
TRACT: Threat Rating and Assessment Collaboration Tool

Robert Hollinger and Doran Smestad

Advised by: George Heineman (WPI), Philip Marquardt (MIT/LL)

Worcester Polytechnic Institute Major Qualifying Project Presentation

October 16th, 2013

Group 51: Cyber Systems and Operations



This work is sponsored by the Assistant Secretary of Defense for Research & Engineering under Air Force Contract #FA8721-05-C-0002. Opinions, interpretations, conclusions and recommendations are those of the author and are not necessarily endorsed by the United States Government.

UNCLASSIFIED



Network Analyst



- Identify cyber vulnerabilities and threats
 - The possibility of a malicious attempt to damage or disrupt a computer network or system.
- Take necessary steps to protect their network against such threats
- Sources of Information
 - Intrusion Detection System (IDS)
 - Intrusion Prevention System (IPS)
 - Server Logs
 - *Online Sources*
- Analyst Tools
 - Tools exist to process many of these sources (e.g. Splunk)
 - However, no tool exists to process the noisy online source data



Problem Area - Sources



Sources of Information:



Twitter



Blogs



Security Updates



Reported Vulnerabilities

The screenshot shows a Twitter feed with the following tweets:

- Puppet Labs @puppetlabs** (14m): See Puppet Enterprise 3.1 in action. ~2 min video: bit.ly/1btn66D #sysadmin [View media](#)
- Slashdot @slashdot** (15m): Lavabit Briefly Allowing Users To Recover Their Data bit.ly/H02f10 [Expand](#)
- SANS ISC @sans_isc** (17m): [Diary] Java Quarterly Updates, (Tue, Oct 15th): I just posted a one-liner on the latest Java Updat... bit.ly/18j2Ftp #sansisc [Expand](#) [Reply](#) [Retweet](#) [Favorite](#) [More](#)
- Dave Lewis @gattaca** (18m): @spacerog I find most search engines won't serve up results when on Tor. Had one site lock me out for using Tor as well. [View conversation](#)
- Splunk Answers @splunkanswers** (19m): Adding Custom MIBs ift.tt/19LqxIH [Expand](#)
- SecurityWeek @SecurityWeek** (20m): APT Attack Targets South Korea, United States for Years securityweek.com/apt-attack-tar

At the bottom of the screenshot, a snippet of text reads: "Multiple security issues in systemd have been discovered by..."

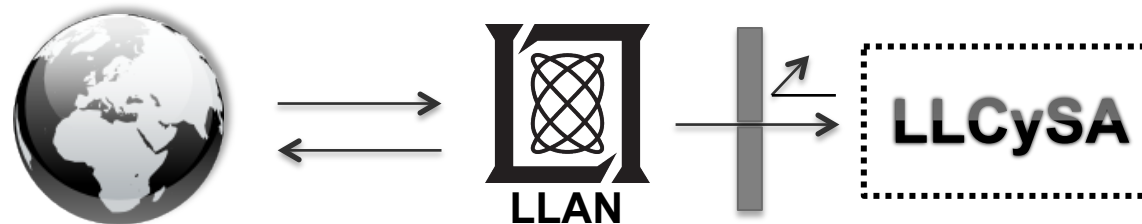


Background



Determine which threats apply to us

- **Lincoln Research Network Operation Center (LRNOC)**
 - Holds Lincoln Laboratory Network Data
 - Research Environment to Build Better Cyber Tools
 - Isolated Network
- **Lincoln Laboratory Cyber Situational Awareness (LLCySA) Platform**
 - Framework to query data from the LRNOC





Problem Statement



1,2 – Analysts receive large amounts of data from online sources.



Sources

Analyst: “Is there a threat?”



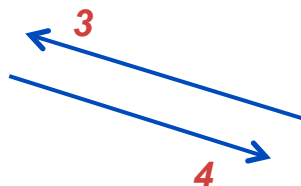
Problem Statement



3,4 – Analysts review source data for possible threats.



Threats



Analyst: "Is there a threat?"



