

# Defense on a Budget: Tips & Tricks for Improving Security

Robert Wagner

@mr\_minion



- 20+ years of IT & Security experience
  - SOC Analyst
  - Security Engineer / Architect
- Hak4Kidz Co-Founder
- BurbSec Co-Organizer
- BurbSecCon Co-Organizer
- @mr\_minion
- My opinions are my own or those of other researchers, and do not necessarily reflect the opinions of my company.

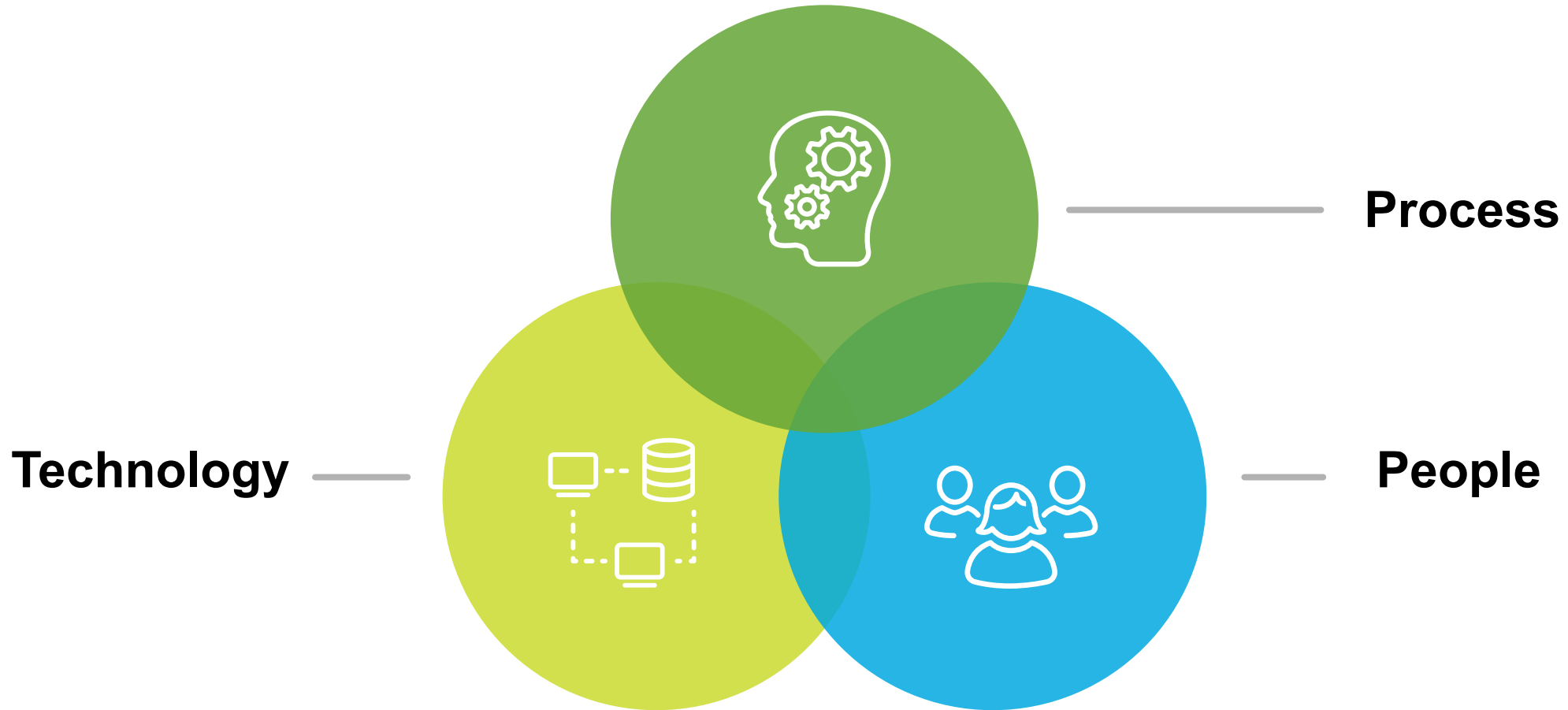
Many thanks to Mike Poor, Ed Skoudis, Mubix, Dave Kennedy, Danny Harris, Ben0xA, Ryan Kova, Dave Herrald, et al

