SOFTWARE ASSURANCE MARKETPLACE

A NATIONAL CYBERSECURITY RESOURCE

Making Condor Safer with…

A Collaborative Marketplace for Continuous Software Assurance

Brooklin Gore, Chief Operations Officer

info@cosalab.org

http://swamp.cosalab.org

U.S. Department of Homeland Security
Science and Technology Directorate

- Software Assurance Marketplace project part of $70+ million multi-year Cyber Security Division effort to improve security of nation's critical information infrastructure

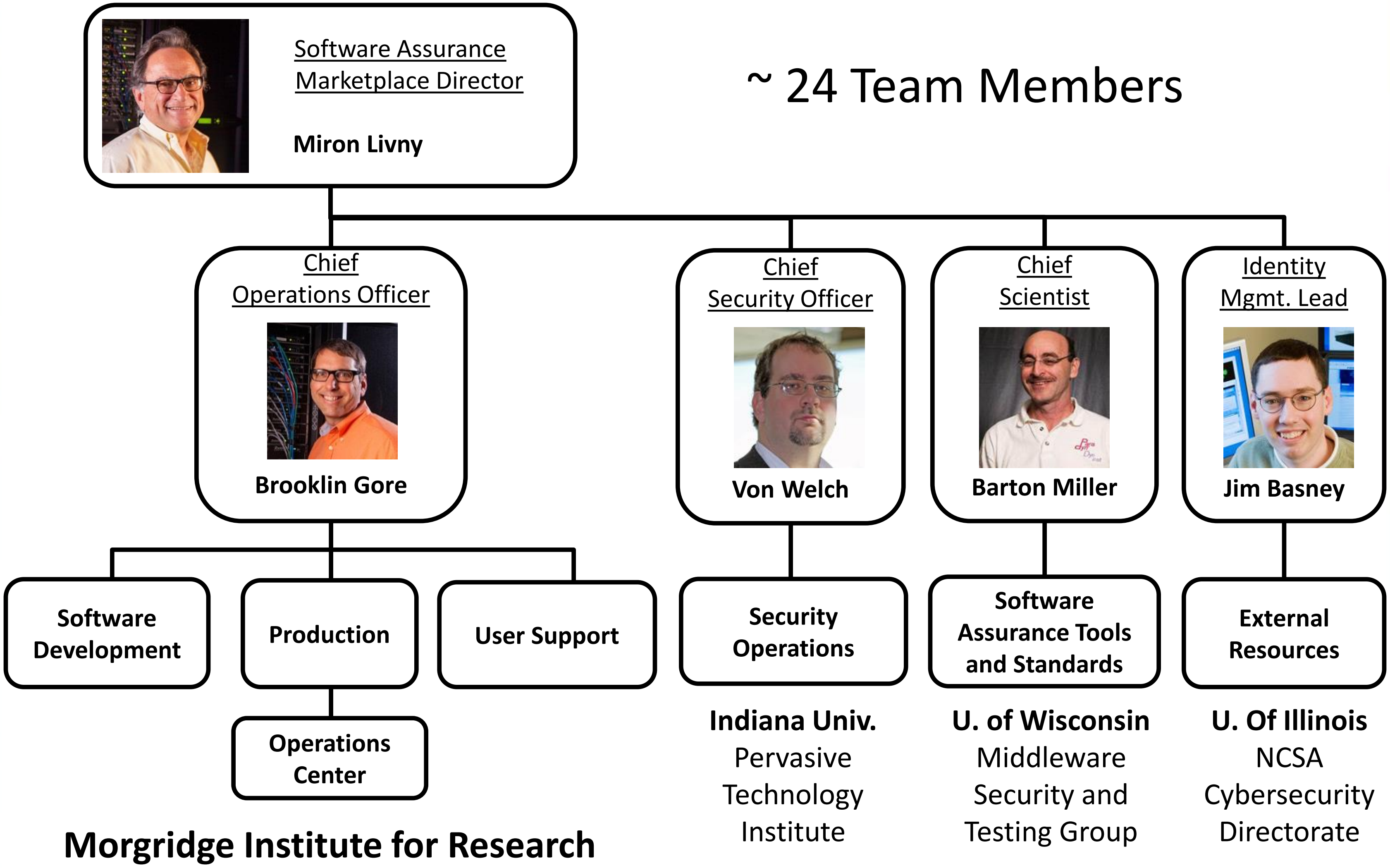
- BAA 11-02 involves 34 awards to 29 academic, commercial and research organizations in 14 technical areas focused on *detecting*, *preventing* and *responding* to cyber attacks

Software Assurance Marketplace

- Six proposals submitted
- Awarded to **Morgridge Institute for Research** with **Indiana University**, **University of Illinois Urbana-Champaign**, and **UW–Madison** as subcontractors
- Offers industry, academia and government agencies ***no-cost access*** to a secure research facility with analytical and reporting capabilities
- Will help the software assurance community improve the security of software used in the nation’s critical infrastructure

SOFTWARE ASSURANCE MARKETPLACE
A NATIONAL CYBERSECURITY RESOURCE

Software Assurance Marketplace Organization



Software Assurance Marketplace Director

Miron Livny

~ 24 Team Members

Chief Operations Officer

Brooklin Gore

Chief Security Officer

Von Welch

Chief Scientist

Barton Miller

Identity Mgmt. Lead

Jim Basney

Software Development

Production

User Support

Operations Center

Morgridge Institute for Research

Security Operations

Indiana Univ.
Pervasive Technology Institute

Software Assurance Tools and Standards

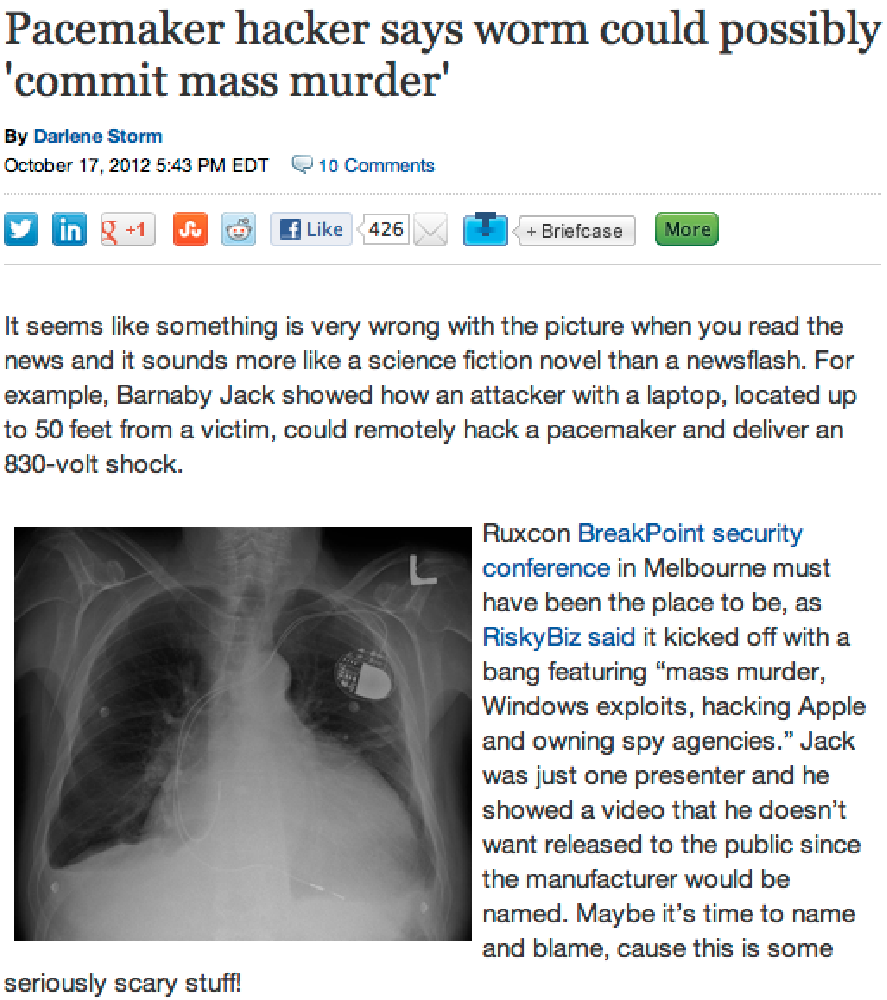
U. of Wisconsin
Middleware Security and Testing Group

External Resources

U. Of Illinois
NCSA Cybersecurity Directorate

SOFTWARE ASSURANCE MARKETPLACE
A NATIONAL CYBERSECURITY RESOURCE

A Growing Need…

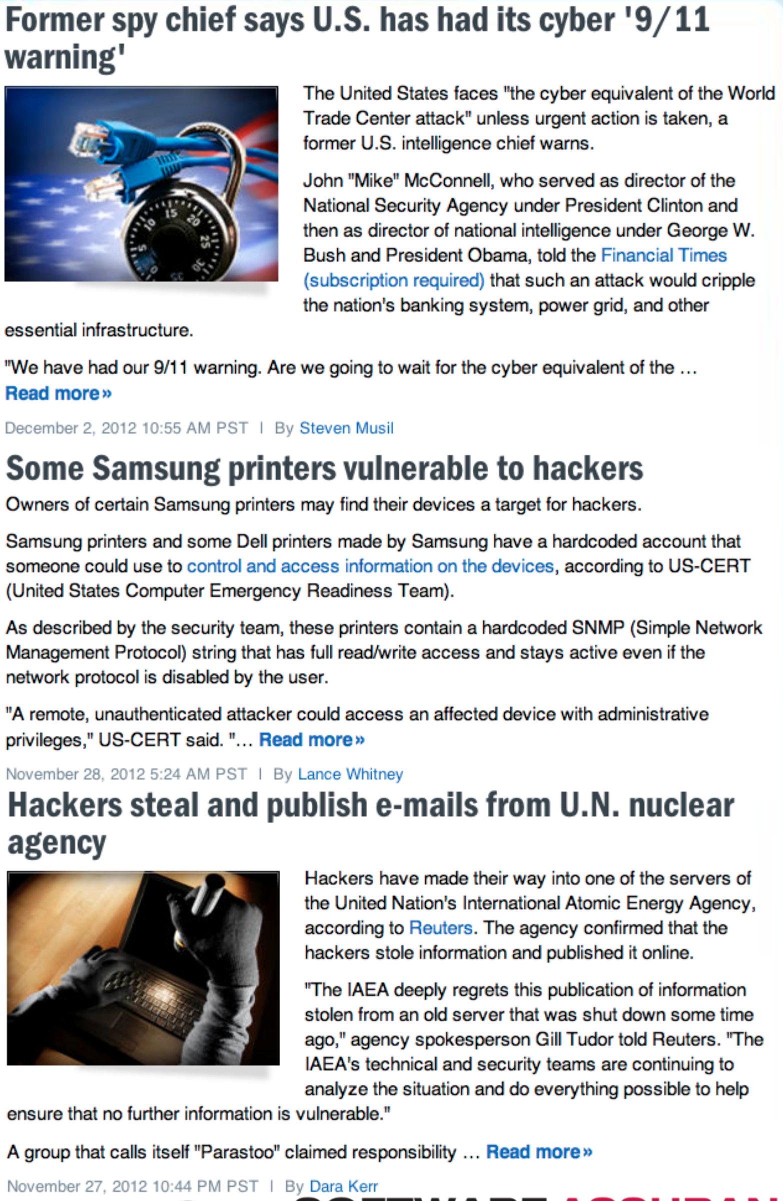


Pacemaker hacker says worm could possibly 'commit mass murder'

By Darlene Storm
October 17, 2012 5:43 PM EDT 10 Comments

It seems like something is very wrong with the picture when you read the news and it sounds more like a science fiction novel than a newsflash. For example, Barnaby Jack showed how an attacker with a laptop, located up to 50 feet from a victim, could remotely hack a pacemaker and deliver an 830-volt shock.

Ruxcon BreakPoint security conference in Melbourne must have been the place to be, as RiskyBiz said it kicked off with a bang featuring "mass murder, Windows exploits, hacking Apple and owning spy agencies." Jack was just one presenter and he showed a video that he doesn't want released to the public since the manufacturer would be named. Maybe it's time to name and blame, cause this is some seriously scary stuff!



Former spy chief says U.S. has had its cyber '9/11 warning'

The United States faces "the cyber equivalent of the World Trade Center attack" unless urgent action is taken, a former U.S. intelligence chief warns.

John "Mike" McConnell, who served as director of the National Security Agency under President Clinton and then as director of national intelligence under George W. Bush and President Obama, told the Financial Times (subscription required) that such an attack would cripple the nation's banking system, power grid, and other essential infrastructure.

"We have had our 9/11 warning. Are we going to wait for the cyber equivalent of the … Read more»

December 2, 2012 10:55 AM PST | By Steven Musil

Some Samsung printers vulnerable to hackers

Owners of certain Samsung printers may find their devices a target for hackers.

Samsung printers and some Dell printers made by Samsung have a hardcoded account that someone could use to control and access information on the devices, according to US-CERT (United States Computer Emergency Readiness Team).

As described by the security team, these printers contain a hardcoded SNMP (Simple Network Management Protocol) string that has full read/write access and stays active even if the network protocol is disabled by the user.

"A remote, unauthenticated attacker could access an affected device with administrative privileges," US-CERT said. "… Read more»

November 28, 2012 5:24 AM PST | By Lance Whitney

Hackers steal and publish e-mails from U.N. nuclear agency

Hackers have made their way into one of the servers of the United Nation's International Atomic Energy Agency, according to Reuters. The agency confirmed that the hackers stole information and published it online.

"The IAEA deeply regrets this publication of information stolen from an old server that was shut down some time ago," agency spokesperson Gill Tudor told Reuters. "The IAEA's technical and security teams are continuing to analyze the situation and do everything possible to help ensure that no further information is vulnerable."

A group that calls itself "Parastoo" claimed responsibility … Read more»

November 27, 2012 10:44 PM PST | By Dara Kerr

Use Cases

Software Developers

Upload software packages for analysis by a suite of software assurance tools and view results via dashboard.

Upload SWA tools and evaluate against large corpus of SW packages and test suites with known weaknesses.

Software Assurance Tool Developers

Software Assurance Marketplace

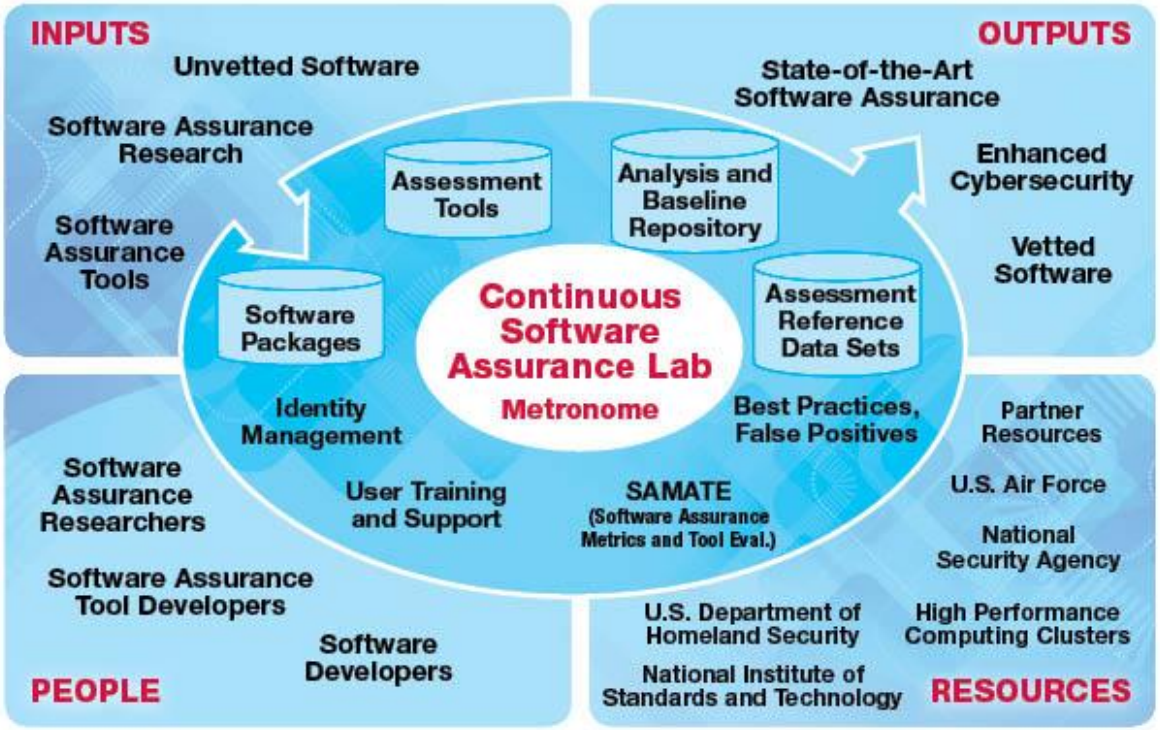
Cybersecurity Researchers

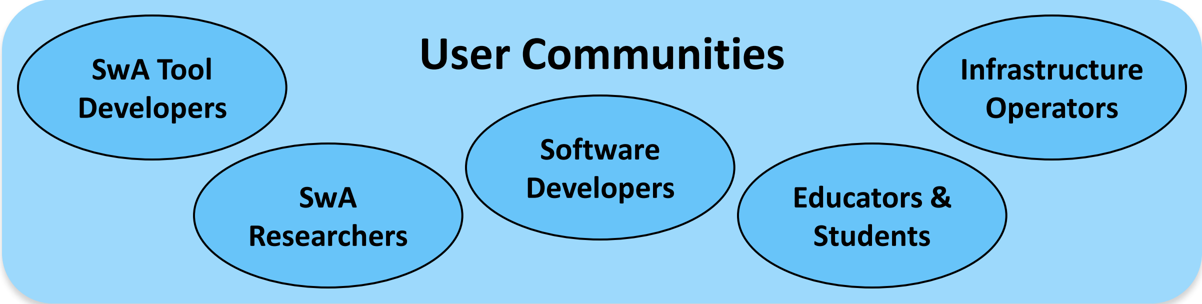
Review data on tool coverage and common weaknesses to improve standards, education and certification programs.

SOFTWARE ASSURANCE MARKETPLACE
A NATIONAL CYBERSECURITY RESOURCE

SOFTWARE ASSURANCE MARKETPLACE

A national cybersecurity resource offering continuous software assurance.


INPUTS
Unvetted Software
Software Assurance Research
Software Assurance Tools
OUTPUTS
State-of-the-Art Software Assurance
Enhanced Cybersecurity
Vetted Software
Assessment Tools
Analysis and Baseline Repository
Software Packages
Assessment Reference Data Sets
Continuous Software Assurance Lab
Metronome
Identity Management
Best Practices, False Positives
User Training and Support
SAMATE (Software Assurance Metrics and Tool Eval.)
Software Assurance Researchers
Software Assurance Tool Developers
Software Developers
PEOPLE
Partner Resources
U.S. Air Force
National Security Agency
U.S. Department of Homeland Security
High Performance Computing Clusters
National Institute of Standards and Technology
RESOURCES



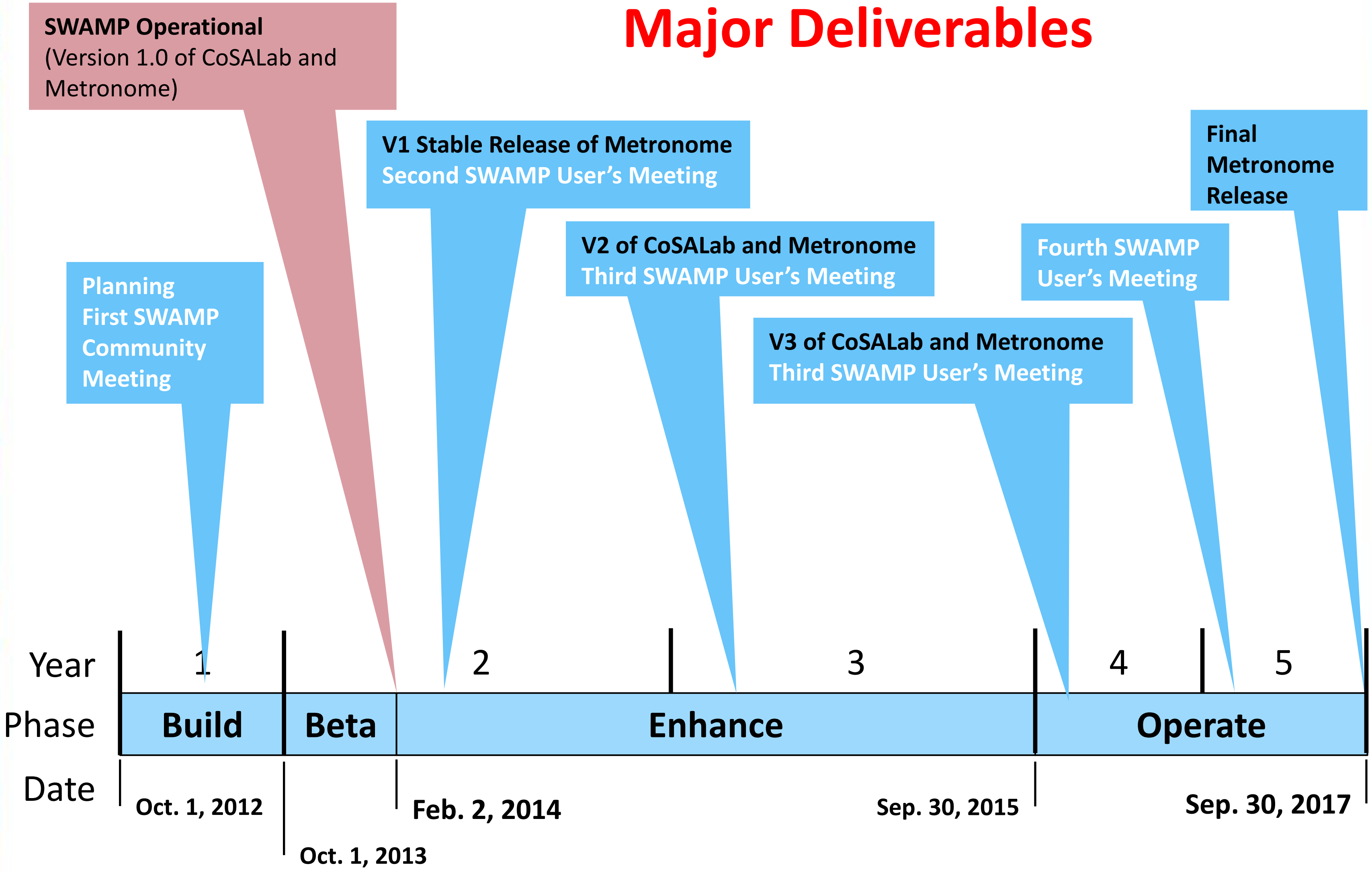
SOFTWARE ASSURANCE MARKETPLACE
A NATIONAL CYBERSECURITY RESOURCE

Making HTCondor Safer with Continuous Software Assurance

- **In the past**
  - Used BaTLab for release build and test
  - Ran Coverity static analysis tool before stable releases
- **Today**
  - Use BaTLab for *per commit* build and test
  - Running Coverity ‘continuously’
  - Working on adding a 2nd tool from GrammaTech
- **Spring 2014**
  - Use SWAMP for continuous integration *and* CSwA
  - Continuous runs with a corpus of open source and commercial static analysis tools
  - Over time, adding dynamic tools, improved results viewing

SOFTWARE ASSURANCE MARKETPLACE
A NATIONAL CYBERSECURITY RESOURCE

Major Deliverables



SWAMP Operational
(Version 1.0 of CoSALab and Metronome)

Planning
First SWAMP Community Meeting

V1 Stable Release of Metronome
Second SWAMP User's Meeting

V2 of CoSALab and Metronome
Third SWAMP User's Meeting

V3 of CoSALab and Metronome
Third SWAMP User's Meeting

Fourth SWAMP User's Meeting

Final Metronome Release

SOFTWARE ASSURANCE MARKETPLACE
A NATIONAL CYBERSECURITY RESOURCE

Jan. 2014 Initial Operating Capabilities

5 Tools

- Clang, cppcheck, Oink (C, C++)
- Findbugs, PMD (Java)
- Commercial – TBD
- Developers bring more

100 Packages

- C, C++, Java Open Source
- Include test suites (e.g. NIST SATE)
- Developers bring more

8 Platforms

- Debian
- Fedora
- Red Hat
- Scientific Linux
- Ubuntu
- Windows

Current + Last Version?

Requests?

(to be defined)

SOFTWARE ASSURANCE MARKETPLACE
A NATIONAL CYBERSECURITY RESOURCE

You are the key!

- **We need your input** – how do you envision using such a resource? What tools, packages, policies, topics, platforms would help you?
- **We need your involvement** – help with tools, packages, standards, technical literature, seminars, training.
- **We need your feedback** – the good, the bad, and the ugly.

Contact us: **info@cosalab.org**

http://swamp.cosalab.org

SOFTWARE ASSURANCE MARKETPLACE
A NATIONAL CYBERSECURITY RESOURCE