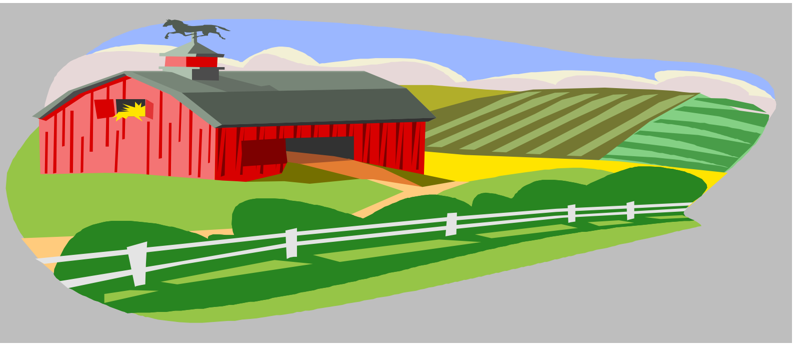
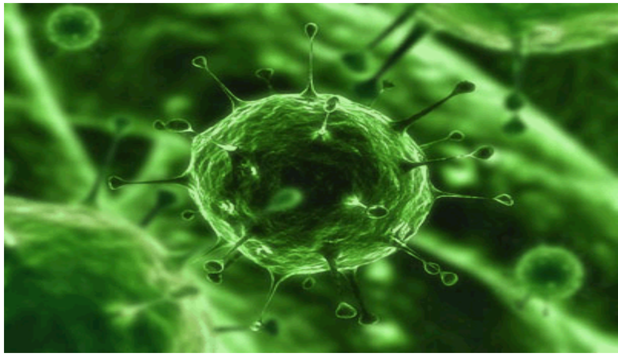
SAND2013-3787C

Exceptional service in the national interest

Sandia National Laboratories





U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

The Problem

- Malware proliferating at exponential rates
- Malware analysis requires advanced skillset
- Limited malware analyst resources available
- Sensitivities around malware based infections make sharing difficult
- Duplication of malware reverse engineering among government departments and agencies and critical infrastructure

What is FARM?

