SES / CIF

Internet2

Combined Industry and Research Constituency Meeting

April 24, 2012

Doug Pearson

Technical Director, REN-ISAC

dodpears@ren-isac.net

Background on REN-ISAC

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.

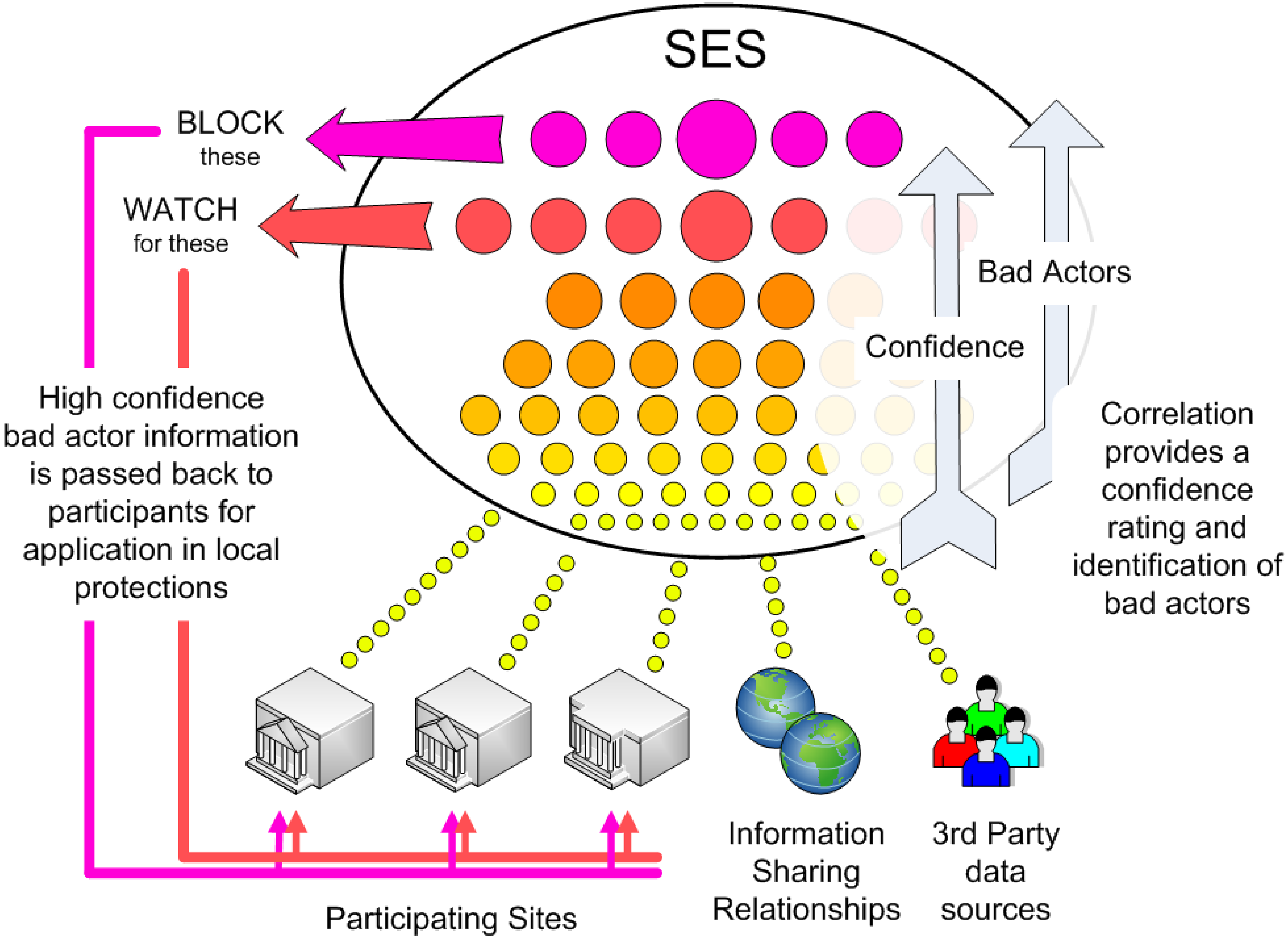
REN-ISAC serves as the R&E trusted partner for served networks, the formal ISAC community, and in other commercial, governmental, and private security information sharing relationships.

