# galois

**TFER: Threat Fusion & Effective Response** 

Galois [gal-wah] Named after French mathematician Évariste Galois www.galois.com





![](_page_3_Picture_0.jpeg)

![](_page_4_Picture_0.jpeg)

![](_page_5_Figure_0.jpeg)

#### Project goals

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

#### DEMONSTRATION

() 1728 Decision Suggest Dy: X								Demonster
IFER 0.3	🔹 Perspe	ctive: default -	EDIT N	BW	REFRESH	Logged in as: Alice	LOG OUT	MANAGE
Threats		Asse	ets			Mitigat	ions	
Sort by unmitigated risk 👻 🛘 🕯		Sort by number of threats	-	1ª	Sort by	number of threats	÷	1±
Debias: 3396-1: linux: Summary Likelihood: 1 Total posed risk: C 2.66   3.33   A 3.33   Total 9.33 Remaining risk: C 2.66   3.33   A 3.33   Total 9.33	*	Silicon Mechanice Rackform iGer 00+00+50+00+52+1f Threats: 22 Import: C MEDUM I M OS: Uburtu Lenove ThridPad X230 PR01014	R133 SM6	2	MS15-1 Threafs Cost Total po C 1.21 Remain C 1.21	13 - Oritical: Cumulative Se 5 0.1 tential benefit: 1.21 A 1.21 ing benefit: 1.21 A 1.21	ecurity Upd	2
Debian: 3381-1: openjdk-7: Summary Likelihood: 1	2	0010015410015211a Theads: 22 Impact: C MEDUM I M OS: Ubuntu	EDIUM A MEDIUM	í	MS15-0 Threats Cost Total po	99 - Critical: Vulnerabilitier : 4 0.1 tential benefit:	a in Microso	2
C 2.66   3.33   A 3.33   Total 9.33 Remaining risk C 2.66   3.33   A 3.33   Total 9.33		Asus Exe PC 1000HE 970AA517 0010015e100152125 Threats: 7	2611	2	C 0.3 Remain C 0.3	0.3 ∧ 0.3 ingbeneft   0.3 ∧ 0.3		
Debian: 3382-1: phpmyadmin: Summary Likelihood: 1	2	Dell PowerEdge 14255C 21 2/2/0	9	2	MS15-0 Threats Cost Total po	91 - Critical: Cumulative Se . 4 0.1 tential benefit:	rcurity Upd	2

C 17EE Deckler Support Sy: X					Demonstrat
TFER 0.3	• Perspective:	default = EDIT	NEW	REFRESH Logged in as: Alice LOG OUT	MANAGE
Threats		Assets		Mitigations	
Sort by unmitigated risk 🛛 🗸 🕴	Sort b	y number of threats	- I <u>*</u>	Sort by number of threats	1±
Ubuntu: 2745-1: QEMU vulnerabilities Likelihood: 1 Total posed risk: 1.66 1 A 1 7000 2.66 Remaining risk: 1.66 1 6 1 Remaining risk:		Lenovo Think/Pad X230 PK0T014 2016 015e10015211a Hz 22 05 HIGH LOW LOW Uburn:	· }	05A-3381 openjdik-7       Threats:     2       Cost:     0.1       Total potential benefit:     7       C     7     7.66       Remaining benefit:     7       C     7     7.66       Remaining benefit:     7	2
Libuntu: 2806-1: Linux kernel (Vivid HWE)	0010 Three impa 05:	015es00152x25 da: 7 ct: CLOW ILOW ∧ LOW Windows	í	USN-2786-1: PHP vulnerabilities Threats: 2 Cost: 0.1 Total potential benefit:	2
Total posed trail:         1         4         1         Total 3.66           Memaining risk:         1         4         1         Total 3.66           C         1.66         1         4         1         Total 3.66	Dell I     Original     Three     Impa	*owerEdge 14255C 21 2/2/09 015e100152188 MS: 4 ct: C LOW I HIGH A HIGH	2	C 3.33 2 A 2 Remaining banafit: C 3.33 2 A 2	
Ubuntu: 2754-1: Thunderbird vulnerabiliti Ukelhood 1 Total posef rink:	• 05: • Peng	Debian uin Computing Relian 26005A P12370	H. >	Cost: 0.1 Total potential benefit:	1

FER 0.3	Perspective: default EDIT NEW	REFRESH Logged in as: Alice LOG OUT	MANAGI
Threats	Assets	Mitigations	
iort by threat name — I	Sort by asset name 👻 🖡	Sort by number of threats *	1ª
PostgreSQL 2015-10-08 Security Update The PostgreSQL Clobal Clevelopment Cloup N.: Likelihood: 1 Total posed risk: C 1 1 6 1 Total 3 Remaining risk:	Dell PowerEdge R410 23 3/26/16 00+00+50+00+52+10 Threats 1 Impact 0 H0H   H0H A H0H 05: Cent05	MS15-113 - Critical: Cumulative Security Upd Threats: 5 Cost: 0.1 Total potential benefit: C 1.21   1.21   1.21 Remaining benefit: C 1.21   1.21   1.21	
2862152 - Valnerability in DirectAccess and I Valnerability in DirectAccess and IPsec Could Likelihood: 1	Dell PowerVault 122T LTO 24 4/15/07     00:00:50:00:52:11     Threats: 0     Impact: 0 MEDIUM   MEDIUM A MEDIUM     OS: CentOS	MS15-107 - Important: Cumulative Security U Threats: 4 Cost: 0.1 Total potential benefit:	
C 0.33         I 0.33         A 0.33         Total 1           Remaining risk:         C 0.33         I 0.33         A 0.33         Total 1	Dell PowerVault 124T LTO-3 25 9/19/12 00:00:50:00:52:12 Threats: 0	C 0.3   0.3 A 0.3 Remaining benefit: C 0.3   0.3 A 0.3	
2896666 - Vulnersbillty in Microsoft Graphics Vulnersbillty in Microsoft Graphics Componen	OS: CentOS	MS15-099 - Critical: Vulnerabilities in Microso Threats: 4 Cost: 0.1 Total potential benefit:	
Total posed risk	<ul> <li>Lenovo ThinkPad X230 PK0T014 2016 09-??</li> </ul>	C 03   03 A 03	

→ C 🗋 localhost:8000		<u>\$</u>
IFER 0.3	Perspective: default EDIT NEW REFRESH	Logged in as: Bob LOG OUT MANAGE
Threats	Assets	Mitigations
Sort by threat name $ I_A^{\tt Z}$	Sort by number of threats - In Sort by n	nitigation name $ \mathbf{I}_{A}^{Z}$
PostgreSQL 2015-10-08 Security Update The PostgreSQL 2015-10-08 Security Update Likelihood: 1 Total posed risk: 0 0 0 A 0 Total 0 Remaining risk: 0 0 0 A 0 Total 0	Silicon Mechanics Rackform iServ R133 SM6	12772-1: PostgreSQL vulnerabilities
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	Concolor:Secolor:S2:1a     Threats: 22     Impact: C MEDIUM   MEDIUM A MEDIUM     Cost:     Ubuntu     Cost:     Ubuntu     Cost:     Total pol     Co     Asus Eee PC 1000HE 970AAS172611     Onion:Secolor:S2:25     Threats: 7	73-1: Linux kernel vulnerabilities 0.1 tential benefit: 10 ∧ 0 ng benefit: 10 ∧ 0
2896666 - Vulnerability in Microsoft Graphics Vulnerability in Microsoft Graphics Componen Likelihood: 1 Total posed risk:	Impact:         C LOW   LOW   A LOW         USN-277           0S:         Windows         USN-277           •         Dell PowerEdge 1425SC 21 2/2/09         Total pot           •         00:00:5e:00:52:08         C 0	V4-1: Linux kernel (OMAP4) vulnerabiL 0 0.1 tential benefit: 1.0

→ C C localhost:8000					승 =
TFER 0.3	Perspective	C default EDIT	NEW REFRES	H Logged in as: Charlie LOG OUT	MANAGE
Threats		Assets		Mitigations	
Sort by unmitigated risk - Debian: 3381-1: openjdk-7: Summary Likelhood: 1 Total posed risk: C 2.66   3.33   A 3.33   Tot Remaining risk: C 2.66   3.33   A 3.33   Tot Debian: 3382-1: phpmyadmin: Summ	Create and switt Perspective name: Aggregat Available perspect Alice (1) default Bob (1) default Charlie (1) default	tch to a new perspective		15. ** Mative Security Upd 21 21 21 21	
Likelihood 1 Total posed risk: 0.2.66   3.33 A 3.33 Tot Remaining risk: 0.2.66   3.33 A 3.33 Totan 9.33	CANCEL	0100150100152120 hreats: 3		CREATE 3	
Debian: 3367-1: wireshark: Summary Likelihood: 1 Total posed risk:		ppece: C LOW I LOW A LOW IS: Android pple iPad 16GB DMPN8214FK14	>	MS15-091 - Critical: Cumulative Security Upd           Threats:         4           Cost:         0.1           Total potential benefit:         C           C         0.77         ♦ 0.77	

C C localhost:8000							5
FER 0.3	<ul> <li>Perspective:</li> </ul>	Aggregated	EDIT	NEW	RĐ	RESH Logged in as: Charlie LOG OL	JT MANAG
Threats		A	ssets			Mitigations	\$
Fort by unmitigated risk $\neg$ $I_z^A$	Sor	t by asset name		1	Z A	Sort by number of threats	- Iž
PostgreSQL 2015-10-08 Security Update Rele The PostgreSQL Clobes Onvelopment Crosp N Likelihood: 1 Total posed risk: C 1 1 A 1 Total 3 Remaining risk: C 1 1 A 1 Total 3		II PowerEdge R410 23 3 1100150100152110 reats 1 pact 0.1801 5 Cent05	1/25/16 HIGH A HIGH			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	
Debian: 3381-1: openjdk-7: Summary Likelihood: 1	000 100 100 100 100 100 100 100	Il PowerVault 122T LTO 1:00:5e:00:52:11 reats: 0 pact: C MEDIUN 2: CentOS	24 4/15/07	NEDIUM	-	MS15-113 - Critical: Cumulative Security Up Threats: 5 Cost: 0.1 Total potential benefit:	xi
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	0 00	II PowerVault 124T LTO	-3 25 9/19/12		2	C 1.21 ↓ 1.21 Å 1.21 Remaining benefit: C 1.21 ↓ 1.21 Å 1.21	
Debian: 3367-1: wireshark: Summary	) Im	pact: C MEDIUN CentOS	A I MEDIUM A N	NEDIUM		MS15-107 - Important: Cumulative Security Threats: 4	
Likelihood: 1 Total posed risk:	* La	novo ThinkPad X230 PK 10015e10015211a	(0T014 2016 09-??		2	Con: 0.1 Total potential benefit: C 0.3   0.3 ∧ 0.3	÷

FER 0.3	Perspective: J	Aggregated EDIT NEW REFRESH	Logged in as: Charlie LOG OUT MANAGE
Threat	Packages installed or	n asset 08:00:27:fb:88:c6	gations
iort by unmitigated risk 🔹	Ubuntu 14.04		.s <b>⊸ l</b> <u>A</u>
PostgreSQL 2015-10-08 Security Up: The PostgreSQL Global Devel	accountsservice adduser apparmor	0.6.35=0ubuntu7 3.113+nmu3ubuntu3 2.8.95=2430=0ubuntu5	vulnerabilities 2
Likelihood: 1 Total posed risk: C 2 I 1.33 A 2 Tot	apt apt=transport=https apt=utils	1.0.1ubuntu2 1.0.1ubuntu2.6 1.0.3ubuntu2	-
Remaining risk: C 2 I 1.33 A 2 To	apt-xapian-index aptitude aptitude-common	0.45ubuntu4 0.6.8.2-lubuntu4 0.6.8.2-lubuntu4	_
Debian: 3381-1: openjdk-7: Summary	aufs-tools base-files base-passwd	1:3:2*20130722-1:1 7:20buntu5 3:5:33	dative Security Upd
Likelihood: 1 Total posed risk: © 2.66   3.33 A 3.33 Tot	bash-completion bind9-host	4.3+60000001 1:2.1=4 1:9.5.dfsg=3	21
Remaining risk: C 2.66 I 3.33 A 3.33 Tor	blosdevname	0.4.1=0ubuntu6	21
Debian: 3382-1: phpmysdmin: Summ	CLOSE		dative Security Upd

