

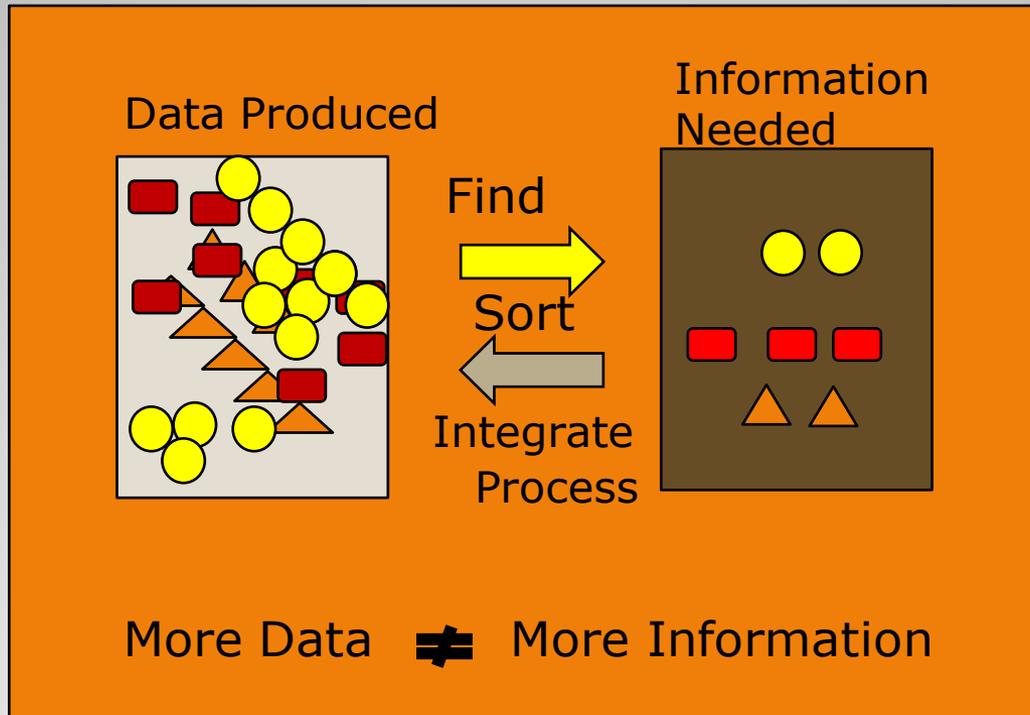
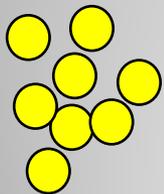
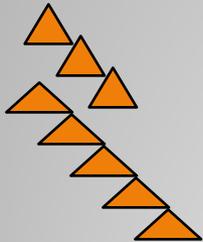
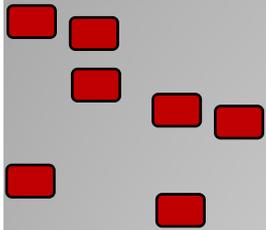
Federated Data Sharing to Support Distributed Incident Response

DOE-IM Conference

Kevin Nauer
Neale Pickett
Christopher Nebergall

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE

- Cyber defenders may be less informed now than before



The Information Gap

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE

- Formalize and build a community of skilled analysts that will cooperatively respond to network incidents
- Share incident data and tools within the DOE and NSE in a decentralized and timely manner to enhance enterprise *situational awareness**

* *Situational awareness – requires perception of what’s currently happening on the network, a comprehension of these events, and projection of what could happen next*

