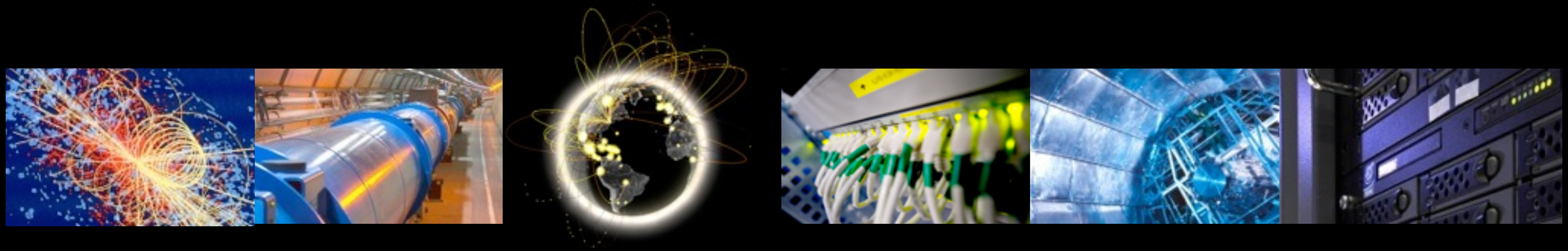
WLCG Security
Intro, Status, Challenges



Jose.Carlos.Luna@cern.ch
WLCG Security Officer

2025.02.11

Intro - CERN

CERN Computer Security

- Local security operations
  - Security reviews, incident response, threat intelligence, …

WLCG Security

- Policies (endorsed by the Management Board)
  - Some probably outdated and need review
- Recommendations, awareness, …
- Coordination and Incident Response
- Oversee major changes (eg: tokens, federated identities…)

EGI IRTF

- Incident Response
- Vulnerability evaluation and tracking
- Policies and procedures