Sources

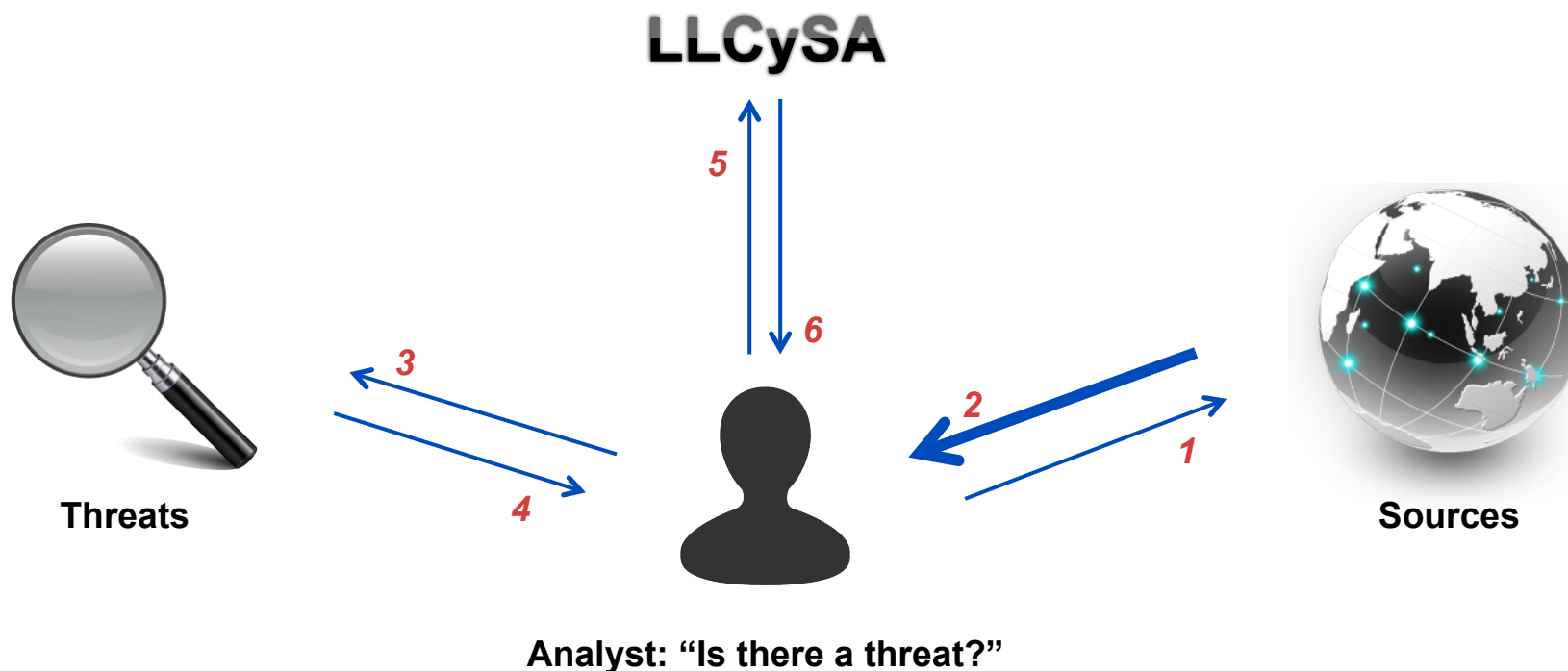




Problem Statement



5,6 – Analysts can query LLCySA to determine relevance.



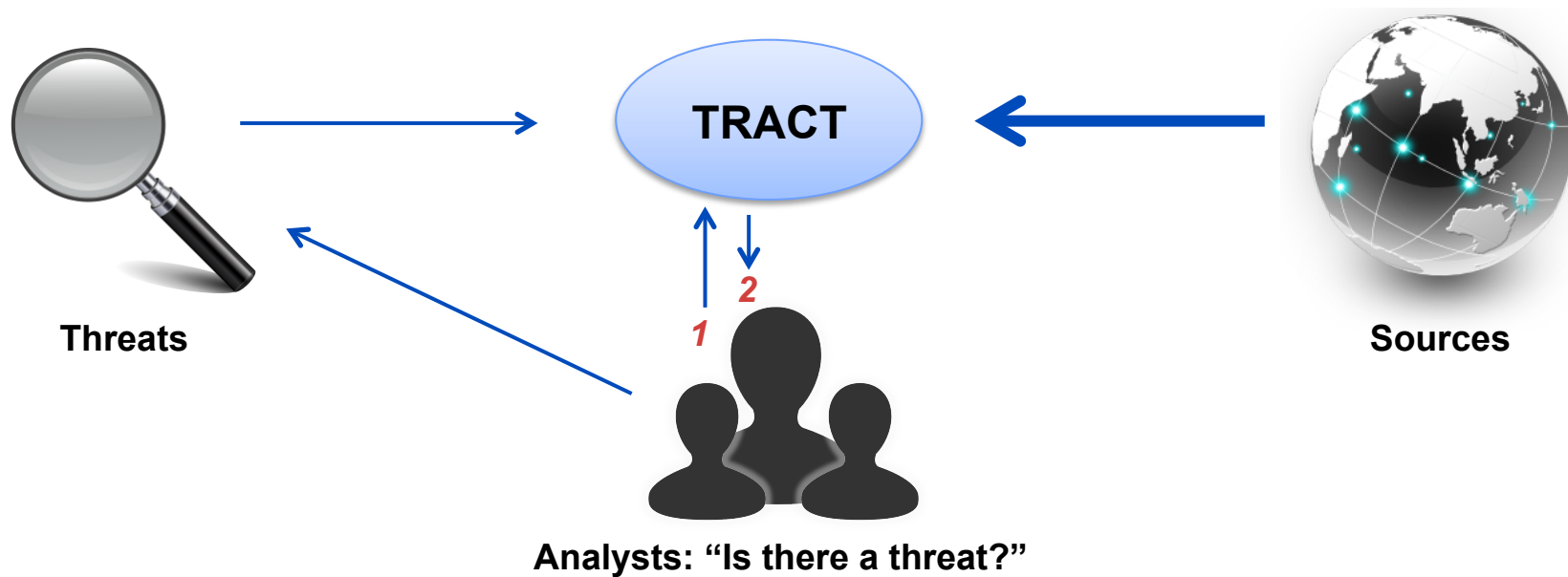
Analysts are required to manually review search, sort, and organize data.



