



IJU 2015

***Vzpostavitev security operational
centra DRO***

mag. Damijan Marinšek

Ministrstvo za javno upravo
Direktorat za informatiko
Sektor za informacijsko varnost

15. 12. 2015



1. Pregled dosedanjih aktivnosti
2. Vizija
3. Sektor za informacijsko varnost - naloge
4. Projekt
5. SOC



V preteklosti smo izvajali operativne naloge informacijske varnosti:

- izvajanje varnostnih pregledov informacijskih sistemov državne uprave od zunaj (od leta 2007)
- izvajanje varnostnih pregledov informacijskih sistemov državne uprave od znotraj (od leta 2011)
- Odzivanje na incidente tudi s sporazumom s SI-CERT od leta 2010
- Anonymous 2012
- Obveščanje
- Preverjanje aplikacij in gradnikov pred produkcijo 2015



Ozaveščeni in strokovno usposobljeni zaposleni v državni upravi z uveljavljanjem potrjenih varnostnih politik v praksi in z ravnanjem v skladu z veljavno Uredbo o informacijski varnostni politiki začnejo zagotavljati predpisano stopnjo informacijske varnosti.



Preventivno delovanje za večjo varnost informacijskih sistemov:

- verifikacija in implementacija varnostnih rešitev,
- sistematično odkrivanje in preprečevanje ranljivosti ter varnostnih groženj v informacijskih sistemih,
- varnostna analiza informacijskih sistemov (omrežja, operacijski sistemi, aplikacije, podatkovne zbirke),
- sistematično izvajanje preventivnih varnostnih preizkusov informacijskih sistemov,
- priprava ukrepov za odpravo varnostnih pomanjkljivosti in izboljšanje varnosti.

Obravnavanje varnostnih incidentov (SIGOV-CERT):

- sprejem in zaznava incidentov,
- zamejitev škode,
- obravnavanje incidentov,
- predlaganje in izvajanje ukrepov,
- izdelava poročil.

Obveščanje, ozaveščanje in sodelovanje:

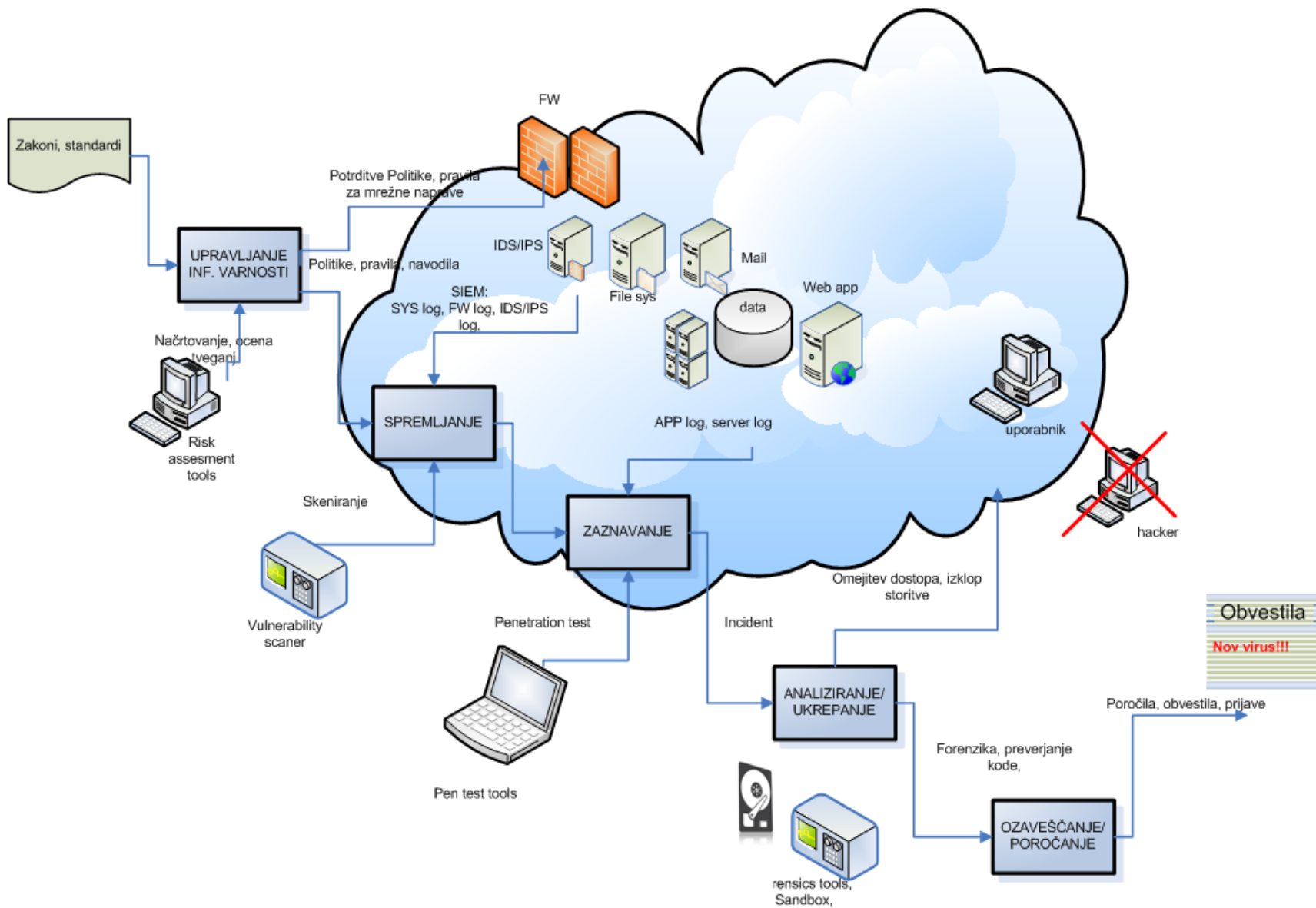
- obveščanje in ozaveščanje skrbnikov sistemov in uporabnikov,
- izvajanje izobraževanja na področju informacijske varnosti.



