MIS|TI PRESENTS

InfoSecWorld

Conference & Expo 2018

TIPS AND TRICKS FOR DEFENDING THE ENTERPRISE USING OPEN SOURCE TOOLS

Paul Asadoorian
Founder & CEO
Security Weekly

Agenda

1. Why should we be talking about open source?
2. How most open source deployments go (Mostly in Paul's world)
3. Why you **should not** use open source security software
4. Why you **should** use open source security software
5. Examples of really good open source security software

Why we should be talking about open source software

My Own Experiences

Late 90s: We didn't learn Linux in many degree programs; my day-job did not want to run software without commercial support

Early 2000s: We ran Solaris at the University (using many open source components) but the platform was not Linux

2007: I helped run a project that deployed Linux and open source software to several schools for security monitoring

Open Source Today

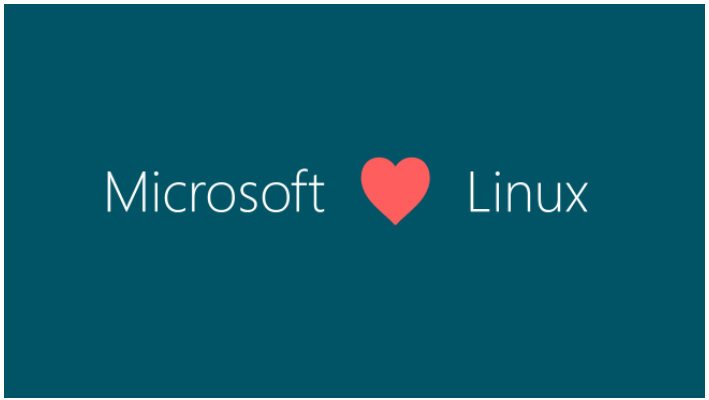
A 2015 study conducted by Black Duck Software of 1,300 C-level IT professionals stated 78% use open source (more than double from 2010)

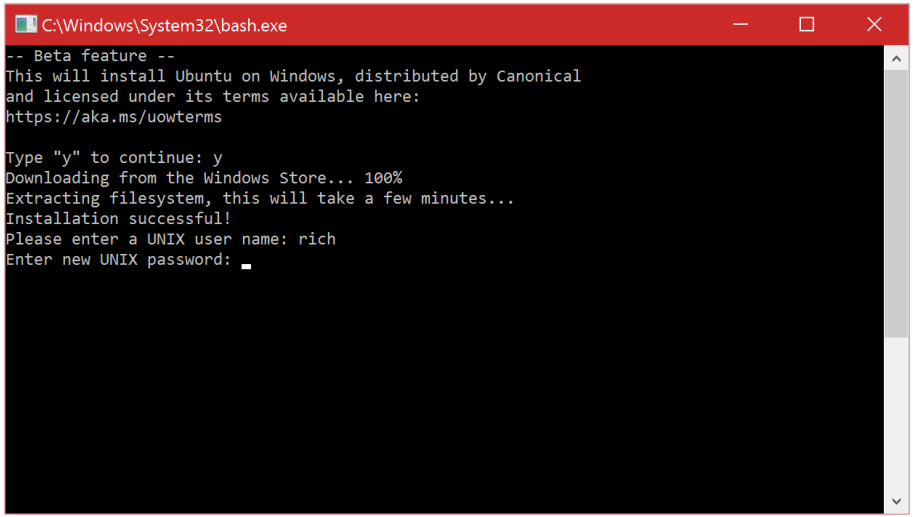
Black Duck Software makes software to find vulnerabilities in open source software in the enterprise. They were acquired in November 2017 by Synopsys for $565 million after taking a total of $75 million in funding.

https://www.csoonline.com/article/3033837/security/open source-security-is-not-as-big-of-a-concern-as-it-once-was.html

From Serving Suggestion To…

“40% of Microsoft's clients using its Azure cloud computing platform are running Linux operating system rather than Windows”





https://www.ciodive.com/news/open source-the-new-normal-in-enterprise-software/438671/

“Some Smart Person”

red canary

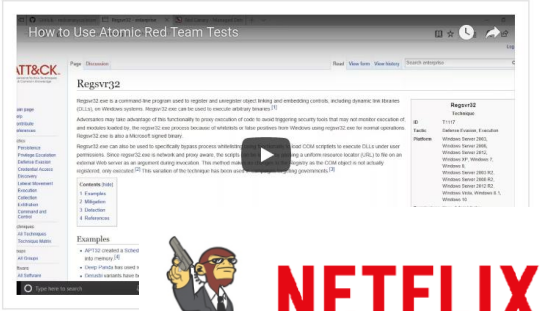
Why Red Canary Managed Detection & Response Features Company

Atomic Red Team

Atomic Red Team is an open source collection of small, highly portable tests mapped to the corresponding techniques in the MITRE ATT&CK framework. These tests can be used to validate detection and response technology and processes.

Get the repo:
https://github.com/redcanaryco/atomic-red-team

Browse popular Atomic Red Team resources below to learn more.



NETFLIX

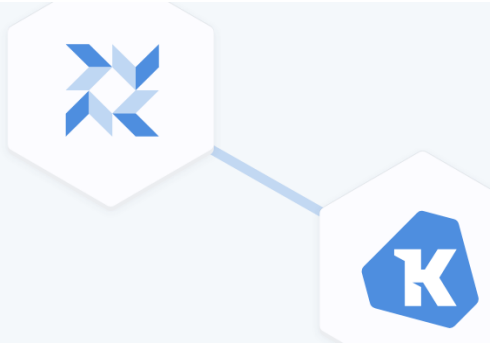
Security Monkey
open source cloud security tracking system

Osquery powers Kolide

FACEBOOK'S OPEN-SOURCE SECURITY SOLUTION

Developed at **Facebook**, **osquery** allows you to easily ask questions about your **Linux**, **Windows**, and **macOS** infrastructure. Whether your goal is intrusion detection, infrastructure reliability, or compliance, **osquery** gives you the ability to empower and inform a broad set of organizations within your company. Learn more at osquery.io

VIEW THE CODE TRY IT NOW



SIMP

The System Integrity Management Platform

Fort Meade, Maryland https://github.com/Nation… simp-dev@googlegroups…

Repositories 195 People 12

Pinned repositories

simp-core
The base SIMP build repository
Ruby 83 33

simp-doc
The SIMP Product Documentation
Ruby 13 19

inspec
InSpec Profile for … STIG
Ruby 3 8

Uber Open Source

Open Source Software at Uber

70+ countries and counting. http://uber.github.io/

Repositories 140 People 70

Pinned repositories

pyro
Deep universal probabilistic programming with Python and PyTorch
Jupyter Notebook 3k 301

RIBs
Uber's cross-platform mobile architecture framework.
Java 3k 210

deck.gl
WebGL2 powered geospatial visualization layers
JavaScript 4.2k 541

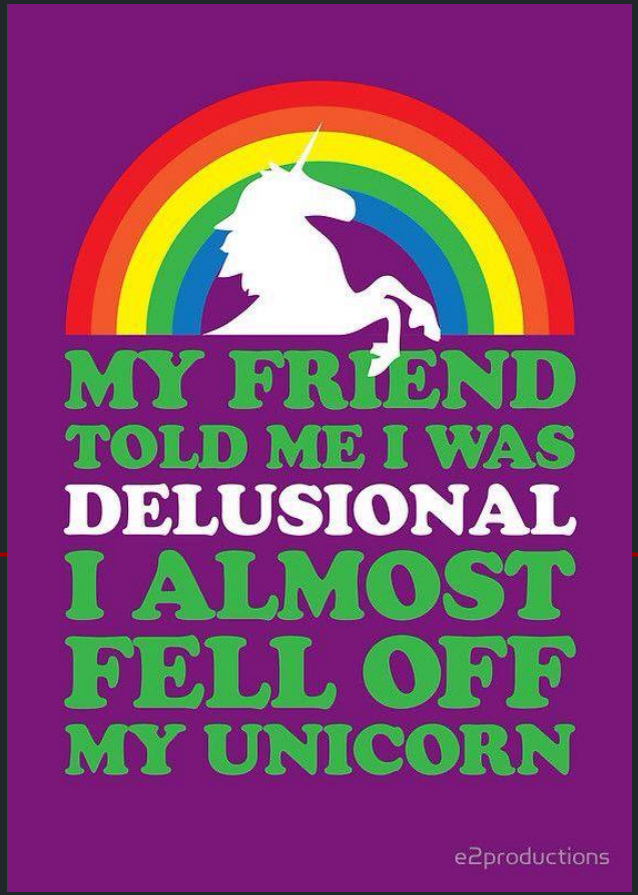
react-map-gl
React friendly API wrapper around MapboxGL JS
JavaScript 3.4k 341

react-vis
Data-Visualization oriented components
JavaScript 3.1k 273

horovod
Distributed training framework for TensorFlow.
C++ 1.7k 231

“We should all use open source!”

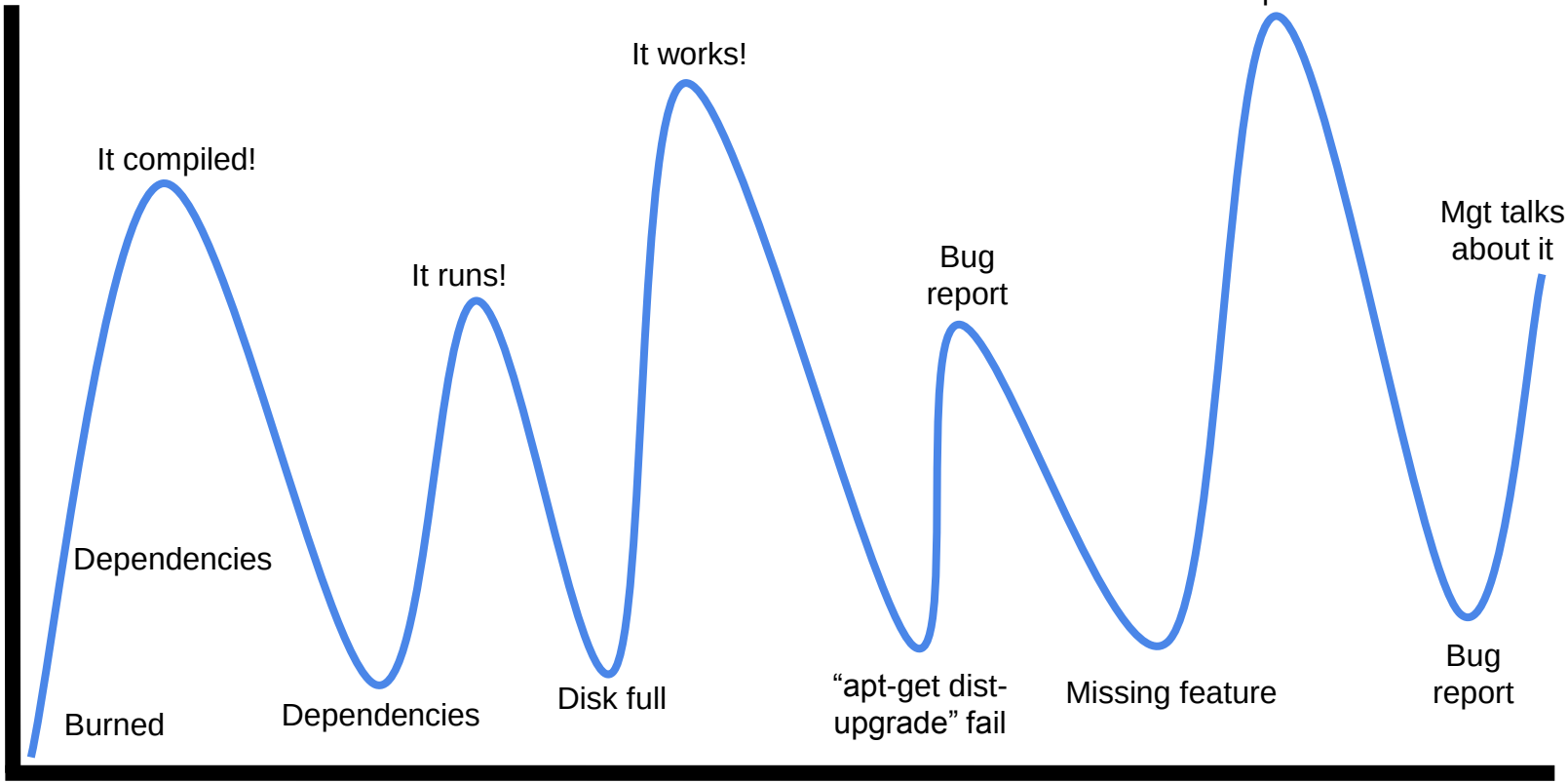
But, here is how most open source projects tend to go (especially mine)



Evolution Of Open Source Projects

Hug Tux

Fork in my eye



The Evolution Of An Open Source Solution In The Enterprise

You got burned in a meeting because you had no visibility into a problem or couldn't solve the problem fast enough

Common question: "How big is the problem?"

(e.g., How many systems are compromised? How did they become compromised?)

The Evolution Of An Open Source Solution In The Enterprise

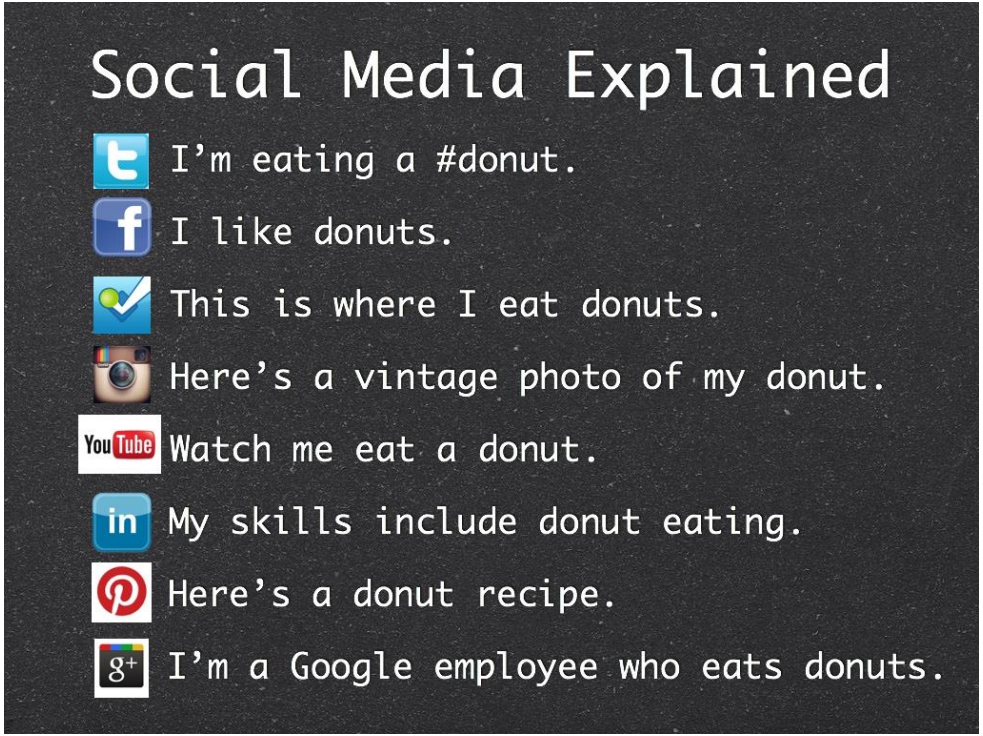
You searched the Internet to find solutions to the problem and found a few commercial vendors that could help

You read the vendor websites, and now you are more confused

The Evolution Of An Open Source Solution In The Enterprise

You asked social media how other people are solving the problem, most just said “Python”

Not naming names…



The Evolution Of An Open Source Solution In The Enterprise

You eventually find some open source software that looks like it might help solve the problem

You download and install the new software, and even get excited

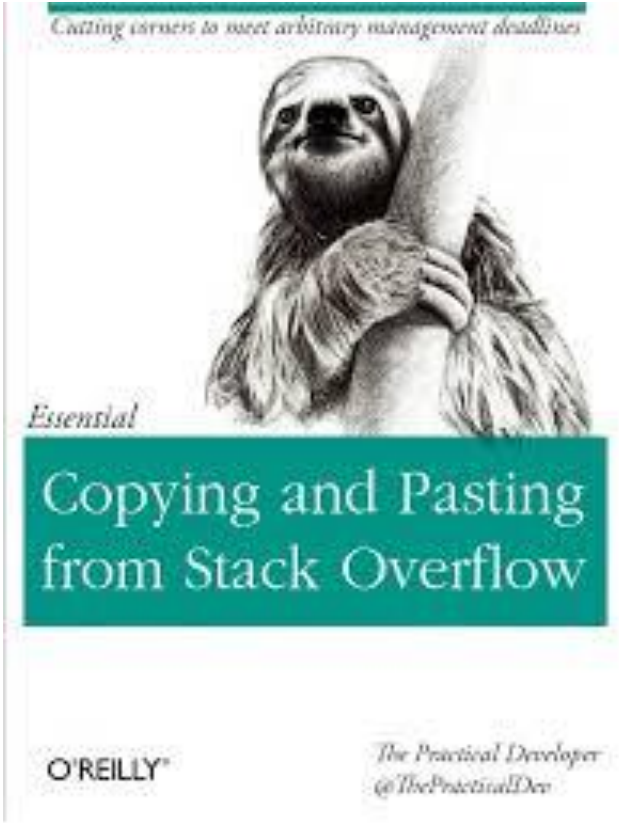
The Evolution Of An Open Source Solution In The Enterprise

Right at the end of the lengthy install process, you get an error

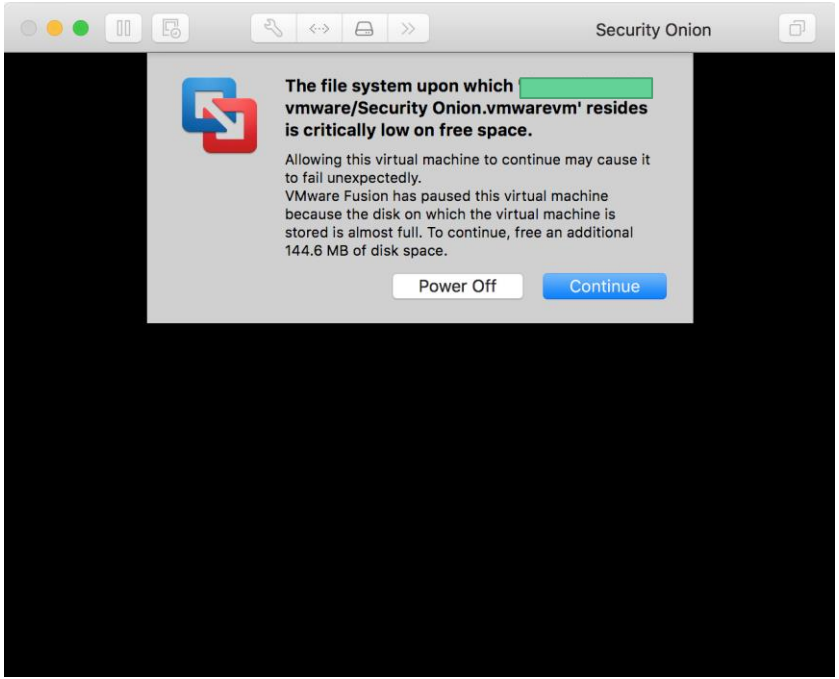
You correct that error only to realize the feature you wanted is in the experimental version, so you start over

The Evolution Of An Open Source Solution In The Enterprise

Encountering installation issues (again), you spend a hour (or more) Googling for the answer, trying different suggestions found on Stack overflow, the open source project's discussion forum and random blog posts



The Evolution Of An Open Source Solution In The Enterprise



You finally get it up and running, only to realize you are out of disk space and have to:

1. Find the logs and delete them
2. Change the retention window
3. Fix the compression script
4. Add more disk space
5. Realize your VM will never have enough space and move to actual hardware...

The Blink/Spore Drive Theory

Star Trek: Discover (Spore drive), Dark Matter (Blink drive)

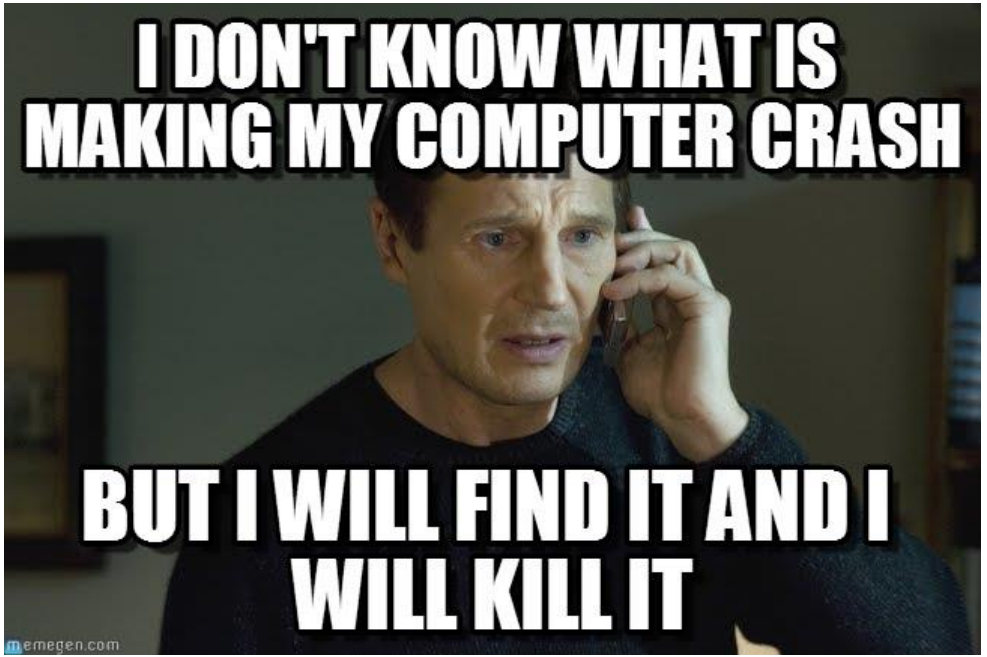
Always issues with the technology

The same goes for bleeding-edge open source technology

The Evolution Of An Open Source Solution In The Enterprise

You finally get it working, and when you show your co-workers how awesome it is, it crashes.

More Googling and Stack Overflow



The Evolution Of An Open Source Solution In The Enterprise

You finally get it working (again), and use it to solve a problem, realizing it's better than some or most commercial software.

You may also realize:

- Ubuntu needs updating, Noooooooooooo.....
- The next version uses completely different technology
- The features you want/need are no longer supported

Why Don’t We Want To Use Open Source Tools?

Why Don’t We Want To Use Open Source Tools?

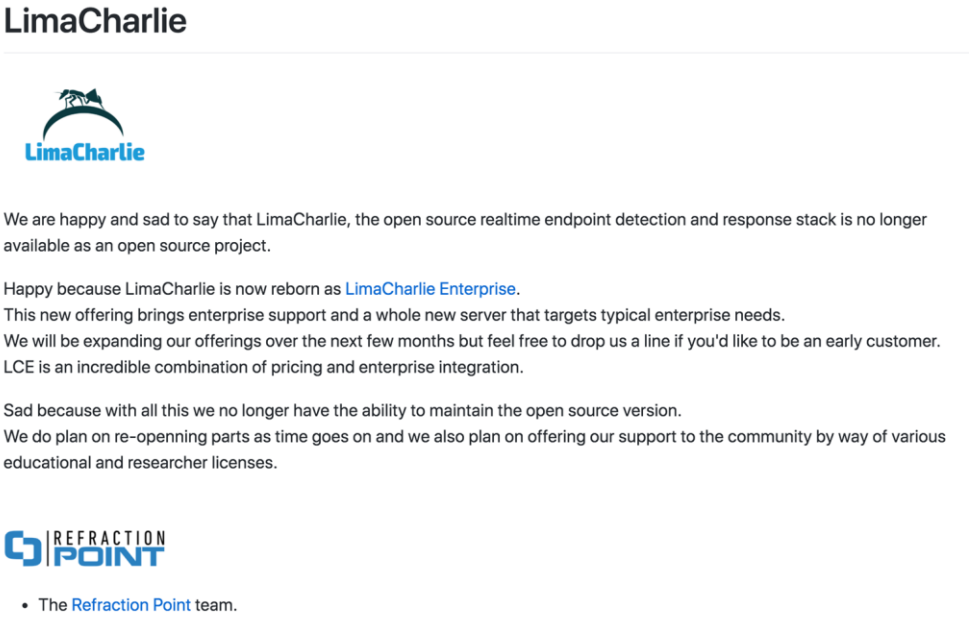
Support - We can’t blame the vendor if something goes wrong, or get help if we encounter a problem.

Why Don’t We Want To Use Open Source Tools?

Bugfixes & New Features - When the author has time, you may get these, or if someone contributes, but its random and not guaranteed.

Why Don’t We Want To Use Open Source Tools?

Projects Can be Ephemeral - You don’t want to spend 6 months implementing a solution only to have it go closed source or abandoned



LimaCharlie

LimaCharlie

We are happy and sad to say that LimaCharlie, the open source realtime endpoint detection and response stack is no longer available as an open source project.

Happy because LimaCharlie is now reborn as LimaCharlie Enterprise.
This new offering brings enterprise support and a whole new server that targets typical enterprise needs.
We will be expanding our offerings over the next few months but feel free to drop us a line if you'd like to be an early customer.
LCE is an incredible combination of pricing and enterprise integration.

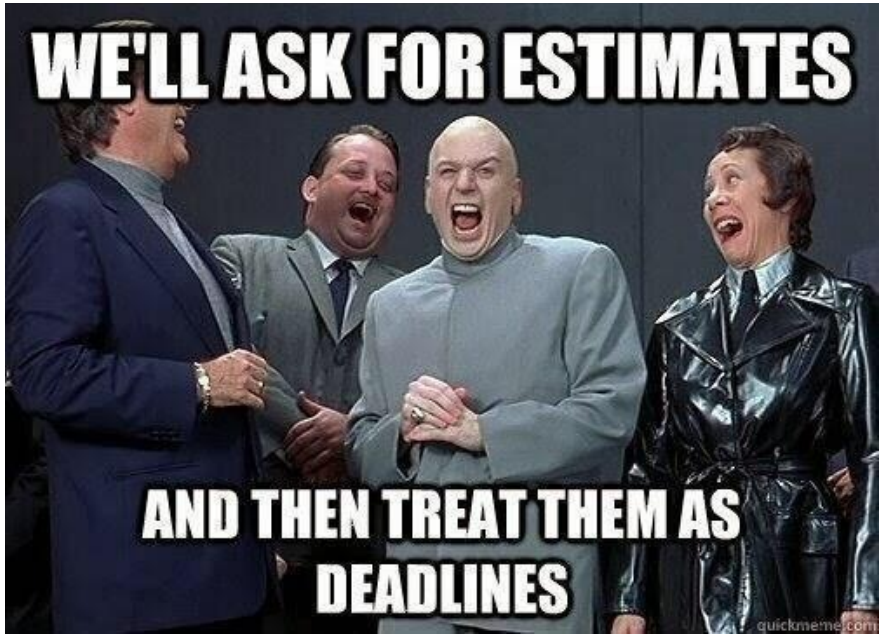
Sad because with all this we no longer have the ability to maintain the open source version.
We do plan on re-openning parts as time goes on and we also plan on offering our support to the community by way of various educational and researcher licenses.

REFRACTION POINT

- The Refraction Point team.

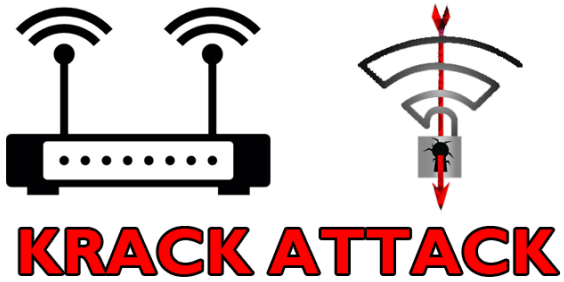
Why Don’t We Want To Use Open Source Tools?

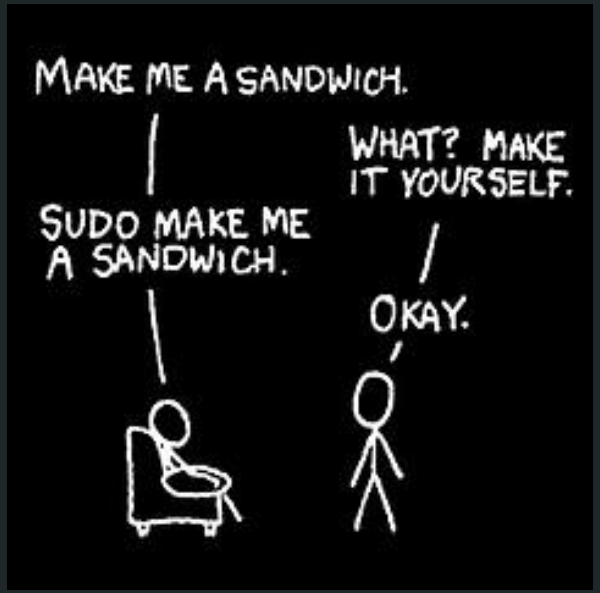
Time - It takes too much time and effort to implement and maintain open source solutions.



Why Don’t We Want To Use Open Source Tools?

Security - Open Source software is not as secure because so many people contribute and there is no commercial entities bottom line at stake





Why Do We Want To Use Open Source Security Tools?

Why Do We Want To Use Open Source Security Tools?

Price - They are free, compared to commercial tools that cost money.

Why Do We Want To Use Open Source Security Tools?

Save time - Rather than build a tool to solve one of my own problems, you can download one from the Internet.

