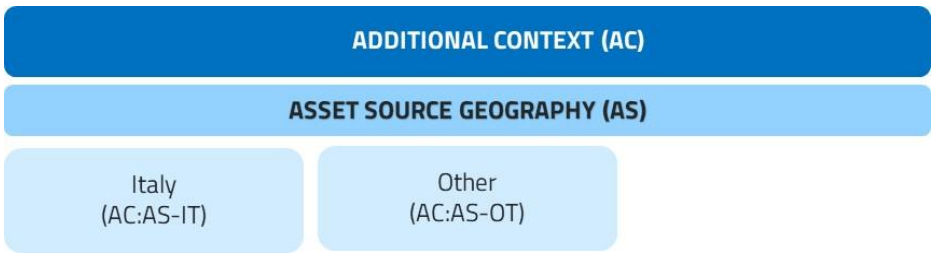

Figura 19: Predicato 'Asset source geography' con i relativi valori

3.4.2.1 Italy (AC:AS-IT)

Italy indica che i beni informatici da cui sono state condotte attività malevole o illecite sono localizzati sul territorio nazionale italiano.

3.4.2.2 Other (AC:AS-OT)

Other indica che i beni informatici da cui sono state condotte attività malevole o illecite sono localizzati al di fuori del territorio nazionale italiano.

3.4.3 Predicato: Involved asset (IN)

Il predicato **Involved asset** identifica le risorse coinvolte nell'evento cyber. I valori relativi a questo predicato possono indicare una o più risorse interessate dall'evento, anche in assenza di impatto.

I valori associati a **Involved asset** identificati dall'Agenzia per la tassonomia degli eventi cyber sono elencati di seguito.

ADDITIONAL CONTEXT (AC)		
INVOLVED ASSET (IN)		
Business e-mail (AC:IN-BU)	Hypervisor (AC:IN-HY)	Industrial Control Systems (AC:IN-IN)
IoT device (AC:IN-IO)	Mobile device (AC:IN-MO)	Network device (AC:IN-NE)
Personal e-mail (AC:IN-PE)	Privileged account (AC:IN-PR)	Unprivileged account (AC:IN-UN)
Server (AC:IN-SR)	Service or application (AC:IN-SE)	Social media (AC:IN-SO)
Security appliance (AC:IN-SA)	VPN account (AC:IN-VP)	Web application (AC:IN-WA)
Workstation (AC:IN-WO)	Other (AC:IN-OT)	

Figura 20: Predicato 'Involved asset' con i relativi valori

3.4.3.1 Business e-mail (AC:IN-BU)

L'utilizzo di tale valore specifica se l'evento ha interessato una o più **caselle di posta elettronica aziendale**, ad esempio: la compromissione della casella, la ricezione di una mail di phishing o spam, anche senza impatto, l'esposizione pubblica di caselle di posta aziendale a seguito di divulgazione, i tentativi di accesso alla casella di posta aziendale.

3.4.3.2 Hypervisor (AC:IN-HY)

L'utilizzo di tale valore specifica se l'evento ha interessato un **hypervisor**. Si definisce hypervisor un sistema che opera da host e consente la creazione e la gestione di una serie di macchine virtuali definite guest, isolandone il sistema operativo o le risorse. Tra questi rientrano, ad esempio, quelli in cui un attore malevolo ha ottenuto accesso all'hypervisor ed eseguito un ransomware, cifrando conseguentemente tutti i sistemi guest contenuti.

3.4.3.3 Industrial Control Systems (AC:IN-IN)

L'utilizzo di tale valore specifica se l'evento ha interessato un sistema industriale. Si definisce **Industrial Control System** (ICS) un sistema informativo utilizzato per controllare processi industriali come la fabbricazione, la movimentazione dei prodotti, la produzione e la distribuzione.

3.4.3.4 IoT device (AC:IN-IO)

L'utilizzo di tale valore specifica se l'evento ha interessato un **dispositivo IoT** (Internet of Things). Si definisce dispositivo IoT un dispositivo fisico dotato di un sistema integrato che gli consente di adempiere a compiti predeterminati e di collegarsi ad una rete per interoperare e scambiare informazioni con altri sistemi. In generale, i dispositivi IoT sono oggetti di uso quotidiano quali per esempio elettrodomestici, veicoli, sensori o telecamere.

