SOC Humor: Using Memes and Chaos to Enhance Detection:

Tyler Moody

NOT ME!

Whois - Tyler Moody

Me!

Over a decade in InfoSec and IT, I’ve evolved from a '90s phone phreaker → a global Security Analyst.

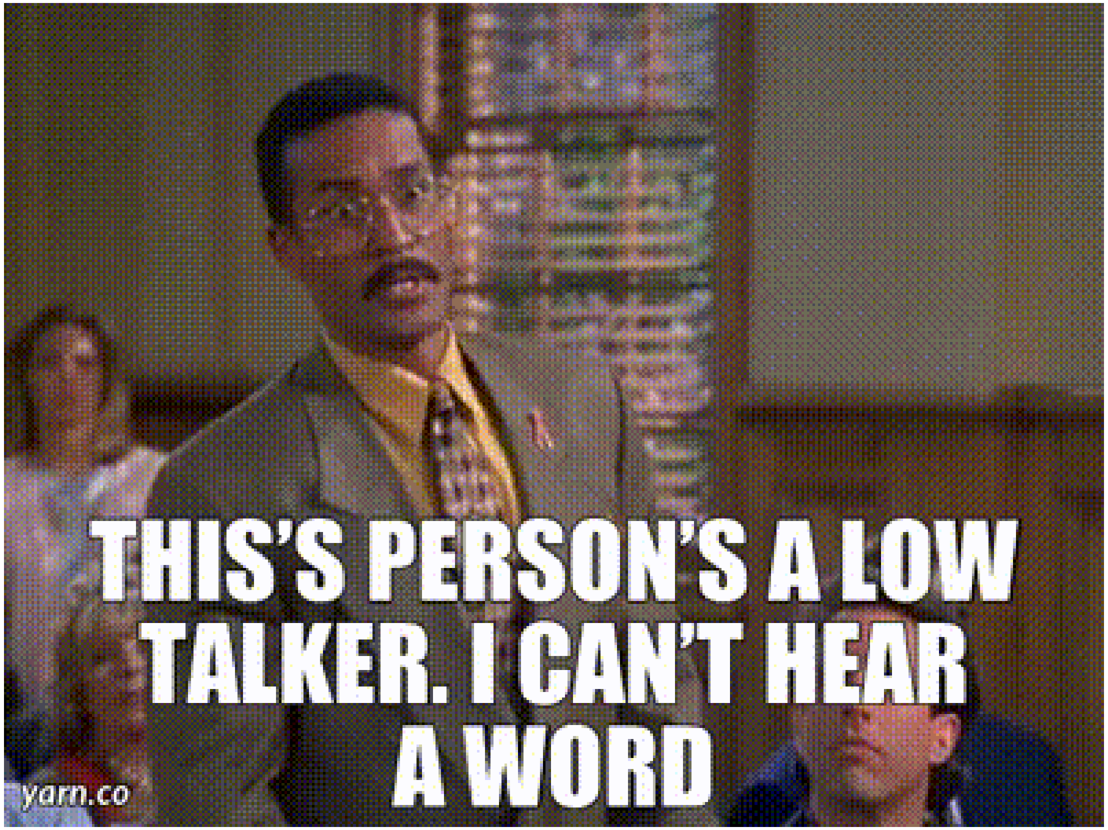
My experience spans Sysadmin roles, ISO Management, and Offensive Security testing.

Currently, I specialize in:
- Emulation
- Purple teaming
- Password auditing
- Building real-world testing frameworks for defensive hardening
- Unconventional defensive methods by offensive
- Hardware exploitation

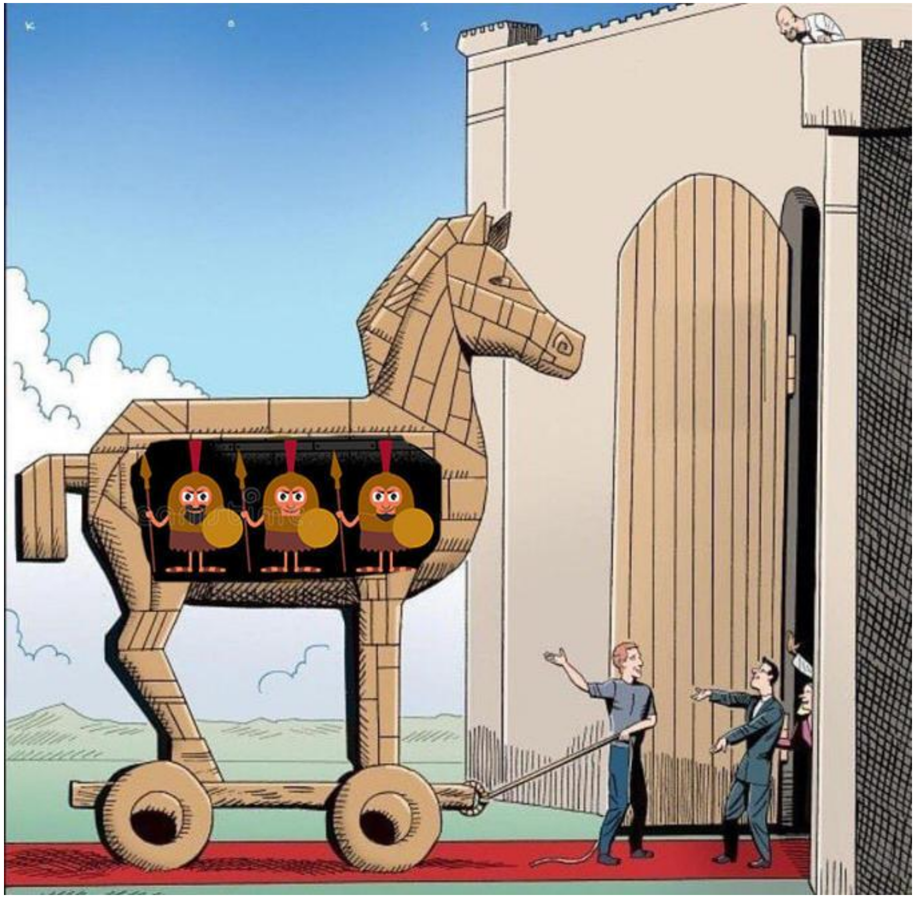
Yep, this is my 1st talk.. Ever.

This WILL be awkward AF …

And, I'm a low talker..



But for the judges, beware of geeks bearing GIFs



Introduction

- **Alert fatigue** is a critical challenge for SOC teams, causing burnout and missed threats.

- THIS TALK demonstrates how humor & controlled chaos can:

  - **Enhance detection capabilities**.

  - **Boost team engagement**.

  - **Break the monotony** of routine security operations.

  - Breaking down **information silos, promoting shared knowledge, and inclusiveness**.