Jose Carlos Luna

jose.carlos.luna@cern.ch

WLCG Security Officer

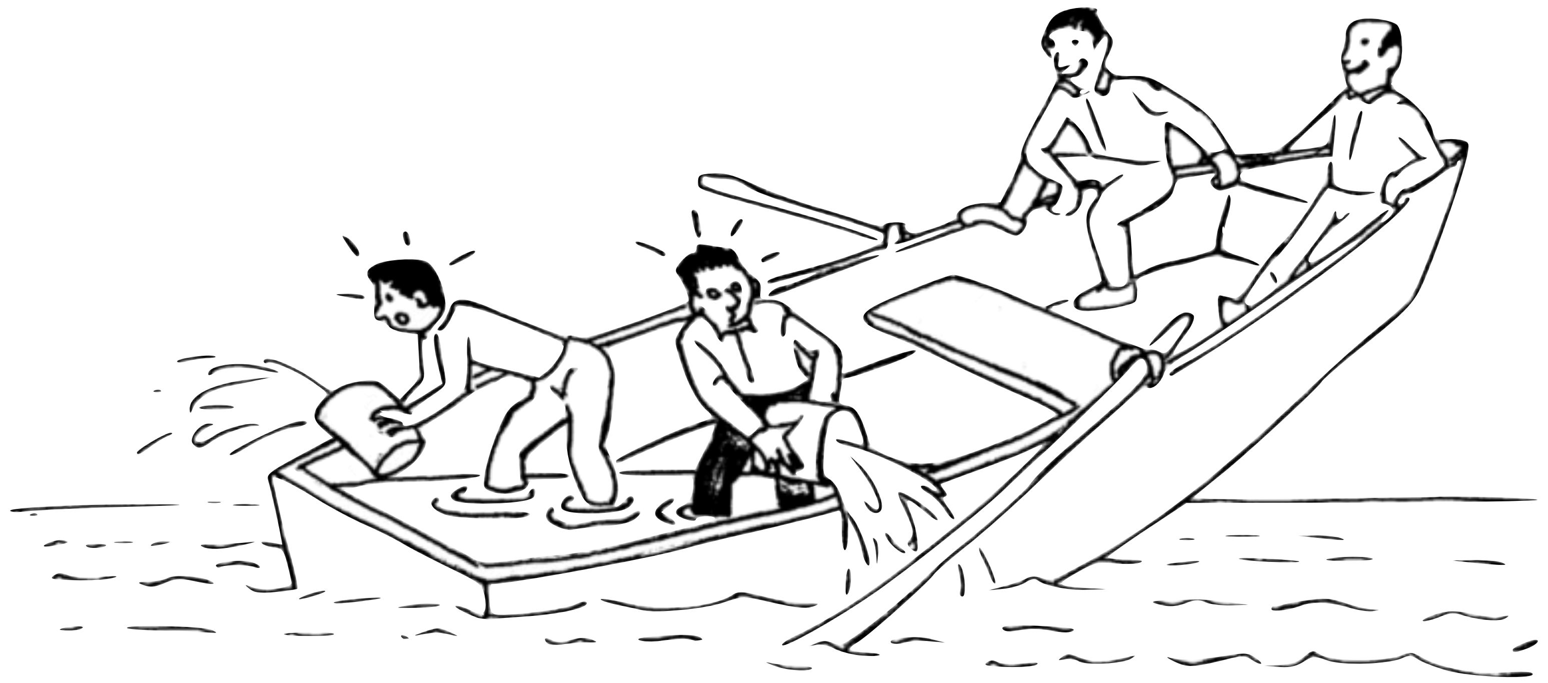
Pau Cutrina

pau.cutrina@cern.ch

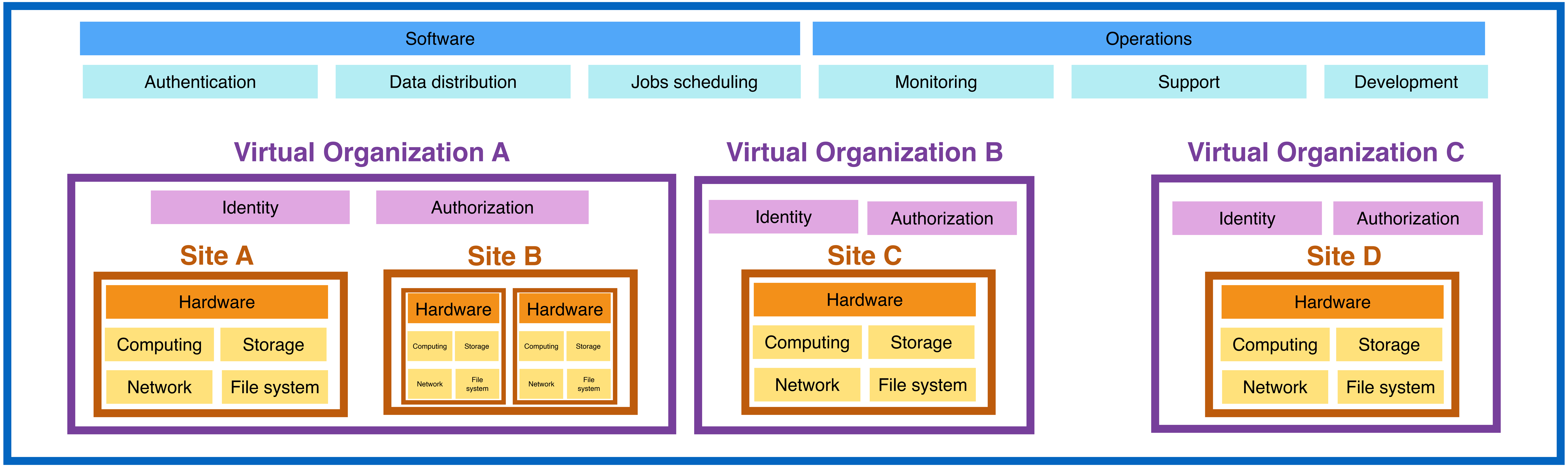
EGI IRTF Lead

Security model - WLCG

- Layered based model
  - Grid infrastructure
    - Resources are **shared**, so connected
    - Security teams at different levels



WLCG (EGI+OSG)



WLCG	World LHC Computing Grid
EGI	European Grid Infrastructure
OSG	Open Science Grid

https://twiki.cern.ch/twiki/bin/view/LCG/WLCGOperationsWeb; https://wlcg-public.web.cern.ch/

Recent Incidents and Threats

- Identity
  - Stolen and lost credentials (frequent!)
    - Malware in employee machines, infostealers
    - Password reuse (database dump breaches are very prevalent today)
    - Infected infrastructure
    - Publicly exposing credentials in software repositories and public pages
      - Or unprotected ssh keys
    - Simply asking “illegitimately” for VO resources (curiosity vs malicious)
    - Towards 2FA as a mitigation for many of these!

Recent Incidents and Threats

- Vulnerabilities
  - Eg: Recent site compromised late (still being recovered)
    - End goal: Cryptomining (using your CPU resources for financial gain)
    - Entry: default credentials on BMC, and then lateral movement: attackers had months
      - Please report asap!
  - Common vulnerabilities and misconfigurations.
    - Or custom code not following best practices
  - Malware and BYOD
  - Supply chain (infected code repositories)

What to do?

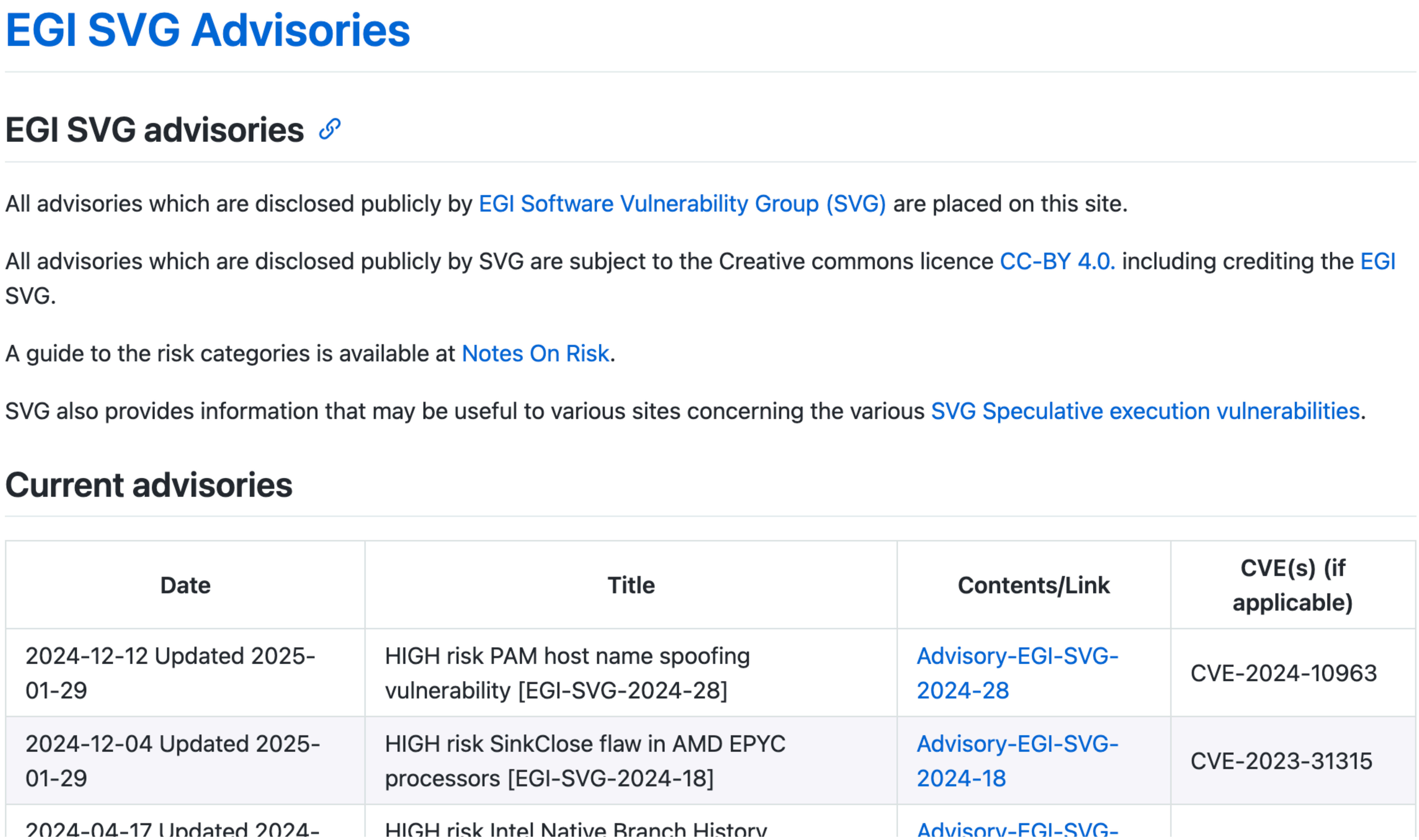
- Prevention
- Detection
- Awareness and Education
- Incident response readiness
  - Everyone has incidents: be ready!

