Slika, ki vsebuje besede steklenica, oblikovanje, cerkev

Opis je samodejno ustvarjen

Projekt

**ThreatInsight**

**Analiza obstoječih**

**rešitev**

Naredil:

**Aljaž Bračko**

26. april, 2024

Vsebina

[1. Uvod 3](#_Toc165138061)

[2. Pregled trga 3](#_Toc165138062)

[3. Podrobna analiza izbranih rešitev 4](#_Toc165138063)

[3.1. Shodan.io 4](#_Toc165138064)

[3.2. Hackertarget.com 4](#_Toc165138065)

[3.3. DomSignal.com 5](#_Toc165138066)

[4. SWOT analiza 1](#_Toc165138067)

[5. Zaključek 1](#_Toc165138068)

# Uvod

Ta dokument je namenjen analizi obstoječih rešitev na področju kibernetske varnosti, ki omogočajo zbiranje in analizo podatkov o ciljih/tarčah, kot so posamezniki, organizacije ali tehnološke infrastrukture. Cilj analize je identificirati značilnosti, funkcionalnosti in omejitve trenutno dostopnih orodij ter storitev. Pridobljene informacije bodo služile kot osnova za razvoj naše spletne aplikacije, ki bo združevala več orodij za izvidništvo na enem mestu za pregled in učinkovito ocenjevanje stanja izbranih tarč.

# Pregled trga

**Trenutne rešitve**

Na trgu obstaja več rešitev, ki omogočajo zbiranje podatkov o tarčah za različne namene kot so skeniranje omrežij, analiza ranljivosti in zaznavanje vdorov.

Nekatera priljubljena orodja in storitve so:

1. **Shodan.io**: Spletna storitev, ki omogoča iskanje naprav, povezanih z internetom, kot so strežniki, naprave IoT, in celo varnostne kamere. Shodan analizira internet v realnem času in zagotavlja podatke o napravah in storitvah, ki so javno dostopne.
2. **Hackertarget.com**: Ponuja spletna orodja za skeniranje omrežja, ki uporabnikom omogočajo izvajanje različnih skeniranj, kot so nmap skeniranja, traceroute, WHOIS iskanja in DNS skeniranja prek spletnega vmesnika.
3. **DomSignal.com**: Storitev, ki ponuja obsežno analizo domen z informacijami o lastništvu, infrastrukturi in tehnoloških »stackih«, ki se uporabljajo na določenih spletnih mestih.

# Podrobna analiza izbranih rešitev

## Shodan.io

**Opis rešitve:** Shodan.io je spletna storitev, ki omogoča iskanje naprav, povezanih z internetom, kot so strežniki, naprave IoT in varnostne kamere. Storitev analizira internet v realnem času in uporabnikom omogoča vpogled v naprave in storitve, ki so javno dostopne.

**Funkcionalnosti in značilnosti:**

* **Iskanje naprav:** Uporabniki lahko iščejo naprave na podlagi različnih kriterijev, kot so IP naslov, geografska lokacija, vrsta naprave in stanje odprtih vrat.
* **Pregled informacij o napravah:** Shodan omogoča vpogled v podrobnosti o najdenih napravah, vključno z uporabljenim operacijskim sistemom, odprtimi vrati in informacijami o SSL certifikatih.
* **Shranjevanje in poročila:** Storitev omogoča shranjevanje rezultatov iskanja in ustvarjanje poročil za nadaljnjo analizo ali dokumentacijo.

## Hackertarget.com

**Opis rešitve:** Hackertarget.com ponuja orodja za skeniranje omrežja, ki jih lahko uporabniki izvajajo preko spletnega vmesnika. To omogoča izvedbo različnih vrst skeniranj, kot so nmap skeniranja, traceroute, WHOIS iskanja in DNS skeniranja.

**Funkcionalnosti in značilnosti:**

**Vrste skeniranj:** Storitev omogoča izvedbo nmap skeniranja, traceroute, WHOIS iskanja in DNS skeniranja, ki so dostopna preko spletnega vmesnika.