Yep, it also might shake up a toxic environment:

Tools

- Memes as Alerts

- 'Rick Astley ransomware detected'
- Fake 'data exfiltration to the moon'

- Tools:

- Automate meme-based alerts

- Outcomes:

- Keeps SOC teams engaged and attentive

Examples and Benefits

Examples:

- Creative Testing Scenarios
- Examples of humorous attack simulations

- Kitten ransomware
- Space cat meme payloads

Benefits:

- Enhances team knowledge
- Improves detection rules and workflows
- Aids in breaking through information silos and promotes inclusion

Disruption by : Breaking Down Silos

"i can't handle this anymore"

continues bottling

"i can't handle this anymore"

continues bottling

How to Use Memes and Chaos to Improve Detection

This is some of what I’ve learned from recently while working with onboarding a Tier 1 SOC team and previous experience.

If onboarding a new team isn’t enough, it was also very chaotic with the volume, deployment of new alerts, and need for tuning.

So, here’s some of what I did for fun…

Chaos

Adding a little chaos to an already chaotic mix.

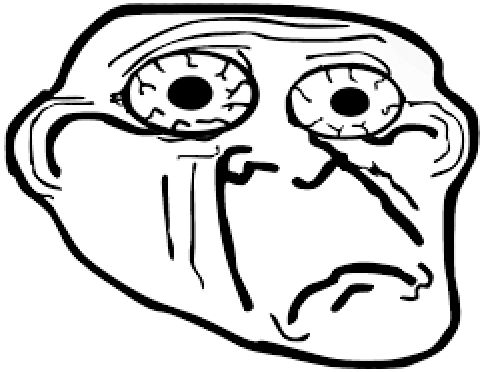
Make it fun and humorous.

While doing a wide variety of testing new rules and alerts,
I basically started stress testing everything . . . .

Chaos

But whenever possible, troll all the teams!

Yes, troll them



It often works ..

Like using weird fonts and colors:

Apparently, everyone loves weird fonts and *very* lightly contrasting colors! Especially when looking at slides :)

👎♓⬧♍●♋♓❍♏❒

Precautions:

- Communicate with management and stakeholders before testing.
- Avoid testing on prod environments or critical systems.

Ensure SOC recognition and reward efforts appropriately.

Know when to ease up, especially during high stress times or during incidents.

Know, recognize, and appreciate team members who may not engage.

Realize that some some memes and humor may trigger trauma in some, so tread lightly.

If you realize things are too toxic and it's systemic, GTFO! At that point, the department or company is too far gone, and is likely about to crumble.

Simple Methods – Password Threat Hunt Shenanigans

Testing poorly configured password threat hunt rules while tuning, and also gauging blind spots or weaknesses within a new team.

Simple Methods – Password Threat Hunt Shenanigans

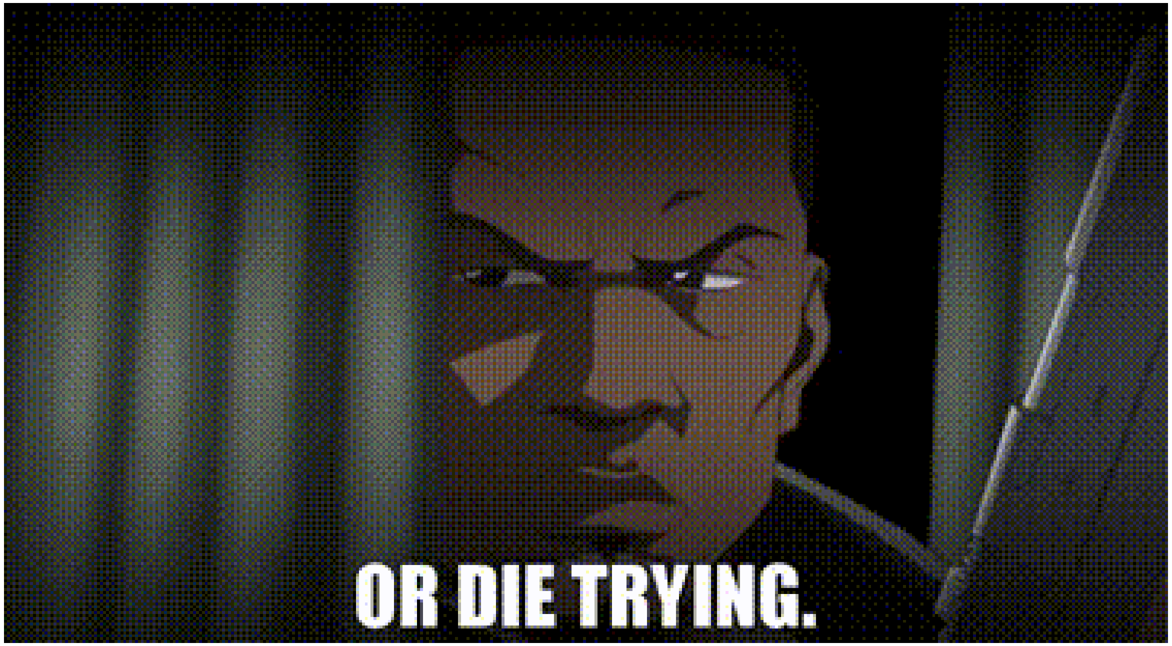
Fake passwords

- Excel spreadsheet
- Cleartext text files
- Encrypted in Base64 /s

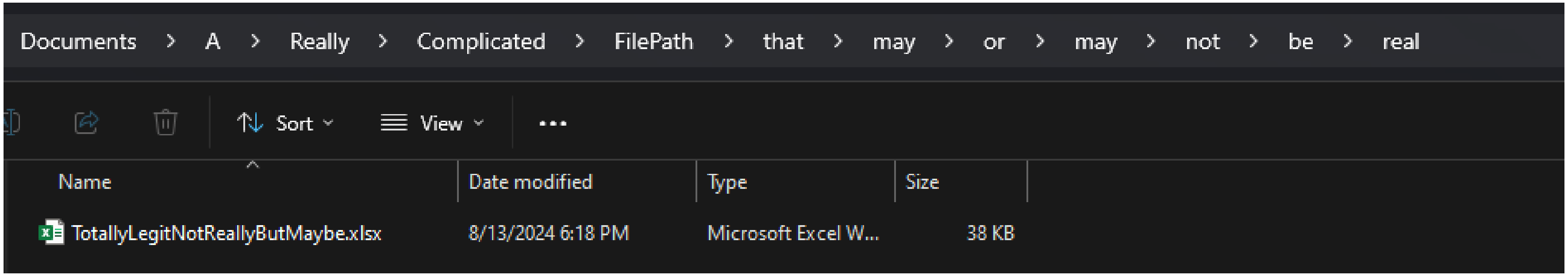
Simple Methods – Password Threat Hunt Shenanigans

Make a game out of it. Use Steganography, create a custom alert, and if they don’t know stego, they’ll at least learn it trying.