Grid Incident Response

- You are not alone! Local security, VOs, EGI and OSG + CERN security
- EGI Policies and Procedures
  - https://confluence.egi.eu/display/EGIPP/SEC01+EGI+CSIRT+Security+Incident+Handling+Procedure
  - How to improve site suspension workflow for security reasons under discussion
- OSG Policies and procedures
  - https://osg-htc.org/security/IncidentDiscoveryReporting
  - First local security teams and contact OSG if anything that could impact OSG/VOs/other sites or if the incident is suspected to originate from OSG infrastructure/jobs
- Identity blocking happens at the VO level
- If lost: Computer.Security@cern.ch

Initiatives: Detection & Prevention

- EGI Security Advisories
  - https://advisories.egi.eu



EGI SVG Advisories

EGI SVG advisories

All advisories which are disclosed publicly by EGI Software Vulnerability Group (SVG) are placed on this site.

All advisories which are disclosed publicly by SVG are subject to the Creative commons licence CC-BY 4.0. including crediting the EGI SVG.

A guide to the risk categories is available at Notes On Risk.

SVG also provides information that may be useful to various sites concerning the various SVG Speculative execution vulnerabilities.

Current advisories

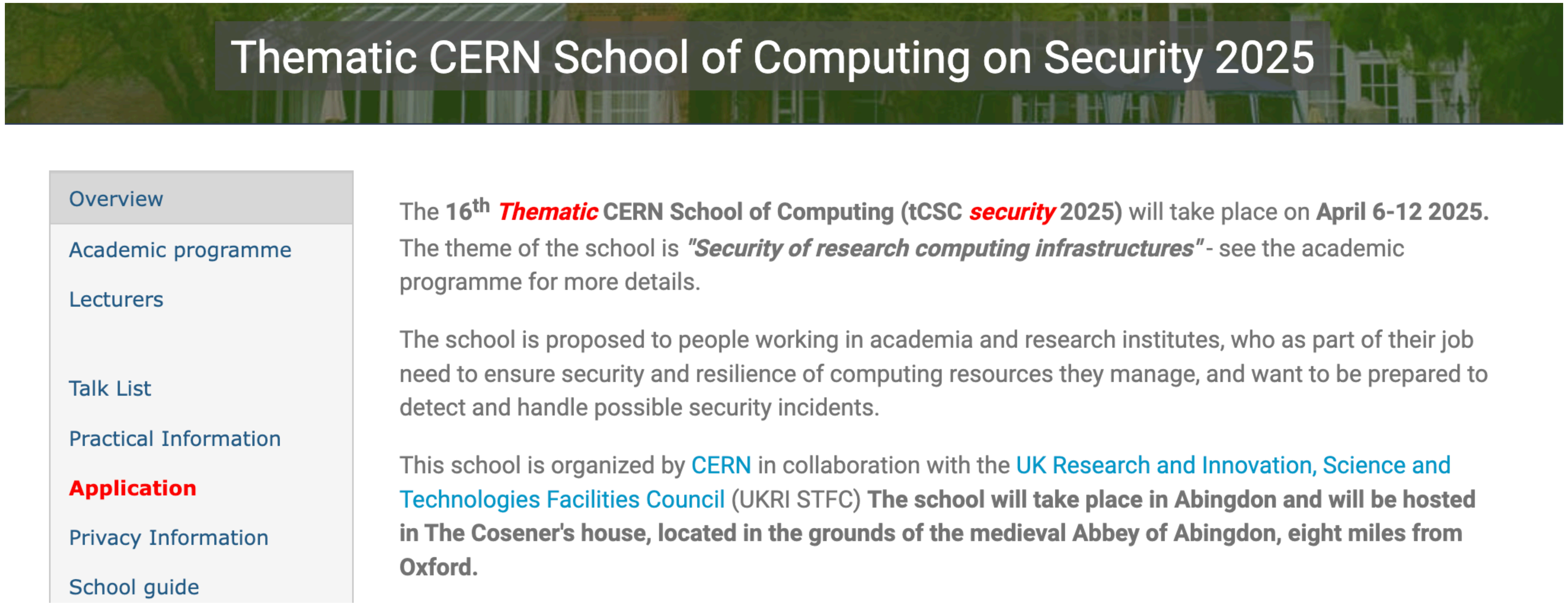
Date	Title	Contents/Link	CVE(s) (if applicable)
2024-12-12 Updated 2025-01-29	HIGH risk PAM host name spoofing vulnerability [EGI-SVG-2024-28]	Advisory-EGI-SVG-2024-28	CVE-2024-10963
2024-12-04 Updated 2025-01-29	HIGH risk SinkClose flaw in AMD EPYC processors [EGI-SVG-2024-18]	Advisory-EGI-SVG-2024-18	CVE-2023-31315
2024-04-17 Updated 2024-	HIGH risk Intel Native Branch History	Advisory-EGI-SVG-	

Initiatives: Detection & Prevention

- EGI Security Advisories
  - https://advisories.egi.eu
- EGI communication challenge
  - Important! Keep security contacts up-to-date. Essential for incident coordination.
- And more: https://csirt.egi.eu/activities/

Initiatives: Detection & Prevention

- Workshops & hands on
  - CERN School of Computing on security
    - https://indico.cern.ch/e/sCSC2025 (inscriptions closed)



Thematic CERN School of Computing on Security 2025

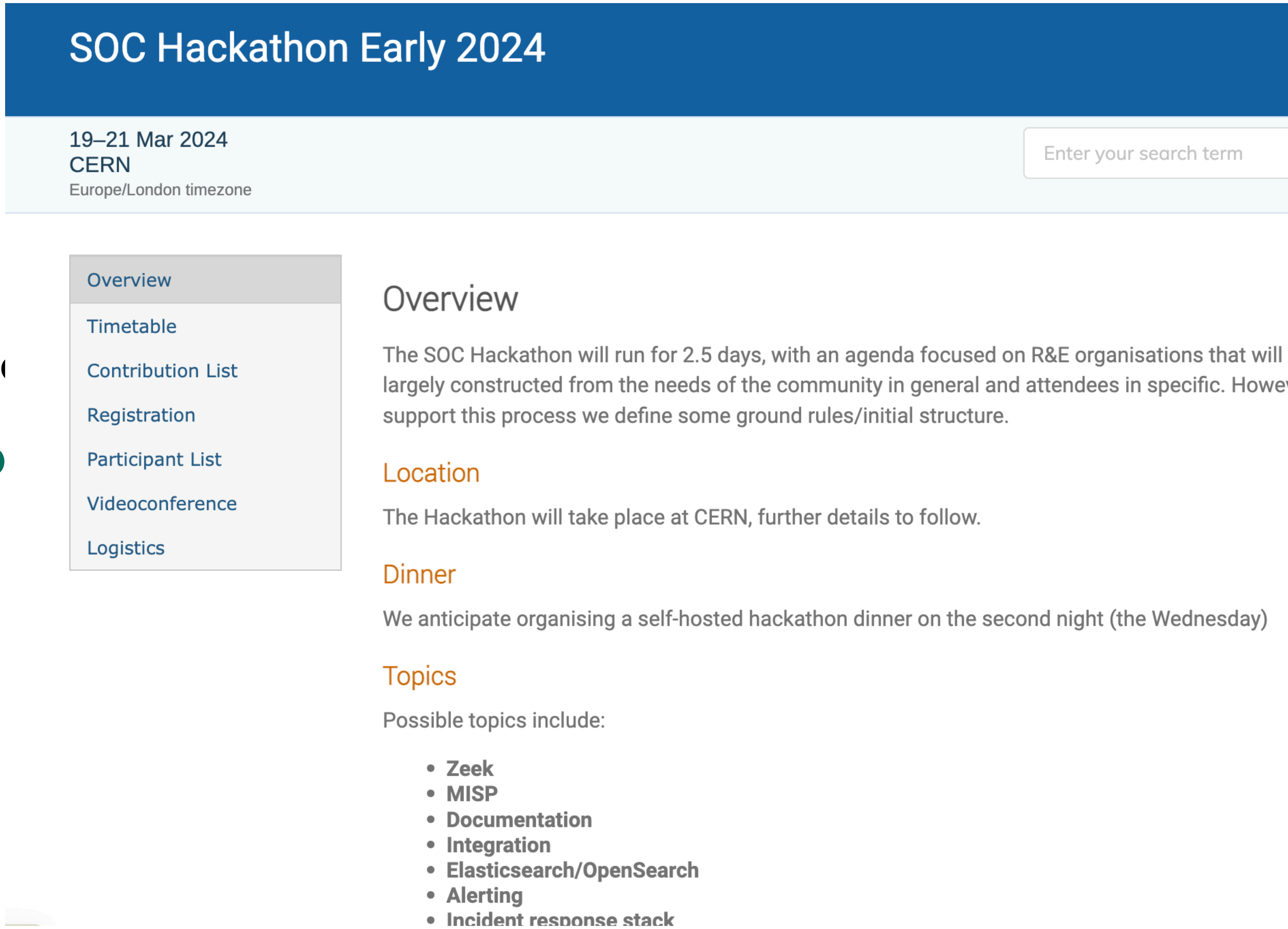
The 16th ***Thematic*** **CERN School of Computing (tCSC *security* 2025)** will take place on **April 6-12 2025.** The theme of the school is ***"Security of research computing infrastructures"*** - see the academic programme for more details.

The school is proposed to people working in academia and research institutes, who as part of their job need to ensure security and resilience of computing resources they manage, and want to be prepared to detect and handle possible security incidents.

This school is organized by CERN in collaboration with the UK Research and Innovation, Science and Technologies Facilities Council (UKRI STFC) **The school will take place in Abingdon and will be hosted in The Cosener's house, located in the grounds of the medieval Abbey of Abingdon, eight miles from Oxford.**

Initiatives: Detection & Prevention

- Workshops & hands on
  - CERN School of Computing on security
    - https://indico.cern.ch/e/sCSC2025 (inscripti
  - Security Operation Center working group
    - https://wlcg-soc-wg-doc.web.cern.ch
    - SOC hackathon on 19-21 March @CERN
      - https://indico.cern.ch/events/1370544



SOC Hackathon Early 2024

19–21 Mar 2024
CERN
Europe/London timezone

Overview

The SOC Hackathon will run for 2.5 days, with an agenda focused on R&E organisations that will largely constructed from the needs of the community in general and attendees in specific. Howe support this process we define some ground rules/initial structure.

