

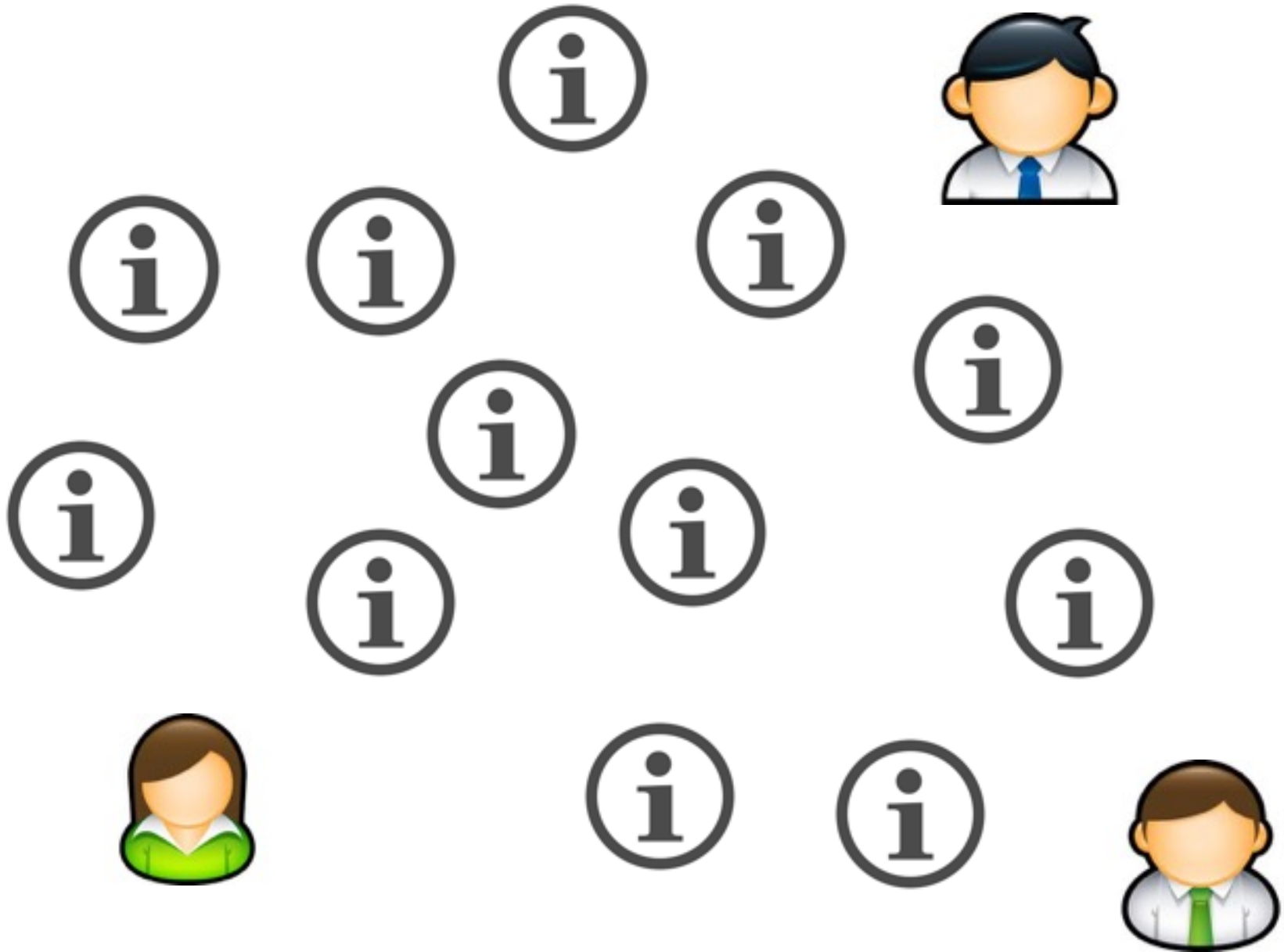
| galois |

