23 September 2017

BSides Zürich

The Social Networks of the Security Community

Jeroen Massar
jeroen@massar.ch

Jeroen Massar

private:

https://jeroen.massar.ch & jeroen@massar.ch

work:

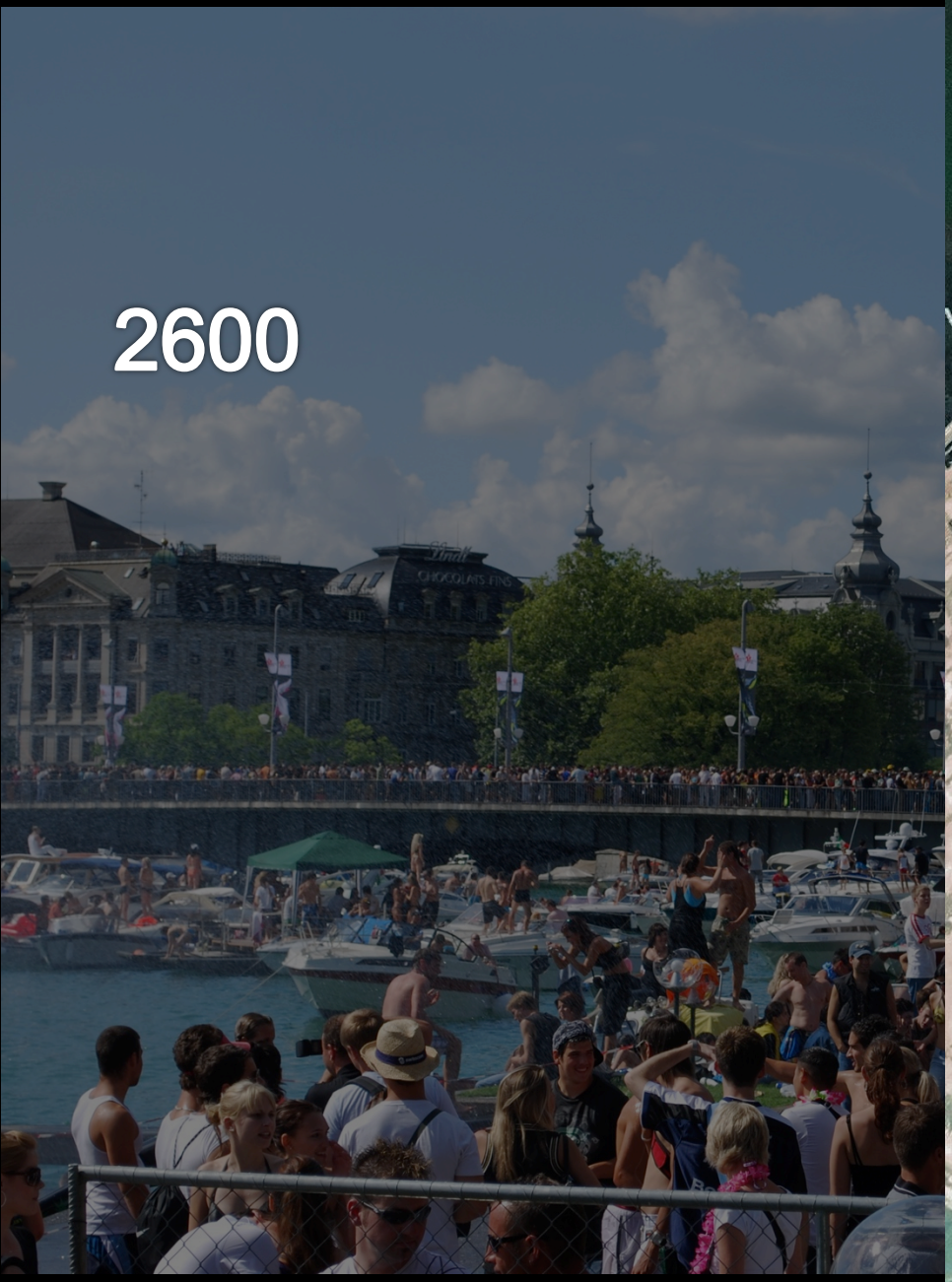
scip AG

funtime:

Secluded.ch / Trident Coder ← hat of the day

Ops-Trust Sysadmin Team

Formerly: SixXS Staff



Volume Thirty-Two, Number One!
DIGITAL EDITION Spring 2015

2600

The Hacker Quarterly

UPI UPI.com @UPI Follow

Pope:"World War III has begun." #TPBISBACK

.78 .13 .28 .17 .88 .30 .75 .27 .19 .4 .1 .76 .60 .86 .77 .11

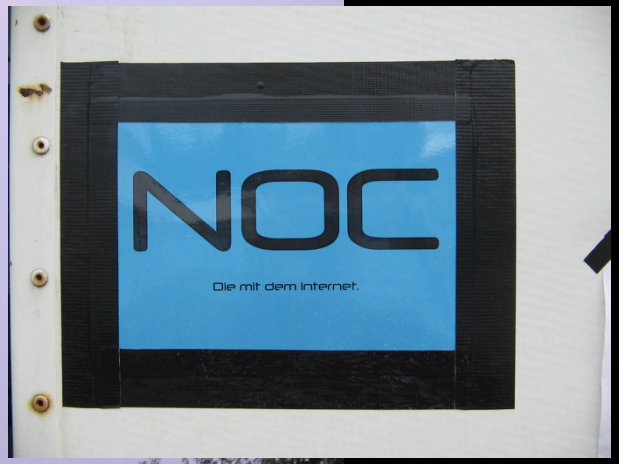
Lattitude
78.252785N

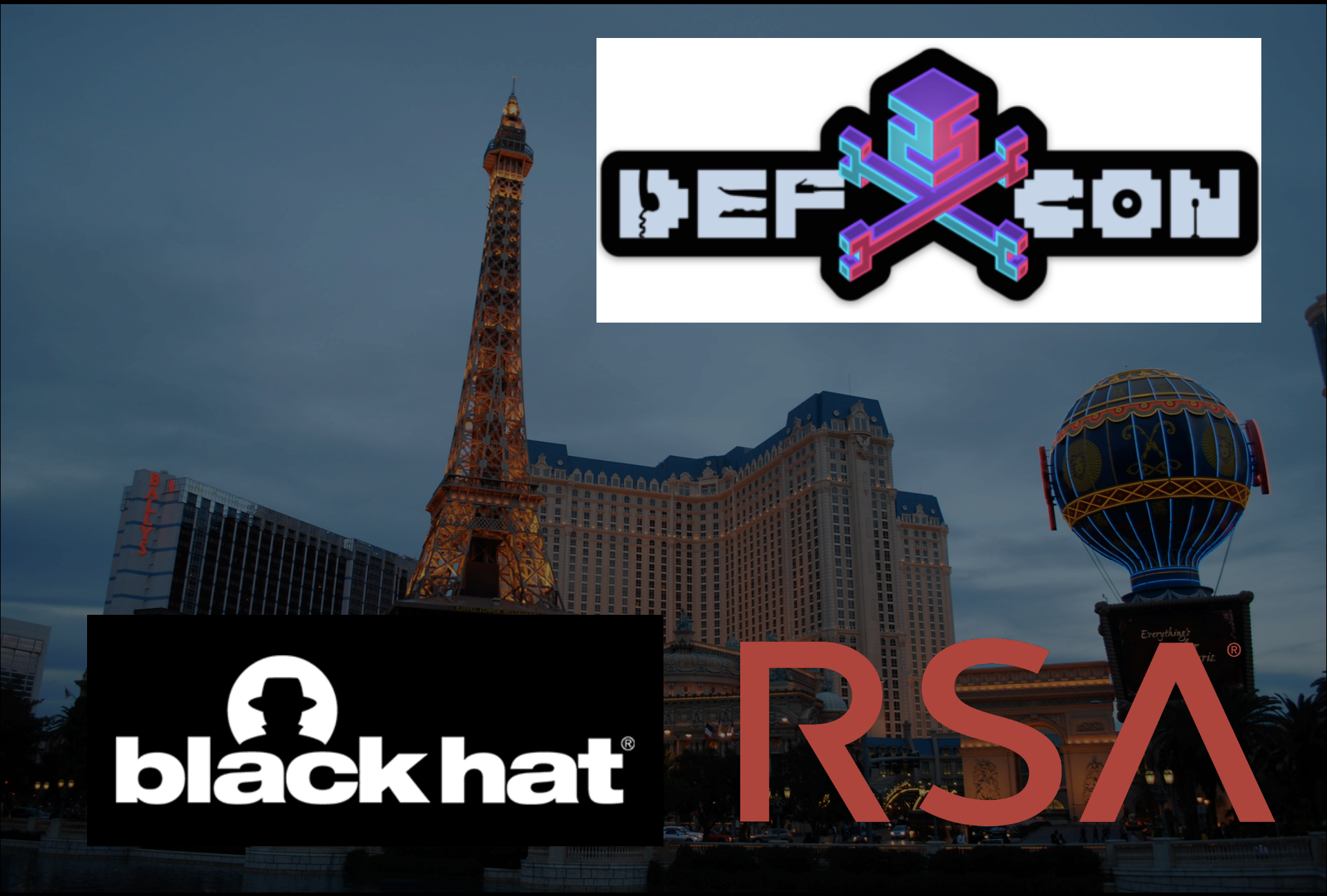
Longitude
15.409617E

Hacktic

1989 - Galactic Hacker Party (GHP)
1993 - Hacking at the End of the Universe (HEU)
1997 - Hacking In Progress (HIP)
2001 - Hackers At Large (HAL)
2005 - What The Hack (WTH)
2009 - Hacking at Random (HAR)
2013 - Observe. Hack. Make. (OHM)
2017 - Still Hacking Anyway (SHA)


CCC


NOC
Die mit dem Internet.

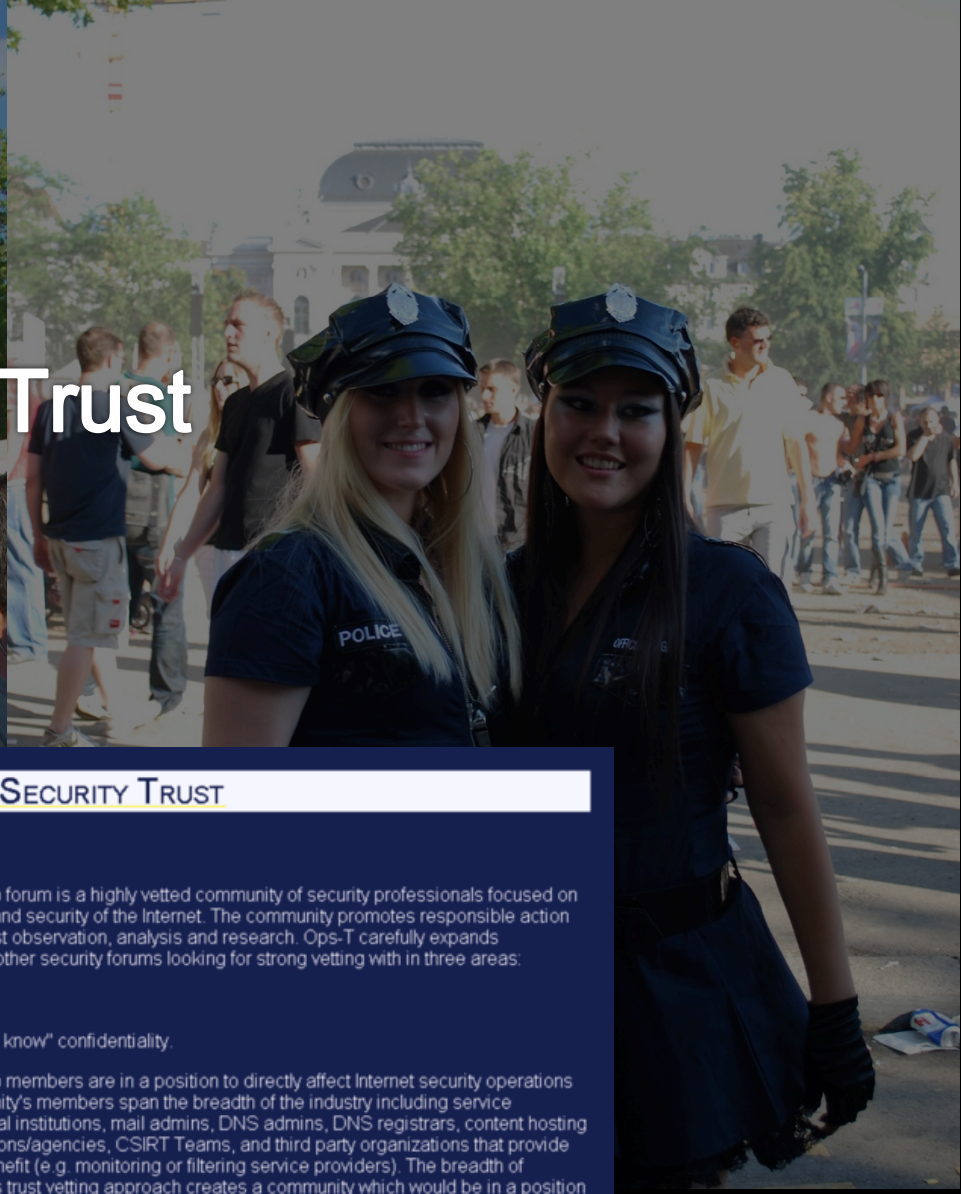

DEF CON
black hat
RSA


RIPE NCC
RIPE NETWORK COORDINATION CENTRE
ARIN
American Registry for Internet Numbers
Juniper
MX960
NANOG
APNIC


FIRST
Improving Security Together
SANS
CERT
COMMUNITY EMERGENCY
RESPONSE TEAM


SIGS
Security Interest
Group Switzerland
OWASP Switzerland
ISSS
Information
Security Society
Switzerland
ISSA
Information Systems Security Association

Ops-Trust



Operations Security Trust

Login

Mission

