ANALISI DELLE MINACCE

ANALISI DEI TWEET

ANALISI DEGLI EXPLOIT

ANTIMALWARE

CYRANO SELF EVALUATION TOOL

ECSO MARKET RADAR

FAKE FOLLOWERS

FAKE REVIEWS

MAPPA ATTACCHI 3D

MARKET RADAR - TOSCANA

ONTOLOGIA

REPORT VULNERABILITÀ

RILEVAMENTO DI DGA

RILEVAMENTO E-MAIL DI SPAM

RILEVAMENTO RANSOMWARE

SCANSIONE VULNERABILITÀ

STRUMENTI PER IL SELF ASSESSMENT

SPARTA ROADMAP

STRUMENTI PER IL GDPR

THESAURUS

VERIFICA DI CONFIGURAZIONI DI SISTEMA

Servizi

Analisi delle minacce

Versione: Beta (non funziona molto bene)

Questo tool online permette agli utenti di scoprire le vulnerabilità note associandovi i possibili attacchi per il prodotto specificato. Inoltre il tool fornisce suggerimenti riguardo le contromisure da adottare per mitigare il rischio di attacco. Il report è visualizzabile attraverso una rappresentazione grafica interattiva.

Input: lista applicazioni da analizzare (non chiaro la struttura dell'input)
Output: 3 istogrammi (attacks, mitigations and cvss) con relative informazioni

Sono richiesti i dati per poter completare e visualizzare i grafici. (API)
Una volta recuperati i dati tramite il servizio, la visualizzazione degli istogrammi non dovrebbe essere complessa.

Analisi dei tweet

Il servizio utilizza una raccolta di tweet provenienti da utenti appartenenti a Twitter. In particolare i tweet raccolti utilizzano parole chiave relative al dominio della Cyber-Security, ad esempio, cyber minaccia, cyber terrorismo, hacker e tanti altri.

Input: nessun input
Output: 2 istogrammi con relative informazioni

Non sono richiesti i dati dell'osservatorio, si utilizzano le API di twitter.
Una volta recuperati i tweet contenenti le parole chiave, dovrebbe essere semplice filtrare i dati per creare gli istogrammi. La risposta tornata è un JSON contenente tutte le info.

Problema: le API di twitter richiedono autenticazione e limitano il numero di richieste. Inoltre, la chiamata alle API di twitter ritorna solo i tweet attuali e non passati. Dovrebbe essererci un modo per filtrare le date. In caso contrario, si richiedono i dati dell'osservatorio.

Analisi degli exploit

Stato: attualmente non disponibile

Il servizio raccoglie informazioni relative ad exploit pubblici aggiornati giornalmente attraverso il repository ufficiale "Exploit Database", che rappresenta una delle collezioni più complete di exploit e shellcode.

Il servizio offre all'utente la possibilità di visualizzare data, descrizione e piattaforma su cui l'exploit è stato condotto mediante la ricerca per data o per parola chiave.

https://www.exploit-db.com/google-hacking-database

E' disponibile utilizzando il servizio fornito su The official Exploit Database repository (python file)

Antimalware

Stato: Servizio disponibile solo per utenti loggati e facenti parte del Consiglio Nazionale delle Ricerche.

Il servizio permette di rilevare comportamenti malevoli in file (ad esempio, eseguibili o documenti) attraverso la scansione di 57 differenti antimalware. Al termine dell'analisi viene fornito un indice di rischio che indica la percentuale con la quale il file è considerato malevolo.

Fake Followers

Servizio di Fake Detection dei follower di un utente Twitter. Il servizio permette di rilevare la percentuale di "Fake Follower" di un particolare utente target Twitter.

I follower sono classificati come "Fake" sulla base di caratteristiche quali il numero di tweet prodotti, frequenza con cui l'account segue nuovi utenti, informazioni di profilo, ecc. Se l'utente target ha un elevato numero di following, il servizio effettua l'analisi su un campione di essi.