Threat Rating and Assessment Collaboration Tool



1,2 – Analysts search data held by TRACT

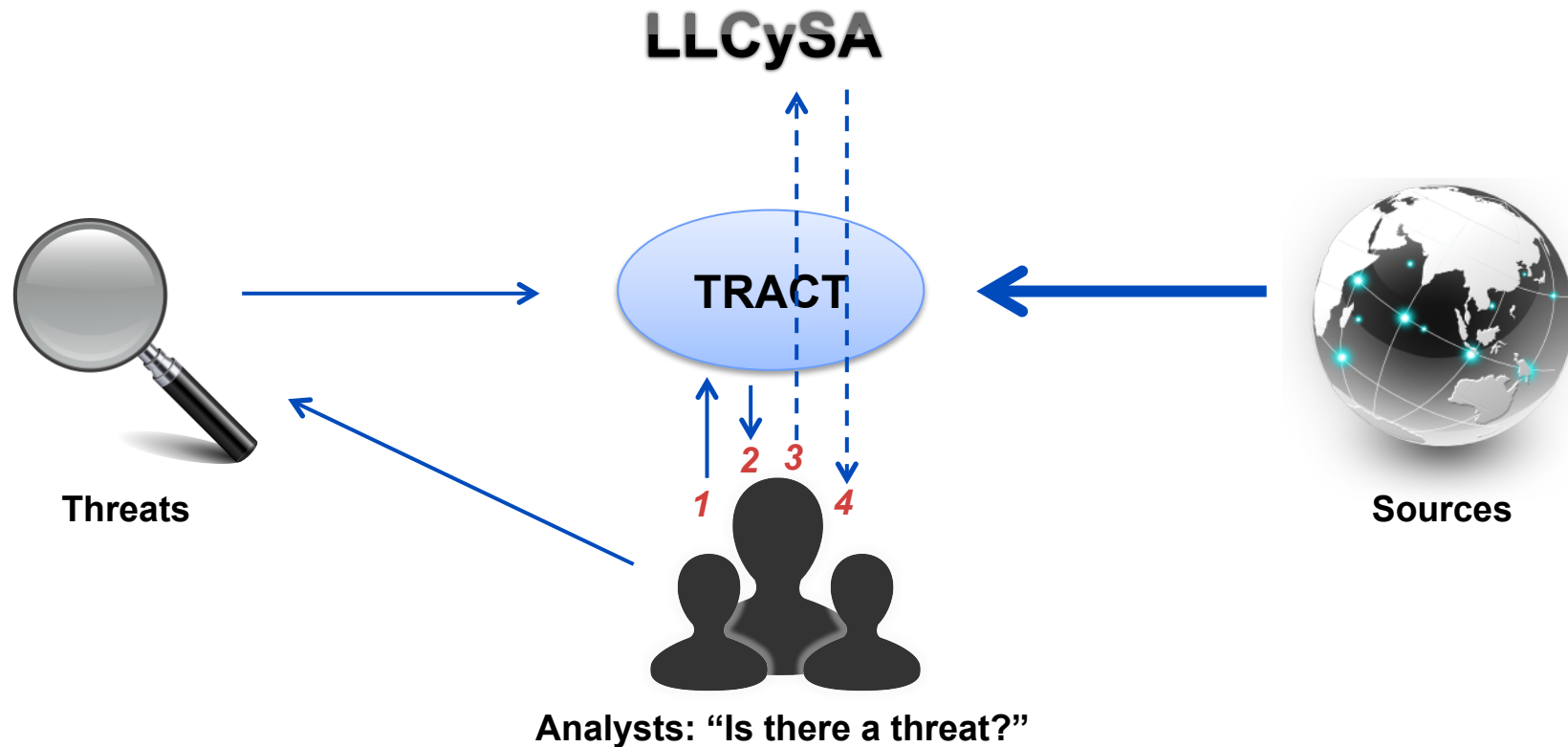




Threat Rating and Assessment Collaboration Tool



3,4 – Analysts query LLCySA to determine relevance



TRACT allows Analysts to collectively process more data with less noise.



Information Retrieval



Information Retrieval:

Location of relevant documents from a corpus of information

Regular Expression:

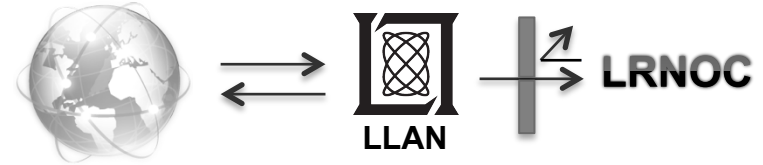
Sequence of characters describing a text pattern

Examples:

- (Firefox)
- (Firefox)|(Chrome)
- (Firefox){0-5}(4)
- ([0-9]{1,3})\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}



Design Considerations



- Transfer of Information
- Permanent Storage of Information
- User Interface communication with the database
- Collaboration between Analysts





User Interface - Welcome



TRACT

Welcome Robert [Dashboard](#)

Global Popular Searches [Load](#)

My Recent Searches [Load](#)

[Flagged Posts](#) [My Saved Searches](#)

Start Search

Regular Expression

Dimension

Time Range From To [Search](#)



