



REPUBLIKA SRBIJA
RATEL
REGULATORNO TELO ZA
ELEKTRONSKE KOMUNIKACIJE
I POŠTANSKE USLUGE



NACIONALNI CERT

REPUBLIKE SRBIJE

dr Marko Krstić

Rukovodilac Službe za informacionu bezbednost

marko.krstic@ratel.rs



SADRŽAJ



- Zakonski okvir i aktivnosti NCERT-a
- Prijava incidenata
- Obuke
- Pružanje saveta i ranih upozorenja
- Threat intelligence
- Analiza malicioznog sadržaja
- MISP - Platforma za deljene informacija o pretnjama



SADRŽAJ



- Zakonski okvir i aktivnosti NCERT-a
- Prijava incidenata
- Obuke
- Pružanje saveta i ranih upozorenja
- Threat intelligence
- Analiza malicioznog sadržaja
- MISP - Platforma za deljene informacija o pretnjama



ZAKONSKI OKVIR

Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima Republike Srbije (Nacionalni CERT)

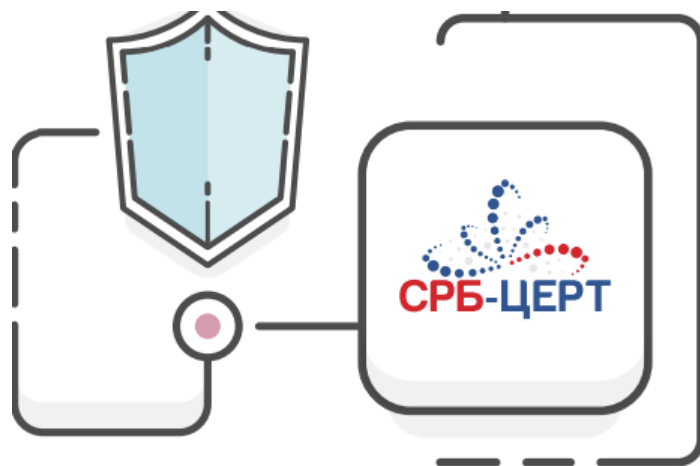
Osnovan je 2017. godine

Deluje u okviru Regulatorne agencije za elektronske komunikacije i poštanske usluge (RATEL), u skladu sa Zakonom o informacionoj bezbednosti





AKTIVNOSTI NACIONALNOG CERT-a



- Analiza sajber pretnji u realnom vremenu
- Zaštita od sajber napada od nacionalnog značaja
- Praćenje stanja o incidentima na nacionalnom nivou
- Analiza rizika i incidenata
- Pružanje ranih upozorenja i tehničkih saveta za zaštitu od sajber incidenata
- Vođenje registra posebnih CERT-ova
- Podizanje svesti javnosti o značaju informacione bezbednosti



SADRŽAJ



- Zakonski okvir i aktivnosti NCERT-a
- **Prijava incidenata**
- Obuke
- Pružanje saveta i ranih upozorenja
- Threat intelligence
- Analiza malicioznog sadržaja
- MISP - Platforma za deljene informacija o pretnjama



PRIJAVA INCIDENATA



Naslovna // Prijavi incident

PRIJAVI
INCIDENT

Prijavi incident

Molimo Vas da odaberete odgovarajuću kategoriju korisnika prijave incidenta

FIZIČKO
LICE



MALO I SREDNJE
PREDUZEĆE



IKT SISTEM OD
POSEBNOG ZNAČAJA



Podaci o pravnom licu

Naziv pravnog lica *

Sediste pravnog lica *

Broj telefona *

Email adresa *

* Molimo Vas da proverite ispravnost vaše imejl adrese

IKT sistem *

Podaci o podnosiocu prijave

Ime i prezime *

Naziv radnog mesta *

Broj telefona *

Email adresa *

* Molimo Vas da proverite ispravnost vaše imejl adrese

Podaci o incidentu

Grupa incidenta *

Vrsta incidenta *

Morate izabrati grupu incidenta

Datum *

03.04.2023

Trajanje incidenta

Dana *

Sati *

Minuta

Sekundi

Opis incidenta

Poverljivost podataka



Informacije o žrtvi koje primi Nacionalni CERT obezbeđuju se i čuvaju bezbedno i pristup istim je ograničen. Širenje podataka o žrtvi može se ostvariti samo uz saglasnost, osim u slučaju incidenta koji je od izuzetnog nacionalnog značaja kao što je zaštita nacionalne bezbednosti.

je zaštita nacionalne bezbednosti.

