Zákon o kybernetické bezpečnosti a SIEM

Course code: IBMSIEM

The course provides an overview of the Cybersecurity Act, its key concepts, and practical application. Participants will learn how to implement legal requirements, identify, and address cybersecurity threats. They will also gain hands-on experience in deploying and utilizing a SIEM system for monitoring and incident response. The course concludes with a discussion on trends, challenges, and best practices.

Course outline

Block I: Introduction to the Cybersecurity Act

- Introduction to Cybersecurity
- Definition of key terms in the Cybersecurity Act
- Framework of legal obligations and responsibilities in cybersecurity
- Practical aspects of compliance with the Act
- Implementation of basic rules and guidelines
- Identification and resolution of cybersecurity threats

Block II: The Role of SIEM in Meeting the Act's Requirements

- Functions and benefits of SIEM in the context of the Cybersecurity Act
- Monitoring and analysis of cybersecurity incidents
- Logging and reporting in compliance with legal standards
- Practical workshop – SIEM implementation
- Configuration and deployment of SIEM to meet legal requirements
- Simulation of cybersecurity incidents and their resolution using SIEM

Block III: Discussion and Conclusion

- Discussion – Experiences and opinions of participants
- Sharing insights and best practices in cybersecurity
- Debates on current trends and challenges

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk