

the evolution of collective intelligence

claimid.com/wesyong

know thy audience

know thy presenter.

REN-What?

- The REN-ISAC mission is to aid and promote cyber security operational protection and response within the higher education and research (R&E) communities. The mission is conducted within the context of a private community of trusted representatives at member institutions, and in service to the R&E community at-large. REN-ISAC serves as the R&E trusted partner for served networks, the formal ISAC community, and in other commercial, governmental, and private security information sharing relationships.

The Basics.

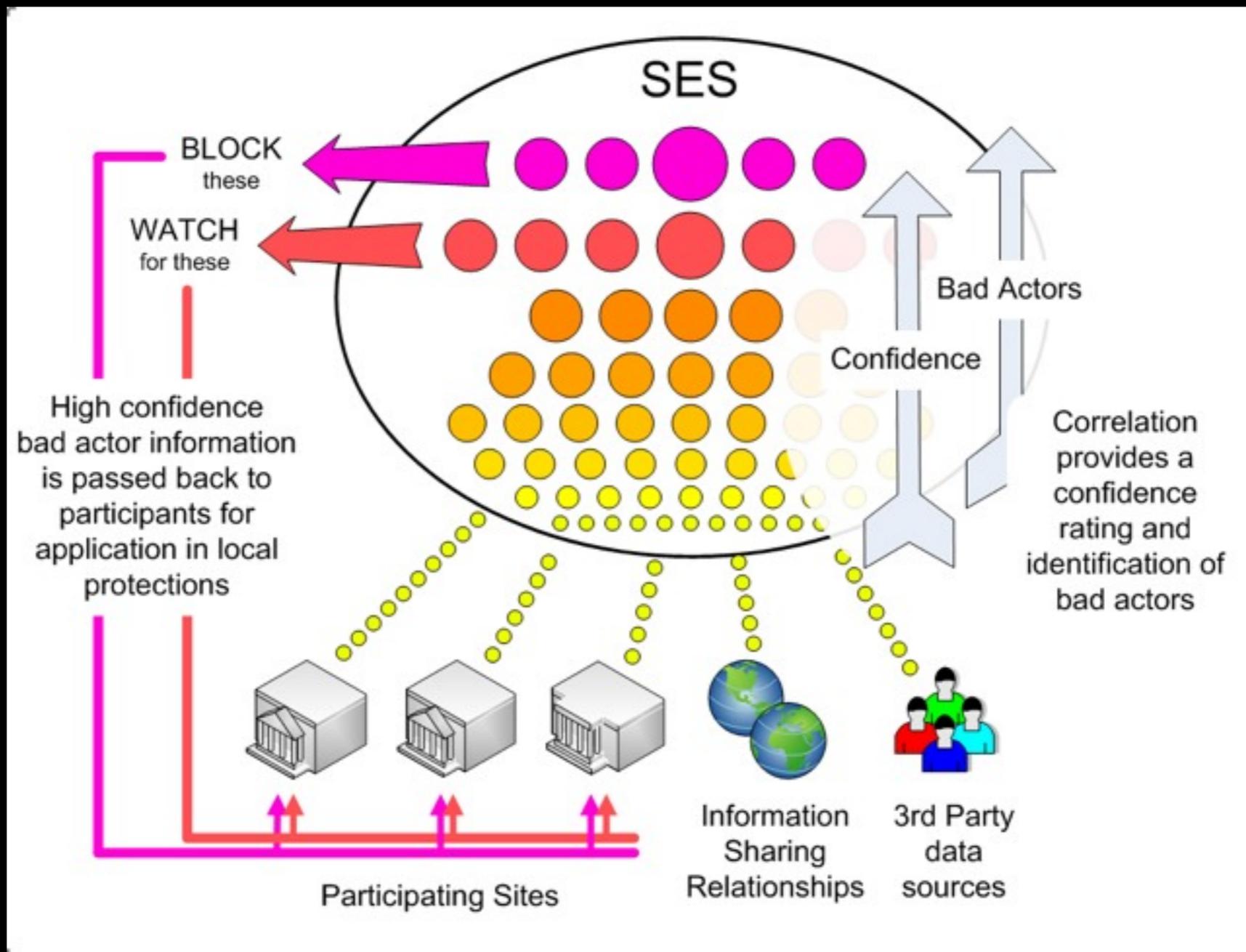
- we send 10-12k notifications to all of north american .edu per month, we act like a CSIRT
- we provide community resources that allow our membership to communicate threat / experience data in a “safe space”
- create trusted interfaces between our membership and the rest of the world (leo, private industry, public resources, etc)
- we also build tools, participate in standards discussions and drink beer.

with-in the REN-ISAC membership

- 325+ Institutions (500+ 'distinct' campuses, state-systems, etc)
- 825+ individual members (role is firefighting with enterprise responsibility)
- Mostly North America (few scattered throughout other english speaking countries)
- lots of ipv4 allocations
- lots and lots of ipv6 allocations in production
- big bandwidth
 - typically a few hundred meg to multi-gig pipes
 - internet2 backbone -- 40-100 gig
- lots of different cultures, perceptions, ideals
- lots of diverse students (laptops coming and going from .kr, .cn, .us, .eu, .etc)
- firewalls... ha. yea right. Not enough tequila for that rat-hole.
- Everyone is their own unique snowflake
- we're solving the information sharing problem within this context.

