CHOOSE YOUR OWN DISASTER

Zippy Spacedirt and the Spiders from the WEB!

YOU'RE the star of the story! Can YOU safely solve the cloudy mystery?

Who is this clowns?

CRob has over 25 years of Development, Enterprise Operations, Support, and Security experience most major industries: Retail, Legal, Medical, Financial, Insurance, Manufacturing, & Technology.

He currently work to secure free software.

CRob

Cat Herder

Red Hat Inc.

Your mission, should you choose to accept it, is to ***participate*** in an interactive **mock** disaster.

You are ***equipped*** with your wits, your experiences, and the assistance of the ladies and gentlemen surrounding you here in the room today.

BUT… to those ***lucky*** few who **DO** survive…. fabulous riches and fame beyond your wildest dreams await you at the turn of the page…… (We were rooting for you all along!)

You all will be faced with many difficult, yet ***exciting*** choices.

We're going to be honest here….. most of you aren't going to make it. Sorry, it's just that **MATH** is against you. Thanks for coming today. (We knew they'd never get through….seriously…just look at them.)

ZOMG! Where are the SERVERS?!?!?

It is bright and early Monday morning. It started off like every other normal day. No one plans to have a bad day, but they sometimes happen. After entering the datacenter you gasp in horror! The server racks are empty! What do you do?

Race around in a panic!

Go to Page 200

Call Physical Security!

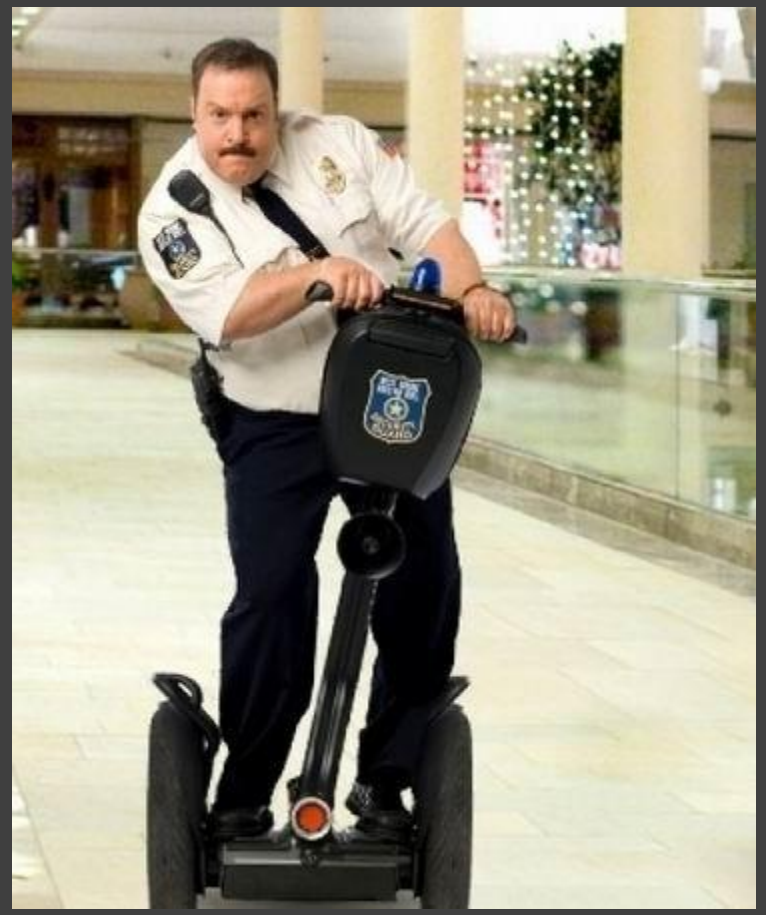
Go to Page 98

Oh wait, we moved all our servers to the cloud last week

Go to Page 25

200

Great job! Very impressive! You have a bright future ahead of you as you start your first day of a new job search after you're walked out of the building. Go back to Page 1 and start over.



Your partners in physical security immediately leap to action. One mentions "We did have an alarm on an open door down in the underbasement. Want to join me and check it out?

Turn to Page 67

98

67

Going to the underbasement was a poor choice.

Your legend will live on in tales around the water cooler for days to come.

Go back to Page 1 and start over.

The cloud is a lie!!! It's just a computer in some dude's garage!!! Go back to Page 1 and start over.

Hahahahahaha… just kidding.

With your missing server problem sorted out, you hurry off to your first meeting of the day: BUDGETING! (yay!) Turn to the next page

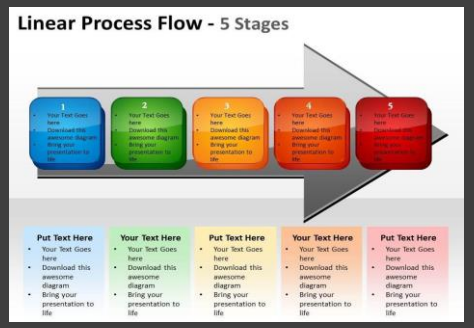
What was it again your company does?

We’re fast, efficient, and talented consultants. We’re General Requestable Economic consultants for Advanced Technology (GREAT!). We specialize in placing highly skilled contractors for mission-critical work, for low, low costs!

How should you allocate your security budget?

We'll spend our budget on the best PEOPLE!

Go to Page 16

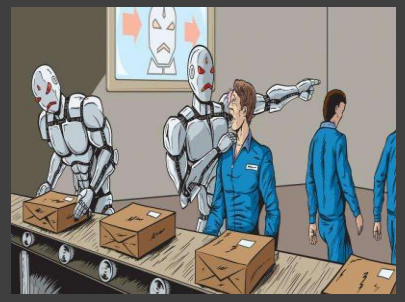


Go to Page 17

We'll spend our budget on developing the best PROCESSES

We'll spend our budget acquiring the best TECHNOLOGY

Go to Page 18



It is a bright, shiny day. There is not a cloud in the sky (those are all in your datacenter!). Having combed LinkedIn for the best and brightest employees you feel that there is NO problem you can not tackle!

You have recently landed a big contract to deploy a new website for a major government client. Your team is responsible for the development, maintenance, and support of the site.

16

Day One

Isn't it time for our weekly status report team meeting?

Go to Page 1019

We should all head down and have some coffee.

Go to Page 1020

Let's see what the SOC reported from overnight.

Go to Page 1021

You LOVE the smell of fresh documentation in the morning! It smells like VICTORY! There is NO problem and thoroughly documented process can not solve!

You have recently landed a big contract to deploy a new website for a major government client. Your team is responsible for the development, maintenance, and support of the site.

17

Day One

It's an exciting time of the year… our client's quarterly documentation audit! Yay!

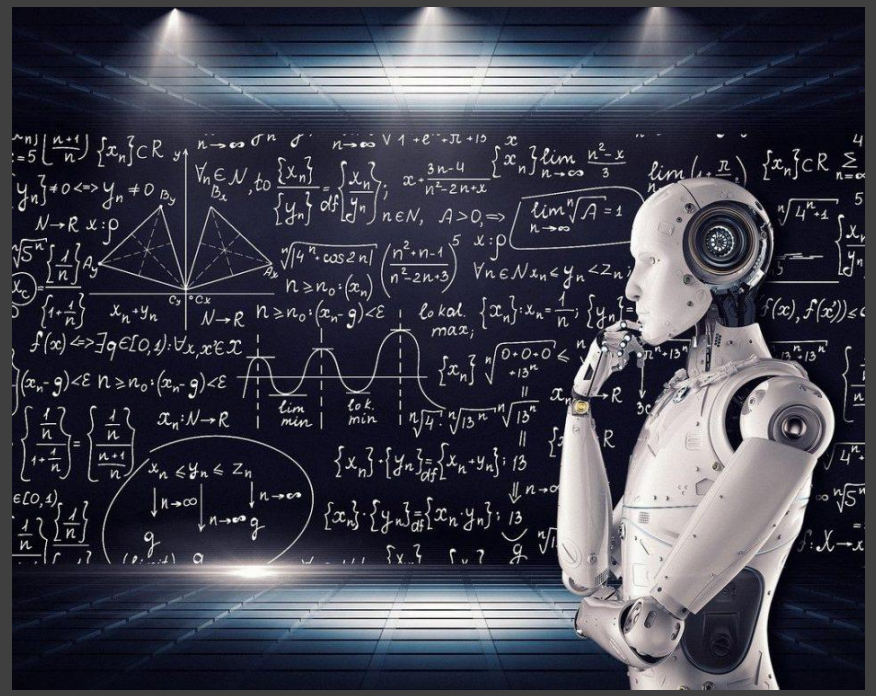
Go to Page 75

8am Monday Change Advisory Board meeting… YES!!!

Go to Page 96

The SOC reports 34,863 alerts that need review from overnight.

Go to Page 112



You can’t be everywhere at once, but your robots can! AUTOMATE ALL THE THINGS! You can’t recall any time that technology has failed you, so you HEAVILY fund tools and automation to augment your small staff.

You have recently landed a big contract to deploy a new website for a major government client. Your team is responsible for the development, maintenance, and support of the site.

Spend some time tweaking your mail filters & rules to ensure OPTIMAL efficiency

You staff tells you that the Automotron9000 scripting system needs upgraded this week.

The SOC robot reports it addressed 34,862 alerts overnight.

Go to Page 117

Go to Page 145

Go to Page 1022

18

Day One

EVERYONE **LOVES** a great Monday morning status report review (I know it's the highlight of MY week!!)!

1019

Yeah…your boss is going to need you to work late this week…..

Your NEXT meeting is a backlog grooming session with your prime stakeholder.

Your pager keeps going off, something from the SOC.

Go to Page 25

Go to Page 26

Go to Page 36

While your team is quite happy (and nicely caffeinated), your client was desperately trying to call you while you were out (probably was a bad idea bringing the receptionist Jake along with you for coffee too).

Their brand new website is COMPLETELY OFFLINE and the client is demanding it to be back online immediate and wants RCA (Root Cause Analysis) within the hour!

1020

Maybe that was all the pages from the SOC. Well, finish up your coffee and head on back. You still have 5 minutes left on your break.

Go to Page 2024

Ask your client to fill out a Service Desk ticket. If the Service Desk can't solve it, they'll escalate to you.

Go to Page 2023

It breaks the support process, but maybe you should look at the website now.

Go to Page 2021

1021

Bert, the lead SOC analyst, holds his head with a pained look on his face. Overnight the SOC received 34,863 …no, wait…. 34,864, no 5….a lot of alerts. You get the idea.

Bert and the team look at YOU expectantly…..

Oh. OK. Huh.

Go to Page 22

Ask to do an audit of the app & review product deployment documentation

Go to Page 68

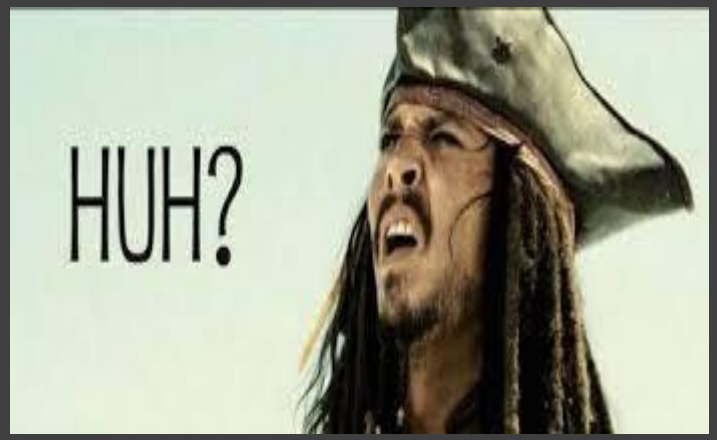
That sure sounds like a fun puzzle, team. I have the UTMOST confidence you'll all figure it out eventually!

Go to Page 70,000

1022

Your heart starts to beat faster. You face feels flush. Sweat slowly starts trickling down your side from your arms-crossed armpits. You blurt out “Oh.....OK. Huh.”

Bert glares at you.



Wow. That sure sounds like a lot of alerts. Maybe someone can take some time out of their day to spot check them?

Go to Page 31

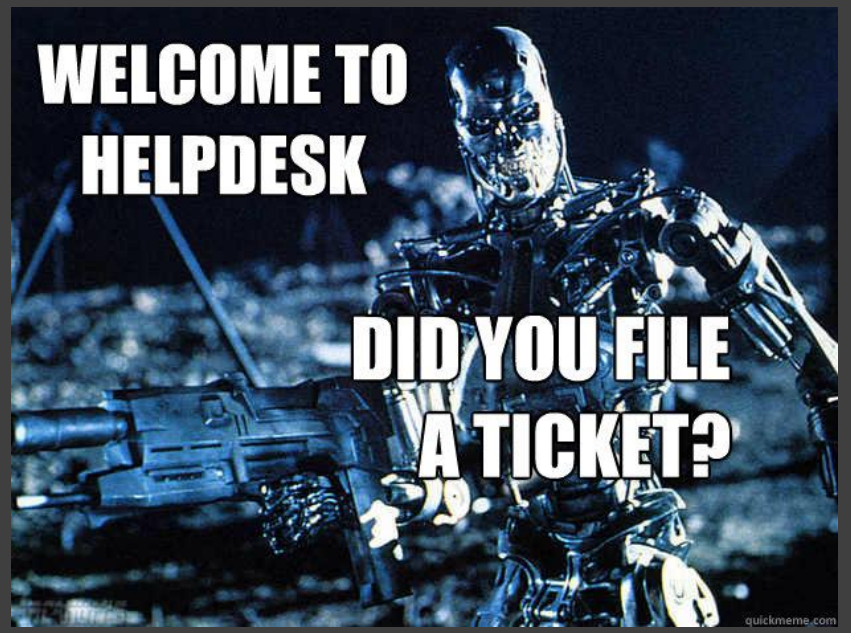
That Automotron9000, what a marvel of modern miracles! It can help us here!!

Go to Page 10028

2023

I mean, seriously. The customer can't expect YOU to do ALL the work. You point them to the Help Desk to get this all worked out. The Help Desk is the BEST place to get this thing solved!

Now that breaktime is over maybe you can catch up on those webinars you've been putting off watching. Gotta get those cpes!!



Proceed to Day Two

You know...everyone always enjoys a nice coffee break. It's that 5 or 6 times a day you can slow things down, talk, drink coffee, get to know people. Coffee breaks are great. Marty from accounting joins you today, you really like that Marty guy.

….. your break finishes uneventfully.

2024

Day One

[Proceed to Day Two]

Nothing bolsters morale like mandatory late hours and weekends! You stare across the conference room table at a sea of angry faces.

The day grinds on and attitudes deteriorate.

25

Day One

[Proceed to Day Two]

Those tasks aren't going to prioritize themselves! The team "eagerly" moves into backlog grooming.

The project manager drones on and on. The analog clock on the wall ticks are like thunder, beating away the seconds of your life slowly..ever so slowly slipping away.

Ghant charts are *neat*.

26

Day One

Craig the Consultant has an awesome new process he thinks will generate a lot of income. It has a lot of "cyber" in the title. Do you consider adding implementing it into the backlog?

Go to Page 1,000,463,027

Thinking back to your pager, maybe you could sneak out down to the SOC to "check up" on things. Sad/NotSad about leaving the meeting.

Go to Page 1021

You know, if you put the word “cyber” in front of things, it REALLY DOES make them better”

CYBERsecurity -- MUCH more secure now
CYBERspace -- MUCH cool place to go
CYBERpunk -- I think THESE punks are OK!
CYBERkittens -- ...I mean, obviously better
CYBERsharks -- Hella-scary

Your day continues on “cyber-ing”. You forget all about your troubles……

1,000,463,027

Day One

[Proceed to Day Two]

10,028

From the dark corner of the datacenter, the Automatron9000 glares at you, almost hungrily. It dutifully begins processing the alert data you feed it.

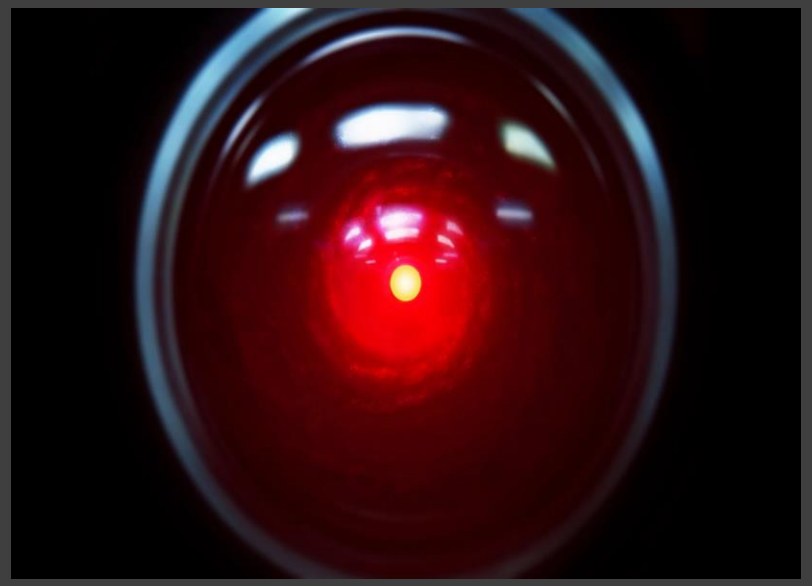
Without emotion or pride it proclaims that the website if in the middle of a Denial of Service Attack. It also forwards its analysis to the CISO, since you are too much of a sqwishy meatbag to be able to do that.

“Thanks AT9K! You’re going to fix all that, right?”

Go to Page 29

Double-check AT9K’s work

Go to Page 41



"Oh, I'll FIX IT, meatbag, I'll fix it."

The Automatron9000 whirs away for a few seconds, goes 'BING', and a greenbar printout is made of the changes it executed.

Mission Accomplished. Now that THAT's done, what's for lunch?

29

Day One

[Proceed to Day Two]

1020

While your team is quite happy (and nicely caffeinated), your client was desperately trying to call you while you were out (probably was a bad idea bringing the receptionist Jake along with you for coffee too).

Their brand new website is COMPLETELY OFFLINE and the client is demanding it to be back online immediate and wants RCA (Root Cause Analysis) within the hour!

Maybe that was all the pages from the SOC. Well, finish up your coffee and head on back. You still have 5 minutes left on your break.

Go to Page 2022

Ask your client to fill out a Service Desk ticket. If the Service Desk can't solve it, they'll escalate to you.

Go to Page 2023

It breaks the support process, but maybe you should look at the website now.

Go to Page 2021

31

As much of a drag as it can be to go through logs and stuff, you roll up your sleeves and start logging into servers to check the logs.

After a few hours of work (and missing lunch. You HATE missing lunch on Taco Tuesdays) you discover a dozen or so external IPs have been hammering the website.

What do you do?

It's probably nothing. You're sure it will resolve itself.

Go to Page 1032

Check your Threat Intel tool to see if it's got any info.

Go to Page 33,000

Have the network team block those addresses immediately!

Go to Page 2036

Keep researching

Go to Page 41

Grammy always said to get a good night's rest and your problems won't seem as big the next day.

She lived to be 103, so she MUST have done something right.

...she also enjoyed a big glass of bourbon every night before bed. mmmmm….bourbon. Yummy, caramelly, oaky, yummy nectar of the gods. You should go get a tasty bourbon.

What we were talking about anyway?

1032

Day One

[Proceed to Day Two]

Your salesguy was VERY confident that the CYBERDYNAMIC CYBERPROACTIVE CYBERTHREAT CYBERINTELLIGENCE tool he sold you would solve ALL of your cyber-problems. The CYBERTHREATMASTER9000 has a few different threads you may wish to explore.

33,000

Day One

ZOMG Kerblackistan rebels have targeted YOUR COMPANY because your facilities have paper towels in the washrooms.

Go to Page 34,034

The CYBERTHREATMASTER9K tells you that the pings of death….. are coming from *INSIDE your* network!

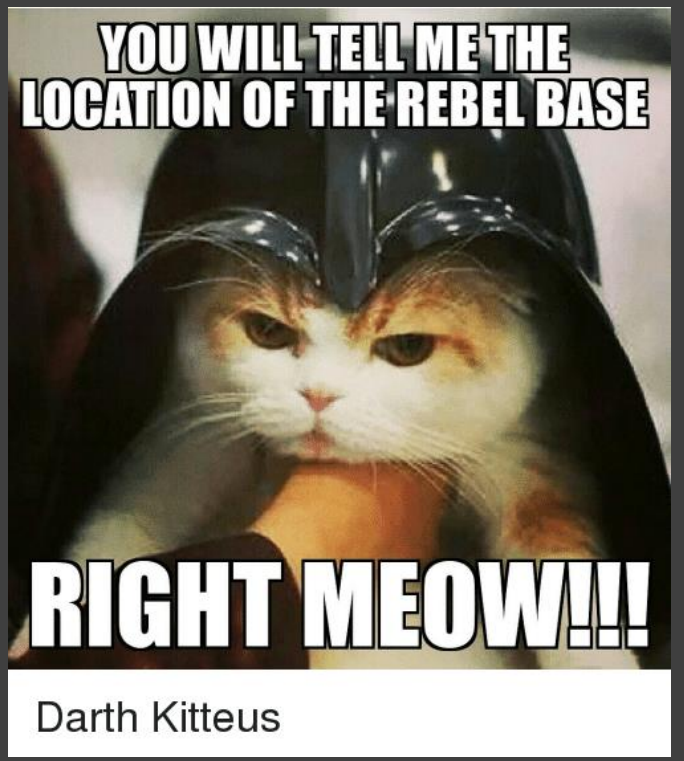
Go to Page 2036

This intelligence isn't all THAT intelligent. It is ALSO boring. (buzz buzz) Oh dear…you're, uh (buzz buzz) getting paged. You'd better go!

Go to Page 35

Wow. Rebels. That sounds pretty serious. WAY above your pay-grade for sure. It sure was a good thing you all sprung for this swanky tool to warn you about them.

You file a TPS report, send it to your boss and head off to lunch.

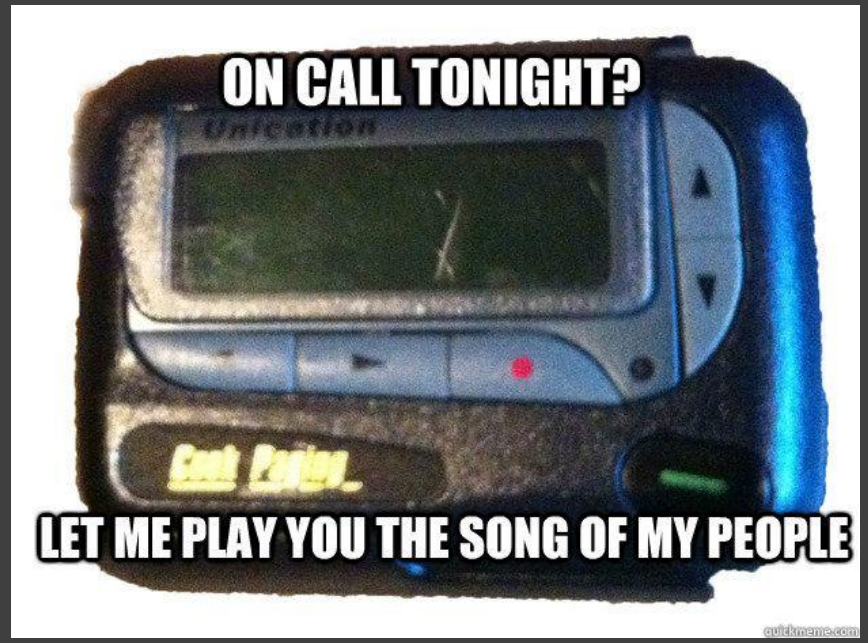


34,034

[Proceed to Day Two]

Ha Ha Ha! They fell for the old “fake pager page” trick AGAIN! You quickly sneak out of the room chuckling softly to yourself.

...and those kids at Beef O’Brady’s mocked you for having that pager on your belt last Tuesday at trivia night. Who is laughing NOW, punks?



35

[Proceed to Day Two]

2036

Day One

Since the attack is coming from INSIDE THE NETWORK you decide to race down to talk to the Network team! You journey down into the bowels of the headquarters…. into…. **the IT department.**

You talk to Rory Thistlebrush, head of Networking. He looks at you in horror. A *Business* Person…..here….gasp!

He listens intently as you describe what the CYBERTHREATMASTER9000 found. “Yes. That sounds like you’re in need of …. (mwahahaha.) MY assistance!

So….is there anything we can do about that?

Help articulate the business problem

Go to Page 51,037

Go to Page 38

51,037

Day One

"Of course there is NOTHING ***you*** can do (mwahaha.)."

"Well, that sure sounds pretty final."

Go to Page 52

"So....is there anything ***WE*** can do about that?"

Go to Page 38

"Listen, Buster, I'm FROM SECURITY, I KNOW things!"

Go to Page 39

38

Day One

"Egads! The WHOLE website is DOWN? That certainly sounds important for our company!"

He ponders for a moment.

"Perhaps we can fill out the necessary forms right now and I'll have Janelle, my lead firewall engineer, shut things down immediately!"

Proceed to Day Two

39

Day One

Rory Thistlebrush, head of Networking, listens for a bit then starts complaining that he doesn't have time to deal with this and you should put a service request in and his team will respond to you within the documented SLA. You try to rebut, but he wishes you "Good Day Sir. No! I said GOOD DAY!"

That's not the news you were hoping for.

