

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

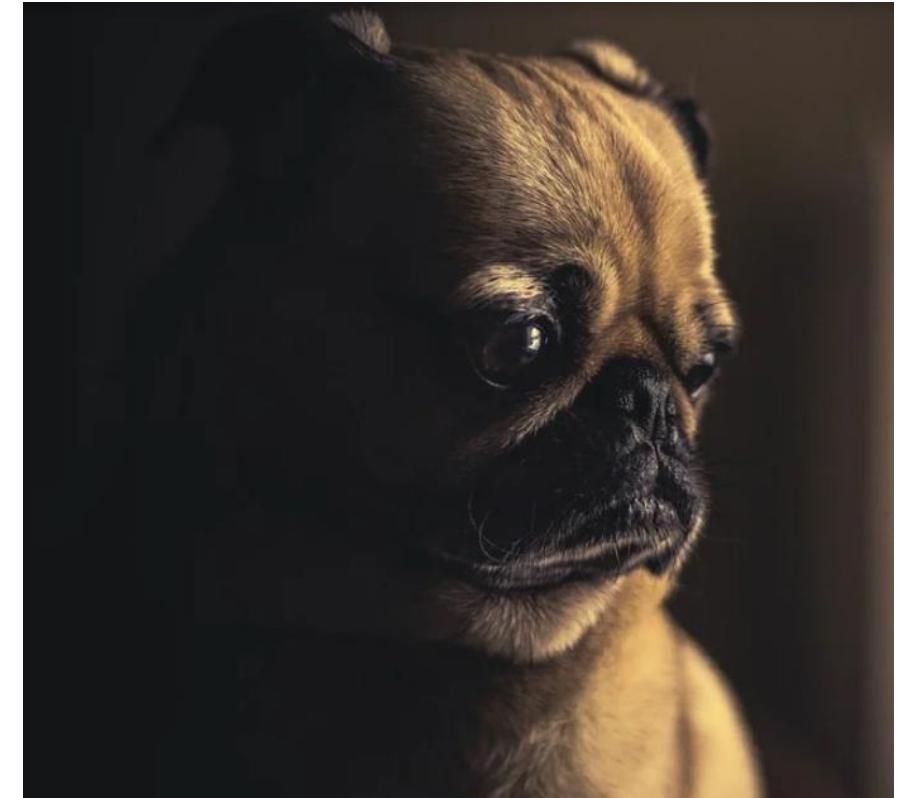
# Logging Problems Identified – Full List

- 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

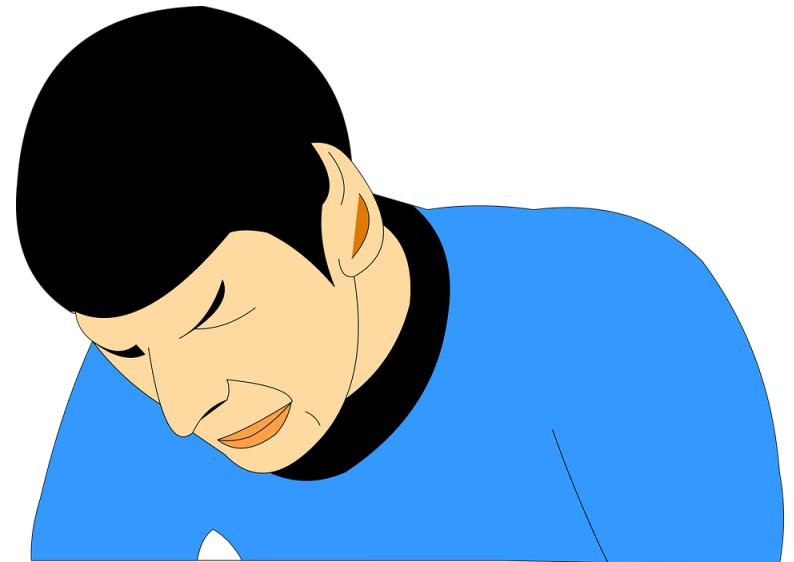
- Incomplete data sources
- Fields parsed to the wrong indices
- Application updates messed up SIEM ingestion
- Time zone misconfigurations
- Takes forever to export
- Source IP addresses masked by proxy



**DFUR**

# Analysis Problems

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



DFUR



# 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

[Edit](#)
[Export ▾](#)
[...](#)

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

[Submit](#)
[Hide Filters](#)
[Account Login Activity](#)
[Application Activity](#)
[Watchlists](#)