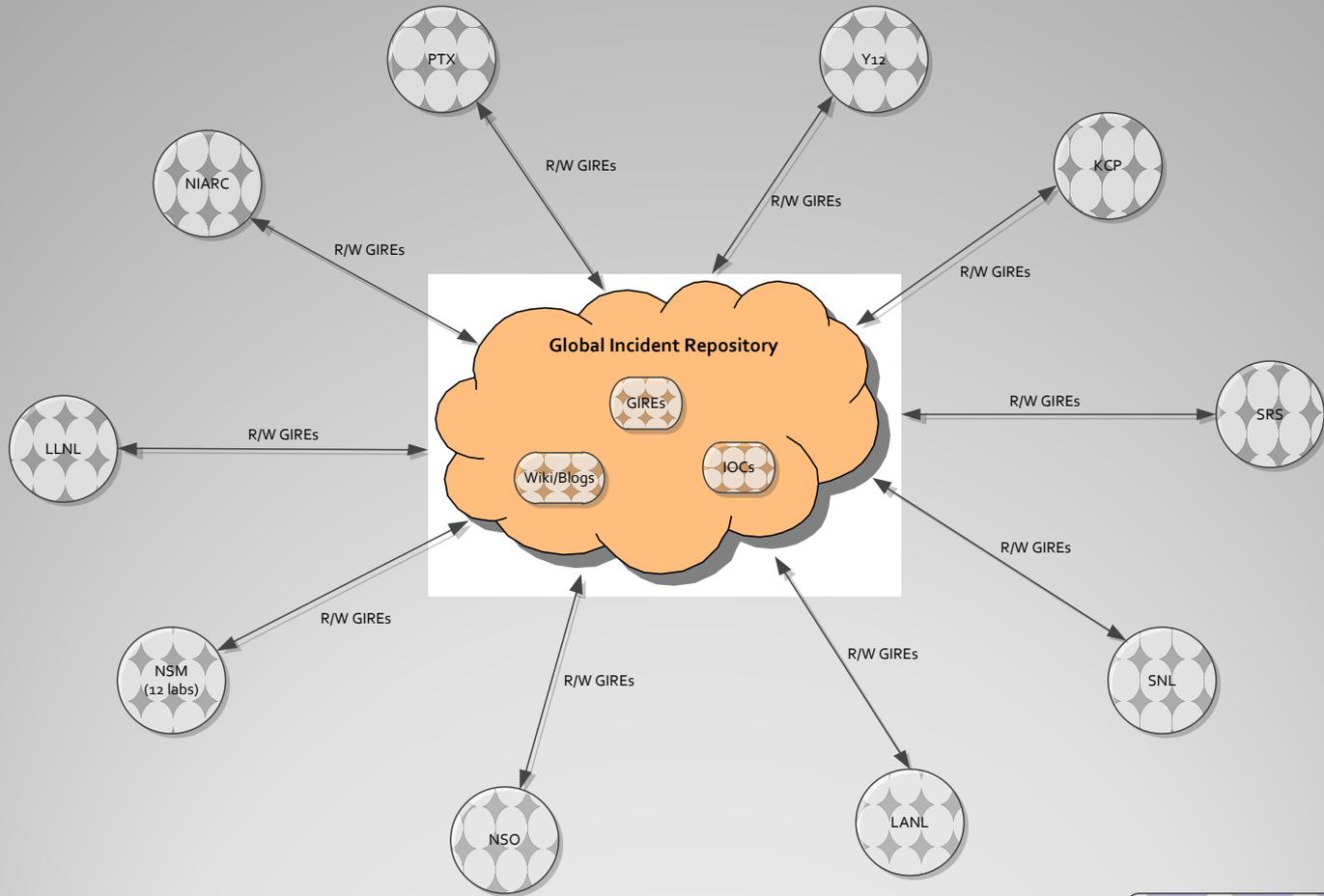
Objectives

- Enable NNSA sites to share cyber security incident data in a near real-time manner
- Enable cyber security analysts to **query once** for information pertaining to a current or potentially undiscovered attack and **retrieve results from many sources** (locally and remotely)
- Demonstrate that a **distributed approach** is more effective than centralized one
 - Maintain site's autonomy over their cyber data and response
 - Foster trust and improve coordination and sharing among sites
- Research and develop technology that can enable these goals

Goals

- Design a distributed intelligent information retrieval system for cyber analysts
- Incorporate these features:
 - Scalable architecture
 - Distributed search and storage technology (inspired by major Internet providers such as Google, Facebook and Amazon)
 - Open source core engine Apache Lucene/Solr
 - Flexible and User oriented
 - Fault tolerant
- Form a multidisciplinary and multi-site team composed of researchers and operational staff
 - Various research/operational orgs – Cognitive Applications, IO Work for Others, CSIRTS, Cyber Security R&D

Federated Data Sharing



LEGEND

- IOC – Indicators of Compromise
- GIR – Global Incident Repository
- GIRE – Global Incident Repository Event

Virtual Global Incident Repository



**Fight crime.
Unravel incidents...
one byte at a time.**

SANS Computer Forensic Investigations and Incident Response Blog

Author Archives: **Gregory Pendergast**

**Review: Mandiant's Incident Response
Conference (MIRCon) Day 2**

Posted by **Gregory Pendergast** on October 15, 2010 – 1:21 pm
Filed under **Computer Forensics**, **Incident Response**

Search for:

Search



October 15, 2010

Sharing Cyber Intelligence

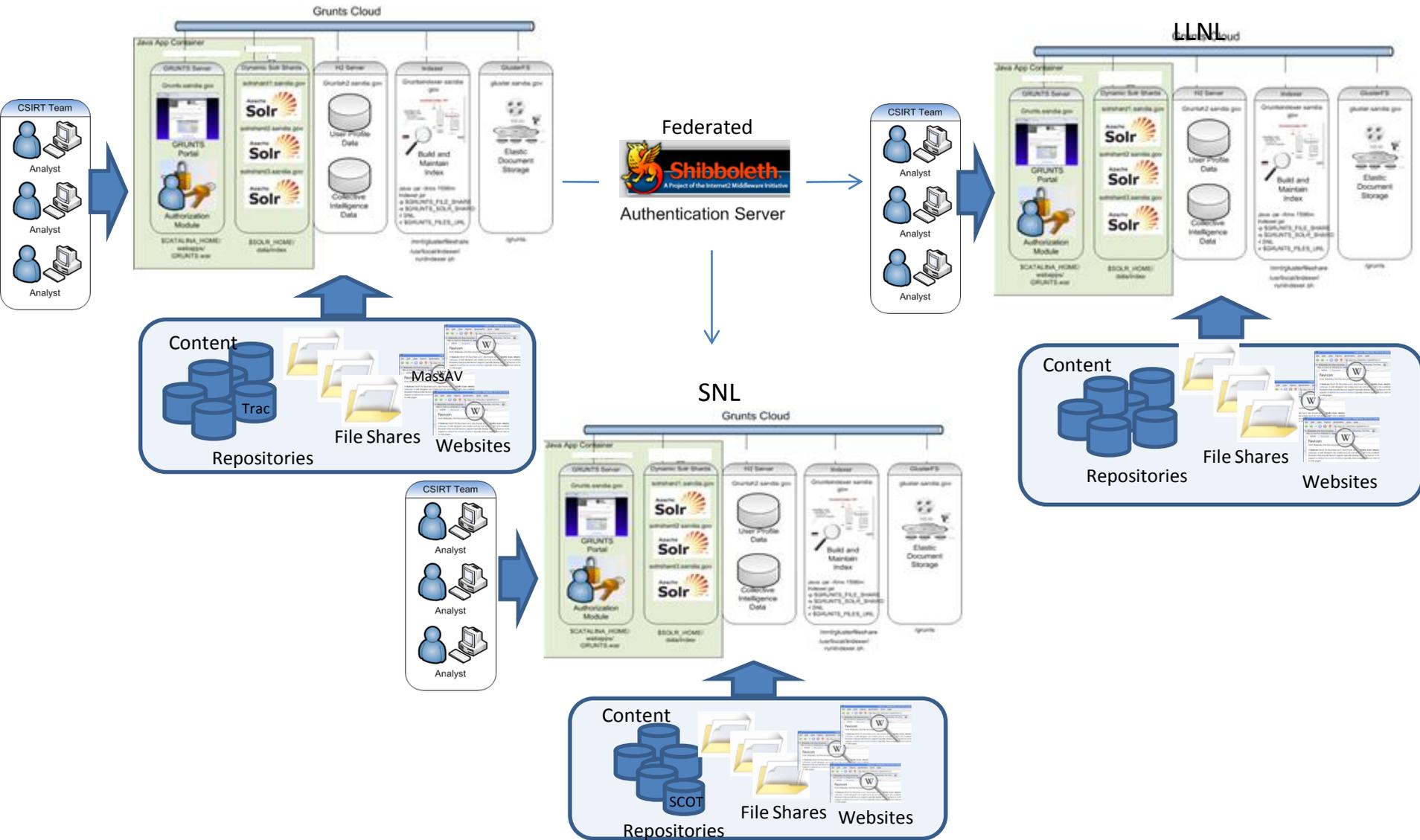
£ in a world where true short supply, this kind of Ren
incident response and personnel sharing makes a follo
forensics experts are in great deal of sense." imp

