Inter Network Cooperation

Merike Kaeo
merike@doubleshotsecurity.com

Operational Security Communities

- What are Operational Security Communities?
- Key Principles for how they work (and not work).
- NSP-SEC Example
- Communities Examples
- OPSEC Trust – Evolution Continues
- FIRST Example
- Summary

Introduction

- There are effective Private Industry “Operational Security” Communities that specialize.
  - Financial Industry
  - Telecommunications Industry
- Effective Incident Response, Cyber-Risk Management, and Investigations require active participation and collaboration in these “Operational Security Communities.”
- These communities have rules, expectations, “trust networks,” and paranoia that makes it hard to find and hard to gain access.
- The presentation’s goal will help organizations understand what the community is all about, how to work with these communities, and how to enter these communities.

Example of Specializations

- Situational Consultation: **OPSEC Trust's Main Team**
- Big Back Bone Security and IP Based Remediation: **NSP-SEC**
- DNS System Security: **DNS-OARC**
- Anti SPAM, Phishing, and Crime: **MAAWG & APWG**
- Vulnerability Management: **FIRST**
- Many other Confidential Groups specializing into specific areas, issues, incidents, and vulnerabilities.

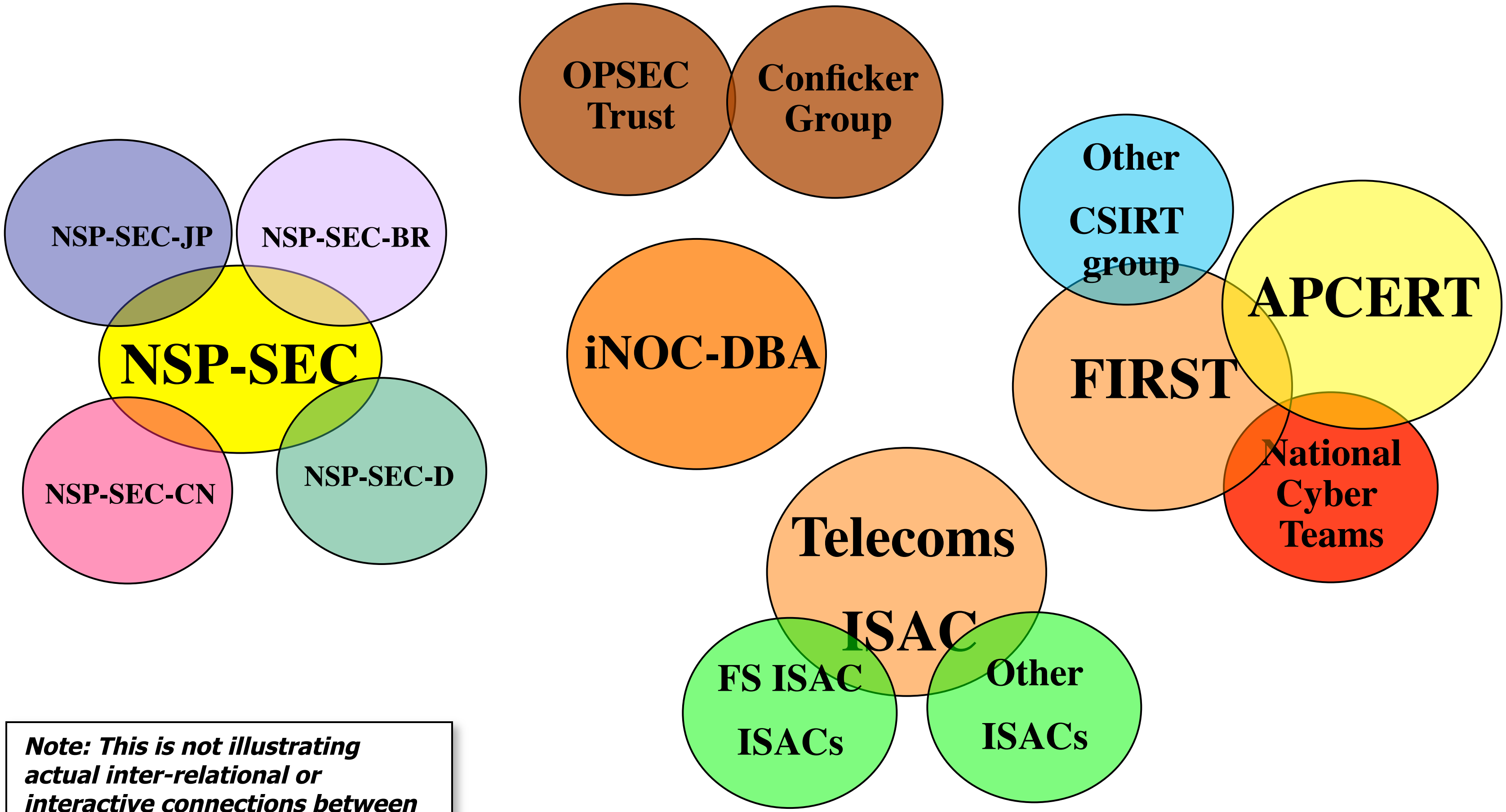
The *Real* Security Problem

- In 2002 ISP/SP Operations Security Engineers could not:
  - Find their *security* colleagues in their directly attached peers.
  - Find security engineers in providers two hops away.
  - Find any security engineers in the big Asia providers.
- If big attacks happened, there was no way for the people who needed to work with each other to <u>find</u> each other, let alone work collectively to mitigate the attack

2003 – A Year of Difference

- Since 2003 ISP/SP Operations Security Engineers can:
  - Find their *security* colleagues in their direct peers and a huge range if global ISP/SPs
  - Work with each other via E-mail, chat, iNOC Phone, and POTs to collectively mitigate attacks and incidents on the Internet
  - Execute Inter-provider Tracebacks and Mitigation
  - Proactive measures to prepare for projected attacks
- What changed?

Aggressive Collaboration is the Key



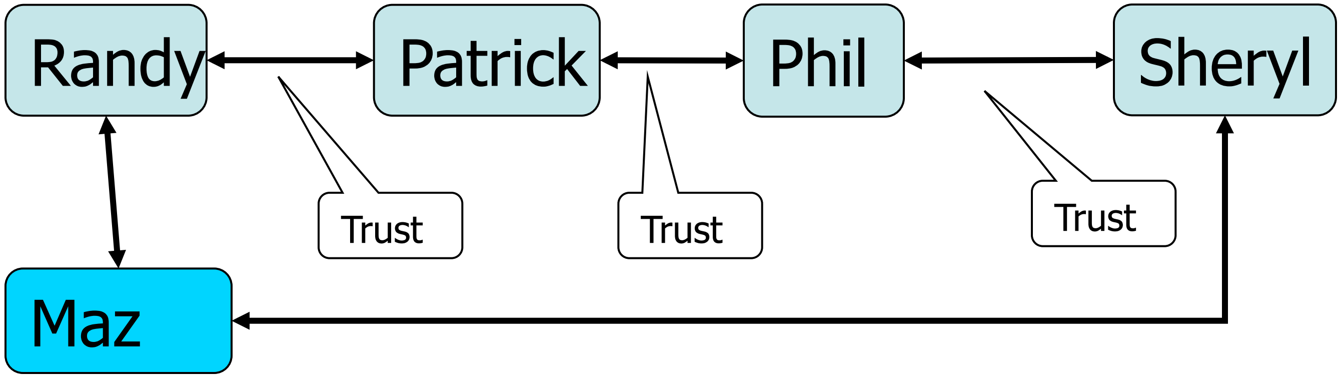
Note: This is not illustrating actual inter-relational or interactive connections between the different communities.

Principles of Collaboration Between Chains of Trust

- Chain of Trust
  - Similar to PGP
  - Transitive trust (with varying degrees)
- Sphere of Trust
- Need to Know
- Chain of Action (new)