Dežurni broj 24/7: 062 20 20 30

E-mail adresa: info@cert.rs

<https://cert.rs/rs/prijava.html>



SADRŽAJ



- Zakonski okvir i aktivnosti NCERT-a
- Prijava incidenata
- **Obuke**
- Threat intelligence
- Analiza malicioznog sadržaja
- MISP - Platforma za deljene informacija o pretnjama



OBUKE



Akt o bezbednosti

- Primena modela Akta o bezbednosti



Cyberbit

- Donacija Kraljevine Norveške
- Tehničke obuke

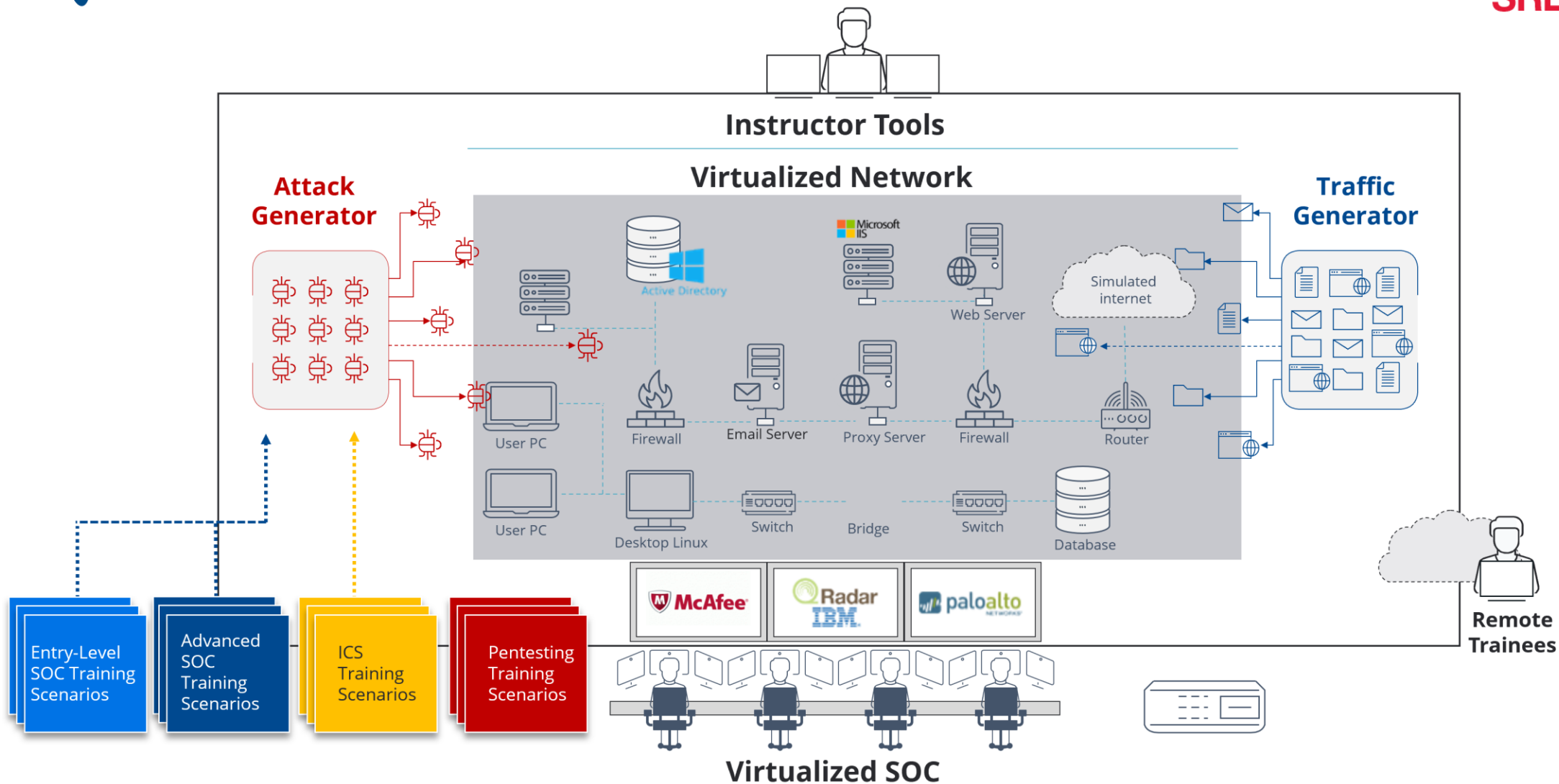


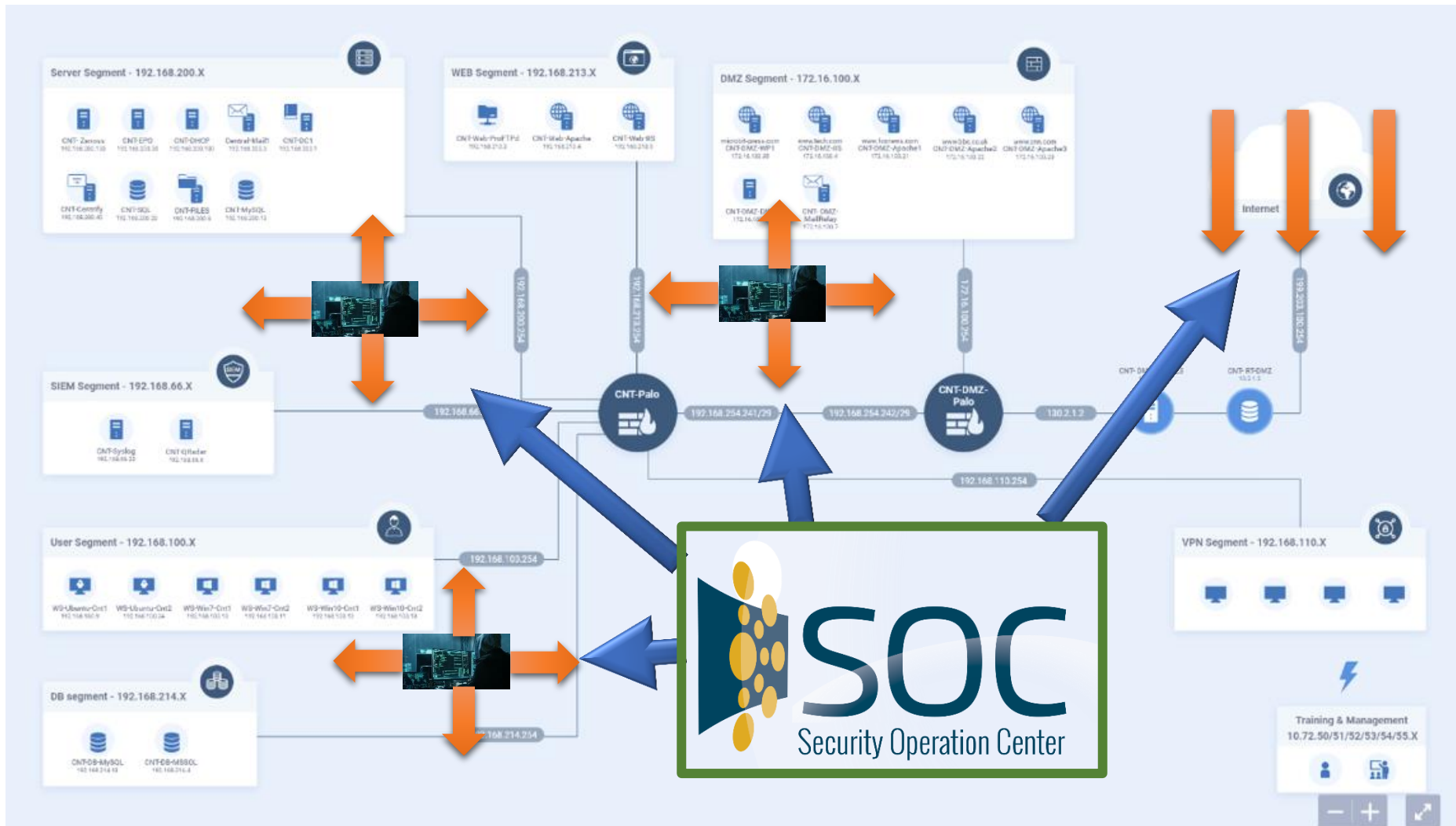
Za bezbedniji klik

- Platforma za podizanje svesti i znanja o informacionoj bezbednosti



Cyberbit







REPUBLIKA SRBIJA
RATEL
REGULATORNO TELO ZA
ELEKTRONSKE KOMUNIKACIJE
I POŠTANSKE USLUGE

SEMINARI I TEHNIČKE VEŽBE



Period 2019 - 2022



Ministarstvo informisanja
i telekomunikacija

355

Broj učesnika

400

Broj učesnika



INSTITUT ZA
STANDARDIZACIJU
SRBIJE



ZA BEZBEDNIJI KLIK



EDUKATIVNI CENTAR

← **Sajber bezbednost**

Sajber bezbednost je praksa zaštite kritičnih sistema i osetljivih informacija od digitalnih napada

DECEMBAR

2 0 800

Fišing

Fišing je najzastupljeniji tip sajber napada

Počni sada →

NOVEMBAR

5 0 12m 0

Kreiranje i bezbednost lozinki

Kreiranje i upravljanje lozinkama na bezbedan način.

Počni sada →

NOVEMBAR

4 0 17m 300

Bezbednost na društvenim mrežama

Važnost zaštite naših ličnih podataka prilikom korišćenja društvenih mreža.

Počni sada →

NOVEMBAR

1 0 20m 400

Ransomver

Bliže upoznavanje korisnika sa Ransomver tipom sajber napada.

