April 2016

Nabble

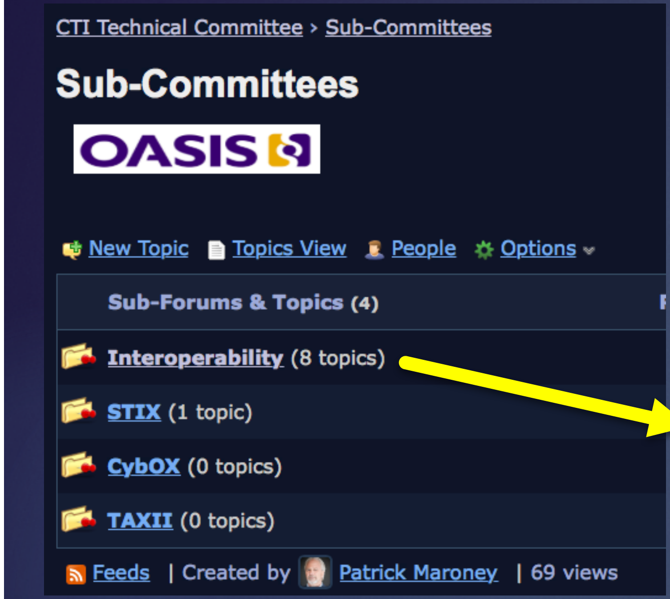
IMPROVING COLLABORATION PROCESSES

Patrick Maroney - CTI TC Interoperability SC

Collaboration Improvements

- Structured Hierarchical Content.
- Granular & flexible subscription/notification options.
- Content organized by specific interest areas.
- Content organized by content types specific to interest areas.
- Move/reorganize content (Topics, Sub-Topics Folders, Subfolders)
- Easily follow all voices in a given conversation over any period of time.
- Reply in sequence to any conversation/posting, at any point in time.
- Edit/revise content.
- Flexible viewing options.
- Post rich content to existing topics/sub-topics via Email.
- Create new topics in any folder/sub-folder via Email.

Structured Hierarchical Content



CTI Technical Committee › Sub-Committees

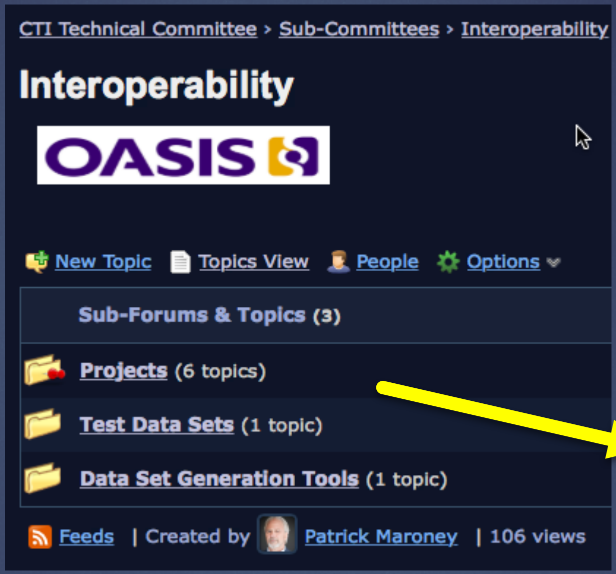
Sub-Committees

New Topic | Topics View | People | Options

Sub-Forums & Topics (4)

- **Interoperability** (8 topics)
- **STIX** (1 topic)
- **CybOX** (0 topics)
- **TAXII** (0 topics)

Feeds | Created by Patrick Maroney | 69 views



CTI Technical Committee › Sub-Committees › Interoperability

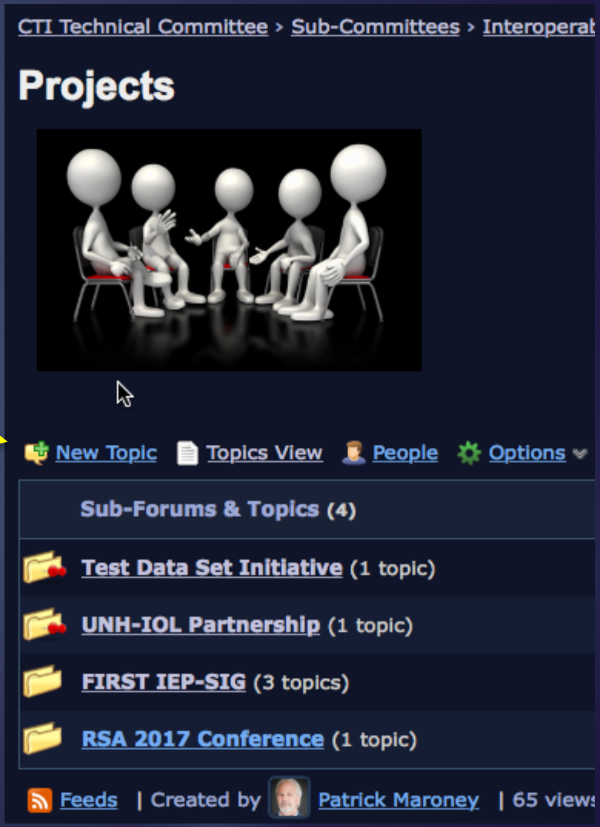
Interoperability

New Topic | Topics View | People | Options

Sub-Forums & Topics (3)

- **Projects** (6 topics)
- **Test Data Sets** (1 topic)
- **Data Set Generation Tools** (1 topic)

