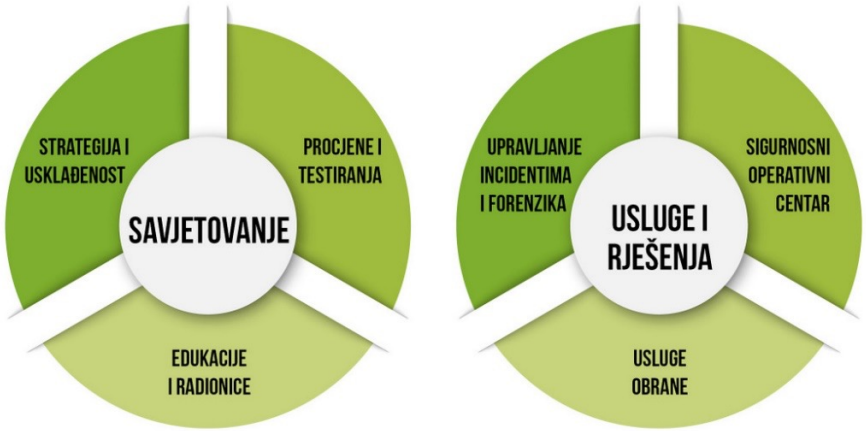
diverto

STANJE INFORMACIJSKE SIGURNOSTI 2021

O Divertu

- Osnovani 2007. godine
- Djelatnost: informacijska sigurnost
- Naše vrijednosti:

- Naš portfelj:



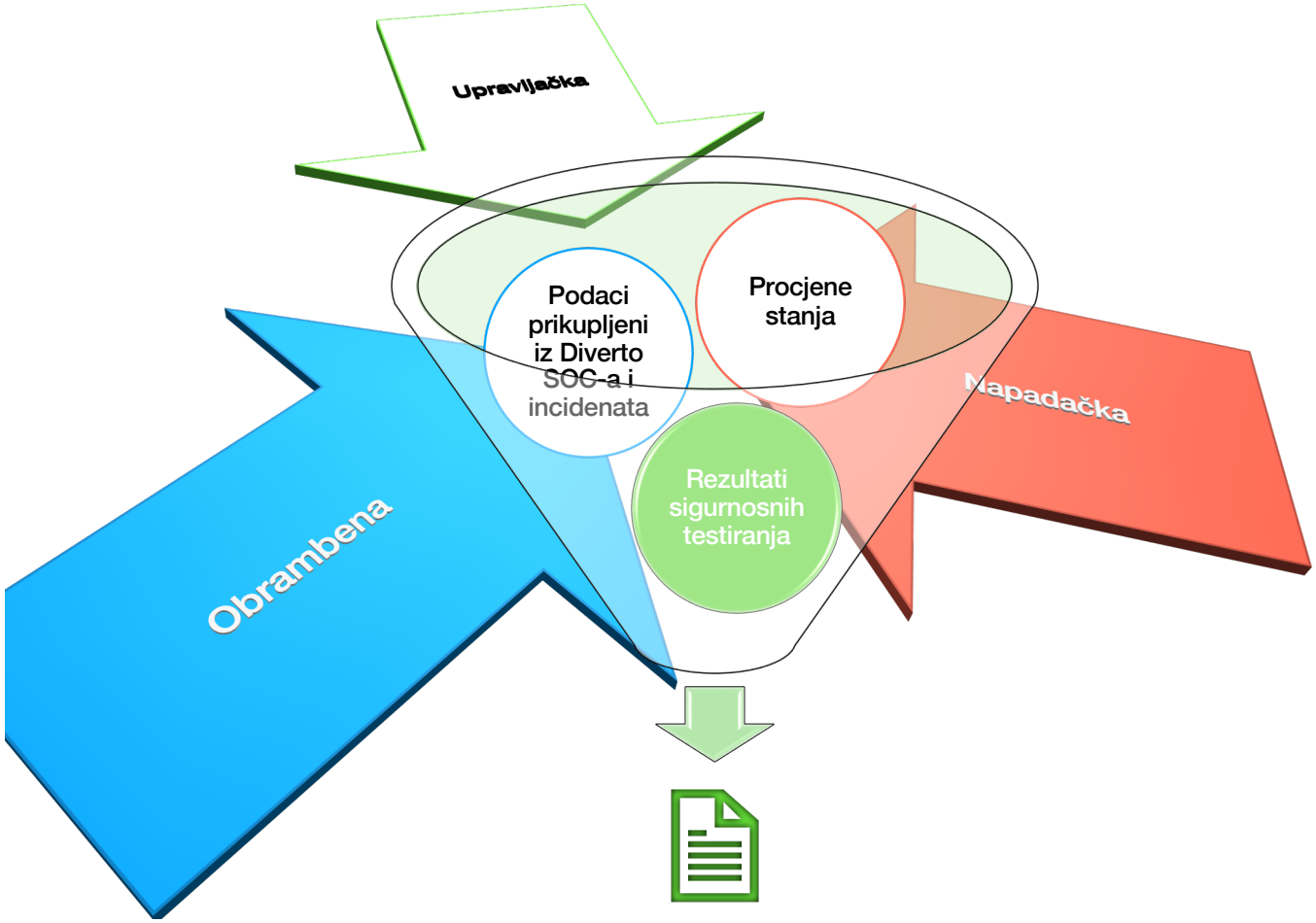
Sadržaj webinara:

1. Stanje informacijske sigurnosti iz tri različite perspektive
2. Incidenti
3. Phishing
4. OT Trendovi
5. DDoS
6. Preporuke
7. Vaša pitanja

Godišnji izvještaj

- Treće izdanje godišnjeg izvještaja
- Fokus
  - Republika Hrvatska
  - Organizacije
- Opseg
  - 2021 godina
- Izdanje
  - Diverto
  - Svibanj, 2022.