# • THE PROBLEM

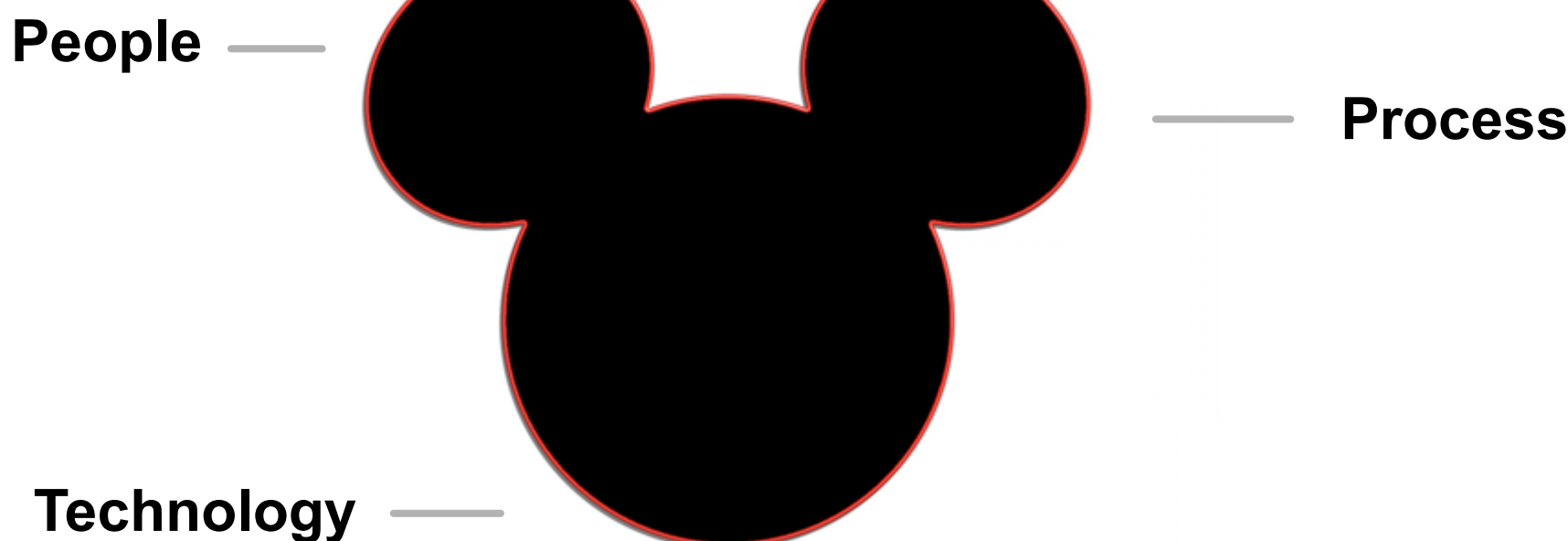
- There's never enough security budget to buy everything we want
- We all need easy, free, or cheap ways to fill our security gaps
- The best place to start is with your most important security tool...

• YOU!!

# Three Interrelated Components of Security



# Too Much Focus on Technology



# Info from Hackers & Researchers

- Free videos online from Defcon, DerbyCon, ShmooCon, TorCon, and others
- Bsides & HackerCons – Bsides Calgary, Edmonton, Vancouver, The Long Con (Winnipeg) etc.
  - There's one in almost every major city
  - They are usually free or cheap!
  - More CISOs and Security Managers are going
- Chicago's BurbSec style meetups – burbsec.com
- InfoSec Taylor Swift @SwiftOnSecurity – <https://DecentSecurity.com>
- @hacks4pancakes -- <https://tisiphone.net/>

# Start Security Contests in Your Company

- Who can report the most security issues
  - Phishing email
  - Workstations behaving strangely
  - Strangers roaming the halls without badges
- Winner gets \$100? \$200?
- Turns your users into Intrusion Detection Systems!
  - Thanks to Ben0xA for this one!

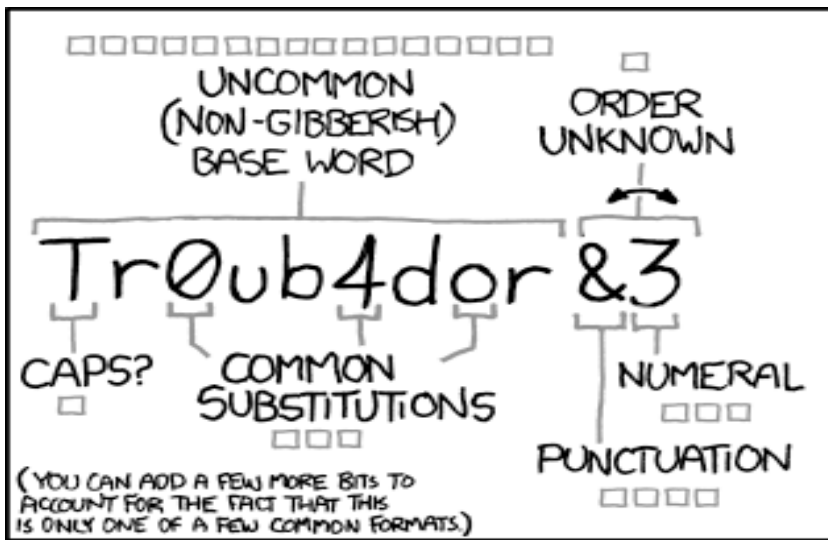
# EMET (Enhanced Mitigation Experience Toolkit)

- Protect the memory of Apps you designate
- Yes, it can be hard to deploy
- Yes, there are bypasses
- Yes, it's EOL in July 2018 – Will you be on Win 10?
- But you've reduced the number of tools an attacker can use
- You've made it much harder for an attacker to win



# Passwords and Password Managers





~28 BITS OF ENTROPY


$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

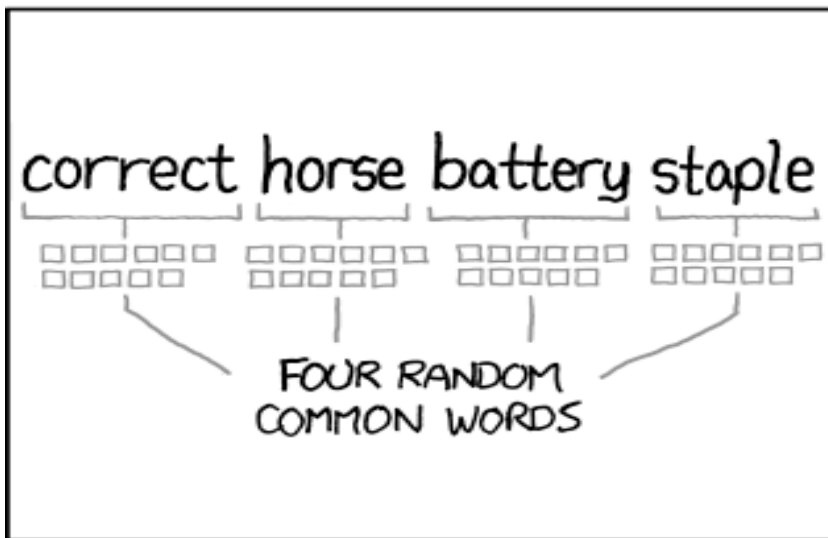
DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...



DIFFICULTY TO REMEMBER: **HARD**




~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!



DIFFICULTY TO REMEMBER: **YOU'VE ALREADY MEMORIZED IT**

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

- KeePass is FREE!

# JAVA Problems?

- Pull your proxy logs and get the list of versions
- The version is in the user agent string
  - e.g. Java/1.6.0\_26
- Block JAVA user agent string at the gateway
- At the very least, block the out of date versions
- Do you really need JAVA going to the outside for more than a few sites?

# Block Extensions at the Email Gateway

- Just do it. Please.
- .386, .ace, .acm, .acv, .ade, .adp, .adt, .ani, .app, .arc, .arj, .asd, .asp, .asx, .avb, .ax, .bas, .bat, .bin, .boo, .btm, .cab, .cbt, .cdr, .cer, .chm, .cla, .cmd, .cnt, .cnv, .com, .cpl, .crt, .csc, .csh, .css, .der, .dll, .drv, .dvb, .email, .exe, .fon, .fxp, .gadget, .gms, .grp, .gvb, .hlp, .hpj, .ht, .HTA, .http, .htt, .inf, .ini, .ins, .iso, .isp, .its, .jar, .jnlp, .job, .js, .jse, .ksh, .lib, .lnk, .mad, .maf, .mag, .mam, .maq, .mar, .mas, .mat, .mau, .mav, .maw, .mcf, .mch, .mda, .mdb, .mde, .mdt, .mdw, .mdz, .mht, .mhtm, .mhtml, .mpd, .mpt, .msc, .msh, .msh1, .msh1xml, .msh2, .msh2xml, .mshxml, .MSI, .mso, .msp, .mst, .nws, .obd, .obj, .obt, .obz, .ocx, .ops, .osd, .ovl, .ovr, .pcd, .pci, .perl, .pgm, .pif, .pl, .plg, .pot, .prf, .prg, .ps1, .ps1xml, .ps2, .ps2xml, .psc1, .psc2, .pst, .pub, .pwz, .qpw, .reg, .sbf, .scf, .scr, .sct, .sfx, .sh, .shb, .shs, .shtml, .shw, .smm, .svg, .sys, .td0, .tlb, .tmp, .torrent, .tsk, .tsp, .tt6, .url, .vb, .vbe, .vbp, .vbs, .vbscript, .vbx, .vom, .vsd, .vsmacro, .vsmacros, .vss, .vst, .vsw, .vwp, .vxd, .vxe, .wbk, .wbt, .wiz, .wk, .wml, .wms, .wpc, .wpd, .ws, .wsc, .wsf, .wsh, .xbap, .xll, .xnk
- <https://blueteamer.blogspot.com/2017/05/file-extensions-to-block-at-email.html>

# AntiVirus

- Not completely useless
- Can be used to search for IOCs
- Heuristics still find some malicious code – do you have it enabled?
- Is anyone checking the AV alerts?



# Lay down some Land Mines

- Honey Files
  - Files with names like "Password List"
  - Alert on access
- Honey Accounts
  - DomainAdmin\_x
    - ▶ Put the "password" in the description
  - Put in admins group
  - Logon hours = 0

# More Landmines

- Honey Database / Honey Tables
- Honey Tokens
  - Use CreateProcessWithLogonW
    - ▶ Free tool: <https://github.com/FuzzySecurity/Powershell-Suite/blob/master/Invoke-Runas.ps1>
    - ▶ Load fake admin account & fake credentials into memory
    - ▶ Alert on use

# Stop Attackers in their Tracks

- Use a web form to authenticate to the proxy
  - Even go so far as asking users to allow a site – 1/day or week
- WPAD Vulnerability Mitigation
  - Make a null routed DNS entry (127.0.0.1) for WPAD
  - Make a null routed (::1) DNS entry for WPADWPADWPAD
  - Disable NetBIOS
- Disable DNS internally for external names space
  - let the proxies handle external dns lookups
  - Turn off forward lookups on internal dns servers
  - Point proxies at DNS servers that only they are allowed to

use



# More Roadblocks

- Local Administrator Password Solution (LAPS)
  - Randomizes local admin password
- Deny access to this computer from the network
  - Computer Configuration\WindowsSettings\Security Settings\Local Policies\User Rights Assignment
  - Apply to local admin group



# Pass the Hash Detection

- index="wineventlog" ( EventCode=4624 Logon\_Type=3 )  
OR ( EventCode=4625 Logon\_Type=3 )  
Authentication\_Package="NTLM" NOT  
Account\_Domain=YOURDOMAIN NOT  
Account\_Name="ANONYMOUS LOGON"

# Finding Unauthorized DNS

## Using Stream, Bro, Tag

- `index=stream sourcetype=stream:dns dest_port=53 dest_ip!=10.0.0.0/8 | stats count by dest_ip`
- `index=bro sourcetype=bro_dns dest_port=53 dest_ip!=10.0.0.0/8 | stats count by dest_ip tag=dns dest_port=53 dest_ip!=10.0.0.0/8 | stats count by dest_ip`
- `tag=dns dest_port=53 dest_ip!=10.0.0.0/8 | stats count by dest_ip`

## ● Finding DNS Spoofing Activity

- `index=bro sourcetype=bro_weird name=dns_unmatched_reply dest_port=53 | stats count by src_ip dest_ip`