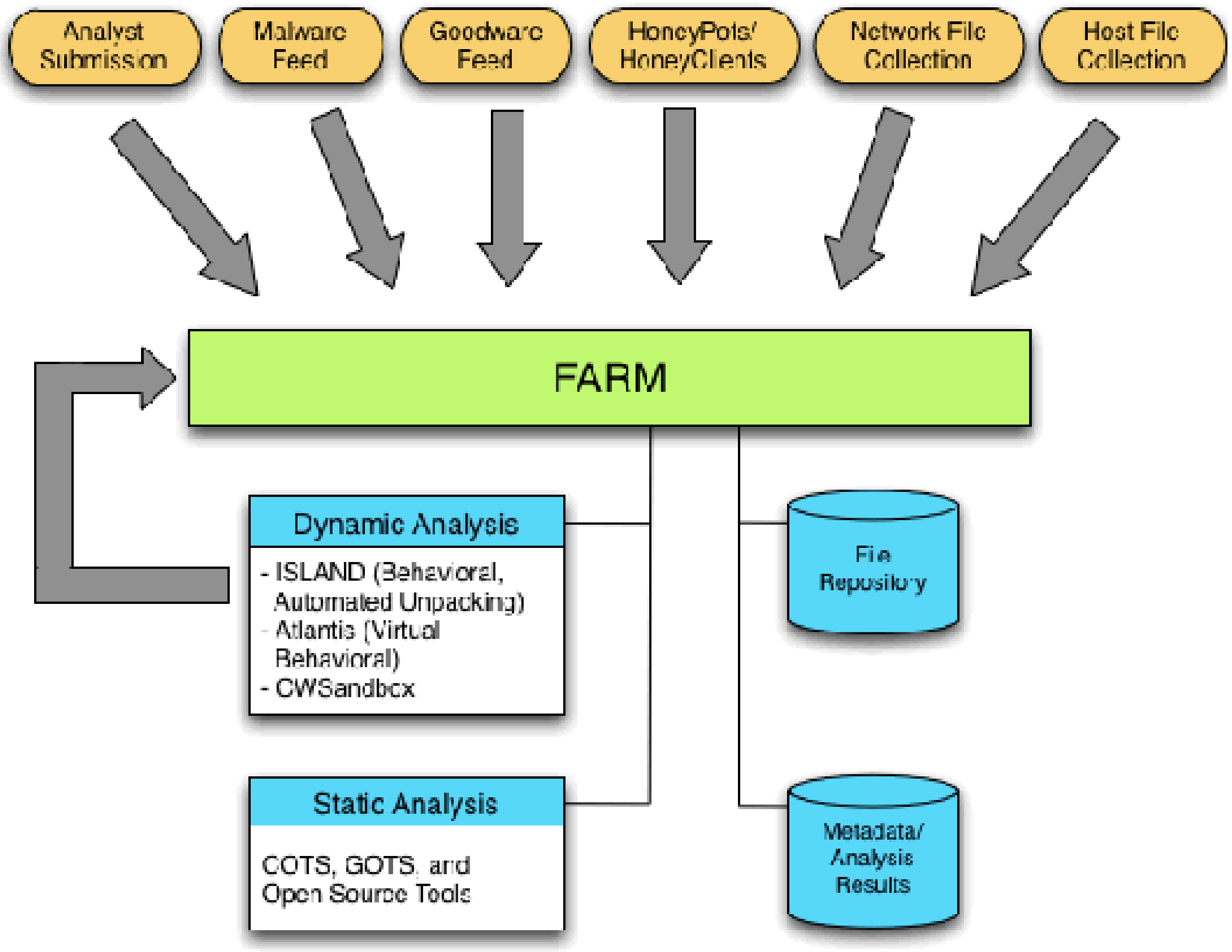
- Forensic Analysis Repository for Malware
    - Modular framework for malware/software analysis.
- Save time and resources
    - Automate as much of the malware/software analysis as possible.
    - Speed up incident response and malware triage.
- Mature technology
    - In operational use since 2008
- Analysis Components
    - Static analysis
    - Dynamic analysis
        - ISLAND: bare metal dynamic analysis: network,file,registry signatures.
        - ATLANTIS: virtual dynamic analysis, unpacking,systemcall trace.
        - Currently developing Android analysis environment

What is it for?

- Triage unknown software
- Create connections between software/malware
- Extract behavioral and static properties from software

Decrease time and effort through automated tools and scalable algorithms

FARM Architecture



Dynamic Analysis

- ISLAND (Behavioral, Automated Unpacking)
- Atlantis (Virtual Behavioral)
- CWSandbox