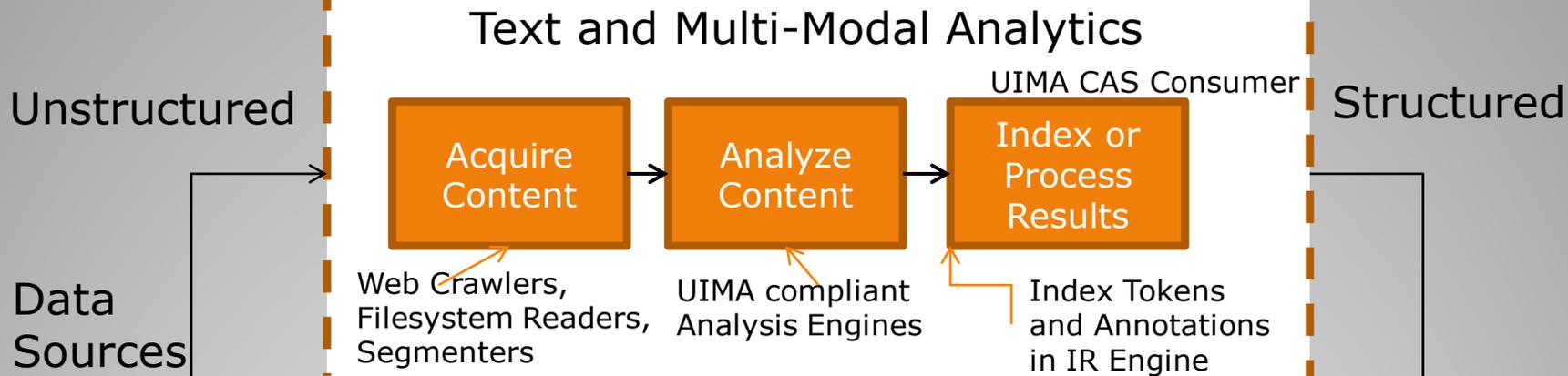
<http://blogs.sans.org/computer-forensics/author/gregorypendergast/>

- Geographically distributed architecture presents many challenges:
 - Distributed resource management
 - Synchronization, configuration, namespace conflicts
 - Distributed Message Passing Service
 - Distributed Storage System
 - Large data storage and remote document retrieval requirements
 - Partitioning of data for horizontal scaleout
 - Data sets will need to be partitioned for distributed analysis via sharding
 - Relevancy ranking across many distributed search index stores
 - Federated Authentication and Authorization
 - Shibboleth and Apache Shiro being considered
 - Intersite Agreements
 - Human coordination and communication issues
 - Management/governance model needed

