Inter-Network Cooperation

Cooperation and Coordination

community, sharing,
incident response, trust

Cooperation and coordination

- To keep the Internet working
  - we are relying on each other

- It’s good to know
  - community
  - point of contact

NOGs

- Network Operations Group is an open forum
    - technology discussions
    - sharing operational best practices
    - compare experience
    - peering coordination
    - establishing personal relationships

Medium for NOGs

- Mailing-list
  - anyone can subscribe
  - traffic depends on events and topics
- In-person meeting
  - participation fee varies, and costs of transports, accommodations
  - high value

NANOG

- North American Network Operators’ Group
  - evolved from the NSFNET "Regional-Techs" meetings in 1994
  - Three meetings each year

https://www.nanog.org/

- program
    - 3 days plenary
- about 500 attendees
    - from Asia and Europe as well
- and side meetings

APRICOT

- Asia and Pacific Operations Conference
    - established in 1996
    - co-located with AP* meetings
- held annually on the last week of Feb
- APRICOT2017, Vietnam
- APRICOT2018, Nepal

http://www.apricot.net/

- Program
  - 5 days workshop
  - 4 days conference and tutorial
  - 1 day APNIC member meeting
- About 700 attendees

SANOG

- South Asian Network Operators Group
    - established in 2003
- Two meetings each year
- SANOG29, 2016, Pakistan
- SANOG30, 2017, India

http://www.sanog.org/

- program
  - 5 days workshop
  - 2 days tutorial
  - 2.5 days conference
- about 250 attendees

JANOG

- Japan Network Operators' Group
  - established in 1997
- local language community - Japanese
- Two meetings each year
- JANOG40, Jul 2017, Fukushima
- JANOG41, Jan 2018, Hiroshima

https://www.janog.gr.jp/

- program
  - 1 day tutorial + BoF
  - 2 days plenary
- about 500 attendees

BoFs

- Birds of a feather(BoF) is a small meeting focused on a specific topic
  - security, peering, and so on
- usually scheduled in advance, sometimes organized on demand

Coffee breaks and social events

- To expand relationships
  - business and personal
- To start/manage a project
  - a face-to-face meeting help to step forward things

NOG operation

- Independent
  - a casual and informal meeting among network operators in the region
- Support from cross industry
  - Service Providers
  - Research and Academics
  - Vendors
  - ISOC, NSRC, APNIC, APIA

Anyone can establish a new NOG

- It‘s just a group and gatherings
- No hierarchy
- No formal relationship among NOGs

- The real challenge would be continuation and getting more involvements

The keys of NOG

- Good meeting contents
  - Should meet operators’ needs and interests
- Involvements of local key players
  - Major network operators, technical experts
- Facilitating communications
  - Mailing list and other communication tools
  - Appropriate managements of meeting and events
- Dynamism
  - New attendees
  - A change of committee members

Other upcoming events

- Upcoming network-related education or training events
    - http://ws.edu.isoc.org/calendar/

CSIRT

- Computer Security Incident Response Team(CSIRT) provides the incident handling service for its constituency
    - may offer other related services as well

- The first CSIRT - CERT/CC was created in 1988 in response to the Morris worm incident

Computer security incident

- Any real or suspected adverse event
- examples:
  - attacks to/from your network
  - compromised host
  - account/information theft
  - spam or IT policy violation

Needs for response

- To limit the damage
- To lower the cost of recovery

- An effective response benefits for organizations
  - motivation to have a CSIRT in your organization

The incident handling service

- A single point of contact to receive incident reports
- Provides response and support to the report
- Announcement to disclose information about specific attack/incident
- Feedback to the report/request

Building your CSIRT

- mission statement
    - what/how to do
- constituency
    - for whom
- structure
    - budget, position within organization
- relationship with other CSIRTs

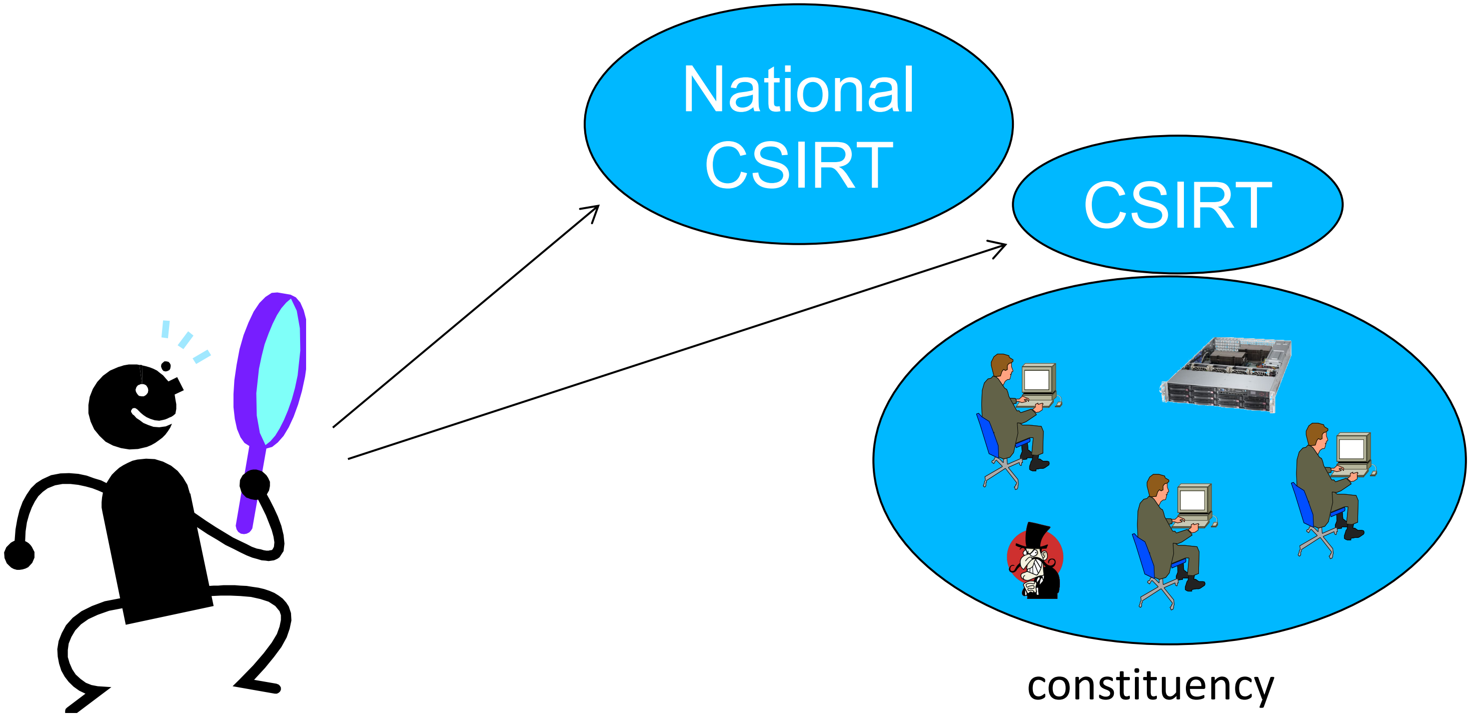
CSIRT types

- National CISRTs
  - a national point of contact to coordinate an incident handling, reduce the number of security incidents in that country
- ISP/xSP CSIRTs
  - provide a secure environment for their customer, and provide response to their customers for security incidents

CSIRT types

- Vendors CSIRTs
  - improve the security of their products
- Enterprise CSIRTs
  - improve the security of their corporation’s infrastructure, and provide on-site response for security incidents

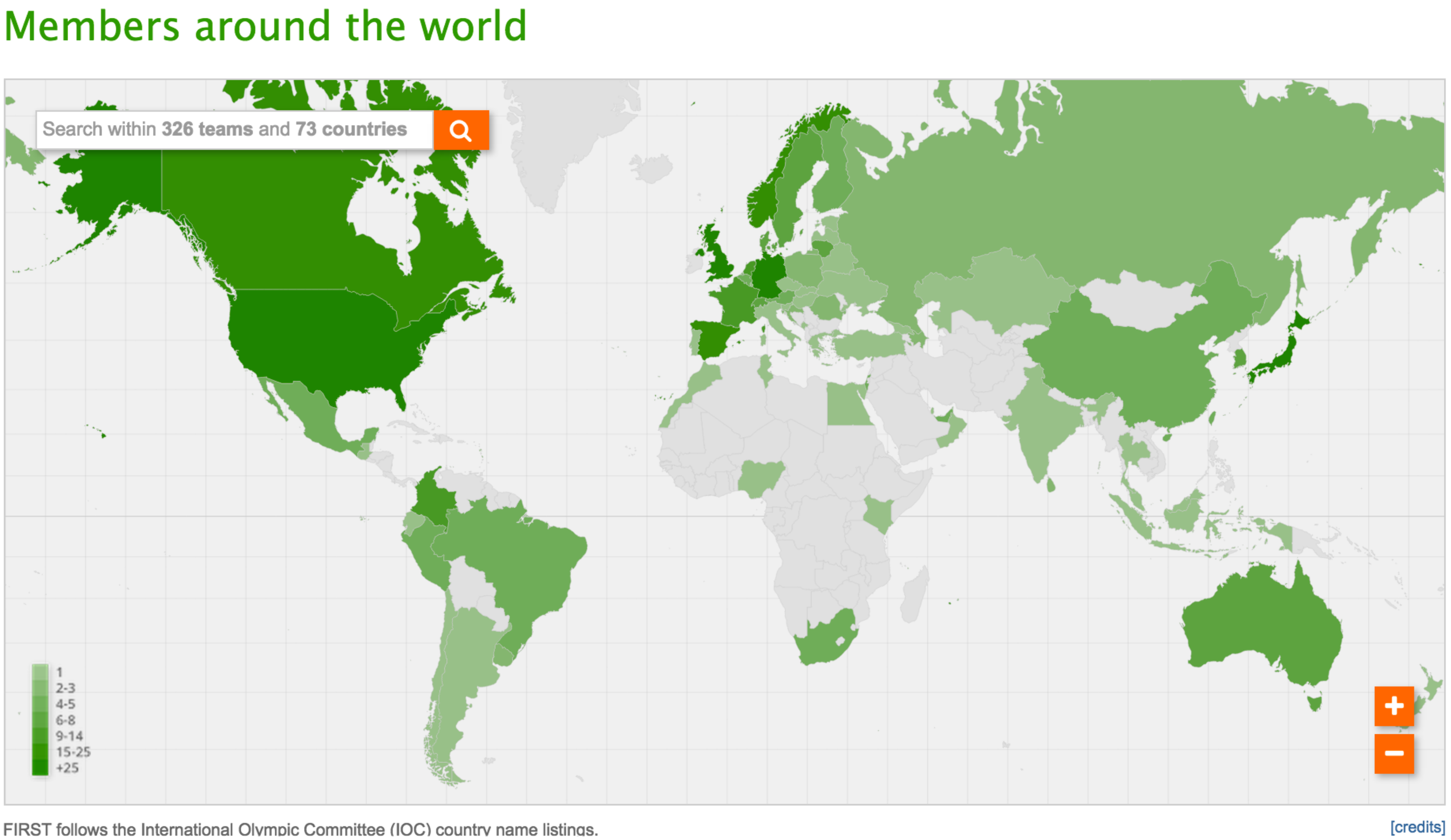
Point of Contact



FIRST

- FIRST is international confederation of trusted CISRTs and security teams.
  - Team constituency, rather than individuals
  - Teams from a wide variety of organizations including educational, commercial, vendor, government and military
- Most services are for members only
- https://www.first.org/