Static Analysis

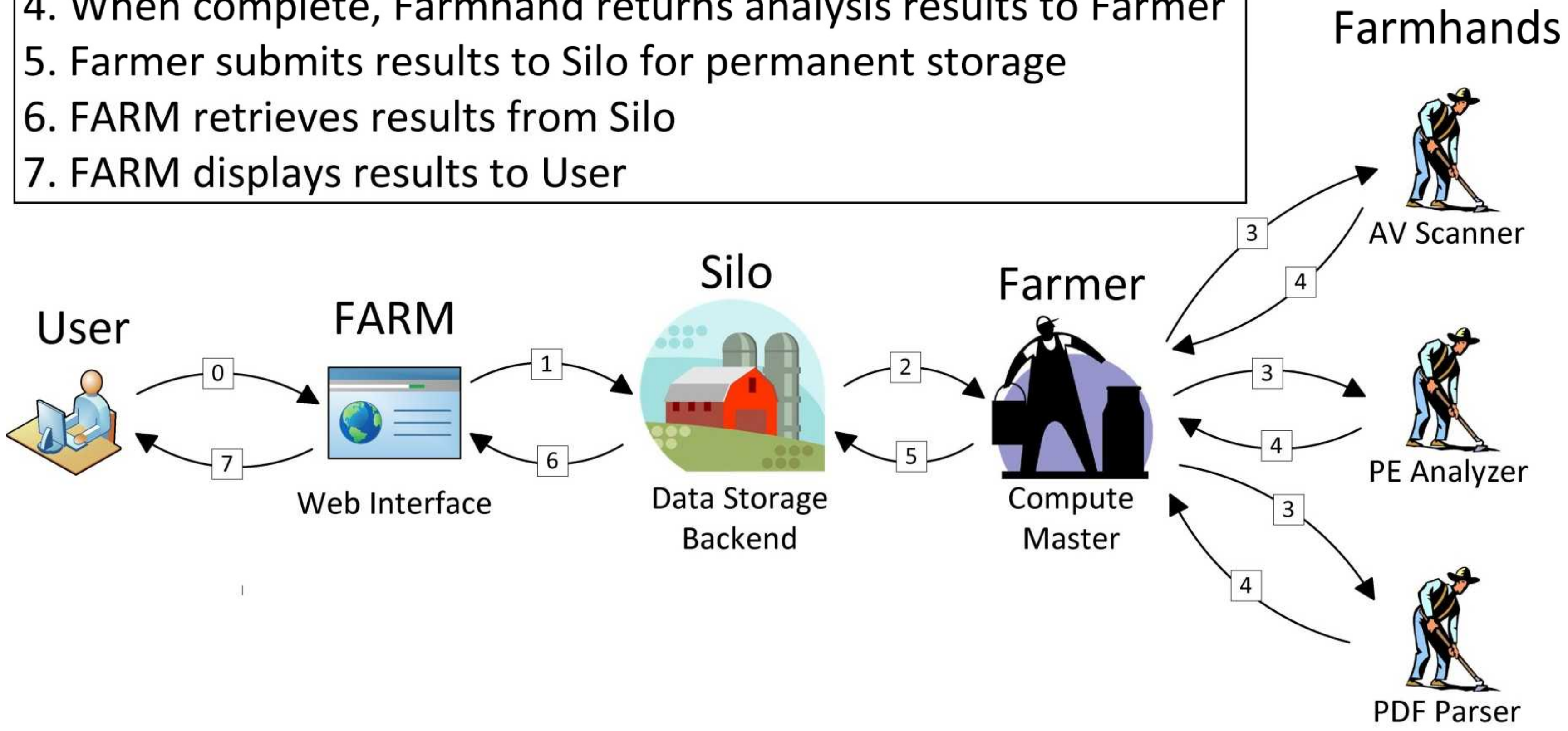
COTS, GOTS, and Open Source Tools

FARM Features

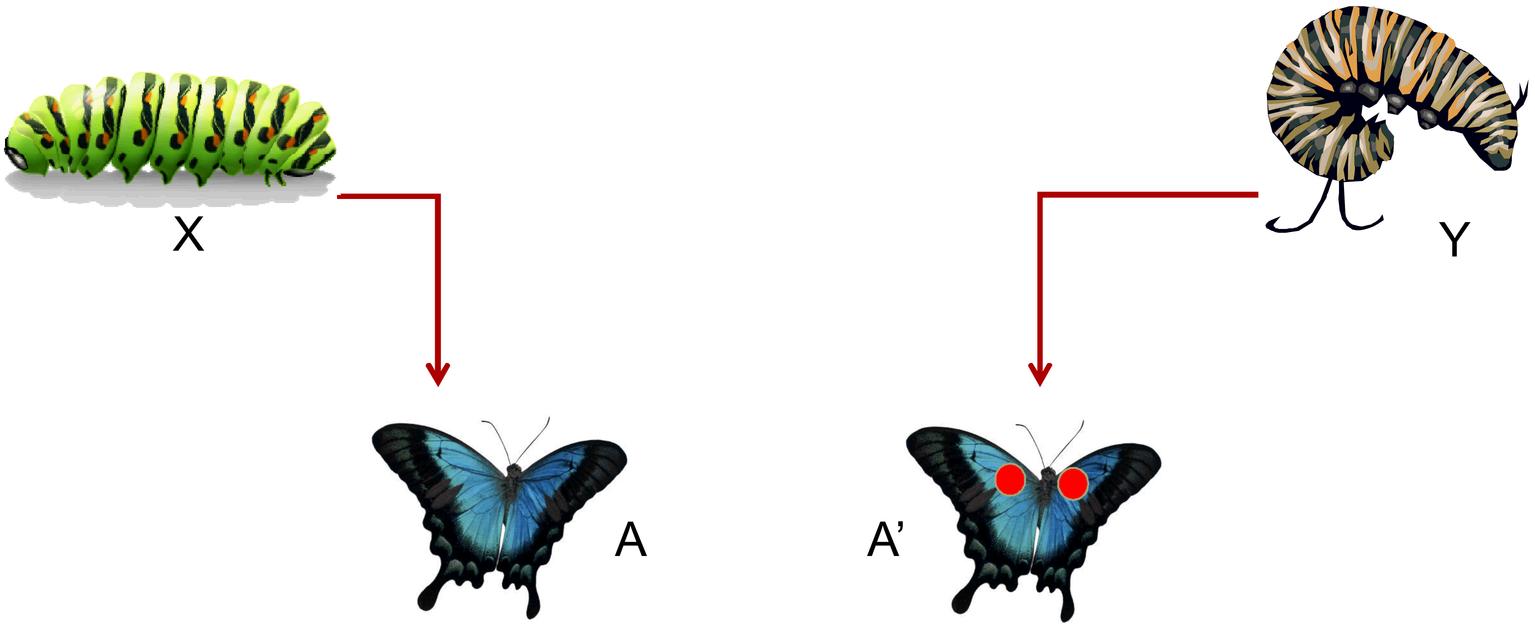
- Scalability
  - Distributed Database
  - Private Cloud-based processing backend
- Modularity:
  - Easily add new analysis modules
  - RESTful API – easy automation and integration with other applications
- Full text search
- Automatic similarity detection
  - Fuzzy hashing
  - Function clustering
- Group-based access controls

Scalability and Modularity

0. User uploads suspicious file to FARM
1. FARM transfers file to Silo; schedules analysis tasks
2. Farmer retrieves list of tasks; schedules tasks for Farmhands
3. Farmhand retrieves a single task
4. When complete, Farmhand returns analysis results to Farmer
5. Farmer submits results to Silo for permanent storage
6. FARM retrieves results from Silo
7. FARM displays results to User



