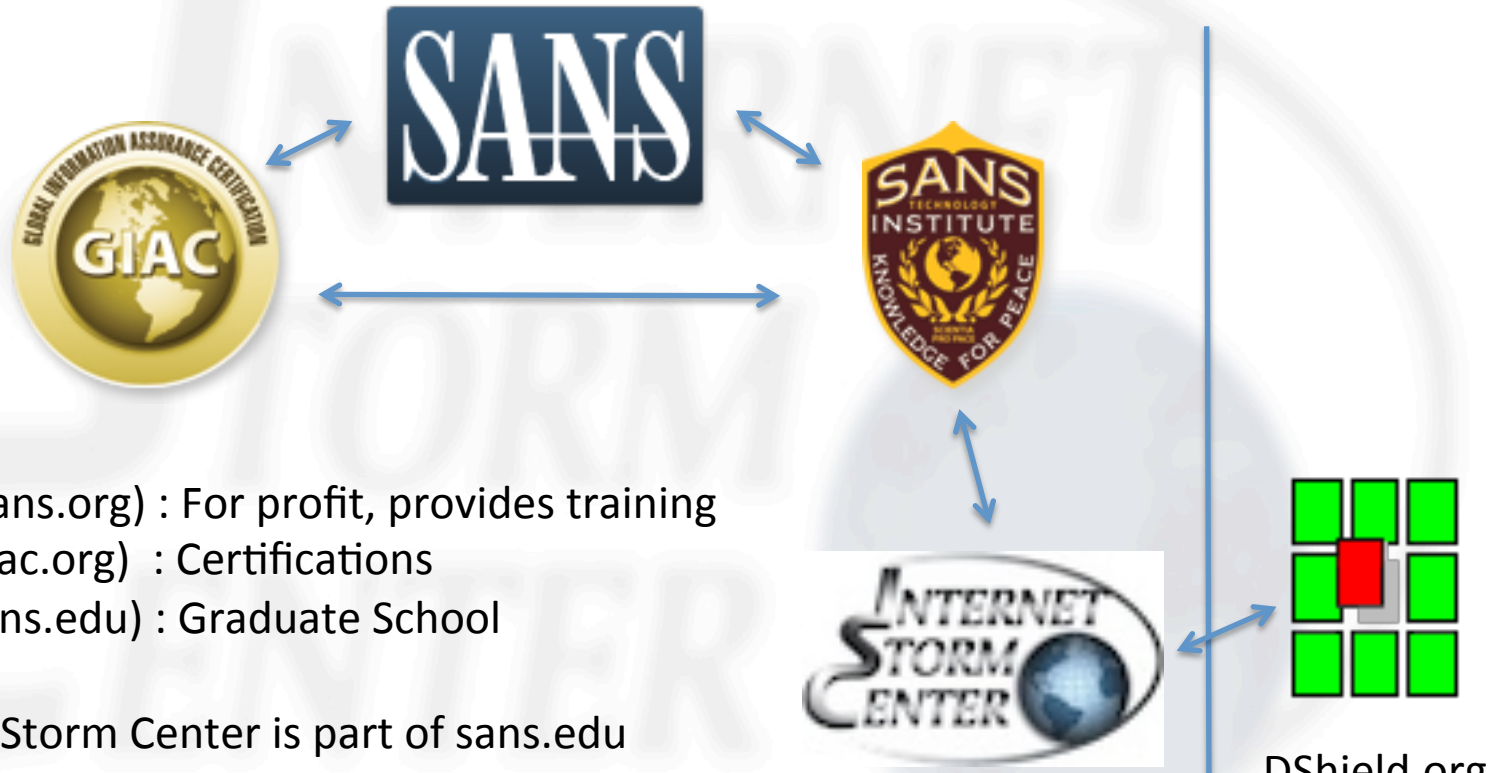
Dshield VPS Sensors request

Intro by Erik Bais on behalf of ISC SANS

vpssensor@dshield.org

SANS / ISC Org Chart



SANS (sans.org) : For profit, provides training
GIAC (giac.org) : Certifications
STI (sans.edu) : Graduate School

Internet Storm Center is part of sans.edu

DShield (dshield.org): distinct entity, not-for-profit.

Brief History

- End 1999: SANS starts “incidents.org” with the mission to coordinate security issues around Y2K.
- Incidents.org survived after Y2K, was found useful as a cooperative security resource
- End 2000: DShield.org started by Johannes Ullrich as a hobby/experiment
- 2001: Johannes hired by SANS to lead Incidents.org
- 2002/3: Incidents.org -> isc.sans.org
- Around 2010: isc.sans.org becomes part of STI (isc.sans.edu)

Internet Storm Center (https://isc.sans.edu)

- Operated by volunteers (“Handlers”)
- Currently about 30 handlers
- Handlers are security practitioners with a diverse background (different industries and countries)
- Main focus is to quickly disseminate information about current threats

DShield.org

- Initially designed to collect firewall logs from home users
- Since expanded to other logs ("404 project", Web application honeypot, ssh scans)
- Started to deploy low interaction honeypots as sensors.

DShield Data Sharing

- "Creative Commons Non Commercial Share Alike License"
- Summary: We share all data, as long as you don't resell it. Just give us credit
- Used in numerous papers / publications. Accessible via web site and APIs

The idea we wanted to pitch today ...

- Setup VPS's in various networks.
- Ask the ISP's to route their allocations (v4 AND v6) to the VPS sensor.
- Manage the sensors centrally using Puppet and centralize the logging.

What will you get out of it...

- ISP will retain full access and obtain customized reports summarizing activity from its system(s)
- The data will be used to give quicker insight in new scans globally.
- Access to the ISC SANS Handlers to discuss security related issues in your network.

Honeypot VPS

- Based on latest Ubuntu
- Low interaction honeypot using kippo and other similar tools (honeyd..)
- Collecting firewall logs from all closed port
- IPv4/6 dual stack preferred
- Require ssh access for remote maintenance

How can you help

- Provide one of the 20 planned VPS's (image can be provided)
- Point your allocations to the VPS, so all un-used IP space is monitored.
- Email us at vpssensor@dshield.org

URLs

- SANS Internet Storm Center: http://isc.sans.edu
- More in-depth preso about ISC SANS & Dshield - https://isc.sans.edu/presentations/london2007.pdf
- ISC API: http://isc.sans.edu/api

Questions ?

- Who has the first question ...

  Or the first VPS .... ☺

Contact us

- Thank you for your time & attention

vpssensor@dshield.org