**CYBERCRIME ONTOLOGY**

**(Ontology Requirement Specification Document)**

**Project Code**

SER1923-CP01-0305

**Project Advisor**

Mr. Fahad Maqbool

**Project Manager**

Dr. Muhammad Ilyas

**Project Team**

BSEF19M005 Syeda Moaddat Naqvi (Team Leader)

BSEF19M003 Anam Razaq (Team Member)

**Submission Date**

11 Oct 2022

**ONTOLOGY REQUIREMENT SPECIFICATION DOCUMENT**

|  |  |
| --- | --- |
| **CyberCrime Ontology ORSD** | |
| **1)** | **Purpose** |
|  | The purpose of building ontology is to provide a knowledge model of attack types of CyberCrime. |
| **2)** | **Scope** |
|  | The ontology has to focus just on CyberCrime attack types, not its whole domain. |
| **3)** | **Implementation Language** |
|  | The ontology has to be implemented in OWL Language. |
| **4)** | **Intended End-Users** |
|  | User 01. Data Operator that deals with the data.  User 02. Reasoners who will verify syntactic structure and consistency of ontology.  User 03. Novice users who are new in this field and have some certain knowledge about CyberCrime.  User 04. Students studying about CyberCrime field. |
| **5)** | **Intended Uses** |
|  | Use 01. Represents the information monitored by authentic sources.  Use 02. Provides latest information about CyberCrime attack types. |
| **6)** | **Ontology Requirements** |
|  | 1. **Non-Functional Requirements** |
|  | NFR1. The ontology must support English Language  NFR2. The ontology must provide latest information about CyberCrime attack types. |
|  | 1. **Functional Requirements** |
|  | * ***CQG1: CyberCrime*** * CQ1.1: What is CyberCrime? * CQ1.2: When was CyberCrime introduced? * CQ1.3: Who is the father of CyberCrime? * CQ1.4: Who was the first cyber-criminal? * CQ1.5: What was the first CyberCrime? * CQ1.6: Who are the main victims of CyberCrime? * CQ1.7: What are the biggest CyberCrime? * CQ1.8: What are the causes of CyberCrime? * CQ1.9: What are the effects of CyberCrime? * CQ1.10: What is the prevention of CyberCrime? * CQ1.11: Which devices are mostly uses for committing CyberCrimes? * ***CQG2: CyberCrime attacks*** * CQ2.1: What are the most common types of CyberCrime attacks? * CQ2.2: What are the three methods through which CyberCrime attack occurs? * ***CQG3: External attacks*** * CQ3.1: What are the most common external attacks? * CQ3.2: What are the preventive methods for external attacks? * ***CQG4: DDOS attacks*** * CQ4.1: What can a DDOS attack do? * CQ4.2: What is the largest DDoS attack? * CQ4.3: What is the best defense against a DDoS attack? * CQ4.4: What is the most effective DDoS method? * CQ4.5: What are the types of DDoS attacks? * CQ4.6: Who are the targets of DDoS attacks? * CQ4.7: Why do DDoS attacks happen? * CQ4.8: How can DDOS attacks detected? * CQ4.9: How is DDoS prevented? * ***CQG5: DOS attacks*** * CQ5.1: What can a DOS do? * CQ5.2: Why do hackers use DoS attacks? * CQ5.3: How are DoS attacks prevented? * CQ5.4: What are the types of DoS attacks? * CQ5.5: How can DoS attacks are detected? * CQ5.6: How is DoS prevented? * ***CQG6: Session hijacking attacks*** * CQ6.1: What is the best defense against session hijacking? * CQ6.2: What are five methods of session hijacking? * CQ6.3: How can session hijacking be prevented? * CQ6.4: On which OSI layer session hijacking happens? * CQ6.5: What are the two main types of session hijacking? * CQ6.6: What was the largest session hijacking attack? * CQ6.7: How we can stop session hijacking? * CQ6.8: How can session hijacking attacks are detected? * ***CQG7: Password attacks*** * CQ7.1: What are the two main types of password attacks? * CQ7.2: What are the preventive methods for password attacks? * ***CQG8: Brute force password attacks*** * CQ8.1: What is the main target of brute force attacks? * CQ8.2: What password requirement will have the highest impact in preventing brute force attacks? * CQ8.3: What cannot be cracked by brute force? * CQ8.4: How many passwords can be brute forced per second? * CQ8.5: How can brute force password attacks be detected? * CQ8.6: How can a brute force password attack be prevented? * ***CQG9: Dictionary password attacks*** * CQ9.1: What are the ways hackers perform dictionary attacks? * CQ9.2: What is the minimum password length to deter dictionary attacks? * CQ9.3: How can dictionary password attacks be detected? * CQ9.4: How can a dictionary password attack be prevented? * ***CQG10: Social engineering attacks*** * CQ10.1: What are the most common social engineering attacks? * CQ10.2: What are the preventive methods for social engineering attacks? * ***CQG11: Phishing attacks*** * CQ11.1: What are the key signs of a phishing attack? * CQ11.2: What are the ways to prevent phishing? * CQ11.3: What is the most common used method for phishing? * CQ11.4: What are some things to avoid if you get a phishing email? * CQ11.5: What should you do if you are a victim of phishing? * CQ11.6: How can phishing attacks be detected? * CQ11.7: Where does phishing mostly occur? * ***CQG12: Pretexting attacks*** * CQ12.1: Are there technical solutions to the problem of pretexting? * CQ12.2: What are the ways to prevent pretexting? * CQ12.3: How is pretexting used in an attack? * CQ12.4: What are signs of pretext calling? * CQ12.5: How many principles make up the pretexting concept? * CQ12.6: What is the best defense against pretexting? * CQ12.7: What kind of information does pretexting usually target? * CQ12.8: How can pre-texting attacks be detected? * ***CQG13: Internal attacks*** * CQ13.1: What are the most common internal attacks? * CQ13.2: What are the preventive methods for internal attacks? * ***CQG14: Unauthorized Access attacks*** * CQ14.1: How can you protect against unauthorized access? * CQ14.2: What are the risks in unauthorized access? * CQ14.3: What is the most likely form of unauthorized user entry? * CQ14.4: What are the three common methods used to protect information from unauthorized access? * CQ14.5: What blocks the entry of unauthorized network access? * CQ14.6: What protects a network from unauthorized people? * ***CQG15: Intellectual property rights attacks*** * CQ15.1: What are the challenges of intellectual property rights? * CQ15.2: What are the ways of protecting intellectual property? * CQ15.3: What is the strongest form of protection for intellectual property? * CQ15.4: How can intellectual property be detected? * CQ15.5: What type of risk is intellectual property? * CQ15.6: Which intellectual property has the longest protection? * CQ15.7: What are the most common forms of intellectual property? * ***CQG16: Sabotage or vandalism attacks*** * CQ16.1: How sabotage can be detected? * CQ16.2: How sabotage can be prevented? * CQ16.3: What is the best defense against sabotage? * ***CQG17: Information extortion attacks*** * CQ17.1: What are the types of extortion? * CQ17.2: How do you control extortion? * CQ17.3: How do you defend your extortion? * CQ17.4: What are the two ways to commit extortion? * ***CQG18: Human error or failure*** * CQ18.1: What cyber threat concerns you the most human error? * CQ18.2: What are different acts of human error or failure? * CQ18.3: Which security threat is considered a human error? * CQ18.4: How can we prevent human error? * CQ18.5: What are the causes of human error? * CQ18.6: What are the three levels of human error? * CQ18.7: What is the four-stage human error detection strategy? * ***CQG19: Espionage or trespass attacks*** * CQ19.1: What are the types of espionage? * CQ19.2: How is espionage carried out? * CQ19.3: What is the threat of espionage? * CQ19.4: How can espionage attacks are detected? * CQ19.5: What are strategies for the prevention of espionage? |