Kako je nastao izvještaj?



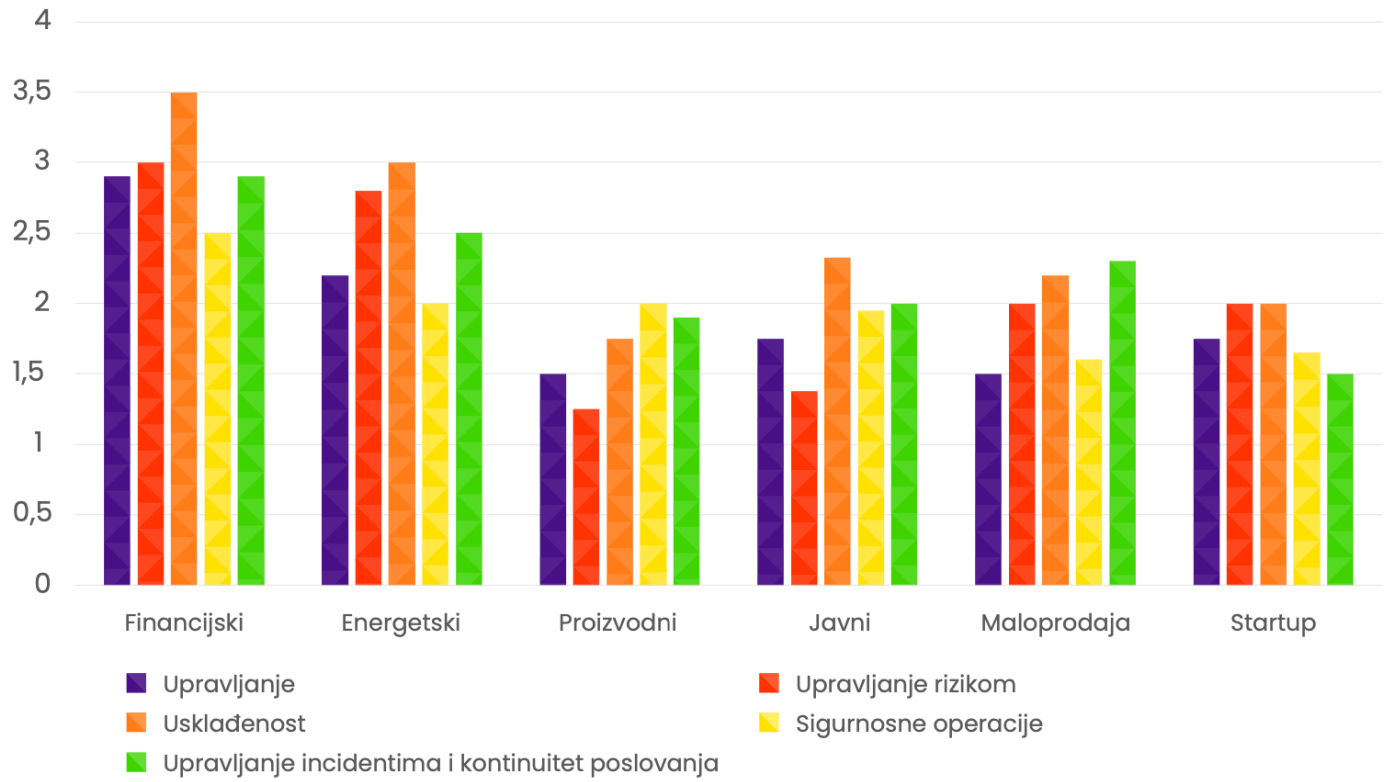
01.01.2021.
31.12.2021.