## Geolocation Analytics

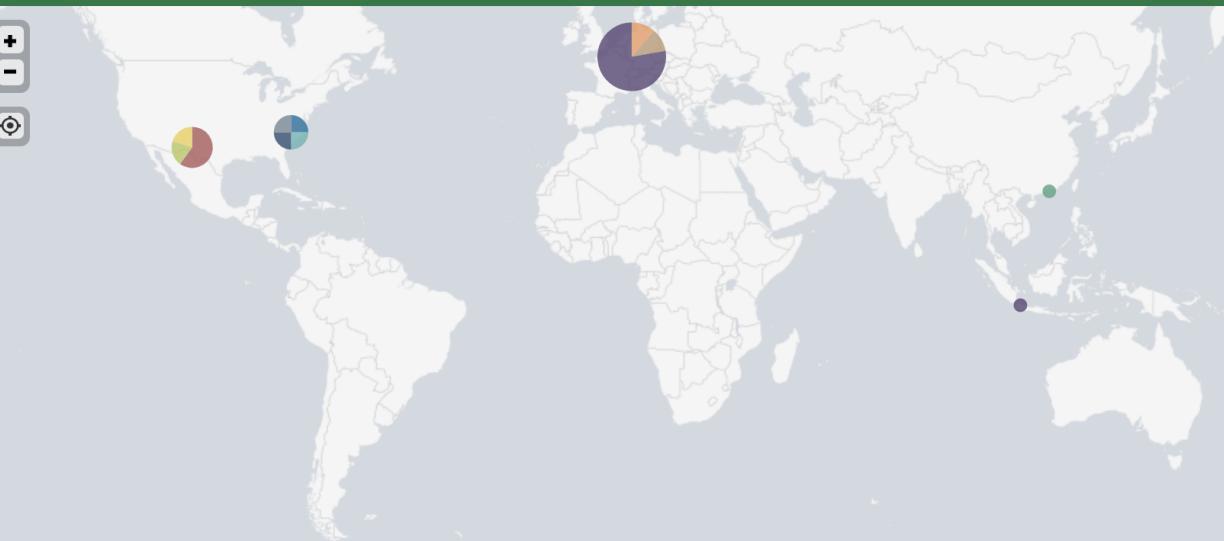
These analytics show geolocation anomalies based on the source IP address of a successful user account authentication attempt.

### 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
labradororable	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

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

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

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

Time	Username	IP Address	Country	Form Email
2020-06-29 10:13:45	jasperlionheart	185.22.172.205	Russia	jasper.s.lionheart2@gmail.com

Time	Username	IP Address	Country	Result
2020-06-29 10:13:45	labradororable	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

19

5

« Prev 1 2 Next »

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	Attempts	Username	Attempts	Provider	Patient							
lunabear	5		1									
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									
100		1		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

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						Organization Creation Geolocation Inconsistent with Organization Location							
<a href="#">« Prev</a> <span style="border: 1px solid #ccc; padding: 2px;">1</span> <span style="border: 1px solid #ccc; padding: 2px;">2</span> <a href="#">Next »</a>													
Username	Entity Name	User IP State	Entity State	IP Addresses	IP Country	Time	Username	Entity Name	Entity State	Event Description	User IP State	IP Address	IP Country
VetStaff1	Little Husky Dieting	not identified	FL	77.243.191.18	Belgium	2020-06-26 23:01:12	VetStaff1	Catitude LLC	VA	Provider Catitude LLC is added by VetStaff1	not identified	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 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; MSNbMSNI; 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; MSNbMSNI; 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
12	4

