Challenges of an MSSP

MIKE BEHAM

JOHANN STOCKINGER

Who are we?

T SECURITY

MIKE BEHAM
Team Lead Security Operations Center

DEUTSCHE TELEKOM CYBER SECURITY AUSTRIA GMBH
Rennweg 97-99
1030 Vienna, Austria
behamm@telekom.com

T SECURITY

JOHANN STOCKINGER
Squad Lead Threat Hunting & Breach Containment

DEUTSCHE TELEKOM CYBER SECURITY AUSTRIA GMBH
Rennweg 97-99
1030 Vienna, Austria
stockingerj@telekom.com

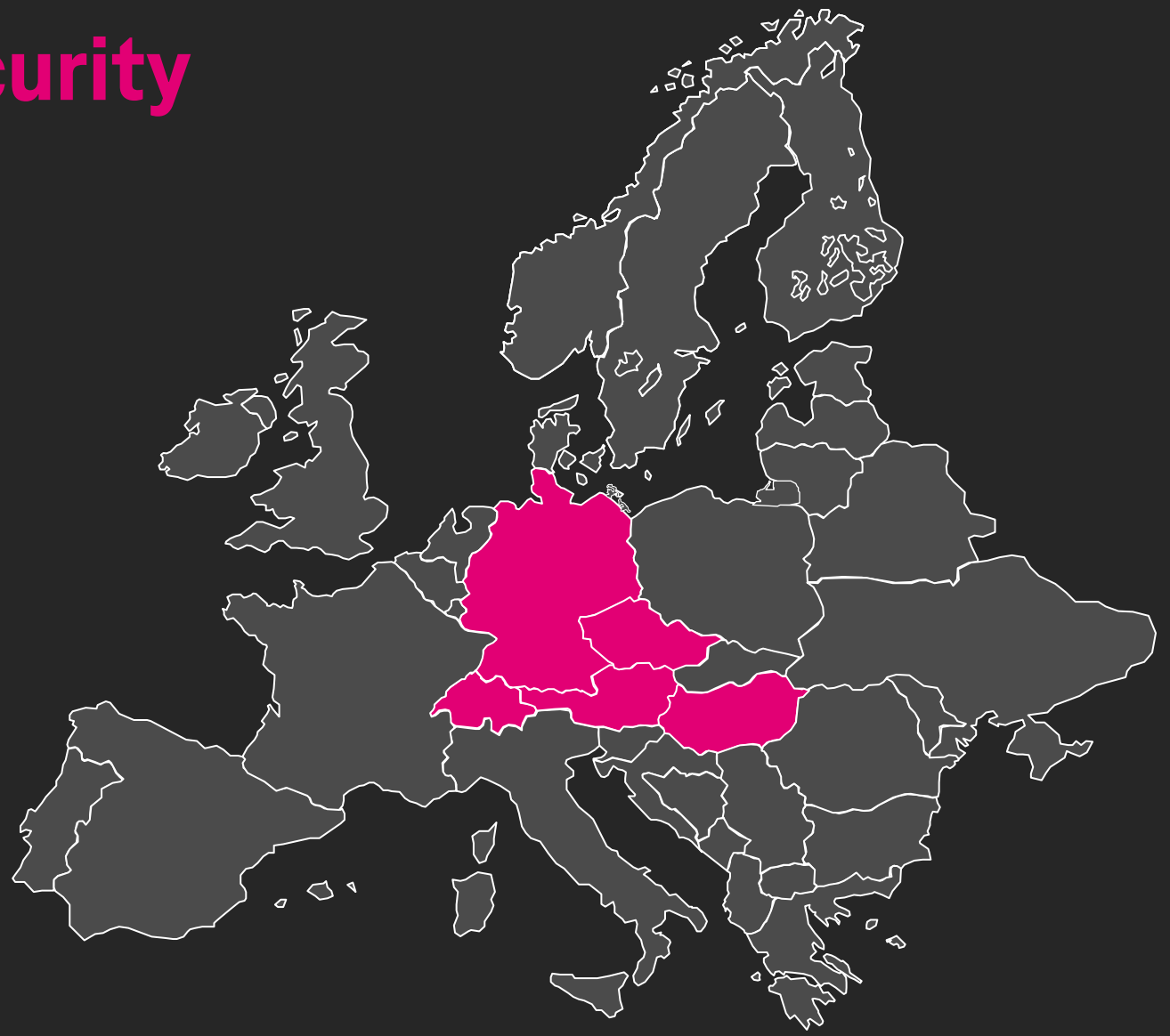
Deutsche Telekom Security

Securing **Deutsche Telekom** and its subsidiaries

Directly providing (managed) security services **to customers**

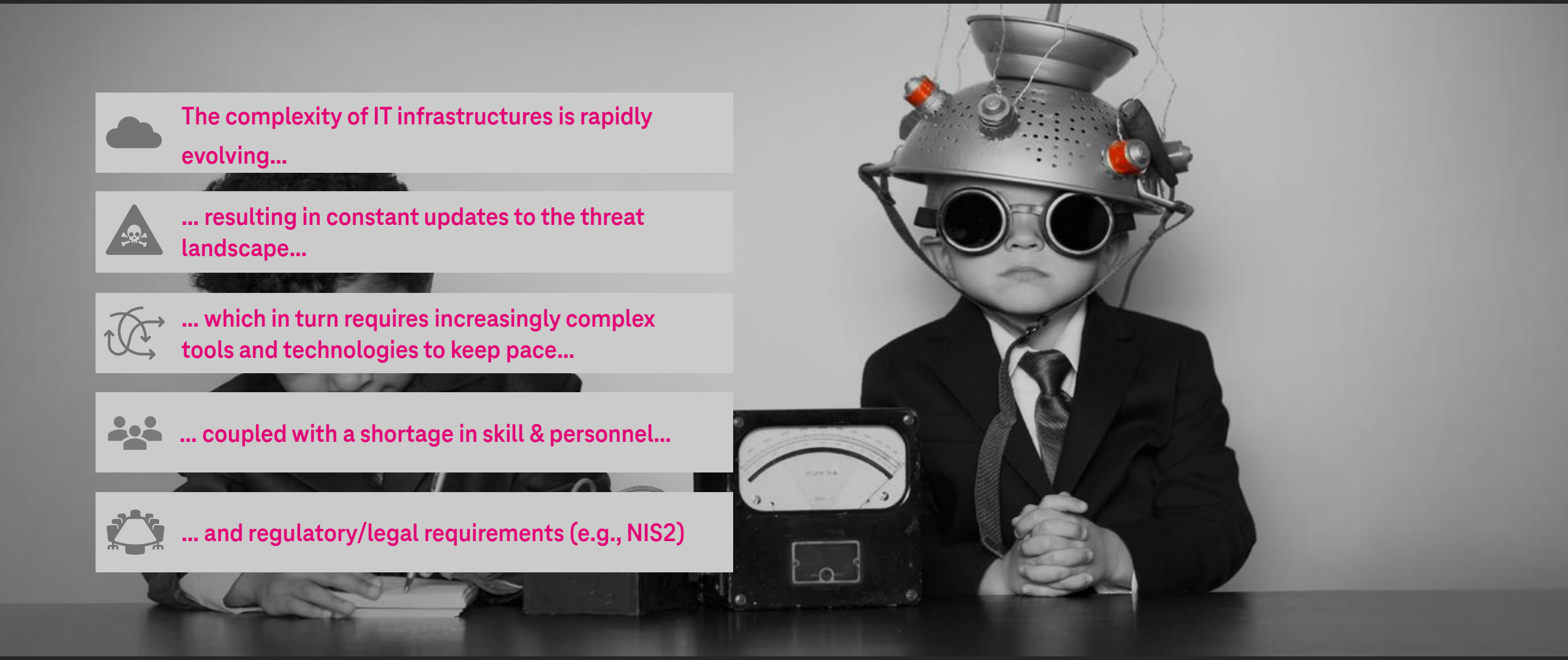
Five Security Operation Centers in Europe (DE, AT, CH, HU, and CZ)

Over **1.600** information security specialists



WE‘RE HIRING!

We live in challenging times...



- The complexity of IT infrastructures is rapidly evolving...
- ... resulting in constant updates to the threat landscape...
- ... which in turn requires increasingly complex tools and technologies to keep pace...
- ... coupled with a shortage in skill & personnel...
- ... and regulatory/legal requirements (e.g., NIS2)

MSSPs can provide and assist with...

- **Expertise**
- **Services**
  - Tools and technologies
  - Resources
- **Specialized knowledge in complex domains, e.g.:**
  - Identity
  - Endpoint
  - OT

Companies often outsource their challenges to MSSPs

MSSPs

The Role of Managed Security Service Providers

MSSPs face challenges as well

- **Obviously, we also deal with…**
  - Staying ahead of the threat landscape and technological advances
  - Skill shortage and talent retention
- **Some challenges are amplified…**
  - Scalability and resource management (e.g., providing IR retainers)
  - Complex regulations – especially cross-border
- **Additionally…**
  - Integration with customer environments – both directions!
  - “Bring your own tool stack”

Some issues we see

- **Lack of clear objectives and requirements**
- **Unrealistic expectations**
  - Going from 0 to 150%
  - Unreasonable time frames
  - Scalability and future needs
- **Overemphasis on cost**
- **Everyone wants references…**
  - But no one wants to be one

The Joy of Tenders

Wants, Reality, and Realistic Expectations

SLA Bondage

- **What could you want an SLA for?**
  - F/P ratios – on that note, what constitutes a false positive?
  - 99.95% uptime for **everything**, 99.9% malware detection…
  - Demand responsibilities without granting capabilities (e.g., access rights, …)
- **Instead, focus on reasonable KPIs**
  - Consider metrics such as time to react (TTR), service availability, …
  - Don’t define KPIs for the sake of having KPIs (e.g., F/P ratio)

May save a significant amount of money ☺

Manage my Assets

- **Establish asset management as part of the SIEM integration**
  - Ensure asset classification according to business criticality, service ownership, etc.
  - Keep asset data up-to-date – including new assets
- **Asset Management is important!**
  - But it should be a dedicated project
  - MSSP services cannot replace a CMDB – in fact, they often require one for proper delivery

No one knows assets better than their owners

The Red Button

- **A (semi) automatic method for isolating production sites**
  - To be triggered “at the discretion of SOC analysts”
  - Goal is to prevent the spread of ransomware…
- **Ransomware is a threat**
  - But it’s the final stage in an attack – after the infrastructure has been compromised

Emphasize prevention and detection across the entire attack chain

We all know MITRE ATT&CK, don't we?

- **Knowledge base of adversary tactics and techniques**
  - Foundation for development of specific threat models
  - Common taxonomy for both offense and defense
- **ATT&CK use cases incorporate a concept of coverage**
  - So obviously we should strife for 100% MITRE ATT&CK coverage, right?

MITRE ATT&CK

How to (kill)chain your SOC

MITRE Coverage

- **ATT&CK documents known adversary behavior**
- **It is NOT intended to provide a checklist of things that need to ALL be addressed**
  - MITRE themselves are very adamant about this in their design philosophy

> *The process of gathering intelligence, implementing defenses based on that intelligence, checking if those defenses work, and improving defenses to better cover threats over time is what should be strived for, not 100% coverage of ATT&CK.*

Thank You!