FIRST members

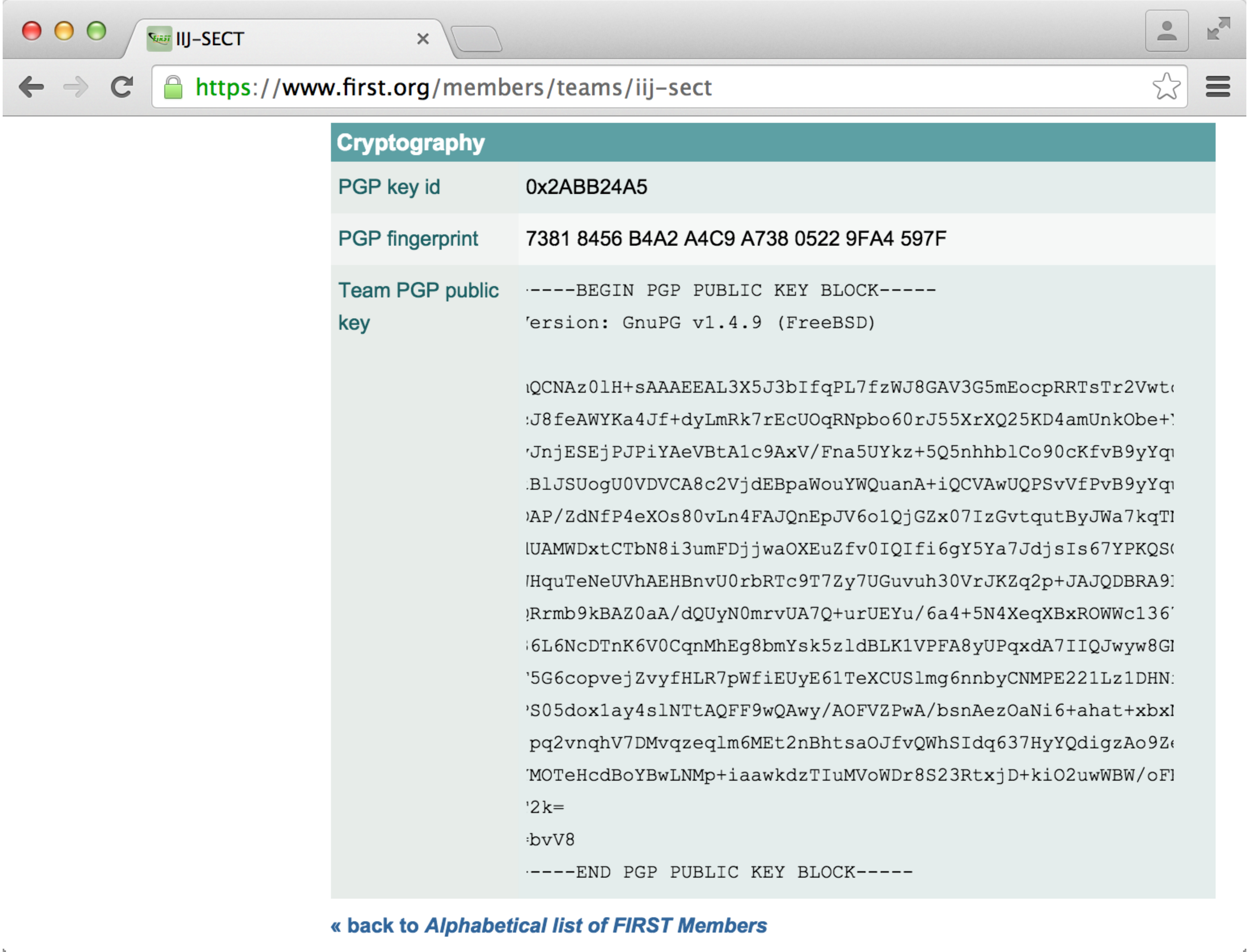


Members around the world

Search within 326 teams and 73 countries

FIRST follows the International Olympic Committee (IOC) country name listings.

[credits]



Cryptography

PGP key id	0x2ABB24A5
PGP fingerprint	7381 8456 B4A2 A4C9 A738 0522 9FA4 597F

Team PGP public key

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
ersion: GnuPG v1.4.9 (FreeBSD)

