

# Captain's Log: Take your application log analysis from Starfleet to Star Fleek

Ryan Tomcik

David Pany

SANS DFIR 2020


July 16, 2020

1:30 EDT


# Introductions



- Ryan Tomcik
  - Senior Consultant – Mandiant IR
  - Background in Splunk use for monitoring and log analysis

 @heferyzan

- David Pany
  - Manager – Mandiant IR
  - Background in Excel/grep log analysis

 @davidpany

- Co-Creators of **DFUR**

# Dog and Feline Urgent Response

- Long standing organization in the pet wellness industry
- Veterinarians use DFUR to process records, make appointments, and order care
- Pets use DFUR to make appointments, pay bills, and see results
- Insurers use DFUR to receive and pay claims to veterinarians
- Starfleet's official veterinary service as of Stardate 74005.8
- DFUR infosec recently took a look at their log sources - ouch

**DFUR**

# Logging Problems Identified – Full List

- Incomplete data sources.
- Fields parsed to the wrong index.
- Application updates messed up SIEM ingestion.
- Data spread across multiple sources.
- Barely anything centralized.
- Time zone misconfigurations.
- The logs are in AM/PM format
- The time zones are not specified or documented anywhere
- Meow
- Takes forever to export.
- Some logs retained for only minutes.
- Source IP addresses masked by proxy.
- Some Logs are text sources.
- Tiny text here.
- This is some really tiny text.
- How small can we make this text?
- What if someone zooms in on this text?
- They will find that this slide is a fraud.
- Hopefully it makes people giggle at least.
- That is really why we are here.
- Tweet.
- Trying to get chuckles is the ultimate goal for a forensicator.
- I hope audience members find our log presentation relevant.
- If we need to fill time we can come back to this slide and read everything.
- Some organizations do have pretty great logging.
- Paper Mario comes out tomorrow, that should be fun to play.
- Okay the font size just started shrinking.
- Another small text here.
- The point of this slide is to show that DFIR has lots of work to do for logging practices
- We're run by cats and dogs though so using a keyboard is really difficult.
- Woof.
- I'm still typing trying to make an example of how many logging problems an organization can have.
- Maybe we should tell a funny pet story here?
- I've only ever seen database transaction logging turned on in one investigation and it was really useful.
- No one ever seems to have NetFlow logs but firewall logs are pretty much just as useful for external log sources
- Ryan will probably make us get rid of this slide
- Font size 8 seems small enough to get away with this realistically.
- If this were blown up on a huge stage though, it might be really hard to read
- Chirp.
- Nothing is worse than a flat text log file where entries are broken up across multiple lines.
- Sometimes log data is stored in 2 separate database tables with no identifier to correlate them.
- The logs were made by the application developers in python 2.7 which is now officially deprecated
- The logs don't contain anything useful
- Some logs have the months spelled out instead of a number

DFUR

# Logging Problems Identified – High Level

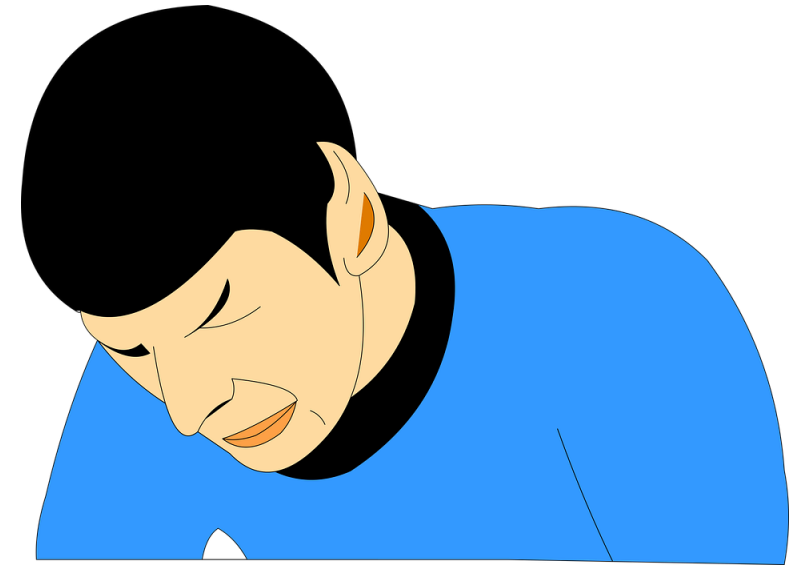
- Incomplete data sources
- Fields parsed to the wrong indices
- Application updates messed up SIEM ingestion
- Time zone misconfigurations
- Takes forever to export
- Source IP addresses masked by proxy



**DFUR**

# Analysis Problems

- Inconsistency during manual analysis (playbooks)
- No documentation of log fields
- Application logs were designed for troubleshooting, not investigating



**DFUR**

# Examples of Facepalm Logs

```

javax.servlet.ServletException: java.lang.NullPointerException
org.apache.shiro.web.servlet.AdviceFilter.cleanup(AdviceFilter.java:196)
org.apache.shiro.web.filter.authc.AuthenticatingFilter.cleanup(AuthenticatingFilter.java:155)
org.apache.shiro.web.servlet.AdviceFilter.doFilterInternal(AdviceFilter.java:148)
org.apache.shiro.web.servlet.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:125)
org.apache.shiro.web.servlet.ProxyedFilterChain.doFilter(ProxyedFilterChain.java:66)
org.apache.shiro.web.servlet.AdviceFilter.executeChain(AdviceFilter.java:108)
org.apache.shiro.web.servlet.AdviceFilter.doFilterInternal(AdviceFilter.java:137)
org.apache.shiro.web.servlet.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:125)
org.apache.shiro.web.servlet.ProxyedFilterChain.doFilter(ProxyedFilterChain.java:66)
org.apache.shiro.web.servlet.AbstractShiroFilter.executeChain(AbstractShiroFilter.java:449)
org.apache.shiro.web.servlet.AbstractShiroFilter$1.call(AbstractShiroFilter.java:365)
org.apache.shiro.subject.support.SubjectCallable.doCall(SubjectCallable.java:90)
org.apache.shiro.subject.support.SubjectCallable.call(SubjectCallable.java:83)
org.apache.shiro.subject.support.DelegatingSubject.execute(DelegatingSubject.java:383)
org.apache.shiro.web.servlet.AbstractShiroFilter.doFilterInternal(AbstractShiroFilter.java:362)
org.apache.shiro.web.servlet.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:125)
java.lang.NullPointerException
com.sonicle.webtop.core.servlet.Login.processRequest(Login.java:76)
com.sonicle.webtop.core.app.AbstractServlet.doGet(AbstractServlet.java:71)
javax.servlet.http.HttpServlet.service(HttpServlet.java:624)
javax.servlet.http.HttpServlet.service(HttpServlet.java:731)
org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
org.apache.shiro.web.servlet.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:112)
com.sonicle.commons.web.ServletUtils.forwardRequest(ServletUtils.java:953)
com.sonicle.webtop.core.servlet.WebTopFormAuthFilter.redirectToLogin(WebTopFormAuthFilter.java:104)
org.apache.shiro.web.filter.AccessControlFilter.saveRequestAndRedirectToLogin(AccessControlFilter.java:192)
org.apache.shiro.web.filter.authc.FormAuthenticationFilter.onAccessDenied(FormAuthenticationFilter.java:168)
org.apache.shiro.web.filter.AccessControlFilter.onAccessDenied(AccessControlFilter.java:133)
org.apache.shiro.web.filter.AccessControlFilter.onPreHandle(AccessControlFilter.java:162)
org.apache.shiro.web.filter.PathMatchingFilter.isFilterChainContinued(PathMatchingFilter.java:203)
org.apache.shiro.web.filter.PathMatchingFilter.preHandle(PathMatchingFilter.java:178)
org.apache.shiro.web.servlet.AdviceFilter.doFilterInternal(AdviceFilter.java:131)
org.apache.shiro.web.servlet.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:125)
org.apache.shiro.web.servlet.ProxyedFilterChain.doFilter(ProxyedFilterChain.java:66)
org.apache.shiro.web.servlet.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:125)
org.apache.shiro.web.servlet.ProxyedFilterChain.doFilter(ProxyedFilterChain.java:66)
org.apache.shiro.web.servlet.ProxyedFilterChain.doFilter(ProxyedFilterChain.java:66)
org.apache.shiro.web.servlet.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:125)
org.apache.shiro.web.servlet.ProxyedFilterChain.doFilter(ProxyedFilterChain.java:66)
org.apache.shiro.web.servlet.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:125)
org.apache.shiro.web.servlet.ProxyedFilterChain.doFilter(ProxyedFilterChain.java:66)
org.apache.shiro.subject.support.SubjectCallable.doCall(SubjectCallable.java:90)
org.apache.shiro.subject.support.SubjectCallable.call(SubjectCallable.java:83)
org.apache.shiro.subject.support.DelegatingSubject.execute(DelegatingSubject.java:383)
org.apache.shiro.web.servlet.AbstractShiroFilter.doFilterInternal(AbstractShiroFilter.java:362)
org.apache.shiro.web.servlet.OncePerRequestFilter.doFilter(OncePerRequestFilter.java:125)

