Forenzika nasilnog ekstremizma u digitalnom okruženju

OSINT obuka

Norway

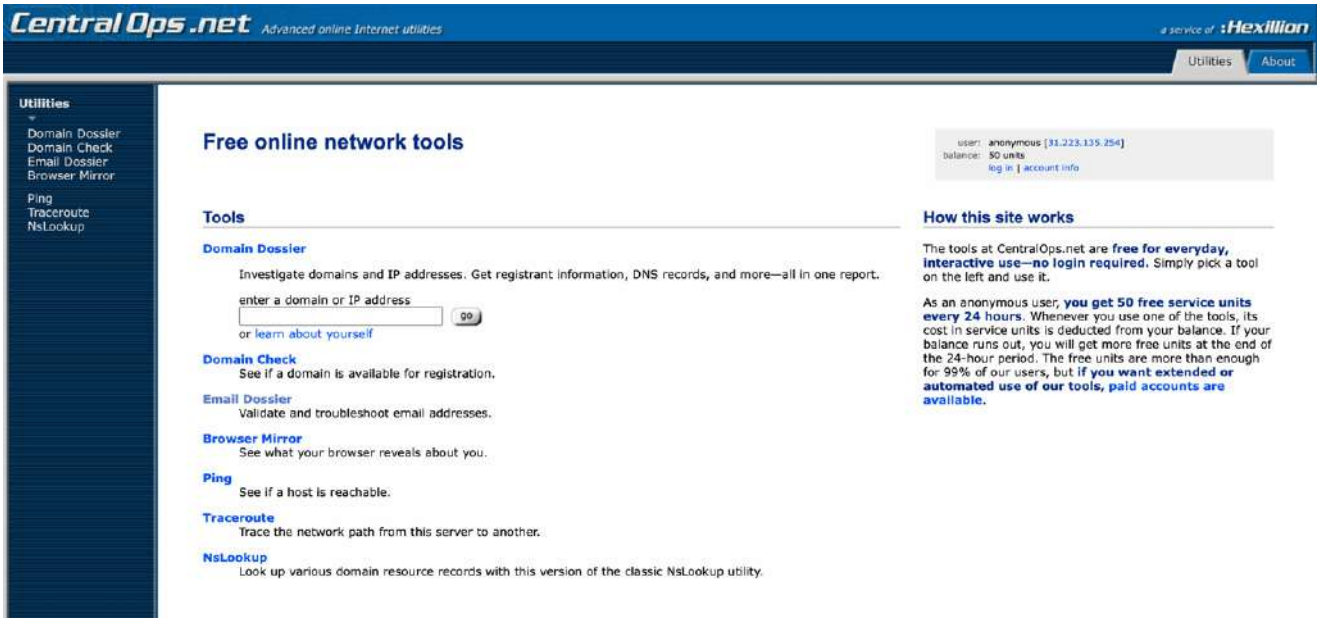
SMART Balkans
Civil Society for Shared Society in the Western Balkans