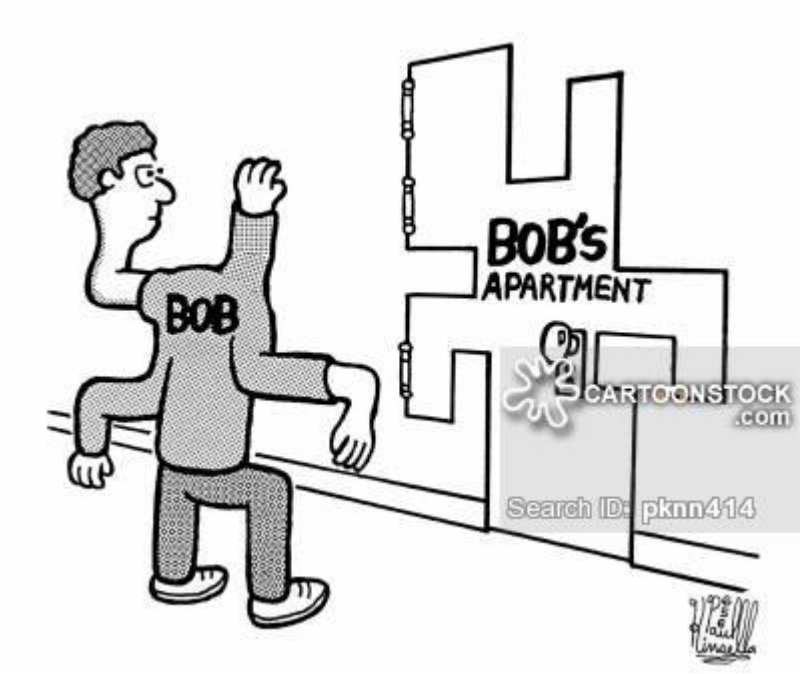
Why Do We Want To Use Open Source Security Tools?

Prototyping - I “think” I can solve a problem this way, but I want to try it first, without trying to learn and pay for a new commercial product.

Why Do We Want To Use Open Source Security Tools?

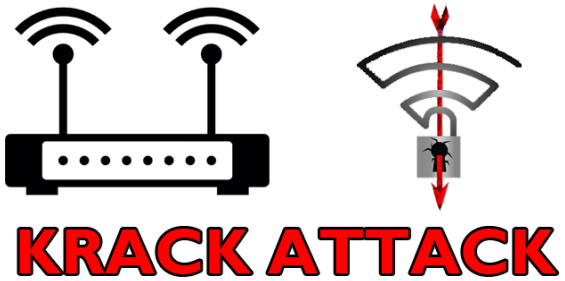
Customization - Since you have access to all the source code, you can customize it as you see fit.

Read your licenses!



Why Do We Want To Use Open Source Security Tools?

Security - So many people are looking at the code, there is no way a security bug could hide.

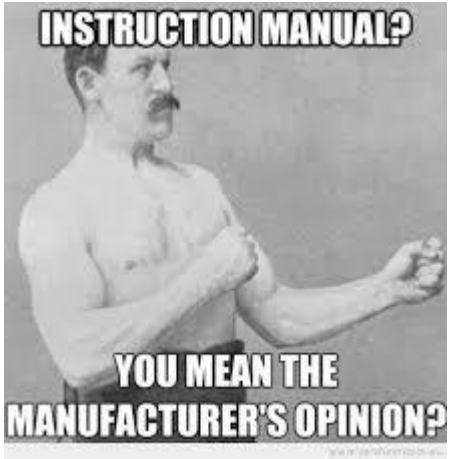


RTFM?

You can find a potential solution and get an idea of what it does and an overview of how it works, and even some installation instructions

You can easily find the most advanced query to detect the most advances types of attacks in your network

Everything in the middle is either missing, explained poorly, or covered in 6 different blog posts and StackOverflow posts on the Internet that you can only find by performing two dozen Google searches…



Examples of really good open source software for enterprise security (defense)

The Security Onion

Created by Doug Burks in 2008 as a dedicated Linux distribution for intrusion detection (Snort was very difficult to get compiled and running)

Today, The Security Onion has its own dedicated training and services company and a yearly conference.

Over 200,000 downloads as of 2015

The Security Onion

Analyst Tools

- Kibana
- CapME
- CyberChef
- Squert
- ELSA
- Sguil
- Xplico

Network Visibility

- NIDS
  - Snort
  - Suricata
- Bro
- Full Packet Capture

Host Visibility

- Beats
- OSSEC HIDS
- Sysmon
- Autoruns
- Syslog

Elastic Stack

- Elastic Stack
- Elastic Architecture
- Elasticsearch
- Logstash
- Kibana
- ElastAlert
- Curator
- FreqServer
- DomainStats
- Docker
- Redis
- Alpha to Beta
- Beta to RC1
- RC1 to RC2
- RC2 to RC3
- ELSA to Elastic
- Data Fields
- Beats

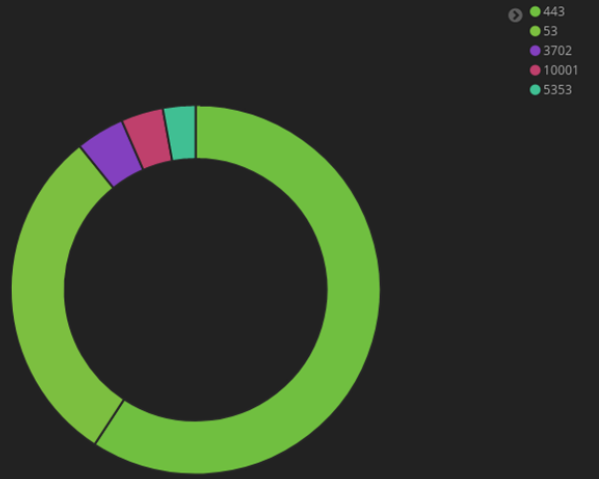
Connections - Destination IP Address

IP Address	Count
138.197.106.247	84,716
174.138.86.78	56,147
239.255.255.250	14,500
255.255.255.255	8,982
104.244.42.2	7,792
104.244.42.130	6,432
224.0.0.251	4,912
104.244.42.66	4,494
104.244.42.194	4,195
192.168.1.99	2,738

Export: Raw Formatted

1 2 3 4 5 ...10 »

Connections - Destination Port (Donut Chart)