3.4.3.5 Mobile device (AC:IN-MO)

L'utilizzo di tale valore specifica se l'evento ha interessato un **dispositivo mobile**, come per esempio uno smartphone o un tablet.

3.4.3.6 Network device (AC:IN-NE)

L'utilizzo di tale valore specifica se l'evento ha interessato un qualsiasi **dispositivo di rete**, come ad esempio router e switch. Per i dispositivi network utilizzati nella gestione della sicurezza aziendale fare riferimento al valore Security appliance (§ 3.4.3.13).

3.4.3.7 Personal e-mail (AC:IN-PE)

L'utilizzo di tale valore specifica se l'evento ha interessato una **casella di posta elettronica personale**, ad esempio: la compromissione della casella, la ricezione di una mail di phishing o spam, anche senza impatto, l'esposizione pubblica di caselle di posta a seguito di divulgazione, i tentativi di accesso alla casella di posta aziendale.

3.4.3.8 Privileged account (AC:IN-PR)

L'utilizzo di tale valore specifica se l'evento ha interessato un **account privilegiato**. Si definisce account privilegiato un'utenza che ha un ruolo di alto livello in termini di autorizzazione nella gestione di un sistema informatico tale da modificarne le componenti critiche. Ad esempio: la compromissione di un account di amministratore locale o di dominio.

3.4.3.9 Unprivileged account (AC:IN-UN)

L'utilizzo di tale valore specifica se l'evento ha interessato un **account senza privilegi**. Si intende con "account senza privilegi" un utente con permessi limitati di accesso e di modifica a un sistema o a un'infrastruttura di rete. Un esempio è rappresentato da un attacco che è iniziato dalla compromissione di un account utente.

3.4.3.10 Server (AC:IN-SR)

L'utilizzo di tale valore specifica se l'evento ha interessato un **server**. Si definisce server un computer o un dispositivo che in una rete gestisce e fornisce risorse. Gli esempi includono file server (per archiviare file), server di stampa (per gestire una o più stampanti), server di posta (per gestire le caselle di posta elettronica) e server di database (per elaborare le query del database).

3.4.3.11 Service or application (AC:IN-SE)

L'utilizzo di tale valore specifica se l'evento ha interessato **servizi o applicazioni**. L'applicazione o il servizio può essere di qualunque natura, ivi incluse applicazioni Web, Mobile, Database, ecc.

3.4.3.12 Social media (AC:IN-SO)

L'utilizzo di tale valore specifica se l'evento ha interessato account di **social media**. Un esempio è rappresentato da un attore malevolo che ha ottenuto in modo illecito le credenziali di un account social aziendale.

3.4.3.13 Security appliance (AC:IN-SA)

L'utilizzo di tale valore specifica se l'evento ha interessato un **qualsiasi dispositivo utilizzato per proteggere i sistemi e la rete** da traffico malevolo e tutti quei sistemi che concorrono alla gestione delle politiche di sicurezza come ad esempio:

- Firewalls/Proxy;
- Intrusion Protection Systems (IPS);
- Unified Threat Management (UTM);
- Network Access Control;
- E-mail Security Gateways;
- Web Application Firewalls (WAF);
- VPN Gateways;
- Network Device Backup and Recovery.

3.4.3.14 VPN account (AC:IN-VP)

L'utilizzo di tale valore specifica se l'evento ha interessato un account connesso ad un profilo **Virtual Private Network** (**VPN**). La VPN è una rete virtuale costruita su reti esistenti in grado di fornire un meccanismo di comunicazione sicuro per i dati e le informazioni IP trasmesse tra le

reti. Un esempio di evento cyber, indicativo per tale valore, è rappresentato da una compromissione o da ripetuti tentativi di accesso non autorizzati di un account VPN utilizzato per accedere alle risorse interne aziendali.

3.4.3.15 Web application (AC:IN-WA)

L'utilizzo di tale valore specifica se l'evento ha interessato un'**applicazione software** che viene eseguita su un server web e fruibile tramite un browser. Alcuni esempi di eventi cyber che coinvolgono web application sono: SQL injection, Cross-Site-Scripting (XSS), Cross-Site-Request Forgery (CSRF), violazione di dati, defacement, session hijacking, etc.