POUZDANOST POVJERLJIVOST STRUČNOST

UPRAVLJAČKA PERSPEKTIVA

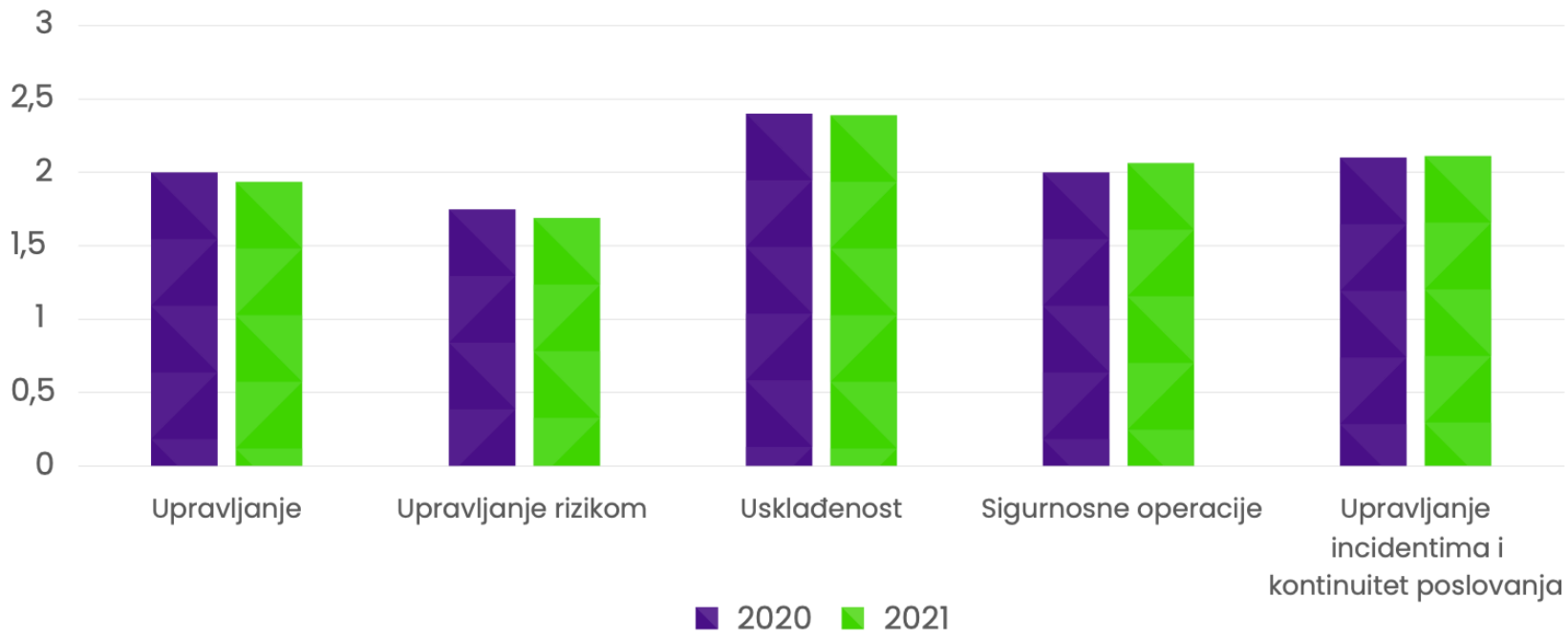
DIVERTO ISTRAŽIVANJE O PERCEPCIJI RIZIKA

Prosječna razina zrelosti – sektori/industrije



Izvor: Diverto

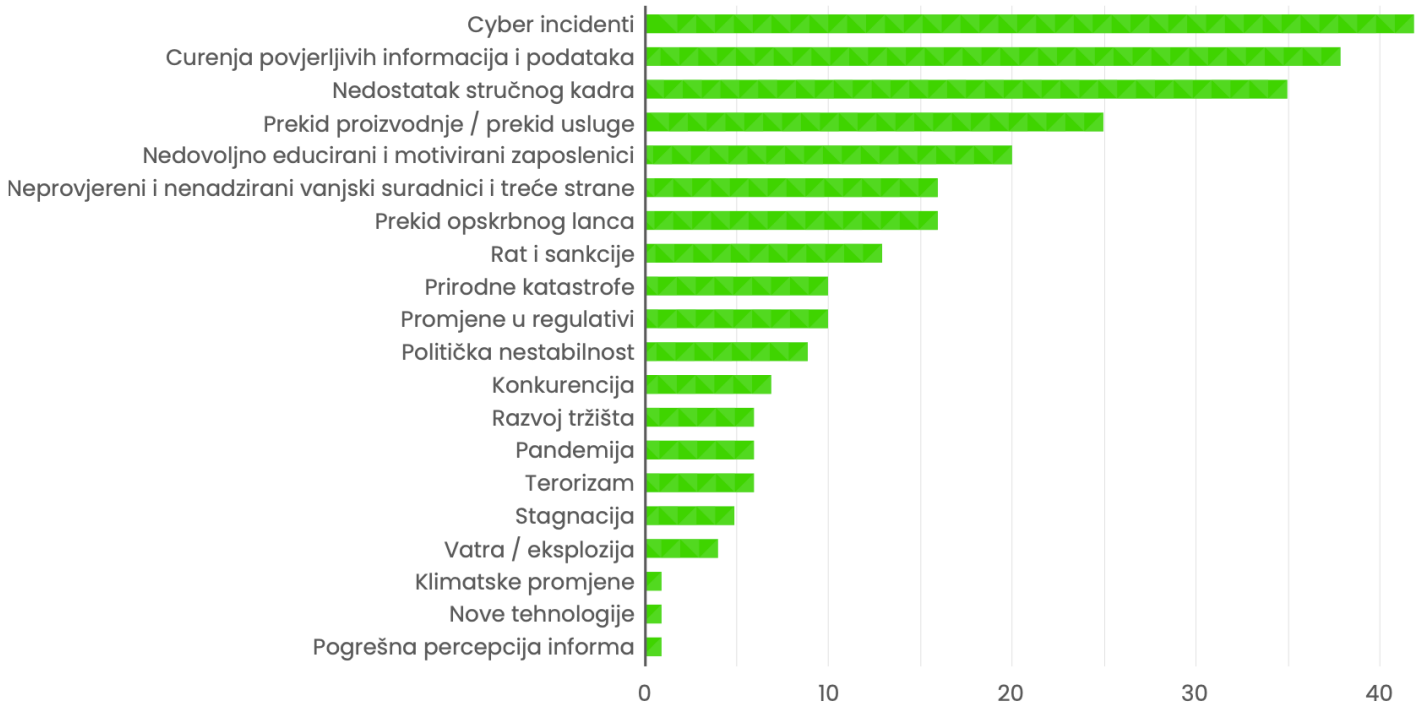
Prosječna razina zrelosti – 2020 vs 2021