Počni sada →

NOVEMBAR

1 0 20m 400

Kreiranje rezervnih kopija podataka

DECEMBAR

1 0 20m 400

Socijalni inženjering

DECEMBAR

1 0 20m 400

Bezbedno korišćenje otvorenog

<https://learn.cert.rs/>



OBUKE

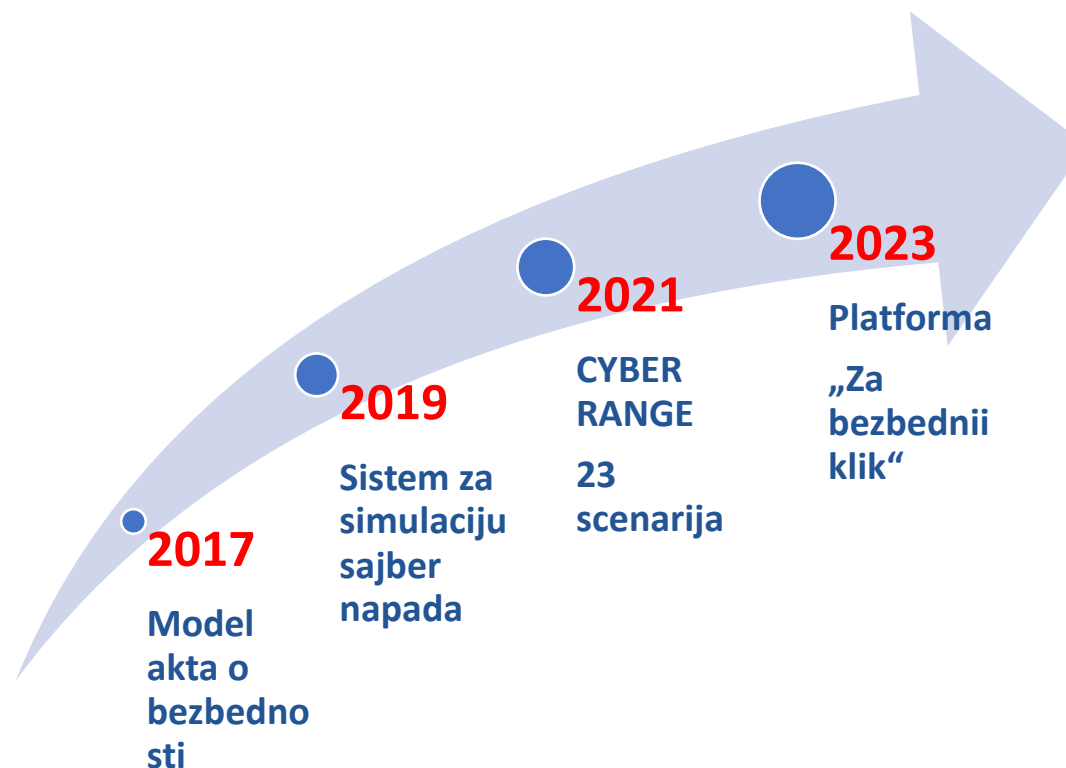


Razumevanje tehnologije

Implementacija mera zaštite

Unapređenje veština i
podizanje nivoa znanja

Detekcija i reakcija na
kritične bezbednosne
aktivnosti





SADRŽAJ



- Zakonski okvir i aktivnosti NCERT-a
- Prijava incidenata
- Obuke
- **Pružanje saveta i ranih upozorenja**
- Threat intelligence
- Analiza malicioznog sadržaja
- MISP - Platforma za deljene informacija o pretnjama



PRUŽANJE SAVETA

BROŠURE





PRUŽANJE SAVETA

PUBLIKACIJE



Naslovna // Publikacije

Publikacije

PRIJAVI
INCIDENT

Nalazite se na stranici Publikacije. Za potrebe lakše pretrage, izaberite željenu kategoriju korisnika i saznajte više o svim dostupnim temama izabrane kategorije.

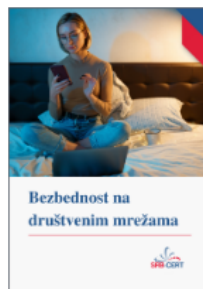
Građani

IKT sistemi od
posebnog značaja

Mala i srednja
preduzeća

Uputstva i
istraživanja

Sve publikacije



Bezbednost na
društvenim mrežama

Bezbednost na društvenim mrežama

- Sve što drugi ljudi mogu saznati o nama, kao korisnicima društvenih mreža, zapravo je dostupno na našim profilima, sadržaju koji objavljujemo, kao i interakcijama koje imamo sa drugim korisnicima.
- Tri osnovna tipa sajber napada na društvenim mrežama su:
 - Malver,
 - Krađa ličnih podataka i
 - Vršnjačko nasilje.
- Kako se možemo zaštititi?

2. Februar 2023 pdf 17.48MB [Saznajte više](#)



Sajber Azbuka

Azbuka osnovnih sajber preporuka koje vam mogu pomoći da budete bezbedniji dok uživate, učite ili radite na internetu.

25. Novembar 2022 pdf 11.60MB [Saznajte više](#)



PRUŽANJE SAVETA

PREPORUKE



Naslovna // Preporuke

Preporuke

PRIJAVI
INCIDENT

Važno

Cisco je objavio nova
bezbednosna ažuriranja

31. Mart 2023

Važno

Mozilla je objavila nova ažuriranja
za Thunderbird 102.9.1

29. Mart 2023

Važno

Apple je objavio nova
bezbednosna ažuriranja

28. Mart 2023

Važno

Google je objavio nova
bezbednosna ažuriranja

28. Mart 2023

Kritično

Cisco je objavio nova
bezbednosna ažuriranja

23. Mart 2023

Važno

Google je objavio nova
bezbednosna ažuriranja

22. Mart 2023

ARHIVA

2023

2022

2021

2020

2019

2018

2017

<https://www.cert.rs/>



REPUBLIKA SRBIJA
RATEL
REGULATORNO TELO ZA
ELEKTRONSKE KOMUNIKACIJE
I POŠTANSKE USLUGE

MEĐUNARODNA SARADNJA





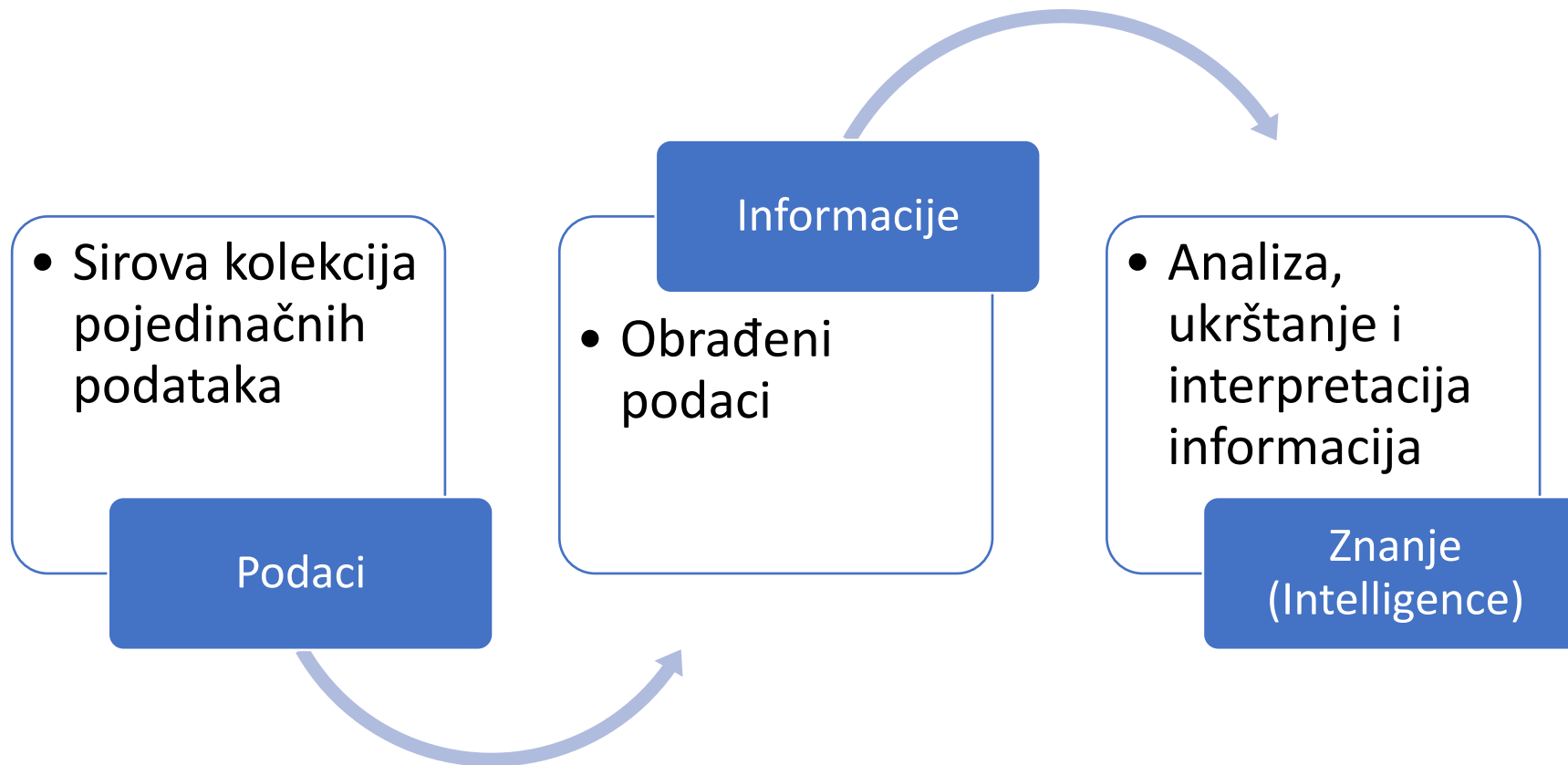
SADRŽAJ



- Zakonski okvir i aktivnosti NCERT-a
- Prijava incidenata
- Obuke
- Pružanje saveta i ranih upozorenja
- **Threat intelligence**
- Analiza malicioznog sadržaja
- MISP - Platforma za deljene informacija o pretnjama



Threat intelligence










Threat intelligence

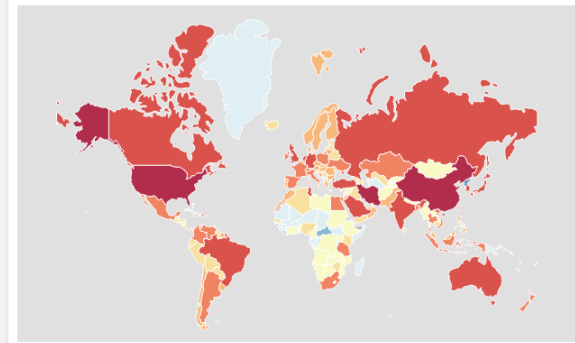


[Dashboard](#) General statistics IoT device statistics Attack statistics

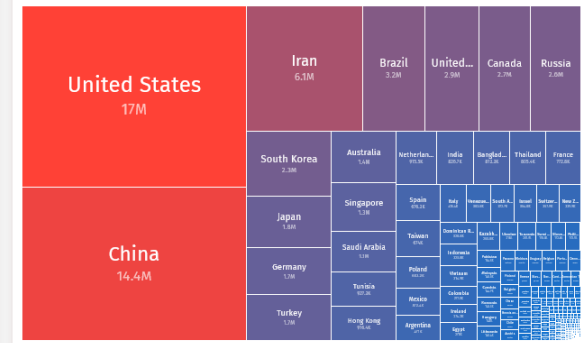
-  Sinkholes »
-  Scans »
-  Honeypots »
-  DDoS »
-  ICS/OT »