CPCD
Centar za promociju civilnog društva

IDM
Institute for Democracy and Mediation

CRPM
Center for Research and Policy Making

CentralOps.net

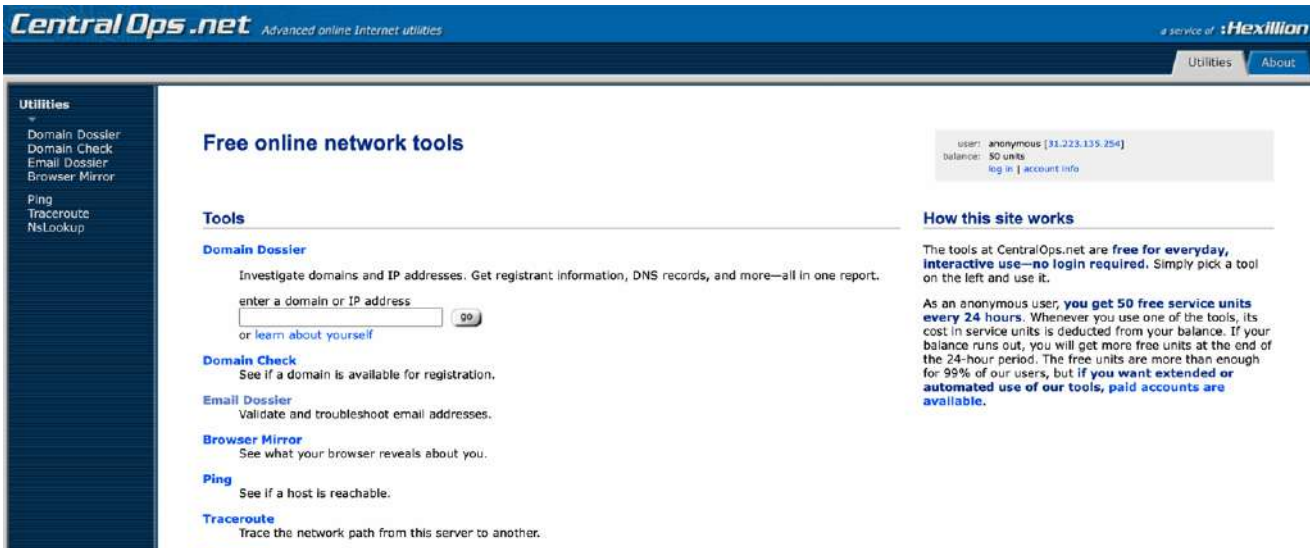


CentralOps.net je alat koji se koristi za razne mrežne pretrage i dijagnostiku. Pruža niz alata kao što su:

- Whoispretraga: Pomaže u dobijanju informacija o registraciji domena.
- Traceroute: Koristi se za praćenje puta kojim mrežni paketi putuju do određenog odredišta.
- Ping: Provjerava mrežnu dostupnost određenog servera ili IP adrese.
- Domain Dossier: Kombinuje više alata za prikupljanje informacija o određenoj domeni, uključujući Whois, DNS, traceroute i ping.
- DNSpretraga: Omogućava provjeru DNS postavki i informacija.

Ovi alati mogu biti korisni za administratore mreže i sigurnosne stručnjake za provjeru mrežnih problema, analizu sigurnosnih prijetnji i optimizaciju mrežnih postavki.

Whois.com



Whois.com je alat koji pruža detaljne informacije o domenima, što može biti korisno za razne svrhe, uključujući sigurnost, istraživanje tržišta i administraciju mreže. Evo detaljnijeg opisa njegovih funkcionalnosti:

Detalji o Registraciji Domene

Whois pretraga vam omogućava da dobijete sljedeće informacije:

1. **Registrant**:

- Ime: Ime osobe ili organizacije koja je registrovala domen.
- Organizacija: Naziv organizacije, ako je primjenjivo.
- Adresa: Fizička adresa registranta.
- Kontakt informacije: Email adresa i telefonski broj.

2. **Registrar**:

- Naziv registrara: Kompanija preko koje je domen registrovan.
- IDregistrara: Jedinstveni identifikator registrara.

3. **Datumi**:

- Datum registracije: Datum kada je domena prvi put registrovana.
- Datum isteka: Datum kada registracija domene ističe, što je korisno za planiranje obnavljanja ili kupovine domena.

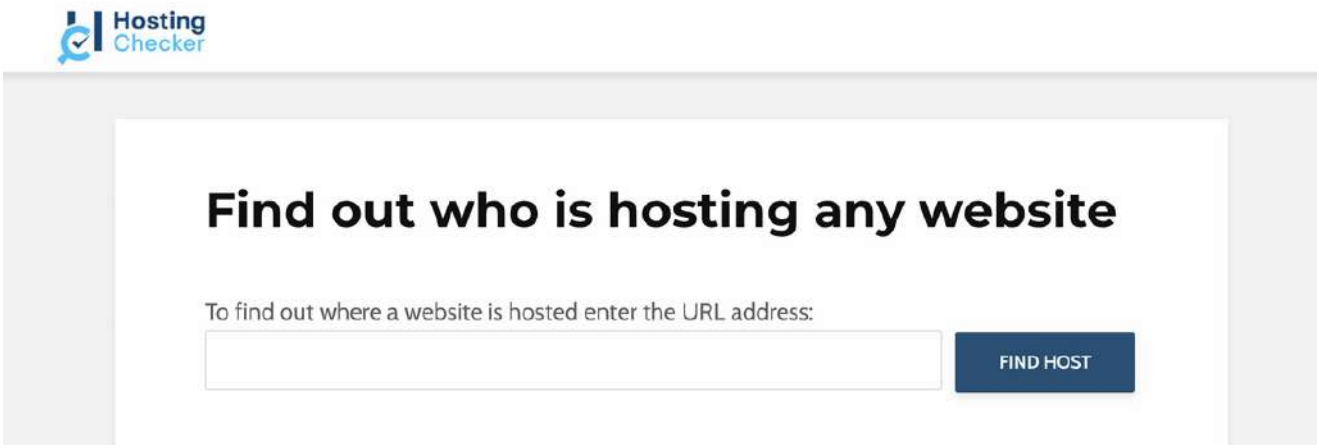
4. Status domene:

- Status: Trenutni status domena, npr. aktivan, zaključan, čekanje na brisanje, itd. Ovo može biti korisno za razumijevanje zašto domen možda nije dostupan ili zašto ne funkcioniše kako se očekuje.

5. Nameserveri:

- Nameserveri: DNS poslužitelji povezani s domenom. Ovo je ključno za razumijevanje gdje su DNS zapisi pohranjeni i kako se saobraćaj usmjerava.