Izvor: Diverto

Divertovo istraživanje o percepciji rizika

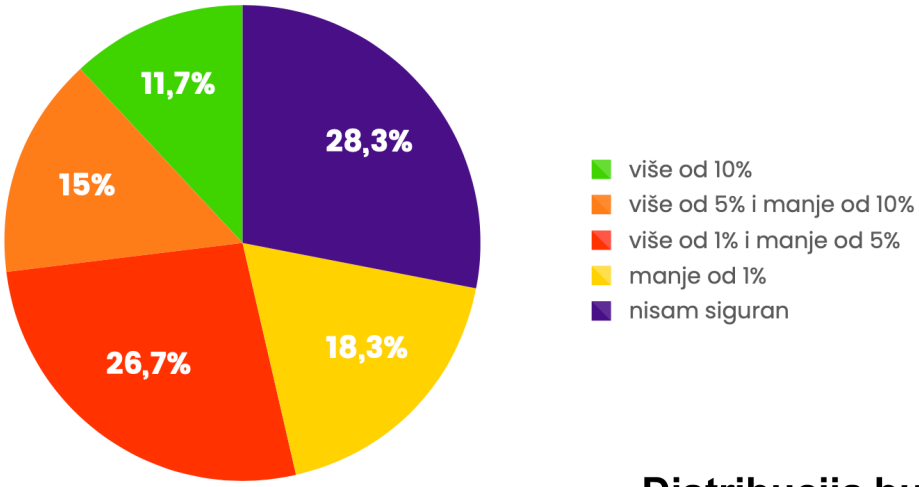
Prema Vašem razmišljanju, što predstavlja najveći rizik za Vašu organizaciju?
Možete izabrati više odgovora. 60 odgovora



Izvor: Diverto

Divertovo istraživanje – budžet za informacijsku sigurnost

Koji postotak IT budgeta trošite na informacijsku / kibernetičku sigurnost?
60 odgovora



73%
ORGANIZACIJA NIJE IMALO ZNAČAJNIH INCIDENATA

27%
ORGANIZACIJA JE IMALO INCIDENT MANJEG ILI VEĆEG OPSEGA

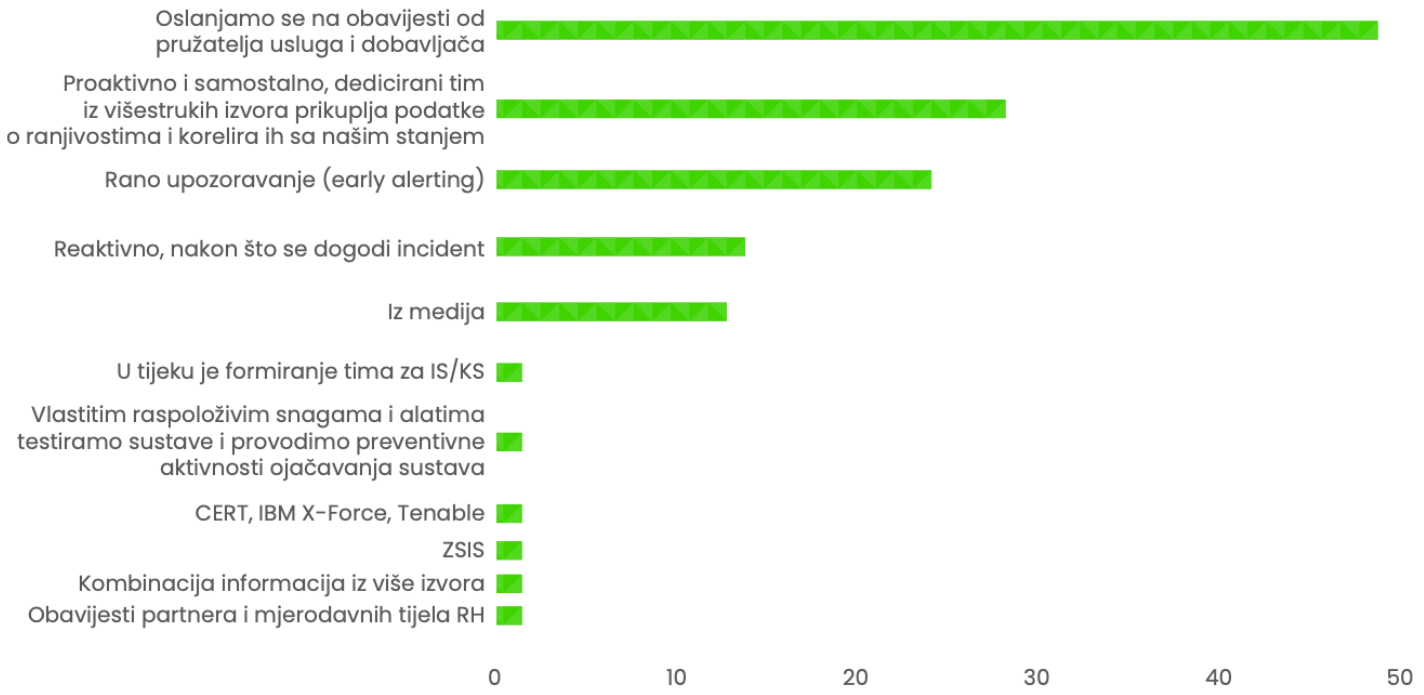
66%
ORGANIZACIJA IMA USPOSTAVLJEN I FUNKCIONIRAJUĆI POSTUPAK ODGOVORA NA INCIDENT

