Cybercrime resilience effectiveness

- common mistakes and how to avoid them -

11 March 2021

Written by

Cristian Zaharia

Manager Ersnt&Young

Head of FTDS

Building a better working world

Cristian Zaharia

Manager I Forensic & Integrity Services EY Romania

Mobile +40 769 641 756
Email cristian.zaharia@ro.ey.com

Professional experience

- 5 years as Police officer in multiple cybercrime investigations conducted by the Romanian Police and DIICOT, many of them in close collaboration with FBI and Secret Service representatives from US Embassy in Bucharest
- Between 2015-2017 I worked as cyber incident coordinator for a series of EMEA and US clients. I was responsible for assuring a fast cyber incident response and take all the measures in order to contain the attack and reduce its effects.
- Between 2017 to the present I have been Consultant for a variety of cybersecurity services: incident handling, incident response, forensics and threat intelligence. In this period Cristian led numerous SOC teams in their purpose to ensure a strong security posture for the clients.

Certifications

- CISSP (ISC2- Certified Information Systems Security Professional)
- SANS-GIAC Certified Intrusion Analyst
- EC-Council- Certified Hacking Forensic Investigation
- Comptia Security+
- Cyber Incident Forensic Responder – IACIS
- Business Relationship Management

Have you been the target of a cyber attack

YES

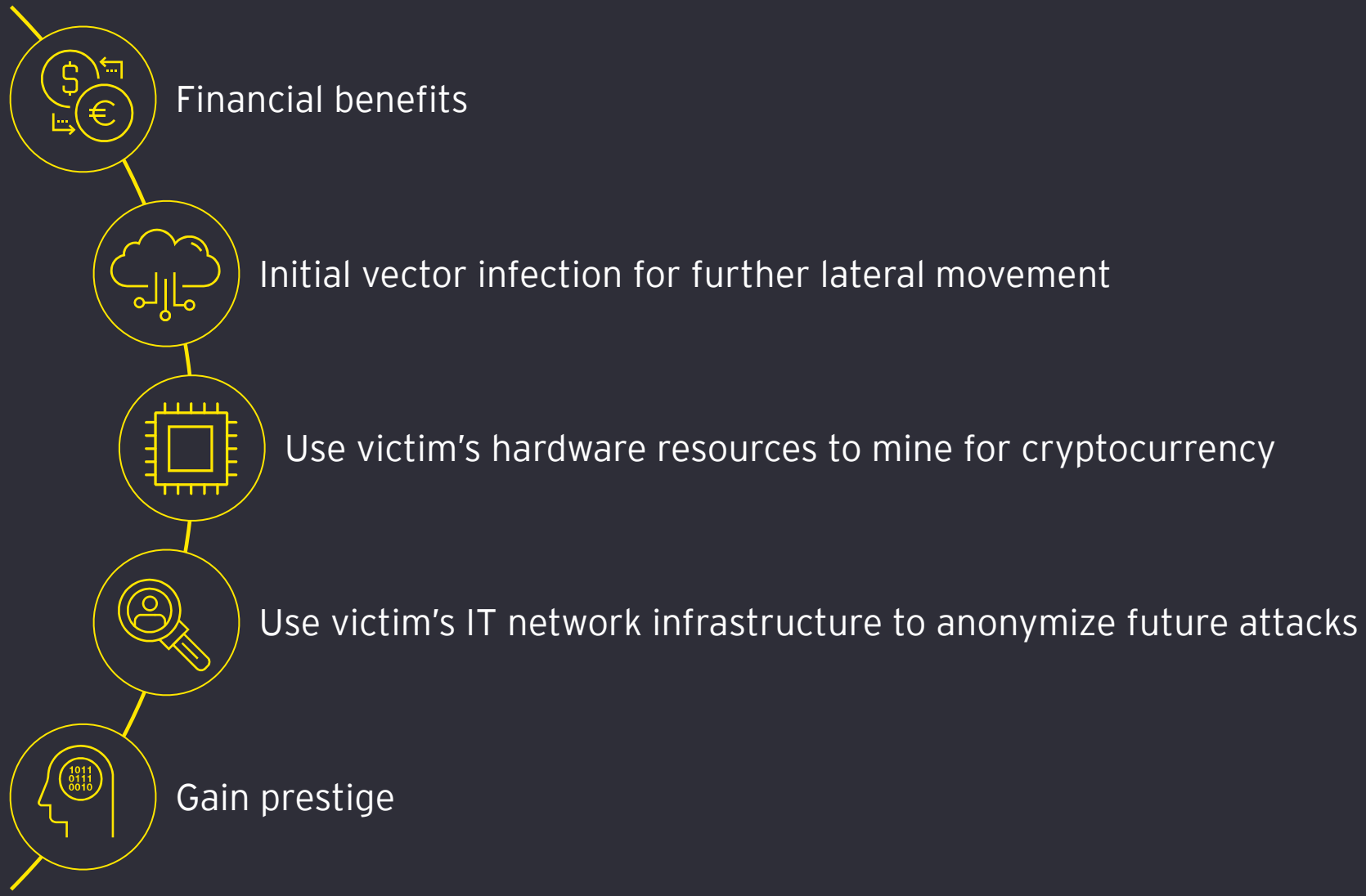
NO

Have you been the victim of a cyber attack

YES

NO

Attackers immediate purpose



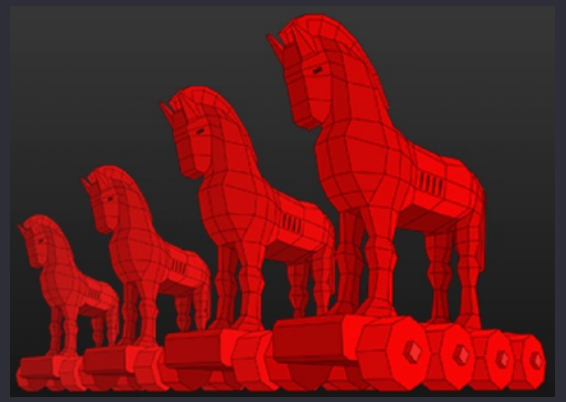
Blue team on the spot

A blue team is a company's own cybersecurity personnel

Adds vital human intelligence to the tools and technologies and is both proactive and reactive

Detect and neutralize the more sophisticated attacks and closely monitor current and emerging threats to preemptively defend the organization.

Never ending game against the red team



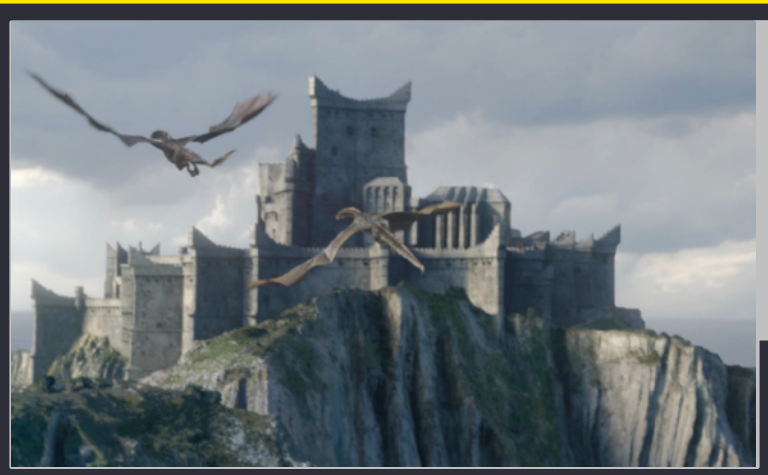
Do you know the current cyber resilience state of your organization?

Yes or No

Do you have a strong cyber resilience program in place?