User Interface - Search



TRACT

Search Results

Search Expression: Firefox
Result Dimension: browser

New Search Save Search LLCySA Query Refine Search

Flag	Type	Source Title	Article Title	Author	Date	Body
<input type="checkbox"/>	twitter-search	Firefox Vulns Search	Firefox vulnerability lang:en	liberty	10/11/13 06:30:45	High-Tech Bridge launches #free real time vulnerability detector for @Firefox #TechNews
<input type="checkbox"/>	twitter-search	Firefox Vulns Search	Firefox vulnerability lang:en	Ville Raassina	10/11/13 03:11:12	Symantec Vulnerability Protection Add-in for Firefox (Browser IPS Addin) - update Symantec Connect Community http://t.co/VSp75v3Ak
<input type="checkbox"/>	twitter-search	Firefox Vulns Search	Firefox vulnerability lang:en	Maldicore Alerts	10/10/13 13:13:26	Vuln: Mozilla Firefox/Thunderbird/SeaMonkey CVE-2013-1737 Security Bypass Vulnerability http://t.co/YWkB50OmZg http://t.co/FfgqYn1u2f
<input type="checkbox"/>	twitter-list	Bchadsworth: List 1	bchadsworth/list-1	Jonathan Cran	10/10/13 11:50:35	RT @antisnatchor: I've just added to @beefproject a Firefox Extension dropper module. Based on @mihi42 original work;-) https://t.co/PohV...
<input type="checkbox"/>	twitter-search	Firefox Vulns Search	Firefox vulnerability lang:en	Maldicore Alerts	10/10/13 09:44:19	Vuln: Mozilla Firefox/Thunderbird/SeaMonkey CVE-2013-1728 Security Vulnerability http://t.co/WrpA1nGiz7 http://t.co/FfgqYn1u2f
<input type="checkbox"/>	twitter-search	Firefox Vulns Search	Firefox vulnerability lang:en	Security News	10/10/13 07:01:53	High-Tech Bridge launches free real time vulnerability detector for Firefox ITProPortal, http://t.co/Q8UmV3HsdI
<input type="checkbox"/>	twitter-search	Firefox Vulns Search	Firefox vulnerability lang:en	Artur Barseghyan	10/10/13 06:40:53	High-Tech Bridge launches free real time vulnerability detector for Firefox http://t.co/Zlafyu5Ckc
<input type="checkbox"/>	twitter-search	Firefox Vulns Search	Firefox vulnerability lang:en	Kemlyn	10/10/13 06:05:01	High-Tech Bridge launches free real time vulnerability detector for Firefox http://t.co/JHF7Mfu8vT via @itproportal



User Interface - Search



The screenshot shows a web browser window titled 'TRACT' displaying search results. The search expression is 'Firefox' and the result dimension is 'browser'. The results are presented in a table with columns: Article Title, Author, Date, and Body.

Article Title	Author	Date	Body
Firefox vulnerability lang:en	liberty	10/11/13 06:30:45	High-Tech Bridge launches #free real time vulnerability detector for @Firefox http://t.co/BibOIZ0H1K #TechNews
Firefox vulnerability lang:en	Ville Raassina	10/11/13 03:11:12	Symantec Vulnerability Protection Add-in for Firefox (Browser IPS Addin) - update Symantec Connect Community http://t.co/VSp75vI3Ak
Firefox vulnerability lang:en	Maldicore Alerts	10/10/13 13:13:26	Vuln: Mozilla Firefox /Thunderbird/SeaMonkey CVE-2013-1737 Security Bypass Vulnerability http://t.co/YWkB50OmZg http://t.co/FfgqYn1u2f
bchadsworth/list-1	Jonathan Cran	10/10/13 11:50:35	RT @antisnatchor: I've just added to @beefproject a Firefox Extension dropper module. Based on @mihi42 original work ;-) https://t.co/PohV...



User Interface - Refine



Cyber Threat Detection Tool

< -> Search Results

Search Expression: (Firefox)

Result Dimension: browser

Cancel Refine

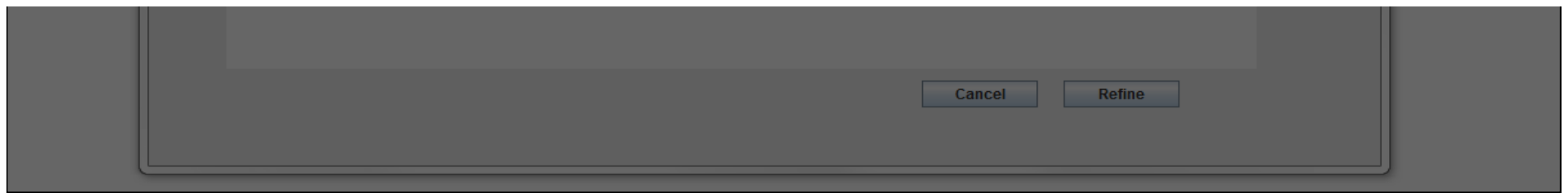
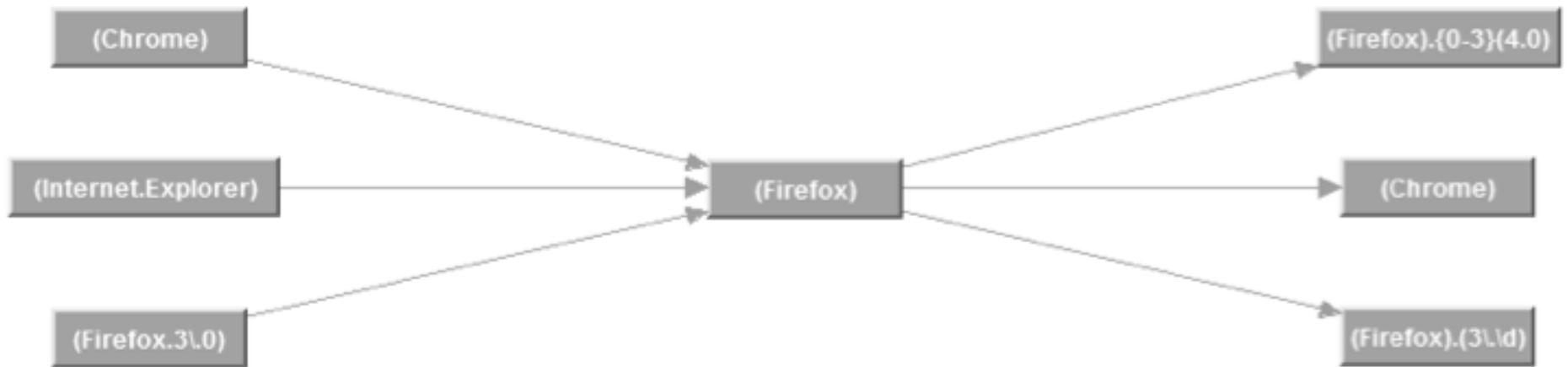
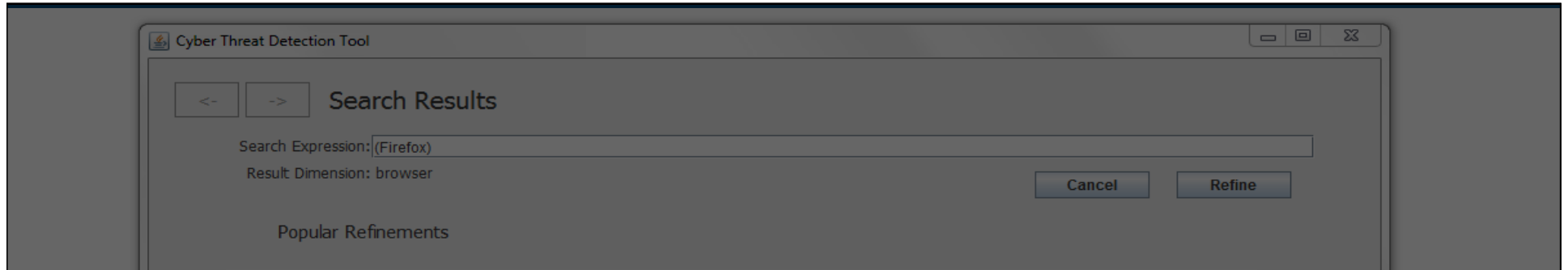
Popular Refinements

```
graph LR; C1["(Chrome)"] --> F["(Firefox)"]; IE["(Internet.Explorer)"] --> F; F3L0["(Firefox.3L0)"] --> F; F --> F034["(Firefox).(0-3)(4.0)"]; F --> C2["(Chrome)"]; F --> F3Ld["(Firefox).(3L,d)"]
```