Distribucija budžeta

Izvor: Diverto

Divertovo istraživanje – informiranje o prijetnjama i ranjivostima

Načini kako se informirate o prijetnjama i ranjivostima Vaših sustava?
Možete izabrati više odgovora. 60 odgovora



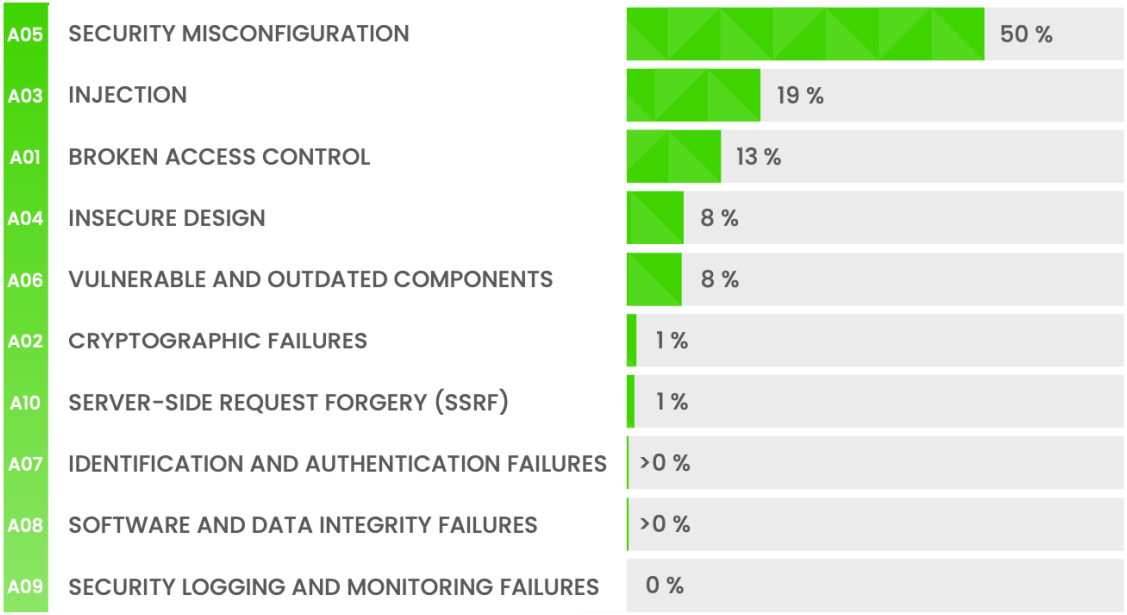
Izvor: Diverto

NAPADAČKA PERSPEKTIVA

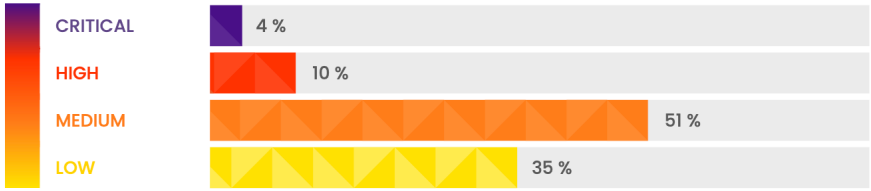
PENETRACIJSKA TESTIRANJA

Ofenzivna/Napadačka perspektiva