- **Nabava potrebne strojne in programske opreme** za izvajanje informacijske varnosti - Security Operational Center, naročilo DRO št.6 :
 - za zajem mrežnega prometa,
 - odkrivanje ranljivosti,
 - izvajanje penetracijskih testov,
 - preverjanje izvorne kode,
 - forenzično analizo,
 - platformo za incident management
 - platformo za ozaveščanje.
- **Izobraževanje in usposabljanje:**
 - tečaji in delavnice za informatike
 - obveščanje in opozarjanje uporabnikov



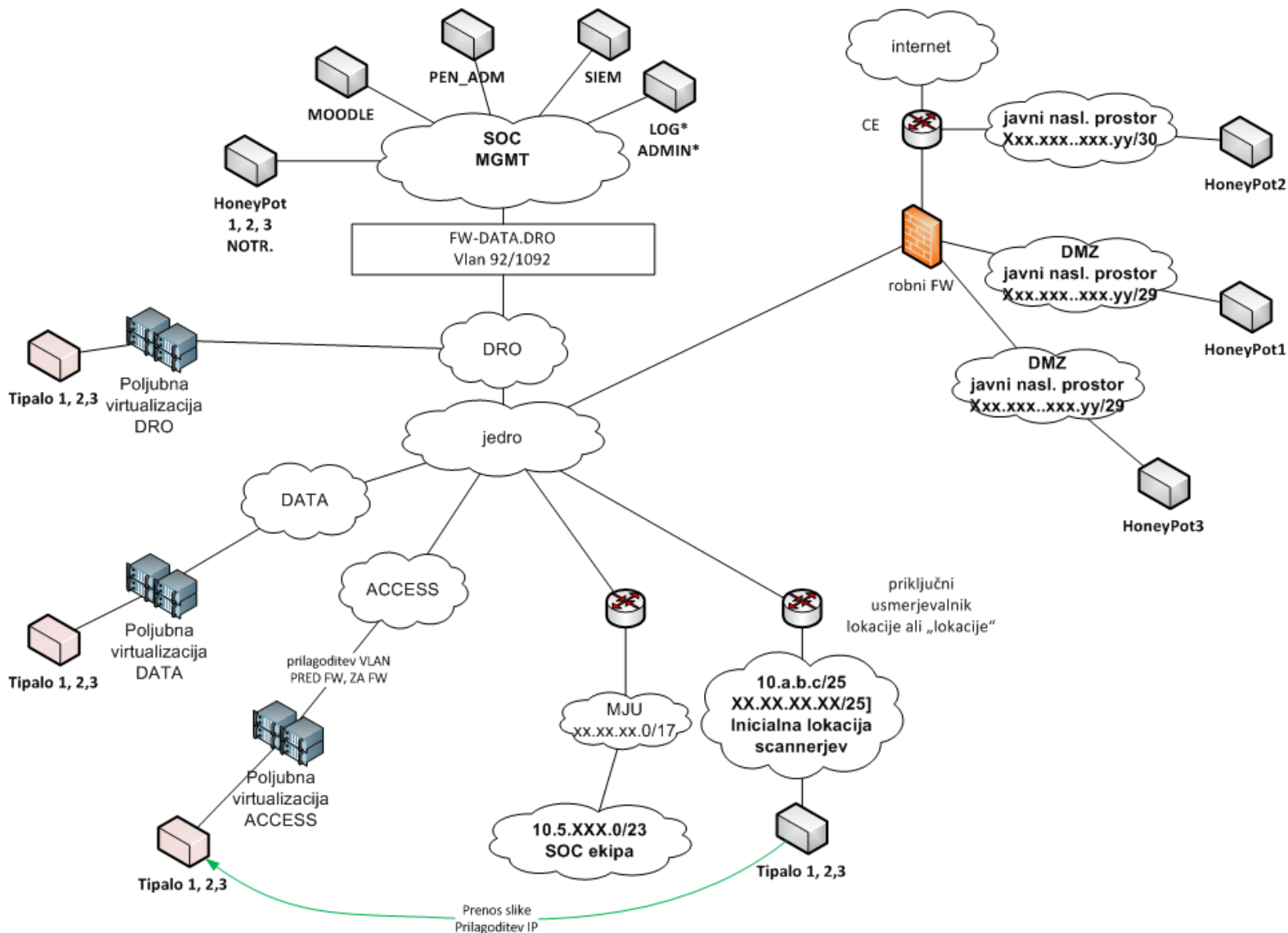
Sektor za informacijsko varnost Security Operational Center SOC