## ● Finding clients connecting to multiple DNS servers

- `tag=dns dest_port=53 dest_ip!=10.0.0.0/8 |bucket _9me span=1s | stats VALUES(dest_ip) AS IP_List dc(dest_ip) AS dis9nct by _9me src_ip | search dis9nct > 2 | table src_ip IP_List dis9nct`

# Finding Extremely Long DNS Queries

- Requires the URL Toolbox and Bro
  - <https://splunkbase.splunk.com/app/2734/>
- Queries Over 2 Standard Deviations
  - `sourcetype=bro_dns | eval len=len(query) | eventstats stdev(len) AS stdev avg(len) AS avg p50(len) AS p50 | eval length=len(query) | where length>(stdev*2) | stats count by length stdev avg p50 qtype_name query | sort -length`
- Queries Over 200 Characters Long
  - `sourcetype=bro_dns | `ut_parse(query)` | eval length=len(query) | search length>200 | stats count by query`

# Queries with High Entropy

- The measure of randomness in a variable
  - The higher the randomness, the higher the measure
  - “Shannon” entropy is most commonly used, but there are different calculations of entropy
- Example: – google.com
  - Shannon Entropy score of 2.6 (low)
  - A00wlkj—(-a.aslkn-C.a.2.sk.esasdfasf1111)-890209uC.4.com
    - ▶ Shannon Entropy score of 4.28 (high)

# More Queries with High Entropy

- Domains with High Entropy
  - `sourcetype=bro_dns | `ut_parse(query)` | lookup FP_entropy_domains domain AS ut_domain | search NOT FP_entropy=* | `ut_shannon(ut_domain)` | search ut_shannon > 4.0 | stats count by query ut_shannon`
- Subdomains with High Entropy
  - `sourcetype=bro_dns | `ut_parse(query)` | lookup FP_entropy_domains domain AS ut_domain | search NOT FP_entropy=* | `ut_shannon(ut_subdomain)` | search ut_shannon > 4.5 | stats count by query ut_shannon`
- Don't forget to filter out CDNs, etc.



New Search

Save As ▾ Close

sourcetype=bro\_dns | `ut\_parse(query)` | lookup FP\_entropy\_domains domain AS ut\_domain | search NOT FP\_entropy=\* | `ut\_shannon(ut\_domain)` | stats count by query ut\_shannon