Proceed to Day Two

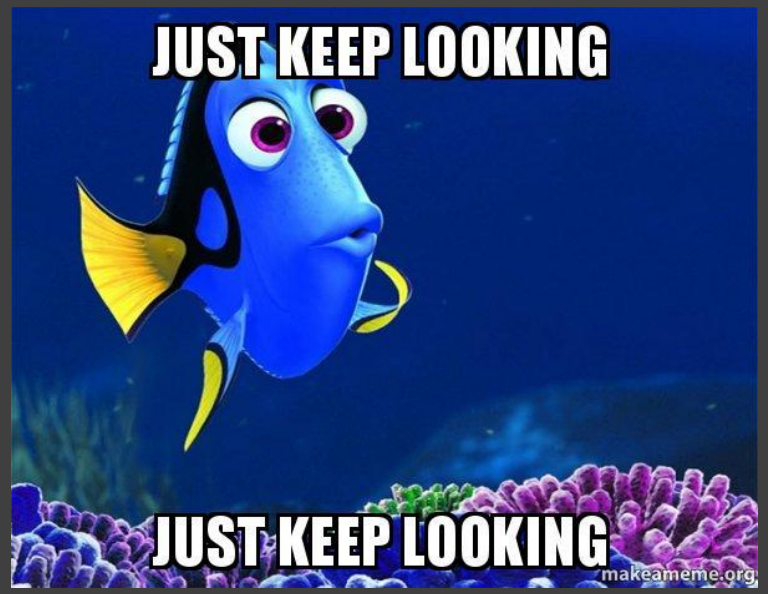
39

Day One

"Yesssssss. Yes indeed. FINAL. (mwahaha). Like all things, this problem will one day whither and die. It will pass the eye of the universe unnoticed as we futilely struggle against all hope to avoid the inevitable (mwahaha)."

That's not the news you were hoping for.

Proceed to Day Two



So you know there were a LOT of alerts, and that that's bad. You know you've got the BEST people to throw at this problem. You do a quick mental check of who isn't on PTO today….

41

Day One

Go talk to that new kid you have doing webadmin stuff, Zack. You heard he's BEASTMODE!

Go to Page 42

Maybe there's something in the website code that's being exploited. Go talk to good old Gary, your WebDev guy.

Go to Page 43

There's GOT to be some clue in these logs. Go to to Lucy the Log Lady, she'll be able to figure it out!

Go to Page 44

Go talk to your boss, Cedric the CISO. Maybe he's seen something like this before?

Go to Page 45

Zack cheerfully smiles at you as you approach his cube. “Sup dog? Check out that sick stream I twitched last night?”

42

“Uh…’bark bark’ to you, my homeslice!” (engage him in comradely banter for a bit)

Go to Page 1046

“Stop talking jibberish! And where is your tie? crocs and a collarless shirt isn’t dresscode!”

Go to Page 2046

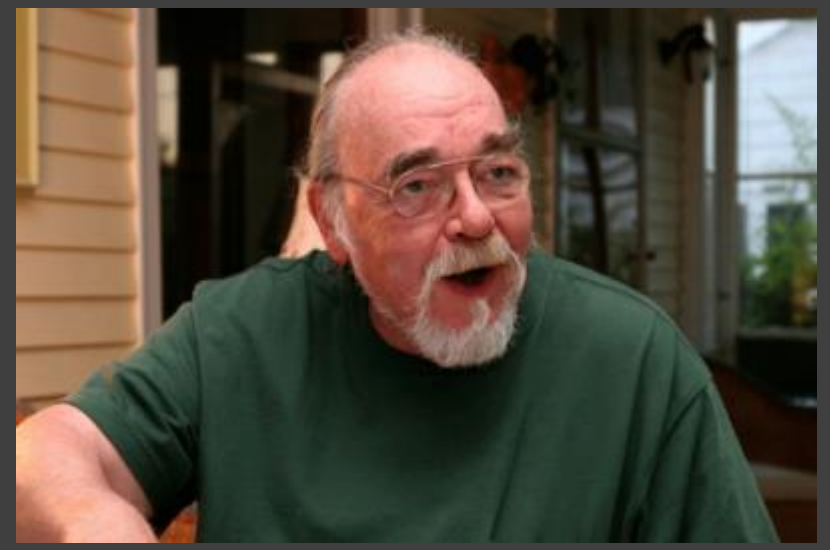
Your pager keeps going off, something from the SOC.

Go to Page 35

43

Day One

"HELLLLLOOOOO!!" Bellows Gary from his cluttered cube. As he stands up to greet you old Starbucks coffee cups go tumbling in all directions. You describe what's going on with the customer's website. He looks thoughtfully at you, a gleam in his eye.



"This reminds me of the time back when the DB2 LPAR had to be IFLed because there was too much pressure on the Zaps. Or was it the Zips?"

Go to Page 56

"Yes, yes. I THOUGHT this might happen. You see we're using the Java Struts 1.0 framework, and you KNOW I told them to update us to the 2.0….""

Go to Page 1057

"Back during Y2K there was a problem, you see. These old Foggie developers were too lazy, you see, they didn't feel like storing the whole date, you see…"

Go to Page 2000

There MUST be more information about all of these alerts in your awesome Elite Enterprise Logging Security System! (™) or EELSS! You go over to talk to Lucy the lady in charge of logging.

Her desk is filled with 5 monitors each with a different scrolling feed.

44

"Cool desk, Trinity. Are the machines plotting to invade Zion today? Where's Keanu?"

Go to Page 61

"Good morning Lucy. Did you happens to see these 34,000 alerts this morning?"

Go to Page 6262

45

Cedric your CSO will know what to do! He's been everywhere and seen everything!

You gently knock on the Mahogany door that leads to his wood-paneled office. The air gently smells of sandalwood and mint. Cedric sits behind a massive oaken desk,a single sheet of paper is the only thing that breaks the emptiness of the top.

Cedric smiles broadly as you step in, offers you a latte from his stainless steel Nuova Simonelli Prontobar Super Automatic Espresso Machine.

"What brings you up the the 53rd floor today?" he asks

Calmly explain the problem and what you've done so far

Go to Page 63

ZOMG YOUR BIGGEST CLIENT'S WEBSITE IS DOWN!!!

Go to Page 65

We have a problem with our biggest client, they are probably losing $10,000 an hour based off of past trends since this is their order-entry portal.

Go to Page 67

Zack's face lights up like Christmas and he jibbers on about Forts at Night and twerking and something called "powning" (whatever the heck THAT is). Inserting a few strategic "Huh!"s and "Rad!"s every so often, Zack seems really pleased. He asks about what you've done so far about the problem. Pondering that, he gives you 3 choices:

1046

Maybe we can fix this with our firewalls?

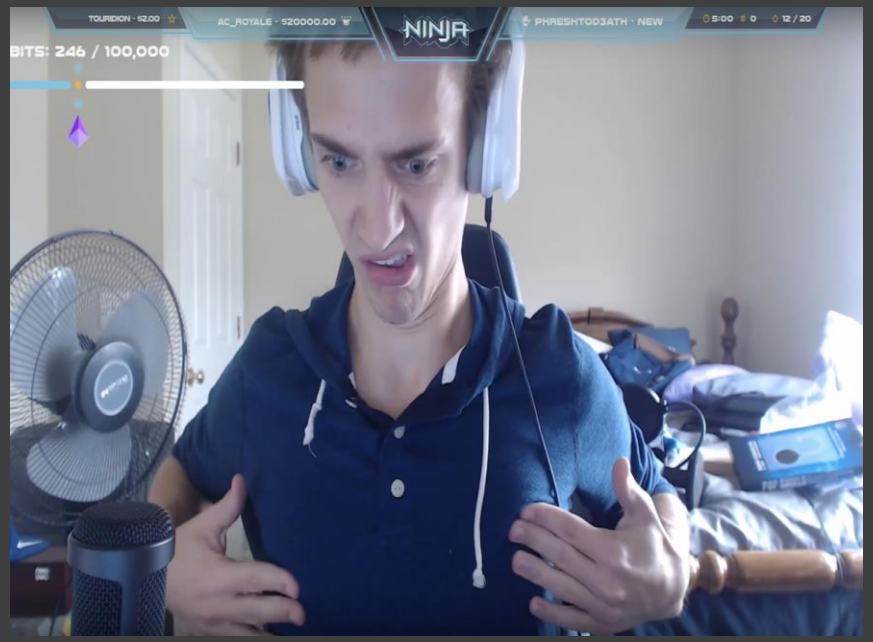
Go to Page 53

Maybe our ISP can help us?

Go to Page 54

"Hold my claw, Brah," Zack says, "I got this watch me work my server magic!"

Go to Page 55



Looking crest-fallen he mutters “Whatevs, Poindexter. Just Slack me whatever it is you want. I’m busy right now.”

2047

Great! Go back to your cube and figure out how to do that.

“No, I’m sorry, I shouldn’t have said that. I’m just under a lot of pressure with the website being down and all.”

Go to Page 47,474

Go to Page 1049

47,
474

You go back to your desk and google what ”Slack” is. After you click around your desktop for a while you find it. You send Zack the details on the 30,000 tickets. You’re pretty sure he’ll get RIGHT on that since you put 3 Smiley Emojis 😀 😀 😀 and the thumbs up 

on the end of the note!

You’re hip. You’re cool.

Proceed to Day Two

1,049

Day One

"That's ok, Brah," he says, wiping a tear from his eye. "Ya know, I've had a bad week myself, my Emotional Support otter, Otto, is sick. He vomited on my lap last night and I totally got zapped by these TOTAL HACKERS like from across the map, no scope and all. Dude. I was SO upset I didn't finish my pizza rolls…"

Look appropriately concerned for poor Otto and the loss of the warm, crispy pizza-flavoured snacks

"Perhaps, a way to make Otto feel better would be to fix this problem…."

"WHAT THE HELL IS WRONG WITH YOU?!? You need to get out of your mom's basement!"

Go to Page 5050

Go to Page 52

Go to Page 5150

As Zack rambles on, talking about some dumb hoodie he wants to buy, but is afraid it might make him look “too serious” your mind’s eye wanders off to thoughts about poor, sick Otto. You think of his poor little face (with just a little vomit hanging from the corner of one side of his mouth), laying back in Zack’s Mom’s basement, probably curled around an old towel or a flip flop or something. His teeny-weeny cutesy-wootsey face wooking awwwlll sad. Poor little guy.

Your day ends in a fur-filled haze.

5050

[Proceed to Day Two]

51,037

Day One

Zack looks at you for a moment. He whispers:

“You are a very bad person. You are not nice.”

He sits back down, puts his headphones on and stares at his monitor for the rest of the day.

Proceed to Day Two

51,037

Day One

"You know, dude, you're right. Sorry about that. Let's get this thing fixed. Maybe you'd like to grab some 'claws after work and we can talk more about Otto then?"

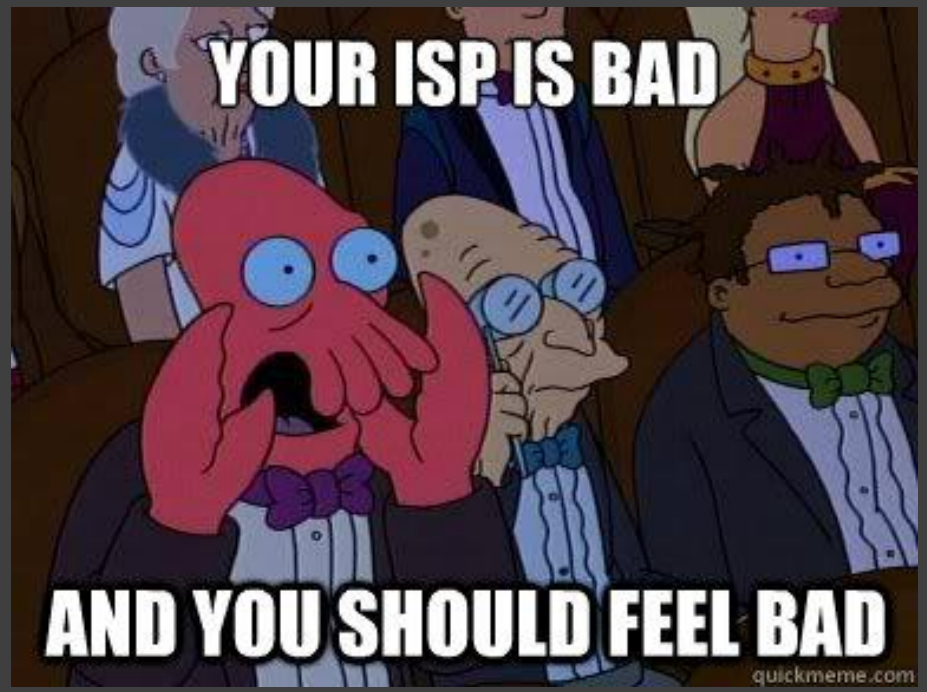
[Proceed to Day Two]

Zack gleefully starts logging into firewalls, IDS and IPS systems blocking all the offending IP addresses in-bound and out-bound.

As he finishes that up you're able to see the customer's website back online and servicing requests.

Whew! It's a good thing THAT'S over!

[Proceed to Day Two]



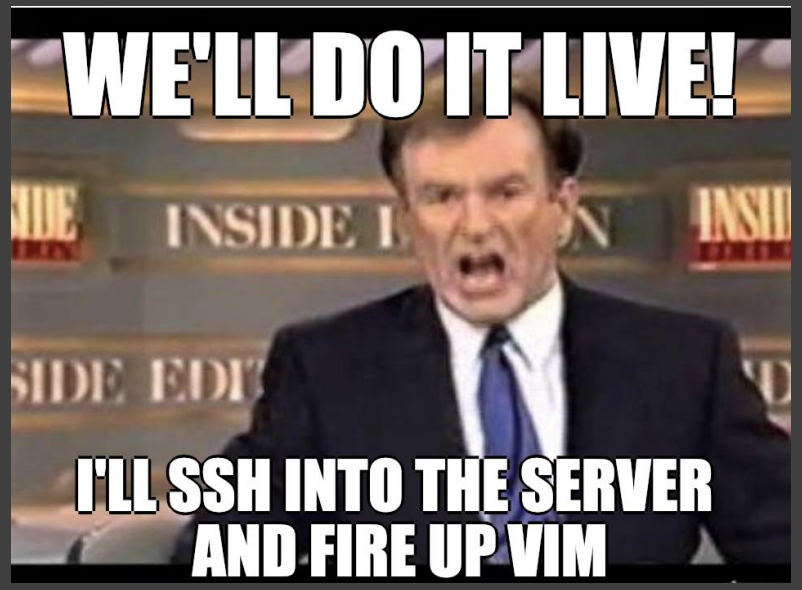
Zack calls up Ian and your ISP. They jabber on for a few minutes talking some strange language. You kind of think he's showing off to impress you. After he hangs up he talks about "blacklists" or "blackholes" or something. Whatever. the website is back online, so the customer will be happy.

54

[Proceed to Day Two]

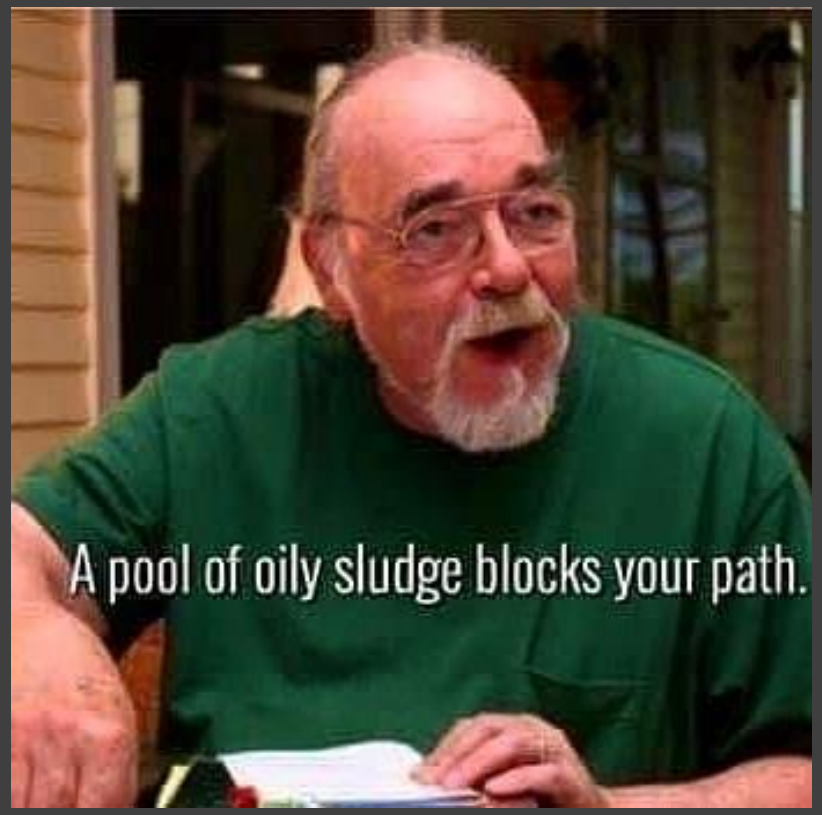
Zack gleefully starts logging into servers. Terminal windows churn away as he starts modifying configurations and appcode on the fly. After a bit he looks over to you, smiling, “Brah, we TOTALLY don’t have to be worried about the DDoS anymore! Claws up!”

You’re not sure that’s a good thing.



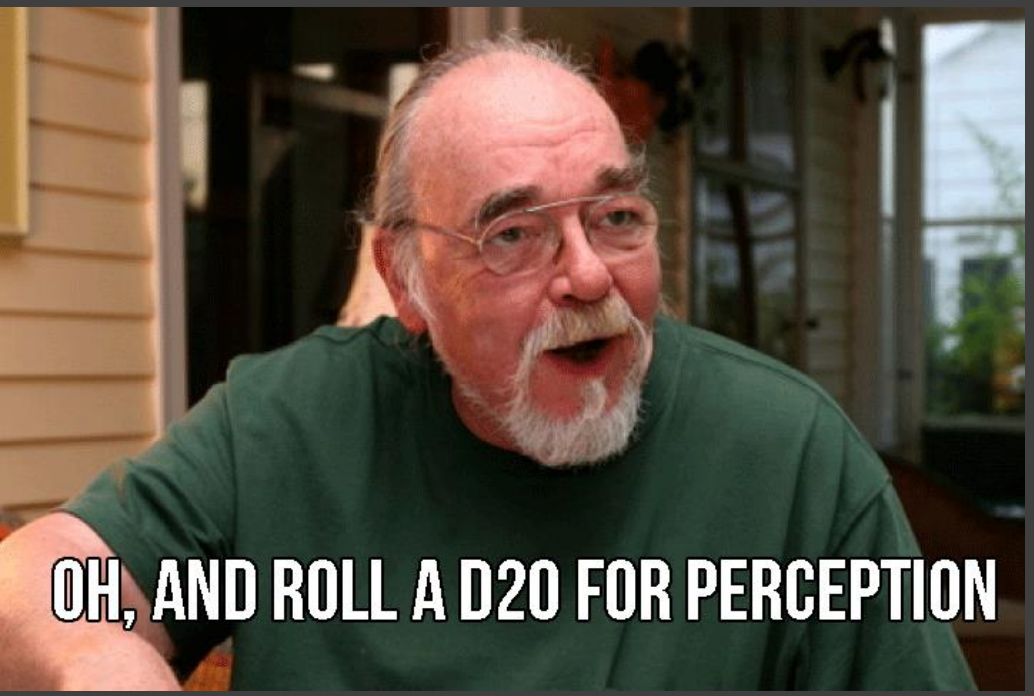
2047

[Proceed to Day Two]



Gary's booming voice goes on for what seems like hours. His vivid recounting of "that one time we did this thing" spins off into many other times something similar to that thing also happened, and also about how lazy developers are today, not like back in his day. When HE was coding developers had STANDARDS they'd follow. Once he wrote such a great piece of code his supervisor came over and said "Gary, THAT'S a nice piece of code" and they both laughed and then went out for coffee. He had decaf that day, because that next day he had to go to the doctor for his test. It's weird, you know, that doctors used to make house calls and they don't do that anymore.

[Proceed to Day Two]



The Webservers aren't up to date with their patching? That doesn't sound good Gary.

2047

Gary wants to tell you about how migrating to a Spring framework will not only increase security, but will boost performance

Go to Page 47,474

"Thanks Gary. i'm going to go talk to server ops to get the new packages updated. I'll talk to you later…….MUCH later."

Go to Page 58

You sllllllooowly back away, wishing Gary a great morning, thanking him for his observations, and hoping he doesn't ask you "What do you do next?"

You've GOT to get the ServerOps team to figure this upgrade out.

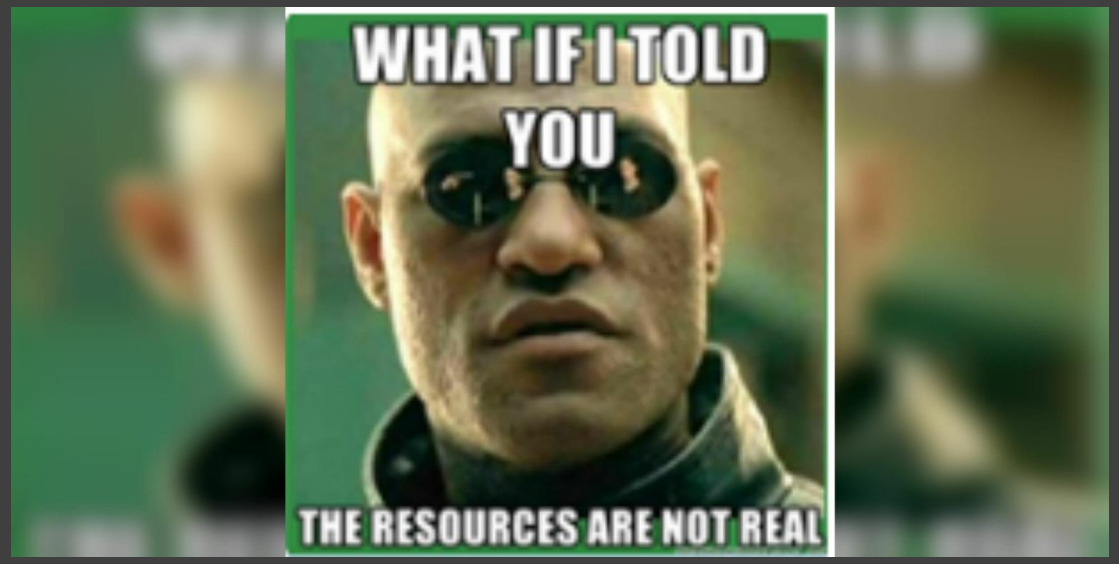
58

"ZOMG!!!! We're on an old version of Struts! Download and deploy it ASAP!!!!"

Go to Page 59,000

Chandan the Server Ops leads explains how that patch is currently in Dev/Test and should be ready to be deployed into Production in 8.5 weeks.

Go to Page 1060



The team looks confused, but Chip the intern was just reading the upstream Apache Struts forum and they were JUST talking about this!

He knows EXACTLY what to do. Chip goes out to the internet, googles “latest struts package”, downloads that, compiles it and immediately starts deploying it throughout the customer’s fleet.

Great! Problem TOTALLY solved!

Proceed to Day Two

You explain to Chandan that your customer can not wait 8.5 weeks, their main website is down NOW.

He makes some calls and arranges for Gary the webapp-guy to do some testing of the new version ASAP.

Gary finds a few minor regressions, but nothing that can't be worked around. Chandan pushes your vendor's Struts update a few hours later.

The website is back online.

58

[Proceed to Day Two]

Lucy looks up from the never-ending firehose of logs and smiles at you. “Thanks for noticing. Yes, I AM going to the team Halloween party after work today as Trinity! You are SO perceptive! I was meaning to stop by and see you, i’ve seen all this weird behaviour on our edge systems….”

61

[Proceed to Day Two]

You start complaining about all the alerts from the morning. She gets angrier and angrier with each word out of your mouth. “Listen MallCop, every hour I have to sift through 2,358,317 unique alerts. EVERY HOUR! Get in line behind all the other clowns that didn’t setup a proper workflow for their usecases. I’ll get to you later……MUCH LATER.

You silently sit in the ServerOps room all day waiting for her to look at the website alerts.

6262

[Proceed to Day Two]

“Oh my,” he exclaims, “this reminds me of the time that ….”

63

“Bill Gates and I were at a government blacksite, supporting a client. We were flown in in the middle of the night, escorted by armed guards….”

Go to Page 64, 640, 064

“Gary Kaspirsky and I were in a data center in Bora Bora tracking down malware…..”

Go to Page 58

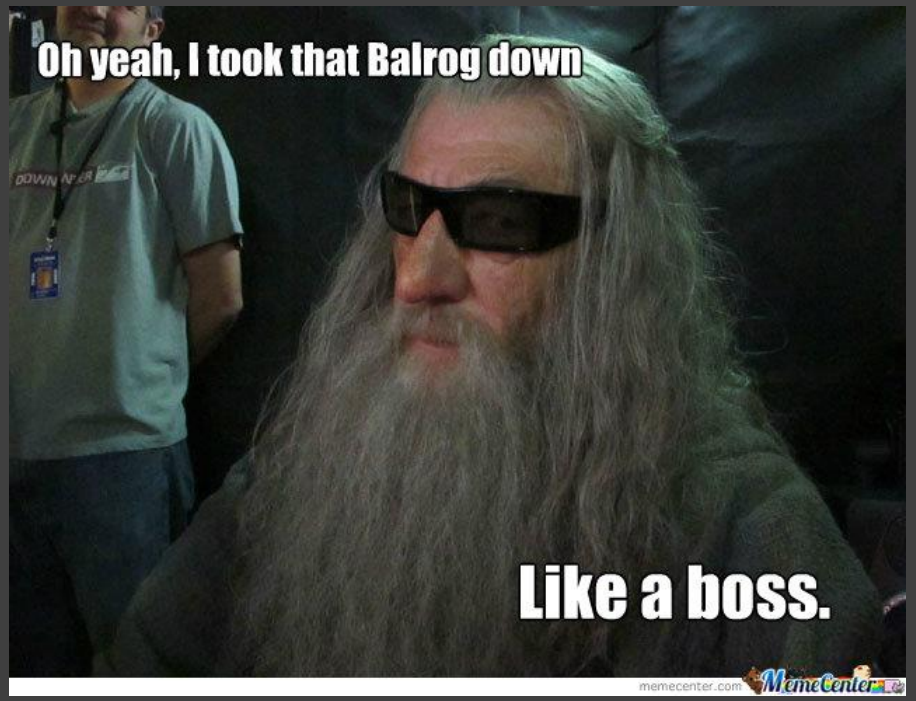
“Steve Jobs and I were at RSA, playing beer pong, but with Pappy Van Winkle instead of beer, with Dave Kennedy….

