

Enable your cybersecurity teams to experience, first-hand, a real-life cyberattack, performed by actual hackers. Working together to mitigate the attack, they will collect live evidence and begin their forensic investigation.

Advanced Forensics Collection in MS Windows

CybergymIEC's Advanced Forensics Collection training will give your team the opportunity to gain practical hands-on experience of defending against a complex malware MS Windows hacking scenario.

Through a series of lectures and practical exercises at one of CybergymIEC's secure training arenas, your team will work together to beat our team of professional Red Hat hackers, gaining an understanding of essential tools and the skills they need to perform at their peak when duty calls.



Participants

- IT/ OT Professionals
- Incident Response Team Members
- Tier 2-3 Security Analysts



Prerequisites

- Understanding of basic information security concepts and tools
- Familiarity with basic computer and operating system architecture
- Basic knowledge of the principles of ethical hacking and penetration testing
- Acquaintance with the key concepts of cybersecurity forensics, such as exploitation, vulnerabilities and information gathering
- Highly recommended: Graduation from CybergymIEC's Basic Windows Forensics (166EN) Training



Training Outcomes

- Deep familiarity with the internal mechanisms of a cyber malware attack
- Understanding of the theory and the practical skills required to perform cyber forensics, in a complex OT/IT environment



Duration

- 16 hours (2 x 8-hour days)