RANJIVOSTI DESKTOP I WEB APLIKACIJA TE SERVISA PO KATEGORIJI

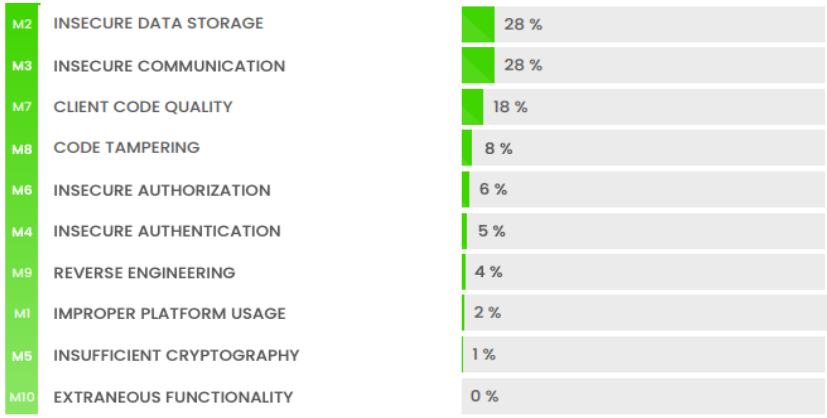


RANJIVOSTI INFRASTRUKTURA PO RIZIKU



SLIKA 6 *Ranjivosti infrastruktura po riziku. [Izvor: Diverto]*

RANJIVOSTI MOBILNIH APLIKACIJA PO KATEGORIJI

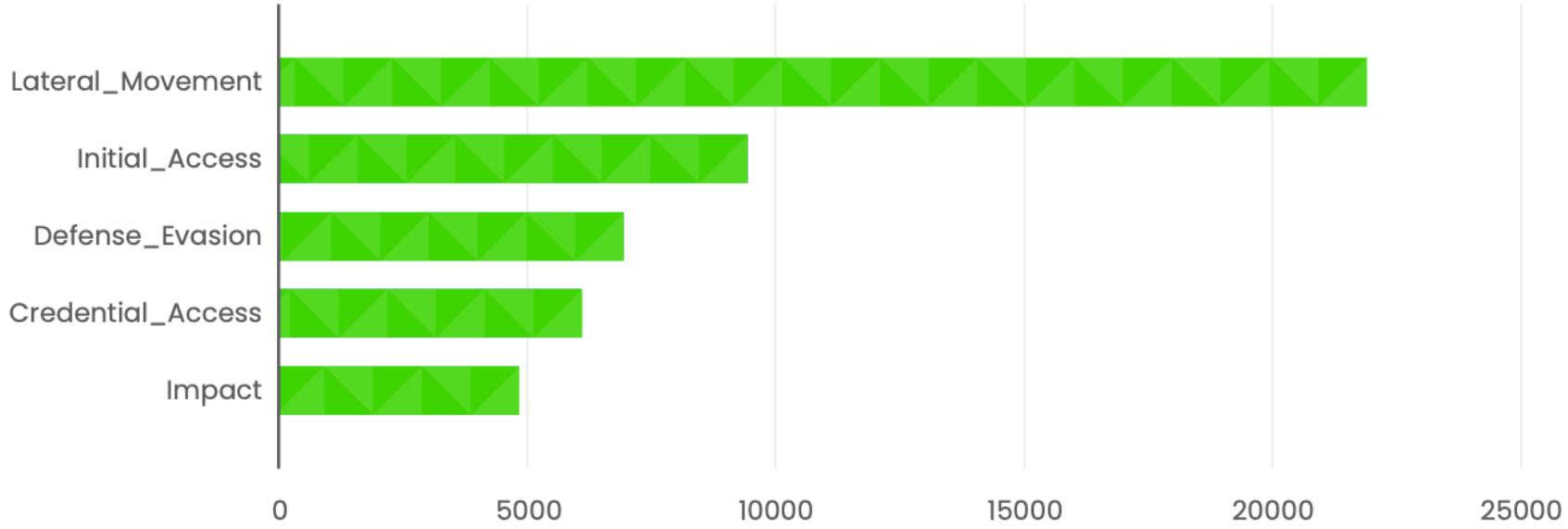


Izvor: Diverto

OBRAMBENA PERSPEKTIVA

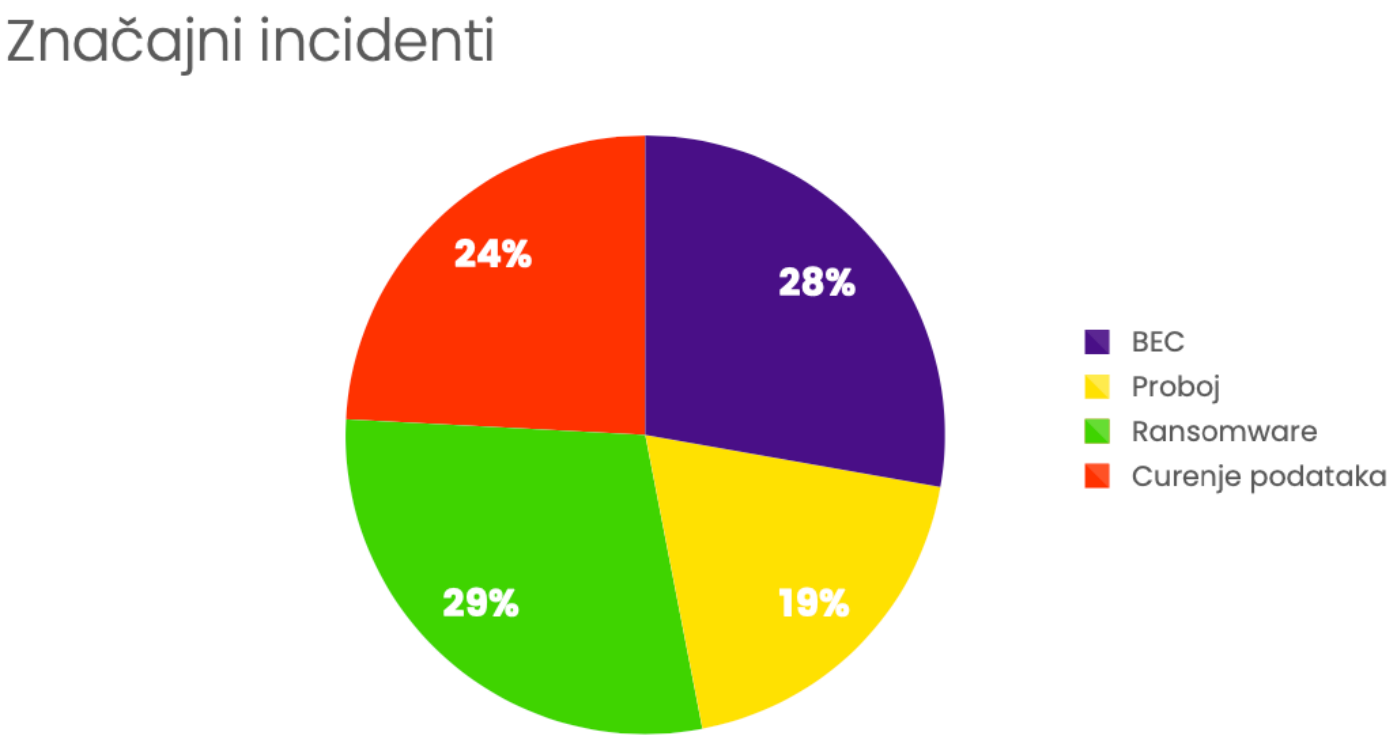
SIGURNOSNO-OPERATIVNI CENTAR I INCIDENTI

