Slika, ki vsebuje besede steklenica, oblikovanje, cerkev

Opis je samodejno ustvarjen

Projekt

**ThreatInsight**

**Specifikacija zahtev za programsko opremo**

Naredil:

**Matevž Nerat**

April 25, 2024

**Vsebina**

[**1.** **Uvod** 3](#_Toc164968023)

[**1.1.** **Namen dokumenta** 3](#_Toc164968024)

[**1.2.** **Obseg storitve** 3](#_Toc164968025)

[**1.3.** **Definicije, akronimi in kratice** 4](#_Toc164968026)

[**1.4.** **Pregled vsebine** 4](#_Toc164968027)

[**2.** **Splošni opis zahtev** 5](#_Toc164968028)

[**2.1.** **Perspektiva produkta** 5](#_Toc164968029)

[**2.2.** **Funkcije produkta** 5](#_Toc164968030)

[**2.3.** **Značilnosti uporabnikov** 6](#_Toc164968031)

[**2.4.** **Omejitve** 6](#_Toc164968032)

[**2.5.** **Predpostavke in odvisnosti** 6](#_Toc164968033)

[**3.** **Specifične zahteve** 7](#_Toc164968034)

[**3.1.** **Zahteve za zunanje vmesnike** 7](#_Toc164968035)

[**3.1.1.** **Uporabniški vmesniki** 7](#_Toc164968036)

[**3.1.2.** **Vmesniki strojne opreme** 7](#_Toc164968037)

[**3.1.3.** **Vmesniki programske opreme** 7](#_Toc164968038)

[**3.1.4.** **Komunikacijski vmesniki** 7](#_Toc164968039)

[**3.2.** **Zahteve delovanja programske opreme** 7](#_Toc164968040)

[**3.3.** **Logične zahteve za podatkovni model** 7](#_Toc164968041)

[**3.4.** **Omejitve pri oblikovanju** 7](#_Toc164968042)

[**3.5.** **Značilnosti IT okolja** 7](#_Toc164968043)

# **Uvod**

## **Namen dokumenta**

Namen specifikacij zahtev za programsko opremo(SZPO) je:

* postavitev osnov za morebiten dogovor o želeni programski opremi – produktu,
* jasen pregled obsega programske opreme,
* pregled/opis uporabnikov programske opreme,
* seznam specifikacij zahtev,
* okviren opis arhitekture

Dokument je namenjen razvojni ekipi in stranki.

## **Obseg storitve**

Stranka želi uvesti produkt, ki integrira različna orodja kibernetske varnosti na skupen enoten vmesnik.

Ime produkta je ThreatInsight.

Proces razvoja produkta bo sledil osnovnim načelom PRINCE2 pri katerem bomo za dostavljanje izdelkov (faza razvoja) sledili načelom agilnega stila.

Produkt zagotavlja:

* Uporabo več kibernetskih orodij
* Shranjevanje rezultatov iskanj orodij
* Procesiranje rezultatov in formiranje rezultata

Produkt ne zagotavlja:

* Pomoč pri izvajanju kibernetskih napadov
* Načinov dostopa do tarč

Namenski cilj produkta je **integracija orodij kibernetskih orodij v skupen uporabniški vmesnik.**

## **Definicije, akronimi in kratice**

Definicije osnovnih pojmov, akronimi in kratice, ki so aktualne za produkt.

Definicije:

|  |  |
| --- | --- |
| **Spletna**  **aplikacija** | Aplikacija (HTML5, CSS3 in Java Script), ki se izvaja na spletnem strežniku in je prilagojena za spletne brskalnike na osebnih ali tabličnih računalnikih |
| **Kibernetska varnost** | Kibernetska varnost je nabor postopkov, najboljših praks in tehnoloških rešitev, s katerimi lahko zaščitite pomembne sisteme in omrežje pred digitalnimi napadi. |
| **Orodja kibernetske varnost** | Orodja/storitve, ki omogočajo lažje pridobivanje podatkov o potencialnih tarčah kibernetskih napadov. |
| **Entiteta »podatki o tarči«** | Poimenovanje skupka podatkov, ki jih uporabnik pridobi z uporabo različnih kibernetskih orodij, ki so na voljo. Ena entiteta ima eno »tarčo«. |
| **Tarča** | Računalniški sistem, omrežje ali organizacija, ki je namenjena ali izpostavljena potencialnim napadom, s ciljem pridobiti, uničiti, spreminjati ali zlorabiti podatke, storitve ali infrastrukturo. |
| **E-mail permutator** | Orodje, ki generira možne različice e-poštnih naslovov glede na določene smernice ali vzorce. |
| **Pročelje** | Uporabniški vmesnik ali zunanji del programske rešitve, ki je viden in dostopen uporabnikom. |
| **Zaledje/Zaledni sistem** | Del programske rešitve, ki deluje na strežniku ali ozadju ter upravlja z logiko, podatki in funkcionalnostmi, ki jih uporabniki ne vidijo neposredno. |