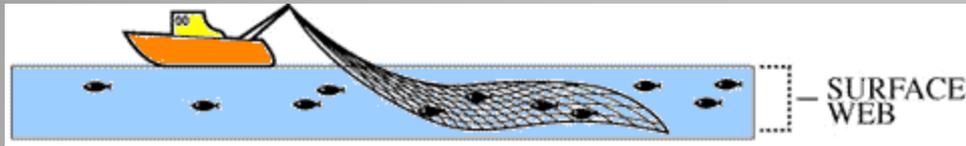
Major Challenges for Data Sharing

Federated Cyber Security Enterprise Incident Response Data Sharing



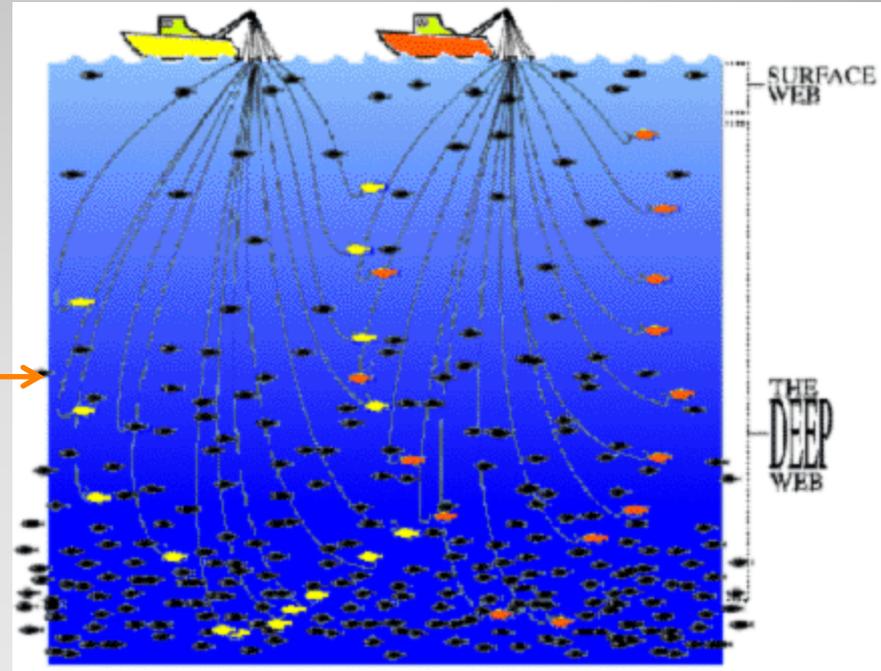


Text Analytics Architecture



Typical Search Engines

Deep Search



Deep Search

- Forensic Incident Response Exercise
 - 2- to 5-day CySec Training/Exercise
 - Exercise reinforces training
 - Malware Reverse-Engineering
 - Protocol Reverse-Engineering
 - Host Forensics
 - Incident Coordination

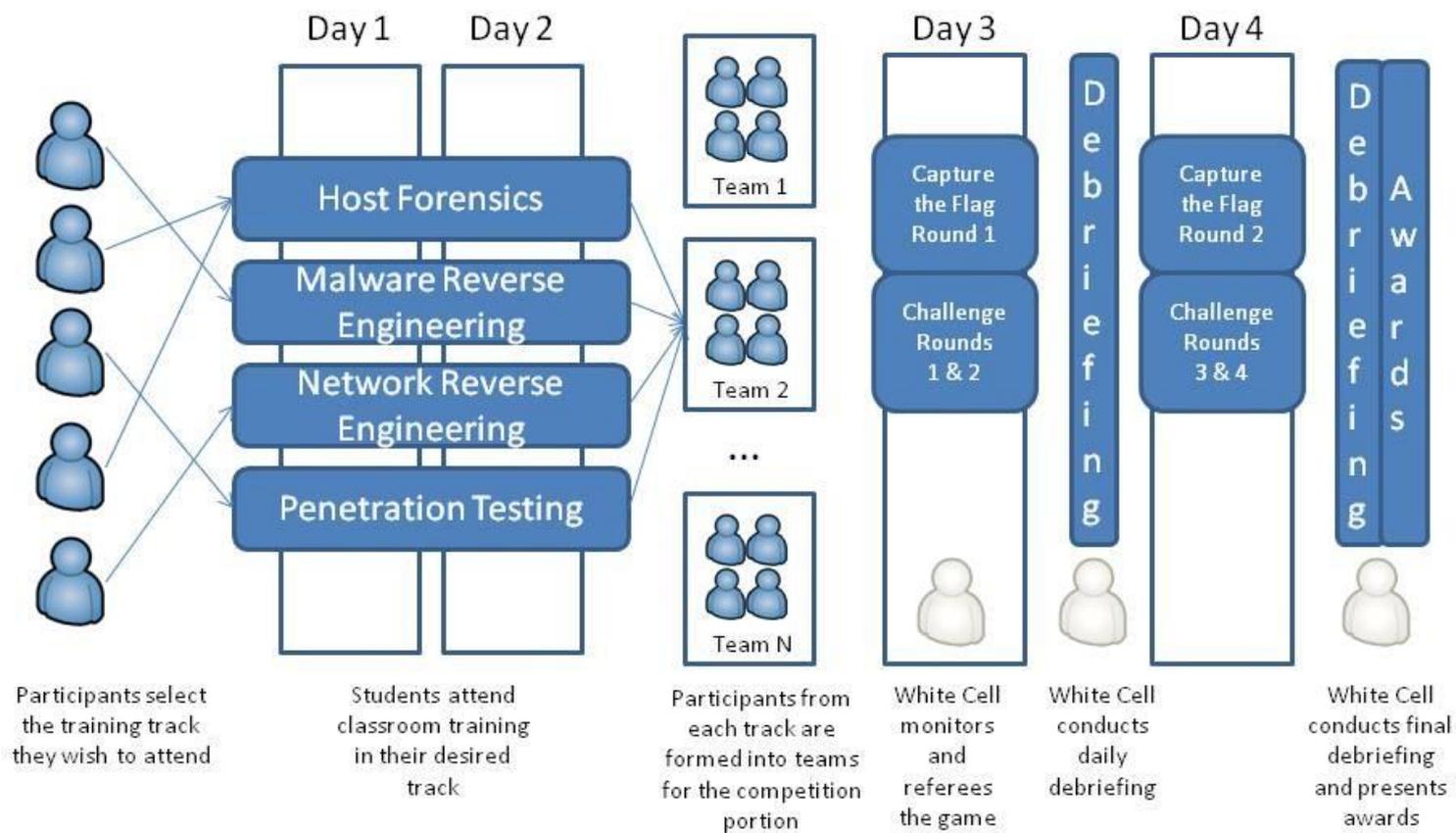


Tracer FIRE

- Intensive Forensic Exercise
 - 5 days working data from a single incident in a war-room style venue
 - Single team focus