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

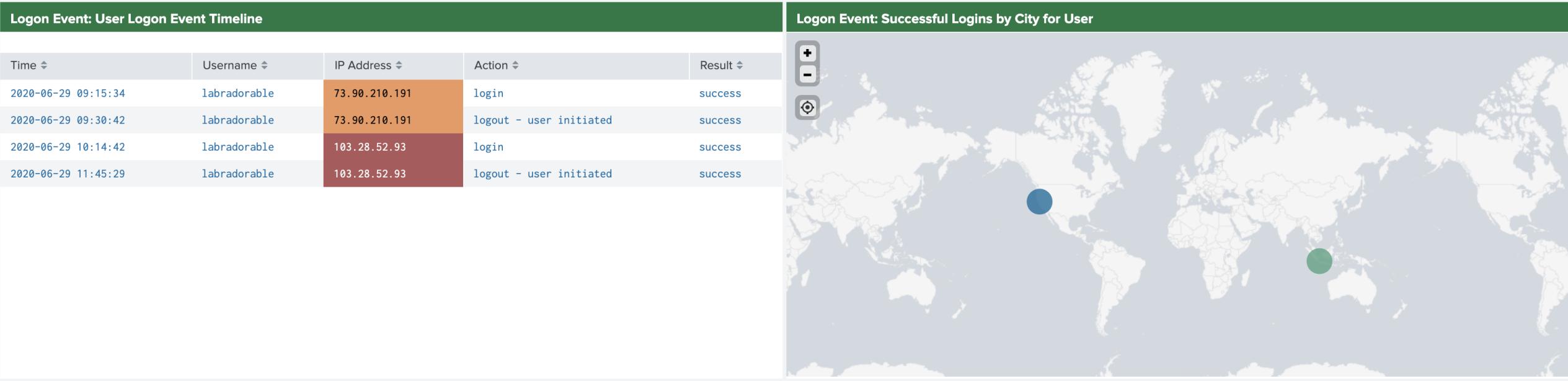
### Account Summary

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	Risk Factor is based on notable user account activities performed during the time window
1 - Username	labradorable	754534	Barkeology Associates Speech Therapy 344 Waldorf Road Sacramento, CA, 94203 (P) 555-2312 (F)	 A circular gauge with a black face and red outer ring, showing a value of 9. The scale ranges from 0 to 20 with increments of 2. The needle is at 9, and the background has green and yellow segments.
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.



Web Application: User-Agents Associated with User				Logon Event: Activity by Source IP for User					Username Reminders and Password Reset Requests				
User-Agent	First Event	Last Event	IP Address	Result	AS Name	State	Country	Count	Time	IP Address	Country	Event Type	Event Desc
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6)	2020-06-29	2020-06-29	103.28.52.93	success	PT Cloud Hosting Indonesia		Indonesia	2	2020-06-29 10:10:05	103.28.52.93	Indonesia	User Account	labradorable has requested a username reminder
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130													
Safari/537.36	09:15:34	09:30:42	73.90.210.191	success	COMCAST-7922 California	California	United States	2	2020-06-29 10:13:45	103.28.52.93	Indonesia	User Account	labradorable has changed password
Mozilla/5.0 (X11; Linux x86_64; rv:10.0) Gecko/20100101	2020-06-29	2020-06-29											
Firefox/10.0	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	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

Last 30 days

labradorable

Submit

Hide Filters

Account Summary Application Activity

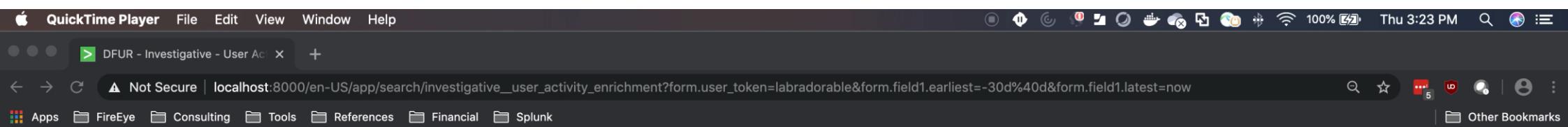
## Application Activity Timeline

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			*	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



### 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 Accounts Added

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									
100			1			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

[Edit](#)[Export](#) ▾

...

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](#)

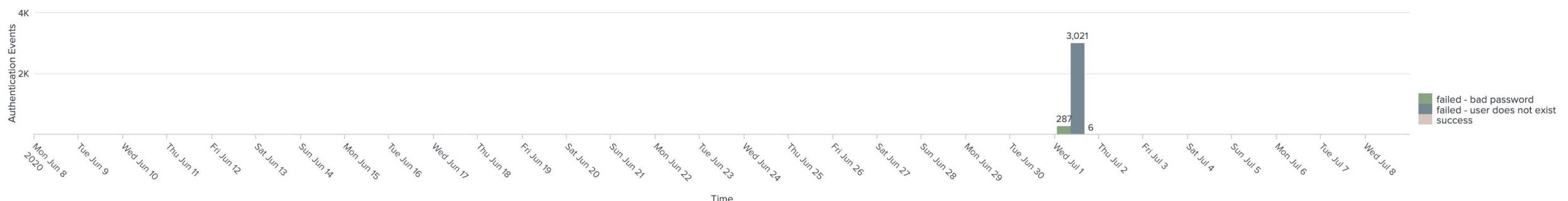
## IP Address Metadata and Organization Summary

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



## IP Address 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			
*	<a href="#">0_Reset Filter</a>							*	<a href="#">0_Reset Filter</a>						
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										
Abigail	1	1	0	2020-07-01 12:13:14	2020-07-01 12:13:14										

Authentication Timeline						
Logon Result						
Success X	Failure X					
		« Prev	1	2	3	4
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.