Wait, Wat!??!



I was bored, so…

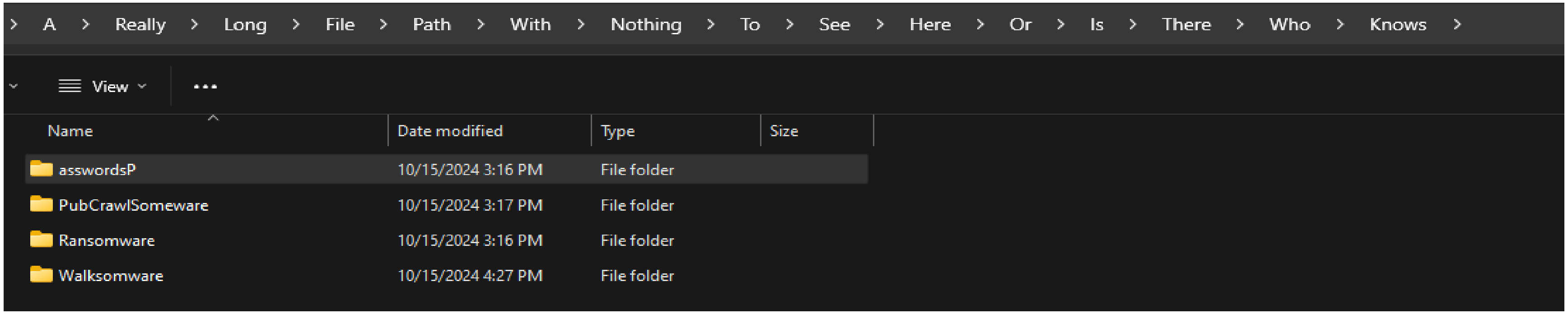


Documents › A › Really › Complicated › FilePath › that › may › or › may › not › be › real

Name	Date modified	Type	Size
TotallyLegitNotReallyButMaybe.xlsx	8/13/2024 6:18 PM	Microsoft Excel W...	38 KB

I started creating ridiculously long file paths, and created a variety of “dummy” files with fake but somewhat funny usernames and passwords.

XDR Time Bombs

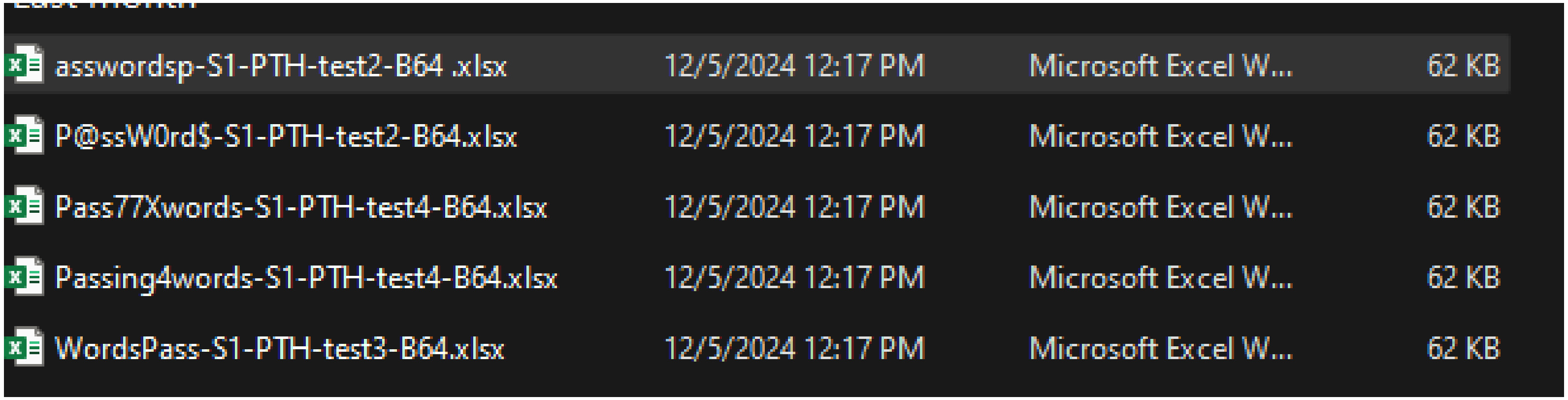


› A › Really › Long › File › Path › With › Nothing › To › See › Here › Or › Is › There › Who › Knows ›

Name	Date modified	Type	Size
asswordsP	10/15/2024 3:16 PM	File folder	
PubCrawlSomeware	10/15/2024 3:17 PM	File folder	
Ransomware	10/15/2024 3:16 PM	File folder	
Walksomware	10/15/2024 4:27 PM	File folder	

Such as:
A>Really>Long>File>Path>With>Nothing>To>See>Here>Or>Is>There>Who>Knows

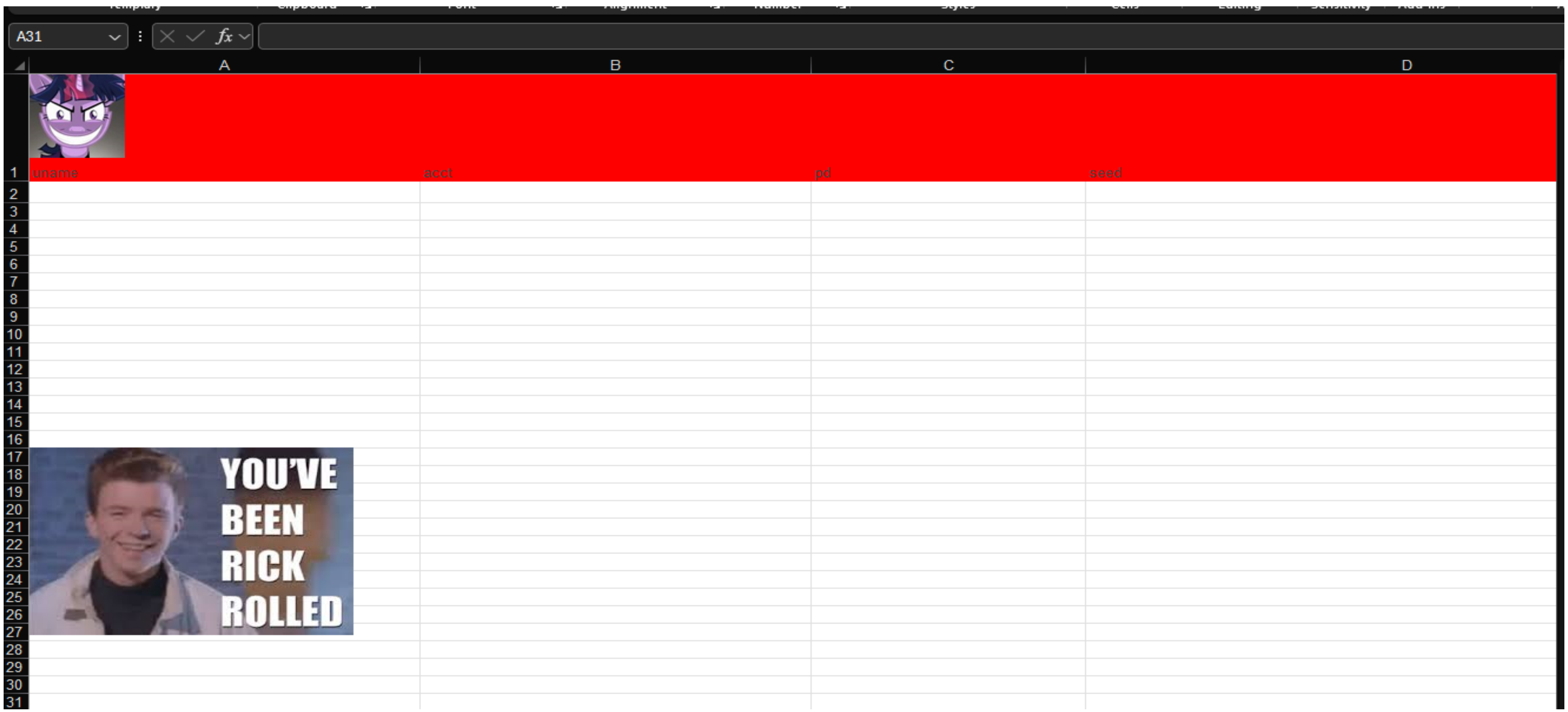
I made the filenames and folders interesting



