You've got mail

From good_guy@security_dude.org

Subject **Compromised Server** 21:21

To cert@your-org.org

Enigmail Decrypted message Details

```
TLP Amber

Hello security Team. Appended is a list of compromised webservers from
your AS. These systems are misused as part of the exploit kit XXX and
currently distribute the ransomware YYYY.

The report is of the form:

IP,server,path,last seen



Thanks
Dude-CERT
```

What do you do?

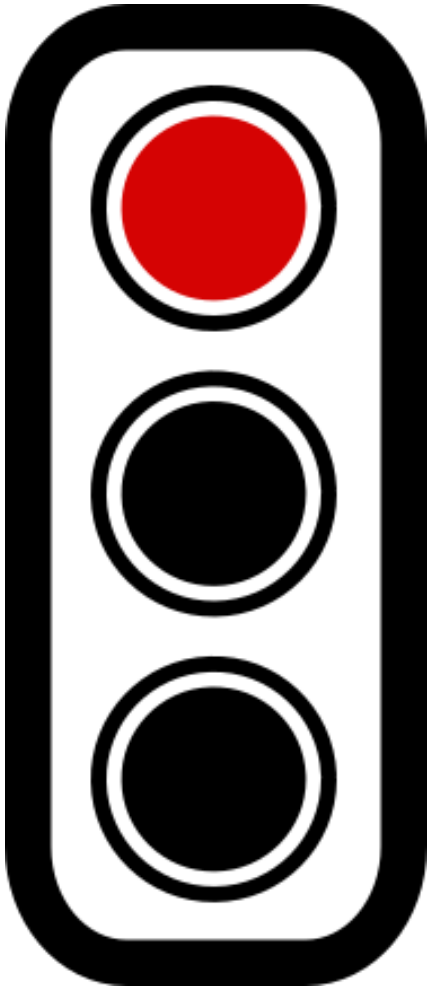
FIRST Improving Security Together

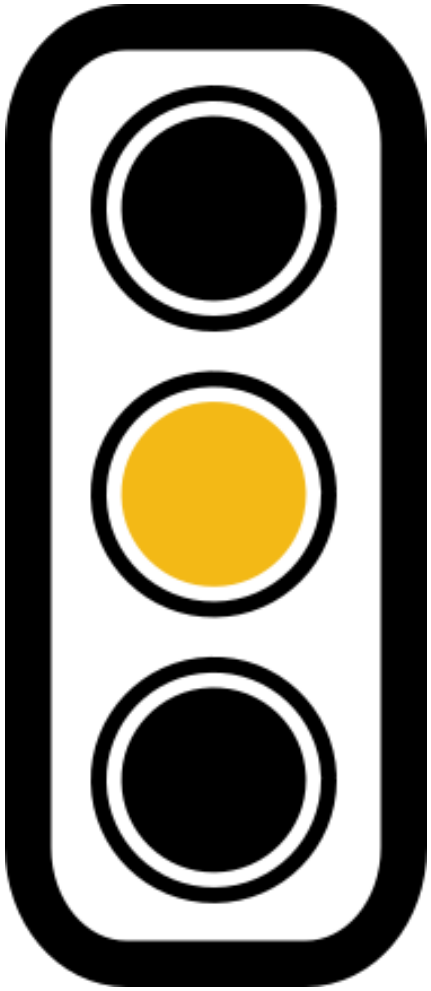
FIRST TLP v1.0: Enabling human info sharing

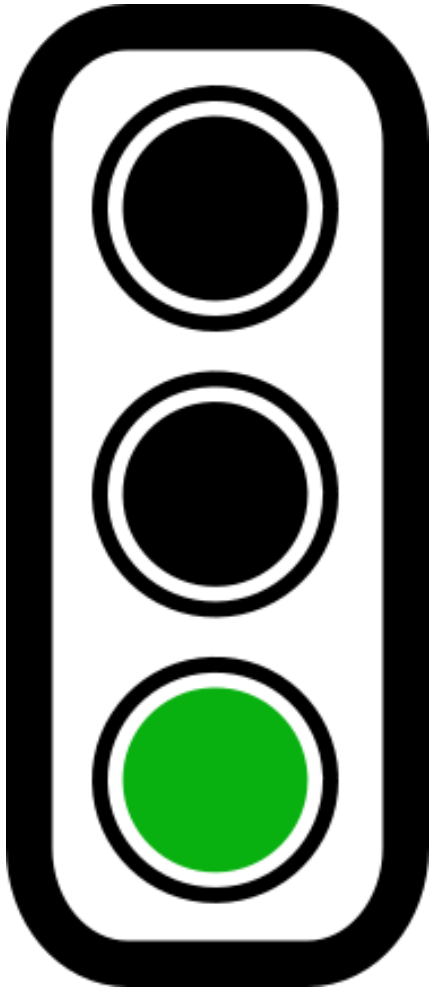
Dr. Serge Droz
OS-CERT
serge.droz@first.org
sed@open.ch

Forum of Incident Response and Security Teams

Traffic light protocol

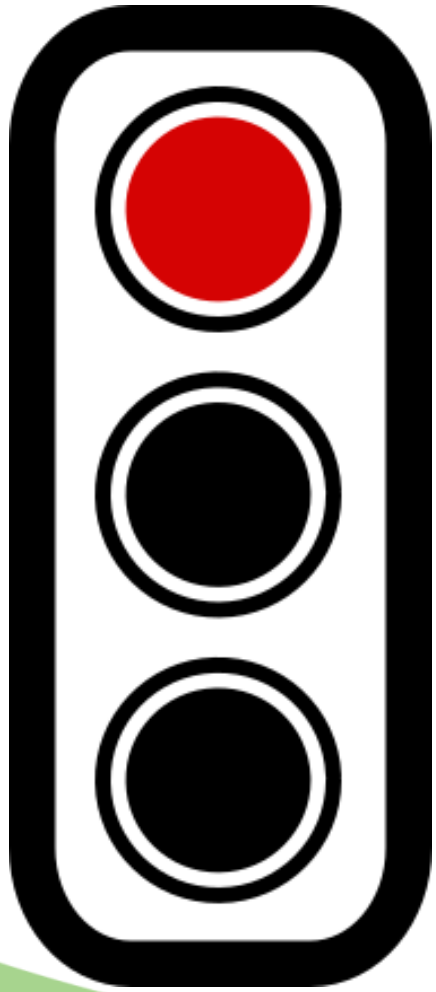






FIRST
Improving Security Together

Red

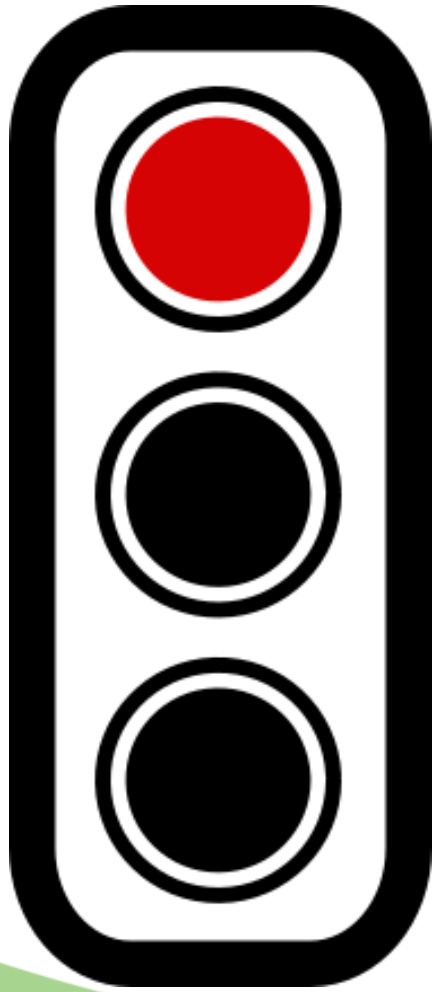


For your ears only

Limited usefulness in the strict sense,
But you can always ask back!

FIRST
Improving Security Together

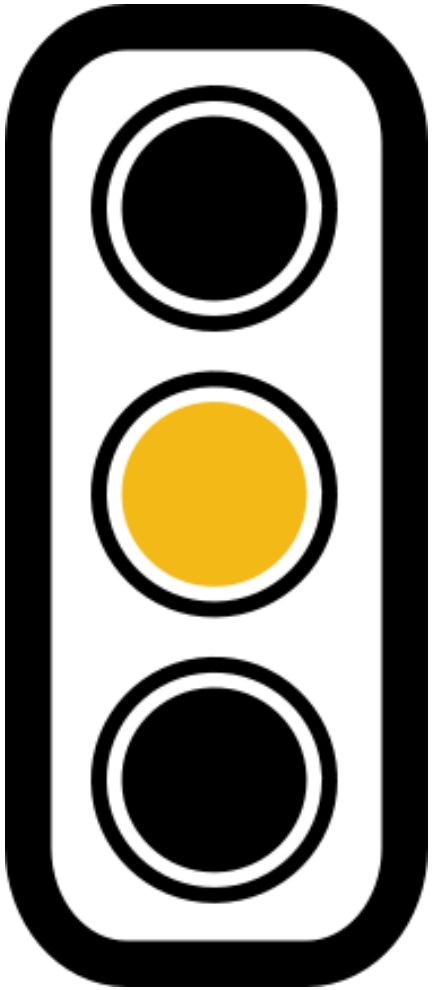
Red



For your ears only

Limited usefulness in the strict sense,
But you can always ask back!

Amber

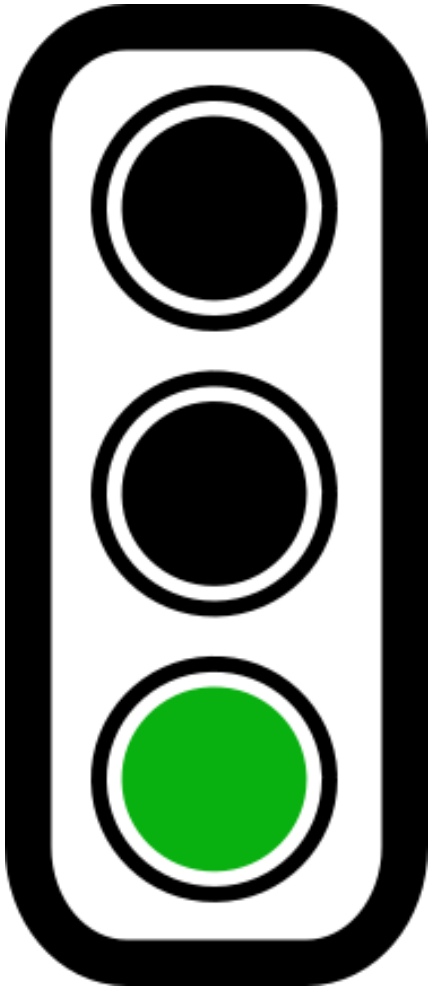


Share on a need to know basis within your org.

What is my Org?