```

Position	Domain	RefDomain	AlexaRank	Matches	MatchedURL	ExtBackURL	IndexedURL	CrawledURL	FirstCrawl	LastSuccess	IP	SubNet	Country	CoTLD	CitationFor	TrustFlow	BackLinks	FirstLinkDate	LastLinkDate	BackLinks	FirstLinkDate	LastLinkDate
1	blogspot.cc	3393548	70	7	764	6.61e+09	5.6774e+08	9964539	#####	#####	216.58.209	216.58.209	US	com	86	92	503	#####	#####	11	#####	#####
2	blogspot.cc	331780	742	7	703	86032596	38072726	2052859	#####	#####	74.125.22	74.125.22	US	uk	55	66	465	#####	#####	24	#####	#####
3	blogspot.de	285198	996	7	1184	92479735	79643330	5715452	#####	#####	216.58.216	216.58.216	US	de	62	63	906	#####	#####	31	#####	#####
4	blogspot.ru	84427	1003	7	147	22064355	22929545	1196726	#####	#####	216.239.38	216.239.38	US	ru	52	46	36	#####	#####	5	#####	#####
5	blogspot.tw	36726	1357	7	188	8658099	23580230	1162573	#####	#####	216.58.217	216.58.217	US	tw	43	44	58	#####	#####	77	#####	#####
6	feedburner	669596	3405	7	217	1.58e+09	38138259	2331839	#####	#####	216.58.212	216.58.212	US	com	84	90	86	#####	#####	48	#####	#####
7	blogspot.hk	16276	4415	7	203	2794275	15752210	885899	#####	#####	173.194.20	173.194.20	US	hk	39	35	160	#####	#####	7	#####	#####
8	blogspot.hi	22982	5746	7	604	9179602	21981410	1122755	#####	#####	216.58.219	216.58.219	US	hi	41	40	500	#####	#####	5	#####	#####
9	blogspot.ni	34254	7951	7	809	7611736	29772994	1676427	#####	#####	216.58.219	216.58.219	US	ni	41	38	599	#####	#####	7	#####	#####
10	webrnamel	425	28164	7	72	13315	9922	9729	#####	#####	184.168.14	184.168.14	US	com	22	14	9	#####	#####	8	#####	#####
11	dshnaps.c	592	273975	7	98	2685	351132	71488	#####	#####	104.28.10	104.28.10	US	com	28	9	10	#####	#####	6	#####	#####
12	blogspot.it	130540	-1	7	126	76190196	24318821	1157004	#####	#####	173.194.20	173.194.20	US	it	56	59	41	#####	#####	9	#####	#####
13	blogspot.nl	141552	-1	7	421	27593487	49203831	2529699	#####	#####	74.125.136	74.125.136	US	nl	52	60	141	#####	#####	14	#####	#####
14	blogspot.cc	44979	-1	7	111	12871056	18358875	879880	#####	#####	216.58.211	216.58.211	US	ar	40	44	30	#####	#####	5	#####	#####
15	blogspot.fr	241912	-1	7	536	96810729	62048647	3802975	#####	#####	74.125.22	74.125.22	US	fr	58	58	204	#####	#####	10	#####	#####
16	blogspot.cc	214471	-1	7	206	1.64e+08	34871099	1984942	#####	#####	74.125.136	74.125.136	US	es	53	63	53	#####	#####	4	#####	#####
17	livejournal	554234	598	6	35	4.11e+08	76051631	2075931	#####	#####	208.93.0	11.208.93.0	US	com	71	83	9	#####	#####	0	#####	#####
18	typedpad	436533	1122	6	1395	2.33e+08	18784983	2000460	#####	#####	190.93.244	190.93.244	US	com	68	77	158	#####	#####	0	#####	#####
19	epicurious.	47561	2604	6	97	3915561	604402	92738	#####	#####	107.23.243	107.23.243	US	com	55	68	26	#####	#####	0	#####	#####
20	metalfiler	27989	2732	6	95	3260260	2803888	266386	#####	#####	54.186.13	54.186.13	US	com	49	58	22	#####	#####	0	#####	#####
21	chov.com	34734	2872	6	383	5611219	4002988	305995	#####	#####	2.16.4.51	2.16.4.0	EU	com	54	61	45	#####	#####	0	#####	#####
22	blogspot.fi	48171	6757	6	630	14832020	30759927	1634026	#####	#####	216.58.219	216.58.219	US	fi	46	47	519	#####	#####	0	#####	#####
23	purewow.co	3967	7352	6	141	199628	183479	100578	#####	#####	54.243.123	54.243.123	US	com	44	25	64	#####	#####	34	#####	#####
24	blogspot.cz	27380	10412	6	138	9768530	23837231	1228798	#####	#####	74.125.136	74.125.136	US	cz	42	43	34	#####	#####	0	#####	#####
25	listofdomain	909	53229	6	48	13946	12085	12471	#####	#####	192.185.10	192.185.10	US	org	20	8	0	#####	#####	7	#####	#####
26	list-of-doms	354	63226	6	46	5315	13121	12768	#####	#####	184.168.14	184.168.14	US	org	20	13	0	#####	#####	11	#####	#####
27	the-globe.c	231	93147	6	24	3648	19248	14188	#####	#####	46.30.212	46.30.212	DK	com	18	0	0	#####	#####	0	#####	#####
28	the-globe.n	289	99771	6	25	691066	20063	18340	#####	#####	46.30.212	46.30.212	DK	net	42	3	0	#####	#####	5	#####	#####
29	thenibble.c	5744	106418	6	182	140249	75143	49807	#####	#####	46.30.212	46.30.212	DK	com	38	30	9	#####	#####	0	#####	#####
30	the-globe.o	263	151099	6	24	5660	18725	12899	#####	#####	46.30.212	46.30.212	DK	org	19	6	0	#####	#####	4	#####	#####
31	paperankre	424	153685	6	32	492495	19560	19522	#####	#####	198.101.9	198.101.9	US	com	30	15	0	#####	#####	6	#####	#####
32	specialtyfo	4874	221433	6	50	366766	93996	70555	#####	#####	198.74.54	198.74.54	US	com	41	57	10	#####	#####	5	#####	#####
33	blogspot.ca	194596	-1	6	218	4153487	19076361	967414	#####	#####	216.58.211	216.58.211	US	ca	48	58	53	#####	#####	6	#####	#####
34	blogspot.be	69357	-1	6	165	1242855	2272288	1216296	#####	#####	216.58.211	216.58.211	US	be	44	42	119	#####	#####	0	#####	#####
35	blogspot.ec	118514	-1	6	111	22328112	20269249	980040	#####	#####	216.58.208	216.58.208	US	au	47	63	43	#####	#####	0	#####	#####
36	food411.co	364	-1	6	36	12961	3493	1818	#####	#####	198.189.2	198.189.0	US	com	26	26	11	#####	#####	0	#####	#####
37	blogspot.se	69632	-1	6	171	31815364	25331801	1204779	#####	#####	216.58.217	216.58.217	US	se	46	47	72	#####	#####	33	#####	#####
38	huffington	555939	103	5	29	1.98e+08	6526950	693276	#####	#####	64.12.79.5	64.12.79.0	US	com	86	86	9	#####	#####	8	#####	#####
39	blogspot.in	137496	129	5	67	54599814	19582189	907818	#####	#####	74.125.22	74.125.22	US	in	50	52	40	#####	#####	4	#####	#####
40	washington	451776	201	5	47	89239690	4264572	649581	#####	#####	204.79.99	204.79.99	US	com	84	88	10	#####	#####	0	#####	#####
41	seriouspost	50603	2739	5	253	3359940	308666	148251	#####	#####	54.243.216	54.243.216	US	com	60	50	88	#####	#####	0	#####	#####
42	bonaparte	26257	4342	5	79	1405521	159997	57256	#####	#####	54.209.127	54.209.127	US	com	51	51	11	#####	#####	0	#####	#####
43	foodandwine	27170	4795	5	88	1090007	145898	71041	#####	#####	216.146.46	216.146.46	US	com	52	66	12	#####	#####	0	#####	#####
44	foodora.com	33891	5010	5	43	3816479	987572	241624	#####	#####	170.171.20	170.171.20	US	com	50	71	0	#####	#####	0	#####	#####
45	tastetrngtbl	5504	17669	5	246	127930	305647	126188	#####	#####	184.72.47	184.72.47	US	com	42	32	83	#####	#####	12	#####	#####
46	finecooking	34668	19855	5	40	4718309	366437	63438	#####	#####	4.26.51.0	4.26.51.0	US	com	47	51	11	#####	#####	0	#####	#####
47	egullet.org	3448	65304	5	175	160751	450660	115777	#####	#####	98.129.229	98.129.229	US	org	37	44	15	#####	#####	0	#####	#####
48	semailand	132	298327	5	36	784	3871830	237984	#####	#####	88.214.226	88.214.226	UK	com	17	21	10	#####	#####	7	#####	#####
49	ruokkavuori	7911	107874	5	15	79614	907961	199030	#####	#####	148.751.31	148.751.31	FI	info	17	11	0	#####	#####	0	#####	#####

