GOSPODARSKO INTERESNO ZDRUŽENJE
DISTRIBUCIJE **ELEKTRIČNE ENERGIJE**

INFORMACIJSKE STORITVE IN INŽENIRING, D.O.O.
INFORMATIKA

8. STRATEŠKA KONFERENCA ELEKTRO-DISTRIBUCIJE

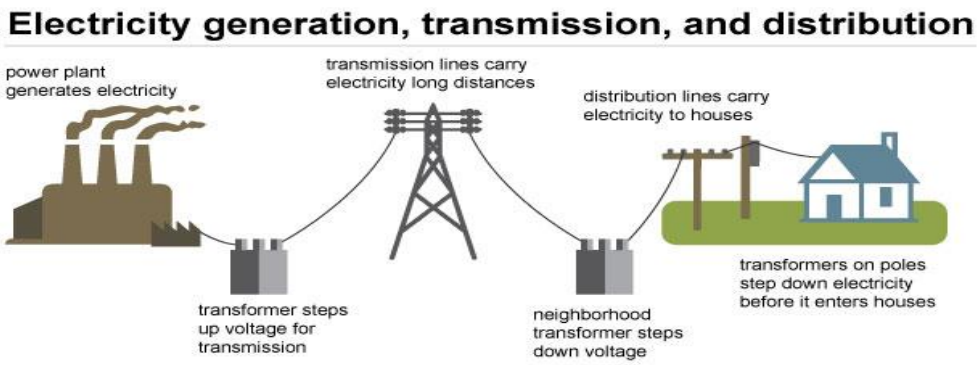
ZAGOTAVLJANJE KIBERNETSKE VARNOSTI – DELUJOČI VOC

GORAZD ROLIH, MAG.