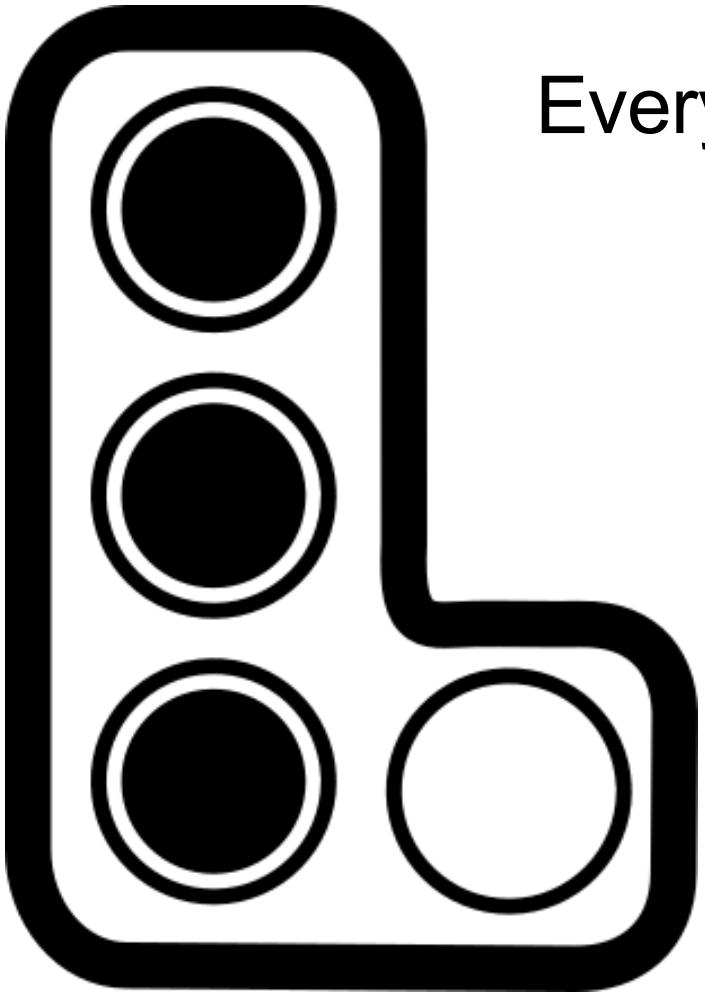
- Hey man, I just know that
- Switzerland.org
- My office mates and myself
- My boss

Green



Everyone, except for the public.

White



Everyone, really!

FIRST
Improving Security Together

TLP is ambiguous, in particular amber!
There are conflicting versions around!

FIRST TLP v1

At the FIRST annual meeting the TLP SIG was founded with the goal to provide a definition that others could refer to and the was more precise.

The SIG hat representatives from different sectors.

https://www.first.org/tlp

What's new

Not much, really

AMBER was changed compared to the US-CERT definition, but is the same as the old TF-CSIRT version.

AMBER: Share within your org
on a need to know basis.

What's new

Not much, really

AMBER was changed compared to the US-CERT definition, but is the same as the old TF-CSIRT version.

AMBER: Share within your org and customers/constituents on a need to know basis.

I did say not much?

You can specify additional constraints!

- TLP Amber, no commercial reuse
- TLP Amber, only within you team

FAQ

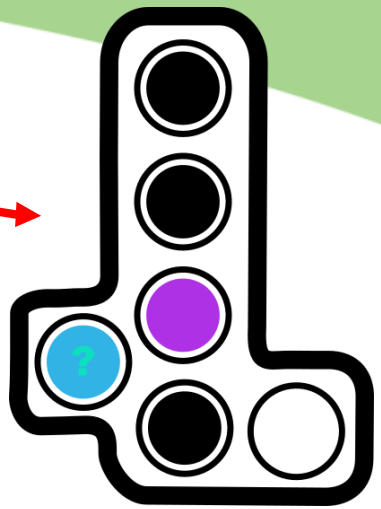
Q: But this is different from before
A: Only to some definitions, and the differences are minor

Q: What about backwards compatibility?
A: See above

Q: Isn’t amber green now, that it can be reshared?
A: No! Sharing is still need to know, and you can share with more strings attached.

FAQ

Avoid this



Q: Why not introduce more colours?
A: TLP should be simple

Q: But then you can't use it for machine sharing
A: Right, for that we have Information Exchange Policy (IEP)
http://www.first.org/global/sigs/iep

Questions

Remember:

Sharing is caring