I <3 logs!

system logs

mail logs

web logs

vpn logs
Log Bongzilla, aka Splunk

Is this how Octocat came to be?

Logs go in…

security alerts

come out
YO DAWG, I HERD YOU LIKE LOGS

SO I PUT SOME LOGS IN YOUR LOGS
SO YOU CAN SPLUNK WHILE YOU SPLUNK
sudo make me a sandwich
Know your patterns.

VPN Connections

July 4th was a Wednesday

People slacking off early on a Friday, eh?

People making up for last week?
That was unexpected...
Etsy XSS detection

Announcement of Bug Bounty program: http://is.gd/UTZ5wD

code push to address reported vulnerabilities
Geolocate all the things!
13 minutes after we announced our security bug bounty program
http://is.gd/UTZ5wD

Method: POST
URL: /your/profile
Data: u"fb_avatar_url=&gender=female&city3=&new_city="
"<img src=x onerror=prompt(1);>&new_region=&new_countrycode=&new_latlon=,&city3_dup="<img src=x’
Etsy

SQLi detection

IP : 216.185.114.219 – unknown

Geolocation : Jurong East, 00, SG

Whois : ThePlanet.com Internet Services, Inc., ARIN, NET216

Requests : 20

Method : GET

URL : /listing/102946830/womens-shirt-beige-tunic-womens-blouse?ref=999999.9%27+union+all+select+0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536%2C0x31303235343830303536+and+%27x%27%3D%27x

Method : GET

URL : /category/furniture?page=499999%27%20union%20select%20unhex(hex(version()))%20

[...]
Etsy

Know when people can’t log in...

Logins (top), Login Errors (bottom)

Closed Account

Wrong Password

Invalid Username

Invalid Email
High number of failed logins

Admin : <username> (<internal login>, <site login>)
IP : 64.124.192.210 - 64.124.192.210.t01419-07.above.net
Geolocation : Brooklyn, NY, US
Whois : ETSY Inc, ARIN, NET64
# of failed logins : 13

Admin : jschauma (jschauma, jschauma)
IP : 207.38.139.33 - 207-38-139-33.c3-0.avec-ubr2.nyr-avec.ny.cable.rcn.com
Geolocation : New York, United States
Whois : RCN Corporation, ARIN, NET207
# of failed logins : 16

doesn’t know what he’s doing; do not trust!
Geolocate all the things!
“Unexpected” login detection

Admin : <username> (<internal login>, <site login>)
IP : 83.160.48.31 - a83-160-48-31.adsl.xs4all.nl
Geolocation : Rotterdam, 11, NL
Whois : XS4ALL Internet BV, RIPE, DEMON-NL-DSL

Admin : <username> (<internal login>, <site login>)
IP : 217.192.56.102 – unknown
Geolocation : Zurich, 25, CH
Whois : The Hub Zuerich Assoc., RIPE, THE-HUB-ZUERICH-NET

Admin : <username> (<internal login>, <site login>)
IP : 24.231.49.240 - unknown
Geolocation : Nassau, 23, BS
Whois : Cable Bahamas, ARIN, CABLEBAHAMAS-NET

Admin : <username> (<internal login>, <site login>)
IP : 200.49.191.120 - map120.network49.191.tigo.net.gt
Geolocation : Guatemala City, 07, GT
Whois : COMCEL GUATEMALA S.A., LACNIC
I said: “Please insert girder!”
Admin : <username> (<internal login>, <site login>)
IP : 50.17.73.70 - ec2-50-17-73-70.compute-1.amazonaws.com
Geolocation : Ashburn, VA, US
Whois : Amazon.com, Inc., ARIN, NET50
Provider : Amazon AWS
Count : 7

Admin : <username> (<internal login>, <site login>)
IP : 207.228.237.110 – unknown
Geolocation : New York, NY, US
Whois : HopOne Internet Corporation, ARIN, NET207
Provider : HopOne
Count : 1
source="info.log" reCAPTCHA status="incorrect" | transaction ip | \ where eventcount > 50 | table ip,eventcount | sort -eventcount
wtf happened here?

Ooh, right... this:
http://is.gd/fognju
http://is.gd/OhRDLY
http://is.gd/WxcAOr
Log it now, log it all.
Geolocate all the things.
Build profiles. (Creepy, I know.)
Reduce false positives. (Whitelists!)
Have defined reactions to all alerts.
Notice the outliers. Explain them.

That’s all, folks! Thanks!