About this data
 Shadowserver scans the entire IPv4 Internet for over 100 different network protocols every day, and also performs IPv6 scans based on IPv6 hitlists for selected protocols. These are "hello" type port scans that do not exploit any vulnerability. They enable identification of misconfigured, vulnerable or abusable devices, unnecessarily exposed attack surfaces, or simply just population enumeration. Population enumeration results can be found under the "population" source type.

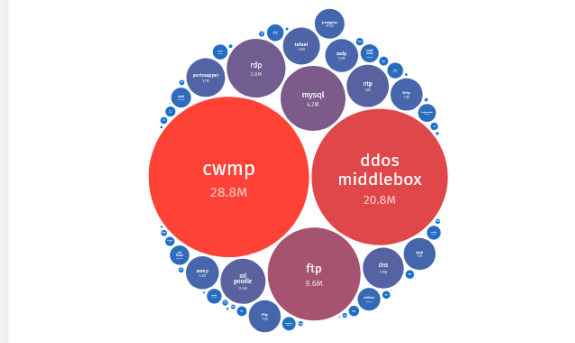
Unique IP addresses per country 2022-10-27



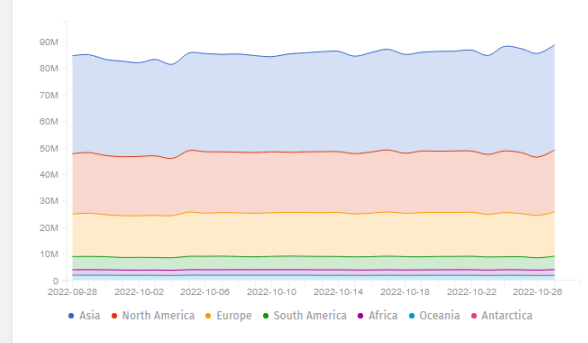
Unique IP addresses per country 2022-10-27



Unique IP addresses per tag 2022-10-27

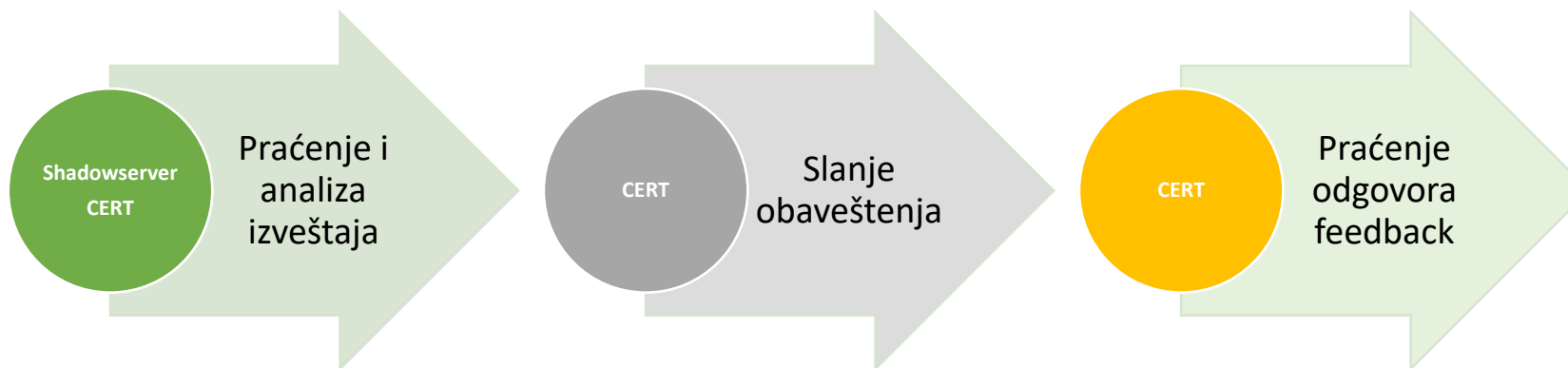


Unique IP addresses over time 2022-09-28 to 2022-10-27





Threat intelligence



- Preko 130 izveštaja
- Microsoft Echange
- Vmware
- Web server Zimbra i ostale http ranjivosti
- LDAP
- Fortinet

- Baze podataka
- PostgreSQL
- SMB (Server Message Block) protokol
- Telnet
- ICS
- Storage sistemi
- Udaljeni pristup (Remote Desktop RDP, VNC)



SADRŽAJ



- Zakonski okvir i aktivnosti NCERT-a
- Prijava incidenata
- Obuke
- Pružanje saveta i ranih upozorenja
- Threat intelligence
- **Analiza malicioznog sadržaja**
- MISP - Platforma za deljene informacija o pretnjama



ANALIZA

MALICIOZNOG SADRŽAJA



Pandora



Lookyloo



URL Abuse



Pandora



Резултат анализе



Нема назнака да је фајл малициозан!