QCNAz0lH+sAAAEEAL3X5J3bIfqPL7fzWJ8GAV3G5mEocpRRTsTr2Vwt
J8feAWYKa4Jf+dyLmRk7rEcUOqRNpbo60rJ55XrXQ25KD4amUnkObe+
JnjESEjPJPiYAeVBtA1c9AxV/Fna5UYkz+5Q5nhhblCo90cKfvB9yYq
BlJSUogU0VDVCA8c2VjdEBpaWouYWQuanA+iQCVAwUQPSvVfPvB9yYq
AP/ZdNfP4eXOs80vLn4FAJQnEpJV6o1QjGZx07IzGvtqutByJWa7kqT
UAMWDxtCTbN8i3umFDjjwaOXEuZfv0IQIfi6gY5Ya7JdjsIs67YPKQS
HquTeNeUVhAEHBnvU0rbRTc9T7Zy7UGuvuh30VrJKZq2p+JAJQDBRA9
Rrmb9kBAZ0aA/dQUyN0mrvUA7Q+urUEYu/6a4+5N4XeqXBxROWWc136
6L6NcDTnK6V0CqnMhEg8bmYsk5zldBLK1VPFA8yUPqxdA7IIQJwyw8G
5G6copvejZvyfHLR7pWfiEUyE61TeXCUSlmg6nnbyCNMPE221Lz1DHN
S05dox1ay4slNTtAQFF9wQAwy/AOFVZPwA/bsnAezOaNi6+ahat+xbx
pq2vnqhV7DMvqzeqlm6MEt2nBhtsaOJfvQWhSIdq637HyYQdigzAo9Z
MOTeHcdBoYBwLNMp+iaawkdzTIuMVoWDr8S23RtxjD+kiO2uwWBW/oF
2k=
bvV8
-----END PGP PUBLIC KEY BLOCK-----
```

« back to *Alphabetical list of FIRST Members*

to be a FIRST member

1. Find two existing Full Members for nominating your team ("sponsors")
2. Inform FIRST Secretariat (FSS) that your team wants to join FIRST.
3. Work with your sponsors so they have a thorough understanding of your team
4. Arrange for a site visit by at least one sponsor
5. Provide all the mandatory information requested in support to your nomination (see Section 2.1.2 of the FIRST Membership Process document for details).
6. Provide any additional information requested by FIRST
7. Your sponsor will submit your application (after a 6-month period, at most).
8. Board of Directors will deliver on your specific nomination
9. If application is approved, pay the membership affiliation fee.