Chain of Trust

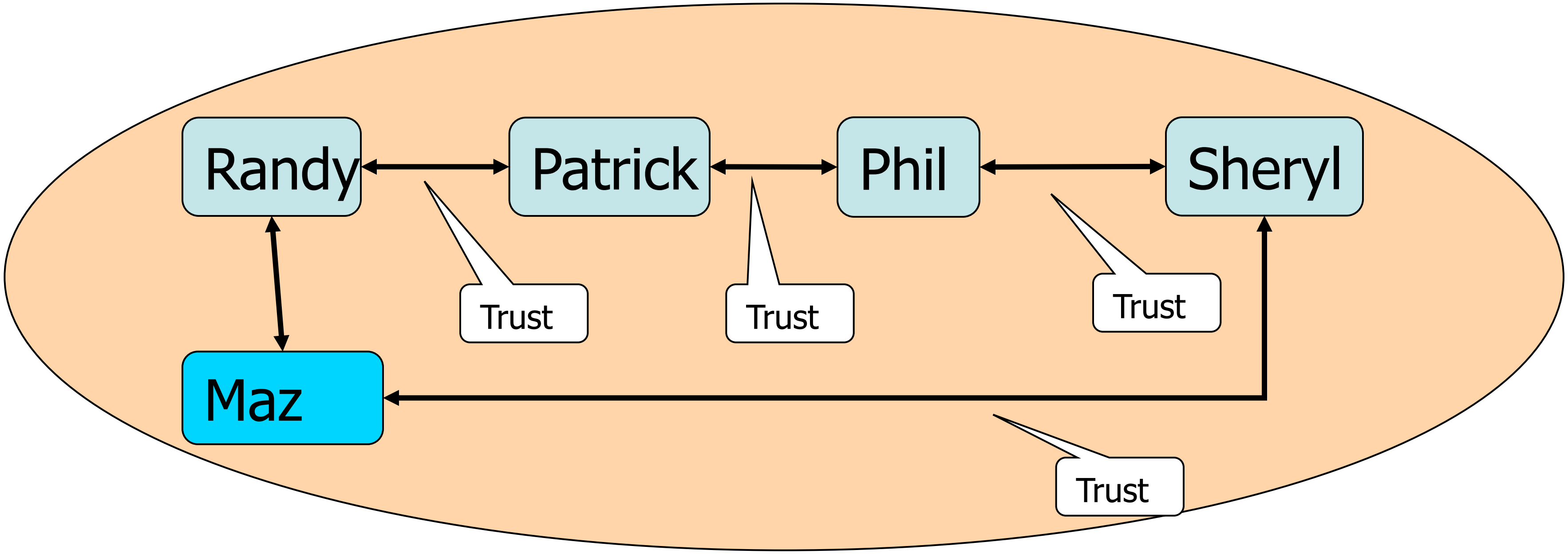
- If I trust you and you trust him, then I can also trust him.



Because Maz trusts Randy, Maz can also trust Patrick.

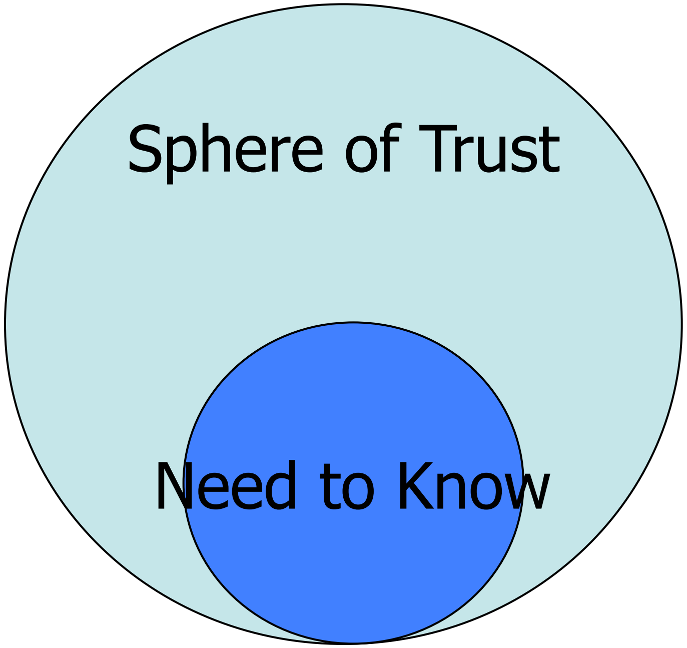
Sphere of Trust

- The group together can be see as a sphere, realm, zone, of trust.



Need to Know in Operation Security

- I trust you. You are someone I can depend on, but you don't really need to know about the details of this incident.
- Not being in a *Need to Know Sphere* does not mean you are not trusted.



Sphere of Action

- You trust someone, but will they be able to do something, be responsive, and/or make something happen?
- Sphere of Action and Chain of Action is a new concept for vetting peers into operational communities.
- Some communities would like to just know something will happen.