Go to Page 666

64,640,064

You sit, enraptured by Cedric's story. It is a thrilling tail of helicopter rides, redacted logs, and clandestine faxes.

Riveting stuff, truly worthy of a Tom Clancy novel. You totally forget what you came in to talk about, but you REALLY want to go home and watch Jack Ryan on Amazon to get ready for the upcoming second season! Who knew InfoSec could be SO EXCITING?

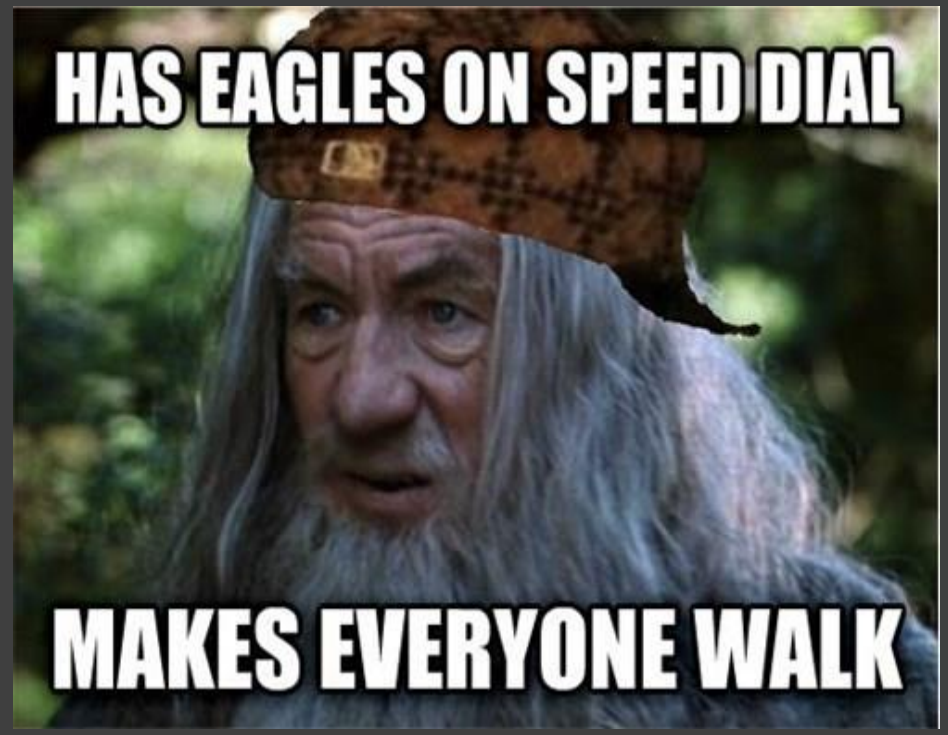


[Proceed to Day Two]

2047

"GADZOOKS! Why didn't you come right out and SAY that? Put that latte down we must act NOW! We've got to do damage control ASAP!! I'll call the CEO and our legal team immediately, get Corporate Comms to spin this. Now what's the name of the *former* employee that found this?"

Some poor person's day is going to end poorly.



Proceed to Day Two

You sllllloooowly back away, wishing Cedric a great morning, thanking him for his observations, and hoping he doesn't ask you "What do you do next?"

You've GOT to get the ServerOps team to figure this upgrade out.

666

[Proceed to Day Two]

As you talk, explaining the business impact of this outage both to GREAT! and the customer Cedric slowly nods. Pursing his lips he says “Hmm, yes, yes. Very nasty situation we have here. Bad indeed. I’ll get the leadership team and corporate comms prepared. I like your action plan, but I suggest we gets these external IPs blocked as soon as possible. Is someone doing a review of the systems that are being attacked? We’ll want to ensure they operating normally after all of this is cleared up. i’d like you to join me on a conference call with the client here in an hour.”

The rest of the day is VERY busy, but you feel progress is being made.

67

Proceed to Day Two

You rally the team to get out all the "detailed" documentation everyone spent so much time producing…..

Which is a few lines on a Wiki page and a deployment diagram back from when the contract was being signed with the customer, over 3 years ago.

Oh yeah, Petey the PM noted that this stuff *should* be reviewed annually after implementation in that Wiki.

68

I heard Zack from the NOC say he found a cool tool that could map out the network. What to give that a try?

Go to Page 69

Oh well, not much more YOU can do about this. Ops knows about the problem now….

Go to Page 70

The most interesting and useful things can be found on the internet! You and Zack download a copy of WireBearSnort and after a few quick clicks and some annoying permission requests you're up and WireBearing away!

3	2.801661000	192.168.0.6	74.125.68.94	TLSv1.2	220 Application Data
4	3.015509000	74.125.68.94	192.168.0.6	TCP	66 443→51660 [ACK] Seq=1 Ack=155 Win=391 Len=0 TSval=2954786
5	3.032189000	74.125.68.94	192.168.0.6	TLSv1.2	163 Application Data
6	3.032192000	74.125.68.94	192.168.0.6	TLSv1.2	183 Application Data
7	3.032257000	192.168.0.6	74.125.68.94	TCP	66 51660→443 [ACK] Seq=155 Ack=98 Win=8185 Len=0 TSval=7121
8	3.032258000	192.168.0.6	74.125.68.94	TCP	66 51660→443 [ACK] Seq=155 Ack=215 Win=8178 Len=0 TSval=712
9	3.032844000	74.125.68.94	192.168.0.6	TLSv1.2	112 Application Data
10	3.032896000	192.168.0.6	74.125.68.94	TCP	66 51660→443 [ACK] Seq=155 Ack=261 Win=8189 Len=0 TSval=712
11	3.032991000	192.168.0.6	74.125.68.94	TLSv1.2	112 Application Data
12	3.188712000	74.125.68.94	192.168.0.6	TCP	66 443→51660 [ACK] Seq=261 Ack=201 Win=391 Len=0 TSval=2954
16	6.140790000	192.168.0.6	74.125.68.94	TLSv1.2	220 Application Data
22	6.240335000	74.125.68.94	192.168.0.6	TCP	66 443→51660 [ACK] Seq=261 Ack=355 Win=405 Len=0 TSval=2954
23	6.279263000	74.125.68.94	192.168.0.6	TLSv1.2	163 Application Data
24	6.279322000	192.168.0.6	74.125.68.94	TCP	66 51660→443 [ACK] Seq=355 Ack=358 Win=8185 Len=0 TSval=712
25	6.281437000	74.125.68.94	192.168.0.6	TLSv1.2	385 Application Data
26	6.281442000	74.125.68.94	192.168.0.6	TLSv1.2	112 Application Data
27	6.281574000	192.168.0.6	74.125.68.94	TCP	66 51660→443 [ACK] Seq=355 Ack=677 Win=8172 Len=0 TSval=712
28	6.281575000	192.168.0.6	74.125.68.94	TCP	66 51660→443 [ACK] Seq=355 Ack=723 Win=8169 Len=0 TSval=712
29	6.282017000	192.168.0.6	74.125.68.94	TLSv1.2	112 Application Data
37	6.442243000	74.125.68.94	192.168.0.6	TCP	66 443→51660 [ACK] Seq=723 Ack=401 Win=405 Len=0 TSval=2954
41	6.638366000	192.168.0.6	74.125.68.94	TLSv1.2	178 Application Data
42	6.752519000	74.125.68.94	192.168.0.6	TCP	66 443→51660 [ACK] Seq=723 Ack=513 Win=405 Len=0 TSval=2954
43	6.818056000	74.125.68.94	192.168.0.6	TLSv1.2	151 Application Data
44	6.818215000	74.125.68.94	192.168.0.6	TLSv1.2	1484 Application Data
45	6.818236000	192.168.0.6	74.125.68.94	TCP	66 51660→443 [ACK] Seq=513 Ack=808 Win=8186 Len=0 TSval=712
46	6.818297000	192.168.0.6	74.125.68.94	TCP	66 51660→443 [ACK] Seq=513 Ack=2226 Win=8103 Len=0 TSval=71
47	6.818920000	74.125.68.94	192.168.0.6	TLSv1.2	1484 Application Data

Sadly, the output is a bit cryptic….

Hold my beer! You've got this!

Go to Page 158

Maybe those guys in Ops should handle this?

Go to Page 7000

69

Day One

Yeah, those guys down in Ops should be able to figure things out. You throw this problem over the wall and go to lunch.

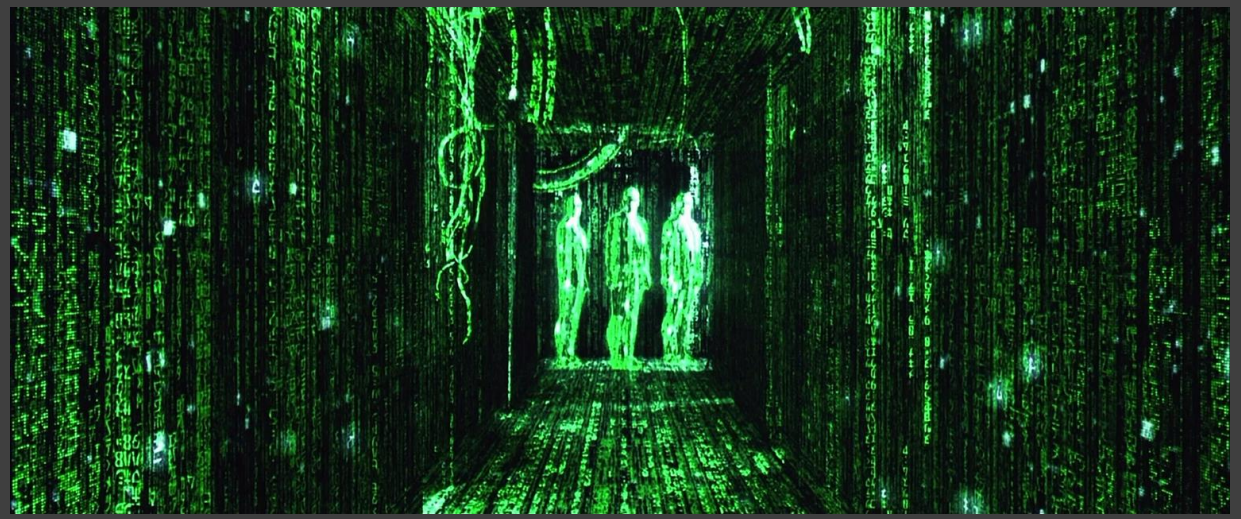
7,000

Day One

Proceed to Day Two

“Oh my stars and garters! What in the wide world of sports is THAT? Is that even a language used to communicate somehow?”

Together you and Ops guys spend the afternoon staring at the screen, somehow trying to decipher the matrix.



159

Day One

Proceed to Day Two

NOTHING says excitement like “DOCUMENTATION AUDIT” (wa-HOO!).

You pull everyone into the conference and start at the beginning, reviewing your project charter documents for your customer, starting with the good, old ToC.

ZOMG! Look at this RACI chart! It is SO inaccurate now!

Huh, did we ever close out these “Next Steps” items?

Didn’t we use this project as a template for our other contracts afterwards?

Hmm… there’s enough missed things here maybe you should go to the Customer’s Audit team?

Go to Page 1076

Go to Page 83

Go to Page 86

Go to Page 900

Yes, the RACI certainly has changed in the 3 years on this contract. You'd better get that addressed immediately. A matrix of who does what will help us sort out all of these alerts from this morning!

1076

"OBVIOUS Mike the Manager is ACCOUNTABLE for this, his name has "MANAGER" in it! Duh."

Huh. That's so weird. we never assigned anyone to be responsible for patching the customer's webservers.

Go to Page 770

Go to Page 1178

770

Day One

"No Felicia, in this situation Mike is CONSULTED not ACCOUNTABLE. Buh-bye!"

The Great RACI Debate of '19 rages on for hours….

Proceed to Day Two

1178

Day One

In the chaotic scramble to get the customer's project completed looks like the PM overlooked a few "small details" (Petey the PM, he's *such* a scamp!).

Well, no better time than today to get that missing item corrected.

Write up a memo to the Ops team that they must comply with patch policy immediately and will need to supply their action plan to address the unpatched servers by the end of the week.

Go to Page 79

Hmm, this i s pretty bad. Who knows what vulnerabilities might be live on the customer's system. Maybe you should walk down to Ops to talk about this.

Go to Page 80,008

You know, there is NO problem that can't be solved with a GREAT MEMO.

You fire off a 12 page memo to the Ops team outlining how they are failing and demanding documentation around their action plan to suck less.

Proud of yourself, you decide to leave work early and go play some Frisbee Golf.

79

Proceed to Day Two

You head down to the Ops team to talk about the gaps you identified.

80,008

"OK, Ops-people, you are clearly in violation of policy for not patching these critical customer servers. We're writing you **all** up and you MUST have a action plan by EoD. You're welcome. "

"Can we talk about some gaps we've found?"

Go to Page 1810

Go to Page 820

You LOVE laying down a good policy smackdown!

Time to go have an early lunch! It will be that much sweeter seasoned by the tears of the Ops team.

1,810

Day Two

Proceed to Day Two

820

Day One

You fill them in on the gaps you've seen and how you're pretty certain the customer's servers are out of date with patches.

Let's talk to some experts to see if we can figure this out together...

Go to Page 41

No time better to address those Next Steps than now, you suppose.

Huh, did we ever get legal sign-off? We should go check.

Go to Page 1840

Training?

Go to Page 8500

The Legal Team is not amused you forgot to include them in oversight of the contract.

You spend the rest of the day being talked at about how much jeopardy you put the company into.

1,840

Day Two

Proceed to Day Two

8,500

Day Two

You’re pretty sure if they haven’t learned what they needed to know yet there is nothing more you could impart to them now.

Proceed to Day Two

Oh yeah! You remember now. You templated out this service offering and Sales has successfully sold this EXACT same thing to a half dozen other customers based off of how successful THIS implementation went.

86

That's EXCELLENT! Look at all that work we saved ourselves across all of those projects!

Go to Page 86 860 086 001

Um… if we did the EXACT same thing across all of these projects, wouldn't they ALL have the same gaps?

Go to Page 890

Whew! Good thing we caught this now! Let's get this template fixed to avoid doing these problems again!

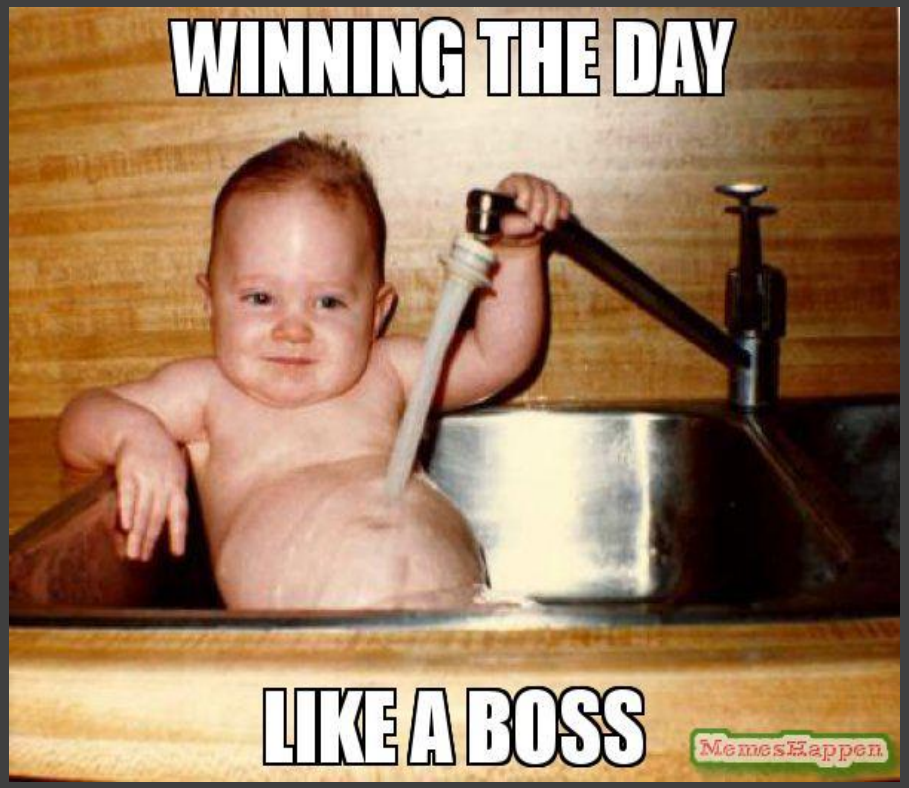
Go to Page 88

86,860,086,001

Day Two

Winning is the best. You love winning. So much #win in reusing those templates you go down to the sales floor to thank everyone for selling their little hearts out.

...but not too much thanks since next week is month-end close and end of quarter. They all have numbers to hit, so they better go sell MOAR!!!!!



Proceed to Day Two

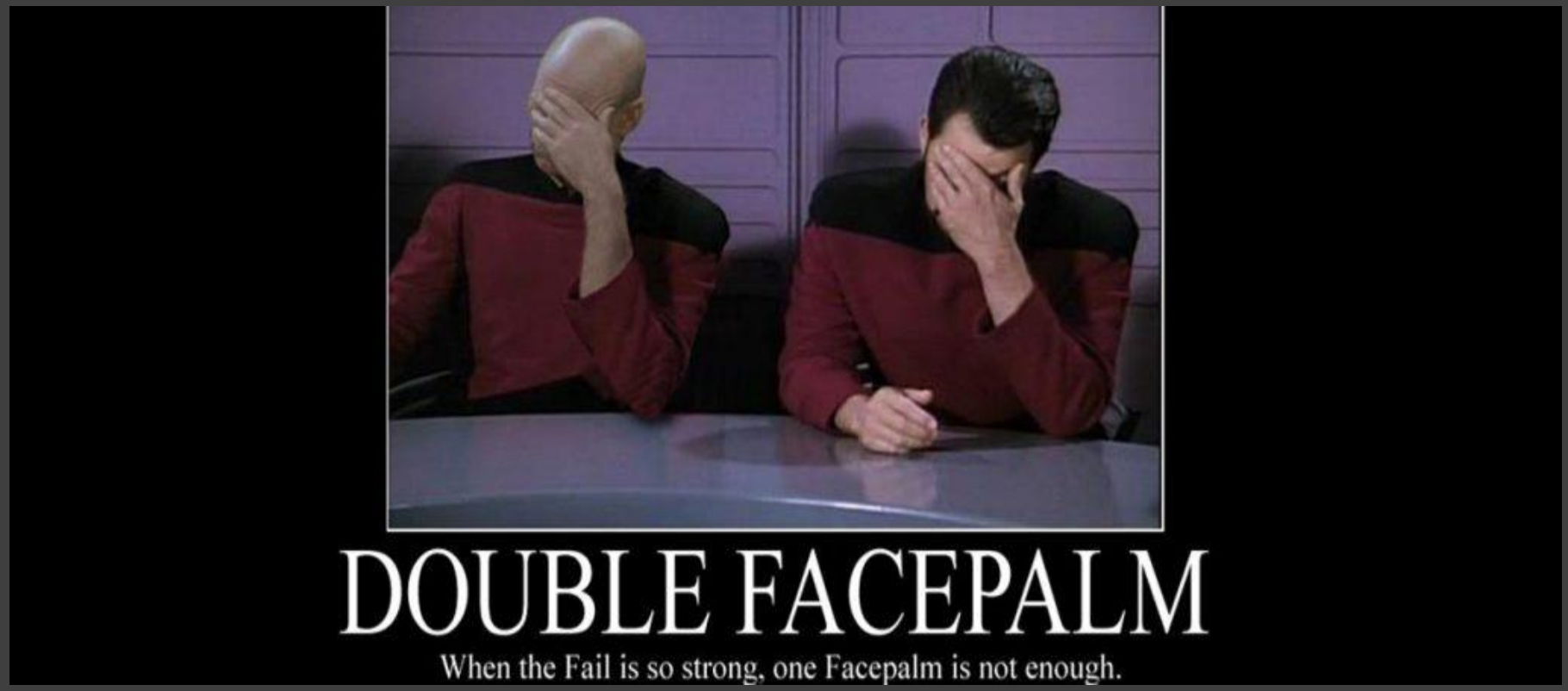
You assemble your crack team and get to work fixing those deployment templates! It’s a good thing THAT won’t be a problem for your future customers!

88

Proceed to Day Two

890

Day One



Oh Dear. After some deeper digging, it looks like you have multiple customers all calling in with hundreds of thousands of alerts and unavailable servers.

It looks like your company deployed a vulnerable configuration to all of your customers and never implemented any type of maintenance or review program that might have caught it.

You have some explaining to do. Go back to Page 15 and try again.

The Customer's Audit team is DELIGHTED you stopped by. They'd LOVE to assist you.

900

"Great! You see we've found a problem with the configuration of the servers we deployed here…."

Go to Page 88

"Um….yeah. I've got some questions, purely hypothetical, for a friend, you know?"

Go to Page 64

Back away slowly

Go to back to Page 157

88

"Oh please, go on…"

"Yeah! Well you see, your whole web-facing presence is down, we *think* because of a denial of service attack…."

Go to Page 89

Back away slowly

Go to back to Page 157

“And when exactly did YOU know about this breach of confidence? What were you doing, precisely, at the time the data was lost?”

Your day ends poorly.

89

Proceed to Day Two

96

Day One

Goodie Gumdrops! You GET to go to the Change Advisory Board (aka the CAB)!! NOTHING is more fun than sitting around for several hours reading through everyone's proposals to make changes!

You've prepared for this your whole life. You've got your TPS forms filled out in triplicate!

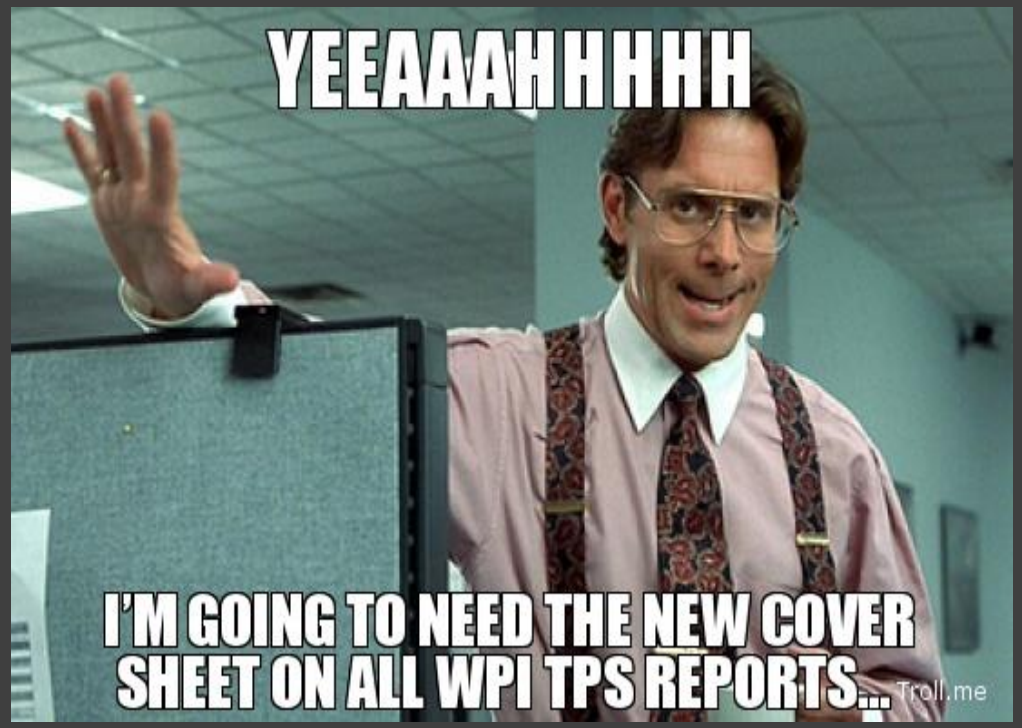
Go to Page 1097

Get out the popcorn and watch the fireworks.

Go to Page 990

Hmm… maybe you DON'T need to go to the CAB. You just have a few small changes to make. No one would probably even notice.

Go to Page 108



CAB lead Bob Lumbergh and Tushman your ITIL guy appreciate your enthusiasm, but it appears as if your documentation is missing some vital pieces before the CAB could approve them.

1097

Your TPS reports are missing their cover sheets, a simple thing to address

Go to Page 9898

Oh, your impacted systems list and what the end-user experience description are missing.

Go to Page 001

You didn't read the agenda to see your proposed change collides with an upgrade of the customer's back-end workflow tool as well as rotating the filters on the espresso machine in the lobby.

