Stake at the heart

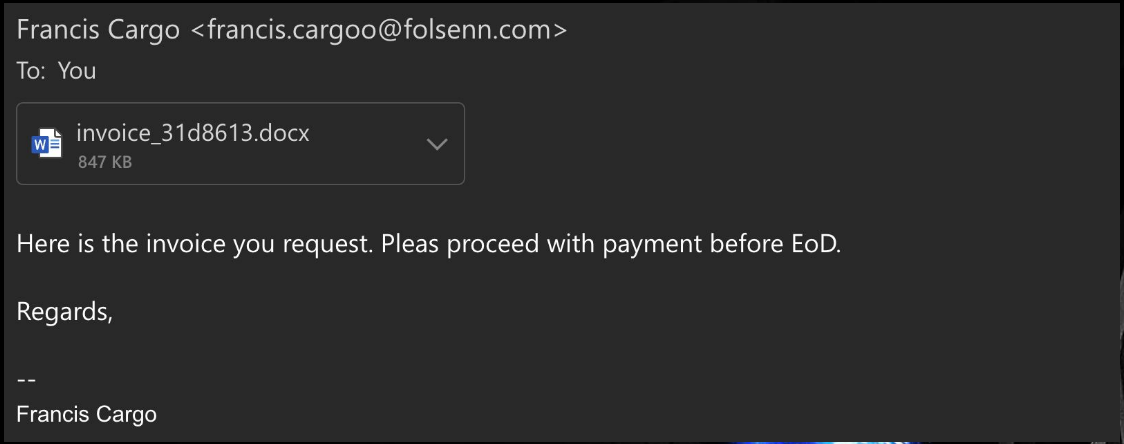
Destroying common security wisdom

Ayoub EL AASSAL

Disclaimer

The opinions expressed during this presentation are my own and do not necessarily reflect those of my current employer or any other affiliated organization. The information and advice shared here are based on my personal experience and expertise in the field of cybersecurity and should not be considered as an official position of my employer.

“Humans are the weakest link in cyber security”



Francis Cargo <francis.cargoo@folsenn.com>

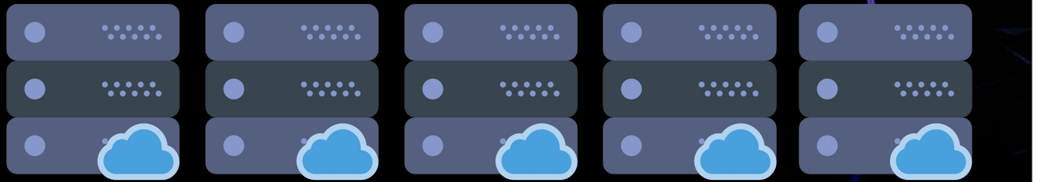
To: You

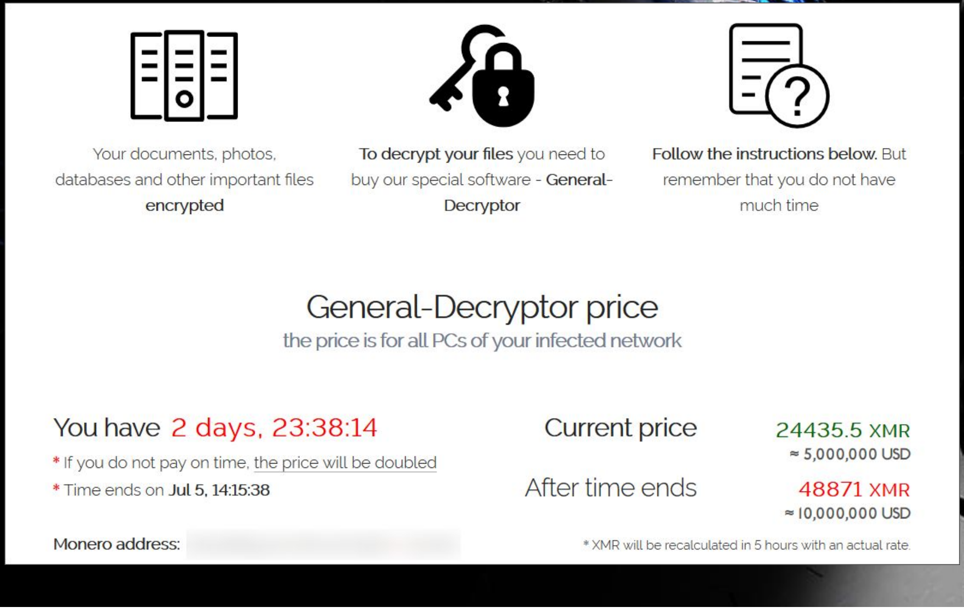
Here is the invoice you request. Pleas proceed with payment before EoD.