Hosting Checker



Hosting Checker je alat koji se koristi za identifikaciju hosting provajdera za određenu web stranicu ili domenu. Ovo može biti korisno iz nekoliko razloga:

Funkcionalnosti Hosting Checkera

1. **Identifikacija hosting provajdera**:

   - Brzina učitavanja: Informacije o brzini učitavanja stranice koje mogu biti korisne za optimizaciju performansi.
   - Uptime statistike: Podaci o dostupnosti web stranice, što je ključno za pouzdanost.

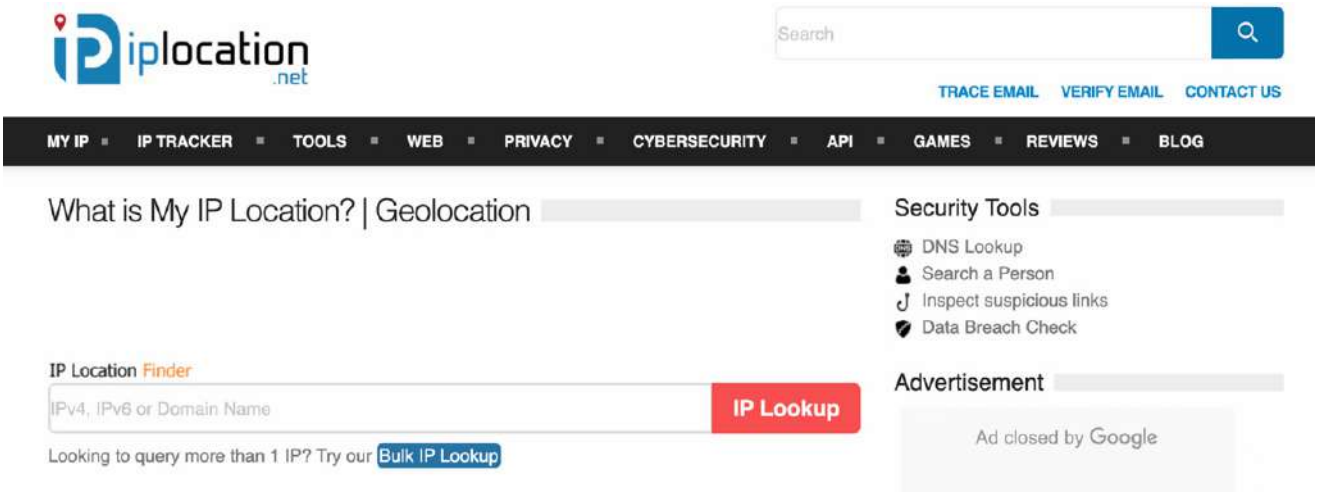
2. **Analiza Performansi**:

   - Provajder usluga: Dobijanje informacija o kompaniji koja pruža hosting usluge za određenu web stranicu ili domenu.
   - Lokacija servera: Informacije o fizičkoj lokaciji servera na kojem je smještena web stranica.

3. **Sigurnosne provjere**:

   - Sigurnosne funkcije: Provjera da li hosting provajder nudi sigurnosne funkcije kao što su SSL certifikati, zaštita od DDoS napada, sigurnosne kopije itd.
   - IPadresa: Dobijanje informacija o IP adresi povezanom sa web stranicom, što može pomoći u otkrivanju potencijalnih sigurnosnih prijetnji.

IPLocation.net



IPLocation.net je alat koji se koristi za određivanje geografske lokacije i drugih informacija povezanih s određenom IP adresom.

Glavne funkcionalnosti:

1. **Geolokacija IP adrese:**

   - Lokacija: Otkrivanje fizičke lokacije IP adrese, uključujući grad, državu i regiju.
   - Koordinate: Prikaz geografskih koordinata (latitude i longitude).