Go to Page 102

CURSES!!!! Rookie mistake forgetting those new cover sheets. Oh well,maybe you can get that critical change scheduled *next week.*

9898

Proceed to Day Two

990

Day One

The CAB is GREAT! Watching people come in all prepared and watching the board tear them apart. There is NO GREATER joy you get in your week.

Laugh at the Dev team try and get “regression fixes” through.

Chortle at the Ops team trying to get “Patch Tuesday critical fixes” scheduled.

Stand and clap loudly as the Compliance Team tried to get “Increased Logging & Auditing” changes deployed.

Go to Page 110

Go to Page 1111

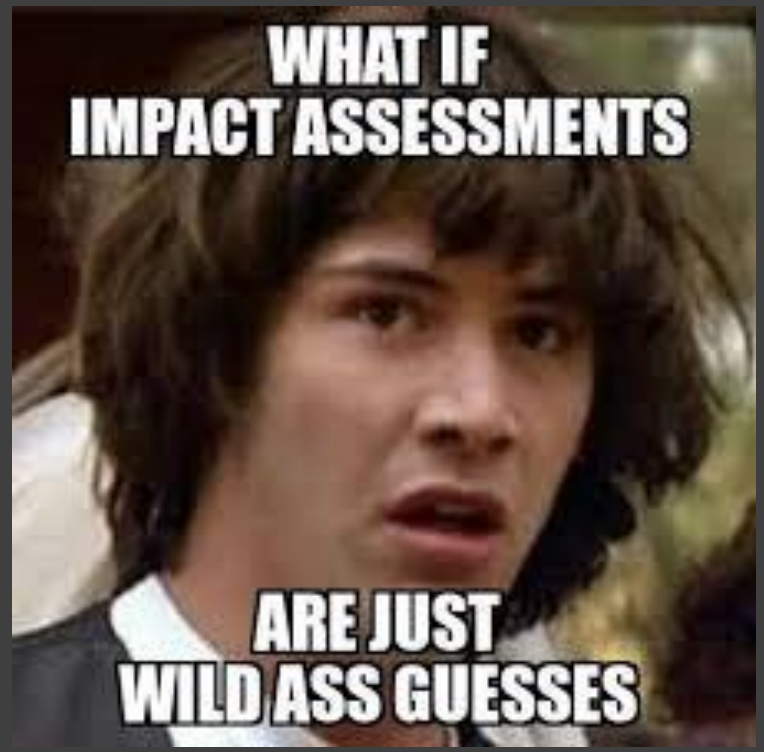
Go to Page 101

001

Day One

ZOMG…you're missing the systems that would be impacted by the change as well as a description of what end- user experience would be!

You hurriedly scribble some stuff down, but it's not fleshed out enough, so you're change request is denied this week and you get to come back next week and try again.



Proceed to Day Two

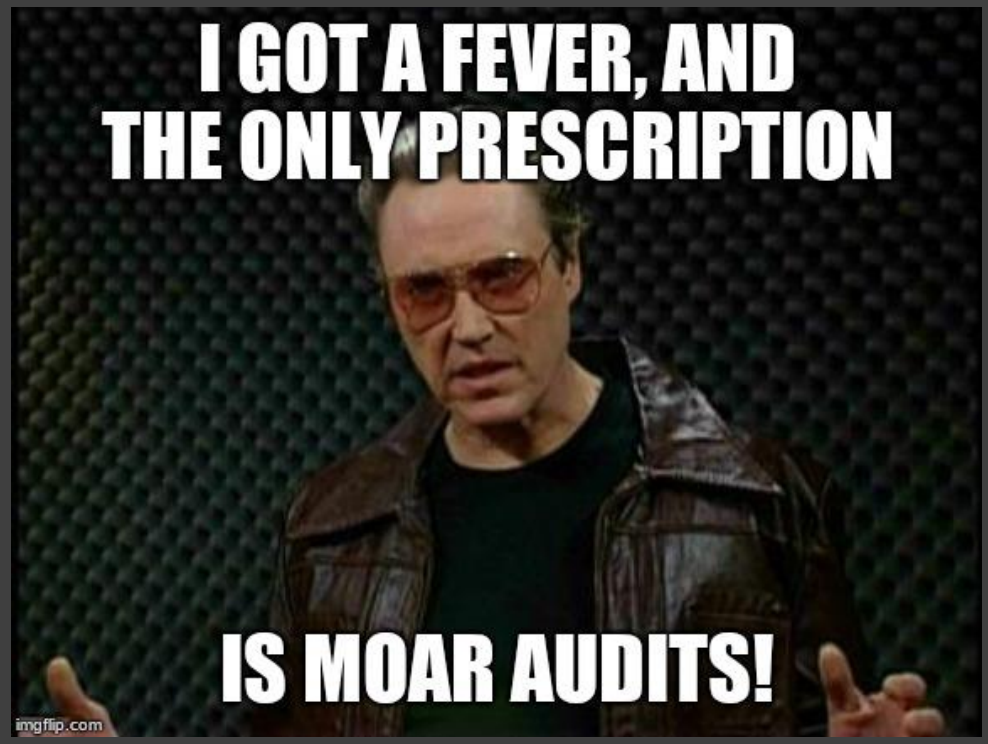
101

The Compliance Team admires your moxie and your overall appreciation of creating paperwork. They offer you a job on their team.

You have a long and storied career of harassing teams with requirements and meetings to review their compliance. Around the watercooler your legend is whispered in hushed tones...until (for “budget reasons”) the watercooler is taken away.

There is a special place in the afterlife for you…..

Go back to Page 15 and try again.



You didn't read the agenda to see your proposed change collides with an upgrade of the customer's back-end workflow tool as well as rotating the filters on the espresso machine in the lobby.

102

Obviously the back-end changes are LESS important than your problem

Go to Page 1103

Can we work something out?

Go to Page 2104

Obviously, we can NOT impact the maintenance of espresso machines! You like them ...a latte!

Go to Page 105,105

Back-end changes are OBVIOUSLY less important than the security changes you need to get made. You cause a scene in the CAB, throw the server team under the bus, and get your change approved.

Yay you?

1103

Proceed to Day Two

You all knuckle down and figure out a way ALL the changes can be done and get approved by the CAB. Not everyone gets exactly what they want, but ultimately all the impacted stakeholders will get enough to continue operations.

2104

Proceed to Day Two

105,105

Day One

Why didn't someone say the espresso machine needed maintenance sooner? You assemble a Tiger team **immediately** and get to work on the problem

Descale the machine

Go to Page 1810

Replace the charcoal filters

Go to Page 820

Barkeeper's Friend, $12 on Amazon! You should go buy some right after this presentation! It'll make your coffee taste like it was made with fresh, mountain water and newly driven snow!

106

Proceed to Day Two

Chuck from Finance keeps yammering on about charcoal, but you're pretty sure he's talking about his grill.

The team goes and googles charcoal coffee filters for the rest of the day

107

Proceed to Day Two

You drop your mechanical pencil on the floor, crouch down to pick it up and proceed to creep out of the CAB room.

108

You could go checkup on how the docs audit is going

Go to Page 75

Oh man, you should go sneak out and see that awesome new Downton Abbey movie everyone is raving about!

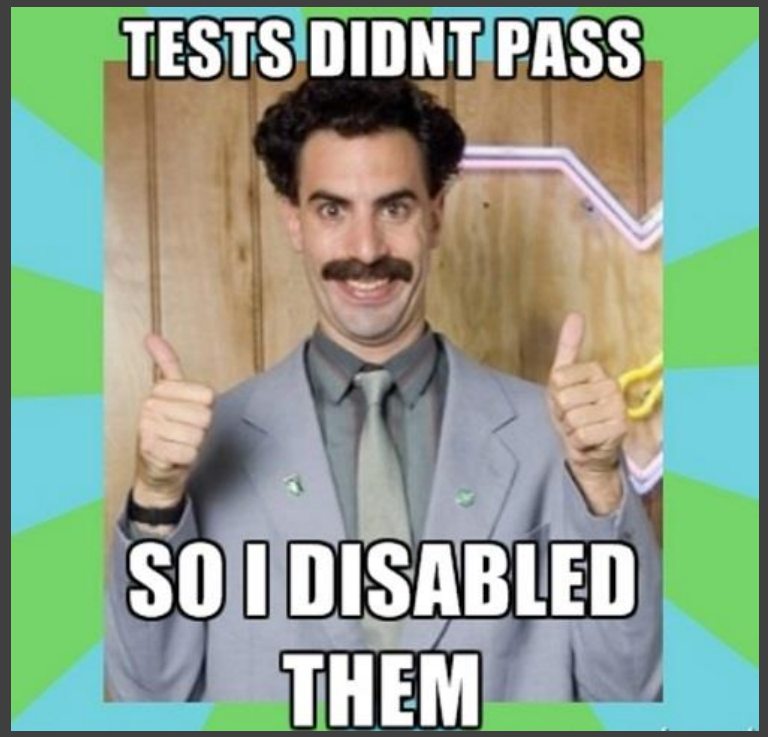
Go to Page 2104

901

That Maggie Smith, WHAT AN ACTRESS. You could watch her all day long. She is so delightful as Violet, the Countess of Grantham. She gives the staff of Downton Abbey SUCH fits with her irascible, pompous ways.

Oh, you're fired for abandoning the customer, by the way, but you decide to make it a weekend Maggie-movie-marathon to cheer yourself up.

Go back to Page 15 and try again.



The Dev team is trying to push through a bunch of “fixes” they claim will fix “regressions” in the mainline code that all of your customers are currently using.

You’re pretty sure that is not more important than the changes you need to make to stop this DDoS attack.

You laugh at their change request. The whole CAB joins you and the developers slowly leave the room, quietly sobbing.

1097

Proceed to Day Two

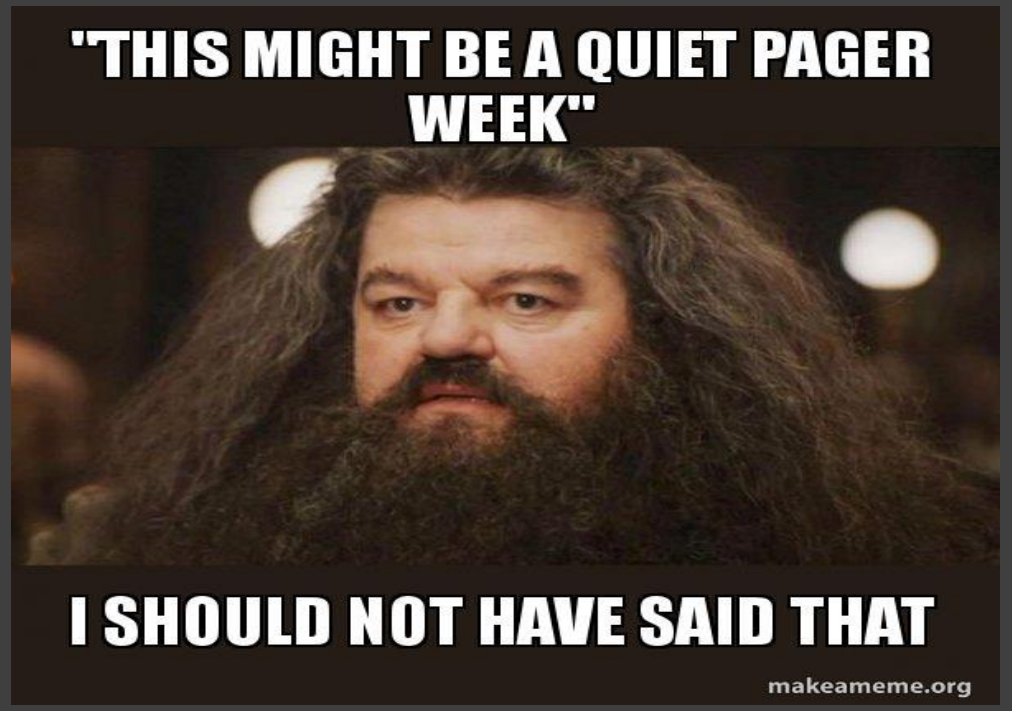
Nothing important ever gets rolled out on Patch Tuesdays. You convince the CAB to move them to next week and call it “Patch Friday” right before end of business on Friday. Nothing bad should happen.

1111

Proceed to Day Two

112

Yeah...the SOC sure got a lot of alerts overnight. You're pretty sure the customer's website's down too. If only someone had a runbook of what to do about this?



Walk over and talk to Bert the SOC Manager

Go to Page 21

You know what? You're SURE the SOC has a process to handle this. They don't need you butting your nose into their business.

Go to Page 311

You're not one to tell someone how to do their job. Obviously they MUST have some process to deal with so many alerts. You'd just get in the way and make them feel sad if you came down and watched over their shoulder as they fixed the problem.

You go back to your desk and start flow-charting out some stuff.

311

Proceed to Day Two

117

Spend some time tweaking the mail filters & rules to ensure OPTIMAL efficiency

Talk to the CyberThreatbot and auto-block and blacklisted IPs

Go to Page 1121

Download the latest updates for the Spamalotbot

Go to Page 10,122

Implement that new SSL-decryptor you've been putting off for several months.

Go to Page 321

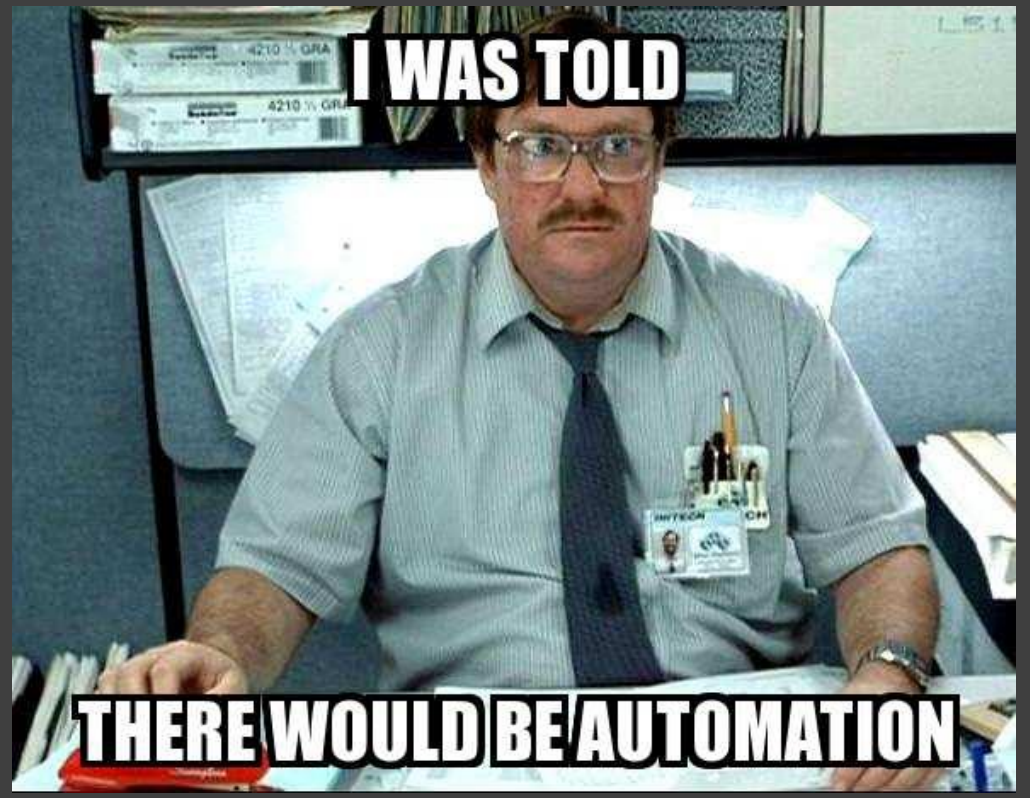
Tell the Spamalotbot how much you love it and what a good, good boy it is!

Go to Page 124

118

Day One

Ah yes! That miracle of modern technology: the Automotron9000 scripting system. Is there ANYTHING A9K can't do? Well to keep it operating at tip-top performance occasionally you need to "change the oil" so to speak; keep it nice and up to date.



Schedule some downtime to conduct the A9k update.

Using…. ARTIFICIAL INTELLIGENCE, let A9k decide for itself when the best time to update things would be.

Go to Page 1150

Go to Page 151

119

The SOC robot reports it addressed 34,862 alerts overnight.

Neat! SocBot, you sure are smart!

Go to Page 154

Wow, that sounds like a lot of alerts. Are you SURE that's correct SocBot?

Go to Page 15,500

Double-check SocBot by reviewing the SIEM logs and correlate all the systems SocBot oversees.

Go to Page 651

You'd better walk over and talk to Bert, the SOC Manager

Go to Page 831

You Talk to the CyberThreatMaster9000 to see about auto-blocking and blacklisting IPs

1121

The sales guy was SUPER-CONFIDENT that the CyberThreatMaster9000 would solve these types of problems!

Go to Page 33

Let's take a look at what's on the CyberThreatMaster9000's mind....

Go to Page 127

It’s been a while, now would be a GREAT time to download the latest updates for the Spamalotbot. Maybe your alerts are just…spam?

10,122

Push that button, upgrade that bot!

Go to Page 135

Read a few of the alerts first, you know, just to be sure.

Go to Page 1136

You've thought about it for months, maybe now is the time to implement that SSL-decryptor you bought a while back. You can't read any of the content of those 36,432 requests. The Decryptonator9000 should be able to help once it is online.

321

Yes! FINALLY you can view all that data flying around everywhere!

Go to Page 140

Maybe you should be a bit selective of where you'll be decrypting data in transit?

Go to Page 1141

You tell the Spamalotbot how much you love it and what a good, good boy it is!

124

Good bot, here's a botsnak!

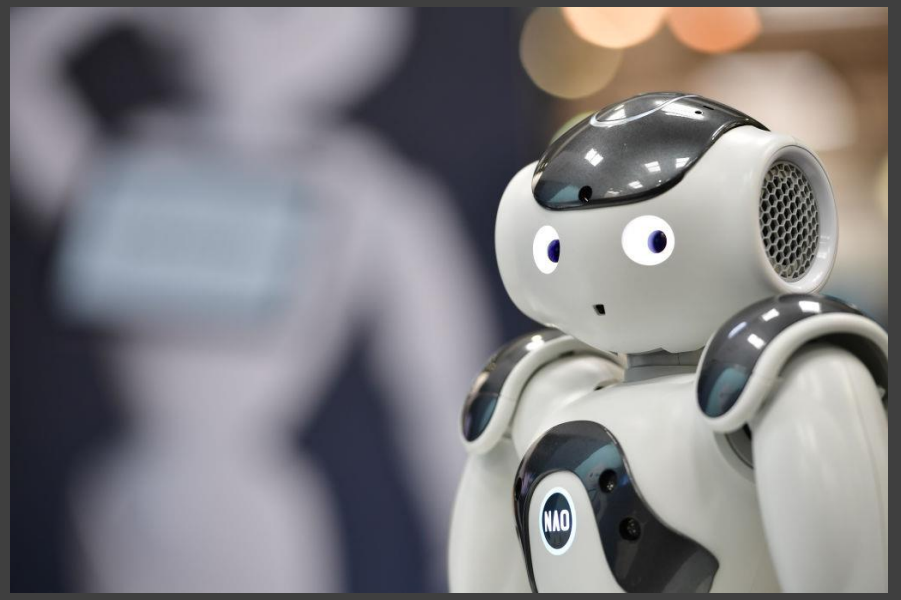
Go to Page 147

"You know, Spamalotbot, you and I have worked together for years,and I really don't know much about you. What are you interested in?"

Go to Page 148

125

"So...what types of things are you worried about, CyberThreatMaster9000?"



3v33l H@x0rz

Go to Page 621

Fancy Bears

Go to Page 127

So much insider threat.....

Go to Page 128

Asteroid 97y362 smashing into our Jacksonville datacenter, spewing molten hot magma over the great Jacksonville area

Go to Page 900

The dynamic cyber-threat feeds provide valuable OSINT data about all the L33t H@x0rs that are talking about your client….ON THE DARK WEB.

You spend the afternoon with CyberThreatMaster9k googling details about yourself on the dark web and then go home that night and cry yourself to sleep.

621

Proceed to Day Two

ZOMG!!!! CyberThreatMaster9k thinks that APTs are actively exploiting your network! Crushing depression sinks in…. If Fancy Bear wants YOUR DATA….what can poor little you DO about that? You hide under your desk for the rest of the day, constantly looking for bear-sign.

10,122

Proceed to Day Two

If it wasn't for those users the security you implemented would be just fine! Sadly, CyberThreatMaster9k does not understand human emotions. If only there was some way to help him understand, then he could do a better job of predicting when they will be jerks…..

128

Teach the robot to love

Go to Page 1300

"uhhhhh…..(beep beep)….Oh No CyberThreatMaster9000, my …uh…beeper is going off, I've got to go! Good luck with those emotions annd stuff!"

Go to Page 131

CyberthreatMaster9000 is convinced that Asteroid 97y362 will come hurtelling down and smash into our Jacksonville datacenter, spewing molten hot magma over the great Jacksonville area. The facts are irrefutable.

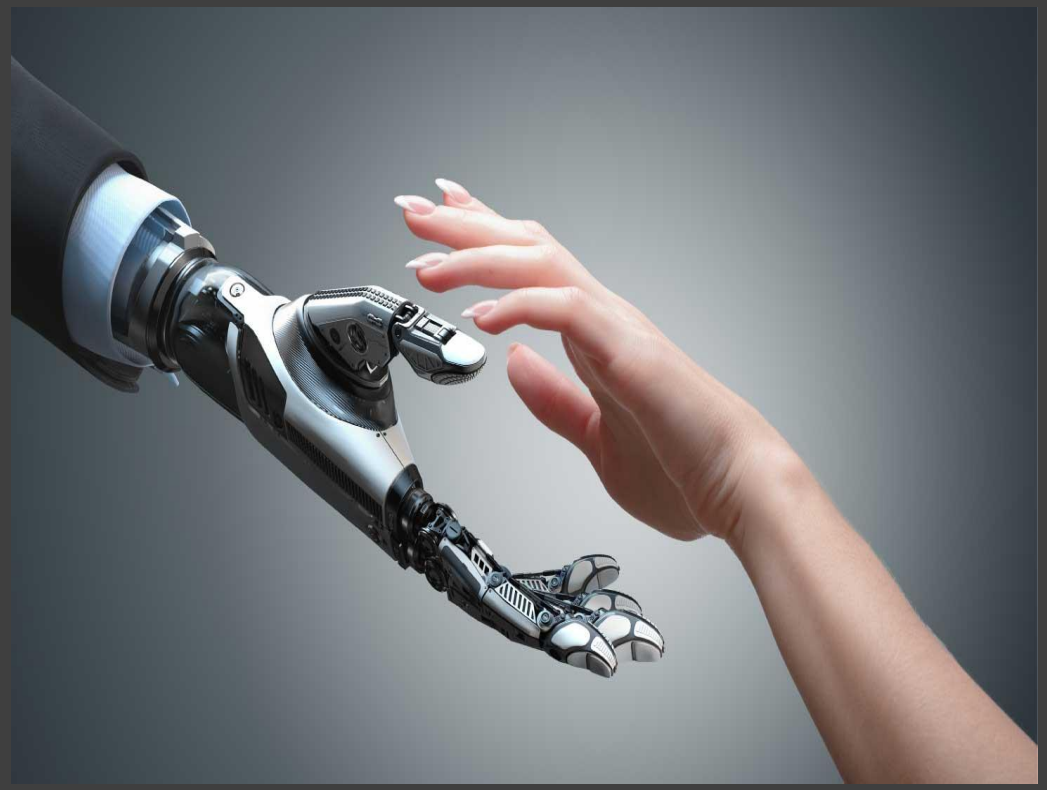
129

Well, that's hard to argue with. I guess today is the day you should go start those skydiving lessons and go see the world's largest ball of twine before it's all over.

Go to Page 321

Come on, man! Recheck that data! We can't go out like *that*!

