BLACKBIRD FOR TRAINING

Advanced User Security & Risk Management



Advanced User Security & Risk Management

Introduction

This course provides an advanced and specialized program in user security, focusing on protecting users, accounts, identities, and privileges from modern cyber threats. It covers human-factor risks, Identity and Access Management IAM, account protection, advanced authentication, social engineering and phishing, insider threats, user behavior monitoring, and user risk management.

The course emphasizes a practical approach through real-world case studies and scenarios that help participants identify user-related risks, detect suspicious activities, and take appropriate measures to protect systems and data.

Course Objectives

By the end of the course, participants will be able to:

- Understand security risks associated with users and the human factor.
- Assess and classify user and account risks.
- Strengthen the protection of identities, accounts, and privileges.
- Apply Identity and Access Management IAM principles.
- Apply Multi-Factor Authentication MFA and modern authentication methods.
- Apply the Principle of Least Privilege.
- Understand and apply Zero Trust principles.
- Detect and analyze phishing and social engineering attacks.
- Identify indicators of insider threats and unusual user behavior.
- Monitor and analyze users' security activities.
- Develop effective approaches to user risk management.

Training Outline

Day 1: User Security Management & Risk Assessment

1. The Role of Users and the Human Factor in Cybersecurity
2. Modern Threats Targeting Users
3. User Risk Assessment and Risk Classification
4. Account, Identity, and Privilege Management
5. Case Study: Assessing User and Account Risks Within an Organization



Day 2: Identity, Authentication & Access Control

1. Identity and Access Management IAM
2. Multi-Factor Authentication MFA
3. Password, Account, and Authentication Security
4. The Principle of Least Privilege
5. Zero Trust and Secure User Access Control

Day 3: Phishing & Social Engineering

1. Phishing and Spear Phishing
2. Social Engineering and User Targeting Techniques
3. Account Takeover and Business Email Compromise BEC
4. Identifying Suspicious Messages, Links, and Communications
5. Analyzing a Targeted Phishing Attack and User/Organizational Response

Day 4: Insider Threats & User Behavior Monitoring

1. Insider Threats and Sources of User-Related Risks
2. Identifying Unusual Behavior and High-Risk Indicators
3. User Activity Monitoring and Behavior Analysis
4. Data Protection and Prevention of Unauthorized Access or Disclosure
5. Detecting Unusual User Activity and Analyzing Associated Risks
6. Final Case Study: Analyzing User Risk and Developing Appropriate Protection and Response Measures

Why Attend This Course? — Wins & Losses

Wins

- Strengthen the protection of users and accounts against cyber threats.
- Improve identity, access, and privilege management.
- Enhance the ability to detect phishing and social engineering attacks.
- Improve the detection of insider threats and suspicious behavior.
- Strengthen user risk monitoring.
- Develop an advanced organizational approach to human-related risk management.

Losses if These Risks Are Not Addressed

- Increased risk of user account compromise.
- Unauthorized access to systems and data.
- Greater exposure to phishing and social engineering attacks.
- Difficulty detecting unusual user activities.
- Increased risk of data leakage or misuse of privileges.
- Greater operational impact from incidents resulting from compromised users.



Conclusion

This course provides an advanced and practical approach to protecting users and managing user-related risks, with a focus on identity and access, authentication, social engineering, phishing, insider threats, and user behavior monitoring.

Through practical case studies and applied scenarios, participants will gain the knowledge and skills required to identify user-related risks and strengthen the protection of accounts, data, and systems

