AUTOMATED HUMAN VULNERABILLITY SCANNING WITH AVA

LAURA BELL

Founder and Lead Consultant - SafeStack

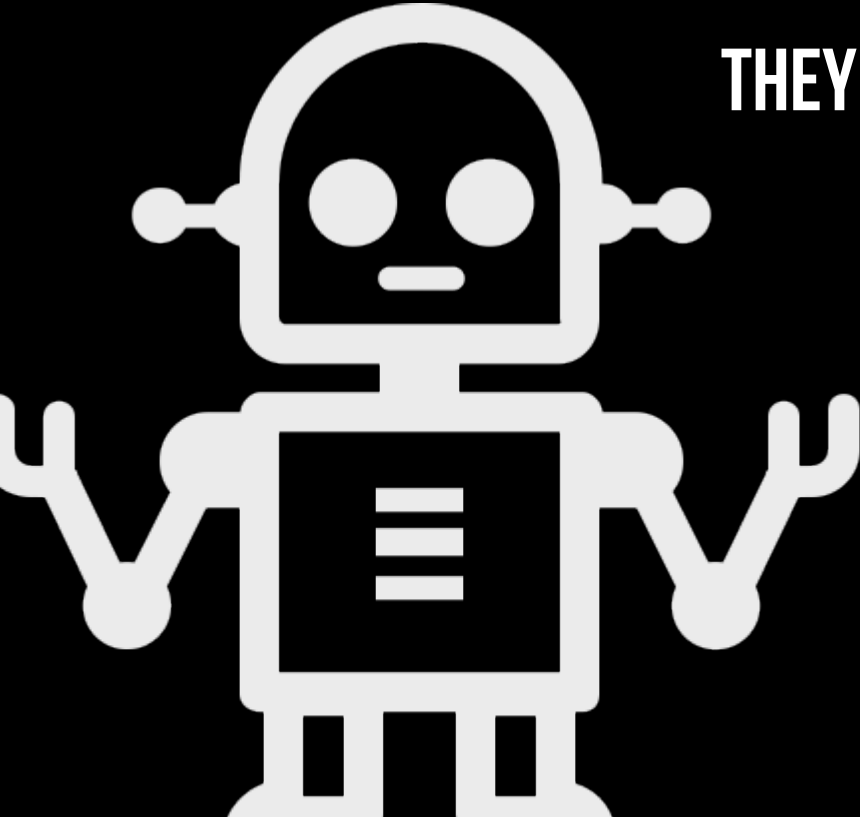@lady_nerd   laura@safestack.io
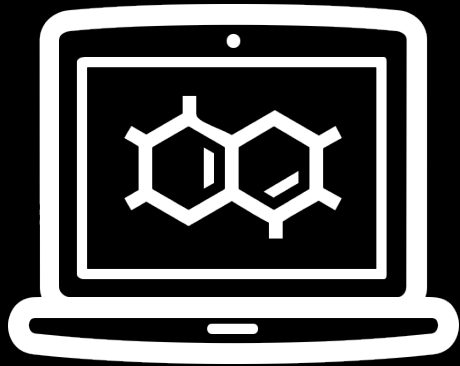
http://safestack.io

#protectyourpeople

WE ARE COMFORTABLE WHEN WE TALK ABOUT TECHNICAL VULNERABILITY

WE DO NOT EMPATHISE OR SYMPATHISE WITH MACHINES
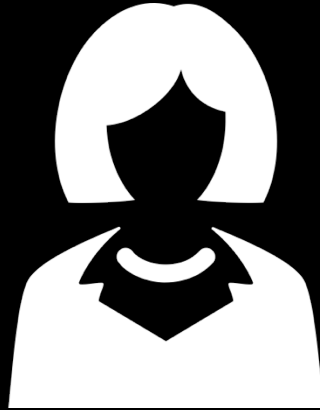
THEY ARE TANGIBLE, INANIMATE OBJECTS.

TECHNOLOGY IS ONLY PART OF THE SECURITY PICTURE

TECHNOLOGY   PEOPLE   PROCESS

TECHNICAL SYSTEMS ARE:

REVIEWED

SCANNED

PENETRATION TESTED

PROCESSES ARE AUDITED

WHAT ABOUT PEOPLE?

