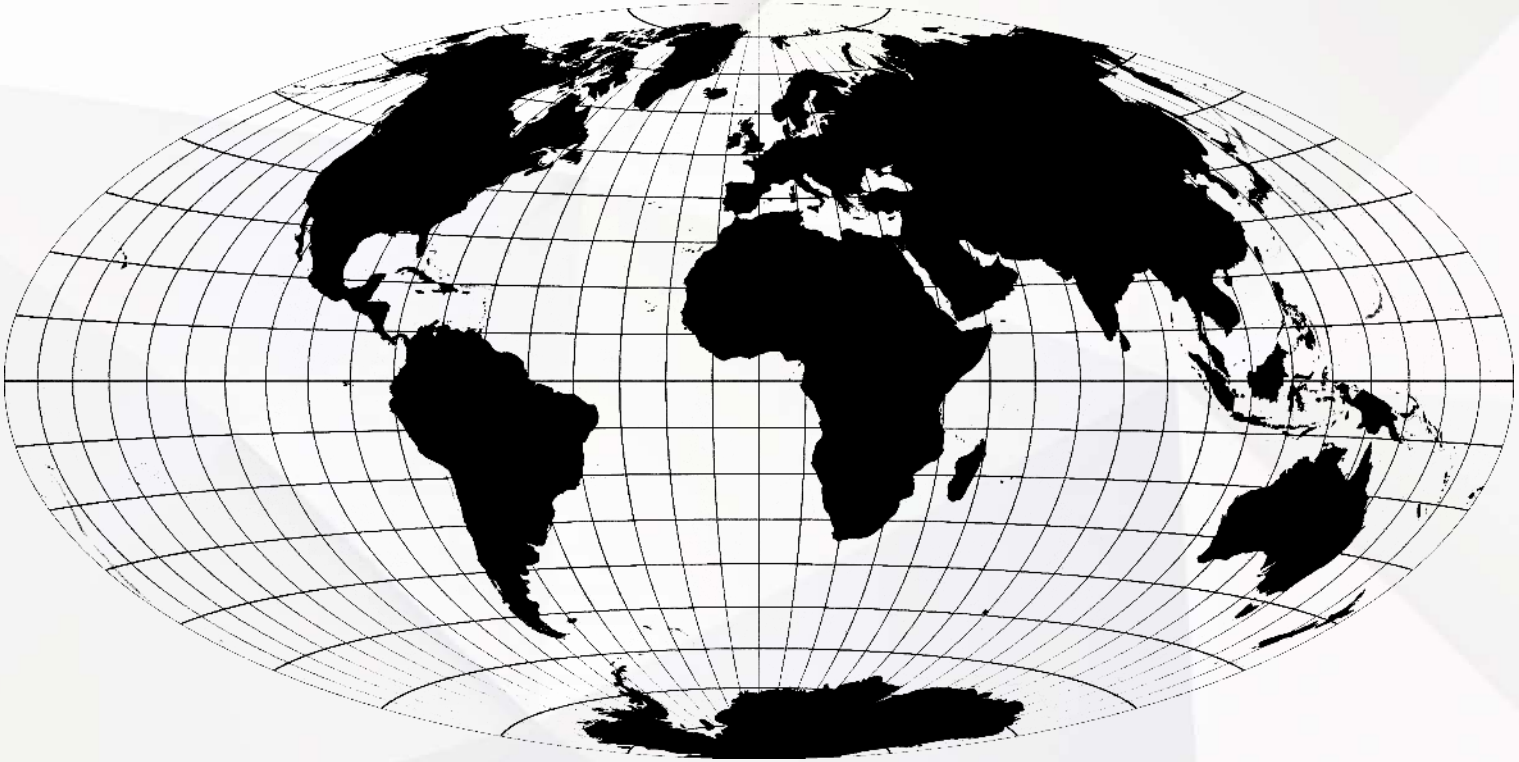
POST-MORTEM OF A DATA BREACH

Janne Kauhanen

@jkauhanen

F-Secure Cyber Security Services



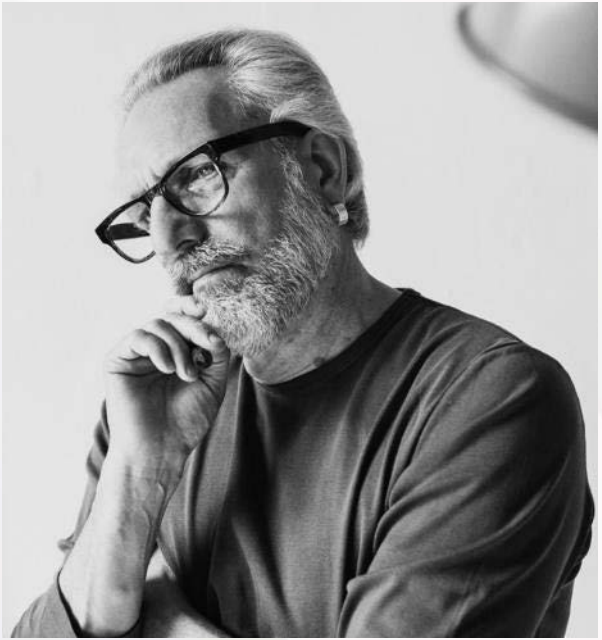
100+ ASSIGNMENTS / 3 YEARS

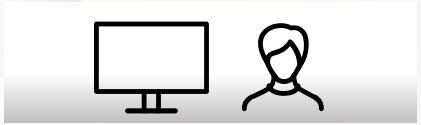
SERVICE PROVIDER ”CORP X”

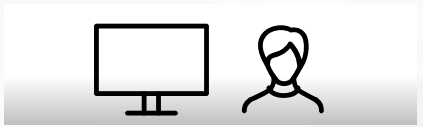
- Listed on several international stock exchanges
- Provides application services, e.g. to financial sector
- Never thought they could be targeted – ”we’re just a regular company”

SITUATION ONE MORNING IN SEPT 2015

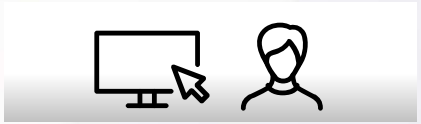
- ”7GB of data was sent from one financial department employees PC to IP-address xxx.xxx.xxx.xxx.”
- F-Secure Labs confirmed the address as a known data exfiltration server, used in a recently activated campaign