Connections - Source Country

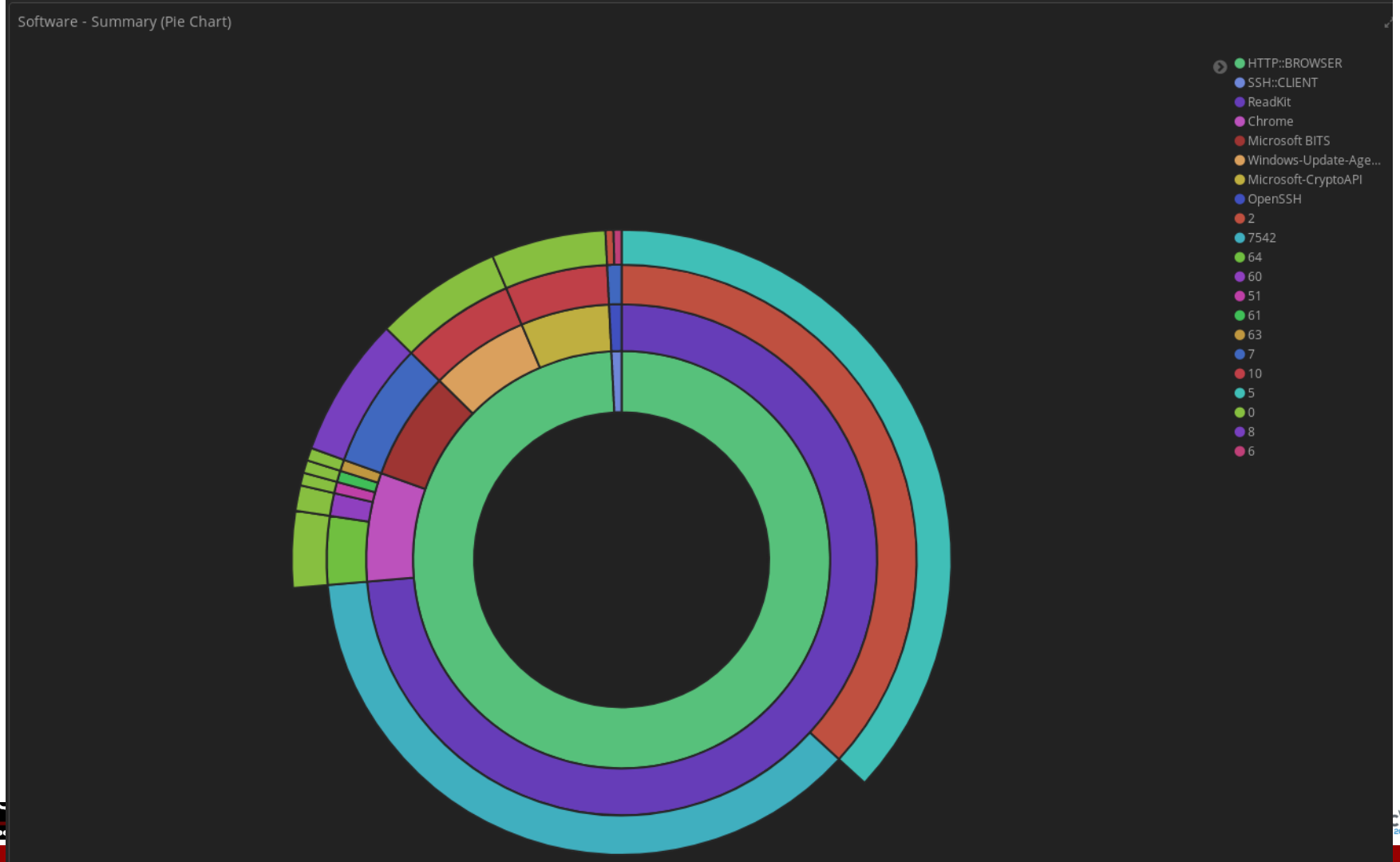
Country	Count
US	758
CA	117
RU	16
NZ	12
FR	11
GB	9
BR	6
UA	5
DE	4
PL	3

Connections - Responder Bytes

Responder Bytes	Count
467,205,433	1
457,609,838	1
344,702,256	1
327,894,882	1
326,768,695	1
319,102,502	1
237,940,936	1
235,794,967	1
227,383,801	1
216,960,904	1

Connections - Missed Bytes

Missed Bytes	Count
18,980	1
4,380	1
0	328,966


Software - Summary (Pie Chart)
HTTP::BROWSER
SSH::CLIENT
ReadKit
Chrome
Microsoft BITS
Windows-Update-Age...
Microsoft-CryptoAPI
OpenSSH
2
7542
64
60
51
61
63
7
10
5
0
8
6

1	1	1	[redacted]	20:53:03	ET POLICY Cleartext WordPress Login	2012843	6	0.071%

alert tcp any any -> any $HTTP_PORTS (msg:"ET POLICY Cleartext WordPress Login"; flow:established,to_server; content:"log="; http_client_body; content:"&pwd="; http_client_body; content:"&wp-submit="; http_client_body; metadata: former_category POLICY; classtype:policy-violation; sid:2012843; rev:2; metadata:affected_product Wordpress, affected_product Wordpress_Plugins, attack_target Web_Server, deployment Datacenter, tag Wordpress, signature_severity Audit, created_at 2011_05_25, updated_at 2017_10_12;)

file: **downloaded.rules:11244**

CATEGORIZE **0** EVENT(S) CREATE FILTER: src dst both

QUEUE	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DESTINATION	AGE	COUNTRY
1	[redacted]	2018-03-06 20:53:03	172.16.1.29	2	RFC1918 (.lo)	45.56.127.229	2	UNITED STATES (.us)

ST	TIMESTAMP	EVENT ID	SOURCE	PORT	DESTINATION	PORT	SIGNATURE
RT	2018-03-06 20:53:03	3.1271	172.16.1.29	60606	45.56.127.229	80	ET POLICY Cleartext WordPress Login

COMMENTS

None.

TAGS

None.

PAYLOAD

IP

VER	IHL	TOS	LENGTH	ID	FLAGS	OFFSET	TTL	CHECKSUM	PROTO
4	5	0	968	1602	2	0	128	38563	6

TCP

R1	R0	URG	ACK	PSH	RST	SYN	FIN	SEQ#	ACK#	OFFSET	RES	WIN	URP	CHECKSUM
0	0	0	1	1	0	0	0	895478132	2227358691	5	0	255	0	18023

HEX	ASCII
50 4F 53 54 20 2F 77 70 2D 6C 6F 67 69 6E 2E 70 68 70 20 48 54 54 50 2F 31 2E 31 0D 0A 48 6F 73 74 3A 20 73 65 63 75 72 65 64 69 67 69 74 61 6C 6C 69 66 65 2E 63 6F 6D 0D 0A 43 6F 6E 6E 65 63	POST /wp-login.p hp HTTP/1.1..Hos t: securedigital life.com..Connec

1	1	1		17:20:14	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 56	2403410	6	0.071%

alert tcp [62.97.242.146,62.99.69.72,62.99.70.47,62.99.76.10,62.99.76.97,62.99.77.193,62.99.79.180,63.135.14.182,63.135.171.99,63.141.239.66,63.143.113.42,63.245.122.93,63.251.114.119,63.251.226.151,64.145.19.218,64.187.167.174,64.204.93.82,64.32.15.181,64.66.28.14,64.66.29.16,65.103.190.218,65.124.192.170,65.154.57.107,65.175.204.208,65.181.54.27,65.183.153.161,65.189.217.153,65.24.235.86,65.27.164.80,65.38.2.180,65.78.159.216,65.99.169.173,66.111.41.250,66.111.41.251,66.111.41.252,66.111.57.16,66.111.57.45,66.111.57.50,66.118.142.171,66.165.223.206,66.169.58.201,66.185.198.180,66.186.182.234,66.186.70.214,66.188.180.148,66.191.6.71,66.206.35.98,66.206.39.125,66.214.194.55,66.215.24.210] any -> $HOME_NET any (msg:"ET CINS Active Threat Intelligence Poor Reputation IP TCP group 56"; flags:S; reference:url,www.cinsscore.com; reference:url,www.networkcloaking.com/cins; threshold: type limit, track by_src, seconds 3600, count 1; classtype:misc-attack; sid:2403410; rev:38912;)

file: **downloaded.rules:1630**

CATEGORIZE **0** EVENT(S) CREATE FILTER: src dst both

QUEUE	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DESTINATION	AGE	COUNTRY
1		2018-03-06 17:20:14	66.118.142.171	2	UNITED STATES (.us)	172.16.1.77	2	RFC1918 (.lo)

ST	TIMESTAMP	EVENT ID	SOURCE	PORT	DESTINATION	PORT	SIGNATURE
RT	2018-03-06 17:20:14	3.15	66.118.142.171	56393	172.16.1.77	80	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 56

COMMENTS

None.

TAGS

None.