IN THIS TALK

1. WHY IS HUMAN-CENTRIC SECURITY SO COMPLEX?

2. ARE THE CURRENT SOLUTIONS EFFECTIVE?

3. A FUTURE FILLED WITH HOPE AND SCARY QUESTIONS?

THE PROBLEM WITH PEOPLE

HUMAN VULNERABILITY IS NATURAL

HUMANS ARE SUFFICIENTLY PREDICTABLE TO MAKE IT SUITABLY ANNOYING WHEN WE FAIL TO PREDICT THEIR BEHAVIOUR.

MODERN APPROACHES

BORDER DEVICES ARE NOT ENOUGH

SECURITY AWARENESS EDUCATION REALLY SUCKS

POSTERS DON'T WORK

STOP IT ALREADY.

Treat your password like your toothbrush...

Don't share it with others!

Change it often!

SLAC
NATIONAL ACCELERATOR LABORATORY

COMPUTER SECURITY

COMPLIANCE HAS US RACING TO THE BOTTOM

RED TEAMING AND
SOCIAL ENGINEERING PENETRATION TESTS

OUTSOURCED PHISHING PROGRAMMES

THE 3 R's OF HABIT FORMATION

1 REMINDER

The cue or trigger that starts the habit.
(Example: Traffic light turns green.)

ROUTINE 2

The action you take. The habit itself.
(Example: You drive through the intersection.)

REWARD

If the reward is positive, then you'll have a desire to repeat the action the next time a reminder pops up. Eventually, this repeitition will form a new habit.

3 The benefit you gain from doing the habit.
(Example: You get closer to your destination.)

LIMITATIONS

1. TARGET CONNECTIVITY IGNORED
2. TEACHING OUTSIDE OF THE WORK ENVIRONMENT
3. LACK OF REINFORCEMENT TO BUILD HABIT AND BEHAVIOURS
4. LACK OF MEASUREMENT
5. LACK OF CONTEXT

