BLUEMARK ACADEMY

Burgundy Team Cyber Security

Duration: 5 Days · **Training format:** Virtual Classroom / Online

Description

For those involved in daily cybersecurity operations, it is a special training program developed to address a significant deficiency in the current training approach.

Those who receive cyber-attack-oriented trainings cannot use the knowledge and skills they acquire here in their daily work. Performing an infiltration test between the tasks of the IT unit constitutes very little part of the daily operation. Therefore, a large part of the knowledge and skills acquired under the title of ethical hacking cannot be used. On the other hand, since defense-oriented information security management trainings are given at the theoretical level, they cannot provide participants with concrete skills that can be used.

In order to address these deficiencies and adapt the traditional blue team / red team approach to the real situation of today's cyber attacks, Sparta has developed the Burgundy Team Training. The aim of the training is to provide the participants with the concrete skills they need and can use in their daily work. Participants gain the skills to simulate cyber attacks while increasing their competence in detecting and preventing attacks.

Delegates will learn

- Cyber Security Theory
- Ethical Hacking
- Penetration Tests
- Package Analysis
- Log Analysis
- Compatibility
- System Analysis

Outline

Cyber Security Theory

- Historical development of cyber attacks
- Current cyber threats
- Anatomy of an attack
- Information security theory

Ethical Hacking

- Types of cyber attacks

- Cyber-attack cycle
- Exploration and screening
- Vulnerability detection

Penetration Tests

- Attacks targeting scanners
- Exploiting known vulnerabilities
- DoS/DDoS attacks
- Attacks on web applications
- SOME (Cyber Incident Response Team)
- Cyber incident detection
- Cyber incident response
- Forensics and Network forensics

Package Analysis

- Capturing traffic on the network
- Principles of Traffic analysis
- Wireshark usage
- Detection of network problems

Log Analysis

- Determination of log sources
- Log collection and monitoring methods
- Log analysis techniques
- Attack detection from logs

Compatibility

- ISO 27001, PCI-DSS, NIST and SANS Critical Controls

System Analysis

- Log review on Windows
- Log review on Linux systems
- Logs and command line tools created by basic attacks

Prerequisites

At least two years of experience in the field of information security

Advanced knowledge of TCP / IP