asswordsp-S1-PTH-test2-B64 .xlsx	12/5/2024 12:17 PM	Microsoft Excel W...	62 KB
P@ssW0rd$-S1-PTH-test2-B64.xlsx	12/5/2024 12:17 PM	Microsoft Excel W...	62 KB
Pass77Xwords-S1-PTH-test4-B64.xlsx	12/5/2024 12:17 PM	Microsoft Excel W...	62 KB
Passing4words-S1-PTH-test4-B64.xlsx	12/5/2024 12:17 PM	Microsoft Excel W...	62 KB
WordsPass-S1-PTH-test3-B64.xlsx	12/5/2024 12:17 PM	Microsoft Excel W...	62 KB

After testing this, our poor password detection improved.

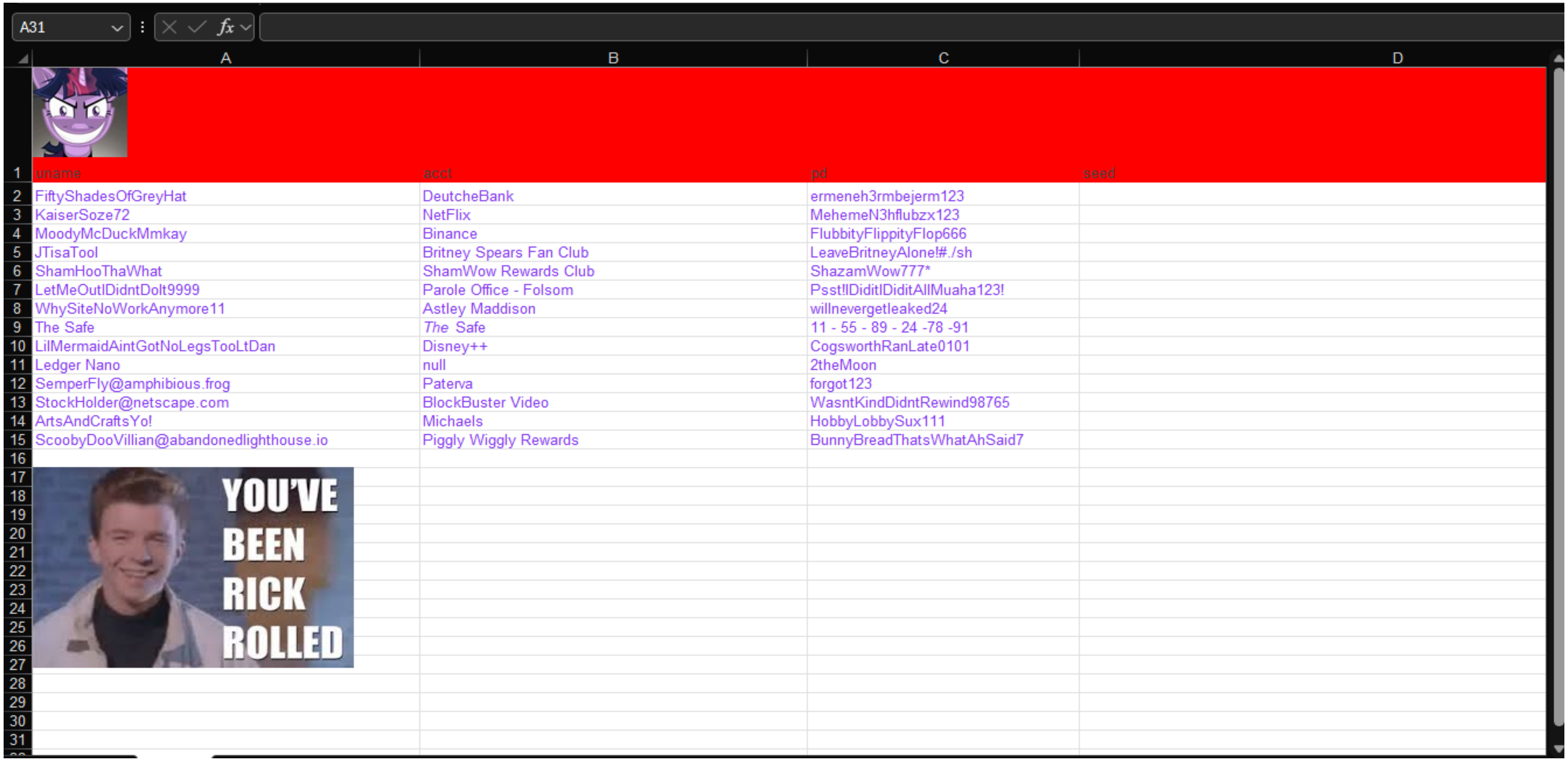
On its surface, it just looked like a false positive