Cancel Refine

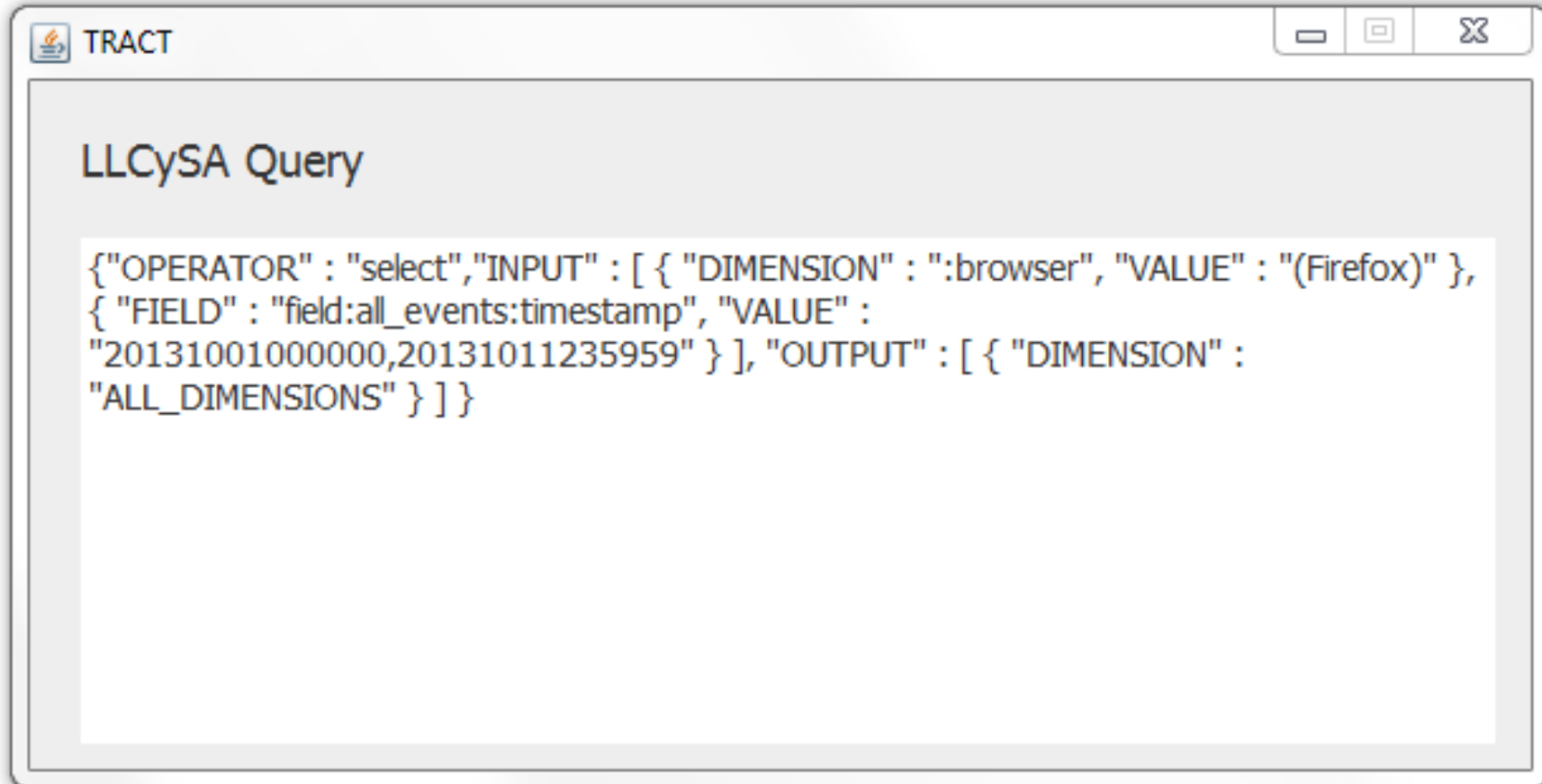


User Interface - Refine





User Interface - LLCySA



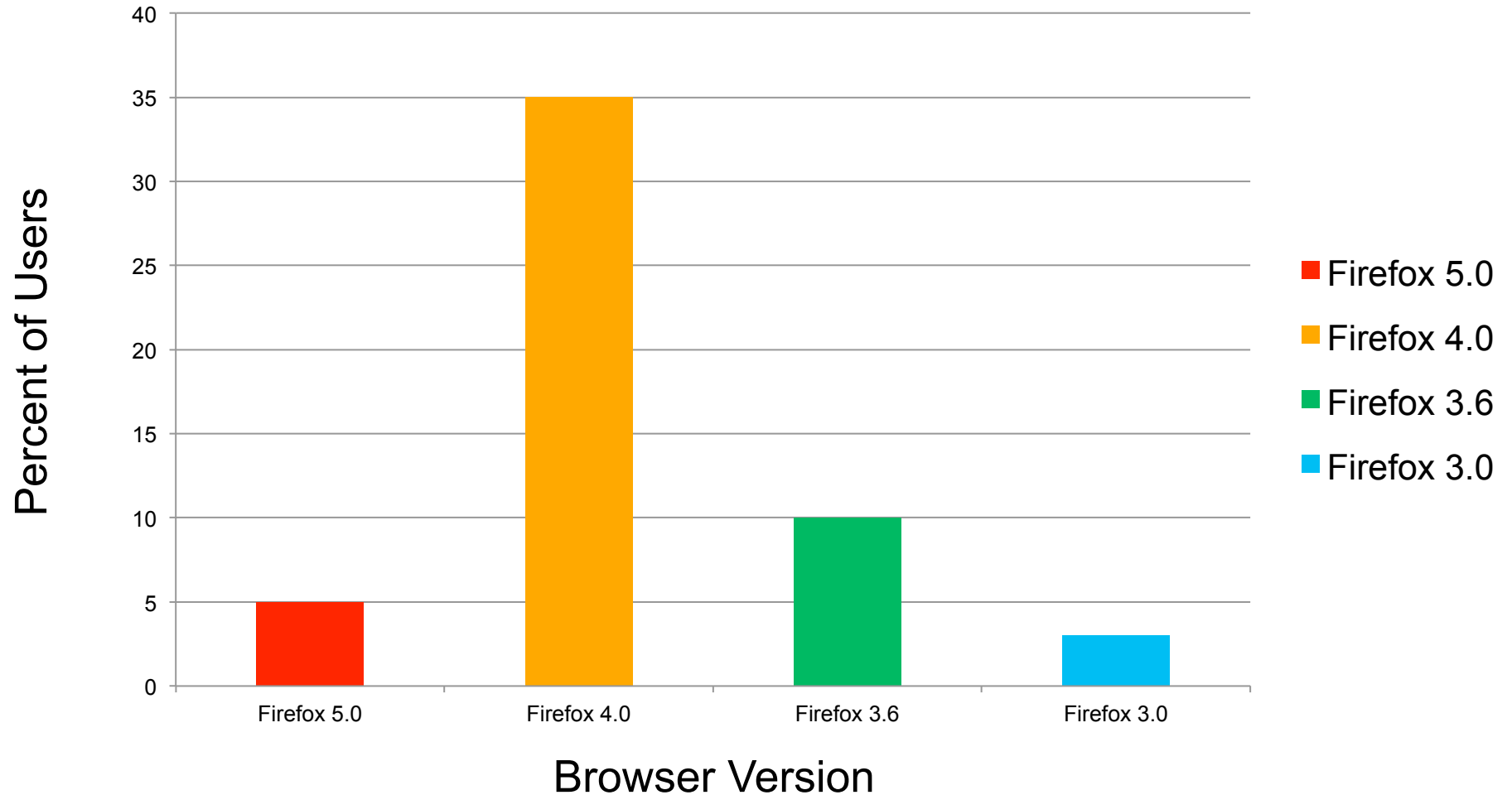


User Interface - LLCySA



**Example Purposes Only
Not Actual Data**

Use of Firefox in Lincoln Laboratory

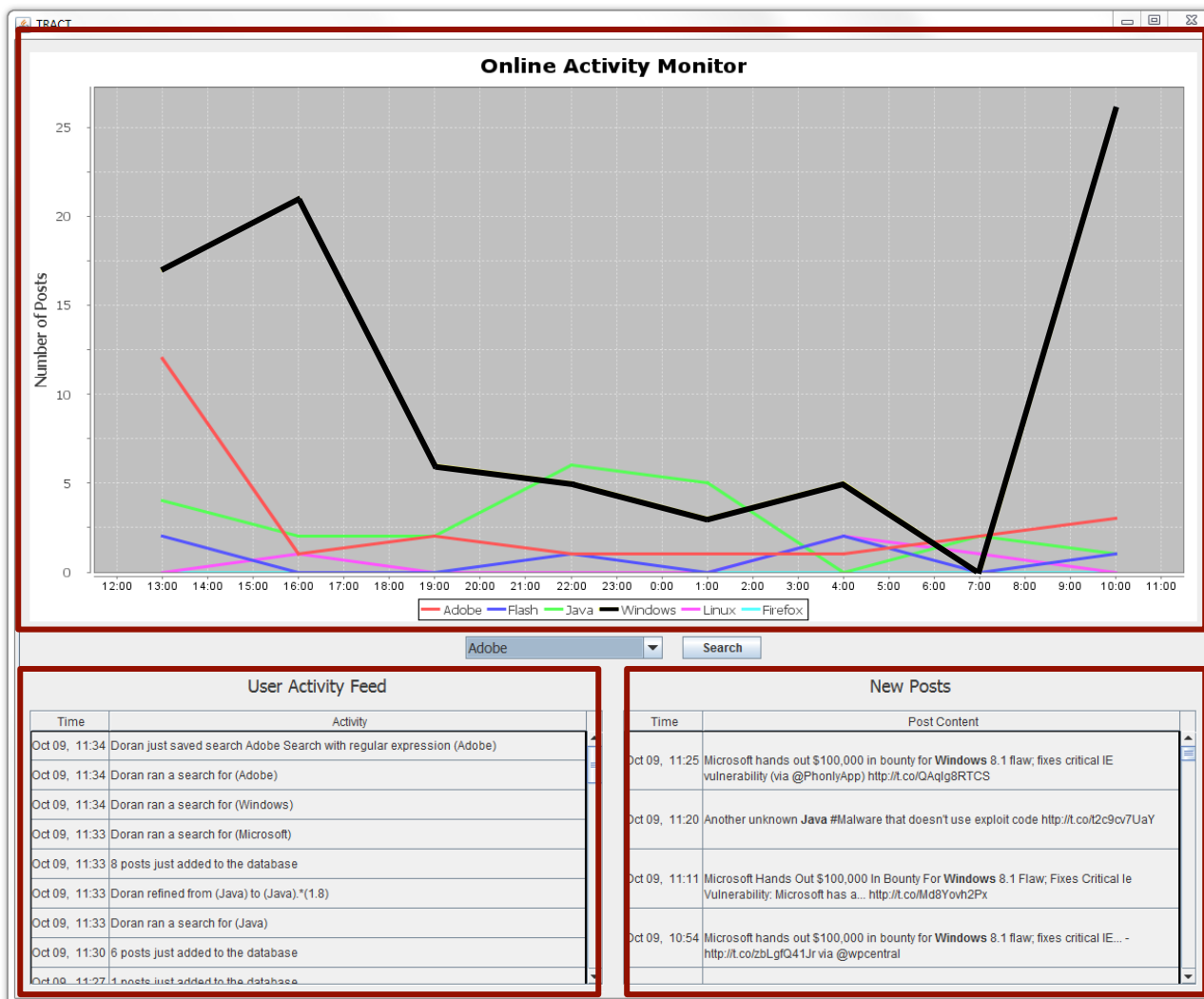




User Interface - Dashboard

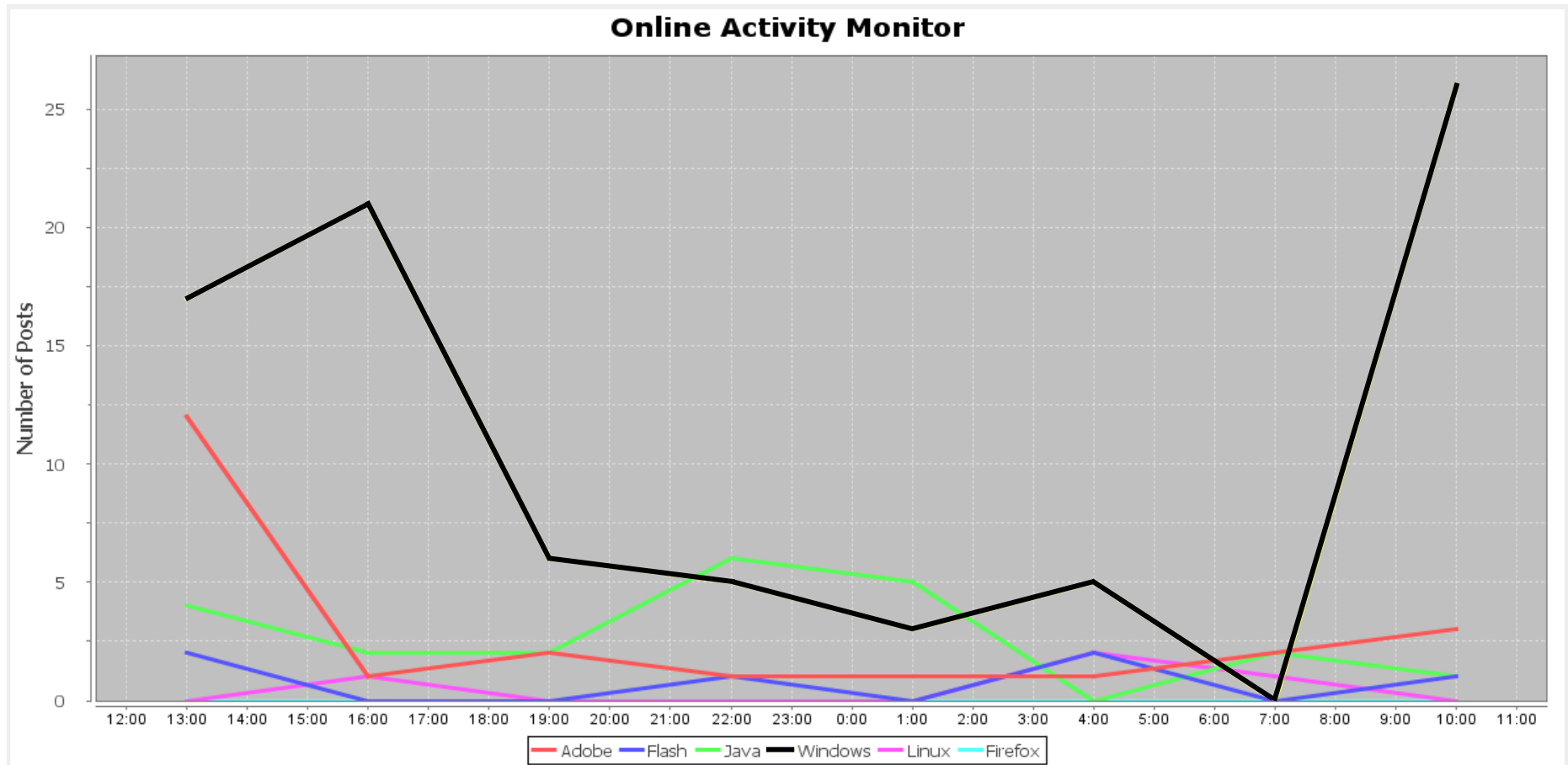


WPI





User Interface - Dashboard





User Interface - Dashboard



Time	Post Content
Oct 09, 11:25	Microsoft hands out \$100,000 in bounty for Windows 8.1 flaw; fixes critical IE vulnerability (via @PhonlyApp) http://t.co/QAqlg8RTCS
Oct 09, 11:20	Another unknown Java #Malware that doesn't use exploit code http://t.co/t2c9cv7UaY