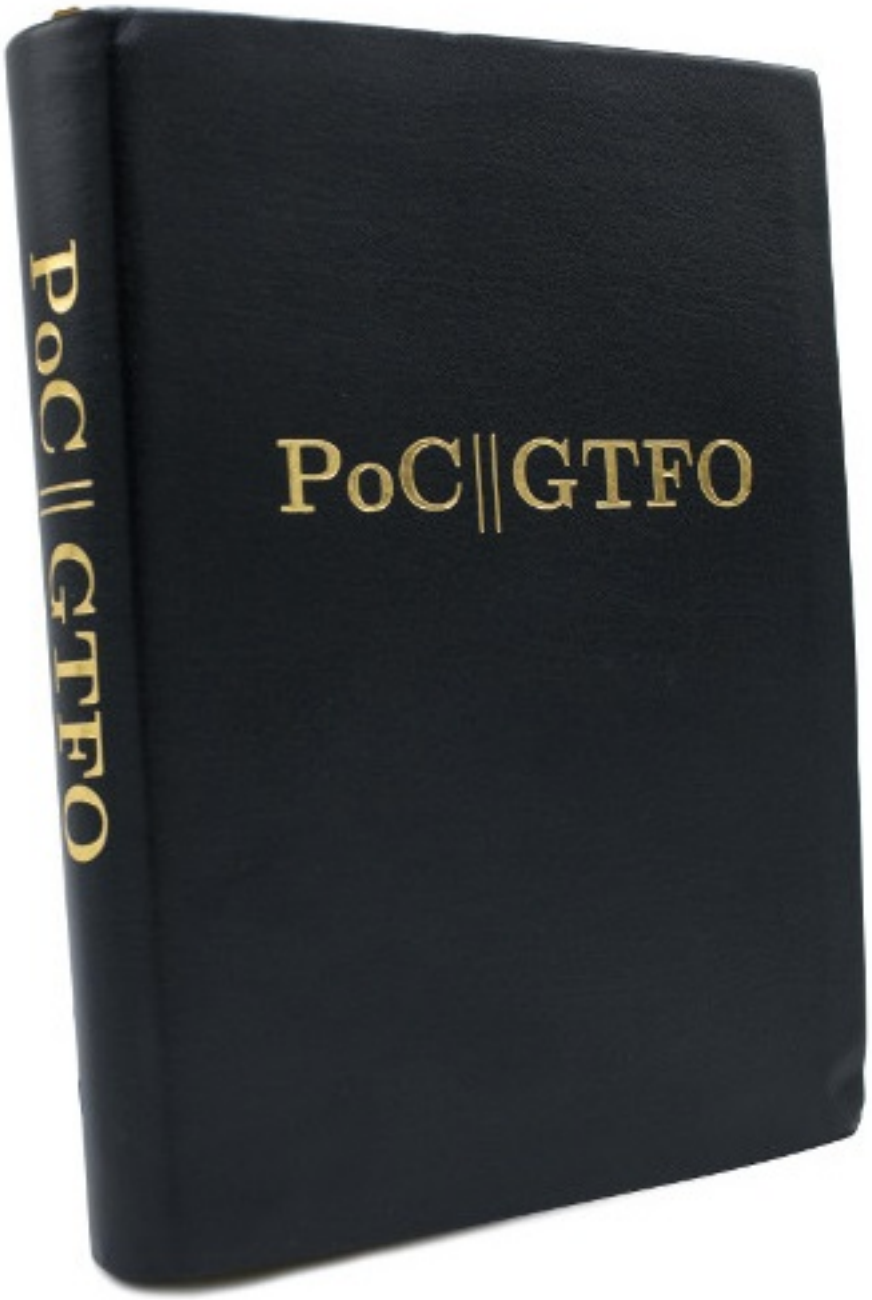
Operations Security Trust (or "Ops-T") forum is a highly vetted community of security professionals focused on the operational robustness, integrity, and security of the Internet. The community promotes responsible action against malicious behavior beyond just observation, analysis and research. Ops-T carefully expands membership pulling talent from many other security forums looking for strong vetting with in three areas:

1. sphere of trust;
2. sphere of action;
3. the ability to maintain a "need to know" confidentiality.

Operations Security Trust (or "Ops-T") members are in a position to directly affect Internet security operations in some meaningful way. The community's members span the breadth of the industry including service providers, equipment vendors, financial institutions, mail admins, DNS admins, DNS registrars, content hosting providers, law enforcement organizations/agencies, CSIRT Teams, and third party organizations that provide security-related services for public benefit (e.g. monitoring or filtering service providers). The breadth of membership, along with an action plus trust vetting approach creates a community which would be in a position to apply focused attention on the malfeasant behaviors which threaten the Internet.

Members:

- will be privy to lists of infected IP addresses, compromised accounts, bot c&c lists and other data that should be acted upon.
- are expected to take appropriate action within their domain of control.
- are expected to contribute data as appropriate and in a fashion that does not violate any laws or corporate policies.

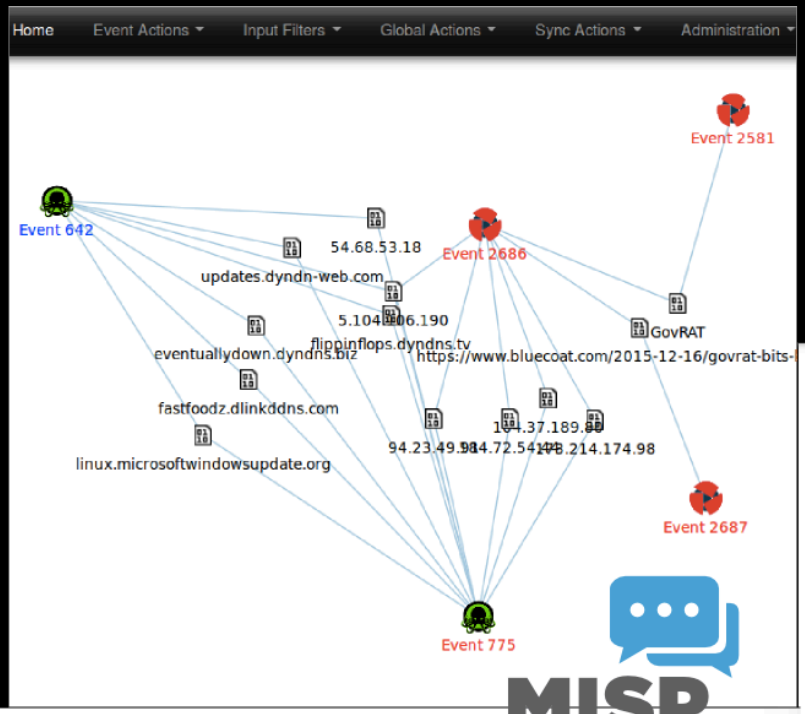

PoC||GTFO
PoC||GTFO


BSIDES
ZURICH


DC4131
DEFCON Switzerland
BEER ON TUESDAY
Hack Happens

AREA 451

SAVE THE DATE
15.-16.JUNE 2018



TLP Taxonomy Library

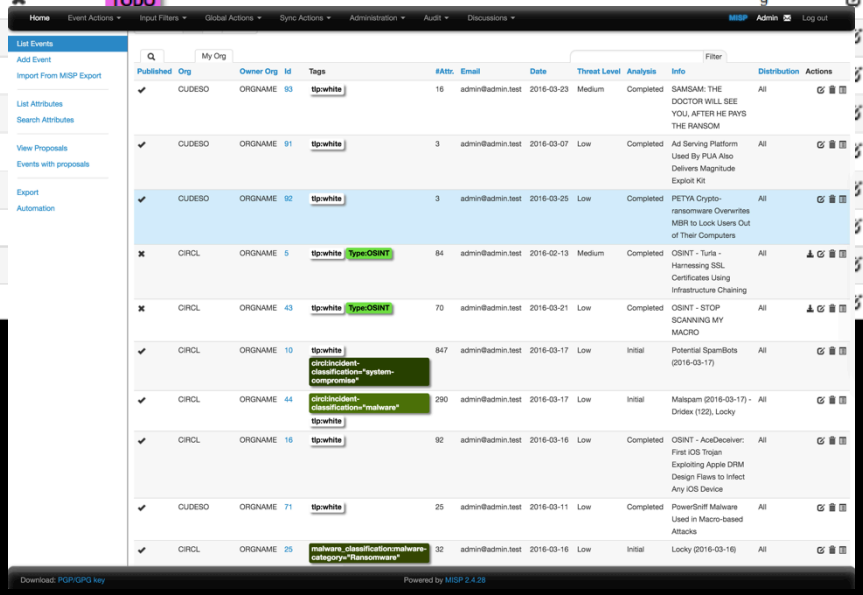
Id	3
Namespace	tlp
Description	The Traffic Light Protocol - or short: TLP - was designed with the objective to create a favorable classification scheme for sharing sensitive information while keeping the control over its distribution at the same time.
Version	1
Enabled	Yes (disable)

« previous | next »