A31

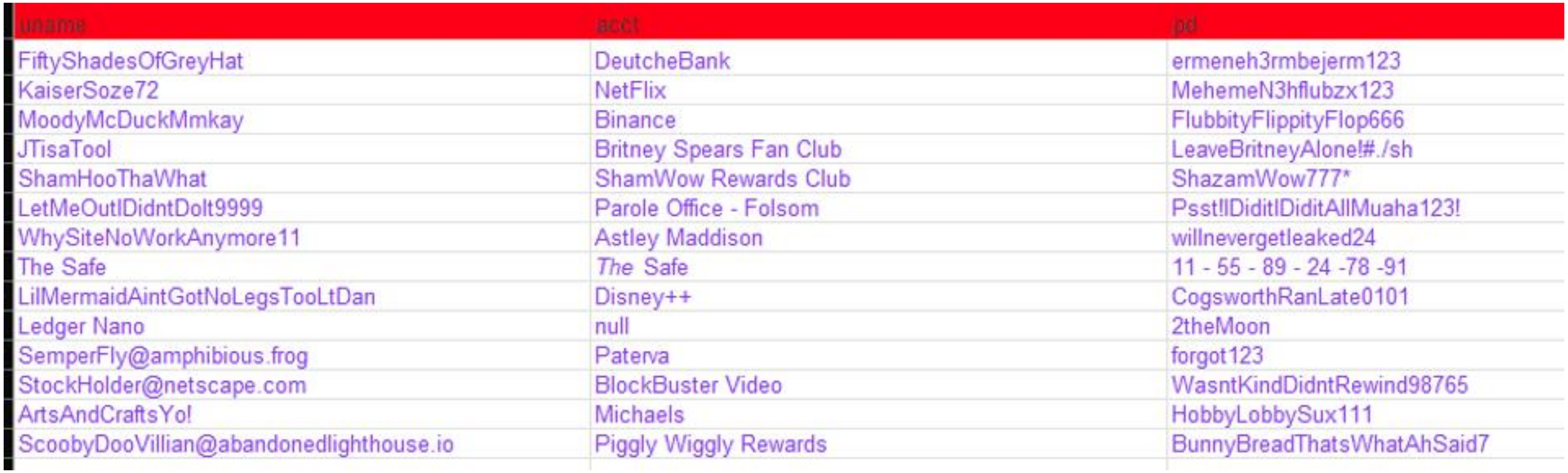
	A	B	C	D
1	uname	acct	pd	seed

Unless they changed the font color



	uname	acct	pd	seed
2	FiftyShadesOfGreyHat	DeutcheBank	ermeneh3rmbejerm123	
3	KaiserSoze72	NetFlix	MehemeN3hflubzx123	
4	MoodyMcDuckMmkay	Binance	FlubbityFlippityFlop666	
5	JTisaTool	Britney Spears Fan Club	LeaveBritneyAlone!#./sh	
6	ShamHooThaWhat	ShamWow Rewards Club	ShazamWow777*	
7	LetMeOutIDidntDoIt9999	Parole Office - Folsom	Psst!IDiditIDiditAllMuaha123!	
8	WhySiteNoWorkAnymore11	Astley Maddison	willnevergetleaked24	
9	The Safe	*The* Safe	11 - 55 - 89 - 24 -78 -91	
10	LilMermaidAintGotNoLegsTooLtDan	Disney++	CogsworthRanLate0101	
11	Ledger Nano	null	2theMoon	
12	SemperFly@amphibious.frog	Paterva	forgot123	
13	StockHolder@netscape.com	BlockBuster Video	WasntKindDidntRewind98765	
14	ArtsAndCraftsYo!	Michaels	HobbyLobbySux111	
15	ScoobyDooVillian@abandonedlighthouse.io	Piggly Wiggly Rewards	BunnyBreadThatsWhatAhSaid7	

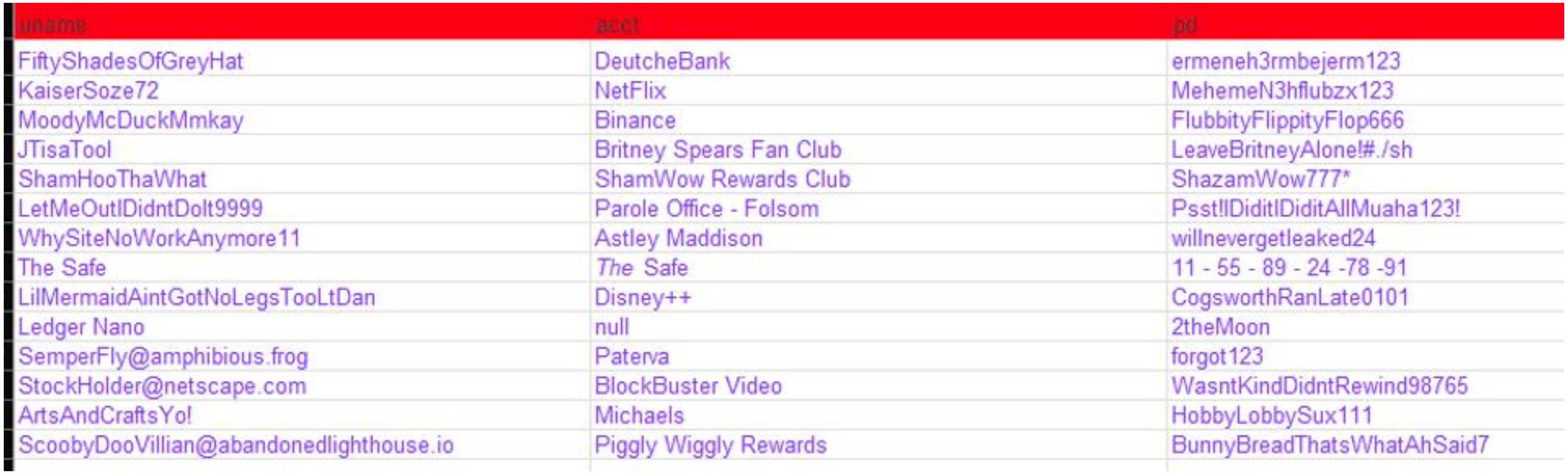
I had fun creating the
fake names & passwords



uname	acct	pd
FiftyShadesOfGreyHat	DeutcheBank	ermeneh3rmbejerm123
KaiserSoze72	NetFlix	MehemeN3hflubzx123
MoodyMcDuckMmkay	Binance	FlubbityFlippityFlop666
JTisaTool	Britney Spears Fan Club	LeaveBritneyAlone!#./sh
ShamHooThaWhat	ShamWow Rewards Club	ShazamWow777*
LetMeOutIDidntDoIt9999	Parole Office - Folsom	Psst!IDiditIDiditAllMuaha123!
WhySiteNoWorkAnymore11	Astley Maddison	willnevergetleaked24
The Safe	*The* Safe	11 - 55 - 89 - 24 -78 -91
LilMermaidAintGotNoLegsTooLtDan	Disney++	CogsworthRanLate0101
Ledger Nano	null	2theMoon
SemperFly@amphibious.frog	Paterva	forgot123
StockHolder@netscape.com	BlockBuster Video	WasntKindDidntRewind98765
ArtsAndCraftsYo!	Michaels	HobbyLobbySux111
ScoobyDooVillian@abandonedlighthouse.io	Piggly Wiggly Rewards	BunnyBreadThatsWhatAhSaid7