Location

The Hackathon will take place at CERN, further details to follow.

Dinner

We anticipate organising a self-hosted hackathon dinner on the second night (the Wednesday)

Topics

Possible topics include:

- **Zeek**
- **MISP**
- **Documentation**
- **Integration**
- **Elasticsearch/OpenSearch**
- **Alerting**
- **Incident response stack**

Initiatives: Incident Response

- Workshop & hands on
  - Forensics and incident response workshop (September 2025 @CERN)
    - Still preparing: https://indico.cern.ch/e/1479123
    - Subscribe for info:
      - https://e-groups.cern.ch/e-groups/EgroupsSubscription.do?egroupName=security-workshop25
-

Initiatives: Incident Response

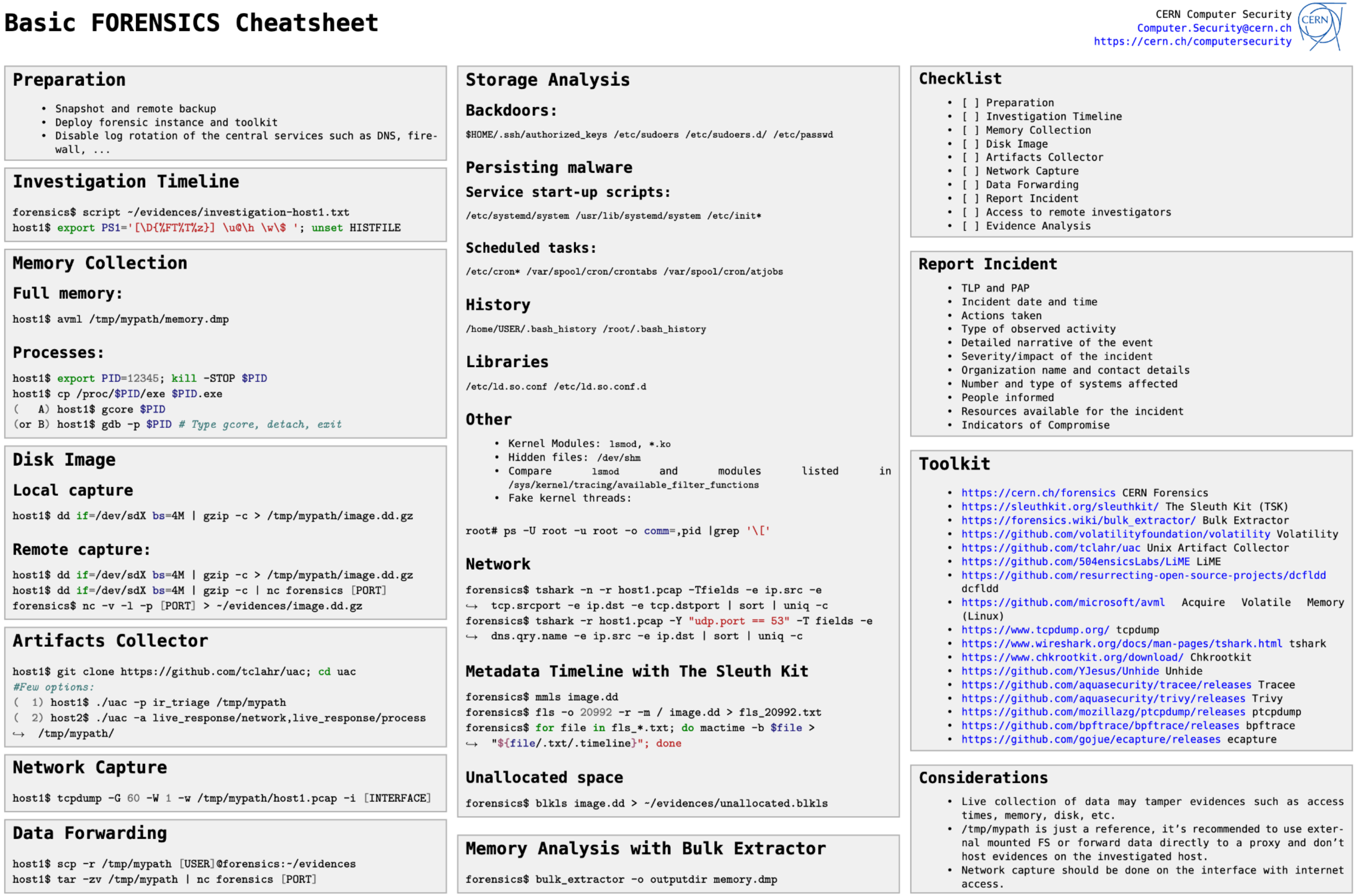
- Workshop & hands on
  - Forensics and incident response workshop (September 2025 @CERN)
    - Still preparing: https://indico.cern.ch/e/1479123
    - Subscribe for info:
      - https://e-groups.cern.ch/e-groups/EgroupsSubscription.do?egroupName=security-workshop25

- Blueprints and toolkits
  - Forensics Cheatsheet & toolkit
    - investigation on the early stages of an incident
  - https://cern.ch/forensics

Initiatives: Incident Response

- Workshop & hands on
  - – Forensics and incident res
    - Still preparing: https://indic
    - Subscribe for info:
      - –https://e-groups.cern.ch/e-

- Blueprints and toolkits
  - – Forensics Cheatsheet & to
    - investigation on the early st
  - – https://cern.ch/forensics



Basic FORENSICS Cheatsheet

CERN Computer Security
Computer.Security@cern.ch
https://cern.ch/computersecurity

Preparation

- Snapshot and remote backup
- Deploy forensic instance and toolkit
- Disable log rotation of the central services such as DNS, firewall, ...