Ниједан технички индикатор сумњивог понашања није пронађен у овом фајлу.

Не постоји стопостотна гаранција да је безбедно отворити овај фајл.

Уколико је преглед фајла у Pandora алату довољан, не морате га отварати на вашем рачунару!

Детаљи о фајлу

Име	ГИИ - ГОДИШЊИ ИЗВЕШТАЈ ЗА 2022. ГОДИНУ ЗА ПОДАТКЕ О ИНФРАСТРУКТУРИ ratel.pdf
Време покретања анализе	Mar 21, 2023 1:26 PM
Величина фајла	2203665 bytes
Врста фајла	PDF file
MimeType	application/pdf
MD5	9088d61a6cf01e334606ee06d984aba0
SHA-1	1e8023b7c63370d0eeb1c5fc276b321331f3ab56
SHA-256	534d6b7f9a695b637288a8bacdb4ffb8e477a111a3d29103ca67322e783192f4

Прикажи детаље

Акције ...

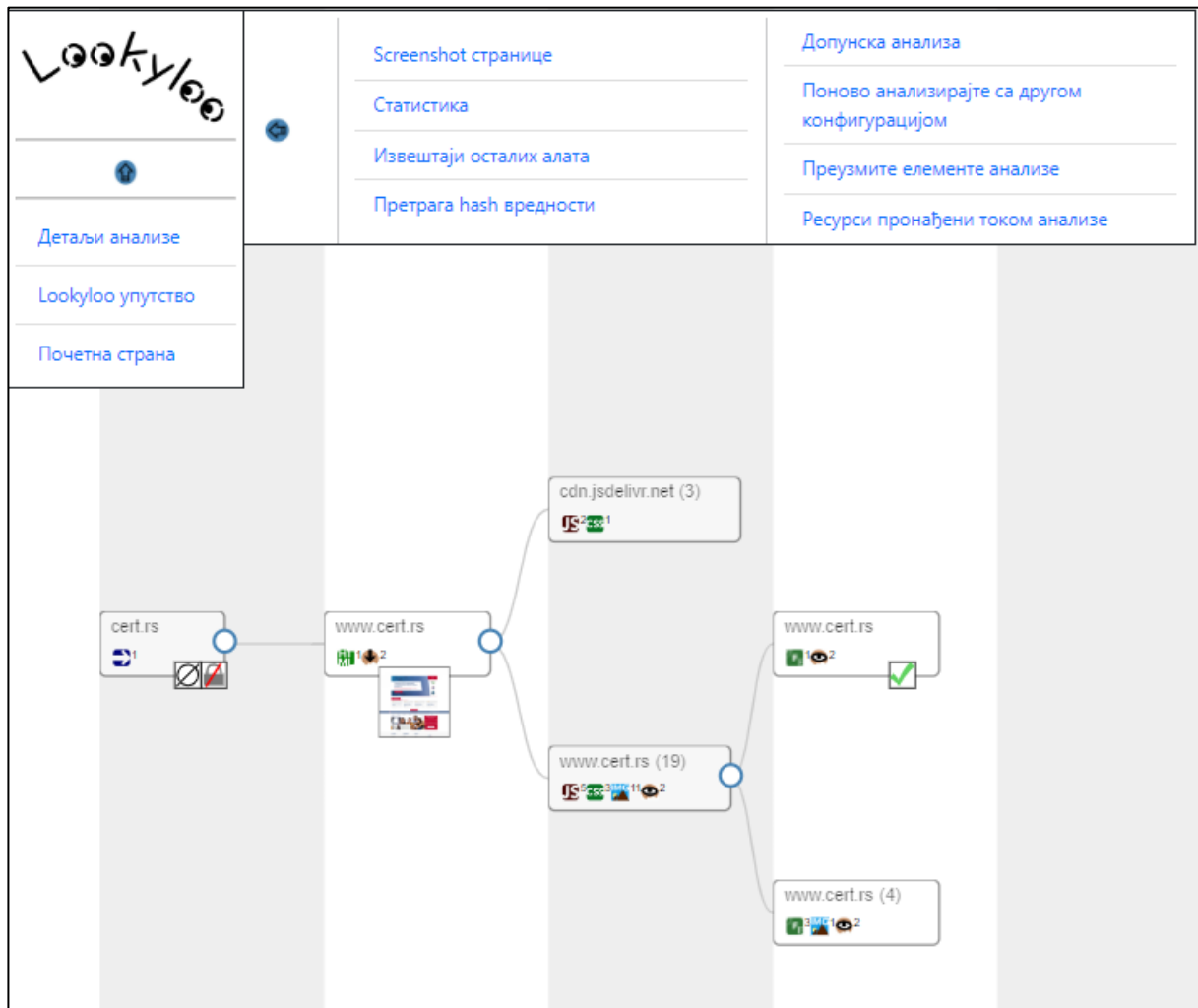
- Поново скенирај фајл
- Пошаљи упозорење Националном ЦЕРТ-у