> I've been working an attack against XXX.YY.236.66/32 and XXX.YY.236.69/32. We're seeing traffic come from <ISP-A>, <ISP-B>, <IXP-East/West> and others.
>
> Attack is hitting both IP's on tcp 53 and sourced with x.y.0.0.
>
> I've got it filtered so it's not a big problem, but if anyone is around I'd appreciate it if you could filter/trace on your network. I'll be up for a while :/

Expectation of Action

- “Lurking” is bad behavior on Operational Security Communities.
- There is an expectation of action – where you use the information to do something within your span of control & influence to fight the badness.
  - Collect more data and share.
  - Use your product to act.
  - Use the information to act (i.e. operator)
  - Improve your product or network.
- *Inability to meet expectations erodes trust and your reputation of someone who acts.*

Community's Integrity

- Maintaining integrity is common sense
- Never **ever** forward information posting within a operational security group without the explicit permission of the person who posted the information
  - Immediate breach of trust
  - Violation of the integrity of the community
- Each individual is accountable to be a steward of the information posted and discussed within the community

NSP-SEC

- NSP-SEC was created by several ISP/SP Security Engineers as a means to meet the following objectives:
  1. Provide a means for ISP/SP Security Engineers to find their colleagues
  2. Create a potential forum for ISP/SP Security Engineers to work on DOS attacks, incidents, and other activities

Finding their Colleagues was the Key

- We know that:
  - Two engineers working together to mitigate an incident is more effective than one engineer working alone
  - Incident mitigation is faster if engineers can communicate with each other during an incident
- NSP-SEC provides that means to find colleagues and perhaps – work on the incidents
  - It is not the exclusive mode of collaboration
  - "Point to Point" collaboration outside of NSP-SEC does happen and is strongly promoted.

NSP-SEC – The Details

- NSP-SEC – *Closed* Security Operations Alias for engineers actively working with NSPs/ISPs to mitigate security incidents.
- Multiple Layers of sanity checking the applicability and trust levels of individuals.
- Not meant to be perfect – just better than what we had before.
- NSP-SEC “hides in plane sight – where anyone interested can find, but not be privy to need to know consultation/actions
  - http://puck.nether.net/mailman/listinfo/nsp-security

NSP-SEC Membership Requirements

Membership in nsp-sec is restricted to those actively involved in mitigation of NSP Security incidents. Therefore, it will be limited to operators, vendors, researchers, and people in the FIRST community working to stop NSP Security incidents. That means no press and (hopefully) none of the "bad guys."