Diverto SOC – TOP 5 MITRE Att&ck



Izvor: Diverto SOC

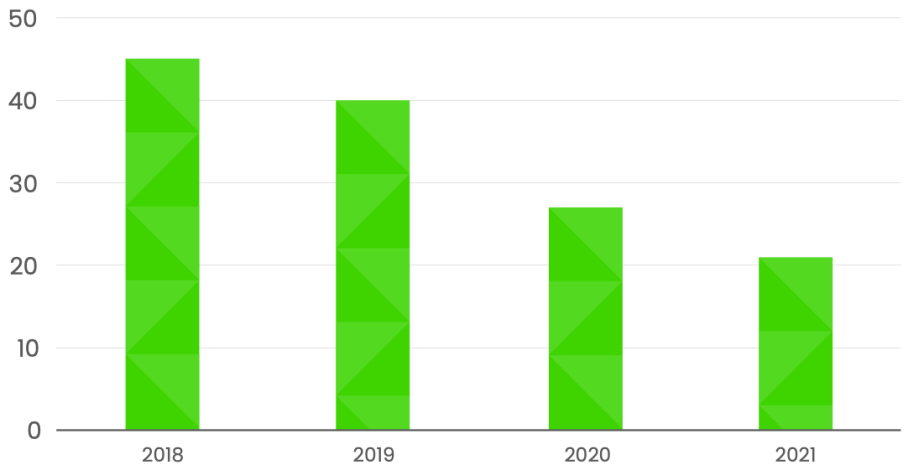
Diverto SOC – značajni incidenti



Izvor: Diverto SOC

PHISHING I OT

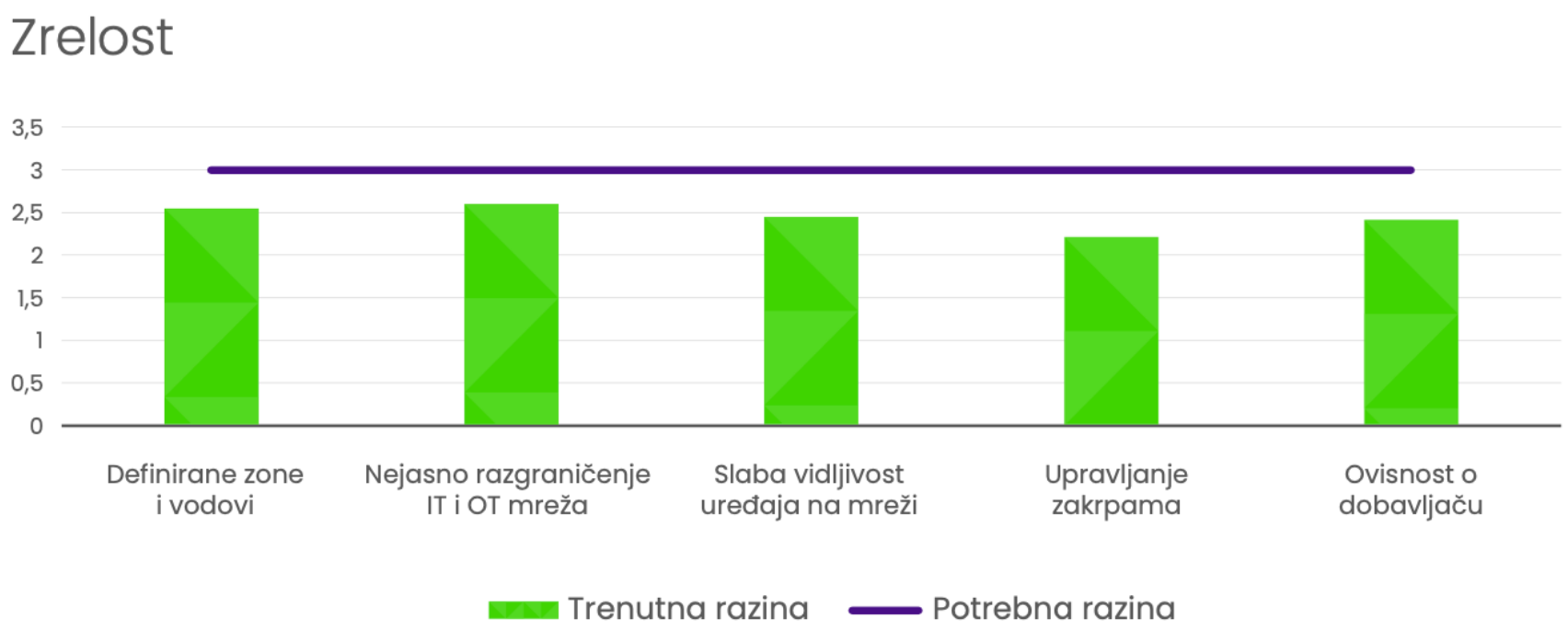
Phishing: postotak „upecanih” primatelja kroz vrijeme