Regards,

--

Francis Cargo





Your documents, photos, databases and other important files **encrypted**

To decrypt your files you need to buy our special software - **General-Decryptor**

Follow the instructions below. But remember that you do not have much time

General-Decryptor price

the price is for all PCs of your infected network

You have 2 days, 23:38:14

* If you do not pay on time, the price will be doubled

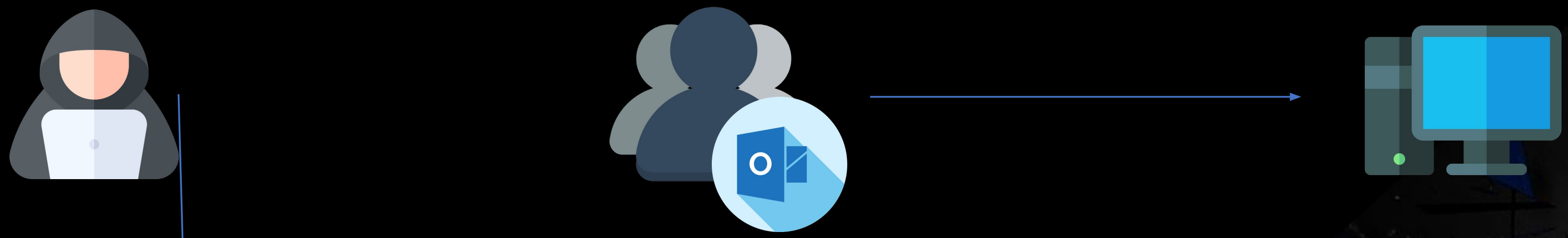
* Time ends on **Jul 5, 14:15:38**

Current price	24435.5 XMR ≈ 5,000,000 USD
After time ends	48871 XMR ≈ 10,000,000 USD

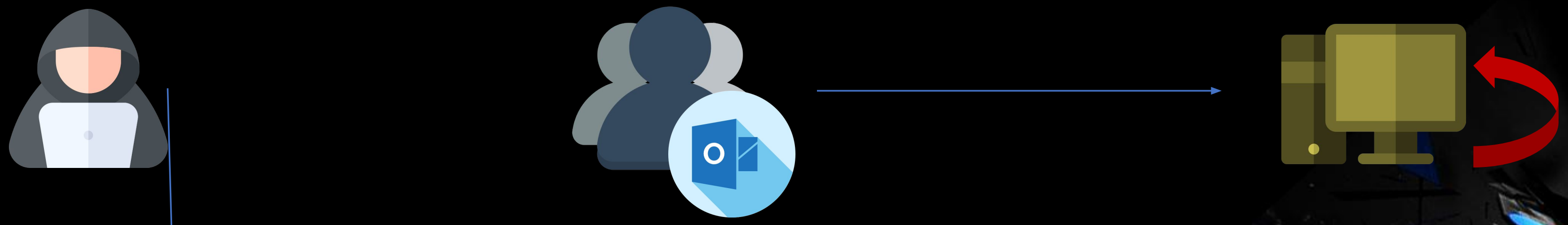
Monero address: [redacted]

* XMR will be recalculated in 5 hours with an actual rate.