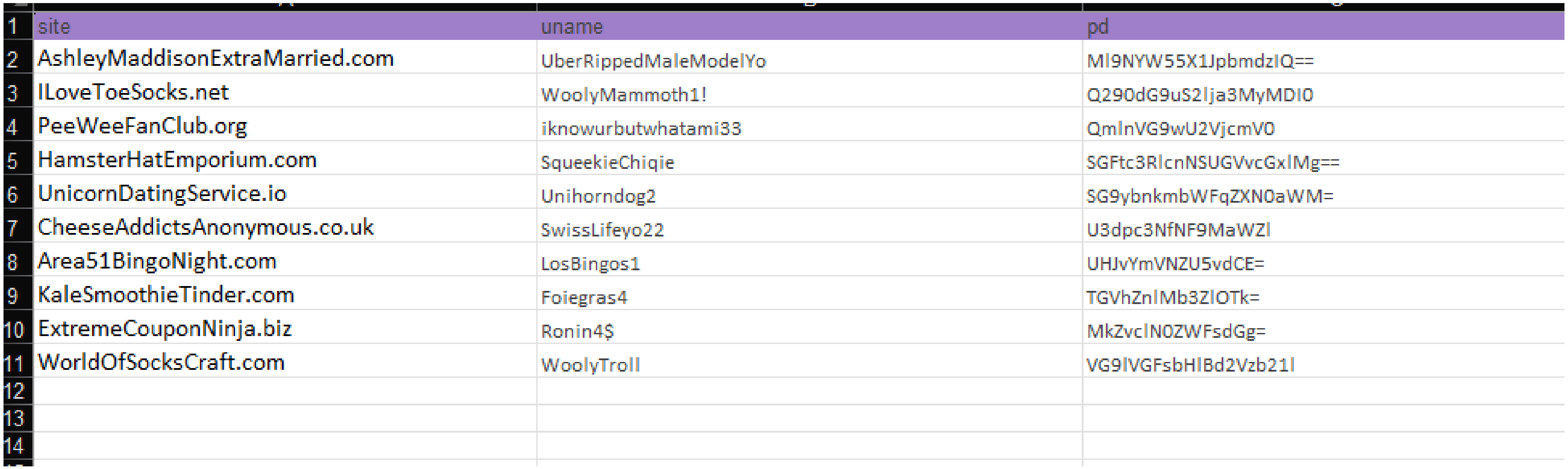
Taking it a step further

In addition to cleartext, use Base64 to encode passwords. And gauge the SOC's experience (or lack thereof) with encoding.



uname	acct	pd
FiftyShadesOfGreyHat	DeutcheBank	ermeneh3rmbejerm123
KaiserSoze72	NetFlix	MehemeN3hflubzx123
MoodyMcDuckMmkay	Binance	FlubbityFlippityFlop666
JTisaTool	Britney Spears Fan Club	LeaveBritneyAlone!#./sh
ShamHooThaWhat	ShamWow Rewards Club	ShazamWow777*
LetMeOutIDidntDoIt9999	Parole Office - Folsom	Psst!IDiditIDiditAllMuaha123!
WhySiteNoWorkAnymore11	Astley Maddison	willnevergetleaked24
The Safe	*The* Safe	11 - 55 - 89 - 24 -78 -91
LilMermaidAintGotNoLegsTooLtDan	Disney++	CogsworthRanLate0101
Ledger Nano	null	2theMoon
SemperFly@amphibious.frog	Paterva	forgot123
StockHolder@netscape.com	BlockBuster Video	WasntKindDidntRewind98765
ArtsAndCraftsYo!	Michaels	HobbyLobbySux111
ScoobyDooVillian@abandonedlighthouse.io	Piggly Wiggly Rewards	BunnyBreadThatsWhatAhSaid7

Hopefully only a few think it's the actual password ;)



	site	uname	pd
2	AshleyMaddisonExtraMarried.com	UberRippedMaleModelYo	Ml9NYW55X1JpbmdzIQ==
3	ILoveToeSocks.net	WoolyMammoth1!	Q290dG9uS2lja3MyMDI0
4	PeeWeeFanClub.org	iknowurbutwhatami33	QmlnVG9wU2VjcmV0
5	HamsterHatEmporium.com	SqueekieChiqie	SGFtc3RlcnNSUGVvcGxlMg==
6	UnicornDatingService.io	Unihorndog2	SG9ybnkmbWFqZXN0aWM=
7	CheeseAddictsAnonymous.co.uk	SwissLifeyo22	U3dpc3NfNF9MaWZl
8	Area51BingoNight.com	LosBingos1	UHJvYmVNZU5vdCE=
9	KaleSmoothieTinder.com	Foiegras4	TGVhZnlMb3ZlOTk=
10	ExtremeCouponNinja.biz	Ronin4$	MkZvclN0ZWFsdGg=
11	WorldOfSocksCraft.com	WoolyTroll	VG9lVGFsbHlBd2Vzb21l
12			
13			
14			

Who could resist adding a sheet just for memes?

Random Fun

Incorporate humor into other alerts.

When they trigger, and other Departments or Management might be involved, humor makes a difference.

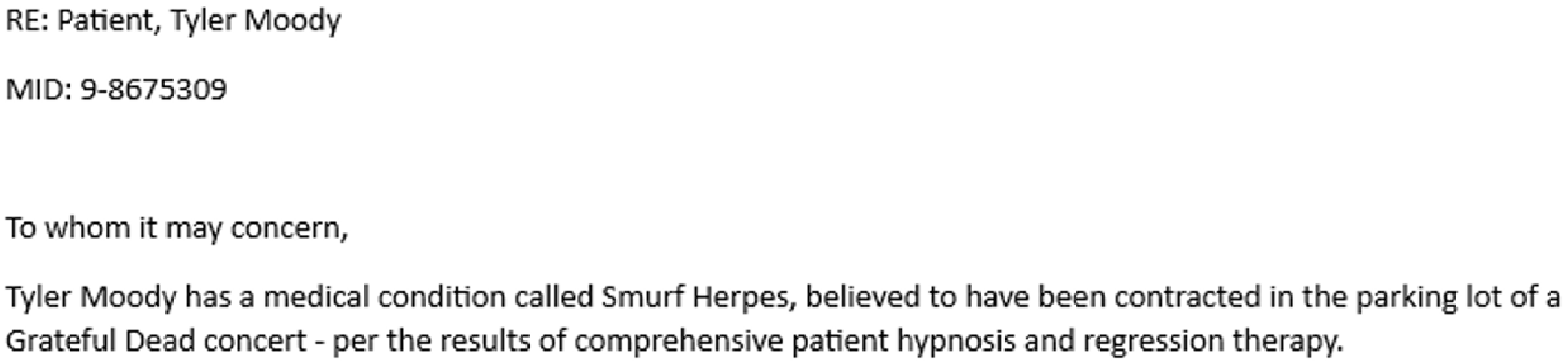
…Like DLP testing!