Yes or No

Perception is Everything…or not



What executives think about their own cyber security program

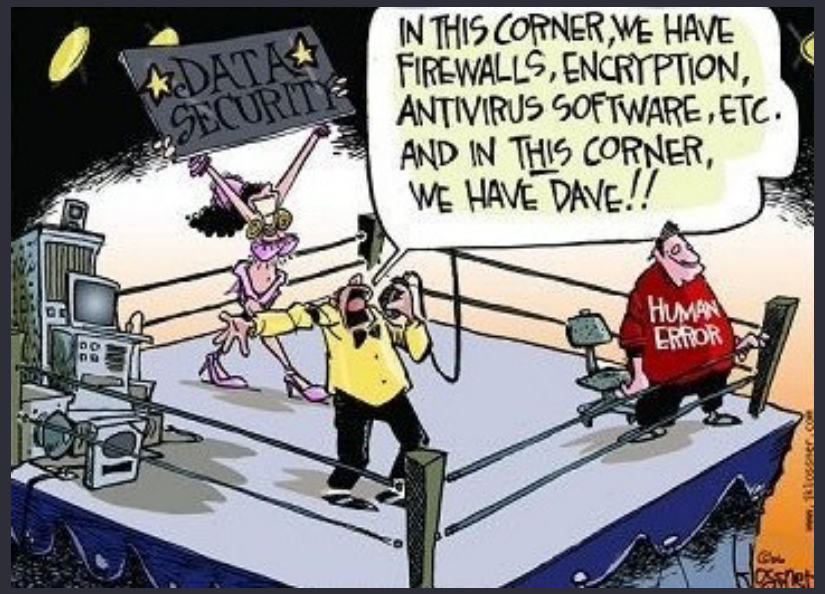
What CIO&CISO think about their incident response capabilities

78 % of the companies which suffered a breach thought they are well secured

How does the blue team look like

How the attacker sees you

The negation theories



1) I don't have something important so I'm not a target

- You always have something valuable for the attacker
- Most of the times, this is not directly visible to the company stakeholders

2) I have everything in place and I'm very well protected

- Attacks techniques are always evolving and adapting: you don't know what you don't know
- Do not forget that there will always be a risk as long as the problem will exist between the keyboard and the chair

Gaps in incident response readiness

Incomplete methodology

- Plans are not tailored to the needs
- Plans are not regularly reviewed and updated
- Plans are used only in real-words scenarios

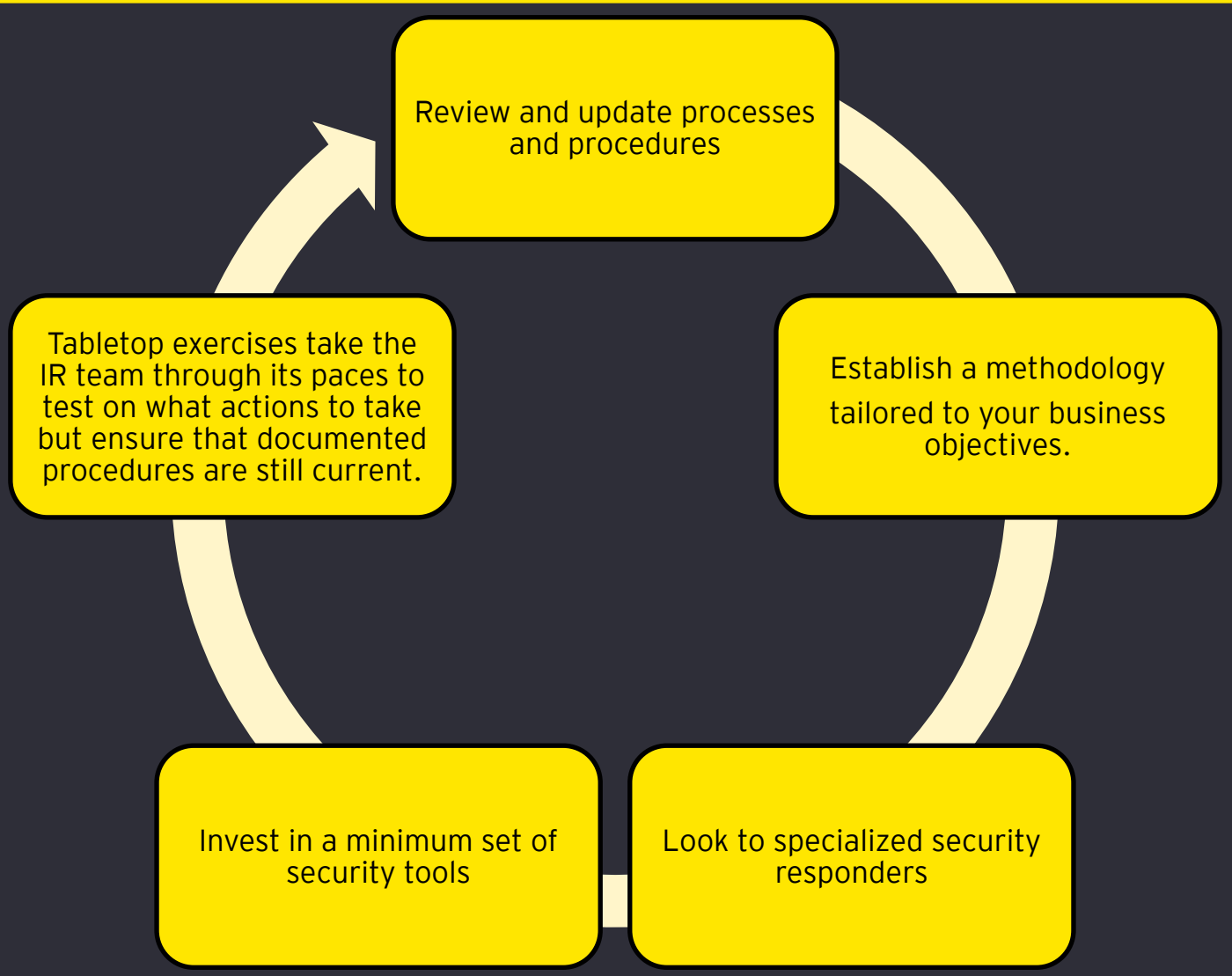
People management

- Lack of skills
- Wrong-size & coverage
- Not focused on automation

Security Tools

- No tools or too few – no visibility
- Tools are inadequate, unmanaged or underutilized
- Inadequate logging

Fill the gaps and be (almost) ready

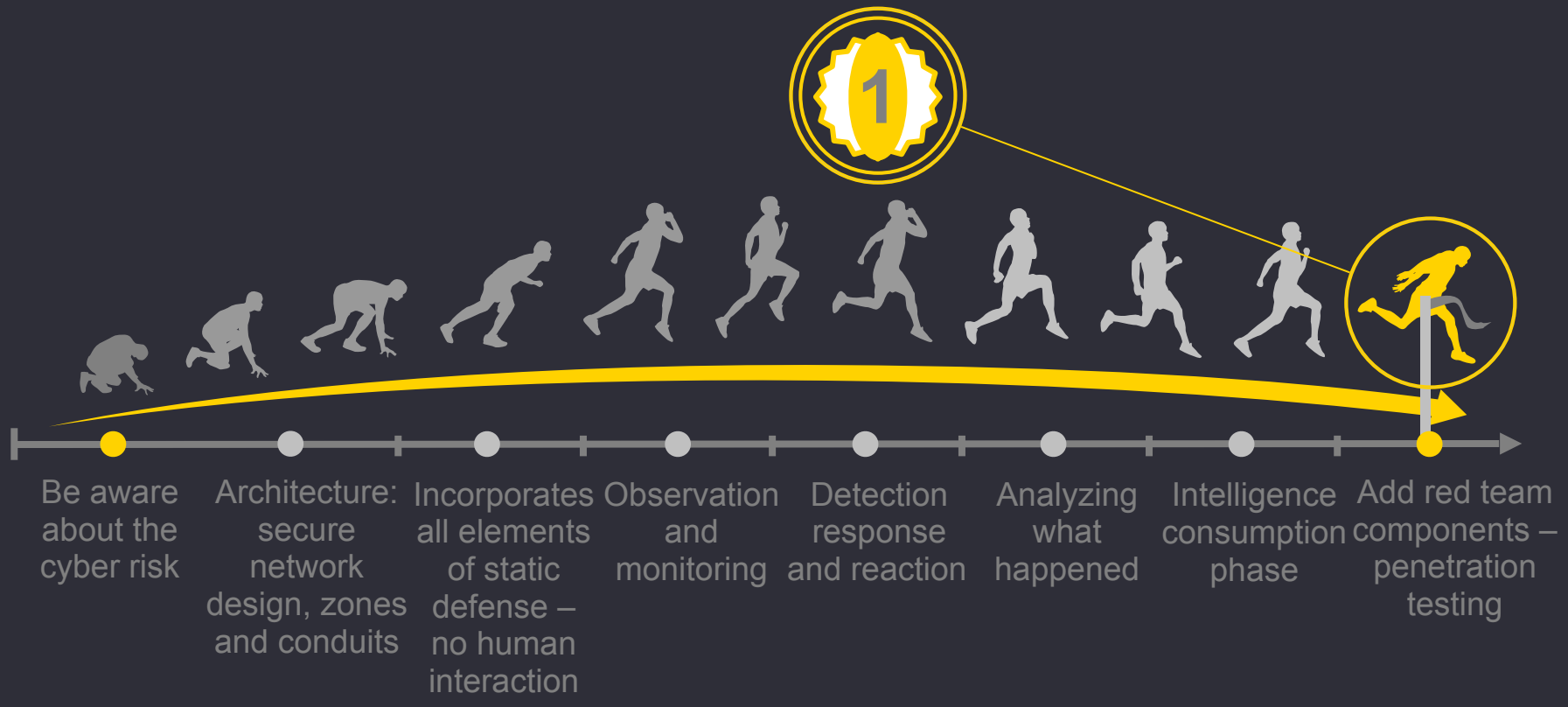


Taking the wrong path during an incident

- The blue team has no authority and visibility in the organization
- Confusing containment with remediation
- Not working as a single entity – lack of collaboration
- Help desk team can jeopardize important evidence

What's next: avoid the arrow before even seeing it

Adopt an active defense approach



How can EY help?

Know the reality

Incident response posture review

Evaluate the current level of Cybercrime Resilience capability, identifying gaps and measures undertaken to fill them.

Cyber Response Readiness

Manage cyber response methodology

Develop a complete Incident Response plan tailored on the client's specific environment along with incident response workflows

Training and Table-Top Exercises

Provide training sessions for existing incident handling workflows and post incident evaluations

Cybercrime investigation

Cyber Incident Response

Handle the aftermath of a cyber attack in a way that limits damage and reduces recovery time and costs.

HUMINT collection & investigation

Traditional investigative approaches, including interviewing witnesses, cross-check correlations of facts and support in government engagements

Digital Forensics

Find computer related crime evidence from digital media like a computer, mobile phone, server, or network.

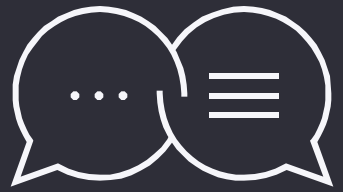
E-discovery

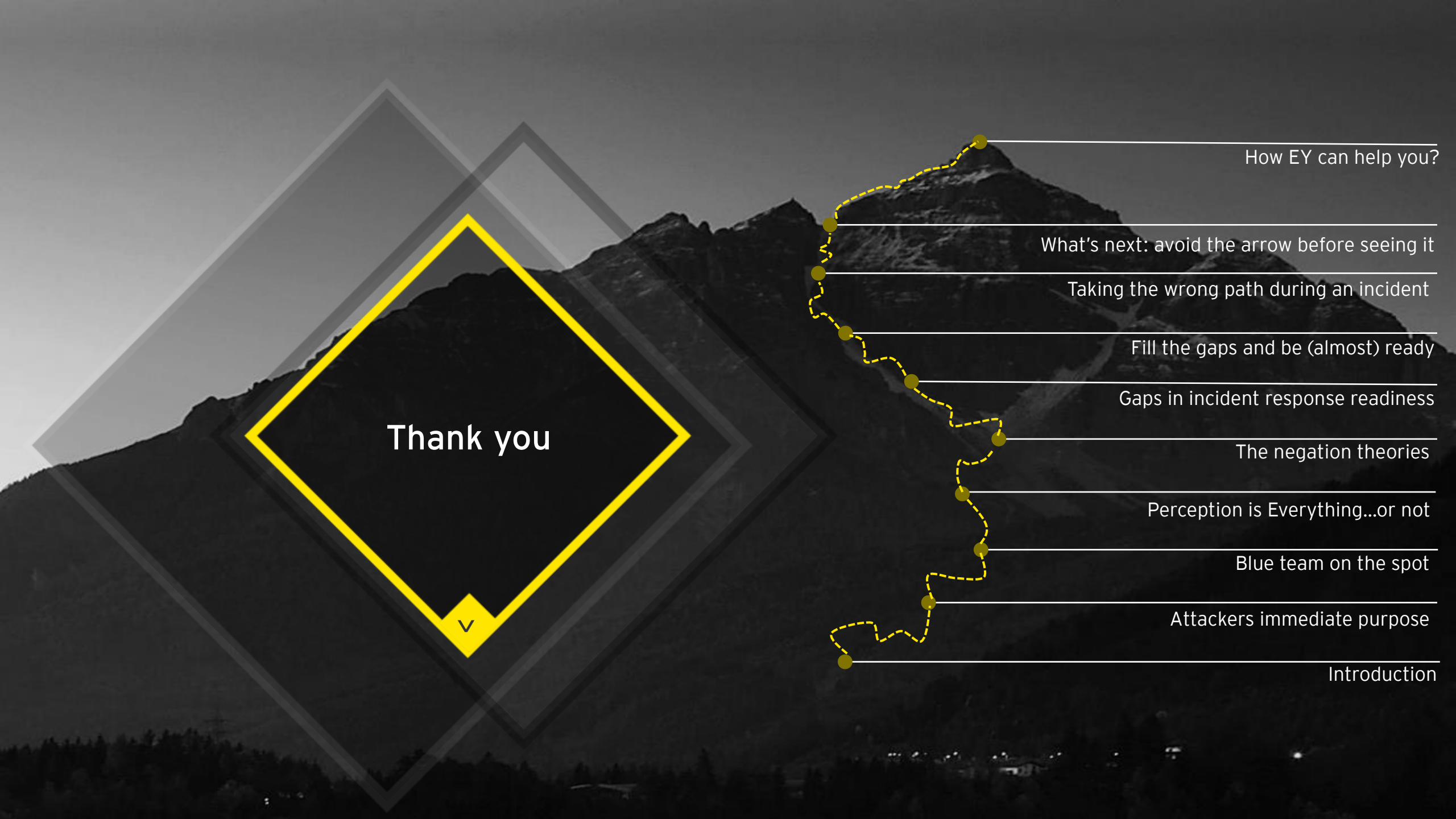
Collecting and analyzing electronically stored information in response to regulatory, fact-finding or legal demand.

Data-Analytics

The extensive use of data, statistical and quantitative analysis and predictive models to drive decision and actions

Q & A




Thank you
How EY can help you?
What's next: avoid the arrow before seeing it
Taking the wrong path during an incident
Fill the gaps and be (almost) ready
Gaps in incident response readiness
The negation theories
Perception is Everything...or not
Blue team on the spot
Attackers immediate purpose
Introduction