Sektor za informacijsko varnost

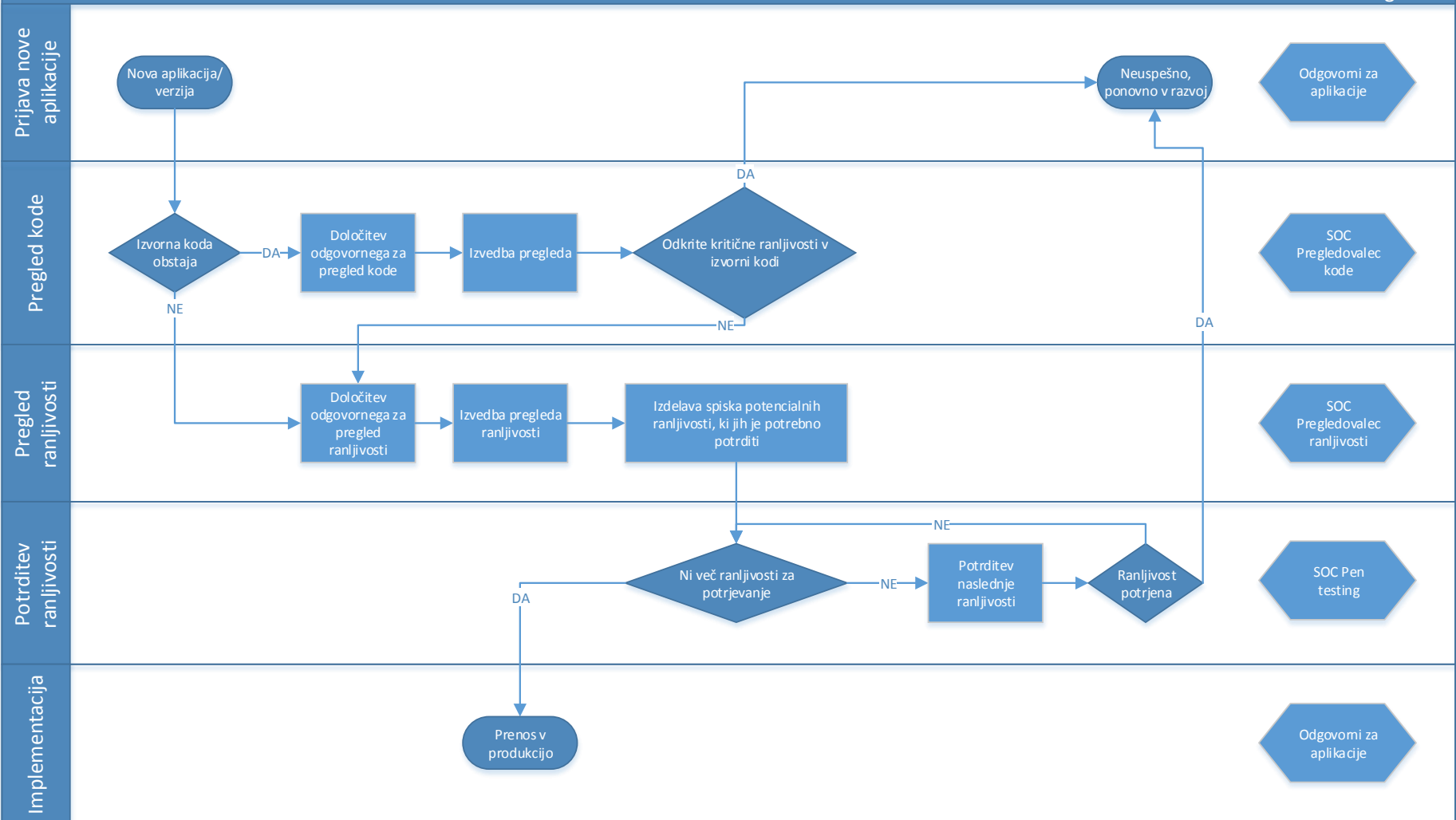
Network shema SOC





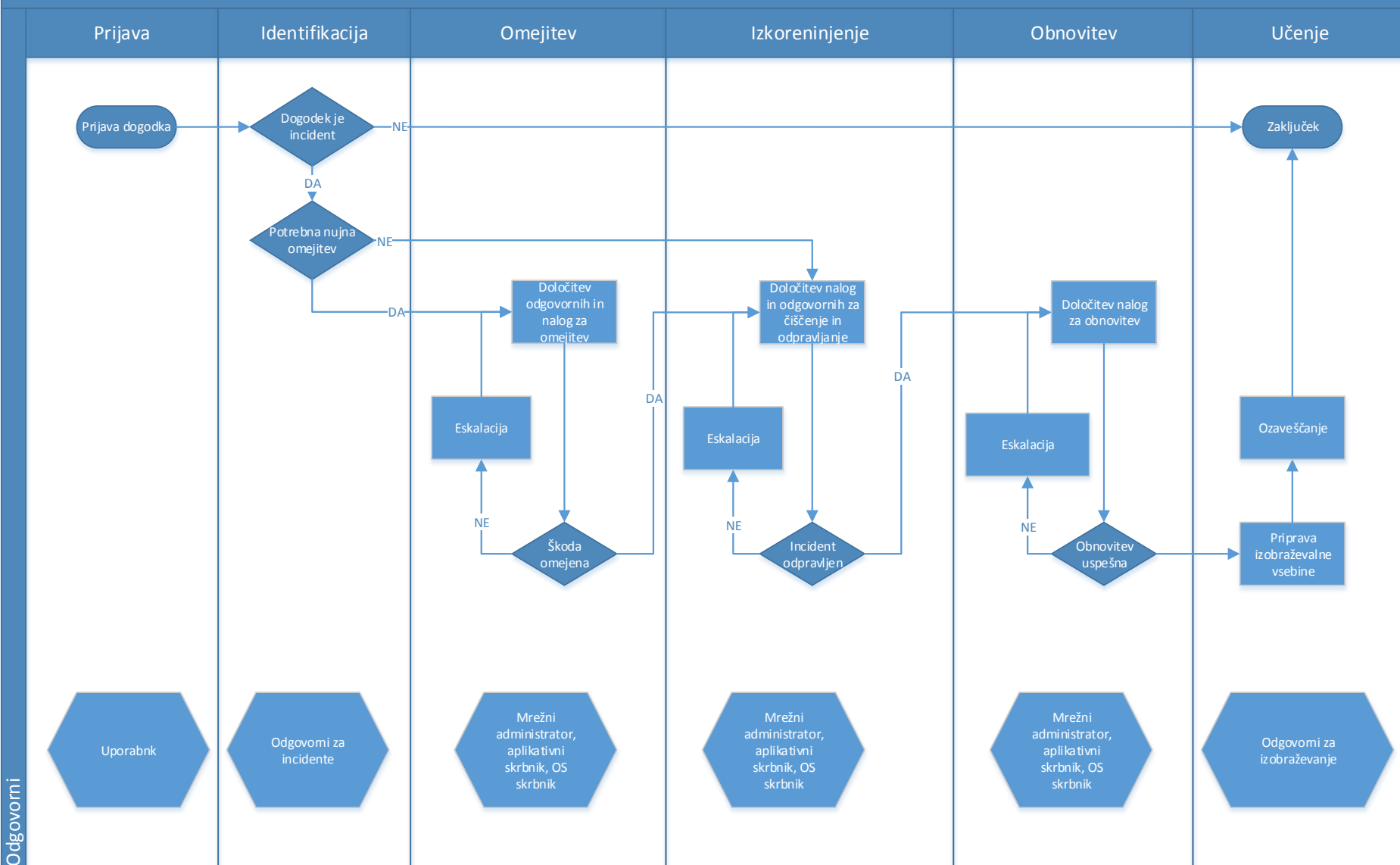