Godina	Postotak primatelja	Broj poslanih poruka
2018	45	1096
2019	40	2206
2020	27	2740
2021	21	7062
		13104

Izvor: Diverto

OT zrelost



Izvor: Diverto

DISTRIBUIRANO USKRAĆIVANJE USLUGE

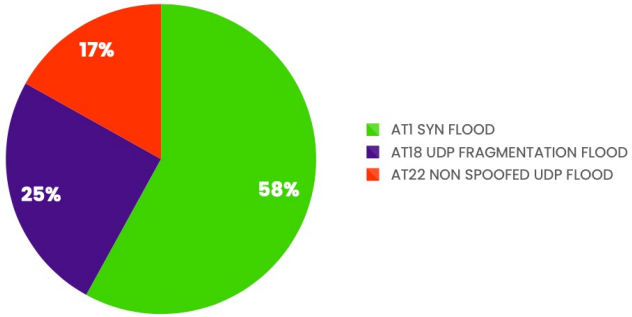
DISTRIBUTED DENIAL OF SERVICE - DDOS

DDoS – najveći napadi po kategoriji

TOP 5 DDoS tehnika po broju pristiglih paketa

1. AT1 SYN FLOOD
2. AT18 UDP FRAGMENTATION FLOOD
3. AT22 NON SPOOFED UDP FLOOD
4. AT3 ACK FLOOD
5. AT25 PING FLOO

Raspodjela najvećih napada po kategoriji



NAJVEĆI NAPAD PO BROJU PAKETA JE 617,6 MILIJARDI PAKETA I TRAJAO JE 1824 MINUTE

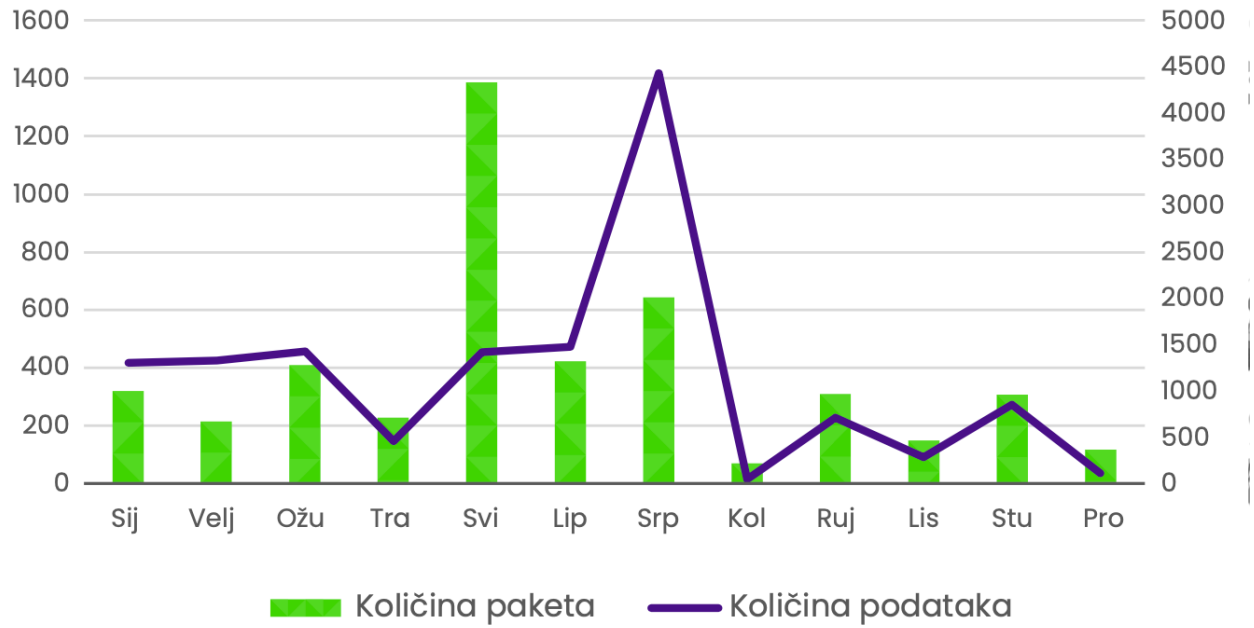
NAJVEĆI NAPAD PO KOLIČINI PODATAKA JE 3,9 TBIT I TRAJAO JE 62 MINUTE

NAJDUŽI NAPAD TRAJAO JE PREKO 47 SATI (2872 MINUTE)

https://www.riorey.com/types-of-ddos-attacks

Izvor: Diverto

DDoS: distribucija napada po mjesecima



Izvor: Diverto

Preporuke

OT/PROCESNI SUSTAVI

Sve češća meta napadača

Veća ranjivost

Veće posljedice

Nedostatna izolacija i nadzor sigurnosti

RIZICI

Rizici se mijenjaju mnogo brže

Lanac opskrbe

Ratovi i ”specijalne operacije”

Napuštanje ručnog i ad-hoc pristupa.

LANAC OPSKRBE

Povećana ovisnost organizacija o svom lancu opskrbe

Solarwinds incident

Proces upravljanja lancem opskrbe

DEVSECOPS

”Shift Left” trend

Integracija sigurnosti u CI/CD

Specijalizirana DAST/SAST/SCA rješenja

SBOM zahtjevi

PITANJA

https://diverto.hr/documents/diverto_stanje_informacijske_sigurnosti_2021.pdf

diverto

information security

www.diverto.hr

Hvala!