<https://community.nethserver.org/t/error-http-status-500/8489>

<https://blog.majestic.com/wp-content/uploads/2015/08/5-excel-raw-results.jpg>

- 2020 Friday – Jun 12 at 11:10:43 PM
- 2020 Monday – Jul 13 at 3:45:04 PM
- 2020 Tuesday – Aug 4 at 2:22:54 AM



# Getting Log Data Up To Fleek Standards

- How can DFUR security team members enhance logs?
  - Parsing and formatting
  - Centralization
  - Determine what log data is relevant to security missions ☆☆☆



**DFUR**



# Threat Modeling

- What types of threats do you face based on industry trends?
  - What would those threats do?
- If you were attacked, what data would you want to have logged and how would you like it to be logged?



DFUR

# DFUR Security Team Threat Meowdeling

- Account takeover
  - Credential stuffing, brute force, one off
  - Bank account modifications
  - PHI/PII access
    - Pet Health Information/Pet Identifying Information
  - Health service modifications or interruptions
- Submitting fraudulent reimbursement claims
- Veterinarians over-prescribing cat-nip



DFUR

# Review Your Current Log Setup

- Investigation Simulation

- Logs should be able to answer all questions you could possibly need
- Analysis should not require an annoying amount of time spent for:
  - Exporting
  - Searching
  - Correlating
  - Formatting



DFUR

# Where Are the New Logs?

- Local Logging
  - Enhanced logs will be amazing for traditional investigations!
  - What retention limitations exist?
- Centralized Logging
  - Costs \$\$
  - Can utilize detection functionality
  - Can develop investigation workflows



DFUR

# Monitoring and Detection Through Logs

- Make your logs work for you
  - Alert on what you can
  - Visualize data sets likely to show anomalies
  - Easy to follow investigation workflows
- Visualizations
  - Maps, Graphs, Tables, Heatmaps
  - Baseline data



DFUR

# splunk Demo



- Commercial log aggregation and analysis tool
- Feature rich and can require lots of experience and training to use effectively
- Used as an example going forward but the concepts are likely applicable to many log platforms

\* All data presented is fictional and any relation to actual users or organizations is coincidental and unfortunate

# DFUR

# DFUR Monitoring - Anomalous Account Activity and Application Usage

This dashboard contains analytics that can be used to identify suspicious login activity, web application interactions, and application transactions that may indicate potential signs of account compromise and application abuse. All names, IP addresses, and incidents portrayed in this dashboard are fictitious.

Last 30 days  Hide Filters

- Account Login Activity
- Application Activity
- Watchlists

## Geolocation Analytics

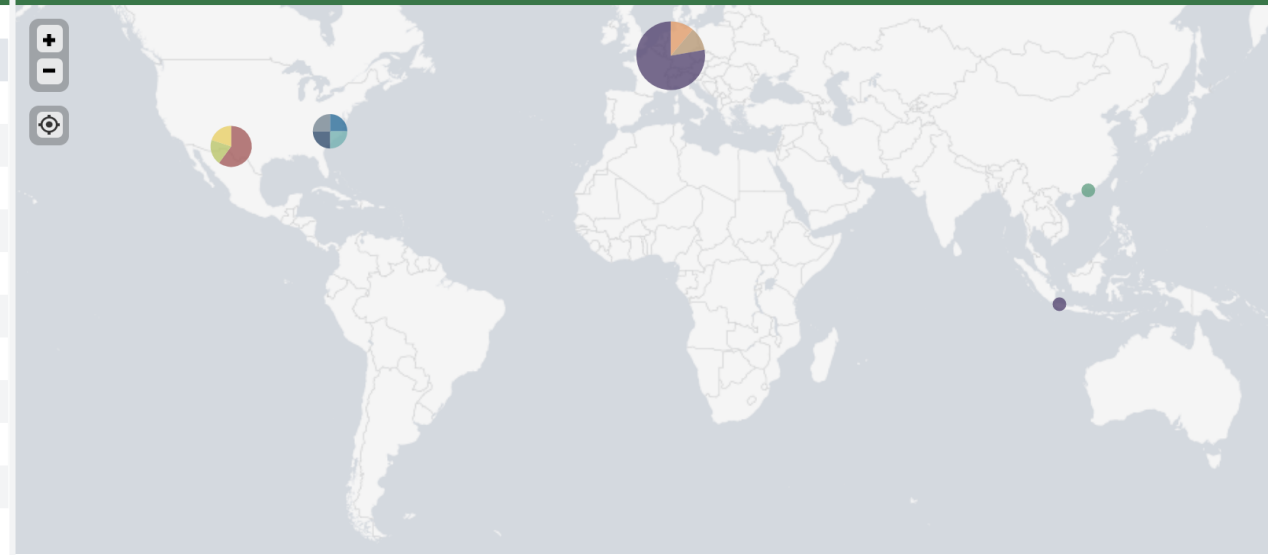
These analytics show geolocation anomalies based on the source IP address of a successful user account authentication attempt.

### Successful Account Logins from non-US Locations

« Prev 1 **2** 3 Next »

Username	Time	IP Address	Country	Action	Result
VetStaff3	2020-06-28 08:59:30	185.216.35.66	Czechia	login	success
VetStaff3	2020-06-29 08:58:13	82.102.20.182	Denmark	login	success
VetStaff3	2020-06-30 08:54:02	82.102.20.182	Denmark	login	success
VetStaff3	2020-07-01 08:54:56	185.216.35.66	Czechia	login	success
david_hisslehoff	2020-06-28 22:45:17	164.132.51.18	France	login	success
fuzz_aldrin	2020-06-26 01:02:08	164.132.51.15	France	login	success
labradorable	2020-06-29 10:14:42	103.28.52.93	Indonesia	login	success
lunabear	2020-07-01 14:58:56	164.132.51.91	France	login	success
missus_claws	2020-07-01 13:51:12	164.132.51.91	France	login	success
picatso	2020-06-28 22:05:48	164.132.51.25	France	login	success

### Successful Account Logins by Source IP Geolocation



### Successful Logins from Multiple States

Username	State Count	States	IP Count	IP Addresses
VetStaff1	4	California Florida New York Virginia	4	193.37.252.54 209.95.50.88 70.32.0.70 91.207.175.121

### Successful Username Reminder Requests from non-US Locations

Time	Username	IP Address	Country	Form Email
2020-06-30 04:00:05	jasperlionheart	185.22.172.205	Russia	jasper.s.lionheart2@gmail

### Successful Password Reset Requests from non-US Locations

Time	Username	IP Address	Country	Result
2020-06-29 10:13:45	labradorable	103.28.52.93	Indonesia	success

# Temporal Analytics

These analytics show temporal anomalies based on the times of successful user account authentication attempts.