**Pregled rezultatov:** Rezultati skeniranja so predstavljeni v pregledni obliki, kar uporabnikom omogoča lažje razumevanje stanja njihovih omrežij.

**Shranjevanje rezultatov:** Uporabniki lahko shranijo rezultate skeniranj, kar omogoča kasnejšo analizo in primerjavo.

## DomSignal.com

**Opis rešitve:** DomSignal.com je storitev, ki uporabnikom ponuja obsežno analizo domen, vključno z informacijami o lastništvu, infrastrukturi in uporabljenih tehnologijah na spletnih mestih.

**Funkcionalnosti in značilnosti:**

* **Analiza domen:** Storitev analizira domene in zagotavlja informacije o lastništvu, registraciji in gostovanju.
* **Tehnološki stacki:** Uporabniki lahko dobijo vpogled v tehnologije, ki se uporabljajo na določenih spletnih mestih, vključno z informacijami o DNS zapisih, SSL certifikatih in drugih varnostnih nastavitvah.
* **Primerjalna analiza:** Omogoča primerjavo več domen hkrati, kar uporabnikom pomaga pri ocenjevanju in primerjanju različnih spletnih mest.

# SWOT analiza

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rešitev | Moči | Slabosti | Priložnosti | Grožnje |
| Shodan.io | -Realnočasno odkrivanje javno dostopnih naprav in storitev.  -Pregledne informacije o napravah. -Možnost shranjevanja rezultatov iskanja in ustvarjanja poročil. | -Omejena dostopnost funkcij v brezplačni različici.  -Zahteva nekaj tehničnega znanja za učinkovito uporabo. | -Razširitev funkcionalnosti z dodajanjem novih kategorij iskanja.  -Povečanje uporabniške baze | -Pojav konkurenčnih rešitev.  -Potencialna zloraba storitve. |
| Hackertarget.com | - Enostavna uporaba preko spletnega vmesnika.  -Raznolike funkcionalnosti za skeniranje omrežja. | -Omejena dostopnost funkcij v brezplačni različici.  -Omejena količina informacij in podatkov preko spletnega vmesnika. | -Razvoj mobilne aplikacije  -Ponudba dodatnih funkcionalnosti. | -Pojav konkurenčnih rešitev.  -Potencialna zloraba storitve. |
| DomSignal.com | -Ponuja obsežne informacije o domenah.  -Omogoča primerjalno analizo več domen hkrati. | -Omejena dostopnost funkcij v brezplačni različici.  -Nekatere informacije niso vedno popolne. | - Razvoj dodatnih orodij za boljšo analizo.  -Sodelovanje z drugimi ponudniki kibernetske varnosti. | -Pojav konkurenčnih rešitev.  -Potencialna zloraba storitve. |

# Zaključek

Spletna aplikacija, ki jo načrtujemo razviti, združuje več orodij v integrirano platformo.

Glavne prednosti naše rešitve v primerjavi z obstoječimi na trgu:

1. **Enotna platforma za več orodij**: Uporabniki lahko dostopajo do različnih orodij na enem mestu, kar izboljša učinkovitost in zmanjša čas, potreben za zbiranje in analizo podatkov.
2. **Poudarek na interaktivnosti in uporabniški izkušnji**: Informacije o tarčah so vizualno predstavljene in podprte z kratkimi razlagami, kar uporabnikom omogoča lažje razumevanje in hitrejše sprejemanje odločitev.
3. **Prilagodljivost in prilagoditve uporabnika**: Možnost prilagajanja parametrov skeniranja omogoča uporabnikom, da prilagodijo orodja svojim specifičnim potrebam.
4. **Shranjevanje in dostop do zgodovinskih podatkov**: Uporabniki lahko shranijo rezultate svojih iskanj in jih kasneje pregledujejo ali spreminjajo, kar omogoča kasnejše nadaljevanje v preiskovanju in monitoring.