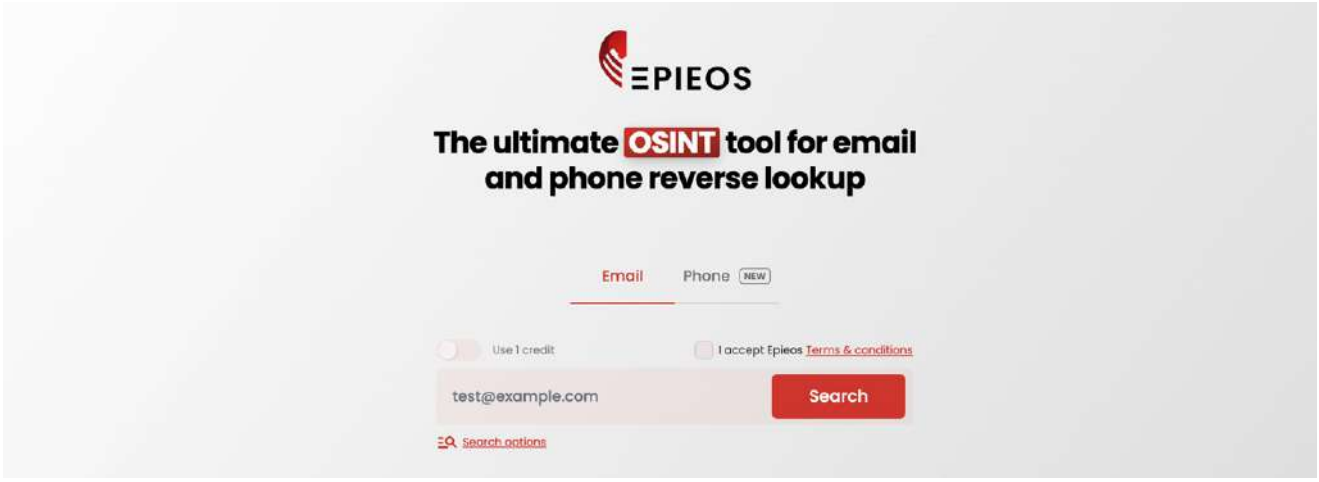
2. **Informacije o provajderu:**

   - ISP (Internet Service Provider): Identifikacija pružatelja internetskih usluga povezanih s IP adresom.
   - AS broj (Autonomous System Number): Informacije o mrežnom entitetu koji kontroliše IP adresu.

3. **Dodatni detalji:**

   - Domain: Povezanost IP adrese s određenim domenima.
   - Proxy i VPN informacije: Identifikacija korištenja proxy servera ili VPN-ova.

Epieos.com



Epieos.com je alat koji se koristi za:

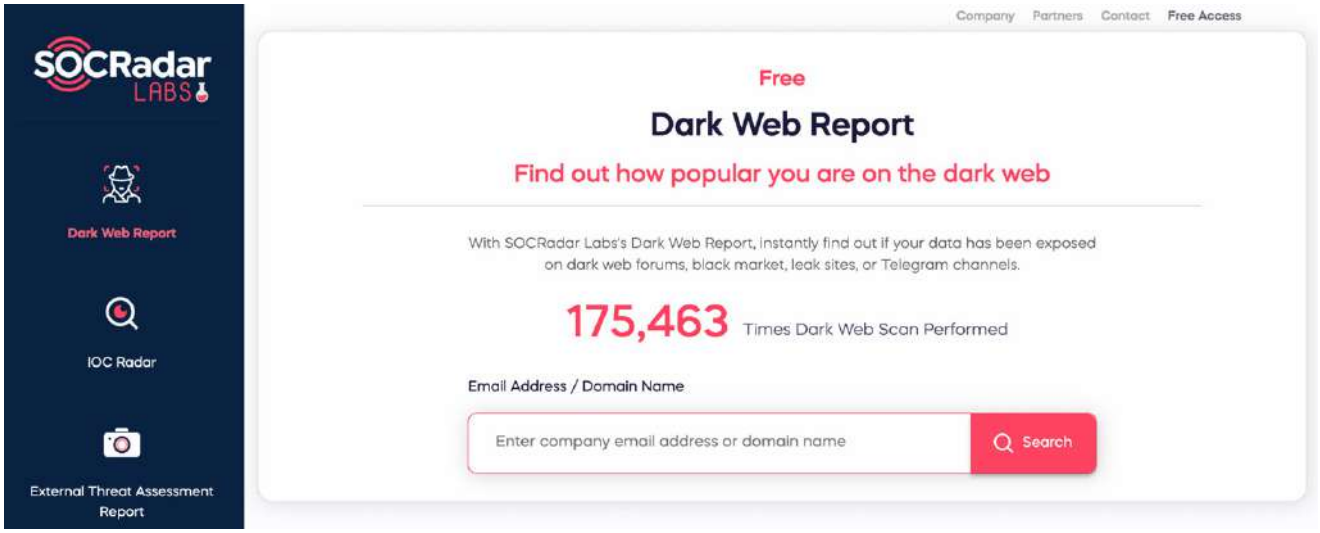
Pretraga email adresa i pretplatničkih bojeva telefona:

- Provjera valjanosti email adrese: Identifikacija da li je email adresa aktivna i valjana.
- Detalji o email domeni: Informacije o domeni povezanoj sa email adresom (email, google maps itd), da li je email adresa povezana sa gmail nalogom, outlook nalogom, duštvenim mrežama (Facebook, Instagram, Snapchat itd).

Pronalaženje Informacija:

- Osobne informacije: Dobijanje informacija o vlasniku email adrese ili broja, kao što su ime, prezime, profilne slike, itd.
- Društvene mreže: Povezanost email adrese sa nalozima na društvenim mrežama.