NOVA GORICA, 3 APRIL 2024

VISOKO KRITIČNI SEKTORJI

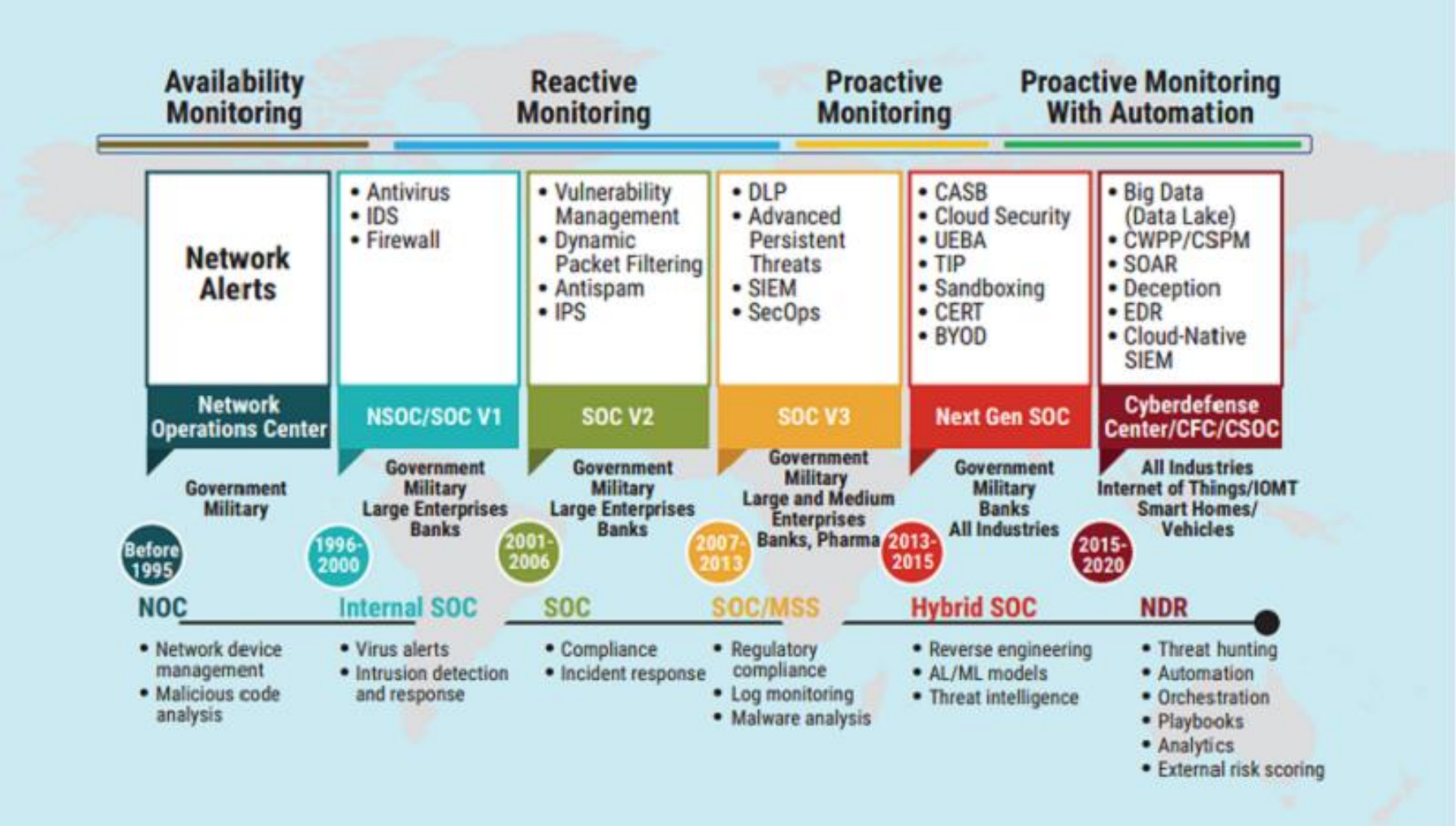
Sektor	Podsektor	Vrsta subjekta
1. Energija	(a) elektrika	—elektroenergetska podjetja, kot so opredeljena v členu 2, točka 57, Direktive (EU) 2019/944 Evropskega parlamenta in Sveta [1], ki opravljajo dejavnosti „dobave“, kot je opredeljena v členu 2, točka 12, navedene direktive
		—operaterji distribucijskega sistema, kot so opredeljeni v členu 2, točka 29, Direktive (EU) 2019/944
		—operaterji prenosnega sistema, kot so opredeljeni v členu 2, točka 35, Direktive (EU) 2019/944
		—proizvajalci, kot so opredeljeni v členu 2, točka 38, Direktive (EU) 2019/944
		—imenovani operaterji trga električne energije, kot so opredeljeni v členu 2, točka 8, Uredbe (EU) 2019/943 Evropskega parlamenta in Sveta [2]
		—udeleženci na trgu, kot so opredeljeni v členu 2, točka 25, Uredbe (EU) 2019/943, ki opravljajo storitve agregiranja, prilagajanja odjema ali shranjevanja energije, kot so opredeljeni v členu 2, točke 18, 20 in 59, Direktive (EU) 2019/944