https://www.first.org/membership

FIRST events

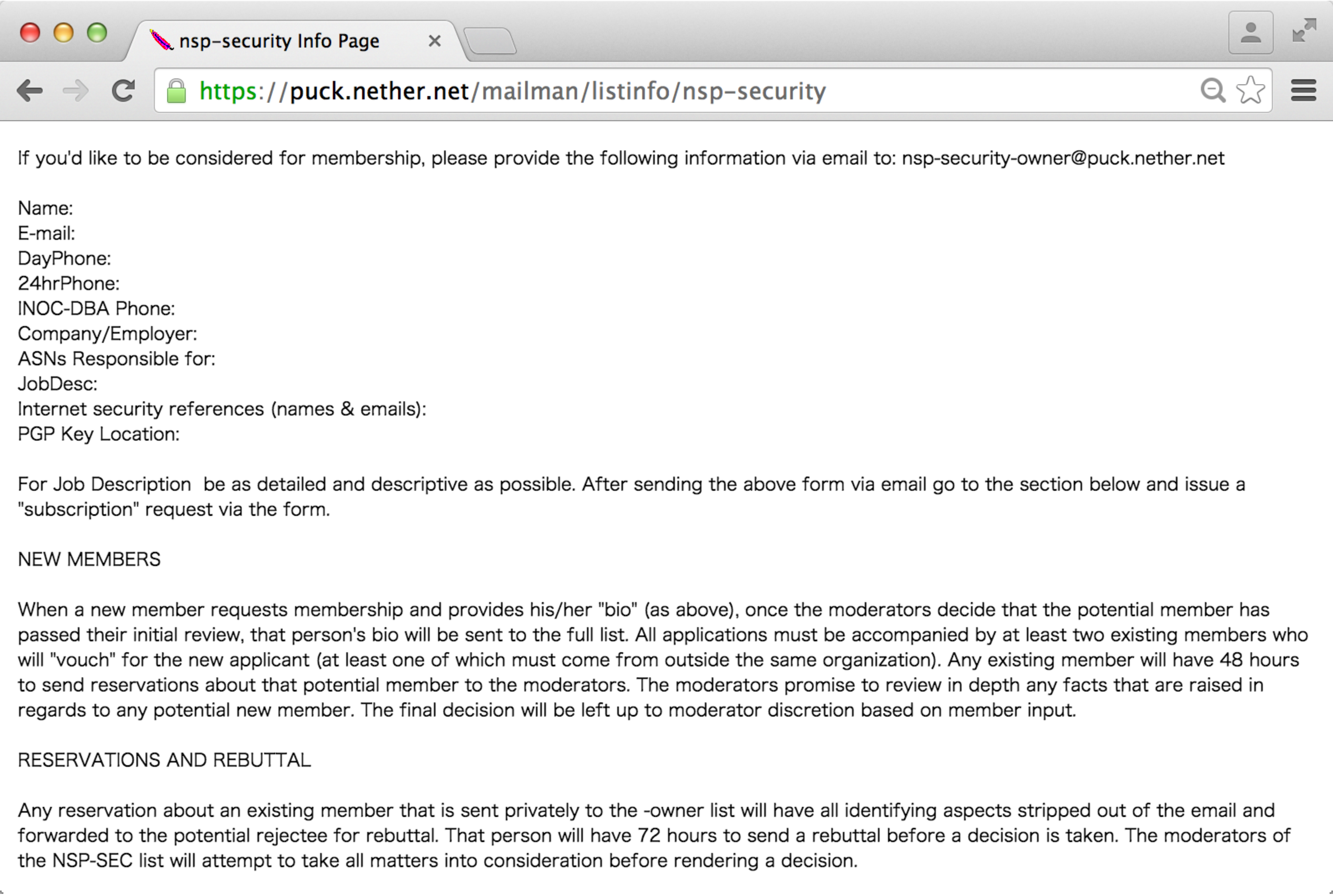
- annual conference
  - every June
  - 29th annual conference
    - San Juan, 11-16 June 2017
  - anyone can attend
- other regional meetings
  - mostly members only

industry based community - ISAC

- Information Sharing and Analysis Center
- Security risks are almost similar in an industry
  - Telecom ISAC
  - Financial ISAC
  - Electricity Sector ISAC
  - ... and many more
- Mostly aiming to protect national critical infrastructures

individual based community

- NSP-SEC
  - https://puck.nether.net/mailman/listinfo/nsp-security
- OPS-TRUST
  - https://openid.ops-trust.net/about



If you'd like to be considered for membership, please provide the following information via email to: nsp-security-owner@puck.nether.net

Name:
E-mail:
DayPhone:
24hrPhone:
INOC-DBA Phone:
Company/Employer:
ASNs Responsible for:
JobDesc:
Internet security references (names & emails):
PGP Key Location:

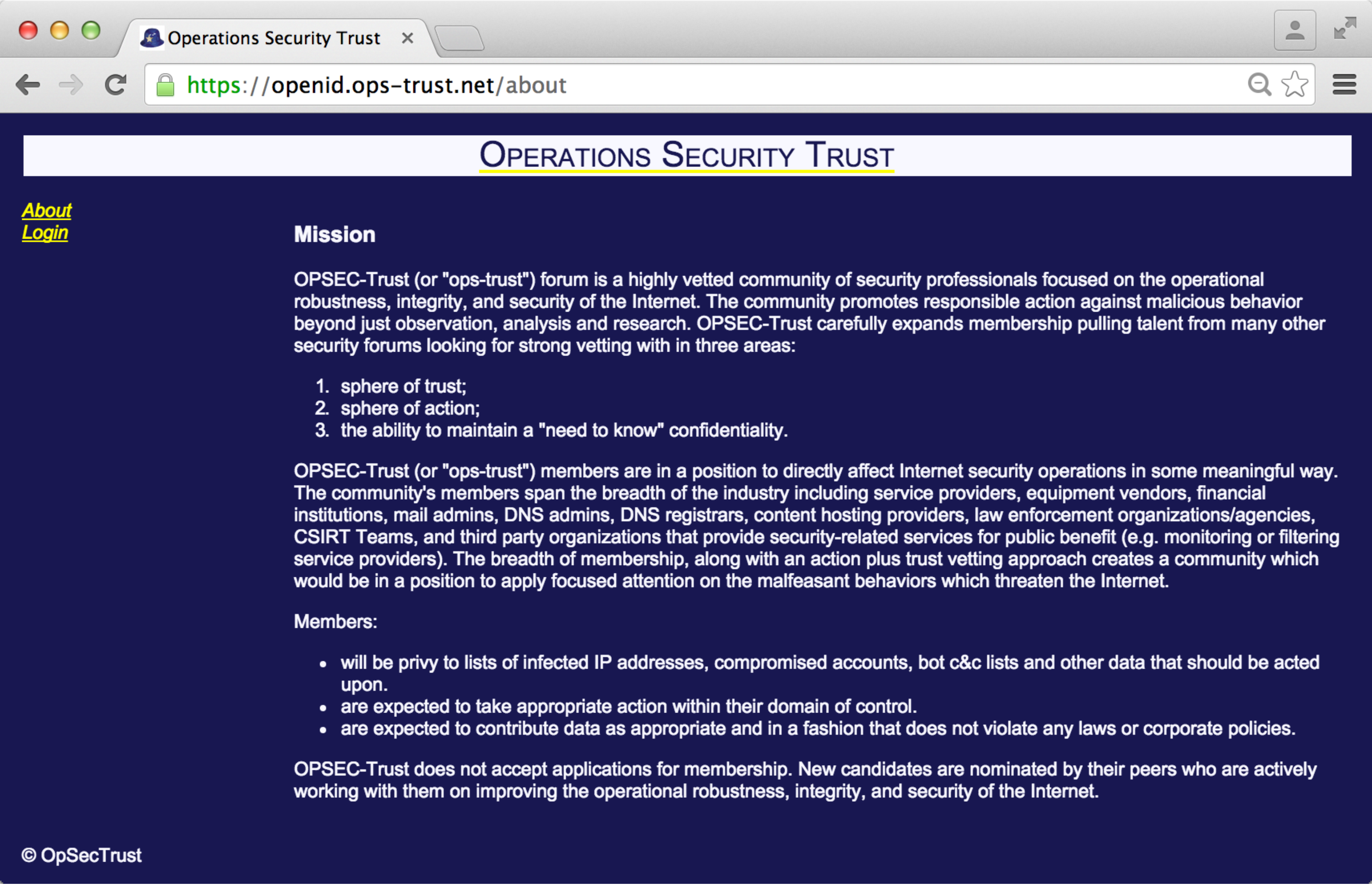
For Job Description be as detailed and descriptive as possible. After sending the above form via email go to the section below and issue a "subscription" request via the form.

NEW MEMBERS

When a new member requests membership and provides his/her "bio" (as above), once the moderators decide that the potential member has passed their initial review, that person's bio will be sent to the full list. All applications must be accompanied by at least two existing members who will "vouch" for the new applicant (at least one of which