CERN Computer Security

Dr. Stefan.Lueders@cern.ch

CSO/CERT Strategy 2015+

Mandate: “Protect the operations and reputation of CERN against cyber-threats.”

- Continue to provide excellence in computer security for CERN and the WLCG;
- Engage even more deeply with the community and industry to better and more early identify APTs against CERN and/or the WLCG;
- Adapt our sensor, online detection & logging infrastructure in order to cope with the increase of bandwidth at the Internet gates and include as data sources all *Intranet* gates, DNS & web logs, and logs from all computing clusters;
- Improve the protection of the human factor against (targeted) APTs: sociologically by more awareness training; technically by better securing critical accounts and workstations (e.g. 2FA; separation ACC dev/ops; HR/FI PCs);
- Seek consolidation of computing services within CERN in order to reduce the current cacophony and its inherent sub-optimal security posture. Continue to provide security consulting where consolidation is not possible;
- Ensure that the mandate is 100% fulfilled during my watch.

The Team

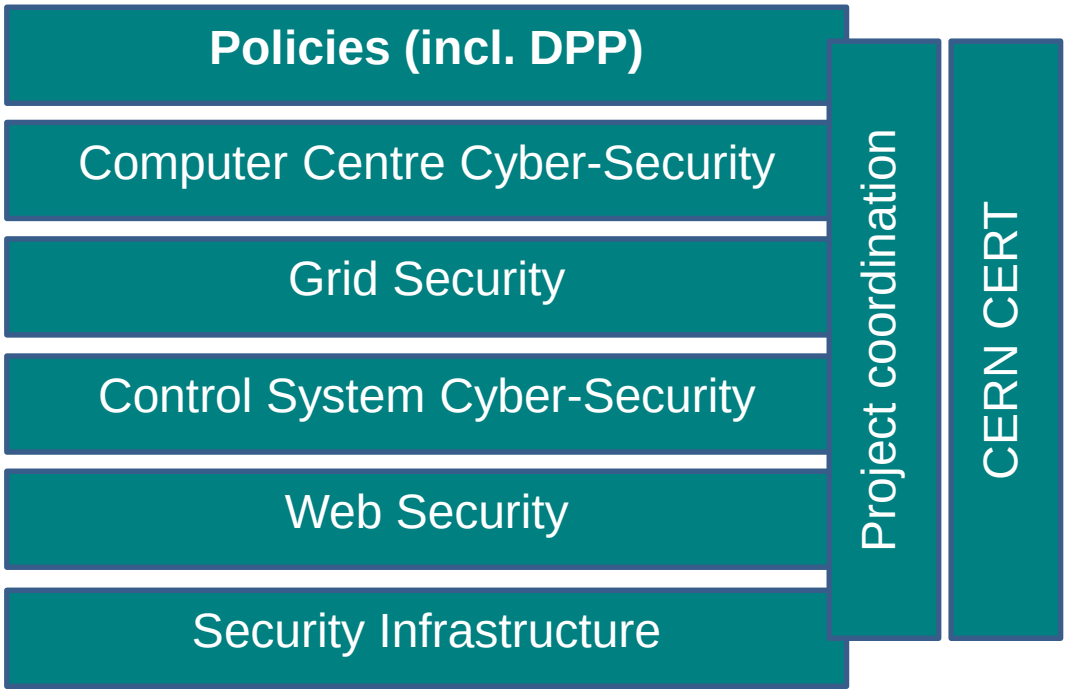
Mandate:
Protect the operations and reputation of the Organization against cyber-threats

Manpower:

- 4 staff + 1 fellow
- 1-5 students
- 5 external in-kind contributions of 10% for first line support

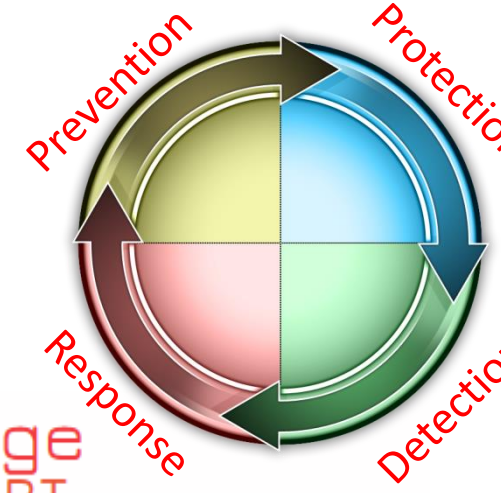
Responsibilities:

- About 40 different on-going or pending projects
- Mostly coordination of external efforts



CERN CERT Portfolio

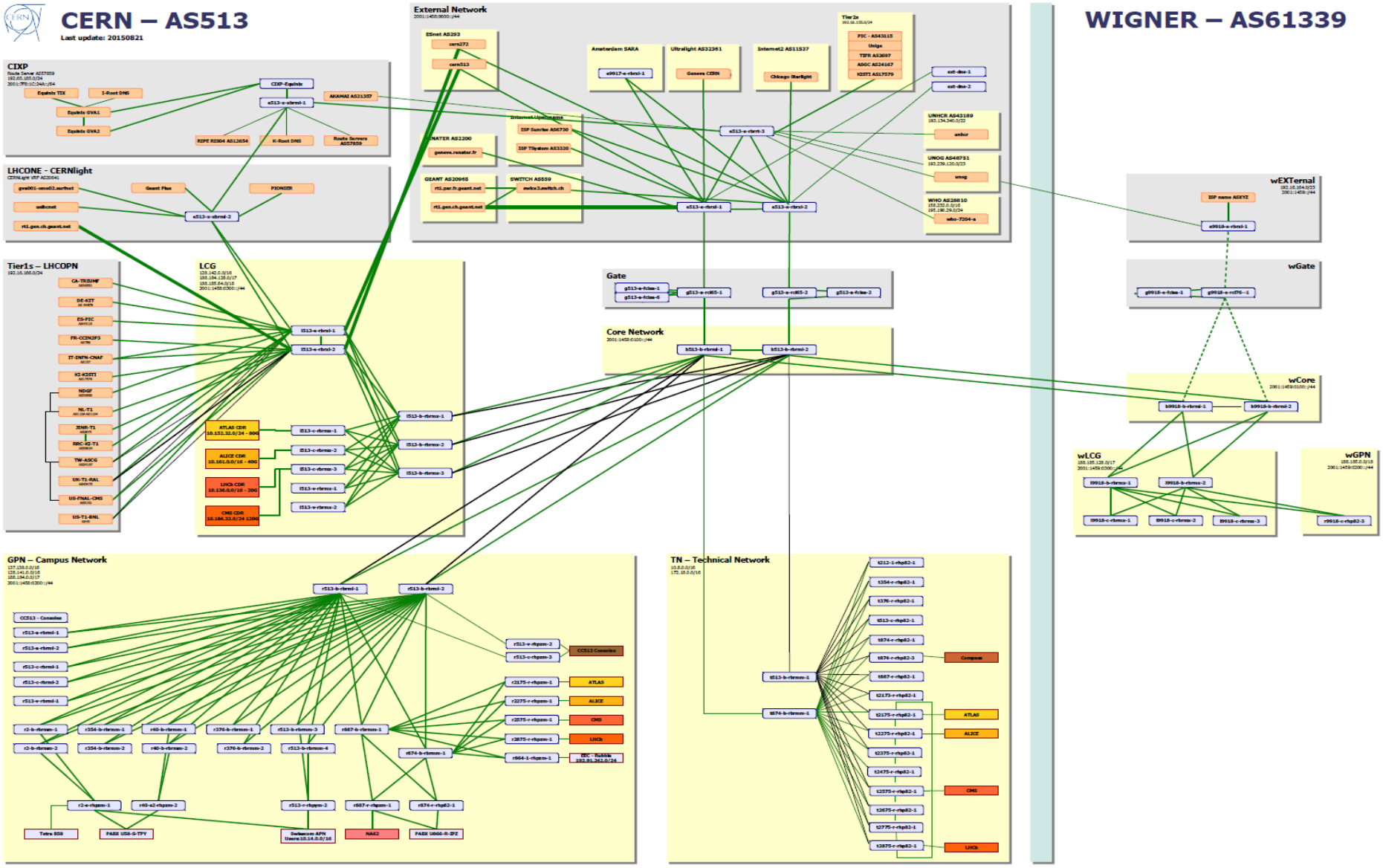
ID federations
pen testing
consulting
central anti-virus
resource inventories
static code analyzers
baselining
SSO/2FA
security policies
audits
reviews
firewalling
awareness
training
central/agile patching
resource life-cycles
network segregation
change of culture
Defense-in-Depth



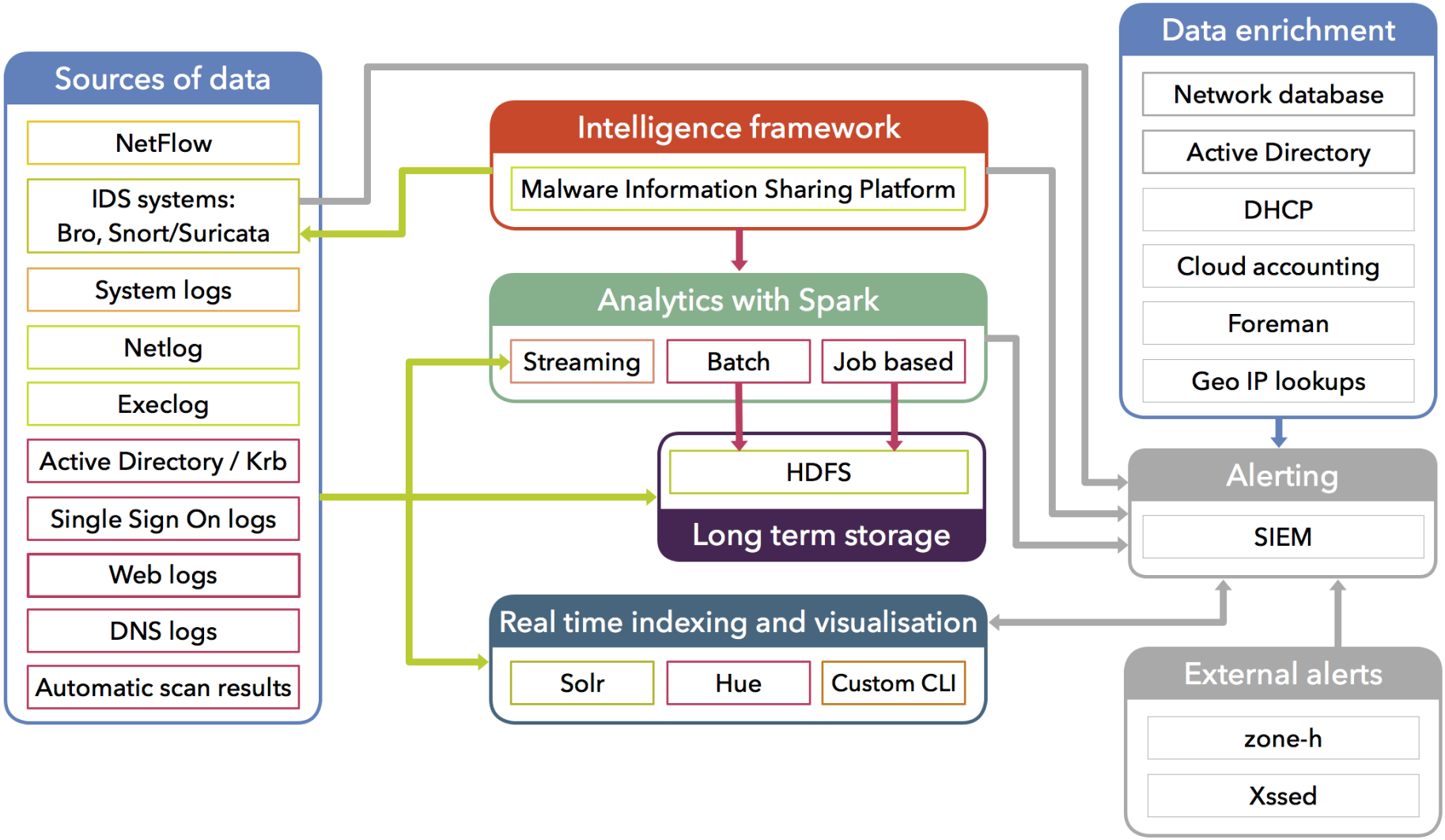
WhiteHat Challenges
vulnerability scanning
statistical traffic analysis
netflow
integrity checkers
DNS verification
credential hunts
SSHgrep
URLgrep
IDS
monitor-the-monitoring
remote login receipts
syslog/netlog analysis/Snoopy
web application checking

triage
CSIRT/CERT
costing
forensics
WLCG Grid Security Officer
Security Event Self-Mitigation Portal

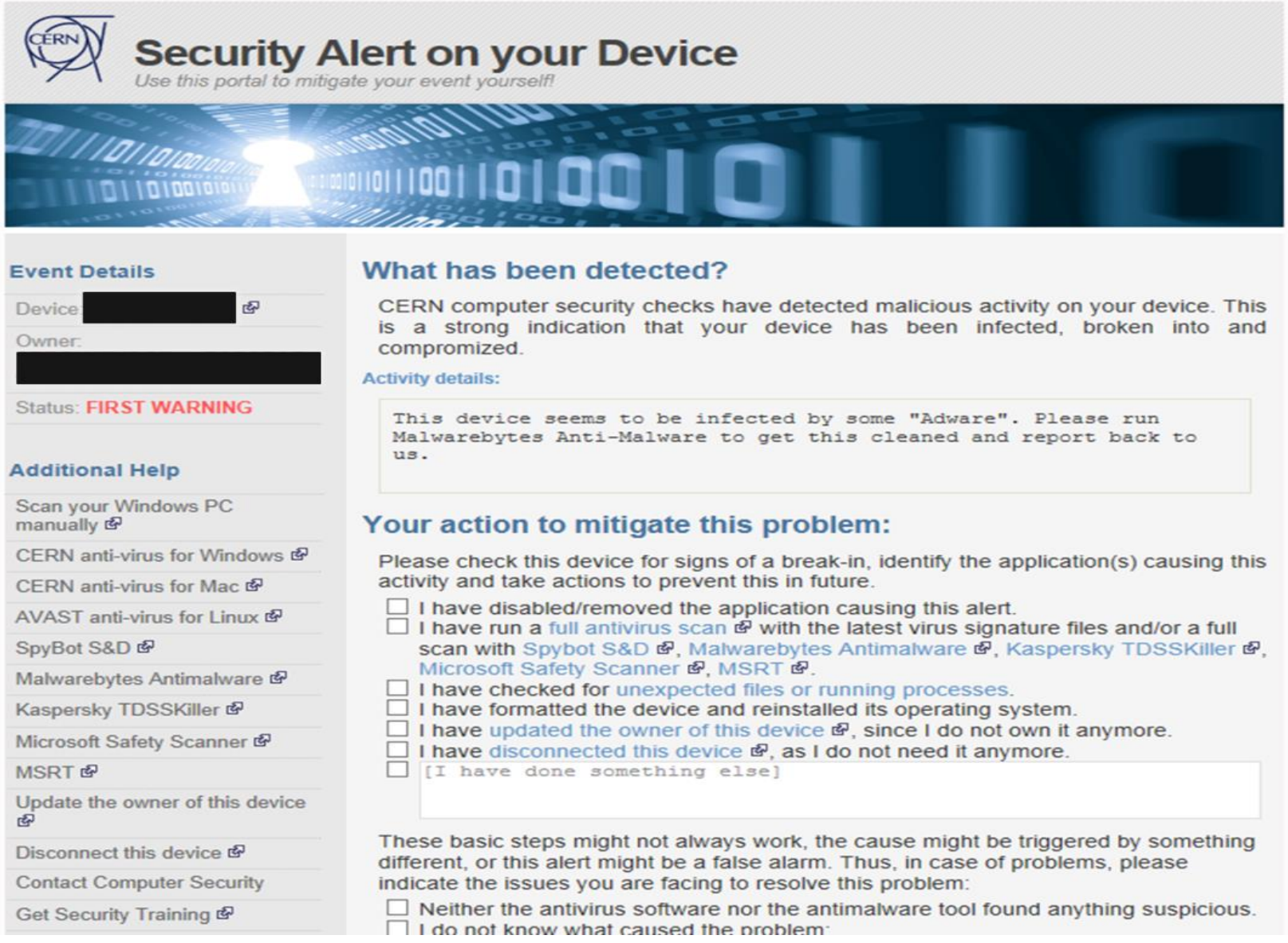
CERN Networking



IDS Infrastructure



Auto-Notify



Security Alert on your Device

Use this portal to mitigate your event yourself!

Event Details

Device: [redacted]

Owner: [redacted]

Status: **FIRST WARNING**

Additional Help

- Scan your Windows PC manually
- CERN anti-virus for Windows
- CERN anti-virus for Mac
- AVAST anti-virus for Linux
- SpyBot S&D
- Malwarebytes Antimalware
- Kaspersky TDSSKiller
- Microsoft Safety Scanner
- MSRT
- Update the owner of this device
- Disconnect this device
- Contact Computer Security
- Get Security Training

What has been detected?

CERN computer security checks have detected malicious activity on your device. This is a strong indication that your device has been infected, broken into and compromized.

Activity details:

```
This device seems to be infected by some "Adware". Please run
Malwarebytes Anti-Malware to get this cleaned and report back to
us.
```

Your action to mitigate this problem:

Please check this device for signs of a break-in, identify the application(s) causing this activity and take actions to prevent this in future.

- ☐ I have disabled/removed the application causing this alert.
- ☐ I have run a full antivirus scan with the latest virus signature files and/or a full scan with Spybot S&D, Malwarebytes Antimalware, Kaspersky TDSSKiller, Microsoft Safety Scanner, MSRT.
- ☐ I have checked for unexpected files or running processes.
- ☐ I have formatted the device and reinstalled its operating system.
- ☐ I have updated the owner of this device, since I do not own it anymore.
- ☐ I have disconnected this device, as I do not need it anymore.
- ☐ [I have done something else]

These basic steps might not always work, the cause might be triggered by something different, or this alert might be a false alarm. Thus, in case of problems, please indicate the issues you are facing to resolve this problem:

- ☐ Neither the antivirus software nor the antimalware tool found anything suspicious.
- ☐ I do not know what caused the problem:

Firewall Requests

Request Information

- Interface name:(*) SL-LAPTOP2

- **Service:**(*) SSH server on port 22/tcp

If Other, then please specify:

- Port number:
- Protocol: TCP
- Application:

Hint: Give the name of the application listening on the port.

- **Expiry date:** / / (DD/MM/YYYY)

Use this date when firewall access is needed for a known duration. The firewall authorisation will be automatically removed on this date.

- **Describe the professional requirement for which direct Internet access is required.**(*)

- **Explain why the recommended methods for accessing CERN from the Internet, as described at http://cern.ch/security/recommendations/en/connecting_to_cern.shtml, cannot be used.** If appropriate, explain why CERN's central services (e.g. web, J2EE, CVS, ...) cannot be used.(*)

- **Explain how you ensure that the device for which firewall access is requested will be kept pro-actively secured for security updates.** (This includes the operating system and all installed applications).(*)

- Enter the name of the Group Leader or the Experiment Technical Coordinator who has endorsed this request. If this request is related to an experiment then please also enter the experiment name.(*)
  - Name:(*)
  - First Name:(*)
  - Department:
  - Group:
  - Experiment Name (if relevant):

Hint: This will be used when escalation in the management hierarchy is required

- ☐ **I confirm that the device is running in its final configuration.**(*)
- ☐ **I confirm that the device is compliant with the relevant CERN Security Baselines (https://cern.ch/security/rules/en/baselines.shtml"(*)**
- ☐ **I confirm that the device is not running controls applications.**(*)
- ☐ **I confirm that the device does not provide unrestricted access to sensitive data.**(*)

Public Webpage

CERN Computer Security

Computer security emergency contact
Computer.Security@cern.ch 70500
Contact en cas d'incident de sécurité informatique

Home | Computing Rules | Recommendations | Training | Services | Reports & Presentations

Vous préférez le français ?

Emergency Response

What to do in an emergency

Contact

How to contact the Computer Security Team

Departmental & experiment contacts

About CERN Computer Security

A word from the DG

Security is not complete without you

CERN Computer Security Announcements

(Previous announcements are here.)

Security needs you

"Academic freedom is a valuable thing, but like any kind of freedom, it comes with responsibility... It is the responsibility of all of us, not just the experts in the IT Department, to protect our IT infrastructure while striking the right balance between security, academic freedom and the unfettered operation of our facilities... At CERN, security is not complete without you."

(Read more in the CERN Bulletin)

Overview

At CERN, due to its unique academic environment and the associated academic freedom, **computer security has been delegated to CERN's users:**

At CERN, the individual users are in first instance responsible for securing their computers, networks, data, systems & services.

The Computer Security Team - and the IT department - are ready to help users