Feeds | Created by Patrick Maroney | 106 views



CTI Technical Committee › Sub-Committees › Interoperat

Projects

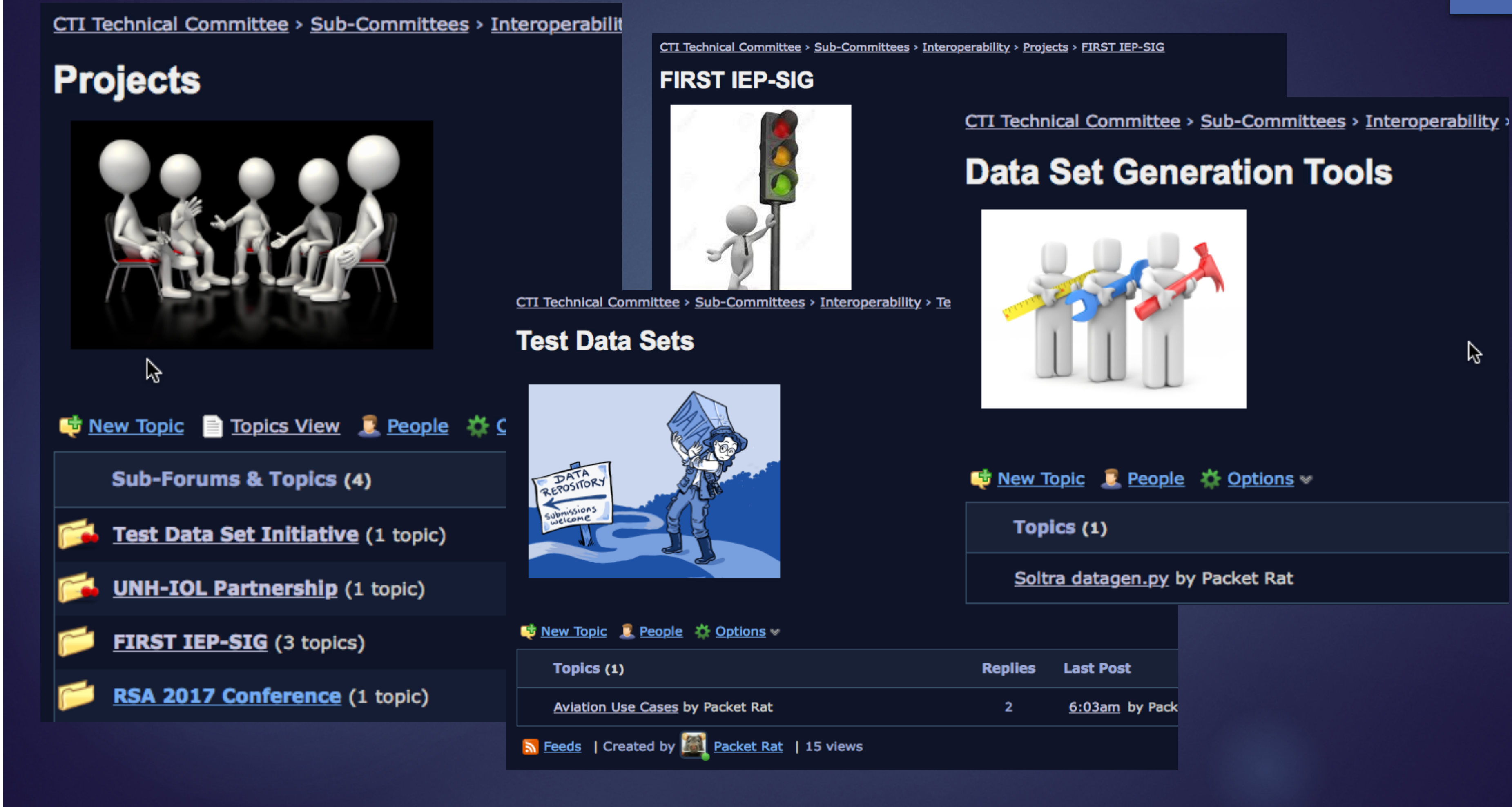
New Topic | Topics View | People | Options

Sub-Forums & Topics (4)

- **Test Data Set Initiative** (1 topic)
- **UNH-IOL Partnership** (1 topic)
- **FIRST IEP-SIG** (3 topics)
- **RSA 2017 Conference** (1 topic)

Feeds | Created by Patrick Maroney | 65 views

Content Organized by Specific Interest Areas



CTI Technical Committee › Sub-Committees › Interoperabilit

Projects

New Topic | Topics View | People | C

Sub-Forums & Topics (4)

- Test Data Set Initiative (1 topic)
- UNH-IOL Partnership (1 topic)
- FIRST IEP-SIG (3 topics)
- RSA 2017 Conference (1 topic)

CTI Technical Committee › Sub-Committees › Interoperability › Projects › FIRST IEP-SIG

FIRST IEP-SIG

CTI Technical Committee › Sub-Committees › Interoperability ›

Data Set Generation Tools

New Topic | People | Options

Topics (1)