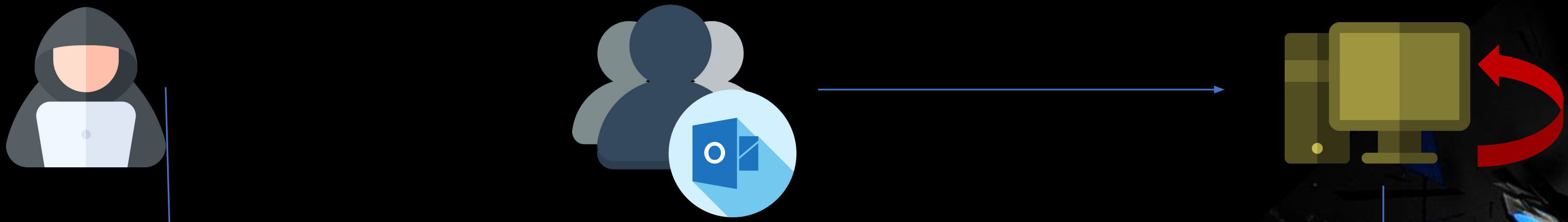
- *What about Spam filters?*
- *Sandbox analysis?*



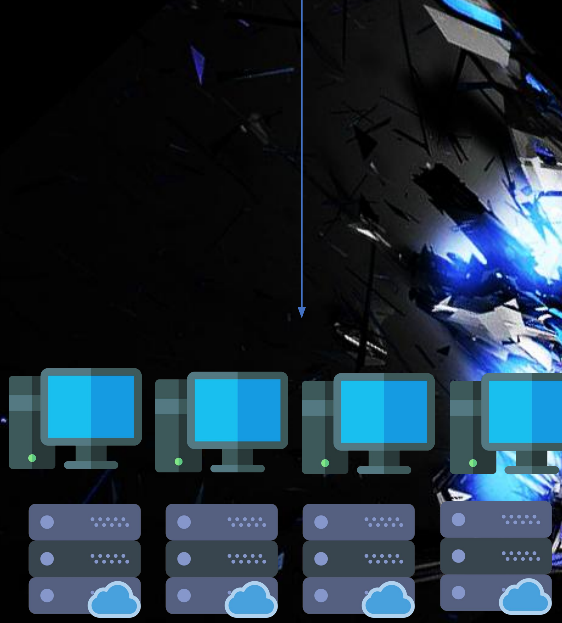
- *Lack of logical isolation?*
- *Full access to the underlying OS' APIs from a text document*
- *EDR/AV bypass or lack there of*