3.4.3.16 Workstation (AC:IN-WO)

L'utilizzo di tale valore specifica se l'evento ha interessato una o più **postazioni di lavoro**. Un esempio è rappresentato da una compromissione o movimento laterale iniziato da una workstation di un dipendente aziendale.

3.4.3.17 Other (AC:IN-OT)

Other identifica gli eventi cyber relativi a Involved asset non identificabili con gli altri valori definiti nel sottoinsieme.

3.4.4 Predicato: Operating system (OS)

Il predicato **Operating system** identifica la piattaforma operativa software interessata da un determinato evento cyber.

I valori associati a **Operating system** identificati dall'Agenzia per la tassonomia degli eventi cyber sono elencati di seguito.

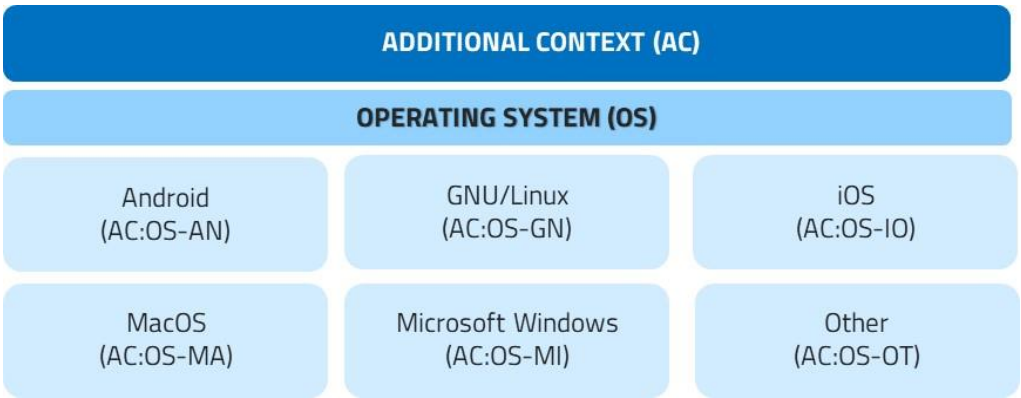

Figura 21: Predicato 'Operating system' con i relativi valori

3.4.4.1 Android (AC:OS-AN)

L'utilizzo di tale valore specifica se l'evento ha interessato un sistema operativo **Google Android**, in qualunque sua versione.

3.4.4.2 GNU/Linux (AC:OS-GN)

L'utilizzo di tale valore specifica se l'evento ha interessato un sistema operativo **GNU/Linux**, in qualunque sua versione.

3.4.4.3 iOS (AC:OS-IO)

L'utilizzo di tale valore specifica se l'evento ha interessato un sistema operativo **Apple iOS**, in qualunque sua versione.

3.4.4.4 MacOS (AC:OS-MA)

L'utilizzo di tale valore specifica se l'evento ha interessato un sistema operativo **macOS**, in qualunque sua versione.

3.4.4.5 Microsoft Windows (AC:OS-MI)

L'utilizzo di tale valore specifica se l'evento ha interessato un sistema operativo **Microsoft Windows** in qualunque sua versione, anche server.

3.4.4.6 Other (AC:OS-OT)

L'utilizzo di tale valore specifica se l'evento ha interessato un **sistema operativo, in qualunque sua versione, diverso** da quelli definiti in questo sottoinsieme (ad esempio: sistemi basati su BSD, Solaris, o sistemi operativi proprietari sviluppati da altri produttori).

3.4.5 Predicato: Outlook (OU)

Il predicato **Outlook** ha l'obiettivo di fornire una prospettiva sull'impatto generato da un evento cyber al momento del rilevamento.

I valori associati a **Outlook** identificati dall'Agenzia per la tassonomia degli eventi cyber sono elencati di seguito.

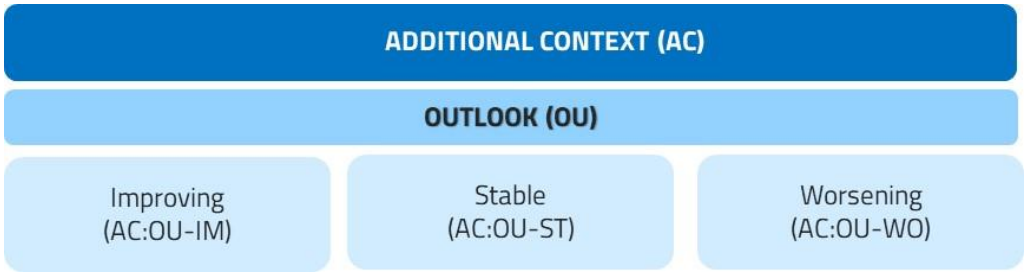

Figura 22: Predicato 'Outlook' con i relativi valori

3.4.5.1 Improving (AC:OU-IM)

Improving identifica un evento cyber in corso per il quale si prevede una riduzione dell'impatto nelle successive sei ore dal momento del rilevamento.

