BLANBU
Beyond Cybersecurity

CYBER SECURITY TRAINING

Training program · 2025

Practical training for your whole team

From cybersecurity fundamentals for employees to advanced techniques for IT professionals — in English or Lithuanian, on-site or remote, with a certificate.

blanbu.com · info@blanbu.lt · +370 600 60680

01 About the training

Blanbu cybersecurity training gives your team practical skills to identify threats, protect data and respond properly to incidents. Sessions are delivered in **English or Lithuanian**, **on-site or remotely**, and each participant receives a **certificate** on completion.

Required under NIS2. Under the EU NIS2 directive, management must ensure employees receive regular cybersecurity training. Basic training satisfies this requirement and provides documented proof (certificates) for audits.

Also available as video. The basics come with the Starter plan (for new hires); the full program (advanced, AI, NIS2) comes with Pro and Enterprise — continuously updated as new threats emerge.

02 Basic Cyber Security Training

Duration	Audience	Languages	Format
4 hours	Employees	EN / LT	On-site / remote

Topics

- › Cyber security fundamentals
- › Modern identity security (MFA, passkeys)
- › Phishing: email, SMS, QR & BEC (exec impersonation)
- › AI threats & deepfake fraud
- › Safe use of AI tools at work
- › Ransomware awareness & protection
- › Data protection & GDPR
- › Social engineering
- › Remote & hybrid work security
- › Incident response
- › Practical exercises
- › Open discussion

Learning outcomes

- ✓ Understand modern threats, including AI-driven attacks and ransomware
- ✓ Recognise phishing across every channel — email, SMS, QR and BEC
- ✓ Use MFA / passkeys and handle AI tools without leaking company data
- ✓ Respond effectively to potential security incidents

03 Advanced Cyber Security Training

Duration	Audience	Languages	Format
8 hours	IT professionals	EN / LT	Hands-on

Topics

- › Network security architecture & Zero Trust
- › Identity & access management (IAM)
- › Cloud & container security (Kubernetes, SaaS)
- › Vulnerability management
- › Detection engineering & MITRE ATT&CK;
- › SIEM, log analysis & threat hunting
- › Penetration testing methodology
- › Ransomware & malware analysis
- › AI / ML security
- › Incident response frameworks
- › Secure development (DevSecOps, OWASP)
- › Hands-on lab exercises

Learning outcomes

- ✓ Design Zero Trust network and identity architecture
- ✓ Secure cloud and container environments
- ✓ Detect threats using SIEM, MITRE ATT&CK; and threat hunting
- ✓ Lead an incident response process, including ransomware

04 Specialized courses

Course	Duration	What it covers
AI Security	4 hours	Safe use of AI tools · AI phishing & deepfakes · Data-leak prevention · Building an AI policy
NIS2 Compliance Workshop	1 day	NIS2 requirements · Risk management · Policy templates · Audit preparation
Individual Training	Flexible	Tailored curriculum · Role-specific focus · Flexible schedule · 1:1 or small group

05 How to book

1 Get in touch
Tell us the level (Basic / Advanced / specialized), team size and language.

2 We tailor the program
We adapt topics and examples to your industry and current security posture.

3 We schedule a date
On-site at your office or remote, at a time that suits your team.

4 Training & certificates
We deliver the session and issue a certificate of completion to each participant.

Book your training: info@blanbu.lt · +370 600 60680 · blanbu.com