PAYLOAD

	VER	IHL	TOS	LENGTH	ID	FLAGS	OFFSET	TTL	CHECKSUM	PROTO
IP	4	5	40	40	94	0	0	245	18123	6

	R1	R0	URG	ACK	PSH	RST	SYN	FIN	SEQ#	ACK#	OFFSET	RES	WIN	URP	CHECKSUM
TCP	0	0	0	0	0	0	1	0	1566210413	0	5	0	1024	0	31234

2	2	1		21:41:17	ET DROP Dshield Block Listed Source group 1	2402000	6	0.149%

alert tcp [196.52.43.0/24,191.101.167.0/24,5.188.86.0/24,181.214.87.0/24,77.72.82.0/24,212.92.127.0/24,77.72.85.0/24,85.93.20.0/24,80.82.77.0/24,180.97.106.0/24,5.188.11.0/24,89.248.168.0/24,146.0.77.0/24,89.38.99.0/24,125.212.217.0/24,208.100.26.0/24,5.188.10.0/24,141.212.122.0/24,148.153.35.0/24,58.218.213.0/24] any -> $HOME_NET any (msg:"ET DROP Dshield Block Listed Source group 1"; flags:S; reference:url,feeds.dshield.org/block.txt; threshold: type limit, track by_src, seconds 3600, count 1; classtype:misc-attack; flowbits:set,ET.Evil; flowbits:set,ET.DshieldIP; sid:2402000; rev:4739;)

file: **downloaded.rules:7435**

CATEGORIZE **0** EVENT(S) CREATE FILTER: src dst both

QUEUE	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DESTINATION	AGE	COUNTRY
1		2018-03-07 21:41:17	141.212.122.80	1	UNITED STATES (.us)	172.16.1.77	2	RFC1918 (.lo)

ST	TIMESTAMP	EVENT ID	SOURCE	PORT	DESTINATION	PORT	SIGNATURE
RT	2018-03-07 21:41:17	3.2619	141.212.122.80	51310	172.16.1.77	443	ET DROP Dshield Block Listed Source group 1

9	1	1	■	13:36:28	ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted	2006380	6	0.671%

alert tcp $HOME_NET any -> any $HTTP_PORTS (msg:"ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted"; flow:established,to_server; content:"|0d 0a|Authorization|3a 20|Basic"; nocase; http_header; content:!"YW5vbnltb3VzOg=="; within:32; http_header; threshold: type both, count 1, seconds 300, track by_src; reference:url,doc.emergingthreats.net/bin/view/Main/2006380; classtype:policy-violation; sid:2006380; rev:12; metadata:created_at 2010_07_30, updated_at 2010_07_30;)

file: **downloaded.rules:11045**

CATEGORIZE **0** EVENT(S) CREATE FILTER: src dst both

QUEUE	ACTIVITY	LAST EVENT	SOURCE	AGE	COUNTRY	DESTINATION	AGE	COUNTRY
9	■	2018-03-07 13:36:28	172.16.1.211	2	RFC1918 (.lo)	34.202.106.239	1	UNITED STATES (.us)

ST	TIMESTAMP	EVENT ID	SOURCE	PORT	DESTINATION	PORT	SIGNATURE
RT	2018-03-07 13:36:28	3.1771	172.16.1.211	50825	34.202.106.239	80	ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted
RT	2018-03-07 13:36:28	3.1772	172.16.1.211	50825	34.202.106.239	80	ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted
RT	2018-03-07 13:36:28	3.1773	172.16.1.211	50825	34.202.106.239	80	ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted
RT	2018-03-07 13:36:28	3.1774	172.16.1.211	50825	34.202.106.239	80	ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted

COMMENTS

None.

TAGS

None.

PAYLOAD

IP

VER	IHL	TOS	LENGTH	ID	FLAGS	OFFSET	TTL	CHECKSUM	PROTO
4	5	0	123	55839	0	0	128	9409	6

TCP

R1	R0	URG	ACK	PSH	RST	SYN	FIN	SEQ#	ACK#	OFFSET	RES	WIN	URP	CHECKSUM
0	0	0	1	1	0	0	0	4048888901	1952767463	5	0	33580	0	63032

DATA

HEX	ASCII
41 75 74 68 6F 72 69 7A 61 74 69 6F 6E 3A 20 42	Authorization: B
61 73 69 63 20 4E 54 41 34 59 32 49 78 4E 54 6B	asic NTA4Y2IxNTk
79 59 6D 46 6B 4F 6A 68 6A 59 6A 6B 7A 4D 6A 4E	yYmFkOjhjYjkzMjN
6B 4E 7A 51 33 4D 7A 41 30 4F 54 42 6A 4E 47 4A	kNzQ3MzA0OTBjNGJ
68 4E 57 55 77 4E 7A 67 33 5A 54 64 69 4D 54 45	hNWUwNzg3ZTdiMTE
31 0D 0A	1..

ASCII

```
Authorization: Basic NTA4Y2IxNTkyYmFkOjhjYjkzMjNkNzQ3MzA0OTBjNGJhNWUwNzg3ZTdiMTE1..
```

RITA - (Real Intelligence Threat Analytics)

Analyzes Bro logs to determine which hosts in your environment have been compromised

Looks for “phone home” traffic patterns, using fancy math (Connection interval, packet size, connection time and connection length are analyzed)

Attaches a score to each host, indicating the probability it is compromised

Get it free here: https://github.com/ocmdev/rita

Works with The Security Onion (stable version, instructions here: https://github.com/Security-Onion-Solutions/security-onion/wiki/RITA)

(Supported by Active Countermeasures, from myself and John Strand)

Similar Projects

Graylog (https://www.graylog.org/) - Open source and free for 5Gb/day of log collection, commercial support available

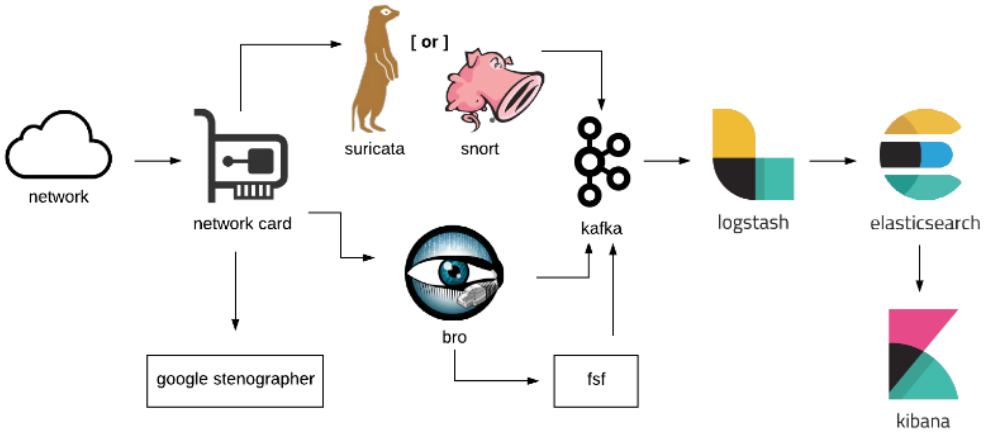
RockNSM (http://rocknsm.io/) - *"Response Operation Collection Kit (ROCK) is a collections platform, in the spirit of Network Security Monitoring, designed by members of the Missouri National Guard's Cyber Team."*

OSSIM (https://www.alienvault.com/products/ossim) - *"AlienVault® OSSIM™, Open Source Security Information and Event Management (SIEM), provides you with a feature-rich open source SIEM complete with event collection, normalization and correlation."*

ROCK NSM

(Response Operation Collection Kit)

MOCYBER's open source Network Security Monitoring platform.