		—upravljavci polnilnega mesta, odgovorni za upravljanje in delovanje polnilnega mesta, ki končnim uporabnikom zagotavlja storitev polnjenja, tudi v imenu in za račun ponudnika mobilnostnih storitev



Tveganja – kritična infrastruktura

- **Napadi z zlonamerno programsko opremo (fišing, ranljivosti, ransomware, kraja poverilnic, vdori, kraja podatkov)**
  - 25-odstotni letni porast ranljivosti (Skybox Security, 2023)
  - Ransomware prizadel 66 % anketirancev (Sophos, 2023)
  - Kiber-kriminal 2022 - 8,4BIO$, 2027 - 23BIO$, [300%] (techtarget.com, 2023)
- **Napadi na industrijske nadzorne sisteme OT, SCADA**
  - V zadnjih treh letih so kibernetski incidenti OT presegli skupno število poročano od let 1991 do 2000, od tega 39 % sektor energije (helpnetsecurity.com, 2023)
- **Napadi onemogočanja storitve (DoS) ali distribuiranega onemogočanja storitve (DDoS)**
  - Aktualno, napadi na spletne strani: Urad predsednice RS, RTV, Policija, HSE, Telekom Slovenije, Delo, Fraport, Krka, gov.si, Banka Slovenije …