SOCradar



SOCradar je OSINT alat.

Glavne funkcionalnosti navedenog alata su:

1. Threat Intelligence:

- Praćenje prijetnji: Praćenje najnovijih cyber prijetnji i ranjivosti u realnom vremenu.
- Analiza prijetnji: Dubinska analiza i kontekstualizacija prijetnji kako bi se bolje razumjele potencijalne opasnosti.

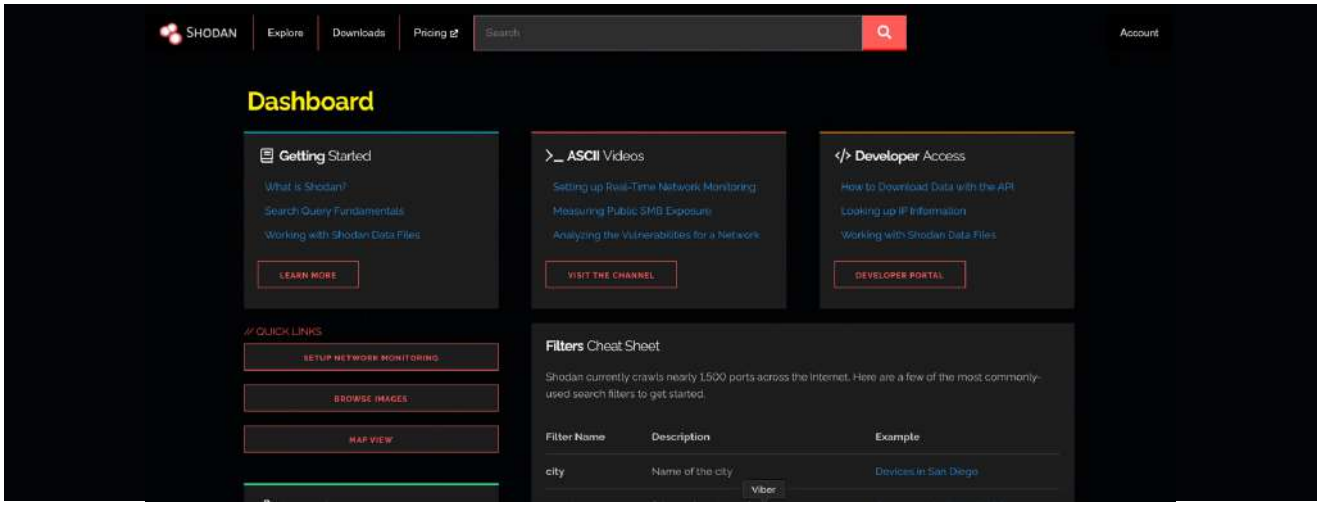
2. Digital risk protection:

- Zaštita digitalnog identiteta: Praćenje i zaštita digitalnih identiteta i osjetljivih informacija od krađe i zloupotrebe.
- Zaštita brenda: Identifikacija i zaštita od napada usmjerenih na ugled i integritet brenda.

3. External attack surface management:

- Praćenje vanjske površine napada: Identifikacija i nadzor vanjskih resursa i imovine koje bi mogle biti mete napada.
- Otkrivanje ranjivosti: Pronalaženje i procjena ranjivosti u vanjskim sistemima i aplikacijama.

Shodan.io



Shodan.io je popularan OSINT (Open Source Intelligence) alat koji omogućava pretragu internetskih uređaja i servisa. Nazivaju ga i "pretraživačem za hakere" jer pruža uvid u uređaje povezane na internet koji su često nedovoljno zaštićeni.

Evo glavnih funkcija i primjena Shodan.io alata:

1. **Pretraga IoT uređaja**: Shodan može otkriti razne IoT uređaje (kao što su kamere, ruteri, termostati) koji su povezani na internet. To je korisno za sigurnosne timove, jer mogu brzo identifikovati nesigurne uređaje u mreži.

2. **Identifikacija otvorenih portova i servisa**: Alat omogućava pretragu po otvorenim portovima i servisima (kao što su FTP, HTTP, SSH), što pomaže u identifikaciji ranjivih mrežnih konfiguracija.