Implementacija programske opreme v DRO

Odgovorni



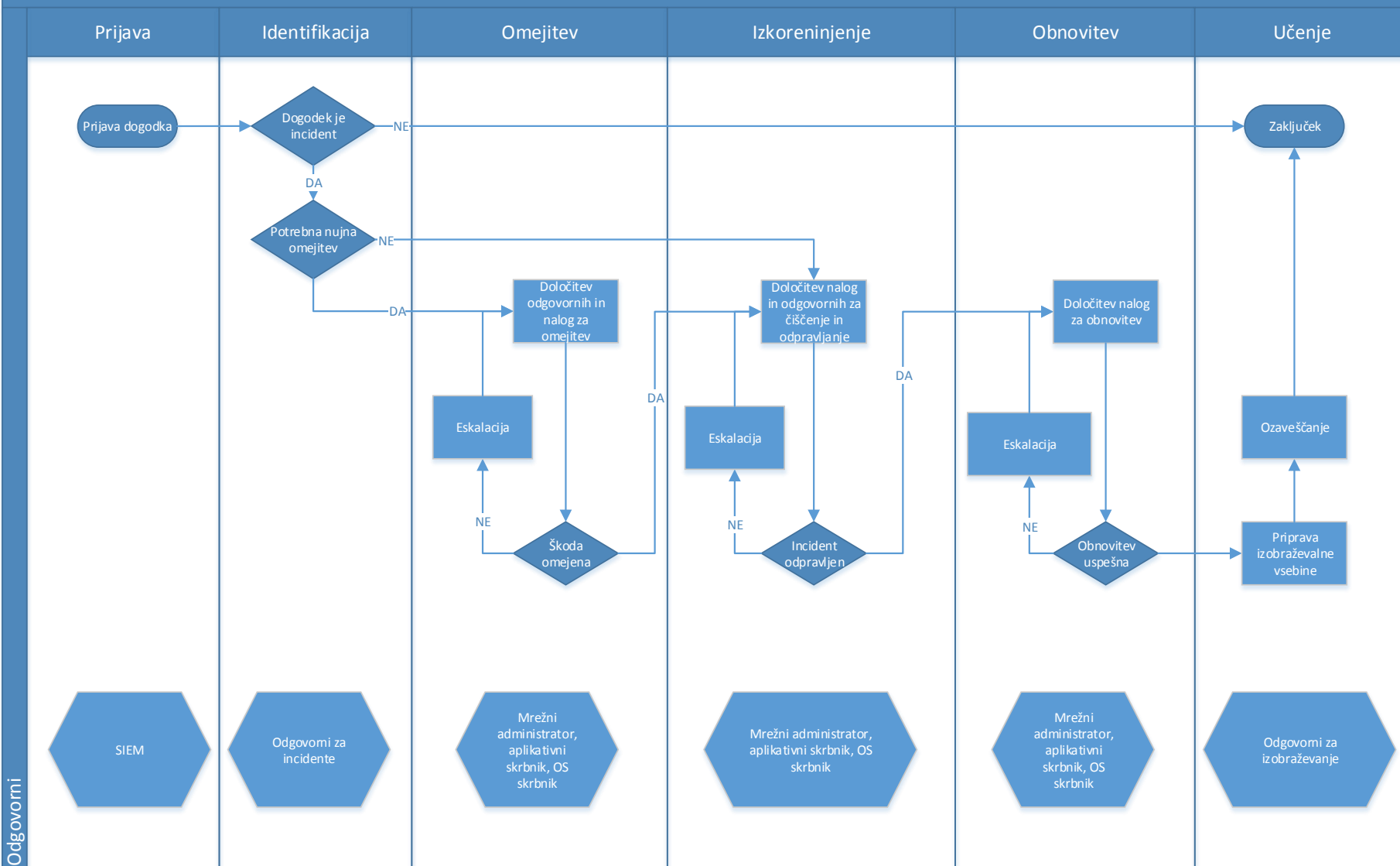


Prijava varnostnega dogodka