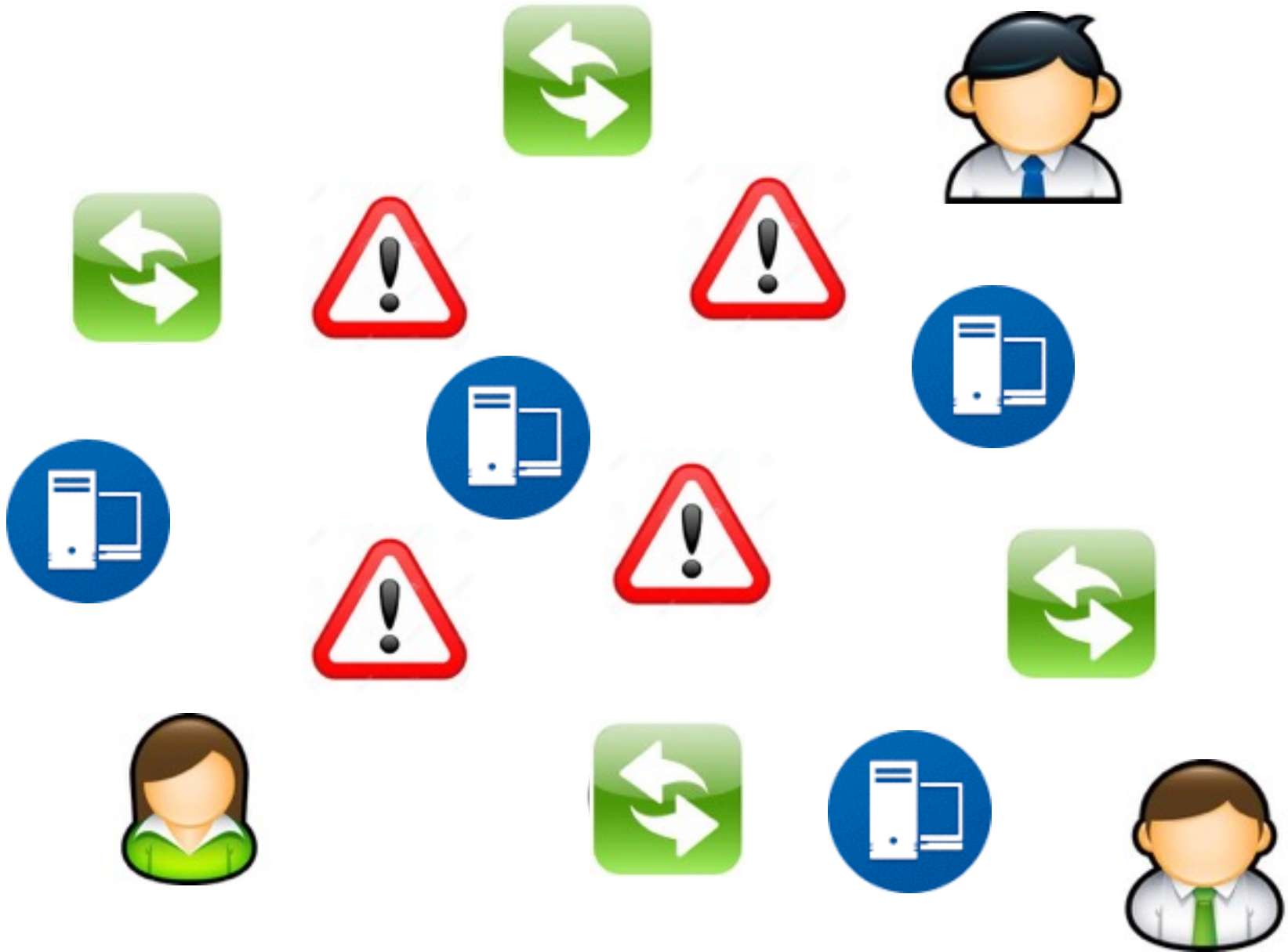
TFER: Threat Fusion & Effective Response

Galois [gal-wah] Named after French mathematician Évariste Galois

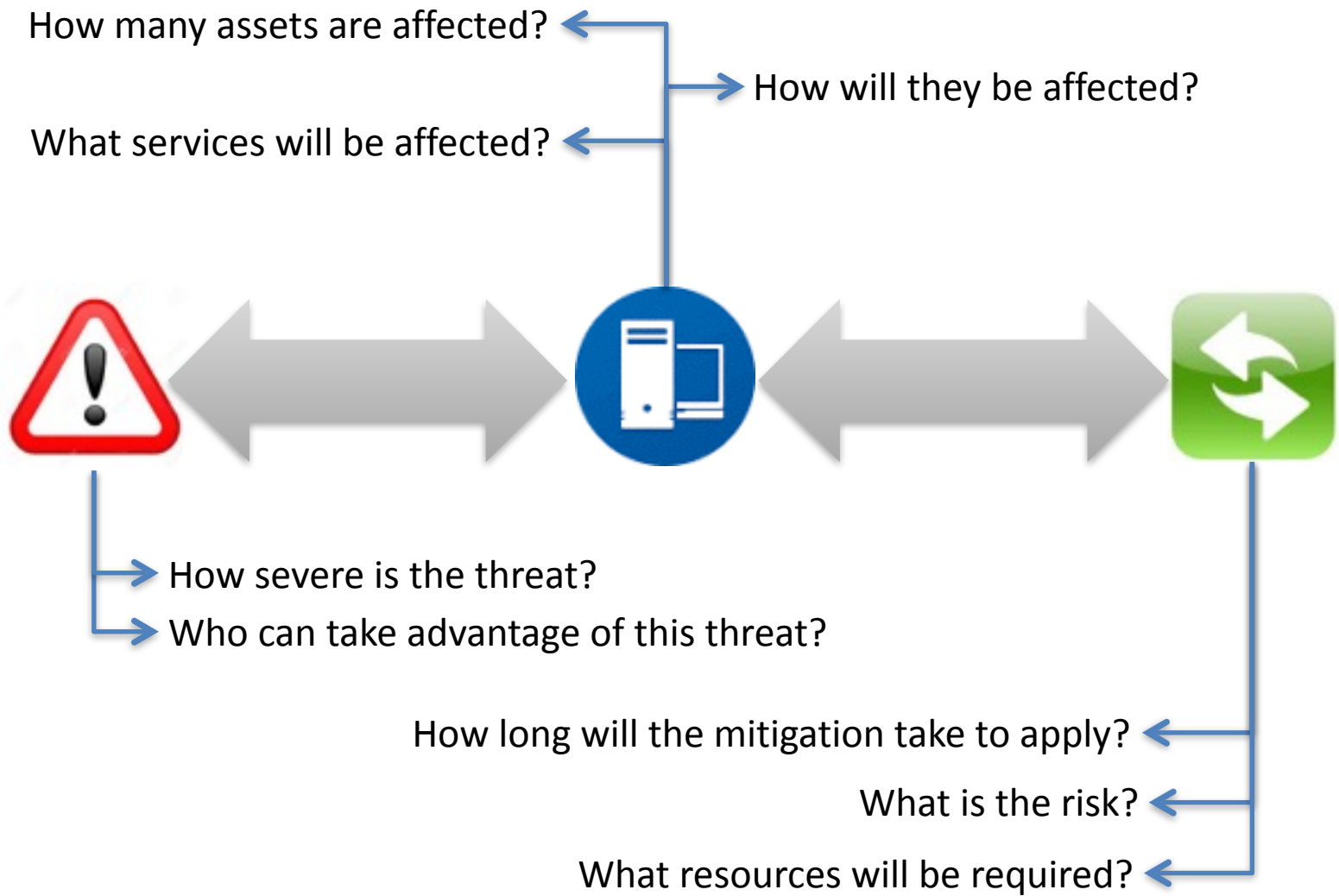
www.galois.com











Project goals

Improve analyst efficiency and collaboration by leveraging existing workflows, standards, and **state of the art automation**, resulting in an **easy-to-understand reference prototype** that links high-level threats to low-level data.

DEMONSTRATION

TFER Decision Support System | localhost:8000 | TFER 0.3 | Perspective: default | EDIT | NEW | REFRESH | Logged in as: Alice | LOG OUT | MANAGE

Threats

Sort by unmitigated risk

- Debian: 3396-1: linux: Summary
 - Likelihood: 1
 - Total posed risk: C 2.66 | I 3.33 | A 3.33 | Total 9.33
 - Remaining risk: C 2.66 | I 3.33 | A 3.33 | Total 9.33
- Debian: 3381-1: openjdk-7: Summary
 - Likelihood: 1
 - Total posed risk: C 2.66 | I 3.33 | A 3.33 | Total 9.33
 - Remaining risk: C 2.66 | I 3.33 | A 3.33 | Total 9.33
- Debian: 3382-1: gdm3-admin: Summary
 - Likelihood: 1
 - Total posed risk: C 2.66 | I 3.33 | A 3.33 | Total 9.33
 - Remaining risk: C 2.66 | I 3.33 | A 3.33 | Total 9.33

Assets

Sort by number of threats

- SiliconMechanics Rackform iServ R133 SM6...
 - 00:00 | 5e:00:52:1f
 - Threats: 22
 - Impact: C MEDIUM | MEDIUM | A MEDIUM
 - OS: Ubuntu
- Lenovo ThinkPad X230 FK0T014 2016-09-1?
 - 00:00 | 5e:00:52:1e
 - Threats: 22
 - Impact: C MEDIUM | MEDIUM | A MEDIUM
 - OS: Ubuntu
- Asus Eee PC 1000HE 970AAS172611
 - 00:00 | 5e:00:52:25
 - Threats: 7
 - Impact: C LOW | LOW | A LOW
 - OS: Windows
- Dell PowerEdge 1425SC 21 2/3/09
 - 00:00 | 5e:00:52:08

Mitigations

Sort by number of threats

- MS15-113 - Critical: Cumulative Security Upd...
 - Threats: 5
 - Cost: 0.1
 - Total potential benefit: C 1.21 | I 1.21 | A 1.21
 - Remaining benefit: C 1.21 | I 1.21 | A 1.21
- MS15-099 - Critical: Vulnerabilities in Micros...
 - Threats: 4
 - Cost: 0.1
 - Total potential benefit: C 0.3 | I 0.3 | A 0.3
 - Remaining benefit: C 0.3 | I 0.3 | A 0.3
- MS15-091 - Critical: Cumulative Security Upd...
 - Threats: 4
 - Cost: 0.1
 - Total potential benefit: C 0.77 | I 0.77 | A 0.77
 - Remaining benefit: C 0.77 | I 0.77 | A 0.77

TFER Decision Support System

localhost:8000

TFER 0.3 Perspective: default EDIT NEW REFRESH Logged in as: Alice LOG OUT MANAGE

Threats

Sort by unmitigated risk

- Ubuntu: 2745-1: QEMU vulnerabilities**
 Likelihood: 1
 Total posed risk: 3.66
 Remaining risk: 3.66
- Ubuntu: 2806-1: Linux kernel (Vivid HWE)...**
 Likelihood: 1
 Total posed risk: 3.66
 Remaining risk: 3.66
- Ubuntu: 2754-1: Thunderbird vulnerabili...**
 Likelihood: 1
 Total posed risk: 3.66

Assets

Sort by number of threats

- Lenovo ThinkPad X1230 PK0T014 2016-0...**
 Threats: 22
 Impact: HIGH | LOW | LOW
 OS: Ubuntu
- Asus Eee PC 1000HE 970AAS172611**
 Threats: 7
 Impact: LOW | LOW | LOW
 OS: Windows
- Dell PowerEdge 1425SC 21 2/3/09**
 Threats: 4
 Impact: LOW | HIGH | HIGH
 OS: Debian
- Penguin Computing Ralios 2600SA P1237090...**
 OS: Debian

Mitigations

Sort by number of threats

- DSA-3381 openjdk-7**
 Threats: 2
 Cost: 0.1
 Total potential benefit: 7.66
 Remaining benefit: 7.66
- DSN-2786-1: PHP vulnerabilities**
 Threats: 2
 Cost: 0.1
 Total potential benefit: 3.33
 Remaining benefit: 3.33
- DSN-2758-1: PHP vulnerabilities**
 Threats: 2
 Cost: 0.1
 Total potential benefit: 3.33
 Remaining benefit: 3.33

localhost:8000

TFER 0.3 Perspective: default EDIT NEW REFRESH Logged in as: Alice LOG OUT MANAGE

Threats Assets Mitigations

Sort by threat name Sort by asset name Sort by number of threats

PostgreSQL 2015-10-08 Security Update ...

The PostgreSQL Global Development Group h...

Likelihood: 1

Total posed risk:

C 1 I 1 A 1 Total 3

Remaining risk:

C 0 I 0 A 0 Total 0

2862152 - Vulnerability in DirectAccess and L...

Vulnerability in DirectAccess and IPsec Could ...

Likelihood: 1

Total posed risk:

C 0.33 I 0.33 A 0.33 Total 1

Remaining risk:

C 0.33 I 0.33 A 0.33 Total 1

2896646 - Vulnerability in Microsoft Graphics...

Vulnerability in Microsoft Graphics Componen...

Likelihood: 1

Total posed risk:

Dell PowerEdge R410 23 3/26/16

00:00:5e:00:00:52:10

Threats: 1

Impact: C HIGH I HIGH A HIGH

OS: CentOS

Dell PowerVault 122T LTO-3 24 4/15/07

00:00:5e:00:00:52:11

Threats: 0

Impact: C MEDIUM I MEDIUM A MEDIUM

OS: CentOS

Dell PowerVault 124T LTO-3 25 9/19/12

00:00:5e:00:00:52:12

Threats: 0

Impact: C MEDIUM I MEDIUM A MEDIUM

OS: CentOS

Lenovo ThinkPad X230 PK0T014 2016-09-??

00:00:5e:00:00:52:1a

MS15-113 - Critical: Cumulative Security Upd...

Threats: 5

Cost: 0.1

Total potential benefit:

C 1.21 I 1.21 A 1.21

Remaining benefit:

C 1.21 I 1.21 A 1.21

MS15-107 - Important: Cumulative Security U...

Threats: 4

Cost: 0.1

Total potential benefit:

C 0.3 I 0.3 A 0.3

Remaining benefit:

C 0.3 I 0.3 A 0.3

MS15-099 - Critical: Vulnerabilities in Microso...

Threats: 4

Cost: 0.1

Total potential benefit:

C 0.3 I 0.3 A 0.3

localhost:8000

TFER 0.3 Perspective: default EDIT NEW REFRESH Logged in as: Bob LOG OUT MANAGE

Threats Assets Mitigations

Sort by threat name Sort by number of threats Sort by mitigation name

★ PostgreSQL 2015-10-08 Security Update ...

The PostgreSQL Global Development Group h...

Likelihood: 1

Total posed risk:

C 0	I 0	A 0	Total 0
-----	-----	-----	---------

Remaining risk:

C 0	I 0	A 0	Total 0
-----	-----	-----	---------

2862152 - Vulnerability in DirectAccess and L...

Vulnerability in DirectAccess and IPsec Could ...

Likelihood: 1

Total posed risk:

C 0.33	I 0.33	A 0.33	Total 1
--------	--------	--------	---------

Remaining risk:

C 0.33	I 0.33	A 0.33	Total 1
--------	--------	--------	---------

2896646 - Vulnerability in Microsoft Graphics...

Vulnerability in Microsoft Graphics Componen...

Likelihood: 1

Total posed risk:

Silicon Mechanics Rackform iServ R133 SM6...

00:00:5e:00:52:1f

Threats: 22

Impact: C MEDIUM | MEDIUM A MEDIUM

OS: Ubuntu

Lenovo ThinkPad X230 PK0T014 2016-09-??

00:00:5e:00:52:1a

Threats: 22

Impact: C MEDIUM | MEDIUM A MEDIUM

OS: Ubuntu

Asus Eee PC 1000HE 970AAS172611

00:00:5e:00:52:25

Threats: 7

Impact: C LOW | LOW A LOW

OS: Windows

Dell PowerEdge 1425SC 21 2/2/09

00:00:5e:00:52:08

★ USN-2772-1: PostgreSQL vulnerabilities

Threats: 0

Cost: 0.1

Total potential benefit:

C 0	I 0	A 0
-----	-----	-----

Remaining benefit:

C 0	I 0	A 0
-----	-----	-----

USN-2773-1: Linux kernel vulnerabilities

Threats: 0

Cost: 0.1

Total potential benefit:

C 0	I 0	A 0
-----	-----	-----

Remaining benefit:

C 0	I 0	A 0
-----	-----	-----

USN-2774-1: Linux kernel (OMAP4) vulnerabil...

Threats: 0

Cost: 0.1

Total potential benefit:

C 0	I 0	A 0
-----	-----	-----

localhost:8000

TFER 0.3 Perspective: default EDIT NEW REFRESH Logged in as: Charlie LOG OUT MANAGE

Threats Assets Mitigations

Sort by unmitigated risk

Create and switch to a new perspective

Perspective name:

Available perspectives:

Alice (1)	default	<input type="text" value="0.5"/>
Bob (1)	default	<input type="text" value="0.5"/>
Charlie (1)	default	<input type="text"/>

CANCEL CREATE

Debian: 3381-1: openjdk-7: Summary
Likelihood: 1
Total posed risk: C 2.66 | 3.33 A 3.33
Remaining risk: C 2.66 | 3.33 A 3.33

Debian: 3382-1: phpmyadmin: Summ
Likelihood: 1
Total posed risk: C 2.66 | 3.33 A 3.33
Remaining risk: C 2.66 | 3.33 A 3.33

Debian: 3367-1: wireshark: Summary
Likelihood: 1
Total posed risk: C 2.66 | 3.33 A 3.33

00:00:50:00:52:20
Threats: 3
Impact: C LOW | LOW A LOW
OS: Android

Apple iPad 160B DMPN8214FK14

MS15-091 - Critical: Cumulative Security Upd...
Threats: 4
Cost: 0.1
Total potential benefit: C 0.77 | 0.77 A 0.77

localhost:8000

TFER 0.3 Perspective: Aggregated EDIT NEW REFRESH Logged in as: Charlie LOG OUT MANAGE

Threats Assets Mitigations

Sort by unmitigated risk Sort by asset name Sort by number of threats

PostgreSQL 2015-10-08 Security Update Rele...

The PostgreSQL Global Development Group h...

Likelihood: 1

Total posed risk:

C 1	I 1	A 1	Total 3
-----	-----	-----	---------

Remaining risk:

C 1	I 1	A 1	Total 3
-----	-----	-----	---------

Debian: 3381-1: openjdk-7: Summary

Likelihood: 1

Total posed risk:

C 2.66	I 3.33	A 3.33	Total 9.33
--------	--------	--------	------------

Remaining risk:

C 2.66	I 3.33	A 3.33	Total 9.33
--------	--------	--------	------------

Debian: 3367-1: wireshark: Summary

Likelihood: 1

Total posed risk:

C 2.66	I 3.33	A 3.33	Total 9.33
--------	--------	--------	------------

Dell PowerEdge R410 23 3/25/16

00:00:5e:00:00:52:10

Threats: 1

Impact: C HIGH I HIGH A HIGH

OS: CentOS

Dell PowerVault 122T LTO 24 4/15/07

00:00:5e:00:00:52:11

Threats: 0

Impact: C MEDIUM I MEDIUM A MEDIUM

OS: CentOS

Dell PowerVault 124T LTO-3 25 9/19/12

00:00:5e:00:00:52:12

Threats: 0

Impact: C MEDIUM I MEDIUM A MEDIUM

OS: CentOS

Lenovo ThinkPad X230 PK0T014 2016-09-??

00:00:5e:00:00:52:1a

USN-2772-1: PostgreSQL vulnerabilities

Threats: 1

Cost: 0.1

Total potential benefit:

C 1	I 1	A 1
-----	-----	-----

Remaining benefit:

C 1	I 1	A 1
-----	-----	-----

MS15-113 - Critical: Cumulative Security Upd...

Threats: 5

Cost: 0.1

Total potential benefit:

C 1.21	I 1.21	A 1.21
--------	--------	--------

Remaining benefit:

C 1.21	I 1.21	A 1.21
--------	--------	--------

MS15-107 - Important: Cumulative Security U...

Threats: 4

Cost: 0.1

Total potential benefit:

C 0.3	I 0.3	A 0.3
-------	-------	-------

← → C localhost:8000

TFER 0.3 Perspective: Aggregated EDIT NEW REFRESH Logged in as: Charlie LOG OUT MANAGE

Threat

Sort by unmitigated risk

PostgreSQL 2015-10-08 Security Upd...
 The PostgreSQL Global Development...
 Likelihood: 1
 Total posed risk:
 C 2 I 1.33 A 2
 Remaining risk:
 C 2 I 1.33 A 2

Debian: 3381-1: openjdk-7: Summary
 Likelihood: 1
 Total posed risk:
 C 2.66 I 3.33 A 3.33
 Remaining risk:
 C 2.66 I 3.33 A 3.33

Debian: 3382-1: phpmyadmin: Summ...
 Likelihood: 1
 Total posed risk:
 C 2.66 I 3.33 A 3.33

Dell PowerEdge R410 23 3/25/16
 00:00:3e:10:52:10
 Threats: 1

Cost: 0.1
 Total potential benefit:
 C 0.77 I 0.77 A 0.77

Packages installed on asset 08:00:27:fb:88:c6

Ubuntu 14.04

accountsservice	0.6.35-0ubuntu7
adduser	3.113+nmu1ubuntu3
apparmor	2.8.95-2410-0ubuntu5
apt	1.0.1ubuntu2
apt-transport-https	1.0.1ubuntu2.6
apt-utils	1.0.1ubuntu2
apt-xapian-index	0.45ubuntu4
aptitude	0.6.8.2-1ubuntu4
aptitude-common	0.6.8.2-1ubuntu4
aufs-tools	1:3.2+20130722-1.1
base-files	7.2ubuntu5
base-passwd	3.5.33
bash	4.3-6ubuntu1
bash-completion	1:2.1-4
bind9-host	1:9.9.5.dfsg-3
binutils	2.24-5ubuntu3.1
biosevnane	0.4.1-0ubuntu6

[CLOSE](#)

localhost:8000

TFER 0.3 Perspective: Aggregated EDIT NEW REFRESH Logged in as: Charlie LOG OUT MANAGE

Threats Assets Mitigations

Sort by unmitigated risk Sort by asset name Sort by number of threats

Ubuntu: 2758-1: PHP vulnerabilities

Likelihood: 1

Total posed risk:
C 1.99 | I 1.66 | A 1.66 Total 5.33

Remaining risk:
C 1.99 | I 1.66 | A 1.66 Total 5.33

Ubuntu: 2785-1: PHP vulnerabilities

Likelihood: 1

Total posed risk:
C 1.99 | I 1.66 | A 1.66 Total 5.33

Remaining risk:
C 1.99 | I 1.66 | A 1.66 Total 5.33

Ubuntu: 2745-1: QEMU vulnerabilities

Likelihood: 1

Total posed risk:
C 1.99 | I 1.66 | A 1.66 Total 5.33

webserver

08:00:27:62:dc:80

Threats: 3

Impact: C LOW | LOW A LOW

ThinkPenguin Snares Penguin GNU / Linux No...

00:00:5e:00:52:26

Threats: 0

Impact: C LOW | LOW A LOW

Silicon Mechanics Storform iS713 SM59325 x

00:00:5e:00:52:20

Threats: 0

Impact: C HIGH | HIGH A HIGH

OS: CentOS

Silicon Mechanics Rackform iServ R335.V4 x...

00:00:5e:00:52:21

Threats: 0

Impact: C LOW | HIGH A HIGH

USN-2758-1: PHP vulnerabilities

Threats: 2

Cost: 0.1

Total potential benefit:
C 3.99 | I 3.33 | A 3.33

Remaining benefit:
C 3.99 | I 3.33 | A 3.33

USN-2786-1: PHP vulnerabilities

Threats: 2

Cost: 0.1

Total potential benefit:
C 3.99 | I 3.33 | A 3.33

Remaining benefit:
C 3.99 | I 3.33 | A 3.33

USN-2724-1: QEMU vulnerabilities

Threats: 1

Cost: 0.1

Total potential benefit:
C 0.66 | I 0.55 | A 0.55

localhost:8000

TFER 0.3 Perspective: Aggregated EDIT NEW REFRESH Logged in as: Charlie LOG OUT MANAGE

Threats Assets Mitigations

Sort by unmitigated risk Sort by asset name Sort by number of threats

Ubuntu: 2758-1: PHP vulnerabilities

Likelihood: 1

Total posed risk:
C 1.99 | I 1.66 | A 1.66 Total 5.33

Remaining risk:
C 1.66 | I 1.33 | A 1.33 Total 4.33

webserver

00:00:27:62:dc:80

Threats: 3

Impact: C LOW | LOW A LOW

ThinkPenguin Snares Penguin GNU / Linux No...

00:00:5e:00:52:26

Threats: 0

Impact: C LOW | LOW A LOW

Silicon Mechanics Storform iS713 SM59325 x

00:00:5e:00:52:20

Threats: 0

Impact: C HIGH | HIGH A HIGH

OS: CentOS

Silicon Mechanics Rackform iServ R335.V4 x...

00:00:5e:00:52:21

Threats: 0

Impact: C LOW | HIGH A HIGH

USN-2786-1: PHP vulnerabilities

Threats: 2

Cost: 0.1

Total potential benefit:
C 3.99 | 3.33 A 3.33

Remaining benefit:
C 3.33 | 2.66 A 2.66

USN-2758-1: PHP vulnerabilities

Threats: 2

Cost: 0.1

Total potential benefit:
C 3.99 | 3.33 A 3.33

Remaining benefit:
C 3.33 | 2.66 A 2.66

USN-2745-1: QEMU vulnerabilities

Threats: 1

Cost: 0.1

Total potential benefit:
C 0.66 | 0.55 A 0.55

Demonstration summary

- Automated results are ready immediately
- Multiple analysts can refine results
 - Input provided according to user capability, expertise, and availability
- Conflicting input is aggregated according to:
 - Assortment of algorithms
 - Human preference
- Result:
 - View of the threat landscape in operational context
 - Prioritization of T/A/M with high risk / pay-off

TFER is a Decision Support System

- Enumerate the threats, assets, and mitigations by automatically pulling from existing sources.
- Use automated analysis to help rank and score information, so that the most important information floats to the top.
- Use manual connections from a collection of analysts to add new links and update the scoring system.
- Allow multi-user perspectives to make cross-analyst deductions work cleanly and easily.

Uncertainty & Hard Numbers

TFER ingests data from a variety of sources, and provides automatic ranking and clustering based on some hard numbers. You saw these as some of the hard numbers in the demo.

The basis for these hard numbers is an extension of Dempster-Shafer Theory, invented as a way to reason about uncertainty when combining evidence from multiple sources.

Stay tuned for David Burke's talk tomorrow to learn more.

THANK YOU.

All trademarks, service marks, trade names, trade dress, product names and logos appearing in these slides are the property of their respective owners, including in some instances Galois, Inc.

All rights are reserved.