3.4.5.2 Stable (AC:OU-ST)

Stable identifica un evento cyber in corso per il quale si prevede che l'impatto rimanga invariato nelle successive sei ore dal momento del rilevamento.

3.4.5.3 Worsening (AC:OU-WO)

Worsening identifica un evento cyber in corso per il quale si prevede che l'impatto si aggravi nelle successive sei ore dal momento del rilevamento.

3.4.6 Predicato: Physical security (PH)

Il predicato **Physical security** identifica gli eventi intenzionali, di natura fisica, con impatto su risorse e servizi informatici. Alcuni esempi possono essere l'accesso fisico non autorizzato a zone riservate da parte di estranei finalizzato al sabotaggio deliberato di una piattaforma operativa o furto di componenti hardware.

I valori associati a **Physical security** identificati dall'Agenzia per la tassonomia degli eventi cyber sono elencati di seguito.

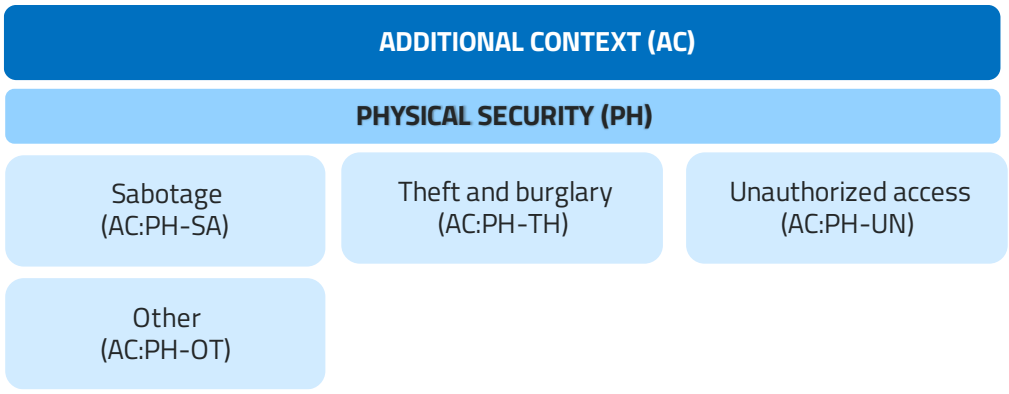

Figura 23: Predicato 'Physical security' con i relativi valori

3.4.6.1 Sabotage (AC:PH-SA)

Sabotage identifica qualsiasi azione intenzionale volta a danneggiare, distruggere o alterare il funzionamento della risorsa informatica o parti di questa. Queste azioni sono compiute con lo scopo di causare la perdita totale o parziale della disponibilità della risorsa informatica.

3.4.6.2 Theft and burglary (AC:PH-TH)

Theft and bulglary identifica gli eventi cyber conseguenti al furto di un bene informatico o parti di esso.

3.4.6.3 Unauthorized access (AC:PH-UN)

Unauthorized access identica gli eventi cyber che si verificano quando chiunque ottiene, senza autorizzazione, accesso fisico ad un bene informatico.

3.4.6.4 Other (AC:PH-OT)

Other identifica gli eventi cyber relativi a Physical security non identificabili con gli altri valori definiti nel sottoinsieme.

3.4.7 Predicato: Vector (VE)

Il predicato **Vector** indica il vettore di attacco utilizzato in un evento cyber. In sicurezza informatica, si definisce vettore d'attacco la modalità con la quale un attore ostile tenta di ottenere l'accesso ad un bene informatico per effettuare attività malevole. Tra i vettori di attacco si annoverano genericamente tattiche, tecniche di attacco e mezzi informatici.

I valori associati a **Vector** identificati dall'Agenzia per la tassonomia degli eventi cyber sono elencati di seguito.