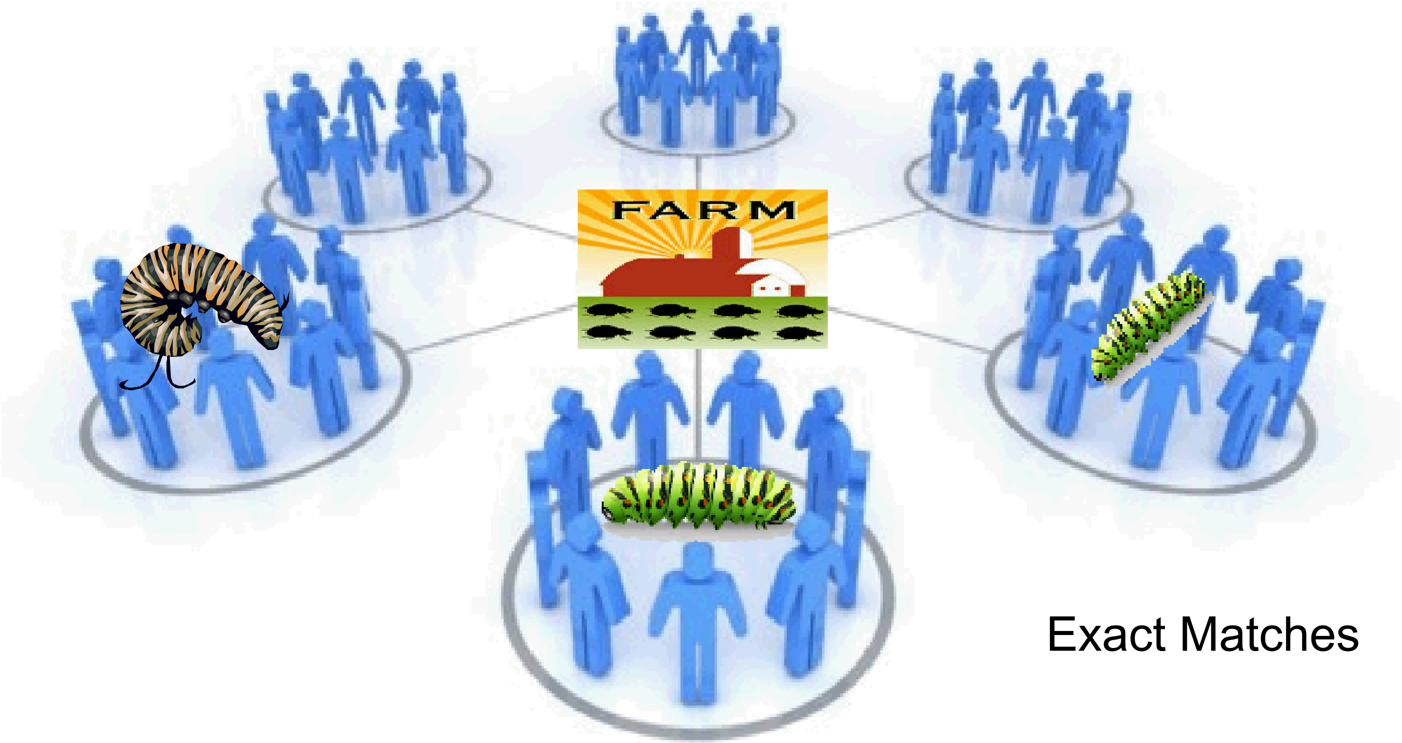
Similarity Detection



A is similar to A’ despite X !=Y

Connecting Communities

Connecting Communities



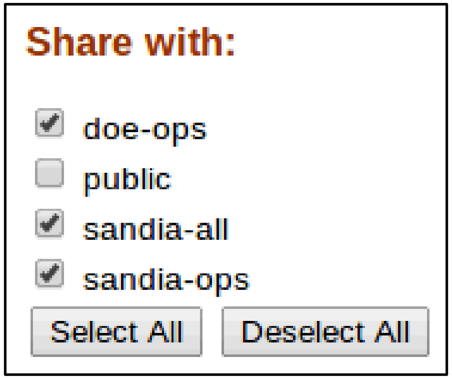
Exact Matches

Connecting Communities

Fuzzy Matches

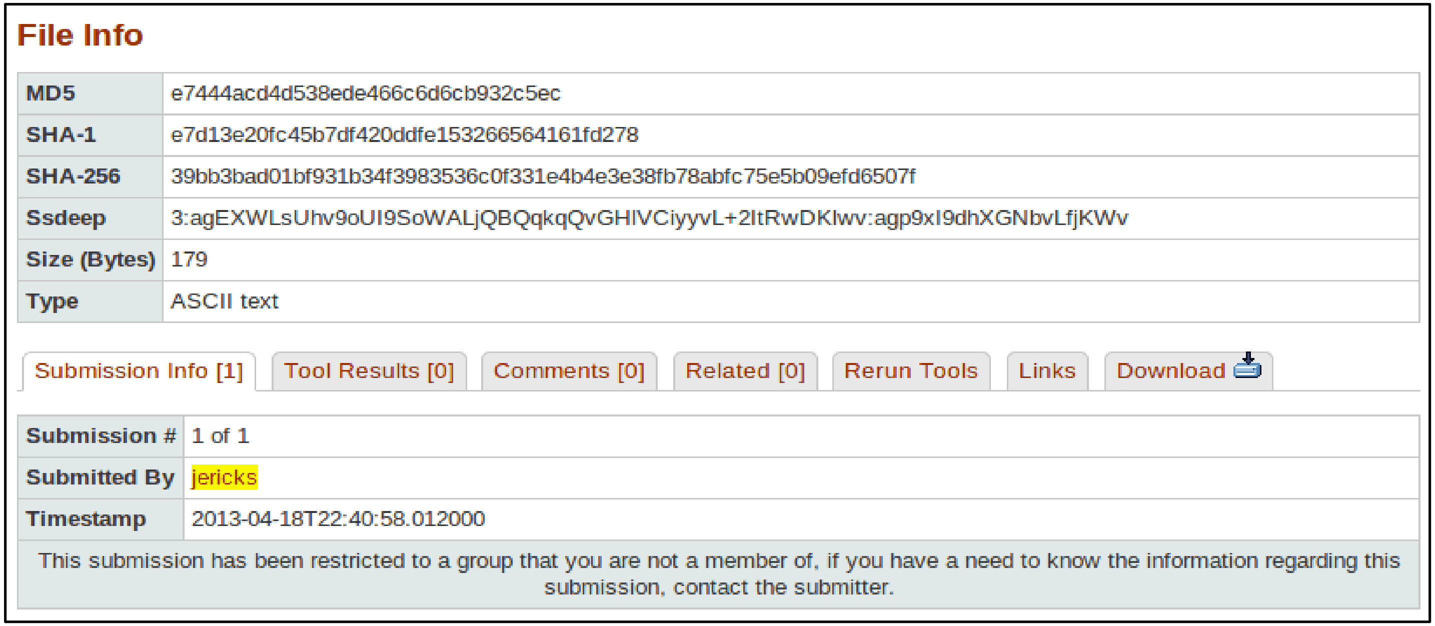
Group-based Access Control

- Restrict sample analysis, metadata
  - Further restrict comments individually
- What can you see without access?
  - Sample hashes and submitter username



Share with:

☑ doe-ops
□ public
☑ sandia-all
☑ sandia-ops



File Info

MD5	e7444acd4d538ede466c6d6cb932c5ec
SHA-1	e7d13e20fc45b7df420ddfe153266564161fd278
SHA-256	39bb3bad01bf931b34f3983536c0f331e4b4e3e38fb78abfc75e5b09efd6507f
Ssdeep	3:agEXWLsUhv9oUI9SoWALjQBQqkqQvGHIVCiyyvL+2ltRwDKlwv:agp9xI9dhXGNbvLfjKWv
Size (Bytes)	179
Type	ASCII text

Submission #	1 of 1
Submitted By	jericks
Timestamp	2013-04-18T22:40:58.012000

This submission has been restricted to a group that you are not a member of, if you have a need to know the information regarding this submission, contact the submitter.