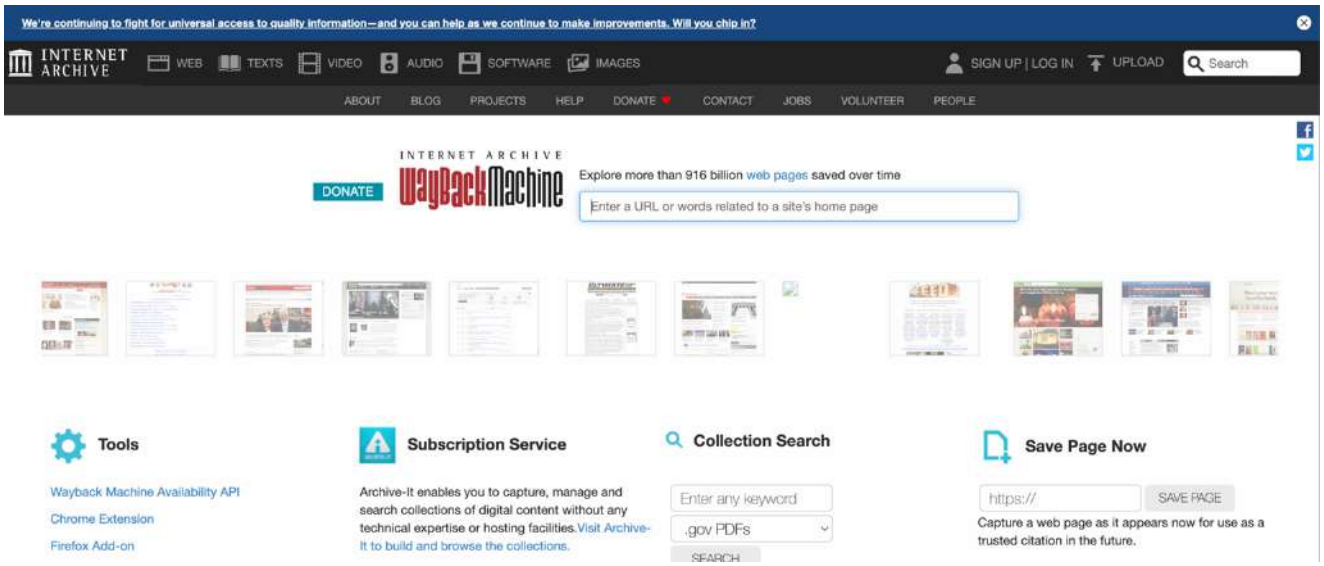
3. **Skener ranjivosti**: Shodan može prepoznati verzije softvera i sistema koje koriste povezani uređaji, što može pomoći u identifikaciji potencijalno ranjivih sistema.

4. **Geolokacija uređaja**: Alat može prikazati geografske lokacije uređaja, što je korisno za procjenu rizika i praćenje izvora sigurnosnih prijetnji.

5. **Podrška u incident response**: Shodan pomaže u otkrivanju kompromitovanih uređaja ili onih koji mogu predstavljati rizik, čime omogućava brže reagovanje na potencijalne incidente.

Zbog mogućnosti identifikacije ranjivih uređaja i servisa, Shodan je veoma važan alat u domenu cyber sigurnosti, kako za defanzivne stručnjake, tako i za napredne istraživače OSINT-a.

Wayback Machine



Wayback Machine je alat koji se koristi za:

Glavne funkcionalnosti:

1. Arhiviranje web stranica:

- Pohrana verzija stranica: Omogućava pregled pohranjenih verzija web stranica kroz vrijeme.
- Periodično arhiviranje: Web stranice se arhiviraju u različitim vremenskim intervalima, omogućavajući pregled promjena kroz vrijeme.

2. Pregled povijesti web stranica:

- Historijski pregledi: Omogućava pregled kako su web stranice izgledale u prošlosti.
- Evolucija sadržaja: Prati promjene sadržaja, dizajna i strukture web stranica.

3. Istraživanje i analiza:

- Istraživanje sadržaja: Korisno za istraživače, novinare i analitičare za pregled historijskog sadržaja.
- SEO analiza: Analiza kako su web stranice evoluirale i kako su promjene uticale na SEO performanse.