ADDITIONAL CONTEXT(AC)		
VECTOR (VE)		
Abuse of functionality (AC:VE-AB)	Compromised domain (AC:VE-CO)	Drive-by compromise (AC:VE-DR)
E-mail (AC:VE-E-)	Exploiting vulnerabilities (AC:VE-EV)	External remote services (AC:VE-EX)
Hardware additions (AC:VE-HA)	Social media (AC:VE-SO)	Supply chain (AC:VE-SU)
Valid accounts (AC:VE-VA)	Other (AC:VE-OT)	

Figura 24: Predicato 'Vector' con i relativi valori

3.4.7.1 Abuse of functionality (AC:VE-AB)

Abuse of functionality identifica gli eventi cyber in cui un attore malevolo sfrutta in modo intenzionale e non convenzionale le funzionalità fornite da un'applicazione o un sito web. In altri termini, può essere descritto come l'abuso di una funzionalità di un'applicazione per ottenere un risultato indesiderato. Ad esempio, nel caso in cui il processo di recupero password non venga implementato nella maniera corretta, un attore malevolo sarà in grado di recuperare informazioni d'interesse (come indirizzo e-mail o nome dell'account).

3.4.7.2 Compromised domain (AC:VE-CO)

Compromised domain specifica se l'evento ha interessato un dominio internet lecito che viene utilizzato per veicolare attacchi informatici, quali ad esempio la distribuzione di malware,

reindirizzamento della navigazione verso risorse malevole, truffe a danno di soggetti target come il furto di dati personali tramite pagine web illecitamente predisposte.

3.4.7.3 Drive-by compromise (AC:VE-DR)

Drive-by compromise identifica gli eventi cyber in cui un utente, tramite la navigazione di un sito web, viene esposto a possibili attacchi, ad esempio tramite lo sfruttamento di vulnerabilità applicative del dispositivo utilizzato o tramite l'uso di codice malevolo, finalizzato alla distribuzione di malware o al furto di token validi per l'accesso applicativo.

3.4.7.4 E-mail (AC:VE-E-)

E-mail identifica gli eventi cyber che utilizzano come vettore d'attacco una casella di posta elettronica (PEC, PEL o PEO).

3.4.7.5 Exploiting vulnerabilities (AC:VE-EV)

Exploiting vulnerabilities identifica gli eventi cyber in cui un attaccante tenta o riesce a sfruttare, sia da internet sia da rete interna, vulnerabilità di un bene informatico al fine di accedervi e ottenerne il controllo illecitamente. Questo valore include sia lo sfruttamento di vulnerabilità note, documentate sul database delle CVE (Common Vulnerabilities and Exposures), sia lo sfruttamento di quelle non note, altresì dette vulnerabilità "0-day".

3.4.7.6 External remote services (AC:VE-EX)

External remote services identifica gli eventi cyber in cui un attore malevolo sfrutta i servizi remoti esposti per accedere e/o persistere all'interno di un bene informatico. Si annoverano in tale categoria tutti quei servizi e meccanismi di accesso che consentono agli utenti di connettersi remotamente alle risorse della rete aziendale. L'abuso di tali servizi può avvenire tramite errate configurazioni, vulnerabilità o l'uso di credenziali valide, per le quali è possibile fare riferimento agli ulteriori e specifici elementi della tassonomia.

3.4.7.7 Hardware additions (AC:VE-HA)

Hardware additions identifica gli eventi cyber in cui un attore malevolo utilizza, in modo non autorizzato, dispositivi hardware per eseguire azioni malevole o illecite, ad esempio per accedere ad un bene informatico o intercettare dati sensibili. Un esempio possono essere gli strumenti utilizzati per catturare informazioni, distribuzione malware tramite storage rimovibile o monitorare senza consenso le attività svolte dalla vittima.

3.4.7.8 Social media (AC:VE-SO)

Social media identifica gli eventi cyber che utilizzano come vettore d'attacco una piattaforma social per perpetrare attività malevole. Tale valore può riferirsi anche alla pubblicazione di contenuti non autorizzati a seguito di accesso sospetto alla piattaforma social in uso.