But what is FARM really good for?

USE CASES

Use Case: Reduce 3rd party software risk

- Prior to installing 3rd party software on a critical system. Submit to FARM.

  - FARM will automatically extract network behavioral signatures from the software -- Input these behavioral signatures into a network based IPS/IDS.

  - FARM will find similar software based on fuzzy hash and functionality to other software already in the repository – if similar to malware behavior, alert and investigate.

Use Case: Collaboration for attribution

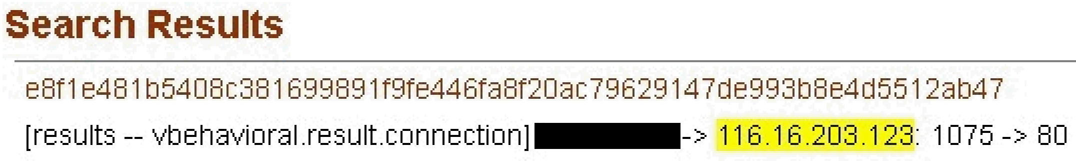
- LLNL IR analyst finds a malware sample related to an APT attacker and submits it to FARM.

- FARM unpacks the malware and finds that the unpacked child is very similar to another very different sample submitted by SNL.

- LLNL IR analyst contacts SNL IR analyst for more information and augments their corresponding IR reports.