Varnostno-operativni center - evolucija

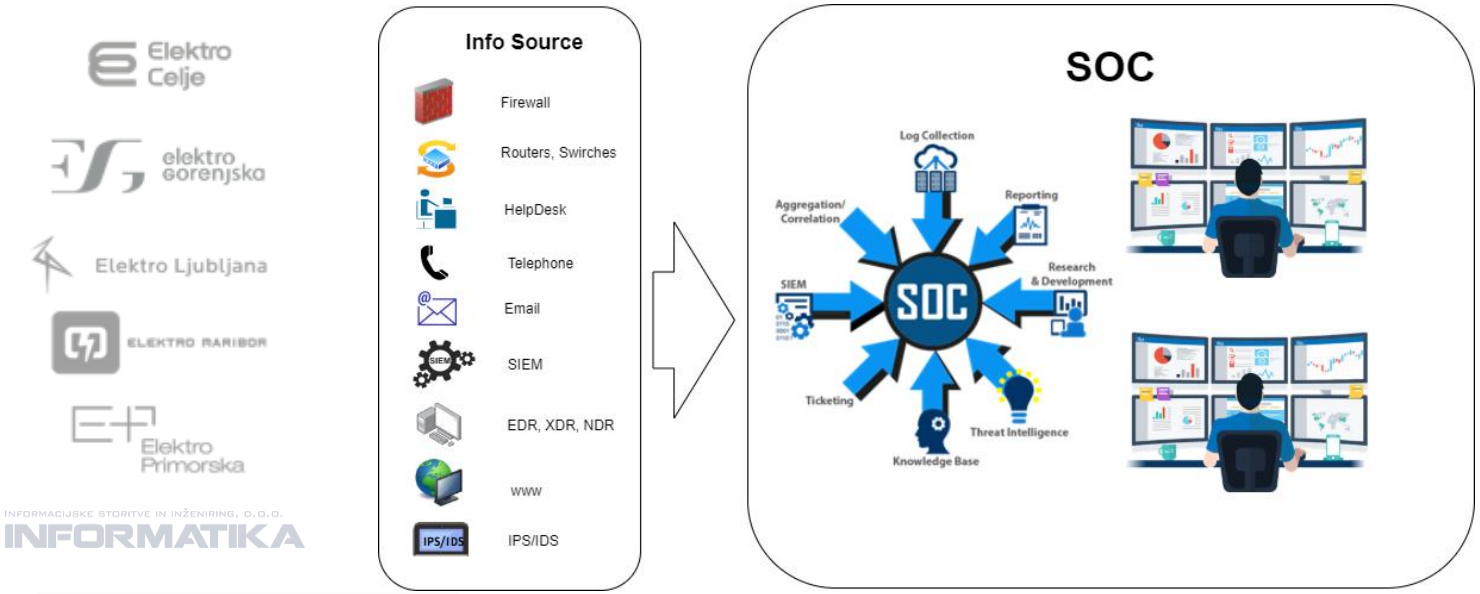


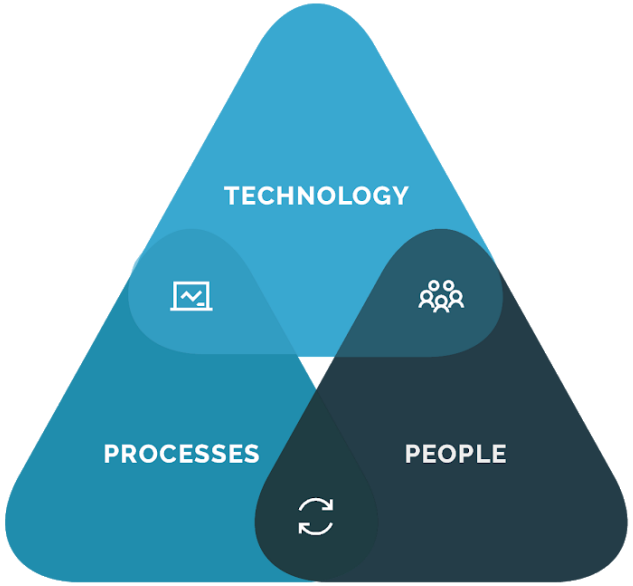
Vir: isaca.org

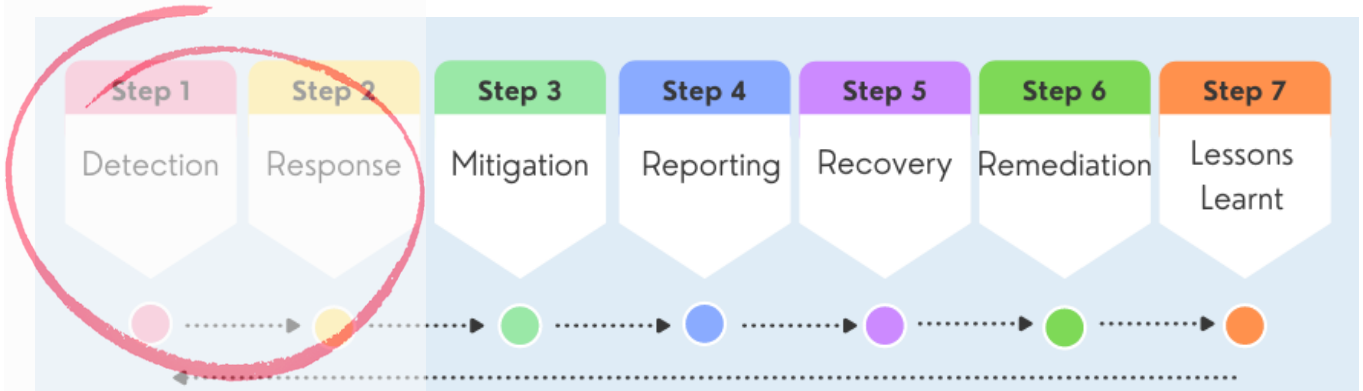
Varnostno-operativni center - naloge

- VOC spremlja in varuje sredstva organizacije (intelektualna lastnina, zaupni podatki, poslovni sistemi in ugled blagovne znamke) pred kibernetskimi grožnjami
- VOC so oči in ušesa organizacije, ki sprožajo alarme ob sumljivih ali nenormalnih dogodkih v kibernetskem prostoru ter omogočajo hitro odzivanje za zmanjšanje vpliva na organizacijo