Attack Simulation

Caldera (https://github.com/mitre/caldera) - From MITRE

Metta (https://github.com/uber-common/metta) - Chris Gates

Atomic Red Team (https://github.com/redcanaryco/atomic-red-team) - Red Canary research

The MITRE ATT&K Framework: https://attack.mitre.org

DNS Blacklisting

PI-Hole (https://pi-hole.net) - DNS blacklisting ad and malware domains

Originally designed for Raspberry PIs, I put mine in the cloud

They run so well, I forget they are there!

Add TachyonNet to resolve bad domains to a real server and collect traffic (http://bit.ly/TachyonNet)

Technical How-To Segment: https://wiki.securityweekly.com/Episode507#Tech_Segment:_Blocking_Ads_and_Malware_With_Pi-hole_In_The_Cloud_-_7:00PM-7:30PM

vFeed - Free, like Free Beer (not speech)

Oh look, a vulnerability!

What is the severity?

What does Debian refer to it as?

Is there an exploit for it?

What other platforms contain the same vulnerability?

(You can automate the discovery of all above questions for free, non-commercial use, with vFeed)

$ **./vfeedcli.py -e json_dump CVE-2016-3074**


```
{
  "exploits": {
    "edb": [
      {
        "file": "platforms/linux/remote/39736.txt",
        "id": 39736,
        "url": "http://www.exploit-db.com/exploits/39736"
      }
    ],
    "elliot D2": null,
    "metasploit": null,
    "saint": null
  },
  "information": {
    "capec": null,
    "category": null,
    "cpe": [
      {
        "id": "cpe:/a:libgd:libgd:2.1.1"
      },
      {
        "id": "cpe:/o:debian:debian_linux:8.0"
      },
      {
        "id": "cpe:/o:debian:debian_linux:7.0"
      }
    ],
    "cve": [
      {
        "id": "CVE-2016-3074",
        "modified": "2017-06-30T21:29:41.920-04:00",
        "published": "2016-04-26T10:59:01.207-04:00",
        "summary": "Integer signedness error in GD Graphics Library 2.1.1 (aka
service (crash) or potentially execute arbitrary code via crafted compressed g
        "url": "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3074"
      }
```

OpnSense

Started as a fork of pfSense® and m0n0wall in 2014, first official release in January 2015.

Why not pfSense? Here's why:

"*While we're not revealing the extent of our plans, we do want to give early notice that, in order to support the increased cryptographic loads that we see as part of pfSense version 2.5, pfSense Community Edition version 2.5 will include a requirement that the CPU supports AES-NI.*"

https://www.netgate.com/blog/pfsense-2-5-and-aes-ni.html

OPNSense on one of these = awesome

Roll over image to zoom in

Qotom

Qotom Q190G4-S01 w/ 4G RAM 32G SSD, Industrial PC Gateway Firewall Router for pfSense, Intel Celeron J1900, 4 Gigabit LAN

13 customer reviews | 12 answered questions

Available from these sellers.

Size: **4G RAM 32G SSD**

2G RAM 16G SSD WIFI	2G RAM 32G SSD	2G RAM 32G SSD WIFI	4G RAM 16G SSD WIFI
4G RAM 32G SSD	4G RAM 64G SSD	8G RAM 16G SSD WIFI	8G RAM 32G SSD
8G RAM 32G SSD WIFI	8G RAM 64G SSD	8G RAM 64G SSD WIFI	8G RAM 128G SSD
8G RAM 128G SSD WIFI			

- Supports pfSense (up to v2.4.x) / Linux distros / Windows 7,8,10.
- 4GB RAM, 32GB SSD pre-installed, No WiFi.
- Intel Celeron Processor J1900 (Quad-Core 2M Cache, 2 GHz, up to 2.41 GHz).
- Can be configured as a firewall, LAN or WAN router, VPN appliance, DHCP Server, DNS Server, and IDS/IPS with optional packages to deliver a high performance, high throughput front-line security.
- 4 Intel Gigabit LAN, VGA, 3x USB 2.0 ports, 1x USB 3.0 port.

› See more product details

New (1) from $184.00 + $29.24 shipping

Security | Compliance | DevOps

Kolide Fleet + osquery

Facebook open source project (osquery), ask questions of your operating system

Kolide Fleet is an open-source management platform

Curious to test OSSEC + Security Onion vs Kolide

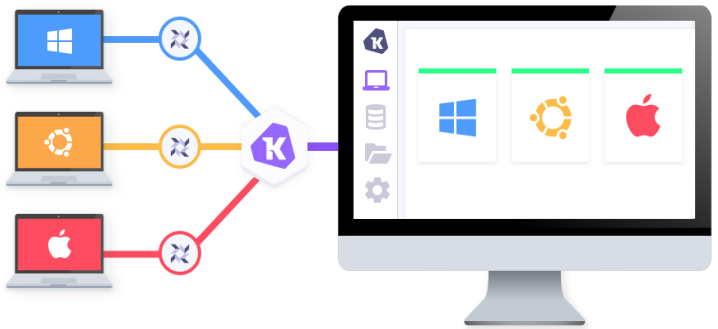
```
osquery> SELECT name, path, pid FROM processes WHERE on_disk = 0;
name = Drop_Agent
path = /Users/jim/bin/dropage
pid = 561
```

Processes running without a binary on disk

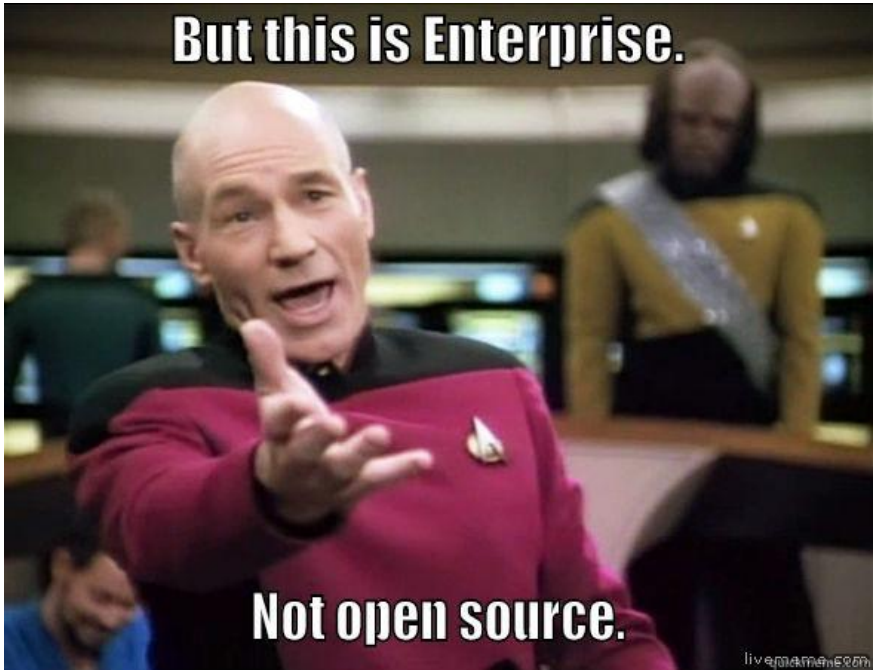
Frequently, attackers will leave a malicious process running but delete the original binary on disk. This query returns any process whose original binary has been deleted or modified (which could be an indicator of a suspicious process).

Kolide Fleet

Open Source Osquery Manager



End



Special thanks to Michael Santarcangelo, Dave Aitel, KT, the Security Weekly staff, Joff Thyer, Doug White, @kevvyg, my Twitter followers, some random infosec people on Facebook, and everyone else I forgot...

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Paul Asadoorian
Founder & CEO
Security Weekly