Soltra datagen.py by Packet Rat

CTI Technical Committee › Sub-Committees › Interoperability › Te

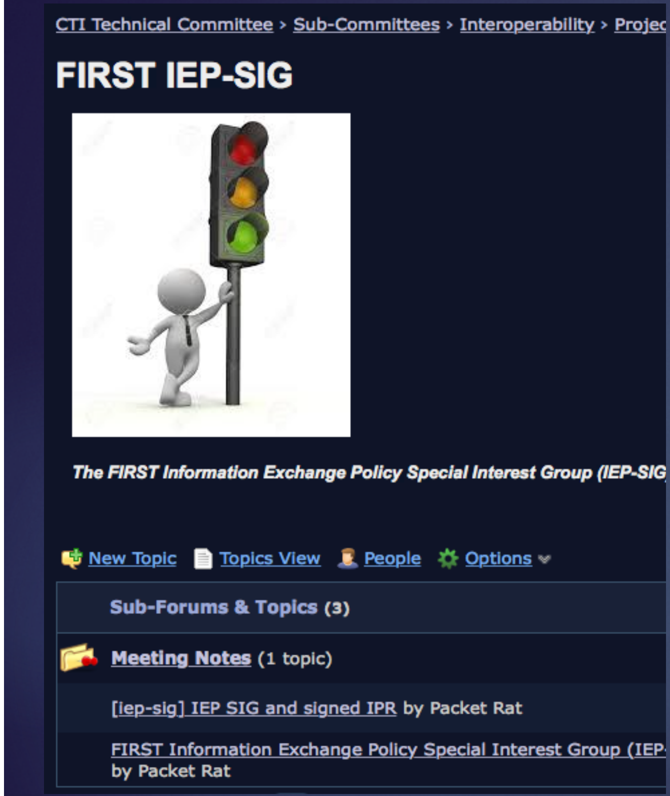
Test Data Sets

New Topic | People | Options

Topics (1)	Replies	Last Post
Aviation Use Cases by Packet Rat	2	6:03am by Pack

Feeds | Created by Packet Rat | 15 views

Further Organization of Content Types specific to Interest Areas



CTI Technical Committee > Sub-Committees > Interoperability > Projec

FIRST IEP-SIG

The FIRST Information Exchange Policy Special Interest Group (IEP-SIG

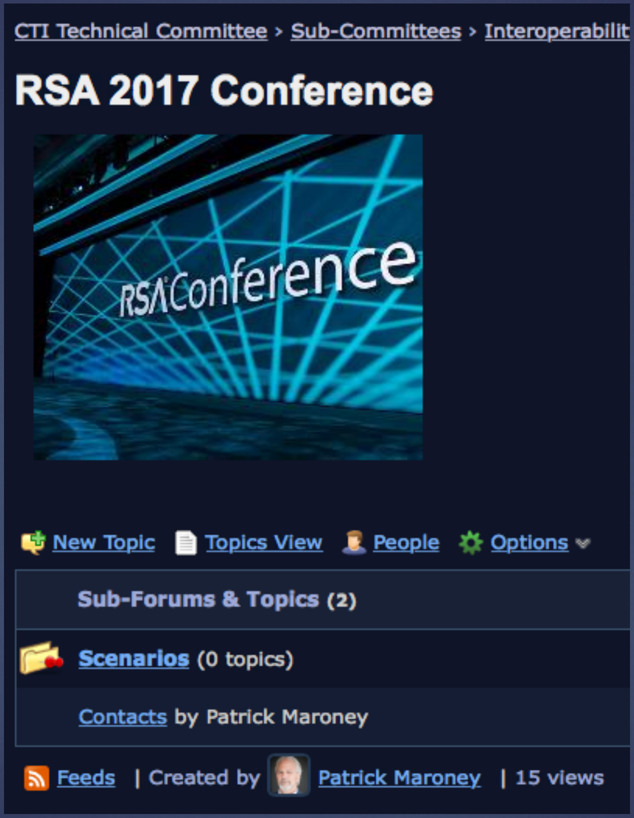
New Topic | Topics View | People | Options

Sub-Forums & Topics (3)

Meeting Notes (1 topic)

[iep-sig] IEP SIG and signed IPR by Packet Rat

FIRST Information Exchange Policy Special Interest Group (IEP-
by Packet Rat



CTI Technical Committee > Sub-Committees > Interoperabilit

RSA 2017 Conference

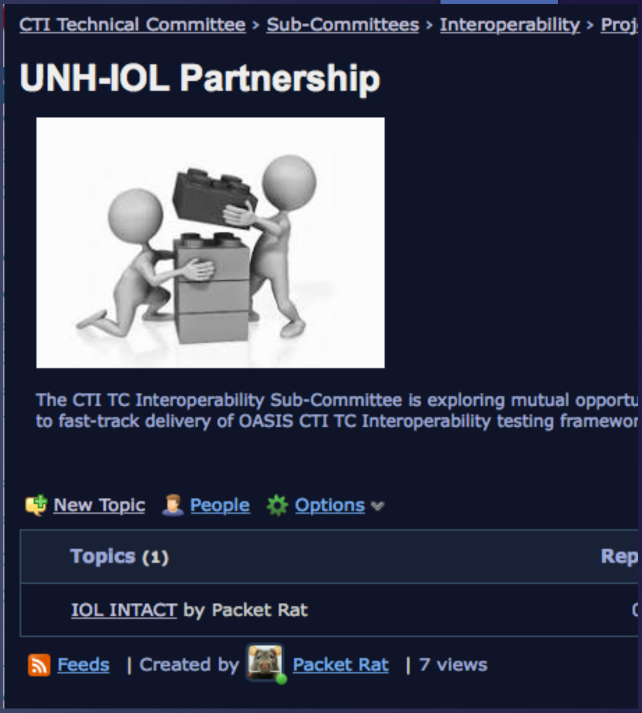
New Topic | Topics View | People | Options

Sub-Forums & Topics (2)

Scenarios (0 topics)

Contacts by Patrick Maroney

Feeds | Created by Patrick Maroney | 15 views



CTI Technical Committee > Sub-Committees > Interoperability > Proj

UNH-IOL Partnership

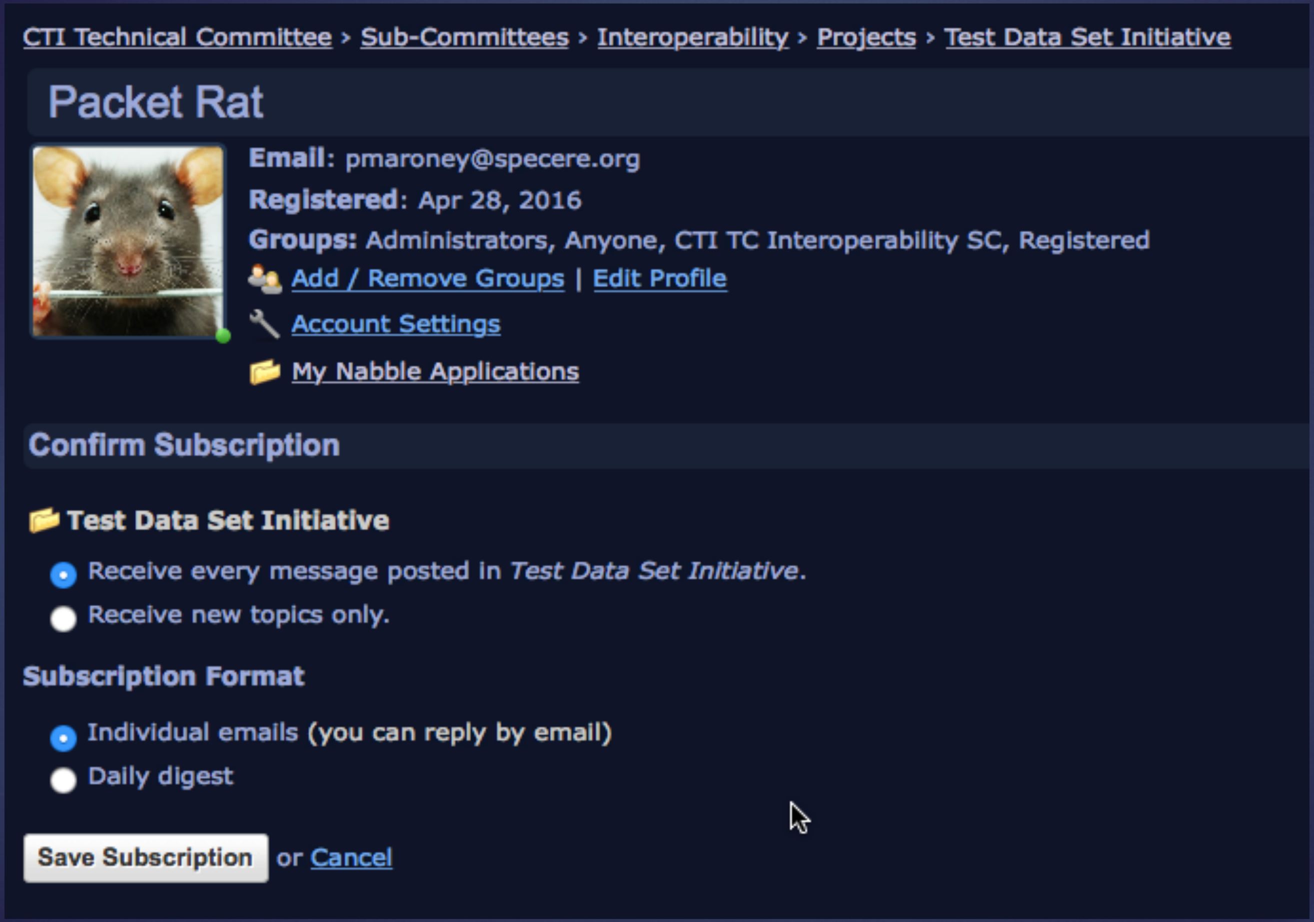
The CTI TC Interoperability Sub-Committee is exploring mutual opportu
to fast-track delivery of OASIS CTI TC Interoperability testing framewor

New Topic | People | Options

Topics (1)	**Rep**
IOL INTACT by Packet Rat	(

Feeds | Created by Packet Rat | 7 views

Granular & Flexible Subscription Options



CTI Technical Committee > Sub-Committees > Interoperability > Projects > Test Data Set Initiative

Packet Rat

Email: pmaroney@specere.org

Registered: Apr 28, 2016

Groups: Administrators, Anyone, CTI TC Interoperability SC, Registered

Add / Remove Groups | Edit Profile

Account Settings

My Nabble Applications

Confirm Subscription

Test Data Set Initiative

● Receive every message posted in *Test Data Set Initiative*.

○ Receive new topics only.

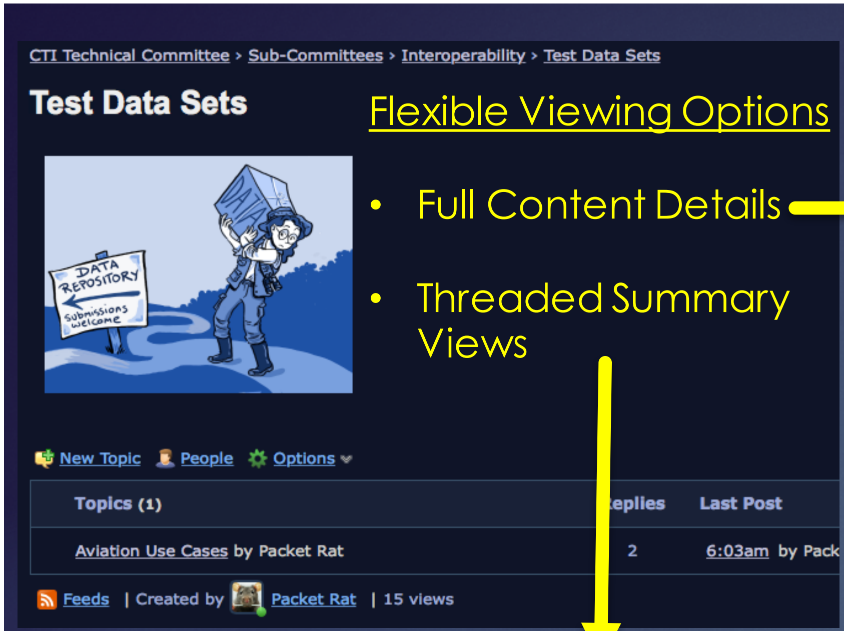
Subscription Format

● Individual emails (you can reply by email)

○ Daily digest

Flexible Viewing Options

- Full Content Details
- Threaded Summary Views



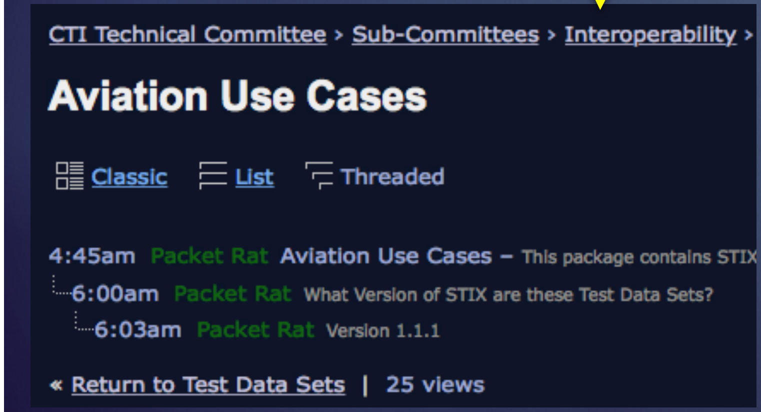
CTI Technical Committee › Sub-Committees › Interoperability › Test Data Sets

Test Data Sets

New Topic People Options

Topics (1)	eplies	Last Post
Aviation Use Cases by Packet Rat	2	6:03am by Pack

Feeds | Created by Packet Rat | 15 views



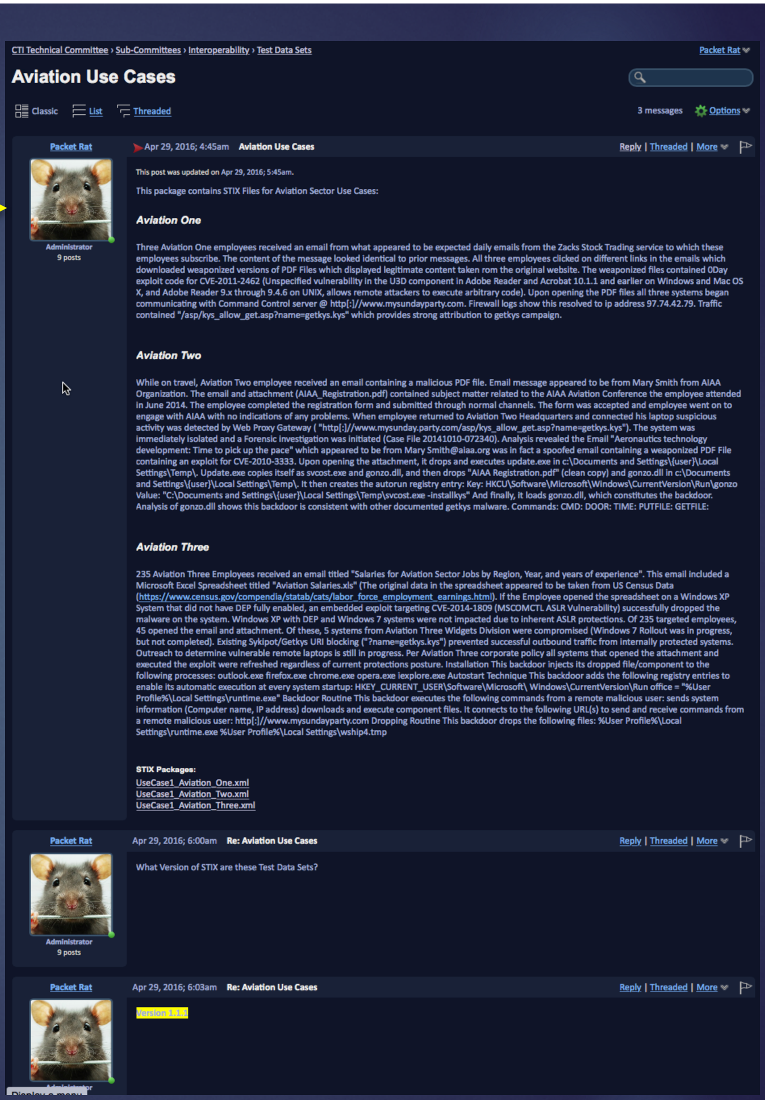
CTI Technical Committee › Sub-Committees › Interoperability ›

Aviation Use Cases

Classic List Threaded

4:45am Packet Rat Aviation Use Cases – This package contains STIX
6:00am Packet Rat What Version of STIX are these Test Data Sets?
6:03am Packet Rat Version 1.1.1

« Return to Test Data Sets | 25 views



CTI Technical Committee › Sub-Committees › Interoperability › Test Data Sets

Packet Rat

Aviation Use Cases

Classic List Threaded

3 messages Options

Packet Rat
Administrator
9 posts

Apr 29, 2016; 4:45am **Aviation Use Cases** Reply | Threaded | More

This post was updated on Apr 29, 2016; 5:45am.

This package contains STIX Files for Aviation Sector Use Cases:

Aviation One

Three Aviation One employees received an email from what appeared to be expected daily emails from the Zacks Stock Trading service to which these employees subscribe. The content of the message looked identical to prior messages. All three employees clicked on different links in the emails which downloaded weaponized versions of PDF Files which displayed legitimate content taken rom the original website. The weaponized files contained 0Day exploit code for CVE-2011-2462 (Unspecified vulnerability in the U3D component in Adobe Reader and Acrobat 10.1.1 and earlier on Windows and Mac OS X, and Adobe Reader 9.x through 9.4.6 on UNIX, allows remote attackers to execute arbitrary code). Upon opening the PDF files all three systems began communicating with Command Control server @ http[:]//www.mysundayparty.com. Firewall logs show this resolved to ip address 97.74.42.79. Traffic contained "/asp/kys_allow_get.asp?name=getkys.kys" which provides strong attribution to getkys campaign.

Aviation Two

While on travel, Aviation Two employee received an email containing a malicious PDF file. Email message appeared to be from Mary Smith from AIAA Organization. The email and attachment (AIAA_Registration.pdf) contained subject matter related to the AIAA Aviation Conference the employee attended in June 2014. The employee completed the registration form and submitted through normal channels. The form was accepted and employee went on to engage with AIAA with no indications of any problems. When employee returned to Aviation Two Headquarters and connected his laptop suspicious activity was detected by Web Proxy Gateway ("http[:]//www.mysunday.party.com/asp/kys_allow_get.asp?name=getkys.kys"). The system was immediately isolated and a Forensic investigation was initiated (Case File 20141010-072340). Analysis revealed the Email "Aeronautics technology development: Time to pick up the pace" which appeared to be from Mary Smith@aiaa.org was in fact a spoofed email containing a weaponized PDF File containing an exploit for CVE-2010-3333. Upon opening the attachment, it drops and executes update.exe in c:\Documents and Settings\{user}\Local Settings\Temp\. Update.exe copies itself as svcost.exe and gonzo.dll, and then drops "AIAA Registration.pdf" (clean copy) and gonzo.dll in c:\Documents and Settings\{user}\Local Settings\Temp\. It then creates the autorun registry entry: Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\gonzo Value: "C:\Documents and Settings\{user}\Local Settings\Temp\svcost.exe -installkys" And finally, it loads gonzo.dll, which constitutes the backdoor. Analysis of gonzo.dll shows this backdoor is consistent with other documented getkys malware. Commands: CMD: DOOR: TIME: PUTFILE: GETFILE:

Aviation Three

235 Aviation Three Employees received an email titled "Salaries for Aviation Sector Jobs by Region, Year, and years of experience". This email included a Microsoft Excel Spreadsheet titled "Aviation Salaries.xls" (The original data in the spreadsheet appeared to be taken from US Census Data (https://www.census.gov/compendia/statab/cats/labor_force_employment_earnings.html). If the Employee opened the spreadsheet on a Windows XP System that did not have DEP fully enabled, an embedded exploit targeting CVE-2014-1809 (MSCOMCTL ASLR Vulnerability) successfully dropped the malware on the system. Windows XP with DEP and Windows 7 systems were not impacted due to inherent ASLR protections. Of 235 targeted employees, 45 opened the email and attachment. Of these, 5 systems from Aviation Three Widgets Division were compromised (Windows 7 Rollout was in progress, but not completed). Existing Sykipot/Getkys URI blocking ("?name=getkys.kys") prevented successful outbound traffic from internally protected systems. Outreach to determine vulnerable remote laptops is still in progress. Per Aviation Three corporate policy all systems that opened the attachment and executed the exploit were refreshed regardless of current protections posture. Installation This backdoor injects its dropped file/component to the following processes: outlook.exe firefox.exe chrome.exe opera.exe iexplore.exe Autostart Technique This backdoor adds the following registry entries to enable its automatic execution at every system startup: HKEY_CURRENT_USER\Software\Microsoft\ Windows\CurrentVersion\Run office = "%User Profile%\Local Settings\runtime.exe" Backdoor Routine This backdoor executes the following commands from a remote malicious user: sends system information (Computer name, IP address) downloads and execute component files. It connects to the following URL(s) to send and receive commands from a remote malicious user: http[:]//www.mysundayparty.com Dropping Routine This backdoor drops the following files: %User Profile%\Local Settings\runtime.exe %User Profile%\Local Settings\wship4.tmp

STIX Packages:
UseCase1_Aviation_One.xml
UseCase1_Aviation_Two.xml
UseCase1_Aviation_Three.xml

Packet Rat
Administrator
9 posts

Apr 29, 2016; 6:00am **Re: Aviation Use Cases** Reply | Threaded | More

What Version of STIX are these Test Data Sets?

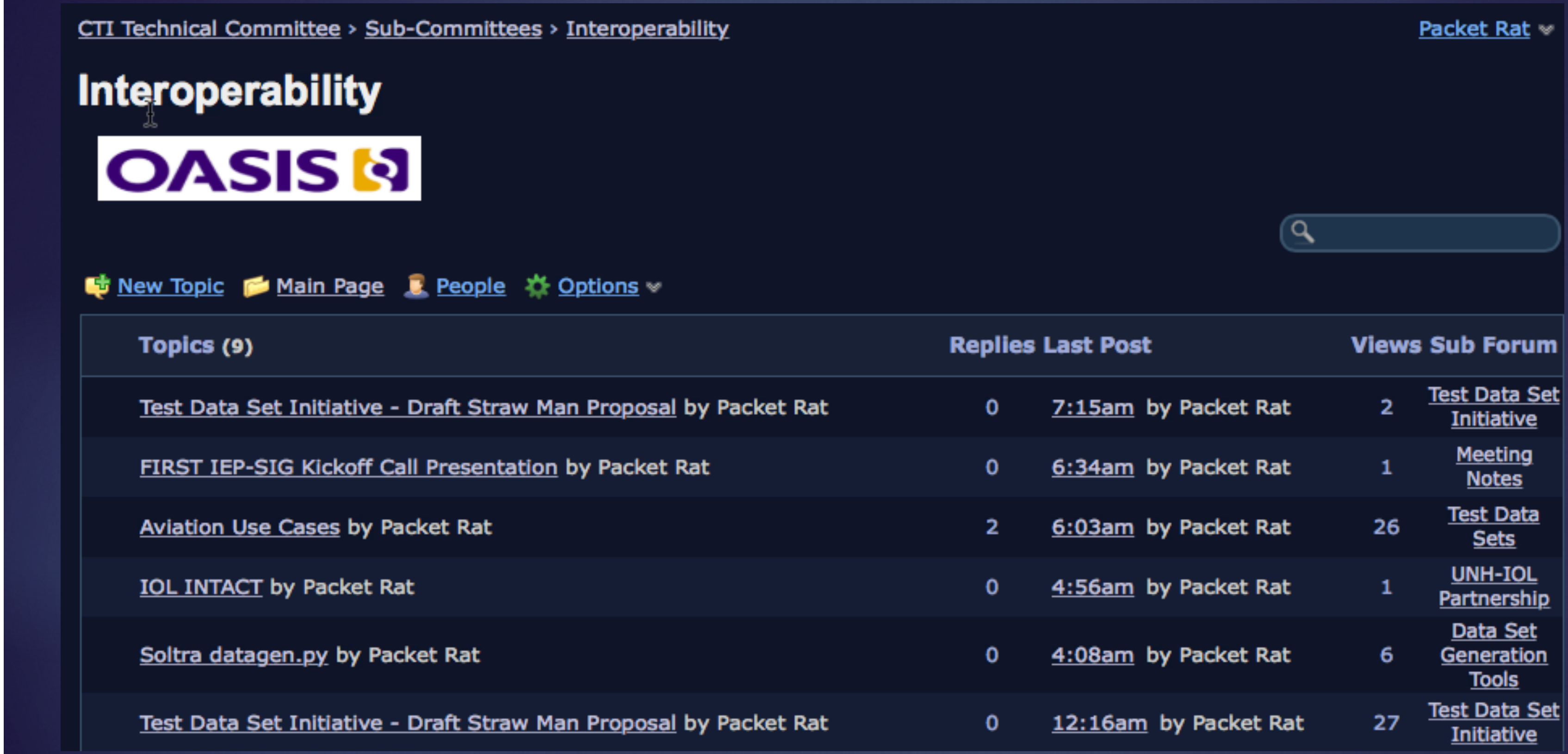
Packet Rat
Administrator

Apr 29, 2016; 6:03am **Re: Aviation Use Cases** Reply | Threaded | More

Version 1.1.1

Flexible Viewing Options: Flat View by most recent update

(from any point in hierarchy)



CTI Technical Committee › Sub-Committees › Interoperability

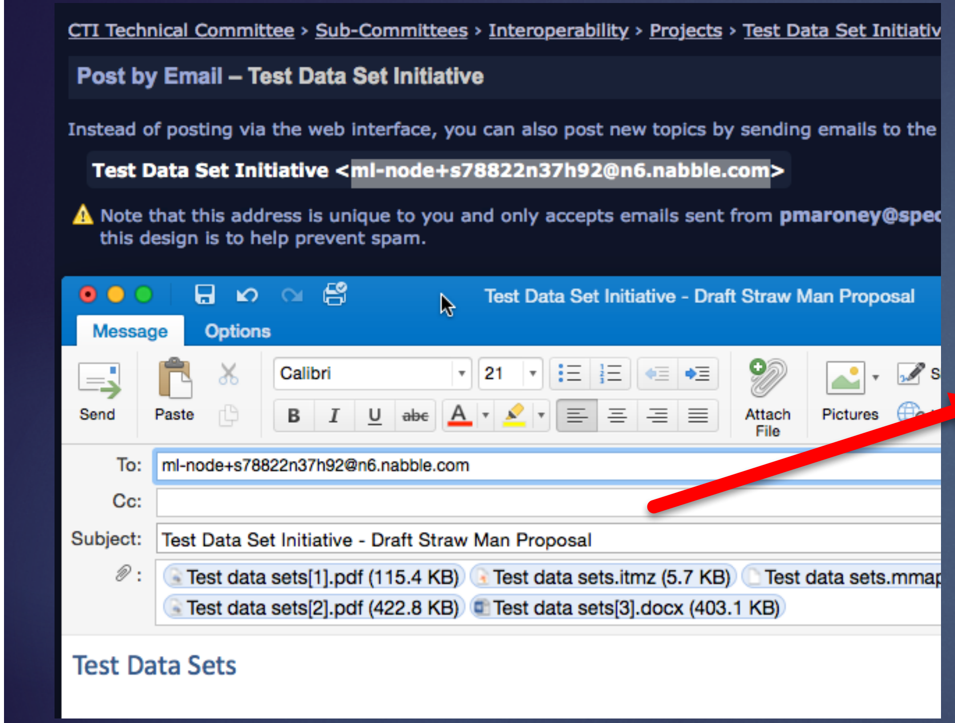
Packet Rat

Interoperability

New Topic Main Page People Options

Topics (9)	Replies	Last Post	Views	Sub Forum
Test Data Set Initiative - Draft Straw Man Proposal by Packet Rat	0	7:15am by Packet Rat	2	Test Data Set Initiative
FIRST IEP-SIG Kickoff Call Presentation by Packet Rat	0	6:34am by Packet Rat	1	Meeting Notes
Aviation Use Cases by Packet Rat	2	6:03am by Packet Rat	26	Test Data Sets
IOL INTACT by Packet Rat	0	4:56am by Packet Rat	1	UNH-IOL Partnership
Soltra datagen.py by Packet Rat	0	4:08am by Packet Rat	6	Data Set Generation Tools
Test Data Set Initiative - Draft Straw Man Proposal by Packet Rat	0	12:16am by Packet Rat	27	Test Data Set Initiative

Create or respond to topics in any folder/sub-folder via Email



CTI Technical Committee › Sub-Committees › Interoperability › Projects › Test Data Set Initiativ

Post by Email – Test Data Set Initiative

Instead of posting via the web interface, you can also post new topics by sending emails to the

Test Data Set Initiative <ml-node+s78822n37h92@n6.nabble.com>

⚠ Note that this address is unique to you and only accepts emails sent from **pmaroney@spec**
this design is to help prevent spam.

Test Data Set Initiative - Draft Straw Man Proposal

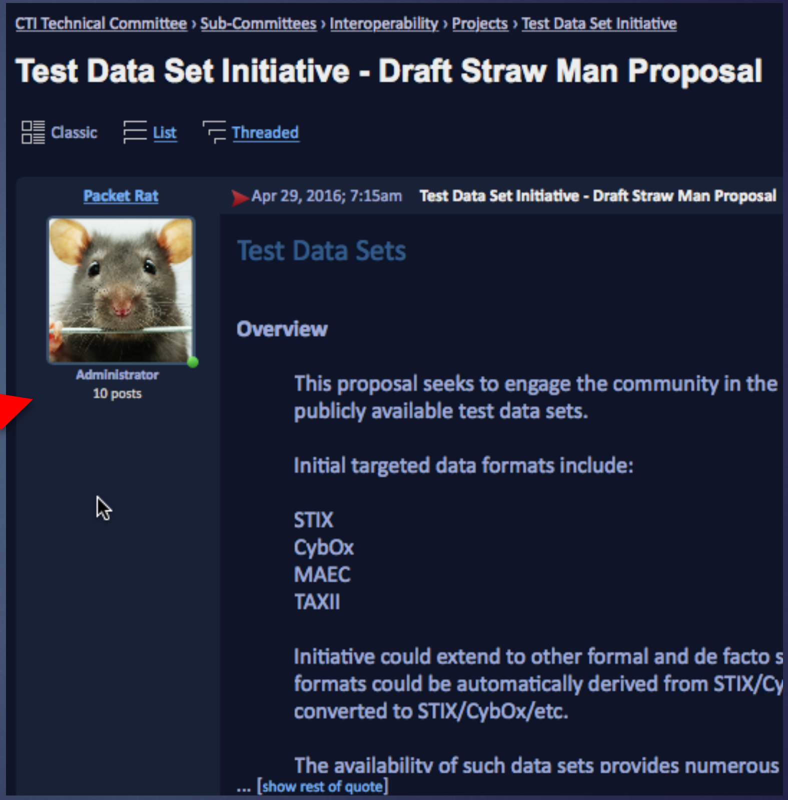
To: ml-node+s78822n37h92@n6.nabble.com

Cc:

Subject: Test Data Set Initiative - Draft Straw Man Proposal

Test data sets[1].pdf (115.4 KB) Test data sets.itmz (5.7 KB) Test data sets.mmap
Test data sets[2].pdf (422.8 KB) Test data sets[3].docx (403.1 KB)

Test Data Sets



CTI Technical Committee › Sub-Committees › Interoperability › Projects › Test Data Set Initiative

Test Data Set Initiative - Draft Straw Man Proposal

Packet Rat

Administrator
10 posts

Apr 29, 2016; 7:15am **Test Data Set Initiative - Draft Straw Man Proposal**

Test Data Sets

Overview

This proposal seeks to engage the community in the
publicly available test data sets.

Initial targeted data formats include:

STIX
CybOx
MAEC
TAXII

Initiative could extend to other formal and de facto s
formats could be automatically derived from STIX/Cy
converted to STIX/CybOx/etc.

The availability of such data sets provides numerous
... [show rest of quote]