3.4.7.9 Supply chain (AC:VE-SU)

Supply chain identifica gli eventi cyber che utilizzano come vettore d'attacco prodotti o servizi forniti da terze parti all'interno della catena di approvvigionamento, che presentano vulnerabilità o che sono stati compromessi prima della distribuzione all'utente finale. Nella fattispecie i criminali informatici possono manomettere la produzione o la distribuzione di un prodotto, hardware o software, installando malware o altri componenti, con lo scopo danneggiare uno o più soggetti, prendendo di mira uno o più elementi della catena di approvvigionamento.

3.4.7.10 Valid accounts (AC:VE-VA)

Valid accounts identifica gli eventi cyber che utilizzano come vettore d'attacco un account valido. L'attaccante può sfruttare a proprio vantaggio e illecitamente le autorizzazioni dell'utenza interessata per effettuare attività malevole come ad esempio ottenere privilegi superiori, attivare persistenza, sottrarre illecitamente informazioni o eseguire codice non autorizzato. Questo tipo di evento può coinvolgere sia utenze privilegiate sia non, per le quali specifiche si rimanda ai relativi valori della tassonomia.

3.4.7.11 Other (AC:VE-OT)

Other identifica gli eventi cyber relativi a Vector non identificabili con gli altri valori definiti nel sottoinsieme.

APPENDICE

TASSONOMIA DEGLI EVENTI CYBER

MACROCATEGORIA	PREDICATO	VALORE	CODICE
BASELINE CHARACTERIZATION (BC)	Impact (IM)	Account compromise	BC:IM-AC
		Application compromise	BC:IM-AP
		Availability	BC:IM-AV
		Data exfiltration	BC:IM-DX
		Data exposure	BC:IM-DE
		Data manipulation	BC:IM-DM
		No impact	BC:IM-NO
		System compromise	BC:IM-SY
		Other	BC:IM-OT
	Root cause (RO)	Human errors	BC:RO-HU
		Malicious actions	BC:RO-MA
		Natural phenomena	BC:RO-NA
		System failure	BC:RO-SY
		Third party failure	BC:RO-TH

MACROCATEGORIA	PREDICATO	VALORE	CODICE
BASELINE CHARACTERIZATION (BC)	Severity (SE)	High	BC:SE-HI
		Low	BC:SE-LO
		Medium	BC:SE-ME
		None	BC:SE-NO
	Victim geography (VG)	Italy	BC:VG-IT
		Africa	BC:VG-AF
		America	BC:VG-AM
		Antarctic	BC:VG-AN
		Asia	BC:VG-AS
		Europe	BC:VG-EU
		Global	BC:VG-GL
		Oceania	BC:VG-OC
THREAT TYPE (TT)	Active scanning (AC)	Credential scanning	TT:AC-CR
		Network scanning	TT:AC-NE
		Vulnerability scanning	TT:AC-VU
		Other	TT:AC-OT
	Availability (AV)	Data encryption	TT:AV-DA
		DDoS	TT:AV-DD

MACROCATEGORIA	PREDICATO	VALORE	CODICE
THREAT TYPE (TT)	**Availability (AV)**	DoS	TT:AV-DO
		Misconfiguration	TT:AV-MI
		Outage	TT:AV-OU
		Other	TT:AV-OT
	Fraud (FR)	Brand abuse	TT:FR-BR
		Extortion	TT:FR-EX
		Masquerade	TT:FR-MA
		Resource misuse	TT:FR-RE
		Spam	TT:FR-SP
		Other	TT:FR-OT
	Brand abuse (BA)	Account impersonation	TT:BA-AI
		Cybersquatting	TT:BA-CS
		Name-logo-impersonation	TT:BA-NI
		Typosquatting	TT:BA-TS
		Other	TT:BA-OT

MACROCATEGORIA	PREDICATO	VALORE	CODICE
THREAT TYPE (TT)	Data exposure (DE)	Authentication data	TT:DE-AU
		Business data	TT:DE-BU
		Financial data	TT:DE-FI
		Personal data	TT:DE-PD
		Other	TT:DE-OT
	Information gathering (IG)	Active scanning	TT:IG-AC
		Sniffing	TT:IG-SN
		Social engineering	TT:IG-SO
		Other	TT:IG-OT
	Malicious code (MA)	Backdoor	TT:MA-BA
		Banker	TT:MA-BK
		Bot	TT:MA-BO
		Coin miner	TT:MA-CO
		Exploit kit	TT:MA-EX
		Hacking tool	TT:MA-HA
		Information stealer	TT:MA-IN