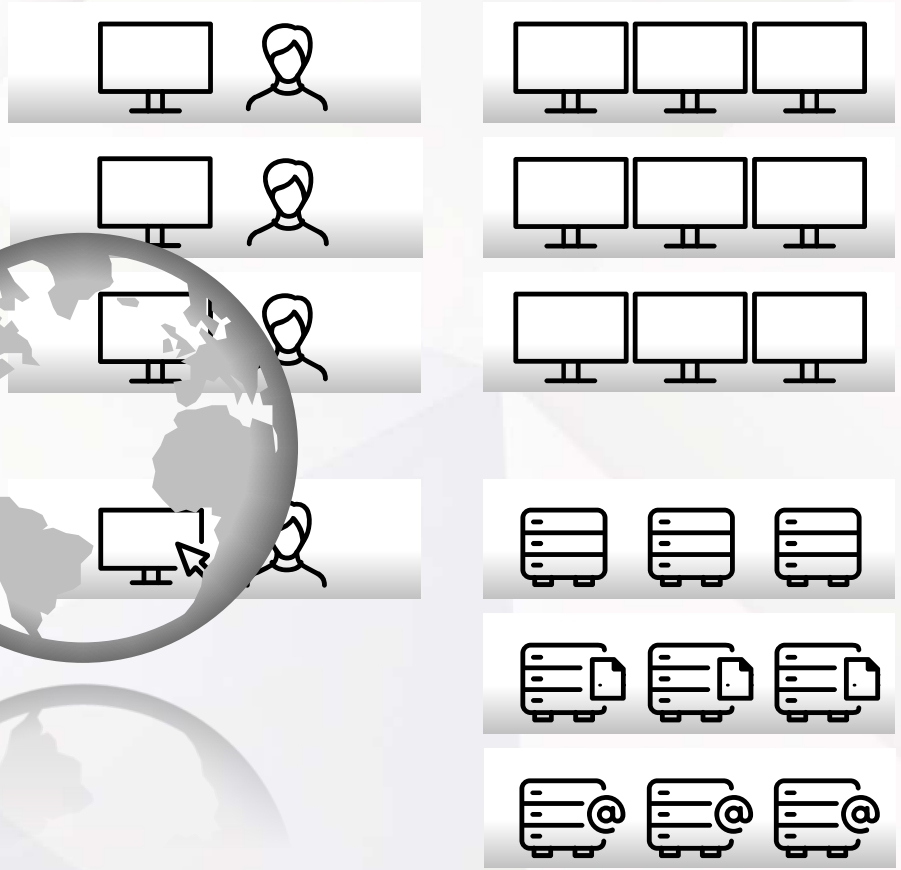
Watering hole



Command & Control

Data Exfiltration

RECON



Watering hole

Command & Control

Data Exfiltration

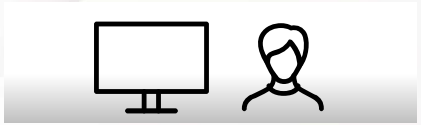
RECON

Watering hole

Command & Control

Data Exfiltration

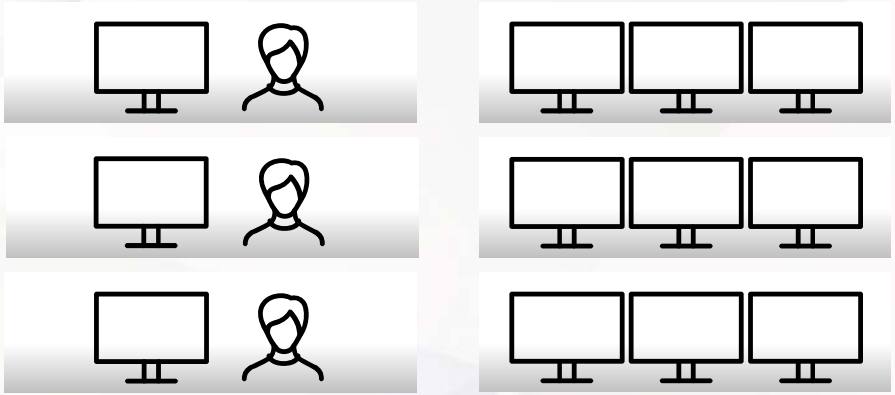
RECON

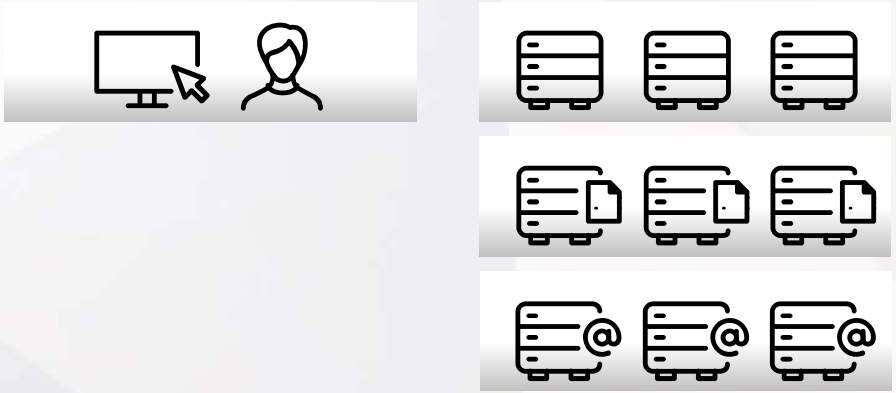


Watering hole

Command & Control

Data Exfiltration

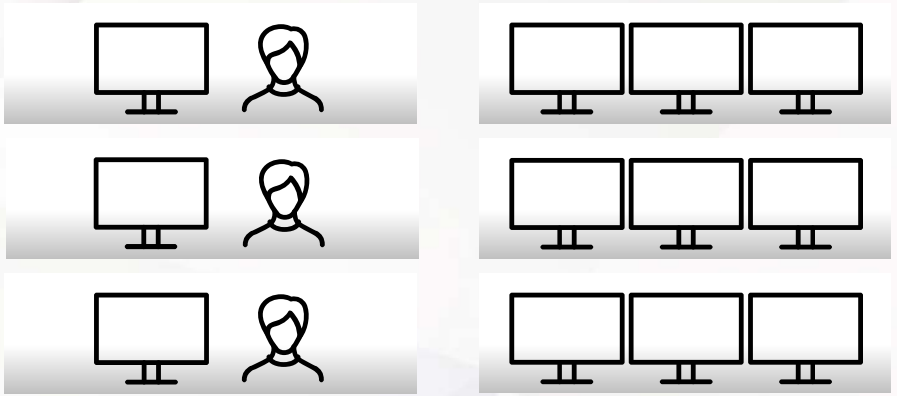


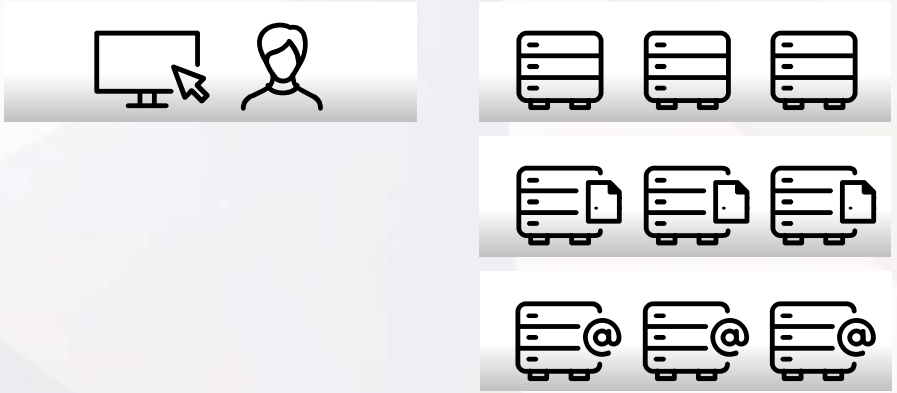


Watering hole

Command & Control

Data Exfiltration



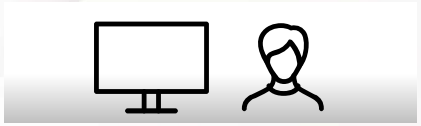


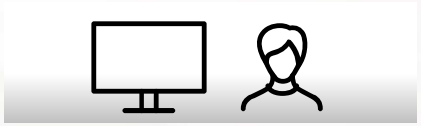
Watering hole

Command & Control

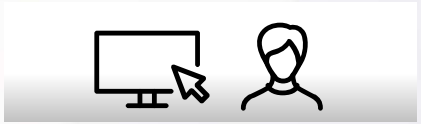
Data Exfiltration

RECON





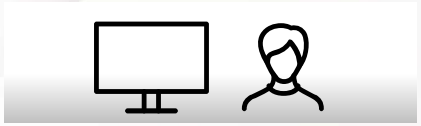
Watering hole

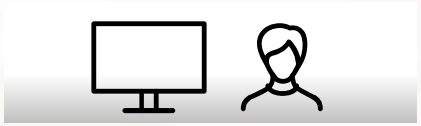


Command & Control

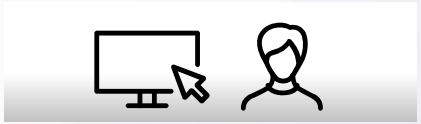
Data Exfiltration

RECON





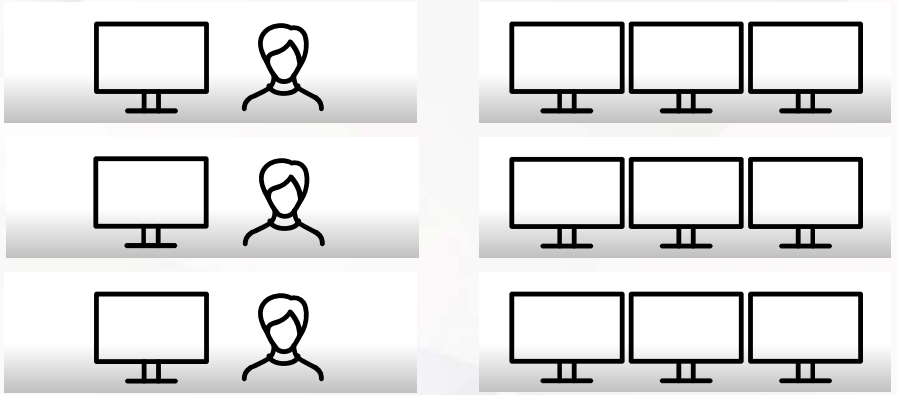
Watering hole



Command & Control

Data Exfiltration

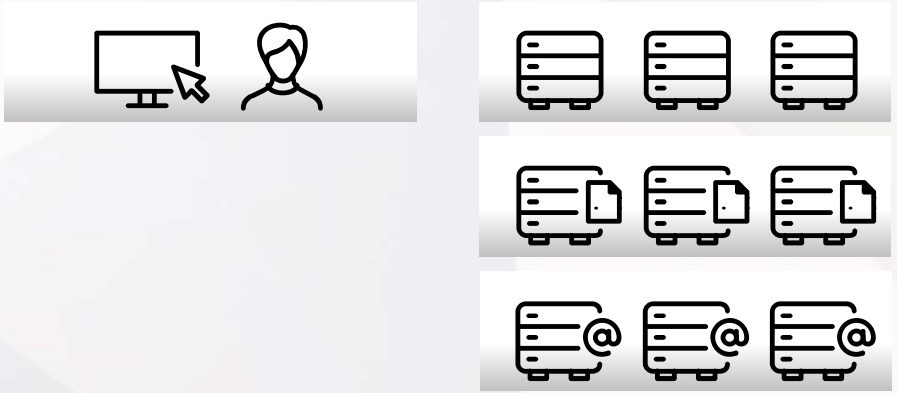
EXPLOITATION



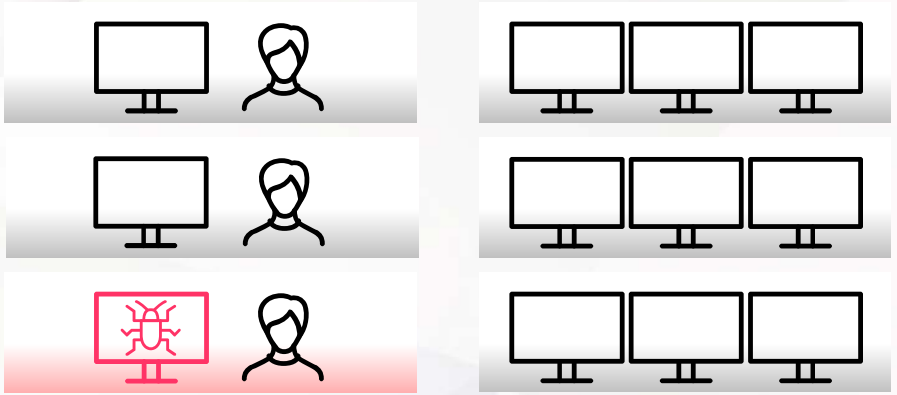
Watering hole

Command & Control

Data Exfiltration



EXPLOITATION

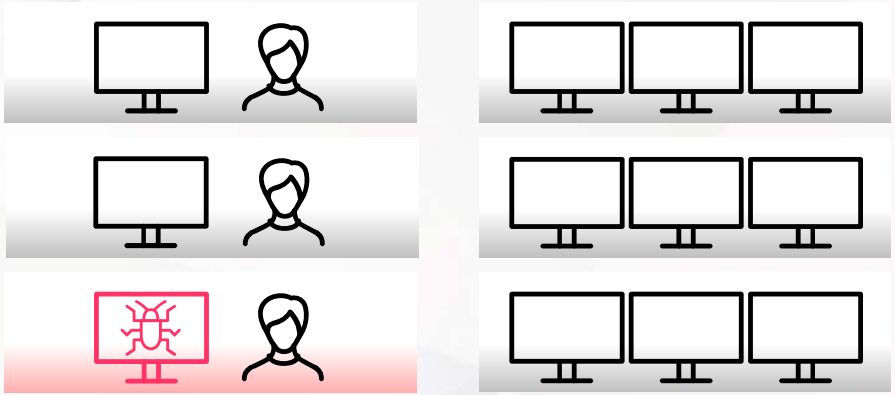


Watering hole

Command & Control

Data Exfiltration

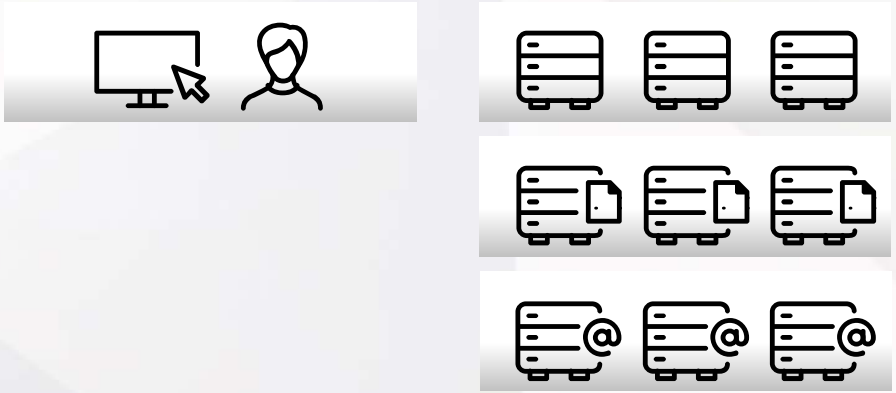
ATTACK KIT DELIVERY



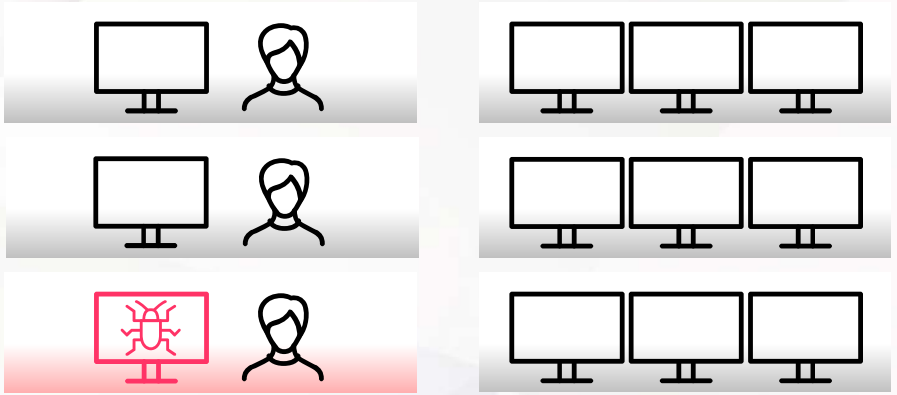
Watering hole

Command & Control

Data Exfiltration



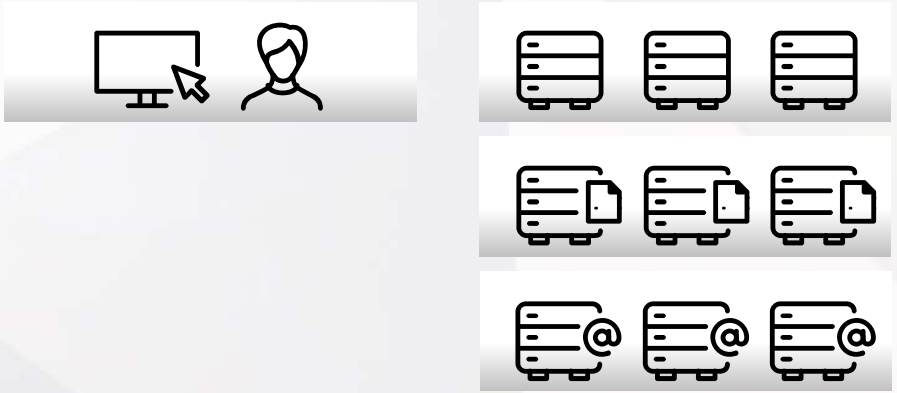
ATTACK KIT DELIVERY



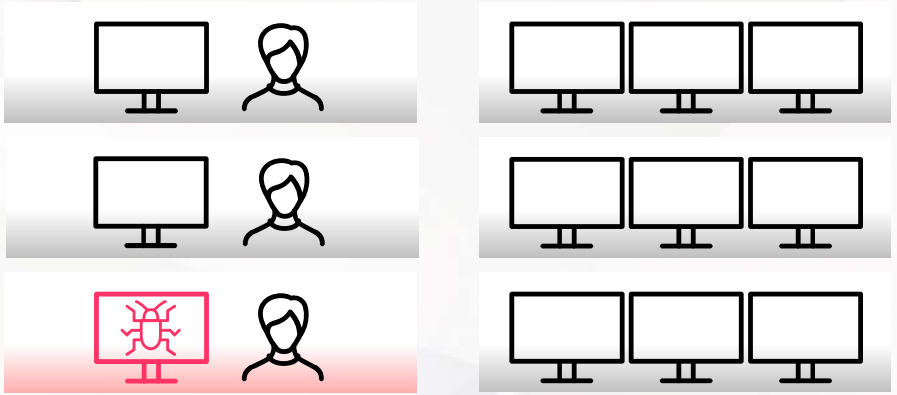
Watering hole

Command & Control

Data Exfiltration



ATTACK KIT DELIVERY

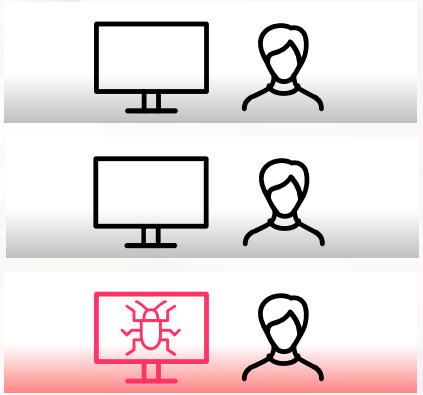


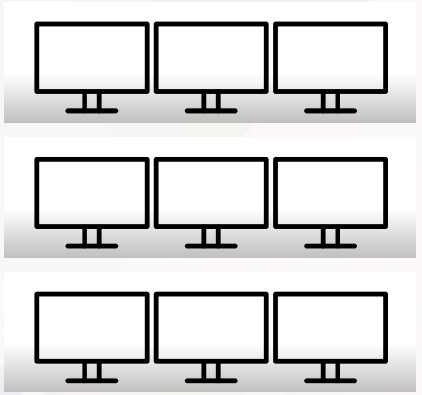
Watering hole

Command & Control

Data Exfiltration

ATTACK KIT DELIVERY

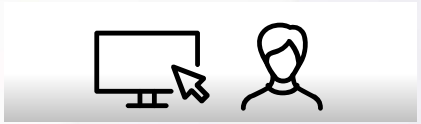


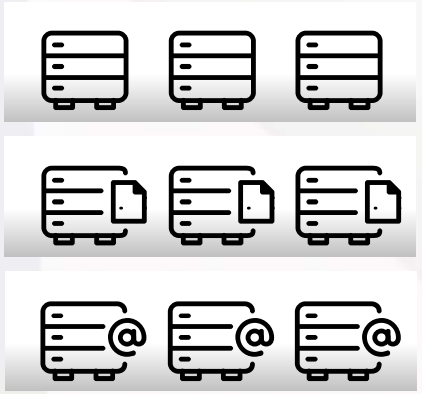


Watering hole

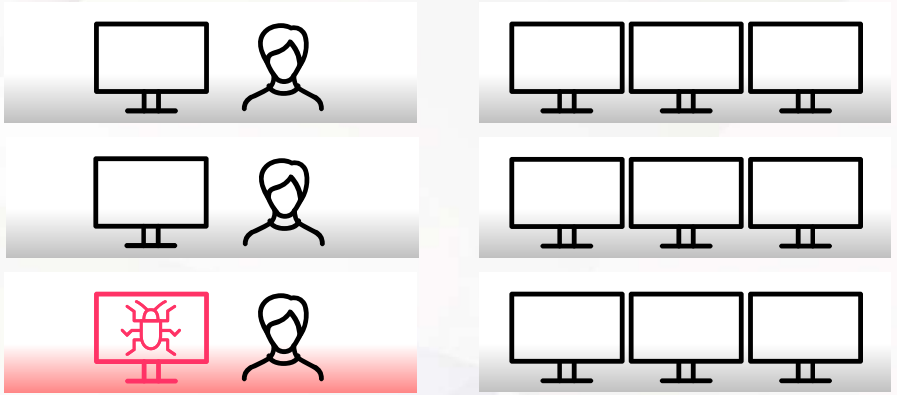
Command & Control

Data Exfiltration





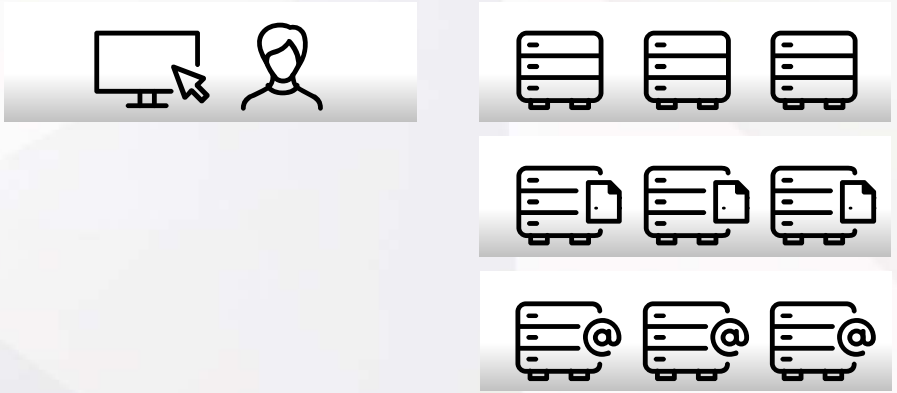
LATERAL MOVEMENT



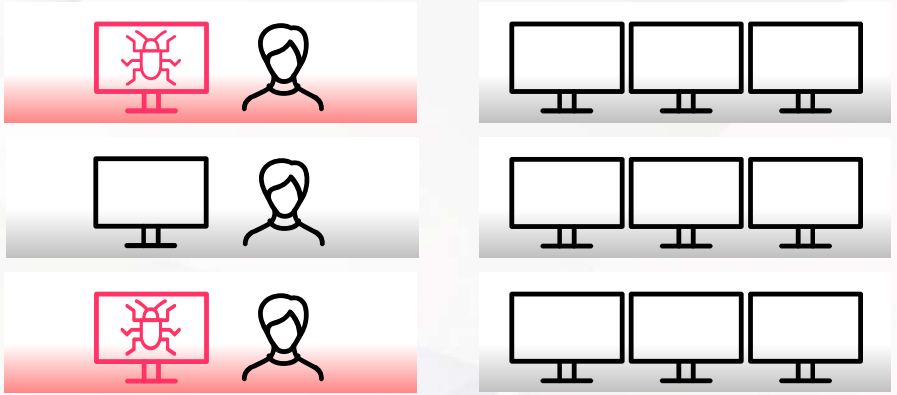
Watering hole

Command & Control

Data Exfiltration



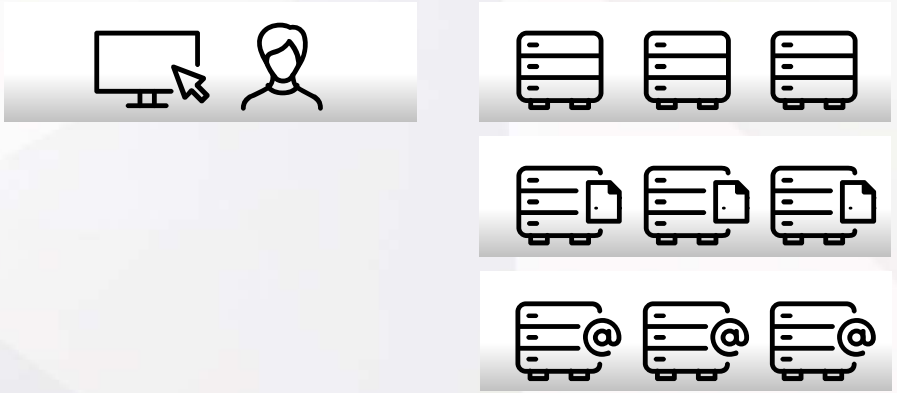
LATERAL MOVEMENT



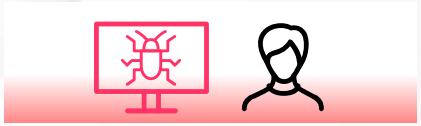
Watering hole

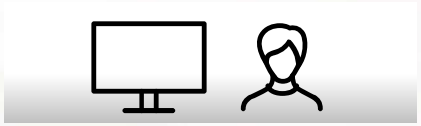
Command & Control

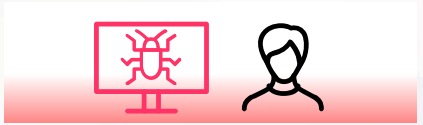
Data Exfiltration

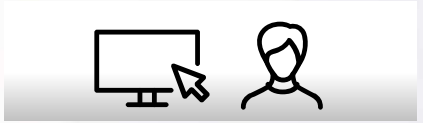


LATERAL MOVEMENT







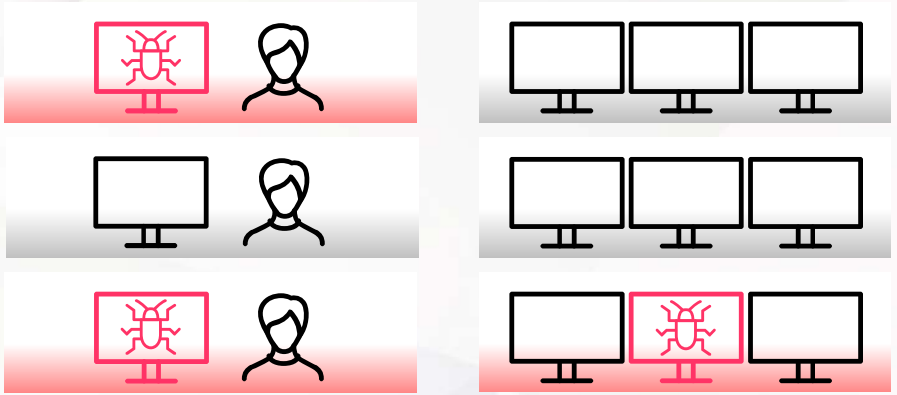


Watering hole

Command & Control

Data Exfiltration

LATERAL MOVEMENT

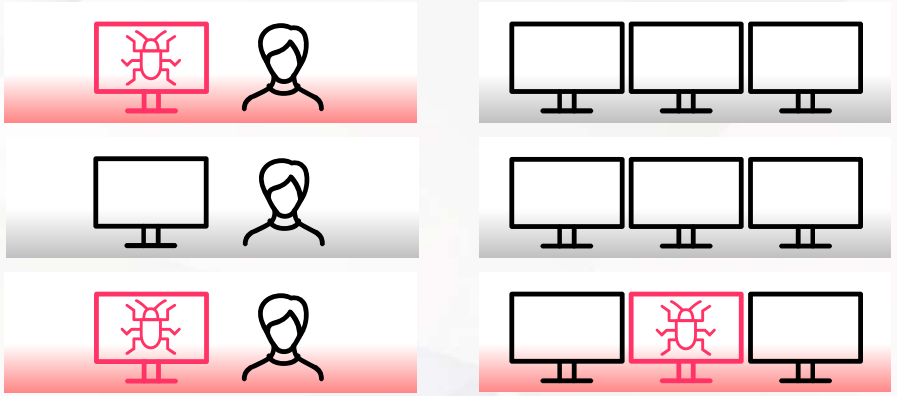


Watering hole

Command & Control

Data Exfiltration

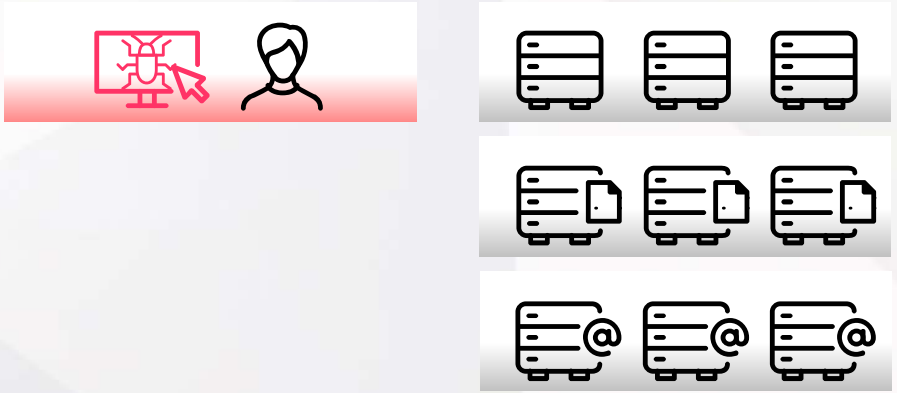
DATA COLLECTION



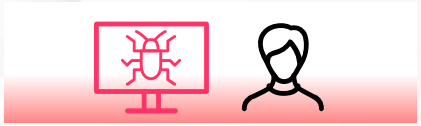
Watering hole

Command & Control

Data Exfiltration



DATA COLLECTION

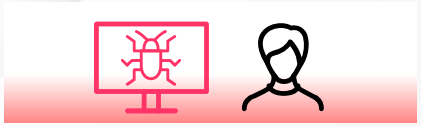


Watering hole

Command & Control

Data Exfiltration

DATA COLLECTION

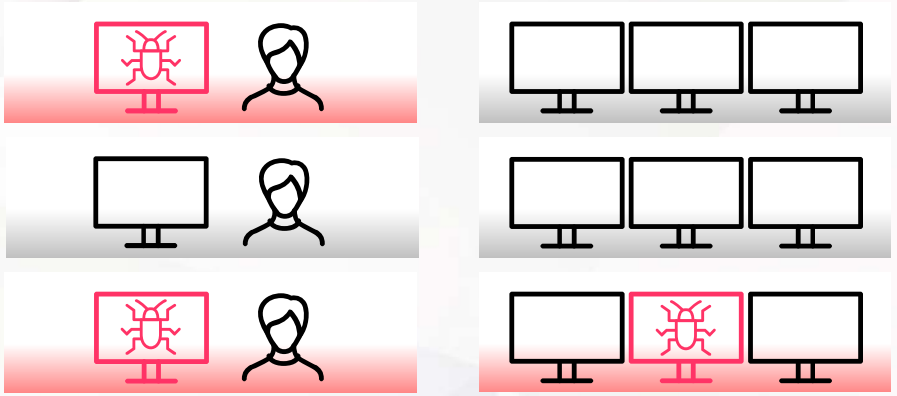


Watering hole

Command & Control

Data Exfiltration

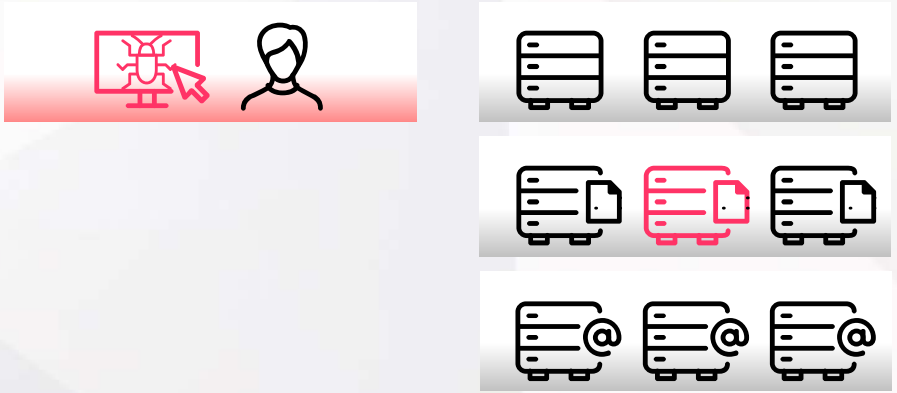
DATA COLLECTION



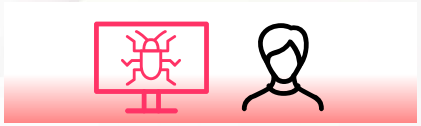
Watering hole

Command & Control

Data Exfiltration



DATA COLLECTION

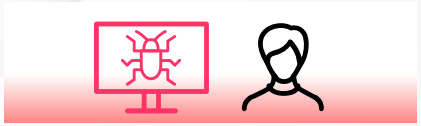


Watering hole

Command & Control

Data Exfiltration

DATA COLLECTION

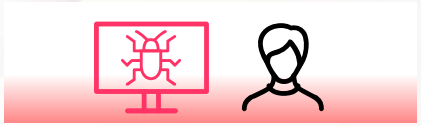


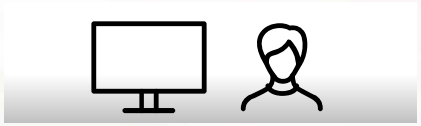
Watering hole

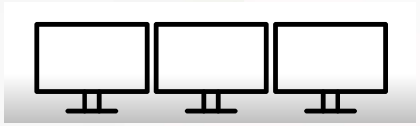
Command & Control

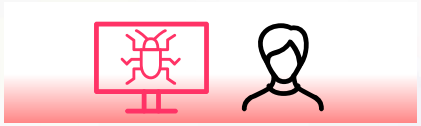
Data Exfiltration

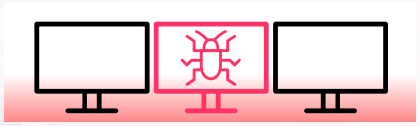
DATA COLLECTION









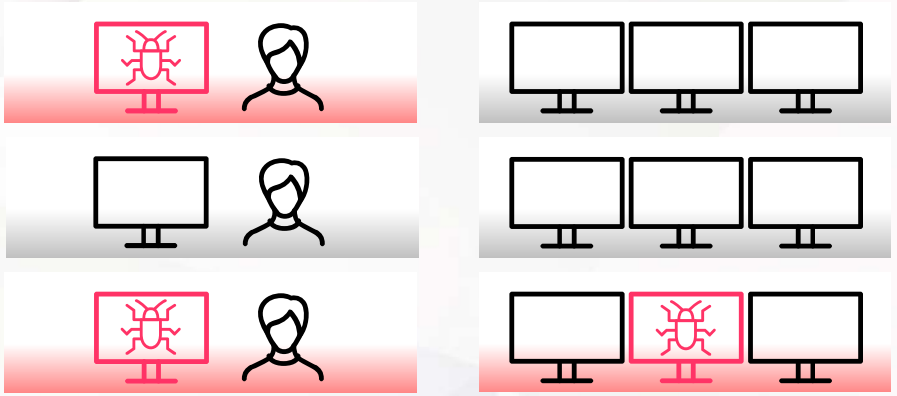


Watering hole

Command & Control

Data Exfiltration

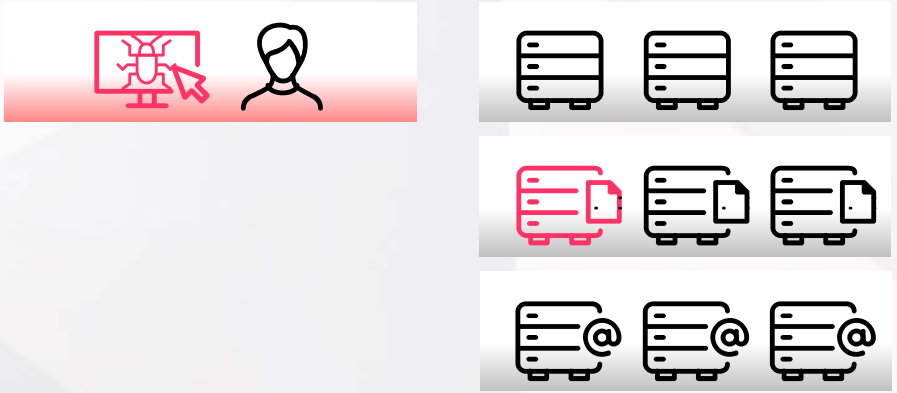
DATA COLLECTION



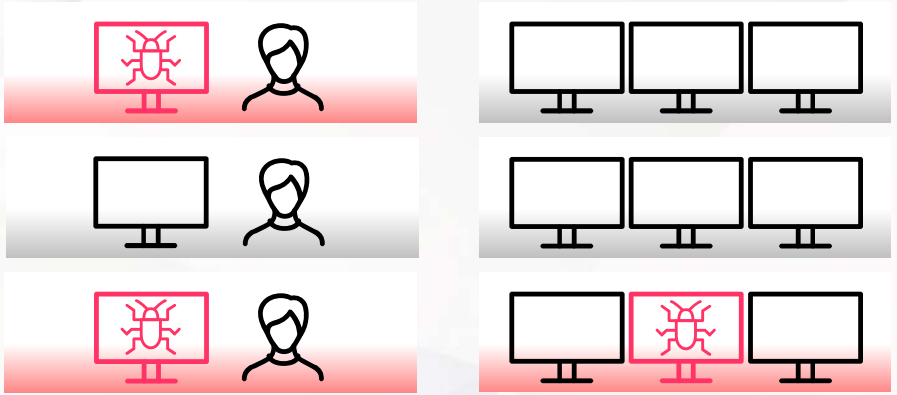
Watering hole

Command & Control

Data Exfiltration



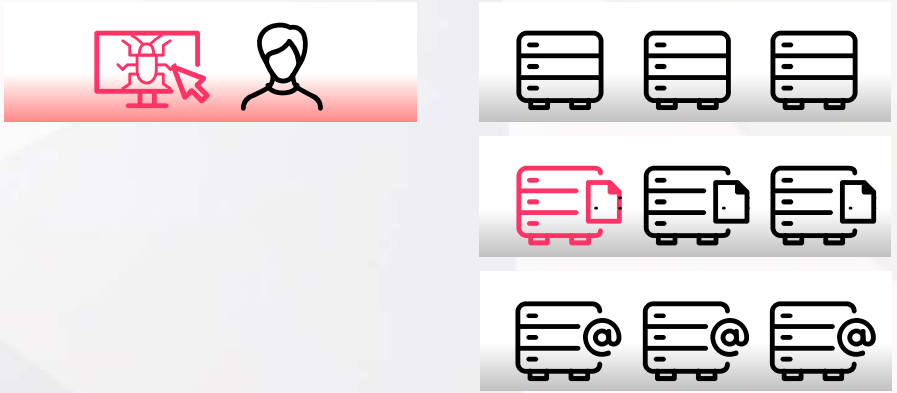
DATA EXFILTRATION



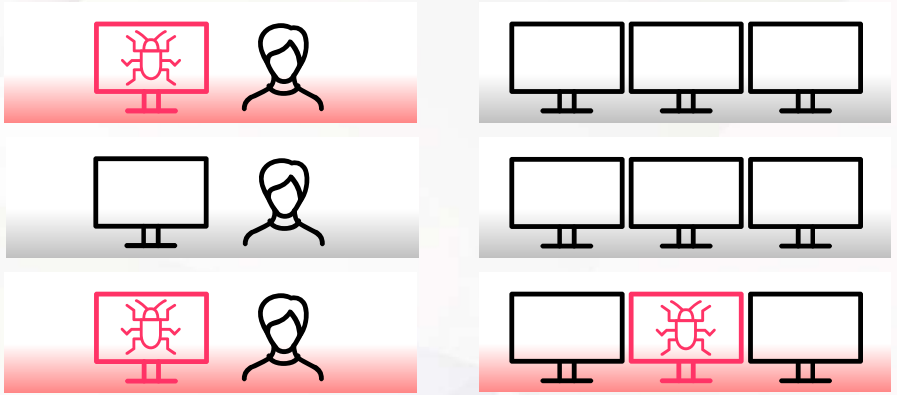
Watering hole

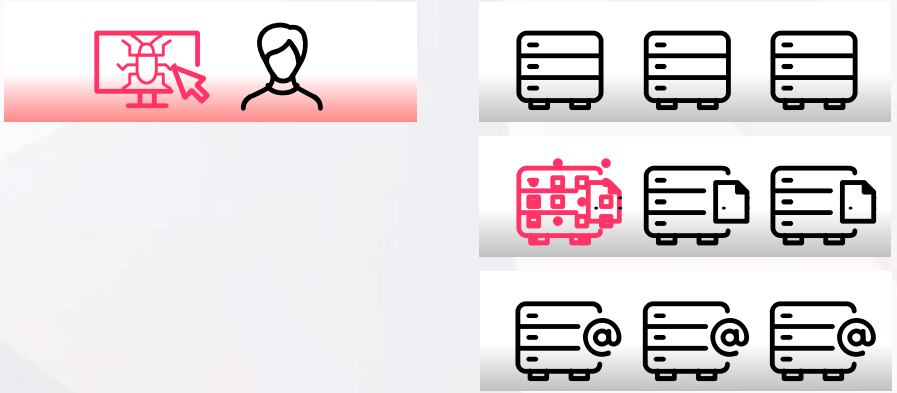
Command & Control

Data Exfiltration



DATA EXFILTRATION



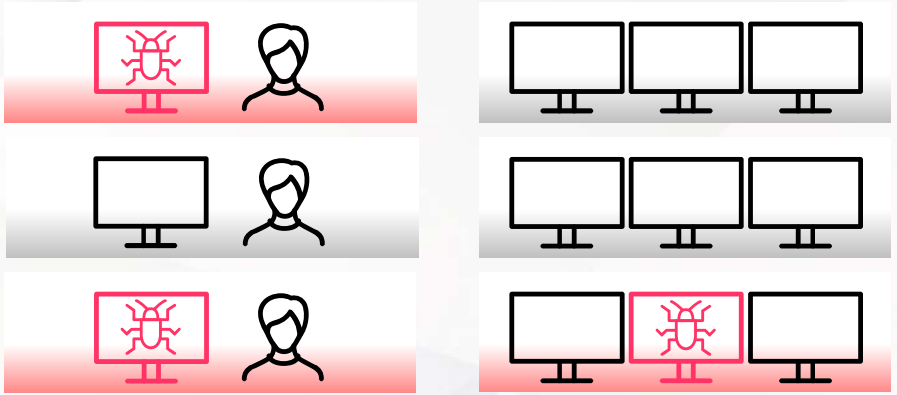


Watering hole

Command & Control

Data Exfiltration

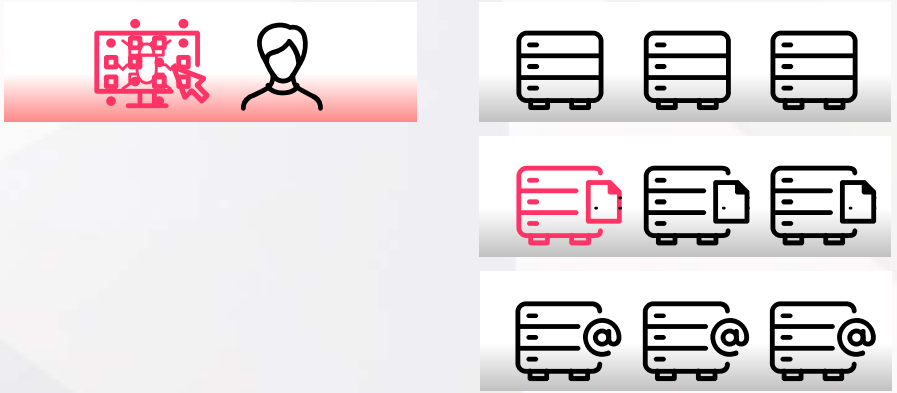
DATA EXFILTRATION



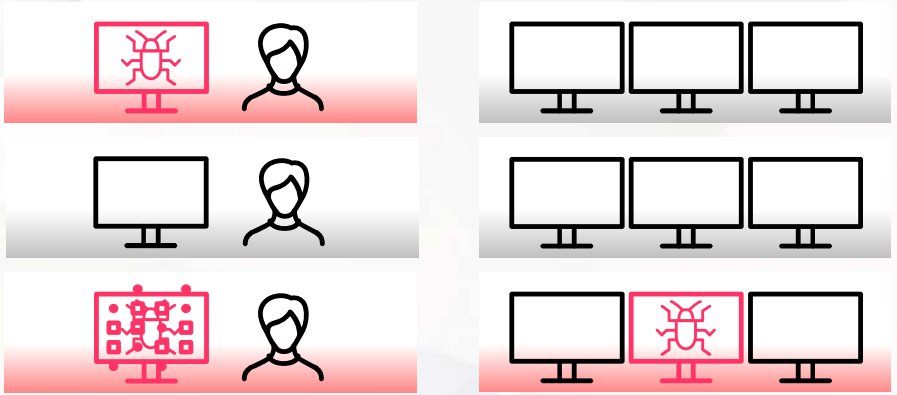
Watering hole

Command & Control

Data Exfiltration



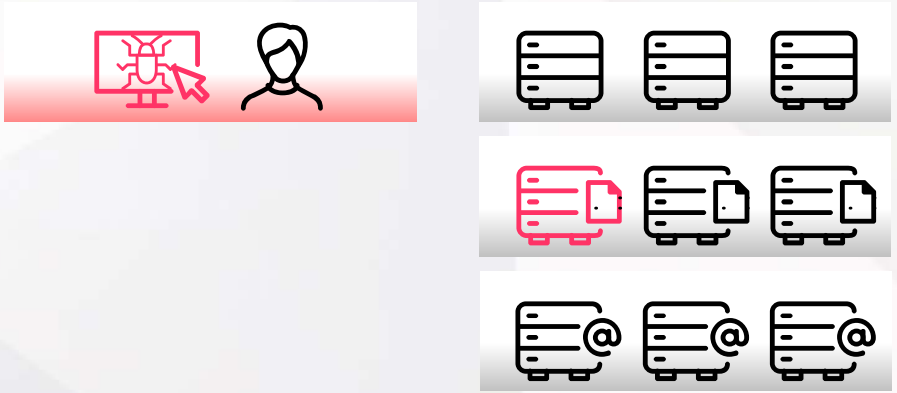
DATA EXFILTRATION



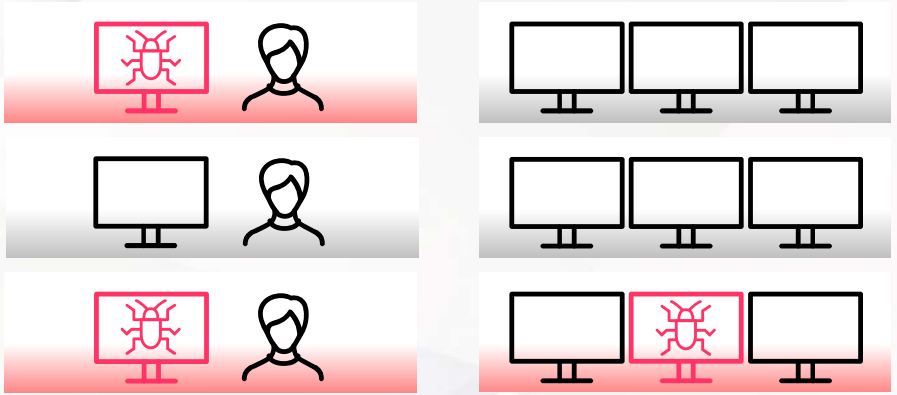
Watering hole

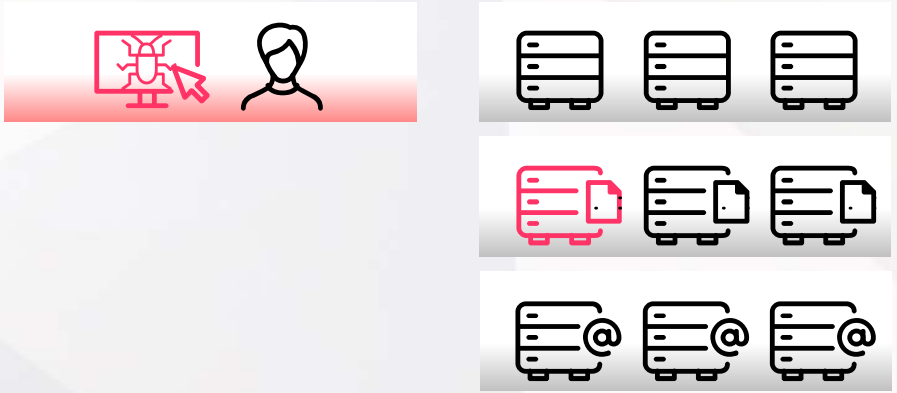
Command & Control

Data Exfiltration



DATA EXFILTRATION





Watering hole

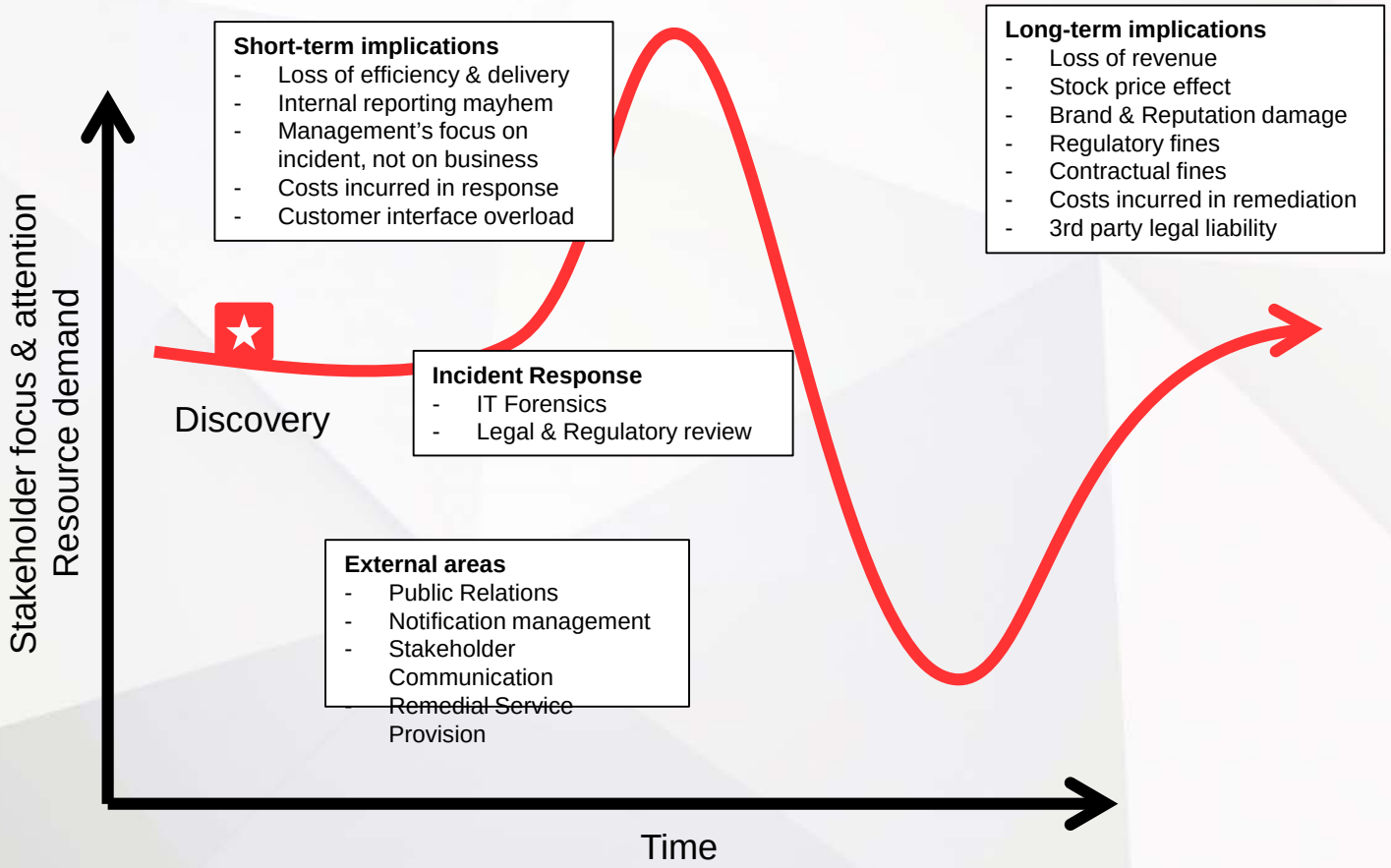
Command & Control

Data Exfiltration

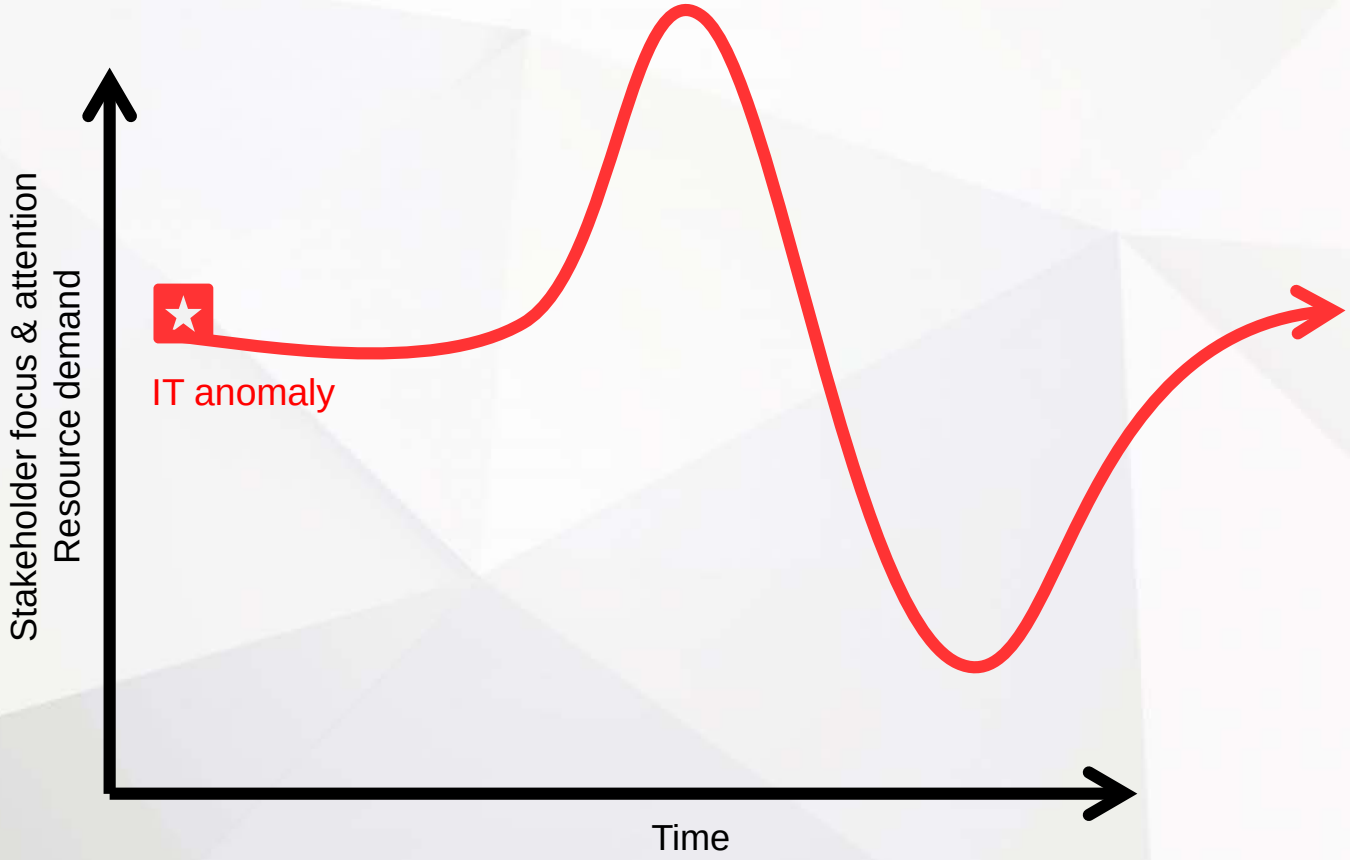
WHAT WAS THE BUSINESS IMPACT ON ”CORP X” ?

F-Secure

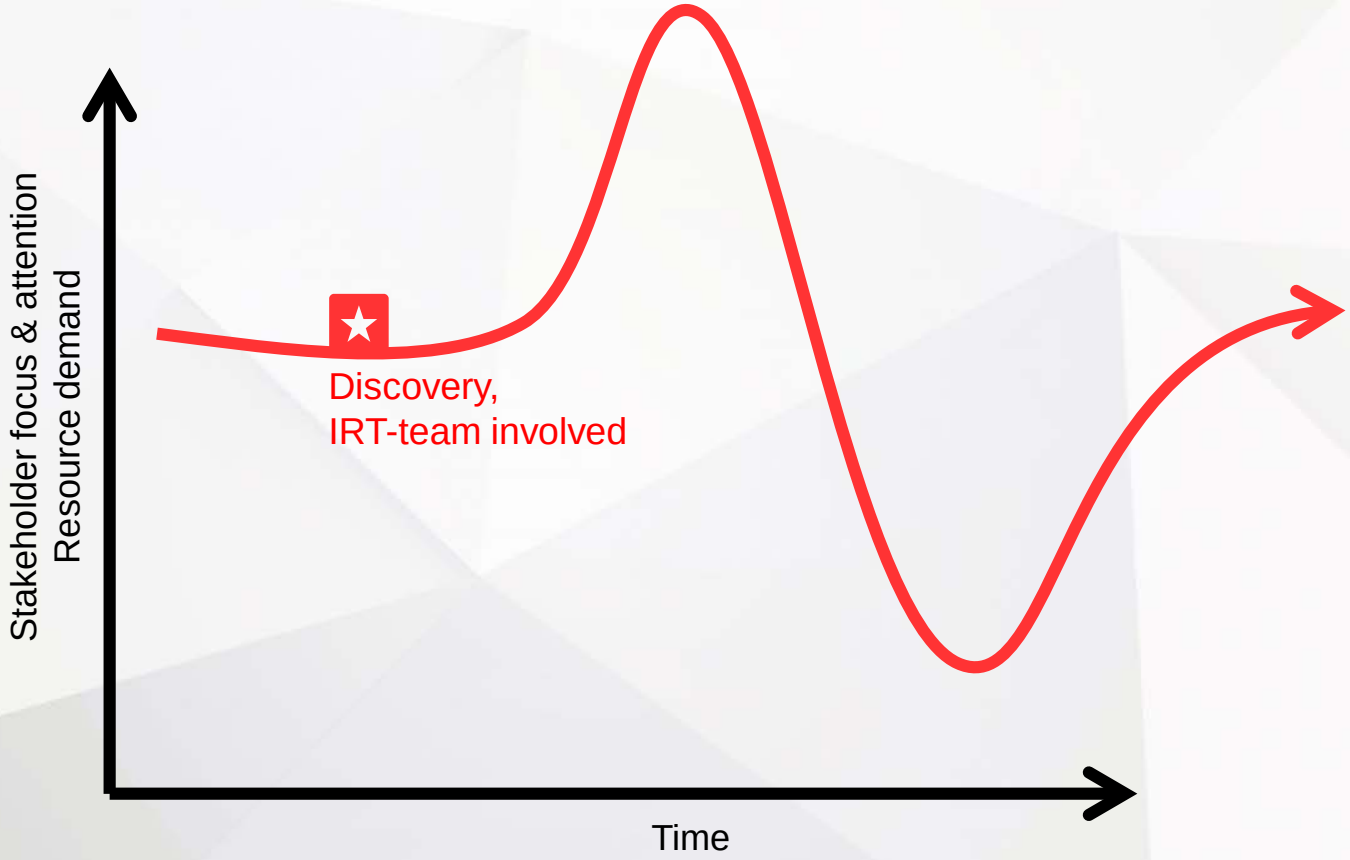
SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE



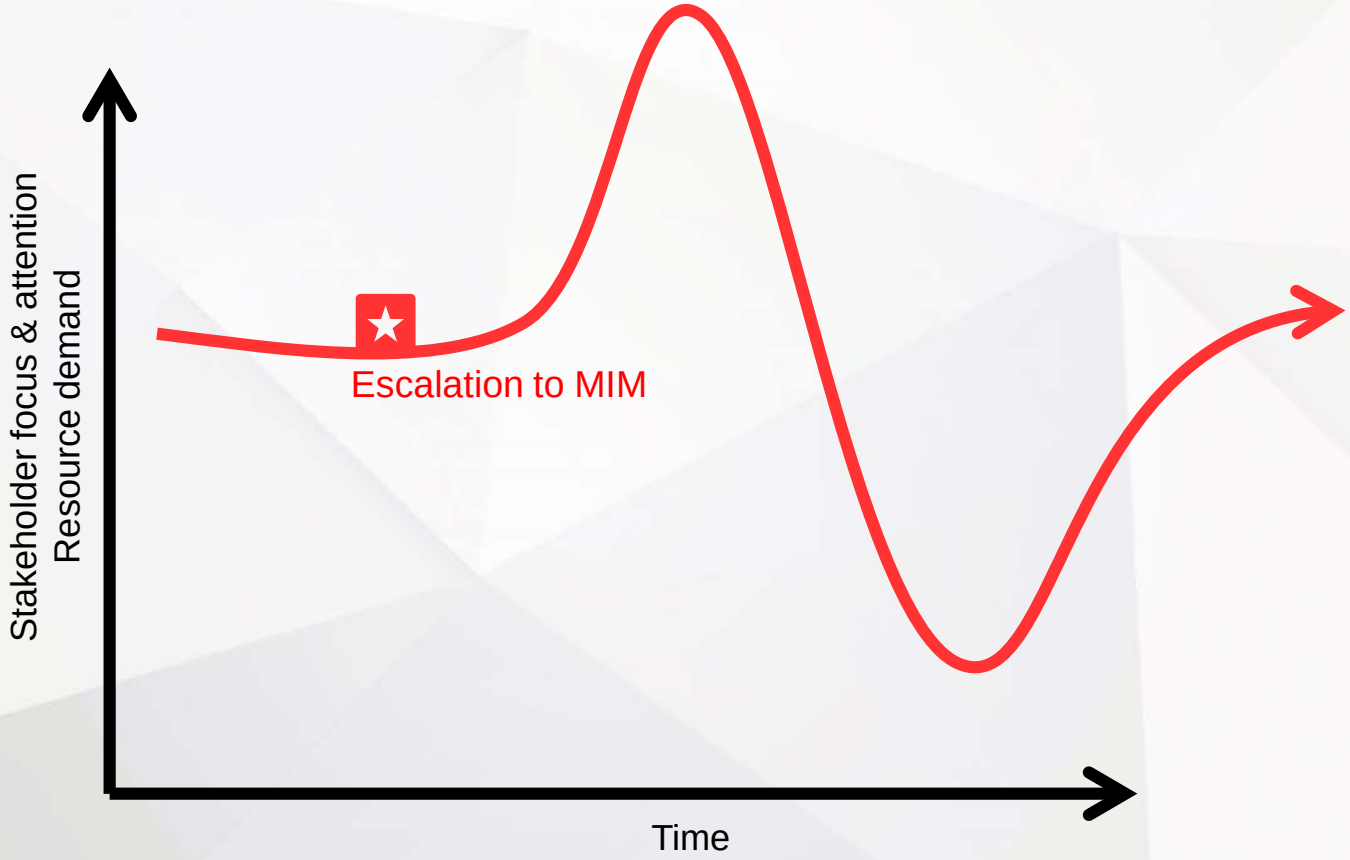
SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE



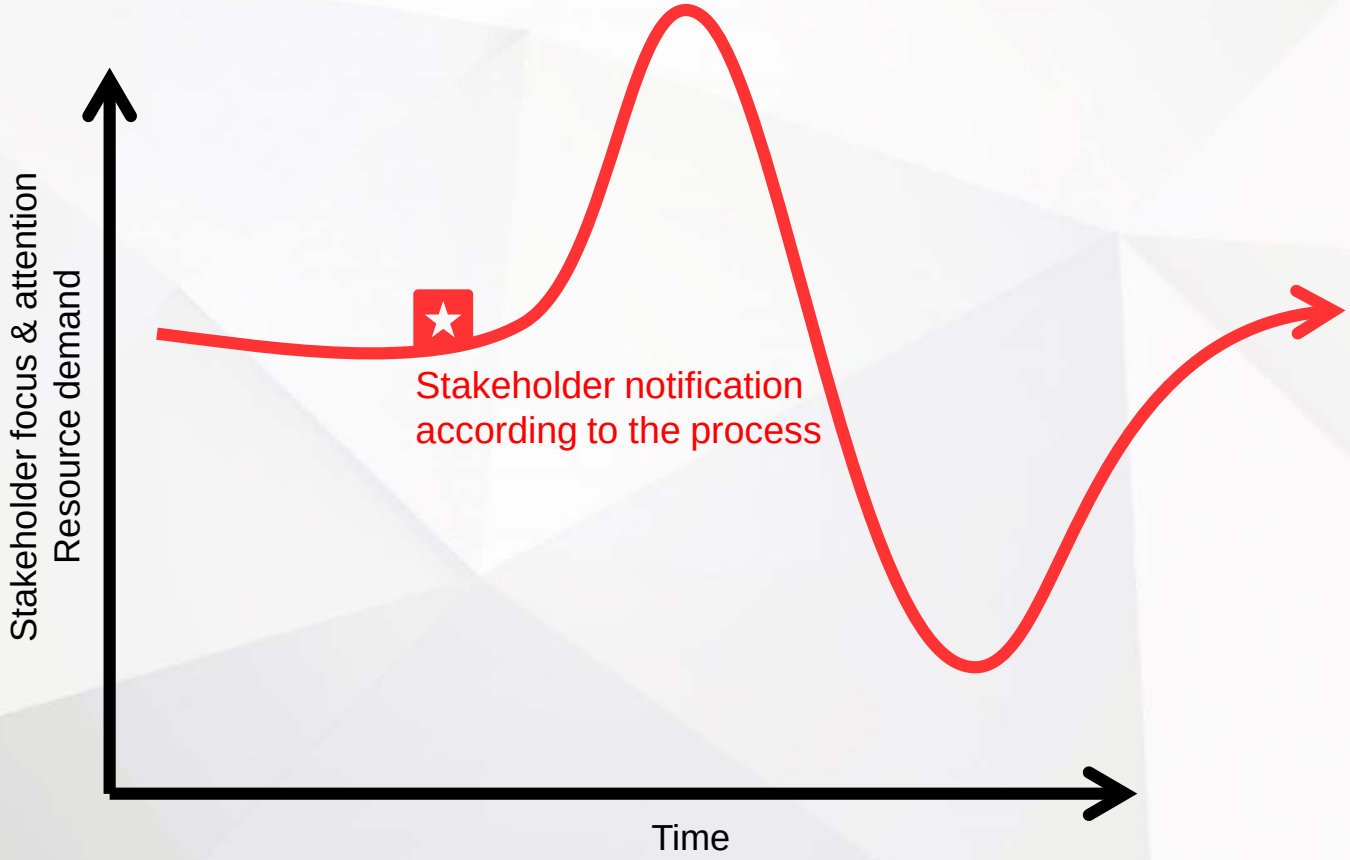
SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE



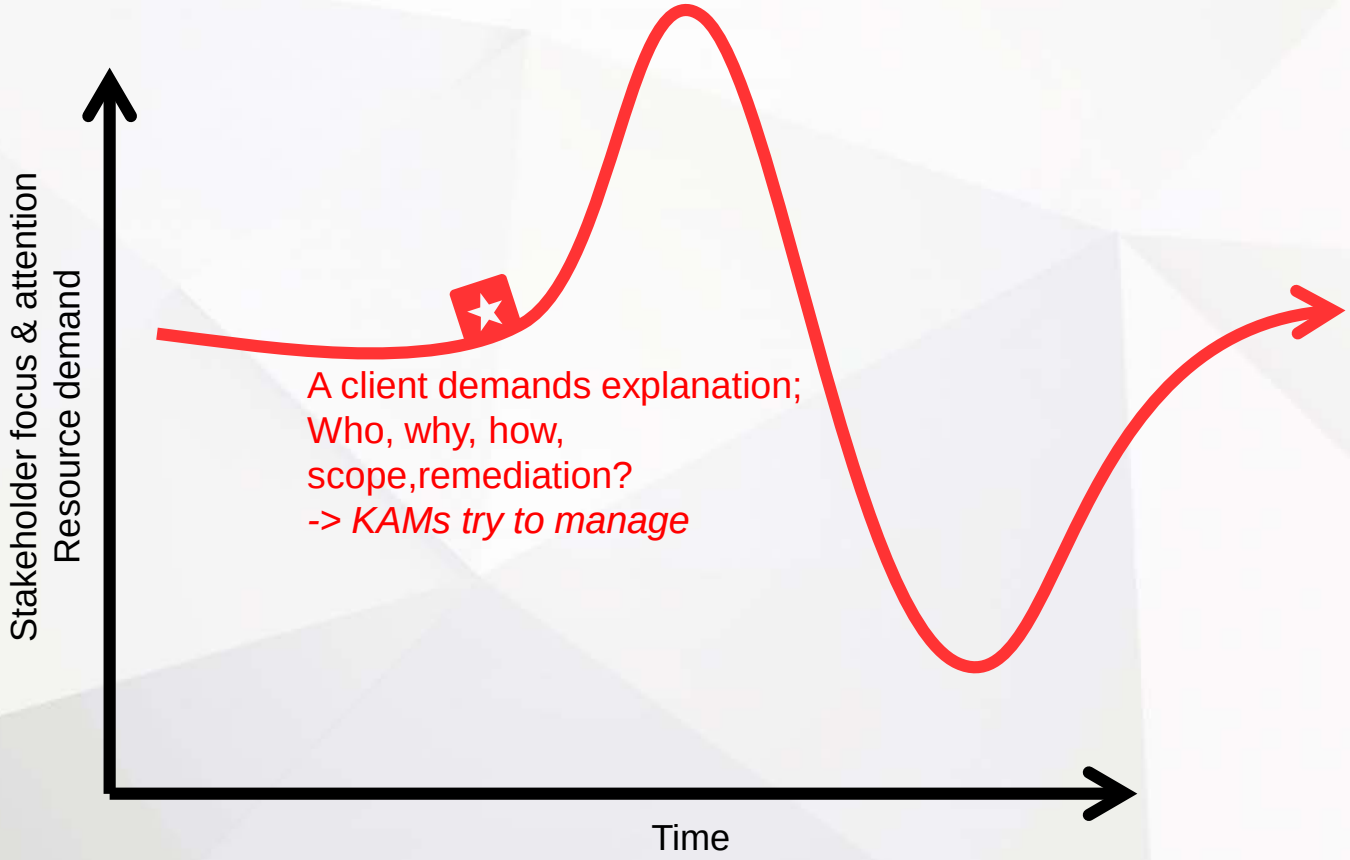
SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE



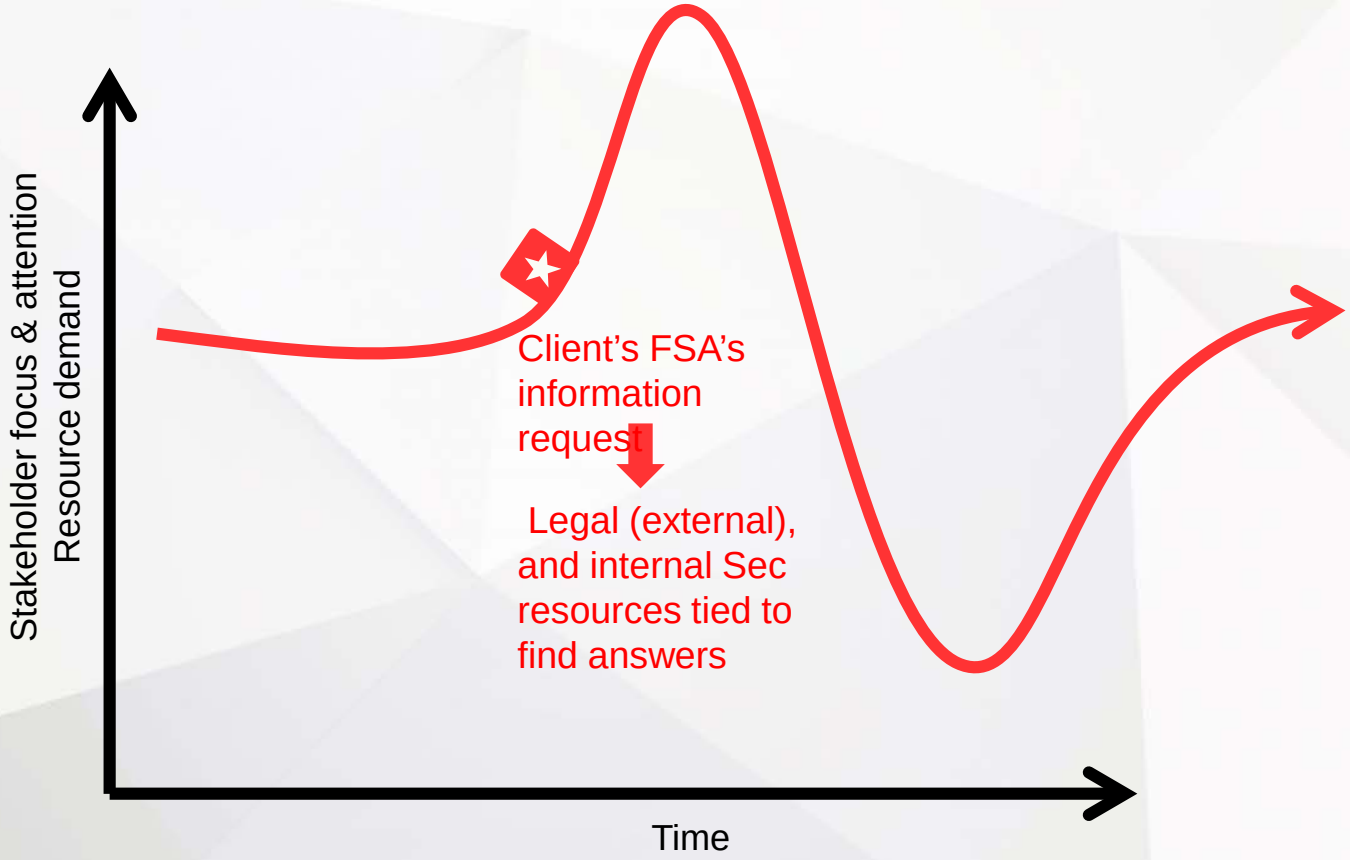
SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE



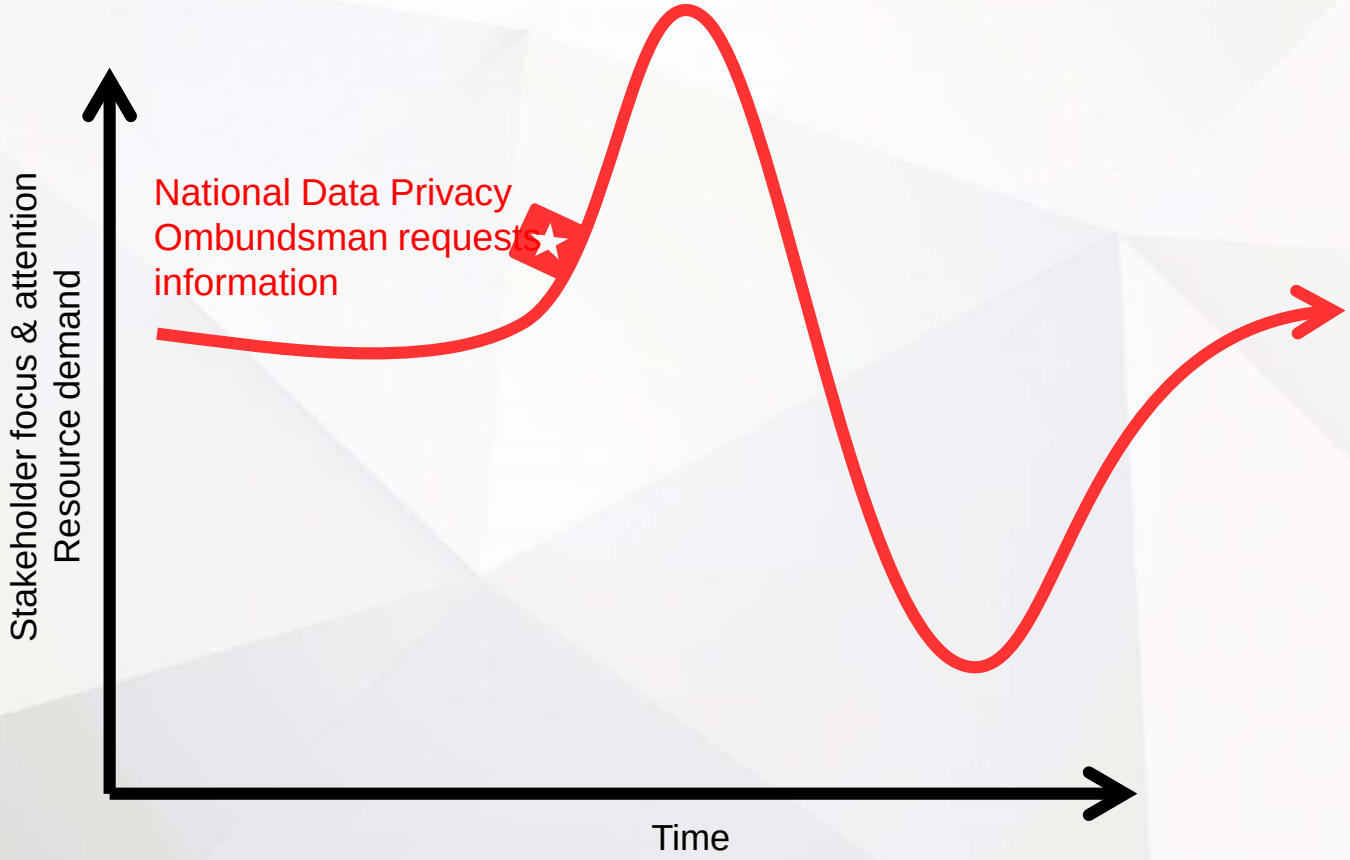
SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE



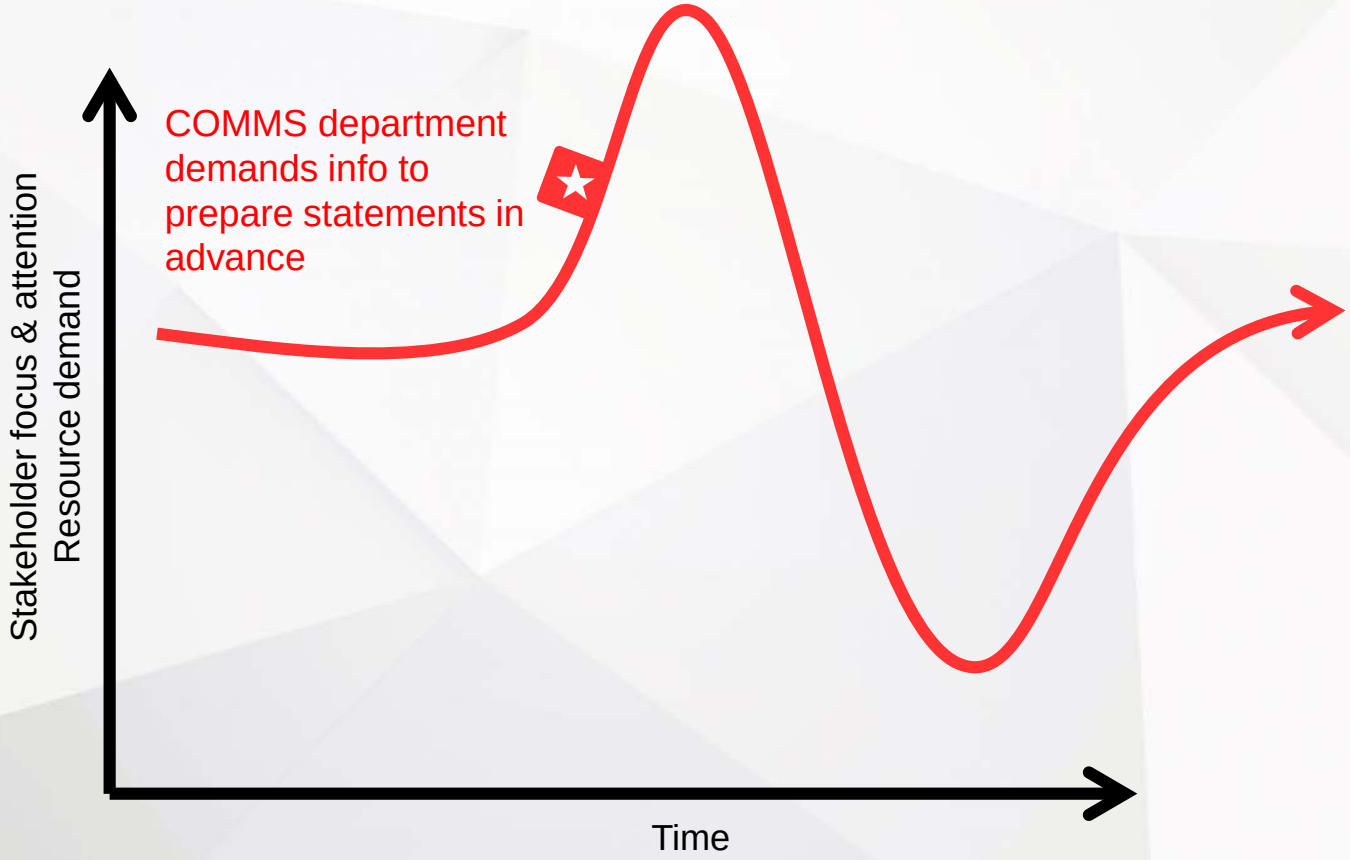
SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE



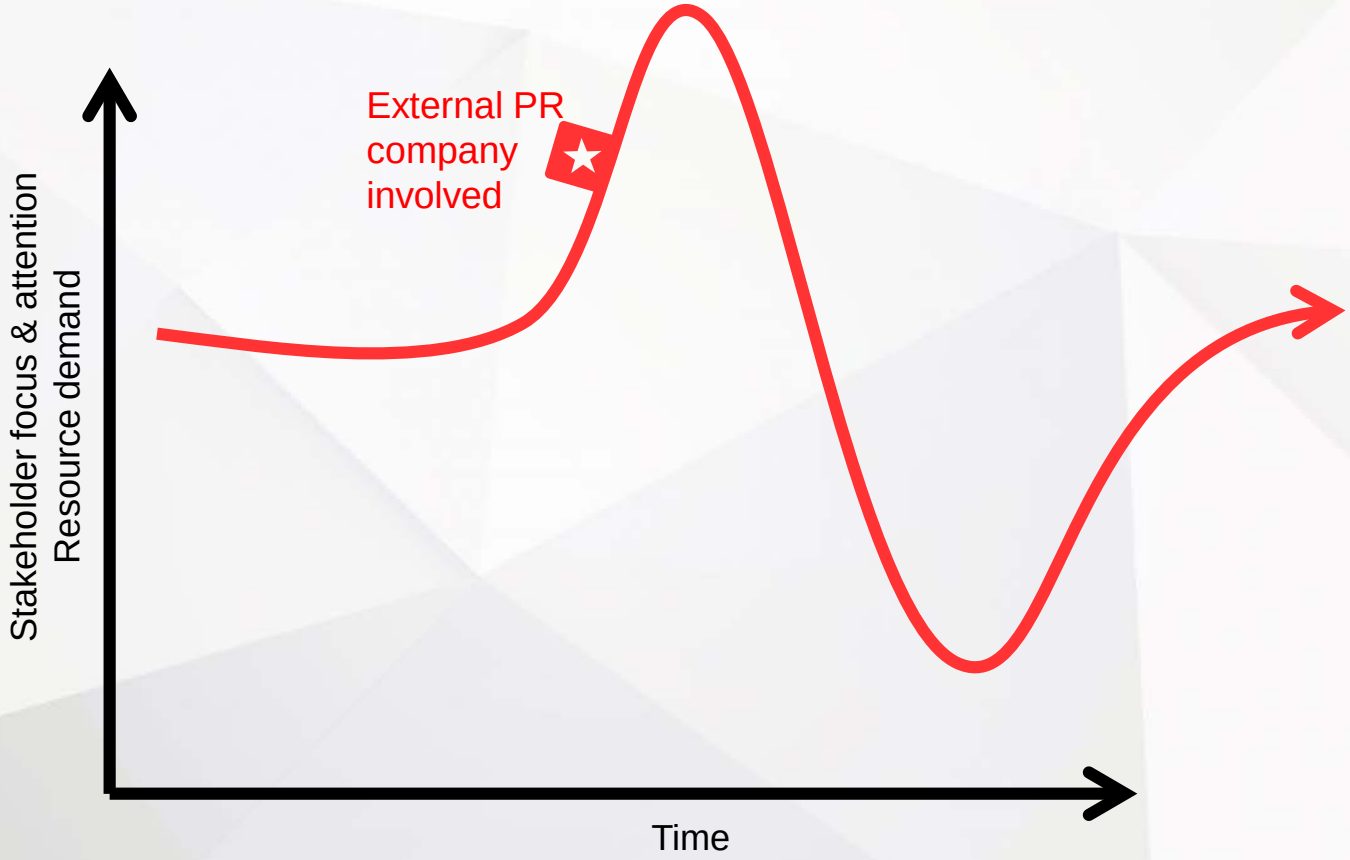
SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE



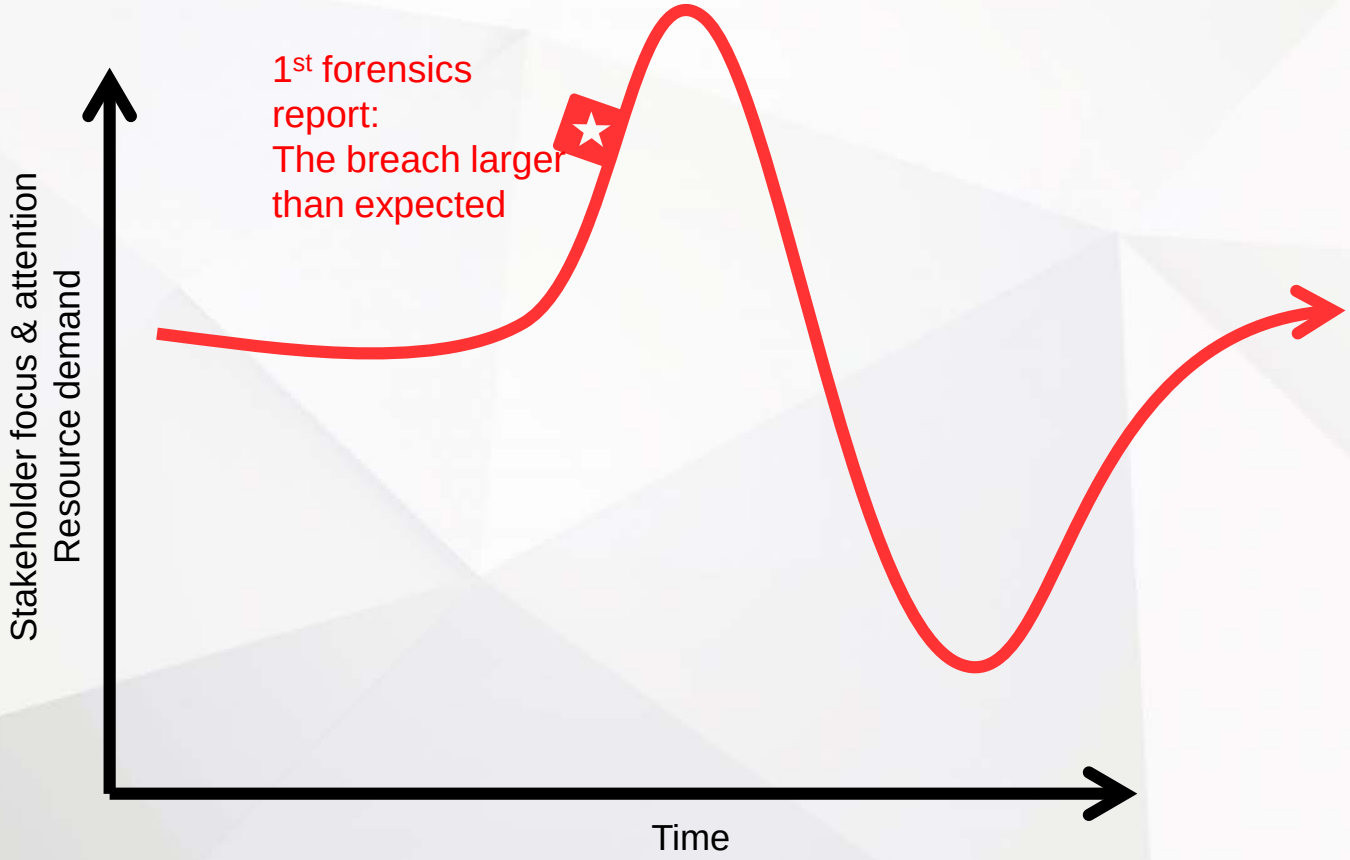
SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE



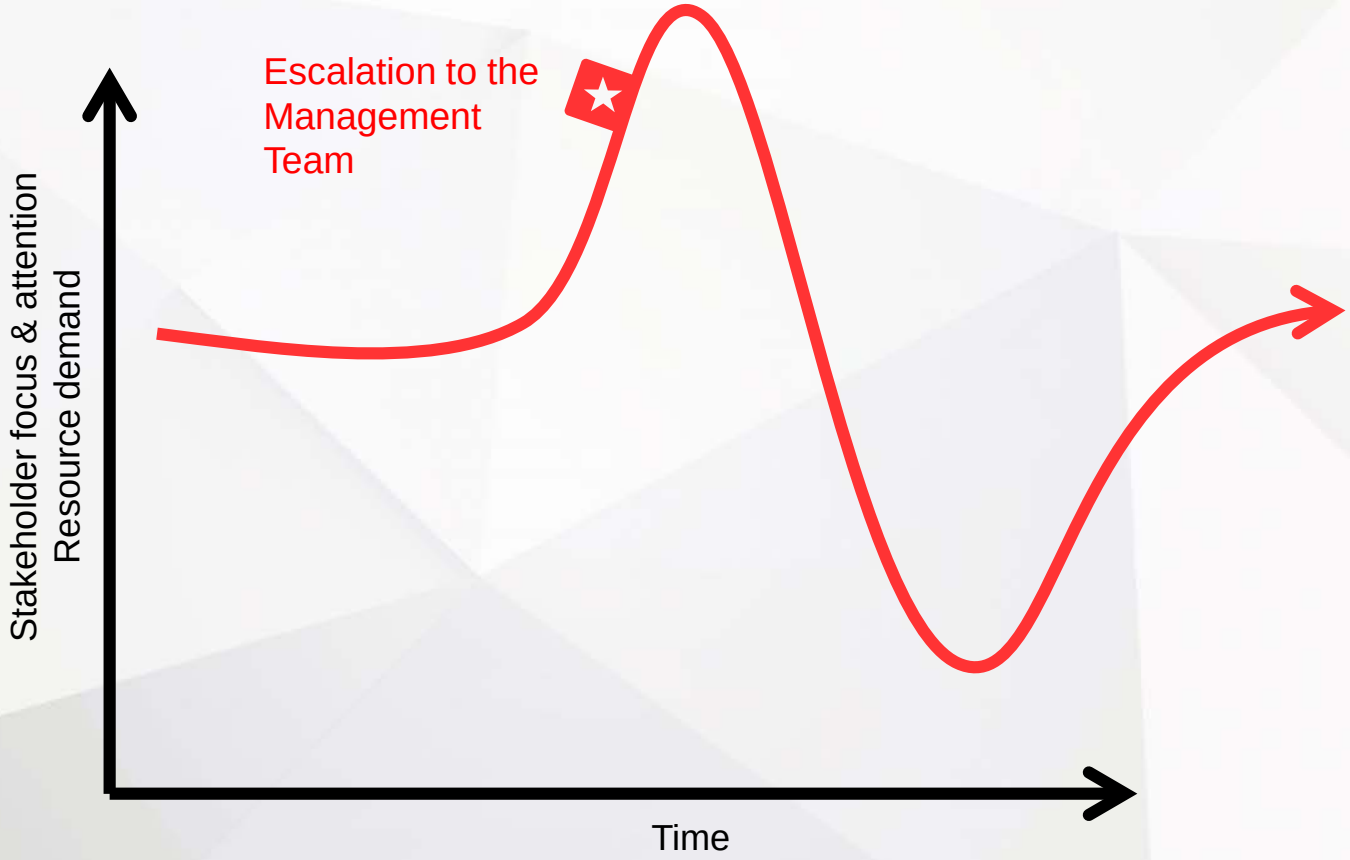
SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE



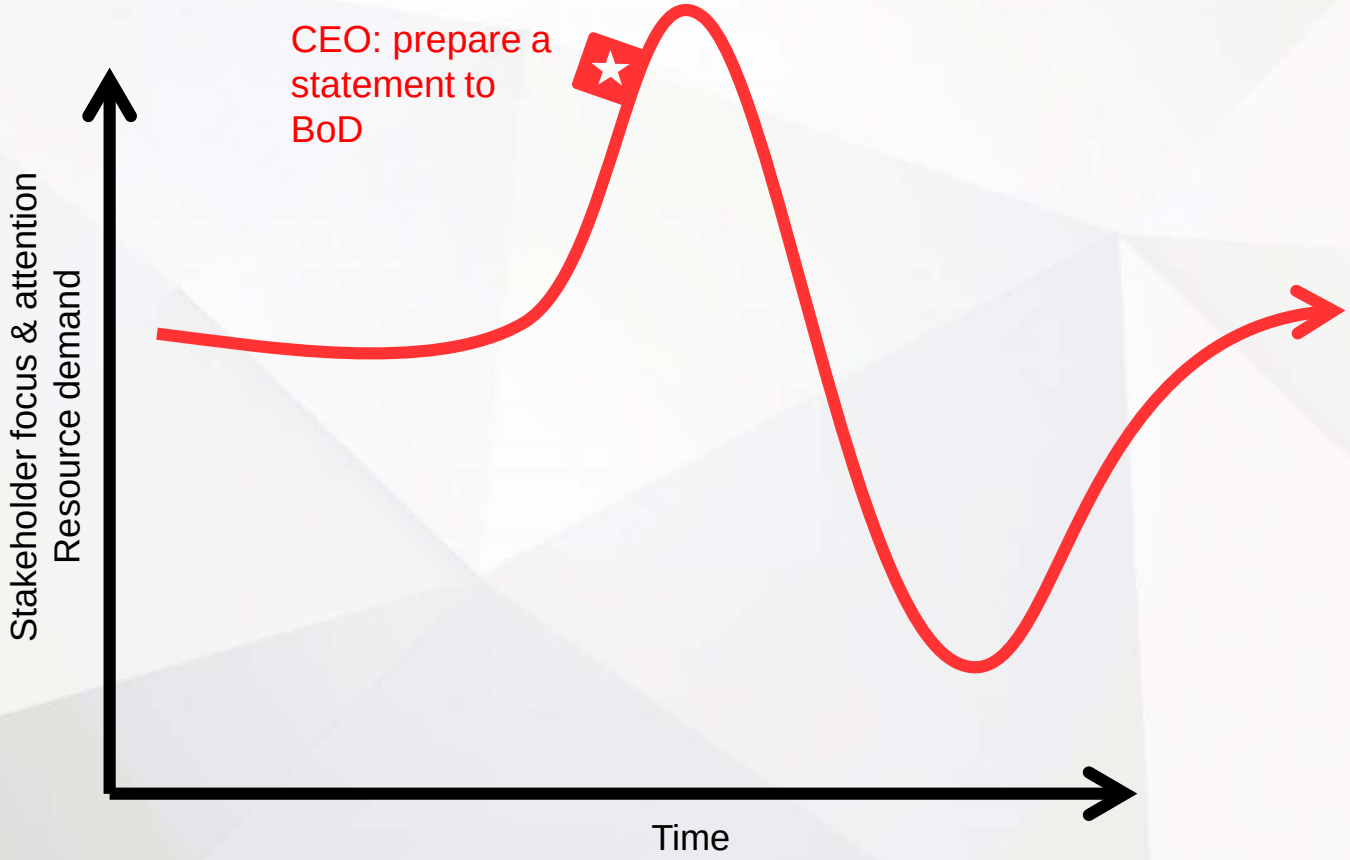
SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE



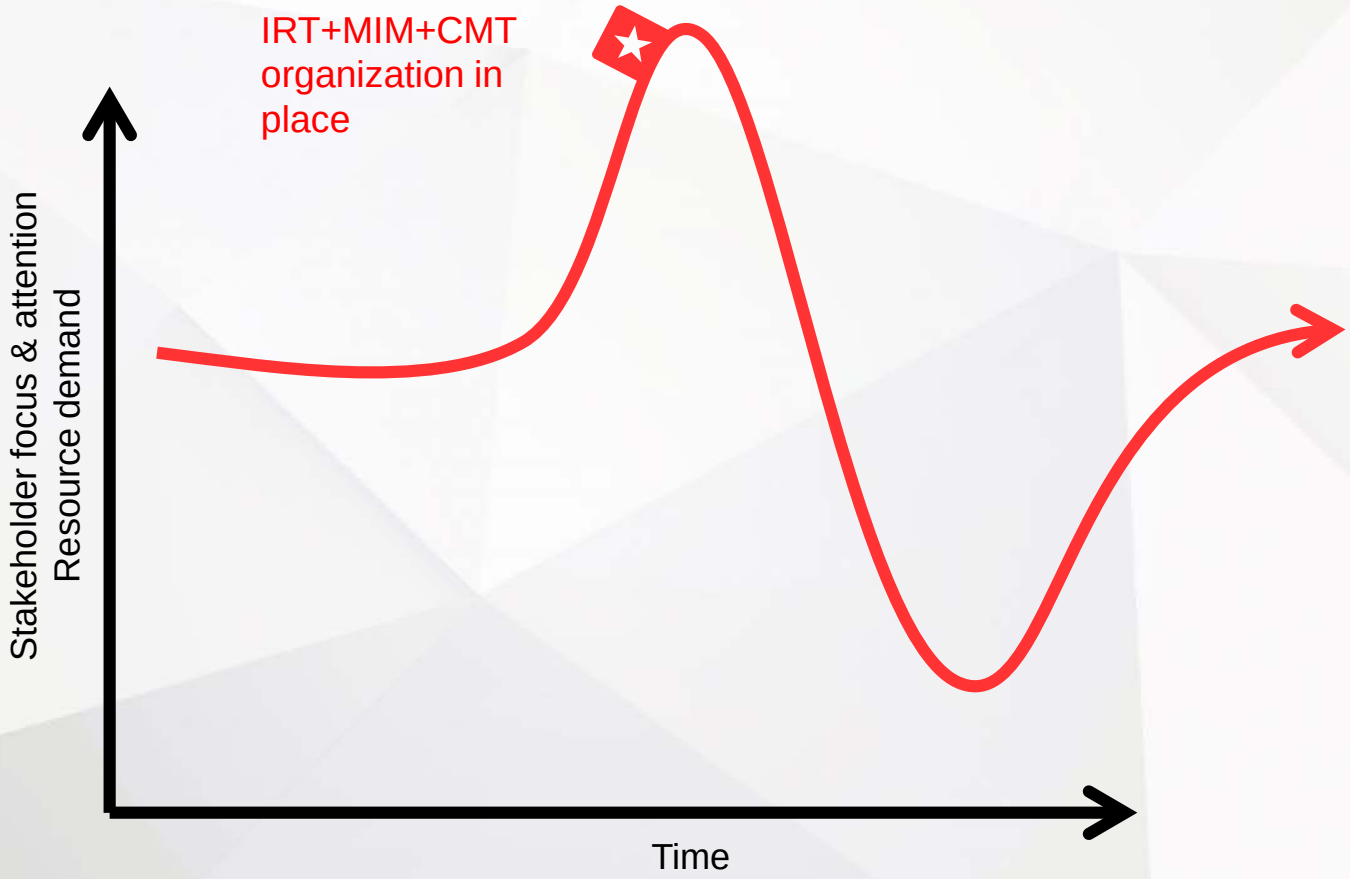
SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE



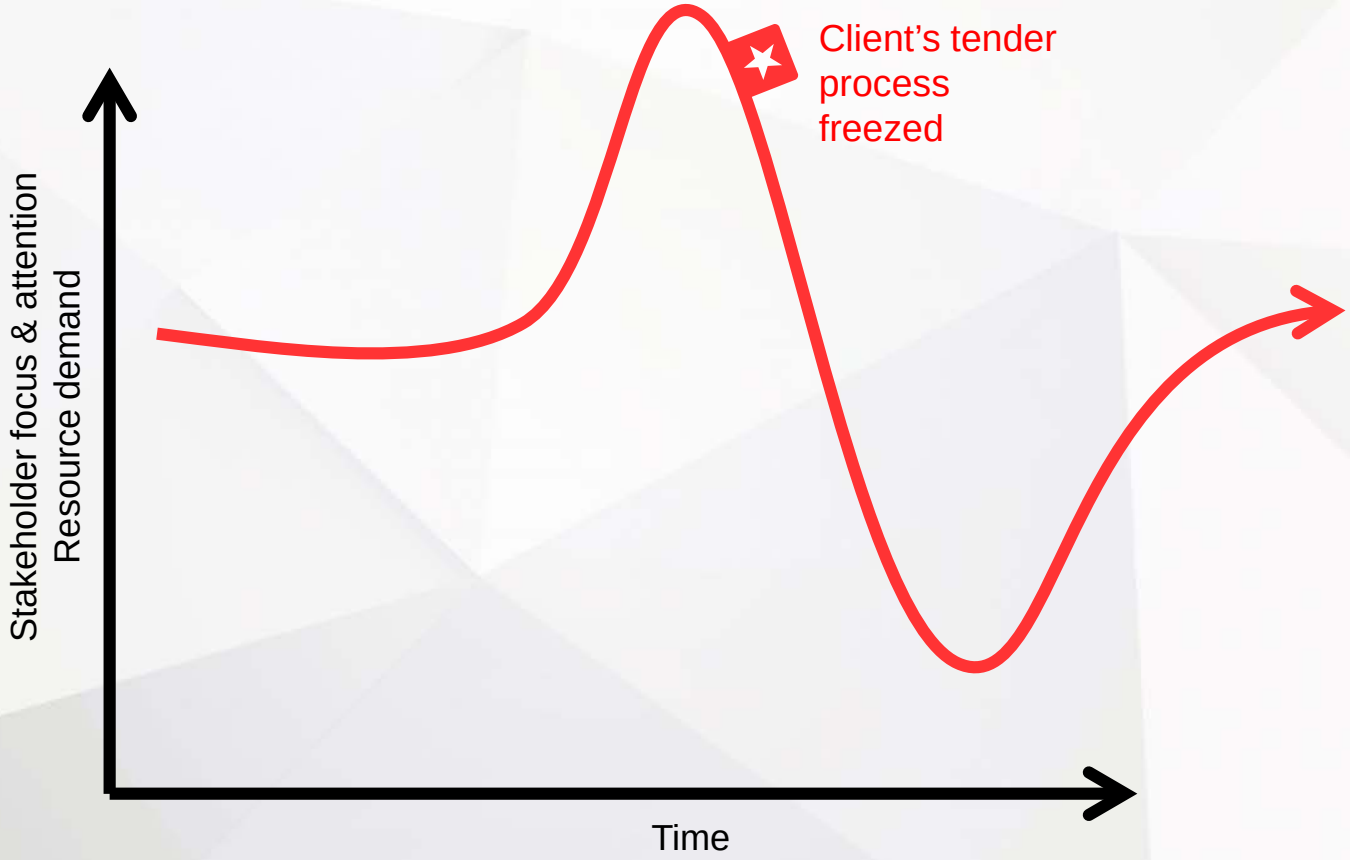
SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE



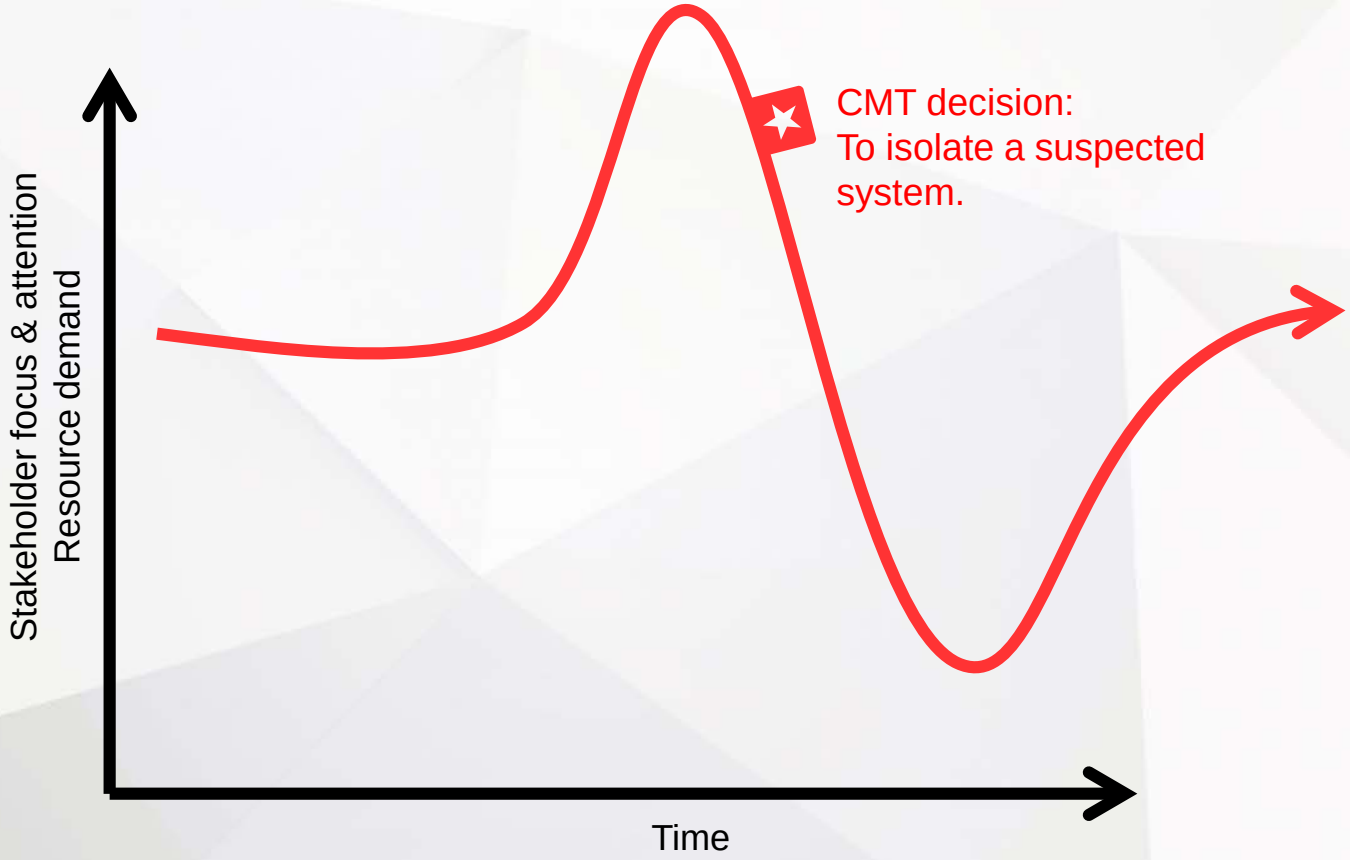
SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE



SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE

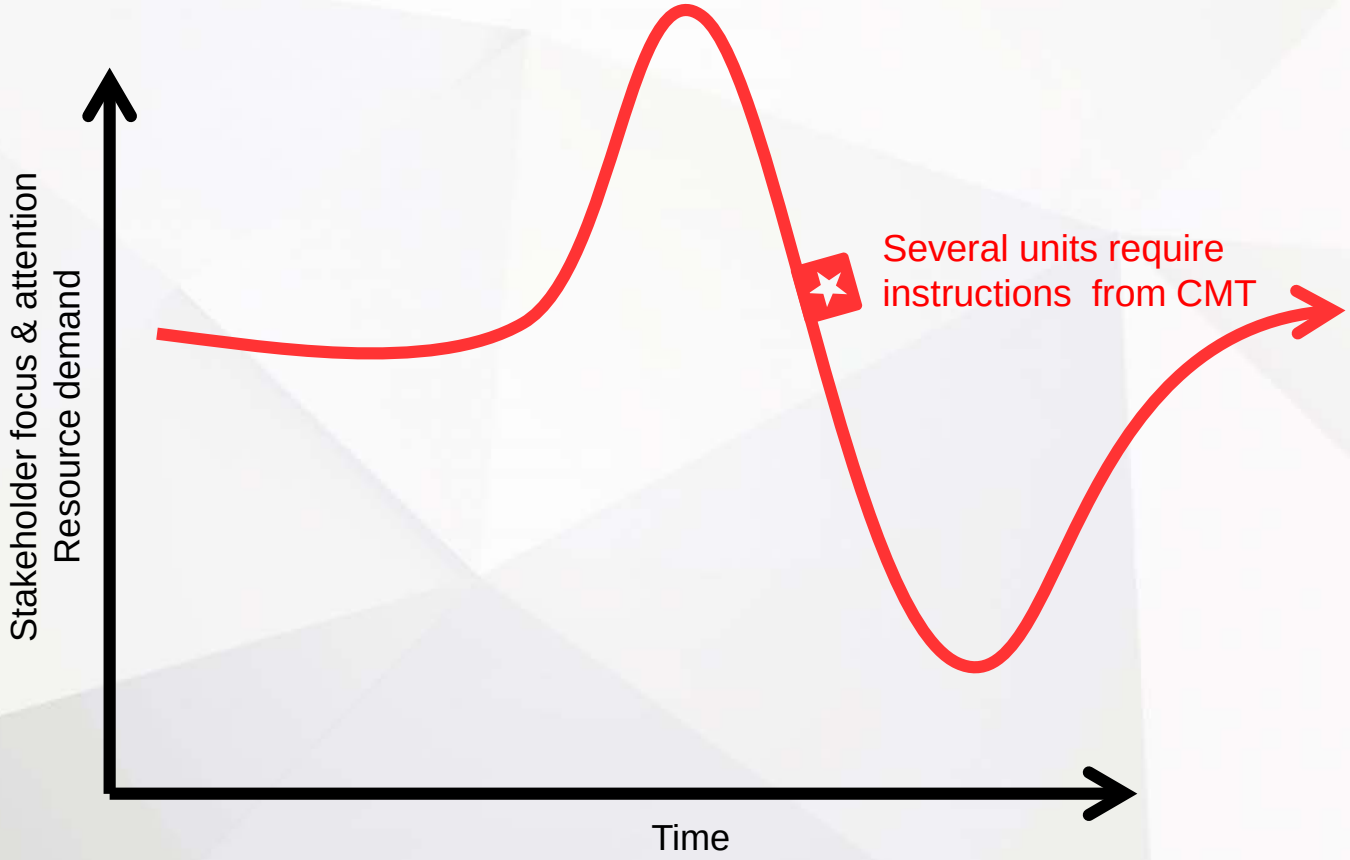


SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE

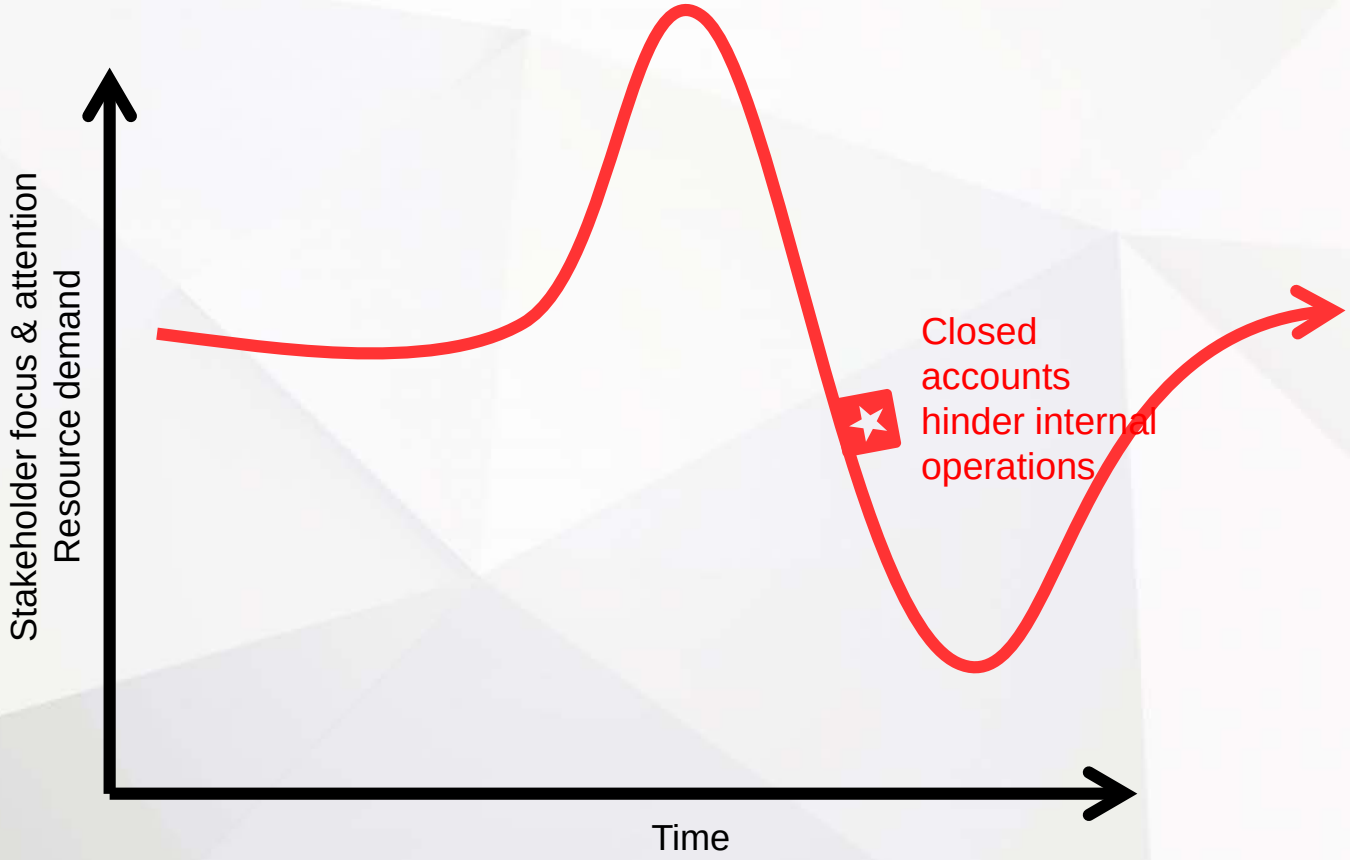


SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE

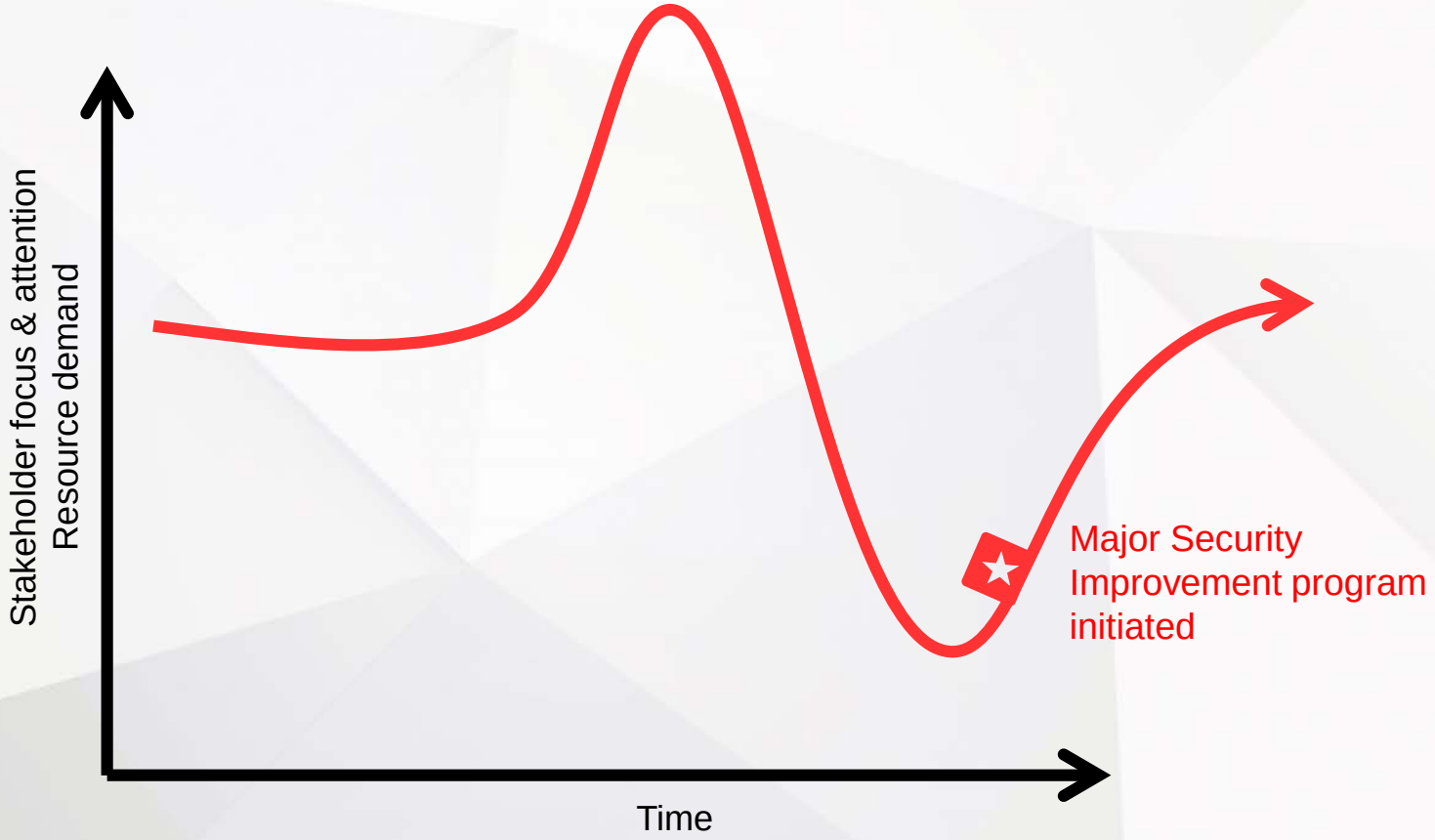
SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE



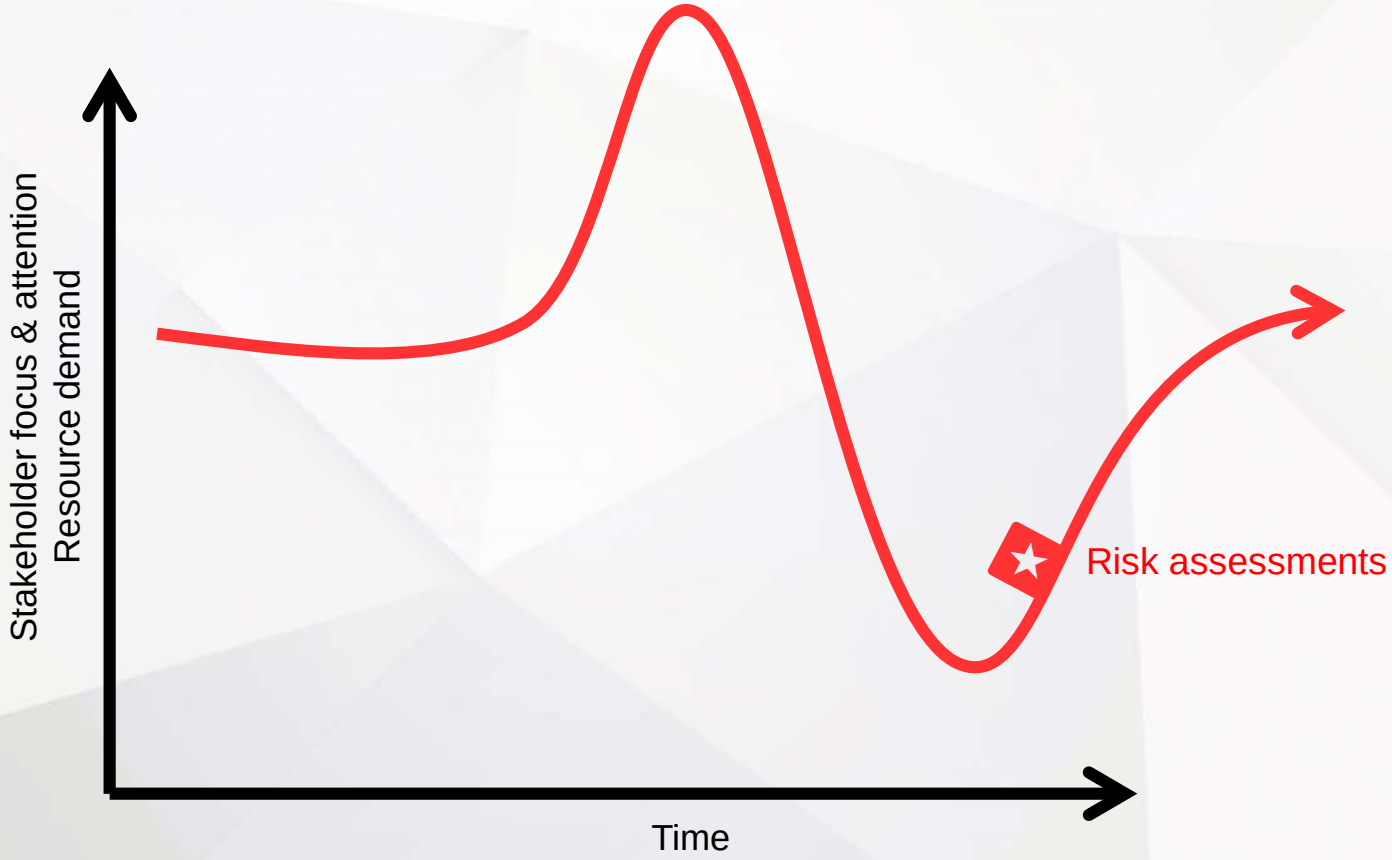
SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE



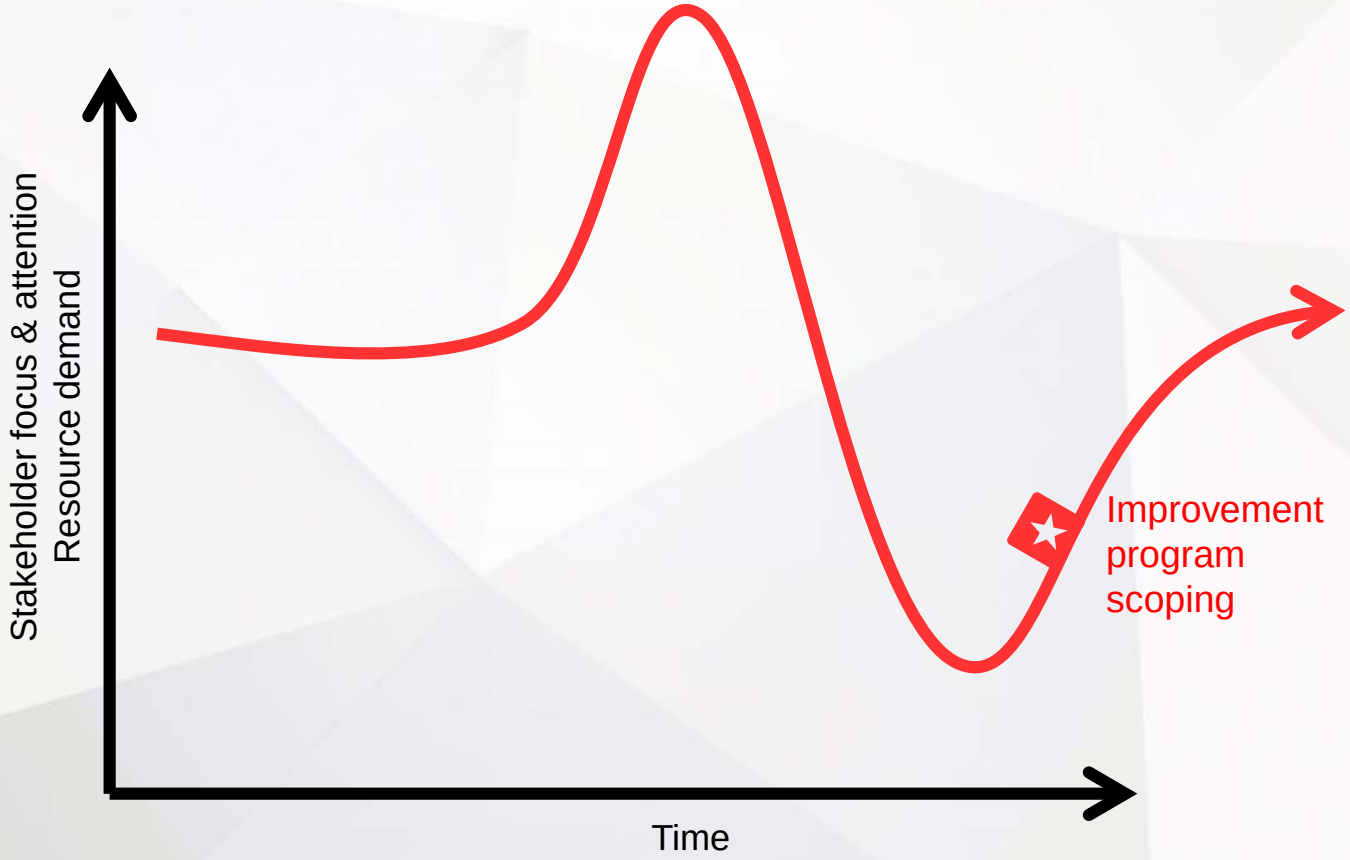
SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE



SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE



SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE



SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE

SUMMARY

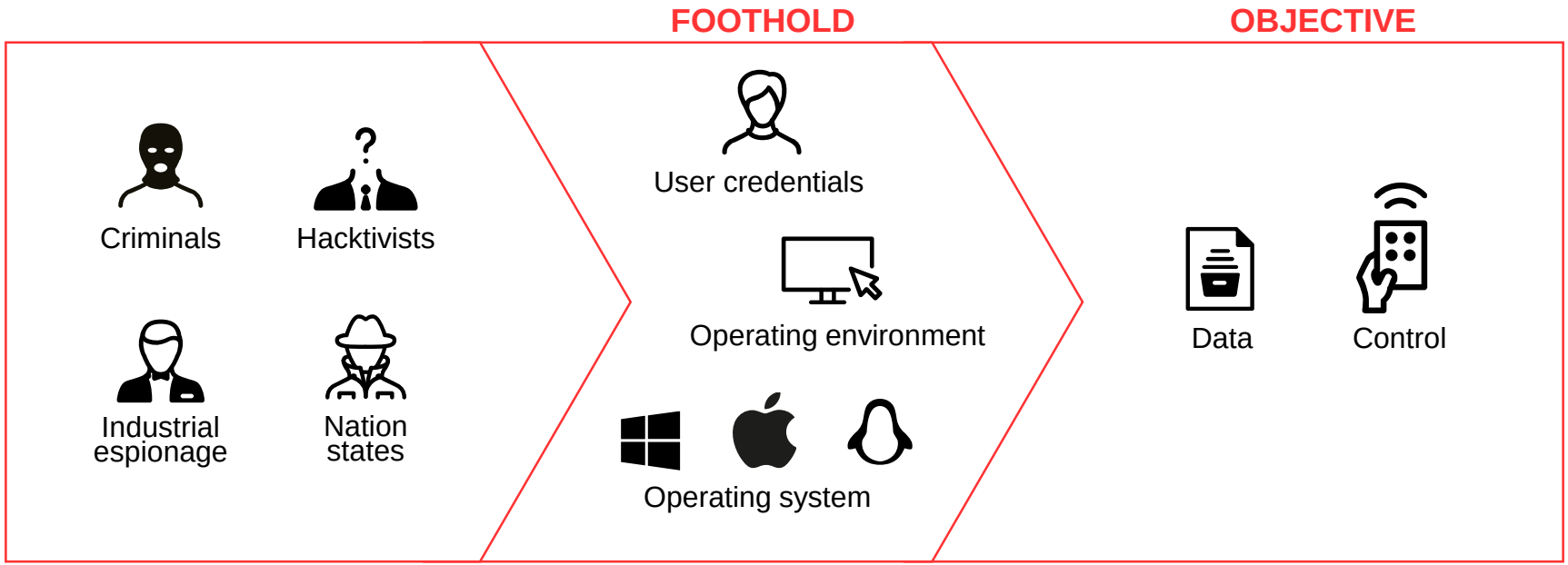
- Succesfull business makes you a potential target
- This case was a textbook example
- Although prepared, the level of business disruption came as a surprise
- You have firedrills – why not cyberdrills ?

HOW TO PREVENT A DATA BREACH

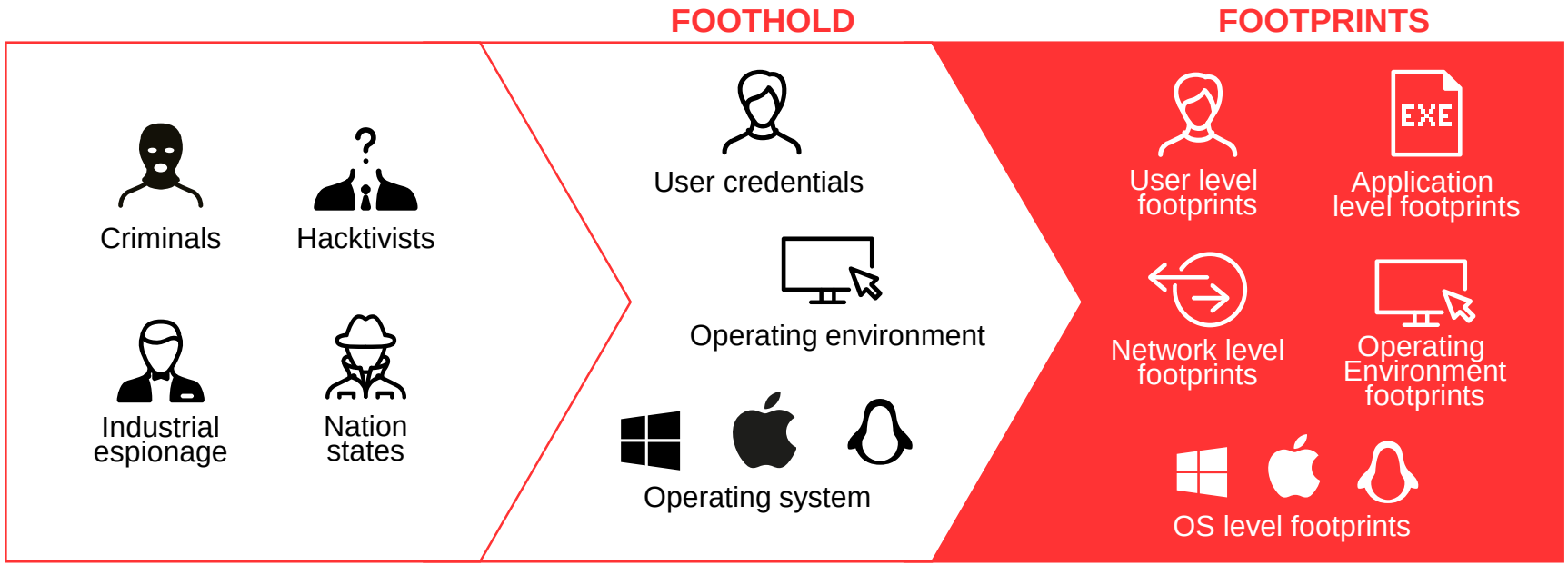
Marko
Finnig

ON AVERAGE IT TAKES TOO LONG TO REACT TO A BREACH

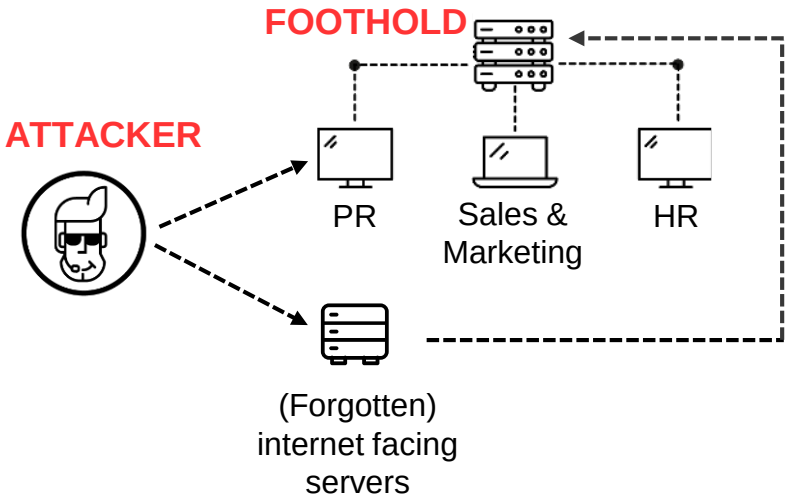
LETS LOOK AT HOW ATTACKERS OPERATE AND WHAT THEY ARE AFTER



IN THE PROCESS, THEY WILL ALWAYS LEAVE (SOMETIMES VERY SUBTLE) FOOTPRINTS



2 COMMON WAYS TO GAIN FOOTHOLD ARE VIA PUBLIC FACING EMPLOYEES AND (FORGOTTEN) SERVERS



99,9 % DO LITTLE DAMAGE

0,1 % DO THE MOST DAMAGE

Usually well covered by the current security solutions in organizations

- Address machine conducted attacks
  - Phishing & exploit (email as vector)
  - Ransomware
  - 99,9 % of the malware
- Solutions (Prevent):
  - Firewall
  - Email security
  - End-point protection
  - ..

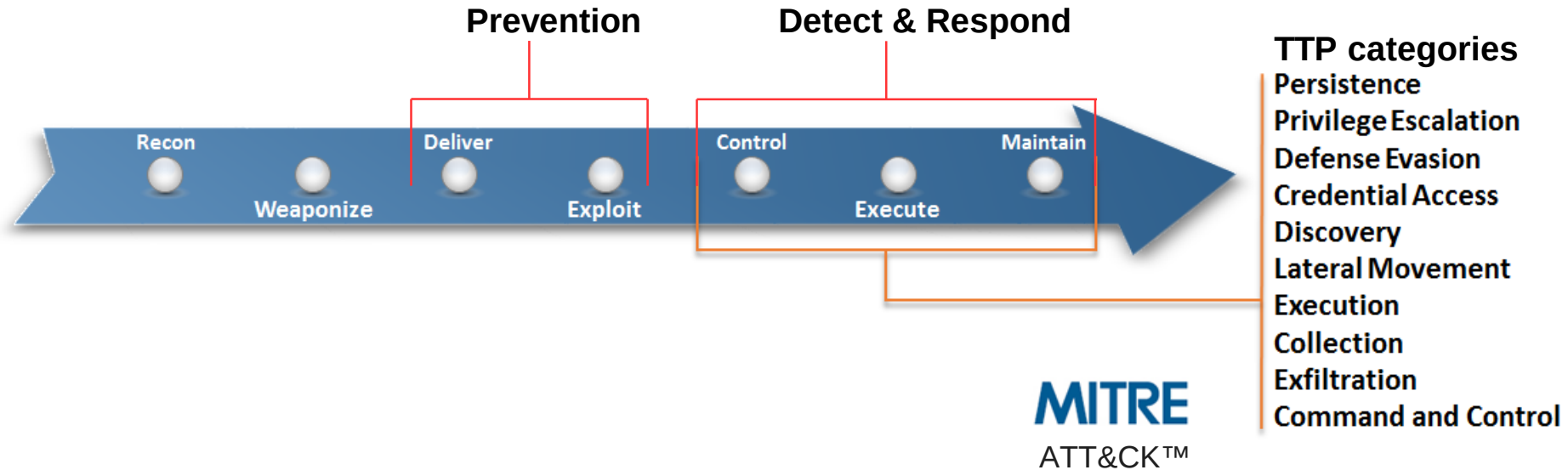
99,9 % DO LITTLE DAMAGE

Usually not covered at all by the current security solutions in organizations...

- Address human conducted attacks
  - Spear-Phishing & exploit (in-memory backdoor)
  - Use of system internals - PowerShell, WMIC, Service Commands ..
  - Use of remote admin tools (RAT) and hacking tools – Orcus, Litemanager, LuminosityLink, Mimikatz
  - Hide command & control traffic – Office365, GMail, HTTPS
- Solutions (Detect & Respond):
  - Managed Detection and Response (end-points)

0,1 % DO THE MOST DAMAGE

EXPAND YOUR CAPABILITIES TO DETECT TECHNIQUES TACTICS PROCEDURES USED BY SKILLED ADVERSARIES



F-Secure

PREVENTION AND DETECTION & RESPONSE APPROACHES ARE FUNDAMENTALLY DIFFERENT

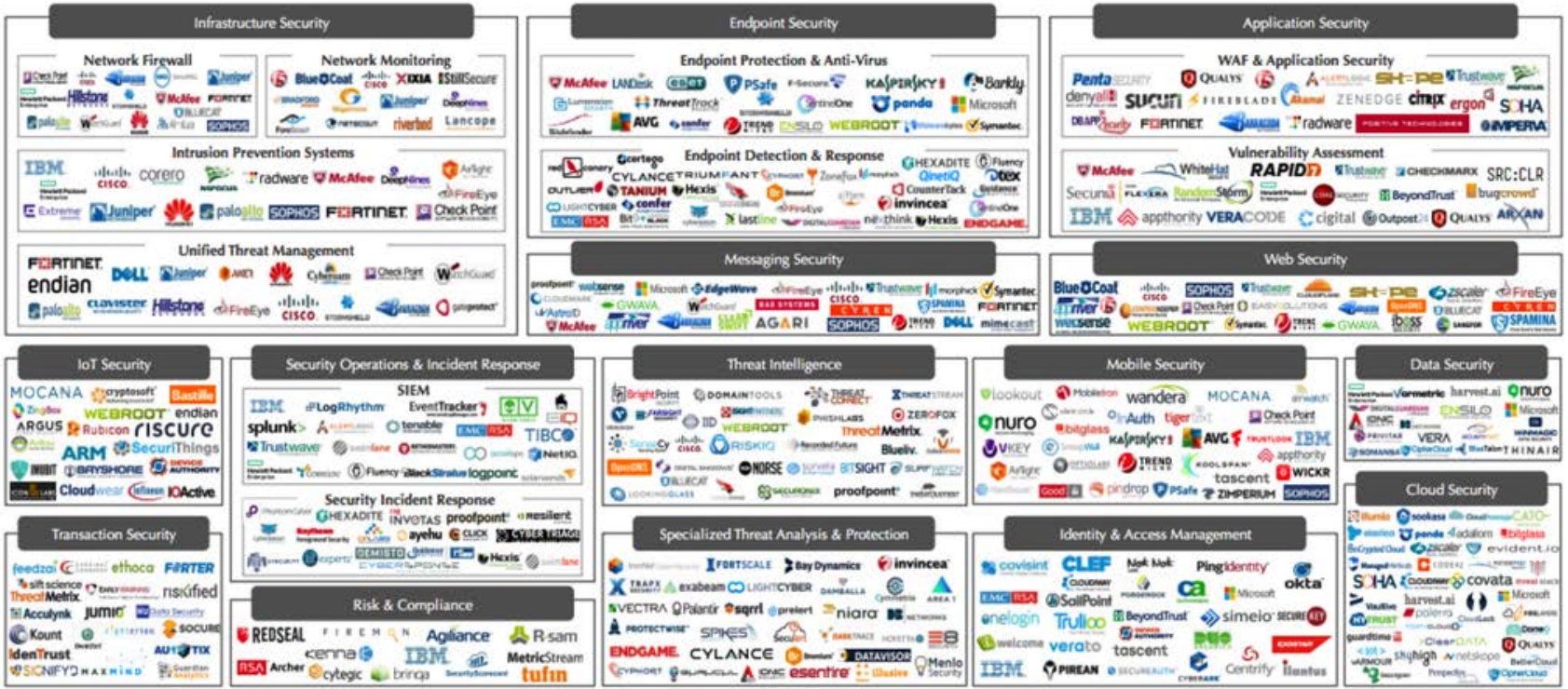
PREVENTION:

- Defenders dilemma: Be right every time, attacker needs to be right only once. Products can be bought and tested by the attacker.

DETECTION & RESPONSE:

- Attackers dilemma: Be right every time, defender needs to be right only once. Services cannot be bought and tested by the attacker.

HOW DO YOU EVALUATE ALL THESE OPTIONS?



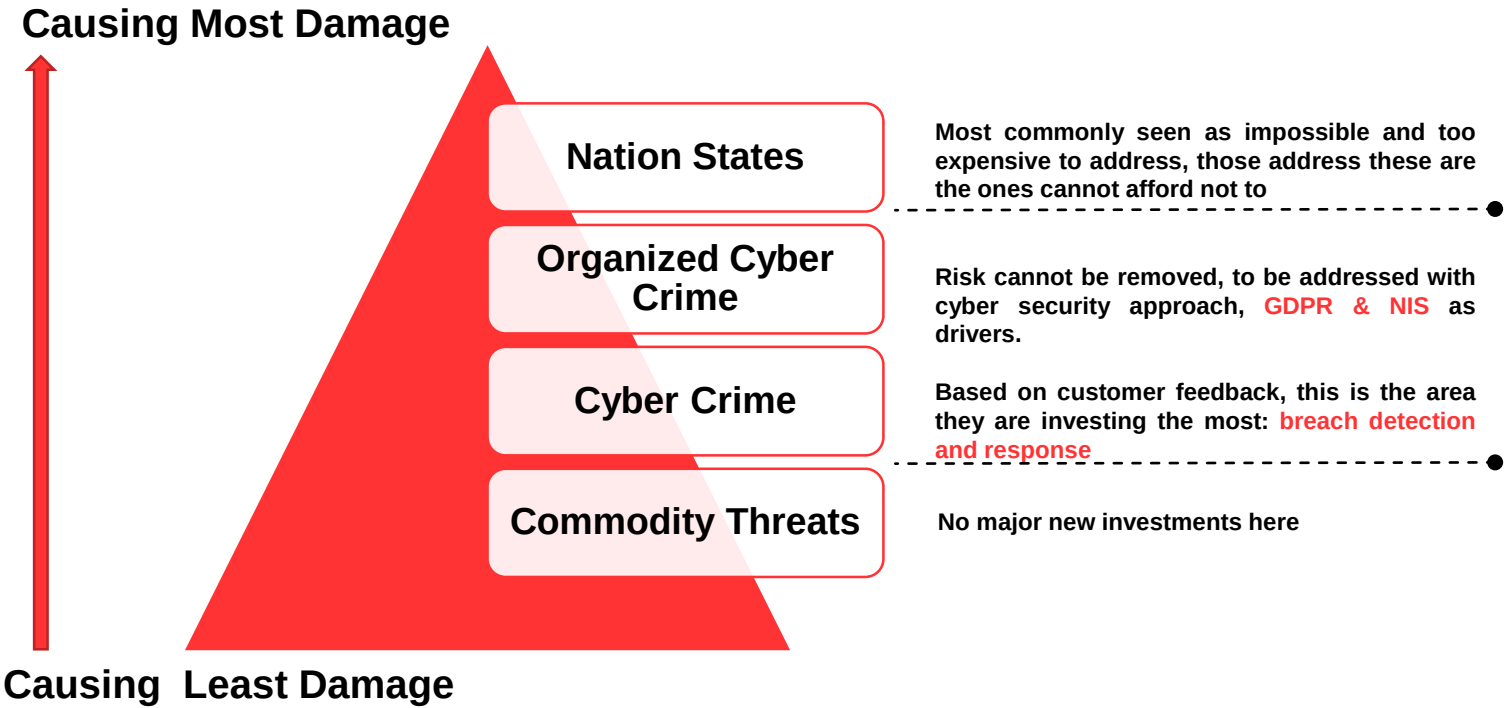
F-Secure.

..OR HOW DO YOU EVEN KNOW HOW GOOD YOUR EXISTING DEFENCES ARE?

THE ONLY WAY TO KNOW FOR SURE IS TO RUN DRILLS

F-Secure

SEPARATE THREAT ACTORS INTO GROUPS TO SUPPORT INVESTMENTS



Most commonly seen as impossible and too expensive to address, those address these are the ones cannot afford not to

Risk cannot be removed, to be addressed with cyber security approach, GDPR & NIS as drivers.

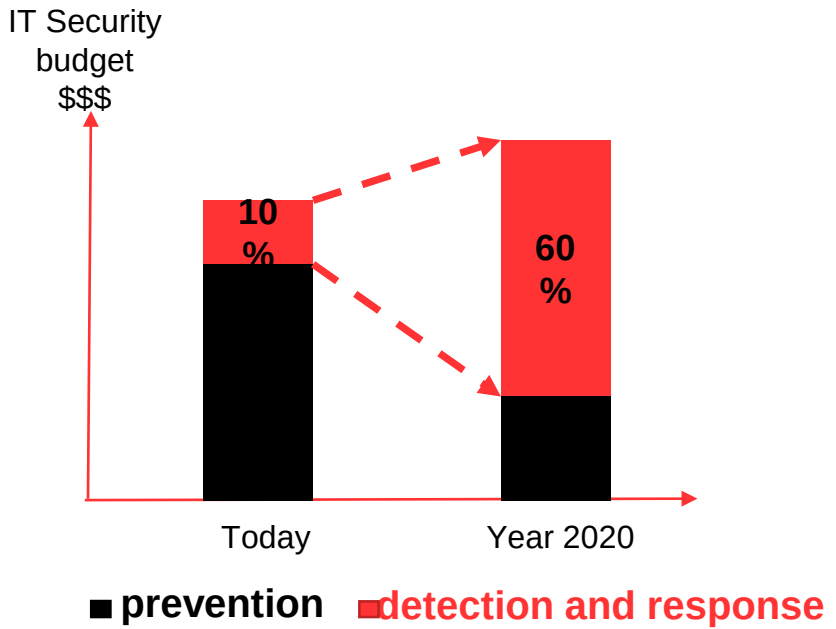
Based on customer feedback, this is the area they are investing the most: breach detection and response

No major new investments here

LARGE SHIFT FROM PREVENTION TO DETECTION AND RESPONSE APPROACHES

Gartner: By 2020, **60 percent** of enterprise information security budgets will be allocated for **rapid detection and response** approaches

Source: Gartner Special Report 'Cybersecurity at the Speed of Digital Business'



SUMMARY

1. Separate threat actors in risk management to support investments
2. Map your “foothold” areas and
3. Extend your capabilities to cover TTPs (with D&R approaches)
4. Establish recurring red vs. blue drill practice

f-secure.com

SWITCH ON FREEDOM