CTRL+ALT+DEFEND:

FROM FAILS TO HACKING THE ART OF EMPLOYEE (IN)SECURITY

BY DANA RUBENA,
IT SECURITY OPERATIONS OFFICER

NO CYBER SECURITY BUDGET VS GOOD CYBER SECURITY BUDGET

- DOES THE BUDGET MATTER?
- THEN WHY DOES CYBER SECURITY STILL FAIL?

SECURITY FAILS

- PROOFPOINT SANDBOXING:
  - PRE-ARMED PHISH SITES
  - ARE YOU HUMAN?
- FORTINET: VPN SPLIT-TUNNELING
- CROWDSTRIKE:
  - FIELSIZE LIMIT
  - ANALYZE ON-WRITE ONLY (REALLY!??)
- MXDR:
  - FAULTY MONITORING ALGORITHMS
  - FAULTY THREAT INTEL
  - PLATFORM, INTEGRATION AND PLAYBOOK LIMITATIONS

USERS BYPASSING SECURITY CONTROLS LIKE HACKERS – THE MEXICO CASE

- PROOFPOINT FAIL
- FORTINET FAIL
- CROWDSTRIKE FAIL
- WHAT SAVED US?
- FRESHLY OPENED OFFICE FAIL
- LOGISTICS FAIL

OUR PROCESSES & IMPROVEMENTS SO FAR

- INCIDENT RESPONSE FRAMEWORK
- WHAT'S THE RESPONSE TIME FRAME AND WHY DOES IT MATTER?
- QA/KX SESSIONS WITH SERVICE DESK
- SECOPS MAIN FOCUS = QA & CONTINUOUS IMPROVEMENTS (SPRINTS)
- EXTENSIVE USER AWARENESS CAMPAIGNS
- MONITORING TTPS VIA EMAIL ATTACK TRENDS

THERE'S JUST ONE PROBLEM…

- 3RD-PARTY IT VENDOR IS USING SINGLE PASSWORD TO ACCESS ALL OUR SERVERS
- IT USERS STORE ACCESS CREDENTIAL LISTS IN SHARED EXCEL FILES
- …

KEY TAKEAWAYS

- IT'S BETTER TO DO LITTLE THAN TO DO NOTHING
- FOCUS MORE ON THE END-USER AWARENESS, LESS ON ADDITIONAL SECURITY TECH YOU CAN BUY