Investigation Timeline

```
forensics$ script ~/evidences/investigation-host1.txt
host1$ export PS1='[\D{%FT%T%z}] \u@\h \w\$ '; unset HISTFILE
```

Memory Collection

Full memory:

```
host1$ avml /tmp/mypath/memory.dmp
```

Processes:

```
host1$ export PID=12345; kill -STOP $PID
host1$ cp /proc/$PID/exe $PID.exe
(   A) host1$ gcore $PID
(or B) host1$ gdb -p $PID # Type gcore, detach, exit
```

Disk Image

Local capture

```
host1$ dd if=/dev/sdX bs=4M | gzip -c > /tmp/mypath/image.dd.gz
```

Remote capture:

```
host1$ dd if=/dev/sdX bs=4M | gzip -c > /tmp/mypath/image.dd.gz
host1$ dd if=/dev/sdX bs=4M | gzip -c | nc forensics [PORT]
forensics$ nc -v -l -p [PORT] > ~/evidences/image.dd.gz
```

Artifacts Collector

```
host1$ git clone https://github.com/tclahr/uac; cd uac
#Few options:
(  1) host1$ ./uac -p ir_triage /tmp/mypath
(  2) host2$ ./uac -a live_response/network,live_response/process
↪  /tmp/mypath/
```

Network Capture

```
host1$ tcpdump -G 60 -W 1 -w /tmp/mypath/host1.pcap -i [INTERFACE]
```

Data Forwarding

```
host1$ scp -r /tmp/mypath [USER]@forensics:~/evidences
host1$ tar -zv /tmp/mypath | nc forensics [PORT]
```

Storage Analysis

Backdoors:

```
$HOME/.ssh/authorized_keys /etc/sudoers /etc/sudoers.d/ /etc/passwd
```

Persisting malware

Service start-up scripts:

```
/etc/systemd/system /usr/lib/systemd/system /etc/init*
```

Scheduled tasks:

```
/etc/cron* /var/spool/cron/crontabs /var/spool/cron/atjobs
```

History

```
/home/USER/.bash_history /root/.bash_history
```

Libraries

```
/etc/ld.so.conf /etc/ld.so.conf.d
```

Other

- Kernel Modules: lsmod, *.ko
- Hidden files: /dev/shm
- Compare lsmod and modules listed in /sys/kernel/tracing/available_filter_functions
- Fake kernel threads:

```
root# ps -U root -u root -o comm=,pid |grep '\['
```

Network

```
forensics$ tshark -n -r host1.pcap -Tfields -e ip.src -e
↪  tcp.srcport -e ip.dst -e tcp.dstport | sort | uniq -c
forensics$ tshark -r host1.pcap -Y "udp.port == 53" -T fields -e
↪  dns.qry.name -e ip.src -e ip.dst | sort | uniq -c
```

Metadata Timeline with The Sleuth Kit

```
forensics$ mmls image.dd
forensics$ fls -o 20992 -r -m / image.dd > fls_20992.txt
forensics$ for file in fls_*.txt; do mactime -b $file >
↪  "${file/.txt/.timeline}"; done
```

Unallocated space

```
forensics$ blkls image.dd > ~/evidences/unallocated.blkls
```

Memory Analysis with Bulk Extractor

```
forensics$ bulk_extractor -o outputdir memory.dmp
```

Checklist

- [ ] Preparation
- [ ] Investigation Timeline
- [ ] Memory Collection
- [ ] Disk Image
- [ ] Artifacts Collector
- [ ] Network Capture
- [ ] Data Forwarding
- [ ] Report Incident
- [ ] Access to remote investigators
- [ ] Evidence Analysis

Report Incident

- TLP and PAP
- Incident date and time
- Actions taken
- Type of observed activity
- Detailed narrative of the event
- Severity/impact of the incident
- Organization name and contact details
- Number and type of systems affected
- People informed
- Resources available for the incident
- Indicators of Compromise