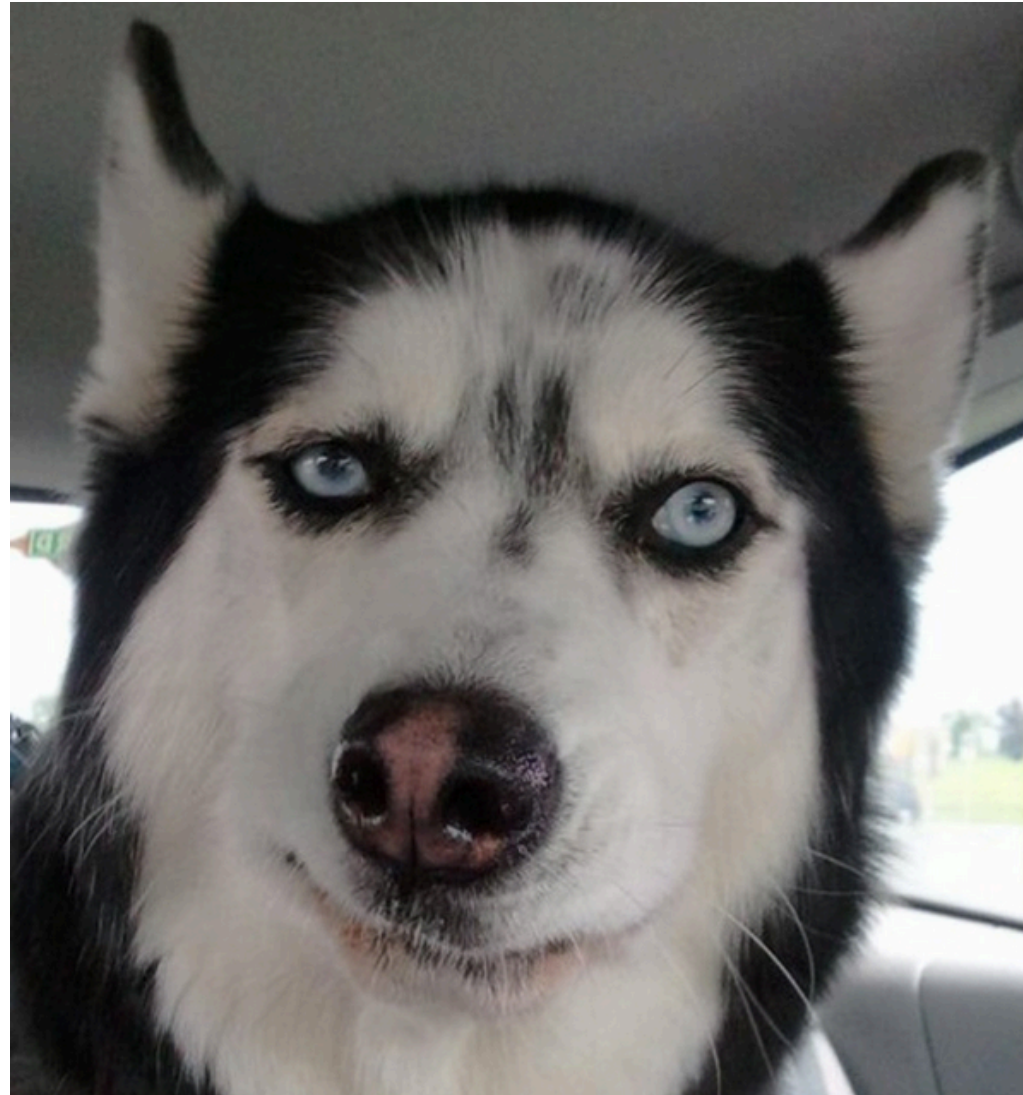
All time ▾ 🔍

✓ 1,621,137 events (before 9/19/15 7:19:31.000 PM)

Job ▾ || ▢ ↗ ⬇ 📄 ⚡ Smart Mode ▾

query ↕	ut_shannon ▾	count ↕
3wirqs5imc.vi9y6kmcksy7xw2rf8e4klb3t.com	4.487122805397798	1
jq94wtm6-vlo9i-a8cdvu4.dti9613wn-lsvbnrgsv3vj0ya.com	4.487122805397798	1
4k4hck0sxe1a4-auxgo67jq-.emy2egline26ztbhlpad7831i.com	4.487122805397797	1
qzpt2o7szq9j4v-rregr.2fzni4p95jvmcwyhbmd7oguzn62.com	4.478232197413861	1
twcn95gmh8aepzl.d4m2kss4mazxbvjy-en9c57f7qy.com	4.478232197413861	1
rdlb2pgcy-zxgnyqpqe.ivczg0s1w4brp-yd5vnu9g.com	4.469670487371861	1
uew0t1ytlmyirhci1.cspexioh91r0qyalid-oxqsftnjq.com	4.453880987666651	1
movhbu4du3nd0g1umrz575d.1q950idlpnkeus2-zrfii.com	4.453660689688184	1

# Free Fun with Algorithms?



# Here's How

- **“R”**
  - r-project.org
- **Scientific Computing Tools for Python – SciPy**
  - SciPy.org
  - <https://matplotlib.org/>
- **Free Splunk Developers License**
  - [https://www.splunk.com/en\\_us/resources/personalized-dev-test-licenses.html](https://www.splunk.com/en_us/resources/personalized-dev-test-licenses.html)
  - Machine Learning Toolkit: <https://splunkbase.splunk.com/app/2890/>



Centers for Medicare &amp; Medicaid Services

type search term here

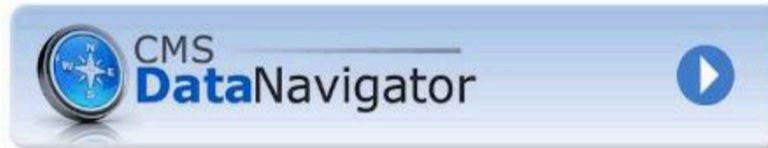
Search

Medicare

Medicaid/CHIP

Medicare-Medicaid  
CoordinationPrivate  
InsuranceInnovation  
CenterRegulations &  
GuidanceResearch, Statistics,  
Data & SystemsOutreach &  
Education