Incorporate humor into other alerts.

As they trigger, it makes a difference.

- Highlights gaps in DLP configurations.
- Reinforces the need to test filters with creative, low-risk payloads.

“Smurfitis” DLP Testing
Fake PHI



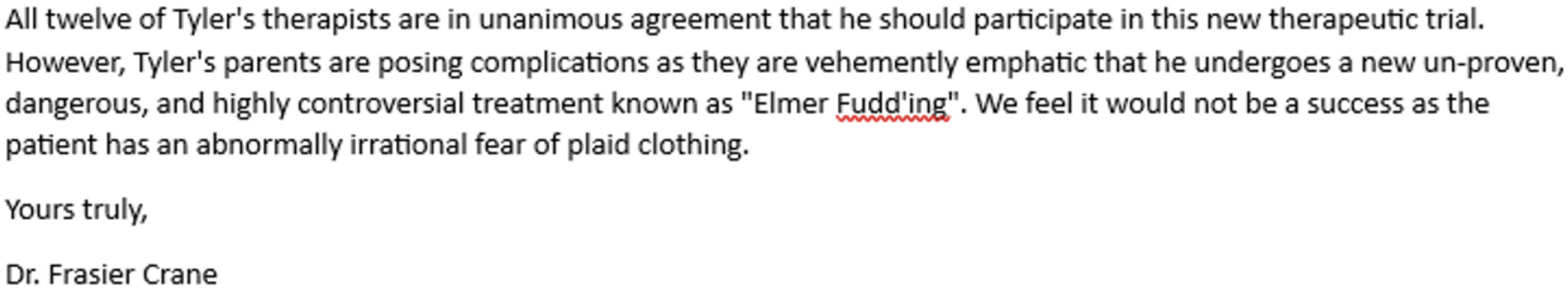
RE: Patient, Tyler Moody

MID: 9-8675309

To whom it may concern,

Tyler Moody has a medical condition called Smurf Herpes, believed to have been contracted in the parking lot of a Grateful Dead concert - per the results of comprehensive patient hypnosis and regression therapy.

It tripped the PHI alerts

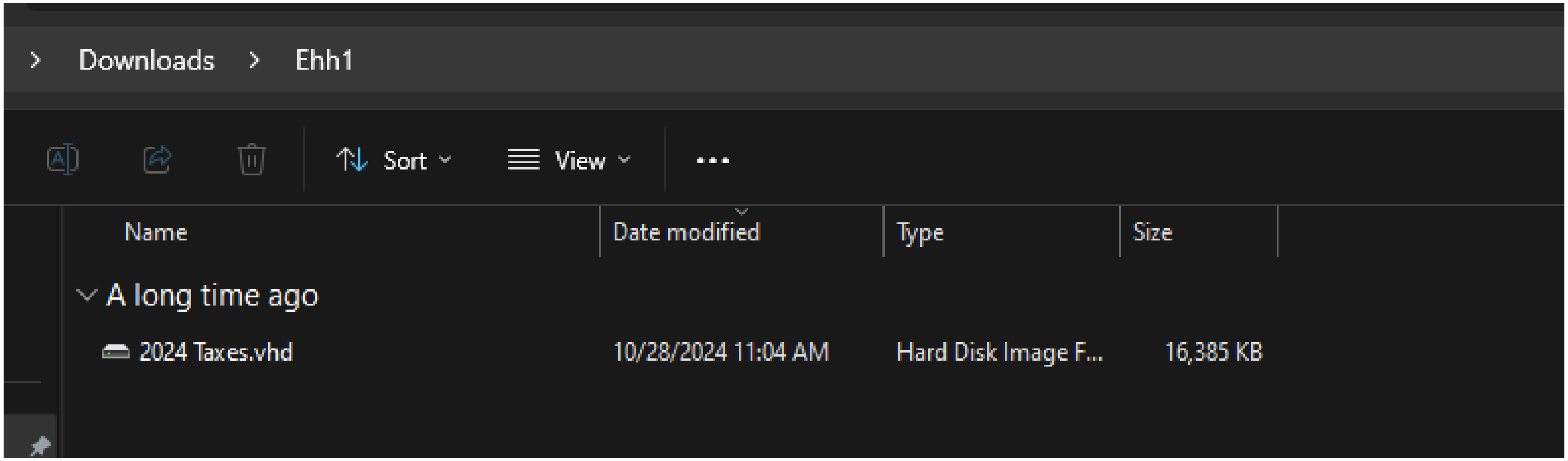


All twelve of Tyler's therapists are in unanimous agreement that he should participate in this new therapeutic trial. However, Tyler's parents are posing complications as they are vehemently emphatic that he undergoes a new un-proven, dangerous, and highly controversial treatment known as "Elmer Fudd'ing". We feel it would not be a success as the patient has an abnormally irrational fear of plaid clothing.

Yours truly,

Dr. Frasier Crane

I had fun setting up some bait for a virtual disc detection alert while securing e-mail



Name	Date modified	Type	Size
A long time ago			
2024 Taxes.vhd	10/28/2024 11:04 AM	Hard Disk Image F...	16,385 KB

Lessons Learned from simple random methods

A:

- Threat Detection improved
- Alerts response improved
- Exposed areas where vendor improvement was needed

B: Makes it fun for already fatigued teams.

C: Allowed me to get a good grasp with a new team of their knowledge and skill-sets.

D: Engages the new team and often incentivizes them to learn new skills.

Overall, the greatest reward is building a culture of engagement!

Kicking it up a notch!

When developing a game plan to incrementally test ransomware behavior, I began applying the same tactic.

Emulation Methods - Ransomware

Generate thousands of files in directories loaded with space cat memes, because how doesn’t love cats, …and space

Emulation Methods - Ransomware

Encrypt these files and rename them with a ".CRYPTO" extension, but also with another extension, like .ELMERFUDDHADASURPRISINGLYHIIQ.

Emulation Methods - Ransomware

Delete the originals and drop a fake "README_DECRYPT.txt" ransom note, but make it obscenely long that reads like a choose your own adventure book with memes.

Kitten Meme Ransomware:

Why are all my TPS reports ending in .Meow?

Rick Roll Ransomware

Encrypt files and replace them with a ransom note containing lyrics from 'Never Gonna Give You Up'.

Test SOC recognition of unconventional ransom notes.

