**PwC Blue Team Summit**

# Response to Cyber Threats

Are you interested in **current threat-based cyber defence methods?** Do you know why and how to carry out **Threat Hunting** and how to secure your **M365 environment** appropriately? Can you use **Threat Intelligence** at 110%?

Let us invite you to the **PwC Cyber Security Summit** where our **security specialists** will take you through six areas within which we will discuss the **SOC – Security Operations Centre**, its management, and what **the process of solving security incidents** looks like in a company's real **environment.**

**4 May 2022, 1.00 p.m. – 4.00 p.m.**

**PwC Czech Republic, Hvězdova 1734/2c, Prague 4**

**REGISTRATION**

The event will be held in **Czech**. Attendance is free of charge.

Feel free to contact Tereza Růžičková, at tereza.ruzickova@pwc.com, +420 732 934 119, with respect to any organisation issues related to the event.

Terms & Conditions concerning the event can be found here HERE.

## PROGRAMME

The Summit will be initiated by **Pavel Marťák, Cyber & Privacy Leader at PwC**. The topic will be presented by **Michal Wojnar, Cyber & Privacy, ISM & Threat Management at PwC**.

**12.30 p.m. – 1.00 p.m. Registration**

**1.00 p.m. – 4.00 p.m. Thematic lectures**

### Operating models of the SOC Expectations vs. reality

**Michal Wojnar**, Cyber & Privacy, ISM & Threat Management at PwC

What are the successful ways to build a first-class Security Operations Centre and what needs to be handled by the organisation in order to do so? The lecture will be focused on operating models, operating rate or outsourcing forms of supplies to the SOC (co-source, MSSP). Be aware of the value that a quality SOC can bring you!

### Cyber space defence using Microsoft Sentinel

**Dušan Obručník**, Cyber Security Professional at PwC

What does a hacker's attack at your company look like? We will take you through the attack from the perspective of the hackers as well as the security analysts, showing you the examples of defence automation using Microsoft Sentinel.

### Security incidents solution process

**Marek Nejedlý**, Head of Incident Response, DFIR & Threat Hunting at PwC

Do you know the difference between solving a security incident and forensic investigation? We will explain to you the difference and present to you the skills essential for a security incident expert. We will also discuss why you should have a security incident team ready and how long a typical response to an incident takes. You can also look forward to a practical example of cyber incident investigation.

### Use of Threat Intelligence

**Ondřej Šrámek**, Digital Forensics and Incident Response at PwC

These days, we are surrounded by information. Without context (information), detection and caution only solves a half of the problem, as you don't know what it was caused by. That's why the Threat Intelligence forms an important part of the Blue Team's work.

### Protection of the M365 environment

**Martin Zbořil**, Cloud Security Specialist at PwC

Thinking that an organisation can secure all the ways of potential user data leakage is naive. Minimising this risk within the Microsoft 365 environment by means of an appropriate combination of security measures is, on the other hand, essential. Or do you not care about data security at your organisation?

### Threat Hunting

**Marek Nejedlý**, Head of Incident Response, DFIR & Threat Hunting at PwC

Defence teams tend to remain passive and do not respond to individual incidents unless they actually take place. Let's not wait for an incident – be active and take on the initiative. Threat Hunting is a proactive part of defence where we actively search for attackers in your company's IT environment. We will present to you the individual stages of the Threat Hunting scenarios and show you a practical example of searching for attackers by means of the latest EDR technologies.

**4.00 p.m. Networking, refreshment**