Kratice:

|  |  |
| --- | --- |
| **API** | Application Programming Interface (aplikacijski programski vmesnik) |
| **DNS** | Domain Name Server (sistem domenskih imen***)*** |
| **DNSSec** | DNS Security |
| **TLS** | Transport Layer Security (kriptografski protokol za prenos podatkov) |
| **IP** | Internet Protocol (internetni protokol) |
| **DPU** | Diagram primerov uporabe |
| **PB** | Podatkovna baza |
| **ISP** | Internet service provider (ponudnik internetnih storitev) |

## **Pregled vsebine**

Vsebina dokumenta se omejuje na zahteve dokumenta in diagrame, ki grafično predstavljajo arhitekturo in delovanje spletne aplikacije.

* Poglavje 1: Uvod, predstavitev izhodiščnega stanja
* Poglavje 2: Splošen opis programske opreme
* Poglavje 3: Specifikacija zahtev sistema (specifične zahteve)

Grafične predstavitve so vključene v dokument ali priključene na konec dokumenta, kot priloga.

# **Splošni opis zahtev**

## **Perspektiva produkta**

Spletna aplikacija predstavlja delno novost med konkurenco, saj združuje rezultate orodij kibernetske varnosti v smiselno celovito predstavitev stanja »tarče«.

Z uporabo aplikacije omogočamo uporabnikom izvajanje faz izvidništva in skeniranja omrežja v sklopu etičnega hekanja. Z integracijo močnih in priznanih orodij/storitev, kot so nmap, WhoIs, HaveIBeenPwned itd. se uporabniki prebijejo do kritičnih podatkov o svoji »tarči«.

Za projekte, ki trajajo dlje časa, ponuja aplikacija shranjevanje in poznejše dostopanje do zbranih podatkov za tarčo.

## **Funkcije produkta**

Produkt ponuja naslednje fukncionalnosti:

* Ustvarjanje/pregledovanje/urejanje/brisanje entitete »podatki o tarči«
* Uporaba orodij za pridobivanje podatkov o tarči
* Uporaba nmap
* Uporaba WhoIs
* Uporaba HaveIBeenPwned
* Uporaba storitve IpGeolocation
* Uporaba storitve TLS/DNSSec
* Uporaba storitve e-mail verifier
* Uporaba storitve e-mail permutator
* Selekcija bistvenih podatkov
* Predvidevanje ranljivosti tarče

## **Značilnosti uporabnikov**

Uporabniki naše spletne rešitve so predvsem strokovnjaki s področja kibernetske varnosti, etični hekerji, informacijski varnostni analitiki ter vsi tisti, ki se ukvarjajo z ocenjevanjem varnosti in ranljivosti informacijskih sistemov. Poleg tega lahko aplikacijo uporabljajo tudi podjetja in organizacije, ki želijo redno spremljati varnost svojih omrežij in preverjati morebitne ranljivosti.

Produkt je prilagojen tudi za začetnike, saj uporabniški vmesnik ponuja opise orodij ter načine uporabe. Za večino rezultatov iskan vsebuje povezave na vire, ki ponujajo razlago.

## **Omejitve**

Večina omejitev izhaja iz obstoječih orodij. Pri ustvarjanju produkta se ne lotevamo reševanja teh omejitev temveč se jim prilagajamo.