## Successful Account Logins During Non-Business Hours

End of Day Hour  Start of Day Hour

Time ↕	Username ↕	IP Address ↕	Country ↕	Action ↕	Result ↕
2020-06-26 20:43:24	bingo1	174.240.9.250	United States	login	success
2020-06-26 22:34:23	scoobs	77.243.191.18	Belgium	login	success
2020-06-26 22:41:01	VetStaff1	77.243.191.18	Belgium	login	success
2020-06-26 23:07:21	VetStaff2	77.243.191.18	Belgium	login	success
2020-06-26 23:11:43	VetStaff3	77.243.191.18	Belgium	login	success
2020-06-28 20:32:48	puggetaboutit	70.88.4.6	United States	login	success
2020-06-29 22:01:13	bingo1	107.77.221.4	United States	login	success
2020-06-26 01:02:08	fuzz_aldrin	164.132.51.15	France	login	success
2020-06-28 21:41:39	snarlsbarkley3	164.132.51.16	France	login	success
2020-06-28 22:05:48	picatso	164.132.51.25	France	login	success



## Potential Password Attack Activity: User-Centric

Failed Attempt Threshold

Successful Attempt Threshold

Portal Selection

Username ⌵	Calendar Day ⌵	Total Count ⌵	Fail Count ⌵	Success Count ⌵	Perc Failed ⌵	First Event ⌵	Last Event ⌵	Uniq IP ⌵	Uniq UA ⌵
lunabear	Jul 01	277	276	1	99.64	2020-07-01 12:04:49	2020-07-01 14:58:56	1	1

## Potential Password Attack Activity: IP-Centric

Failed Attempt Threshold: 
 Successful Attempt Threshold: 
 Portal Selection:

IP Address ↕	Calendar Day ↕	Total Count ↕	Fail Count ↕	Success Count ↕	Perc Failed ↕	Results ↕	First Event ↕	Last Event ↕	User-Agent ↕	AS Name ↕	Country ↕
164.132.51.15	Jun 26	162	161	1	99.38	Invalid Accts: 161 Bad PW: 0	2020-06-26 01:00:50	2020-06-26 03:59:44	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36	OVH SAS	France
164.132.51.16	Jun 28	169	168	1	99.41	Invalid Accts: 167 Bad PW: 1	2020-06-28 21:00:49	2020-06-28 22:58:46	password-spay-toolkit-v3	OVH SAS	France
164.132.51.18	Jun 28	161	160	1	99.38	Invalid Accts: 160 Bad PW: 0	2020-06-28 21:01:18	2020-06-28 22:59:23	password-spay-toolkit-v3	OVH SAS	France
164.132.51.25	Jun 28	179	178	1	99.44	Invalid Accts: 178 Bad PW: 0	2020-06-28 21:00:00	2020-06-28 22:59:50	password-spay-toolkit-v3	OVH SAS	France
164.132.51.91	Jul 01	3311	3308	3	99.91	Invalid Accts: 3021 Bad PW: 287	2020-07-01 12:00:04	2020-07-01 14:59:53	Mozilla/5.0	OVH SAS	France

### Haversine Distance: Impractical Travel between Account Logins (Distance >= 1,000 Miles)

Username ↕	Time ↕	IP Address ↕	Region ↕	Country ↕	Next Time ↕	Next IP ↕	Next State ↕	Next Country ↕	Distance (mi) ↕	Time Diff (hrs) ↕	Speed ↕
labradorable	2020-06-29 09:15:34	73.90.210.191	California	United States	2020-06-29 10:14:42	103.28.52.93		Indonesia	8690.73	0.99	8818
VetStaff1	2020-06-26 22:41:01	77.243.191.18		Belgium	2020-06-27 08:56:00	91.207.175.121	California	United States	5613.28	10.25	548
VetStaff2	2020-06-28 08:57:24	86.105.25.76		Romania	2020-06-29 08:48:23	119.81.253.242	Central and Western District	Hong Kong	5085.44	23.85	213
lunabear	2020-06-30 09:10:42	73.90.210.191	California	United States	2020-07-01 14:58:56	164.132.51.91		France	5485.58	29.80	184
VetStaff2	2020-06-26 23:07:21	77.243.191.18		Belgium	2020-06-27 08:59:14	86.105.25.76		Romania	1000.36	9.86	101
VetStaff1	2020-06-27 08:56:00	91.207.175.121	California	United States	2020-06-28 08:58:17	193.37.252.54	Florida	United States	2321.44	24.04	97
VetStaff1	2020-06-28 08:58:17	193.37.252.54	Florida	United States	2020-06-29 08:59:11	209.95.50.88	New York	United States	1087.67	24.02	45

## Reputation and Hosting Analytics

These analytics show anomalies based on the reputation and hosting information for source IP addresses associated with successful user account authentication attempts.

### Successful Authentications from Multiple ASNs

Username ↕	AS Count ↕	AS Name ↕	IP Count ↕	IP Addresses ↕
VetStaff1	3	ASN-GIGENET HOSTINGSERVICES-INC M247 Ltd	5	193.37.252.54 209.95.50.88 70.32.0.70 77.243.191.18 91.207.175.121
bingo1	3	ATT-MOBILITY-LLC-AS20057 CELLCO UNIFIEDLAYER-AS-1	3	107.77.221.4 174.240.9.250 50.116.76.236
VetStaff2	2	M247 Ltd SOFTLAYER	3	119.81.253.242 77.243.191.18 86.105.25.76
labradorable	2	COMCAST-7922 PT Cloud Hosting Indonesia	2	103.28.52.93 73.90.210.191
lunabear	2	COMCAST-7922 OVH SAS	2	164.132.51.91 73.90.210.191

## Organization Analytics

These analytics show anomalies associated with organization registration and user source IP address geolocation.

### User Activity Geolocation Inconsistent with Organization Location

« Prev **1** 2 Next »

Username ↕	Entity Name ↕	User IP State ↕	Entity State ↕	IP Addresses ↕	IP Country ↕
VetStaff1	Little Husky Dieting	not identified	FL	77.243.191.18	Belgium
VetStaff1	Little Husky Dieting	CA	FL	91.207.175.121	United States
VetStaff1	Little Husky Dieting	NY	FL	209.95.50.88	United States
VetStaff1	Little Husky Dieting	VA	FL	70.32.0.70	United States
VetStaff1	Catitude LLC	not identified	VA	77.243.191.18	Belgium
VetStaff1	Catitude LLC	CA	VA	91.207.175.121	United States
VetStaff1	Catitude LLC	FL	VA	193.37.252.54	United States
VetStaff1	Catitude LLC	NY	VA	209.95.50.88	United States
VetStaff2	Catitude LLC	not identified	VA	77.243.191.18 86.105.25.76	Belgium Romania
VetStaff2	Catitude LLC	not identified	VA	119.81.253.242	Hong Kong

### Organization Creation Geolocation Inconsistent with Organization Location

Time ↕	Username ↕	Entity Name ↕	Entity State ↕	Event Description ↕	User IP State ↕	IP Address ↕	IP Country ↕
2020-06-26 23:01:12	VetStaff1	Catitude LLC	VA	Provider Catitude LLC is added by VetStaff1	not identified	77.243.191.18	Belgium

### Organization Creation Metadata Inconsistent with NPPES Database

Time ↕	Username ↕	NPI ↕	Entity Name ↕	NPPES Org Name ↕	Name Match? ↕	Entity City ↕	NPPES City ↕	City Match? ↕	Entity State ↕	NPPES State ↕	State Match? ↕	Entity Street ↕	NPPES Street ↕
2020-06-26 23:01:12	VetStaff1	1023423222	Catitude LLC	Little Husky Dieting	No	Fairfax	Fort Myers	No	VA	FL	No	476 Scratchpost Lane	9873 Snackely Ave.

# User Analytics

These analytics show behavioral anomalies associated with user account activity.