Use Case: Behavioral Metadata Search

- New malware indicators become available through external collaborator studying Waledac Botnet
  - Analyst feeds known bad IP address into search to determine if FARM has analyzed samples that use the given IP address



Search Results

e8f1e481b5408c381699891f9fe446fa8f20ac79629147de993b8e4d5512ab47

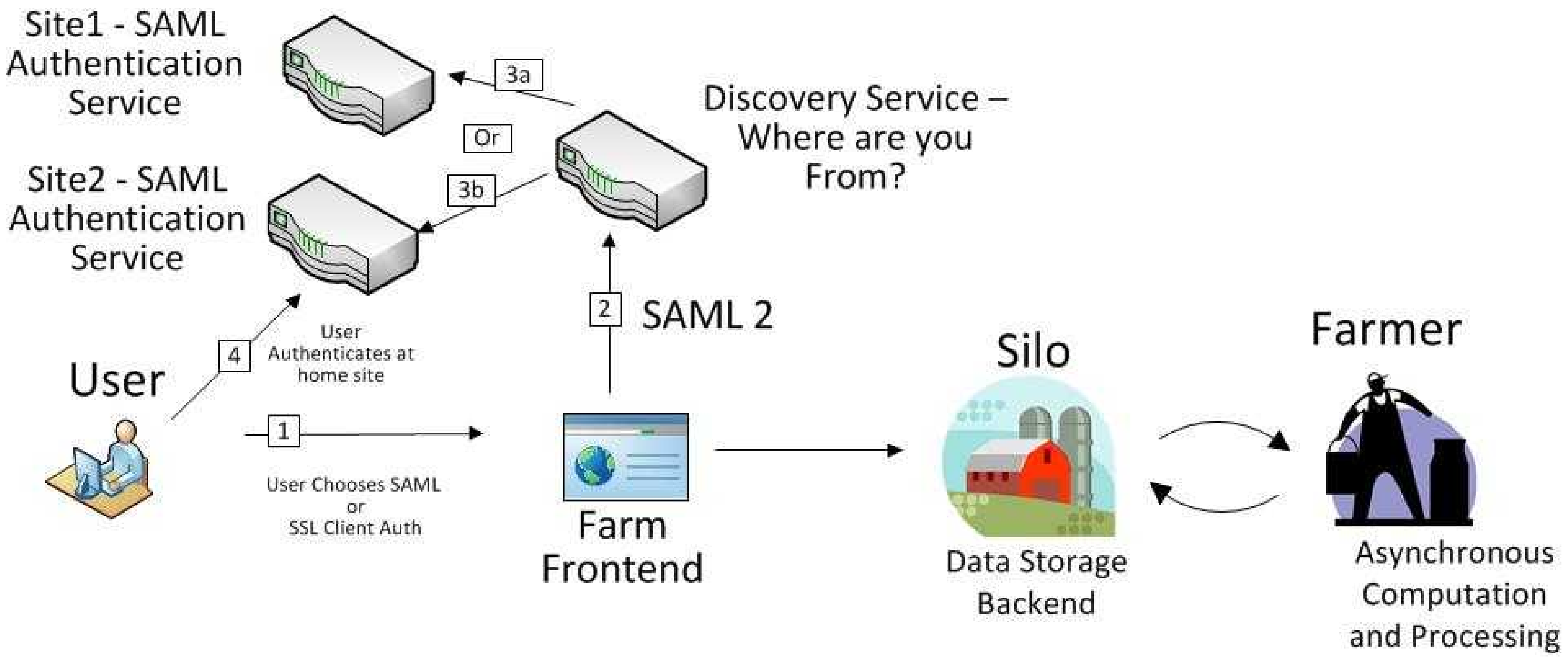
[results -- vbehavioral.result.connection] [redacted] -> 116.16.203.123: 1075 -> 80

Interested in bringing FARM into your organization’s IR workflow?

HOW TO CONNECT

Authentication

- Two options:
  - SAML Authentication
  - SSL Client Authentication


Site1 - SAML Authentication Service
3a
Or
Discovery Service – Where are you From?
Site2 - SAML Authentication Service
3b
2
SAML 2
User
4
User Authenticates at home site
1
User Chooses SAML or SSL Client Auth
Farm Frontend
Silo
Data Storage Backend
Farmer
Asynchronous Computation and Processing

Want to see FARM in action?

VIDEO PRESENTATION

Questions?

- Please contact farm@sandia.gov for additional questions or to request access to FARM.