Ostale funkcionalnosti:

- Pregled sadržaja
- Pregled teksta
- Tekstualni sadržaj
- Metadata
- Putanja do originala



Lookyloo



- Легенда**
- Неенкриптовани захтеви
 - Празни одговори
 - Примљени колачићи
 - Читање колачића
 - Редирекција
 - iFrame
 - Javascript
 - Font
 - HTML
 - JSON
 - CSS
 - EXE
 - Слика
 - Видео
 - Непознат садржај



URL Abuse



URL Abuse

URL Abuse je servis za proveru URL-ova.
[Više informacija o servisu](#)



URL поље

Унесите URL који желите да истражите.

Провери

Proverava:

- [VirusTotal](#)
- Google SafeBrowsing
- [EU Phishing Initiative](#)



SADRŽAJ



- Zakonski okvir i aktivnosti NCERT-a
- Prijava incidenata
- Obuke
- Threat intelligence
- Analiza malicioznog sadržaja
- **MISP - Platforma za deljene informacija o pretnjama**



MISP



- MISP (Malware Information Sharing Platform)
- Platforma za deljenje informacija o pretnjama
- Open source platforma koja se koristi za razmenu i deljenje informacija sa sajber zajednicom o različitim vrstama sajber napada u cilju brže detekcije sajber napada.
- Centralna baza podataka o indikatorima kompromitovanja i sadrži informacije tehničkog i netehničkog karaktera.
- Registrovanim operatorima IKT sistema od posebnog značaja će biti kreirani nalozi za pristup MISP platformi u cilju razmene informacija o aktuelnim rizicima i pretnjama u oblasti informacione bezbednosti i promovisanja primera dobre prakse
- Platformi se može pristupiti putem linka: misp-cr.cert.rs



MISP



The screenshot displays the MISP web interface. The top navigation bar includes links for Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, Logs, and API. The main content area is titled "Events" and features a search bar, a pagination control (showing 1-21), and a filter dropdown. A table lists several events with columns for Creator org, Owner org, ID, Clusters, Tags, #Attr, #Corr, Creator user, Date, and Info. The events listed include PANW, MORS_142, CERT-EE_8833, and Truesec_CDC, each with associated tags like "malware", "ransomware", "phishing", and "intrusion-set".

Creator org	Owner org	ID	Clusters	Tags	#Attr	#Corr	Creator user	Date	Info
✓ PANW		361		misp-galaxy:intrusion-set="PlugX malware", campaign, intrusion-set	18	1	admin@cert.rs	2023-01-26	PlugX malware
✓ MORS_142		357	Android Q, LokiBot, Attack Pattern, Obfuscated Files or Information - T1027, Access Token Manipulation - T1134	Loki Bot, Lokibot, malware:name="lokibot"	47	1	admin@cert.rs	2023-01-26	Lokibot downloader in docx email attachment
✓ CERT-EE_8833		356	Attack Pattern, Input Capture - T1056, Phishing - T1566	Phishing, ip:private	2		admin@cert.rs	2023-01-26	Phishing URL findings
✓ Axur_4587		360		Ransomware	1		admin@cert.rs	2023-01-26	Somacis
✓ Axur_4587		359		Ransomware	1		admin@cert.rs	2023-01-26	Crescent Crown Distributing
✓ Axur_4587		358		Ransomware	1		admin@cert.rs	2023-01-26	ADMIRAL Sportwetten
✓ Axur_4587		364		Ransomware	1		admin@cert.rs	2023-01-25	Bom Calçado
✓ Axur_4587		363		Ransomware	1		admin@cert.rs	2023-01-25	First International Food
✓ SNCB-NMBS		362	Attack Pattern, Spearphishing Link - T1566.002, Input Capture - T1056, Sector, Transport	tip:white, vers:action:social:variety="Phishing", circ:incident-classification="phishing", phishing, ecslrt:fraud="phishing", enisa:malicious-activity-abuse="phishing-attacks", Phishing Site, CSIRT_Social_Engineering, europol-incident:information-gathering="phishing"	5		admin@cert.rs	2023-01-24	Phishing - Password notification O365
✓ Truesec_CDC		368	Malpedia, Raspberry Robin, Silence, Attack Pattern, Disable or Modify Tools - T1562.001, Replication Through Removable Media - T1091, Tool, Raspberry Robin	tip:green, cssa:origin="manual_investigation", industry:nace="M - PROFESSIONAL, SCIENTIFIC AND TECHNICAL ACTIVITIES", industry:nace="P - EDUCATION"	18	2	admin@cert.rs	2022-10-28	C2 traffic seen from an internal system, internal Raspberry Robin



REPUBLIKA SRBIJA
RATEL
REGULATORNO TELO ZA
ELEKTRONSKE KOMUNIKACIJE
I POŠTANSKE USLUGE



NACIONALNI CERT **REPUBLIKE SRBIJE**

dr Marko Krstić

Rukovodilac Službe za informacionu bezbednost

marko.krstic@ratel.rs