to the point

the Security Event System



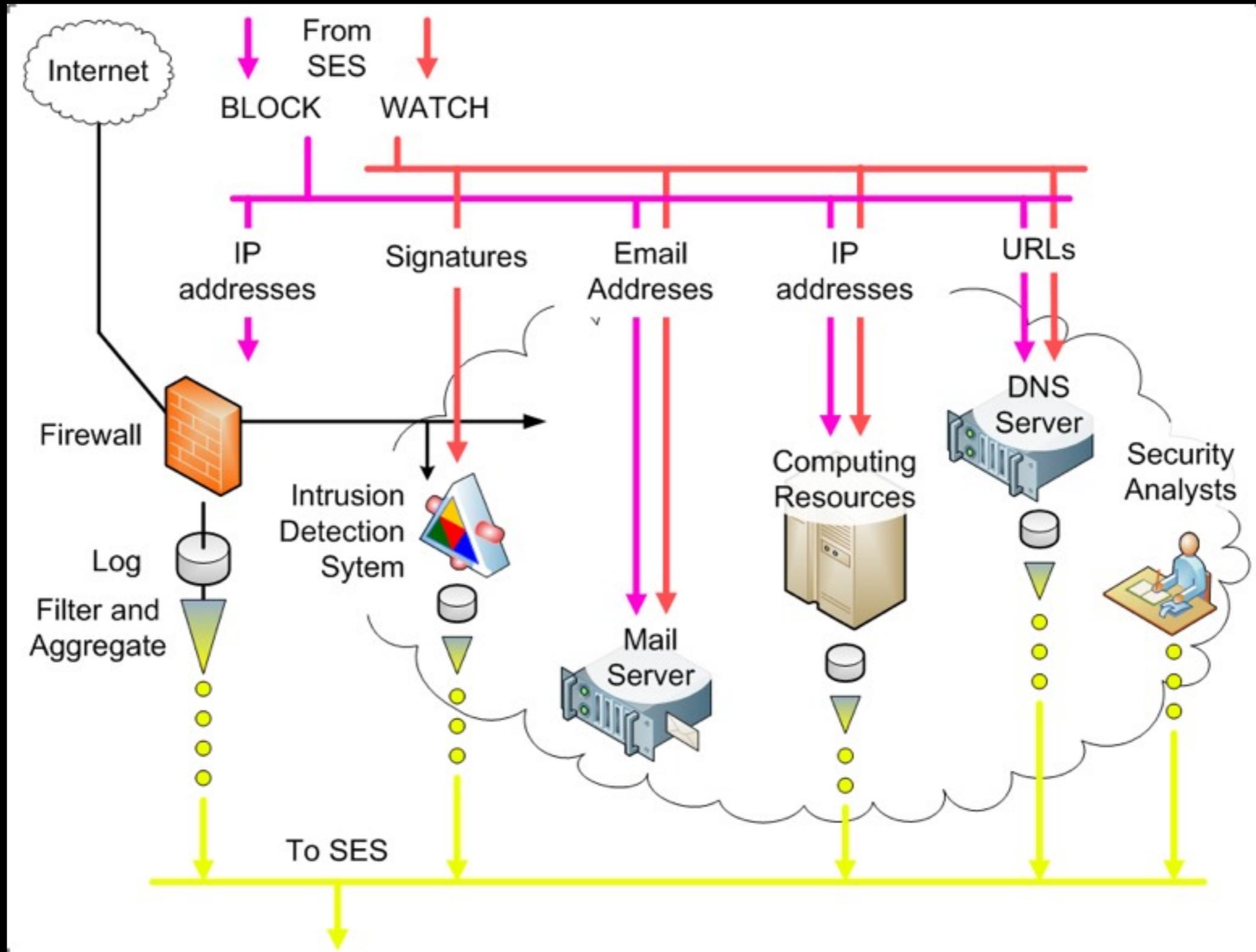
some history

- August 2008
 - Development began on v1 (courtesy of Internet2 and the DoJ)
- Feb 2009 - May 2010
 - v1 Beta within RI community
- January 2010 (courtesy of our member fee's)
 - v2 prototype development started
- May 2010
 - production v1 deployment to RI community
- August 2010
 - v2 Beta2 deployment to select members of RI Community
- August 2011
 - v2 Beta3 deployment to entire RI community
- October 2011
 - v2 Production Deployment
- November 2011 (Courtesy of the NSF)
 - v3 prototype development begins (more on that towards the end)

SES v1 goals

- Mostly “event” standardization (IDMEF)
- Extending existing tools (RT, Prelude, etc...)
- Federation-al involvement
- Security Event Management
- Generating Intelligence Feeds (Block lists, etc)
- provide simple, false-positive proof correlation
- Lower the barriers to entry when it comes to data-sharing

Machine-to-Machine



how v1 rolled out.

- “SES” has 10+ sites Sharing automated, machine generated data between 50 and 20,000 data-points per day per site.
- (SSH|Telnet|FTP|VNC|Pushdo|Darknet) Scanners.
- Near realtime in most cases, from live sensors as well as honeypots
- Leveraging Snort, Nepenthes, syslogs, Custom Darknet scripts via the current SES API (libprelude)
- We create a “correlated scanners” (multi-location) into a mitigation feed for sites to pull down.
- We also have a web page users can manually enter malicious domain-names, malware drop sites, botnet C&C into which produce various other mitigation feeds (stuff they’ve manually investigated).

Correlated Event Data

(prelude IDS)

- Open Source; Open Standards. 10 years of “IDS” intelligence experience.
- Commercially backed (they should be around for a while)
- Provides a standardized SQL based data-warehouse
- Handles the event API (securely with easy to use open TLS based tools, and in a fast binary mode of operation)
- pre-written parsers for lots of different log formats ‘out of the box’
- Lots of easy to use client side API’s (perl, python, C++, Java, .. (wow does java suck), etc...) for the automation of data in through customized correlation platforms (eg: darknet data, pre-correlated data, honeypot data, etc...)
- Most scripts are 20-lines of code or less, easier to maintain, off-load heavy-lifting to the API
- Provides a [python] correlation platform for realtime event correlation
- Where do the events go once they’ve been correlated?

Prewikka - SES Correlation the REN-ISAC **Prelude console**

- Events
- Agents
- Statistics
- Settings
- About

wes@ren-isac.net on thursday 02 september 2010

Alerts	CorrelationAlerts	ToolAlerts			
Classification	Source	Target	Analyzer	Time	
13 x TCP packet dropped (failed)	cpe-76-180-161-35.buffalo.res.rr.com	ses-qa.ren-isac.net	netfilter (ses-qa.ren-isac.net)	00:35:22 - 00:34:15	<input type="checkbox"/>
2 x TCP packet dropped (failed)	219.237.201.88	ses-qa.ren-isac.net	netfilter (ses-qa.ren-isac.net)	2010-09-01 11:16:00 - 2010-09-01 11:15:57	<input type="checkbox"/>
TCP packet dropped (failed)	ls.ecn.purdue.edu:50720/tcp	ses-qa.ren-isac.net:22/tcp Process name: kernel	netfilter (ses-qa.ren-isac.net)	2010-09-01 08:36:57	<input type="checkbox"/>
3 x TCP packet dropped (failed)	119.62.128.113	ses-qa.ren-isac.net	netfilter (ses-qa.ren-isac.net)	2010-09-01 00:49:07 - 2010-08-02 08:23:34	<input type="checkbox"/>
2 x TCP packet dropped (failed)	124.12.90.169	ses-qa.ren-isac.net	netfilter (ses-qa.ren-isac.net)	2010-08-31 00:04:25 - 2010-08-31 00:04:16	<input type="checkbox"/>
2 x ICMP packet dropped (failed)	pinge4.netsec.colostate.edu	ses-qa.ren-isac.net	netfilter (ses-qa.ren-isac.net)	2010-08-30 20:22:18 - 2010-07-22 19:35:26	<input type="checkbox"/>
2 x TCP packet dropped (failed)	58.49.104.164	ses-qa.ren-isac.net	netfilter (ses-qa.ren-isac.net)	2010-08-29 20:48:59 - 2010-08-29 20:48:56	<input type="checkbox"/>
2 x Log file rename (succeeded) 1 x Log file deletion (succeeded) 14 x Log file inconsistency (succeeded) 1 x Log file deletion (succeeded)	n/a	n/a	prelude-lml (ses-qa.ren-isac.net)	2010-08-29 06:25:01 - 2010-07-04 06:25:01	<input type="checkbox"/>
2 x TCP packet dropped (failed)	reverse-89-106-24-98.grid.com.tr	ses-qa.ren-isac.net	netfilter (ses-qa.ren-isac.net)	2010-08-28 14:42:30 - 2010-08-28 14:42:27	<input type="checkbox"/>
10 x TCP packet dropped (failed)	149-166-10-200.dhcp-in.lupui.edu	ses-qa.ren-isac.net	netfilter (ses-qa.ren-isac.net)	2010-08-27 19:13:32 - 2010-08-27 19:12:25	<input type="checkbox"/>
TCP packet dropped (failed)	search.comodo.com:46828/tcp	ses-qa.ren-isac.net:443/tcp Process name: kernel	netfilter (ses-qa.ren-isac.net)	2010-08-26 10:15:53	<input type="checkbox"/>
2 x ICMP packet dropped (failed)	ptr.isi.edu	ses-qa.ren-isac.net	netfilter (ses-qa.ren-isac.net)	2010-08-26 01:54:36 - 2010-07-22 19:35:26	<input type="checkbox"/>
3 x TCP packet dropped (failed)	113.65.142.109	ses-qa.ren-isac.net	netfilter (ses-qa.ren-isac.net)	2010-08-24 03:53:42 - 2010-08-24 03:53:34	<input type="checkbox"/>
TCP packet dropped (failed)	218.78.209.241:12346/tcp	ses-qa.ren-isac.net:22/tcp Process name: kernel	netfilter (ses-qa.ren-isac.net)	2010-08-23 16:26:26	<input type="checkbox"/>
TCP packet dropped (failed)	lwi70.lwinet.rug.nl:2019/tcp	ses-qa.ren-isac.net:22/tcp Process name: kernel	netfilter (ses-qa.ren-isac.net)	2010-08-22 17:00:02	<input type="checkbox"/>
2 x TCP packet dropped (failed)	118-166-217-233.dynamic.hinet.net	ses-qa.ren-isac.net	netfilter (ses-qa.ren-isac.net)	2010-08-21 14:05:22 - 2010-08-21 14:05:16	<input type="checkbox"/>
TCP packet dropped (failed)	202.100.85.17:20363/tcp	ses-qa.ren-isac.net:22/tcp Process name: kernel	netfilter (ses-qa.ren-isac.net)	2010-08-21 01:40:21	<input type="checkbox"/>
3 x TCP packet dropped (failed)	114-45-67-4.dynamic.hinet.net	ses-qa.ren-isac.net	netfilter (ses-qa.ren-isac.net)	2010-08-20 22:49:57 - 2010-08-20 22:49:48	<input type="checkbox"/>
2 x TCP packet dropped (failed)	213.80.73.45	ses-qa.ren-isac.net	netfilter (ses-qa.ren-isac.net)	2010-08-20 16:51:36 - 2010-07-28 04:39:30	<input type="checkbox"/>
2 x TCP packet dropped (failed)	66-190-188-24.dhcp.unas.co.charter.com	ses-qa.ren-isac.net	netfilter (ses-qa.ren-isac.net)	2010-08-19 02:37:27 - 2010-08-19 02:37:24	<input type="checkbox"/>
2 x TCP packet dropped (failed)	218.242.38.162	ses-qa.ren-isac.net	netfilter (ses-qa.ren-isac.net)	2010-08-18 09:26:17 - 2010-08-18 09:26:14	<input type="checkbox"/>
2 x TCP packet dropped (failed)	202.69.15.126	ses-qa.ren-isac.net	netfilter (ses-qa.ren-isac.net)	2010-08-17 21:18:29 - 2010-08-17 21:18:26	<input type="checkbox"/>
ICMP packet dropped (failed)	166.111.34.236:icmp	ses-qa.ren-isac.net:icmp Process name: kernel	netfilter (ses-qa.ren-isac.net)	2010-08-17 13:36:16	<input type="checkbox"/>
5 x ICMP packet dropped (failed)	218.76.65.98	ses-qa.ren-isac.net	netfilter (ses-qa.ren-isac.net)	2010-08-16 19:38:35 - 2010-07-13 04:48:40	<input type="checkbox"/>
3 x ICMP packet dropped (failed)	218.76.65.101	ses-qa.ren-isac.net	netfilter (ses-qa.ren-isac.net)	2010-08-16 05:30:41 - 2010-07-17 14:26:50	<input type="checkbox"/>
TCP packet dropped (failed)	120.107.160.13:16963/tcp	ses-qa.ren-isac.net:22/tcp Process name: kernel	netfilter (ses-qa.ren-isac.net)	2010-08-15 12:13:06	<input type="checkbox"/>
TCP packet dropped (failed)	6.1924.fr:43210/tcp	ses-qa.ren-isac.net:443/tcp Process name: kernel	netfilter (ses-qa.ren-isac.net)	2010-08-14 23:38:56	<input type="checkbox"/>
2 x TCP packet dropped (failed)	221.118.137.163	ses-qa.ren-isac.net	netfilter (ses-qa.ren-isac.net)	2010-08-14 19:08:20 - 2010-08-14 19:08:17	<input type="checkbox"/>
2 x TCP packet dropped (failed)	66.71.246.164	ses-qa.ren-isac.net	netfilter (ses-qa.ren-isac.net)	2010-08-13 22:37:19 - 2010-08-13 22:37:16	<input type="checkbox"/>
2 x TCP packet dropped (failed)	118.97.9.49	ses-qa.ren-isac.net	netfilter (ses-qa.ren-isac.net)	2010-08-13 21:28:57 - 2010-08-13 21:28:54	<input type="checkbox"/>
2 x TCP packet dropped (failed)	157.86.113.92	ses-qa.ren-isac.net	netfilter (ses-qa.ren-isac.net)	2010-08-13 01:55:09 - 2010-08-13 01:55:06	<input type="checkbox"/>
2 x TCP packet dropped (failed)	222.218.124.110	ses-qa.ren-isac.net	netfilter (ses-qa.ren-isac.net)	2010-08-12 01:22:30 - 2010-08-12 01:22:28	<input type="checkbox"/>
TCP packet dropped (failed)	111.1.8.105:34068/tcp	ses-qa.ren-isac.net:22/tcp Process name: kernel	netfilter (ses-qa.ren-isac.net)	2010-08-11 17:26:06	<input type="checkbox"/>
3 x TCP packet dropped (failed)	202.117.10.254	ses-qa.ren-isac.net	netfilter (ses-qa.ren-isac.net)	2010-08-11 11:24:57 - 2010-08-10 20:24:47	<input type="checkbox"/>
ssh scanner (succeeded)	192.168.1.1	'10.0.0.0/8':22/TCP	prelude-qa (ses-dev.ren-isac.net)	2010-08-11 05:12:35	<input type="checkbox"/>
TCP packet dropped (failed)	119.62.128.115:51631/tcp	ses-qa.ren-isac.net:22/tcp Process name: kernel	netfilter (ses-qa.ren-isac.net)	2010-08-08 17:37:34	<input type="checkbox"/>

Filter:

Period:

Timezone:

Limit:

Refresh:

2010-01-01 00:00:00
2011-01-01 00:00:00
+00:00

1 ... 50 (total: 2233)

tracking tickets.

- Handles ACL/UI/Basic workflow
- Has functionality to build out “federations” using ACL’s and the “groups” model.
- Mature code base (10+ years)
- Large customer base
- Prioritize, index and transactional-ize security conversations around correlated events
- Closest thing to your inbox (replace mailing list?)
- PGP friendly!

- Home
- New Report
- Help
- Preferences

REN-ISAC / SES Data Entry

Select a report type based on the highest level description of the report.

Submission entry may take a few seconds while additional data may be added to certain types of submissions (whois, passivedns, etc...)

- Scanner** *ssh, ftp, telnet, rdp, etc*
- BotnetInfrastructure** *C&C's, rogue dns servers or other botnet infrastructure representing the likely post-infection of a host*
- MalwareUrl** *malware infrastructure identified by url, eg: drop, config, exploit sites, or other infrastructure used to spread malware (usually pre-infection with the likely chance of infection if communicated with)*
- MalwareInfrastructure** *malware infrastructure identified by ip-address, eg: drop, config, exploit sites, or other infrastructure used to spread malware (usually pre-infection with the likely chance of infection if communicated with)*
- MaliciousDomain** *malicious domains, zeus domains, torpig domains, etc... (domains only, including hostnames, FQDN's or hostnames, no urls)*
- PhishingUrl** *data collection sites, credential drops, fake logins, etc...*
- PhishingReplyTo** *e-mail reply-to's used in phishing attempts*
- SuspiciousCIDR** *suspicious CIDR blocks (known to be 80% malicious or used for malicious purposes)*
- Other** *other stuff*

Browser tabs: [PREWIKKA] x SES Data Entry x

Address bar: <https://ses-qa.ren-isac.net/Minimal/Front.html>

Page header: RT for ses-qa.ren-isac.net Logged in as wes@ren-isac.net | Preferences | Logout

Navigation menu: Home, New Report, Help, Preferences

REN-ISAC / SES Data Entry

Search

*****submissions may require processing time while additional data is added (e.g. whois, passivedns, etc.)*****

<p>address <input type="text" value="192.168.1.1"/></p> <p>port <input type="text" value="6667"/></p> <p>protocol <input type="text" value="tcp"/></p> <p>description <input type="text" value="botnet infrastructure"/></p> <p>details <div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;">this is a bad host...</div></p> <p>action taken <div style="border: 1px solid #ccc; padding: 2px; display: inline-block;"> nothing <input checked="" type="checkbox"/> investigated block-host other </div></p> <p>restriction <input type="text"/></p> <p>attachment <input type="button" value="Choose File"/> No file chosen</p>	<p><i>comma delimited for multiple reports (eg: "192.168.1.1,192.168.1.2")</i></p> <p><i>of the form: 21,22,80-89</i></p> <p><i>if multiple addresses exist, entire portlist will be tagged with each address</i></p> <p><i>eg: tcp/udp/other</i></p> <p><i>any additional high-level keywords will be used to 'tag' the data (eg: "torpig", "zeus", "fastflux", etc...)</i></p> <p><i>e.g. full message headers, analysis, etc...</i></p> <p><i>what local action was taken as a result of this information?</i></p> <p><i>according with REN-ISAC Information Sharing Policy</i></p>
--	--

RT for ses-qa.ren-isac.net Logged in as wes@ren-isac.net | Preferences | Logout

REN-ISAC / #2634: other - 64.34.164.146 Search

- Home
- New Report
- Help
- Preferences

The Basics

Restriction: PRIVILEGED
 Address category: ipv4-addr
 Address: 64.34.164.146
 Service Portlist: 22
 Service Protocol: 6
 ASN: 30099 SB-2 ServerBeach
 CIDR: 64.34.160.0/20
 Expectation action: investigate
 DetectTime: (no value)
 MemberContribWeb: YES
 System category: (no value)
 Impact severity: medium
 Assessment Impact: other

People

Owner: "Wes Young" <wes@ren-isac.net>
 Requestors:
 Cc:
 AdminCc: Group: DutyTeam FEDERATION_RENISAC_NET

Status

Status: open
 Created: 2010-05-27T01:53:50Z
 Closed: Not set
 Updated: 2010-05-27T01:53:59Z by wes@ren-isac.net

History Brief headers — Full headers

2010-05-27T01:53:50Z wes@ren-isac.net - Ticket created Reply Comment Forward Encrypt/Decrypt
 Subject: other

[Download \(untitled\)](#)

```
<IODEF-Document version="1.0" xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" x
```

2010-05-27T01:53:50Z RT_System - AdminCc DutyTeam FEDERATION_RENISAC_NET added

2010-05-27T01:53:50Z RT_System - HowReported Email added

2010-05-27T01:53:50Z RT_System - State new added

2010-05-27T01:53:51Z RT_System - Restriction need-to-know added

2010-05-27T01:53:51Z RT_System - Address category ipv4-addr added

2010-05-27T01:53:51Z RT_System - Address 64.34.164.146 added

2010-05-27T01:53:51Z RT_System - Service Portlist 22 added

2010-05-27T01:53:51Z RT_System - Service Protocol 6 added

2010-05-27T01:53:51Z RT_System - Expectation action investigate added

2010-05-27T01:53:51Z RT_System - Assessment Impact other added

2010-05-27T01:53:52Z RT_System - CIDR 64.34.160.0/20 added

2010-05-27T01:53:52Z RT_System - Comments added Reply Comment Forward Encrypt/Decrypt

30099 SB-2 ServerBeach | 64.34.160.0/20 | US | arin | 2004-07-15 Download (untitled) text/plain 64b

2010-05-27T01:53:52Z RT_System - Restriction need-to-know changed to PRIVILEGED

2010-05-27T01:53:52Z RT_System - Impact severity medium added

2010-05-27T01:53:52Z RT_System - Subject changed from 'other' to 'other - 64.34.164.146'

2010-05-27T01:53:52Z RT_System - Comments added Reply Comment Forward Encrypt/Decrypt

Peer 1 Network Inc. PEER1-BLK-08 (NET-64-34-0-0-1)
 64.34.0.0 - 64.34.255.255
 ServerBeach PEER1-SERVERBEACH-02A (NET-64-34-160-0-1)
 64.34.160.0 - 64.34.175.255

ARIN WHOIS database, last updated 2010-05-26 20:00
 # Enter ? for additional hints on searching ARIN's WHOIS database.
 #
 # ARIN WHOIS data and services are subject to the Terms of Use
 # available at https://www.arin.net/whois_tou.html

2010-05-27T01:53:59Z RT_System - Comments added Reply Comment Forward Encrypt/Decrypt

Passive DNS Data Download (untitled) text/plain 1.3k

query	answer	firstseen	lastseen	rrtype	t1
...	...	2008-03-25T08:14:26Z	2008-04-03T16:30:41Z	12	86400
...	...	2006-08-14T15:20:21Z	2008-04-03T16:30:45Z	1	86400
...	...	2008-05-17T05:30:12Z	2008-05-30T15:53:44Z	1	86400
...	...	2009-01-31T01:14:09Z	2009-01-31T01:14:09Z	1	3600
...	...	2009-04-18T17:23:35Z	2009-06-20T10:55:42Z	1	1800
...	...	2009-08-17T09:51:30Z	2009-08-31T10:02:59Z	1	60
...	...	2009-05-21T21:28:13Z	2009-12-16T12:03:58Z	1	360
...	...	2009-05-19T10:06:29Z	2009-12-16T12:01:56Z	1	43200
...	...	2009-05-21T21:28:31Z	2009-12-16T12:04:01Z	1	360
...	...	2009-11-25T03:55:24Z	2009-11-25T03:55:24Z	1	60
...	...	2009-01-11T11:55:31Z	2009-12-01T13:51:20Z	1	86400
...	...	2009-08-06T10:24:53Z	2010-04-19T17:55:04Z	1	30
...	...	2010-05-23T12:52:01Z	2010-05-23T12:52:07Z	1	3600

2010-05-27T01:53:59Z RT_System - Given to wes@ren-isac.net

- Home
- New Report
- Help
- Preferences

REN-ISAC / Member Reports Search

#	Subject	Created	Last Updated
2634	other - 64.34.164.146	2010-05-27T01:53:50Z	2010-05-27T01:53:59Z
2633	[]other - test 1 - privileged - 1.5.6.7	2010-05-26T20:22:08Z	2010-05-26T20:22:17Z
2632	[]other - restricted - 1.7.6.5	2010-05-26T20:20:35Z	2010-05-26T20:20:44Z
2631	[]other - privileged - 1.5.1.1	2010-05-26T20:19:54Z	2010-05-26T20:19:59Z
2630	suspicious cidr - restricted - 1.1.2.0/24	2010-05-26T20:19:02Z	2010-05-26T20:19:07Z
2629	suspicious cidr - privileged - 1.1.1.0/24	2010-05-26T20:18:24Z	2010-05-26T20:18:30Z
2628	malware infrastructure - restricted - 2.2.2.2	2010-05-26T20:17:41Z	2010-05-26T20:17:56Z
2627	malware url - restricted - http://malware2.com	2010-05-26T20:17:40Z	2010-05-26T20:17:41Z
2626	malware infrastructure - privileged - 1.0.10.1	2010-05-26T20:17:05Z	2010-05-26T20:17:11Z
2625	malware url - privileged - http://malware1.com	2010-05-26T20:17:04Z	2010-05-26T20:17:05Z
2624	phishing replyto - restricted - phish2@dd.com	2010-05-26T20:16:32Z	2010-05-26T20:16:33Z
2623	phishing replyto - privileged - phish1@dd.com	2010-05-26T20:16:04Z	2010-05-26T20:16:05Z
2622	phishing url - restricted - http://www.phish2.com	2010-05-26T20:15:30Z	2010-05-26T20:15:31Z
2621	phishing url - privileged - http://www.phish1.com	2010-05-26T20:15:05Z	2010-05-26T20:15:06Z
2620	malicious domain - restricted - domain2.com	2010-05-26T20:14:37Z	2010-05-26T20:14:38Z
2619	malicious domain - privileged - domain1.com	2010-05-26T20:14:10Z	2010-05-26T20:14:12Z
2618	malware infrastructure - restricted - 1.0.0.5	2010-05-26T20:13:36Z	2010-05-26T20:13:45Z
2617	malware infrastructure - privileged - 1.0.0.4	2010-05-26T20:12:53Z	2010-05-26T20:13:01Z
2616	botnet infrastructure - restricted - 1.0.0.3	2010-05-26T20:12:14Z	2010-05-26T20:12:24Z
2615	botnet infrastructure - privileged - 1.0.0.2	2010-05-26T20:11:34Z	2010-05-26T20:11:45Z
2614	scanner - restricted - 1.0.0.1	2010-05-26T20:10:24Z	2010-05-26T20:10:39Z
2613	scanner - privileged - 1.3.4.5	2010-05-26T20:09:12Z	2010-05-26T20:09:29Z
2612	suspicious cidr - 216.104.36.0/24	2010-05-11T23:04:10Z	2010-05-11T23:04:15Z
2611	malware infrastructure - 82.211.7.32	2010-05-10T18:40:53Z	2010-05-10T18:40:58Z
2610	malware infrastructure - 68.168.216.6	2010-05-10T18:40:48Z	2010-05-10T18:40:53Z
2609	malware url - http://spellload.ru/welcome.php?id=9&pid=2&1=1	2010-05-10T18:40:46Z	2010-05-10T18:40:58Z

Search for bad-actor data

By default, the ticket subject will be searched. The string can be any text, including but not limited to, IP address, e-mail address, domain name, URL, or SES ticket id

By specifying **asn:integer** the ticket ASN field will be searched

By specifying **cidr:network/mask** the ticket CIDR field will be search; however, a network/mask search of the subject field can also be performed and may yield different results depending on the data supplied in individual tickets.

Searching the full text of every ticket can take a long time, but if you need to do it, you can search for any word in the full ticket history by **fulltext:word**

To list the most recent records, use %

Feeds

```
See: http://tools.ietf.org/html/draft-ietf-inch-iodef-14#section-3.17
http://tools.ietf.org/html/draft-ietf-inch-iodef-14#section-2.10
Example: "2,5-15,30,32,40-50,55-60"
Regex: "\d+(\-\d+)?(\,\d+(\-\d+)?)*"

# Restriction - Sets the expectation to which the data can be (or cannot be) shared.
# - Ref: http://www.ren-isac.net/docs/information\_sharing\_policy.html#04 for more detailed information

# Description - Short description of the data (subject).

# Impact severity - See: http://tools.ietf.org/html/rfc5070#section-3.10.1
# - An estimate of the relative severity of the activity.

# NA - Severity undetermined, data should be considered suspicious but possibly unreliable

# low - Severity low, data should be considered suspicious
# - Results from data should be used as supplemental data in an investigation
# - Data may have been machine generated, but partially correlated with other data
# - Data may have been manually inputted by a single institution, where only an observation was made, little or no action was taken
in response of the data

# medium - Severity medium, data should be considered highly suspect and / or malicious in nature
# - Results from this data should be used as the basis for an investigation
# - Data may be the result of several sites inputting data they have "acted" on locally
# - Data may be the result of one or more sites blocking the data being described in the data record

# high - Data should be considered highly malicious in nature
# - Data has been manually vetted (either by record or by process) by the operations team as having an extremely low chance for any
legitimate communication with the data being described
# - Data should be used as the basis for an investigation and should be blocked where possible

# Expectation action - See: http://tools.ietf.org/html/rfc5070#section-3.13
# - REN-ISAC Recommended Action to be taken with the data:

# nothing - Monitor for suspicious traffic, use with correlation to escalate possible threats

# investigate - Investigate the systems(s) listed in the event.
# - Data has been submitted by 1 or 2 sites but hasn't been "vetted" or heavily researched. This data should be
# considered suspicious but only "acted on" at your own discretion. It should be useful in correlation but
# require other data and analysis to support any action taken because of it.

# block-host - Block traffic from the machine(s) listed.
# - Data has been manually confirmed and vetted by the REN-ISAC or its trusted information sharing partners.
# Within reason; proactive blocking of addresses should provide minimal risk.

# Assessment Confidence - RESERVED FOR FUTURE USE
# See: http://tools.ietf.org/html/rfc5070#section-3.10.4
# The element content expresses a numerical assessment in the confidence of the data

# Reference - Reference url where more information about each record can be found

# Scanner Threat Feed
# Last update: 2010-09-02 18:24:04 UTC

# ASN | CIDR | Address | Service Protocol | Service Portlist | Restriction | Description | Impact severity | Expectation action | Assessment Confidence |
Created | LastUpdated | Reference
NA | NA | 1.3.4.5 | tcp | 993 | PRIVILEGED | scanner - privileged - 1.3.4.5 | medium | investigate | NA | 2010-05-26T20:09:12Z | 2010-05-26T20:09:29Z |
https://ses-qa.ren-isac.net/Minimal/Display.html?id=2613
NA | NA | 1.0.0.1 | tcp | 994 | RESTRICTED | scanner - restricted - 1.0.0.1 | medium | investigate | NA | 2010-05-26T20:10:24Z | 2010-05-26T20:10:39Z |
https://ses-qa.ren-isac.net/Minimal/Display.html?id=2614
```

Lessons Learned v I

- Database design to support high-volume at performance
- Database design, small, concise, and easily adapted
- Database design to support “schema-less” data
- <http://bret.appspot.com/entry/how-friendfeed-uses-mysql>
- <http://labs.google.com/papers/bigtable.html>
- Standards-based, but don't tie to a single standard – make design decisions that accommodate multiple data representation standards in a single database
- Learn from other's successes and mistakes
- Community engagement for determining design priorities
- Feedback from a team of knowledgeable early adopters
- pilot pilot pilot with your community! they'll be the ones using it!

Collective Intelligence

(v2)

- Locally correlated Events (typically malicious ip-infrastructure)
- Spamhaus DROP list (hijacked networks)
- Malwaredomains.com feed (malware hashes, malware domains, malware ip-infrastructure)
- Malwaredomainlist.com feed (malware urls, malware domains)
- DShield List(s) (scanning ip-infrastructure)
- Phishtank Data (phishing urls, phishing ip-infrastructure)
- Zeustracker data (binary urls, config urls, domains, ip-infrastructure)
- From each domain, you have massive potential intelligence from the name-servers involved with each domain.
- Whitelists (domains, ip-infrastructure... dnswhl.org)
- Passive domain lookup data (not necessarily malicious addresses, but a good reference to have along side your intelligence).
- Locally discovered intel (potentially all of the above)

where we stole the idea from

<http://bret.appspot.com/entry/how-friendfeed-uses-mysql>

- Our datastore stores schema-less bags of properties (e.g., JSON objects or Python dictionaries). The only required property of stored entities is id, a 16-byte UUID. The rest of the entity is opaque as far as the datastore is concerned. We can change the "schema" simply by storing new properties.
- We index data in these entities by storing indexes in separate MySQL tables. If we want to index three properties in each entity, we will have three MySQL tables - one for each index. If we want to stop using an index, we stop writing to that table from our code and, optionally, drop the table from MySQL. If we want a new index, we make a new MySQL table for that index and run a process to asynchronously populate the index without disrupting our live service.
- As a result, we end up having more tables than we had before, but adding and removing indexes is easy. We have heavily optimized the process that populates new indexes (which we call "The Cleaner") so that it fills new indexes rapidly without disrupting the site. We can store new properties and index them in a day's time rather than a week's time, and we don't need to swap MySQL masters and slaves or do any other scary operational work to make it happen.

schema-less data

- store anything and everything (xml, plain-text, binary blobs, etc).
- If you wanna add/remove something, just alter the table (no index locking issues).
- structure what you can (json, xml, whatever), even if it's a simple key-pair. (hint: standards help document the data, but isn't required, it's a good thing if you want anyone else to leverage your data, or send you data).
- unstructured data integration (sometimes good intel is in e-mail form)
- everything has a uuid (derived by a sha1 based uuid of the 'blob' hash).
- known relationships to the blob are stored within the blob and indexed for searching (eg: a uuid pointing at another uuid).

ideals.

