BTA-BSEC: Blockchain Security

Course Code: BTA-BSEC
Duration: 3 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

This dynamic Blockchain Security course covers all known aspects of Blockchain security that exist in the Blockchain environment today. This course provides a detailed overview of all Blockchain security issues, including threats, risk mitigation, node security integrity, confidentiality, best security practices, advanced Blockchain security and more. The in-depth lab sessions will provide the student with practical, real world tools for not only recognizing security threats, but mitigation and prevention as well.

SKILLS COVERED

Those who attend the Security for Blockchain Professionals course and pass the exam certification will have a demonstrated knowledge of:

- Identifying and differentiating between security threats and attacks on a Blockchain network.
- Blockchain security methods, best practices, risk mitigation, and more.
- All known (to date) cyber-attack vectors on the Blockchain.
- Performing Blockchain network security risk analysis.
- A complete understanding of Blockchain's inherent security features and risks.
- An excellent knowledge of best security practices for Blockchain System/Network Administrators.
- Demonstrating appropriate Blockchain data safeguarding techniques.

WHO SHOULD ATTEND?

Existing architects, software developers, system and network administrators who are responsible for implementing, identifying, and managing security on their Blockchain network. Also, those who are responsible for, and are required to mitigate, recognize, and resolve Blockchain security problems. Students will participate in security labs which will go in-depth into security best practices, known attack vectors, threat identification, response techniques, and much more.

Due to the in-depth focus on technical cyber-security methods, and the broad scope of this course, those with current cyber-security knowledge, Blockchain architecture, and/or experienced programmers will benefit the most from this course, including:

- Blockchain Architects
- Blockchain Developers
- Application Developers
- Blockchain System Administrators
- Network Security Architects
- Cyber Security Experts
- IT Professionals w/cyber security experience

PREREQUISITES

This course is highly technical. To prepare for the class student should know:

- Have a comprehensive understanding of Hyperledger, Ethereum, or Blockchain Architecture

MODULES

Module 1: Fundamental Blockchain Security

- Cryptography for the Blockchain
- A Brief Introduction to Blockchain
- Blockchain Security Assumptions

- Limitations of Basic Blockchain Security

Module 2: Consensus in the Blockchain

- Blockchain Consensus and Byzantine Generals
- Introduction to Blockchain Consensus Security

- Proof of Work

- Proof of Stake
- Other Blockchain Consensus Algorithms

Module 3: Advanced Blockchain Security Mechanisms

- Architectural Security Measures
- Permissioned Blockchains
- Checkpointing
- Advanced Cryptographic Solutions

- Multiparty Signatures

- Zero-Knowledge Proofs
- Stealth Addresses
- Ring Signatures
- Confidential Transactions

Module 4: Smart Contract Security

- Introduction to Smart Contracts
- Smart Contract Security Considerations
- Smart Contract Code Auditing

Module 5: Blockchain Risk Assessment

- Blockchain Risk Considerations
- Regulatory Requirements
- Blockchain Architectural Design

Module 6: Basic Blockchain Security

- User Security
- Node Security
- Network Security

Module 7: Blockchain for Business

- Introduction to Ethereum Security
- Introduction to Hyperledger Security
- Introduction to Corda Security

Module 8: Securely Implementing Business Blockchains

- Business Operations
- Data Management
- Infrastructure
- Legal and Regulatory Compliance

Module 9: Network-Level Vulnerabilities and Attacks

- 51% Attacks
- Denial of Service Attacks
- Eclipse Attacks
- Replay Attacks
- Routing Attacks
- Sybil Attacks

Module 10: System-Level Vulnerabilities and Attacks

- The Bitcoin Hack
- The Verge Hack
- The EOS Vulnerability
- The Lisk Vulnerability

Module 11: Smart Contract Vulnerabilities and Attacks

- Reentrancy
- Access Control
- Arithmetic
- Unchecked Return Values
- Denial of Service
- Bad Randomness
- Race Conditions
- Timestamp Dependence

- Short Addresses

Module 12: Security of Alternative DLT Architectures

- Introduction to DAG-Based DLTs
- Advantages of DAG-Based DLTs
- Limitations of DAG-Based DLTs

END OF PAGE