Input: username di twitter + autorizzazione per poter utilizzare l'app

Output: percentuale e numero di fake followers

Stato: al momento della prova, non mi lasciava autorizzare l'app quindi non l'ho potuto sperimentare

Si richiede il servizio esterno per poter calcolare il numero di fake (API)

Fake Reviews

Versione: Beta

Il servizio utilizza una raccolta di recensioni online provenienti da utenti appartenenti a TripAdvisor, che abbiano recensito attività di ristorazione nelle province della Toscana. Il servizio stima l'affidabilità di una recensione sulla base di caratteristiche della recensione stessa e sulla base di caratteristiche del recensore.

Il servizio è in versione beta, la campionatura delle attività di ristorazione non è completa, e i risultati, una volta raggiunta la totalità delle recensioni disponibili, sono soggetti a cambiamento.

Input: nessun input richiesto

Output: mappa (svg interactive) suddivisa nelle varie province della regione con relativa percentuale di fake reviews.

Per la generazione della mappa si prosegue in modo autonomo, per i dati relativi alla fake reviews è richiesto il servizio esterno (API)

Mappa attacchi 3D

Il servizio mostra una rappresentazione 3D del traffico di rete relativo ad attacchi ad una honeypot a Pisa. Inoltre, il servizio può essere utilizzato per mostrare le sorgenti e destinazioni di una campagna di email di spam.

Input: nessun input
Output: una mappa 3D (molto complessa, terra fattibile ma tratte in 3D complesse) con relativo traffico di rete. E’ possibile filtrare tale traffico con degli appositi switch

Si richiedono i dati dal servizio da mappare sulla terra (API)

Ontologia

Un’ontologia rappresenta una risorsa importante per organizzare la conoscenza di un dominio in maniera più dettagliata attraverso una chiara esplicitazione di tutte le tipologie di relazioni semantiche che vengono a crearsi tra i concetti. Partendo dalla selezione terminologica a monte pensata per la creazione del thesaurus, la seguente sistematizzazione ontologica rende più specifici i rapporti di associazione presenti tra i termini del thesaurus.

Nell’ontologia, quindi, i concetti di un dominio definiti attraverso le classi vengono relazionate in modo definito e univoco dalle relazioni in modo da ottimizzare il processo di disambiguazione semantica della rappresentazione della conoscenza. Ogni classe può avere delle sottocategorie che, come da regola per la creazione delle ontologie, ereditano le sue relazioni con le altre classi di un dominio che si desidera descrivere e rappresentare.

L’ontologia qui presente è stata realizzata sul modello del thesaurus italiano sulla Cybersecurity creato per l’OCS e tutte le relazioni tra le classi rappresentano un mapping più preciso dei rapporti di associazione e di gerarchia all’interno del suddetto vocabolario controllato.

La visualizzazione dell’ontologia è stata realizzata utilizzando il software WebVOWL.

Output: si può riutilizzare lo stesso link per riportare la rappresentazione in quanto non è specifica per la regione Toscana.

Report Vulnerabilità

Il servizio offre la possibilità di cercare informazioni, note pubblicamente, relative a vulnerabilità di sicurezza software e hardware. Tale servizio non si limita a fornire una descrizione generale delle vulnerabilità cercate, ma offre una visione globale di esse riportando le piattaforme software/hardware coinvolte, gli "attack pattern" ed i possibili "exploit" esistenti usati per sfruttare la vulnerabilità

Input: ricerca CVE per id - data - parola chiave
Output: lista con i risultati della ricerca usando il servizio offerto cve-search.

Non è richiesto il servizio dell’osservatorio

Rilevamento di DGA

Il servizio analizza un log di richieste DNS (formato CEF) e identifica se all'interno sono stati risolti dei nomi a dominio che fanno riferimento ad un Domain Generating Algorithm (DGA). Questi, sono utilizzati da malware per registrare nuovi domini con lo scopo di evitare che il malware dipenda da un dominio fisso o da un indirizzo IP cosicché possa venire rapidamente bloccato.