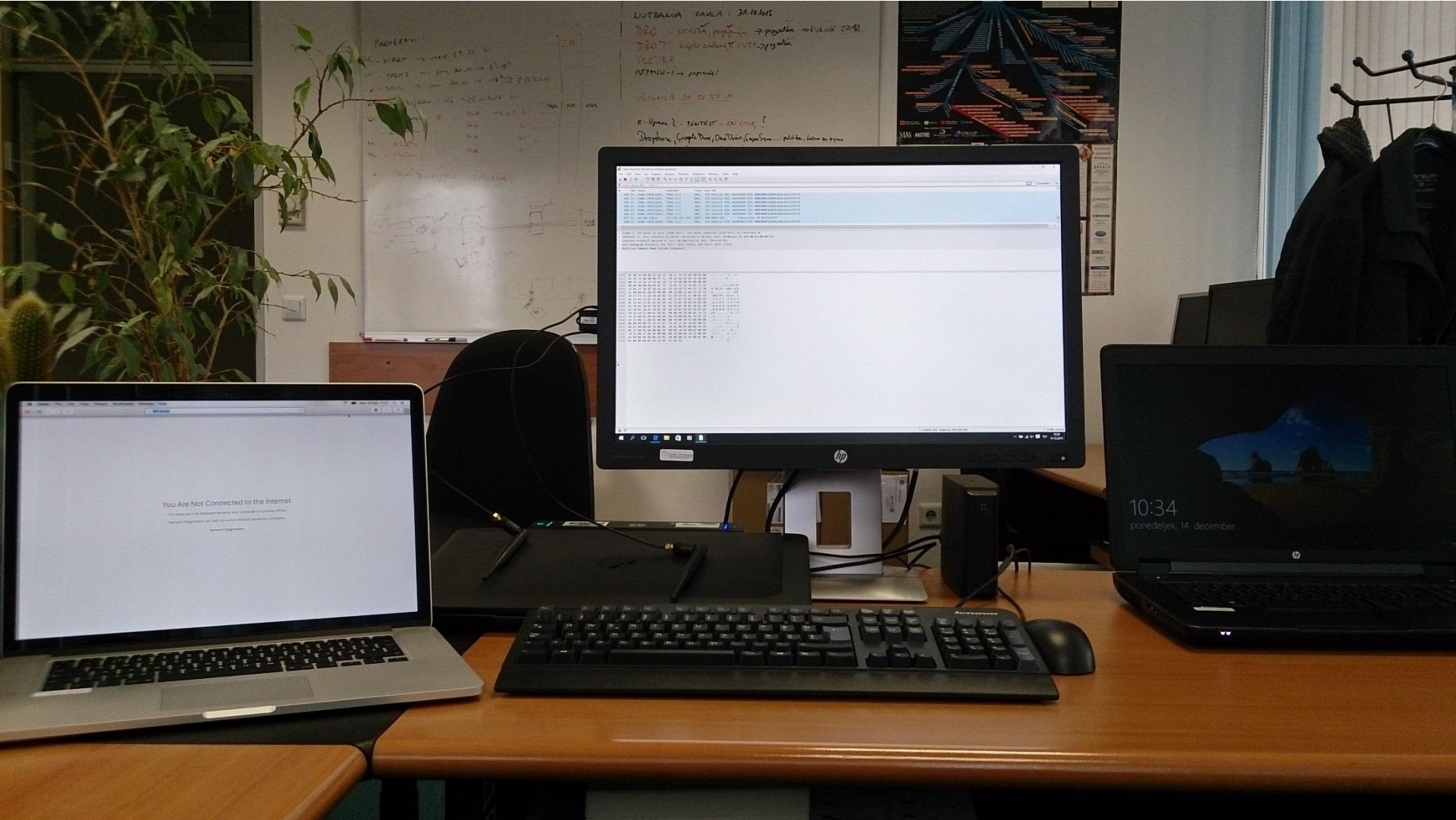




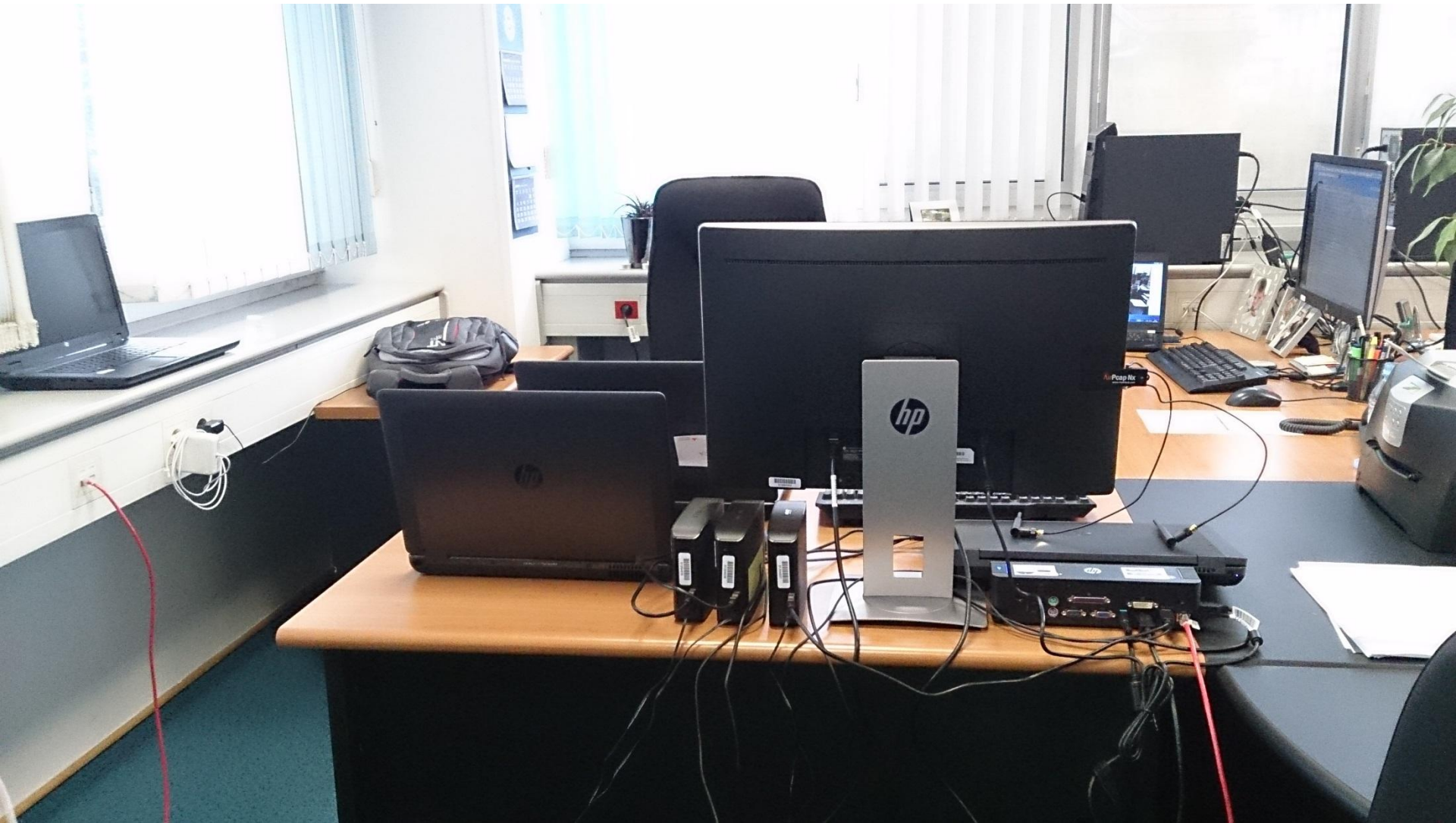
Samodejna prijava varnostnega dogodka iz SIEM sistema