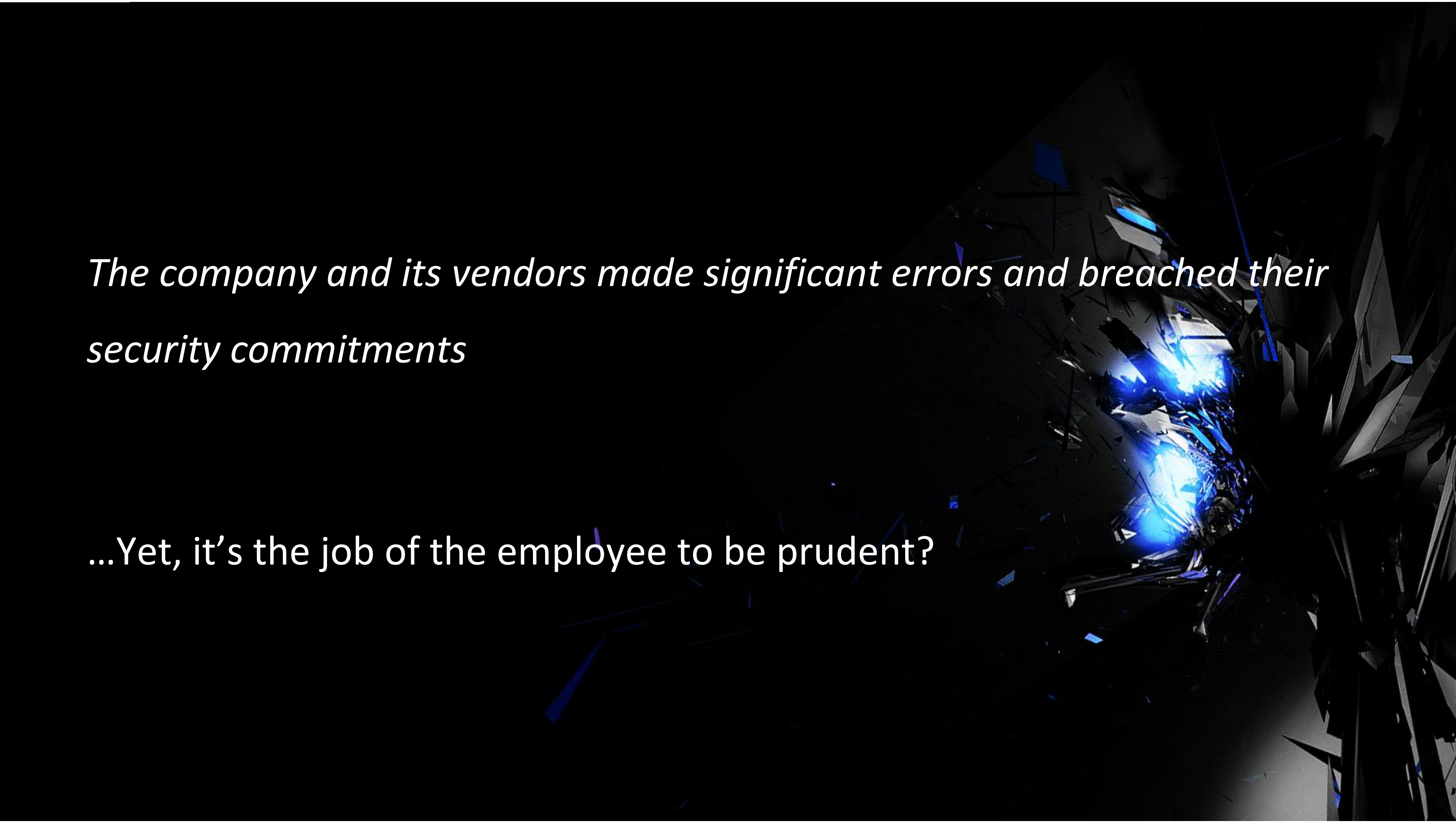


- *Lack of patching or even availability of a patch*
- *Bypass any system detection/protection*