## Multiple User Agents Used

Username ↕	Unique UAs ↕	User-Agent ↕
VetStaff2	2	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:60.0) Gecko/20100101 Firefox/60.0 Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0; MSN 9.0;MSN 9.1;MSN 9.6;MSN 10.0;MSN 10.2;MSN 10.5; MSNbsMSNI; MSNmen-us; MSNcIA)
VetStaff3	2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.74 Safari/537.36 Edg/79.0.309.43 Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0; MSN 9.0;MSN 9.1;MSN 9.6;MSN 10.0;MSN 10.2;MSN 10.5; MSNbsMSNI; MSNmen-us; MSNcIA)
bingo1	2	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36 Mozilla/5.0 (iPhone; CPU iPhone OS 13_1_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.1 Mobile/15E148 Safari/604.1
labradorable	2	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36 Mozilla/5.0 (X11; Linux x86_64; rv:10.0) Gecko/20100101 Firefox/10.0
lunabear	2	Mozilla/5.0 Mozilla/5.0 (Windows Mobile 10; Android 8.0.0; Microsoft; Lumia 950XL) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Mobile Safari/537.36 Edge/40.15254.603

## Multiple Bank Accounts Added

Username ↕	First Event ↕	Last Event ↕	Unique Routing Num ↕	Unique Acct Num ↕	Provider Count ↕	Entity Name ↕	Banks Added ↕
labradorable	2020-06-29 10:23:32	2020-06-29 11:14:32	2	2	1	Barkeology Associates	2

## User Behavior Analytic over Time Span

Time Span (Hours)  Analytic Points

Searches for 3 or 4 events (points) occurring within Time Span: Username Reminder, Password Change, Bank Account Added, ePayment Enrollment Changed

Username ↕	Entity Name ↕	First Event ↕	Duration (hrs) ↕	Event Count ↕	Combined Events ↕
labradorable	Barkeology Associates	2020-06-29 10:10:05	0.70	4	2020-06-29 10:10:05 - User Account - labradorable has requested a username reminder 2020-06-29 10:13:45 - User Account - labradorable has changed password 2020-06-29 10:23:32 - Bank Account - Bank account added for provider Barkeology Associates with routing number 124085024 account number .....4953 and nickname Barkeology Associates 2020-06-29 10:52:17 - ePayment Change - ePayment enrollment submitted by provider Barkeology Associates for Barkeology Associates.....4953 to insurance company

# Bank Account Analytics

These analytics show anomalies associated with bank accounts that are added and assigned to entities by user accounts.

## Bank Account Routing Number Metadata Inconsistent with Organization Location

Time	Username	Entity Name	Routing Num	Acct Num	Bank Nickname	Routing Bank	Provider State	Routing State	State Match?
2020-06-29 10:23:32	labradorable	Barkeology Associates	124085024	.....4953	Barkeology Associates	Green Dot	CA	none	No
2020-06-29 11:14:32	labradorable	Barkeology Associates	123103729	.....2312	Bark	U.S. Bank	CA	ID	No

Last 30 days



Submit

Hide Filters

Account Login Activity

Application Activity

Watchlists

## Organization Watchlist

These analytics show events associated with an organization name or ID that has been placed on a custom watchlist.

## User Account Watchlist

These analytics show events associated with a user account name or user ID that has been placed on a custom watchlist.

## IP Address Watchlist

These analytics show events associated with an IP address that has been placed on a custom watchlist.

## Bank Account Watchlist

These analytics show events associated with a bank account that has been placed on a custom watchlist.



# DFUR – Scenario #1 – Account Takeover

- User hasn't been receiving claims payments
- Logged into account and verified that banking information is not correct
- Username: labradorable



**DFUR**

# DFUR - Investigative - User Activity Enrichment

Edit Export ...

This dashboard shows activity for a specific Username or User ID over a specific window of time to provide additional context and highlight potentially suspicious data points (e.g., login from different cities). All names, IP addresses, and incidents portrayed in this dashboard are fictitious.

Time Picker Username or User ID

Last 30 days labradorable **Submit** Hide Filters

Account Summary Application Activity

## Account Summary

These panels show a basic summary of the user account metadata and risk factor metric.

User Details		Assigned Organizations		Risk Factor
Field	Value	Entity ID	Entity Info	<p>Risk Factor is based on notable user account activities performed during the time window</p> 
1 - Username	labradorable	754534	Barkeology Associates Speech Therapy 344 Waldorf Road Sacramento, CA, 94203 (P) 555-2312 (F)	
2 - User ID	8753346			
3 - Email	fleased_to_meetchu@l33tbomb.com			
4 - Account Last Modified	2020-06-29 10:15:34			
5 - Password Last Modified	2020-06-29 10:13:45			
6 - Last Login	2020-06-29 10:14:42			
7 - Account Created	2019-08-10 10:21:43			
8 - First	Poppy			
9 - Middle	n/a			
10 - Last	Sheds			
11 - Phone Number	555-2312			
12 - Role	Admin			
13 - Entity Name(s)	Barkeology Associates			

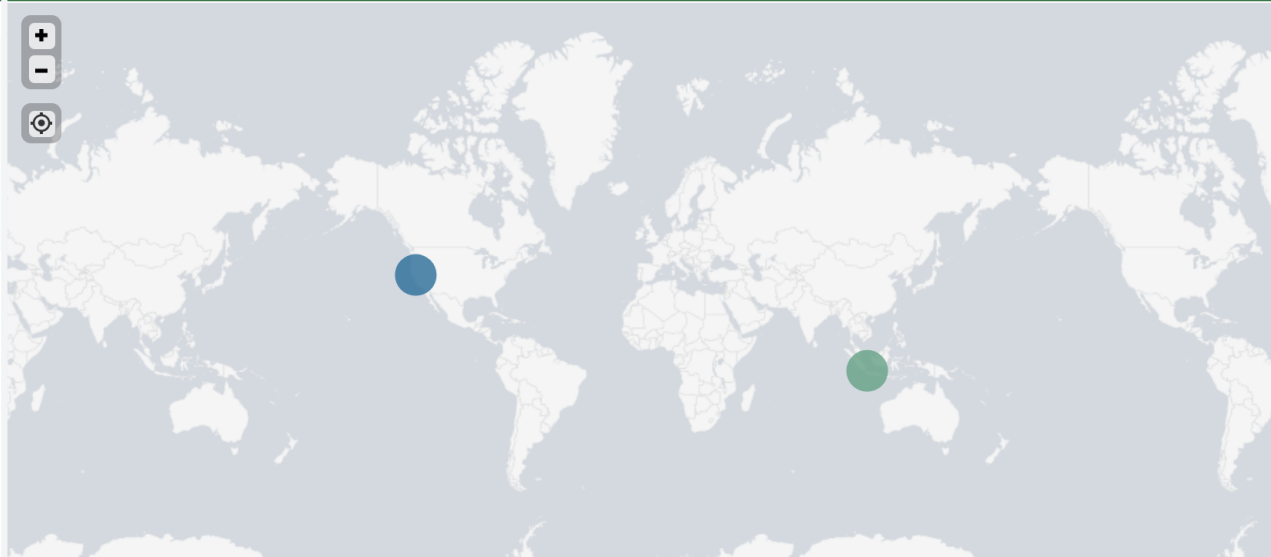
# Remote Access Analytics

These analytics show a basic summary of user logon attempts and other remote access details.

## Logon Event: User Logon Event Timeline

Time ↕	Username ↕	IP Address ↕	Action ↕	Result ↕
2020-06-29 09:15:34	labradorable	73.90.210.191	login	success
2020-06-29 09:30:42	labradorable	73.90.210.191	logout - user initiated	success
2020-06-29 10:14:42	labradorable	103.28.52.93	login	success
2020-06-29 11:45:29	labradorable	103.28.52.93	logout - user initiated	success

## Logon Event: Successful Logins by City for User



## Web Application: User-Agents Associated with User

User-Agent ↕	First Event ↕	Last Event ↕
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36	2020-06-29 09:15:34	2020-06-29 09:30:42
Mozilla/5.0 (X11; Linux x86_64; rv:10.0) Gecko/20100101 Firefox/10.0	2020-06-29 10:14:42	2020-06-29 11:45:29

## Logon Event: Activity by Source IP for User

IP Address ↕	Result ↕	AS Name ↕	State ↕	Country ↕	Count ↕
103.28.52.93	success	PT Cloud Hosting Indonesia		Indonesia	2
73.90.210.191	success	COMCAST-7922	California	United States	2

## Username Reminders and Password Reset Requests

Time ↕	IP Address ↕	Country ↕	Event Type ↕	Event Desc ↕
2020-06-29 10:10:05	103.28.52.93	Indonesia	User Account	labradorable has requested a username reminder
2020-06-29 10:13:45	103.28.52.93	Indonesia	User Account	labradorable has changed password

## Haversine Distance: Impractical Travel between Account Logins (Distance >= 1,000 Miles)

Username ↕	Time ↕	IP Address ↕	Region ↕	Country ↕	Next Time ↕	Next IP ↕	Next State ↕	Next Country ↕	Distance (mi) ↕	Time Diff (hrs) ↕	Speed ↕
labradorable	2020-06-29 09:15:34	73.90.210.191	California	United States	2020-06-29 10:14:42	103.28.52.93		Indonesia	8690.73	0.99	8818

# DFUR - Investigative - User Activity Enrichment

[Edit](#) [Export](#) [...](#)

This dashboard shows activity for a specific Username or User ID over a specific window of time to provide additional context and highlight potentially suspicious data points (e.g., login from different cities). All names, IP addresses, and incidents portrayed in this dashboard are fictitious.