Varnostno-operativni center - CyOPS

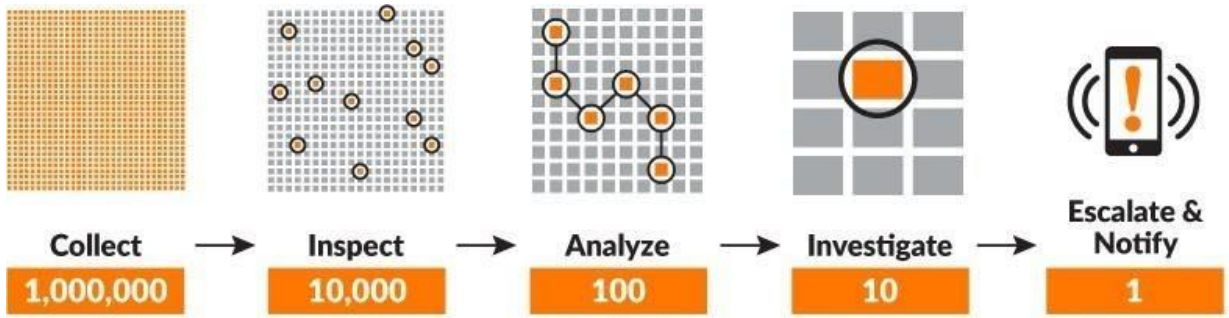






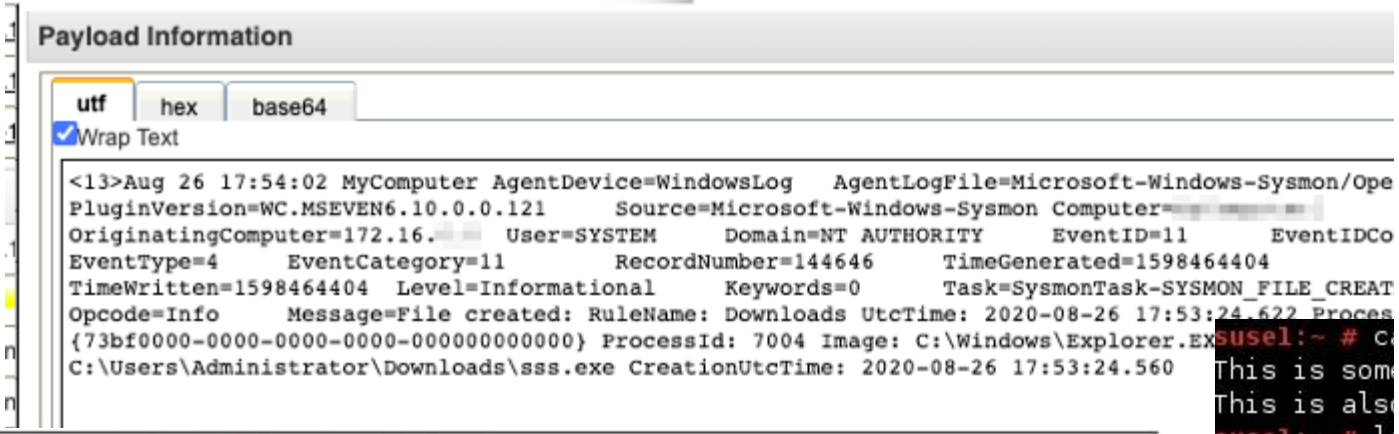
Varnostno-operativni center – analiza incidentov

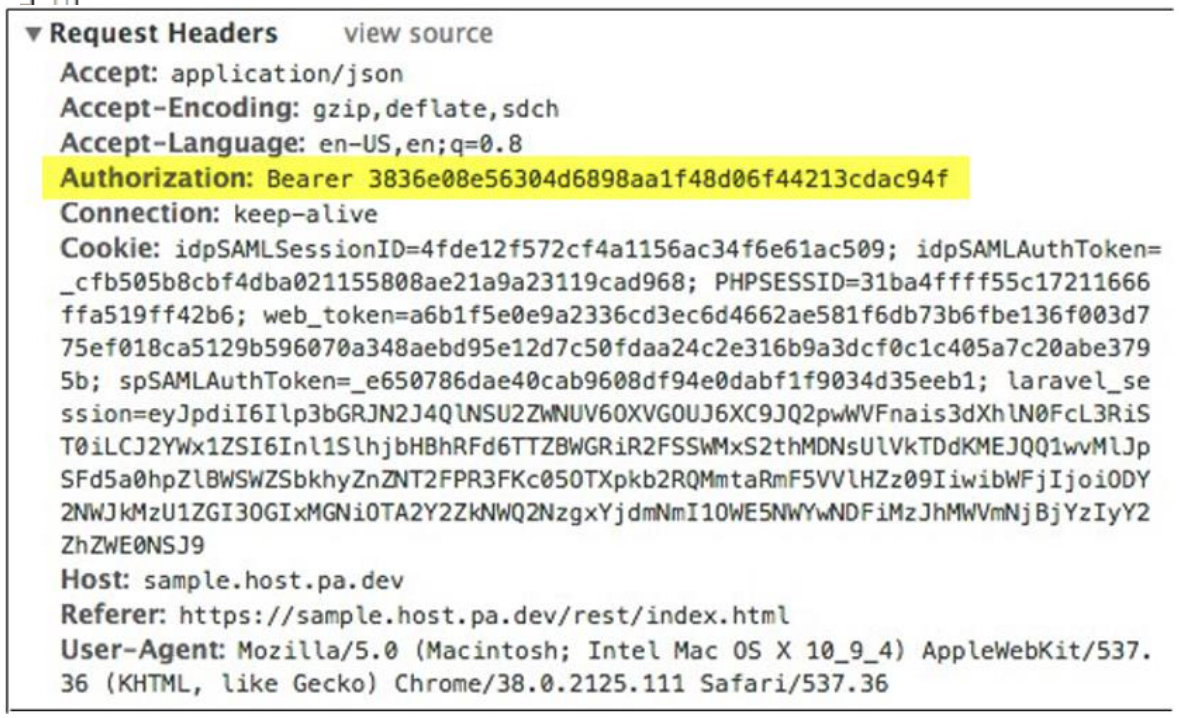
Št. Dogodkov (letno)	Št. kibernetski dogodki	Št. potencialnih incidentov
XXXXXXXX	XXX	X



