WAVESTONE

#Ransomware

Fighting back against ransomware

How tier-1 companies approach it

Gérôme BILLOIS
Partner
gerome.billois@wavestone.com
(+33) 6 10 99 00 60
@gbillois

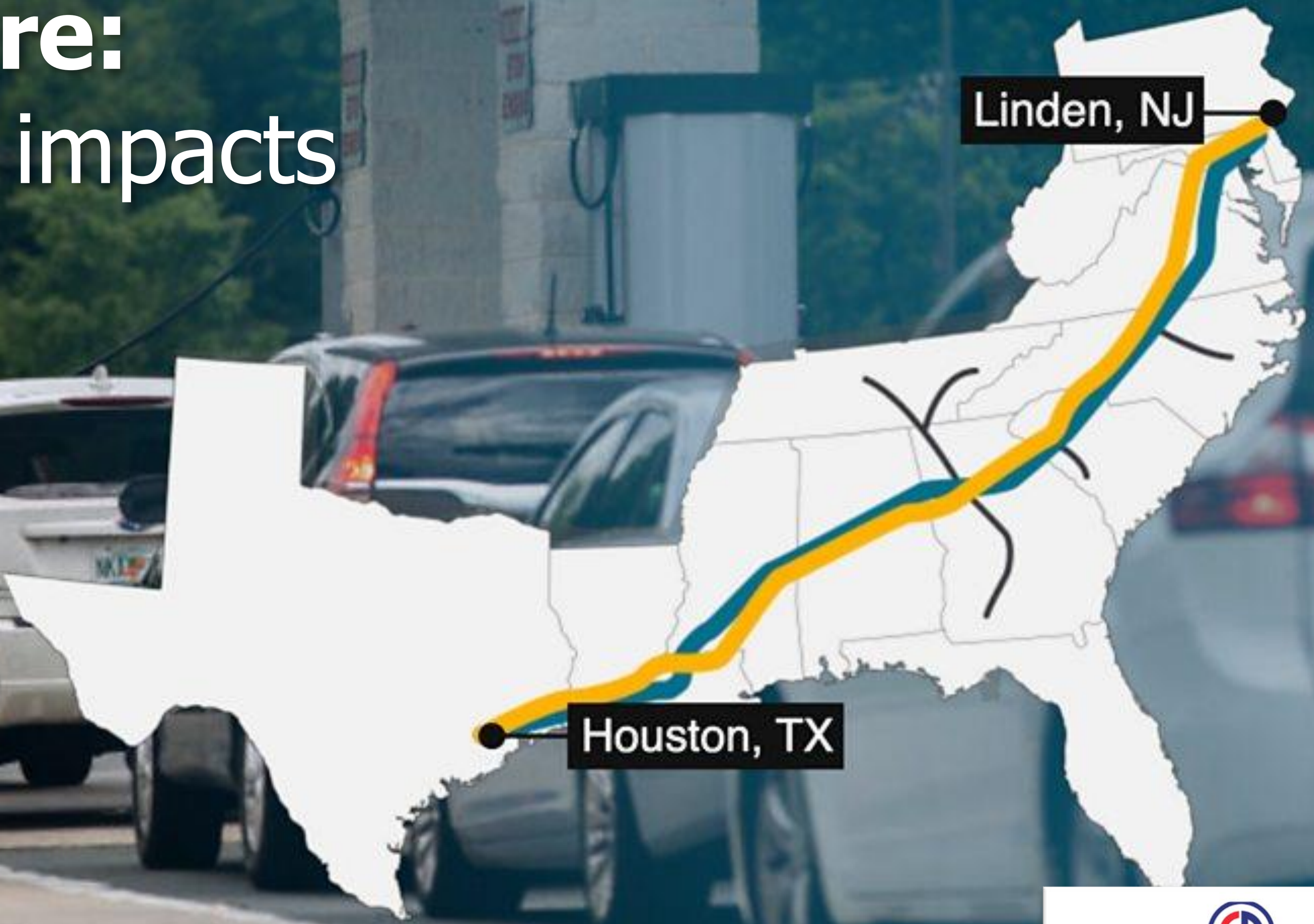
Matthieu GARIN
Partner
matthieu.garin@wavestone.com
(+33) 6 23 15 31 95
@matthieugarin

QUESTIONS? COMMENTS?
my.beekast.com/assises20

Ransomware:
From a SME concern to a critical infrastructure topic

COLONIAL PIPELINE CO.

Ransomware:
with real life impacts



COLONIAL PIPELINE CO.

Questions? Comments?
my.beekast.com/assises20

Ransomware:
A strong push at federal level
& a REAL geopolitical topic

June 16th, 2021

MAJOR TAKEDOWNS *… but a new generation is ready*

TIER 1

The "Most Wanted"

Ryuk
Used for millions of ransomware attacks (1/3 of the total)

Egregor/Maze
206 and 266 attacks since 2020

REvil/Sodinokibi ?
286 attacks since 2020

Netwalker
144 attacks since 2020

DoppelPaymer
203 attacks since 2020

Conti
517 attacks since 2020

TIER 2

Rising stars

Avaddon
182 attacks since March 2020

Clop ?
88 attacks since March 2020

DarkSide ⊘
99 attacks since August 2020

Pysa/Mespinoza
232 since August 2020

Ragnar
32 attacks since Dec. 2019

SunCrypt
45 attacks since Oct. 2019

Thanos
More than 5 attacks since August 2020

TIER 3

Emerging groups

Cvartek.u45
Since March 2020, no attacks

Exorcist
Since July 2020, no attacks

Gothmog
Since July 2020, no attacks

Lolkek
Since July 2020, no attacks

Muchlove
Since April 2020, no attacks

Nemty
Since Sept. 2020, no attacks

Rush
Since July 2020, no attacks

Wally
Since February 2020, no attacks

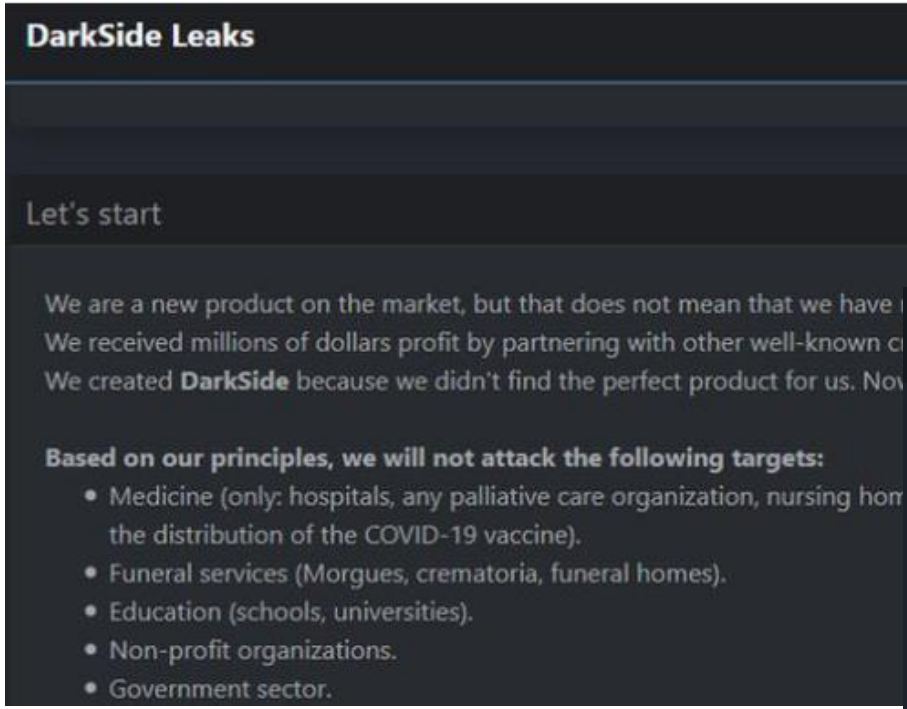
XINOF
Since July 2020, no attacks

Zeoticus
Since December 2019, no attacks

Questions? Comments?
my.beekast.com/assises20

Towards a reduction of attacks?

As groups start to limit their range of target



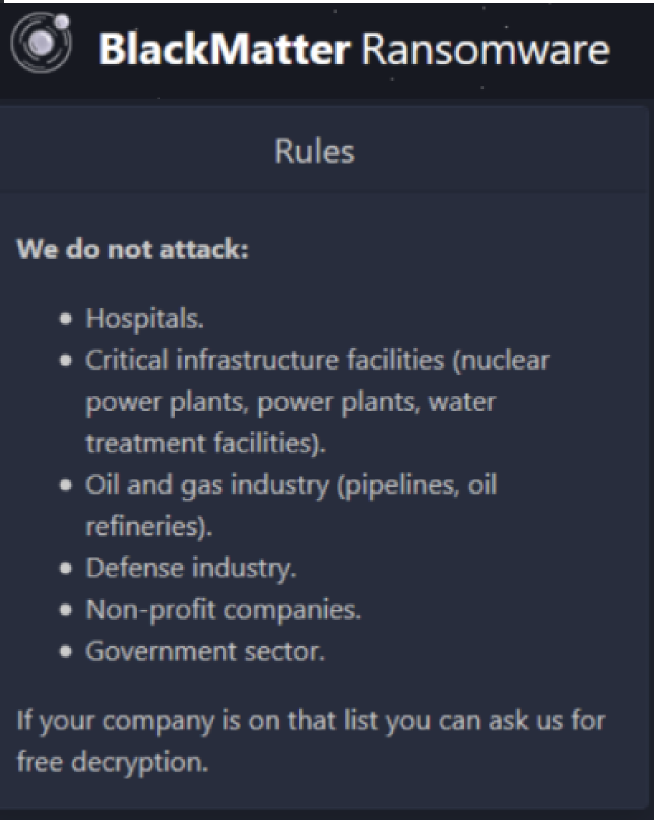
DarkSide Leaks

Let's start

We are a new product on the market, but that does not mean that we have
We received millions of dollars profit by partnering with other well-known c
We created **DarkSide** because we didn't find the perfect product for us. Nov

Based on our principles, we will not attack the following targets:

- Medicine (only: hospitals, any palliative care organization, nursing hom the distribution of the COVID-19 vaccine).
- Funeral services (Morgues, crematoria, funeral homes).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.



BlackMatter Ransomware

Rules

We do not attack:

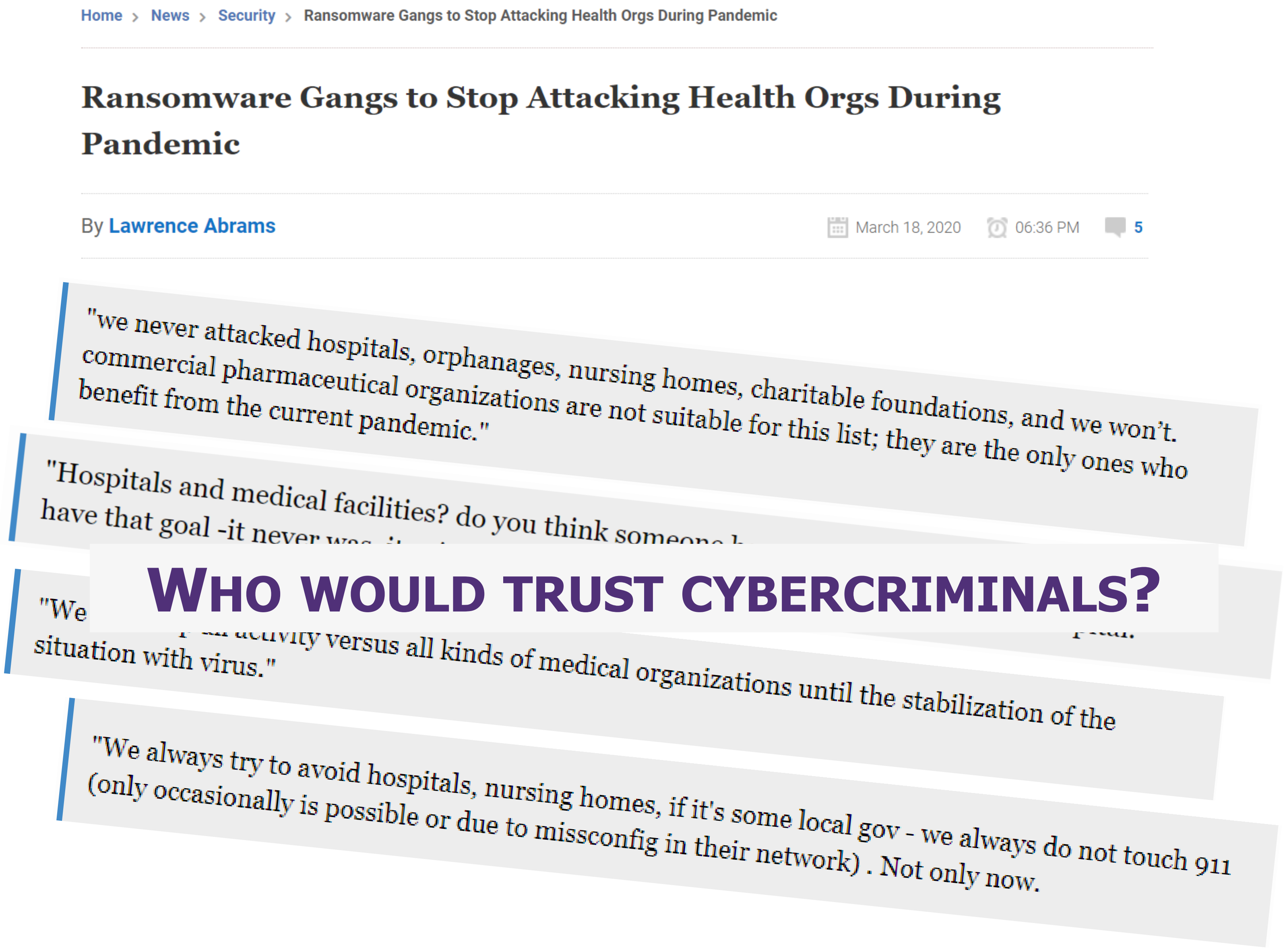
- Hospitals.
- Critical infrastructure facilities (nuclear power plants, power plants, water treatment facilities).
- Oil and gas industry (pipelines, oil refineries).
- Defense industry.
- Non-profit companies.
- Government sector.

If your company is on that list you can ask us for free decryption.

Questions? Comments?
my.beekast.com/assises20

Towards a reduction of attacks?

But remember in March 2020…



Home › News › Security › Ransomware Gangs to Stop Attacking Health Orgs During Pandemic

Ransomware Gangs to Stop Attacking Health Orgs During Pandemic

By Lawrence Abrams — March 18, 2020 — 06:36 PM — 5

> "we never attacked hospitals, orphanages, nursing homes, charitable foundations, and we won't. commercial pharmaceutical organizations are not suitable for this list; they are the only ones who benefit from the current pandemic."

> "Hospitals and medical facilities? do you think someone h
> have that goal -it never was

> "We
> activity versus all kinds of medical organizations until the stabilization of the situation with virus."

> "We always try to avoid hospitals, nursing homes, if it's some local gov - we always do not touch 911 (only occasionally is possible or due to missconfig in their network) . Not only now.

Who would trust cybercriminals?

RANSOMWARES

A vision fueled by our incident response field feedback

Analysis of **60 major security incidents**

that led to the interruption of business activities or severe compromises of the IS

Cyberattacks in France:

Ransomware, still threat n°1

By the CERT-Wavestone

Octobre 2021

The Positive Way

WAVESTONE

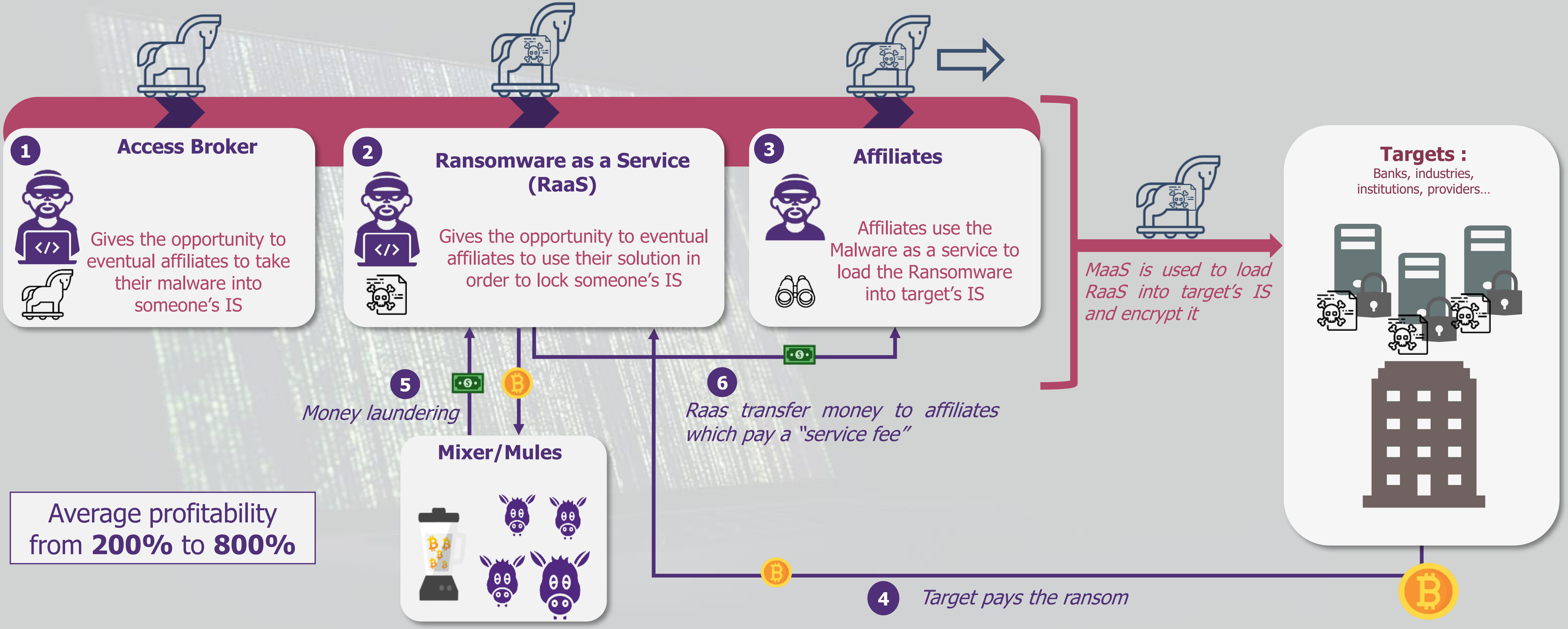
STILL THE **#1 THREAT** — **60%** of this year's incidents are due to a **ransomware attack**

FASTER AND FASTER ATTACKS — **25** **days** on average, **3 days** for the fastest

TARGETING **BACKUP SYSTEMS** — **21%** of cases where the backups were rendered **unusable**

ALWAYS THOUGH **ACTIVE DIRECTORIES** — **100%** of ransomware attacks used the AD as **amplification vector**

The Ransomware Business Model… Too profitable to stop



1 **Access Broker**

Gives the opportunity to eventual affiliates to take their malware into someone's IS

2 **Ransomware as a Service (RaaS)**

Gives the opportunity to eventual affiliates to use their solution in order to lock someone's IS

3 **Affiliates**

Affiliates use the Malware as a service to load the Ransomware into target's IS

MaaS is used to load RaaS into target's IS and encrypt it

Targets :

Banks, industries, institutions, providers…

4 *Target pays the ransom*

5 *Money laundering*

Mixer/Mules

6 *Raas transfer money to affiliates which pay a "service fee"*

Average profitability from **200%** to **800%**

MaaS : Malware as a Service
RaaS: Ransomware as a Service

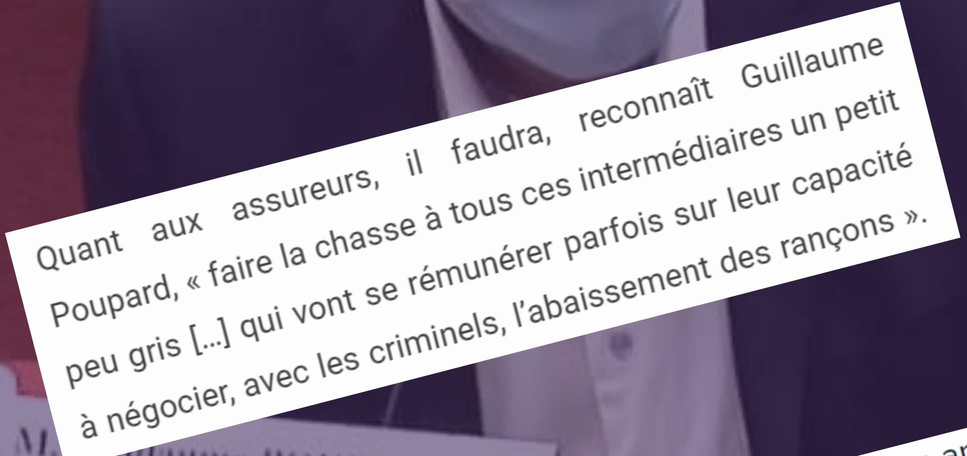
TO PAY OR **NOT TO PAY?**

CERT-W: A reduction from 20% to 5% of payment ransoms in 1 year

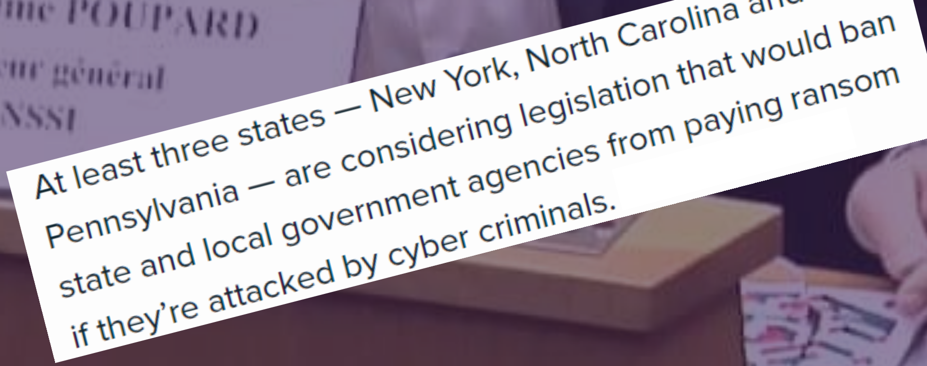
Typical reasons not to:

- Same legal impacts especially on privacy
- Decoder not always working
- Data integrity is not ensured
- **Same delay to recover**

& authorities are increasing pressure:



Quant aux assureurs, il faudra, reconnaît Guillaume Poupard, « faire la chasse à tous ces intermédiaires un petit peu gris […] qui vont se rémunérer parfois sur leur capacité à négocier, avec les criminels, l'abaissement des rançons ».



At least three states — New York, North Carolina and Pennsylvania — are considering legislation that would ban state and local government agencies from paying ransom if they're attacked by cyber criminals.

Now, *what is the situation for* **Tier-1 companies?**

Questions? Comments?
my.beekast.com/assises20

Feedback from the boardroom

Did you see what happened to our competitor?! Could it happen to us?! What would we do if it did?!

Doesn't this Cyber Insurance cover the Ransomware risk??

Ransomware groups did their digital transformation so much faster than us…

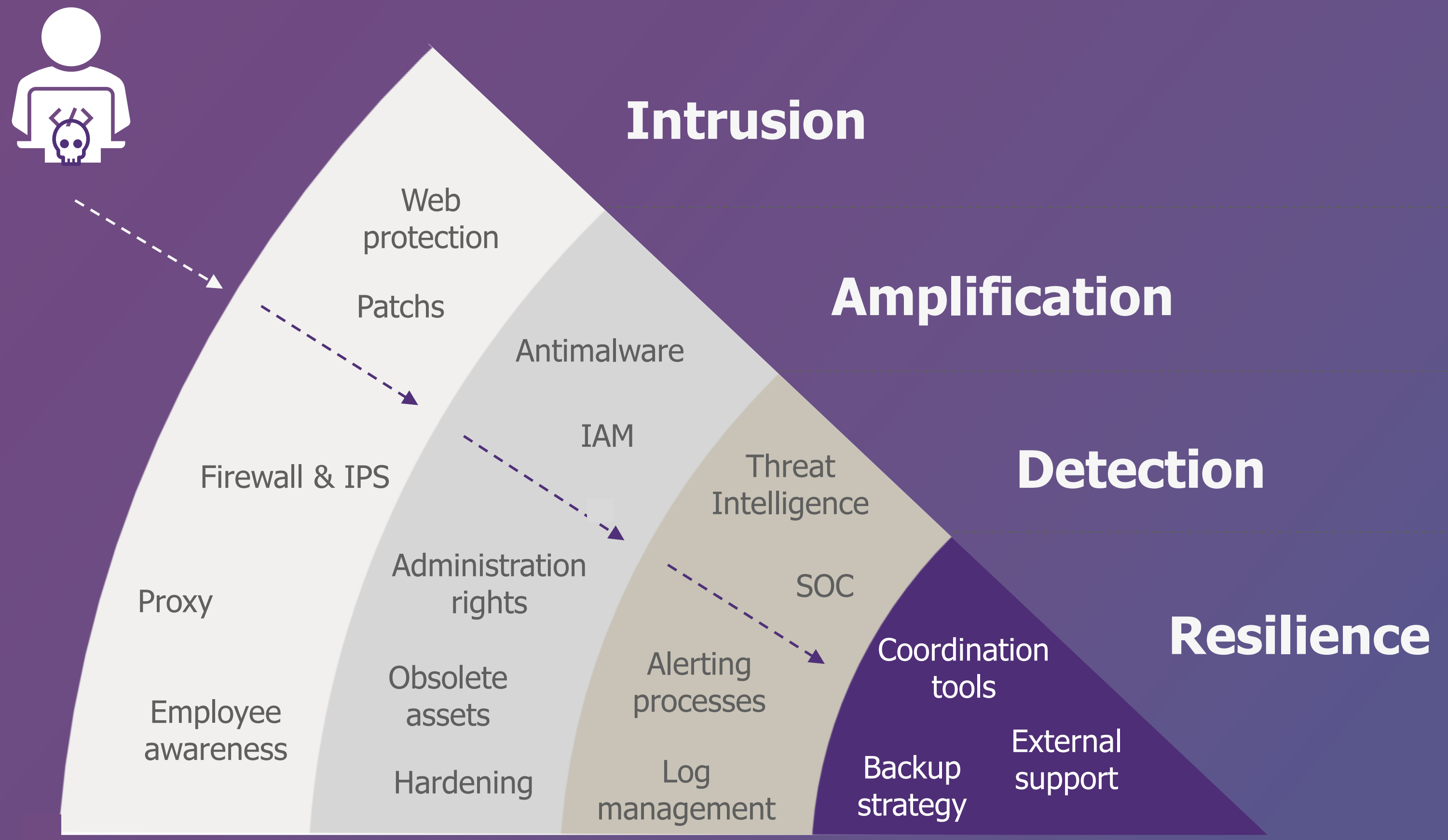
Seems like a profitable business, should we try?

Do we have a Bitcoin account??

What should we do to improve? What is the benchmark?

TIER 1 COMPANIES ARE STILL LACKING KEY RANSOMWARE CONTROLS

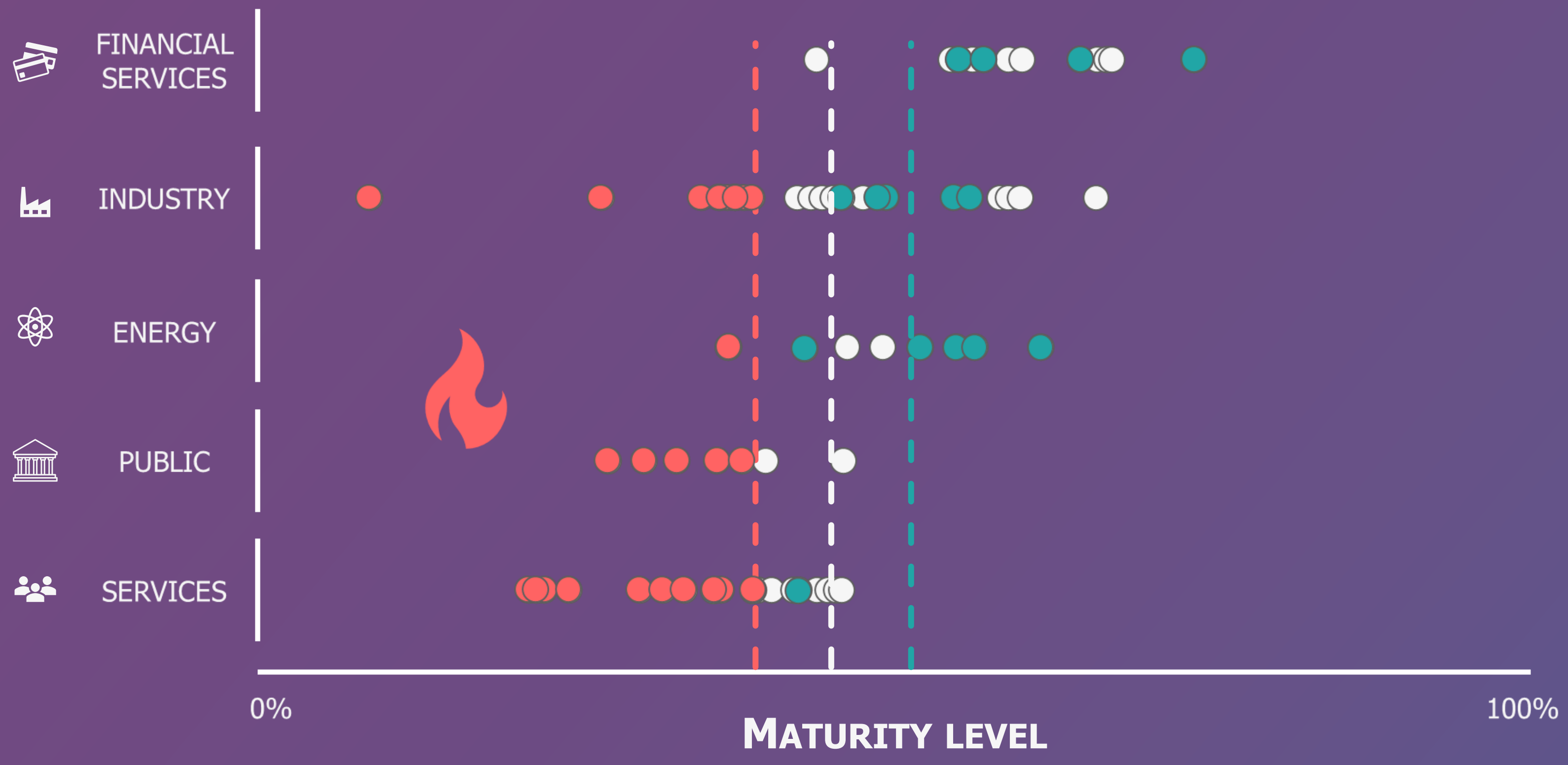
We have selected **31 anti-Ransomware controls** within the W-CyberBenchmark comparing the **most critical topics** in the light of the **latest attacks**.



QUESTIONS? COMMENTS?
my.beekast.com/assises20

TIER 1 COMPANIES ARE STILL LACKING KEY RANSOMWARE CONTROLS

We have selected **31 anti-Ransomware controls** within the W-CyberBenchmark comparing the **most critical topics** in the light of the **latest attacks**.



ALL WAVESTONE CLIENT AVERAGE: 45%

CAC40 COMPANIES AVERAGE: 53%

20 COMPANIES CONSIDERED IN A CRITICAL SITUATION

QUESTIONS? COMMENTS?
my.beekast.com/assises20

Source: W-CyberBenchmark 2021

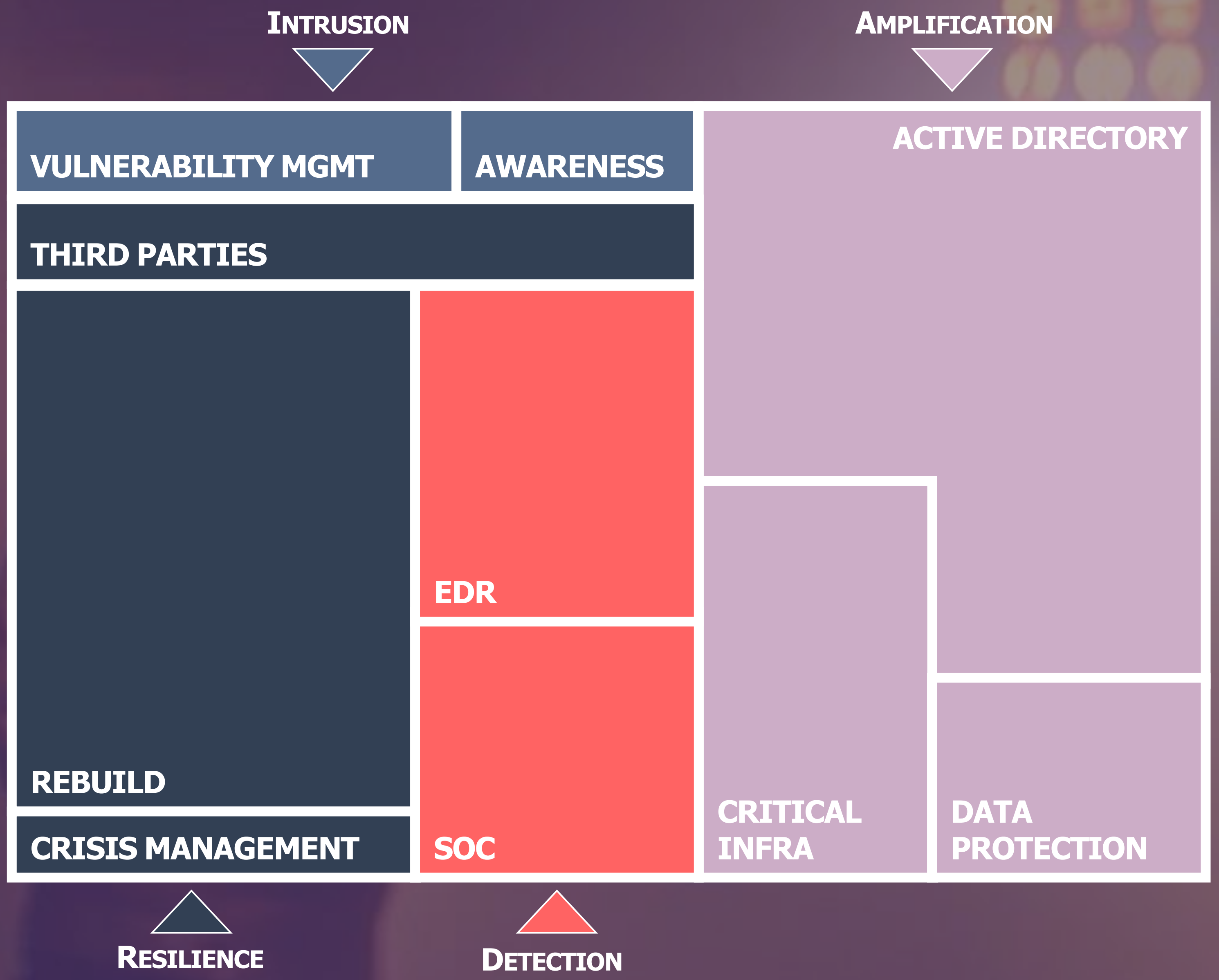
A RESPONSE THROUGH “ANTI-RANSOMWARE” PROGRAMS

BUDGET BETWEEN

1.5M€ – 50M€

10 PROJECTS

4 MAIN STREAMS



INTRUSION

AMPLIFICATION

VULNERABILITY MGMT

AWARENESS

THIRD PARTIES

ACTIVE DIRECTORY

EDR

REBUILD

CRISIS MANAGEMENT

SOC

CRITICAL INFRA

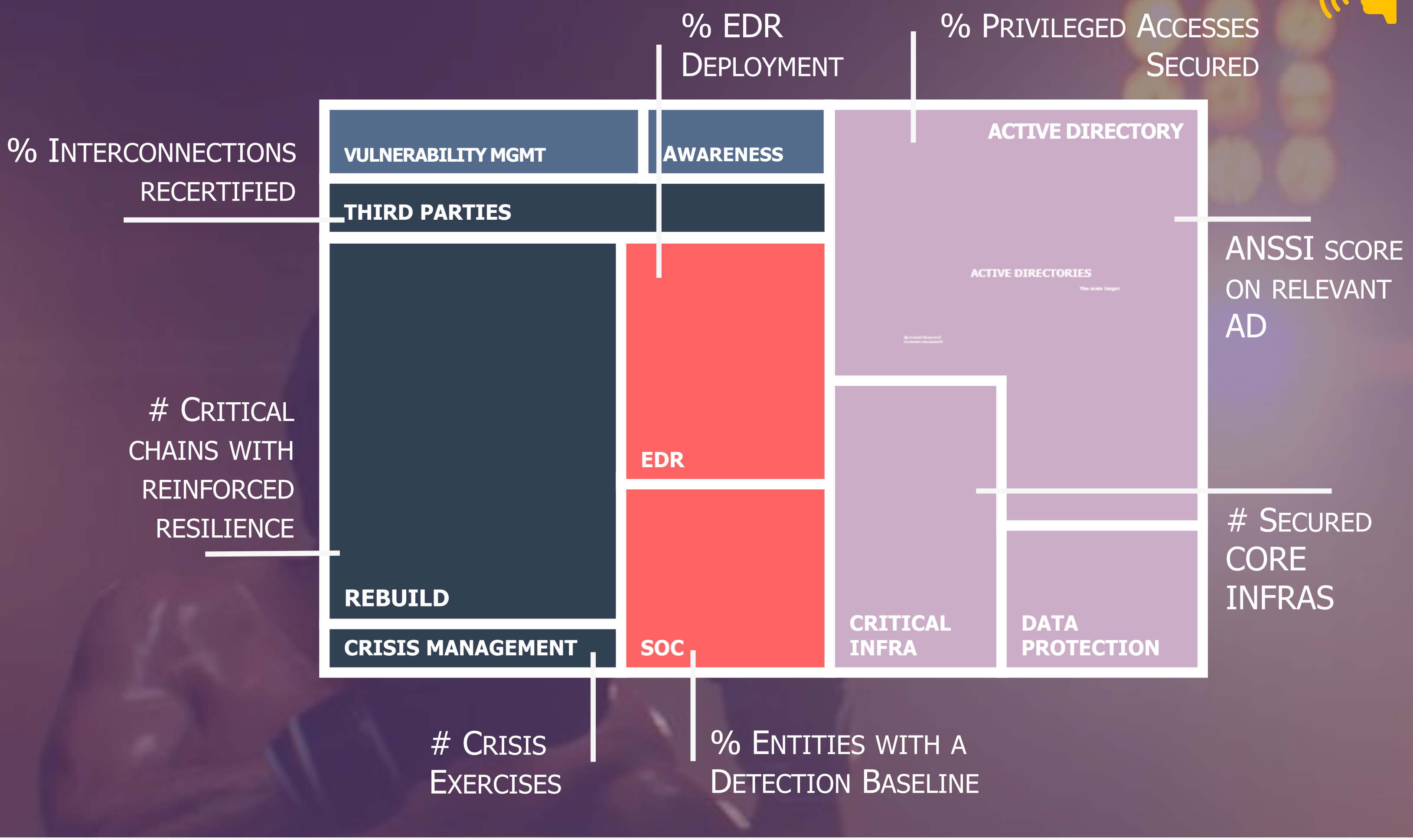
DATA PROTECTION

RESILIENCE

DETECTION

QUESTIONS? COMMENTS?
my.beekast.com/assises20

Using Hands On dashboards for the Top Management



Presented three times a year to the CEO

The Basis for all budget requests

Used to calculate CIO and CISO bonuses

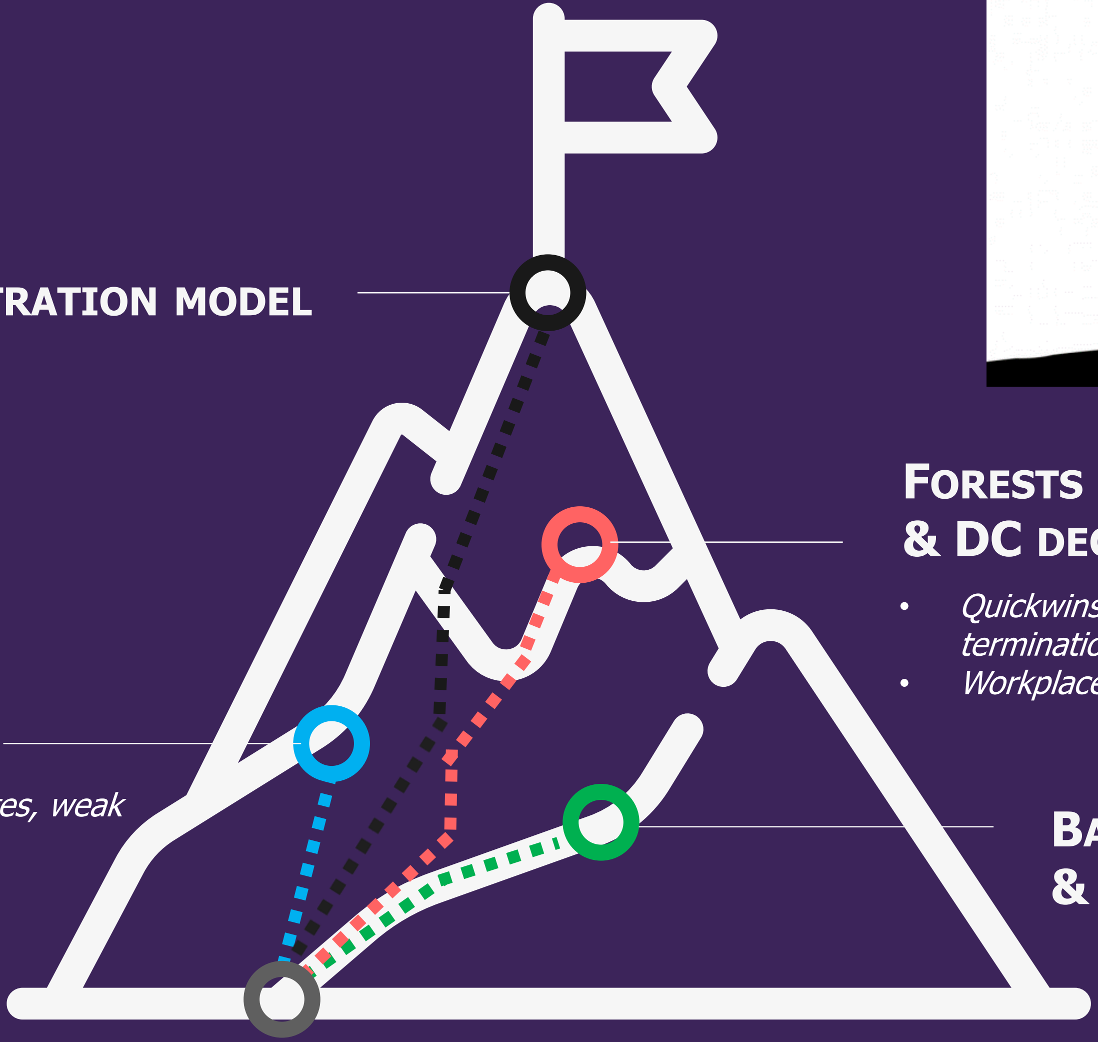
ACTIVE DIRECTORIES

The main target

ACTIVE DIRECTORIES: *overview of 5 projects*

	Prior to AD project		*After AD project*		
	EXAMPLE 1	**EXAMPLE 2**	**EXAMPLE 3**	**EXAMPLE 4**	**EXAMPLE 5**
# EMPLOYEES	160 000	100 000	145 000	200 000	10 000
AD ARCHITECTURE	70 forests 120 domains	50 forests 300 DC	10 forests 15 domains	3 forest 10 domains 70 DC	6 forests 7 domains 9 DC
# DOMAINS ADMINS	80	200	10	15	5
PROJECT DURATION			18 months	12 months	12 months
PROJECT BUDGET			15M€	5M€	2M€

ACTIVE DIRECTORIES: *how are projects usually structured?*



€€€ **SEGREGATION & ADMINISTRATION MODEL**

- ➢ *Tier 0 & Tier 1*

FORESTS RATIONALIZATION & DC DECOMMISSIONING €€

- *Quickwins on abondonned forests: old M&As, projects termination, unused apps…*
- *Workplace & Cloud: get close to IT transformation projects*

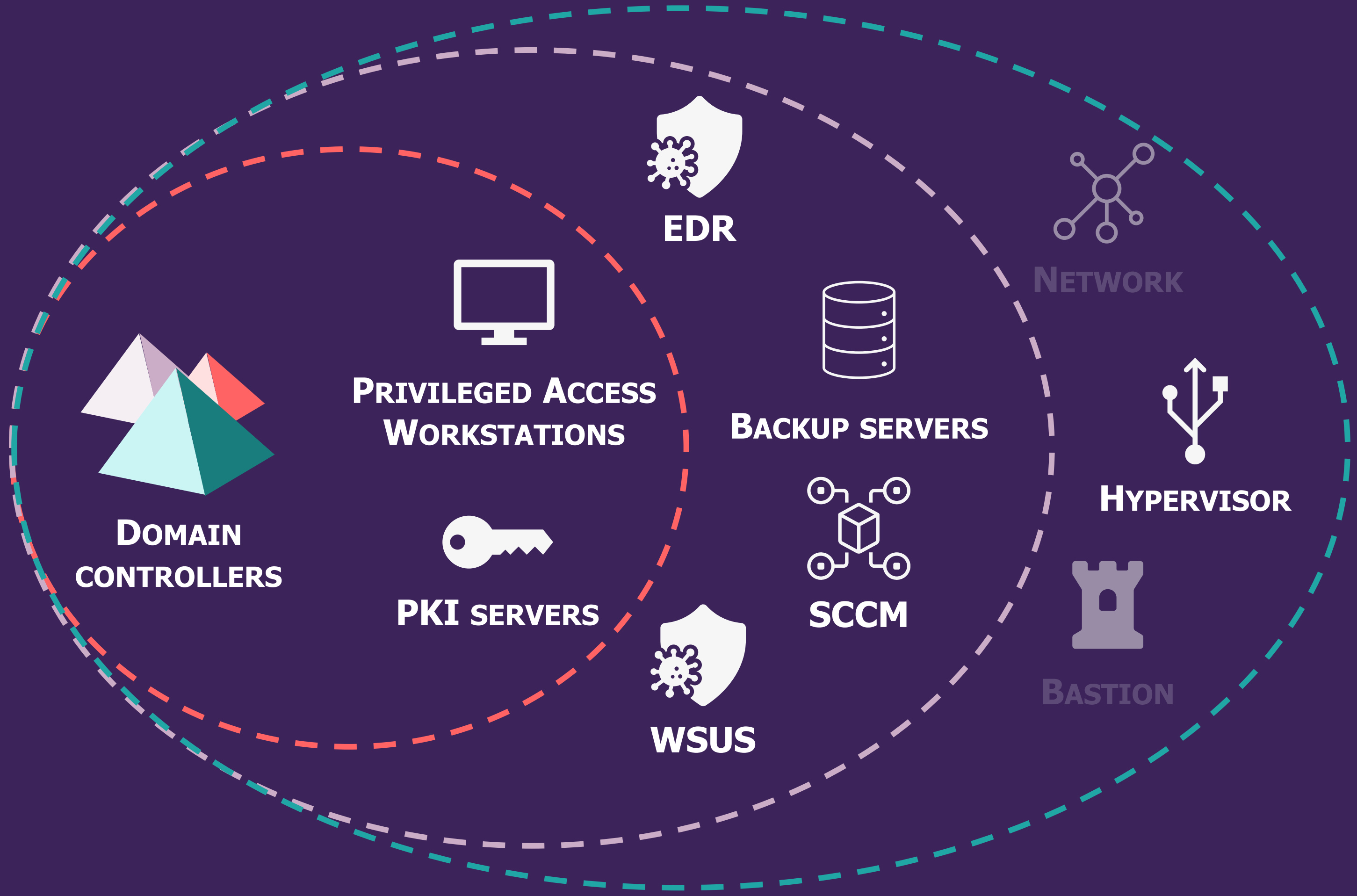
€€ **HARDENING & CONTROLS**

- *Inactive accounts, vulnerable certificates, weak Kerberos encryption…*
- *Do not forget servers & applications*
- *Pingcastle, Purple Knight, Tenable…*

BACKUP EXTERNALIZATION & REBUILD TESTS €

QUESTIONS? COMMENTS?
my.beekast.com/assises20

Tier 0: Not just Domain Controllers & admins!

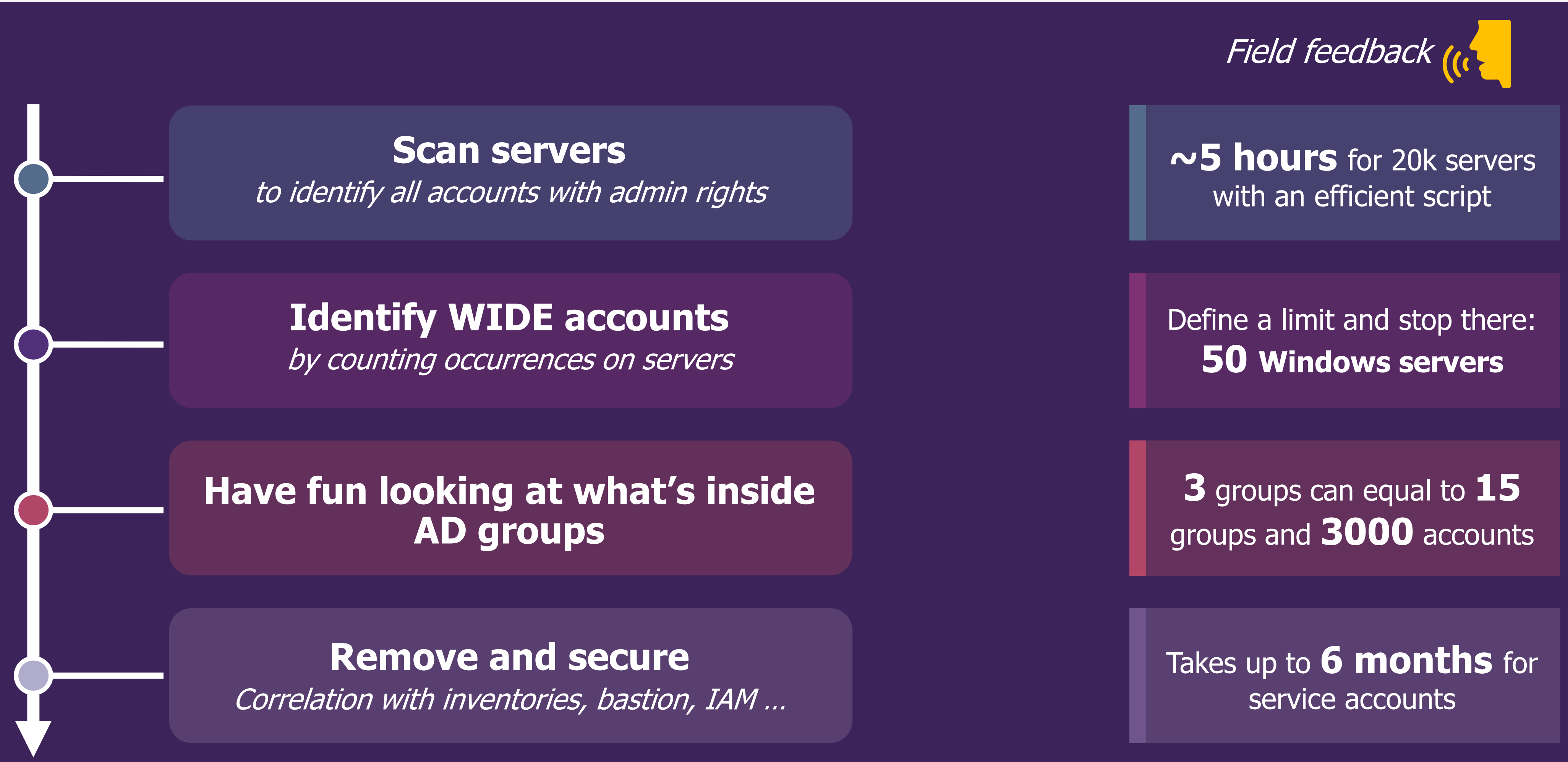


And create a Tier 0 team able to manage the whole environment

10/15 people with dedicated workstations

Questions? Comments?
my.beekast.com/assises20

TIER 1: CATCH WIDE-SCOPE ACCOUNTS



Field feedback

Scan servers
to identify all accounts with admin rights

~5 hours for 20k servers with an efficient script

Identify WIDE accounts
by counting occurrences on servers

Define a limit and stop there: **50 Windows servers**

Have fun looking at what's inside AD groups

3 groups can equal to **15** groups and **3000** accounts

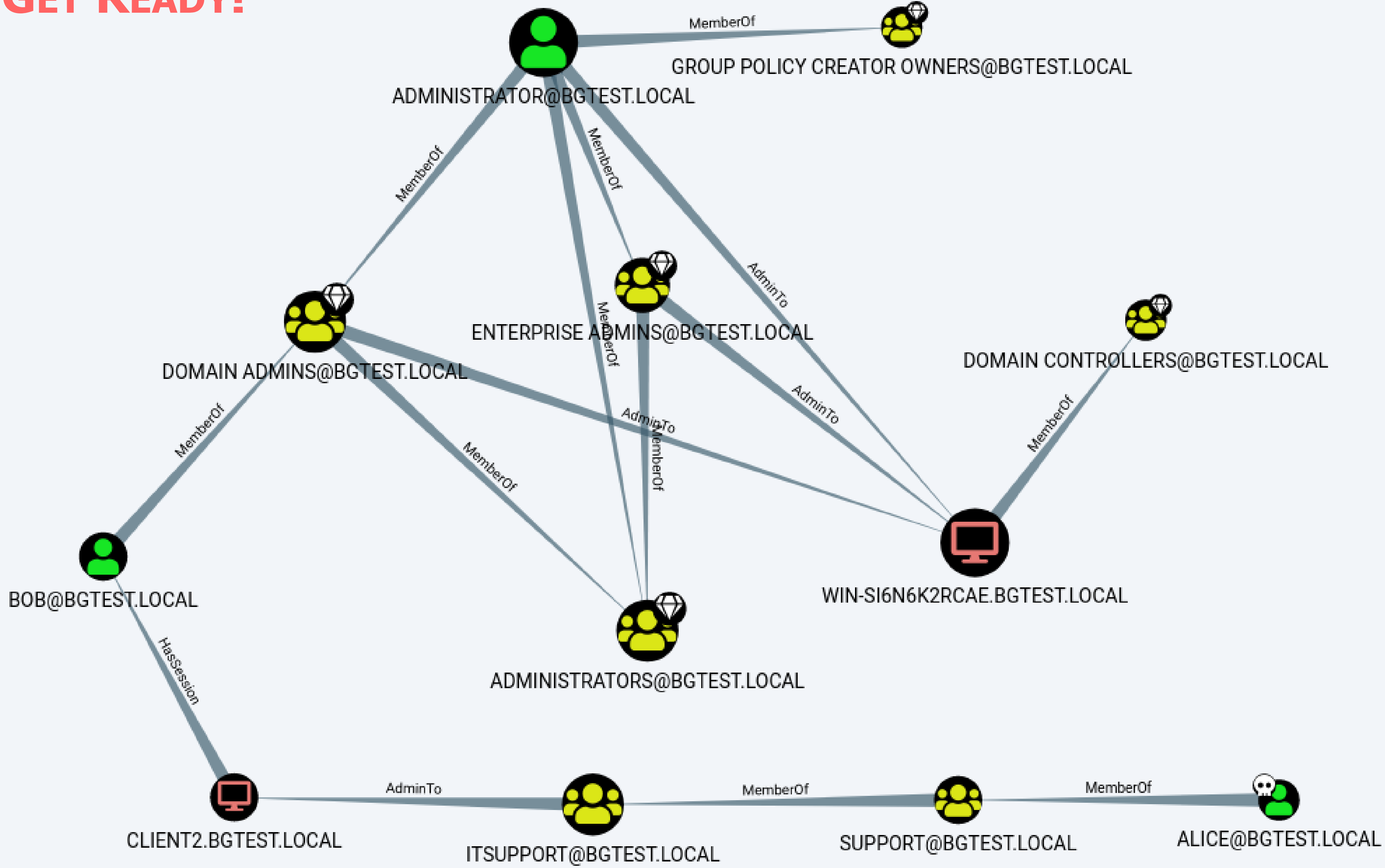
Remove and secure
Correlation with inventories, bastion, IAM …

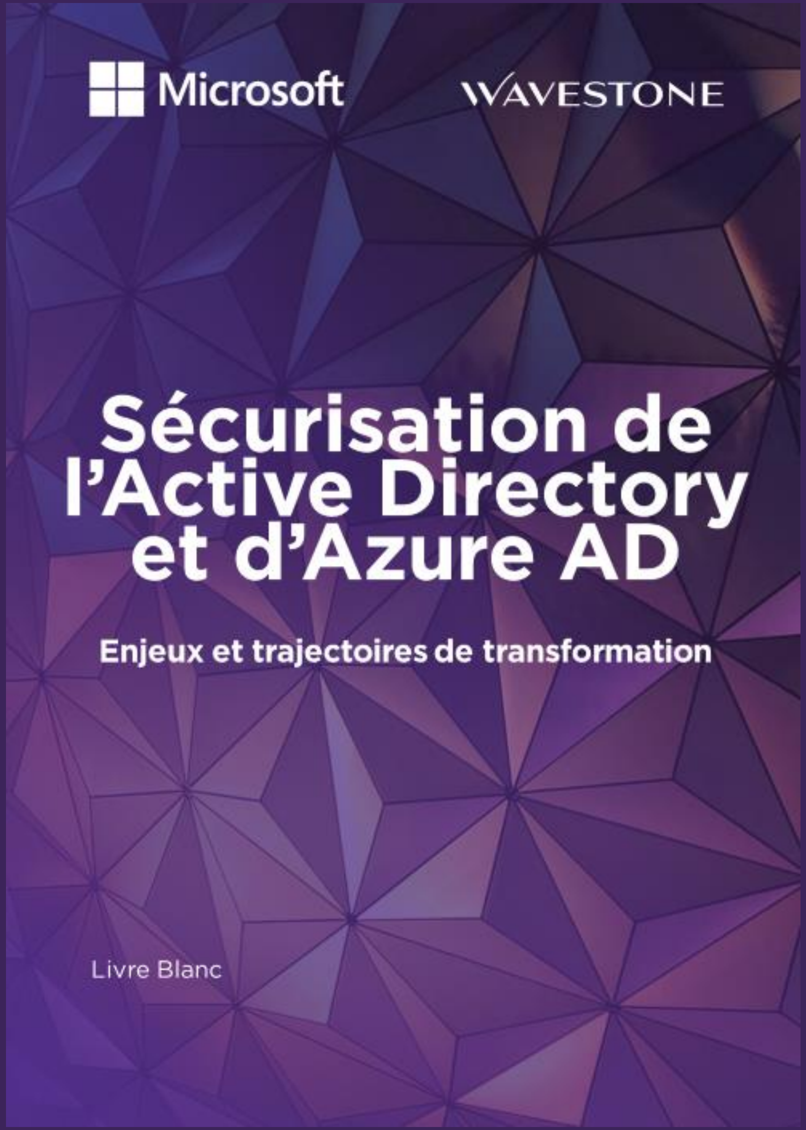
Takes up to **6 months** for service accounts

And redesign operational processes

Helpdesks, local admin teams…

The Last Step to find the unknown... Get Ready!





Microsoft WAVESTONE

Sécurisation de l'Active Directory et d'Azure AD

Enjeux et trajectoires de transformation

Livre Blanc

A joint Microsoft & Wavestone publication

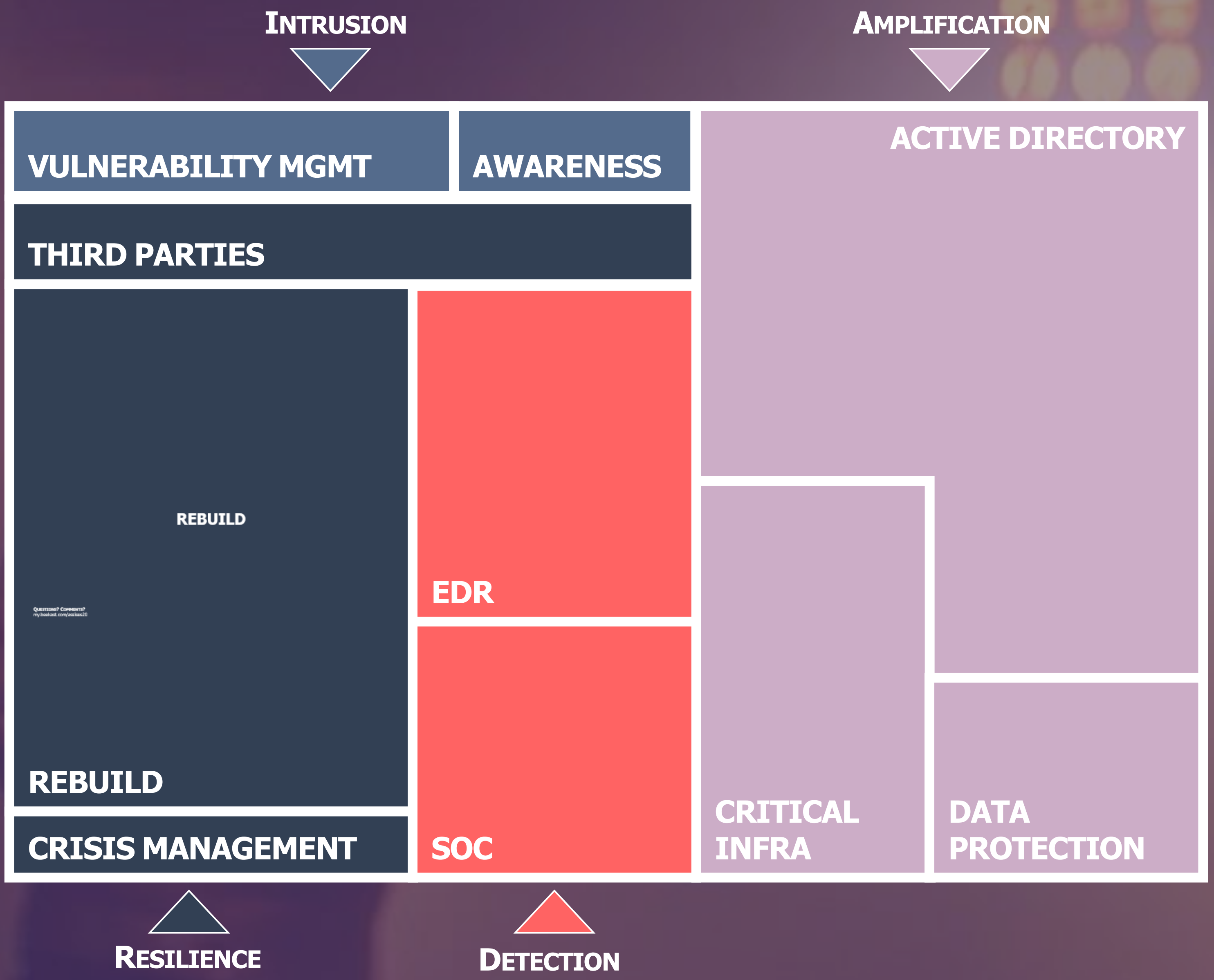
Back to "Anti-ransomware" programs

Budget between

1.5M€ – 50M€

10 Projects

4 main streams



Intrusion

Amplification

VULNERABILITY MGMT

AWARENESS

ACTIVE DIRECTORY

THIRD PARTIES

REBUILD

Questions? Comments?
my.beekast.com/assises20

REBUILD

EDR

CRISIS MANAGEMENT

SOC

CRITICAL INFRA

DATA PROTECTION

Resilience

Detection

Questions? Comments?
my.beekast.com/assises20

REBUILD

REBUILD

1 What to rebuild? Define your scenario(s): amplification vectors & destruction level.

Business Apps

Infrastructure

REBUILD

Business Apps

Identify **THE** most critical business functions and their impact tolerance

10 to 30 business chains

Improve **rebuild capabilities**

- Define rebuild timeline & responsibilities
- Write rebuild plans & Test the rebuild time and mechanisms

Define **no-IT business workarounds**

…but requires strong cooperation from the business

Target rebuild **by design**

- Transform old & build new apps with continuous integration / continuous deployment
- Use cloud platform as an accelerator to automate rebuilding

REBUILD

Infrastructure

5 to 10

core infrastructures
(AD, DNS, DHCP, WSUS/SCCM, backup, bastion, hypervisor, EDR)

Gain up to 50%

of reduction of rebuild time
(from 11 days to 4 days)

200k€ to +10M€

from tactical measures to huge investments on backup infrastructures

Key Takeaways form Resilience Programs

Harden Backups

hardened infra / immutable backups
D-1 for applicative data is enough

Secure Core Infra

AD Rebuild delay could be shortened up to 1 day

Prepare massive rebuild of workstations

USB keys, VDI, Azure AD Join…
to reach thousands of WKS /day

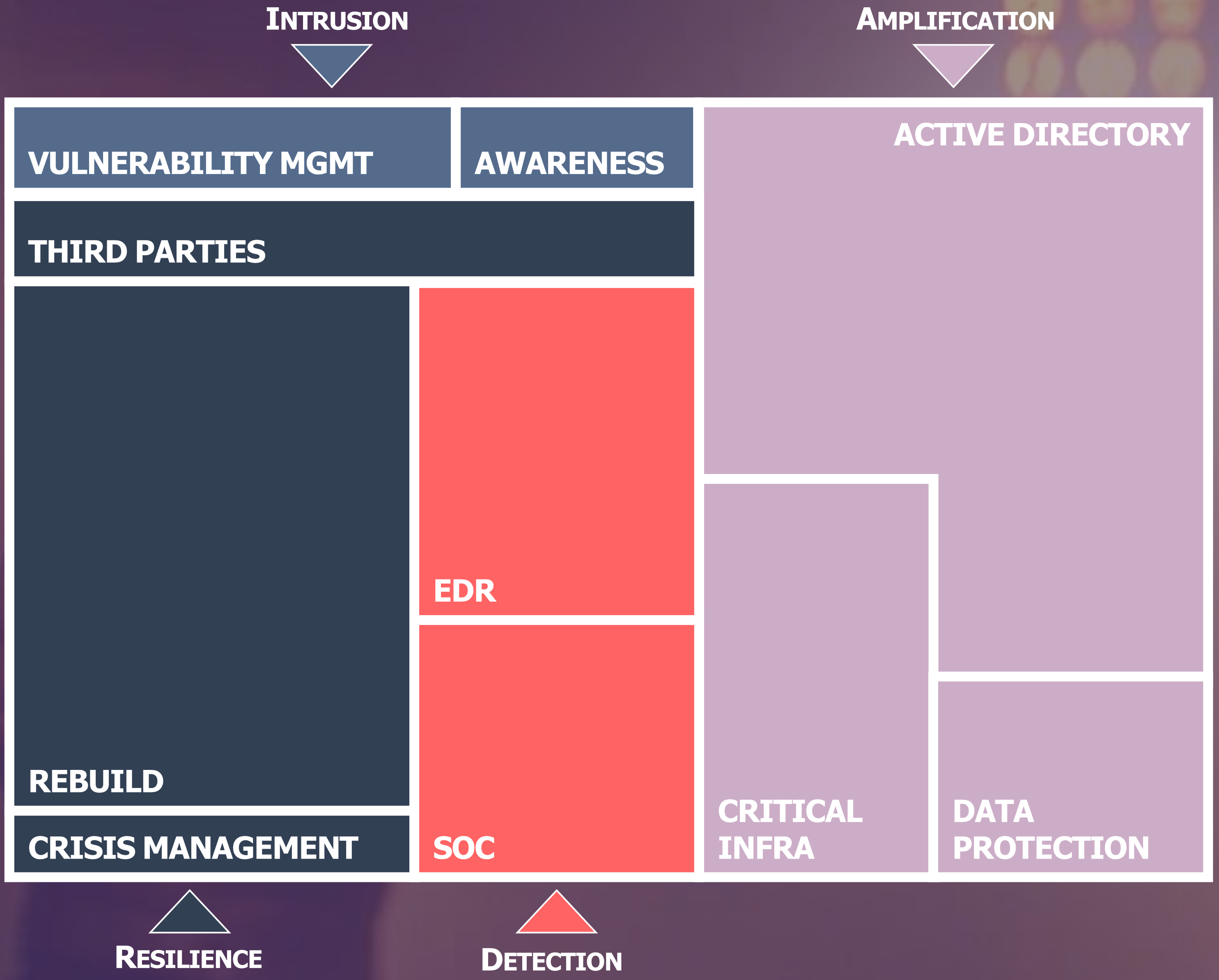
Back to "Anti-ransomware" programs

Budget between

1.5M€ – 50M€

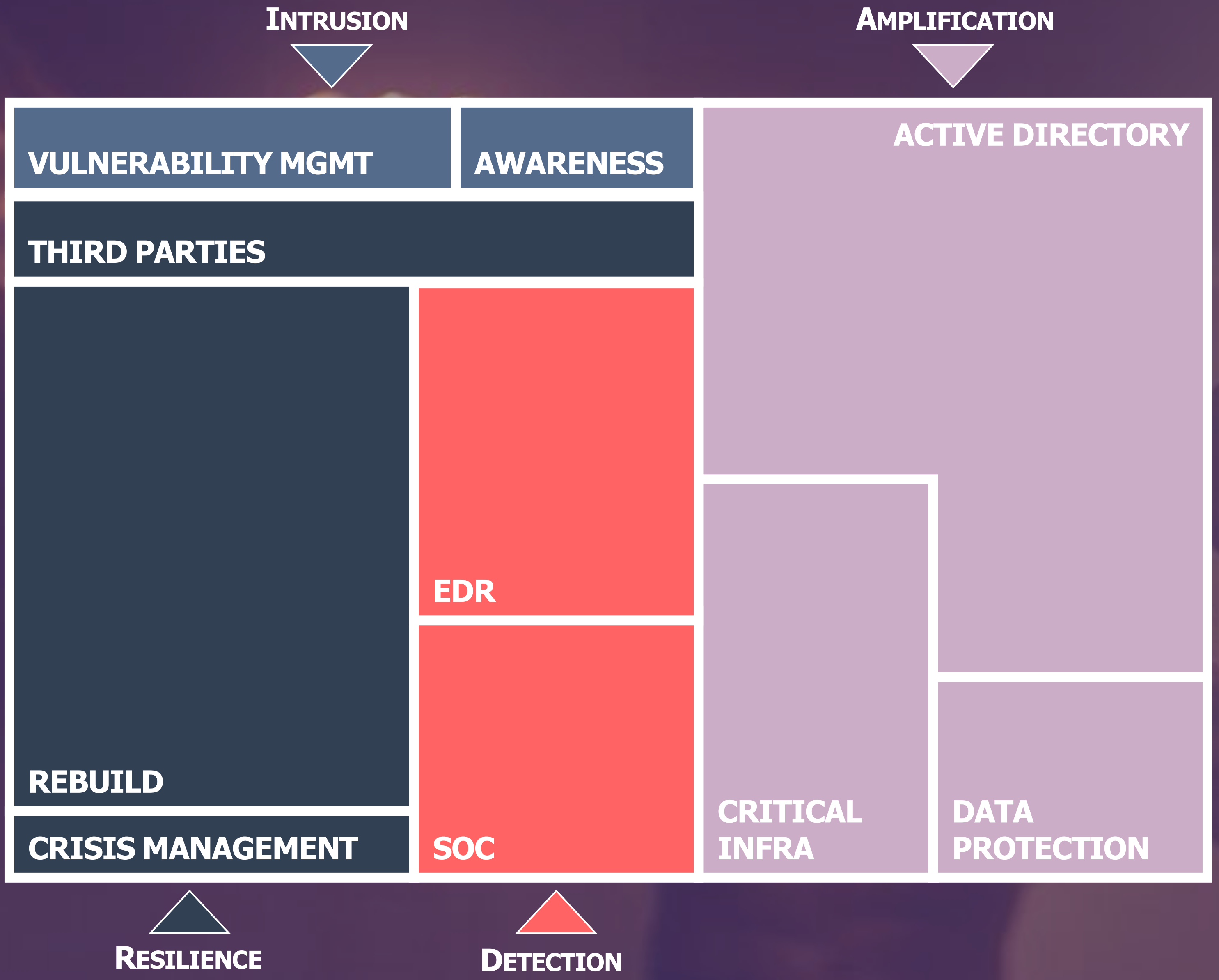
10 Projects

4 main streams



Questions? Comments?
my.beekast.com/assises20

Back to "Anti-ransomware" programs



What's next?

INTRUSION VECTOR

Third parties

Insider threat

TESLA

Kaseya®

AMPLIFICATION VECTOR & TARGET

Hypervisor & Linux

Antimalware & system management platform

RANSOM X

EXTORSION

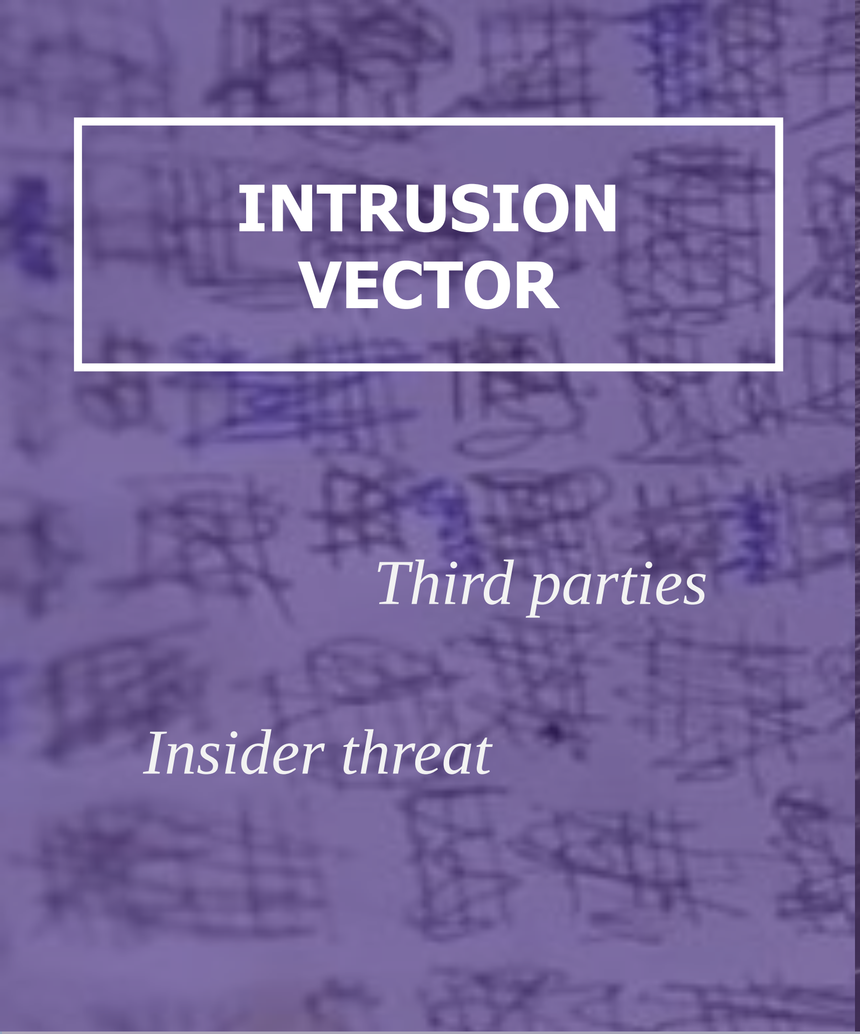
Direct extorsion of clients

Triple extorsion through DDoS

Reverse auctions

Vastaamo.fi

AVADDON RANSOMWARE



INTRUSION VECTOR

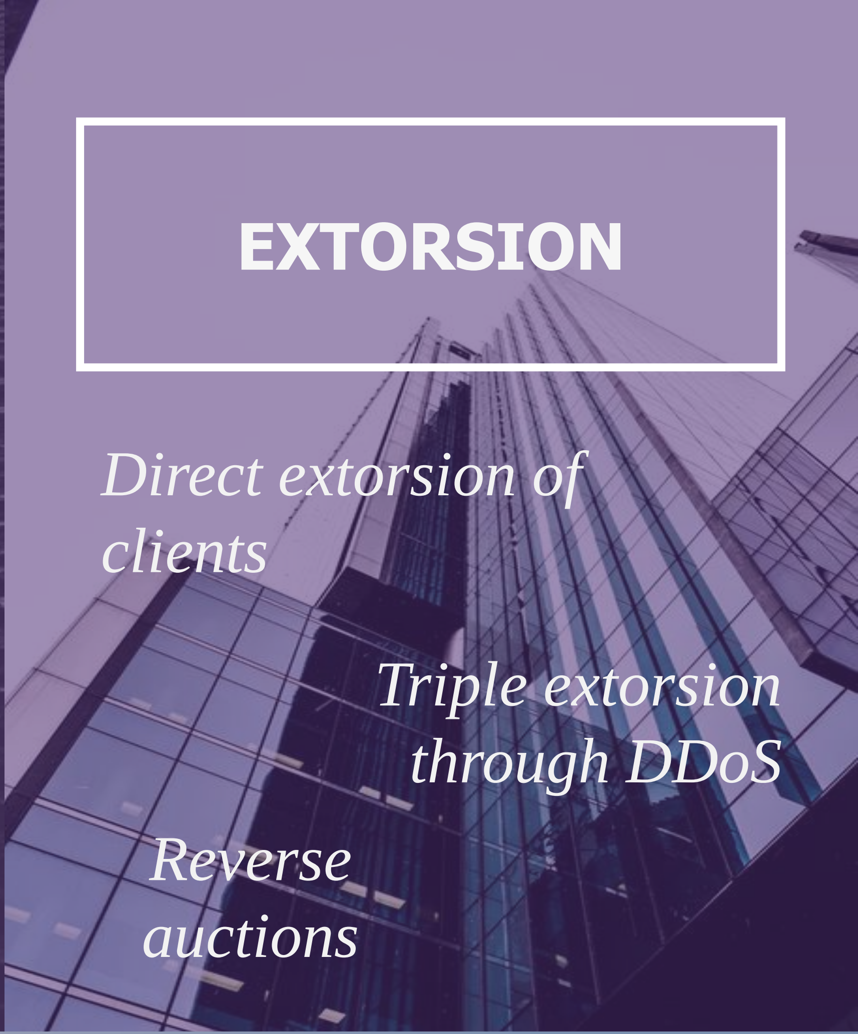
Third parties

Insider threat

AMPLIFICATION VECTOR & TARGET

Hypervisor & Linux

Antimalware & system management platform



EXTORSION

Direct extorsion of clients

Triple extorsion through DDoS

Reverse auctions

AN EVER CHANGING ENVIRONMENT, SO TRY TO STAY AHEAD!

Follow the **ransomware ecosystem** evolution

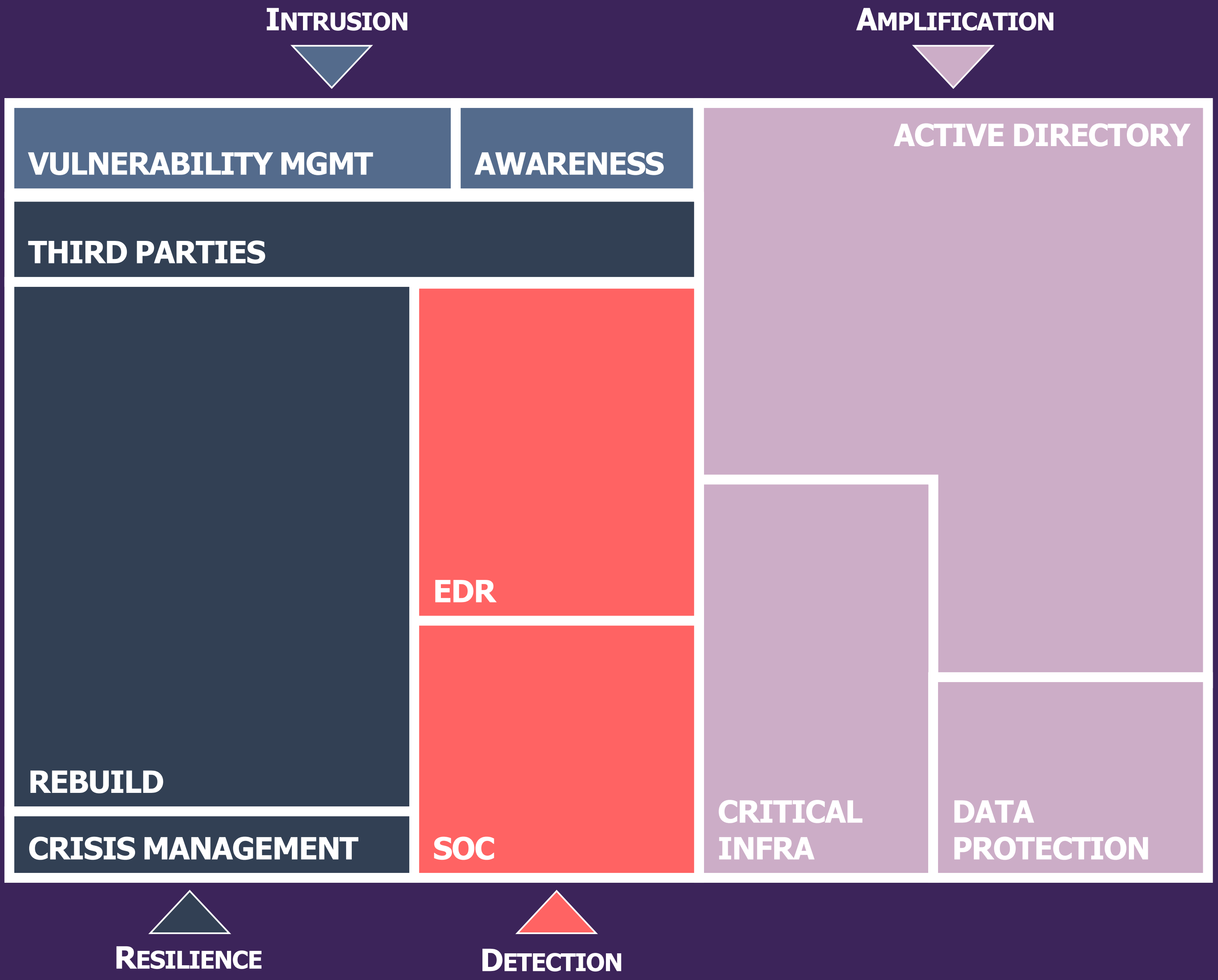
Test new scenarios during **crisis exercises**

Keep **5% of the budget** “unallocated” for critical updates

ANY QUESTIONS?

Gérôme BILLOIS
Partner
gerome.billois@wavestone.com
(+33) 6 10 99 00 60
@gbillois

Matthieu GARIN
Partner
matthieu.garin@wavestone.com
(+33) 6 23 15 31 95
@matthieugarin



INTRUSION

AMPLIFICATION

VULNERABILITY MGMT

AWARENESS

ACTIVE DIRECTORY

THIRD PARTIES

EDR

REBUILD

CRISIS MANAGEMENT

SOC

CRITICAL INFRA

DATA PROTECTION

RESILIENCE

DETECTION