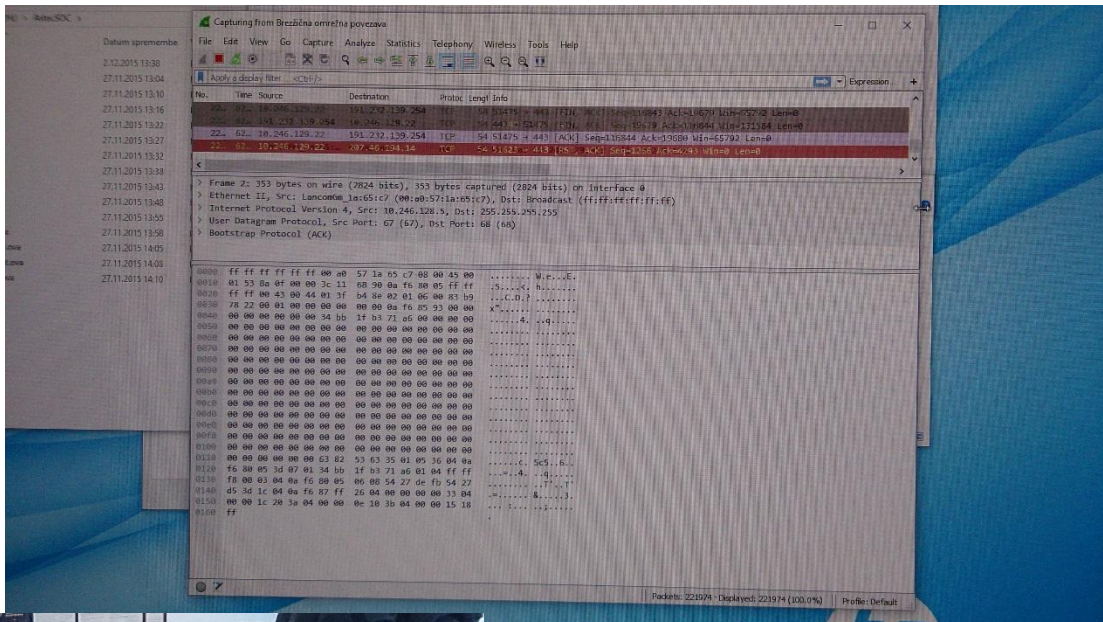
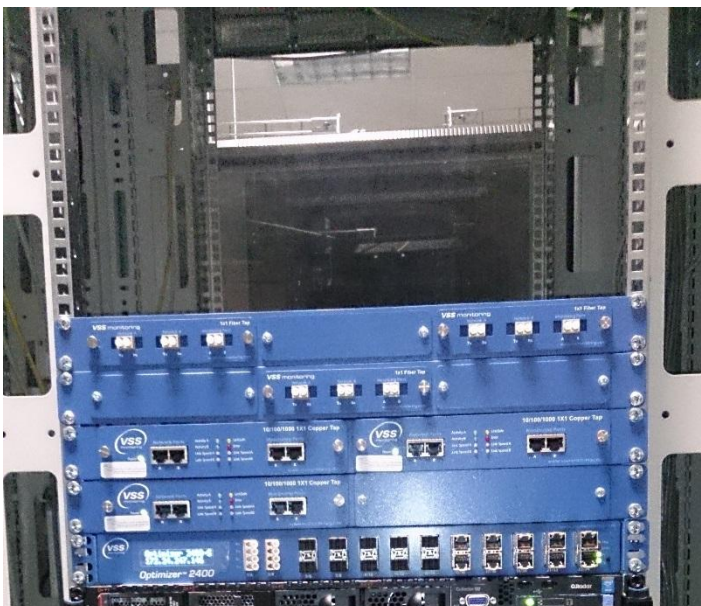