MACROCATEGORIA	PREDICATO	VALORE	CODICE
THREAT TYPE (TT)	Malicious code (MA)	Loader	TT:MA-LO
		Potentially Unwanted Program	TT:MA-PO
		Ransomware	TT:MA-RA
		Remote Access Tool	TT:MA-RE
		Rootkit	TT:MA-RO
		Trojan	TT:MA-TR
		Virus	TT:MA-VI
		Webshell	TT:MA-WE
		Wiper	TT:MA-WI
		Worm	TT:MA-WO
		Unknown	TT:MA-UN
	Social engineering (SO)	Baiting	TT:SO-BA
		Phishing	TT:SO-PH
		Smishing	TT:SO-SM
		Spear-phishing	TT:SO-SP
		Vishing	TT:SO-VI

MACROCATEGORIA	PREDICATO	VALORE	CODICE
THREAT TYPE (TT)	Social engineering (SO)	Watering-hole	TT:SO-WA
		Other	TT:SO-OT
	Vulnerability (VU)	0-day vulnerability	TT:VU-0-
		N-day vulnerability	TT:VU-N-
		Proof-of-concept	TT:VU-PC
		Security misconfiguration	TT:VU-SE
		Unwanted exposed services	TT:VU-UN
		Weak cryptography	TT:VU-WE
		Other	TT:VU-OT
THREAT ACTOR (TA)	Adversary motivation (AM)	Destruction	TA:AM-DE
		Espionage	TA:AM-ES
		Ideology	TA:AM-ID
		Influence and disinformation	TA:AM-IN
		Profit	TA:AM-PR
		Other	TA:AM-OT

MACROCATEGORIA	PREDICATO	VALORE	CODICE
THREAT ACTOR (TA)	Adversary type (AD)	Criminal	TA:AD-CR
		Hacktivist	TA:AD-HA
		Insider	TA:AD-IN
		Nation state	TA:AD-NA
ADDITIONAL CONTEXT (AC)	Abusive content (AB)	Disturbing content	AC:AB-DI
		Harmful speech	AC:AB-HA
		Other	AC:AB-OT
	Asset source geography (AS)	Italy	AC:AS-IT
		Other	AC:AS-OT
	Involved asset (IN)	Business e-mail	AC:IN-BU
		Hypervisor	AC:IN-HY
		Industrial Control Systems	AC:IN-IN
		IoT device	AC:IN-IO
		Mobile device	AC:IN-MO
		Network device	AC:IN-NE
		Personal e-mail	AC:IN-PE

MACROCATEGORIA	PREDICATO	VALORE	CODICE
ADDITIONAL CONTEXT (AC)	Involved asset (IN)	Privileged account	AC:IN-PR
		Unprivileged account	AC:IN-UN
		Server	AC:IN-SR
		Service or application	AC:IN-SE
		Social media	AC:IN-SO
		Security appliance	AC:IN-SA
		VPN account	AC:IN-VP
		Web application	AC:IN-WA
		Workstation	AC:IN-WO
		Other	AC:IN-OT
	Operating system (OS)	Android	AC:OS-AN
		GNU/Linux	AC:OS-GN
		iOS	AC:OS-IO
		MacOS	AC:OS-MA
		Microsoft Windows	AC:OS-MI
		Other	AC:OS-OT

MACROCATEGORIA	PREDICATO	VALORE	CODICE
ADDITIONAL CONTEXT (AC)	Outlook (OU)	Improving	AC:OU-IM
		Stable	AC:OU-ST
		Worsening	AC:OU-WO
	Physical security (PH)	Sabotage	AC:PH-SA
		Theft and burglary	AC:PH-TH
		Unauthorized access	AC:PH-UN
		Other	AC:PH-OT
	Vector (VE)	Abuse of functionality	AC:VE-AB
		Compromised domain	AC:VE-CO
		Drive-by compromise	AC:VE-DR
		E-mail	AC:VE-E-
		Exploiting vulnerabilities	AC:VE-EV
		External remote services	AC:VE-EX
		Hardware additions	AC:VE-HA
		Social media	AC:VE-SO
		Supply chain	AC:VE-SU
		Valid accounts	AC:VE-VA
		Other	AC:VE-OT

Tabella 1: Tassonomia degli eventi cyber