### 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.

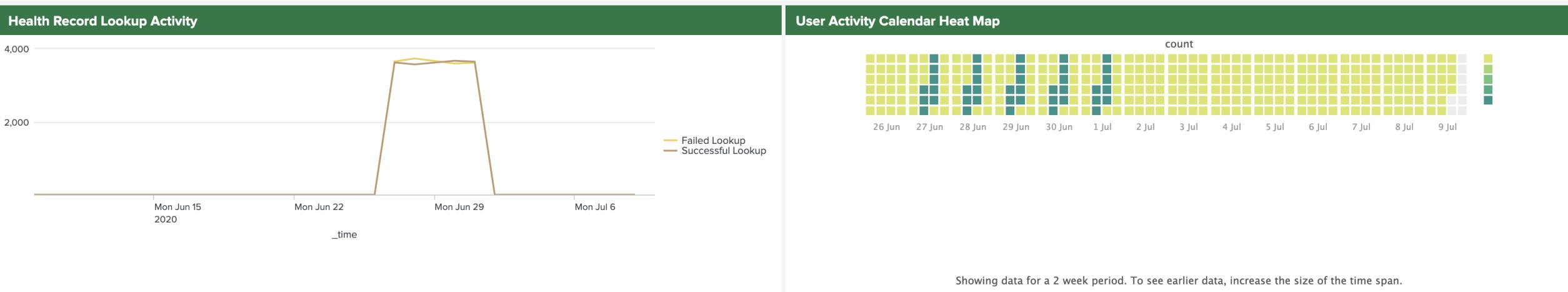
## User Metadata Analytics

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

## User Activity Analytics

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



## 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

[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	Risk Factor is based on notable user account activities performed during the time window
1 - Username	VetStaff1	431133	Little Husky Dieting Nutrition 9873 Snackely Ave. Fort Myers, FL, 33901 (P) 555-8532 (F)	 A circular gauge with a black face and red outer ring, ranging from 0 to 20. The needle is positioned at the number 13.
2 - User ID	3464278	986454	Catitude LLC DME 476 Scratchpost Lane Fairfax, VA, 22031 (P) 555-5123 (F)	
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			
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

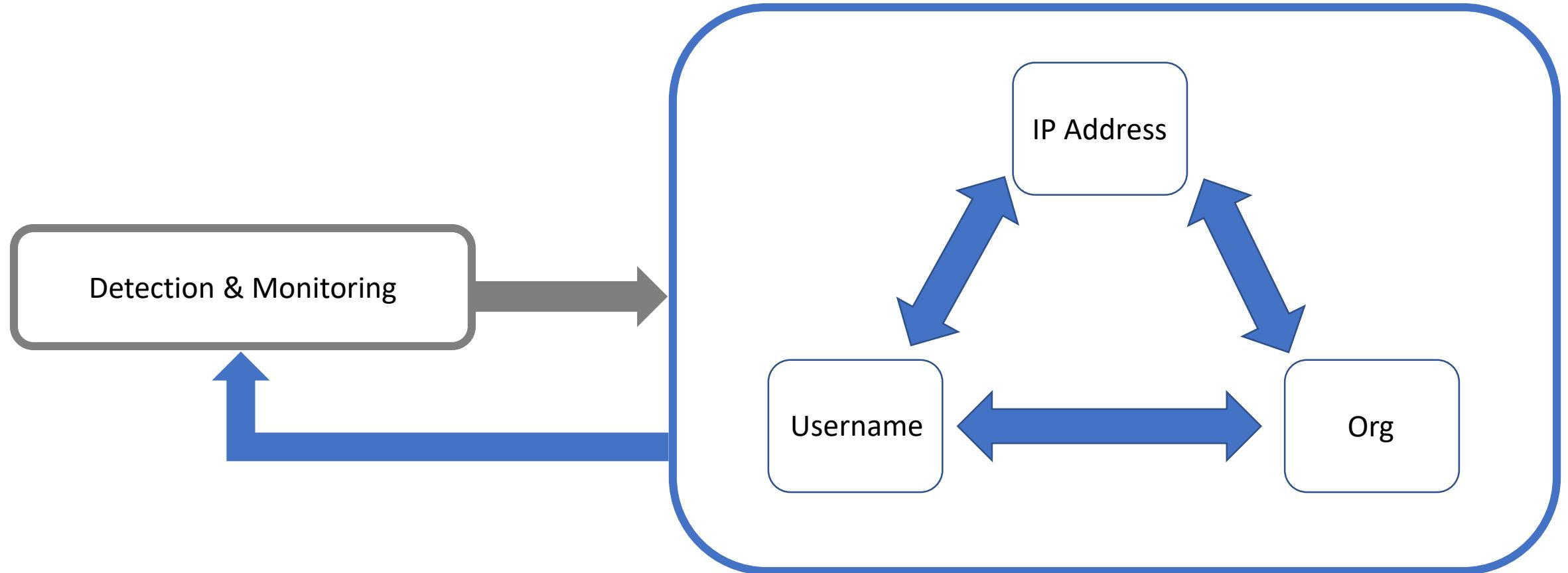
Time	IP Address	Username	Entity Name	Entity ID	NPI	Street Address	City	State
2020-06-26 23:01:12	77.243.191.18	VetStaff1	Catitude LLC	986454	1023423222	476 Scratchpost Lane	Fairfax	VA