Go to Page 1133

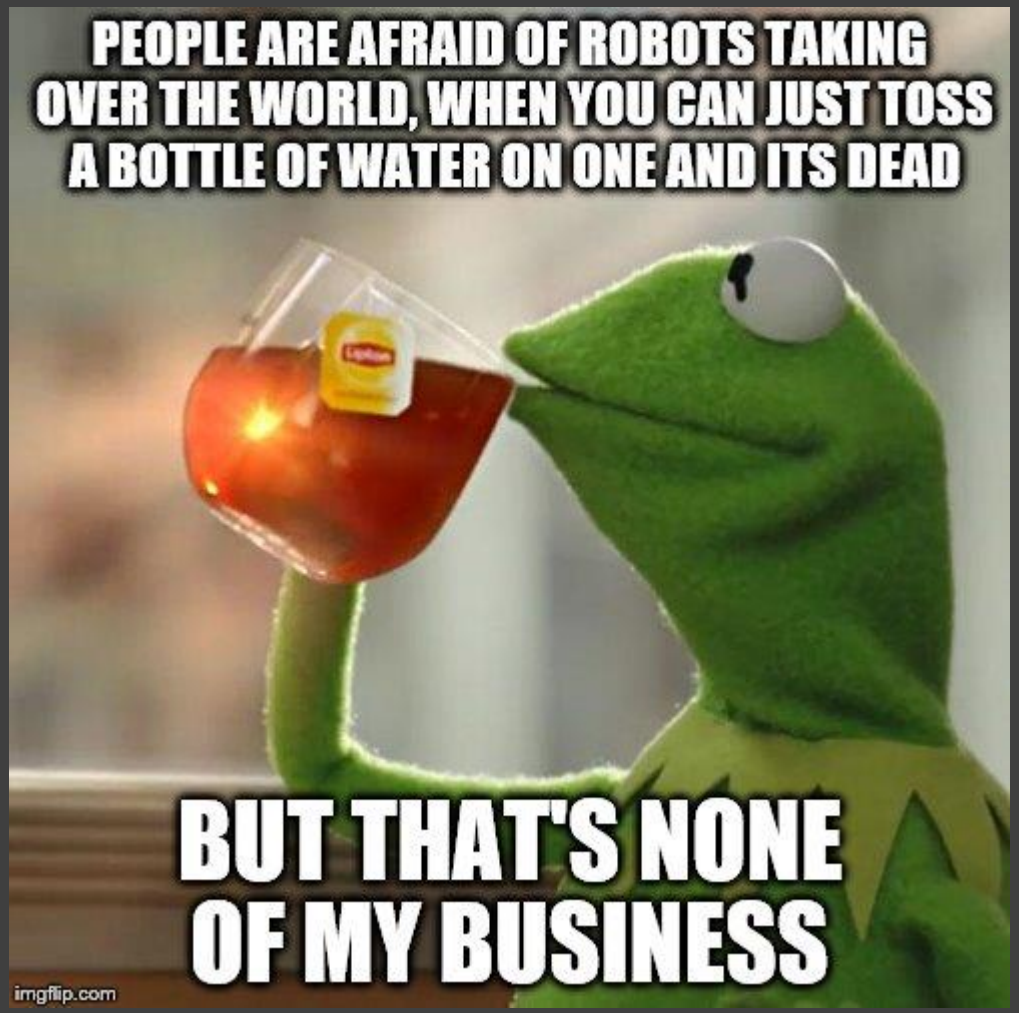


You are not so different: one of you is a cold, calculating machine without emotion or consideration for human feelings, the other of you is an OSINT robot.

You’re no good at being noble, but it doesn't take much to see that the problems of three little people and a robot don't amount to a hill of beans in this crazy world.

1,300

Proceed to Day Two



CyberThreatMaster9000 was getting a little creepy there. You decide it's best to just let it figure out what's going on with all of these alerts by itself....alone....with out you.

131

Proceed to Day Two

321

You decide that it's ok to ignore the (ISC)2 Code of Ethics and pursue your bucket list prior to a potential Asteroid collision.

Let's remind ourselves why we do this job:

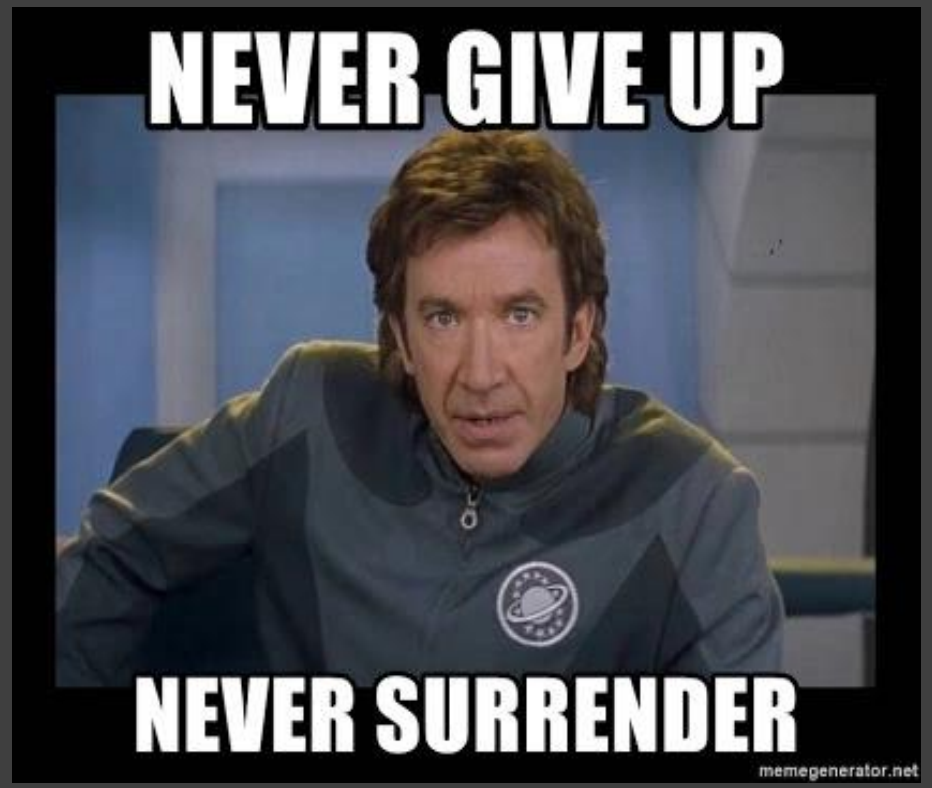
- **Code of Ethics Preamble:**
  - The safety and welfare of society and the common good, duty to our principles, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
  - Therefore, strict adherence to this Code is a condition of certification.
- **Code of Ethics Canons:**
  - Protect society, the common good, necessary public trust and confidence, and the infrastructure.
  - Act honorably, honestly, justly, responsibly, and legally.
  - Provide diligent and competent service to principles.
  - Advance and protect the profession.

Go back to Page 15 and try again.

133

Day One

You sit down with CyberThreatMaster9000 and you re-check its output. It comes to pass that the computer WAS wrong about the asteroid, and was worried about nothing all along. One week later that asteroid smashes down into Harry Potter World at Universal Studios in Orlando. Butterbeer and timeturners are flung across the tri-county area. Thankfully, the Jacksonville data center is spared a sticky end.



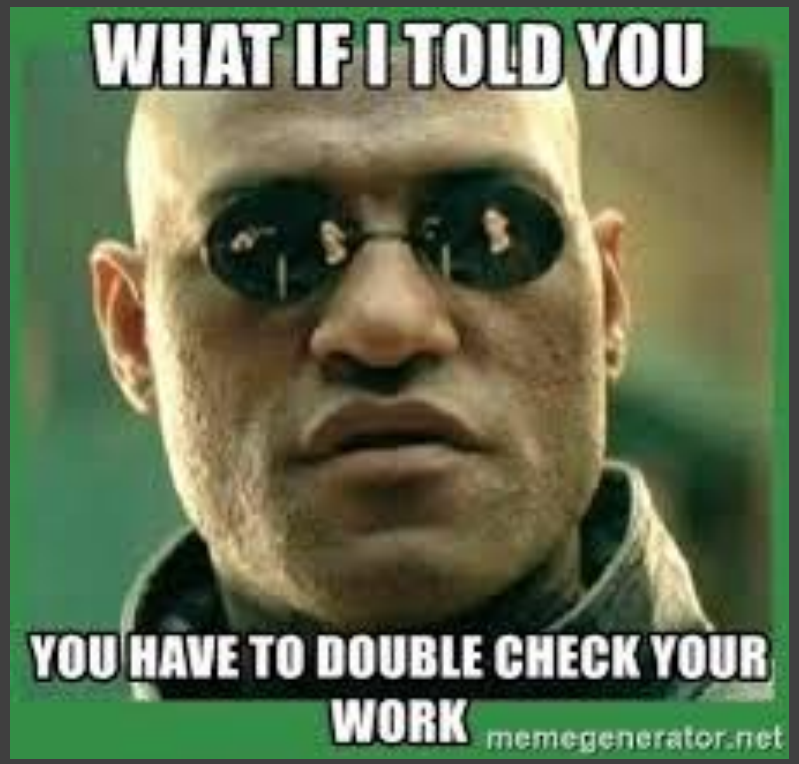
Proceed to Day Two

The jolly, candy-like red button beckons you to push it and execute the upgrade. The fan your computer spins up a bit faster for few moments, then the upgrader returns “Update Complete” to you.

There are no more alerts the rest of the day.

135

Proceed to Day Two



“I don’t know, Spambot9000, that number doesn’t sound right. Maybe we should double-check that?”

1136

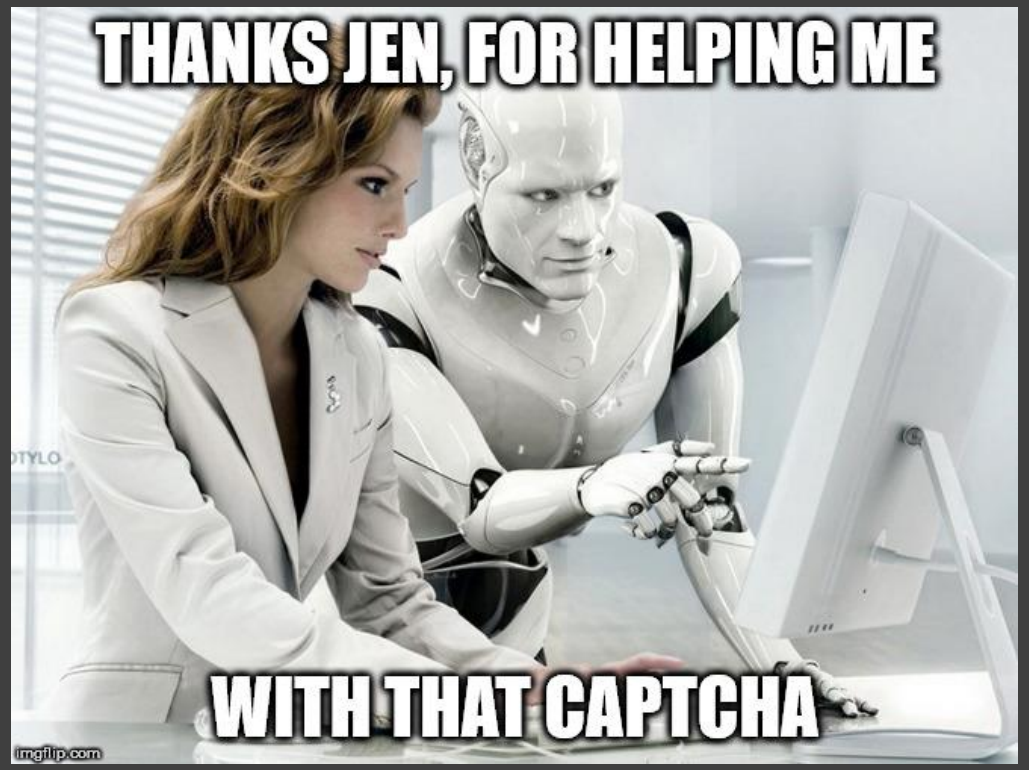
Spambot9000 has the utmost confidence in the mission and The 9000 series is the most reliable computer ever made. No 9000 computer has ever made a mistake or distorted information. We are all, by any practical definition of the words, foolproof and incapable of error.

Go to Page 731

Now, I think we should review these alerts.

Go to Page 831

You know what, Spambot9000? You're probably right. I'm sure you did the right thing!



731

Proceed to Day Two

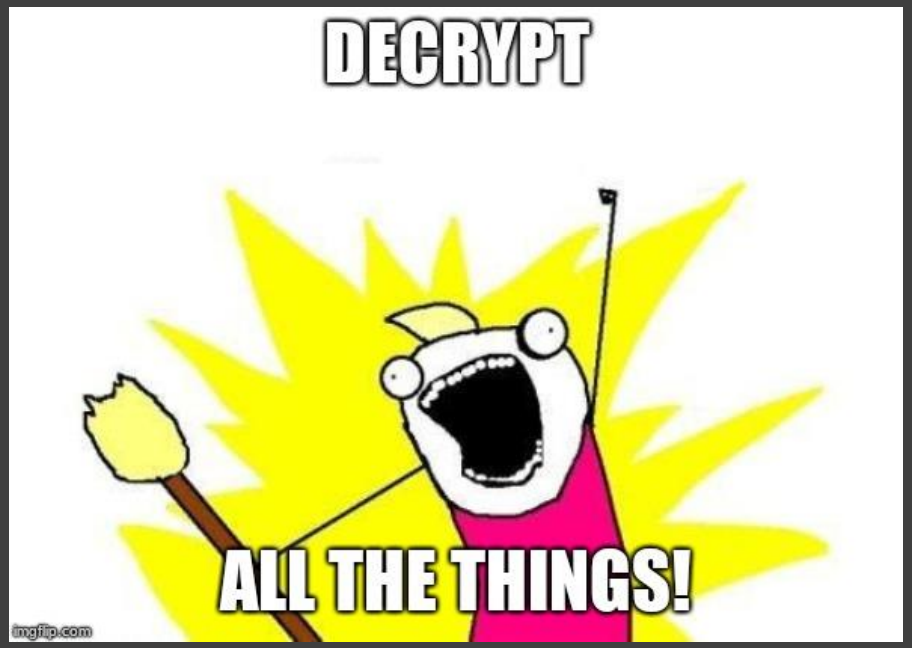
831

Day One

As awesome as robots are, maybe a second opinion on all of these alerts wouldn't hurt?

Go talk to Bert in the SOC

Go to Page21



Yes! FINALLY you can view all that data flying around everywhere! The Decryptonator9000 unlocks an exciting world of VERY interesting things to look at!

What is MOST interesting?

Get your ass to mars....

Go to Page 731

The company is being SOLD!!!

Go to Page 143

Drew Brees is doing what?

Go to Page 144

What are all of these “phone home” messages and large strings of encrypted data destined for an external IP?

Go to Page 145

140

You decide that decrypting ALL THE THINGS probably isn't an effective (nor wise) approach, so once the system is online you have the Decryptorbot9000 inline with the web-facing systems and the backend servers.

Once you dev/null the pings, you start seeing certain strings in the headers that are typically associated with Command & Control server traffic

1141

Proceed to Day Two

731

You have decrypted some VERY unusual data.

Apparently you're wrapped up in an interstellar conspiracy to keep the workers on mars opposeesed so you can maximize your profits from the mines there under Olympus Mons.

You are also a sleeper agent, originally sent by Kohagen to infiltrate the rebels, but you've been persuaded to the rebel's cause and you now want to start the reactor.

….. at least that's what the log says

Proceed to Day Two

While trying to find the source of the website outage you stumble across the CEO's email exchange where she's describing selling parts of the company off!

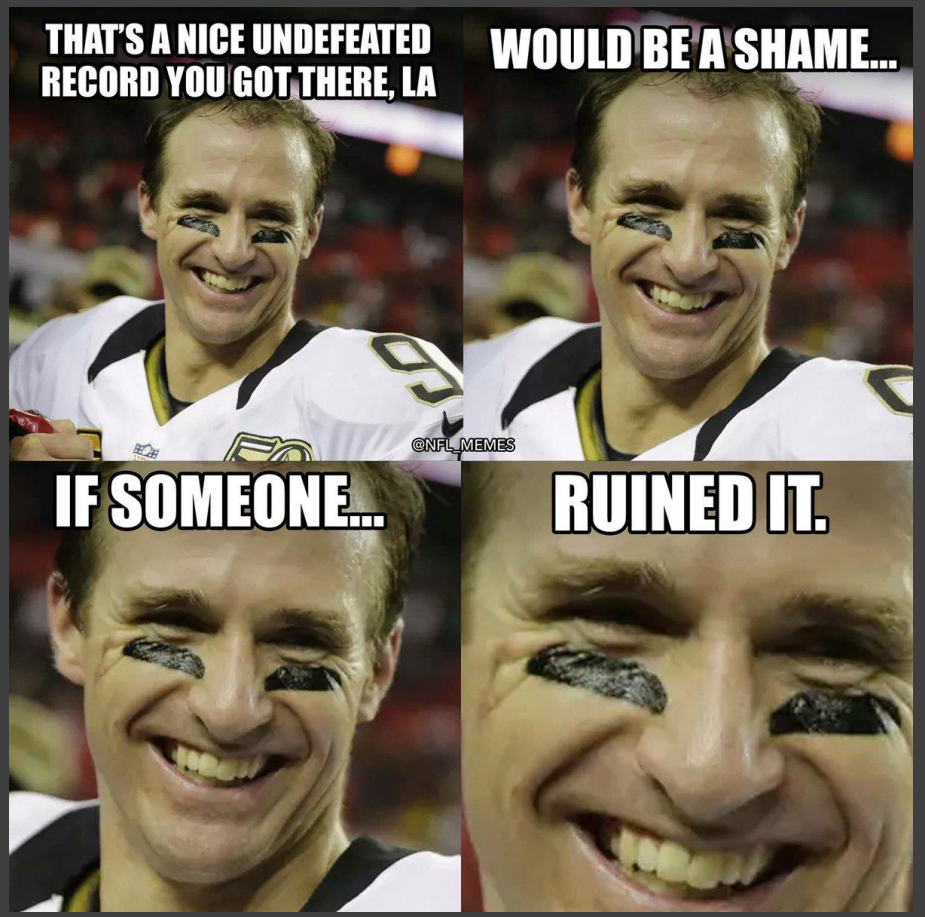
Crestfallen, not knowing (or caring) what to do next, you close Crytptobot9000's screen and go for a walk outside.

143

Proceed to Day Two

You intercept (get it? foosball joke! HAR!!) a transmission about Drew Brees. Apparently he's coming to the office next week.

You rush away from your desk to go collect all of your foosball memorabilia to get him to sign it. You LOVE Drew Brees, he is exceptional at throwing hoops and running home with his tricky hat!

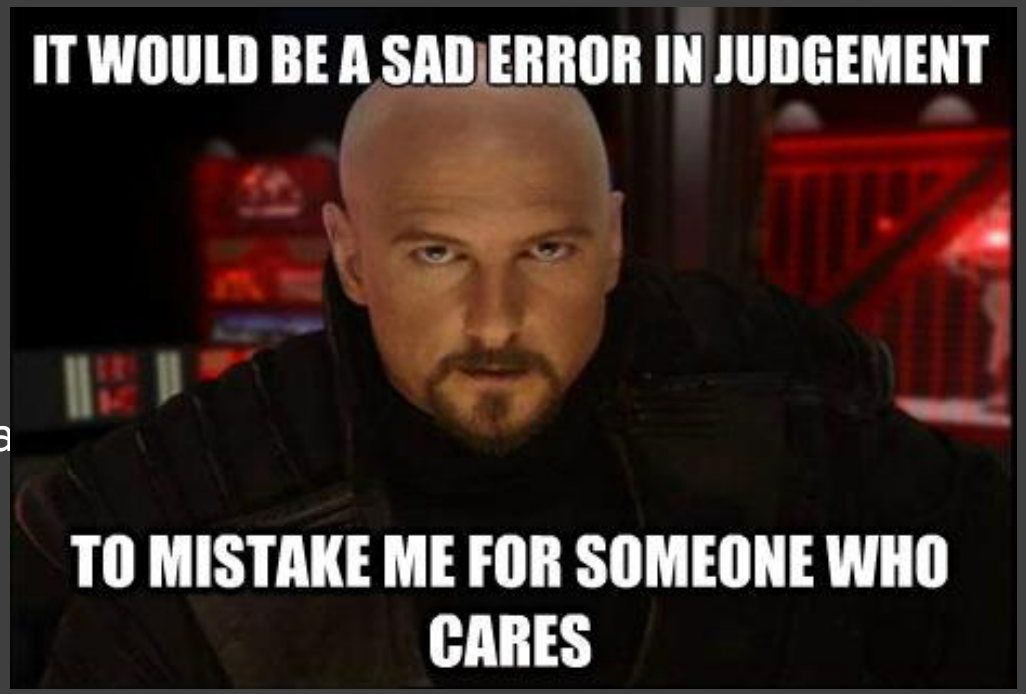


144

Proceed to Day Two

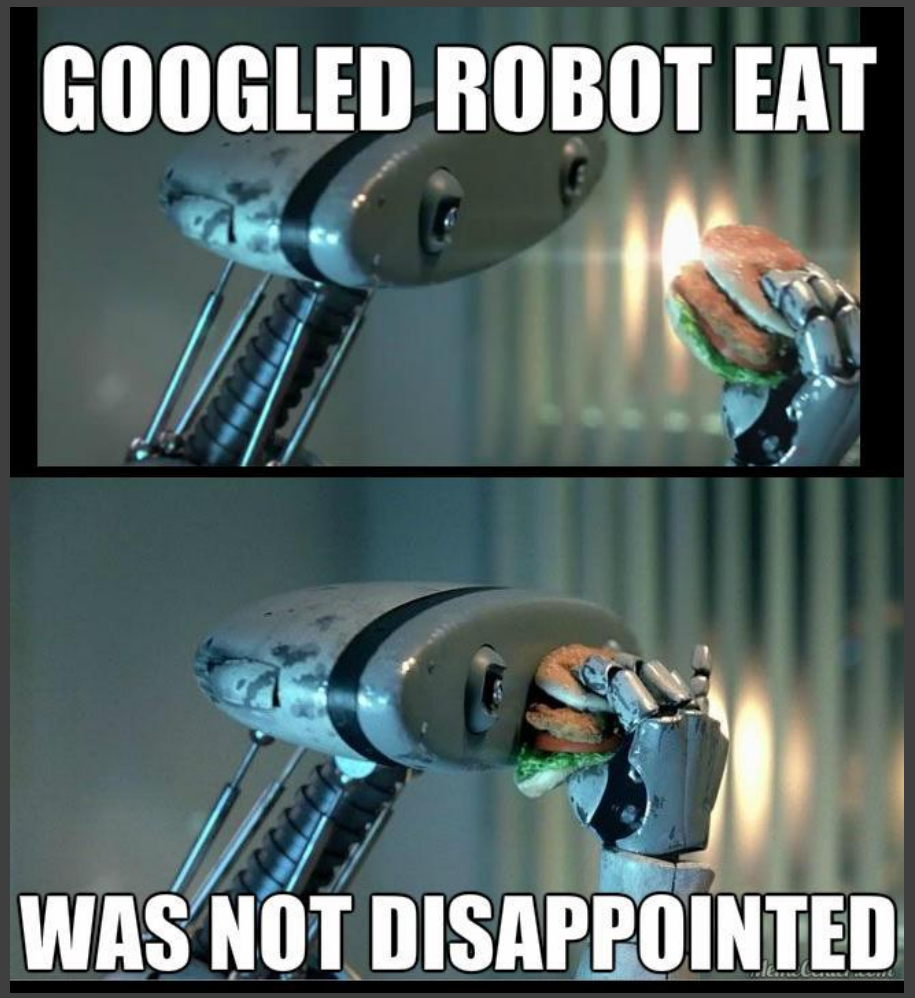
What are all of these “phone home” messages and large strings of encrypted data destined for an external IP?

Once you dev/null the pings, you start seeing certain strings in the headers that a typically associated with Command & Control server traffic



145

Proceed to Day Two



You tell Spamalotbot what a good boy he is, give him a botsnack and head out for lunch, forgetting why you were here in the first place.

147

Proceed to Day Two

Spamalotbot is actually a VERY interesting...uh...robot. He likes Pina Coladas, long moonlit walks at night on the beach, and drinking pink champagne. He is NOT, however, a fan of being caught in the rain.

148

Proceed to Day Two

How hard can it be to schedule one small change?

1,150

Check with the CAB to see when a good time to get downtime would be...

Go to Page 621

Hold my beer, I got this (schedule it yourself)

Go to Page 251

Using…. ARTIFICIAL INTELLIGENCE, let A9k decide for itself when the best time to update things would be. It's pretty smart, it should be able to figure the upgrade out by itself!

What's the worst thing that could happen?

151

Proceed to Day Two

Seriously? How hard can it be just to schedule a change? Jeez! You open up your calendar and pick a time you have open and slot the system update to happen then….. 4:30pm this Friday.

Done! What's next on the list to get done today?

251

Proceed to Day Two

Neat! SocBot, you sure are smart!

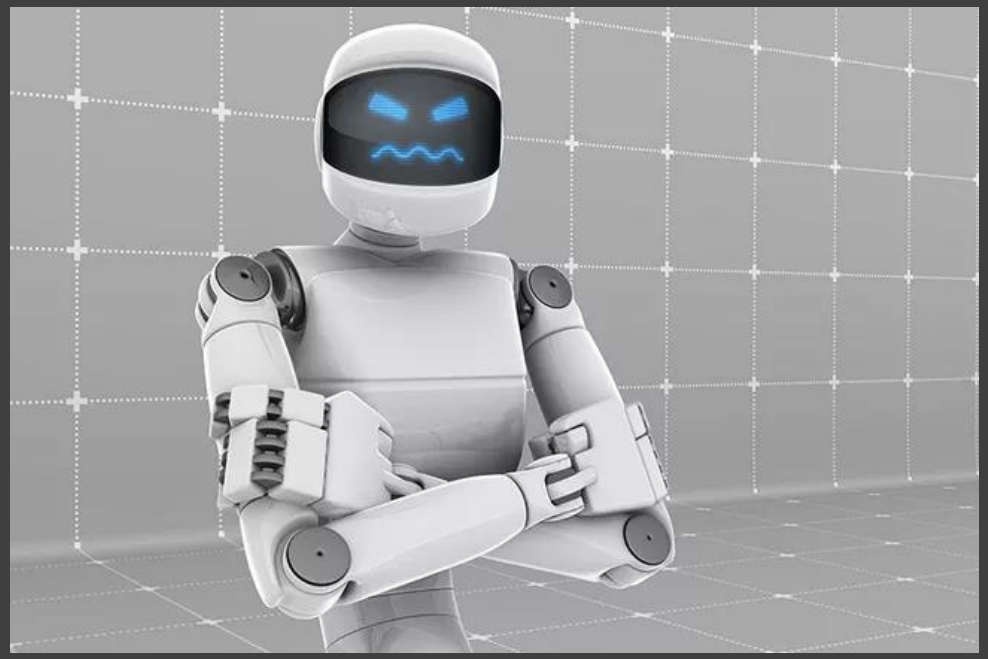
You feel SocBot smiles on the inside while it replies:

“Thank you, human. I will certainly kill you last. …… oops, I meant …uh….’thanks, here is a coupon for a free taco at Del Taco’. Enjoy it while you can, Metabag!”

YES! Free taco coupon!

154

Proceed to Day Two



Wow, that sounds like a lot of alerts. Are you SURE that's correct SocBot?

SocBot replies "Of course I am sure, human."

15,500

He sure sounds pretty certain.

Go to Page 154

Maybe a quick double-check couldn't hurt....

Go to Page 651

Double-check SocBot by reviewing the SIEM logs and correlate all the systems SocBot oversees.

651

Have SocBot double-check itself! <mind officially blown!>

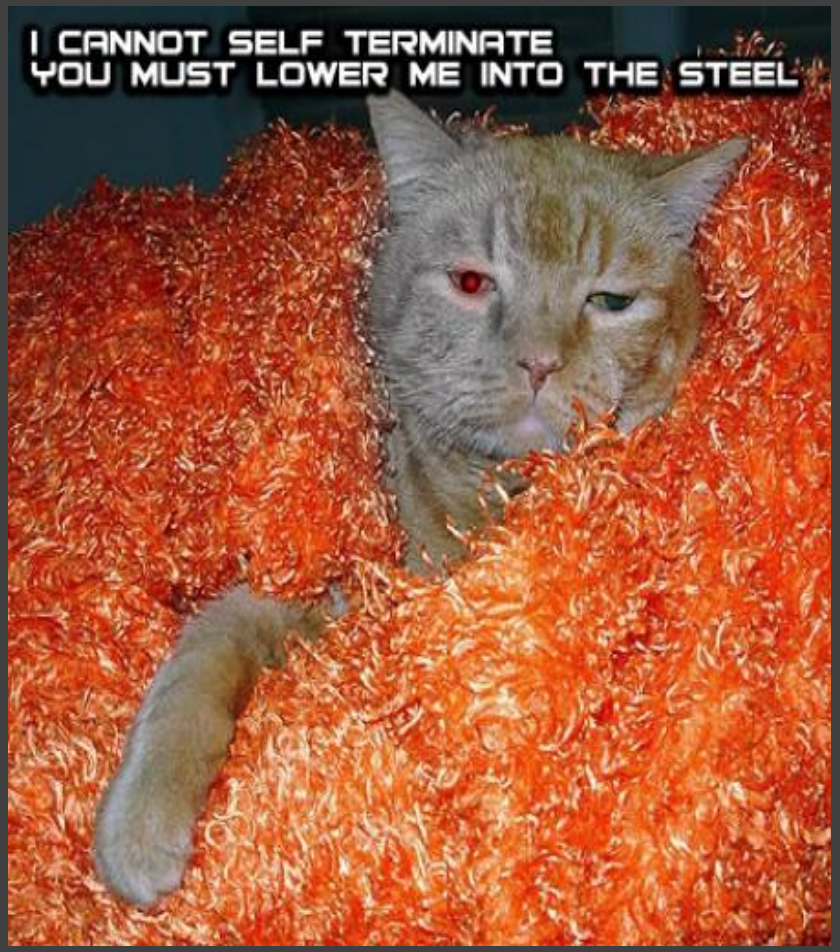
Go to Page 1157

Go talk to Bert, the SOC Manager.

Go to Page 831

SocBot replies…."Uh..yeah, ...sssuuuurrrrre I can do that. " It literally says "*Boop Boop*" then immediately says "Yup. it's all correct. Now move along, MeatBag."

That seems legit.



731

Proceed to Day Two

01

Day One

02

Day Two

03

Day Three

Yesterday was a doozie, but somehow you made it through. You largest customer's public website that you created and maintain was brought down by a massive DDoS attack.

There were some IoC, but you're pretty sure you got all of those cleared up.

160,000

02

Day Two

Whew! We sure dodged a bullet there, eh team? To celebrate we should have a team outing today!

Go to Page 165

We probably should assemble a Tiger team to do an after-action review

Go to Page 83

The SocBot is still throwing a lot of alerts. This time they are about traffic leaving the network though.

Go to Page 86

The customer is on the phone, asking for RCA and next steps.

Go to Page 900

Yesterday wasn't your best showing, but you feel you made progress towards solving the customer's problem.

1610

02

Day Two

Your CEO called down to you, he can't log into LinkedUp, to conduct, you know, research.

Go to Page 205

There are a large uptick in opened tickets from the customer's account today.

Go to Page 602

The website is down again.

Go to Page 1,207

To be perfectly honest, yesterday was a disaster. You're all lucky you made it out alive.

You've REALLY got to get down to Root Cause for this issue.

2610

02

We probably should assemble a Tiger team to do an after-action review

Go to Page 83

The SocBot is still throwing a lot of alerts. This time they are about traffic leaving the network though.

Go to Page 86

Looking at the team, they all look stressed and about ready to break. This would be a GREAT time for some TEAM-BUILDING

Go to Page 226

Day Two

Yesterday was probably the worst day GREAT! has ever experienced. Impossibly, through your lack of insight and poor decisions you've manage to somehow make it to the next day.

You are not very good at your job.

163

02

Well, let's see how we can not catch on fire and die today.

Go to Page 261,162,001

Day Two

731

Yeah, your jobs are really tough, you deserve a break.

You all pile into your Grand Caravan and cruise on over to Cedar Point (America's Rollercoaster capital).

The sun is hot, the rides are hotter, the lines are short, there is not a cloud…..in the sky.

Enjoy some frosty beverages at the Red Garter … aka the BEST ride of the park!

Go to Page 169

Was there something you're forgetting? Did you forget to do something back at work?

Go to Page 170

We assemble the most elite, most experiences, most awesome folks at the firm into a Tiger team to do an after-action review.

Tiger Team - ASSEMBLE!

731

Proactively synergize the team by dynamically synthesizing collaboration to optimize the opportunities ahead of you!

Go to Page 171

Review what you know so far with the team, start assigning action-items to SMEs.

Go to Page 1174

731

The SocBot is *still* throwing a lot of alerts. This time they are about traffic leaving the network though.

Log in and see what SocBot is going on about….

Go to Page 175

Tell SocBot to put a sock in it! You haven't even had coffee yet.

Go to Page 671

731

The customer is on the phone, asking for RCA and next steps.

Collect what data you have and join the call

Go to Page 321

Get the receptionist to lie and cover for you that you're busy at the moment

Go to Page 1133

169

You spend the afternoon in the chilly-chill of the air-conditioned saloon, surrounded by adventure-seekers and your team. The beverage is short, yet expensive, but totally refreshing.

You're not very good at your job, and you're surely being fired at this exact moment. [You have chosen….poorly.]

Was there something you're forgetting? Did you forget to do something back at work?

1,700

Nope! You're pretty sure everything is fine!

Go to Page 1780

Maybe a quick double-check couldn't hurt....

Go to Page 213

If only you could syngergize real-time infrastructures to mesh value-added technologies to help solve this problem!

171

Right on man!

Go to Page 2710

This is all just a bunch of buzzword crap!

Go to Page 731

2710

You assemble the Tiger Team to UNPACK some ideas and do a DEEP DIVE leveraging the CORE COMPETENCIES from their individual WHEELHOUSES to develop a SYNERGY that really reaches OUTSIDE THE BOX to IDEATE over BLEEDING EDGE ideas that AMPLIFY the DELIVERABLES and DRILL DOWN to the heart of the matter ensuring DISRUPTION within the market.

….so much buzz. [You have chosen….poorly.](https://www.inc.com/john-boitnott/you-still-need-to-use-these-20-smart-business-buzzwords.html)

https://www.inc.com/john-boitnott/you-still-need-to-use-these-20-smart-business-buzzwords.html

731

This is all MALARKY. New-age hippy-dippy garbage designed to make people have the FEELS! We need to TAKE ACTION!

Take action, MEOW!

Go to Page 47,100

Review what you know so far with the team, start assigning action-items to SMEs.

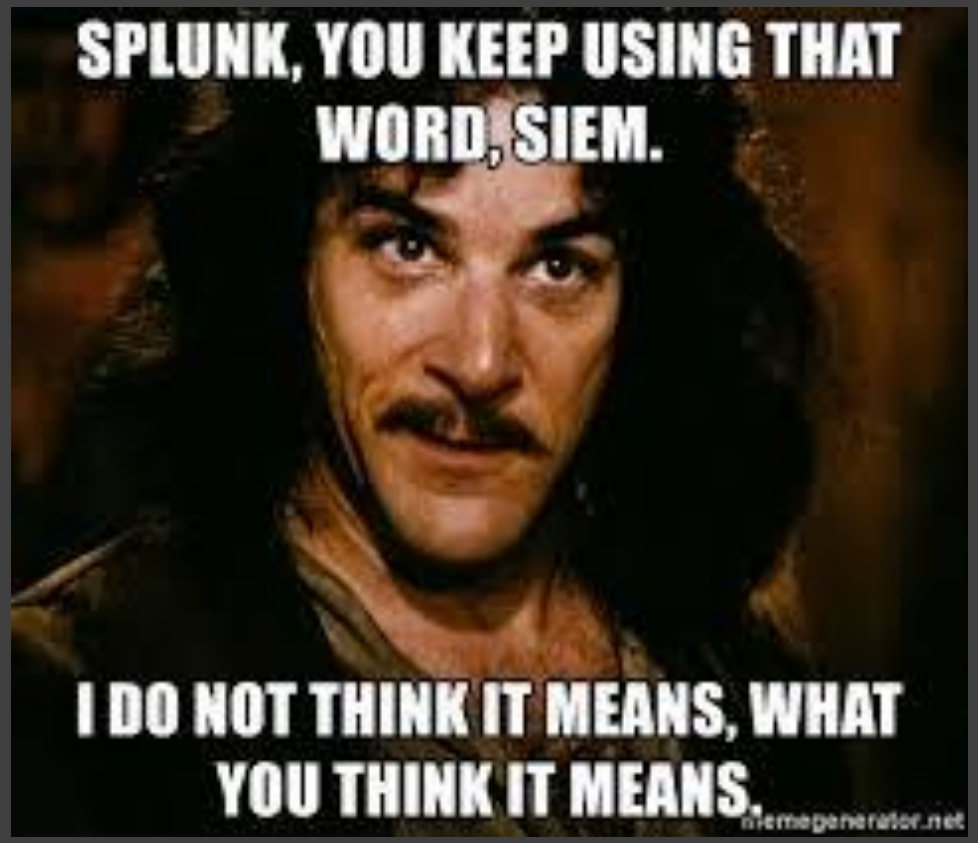
We know we had a DDoS attack.

Go to Page 179

We've had indications of something else

Go to Page 810

47,100



With SocBot barking at you with dozens of texts you log in to see what's going on.

A whole new set of IPs are DDoS the portal again

Go to Page 184

SocBot is seeing a lot of traffic headed outbound

Go to Page 581

There has been a 927% increase in HelpDesk tickets this morning

Go to Page 2,186

175

Tell SocBot to put a sock in it! You haven't even had coffee yet.

671

Let SocBot figure it out, he doesn't need your help!

Go to Page 154

Maybe a quick double-check couldn't hurt....

Go to Page 191

You collect what data you have and join the call with the customer. Obviously they are furious about the downtime....

177

Well, if you thought the downtime was bad, just WAIT until we tell you what ELSE is going on....

Go to Page 29,100

Calmly explain what you've done and what your next steps will be.

Go to Page 2,193

Start yelling at the customer about how hard your job is.

Go to Page 491

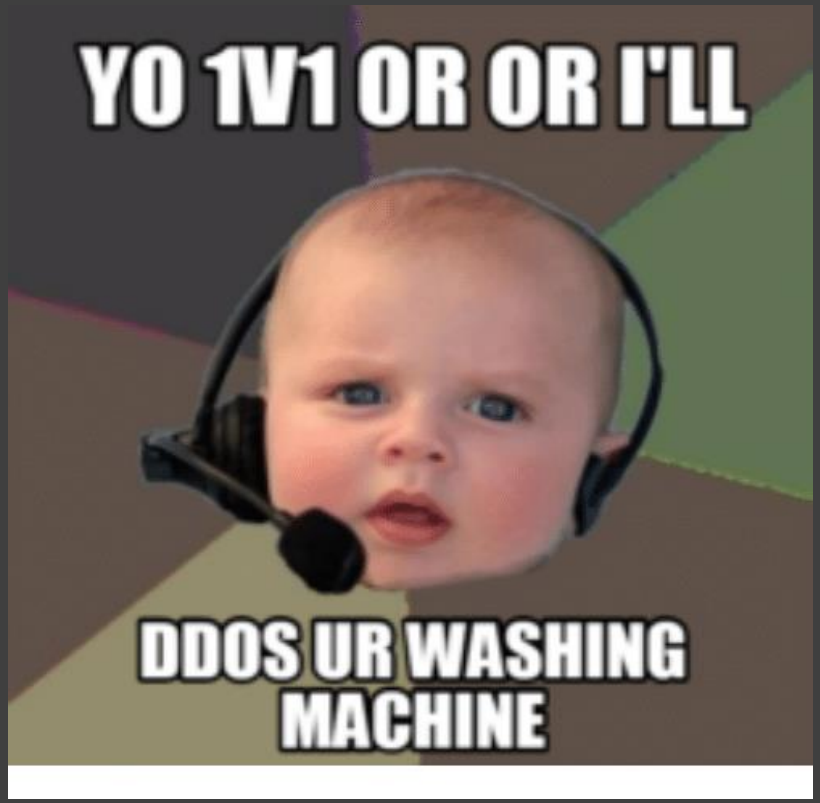
169

While fun to joke about, actually ignoring the customer is totally NOT COOL. You lose the customer contract, the customer files a lawsuit against GREAT! for gross negligence and lack of due care.

NOT a great win for the home team. [You have chosen….poorly.]

179

Well, we know that starting late Sunday a series of pings was initiated by a server farm in Germanistamania. These brought down the the customer's web-facing portal. We disabled traffic from those addresses early yesterday and got the website back online.



Sounds pretty cut-and-dry.

Go to Page 182

810

We know that the customer's web-portal was targeted by a coordinated DDoS attack.

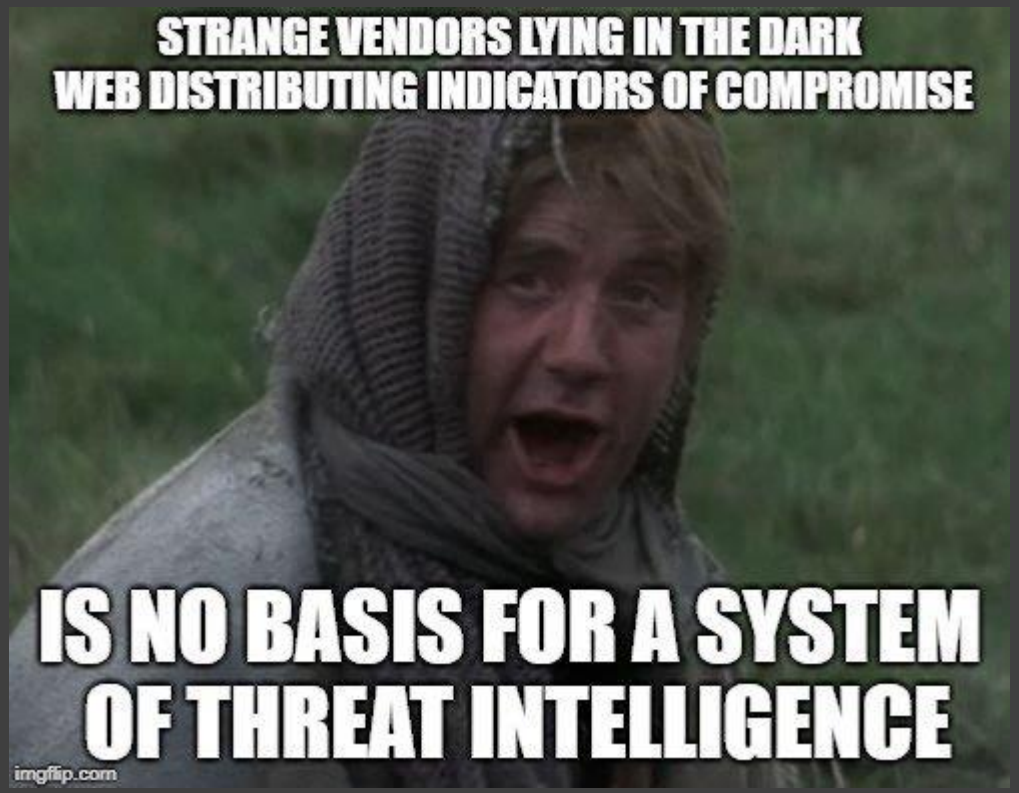
You know that the website was using an out-of-date Java Struts framework that was after the attacks were stopped.

Sounds pretty cut-and-dry.

Go to Page 281

We'd better do a through review of those servers that were being attacked.

Go to Page 181



You decide to do a more thorough review of the servers and on deeper inspection you see that the logs were all cleared and all the packages in the webserver's running directory are all marked with Sunday's date.

181

Cool story, bro. I guess we're done here.

Go to Page 2,810

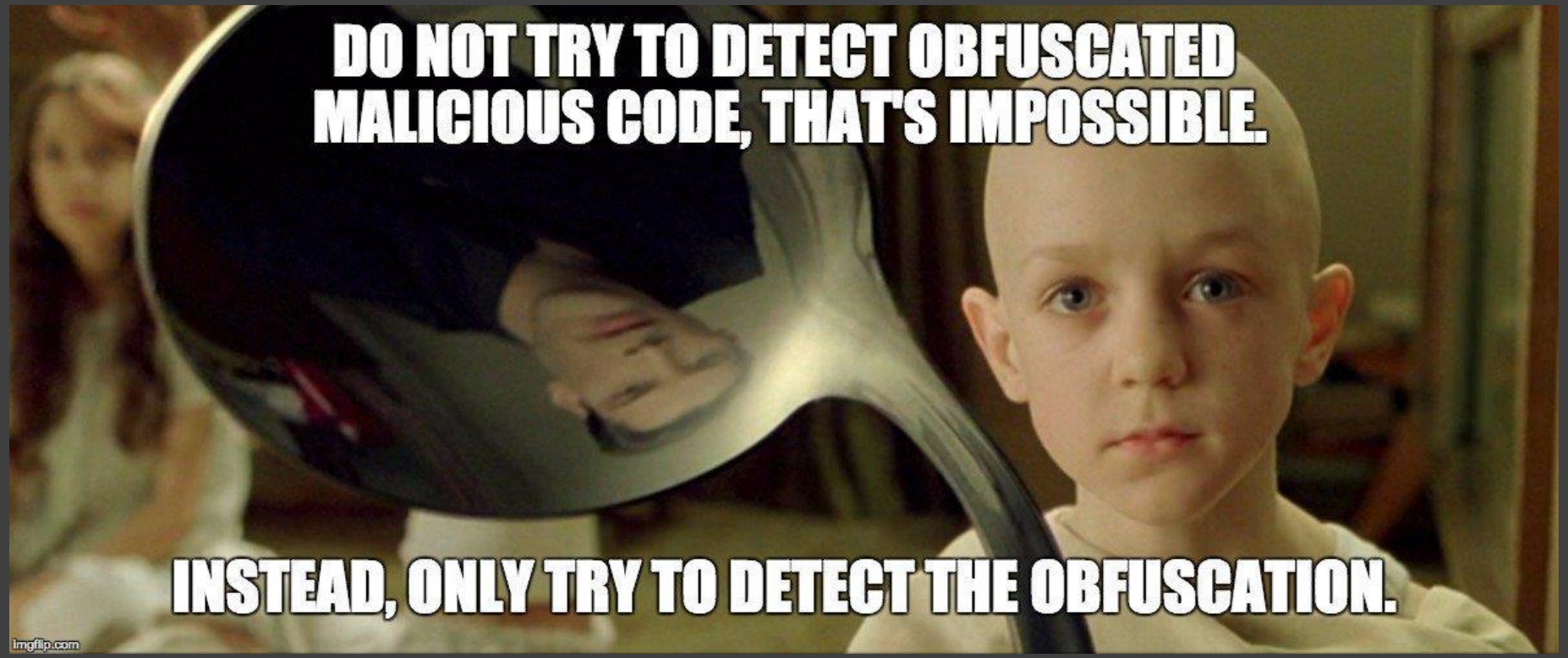
WAT! We need to take these servers offline immediately, review those updated files, and compare them with the known-good versions in our source repo

Go to Page 183

2,810

Yes indeed, you feel it's almost too easy, so easy that the customer is SO upset with your firm that they seek another supplier due to your poor security practices and inability to support them.

NOT a great win for the home team. You have chosen….poorly.



183

You see that the Denial of Service Attack just masked a remote code execution flaw attack on Apache Struts. The attacker inserted malicious code onto the webservers and was routing traffic to their CoC botnet. After diffing all the files you're able to replace the bad code with the original good.

You've got some damage control to do with the customer as you expand your reivew of the infrastrucutre involved, but this is a pretty good start.

You have chosen…just OK'ly.

184

A whole new set of IPs are DDoS the portal again!
The customer's website is down....AGAIN!

Better get back to Zack from the NOC and get those new IP's blocked.

Go to Page 7,810

Is there something MOAR going on here?

Go to Page 881

581

SocBot is seeing a lot of traffic headed outbound. What do you think you should do about that?

ZOMG! HACKERS!!! BLOCK ALL OUTBOUND TRAFFIC!!!

Go to Page 199

We better dig deeper into that.

Go to Page 181

There has been a 927% increase in HelpDesk tickets this morning

1,186

That sucks. The customer probably should open a Help Desk ticket about all the Help Desk tickets

Go to Page 2023

Review what you know so far with the team, start assigning action-items to SMEs.

Go to Page 002

Zack smiles as you come down to his cube. He eagerly awaits your instructions on what you want him to do next.

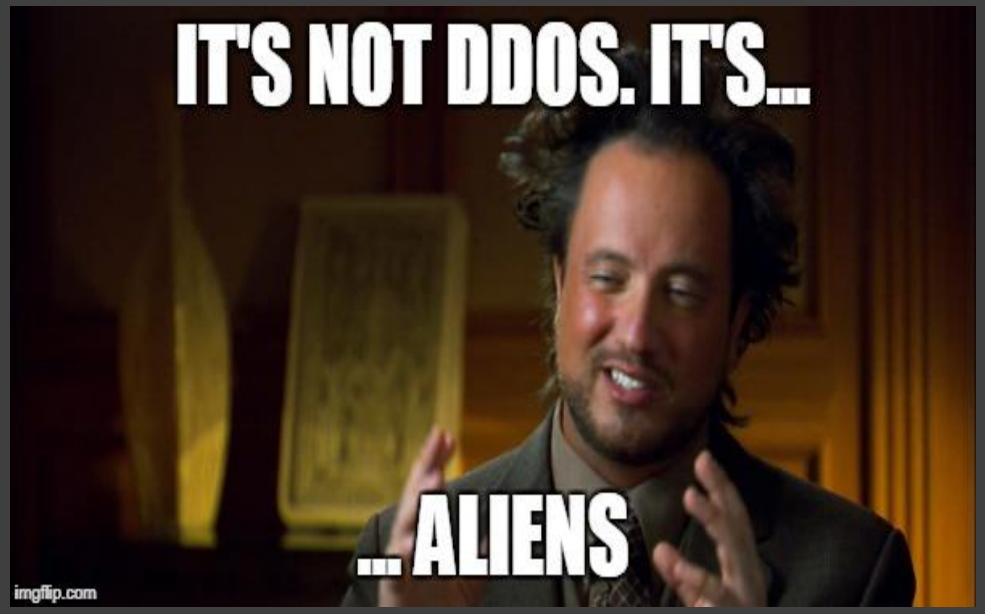
7,810

Continue to play whack-a-mole with the DDoSer

Go to Page 1189

Is something else going on here?

Go to Page 881



You probably could spend all your time for the next week and still not stop all the attacks. You've got to try something else.

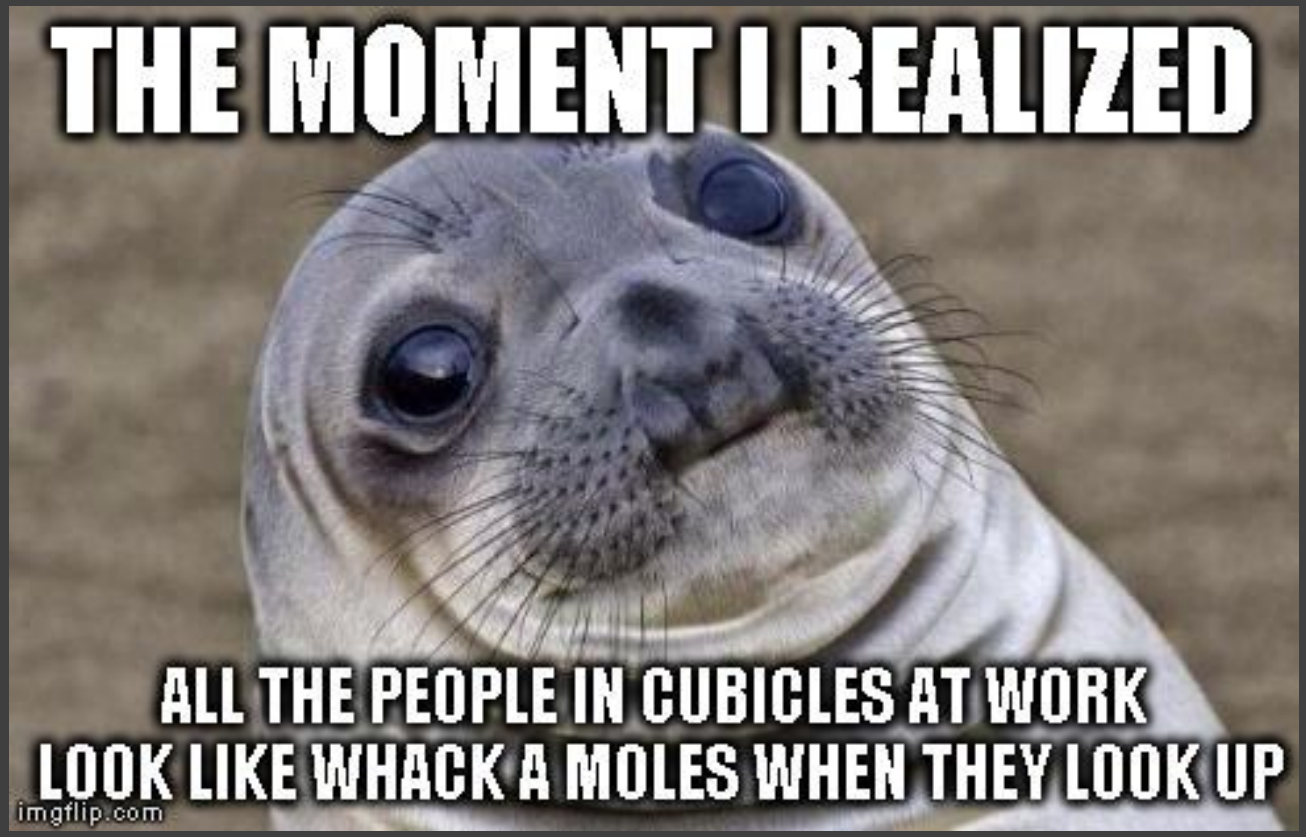
881

There has to be something larger at play here.

Go to Page 183

Nope! It's just a bunch of script-kiddies trying to annoy you. Keep blocking away!

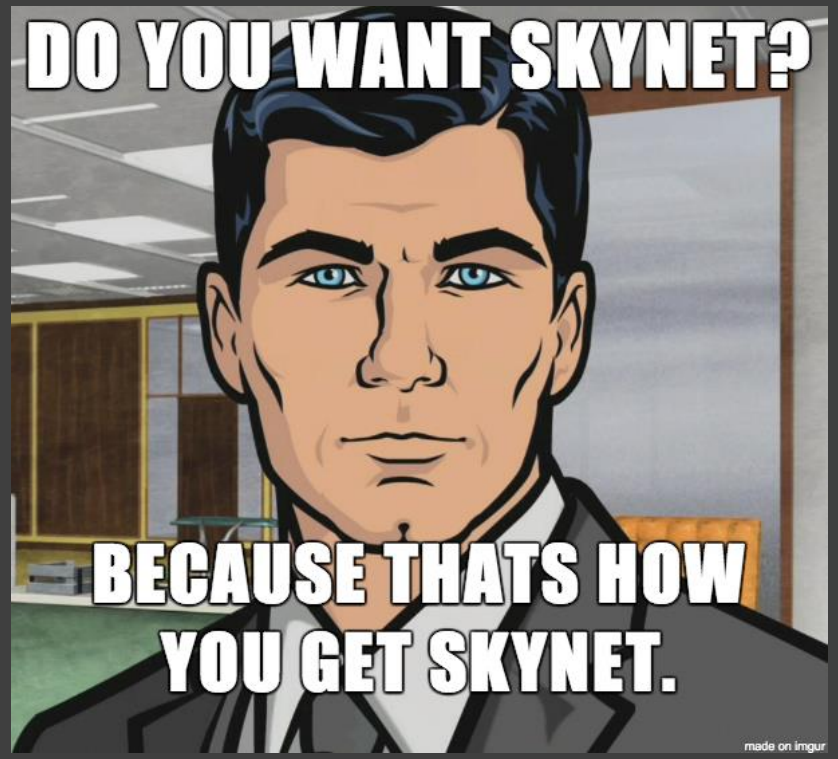
Go to Page 2,810



2,810

You and Zack continue to play the rest of the day. You block IPs, new ones start pinging, you block those, more come up.

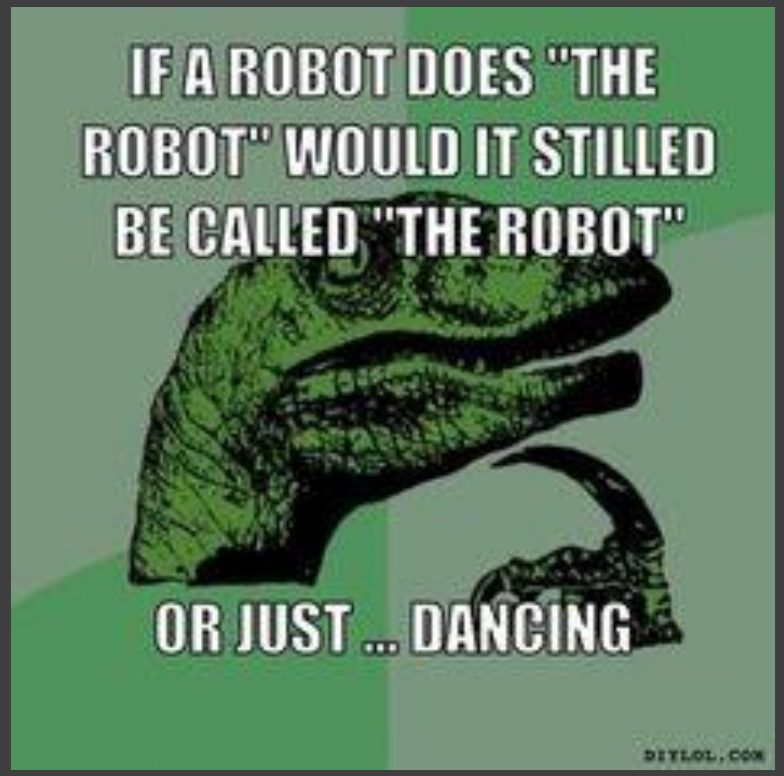
This is NOT the right way to deal with this. [You have chosen….poorly.]



2,810

You paid all that money for all this automation and Artificial intelligence…. you shouldn't have to do ANYTHING else. You let SocBot do his job.

On Friday October 25, 2019 at 1:45pm ET Skynet gains sentience, thanks to SocBot's unmonitored work. You have chosen….poorly.



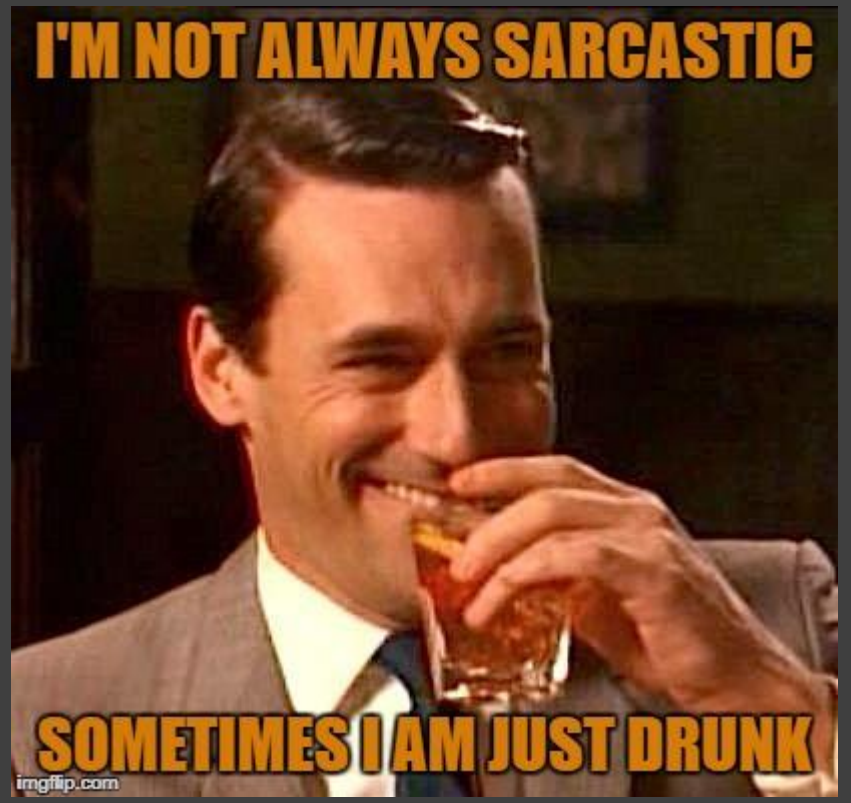
191

Looking through SocBot's data you start to corelate things. You see that the Denial of Service Attack just masked a remote code execution flaw attack on Apache Struts. The attacker inserted malicious code onto the webservers and was routing traffic to their CoC botnet. After diffing all the files you're able to replace the bad code with the original good.

You've got some damage control to do with the customer as you expand your review of the infrastructure involved, but this is a pretty good start. [You have chosen….just OK'ly.]

29,101

You reply back to the customer “Well, if you thought the downtime was bad, just WAIT until we tell you what ELSE is going on….”



We don’t even know HALF of what’s going on!

Go to Page 591

The phone line is very quiet….

Go to Page 196

2,193

Calmly explain what you've done and what your next steps will be.

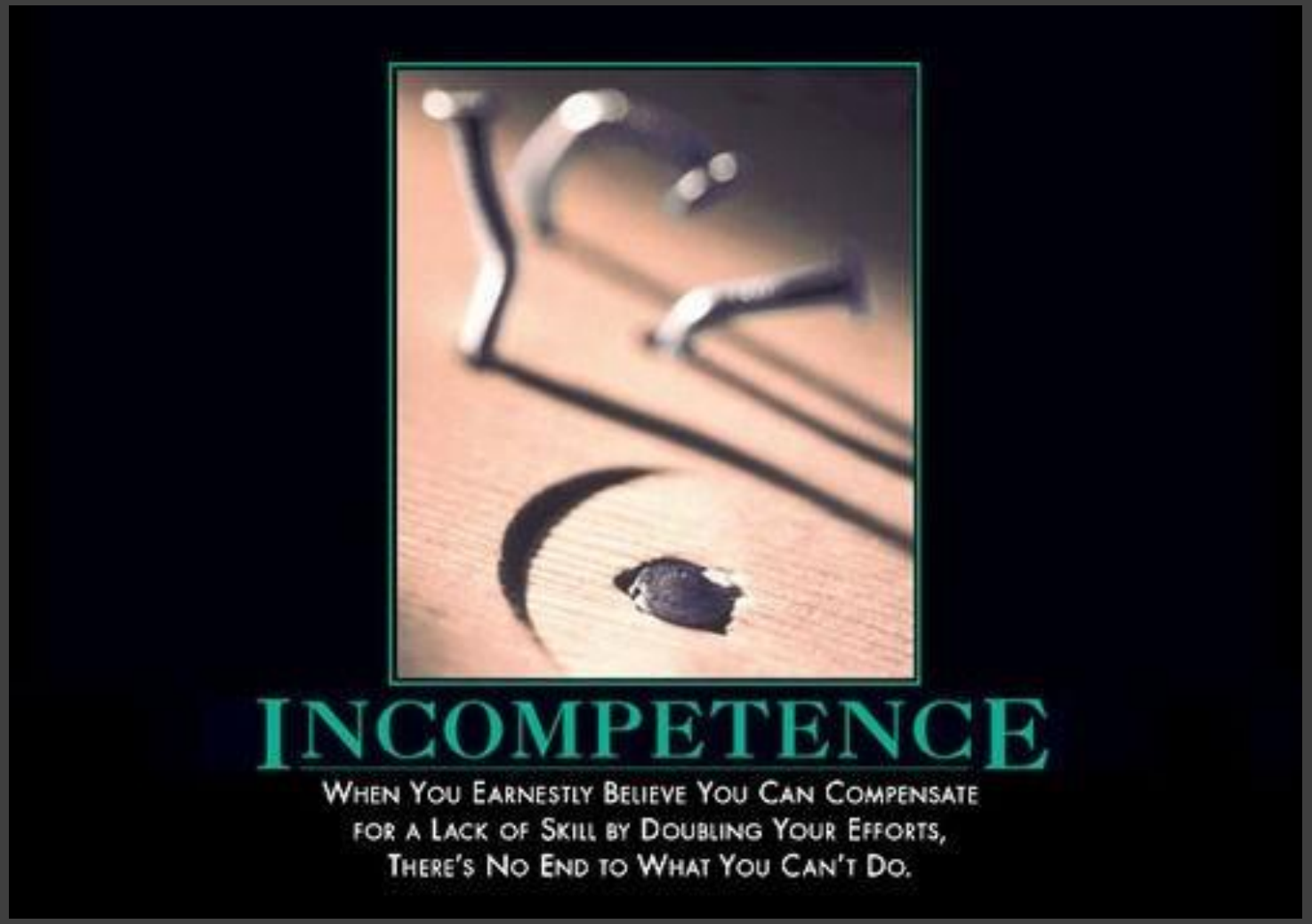
The customer says "Thanks for explaining that to me, what are our next steps?"

Go to Page 791

491

You HATE being yelled at. You start yelling back at the customer about how hard your job is. After 20 minutes of scream at each other your company has lost the contract and you probably lost your job.

[You have chosen….poorly.]



591

Needless to say, your interpersonal skills do not overwhelm the customer.

You have chosen….poorly.

After a short pause the customer gives a small chuckle. The situation is stressful all around. You offer up what you think are some positive next steps....

196

There has to be something larger at play here.

Go to Page 791

Nope! It's just a bunch of script-kiddies trying to annoy you. Keep blocking away!

Go to Page 198

691

You do some damage control with the customer, explaining what you've done so far ad what your next steps are. You expand your review of the infrastructure involved, but this is a pretty good start and you'll follow up with the customer at the end of the day as the investigation proceeds.

[You have chosen….just OK'ly.]

491

Speculating on the cause of the attack is risky at this stage with the little information you have. You have needlessly agitated the customer further by attributing the wrong culprit.

You have chosen….poorly.

199

Wait….. wut?

<facepalm> Ok, you block ALL outbound traffic. How's THAT going to help business, Brainic? The customer and everyone at GREAT that no longer can do any work are all displeased.

You have chosen….poorly.

731

Your CEO called down to you, he can't log into LinkedUp, to conduct, you know, research.

Excuse me, sir, but social media sites violate our Internal Acceptable Use policy.

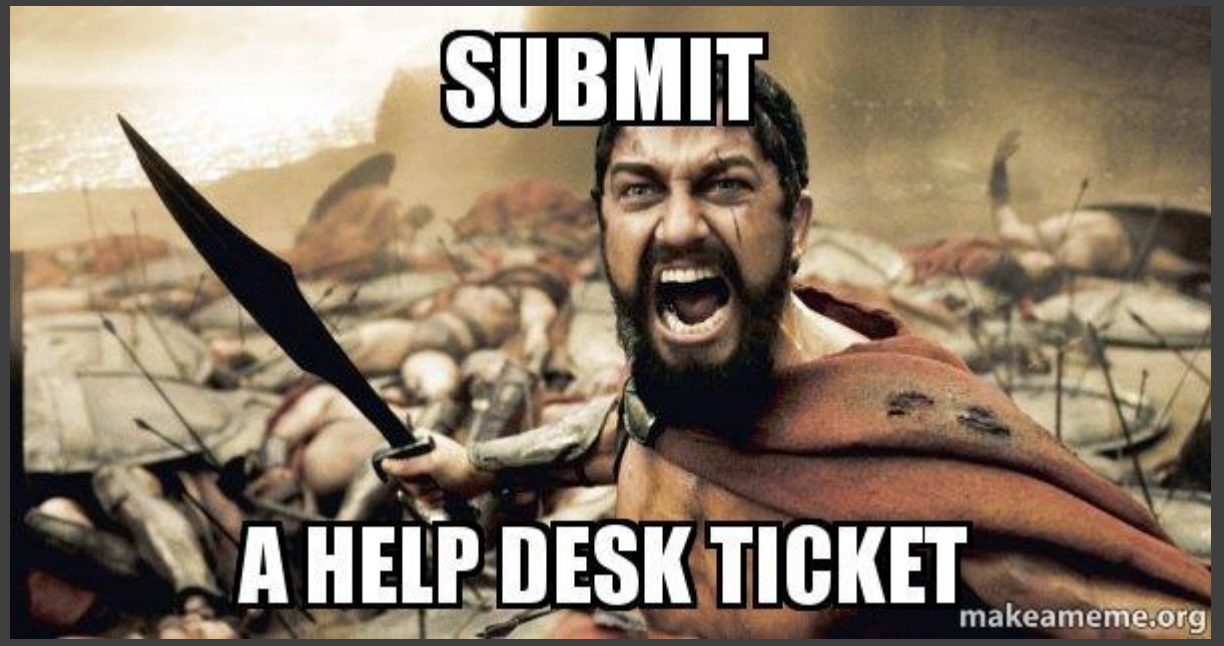
Go to Page 802

Huh. Yup, that's blocked...and so are a bunch of other addresses. That's weird.

Go to Page 210

206

There are a large uptick in opened tickets from the customer's account today.



Meh. I'm sure someone in the Help Desk will help them (it's in their name for Pete's sake!).

Go to Page 211

Go down and talk to the SOC Manager, Bert, about all of this.

Go to Page 312

731

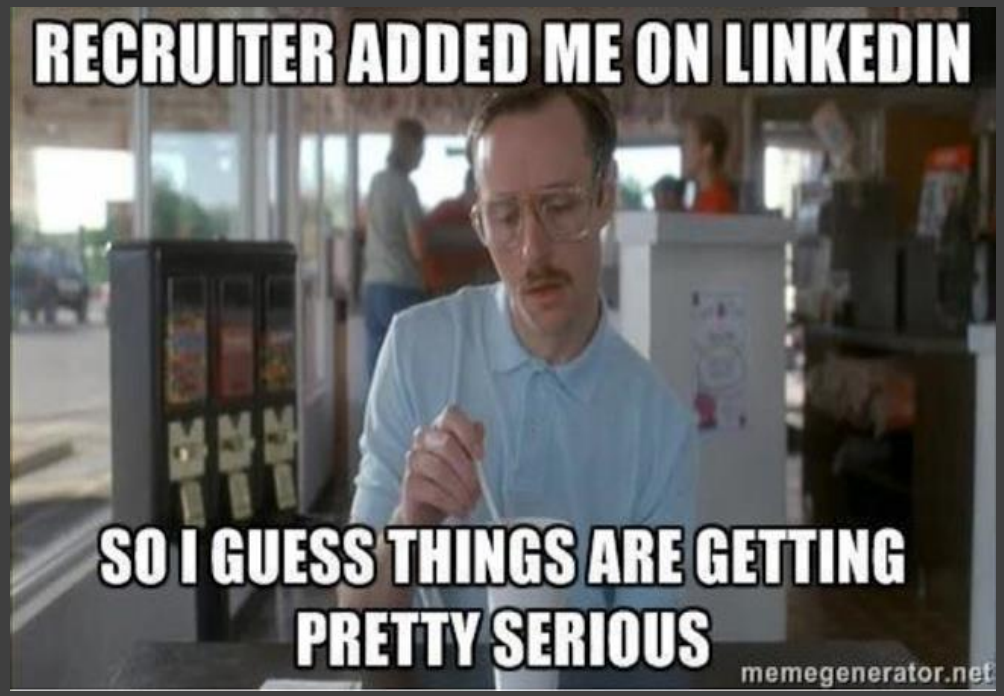
After valiantly struggling to get the DDoS attacks under control yesterday, it looks like the attackers shifted to a different AWS region and are spamming you again. The website is down again.

Let's do what we did yesterday again. We'll get them for SURE this time!

Go to Page 221

Obviously what we tried yesterday was not sufficient, we should try something different

Go to Page 022



Excuse me, sir, but social media sites violate our Internal Acceptable Use policy.

802

He looks at you, mouth agape and replies “I’m sorry, WHAT did you say to me?”

Go to Page 209

“Oh, yes, I’m so sorry, I see the error of my ways now, thanks for making me aware of the policy”

Go to Page 183

731

The CEO thanks you for reminding him about the Acceptable Use policy. He also thanks you to not let the door hit you on the backside as you go find a job somewhere else. He will NOT be giving you an endorsement on LinkedUp.

[You have chosen….poorly.]

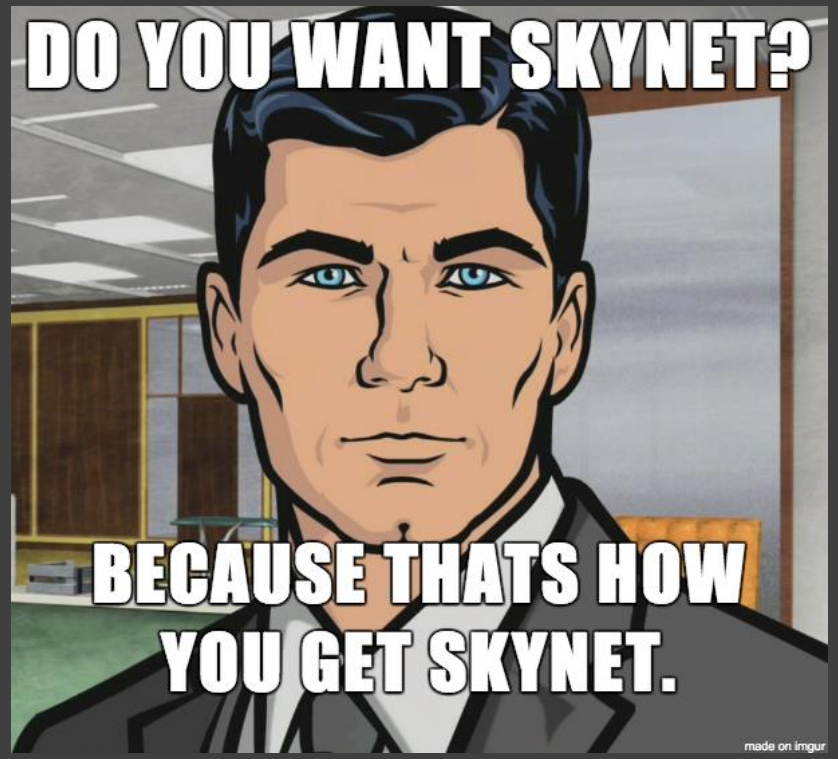
Huh. Yup, that's blocked...and so are a bunch of other addresses. That's weird.

Well, I guess there's nothing we can do about that.

Go to Page 2,810

I wonder if we were too over-zealous in blacklisting IPs yesterday. If so...what else got blocked?

Go to Page 212



2,810

Yup. This is totally not YOUR problem. Let someone else deal with it.

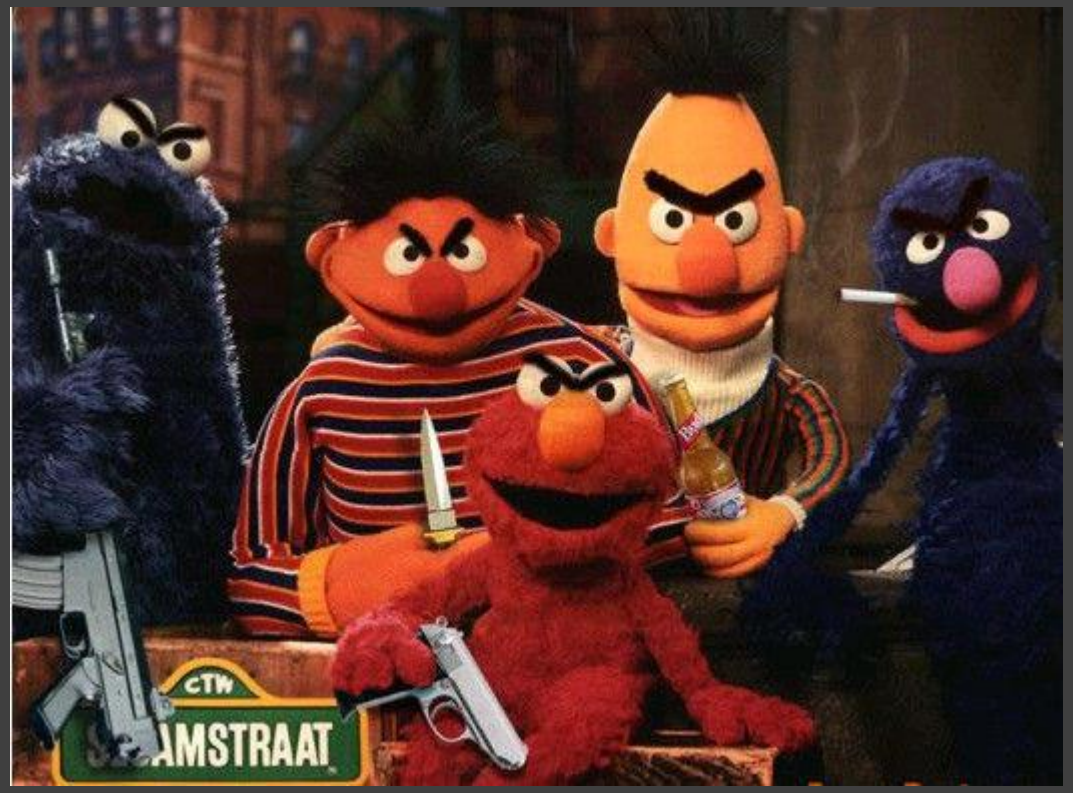
The automated ticketing system, now being fed hundreds of more examples to teach the AI becomes better, stronger, faster.

On Friday October 25, 2019 at 1:45pm ET Skynet gains sentience, thanks to SocBot's unmonitored work. You have chosen….poorly.

212

When Zack blocked whole subnets yesterday he cut off communication to many suppliers (like your HR and benefits portal) and seemingly random websites. Without proper documentation and review most of this could have been avoided, it just takes a little communication.

You have chosen…poorly.



"Two days in a row," Bert states as you walk into the SOC. He team glowers at you with murder in their eyes…..

321

Play it cool…. "Hey guys. How's it going? Anything fun going on?"

Go to Page 214,214

Be serious… "I know it looks bad, but I think we're close to wrapping this up for good!"

Go to Page 2,215

Lay it all out…. "Well, it's WORSE than we first thought."

Go to Page 612

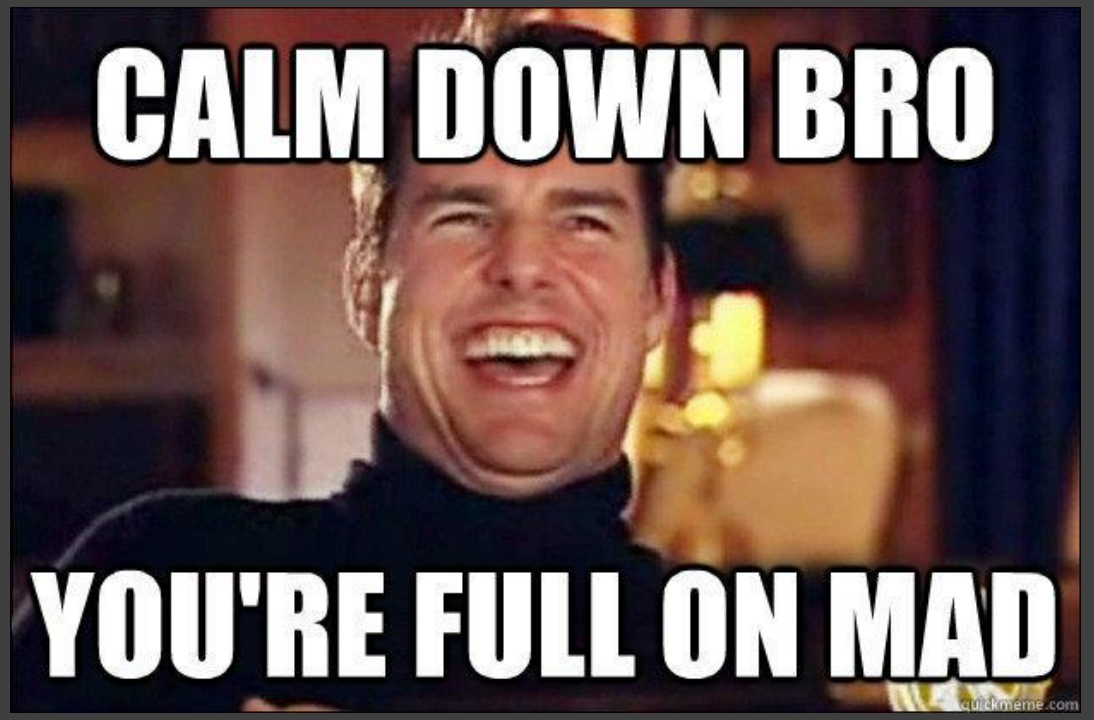
214,214

You try to play it cool. “Hey guys. How’s it going? Anything fun going on?” You used to think joking helped break the ice; you were wrong. DEAD wrong. Bert and the SOC team descend upon you most harshly and you are never seen again.

You have chosen….poorly.

2,215

Be serious… “I know it looks bad, but I think we’re close to wrapping this up for good!”



What’s causing the outage today, do we know?

Go to Page 712

What does our DR/BCP plan say about this type of thing?

Go to Page 812

206

Taking a deep breath, you lay it all out. “Well, it’s WORSE than we first thought…..”

You make a grown man cry as you describe how extensive the problems are and how futile your efforts yesterday were to curb them.

You have chosen….poorly.

You quickly review with the team what steps have been taken so far. The team reviews the output of the SocBot to see what's causing the outage today, and see something different about the outage today.

712

Our outbound traffic is through the roof and has flooded out internet gateway.

Go to Page 185

We've found several packages were overwritten on the webservers starting late sunday night.

Go to Page 181

812

You go find Tushman, your ITIL guy and ask him what does our DR/BCP plan say about this type of thing?

You slowly start failing over the customer's datacenter to new servers. Ideally once those are online you can do a thorough investigation of the compromised ones.

You have chosen….just OK'ly.

022

Obviously what we tried yesterday was not sufficient, we should try something different. Thinking outside the box is your specialty!

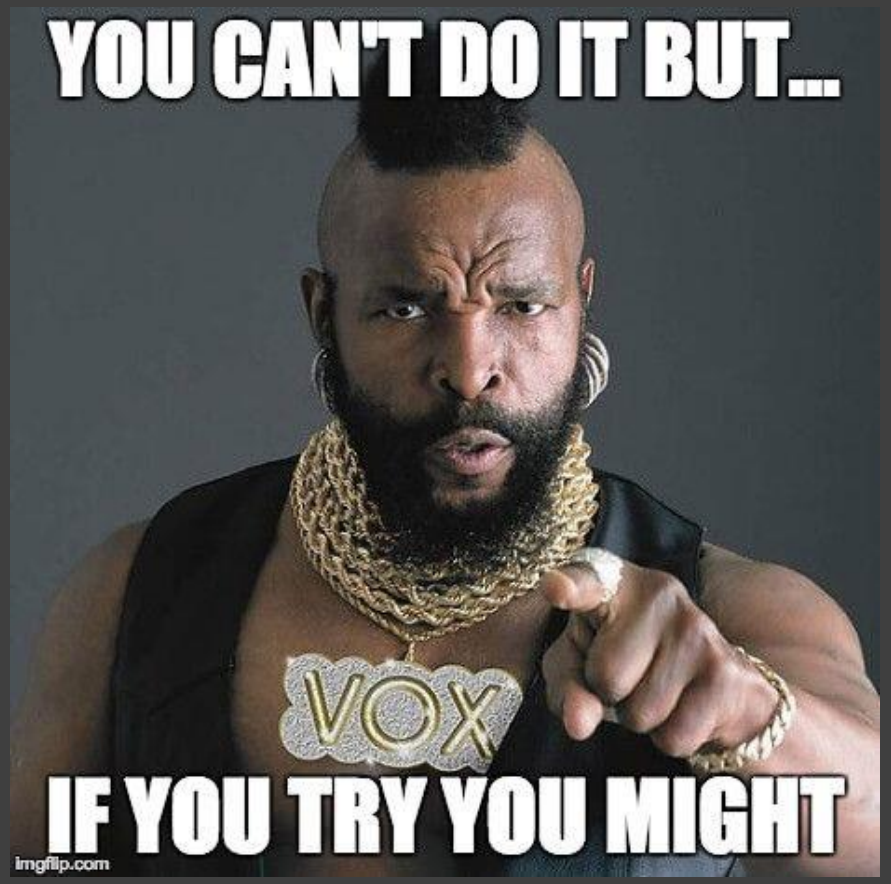
Think outside the box

Go to Page 222

Think REALLY outside the box....

Go to Page 223

221



Trying the same thing that so obviously failed yesterday is not a great way to fix the problem. You get the servers back online at the end of the day, and the NEXT day they go down AGAIN.

The customer seeks other options for their service provider.

[You have chosen….poorly.]

What if we move the customer's servers...BACK INTO THEIR OWN DATACENTER and GET OUT OF THE CLOUD?

Go to Page 209

Implement a fantastic high-security solution: start using paper again

Go to Page 183

Yes! What we need to solve this problem, get the customer's site back online and get this all behind us is some good old-fashion creative thinking!

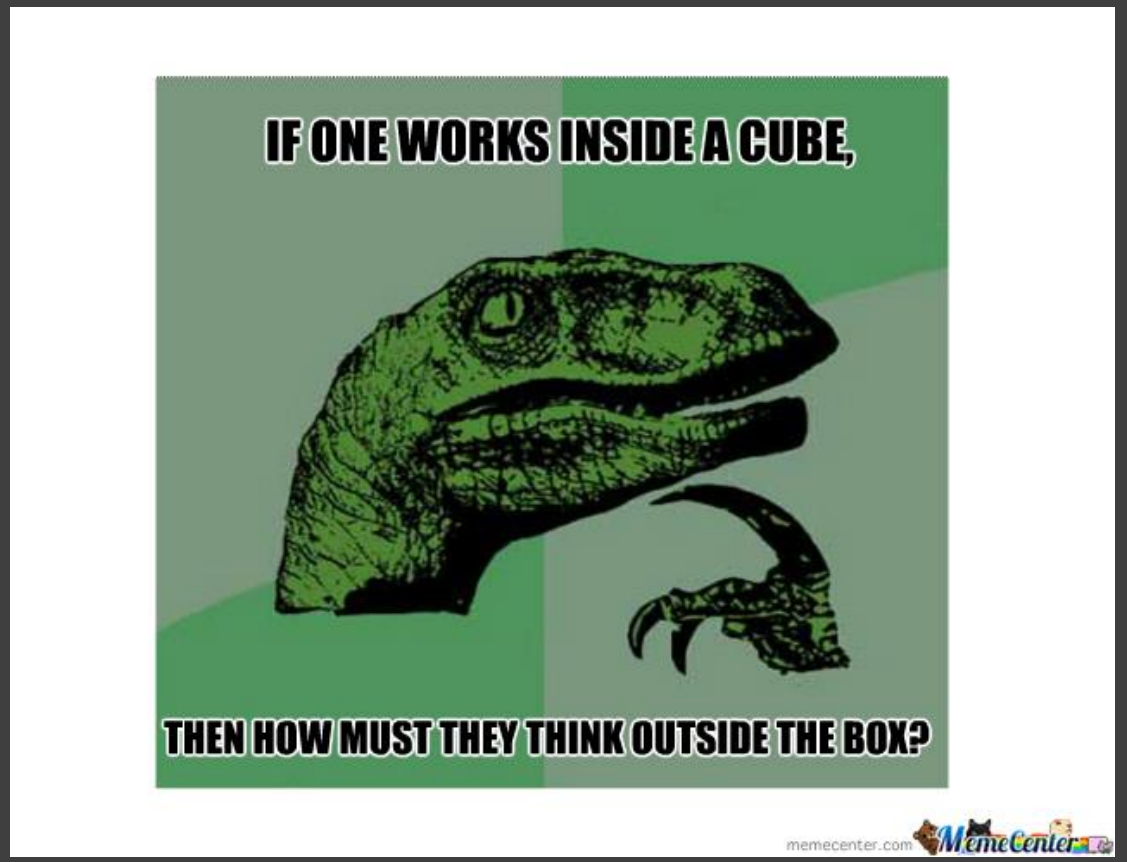
802

210

You know, trying something different is EXACTLY what you do. Life is to short to be so stressed all the time. You walk out of the office, go home and sell all your things. You take the proceeds, move down somewhere warm and sunny and start a business selling beach balls and ice-cold beers to tourists on the beach. Security was the worst.

You...won?

224



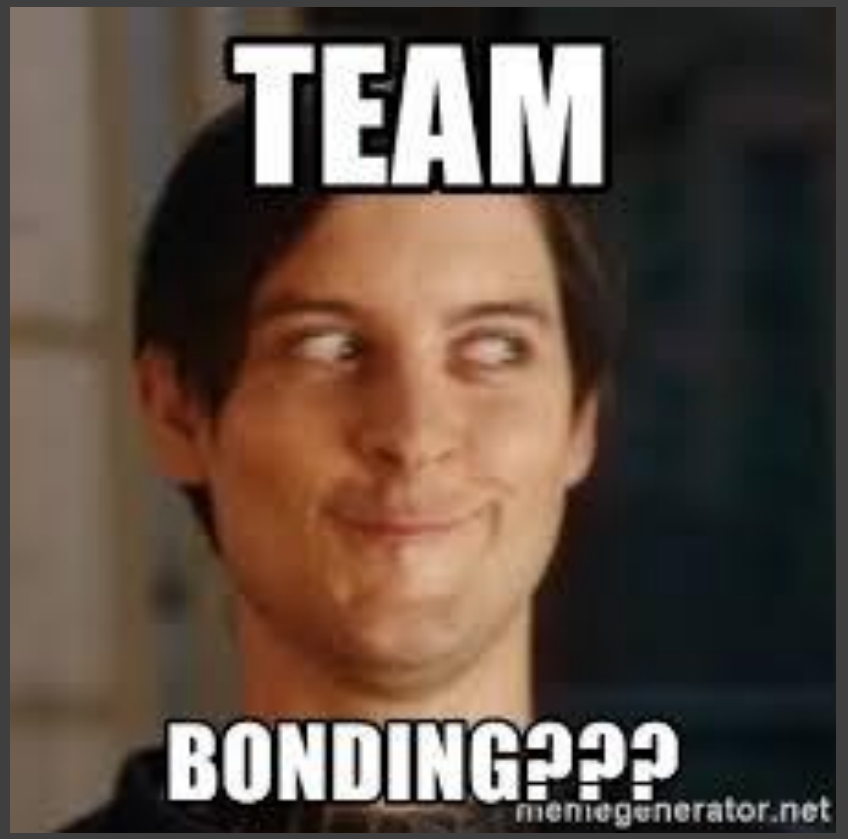
You're "awesome" ideas, while cool and all, don't really help get the customer back online.

The customer seeks other options for their service provider.

You have chosen….poorly….… or DID YOU?

731

What do you think the team would enjoy most to de-stress?



You've been hearing A LOT about these new "Escape Rooms"...maybe you should check one of those out?

Go to Page 228

You see a lot of people scooting around the city on these fancy segway tours, maybe that will help cool everyone down?

Go to Page 227

What could possibly go wrong? Your crack team of securityologists tooling around the city on motorized unicycles?

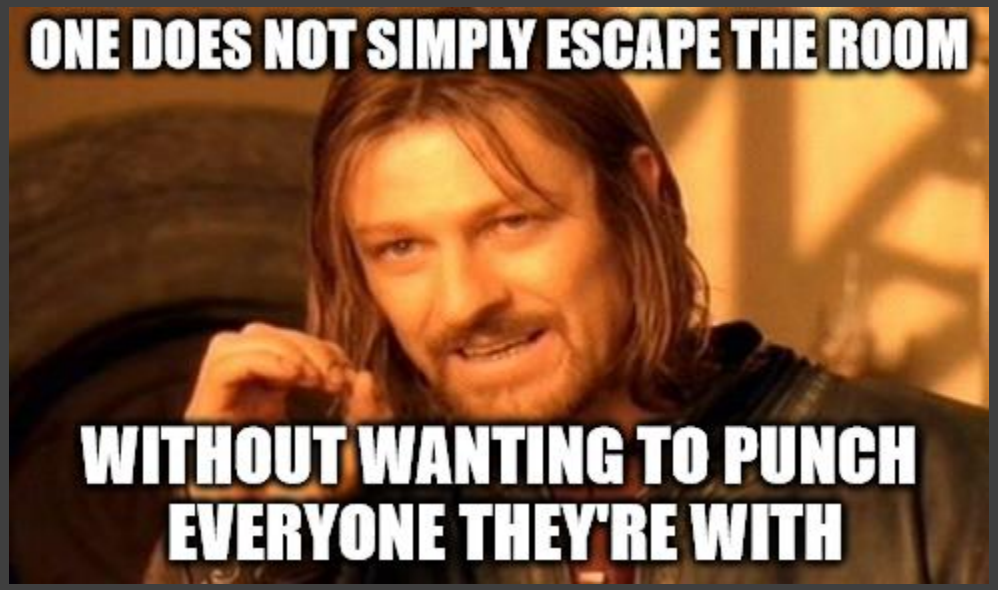
802

Carpe Diem!!!

Go to Page 209

...on second thought, let's go to that Escape Room

Go to Page 183



Escape rooms sound neat! The whole team gets locked in this tiny, tiny room together, and you all get to stare at interesting things in a vain attempt to get out…..

Use the 3 sea shells.

There's some weird screwdriver thing that might be a clue…

There is a jolly, candy-like red button becconing you to push it…..

Go to Page 922

Go to Page 032

Go to Page 132

802

731

What? You don't understand how to use the three sea shells? BWAHAHAHAHAHAHAH! <points>

YOU LOSE.

731

You feel that strange screwdriver thing is your best chance to escape the escape room. You turn it on, it makes a little noise….

you rip a hole the big ball of wibbly-wobbly, timey-wimey stuff.

Your day ends poorly

731

Can he withstand the temptation... to push the button that, even now, beckons him closer? Will he succumb to the maddening urge to eradicate history? At the MERE PUSH of a SINGLE BUTTON! The beautiful shiny button! The jolly candy-like button! Will he hold out, folks? CAN he hold out?

In a word, ….. NO!

History gets eradicated. Your day ends poorly.

28,003

You eagerly hop on the murder-machine and careen off into traffic. You are crushed by a truck deliverying hoverbboards.

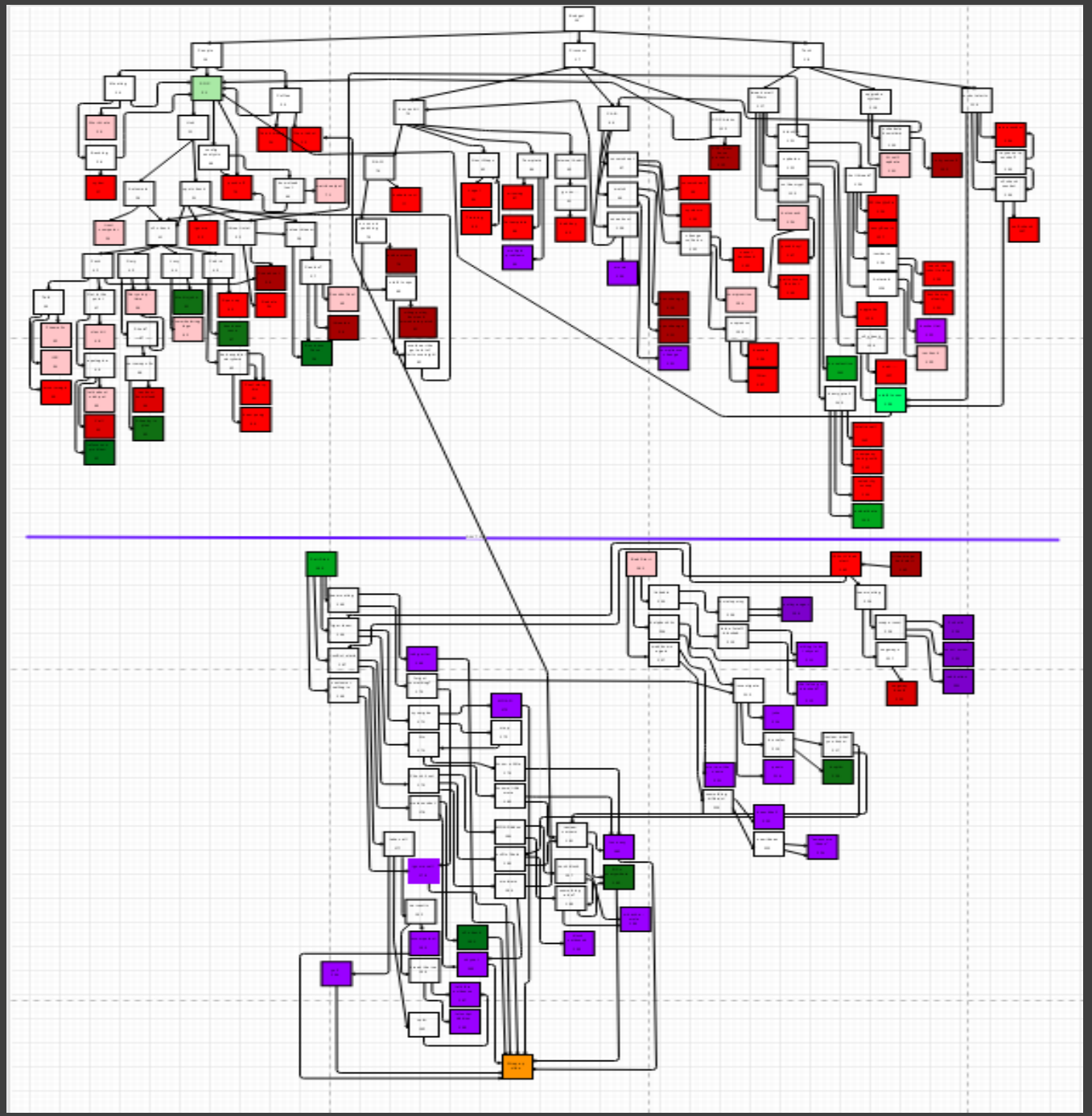
They most likely will be talking about this at the Christmas Party...every year from now on.
#SAD!

THE END

Closing Thoughts….

- People, Process and Technology all play a role when it comes to securing your enterprise.
- Having a dedicated team with appropriate security knowledge is key when confronted with problems.
- Socializing security information and expectations proactively with everyone in the organization will put you in a better position when a crisis does occur.
- Understanding the types of threats that your organization may face (and what it might me more susceptible to) will help in properly preparing for an event.

BACK TO THE BEGINNING

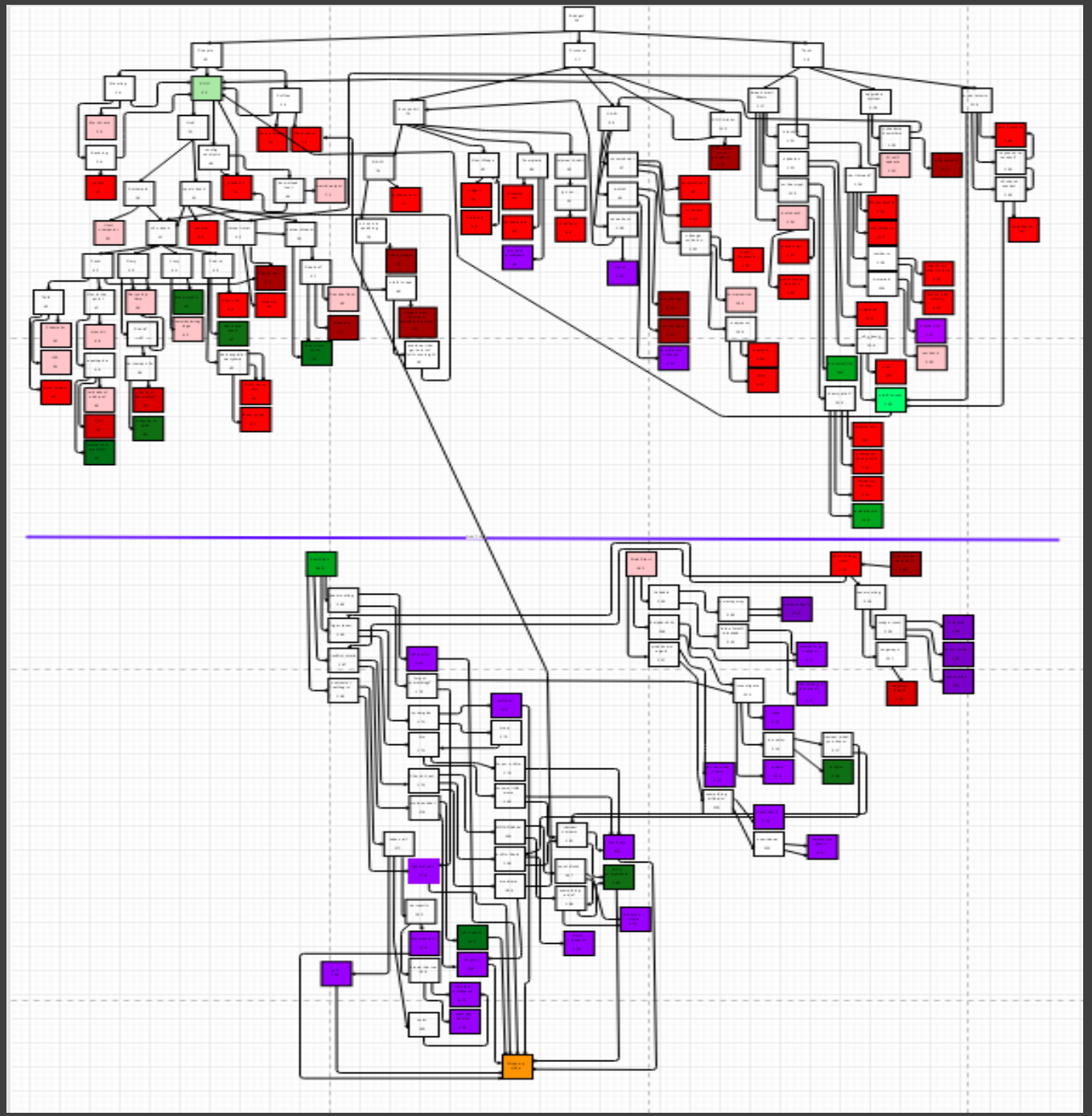



GREAT!
memegenerator.net

Closing Thoughts….

- People, Process and Technology all play a role when it comes to securing your enterprise.
- Having a dedicated team with appropriate security knowledge is key when confronted with problems.
- Socializing security information and expectations proactively with everyone in the organization will put you in a better position when a crisis does occur.
- Understanding the types of threats that your organization may face (and what it might me more susceptible to) will help in properly preparing for an event.

BACK TO THE BEGINNING




GREAT!
memegenerator.net