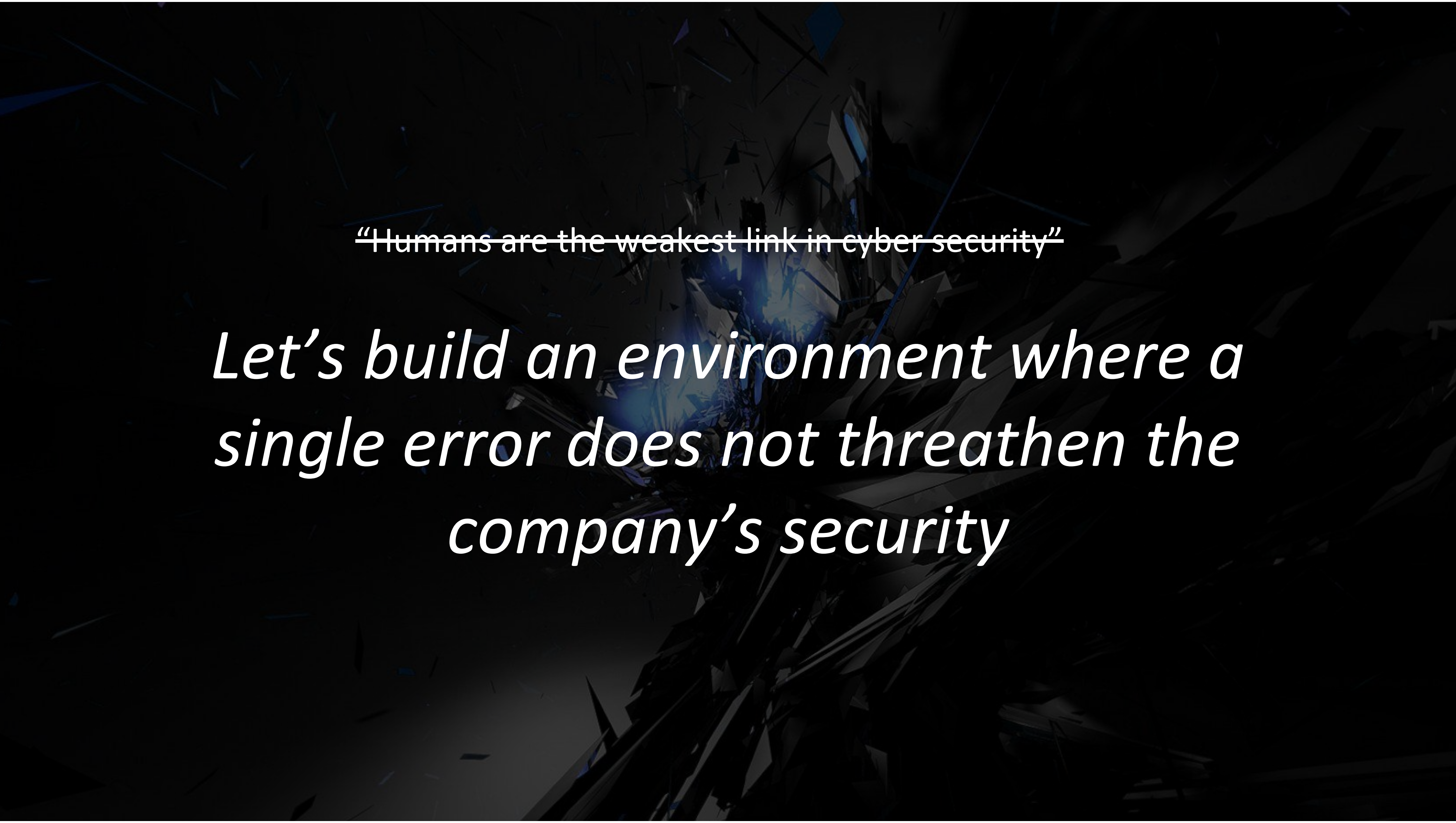
- *No network isolation*
- *Same password everywhere*
- *Clear text protocols*
- *Broken authentication protocols*
- *No detection of unusual behavior*
- *Etc.*





The company and its vendors made significant errors and breached their security commitments

…Yet, it’s the job of the employee to be prudent?



~~“Humans are the weakest link in cyber security”~~

Let’s build an environment where a single error does not threathen the company’s security

“The job of the security team is finding vulnerabilities”

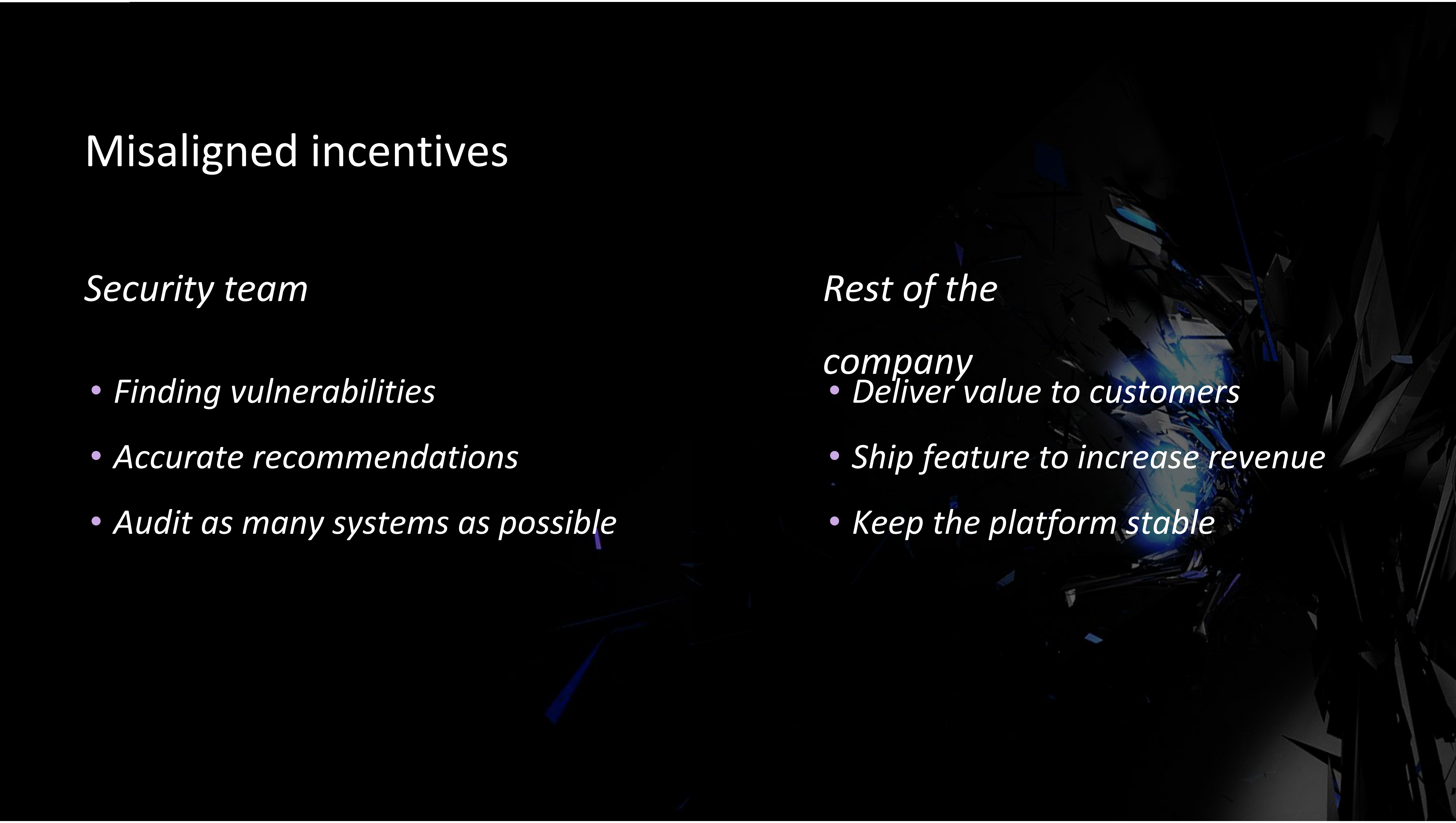
A common operating system in security:

- *Second/third line of defense*
- *Auditing systems and processes*
- *Pages of vulnerabilities and recommendations*

…Of course after 2 years, barely anything changes

An auditor’s paradox

Pointing vulnerabilities brings zero value to the customer of that business



Misaligned incentives

Security team

- *Finding vulnerabilities*
- *Accurate recommendations*
- *Audit as many systems as possible*

Rest of the company

- *Deliver value to customers*
- *Ship feature to increase revenue*
- *Keep the platform stable*

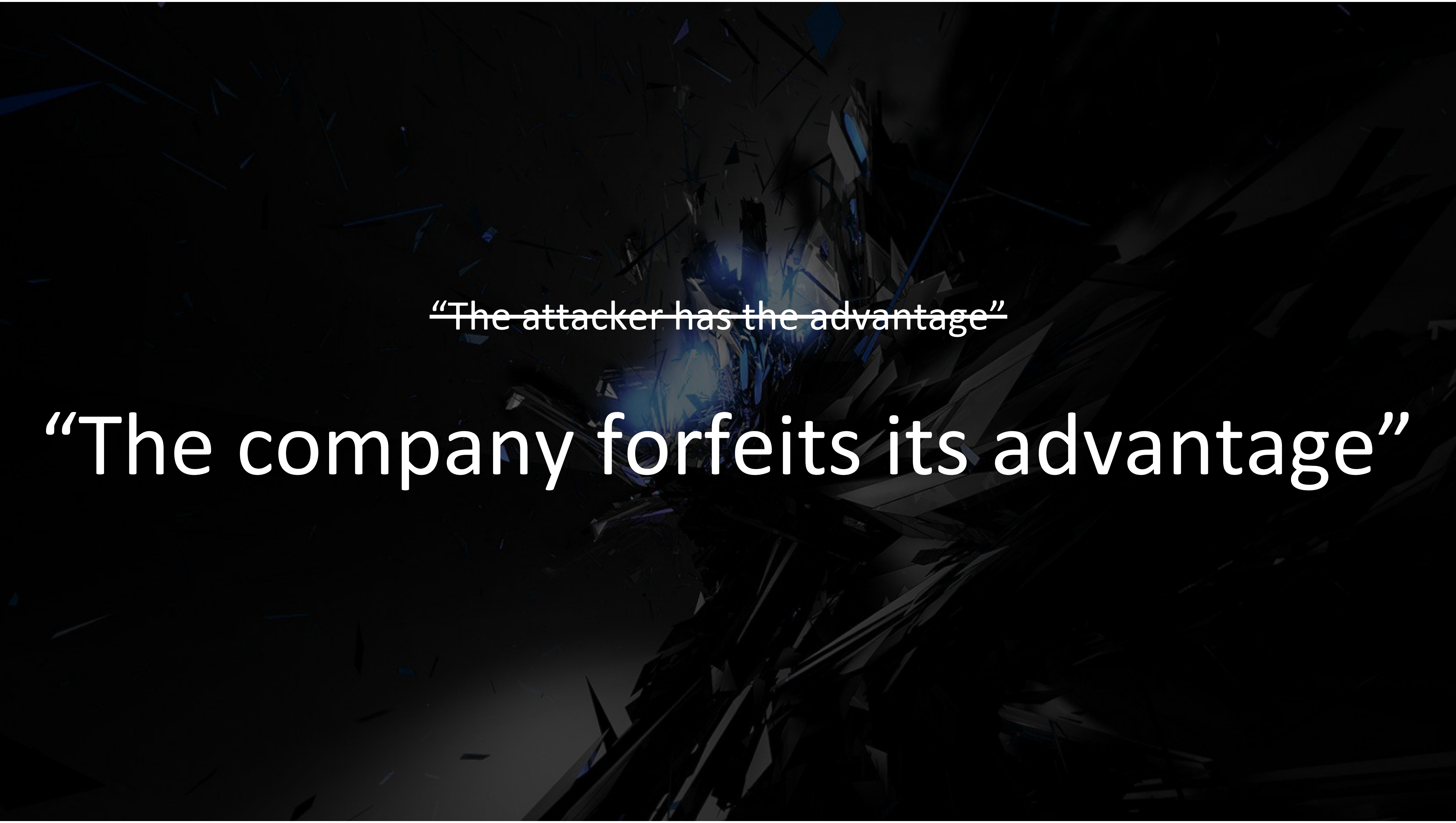
We need to align our goals

- *Yes to auditing systems but…*
- *Security team with a mandate to fix vulnerabilities*
- *Ownership of projects*

~~“The job of the security team is finding vulnerabilities”~~

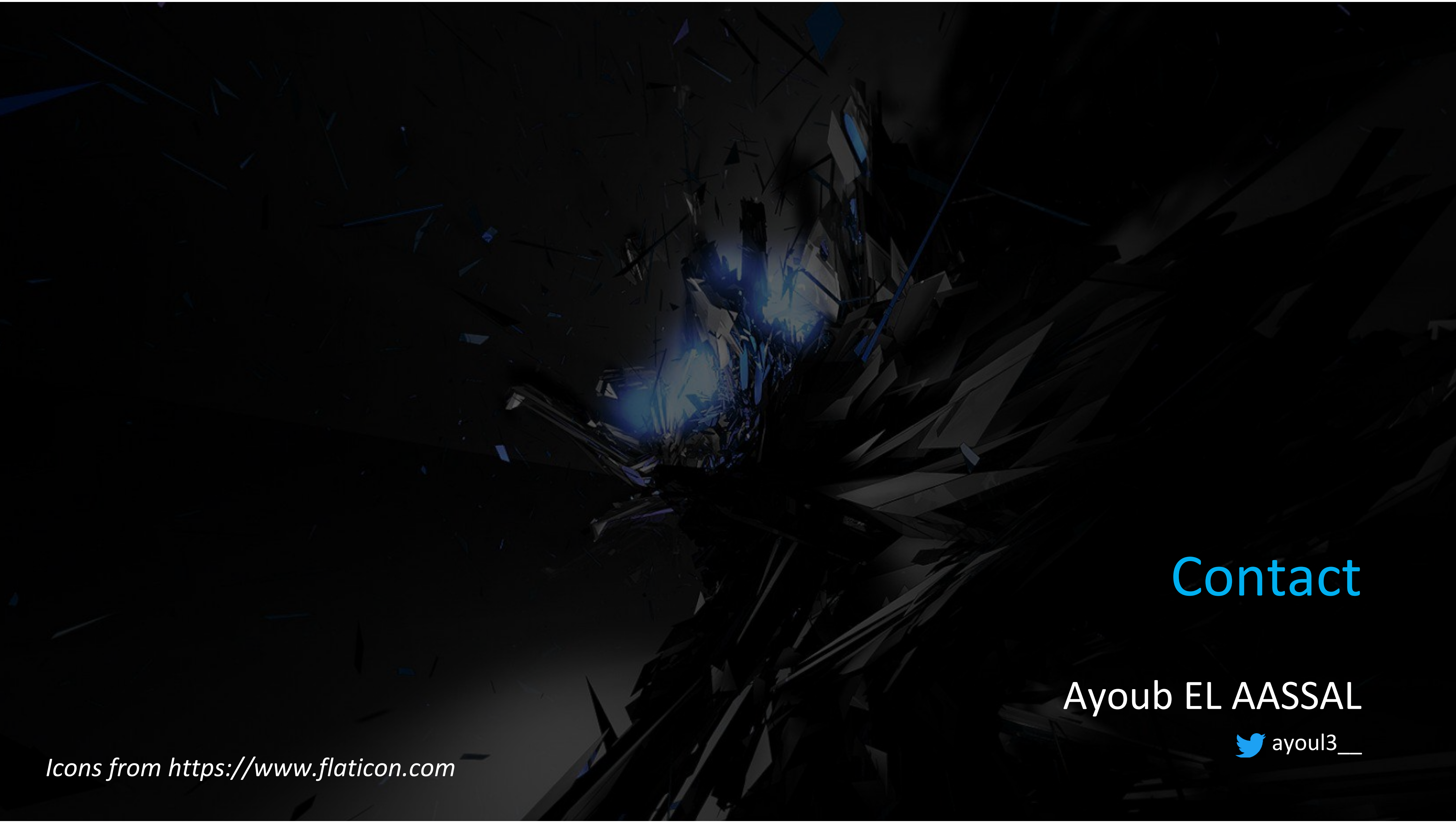
The job of the security team is to fix vulnerabilities

“The attacker has the advantage”



~~“The attacker has the advantage”~~

“The company forfeits its advantage”



Contact

Ayoub EL AASSAL

ayoul3__

Icons from https://www.flaticon.com