Toolkit

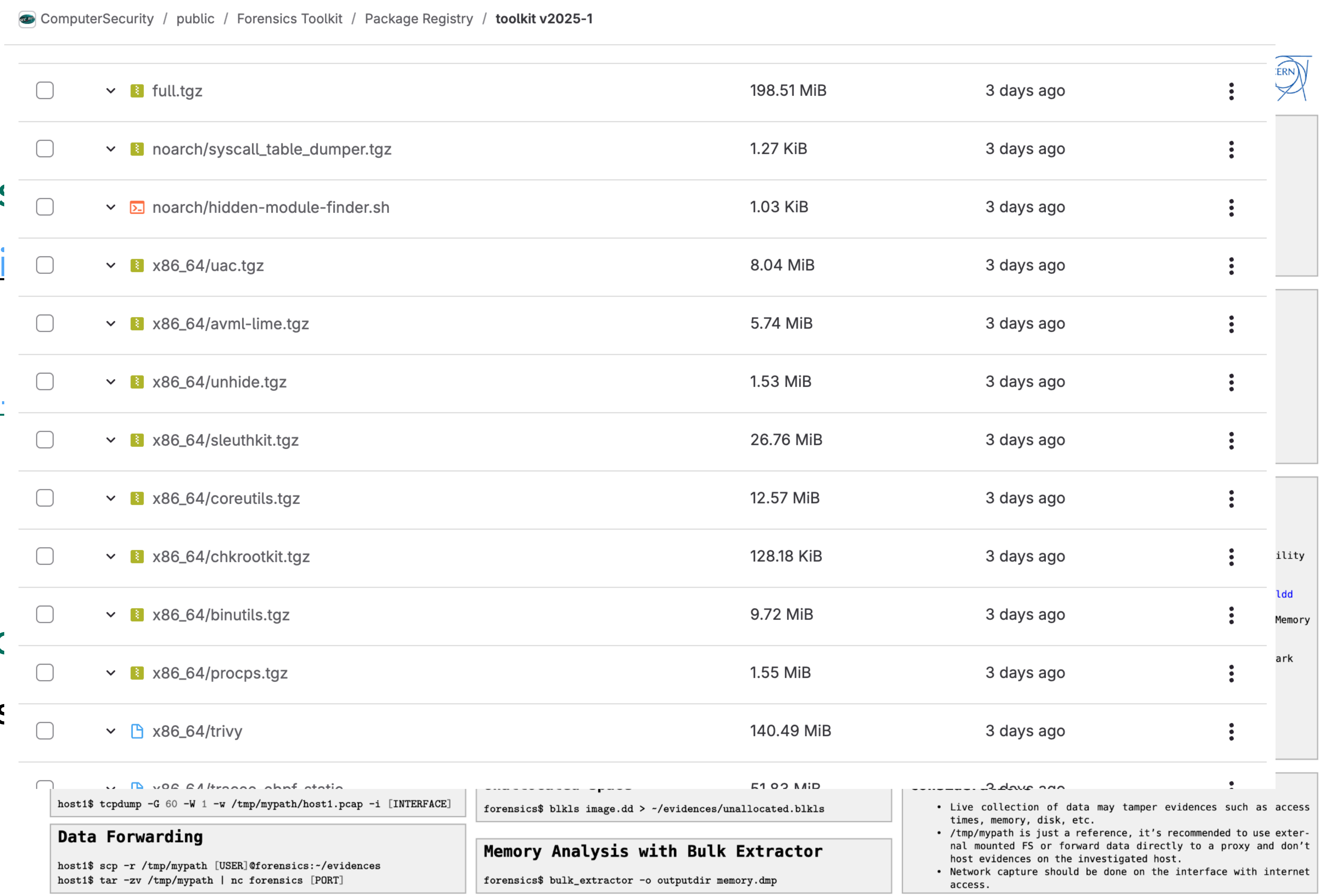
- https://cern.ch/forensics CERN Forensics
- https://sleuthkit.org/sleuthkit/ The Sleuth Kit (TSK)
- https://forensics.wiki/bulk_extractor/ Bulk Extractor
- https://github.com/volatilityfoundation/volatility Volatility
- https://github.com/tclahr/uac Unix Artifact Collector
- https://github.com/504ensicsLabs/LiME LiME
- https://github.com/resurrecting-open-source-projects/dcfldd dcfldd
- https://github.com/microsoft/avml Acquire Volatile Memory (Linux)
- https://www.tcpdump.org/ tcpdump
- https://www.wireshark.org/docs/man-pages/tshark.html tshark
- https://www.chkrootkit.org/download/ Chkrootkit
- https://github.com/YJesus/Unhide Unhide
- https://github.com/aquasecurity/tracee/releases Tracee
- https://github.com/aquasecurity/trivy/releases Trivy
- https://github.com/mozillazg/ptcpdump/releases ptcpdump
- https://github.com/bpftrace/bpftrace/releases bpftrace
- https://github.com/gojue/ecapture/releases ecapture

Considerations

- Live collection of data may tamper evidences such as access times, memory, disk, etc.
- /tmp/mypath is just a reference, it's recommended to use external mounted FS or forward data directly to a proxy and don't host evidences on the investigated host.
- Network capture should be done on the interface with internet access.

Initiatives: Incident Response

- Workshop & hands on
  - Forensics and incident res
    - Still preparing: https://indi
    - Subscribe for info:
      - https://e-groups.cern.ch/e
- Blueprints and toolkits
  - Forensics Cheatsheet & to
    - investigation on the early s
  - https://cern.ch/forensics



ComputerSecurity / public / Forensics Toolkit / Package Registry / **toolkit v2025-1**

☐	full.tgz	198.51 MiB	3 days ago
☐	noarch/syscall_table_dumper.tgz	1.27 KiB	3 days ago
☐	noarch/hidden-module-finder.sh	1.03 KiB	3 days ago
☐	x86_64/uac.tgz	8.04 MiB	3 days ago
☐	x86_64/avml-lime.tgz	5.74 MiB	3 days ago
☐	x86_64/unhide.tgz	1.53 MiB	3 days ago
☐	x86_64/sleuthkit.tgz	26.76 MiB	3 days ago
☐	x86_64/coreutils.tgz	12.57 MiB	3 days ago
☐	x86_64/chkrootkit.tgz	128.18 KiB	3 days ago
☐	x86_64/binutils.tgz	9.72 MiB	3 days ago
☐	x86_64/procps.tgz	1.55 MiB	3 days ago
☐	x86_64/trivy	140.49 MiB	3 days ago
☐	x86_64/tracee-ebpf-static	51.83 MiB	3 days ago

```
host1$ tcpdump -G 60 -W 1 -w /tmp/mypath/host1.pcap -i [INTERFACE]
```

Data Forwarding

```
host1$ scp -r /tmp/mypath [USER]@forensics:~/evidences
host1$ tar -zv /tmp/mypath | nc forensics [PORT]
```

```
forensics$ blkls image.dd > ~/evidences/unallocated.blkls
```