AVA
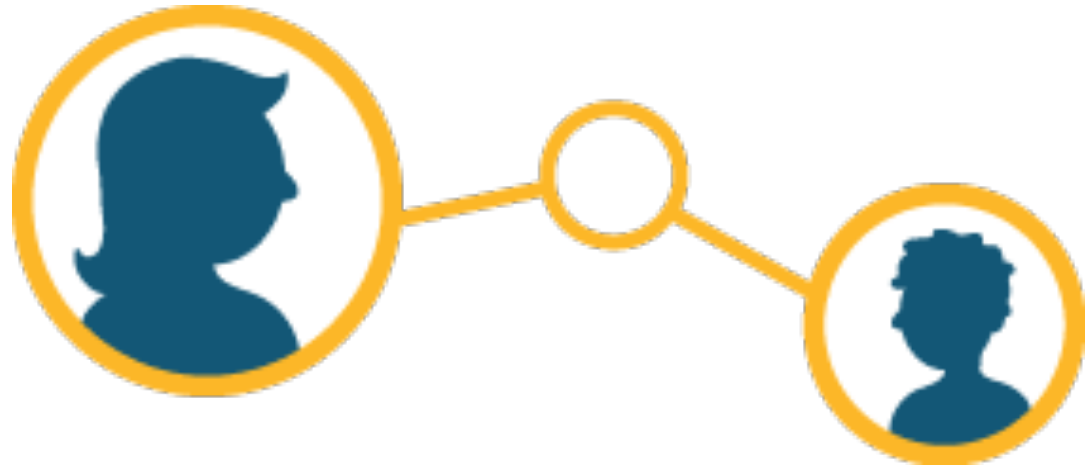# FIRST GENERATION
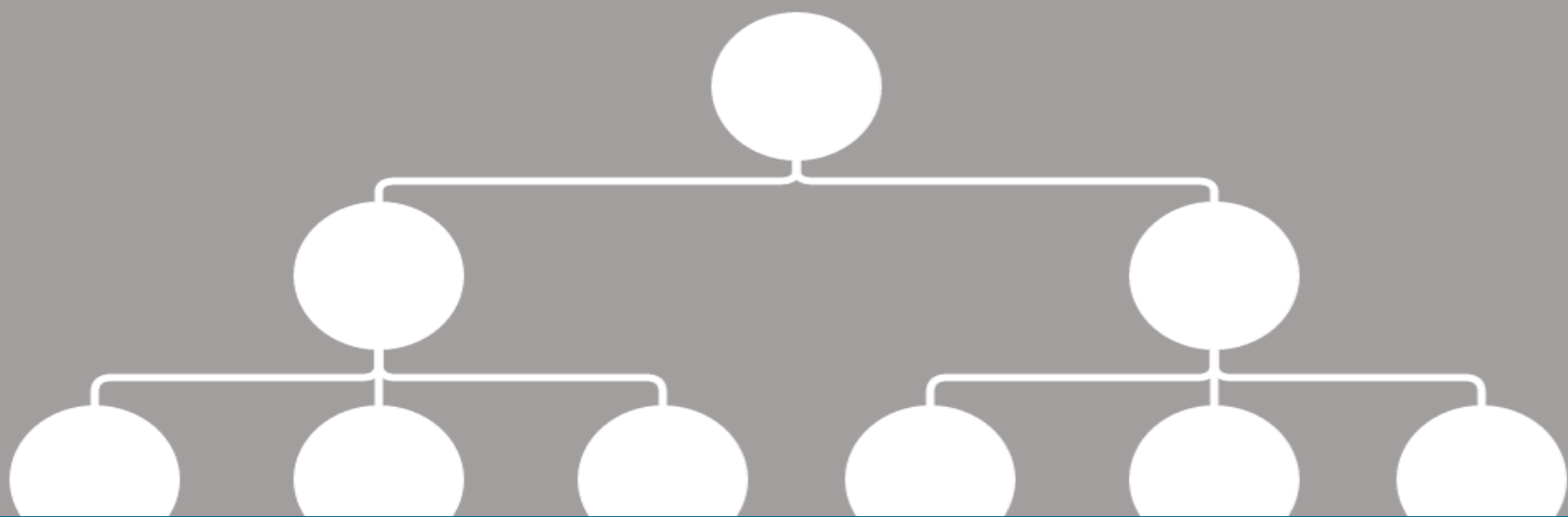# PROOF OF CONCEPT
3- PHASE
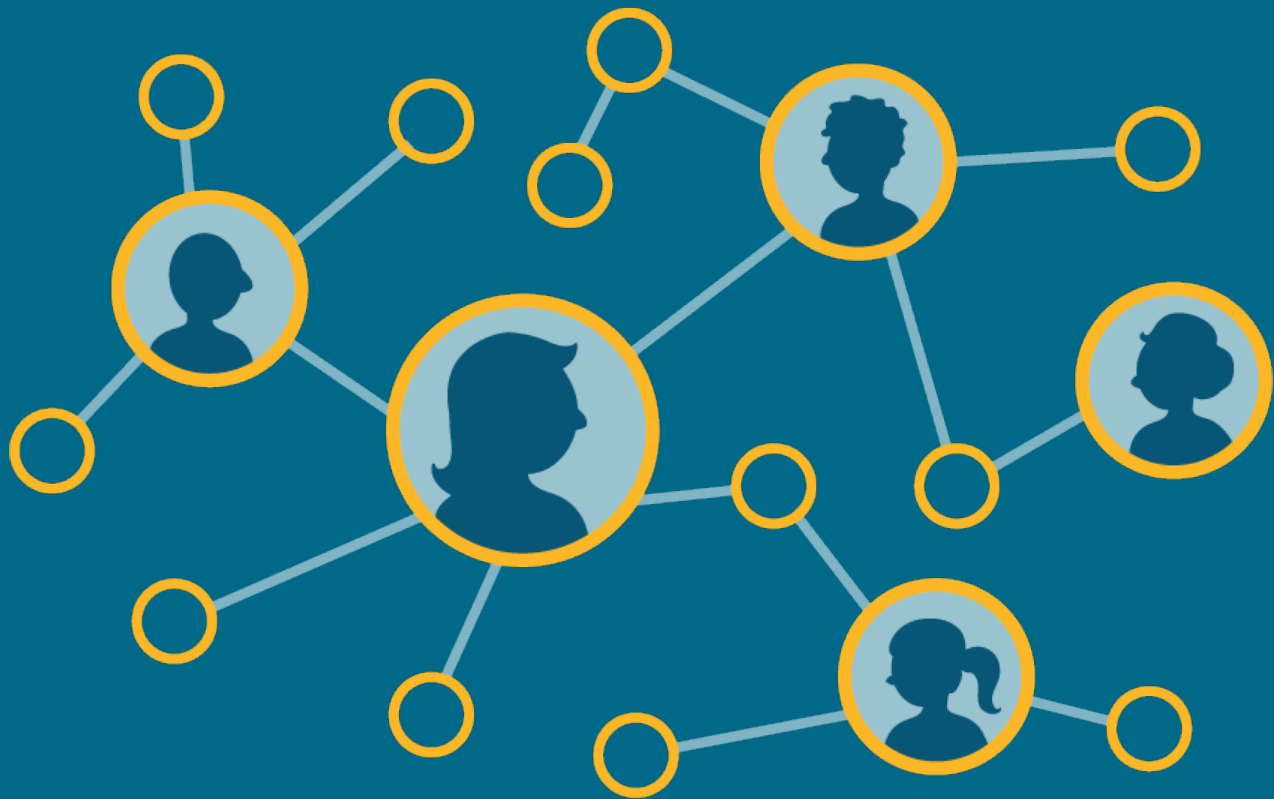# AUTOMATED
HUMAN VULNERABILITY
SCANNER

PHASE 1
KNOW

WE DON'T KNOW WHAT OUR ORGANISATIONS LOOK LIKE

HUMAN SECURITY RISK IS MAGNIFIED BY CONNECTION

ACTIVE DIRECTORY
TWITTER
LINKEDIN
FACEBOOK
EMAIL PROVIDERS

→

PEOPLE
IDENTIFIERS
GROUPS
RELATIONSHIPS
DATA

FRIENDS
LAST LOGIN
LOCATION

CONTACTS
PW EXPIRES?
TIME STAMPS

FREQUENCY
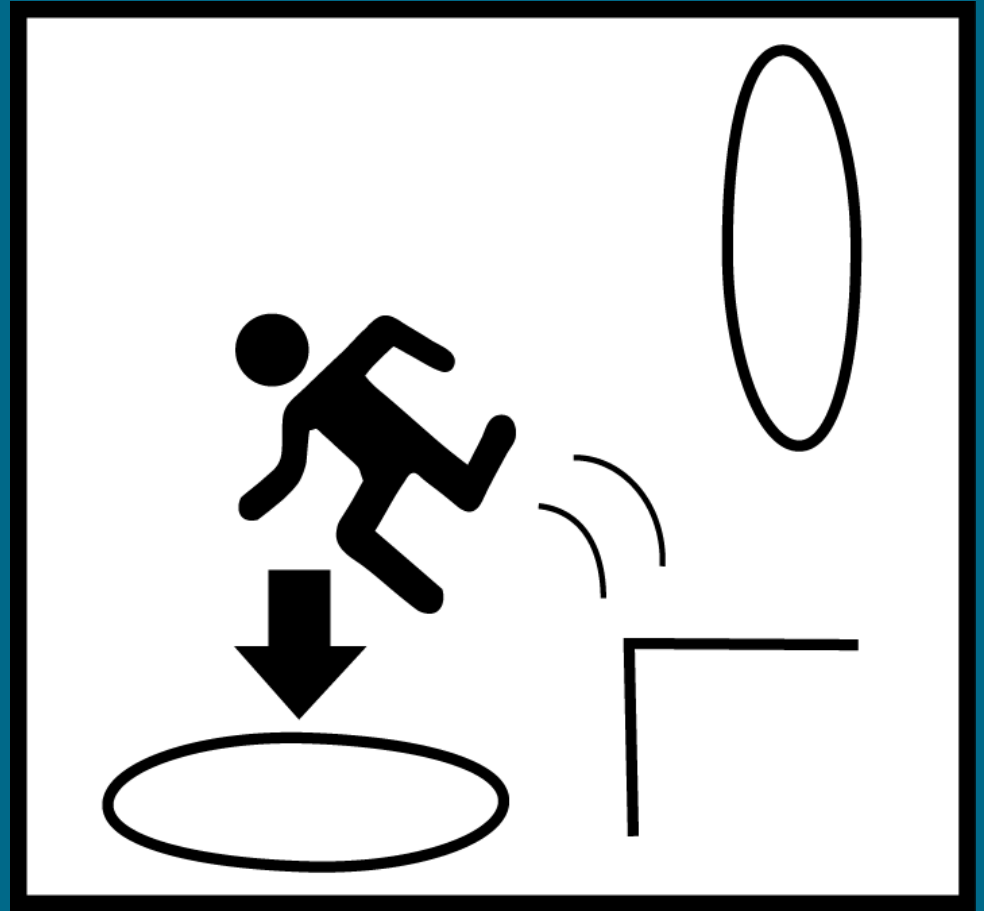DISABLED?
SENDER

ALIASES
INFLUENCE
RECEIVER

PROFILES
ADMIN?
USER AGENT

PHASE 2
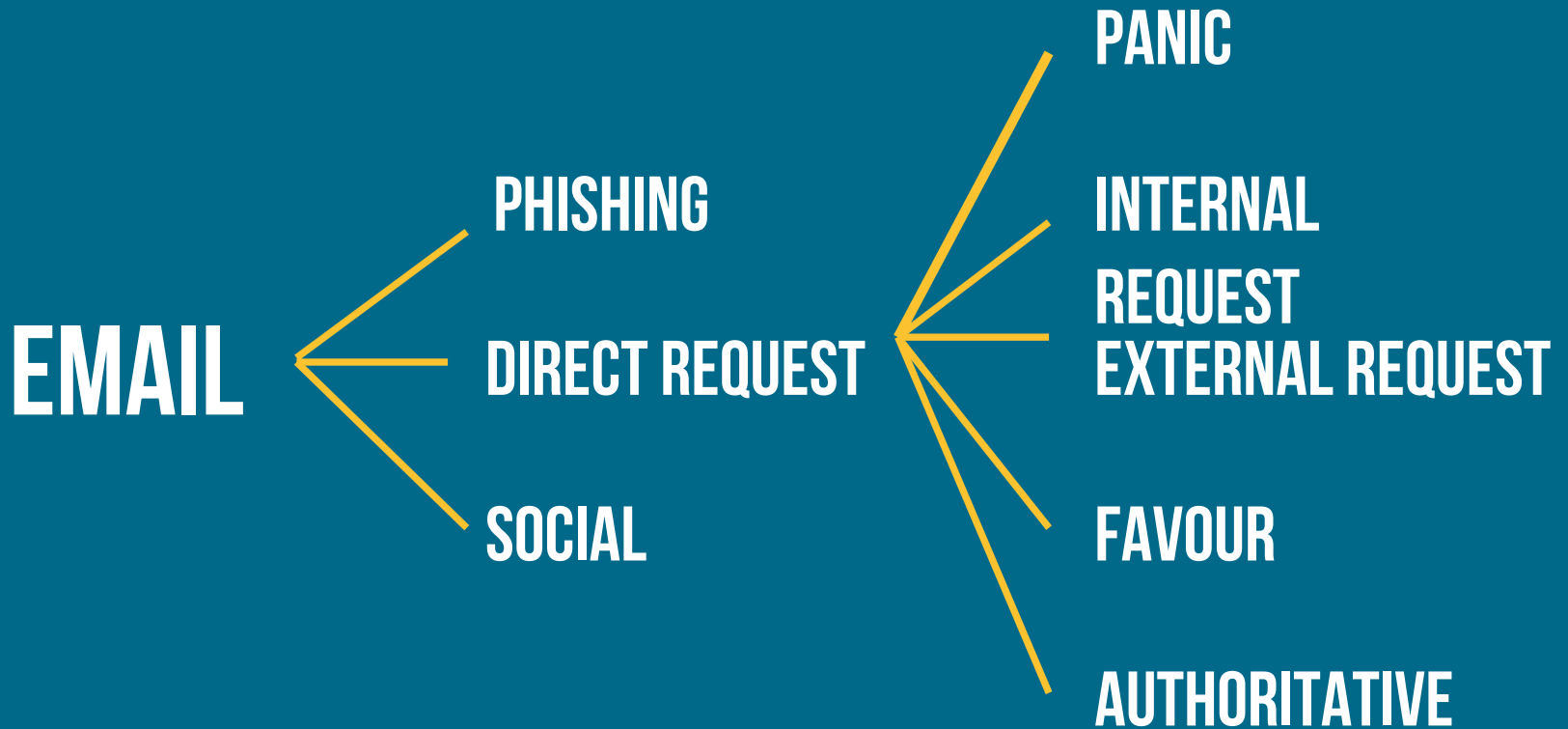TEST

THREAT INJECTION AND BEHAVIOUR MONITORING

EMAIL

SOCIAL NETWORKS

REMOVABLE MEDIA

FILES AND HONEYPOTS

SMS

ATTACK VECTORS THAT MEAN SOMETHING

EMAIL

PHISHING

DIRECT REQUEST

SOCIAL

PANIC

INTERNAL REQUEST

EXTERNAL REQUEST

FAVOUR

AUTHORITATIVE

EMAIL ATTACKS THAT GO **BEYOND** PHISHING

The URL may be different on different messages.
Subject: Security Alert: Update Java (*See Kronos Note)
Date: February 22, 2013

If you require assistance, please contact the Help Center.
****
****

Oracle has released an update for Java that fixes 50 security holes, including a
critical hole currently being exploited in the wild.
The IT Security Office strongly recommends that you update Java as

REMOVING THE **BOUNDARIES** BETWEEN BUSINESS AND PERSONAL

SECURITY **FAILS** WHEN IT IS TREATED LIKE A SPECIAL EVENT

INSTANT, SCHEDULED AND RECURRING

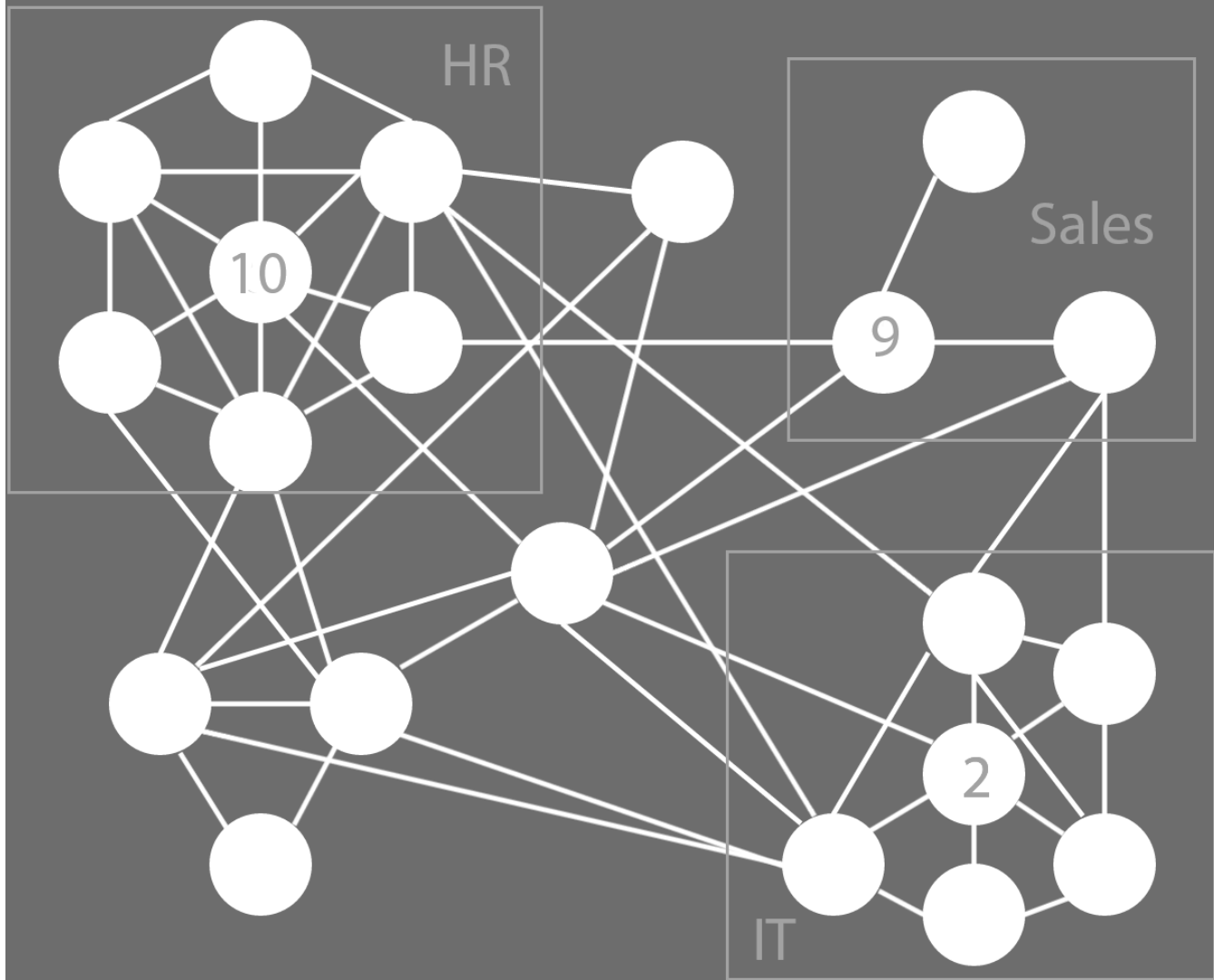GIVE THE OPTION OF SUCCEEDING AND REINFORCE GOOD BEHAVIOURS
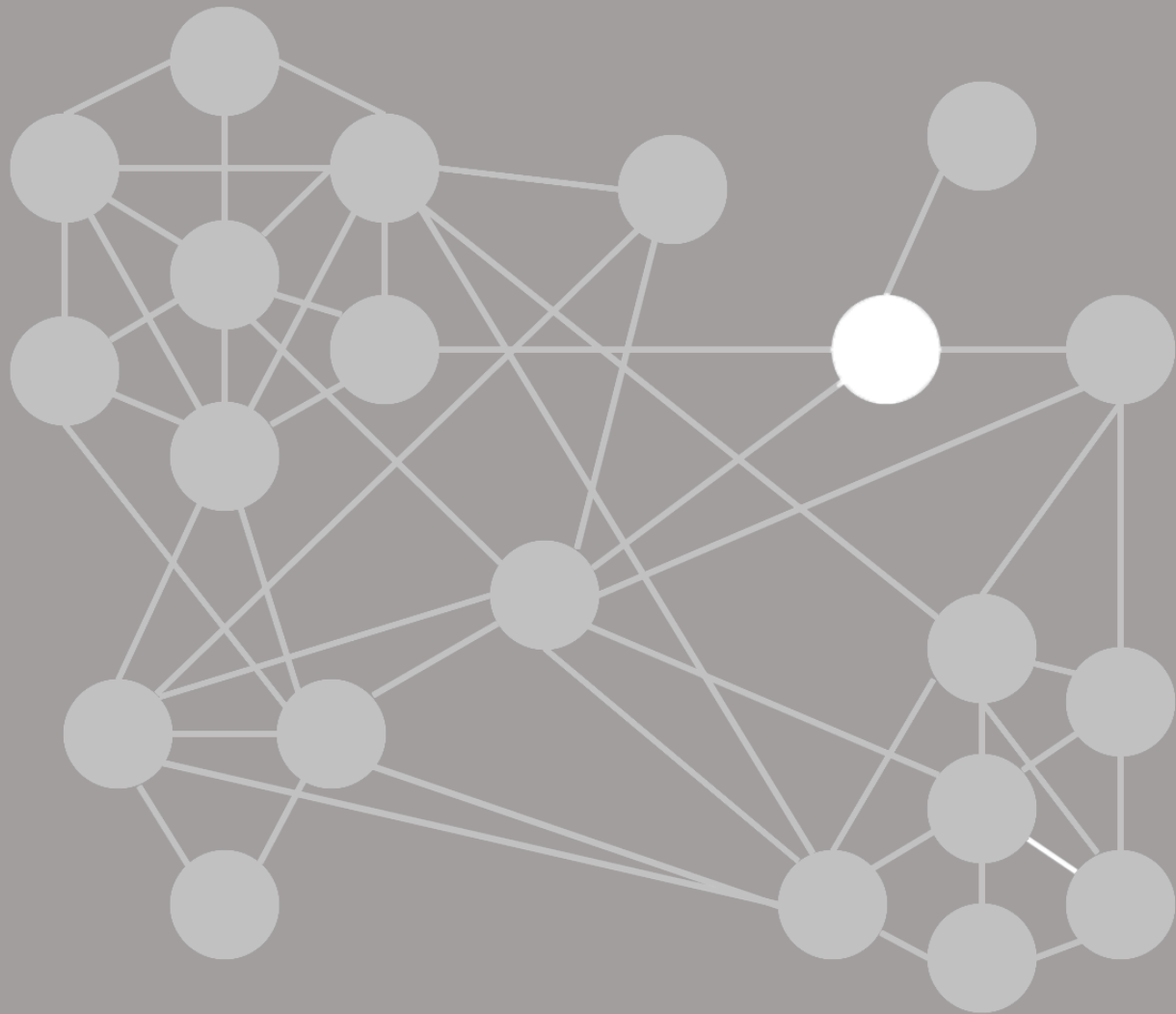
PHASE 3

ANALYSE

MEASURING
IMPACT
OF
TRAINING

AND NOW FOR SOMETHING A
LITTLE BIT DIFFERENT

BRIDGES, WEAK LINKS AND TARGETING

PIVOTING
AND
PROPAGATION

TECHNOLOGIES

- DJANGO
- POSTGRESQL
- CELERY
- REDIS
- BOOTSTRAP

- OPEN SOURCE
- GPL
- DOCKER

- INTEGRATES WITH EXCHANGE, AD AND GOOGLE APPS FOR BUSINESS

DEMO

DEAR DEMO GODS

PLEASE BE KIND.

HERE IS A KITTEN.

I HOPE IT APPEASES YOU.

FROM
LAURA

CASE STUDIES

THE PROCESS

- CANDIDATE AND VOLUNTEER REQUESTS SUBMITTED TO SOCIAL MEDIA AND CONTACTS
- VOLUNTEERS BRIEFED
- REMOVED VOLUNTEERS INCLUDING CHILDREN, STUDENTS OR HEALTH DATA
- ACTIVE DIRECTORY USERS AND GROUPS COLLECTED FROM ACTIVE DIRECTORY SERVER AND STORED IN JSON FILES
- JSON FILES PROCESSED TO REMOVE PERSONAL INFORMATION
- AVA KNOW USED TO PARSE AND IDENTIFY PATTERNS

[SWITCH TO CASE STUDY]

BE YOUR OWN CASE STUDY
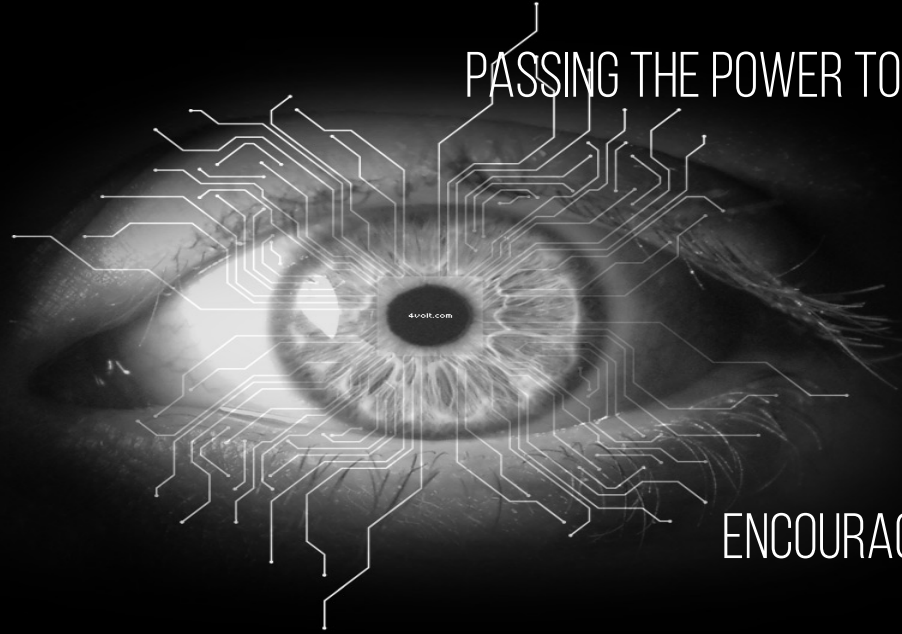
DETAILS, INSTRUCTIONS AND SCRIPTS AVAILABLE
HTTP://AVA.READTHEDOCS.ORG/EN/LATEST/

CHALLENGES

PRIVACY

BALANCE BETWEEN WHAT YOU NEED TO SEE AND WHAT YOU'D LIKE TO SEE

PASSING THE POWER TO THE PEOPLE NOT THE MANAGERS

ENCOURAGING COMMUNITY AND COLLABORATION

OPENNESS, HONESTY AND PLAIN ENGLISH

MOMENTUM

NEW SHINY TOYS NEVER HAVE A LONG LIFE SPAN

SMALL ACTIONS ON A REGULAR BASIS

SCHEDULING AND AUTOMATION

GAMIFICATION AND INCENTIVES.

WHERE NEXT?

FROM RESEARCH PROJECT TO REAL LIFE

TESTING
CONTINUOUS INTEGRATION
ROADMAP DEVELOPMENT
FEATURE DEVELOPMENT

SECURITY CULTURE CHANGE AS A SERVICE?

COLLABORATION

IF YOU ARE READING THIS AND WORK FOR
THESE PLACES, WE WANT TO TALK

GOOGLE
FACEBOOK
TWITTER
LINKEDIN
MICROSOFT

PLUS

ANY ORGANIZATION THAT WANTS TO DO SAFE,
CONSENSUAL HUMAN SECURITY SCIENCE

WHAT ABOUT PEOPLE?

TL;DR

1. **HUMAN-CENTRIC SECURITY** IS COMPLEX

2. AVA HOPES TO BRING A **NEW APPROACH**, GET INVOLVED

3. **WATCH THIS SPACE**, MUCH MORE TO COME

QUESTIONS?

#protectyourpeople

LAURA BELL

Founder and Lead Consultant - SafeStack

@lady_nerd   laura@safestack.io

http://safestack.io