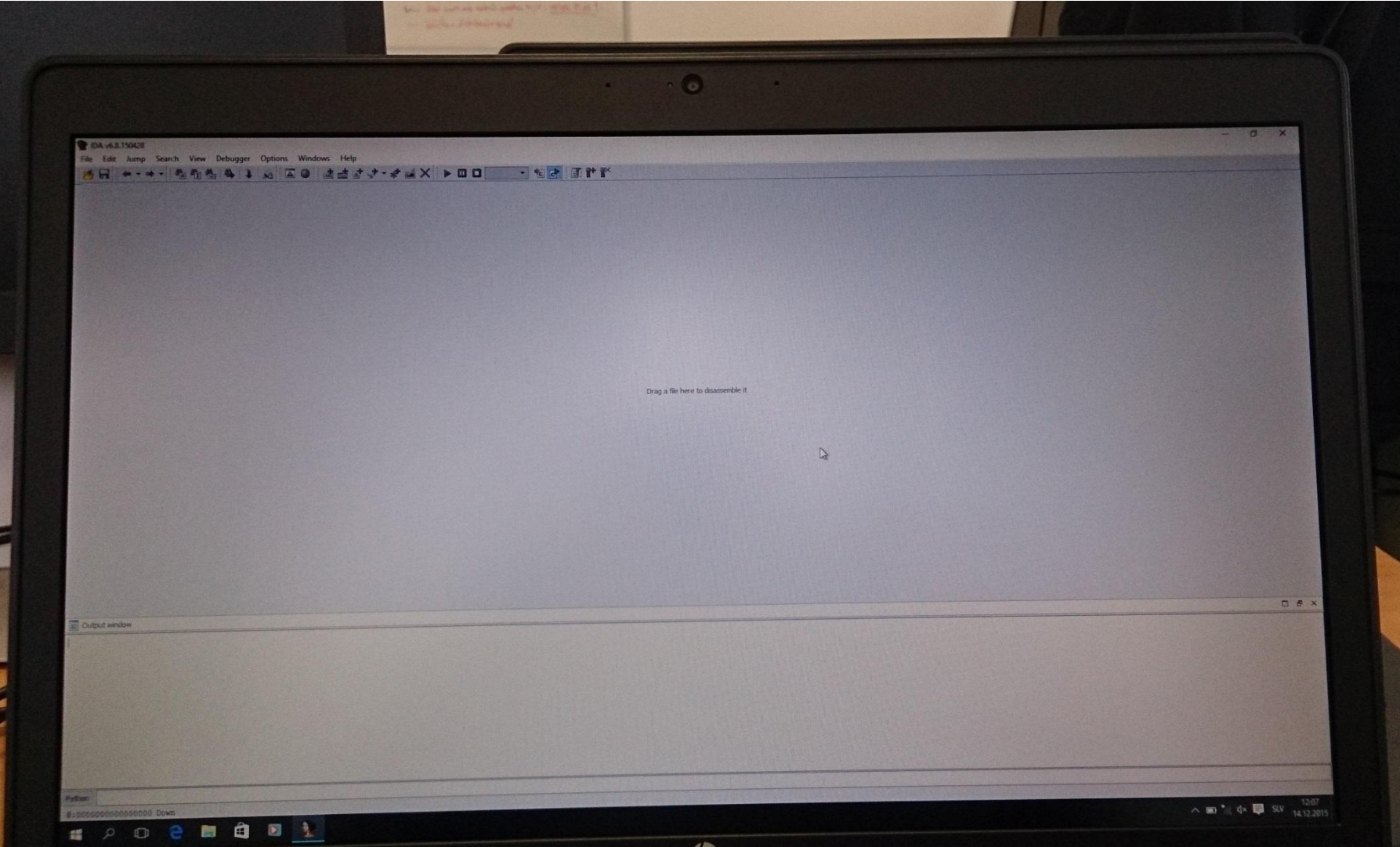


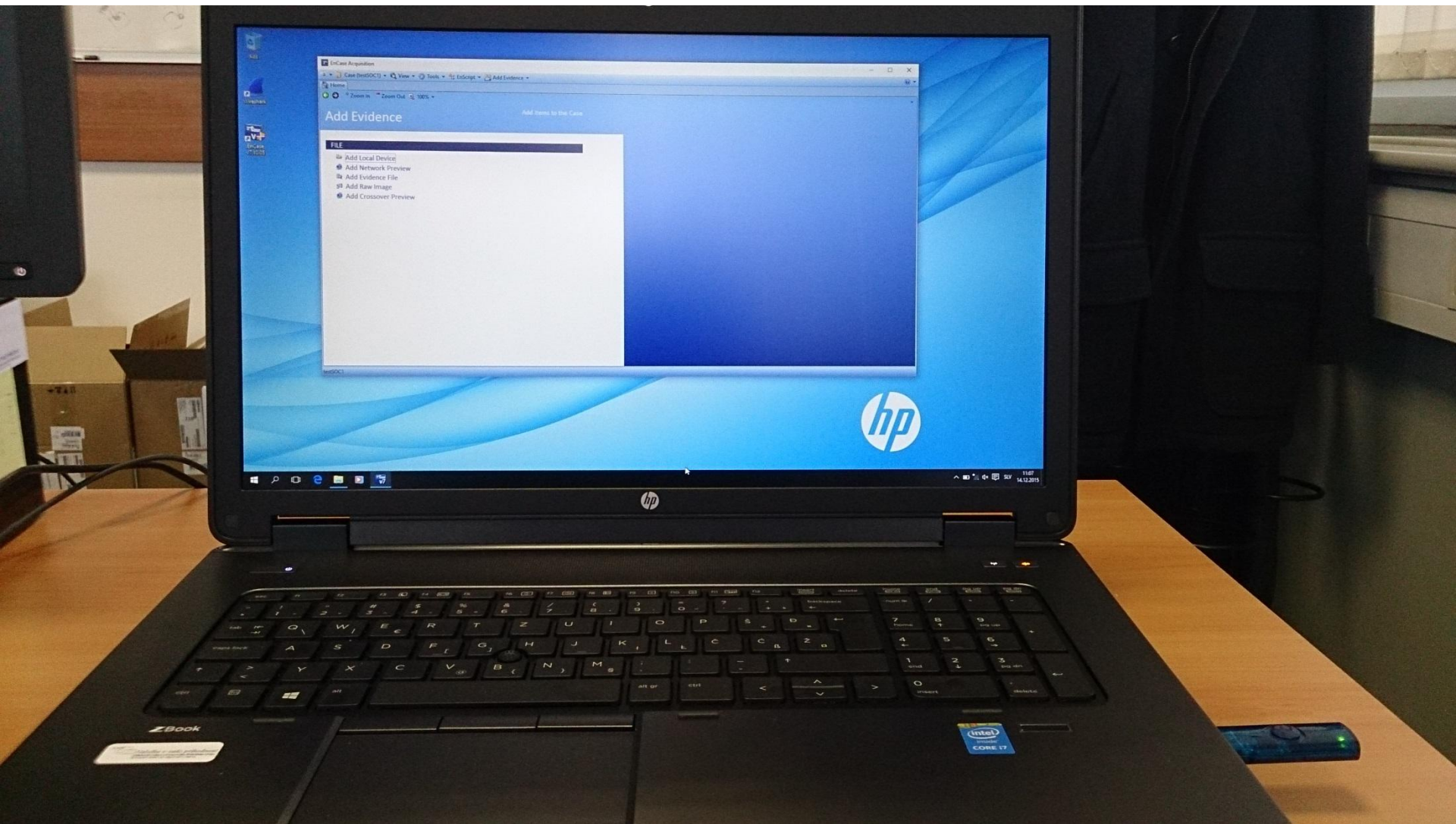


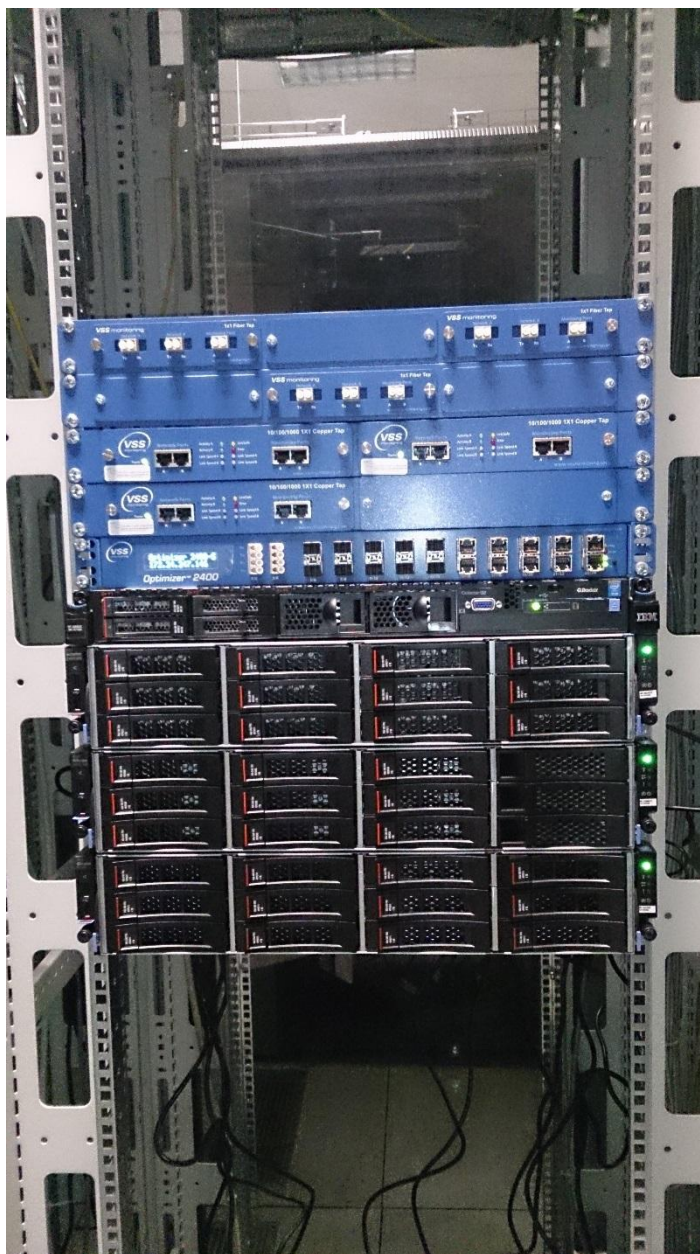














The screenshot displays a network traffic analysis tool interface with three overlapping windows showing file transfer details and directory listings.

Top Window: File Transfer Details

Destination	Protoc	Len	Info
H:\AstecSOC			

Middle Window: Directory Listing (AstecSOC)

Ime	Datum spremembe	Vrsta
Nova mapa	2.12.2015 13:38	Mapa z datotekami
SOC Burp 1.ova	27.11.2015 13:04	Datoteka OVA
SOC Burp 2.ova	27.11.2015 13:10	Datoteka OVA
SOC Canvas 1.ova	27.11.2015 13:16	Datoteka OVA
SOC Canvas 2.ova	27.11.2015 13:22	Datoteka OVA
SOC Kali 1.ova	27.11.2015 13:27	Datoteka OVA
SOC Kali 2.ova	27.11.2015 13:32	Datoteka OVA
SOC Kali 3.ova	27.11.2015 13:38	Datoteka OVA
SOC Kali 4.ova	27.11.2015 13:43	Datoteka OVA
SOC Kali 5.ova	27.11.2015 13:48	Datoteka OVA
SOC Moodle.ova	27.11.2015 13:55	Datoteka OVA
SOC Nessus - SC.ova	27.11.2015 13:58	Datoteka OVA
SOC NessusScanner.ova	27.11.2015 14:05	Datoteka OVA
SOC Poligon RedHat.ova	27.11.2015 14:08	Datoteka OVA