xx% FP

INFORMATIKA






```
factory = kmldom.KmlFactory_GetFactory()
document = factory.CreateDocument()

for couchsurfer in COUCHSURFERS:
  social_capital_normalized = couchsurfer.social_capital()/normalization_val
  placemark = factory.CreatePlacemark()
  placemark.set_name(couchsurfer.id)
  coordinates = factory.CreateCoordinates()
  coordinates.add_latlngalt(couchsurfer.lat, couchsurfer.lng, 0)
  coordinates.add_latlngalt(couchsurfer.lat, couchsurfer.lng,
                            social_capital_normalized)
  linestring = factory.CreateLineString()
  linestring.set_altitudemode(1)  # Above sea level (absolute)
  linestring.set_tessellate(True)
  linestring.set_coordinates(coordinates)
  placemark.set_geometry(linestring)
  if social_capital_normalized < .333:
    placemark.set_styleurl('#Style1')
  elif social_capital_normalized < .666:
    placemark.set_styleurl('#Style2')
  else:
    placemark.set_styleurl('#Style3')
  document.add_feature(placemark)
kml = factory.CreateKml()
kml.set_feature(document)
print kmldom.SerializePretty(kml)
```

```
susel:~ # c
This is som
This is als
susel:~ # l
susel:~ # tail /var/log/messages
Nov  5 19:47:40 susel dhcpcd[3022]: eth0: leased 192.168.198.128 for 1800 second
s
Nov  5 19:47:40 susel dhcpcd[3022]: eth0: adding IP address 192.168.198.128/24
Nov  5 19:47:40 susel dhcpcd[3022]: eth0: adding default route via 192.168.198.2
 metric 0
Nov  5 19:47:40 susel ifup:     eth0      device: Intel Corporation 82545EM Giga
bit Ethernet Controller (Copper) (rev 01)
Nov  5 19:47:40 susel SuSEfirewall2: SuSEfirewall2 not active
Nov  5 19:55:28 susel root: This is a log message
Nov  5 19:57:45 susel root[22392]: This is another log message.
Nov  5 19:58:12 susel syslog-ng[1320]: Log statistics; dropped='pipe(/dev/xconso
le)=0', dropped='pipe(/dev/tty10)=0', processed='center(queued)=991', processed=
'center(received)=536', processed='destination(messages)=506', processed='destin
ation(mailinfo)=2', processed='destination(mailwarn)=0', processed='destination(
localmessages)=117', processed='destination(newserr)=0', processed='destination(
mailerr)=0', processed='destination(netmgm)=0', processed='destination(warn)=170
', processed='destination(console)=83', processed='destination(null)=10', proces
sed='destination(mail)=2', processed='destination(xconsole)=83', processed='dest
ination(firewall)=0', processed='destination(acpid)=18', processed='destination(
newscrit)=0', processed='destination(newsnotice)=0', processed='source(src)=536'
Nov  5 20:01:53 susel logger: This is some text.
Nov  5 20:01:53 susel logger: This is also some text.
```

VOC Informatika – QUO VADIS?

- Razvoj VOC
  - Zakonodaja, standardi dobre prakse (ZInfV, NOKI, NCCS, ISO, NIST …)
  - Napredne, proaktivne zmogljivosti, orodja in metode (AI, ML, TI, TH, CTI, SOAR, UBA …)
  - Projekti (nacionalni, Horizon, Digital Europe)

- Izgradnja CSIRT in VOC elektro-energetike
  - Konsolidacija virov in obstoječih zmogljivosti
  - Specifika energetike
  - Hitrejše zgodnje opozarjanje, opozorila, obvestila in deljenje informacij
  - Neposredna koordinacija in centralizirano obvladovanje tveganj in kolaboracija deležnikov energetike
  - Enotna vstopna točka, enoten protokol obveščanja, poročanja, enotna evidence
  - Skladnost z zakonodajo

GOSPODARSKO INTERESNO ZDRUŽENJE
DISTRIBUCIJE **ELEKTRIČNE ENERGIJE**

INFORMACIJSKE STORITVE IN INŽENIRING, D.O.O.
INFORMATIKA

INFORMATIKA d.o.o.
Vetrinjska ulica 2 | 2000 Maribor | Slovenia
T: +386 2 707 10 00
E-mail: info@informatika.si
www.informatika.si

GORAZD.ROLIH@INFORMATIKA.SI