Oct 09, 11:11	Microsoft Hands Out \$100,000 In Bounty For Windows 8.1 Flaw; Fixes Critical Ie Vulnerability: Microsoft has a... http://t.co/Md8Yovh2Px
Oct 09, 10:54	Microsoft hands out \$100,000 in bounty for Windows 8.1 flaw; fixes critical IE... - http://t.co/zbLgfQ41Jr via @wpcentral



User Interface - Dashboard



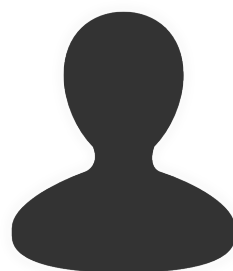
Time	Activity
Oct 09, 11:34	Doran just saved search Adobe Search with regular expression (Adobe)
Oct 09, 11:34	Doran ran a search for (Adobe)
Oct 09, 11:34	Doran ran a search for (Windows)
Oct 09, 11:33	Doran ran a search for (Microsoft)
Oct 09, 11:33	8 posts just added to the database
Oct 09, 11:33	Doran refined from (Java) to (Java).*(1.8)
Oct 09, 11:33	Doran ran a search for (Java)
Oct 09, 11:30	6 posts just added to the database
Oct 09, 11:27	1 posts just added to the database



Evaluation



LRNOC



Analysts

LLCySA

- Dedicated display to show our Dashboard in the LRNOC
- Ingestion of user refinement data into the LLCySA platform
- Received positive reaction from Analysts and they plan to use it in their work



Conclusion



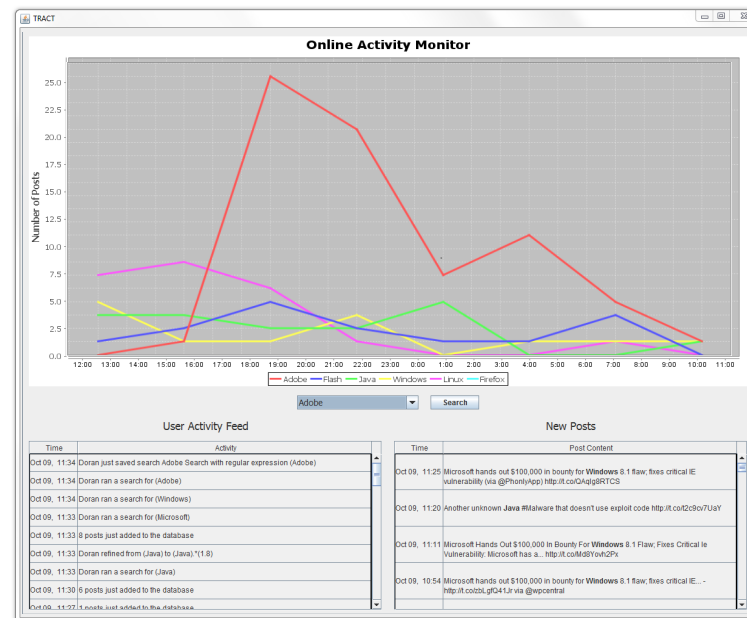
- Identified a gap in the analyst toolset
- Developed system to assist analysts in the process of gaining relevant threat information from online sources
- Reviewed system with analysts

Puppet Labs @puppetlabs 14m
See Puppet Enterprise 3.1 in action. ~2 min video: bit.ly/1btn66D
#sysadmin
[View media](#)

Slashdot @slashdot 15m
Lavabit Briefly Allowing Users To Recover Their Data bit.ly/H02f10
Expand

SANS ISC @sans_isc 17m
[Diary] Java Quarterly Updates, (Tue, Oct 15th):
I just posted a one-liner on the latest Java Updat... bit.ly/18j2Ftp
#sansisc
Expand [Reply](#) [Retweet](#) [Favorite](#) [More](#)

Dave Lewis @gattaca 18m
[@spacerog](#) I find most search engines won't serve up results when on Tor. Had one site lock me out for using Tor as well.
[View conversation](#)





Future Work



Advanced Information Retrieval



Full Graphing of Refinements



Full integration with LRNOC



LRNOC





Acknowledgements



Philip Marquardt, MIT/LL Advisor, LRNOC Lead

George Heineman, WPI Advisor

David O'Gwynn, LLCySA Technical Staff

Kathleen Haas, MQP Coordinator

Ted Clancy, WPI Project Site Lead



Backup Slides



BACKUP SLIDES



System Flow of Information



WPI