→ C localhost 8000					<u></u>
TFER 0.3	Perspective: Aggregated	EDIT NEW	r REFI	ESH Logged in as: Charlie LO	G OUT MANAGE
Threats	A	ssets		Mitigation	ns
Sort by unmitigated risk $\neg$ $l_z^A$	Sort by asset name	*	1ª	Sort by number of threats	$ l_z^A$
Ubuntu: 2758-1: PHP vulnerabilities Likelihood: 1 Total posed risk: 0.1.99 1.66 1.66 Total 5.23	webserver 08+00+27+62+do+80 Threats: 3 Impact:   LOW	LOW A LOW	2	USN-2758-1: PHP vulnerabilities Threats: 2 Cost: 0.1 Total potential benefit: C 3.99   3.33 / 3.33	2
Remaining risk: C 1.99 I 1.66 A 1.66 Total 5.33 Ubuntu: 2786-1: PHP vulnerabilities	ThinkPenguin Snares Pan     0010015+100152126     Threats: 0     Impact: C LOW 1	guin GNU / Linux No	2	Remaining benefit: C 3.99 I 3.33 A 3.33 USN-2786-1: PHP vulnerabilities Threats: 2	2
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	Silicon Mechanics Storfor     00+00150+00+52+20     Threats: 0     Impact: C HIGH     OS: CentOS	m (5713 SM59325 x HIGH A HIGH	2	Cost: 0.1 Total potential benefit: C 3.99   3.33   A 3.33 Remaining benefit: C 3.99   3.33   A 3.33	:
Ubuntu: 2745-1: QEMU vulnerabilities Likelihood: 1 Total posed risk:	Silicon Mechanics Rackfor OC:00:56:00:52:21 Threats: 0 Impact: C LOW	rm iServ R335.V4 x	2	USN-2724-1: QEMU vulnerabilities Threats: 1 Cost: 0.1 Total potential benefit: C 0.66   0.55   0.55	2

→ C i localhost:8000		
rfer 0.3 🔹	Perspective: Aggregated EDIT NEW REFRESH Logged in as: Charlie LOG OUT	MANAGE
Threats	Assets Mitigations	
Sort by unmitigated risk $\neg$ $I_z^A$	Sort by asset name v 12 Sort by number of threats v	I≜
Ubunts: 2758-1: PHP vulnerabilities Likelihood: 1 Total posed risk: C 1.99 1.66 4.1.66 Total 5.32	webserver     08x00x27x62x60x80       Threats:     3       Impact:     0 LOW    LOW    LOW	2
Remaining rick: C 1.66 I 1.33 A 1.33 Total 4.33 Ubuntu: 2745-1: QEMU vulnerabilities	ThinkPenguin Snares Penguin GNU / Linux No     Oct-00159126     Threats: 0     Impact: C LOW I LOW & LOW     USN-2758-1: PHP vulnerabilities     Threats: 2	2
Likelihood: 1 Total posed risk: 0 1.99 II.66 A 1.66 Total 5.33 Remaining risk: 0 1.66 II.33 A 1.33 Total 4.33	Silicon Mechanics Storform iS713 SM59325 x:         Silicon Mechanicon Silicon Mechanics Storform iS713 SM59325 x:	
Ubuntu: 2786-1: PHP vulnerabilities Likelihood: 1 Total posed risk:	Silicon Mechanics Rackform iServ R335.V4 x         USN-2745-1: QEMU vulnerabilities           00:00:5e:00:52:21         Threats:         1           Threats:         0         0.1           Threats:         0         0.1           Impact:         C LOW   HIGH   A HIGH         C 0.66   0.55   A 0.55	2

#### **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 crossanalyst 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.