Tracer Inferno



Tracer FIRE Event Sequence



What should the learning objectives be for cyber defense scenarios?

What instructional content should we include to improve performance of CSIR individuals and teams?

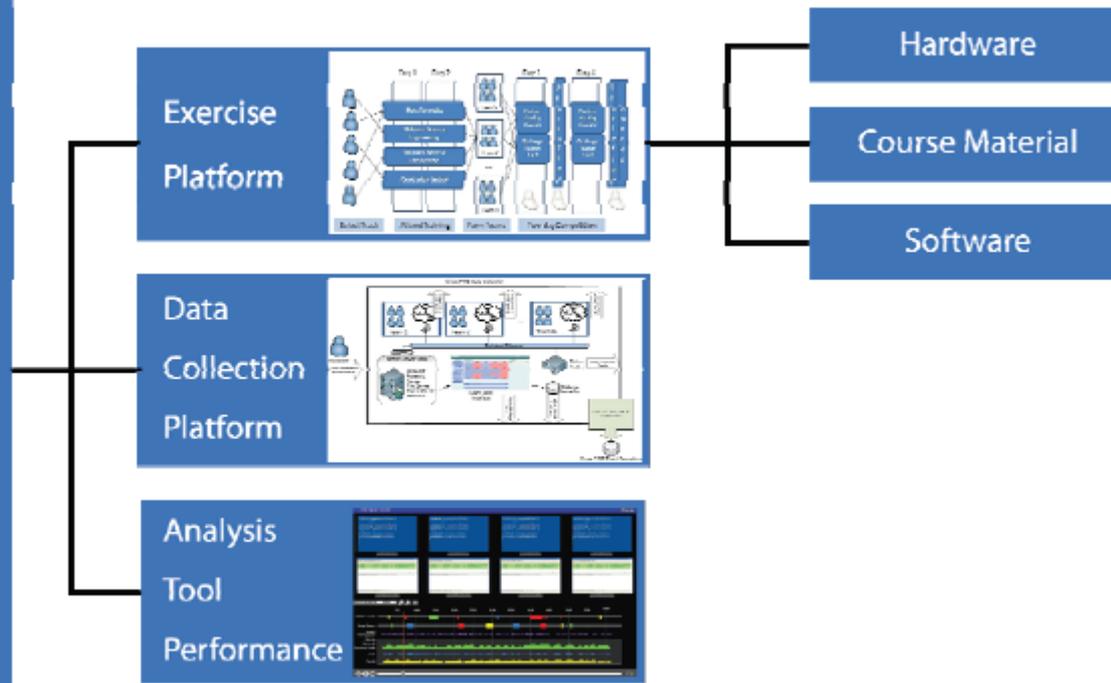
What training performance measures and observables should be collected?

What kind of immersive learning environment best supports Tracer FIRES and INFERNOs?

What fidelity level is required for effective training?