SOC Poligon SUSE.ova	27.11.2015 14:10	Datoteka OVA

Bottom Window: Directory Listing (CheckMarx)

Ime	Datum spremembe	Vrsta	Velikost
OVF1	27.11.2015 13:48	Mapa z datotekami	
Win2012CheckMarx.mf	27.11.2015 6:55	Datoteka MF	1 KB
Win2012CheckMarx.ovf	27.11.2015 6:46	Datoteka OVF	18 KB
Win2012CheckMarx-disk2.vmdk	27.11.2015 6:55	Datoteka VMDK	8.330.283 KB

Bottom Left: Hex Dump

```
00 0a f6 80 05 06 08 54 27 de fb 54 27 .....T...T
00 0a f6 87 ff 26 04 00 00 00 00 33 04 .-.....&....3.
20 3a 04 00 00 0e 10 3b 04 00 00 15 18 ...:.....;
```



Neposredni:

- enotna informacijska varnost v državni upravi: prihranek pri nabavi opreme in izvajanju storitev
- upoštevanje varnostnih standardov pri razvoju programske opreme.

Posredni:

- boljše odzivanje na varnostne grožnje in incidente
- večja ozaveščenost in obveščenost uporabnikov
- zmanjšanje varnostnih incidentov.

„Brez projekta“:

- večja varnostna tveganja, možnosti vdorov, odtekanja podatkov
- ogrožanje in onemogočanje državne infrastrukture in servisov.



Hvala za pozornost!

mag. Damijan Marinšek
damijan.marinsek@gov.si