BSIDESSF PLAYS

INCIDENT RESPONSE

WHITNEY MERRILL
MAYA KACZOROWSKI

APR 26 2025

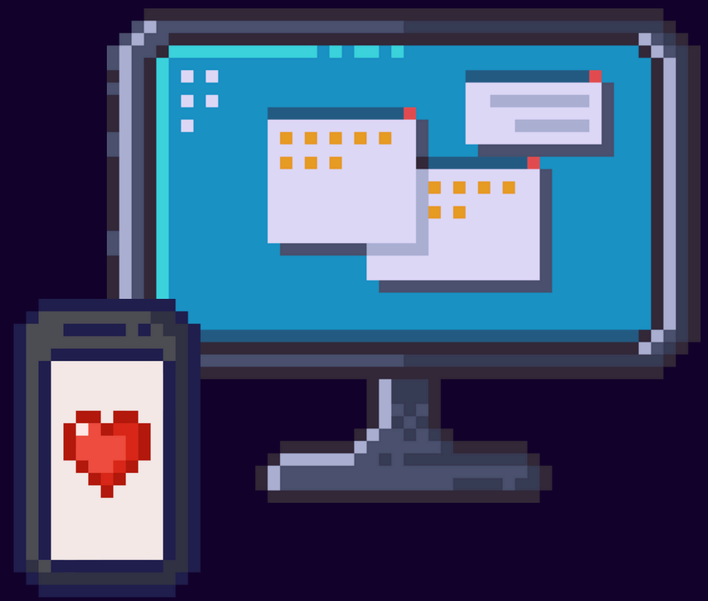
INCIDENT!!!

AAHHHHHHH

HOW THIS WORKS

CANVA.LIVE DO IT LIVE

THERE IS NO HIDDEN AGENDA, AND THERE ARE NO TRICK QUESTIONS. THE RESOURCES AND WRITTEN MATERIALS PROVIDED ARE THE BASIS FOR DISCUSSION



MAYA

WHITNEY

MEET YOUR INCIDENT RESPONSE TEAM

NOT YOUR LAWYER

YOU

WHO ARE YOU?

TL FOR GROWTH

B2B FINTECH HYPERFINANCE

LEVEL 01

INITIAL REPORT & RESPONSE

START


YOU
SIGNUPS ARE DROPPING OFF...
DID YOU PUSH ANY CHANGES TO PRODUCT?
you can do it
THE OFFICE

WHAT DO YOU DO?

ROLL BACK MOST RECENT CHANGE

DIG DEEPER INTO THE DATA, E.G., COHORT ANALYSIS

WAIT AND SEE, MAYBE IT WILL GO AWAY


YOU
OH NO...I ROLLED BACK THE CHANGE, SIGNUPS ARE STILL DROPPING OFF
you can do it


HEY MAYA! WE ARE SEEING AN INCREASE IN TICKETS FROM CUSTOMERS
CUSTOMER SUPPORT


MAYA
I'M GOING TO LOOK AT SOME OF THE REPORTS... PEOPLE ARE COMPLAINING
I CAN'T SIGN UP. WHEN I SCAN MY DRIVER'S LICENSE, IT'S NOT MY NAME AND PHOTO.

CUSTOMER SUPPORT REACHES OUT AGAIN

REACH OUT TO THE VENDOR WHO PROVIDES THE SERVICE

IMMEDIATELY SHUT DOWN THE SERVICE AND REVERT TO ONLY MANUAL VERIFICATION. BUT GROWTH!

REACH OUT TO YOUR FRIEND ON SECURITY AND LET THEM KNOW YOU'RE SEEING SOMETHING WEIRD.