Time Picker:  Username or User ID:  [Submit](#) [Hide Filters](#)

[Account Summary](#) [Application Activity](#)

## Application Activity Timeline

This panel shows a timeline of application activity associated with the user. Time of day (TOD) anomalies are actions performed between 19:00 UTC and 5:00 UTC.

Actions by: Calendar Day					Actions by: IP Address				Actions by: Event Type			
Calendar Day	First Event	Last Event	TOD Anom	Actions	IP Address	First Event	Last Event	Actions	Event Type	First Event	Last Event	Actions
*	0_Reset Filter				*	0_Reset Filter						
Jun 29	2020-06-29 09:20:14	2020-06-29 11:34:11	0	10	73.90.210.191	2020-06-29 09:20:14	2020-06-29 09:20:14	1	Patient Viewed	2020-06-29 09:20:14	2020-06-29 09:20:14	1
					103.28.52.93	2020-06-29 10:10:05	2020-06-29 11:34:11	9	User Account	2020-06-29 10:10:05	2020-06-29 10:15:34	3
									Bank Account	2020-06-29 10:23:32	2020-06-29 11:34:11	4
									ePayment Change	2020-06-29 10:52:17	2020-06-29 11:02:13	2

### Activity Event Timeline: labradorable

Time	Username	User ID	IP Address	Event Type	Event Desc
2020-06-29 09:20:14	labradorable	8753346	73.90.210.191	Patient Viewed	Patient profile information viewed
2020-06-29 10:10:05	labradorable	8753346	103.28.52.93	User Account	labradorable has requested a username reminder
2020-06-29 10:13:45	labradorable	8753346	103.28.52.93	User Account	labradorable has changed password
2020-06-29 10:15:34	labradorable	8753346	103.28.52.93	User Account	labradorable has changed account email from poppy.sheds@barkeology.com to fleased_to_meetchu@133tbomb.com
2020-06-29 10:23:32	labradorable	8753346	103.28.52.93	Bank Account	Bank account added for provider Barkeology Associates with routing number 124085024 account number .....4953 and nickname Barkeology Associates
2020-06-29 10:46:11	labradorable	8753346	103.28.52.93	Bank Account	The 588 Form for Barkeology Associates.....4953 was uploaded by labradorable for provider Barkeology Associates
2020-06-29 10:52:17	labradorable	8753346	103.28.52.93	ePayment Change	ePayment enrollment submitted by provider Barkeology Associates for Barkeology Associates.....4953 to insurance company
2020-06-29 11:02:13	labradorable	8753346	103.28.52.93	ePayment Change	ePayment removal request submitted by provider Flexeon Partners for USBANK Czeching.....1242 to insurance company
2020-06-29 11:14:32	labradorable	8753346	103.28.52.93	Bank Account	Bank account added for provider Barkeology Associates with routing number 123103729 account number .....2312 and nickname Bark

10:14:42 11:45:29

**Haversine Distance: Impractical Travel between Account Logins (Distance >= 1,000 Miles)**

Username	Time	IP Address	Region	Country	Next Time	Next IP	Next State	Next Country	Distance (mi)	Time Diff (hrs)	Speed
labradorable	2020-06-29 09:15:34	73.90.210.191	California	United States	2020-06-29 10:14:42	103.28.52.93		Indonesia	8690.73	0.99	8818

**Notable Application Actions**

These analytics show a basic summary of actions performed by the account using the web application.

**Organizations Registered by User**

No results found.

**Bank Accounts Added**

Time	Username	Organization	Entity ID	Routing Num	Acct Num
2020-06-29 10:23:32	labradorable	Barkeology Associates	754534	124085024	.....4953
2020-06-29 11:14:32	labradorable	Barkeology Associates	754534	123103729	.....2312

**User Account sAdded**

No results found.

# DFUR – Scenario #2 – Cred Stuffing

- Provider and Patient application users reporting account lockouts
- Need to investigate evidence of password attack activity



**DFUR**

### Potential Password Attack Activity: IP-Centric

Failed Attempt Threshold: 
 Successful Attempt Threshold: 
 Portal Selection: Provider X Patient X

IP Address	Calendar Day	Total Count	Fail Count	Success Count	Perc Failed	Results	First Event	Last Event	User-Agent	AS Name	Country
164.132.51.15	Jun 26	162	161	1	99.38	Invalid Accts: 161 Bad PW: 0	2020-06-26 01:00:50	2020-06-26 03:59:44	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36	OVH SAS	France
164.132.51.16	Jun 28	169	168	1	99.41	Invalid Accts: 167 Bad PW: 1	2020-06-28 21:00:49	2020-06-28 22:58:46	password-spay-toolkit-v3	OVH SAS	France
164.132.51.18	Jun 28	161	160	1	99.38	Invalid Accts: 160 Bad PW: 0	2020-06-28 21:01:18	2020-06-28 22:59:23	password-spay-toolkit-v3	OVH SAS	France
164.132.51.25	Jun 28	179	178	1	99.44	Invalid Accts: 178 Bad PW: 0	2020-06-28 21:00:00	2020-06-28 22:59:50	password-spay-toolkit-v3	OVH SAS	France
164.132.51.91	Jul 01	3311	3308	3	99.91	Invalid Accts: 3021 Bad PW: 287	2020-07-01 12:00:04	2020-07-01 14:59:53	Mozilla/5.0	OVH SAS	France

# DFUR - Investigative - IP Address Enrichment

This dashboard shows activity for a specific IP Address over a specific window of time to provide additional context and highlight potentially suspicious data points. All names, IP addresses, and incidents portrayed in this dashboard are fictitious.

Time Picker      IP Address

Between Date-times      164.132.51.91      **Submit**      [Hide Filters](#)

## IP Address Metadata and Organization Summary

The panels below show metadata and organization activity associated with the IP address.

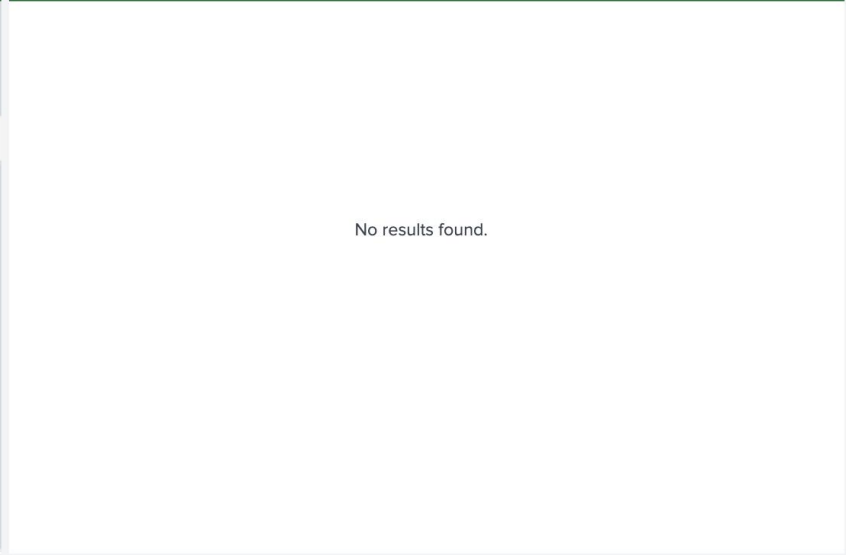
### IP Address Metadata

Field ↕	Value ↕
1 - IP Address	164.132.51.91
2 - Region	
3 - Country	France
4 - AS Name	OVH SAS

### IP Geolocation Visualization

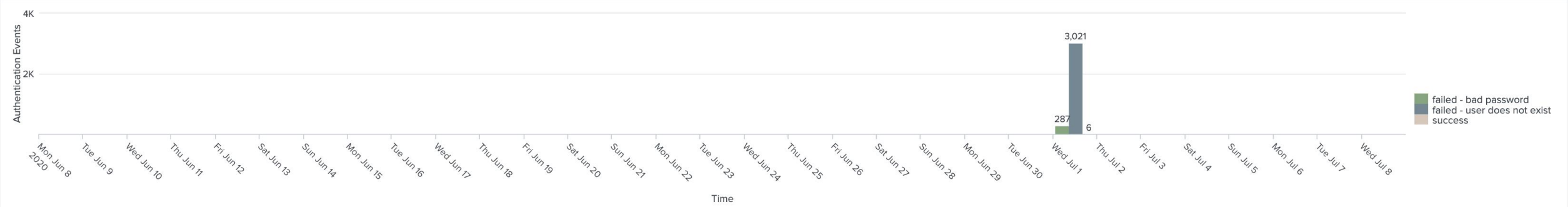


### Organization Activity



## IP Address Activity Timeline

This panel shows a timeline of IP address activity as recorded in the authentication events.