http://puck.nether.net/mailman/listinfo/nsp-security

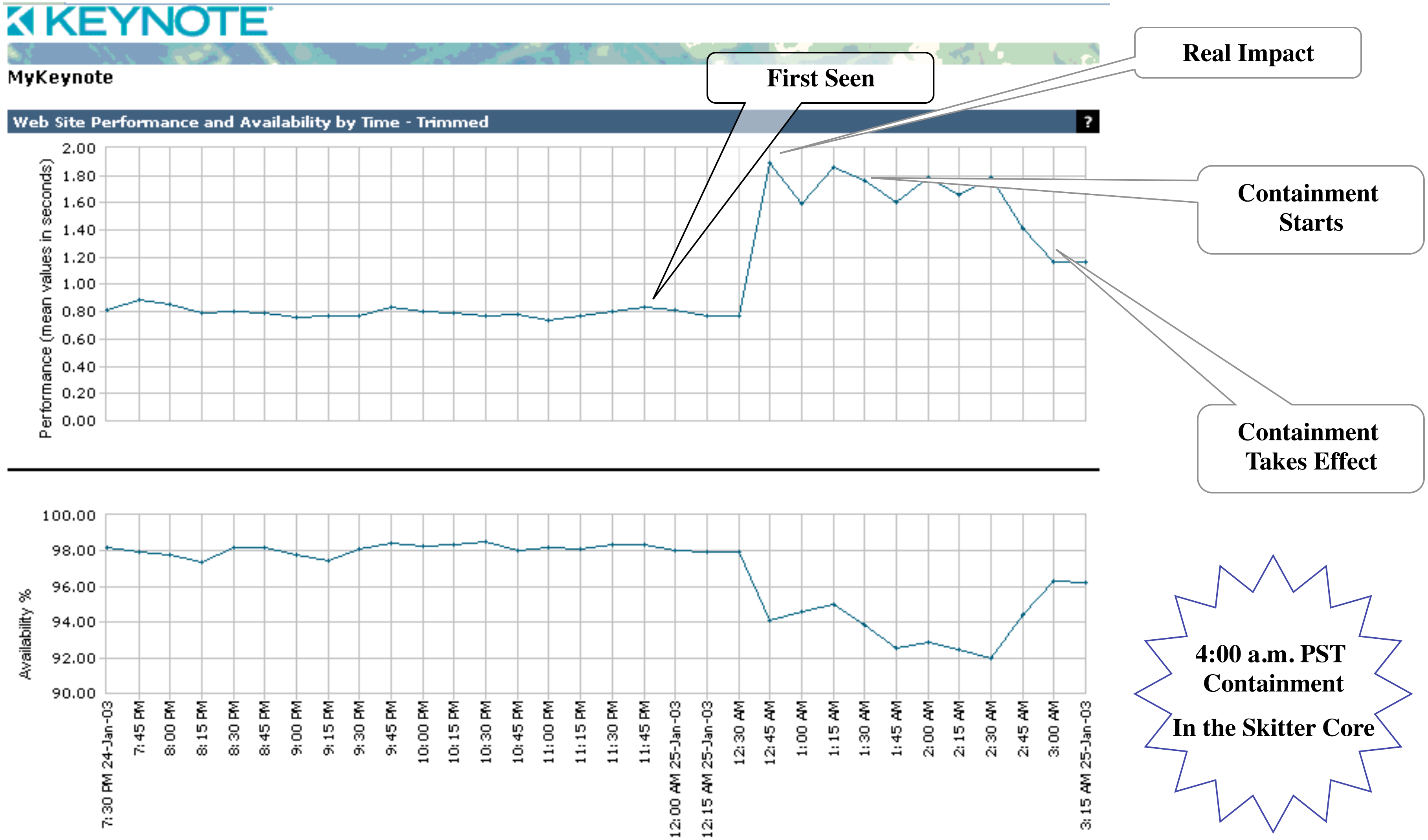
NSP-SEC Membership Requirements

- Being a “Security Guru” does not qualify for NSP-SEC Membership.
- Being “from the *Government*” does not qualify for NSP-SEC Membership.
- You need to be someone who *touches* a router in a ISP/SP backbone, can tell someone to *touch* a router, offer some *service* to the forum, or develop BCPs for the community.
- If you do not contribute, you do not get to participate.

NSP-SEC's Role during Slammer

- The ISPs were the first to notice something was happening
  - Circuits saturated, routers spiking, BGP sessions flapped, and customers complained
- NSP-SEC was the first reporter of the worm
- CERT/FIRST Teams got their alert from NSP-SEC
- NSP-SEC members were the ones who dump the packets, analyzed the worm, characterized its spread, and came up with a way to contain the worm

Impact of NSP-SEC's Containment



MyKeynote

Web Site Performance and Availability by Time - Trimmed

Real Impact

First Seen

Containment Starts

Containment Takes Effect

4:00 a.m. PST Containment

In the Skitter Core

Operational Security Group Examples

- The following are some example which will provide you a tool and context of the types of groups.
  - Some are open to all.
  - Some are personality driven
  - Some are interest driven
  - Some are highly peer vetted
  - Some are peer meshed – where only the best of the best are involved (definition of best varies on who you talk to ☺)

DNS Operations

- An open public forum for informal reporting, tracking, resolving, and discussing DNS operational issues including outages, attacks, errors, failures, and features. Note that discussion of non-ICANN root systems is explicitly off-topic.
- https://lists.dns-oarc.net/mailman/listinfo/dns-operations
- Sponsored by DNS-OARC
  - www.dns-orac.net

OPSEC Trust Mission

OPS-TRUST

Mission

OPSEC-Trust (or "ops-trust") is a highly vetted community of security professionals focusing on the operational robustness, integrity, and security of the Internet. The community promotes mindful action against malicious behavior vs observation/analysis/research. OPSEC Trust carefully expands membership pulling from talent in many other security forums looking for strong vetting with in three areas ; sphere of trust, sphere of action, and 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 breath of the industry including service providers, equipment vendors, financial institutions, mail admins, DNS admins, and 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 a an action/trust vetting approach provides creates a community which would be in a position to apply focused attention on the malfeasant behaviors which threaten the Internet.

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.

https://ops-trust.net/

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 mission statement

- FIRST members develop and share technical information, tools, methodologies, processes and best practices
- FIRST encourages and promotes the development of quality security products, policies & services
- FIRST develops and promulgates best computer security practices
- FIRST promotes the creation and expansion of Incident Response teams and membership from organizations from around the world
- FIRST members use their combined knowledge, skills and experience to promote a safer and more secure global electronic environment.

annual FIRST conference

- Open to anyone
  - Any individual with interest, involvement or responsibility in the field of incident response and computer security
- 26th annual FIRST conference
  - Boston, USA
  - 22 -27 Jun 2014
- http://conference.first.org/

The Security World has Changed!

- Research, Vendor, and Security hacking used to be the core drivers in the cyber-security world’s “white hat” community.
- Today, the industry drive and innovation is directly related to an “Operational Security” community where trust, action, and results are dominating factors.