Input: un file da analizzare
Output: il risultato dell'analisi usando il servizio offerto DGA Domains detection (python file)

Rilevamento E-mail di Spam

Il servizio analizza gruppi di email file (formato .eml e in lingua inglese) per identificare le email indesiderate (SPAM). Il servizio inoltre separa le email di SPAM in classi che identificano l'obiettivo della mail, dividendole in:

- Advertisement: Pubblicità indesiderata dove l'unico intento è quello di pubblicizzare un prodotto, senza l'autorizzazione del ricevente a ricevere comunicazioni pubblicitarie.
- Portal: Email malevole che indirizzano il lettore a cliccare su un link che ridirige dopo diversi step intermedi a pagine di pubblicità di diversi tipi di prodotti divisi per categorie (portal).
- Malware: L'email trasporta un allegato malevolo con l'intento di infettare il dispositivo del ricevente.
- Phishing: L'email tenta di convincere l'utente a rivelare credenziali di servizi ai quali ha accesso.
- Confidential Trick: Email di truffa che tentano di spingere il ricevente a pagare una somma di denaro.

Inoltre il servizio separa le email per similarità strutturale, identificando le email che appartengono alla stessa campagna di SPAM, ossia gruppi di email inviate dallo stesso Spammer con un preciso obiettivo.

Input: un file da analizzare

Non essendo presente alcun riferimento a progetti pubblici su GitHub, **si ha la necessità di richiedere il servizio all'osservatorio**.

Rilevamento Ransomware

Il servizio si prefigge di individuare comportamenti tipici dei ransomware quali, ad esempio, la cifratura di una cartella. A differenza degli anti malware basati su signature, il seguente servizio si prefigge di individuare minacce delle quali la signature non è stata ancora generata. Il servizio effettua un'analisi statica utilizzando informazioni sulla frequenza dei pattern di opcode presenti all' interno dell'applicazione in analisi.

Input: un file da analizzare

Non essendo presente alcun riferimento a progetti pubblici su GitHub, **si ha la necessità di richiedere il servizio all'osservatorio**.

Rilevamento Vulnerabilità

Stato: Servizio disponibile solo per utenti loggati e facenti parte del Consiglio Nazionale delle Ricerche.

Il servizio offre una piattaforma che consente agli utenti registrati di verificare eventuali problemi di performance e sicurezza presenti sui loro sistemi/servizi. In particolare, la piattaforma offre le seguenti principali funzionalità:

- Controlli real time;
- Controlli periodici;
- Generazione di report ad hoc;
- Controlli sia IPv4 che IPv6.

Thesaurus

Il servizio mira ad offrire una rappresentazione della conoscenza del dominio della Cybersecurity attraverso la creazione di un vocabolario controllato, un thesaurus, contenente i termini appartenenti a questo campo di studio e una serie di relazioni semantiche che intercorrono tra questi ultimi. Le relazioni terminologiche sono di tre tipi: di gerarchia (Broader Term, BT, Narrower Term, NT), di associazione (Related Term, RT) e di sinonimia (Use, USE, Used For, UF). Le relazioni esistenti all'interno di questo strumento di organizzazione della conoscenza di dominio hanno come funzione principale quella di sviluppare un sistema di rimandi e rinvii semantici tra i termini presenti nel thesaurus volto a creare un network terminologico per il recupero dell'informazione del dominio di interesse e per i processi di indicizzazione.

N.B. Il servizio offerto è stato creato utilizzando TemaTrees. E' facilmente incorporabile in qualsiasi pagina web utilizzando un iframe.

Verifica configurazioni di sistema

Stato: Servizio disponibile solo per utenti loggati e facenti parte del Consiglio Nazionale delle Ricerche.