## Research, Statistics, Data & Systems



### CMS Information Technology

[Access to CMS Data & Application](#)[Agile Transformation](#)[Blue Button 2.0](#)[CIO Resource Library](#)[Data Administration](#)[Database Administration](#)[Division of Identity Management Enterprise Systems \(EIDM\)](#)[Earned Value Management](#)[Enterprise Architecture](#)[Enterprise IT Investment Management](#)[HIPAA Eligibility Transaction System \(HETS\) Help \(270/271\)](#)[Information Security](#)

### Monitoring Programs

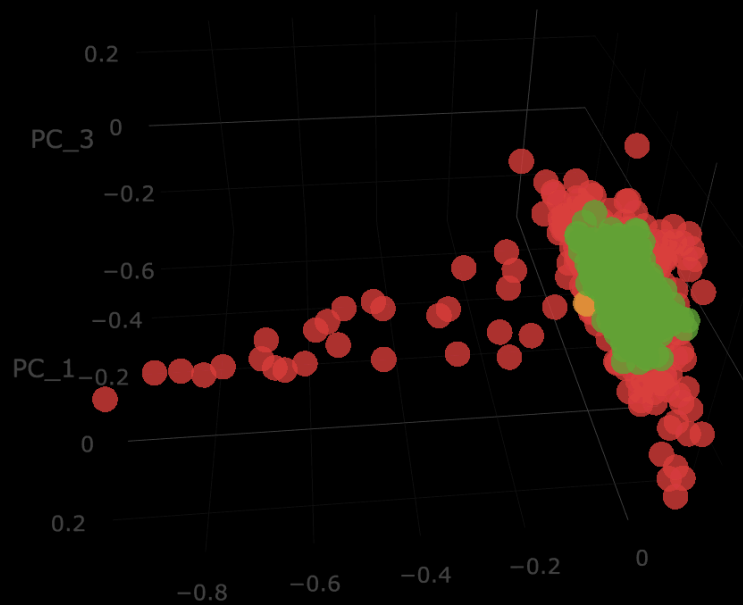
[Medicaid and CHIP Compliance](#)[Medicare Fee-for-Service Compliance Programs](#)[Medicare Risk Adjustment Data Validation Program](#)[Part C and Part D Program Integrity Program](#)[Parts C and D Recovery Audit Program](#)[Qualified Entity Program](#)

### Research

[Actuarial Studies](#)[Alliance to Modernize Healthcare FFRDC](#)[Consumer Assessment of Healthcare Providers & Systems \(CAHPS\)](#)[Consumer Research](#)

## CMS news

[Fact Sheet: Data on 2019 Individual Health Insurance Market Conditions](#)[Press Release: Premiums on the Federally-facilitated Exchanges drop in 2019](#)[Press Release: CMS Takes Steps to help with Hurricane Michael Emergency Response](#)[Press Release: Medicare provides continued access to high-quality health coverage choices in 2019](#)[Press Release: CMS Announces Participants in New Value-Based Bundled Payment Model](#)[View more news & links](#)

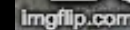


- cluster: Opioid anomalies (463)
- cluster: Other anomalies (2)
- cluster: Typical providers (356)

	PC_1	PC_2	PC_3	Specialty	NPI	Provider	City	State	anomaly_ratio	Opioids_pct	Opioids_tot	Total Claims	Drug:OXYCONTIN	Drug:SUBSYS	Drug:SUBOXONE
1	0.0845	-0.4587	-0.0027	Interventional Pain Management	1801819206	BART GATZ	GREENACRES	FL	48.90	90.52	3,280,572.48	3,624,144.95	4.645293	43.5893308	0.6234878
2	-0.0130	-0.3161	-0.0388	Interventional Pain Management	1053372201	JOHN COUCH	MOBILE	AL	34.53	85.66	2,068,677.68	2,415,055.88	15.565967	32.025406	
3	0.0770	-0.5361	-0.0354	Interventional Pain Management	1558353078	ALEXANDER WEINGARTEN	SYOSSET	NY	56.61	76.69	1,907,121.55	2,486,688.24	7.566583	53.4179862	0.203226







# Thank You

Robert Wagner

[rwagner@splunk.com](mailto:rwagner@splunk.com)

<https://www.linkedin.com/in/robertwagner2/>

This presentation available upon request

**splunk**>

Many thanks to