Prednosti wayback machine alata

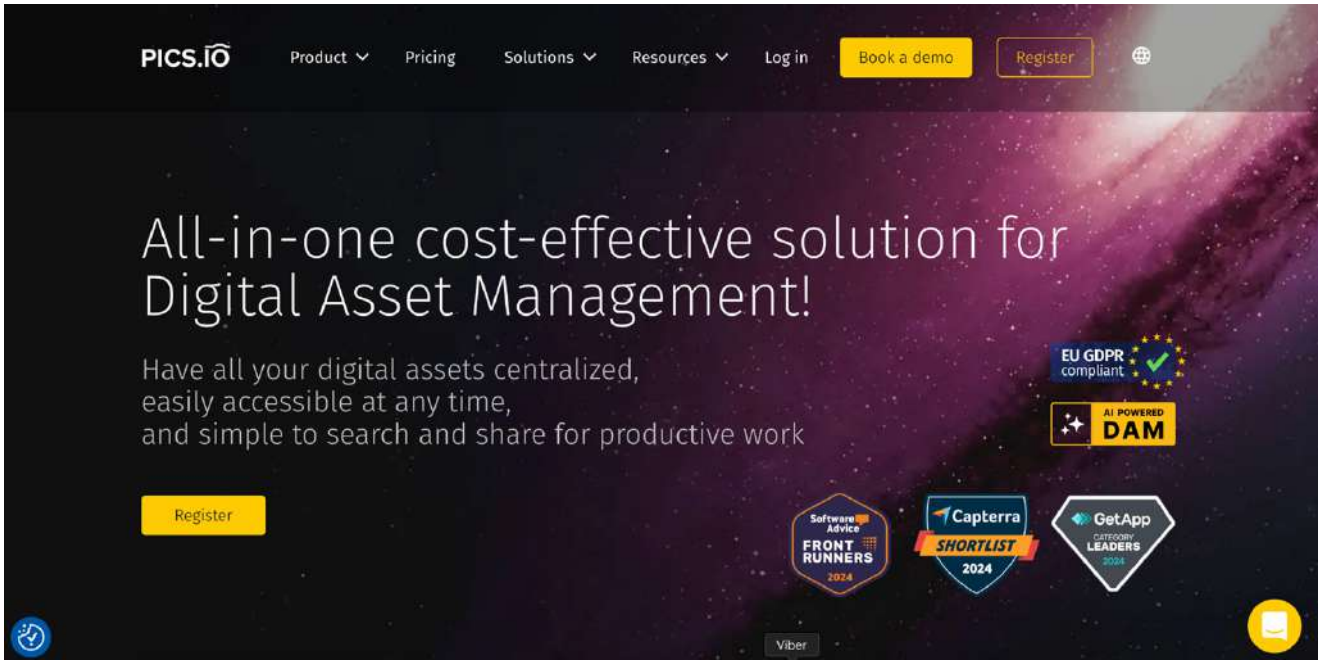
1. **Historijska dokumentacija**: Pomaže u dokumentovanju historijskog stanja web stranica za potrebe istraživanja i analize.

2. **Pravne i sigurnosne provjere**: Provjera istorijskog sadržaja za pravne ili sigurnosne potrebe, kao što je dokazivanje promjena na web stranici.

3. **Oporavak izgubljenog sadržaja**: Oporavak sadržaja koji je izbrisan ili izgubljen s trenutne verzije web stranice.

4. **Edukacija i trening**: Koristi se kao edukativni alat za proučavanje razvoja web dizajna i tehnologija kroz vrijeme.

Pics.io



Pics.io je alat koji se koristi za pregled i upravljanje EXIF podacima slika. EXIF (Exchangeable Image File Format) podaci sadrže metapodatke o fotografijama koje pružaju dodatne informacije o snimljenim slikama.

Glavne funkcionalnosti:

1. Pregled EXIF podataka:

- Informacije o kameri: Podaci o modelu kamere i objektivu koji su korišteni za snimanje fotografije.
- Postavke snimanja: Detalji kao što su otvor blende, brzina zatvarača, ISO vrijednost, žarišna duljina, itd.
- Datum i vrijeme: Informacije o datumu i vremenu kada je fotografija snimljena.

2. Lokacijski podaci:

- GPSKoordinate: Ako je GPS bio omogućen, EXIF podaci mogu uključivati geografske koordinate mjesta gdje je fotografija snimljena.
- Lokacija: Automatsko povezivanje GPS koordinata s fizičkom adresom ili lokacijom.

3. Uređivanje i uklanjanje EXIF podataka:

- Uređivanje metapodataka: Mogućnost dodavanja, mijenjanja ili brisanja određenih EXIF podataka.
- Anonimizacija: Uklanjanje osjetljivih informacija, poput lokacijskih podataka, prije dijeljenja fotografija.

World Imagery Wayback

World Imagery Wayback je alat koji se koristi za pregled historijskih satelitskih snimaka Zemlje. Ovaj alat omogućava korisnicima da vide kako su se određena područja mijenjala kroz vrijeme koristeći satelitske slike iz različitih vremenskih perioda.

Glavne funkcionalnosti:

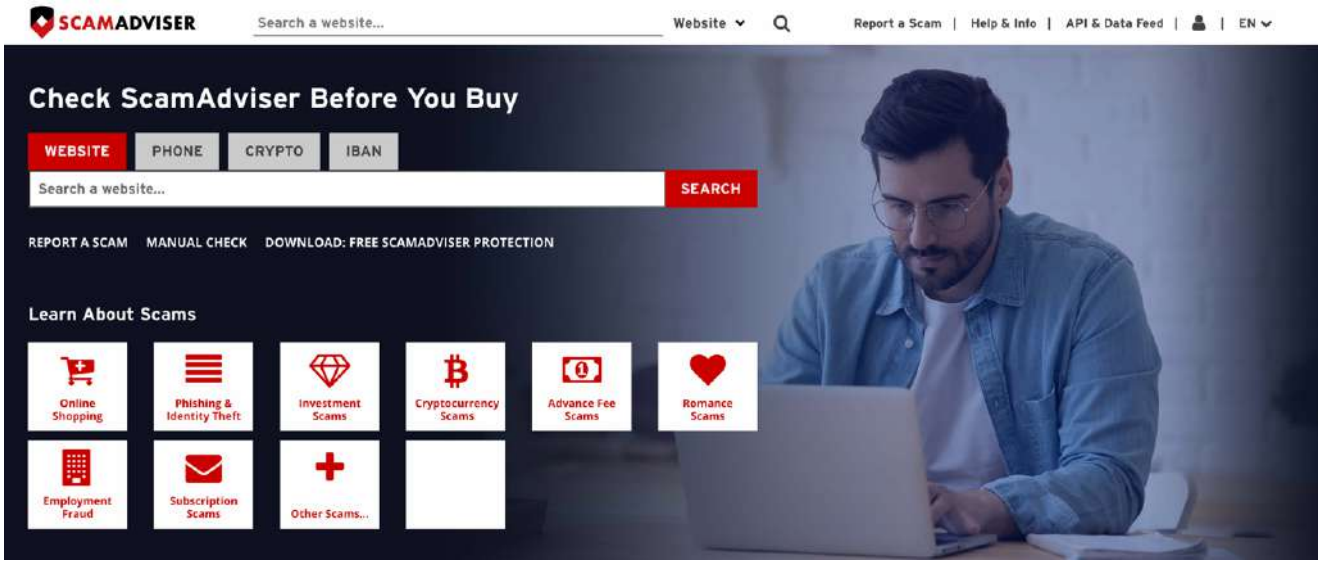
1. Pregled povijesnih slika:

- Satelitske slike kroz vrijeme: Prikaz historijskih satelitskih snimaka određenih područja kako bi se vidjele promjene u krajoliku, urbanizaciji, prirodnim resursima, itd.
- Vremenski slider: Alat koji omogućava lako prebacivanje između različitih vremenskih perioda.

2. Analiza promjena:

- Uspoređivanje slika: Uspoređivanje satelitskih slika iz različitih godina za analizu promjena u okolišu, gradnji, poljoprivredi, itd.
- Detekcija promjena: Automatska ili ručna identifikacija promjena na osnovu satelitskih snimaka.

ScamAdviser.com



ScamAdviser.com je OSINT alat namjenjen za provjeru pouzdanosti i legitimiteta web sajtova. Pomaže korisnicima da identifikuju potencijalne prevare i nesigurne sajtove na internetu.

Evo kako ScamAdviser može da se koristi i koje su mu glavne funkcije:

1. **Provjera kredibiliteta sajta**: ScamAdviser analizira informacije o domenu uključujući registraciju, starost sajta, vlasnika domena, i lokaciju servera. To je korisno za identifikaciju sajtova koji izgledaju sumnjivo ili koji imaju kratku historiju, što može biti znak potencijalne prevare.

2. **Analiza reputacije**: Koristi podatke iz različitih izvora kako bi prikazao reputaciju sajta. Na primjer, ako je sajt prijavljivan kao prevara od strane korisnika ili se nalazi na crnim listama, ScamAdviser će to označiti.

3. **Rangiranje rizika**: ScamAdviser daje procjenu rizika, što je indikator da li se sajt može smatrati sigurnim ili rizičnim. Ovo uključuje faktore kao što su HTTPS enkripcija, kvalitet sadržaja, i transparentnost podataka o vlasniku.

4. **Detekcija sumnjivih šema**: ScamAdviser može identifikovati obrasce ponašanja sajta koji ukazuju na phishing ili malver, kao što su lažni pop-up oglasi, podaci o vlasnicima koji su skriveni, i neusklađenosti u kontakt informacijama.

5. Provjera online prodavnica: Koristan je za provjeru e-commerce sajtova, pomažući korisnicima da izbjegnu prevare prilikom online kupovine. Ako sajt ima nisku ocenu ili mnogo negativnih komentara korisnika, to može biti znak da je reč o prevarantskoj prodavnici.

U domenu cyber sigurnosti, ScamAdviser se koristi za proaktivnu zaštitu, posebno kada se procjenjuje bezbjednost i pouzdanost web sajtova koji su relativno novi ili koji privlače sumnju zbog nepoznatih faktora.

Forenzika nasilnog ekstremizma u digitalnom okruženju

Projekat podržava SMART Balkan - Civilno društvo za povezan Zapadni Balkan, implementiraju Centar za promociju civilnog društva (CPCD), Center for Research and Policy Making (CRPM) i Institute for Democracy and Mediation (IDM) i finansijski podržava Ministarstvo vanjskih poslova Kraljevine Norveške.

Autori:

Ozrenko Đurić Branko Petrović Cyber wings team