- Data Normalization (format, confidence, severity, etc).
- Largely diverse (and usually large) data-sets
- data is “living”, it’s only as fresh as your last record or trend. (as the insert() completes, it’s already become stale, regardless if you’ve updated the “lastUpdated” column).
- Even within similar data-sets, some intel may become stale more quickly than others (scanners vs botnet C&C’s)
- ultimately data is from PEOPLE (eg: human beings). Whether it’s a sensor that was programmed by someone with a bias towards something, or a forensics investigation. We must interpret that data from their context to our context EVERY TIME before we can make use of it.
- search vs feeds and distinguishing the difference (presentation layer)
- is there already something like this out in real-life?
- i can has API? (application integration, reaching an intelligence driven infrastructure)

the basics

- Takes data from public and private sources, pre-processes it, normalizes it down to your favorite standard (eg: IDMEF, IODEF, ICSG, json keypairs, etc...) and stores in along side it's counterpart data points.
- Malware metadata is stored along side suspicious networks data (reads: re-use-a-ble)
- Malicious Domains data is stored along side phishing url data.
- The main intelligence stream warehouses everything in blob's and uses 'cookie cutter' style index partitions (eg: regular tables) to be derived from the specific parts of the data worth using in analytics/mitigation's.
- the web api (REST) works the same way

parsing. is. hard.

- cif_feedparser
- everything (well, most things) are just config mappings
- threading magic

```
; Spamhaus DROP List 8/9/11 - (c) 2011 The Spamhaus Project
109.196.140.0/24 ; SBL101917
109.94.212.0/22 ; SBL84898
110.232.160.0/20 ; SBL79387
110.44.128.0/20 ; SBL79386
113.20.160.0/19 ; SBL79384
116.199.128.0/19 ; SBL56563
116.68.136.0/21 ; SBL102578
121.46.64.0/18 ; SBL72673
122.202.96.0/19 ; SBL87493
128.168.0.0/16 ; SBL51908
128.199.0.0/16 ; SBL62478
129.76.64.0/18 ; SBL101405
130.201.0.0/16 ; SBL101200
130.222.0.0/16 ; SBL101196
132.145.0.0/16 ; SBL101575
132.232.0.0/16 ; SBL9176
132.240.0.0/16 ; SBL68517
134.127.0.0/16 ; SBL101572
134.172.0.0/16 ; SBL101573
134.175.0.0/19 ; SBL114667
134.209.0.0/16 ; SBL101574
134.23.0.0/16 ; SBL101571
134.33.0.0/16 ; SBL7097
136.228.0.0/16 ; SBL89254
138.43.0.0/16 ; SBL69354
139.167.0.0/16 ; SBL64740
14.1.96.0/19 ; SBL97058
14.102.160.0/19 ; SBL96728
140.170.0.0/16 ; SBL79701
143.135.0.0/16 ; SBL84946
143.49.0.0/16 ; SBL7182
143.95.0.0/16 ; SBL93865
148.105.0.0/16 ; SBL103491
148.178.0.0/16 ; SBL79700
148.248.0.0/16 ; SBL84763
150.141.0.0/16 ; SBL79702
150.230.0.0/16 ; SBL78129
151.133.0.0/16 ; SBL88602
```

```
[spamhaus_drop]
feed = 'http://www.spamhaus.org/drop/drop.lasso'
regex = "^(\\S+)\\s;\\s(\\S+)$"
regex_values = 'address,reference'
source = 'spamhaus.org'
impact = 'malicious network'
description = 'hijacked'
confidence = 95
severity = medium
alternativeid = 'http://www.spamhaus.org/sbl/sbl.lasso?query=<reference'
detection = daily
```

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼ <mb1>
  ▼ <url>
    <id>100120</id>
    <uri>http://lermensagens000.com.sapo.pt/</uri>
    <date>20081207235755UTC</date>
    <av_info>Trojan-Downloader.Win32.Delf.gcw</av_info>
    <asn>0</asn>
    <asn_data/>
  </url>
  ▼ <url>
    <id>100122</id>
    <uri>http://microsoft2008.com.sapo.pt/</uri>
    <date>20081208020523UTC</date>
    <av_info>Trojan-Downloader.Win32.Delf.gcw</av_info>
    <asn>0</asn>
    <asn_data/>
  </url>
  ▼ <url>
    <id>100388</id>
    <uri>http://cartaoamizade000.com.sapo.pt/</uri>
    <date>20081211123415UTC</date>
    <av_info>Trojan-Downloader.Win32.Delf.gcw</av_info>
    <asn>0</asn>
    <asn_data/>
  </url>
  ▼ <url>
    <id>101040</id>
    <uri>http://blogfotos2008.com.sapo.pt/</uri>
    <date>20081216152628UTC</date>
    <av_info>Trojan-Downloader.Win32.Agent.baua</av_info>
    <asn>0</asn>
    <asn_data/>
  </url>
```