Memory Analysis with Bulk Extractor

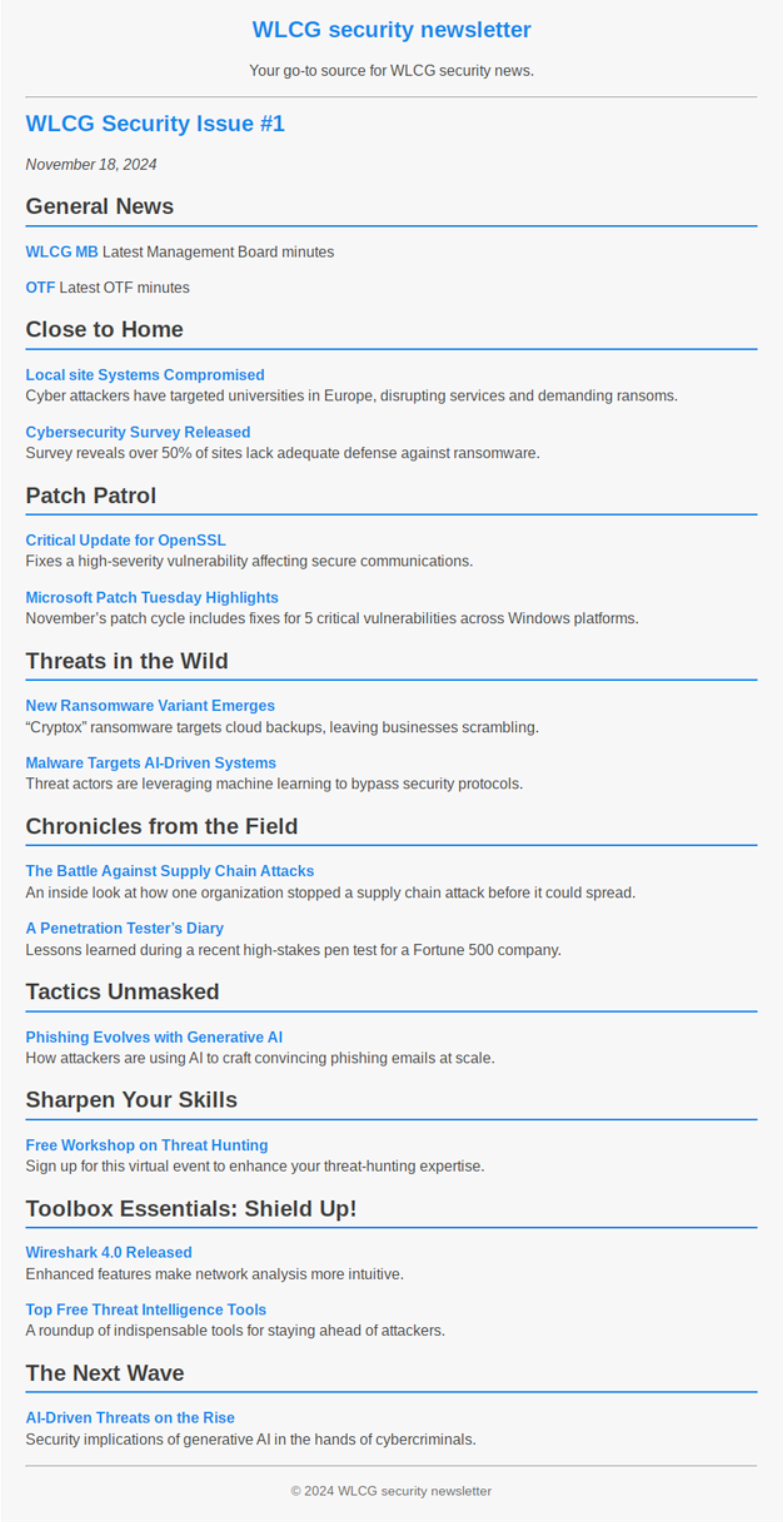
```
forensics$ bulk_extractor -o outputdir memory.dmp
```

- Live collection of data may tamper evidences such as access times, memory, disk, etc.
- /tmp/mypath is just a reference, it's recommended to use external mounted FS or forward data directly to a proxy and don't host evidences on the investigated host.
- Network capture should be done on the interface with internet access.

Initiatives: Awareness

- Every other month newsletter (coming soon)
  - Subscribe:
    - https://e-groups.cern.ch/e-groups/EgroupsSubscription.do?egroupName=wlcg-security-newsletter

- Recurrent slot in the OTF
  - Status, recent incidents, news



WLCG security newsletter

Your go-to source for WLCG security news.

WLCG Security Issue #1

November 18, 2024

General News

WLCG MB Latest Management Board minutes

OTF Latest OTF minutes

Close to Home

Local site Systems Compromised
Cyber attackers have targeted universities in Europe, disrupting services and demanding ransoms.

Cybersecurity Survey Released
Survey reveals over 50% of sites lack adequate defense against ransomware.

Patch Patrol

Critical Update for OpenSSL
Fixes a high-severity vulnerability affecting secure communications.

Microsoft Patch Tuesday Highlights
November's patch cycle includes fixes for 5 critical vulnerabilities across Windows platforms.

Threats in the Wild

New Ransomware Variant Emerges
"Cryptox" ransomware targets cloud backups, leaving businesses scrambling.

Malware Targets AI-Driven Systems
Threat actors are leveraging machine learning to bypass security protocols.

Chronicles from the Field

The Battle Against Supply Chain Attacks
An inside look at how one organization stopped a supply chain attack before it could spread.

A Penetration Tester's Diary
Lessons learned during a recent high-stakes pen test for a Fortune 500 company.

Tactics Unmasked

Phishing Evolves with Generative AI
How attackers are using AI to craft convincing phishing emails at scale.

Sharpen Your Skills

Free Workshop on Threat Hunting
Sign up for this virtual event to enhance your threat-hunting expertise.

Toolbox Essentials: Shield Up!

Wireshark 4.0 Released
Enhanced features make network analysis more intuitive.

Top Free Threat Intelligence Tools
A roundup of indispensable tools for staying ahead of attackers.

The Next Wave

AI-Driven Threats on the Rise
Security implications of generative AI in the hands of cybercriminals.

© 2024 WLCG security newsletter

Challenges Ahead

- Tokens (still some way ahead)
  - Flexibility, closer to industry standards, but new(-er) paradigm
  - And a lot of decisions to be made:
    - Just OAUTH itself has +30 RFC (https://oauth.net/specs), add OIDC on top and more specs
  - Security, Traceability, Incident contention while having robust operations

- Analysis facilities
  - Changing the paradigm on identity/resources and their use
  - Devil is always in the details, for security how it is done even more important
  - Details needed… We are here to help, please involve security early!

Questions?

jose.carlos.luna@cern.ch