REN-ISAC

- Private information sharing community
  - Restricted to full time information security professionals in higher education, teaching hospitals, and FFRDCs; generally limited to “five eyes” nations
  - 340+ member institutions, represented by ~900 persons
  - Private, commercial, and governmental information sharing relationships
- CSIRT for US .edu
  - e.g. 12,000 notifications per month concerning infected machines)
- Hosted at Indiana University, and supported with the help of Louisiana State University, Internet2, EDUCAUSE, and nominal membership fees

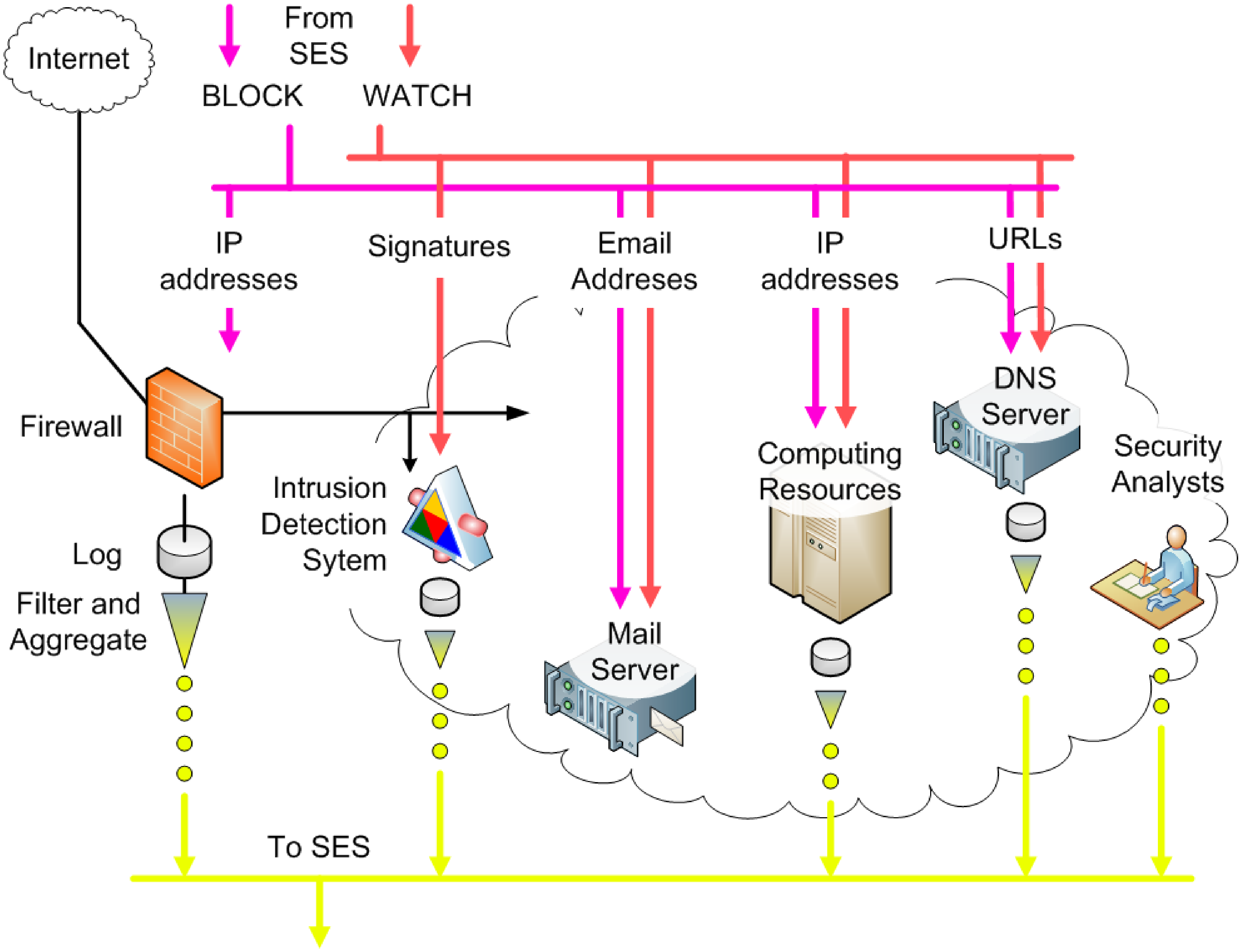
SES and CIF

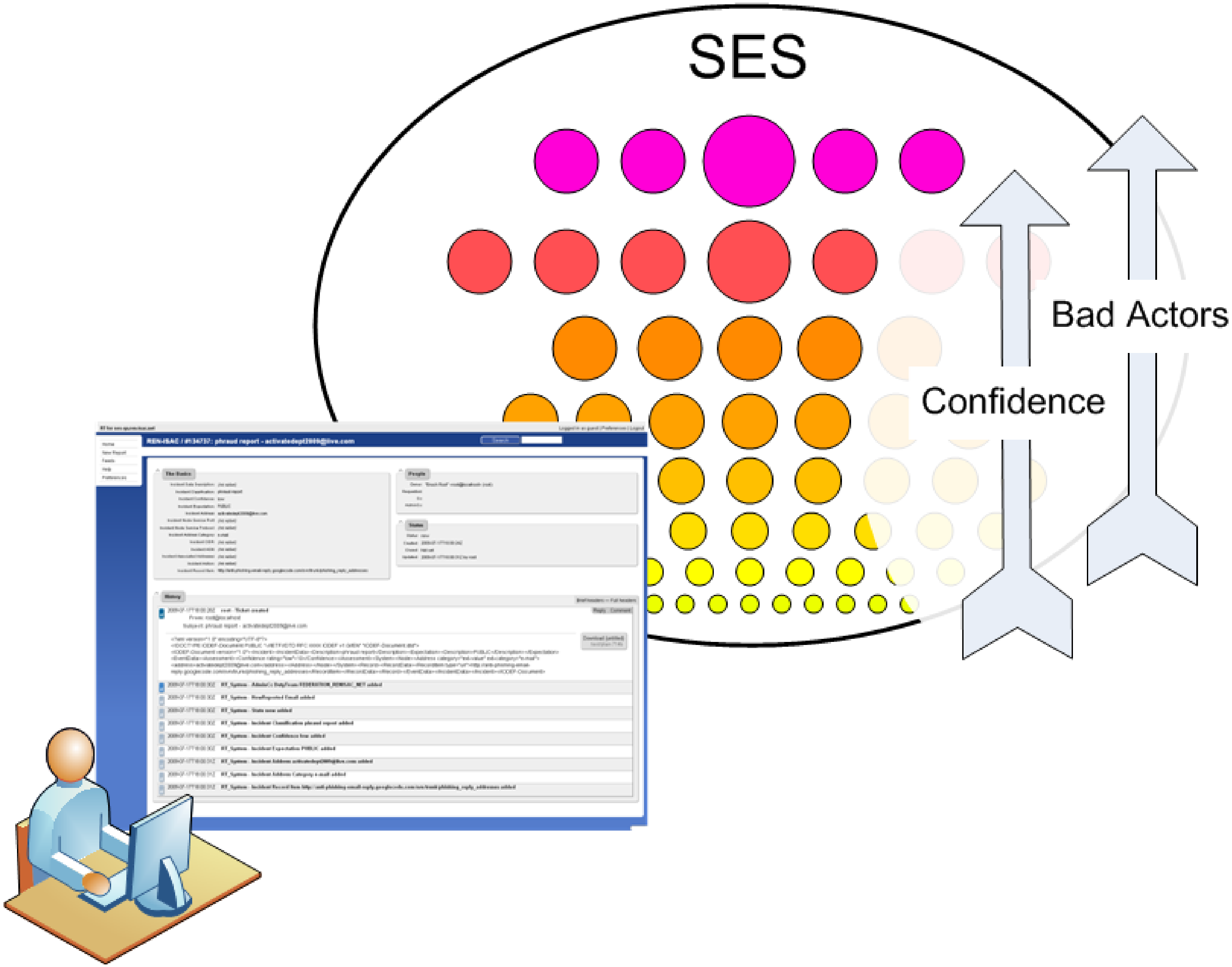
- Naming disentanglement
  - Security Event System (SES)
  - Collective Intelligence Framework (CIF)
  - It all started out as “SES”, but around version 2 time, we evolved (broadened) our model to a framework for collective intelligence concerning malicious actors and reputation of Internet elements, hence “CIF”.
  - The open source tool/framework is now CIF
  - Our implementation in REN-ISAC is SES



High confidence bad actor information is passed back to participants for application in local protections

Correlation provides a confidence rating and identification of bad actors


Internet
From
SES
BLOCK
WATCH
IP
addresses
Signatures
Email
Addreses
IP
addresses
URLs
Firewall
Log
Filter and
Aggregate
Intrusion
Detection
Sytem
Mail
Server
Computing
Resources
DNS
Server
Security
Analysts
To SES



REN-ISAC / #134737: phraud report - activatedept2009@live.com

The Basics

People

Status

History

Subject: phraud report - activatedept2009@live.com

Security Threat Indicators

- IP address
  - representing just about any type of compromised host or source of threat, e.g. a botnet command and control (C&C) host or drone, a distributed denial-of-service (DDoS) attack source, a host scanning the Internet for vulnerable machines, etc.
- Fully Qualified Domain Name (FQDN)
  - e.g. botnet C&C, suspicious name server, other botnet infrastructure
- Domain name
  - consistently malicious domains
- URL
  - representing for example, a malware download or phishing sites
- Classless Inter-Domain Routing (CIDR) block
  - representing a miscreant-heavy address range (e.g. Russian Business Network), and as descriptive information for IPv4 address-based records
- E-Mail address
  - for example, a phishing Reply-To address
- Malware hashes