Omejitve:

* Časovno potratno skeniranje omrežja
* Plačljive storitve/orodja oziroma njihovi API-ji
* Neznanje uporabe rešitve s strani za začetnike

## **Predpostavke in odvisnosti**

Predpostavke za uporabo:

* Internetna povezava
* Sodoben spletni brskalnik

Odvisnosti produkta od zunanjih storitev:

* Odvisnost od ponudnikov API-jev do nekaterih orodij
* Odvisnost od ponudnika gostovanja

Za pravilno delovanje morajo naštete predpostavke in odvisnosti biti na voljo in delujoče. Morebitne motnje ali nedelujoči API-ji onemogočajo celovito delovanje aplikacij ter posledično povzročajo slabšo kakovost produkta.

# **Specifične zahteve**

## **Tehnične zahteve**

### **Uporabniški vmesniki**

Rešitev bo spletna aplikacija, torej bo prilagojena za uporabo v namiznih spletnih brskalnikih, kot v mobilnih brskalnikih.

Uporabniški vmesnik bo implementiran z uporabo programskega ogrodja React, ki deluje v Node.js okolju. Za navigiranje med stranmi bo uporabljen react-router.

React je ogrodje, ki omogoča dinamično spreminjanje spletne aplikacije, zato je za produkt ključnega pomeni pri spreminjanju stanja spletne aplikacije ob pridobivanju podatkov.

Pročelje bo obstajalo v zabojniku, katerega slika bo naložena v gostovanje

ponudniku gostovanja zabojniških okolij. Za doseg tega rezultata bo

uporabljeno orodje Docker.

### **Zaledni sistem**

Zaledni sistem bo prilagojen namenom integracije, kjer bo vsaka storitev oziroma orodje sistematično razporejeno z vsemi podpornimi tehnikami za uspešno pridobitev in združevanje informacij. Nekatere storitve bodo ročno implementirane za katere bo zagotovljeno primerno ogrodje glede na potrebe.

Glede na manjše zahteve po procesnih moči bo zaledni sistem implementiran v ogrodju Express.js v okolju Node.js.

Tako kot pročelje bo tudi zaledje delovalo v zabojniku in gostovano pri ponudniku gostovanj zabojnikov.

### **Podatkovna baza**

Produkt bom prejemal ogromno informacij, ki so lahko ob vsakem klicu drugačne in se spremeni tudi njihova struktura, zato se bo za dolgotrajno hranjenje podatkov uporabila NoSql podatkovna baza.

### **Komunikacijska struktura**

Komunikacija med pročeljem in zaledjem bo omogočena preko REST API-ja, ki ga bo ponujal zaledni sistem.

Komunikacija z podatkovno bazo bo potekala skozi zaledje, tako da bo zaledje pridobilo podatke iz baze in jih posredovalo v pročelje za prikaz.

Zaledje bo prav tako poskrbelo za pridobivanje podatkov od izbranih API-jev orodij. Vsa orodja ponujajo REST API vmesnik, ki omogoča preprost način pridobivanja podatkov.

## **Zahteve delovanja programske opreme**

Funkcionalne zahteve:

* Ustvarjanje entitete »podatki o tarči«,
* Pregledovanje entitete »podatki o tarči«,
* Urejanje entitete »podatki o tarči«,
* Brisanje entitete »podatki o tarči«,
* Uporaba nmap in prikaz/pregled rezultatov(možnost prilagajanja skeniranja(TCP skeni, OS zaznavanje, agresivnost,…)
* Uporaba storitve WhoIs in prikaz/pregled (domena/ip, lastnik, gostovanje,…)
* Uporaba orodja HaveIBeenPwned(vnos maila oz. gesla) in prikaz/pregled rezultatov
* Uporaba storitve IpGeolocation(vnos IP/domene) in prikaz/pregled države, mesta, časovne cone, ISP ponudnika,..
* Uporaba storitve TLS/DNSSec in prikaz/pregled verzije šifriranja, certifikat, aktiviranost DNSSec
* Uporaba storitve E-mail verifier in prikaz/pregled zaznanih e-mail naslovov oz. domen
* Uporaba storitve E-mail permutator in prikaz/pregled generiranih e-mail naslovov
* Selekcija bistvenih podatkov

Nefunkcionalne zahteve:

* Varovanje osebnih podatkov
* Učinkovitost (odziven čas)
* Dostopnost
* Intuitiven in zanimiv uporabniški vmesnik
* Skladnost z zakonom
* Zanesljivost
* Zaščita sistema pred kibernetskimi napadi

# **Priloge**

Seznam prilog z opisom: