RED TEAM

http://fedoraproject.org/wiki/SIGs/Red_Team

Fedora Red Team SIG Update

Jason Callaway | jasoncallaway@fedoraproject.org

This presentation is licensed CC-BY-SA

Agenda

- History of the SIG
- Overview of projects
- Community response
- Why the Fedora Project should care
- How you can help

History

- Born at Def Con 24
- Originally penetration testing-focused on build infrastructure
- "If we're going to get into cyber, we'd better harden the **** up"
- Organizational contrarians a-la Zenko's Red Team: How to Succeed by Thinking Like the Enemy
- Really took off at Def Con 25

Current projects

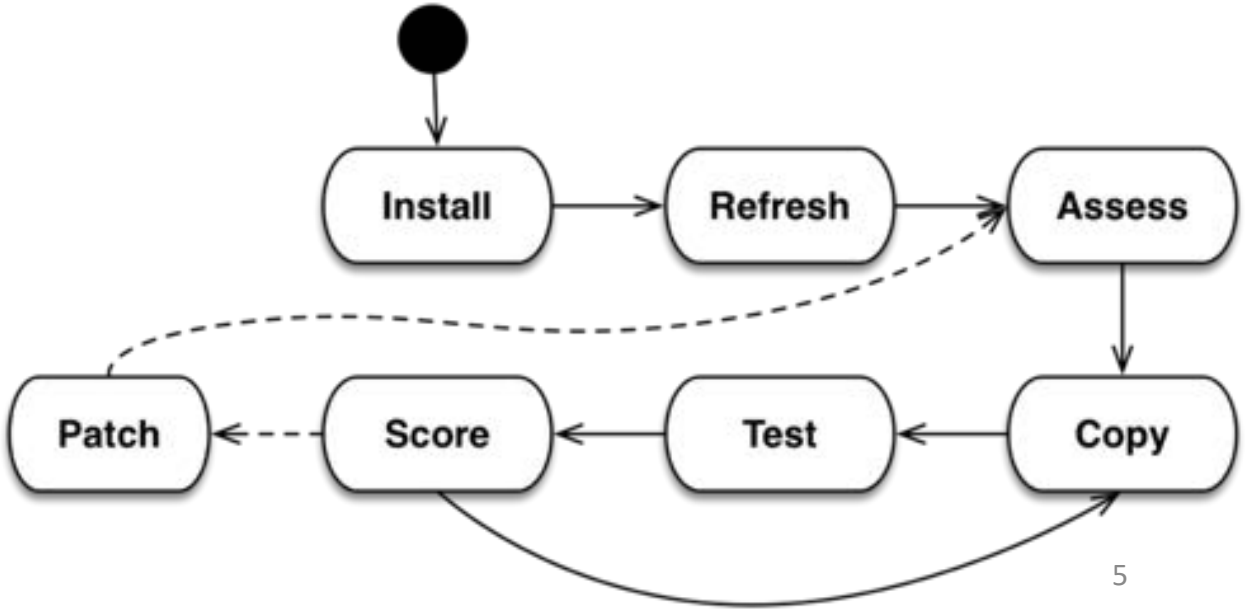
- Enterprise Linux Exploit Mapper (ELEM)
  - https://github.com/fedoraredteam/elem *
- Cyber Test Lab
  - https://github.com/fedoraredteam/cyber-test-lab *
- Red Container
  - https://github.com/fedoraredteam/red-container *
- cyber-range-target
  - https://github.com/fedoraredteam/cyber-range-target
- Compliance / fedoraredteam.compliant *
  - https://github.com/fedoraredteam/compliance

* Has community contributions

ELEM

RED TEAM

- Maps local vulnerabilities to known exploits
- Crowdsourced exploit curation, STRIDE
- Shows value of supported open source
- https://youtu.be/NX931nfyAmg



Cyber Test Lab

- Inspired by Cyber ITL (http://cyber-itl.org/)
- Quantitative analysis of risk on a per-ELF binary basis
- "How hard would it be for a security researcher to find a new 0-day in THIS binary?"

What CTL does

- Static analysis (alpha today)
- Dynamic analysis (fuzzing in the future)
- On per-binary basis
  - Position independent execution (ASLR)
  - Fortified functions
  - Stack protection (NX bit)
  - Read-only relocations (RELRO)
  - Immediate binding
  - Cyclomatic complexity, cycle cost
  - Function size, branch frequency (future)
  - Function riskiness (future)

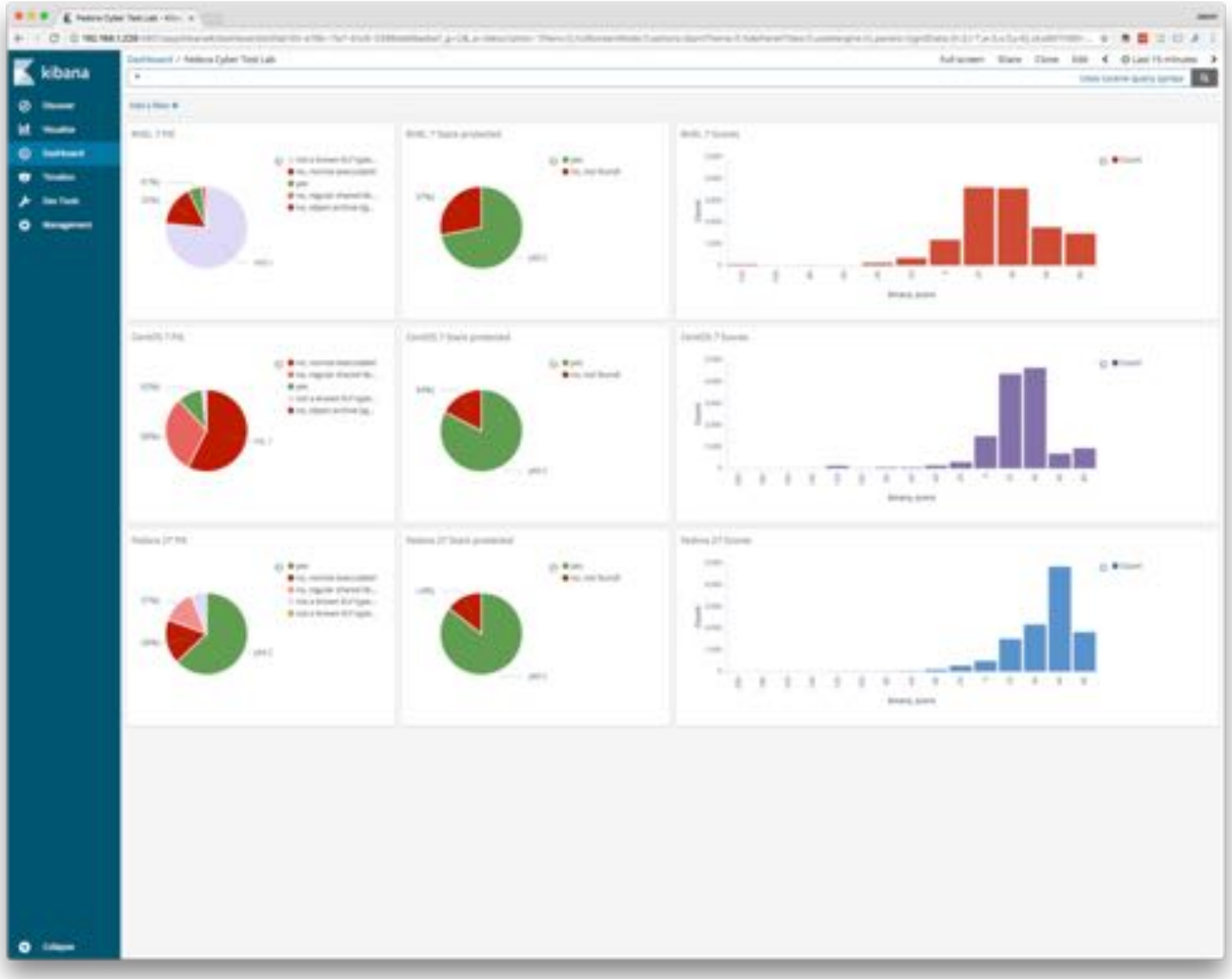
CTL Example Output

RED TEAM


```
{ "results": {
        "complexity": { "r2 aa": {  "afCc": 4, "afC": 112 } },
        "usr/bin/agr": {
            "report-functions": [ "__memcpy_chk", "strtol", "tcsetattr", "strrchr",  "__libc_start_main", ...
            "hardening-check": {
                " Read-only relocations": "yes",
                " Position Independent Executable": "no, normal executable!",
                " Stack protected": "yes",
                " Fortify Source functions": "yes (some protected functions found)",
                " Immediate binding": "no, not found!"          },
         "filename": "usr/bin/agr”
        "metadata": { "spec_data": {
            "Group": " Applications/Text",
            "Name": " AGReader",
            "License": " GPL+",
            "URL": " http://main.aminet.net/misc/unix/",  ...
```

CTL Pending Update

RED TEAM



Red Container

- The world doesn’t need another Kali Linux
- Kali, Black Arch, Parrot, lots of offensive distros
- Primarily a packaging effort, make the tools easy to consume
- Open Container Initiative changes this game
- Containerize offensive tools, make them easy to install anywhere
- Want to run MSF with PostgreSQL backend? Great! Do it on RHEL, Debian, Windows…

cyber-range-target

- "Cyber Range" is a thing
- Training, certification, R&D
- Need to be able to deliberately make a system vulnerable to specific CVEs
- Ansible role, elegant AF

```yaml
---
- hosts: webservers
  remote_user: admin
  become: true
  roles:
    - fedoraredteam.cyber-range-target
  vars:
    cves_to_test:
      - CVE-2014-6271
```

Compliance

- Security compliance sucks, but for many it’s a legal requirement, i.e., FISMA
- But does it work?
- Red team approach to compliance using FRT tooling
- Constructive feedback
- Ansible role to implement controls, cross platform
  - fedoraredteam.compliant

Community Response

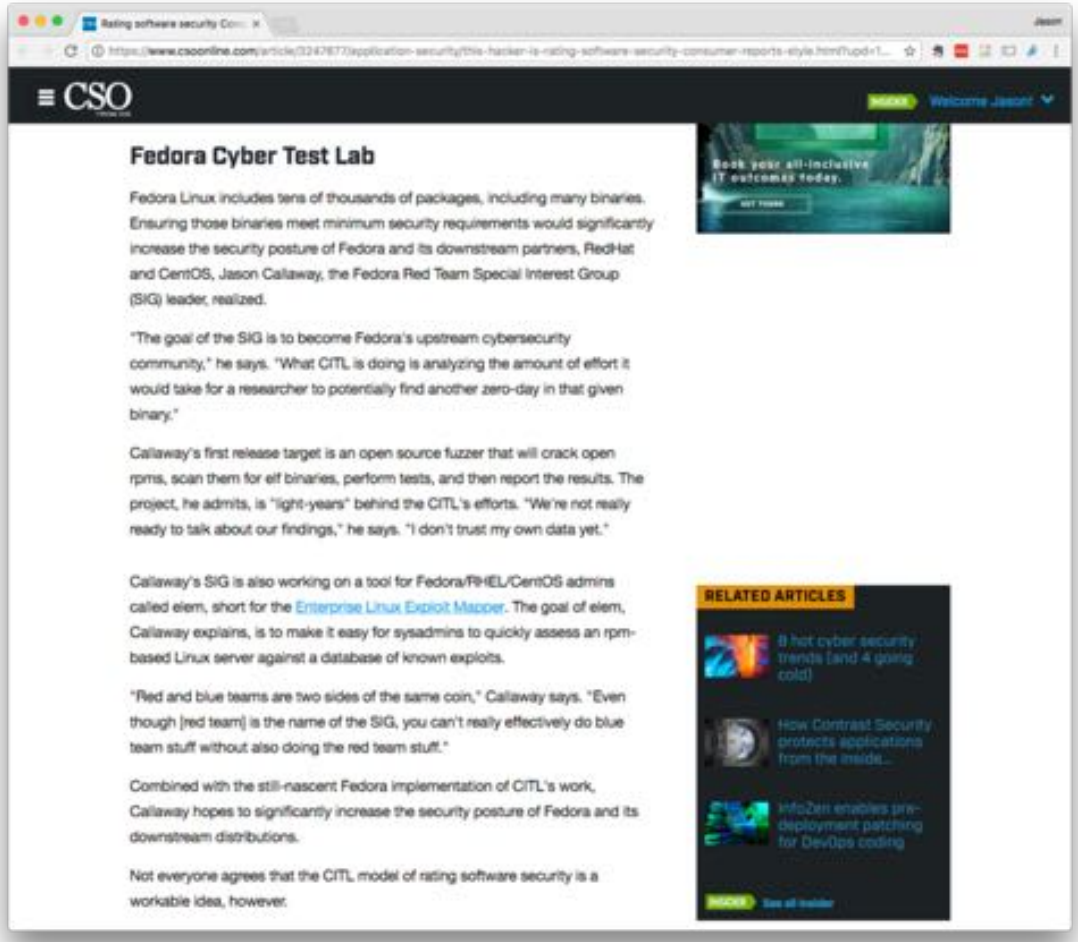
RED TEAM

Community Response

RED TEAM

Articles

RED TEAM



CSO

Fedora Cyber Test Lab

Fedora Linux includes tens of thousands of packages, including many binaries. Ensuring those binaries meet minimum security requirements would significantly increase the security posture of Fedora and its downstream partners, RedHat and CentOS, Jason Callaway, the Fedora Red Team Special Interest Group (SIG) leader, realized.

"The goal of the SIG is to become Fedora's upstream cybersecurity community," he says. "What CITL is doing is analyzing the amount of effort it would take for a researcher to potentially find another zero-day in that given binary."

Callaway's first release target is an open source fuzzer that will crack open rpms, scan them for elf binaries, perform tests, and then report the results. The project, he admits, is "light-years" behind the CITL's efforts. "We're not really ready to talk about our findings," he says. "I don't trust my own data yet."

Callaway's SIG is also working on a tool for Fedora/RHEL/CentOS admins called elem, short for the Enterprise Linux Exploit Mapper. The goal of elem, Callaway explains, is to make it easy for sysadmins to quickly assess an rpm-based Linux server against a database of known exploits.

"Red and blue teams are two sides of the same coin," Callaway says. "Even though [red team] is the name of the SIG, you can't really effectively do blue team stuff without also doing the red team stuff."

Combined with the still-nascent Fedora implementation of CITL's work, Callaway hopes to significantly increase the security posture of Fedora and its downstream distributions.

Not everyone agrees that the CITL model of rating software security is a workable idea, however.

RELATED ARTICLES

phoronix

ARTICLES & REVIEWS | NEWS ARCHIVE | FORUMS | CATEGORIES

Fedora Launches The "Red Team" For Dealing With Cybersecurity

Written by Michael Larabel in Fedora on 18 September 2017 at 12:28 PM EDT. 20 Comments

The Fedora Red Team is a new special interest group (SIG) within the Fedora ecosystem for dealing with cybersecurity.

The new team's Wiki page explains, "The goal of the Fedora Red Team (FRT) is to become Red Hat's upstream cybersecurity community. This SIG is the community focal point for offensive tooling, exploit curation, standards, and reference architectures."

The Red Team's mission statement comes down to: "To be the catalyst in the enterprise Linux community that enables Computer Network Operations, the open source way."

Jason Callaway of the newly-founded Fedora Red Team has written a blog post this weekend to describe more about the SIG's planned objectives and work.

20 Comments

About The Author

Michael Larabel is the principal author of Phoronix.com and founded the site in 2004 with a focus on enriching the Linux hardware experience. Michael has written more than 10,000 articles covering the state of Linux hardware support, Linux performance, graphics drivers, and other topics. Michael is also the lead developer of the Phoronix Test Suite, Phoromatic, and OpenBenchmarking.org automated benchmarking software. He can be followed via Twitter or contacted via MichaelLarabel.com.

Latest Linux News

Btrfs Updates Sent In For The Linux 4.17 Kernel
Fedora 28 Beta Released
GCC 7.3 vs. GCC 8.0 vs. LLVM Clang 6.0 On The POWER9 Raptor Talos II
IBM s390 Continues Working On Spectre Defense With Linux 4.17, VirtIO GPU Emulation
Linux 4.17 Kicks Off Another Busy Cycle
AMDVLK Updated With Fresh Batch Of Fixes
GnuCash 3.0 Released, Ported To GTK3 Toolkit
XFS Gets Lazy Time Support In Linux 4.17, Other Improvements
RadeonSI Now Supports KHR_blend_equation_advanced, Needed For OpenGL ES 3.2
Wayland 1.15 & Weston 4.0 Release Candidates Published

Latest Featured Articles

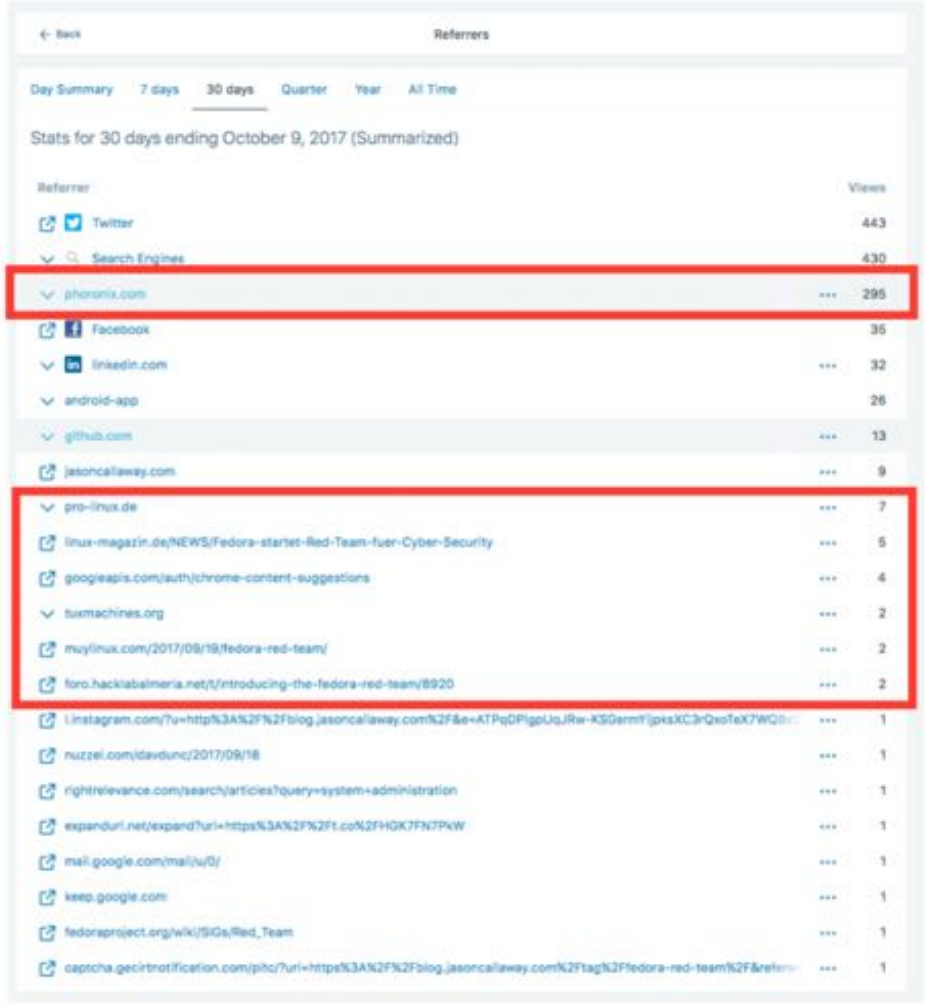
Linux RAID Performance On Dual NVMe SSDs
A Look At Ubuntu 10.04 To Ubuntu 18.04 Linux Performance
Windows 10 vs. Windows WSL vs. Linux - Ubuntu / openSUSE / Debian / Clear Linux
Linux 4.4 To 4.16 Kernel Benchmarks With AMD Ryzen Threadripper
Linux 4.16 File-System HDD & SSD Tests With EXT4/F2FS/Btrfs/XFS

Support Phoronix

https://www.csoonline.com/article/3247677/application-security/this-hacker-is-rating-software-security-consumer-reports-style.html?upd=1522773734975

https://www.phoronix.com/scan.php?page=news_item&px=Fedora-Red-Team

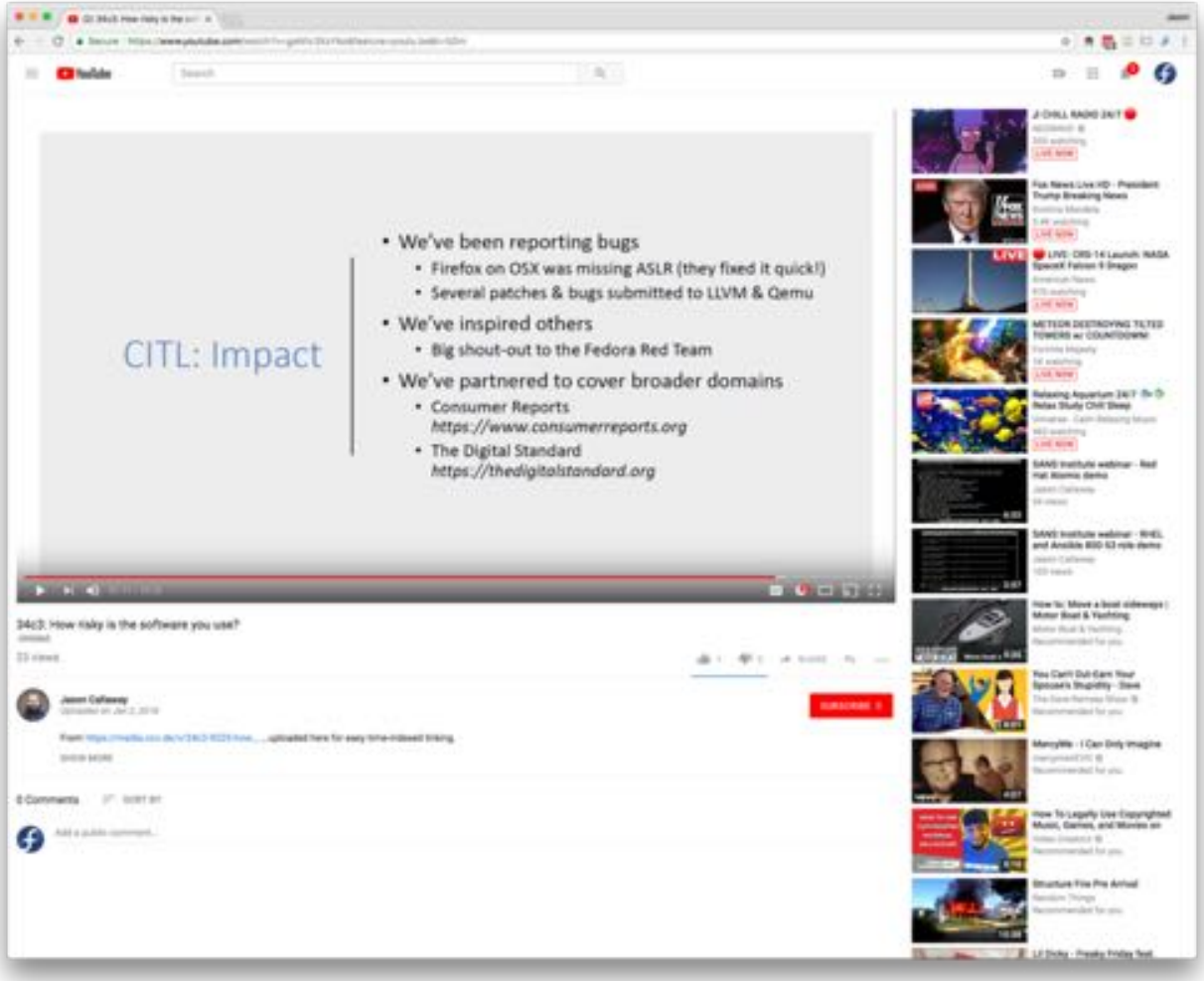
Other articles



https://blog.jasoncallaway.com/2017/09/17/introducing-the-fedora-red-team/

34c3 shout out

RED TEAM



https://youtu.be/gaWlv3XxYko?t=50m

Why you should care

- Big opportunity here for the Fedora Project
- Make Fedora Linux more secure
- Make all Linuxes more secure
- Thought leadership
- It’s the right thing to do

How you can help

1. Amplification
2. Pull requests

Thank you