SES v1 (2008-10)

- Removes the human interrupt from the observe – protect cycle
  - Machine-to-machine capabilities rather than e-mail or web-based information sharing portals passing around PDF and XLS files.
- Automated and manual submission of threat indicators
- Data derived from participating members, plus incorporation of data from high-value information sharing partners
- Generates intelligence feeds (block lists, watch lists, etc.)
- Supports query (via RT)
- Simple correlation (e.g. this site scanned 10 universities)
- Built on open source components and lots of glue
  - Best Practical’s Request Tracker for Incident Response (RTIR) for basic human interface and correlated event repository,
  - Prelude Technologies Prelude Manager for raw event repository and correlation, and libprelude API for automated client submission
- Lowered the barriers to entry for data-sharing
- We got something working in 18-months for ~$120k, a substantial component of that being a DoJ grant through Internet2; no tools, just developed the process and glue-code.

SES v2 (2010-12): Collective Intelligence

- Better support for analysts (incident investigations, reputation query, etc.)
- Improved and more flexible interfaces
  - sophisticated API, CLI client, browser plugin, integrate with tools
- Improved underlying repository architecture for scaling and performance (no SQL and big data concepts)
- Became a comprehensive threat intelligence repository through the incorporation of LOTS of external data*
- 18-24 months, ~$350k

SES v2 : Collective Intelligence

- *External data, such as:
  - 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)
  - Private information sharing relationships
  - Whitelists (alexa top 10, 100, 1000, 10000, mirc servers.ini, etc)
- And, as data in ingested, additional discovery, such as:
  - AS, domain, whois record, network block information
  - From each domain, the name-servers involved supporting that domain; yields very useful intelligence concerning the criminal infrastructure

SESv3 (2011-14) : Inter-federation and more

- Objectives:
  - Inter-federation
    - Technical frameworks, policies, and legal agreements for information sharing among disparate trust communities
  - Incorporate additional data types (e.g. BGP and passive DNS), to
    - Increase the reputational knowledge and forensic history
    - Provide capabilities to identify complete pictures of criminal infrastructure
  - Incorporate and correlate unstructured human intelligence (e.g. mailing lists, IRC conversations, blog posts, etc.) along with the structured event data.
  - Solve the scaling problem once and for all (hadoop, hbase (fingers-crossed))
  - Incorporate API access into common incident handler and responder tools, e.g. ticketing systems,
  - Improve the process framework and communications (Apache Thrift, 0MQ)
- SESv3 work funded by the National Science Foundation, NSF under SDCI Sec: SESv3, award OCI-1127425.

Summation

What we have

A security tool and service that …

S
E
S
&
C
I
F

- Removes the human interrupt from the observe – protect cycle
- Provides collection, storage, and access to security event information within a trust community (e.g. the REN-ISAC membership)
- Incorporates observations sourced from within the trust community, and from external public sources, and private, commercial, and governmental information sharing partners
- Works with a wide variety of indicators (IP addresses, domains, URLs, e-mail addresses, hashes, etc.)
- Correlates and weights observations to develop confidence in the identification of malicious actors, and reputation of Internet elements
- Provides query access (supporting analysts), and feeds (supporting local protection systems, e.g. IDS, firewalls, sinkholes, etc.)
- Utilizes advanced, standard, and evolving practices for storage, access, and data sharing (e.g. hadoop, hbase, IODEF, protocol buffers, etc.)
- Supports inter-federated sharing between trust communities via data marking (e.g. "share w/trusted partners", "share w/LE"), and policy controls
- Is being used and further developed in the REN-ISAC community.
- Is being deployed in communities external to REN-ISAC

Why am I presenting here?

- Seek to explore relationship of this tool to the research and industrial partner communities.
  - Is there value for instance(s) of the tool stood up by and for academic researchers, to normalize and facilitate research access to security data?
  - Value in commercial security setting?
    - We've seen adoption already! (see community at google code)
  - Value of integrating (API) query into security tools commonly used by security incident handlers and analysts.
  - Value of security threat information sharing relationship with industrial partners.
  - Stimulate interest in contributing to the project.
    - Deploy, test, and feedback
    - Code
    - $$$ (always welcome)

References and Contact

SES project:

http://www.ren-isac.net/ses/

Open source CIF:

http://code.google.com/p/collective-intelligence-framework/

REN-ISAC

http://www.ren-isac.net

Doug Pearson
Technical Director, REN-ISAC
dodpears@ren-isac.net
812-855-3847