### Bank Accounts Added

User Accounts Added				
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

No results found.

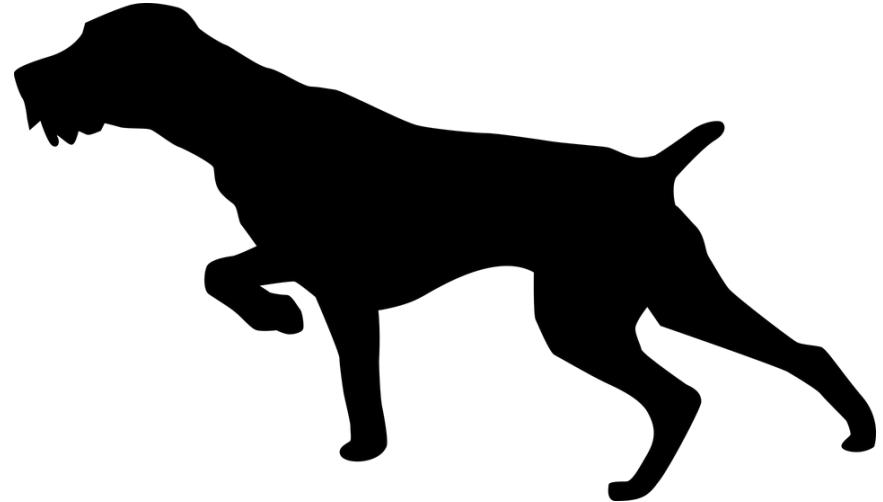
# Pivoting Concepts



**DFUR**

# Applications Where Logs Are Important

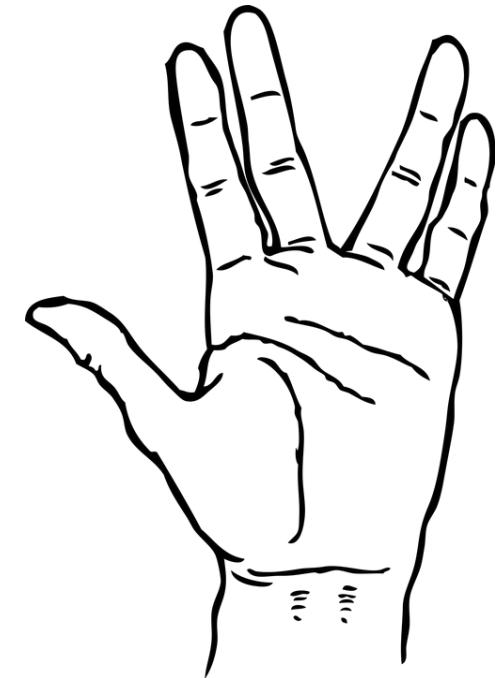
- eCommerce
- Financial transactions
- Healthcare services
- MSP
- Travel agents
- Any other type of log data that you could need to analyze



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