# Remote Access Analytics

These analytics show a basic summary of user logon attempts and other remote access details.

Logon Activity by User Account						Logon Activity by User-Agent						
Username	Total Count	Failed Auth	Successful Auth	First Event	Last Event	User-Agent	Total Count	Failed Auth	Successful Auth	Total Usernames	First Event	Last Event
* 0_Reset Filter						* 0_Reset Filter						
Aaren	1	1	0	2020-07-01 14:14:07	2020-07-01 14:14:07	Mozilla/5.0	3311	3308	3	3035	2020-07-01 12:00:04	2020-07-01 14:59:53
Aarika	1	1	0	2020-07-01 13:24:08	2020-07-01 13:24:08							
Abagael	1	1	0	2020-07-01 13:01:13	2020-07-01 13:01:13							
Abagail	1	1	0	2020-07-01 12:13:14	2020-07-01 12:13:14							

## Authentication Timeline

Logon Result

Time	Username	application_name	IP Address	Action	Result	User-Agent
2020-07-01 12:00:04	Karon	patient_portal	164.132.51.91	login	failed - user does not exist	Mozilla/5.0
2020-07-01 12:00:08	Fedora	patient_portal	164.132.51.91	login	failed - user does not exist	Mozilla/5.0
2020-07-01 12:00:12	Kaye	patient_portal	164.132.51.91	login	failed - user does not exist	Mozilla/5.0
2020-07-01 12:00:19	Claire	patient_portal	164.132.51.91	login	failed - user does not exist	Mozilla/5.0
2020-07-01 12:00:21	Gianna	patient_portal	164.132.51.91	login	failed - user does not exist	Mozilla/5.0
2020-07-01 12:00:21	Hatty	patient_portal	164.132.51.91	login	failed - user does not exist	Mozilla/5.0
2020-07-01 12:00:26	Jemmy	patient_portal	164.132.51.91	login	failed - user does not exist	Mozilla/5.0
2020-07-01 12:00:27	Ingaberg	patient_portal	164.132.51.91	login	failed - user does not exist	Mozilla/5.0
2020-07-01 12:00:30	Janaya	patient_portal	164.132.51.91	login	failed - user does not exist	Mozilla/5.0
2020-07-01 12:00:31	Brittan	patient_portal	164.132.51.91	login	failed - user does not exist	Mozilla/5.0

# DFUR – Scenario #3 – Fraudulent Registration

- Insurance provider reports suspicious activity associated with organization
- High number of failed health record lookups



**DFUR**

# DFUR - Investigative - Organization Enrichment Dashboard

Edit Export ...

This dashboard shows activity for a specific organization over a specific window of time to provide additional context and highlight potentially suspicious data points. All names, IP addresses, and incidents portrayed in this dashboard are fictitious.

Time Picker Entity ID (#####)

Between Date-times 986454 Submit Hide Filters

## Organization Summary

These panels show a basic summary of the organization metadata.

Entity Details		User Activity Source IP Geolocation	Assigned Users				
Field	Value		Username	Name	Email	Role	Account Created
1 - Entity ID	986454		VetStaff1	Vet Tech	cats.can.1@gmail.com	Admin	2020-06-26 22:36:23
2 - Entity Name	Catitude LLC		VetStaff2	Vet Tech	cats.can.2@gmail.com	User	2020-06-26 23:06:32
3 - Entity Type	Provider		VetStaff3	Vet Tech	cats.can.3@gmail.com	User	2020-06-26 23:10:17
4 - Entity Category	DME						
5 - Date Created	2020-06-26 23:01:12						
6 - Last Modified	2020-06-26 23:01:12						
7 - Street Address	476 Scratchpost Lane						
8 - City	Fairfax						
9 - State	VA						
10 - ZIP Code	22031						
11 - TIN	n/a						
12 - NPI	1023423222						
13 - Primary Number	555-5123						
14 - Primary Admin ID	3464278						

NPPES Information Cross-Reference											
NPI	Entity Name	NPPES Org Name	Name Match?	Entity City	NPPES City	City Match?	Entity State	NPPES State	State Match?	Entity Street	NPPES Street
1023423222	Catitude LLC	Little Husky Dieting	No	Fairfax	Fort Myers	No	VA	FL	No	476 Scratchpost Lane	9873 Snackely Ave.

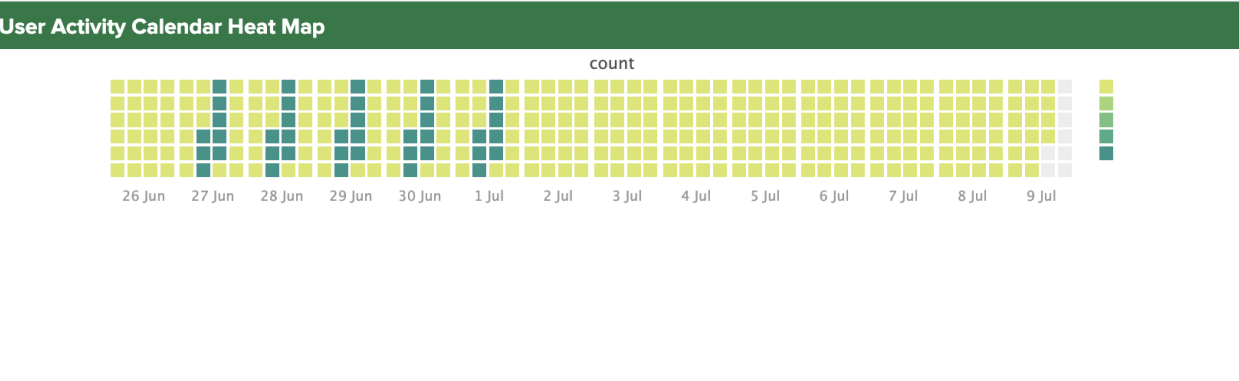
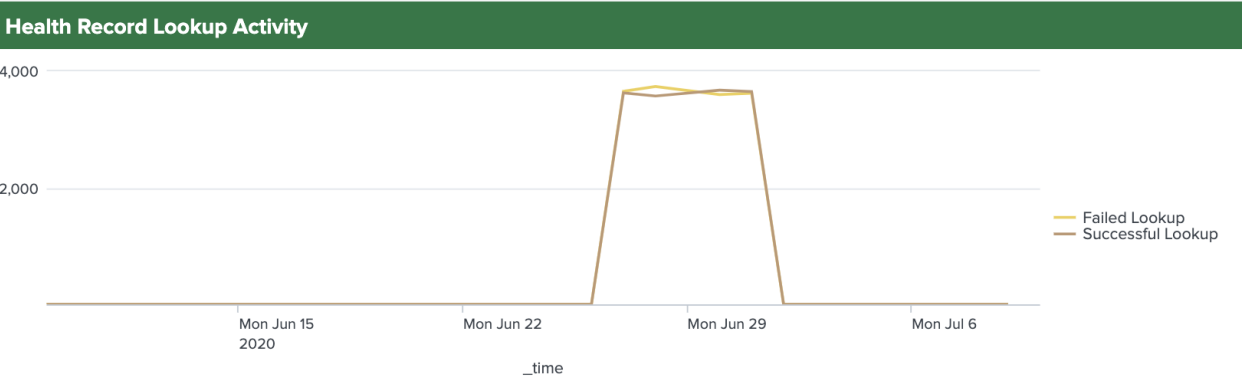
# User Metadata Analytics

These panels show analytics based on user account details and associated metadata.

Unique Source IPs by User		Mail Domains by User		User Count by Source IP			
Username	IP Count	Mail Domain	User Count	IP Address	Country	AS Name	User Count
VetStaff1	5	gmail.com	3	77.243.191.18	Belgium		3
VetStaff2	3			119.81.253.242	Hong Kong		1
VetStaff3	3			185.216.35.66	Czechia		1
				193.37.252.54	United States		1
				209.95.50.88	United States		1
				70.32.0.70	United States		1
				82.102.20.182	Denmark		1
				86.105.25.76	Romania		1
				91.207.175.121	United States		1

# User Activity Analytics

These panels show analytics based on user activity in the DFUR application.