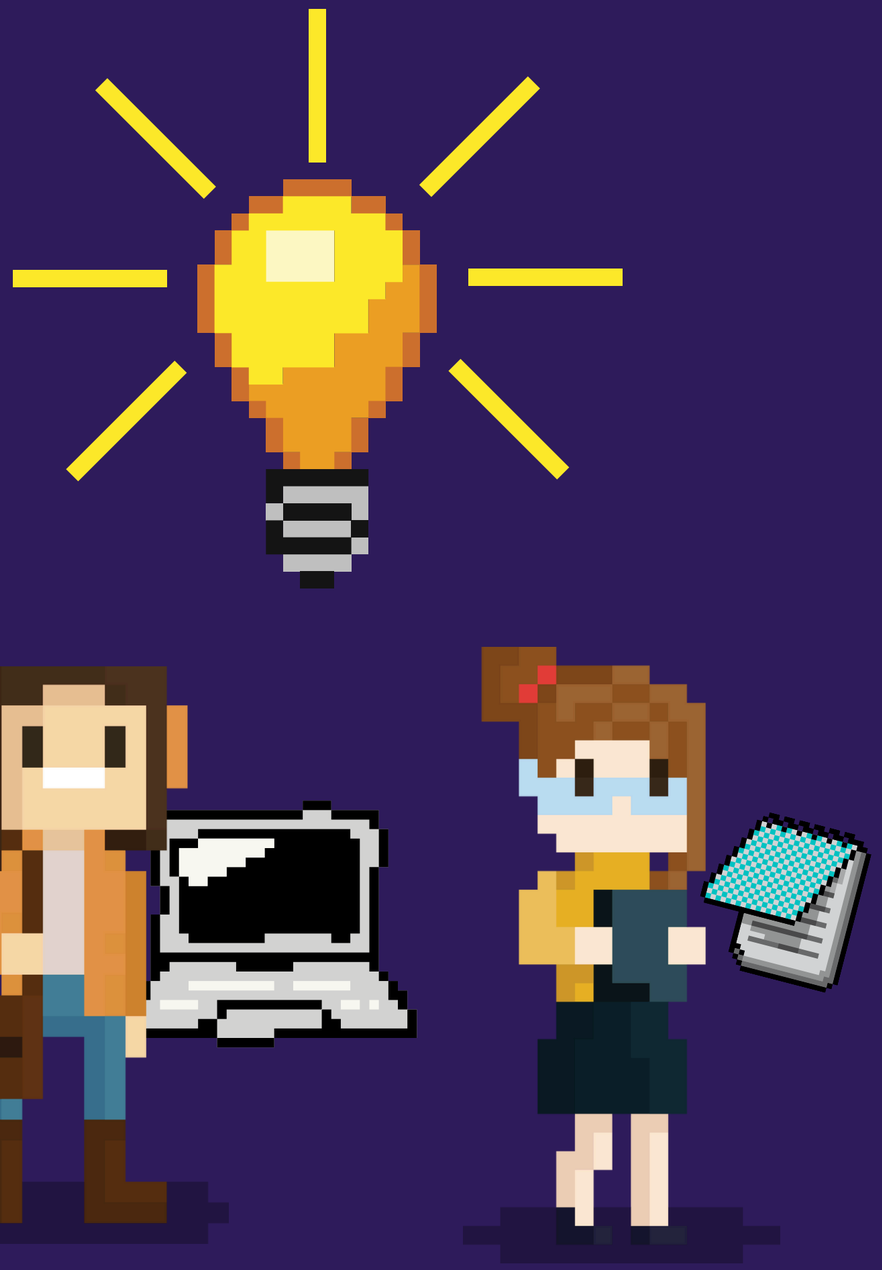

MAYA
I HAVEN'T HEARD BACK FROM THE VENDOR, IT'S BEEN 4 HOURS!
I'LL START POKING INTO THE LOGS TO SEE WHAT'S GOING ON


DEAR
CUSTOMER,
WE ARE
INVESTIGATING
PS.
RENEWAL...
THE VENDOR

VENDOR REACHES OUT. WHAT DO YOU WANT TO DO?

- WAIT UNTIL MONDAY MORNING UNTIL YOU CAN TALK TO THE BILLING OWNER.
- EMAIL THE VENDOR BACK
- DECLARE AN INCIDENT?
- (IF YOU HAVEN'T YET) SHUT DOWN THE SERVICE


MAYA
INCIDENT!



NOTES

- HAVE A SINGLE PLACE FOR TRIAGE
- ANYONE CAN DECLARE AN INCIDENT

LEVEL 02

INVESTIGATION & CONTAINMENT

YOU'RE THE INCIDENT COMMANDER NOW

LOOK AT ME

I'M THE CAPTAIN NOW


1up


DEAR
CUSTOMER,
WE ARE
COMPROMISED!
PS.
RENEWAL...
THE VENDOR


MAYA
I'VE INVESTIGATED.
I CAN REPRODUCE THE BUG!

MAYA

YOU'RE ABLE TO REPRO THE BUG... DO YOU?

- LOOP IN COUNSEL
- (IF YOU HAEN'T YET) SHUT DOWN THE SERVICE
- TELL AN ENG TO GO LOOK AT LOGS
- EMAIL THE VENDOR BACK ASKING WHEN IT WILL BE FIXED


SOMETHING WRONG?
CALL ANH PHOONG
ACCIDENT & INJURY LAWYERS PHOONG LAW
866-GOT-PAIN


MAYA
THE WAR ROOM
WHITNEY
A/C PRIV
HEY WHITNEY, ARE THERE ANY POTENTIAL LEGAL RISKS?
A/C PRIV
POTENTIALLY! LOOP ME INTO EVERYTHING, AND IF YOU NEED TO LOOP SOMEONE ELSE IN LMK.
you can do it
THE OFFICE

OK SO WE
AGREED TO:

1. LOOP IN COUNSEL

2. CHECK THE LOGS

3. EMAIL VENDOR

MAYA

TO: MAYA@
FROM: WHITNEY
ATTORNEY-CLIENT PRIVILEGED - CONFIDENTIAL

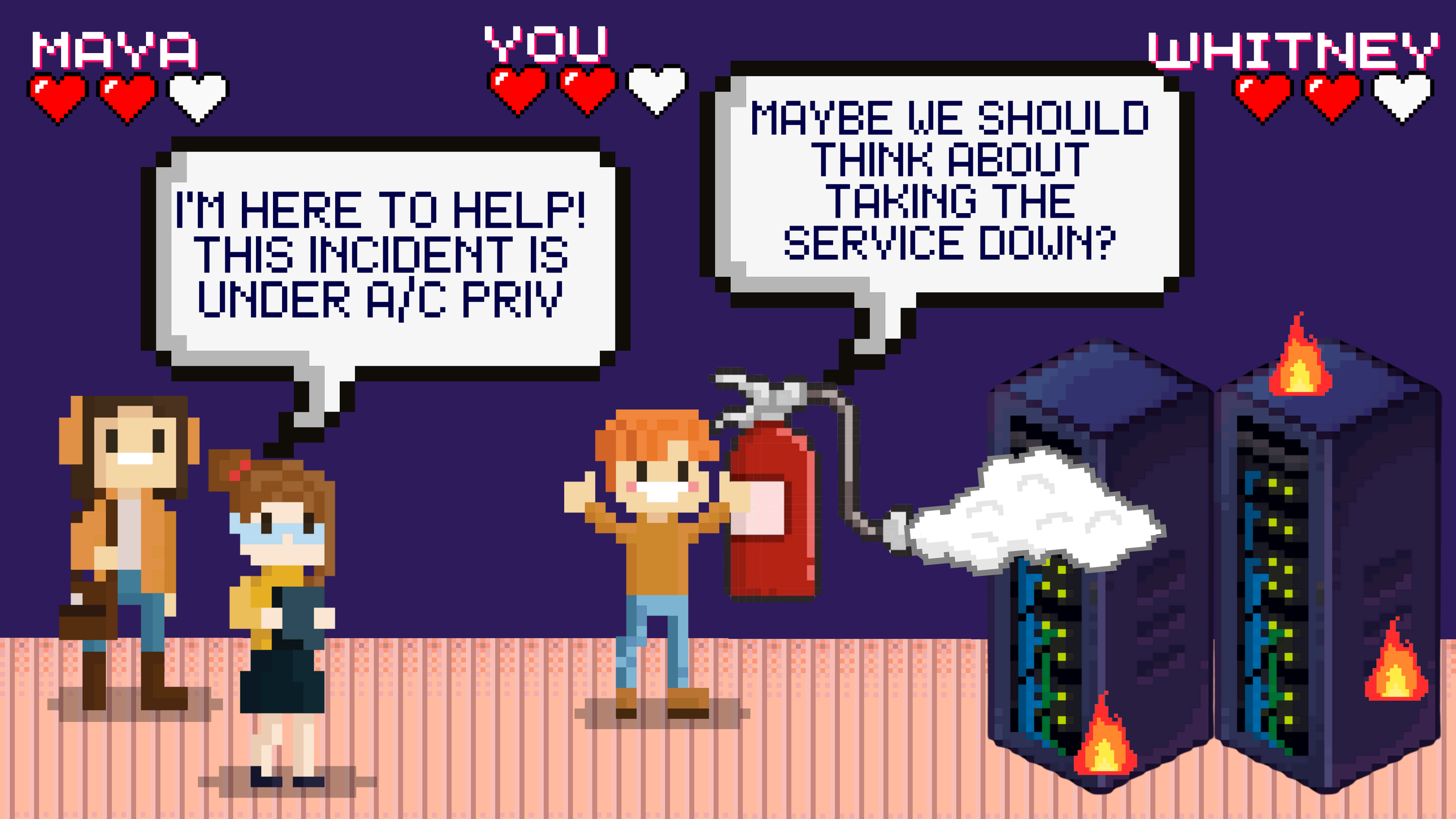
HOW MANY PEO

WHERE ARE TH

TIMELINE NEED
BEEN HAPPENI

AND WAS THE ACCESS TO DATA TEMPORARY OR CONTINUED?

PLEASE LET ME KNOW YOUR FINDINGS - YOURS IN LAW, WHITNEY


MAYA
YOU
WHITNEY
I'M HERE TO HELP! THIS INCIDENT IS UNDER A/C PRIV
MAYBE WE SHOULD THINK ABOUT TAKING THE SERVICE DOWN?


MAYA
YOU
WHITNEY
DON'T FORGET IT'S END OF QUARTER!
WHITNEY, WE SHOULD SHUT THIS DOWN!

MAYA

YOU

WHITNEY

YOU WANT TO SHUT DOWN THE SERVICE, DO YOU...

- MAKE THE DECISION YOURSELF
- MAKE THE DECISION WITH COUNSEL
- REACH OUT TO YOUR BOSS
- SET UP A MEETING WITH RELEVANT EXECS AND STAKEHOLDERS TO BRIEF AND MAKE A DECISION.

DECISIONS: DEPENDS ON COMPANY CULTURE

I. RACI/RAPID
II. TRUST YOUR GUT
III. EASILY REVERSIBLE VS. NOT
IV. RUN TABLETOPS
V. PLAYBOOKS & DOCS


WE ARE SEEING WAY MORE TICKETS — IT SOUNDS LIKE NO ONE CAN SIGN UP?
CUSTOMER SUPPORT
ANY COMMENT?
WE GO TO PRESS IN ONE HOUR
REPORTER

HOW DO YOU COMMUNICATE INTERNALLY?

POST IN #GENERAL

DRAFT COMMS FOR YOUR EXEC TO SHARE WITH OTHER EXECS

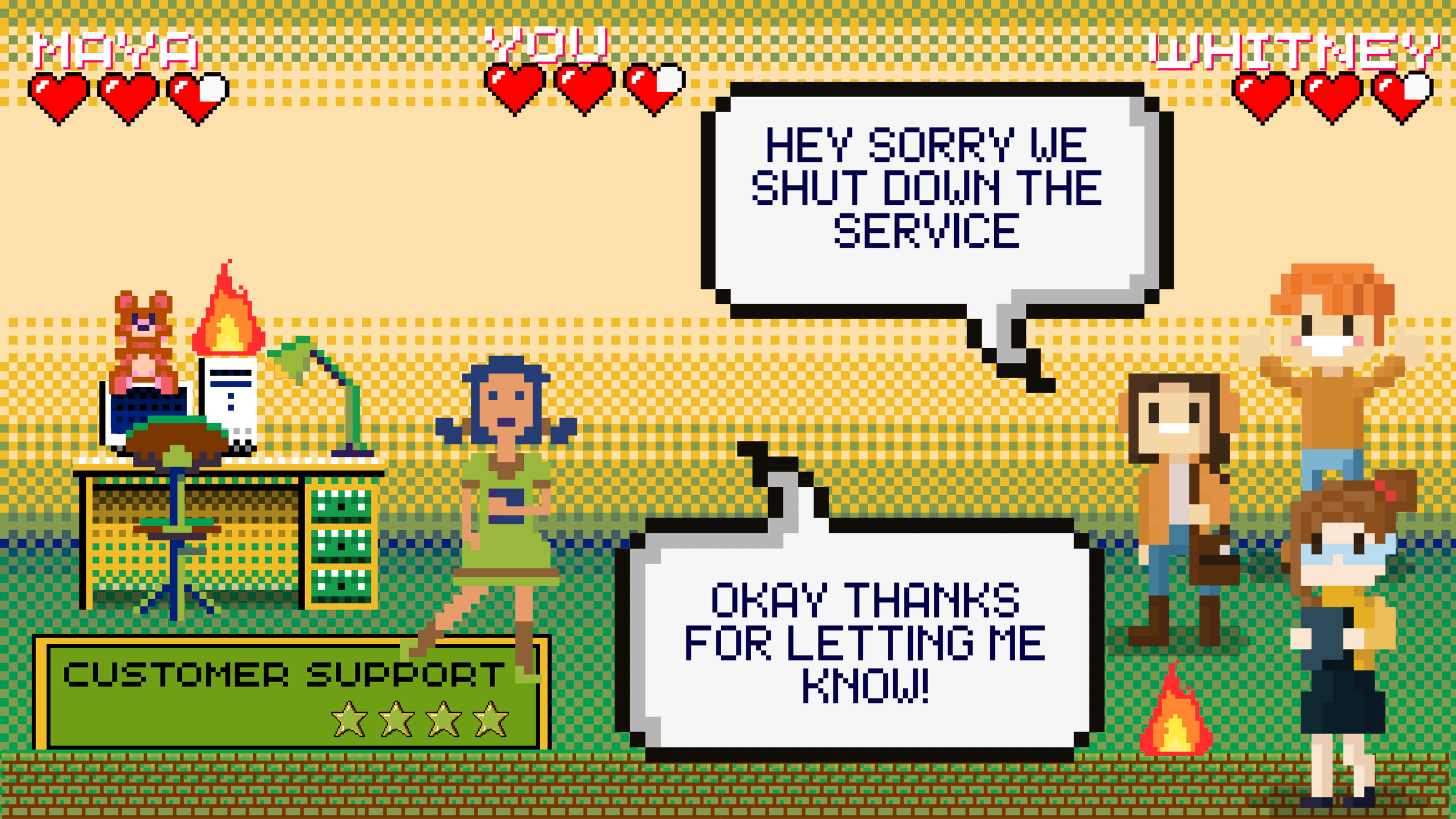
WRITE AN UPDATE TO A SHORTLIST OF LOOPED-IN USERS

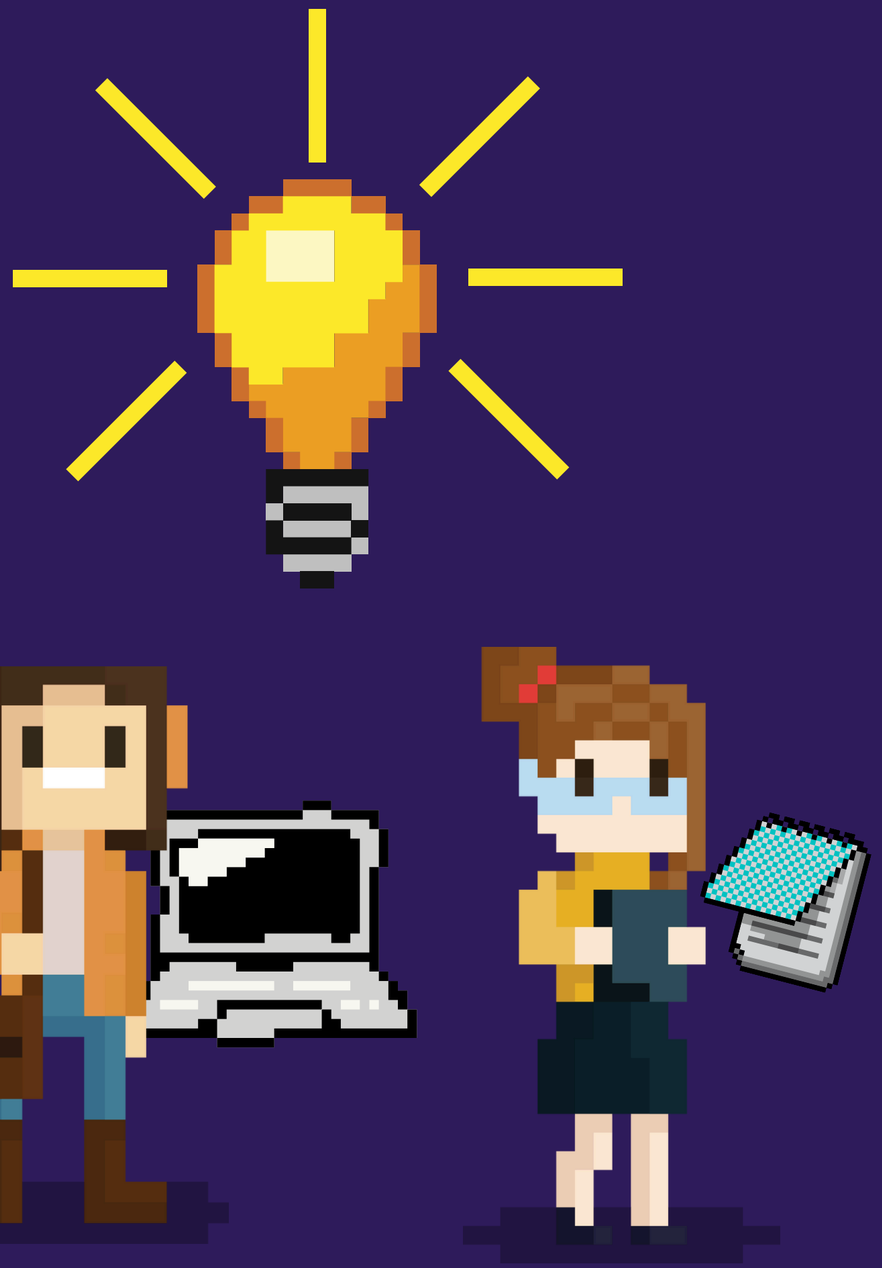
DON'T DO ANYTHING (SSHHHHHH!)

MAYA

YOU

WHITNEY





NOTES

- DELEGATE
- COMMUNICATE WITH CARE
- COMMUNICATE REGULARLY

LEVEL 03

ERADICATION & RECOVERY

SERVICE IS SHUT DOWN

SYSTEM ERROR !

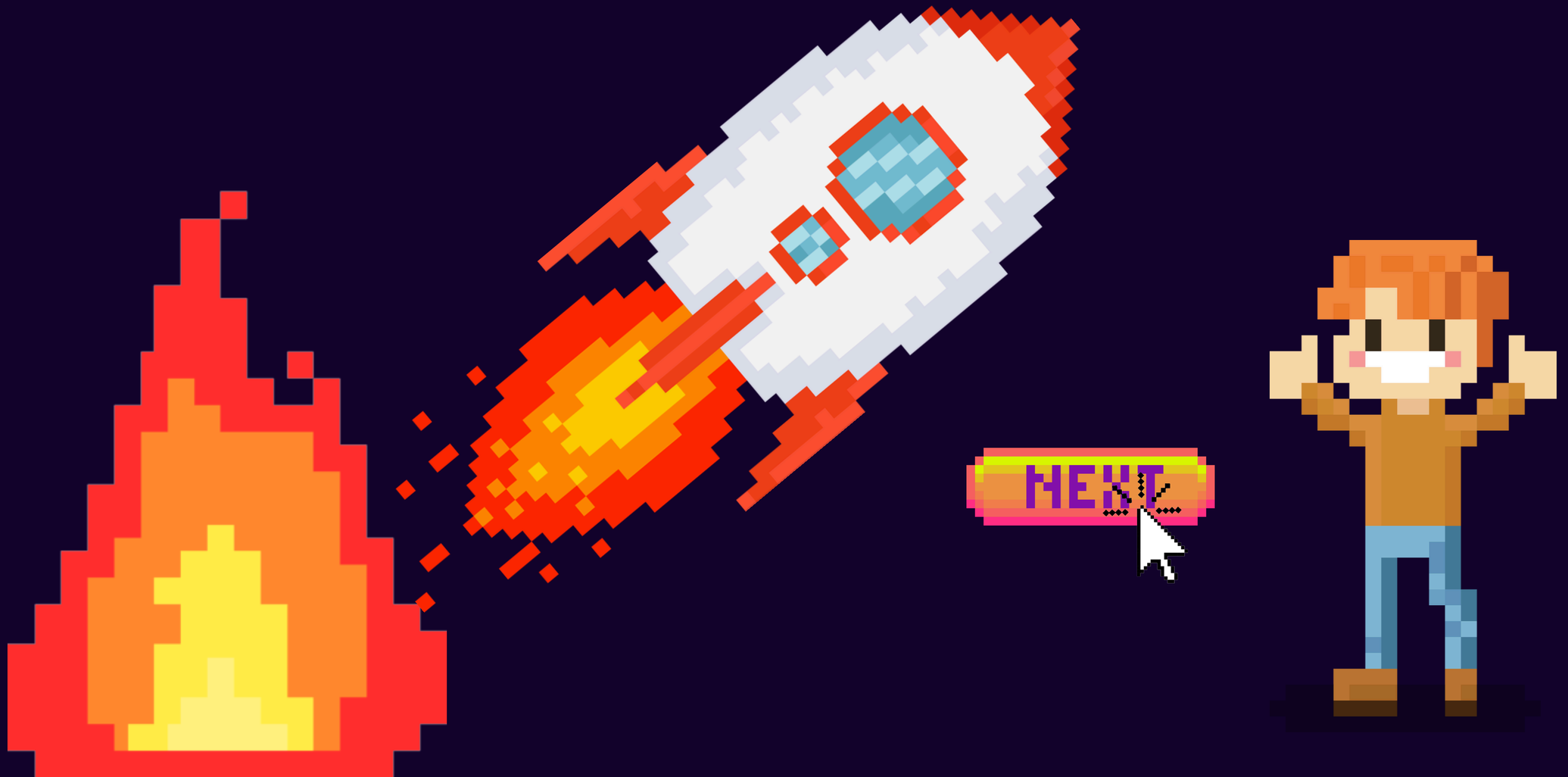
OK NO

WHAT DO YOU DO?

- REREAD YOUR VENDOR CONTRACT
- LOOK INTO ALTERNATIVE VENDORS
- LOOK INTO BUILDING YOUR OWN SOLUTION
- WAIT ON THE VENDOR


YOU
YAY FINALLY
WE FOUND THE ISSUE, AND WE HAVE A FIX!

FIX IS COMING IN HOT



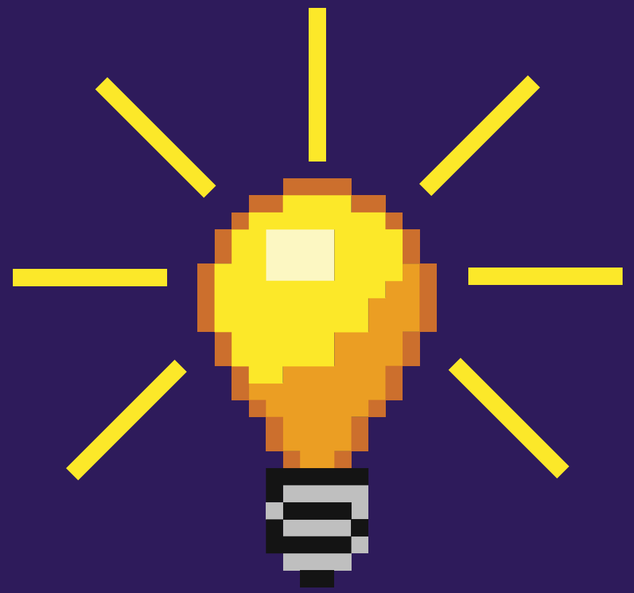
WHAT DO YOU SAY?

NOTHING

CONFER WITH COUNSEL ON OBLIGATIONS

COMMUNICATE EVEN IF NOT REQUIRED TO


YOU
FIX IS COMING IN HOT
HEY EVERYONE, WE'RE ROLLING OUT A FIX
NEXT

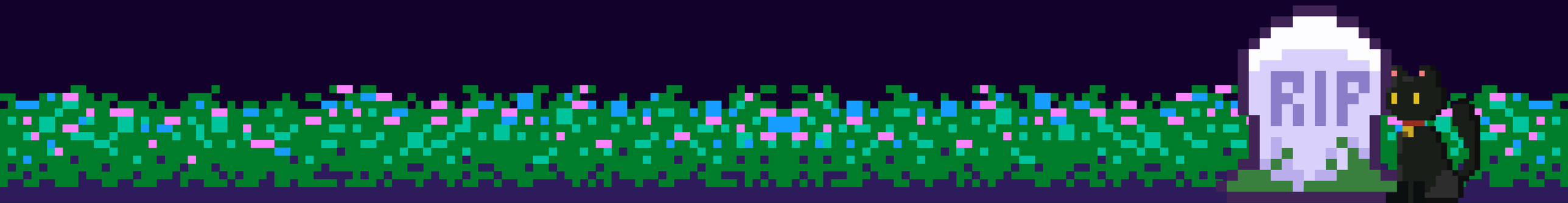


NOTES

- PLAN FOR RESILIENCY
- LOOP IN COUNSEL
- RESPECT REPORTING TIMELINES

LEVEL 04

POST-MORTEM



POST-MORTEM

WHAT WENT WELL?

WHAT WENT POORLY?

NEW HIGH SCORE

TAKEAWAYS

BE VIGILANT

PREPARE

COMMUNICATE

WORK WITH COUNSEL

INCIDENT RESPONSE IS EVERYONE'S RESPONSIBILITY

HELPFUL RESOURCES

INCIDENT RESPONSE POLICIES

https://github.com/securitytemplates/sectemplates/tree/main/incident-response/v1
https://github.com/tailscale/security-policies/blob/main/incident-response-process/index.md

NO STARCH PRESS: "CYBERSECURITY TABLETOP EXERCISES"

CISA TABLETOP EXAMPLES

THESE SLIDES: BSIDESSF2025.MY.CANVA.SITE


THANK YOU
NEW GAME