must come from outside the same organization). Any existing member will have 48 hours to send reservations about that potential member to the moderators. The moderators promise to review in depth any facts that are raised in regards to any potential new member. The final decision will be left up to moderator discretion based on member input.

RESERVATIONS AND REBUTTAL

Any reservation about an existing member that is sent privately to the -owner list will have all identifying aspects stripped out of the email and forwarded to the potential rejectee for rebuttal. That person will have 72 hours to send a rebuttal before a decision is taken. The moderators of the NSP-SEC list will attempt to take all matters into consideration before rendering a decision.



Operations Security Trust

Mission

OPSEC-Trust (or "ops-trust") 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. OPSEC-Trust 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.

OPSEC-Trust (or "ops-trust") 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.

OPSEC-Trust does not accept applications for membership. New candidates are nominated by their peers who are actively working with them on improving the operational robustness, integrity, and security of the Internet.

CVE

- Common Vulnerabilities and Exposures
- Dictionary of common names (ex. CVE identifiers) for publicly known security vulnerabilities
- https://cve.mitre.org/

- We can use a common name to specify a security vulnerability

example: CVE-2015-5986

- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5986
- target
  - ISC BIND 9.9.7 before 9.9.7-P3 and 9.10.x before 9.10.2-P4
- impact
  - vulnerable ISC BIND allows remote attackers to cause a denial of services

ISC BIND release note

- https://kb.isc.org/article/AA-01301/81/BIND-9.10.2-P4-Release-Notes.html

Introduction

:

BIND 9.10.2-P4 addresses security issues described in CVE-2015-5722 and CVE-2015-5986.

CVSS

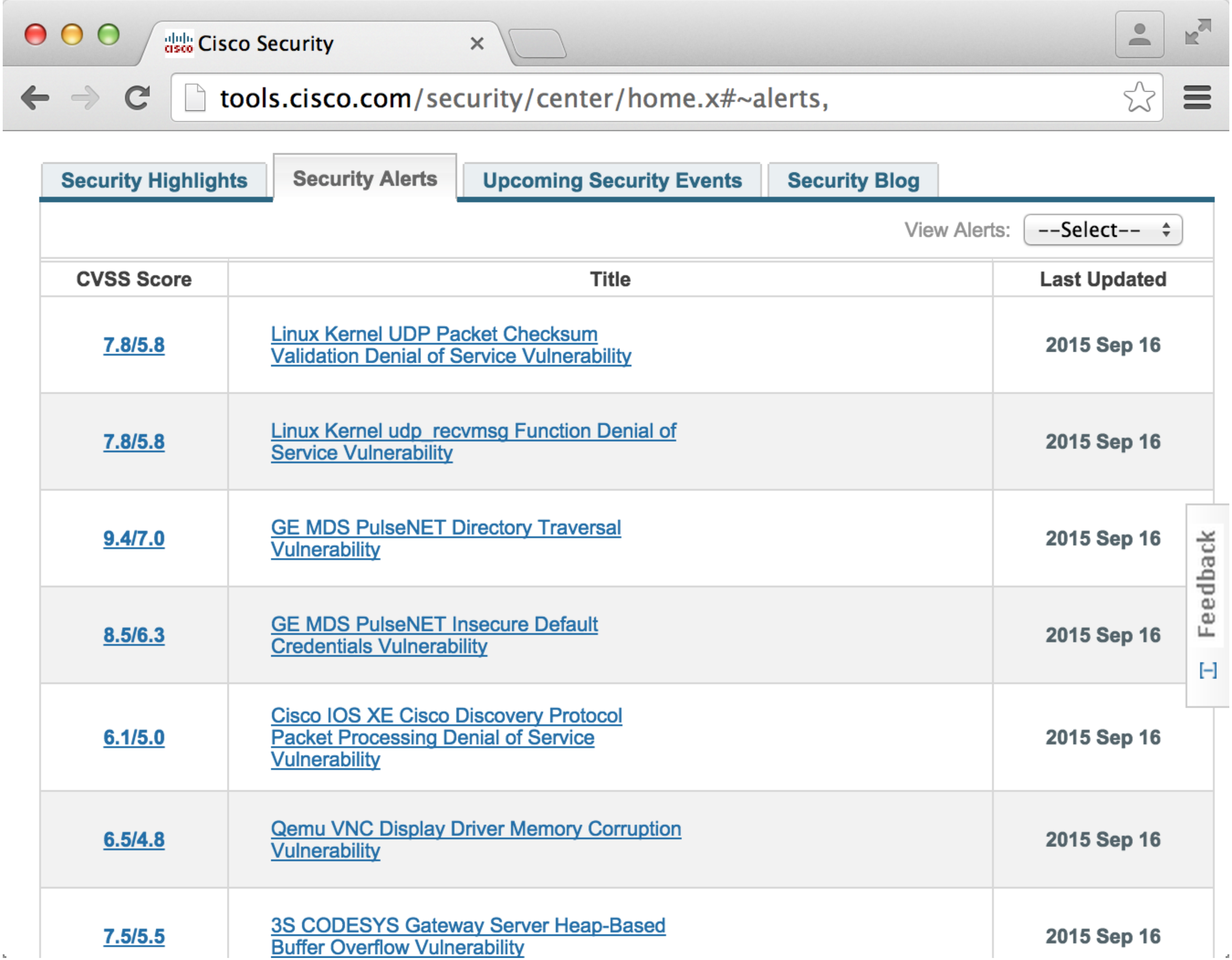
- Common Vulnerability Scoring System
- https://www.first.org/cvss/
  - CVSSv3 is released in 2015
- An open framework for communicating the characteristics and impact of IT vulnerabilities

CVSS Scores

- Base Score
  - technical evaluation
- Temporal Score
  - environmental evaluation
  - proof of concept code/attack code
  - could be changed over the time

CVSS Scores

Security Level	Score
Critical	9 - 10
High	7 - 8.9
Medium	4 - 6.9
Low	0.1 - 3.9
Info	0



View Alerts: --Select--

CVSS Score	Title	Last Updated
7.8/5.8	Linux Kernel UDP Packet Checksum Validation Denial of Service Vulnerability	2015 Sep 16
7.8/5.8	Linux Kernel udp_recvmsg Function Denial of Service Vulnerability	2015 Sep 16
9.4/7.0	GE MDS PulseNET Directory Traversal Vulnerability	2015 Sep 16
8.5/6.3	GE MDS PulseNET Insecure Default Credentials Vulnerability	2015 Sep 16
6.1/5.0	Cisco IOS XE Cisco Discovery Protocol Packet Processing Denial of Service Vulnerability	2015 Sep 16
6.5/4.8	Qemu VNC Display Driver Memory Corruption Vulnerability	2015 Sep 16
7.5/5.5	3S CODESYS Gateway Server Heap-Based Buffer Overflow Vulnerability	2015 Sep 16