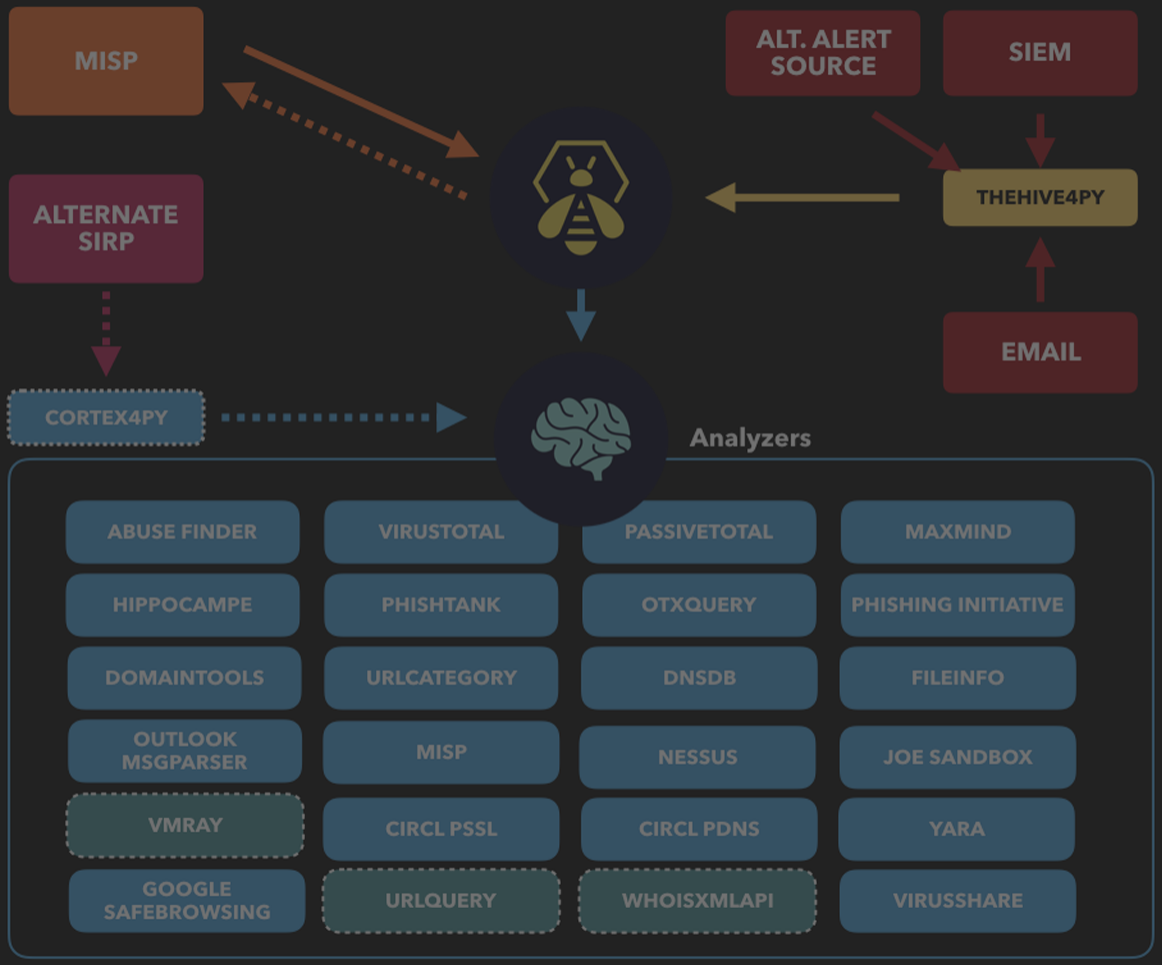
Filter

	Tag	Expanded	Events	Tag	Action
☐	tlp:red	(TLP:RED) Information exclusively and directly given to (a group of) individual recipients. Sharing outside is not legitimate.	3	TLP:RED	
☐	tlp:amber	(TLP:AMBER) Information exclusively given to an organization; sharing limited within the organization to be effectively acted upon.	131	TLP:AMBER	
☐	tlp:green	(TLP:GREEN) Information given to a community or a group of organizations at large. The information cannot be publicly released.	550	TLP:GREEN	
☐	tlp:white	(TLP:WHITE) Information can be shared publicly in accordance with the law.	531	TLP:WHITE	
☐	tlp:ex:chr	(TLP:EX:CHR) Information extended with a specific tag called Chatham House Rule (CHR). When this specific CHR tag is mentioned, the attribution (the source of information) must not be disclosed. This additional rule is at the discretion of the initial sender who can decide to apply or not the CHR tag.	11	TLP:EX:CHR	

Id	Exportable	Name	Taxonomy	Tagged events	Actions
6	✖	APT		31	
7	✖	Actionable:NO		5	
3	✖	TLP:AMBER	tlp	131	
8	✖	TLP:EX:CHR	tlp	11	
5	✖	TLP:GREEN	tlp	550	
4	✖	TLP:RED	tlp	3	
2	✖	TLP:WHITE	tlp	531	
10	✖	TO:HIDE		2	
9	✖	TODO		9	
11					
1					
18					
19					
20					
21					
22					
23					



TheHive Project

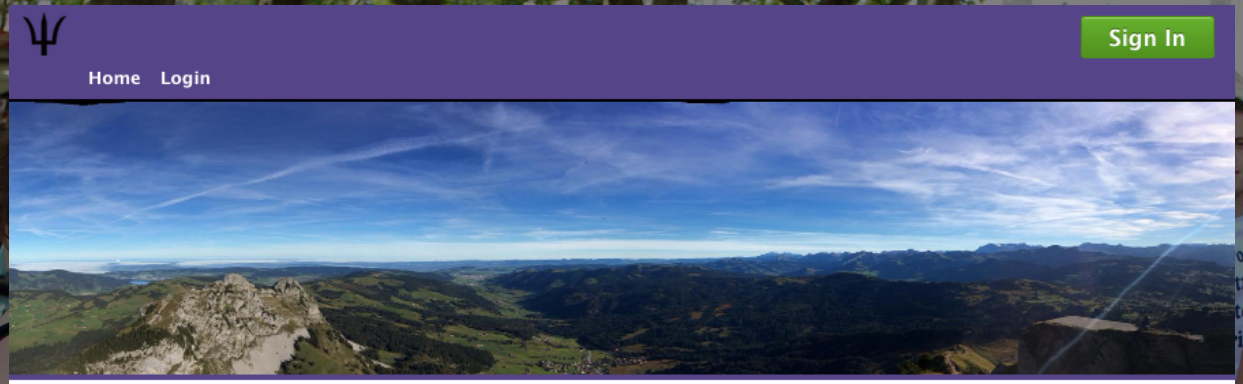


GNU Mailman

Schleuder

https://schleuder.nadir.org/

Trident



Home

Home

Mission

Operations Security Trust (or "Ops-T") forum is a highly vetted community of security professionals focused on the operational robustness, integrity, and security of the Internet. The community promotes responsible action against malicious behavior beyond just observation, analysis and research. Ops-T carefully expands membership pulling talent from many other security forums looking for strong vetting with in three areas:

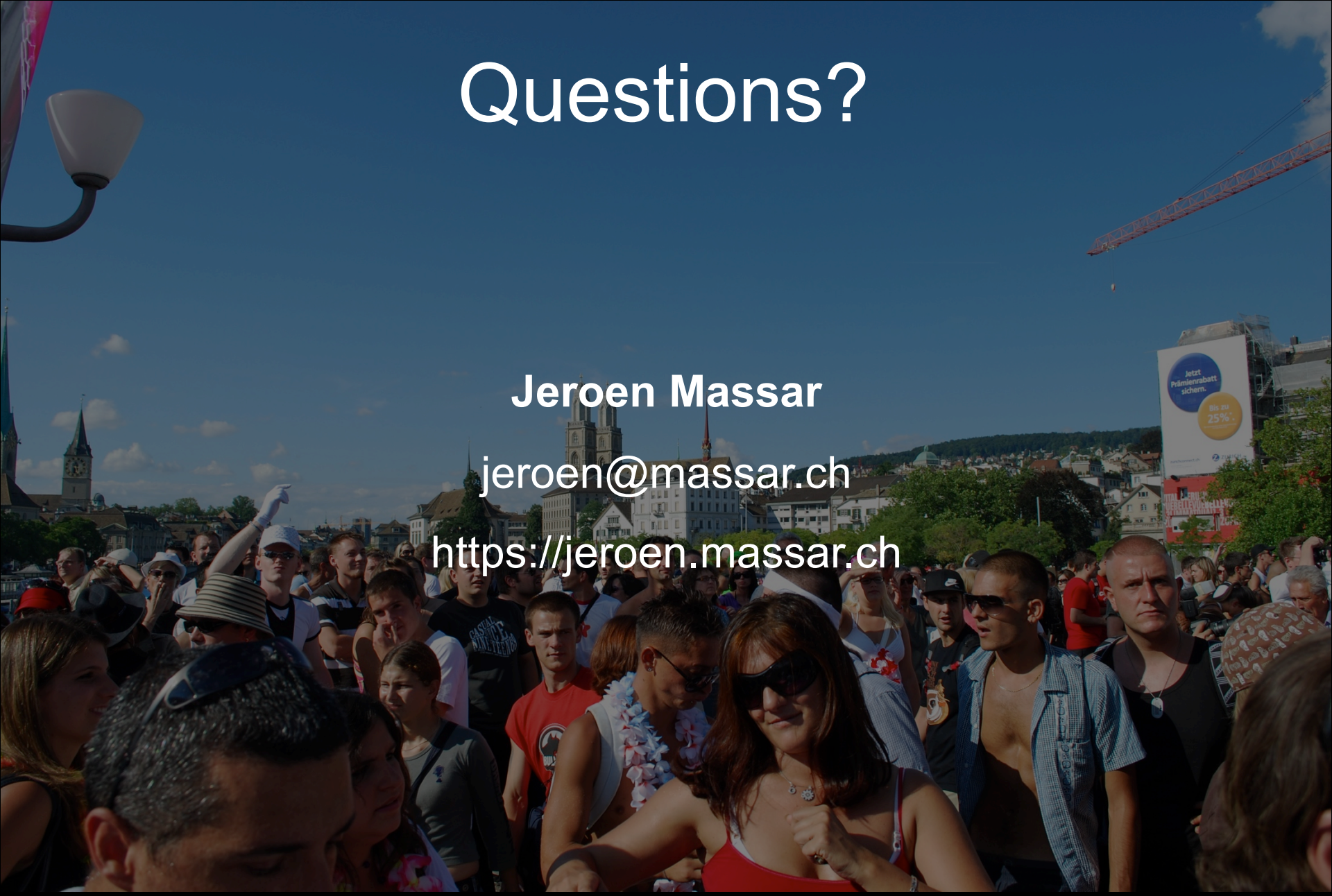
* sphere of trust;
* sphere of action;
* the ability to maintain a "need to know" confidentiality.

Operations Security Trust (or "Ops-T") members are in a position to directly affect Internet security operations in some meaningful way. The community's members span the breadth of the industry including service providers, equipment vendors, financial institutions, mail admins, DNS admins, DNS registrars, content hosting providers, law enforcement organizations/agencies, CSIRT Teams, and third party organizations that provide security-related services for public benefit (e.g. monitoring or filtering service providers). The breadth of membership, along with an action plus trust vetting approach creates a community which would be in a position to apply focused attention on


Mentoring!
36
CAFE ODEON BAR
ODEO


Trust?

Questions?



Jeroen Massar

jeroen@massar.ch

https://jeroen.massar.ch