Il servizio mira ad offrire una rappresentazione della conoscenza del dominio della Cybersecurity attraverso la creazione di un vocabolario controllato, un thesaurus, contenente i termini appartenenti a questo campo di studio e una serie di relazioni semantiche che intercorrono tra questi ultimi. Le relazioni terminologiche sono di tre tipi: di gerarchia (Broader Term, BT, Narrower Term, NT), di associazione (Related Term, RT) e di sinonimia (Use, USE, Used For, UF).

Le relazioni esistenti all'interno di questo strumento di organizzazione della conoscenza di dominio hanno come funzione principale quella di sviluppare un sistema di rimandi e rinvii semantici tra i termini presenti nel thesaurus volto a creare un network terminologico per il recupero dell'informazione del dominio di interesse e per i processi di indicizzazione.

Image-based APK malware classification

Versione: beta

Questo servizio converte un file APK in una immagine, ed in seguito prova a classificare l'immagine generata utilizzando un modello di Convolutional Neural Network pre-addestrato per classificare malware rappresentanti come immagini. La conversione è realizzata leggendo i byte del file APK e convertendoli, uno ad uno, in pixel di una immagine in bianco e nero. Il servizio può classificare l'input in una delle seguenti famiglie di malware: ['Airpush' 'Dowgin' 'FakeInst' 'Fusob' 'Jisut' 'Mecor'].

Input: un file apk
Output: classificazione del malware

Non essendo presente alcun riferimento a progetti pubblici su GitHub, **si ha la necessità di richiedere il servizio all'osservatorio**.

Questionari

Molti dei servizi offerti sono dei questionari, che richiedono informazioni per il completamento di statistiche. I questionari in sé sono facilmente implementabili in pagine web, tuttavia essi **richiedono un servizio esterno per elaborare i dati** inviati.

Cyrano self evaluation tool

Il servizio offre uno strumento semplice e rapido per l'autovalutazione per il calcolo del rischio cibernetico. Il servizio richiede due tipi di input: quelli relativi alle misure di sicurezza e quelli sulle risorse dell'azienda. A questionario completo, il servizio stima le perdite annuali previste per ogni minaccia e inoltre fornisce un valore sul rischio totale.

Input: 3 tipi di questionario (veloce, standard, completo)

Output: Rischio perdite dovuto a minacce

Ecso Market Radar

Il servizio offre un questionario per verificare la conformità dei prodotti e servizi attivati da un'organizzazione in merito alla cybersecurity. I dati raccolti per l'ECSO Cybersecurity Market Radar sono trattati con la massima riservatezza ed esclusivamente dall'organizzazione europea per la sicurezza informatica (ECSO). Le risposte al questionario riguardanti ricavi e dipendenti dell'azienda vengono raccolte in forma anonima e non vengono ricondotte a una singola azienda. I risultati servono per definire la situazione globale del settore della cybersecurity, e vengono utilizzati esclusivamente come dati aggregati, raggruppati in base alle dimensioni dell'azienda e all'origine geografica.

Input: 1 tipo di questionario

Strumenti per il GDPR

Il servizio offre un sondaggio per la verifica della conformità di un’organizzazione al GDPR (General Data Protection Regulation) che ne disciplina il trattamento dei dati personali. Il GDPR si applica a tutte le attività di trattamento dei dati condotte da organizzazioni operanti all’interno della UE ma anche a quelle organizzazioni che risiedono al di fuori della UE e che forniscono prodotti e servizi a individui nella UE.

Input: 2 tipi di questionario (breve, completo)

Strumenti per il Self Assessment

Il servizio offre uno strumento semplice e rapido per l'autovalutazione per il calcolo del rischio cibernetico. Il servizio richiede due tipi di input: quelli relativi alle misure di sicurezza e quelli sulle risorse dell'azienda. A questionario completo, il servizio stima le perdite annuali previste per ogni minaccia e inoltre fornisce un valore sul rischio totale.

Input: 3 tipi di questionario (veloce, standard, completo)