Proposed Performance Monitoring

Cross FIRE System



Cross FIRE Cyber Incident Response Performance Measurement System

SAML provides the mechanism for sharing tools/data between sites

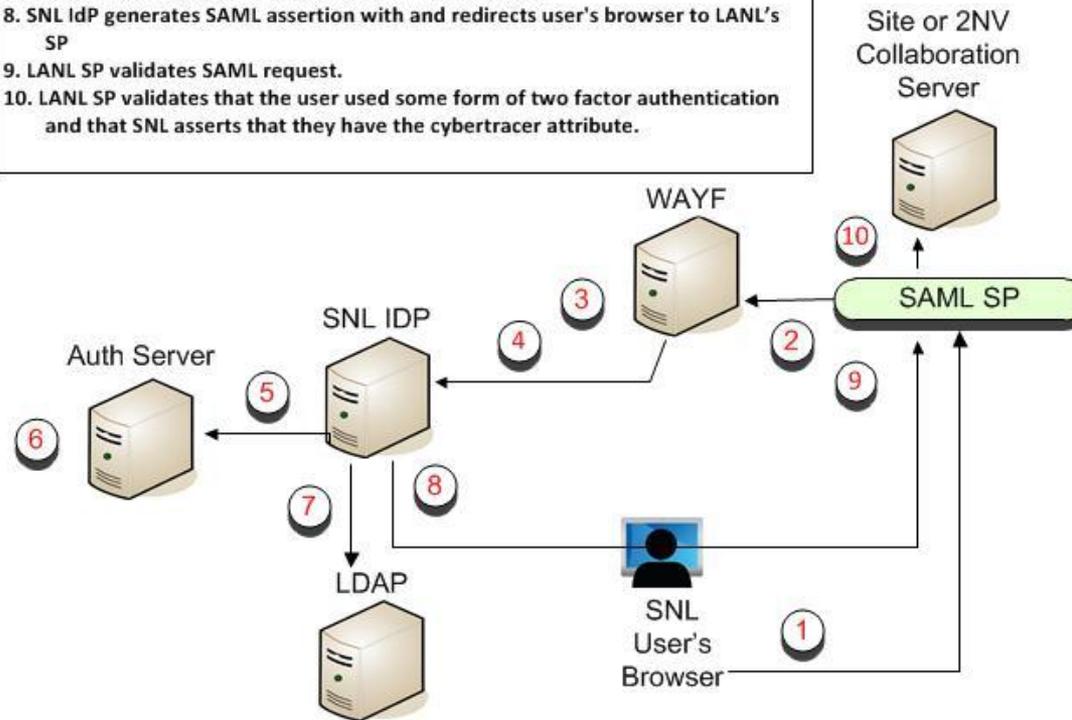
- Shared Attributes
 - Authentication Type
 - Phone Number
 - Email address
 - Citizenship
 - Cyber Tracer Member

SAML

Collaboration with SAML

SP Initiated SSO

1. User's browser requests URL at LANL for collaboration site
2. SAML SP intercepts request and redirects user to a WAYF (Where Are You From) service
3. User selects Sandia National Laboratories
4. WAYF service redirects user to SNL IDP
5. Site IDP Auth plugin requests 2 factor auth if user not already logged in, using any 2 factor compatible site authentication (HSPD12, SecurID, Cryptocard, etc)
6. Auth Server validates credentials.
7. SNL IDP obtains user attributes from site LDAP Server
8. SNL IDP generates SAML assertion with and redirects user's browser to LANL's SP
9. LANL SP validates SAML request.
10. LANL SP validates that the user used some form of two factor authentication and that SNL asserts that they have the cybertracer attribute.



CyberTracer Collaboration Portal

Choose one of the following authentication methods:

- [SAML Federation](#)
- [SSL Client Certificate](#)

For instructions on how to obtain a trusted certificate, see [CSR Generation](#).

If you plan to use client certificate mechanisms for authenticating, make sure that your system supports **secure TLS renegotiation**.

Collaboration Portal

SAML Discovery Service

Select the Identity Provider with which to authenticate:

LANL	▼	submit
LANL		
SNL		
KCP		



Authorization Required

This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., username and password) or your browser doesn't understand how to supply the credentials required.

Apache/2.2.3 (Red Hat) Server at idpserver.sandia.gov Port 443

Authentication Required ✕

 A username and password are being requested by https://idpserver.sandia.gov. The site says: "Two Factor Authentication"

User Name:

Password:

CyberTracer Collaboration Portal

For instructions on obtaining a certificate to access resources, see [CSR Generation](#).

Links to all available resources are shown below.

Applications

- [Trac](#): a wiki, subversion portal and issue-tracking system.
- [MassAV](#): a malware analysis system and repository.
- [MassAV Beta](#): the current development version of MassAV. It will have bugs.
- [CGI IRC](#): a CGI Internet Relay Chat (IRC) client.
- **Secure IRC**: an IRC server on port 6697. To obtain access, send a CSR to [administrator](#). [More info...](#)

Shared Files

- [DAV](#): web-accessible files.
- **git repositories**: more files are accessible via git and SSH. To obtain access to the collab repository, upload your SSH public key using the [gitosis key submission form](#) or send your public key to [administrator](#).

```
$ git clone gitosis@server.lanl.gov:collaboration
```