# DFUR - Investigative - User Activity Enrichment

This dashboard shows activity for a specific Username or User ID over a specific window of time to provide additional context and highlight potentially suspicious data points (e.g., login from different cities). All names, IP addresses, and incidents portrayed in this dashboard are fictitious.

Time Picker: Between Date-times  
Username or User ID: VetStaff1  
Submit Hide Filters

Account Summary Application Activity

## Account Summary

These panels show a basic summary of the user account metadata and risk factor metric.

User Details		Assigned Organizations		Risk Factor
Field	Value	Entity ID	Entity Info	<p>Risk Factor is based on notable user account activities performed during the time window</p> 
1 - Username	VetStaff1	431133	Little Husky Dieting Nutrition 9873 Snackely Ave. Fort Myers, FL, 33901 (P) 555-8532 (F)	
2 - User ID	3464278			
3 - Email	cats.can.1@gmail.com			
4 - Account Last Modified	2020-06-26 22:36:23			
5 - Password Last Modified	2020-06-26 22:41:01			
6 - Last Login	2020-07-01 08:58:53	986454	Catitude LLC DME 476 Scratchpost Lane Fairfax, VA, 22031 (P) 555-5123 (F)	
7 - Account Created	2020-06-26 22:36:23			
8 - First	Vet			
9 - Middle	n/a			
10 - Last	Tech			
11 - Phone Number	555-5123			
12 - Role	Admin			
13 - Entity Name(s)	Catitude LLC Little Husky Dieting			

# Notable Application Actions

These analytics show a basic summary of actions performed by the account using the web application.

## Organizations Registered by User

Time ↕	IP Address ↕	Username ↕	Entity Name ↕	Entity ID ↕	NPI ↕	Street Address ↕	City ↕	State ↕
2020-06-26 23:01:12	77.243.191.18	VetStaff1	Catitude LLC	986454	1023423222	476 Scratchpost Lane	Fairfax	VA

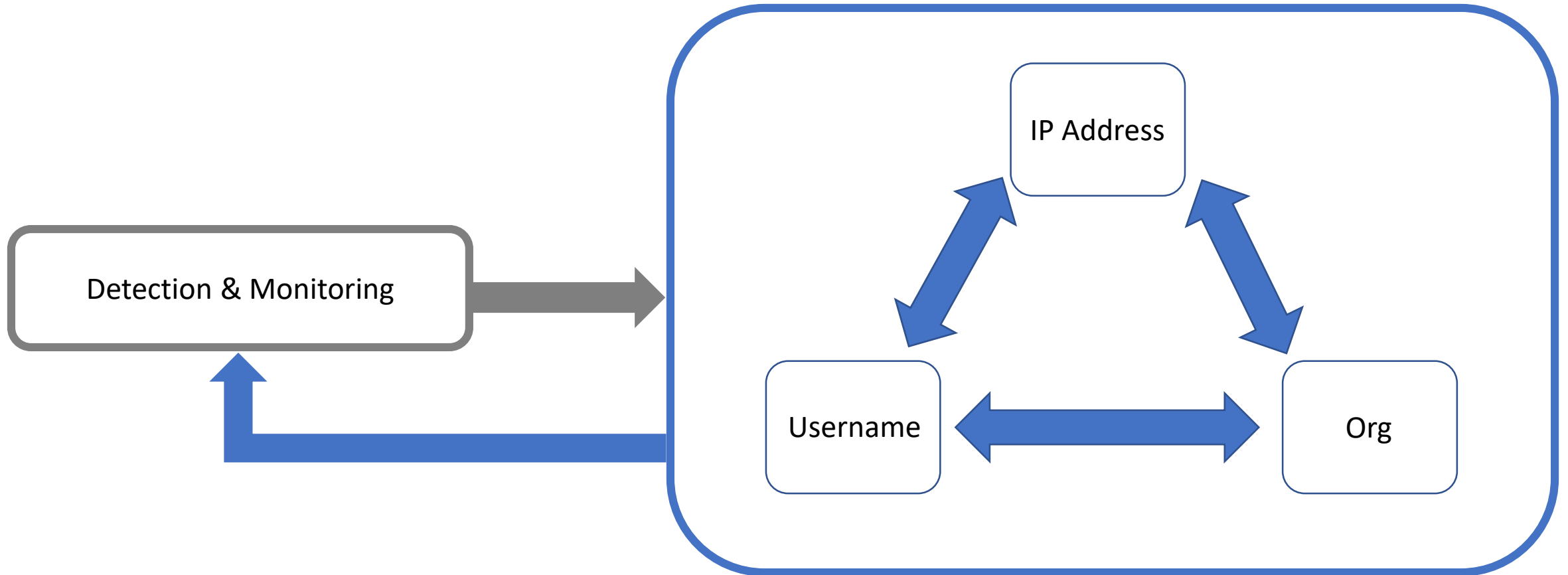
## Bank Accounts Added

No results found.

## User Account sAdded

Time ↕	Username ↕	Created Account ↕	Event Type ↕	Event Desc ↕
2020-06-26 23:10:17	VetStaff1	VetStaff3	User Account	User account VetStaff3 is added by VetStaff1
2020-06-26 23:06:32	VetStaff1	VetStaff2	User Account	User account VetStaff2 is added by VetStaff1

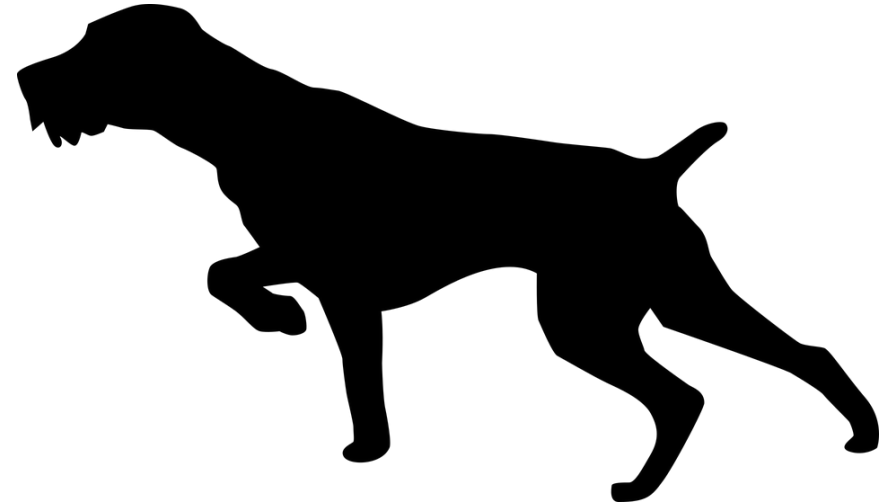
# Pivoting Concepts



**DFUR**

# Applications Where Logs Are Important

- eCommerce
- Financial transactions
- Healthcare services
- MSP
- Travel agents
- Any other type of log data that you could need to analyze

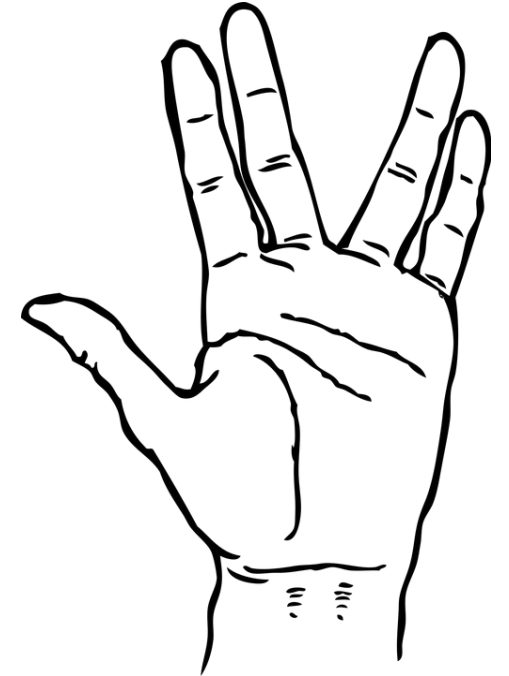


**DFUR**



# Logging Recommendations

- X-Forwarded-For to log true source IP addresses
- Time Zone Documentation – UTC preferred
- Session IDs to connect all relevant events
- Test how long it takes to export log data
- Log both successful and failed activities



**DFUR**

# Final Thoughts

- Reflect on your current logs and capabilities to improve
- Develop investigative workflows that are reliable and repeatable
- Identify pivot points between your data sources, make it easy to move between them
- Lower the technical barrier for analysis



DFUR

# Questions?

- @heferyzan
- @davidpany

**DFUR**