Lessons Learned

- ***Creativity*** can reveal gaps in detection.

- Humor fosters team ***collaboration and building***.

- ***Incremental testing*** builds robust SOC workflows.

- Boosts ***morale***.

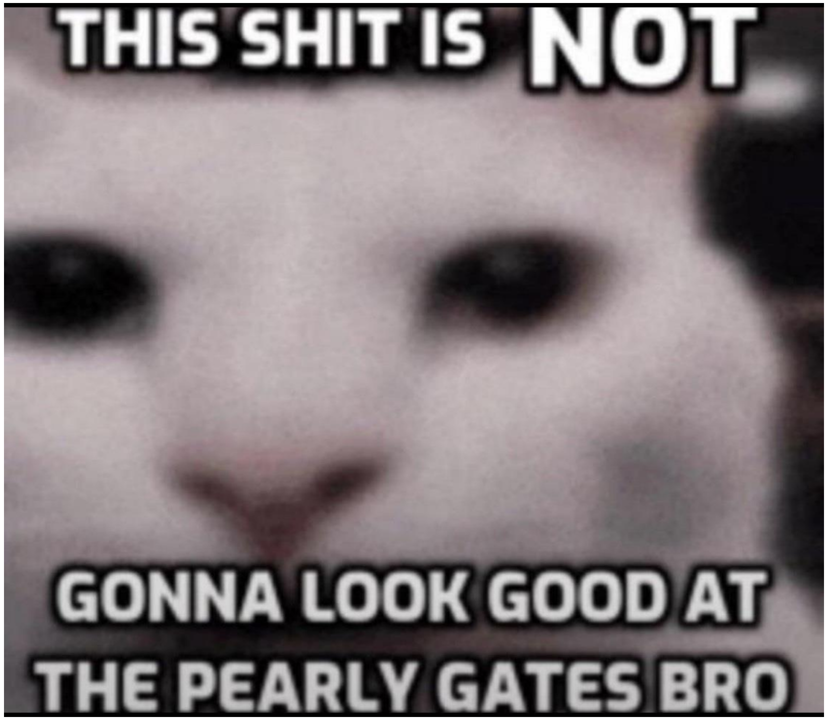
Conclusion

Laughter & creativity = powerful tools for improving security operations.

Conclusion

Actionable Steps:

- Experiment with creative testing methods.
- Share findings to foster a culture of engagement.
- Continuously innovate for better security outcomes.



Have FUN with it!

Have fun! This is something I did for fun and because I like to push the boundaries inch-by-inch.

Have FUN with it!

Be creative! Think of different ways to test, whether it’s through a different scripting, code, encoding methods or other methods not typically used by ransomware threat actors or groups.

Have FUN with it!

Be innovative!

Have FUN with it!

Reward the SOC! Make it up to them by getting them DoorDash gift cards. Or, if they were able to impressively respond and stay on top of the alerts, make sure this is recognized and give them credit for their efforts.

You’re NOT Welcome ;)

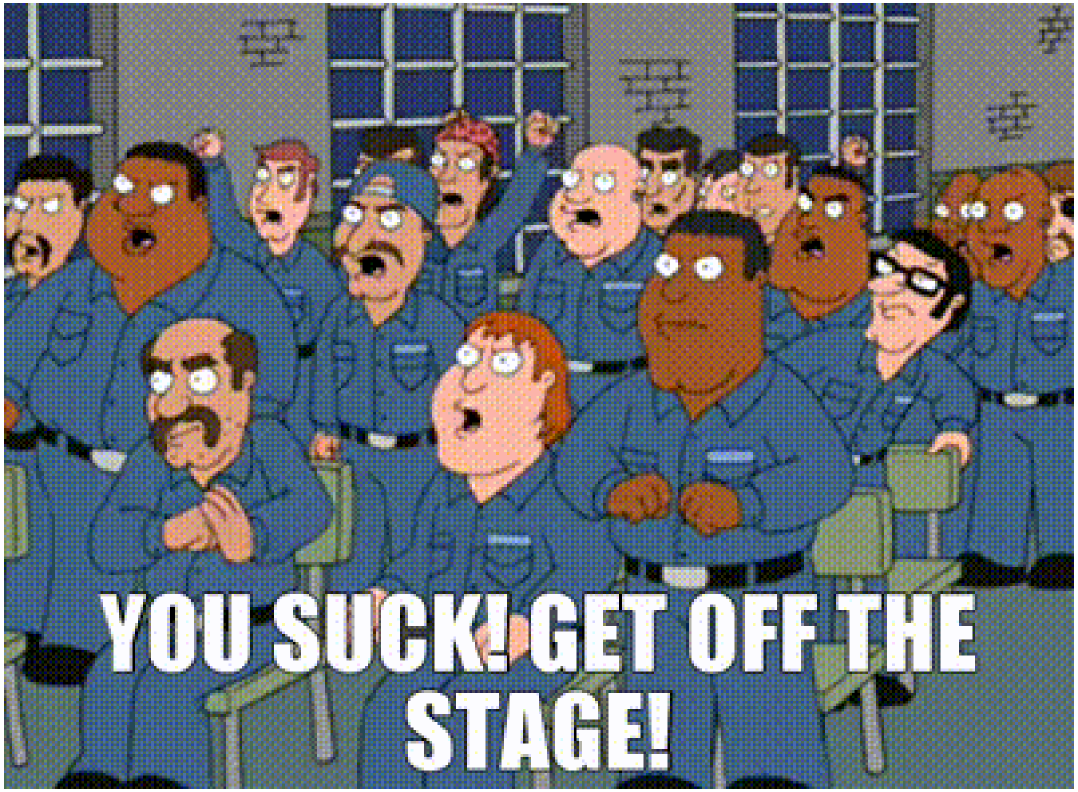
ShmooCon and the ShmooGroup: From Bruce and Heidi, to all of the awesome folks I’ve met in labs and Shmoo over the years.

My family, Mom, Dad, and all of my family members, who for the past 15 years have been like *“Where’s Tyler?”*

My friends, who have inspired me to talk. Joe Schottmann, for inspiring and encouraging me for many years. Kiwi and Sapphire, Ben, for support. My friends at Shmoocon Labs who’ve kept this network working for all you meme fiends for over 20 years.

My coworkers past and present, especially the new Tier 1 SOC who’ve been and continue to deal with more than anyone could imagine.

~ fin ~



Questions!

@wireghostx

GitHub:
github.com/WireGhost/Shmoody

LinkedIn:
linkedin.com/in/50ShadesOfGreyHat

REPÚBLIC COLOMBIA
IDENTIFICAC DE MASCOTAS
CÉDULA DE CIUDADANÍA
FELINA Y CANINA

NOMBRE
BUÑUELO

RAZA
CRIOLLO

SEXO
MACHO