```
[mpatrol_urls]
feed = 'http://www.malware.com.br/cgi/submit?action=list_xml'
impact = 'malware url'
source = 'malware.com.br'
node = 'url'
elements = 'uri,id,date,av_info'
elements_map = 'address,id,detecttime,description'
alternativeid = 'http://www.malware.com.br/cgi/search.pl?id=<id>'
```

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<rss version="2.0">
  ▼<channel>
    <title>SpyEye Tracker BinaryURL RSS Feed</title>
    <link>https://spyeyetracker.abuse.ch/monitor.php</link>
    ▼<description>
      SpyEye Tracker. This feed shows the latest fourty SpyEye BinaryURLs.
    </description>
    <language>en</language>
    <docs>http://www.rssboard.org/rss-specification</docs>
    <generator>RSS Feed Engine by abuse.ch</generator>
    <managingEditor>admin@abuse.ch (admin)</managingEditor>
    <webMaster>admin@abuse.ch (admin)</webMaster>
    ▼<item>
      <title>217.116.198.29/build.exe (2011-07-28)</title>
      ▼<link>
        https://spyeyetracker.abuse.ch/monitor.php?host=217.116.198.29
      </link>
      ▼<description>
        SpyEye BinaryURL: http://217.116.198.29/build.exe, Status: offline, MD5 hash: 598b42846ac8a301ea44a80b397e2056, Virustotal: 3/43(7.00)
      </description>
      ▼<guid>
        https://spyeyetracker.abuse.ch/monitor.php?host=217.116.198.29&id=8af7352277df809d221c9a11b0adacb9
      </guid>
    </item>
    ▼<item>
      <title>egyxi.com/images/e-cards.exe (2011-07-04)</title>
      ▼<link>
        https://spyeyetracker.abuse.ch/monitor.php?host=egyxi.com
      </link>
      ▼<description>
        SpyEye BinaryURL: http://egyxi.com/images/e-cards.exe, Status: offline, MD5 hash: da024616c323579eb019c579aef773ec, Virustotal: 24/42(57.10)
      </description>
      ▼<guid>
        https://spyeyetracker.abuse.ch/monitor.php?host=egyxi.com&id=f08e10621d07264be06f40cc8e8a682a
      </guid>
    </item>
  </channel>
</rss>
```

```
36 [binaries]
37 feed = 'https://spyeyetracker.abuse.ch/monitor.php?rssfeed=binaryurls'
38 regex_description = '^SpyEye BinaryURL: ([\s\S]*), Status: \S+, MD5 hash: ([\s\S]*),'
39 regex_description_values = 'address,malware_md5'
40 regex_title = "(\d{4}-\d{2}-\d{2})"
41 regex_title_values = 'detecttime'
42 regex_link = "(\S+)"
43 regex_link_values = 'alternativeid'
44 impact = 'botnet url'
45 description = 'spyeye binary'
46 severity = 'high'
47 confidence = 85
```

; For providing suggestions, new servers or networks see <http://www.mirc.com/serverli>
Click to go back, hold to see history

[timestamp]

date=30/07/2010

[networks]

n0=DALnet

n1=EFnet

n2=GameSurge

n3=IRCnet

n4=LinkNet

n5=Quakenet

n6=Undernet

n7=WebChat

[servers]

n0=Random serverSERVER:irc.dal.net:6660-6667GROUP:DALnet

n1=AS, MY, MesraSERVER:mesra.kl.my.dal.net:6665-6668,7000GROUP:DALnet

n2=AS, SG, HotspeedSERVER:hotspeed.sg.as.dal.net:6665-6668,7000GROUP:DALnet

n3=EU, NO, PowertechSERVER:powertech.no.eu.dal.net:6665-6668,7000GROUP:DALnet

n4=US, FL, RumbleSERVER:rumble.fl.us.dal.net:6665-6668,7000GROUP:DALnet

n5=US, NY, BroadwaySERVER:broadway.ny.us.dal.net:6665-6668,7000GROUP:DALnet

n6=Random serverSERVER:irc.efnet.info:6667GROUP:EFnet

n7=Random serverSERVER:irc.efnet.org:6667GROUP:EFnet

n8=AS, IsraelSERVER:irc.inter.net.il:6667GROUP:EFnet

n9=CA, ON, TorontoSERVER:irc.igs.ca:6665GROUP:EFnet

n10=EU, DK, AarhusSERVER:irc.inet.tele.dk:6661-6669GROUP:EFnet

n11=EU, FI, HelsinkiSERVER:efnet.cs.hut.fi:6667GROUP:EFnet

n12=EU, HU, PecsSERVER:irc.pte.hu:6665-6669,7000,9000GROUP:EFnet

n13=EU, NL, AmsterdamSERVER:efnet.xs4all.nl:6661-6669GROUP:EFnet

n14=EU, NL, EdeSERVER:irc.efnet.nl:6660-6669GROUP:EFnet

n15=EU, NO, HomelienSERVER:irc.homelien.no:6666,6667,7000GROUP:EFnet

n16=EU, PL, WarszawaSERVER:irc.efnet.pl:6667GROUP:EFnet

n17=EU, SE, BorlangeSERVER:irc.du.se:6666-6669,7000GROUP:EFnet

n18=US, AZ, Phoenix (Blackened)SERVER:irc.blackened.com:6665-6669GROUP:EFnet

n19=US, AZ, Phoenix (Easynews)SERVER:irc.easynews.com:6660,6665-6667,7000GROUP:EFnet

n20=US, CA, San Jose (Blessed)SERVER:irc.blessed.net:6665-6669GROUP:EFnet

Source path: [svn/](#) [trunk/](#) [server/](#) [etc/](#) 00_mirc_whitelist.cfg

```
1 feed = http://www.mirc.com/servers.ini
2 alternativeid = 'http://www.mirc.com/servers.ini'
3 alternativeid_restriction = public
4 detection = daily
5 source = 'mirc.com'
6 severity = 'null'
7 restriction = need-to-know
8 confidence = 85
9 description = 'known irc host'
10 protocol = 6
11
12 [domains]
13 regex = 'SERVER:([a-zA-Z0-9-\.]+\.[a-z]{2,3}):(\S+)GROUP'
14 regex_values = 'address,portlist'
15 impact = 'domain whitelist'
16 first_run = true
17 period = daily
```

free. as in beer.

Project References (standards stuff)

- RT::IODEF
 - RT-IODEF: integrating IODEF into RT
 - project: <http://code.google.com/p/perl-rt-iodef/>
 - code: <http://search.cpan.org/~saxjazman/RT-IODEF/>
- XML::IODEF: Perl module for manipulating IODEF with Perl
 - project: <http://code.google.com/p/perl-xml-iodef/>
 - code: <http://search.cpan.org/~saxjazman/XML-IODEF/>
- XML-Malware: Perl extension for representing malware in XML
 - project: <http://code.google.com/p/perl-xml-malware/>
 - code: <http://search.cpan.org/~saxjazman/XML-Malware/>
- python-xml-malware: Python framework for representing malware in XML
 - project: <http://code.google.com/p/python-xml-malware/>
- XML-IODEF-PhraudReport: extending XML::IODEF to use with Phishing Extensions
 - project: <http://code.google.com/p/xml-iodef-phraudreport/>
 - code: <http://search.cpan.org/~saxjazman/XML-IODEF-PhraudReport/>
- perl-arcsight-iodef: convert ArcSight XML to a standardized IODEF
 - project: <http://code.google.com/p/perl-arcsight-iodef/>

Project References (and future work, v3)

- www.ren-isac.net/ses -- main project page
- <http://code.google.com/p/collective-intelligence-framework/>