Cyber Shield Intelligence

CSI

CYBER SHIELD

INTELLIGENCE

TRANING CATALOG

Register and start training now.

Artificial Intelligence Training

Master AI skills for future success.

Cyber Security Training

Build essential cybersecurity skills for digital protection.

TABLE OF CONTENTS

Contents

LETTER FROM THE Founders

Dear Valued Partner,

It is with great pride and purpose that we present to you the training catalog of Cyber Shield Intelligence. As founders, we are driven by a shared vision—to empower individuals and organizations with the knowledge and skills needed to navigate the fast-evolving worlds of Artificial Intelligence and Cybersecurity.

In a time when digital transformation is no longer optional, but essential, the demand for intelligent systems and resilient security has never been greater. Our programs are thoughtfully designed to equip professionals with cutting-edge expertise, real-world insights, and hands-on capabilities that meet today's challenges and anticipate tomorrow's threats.

We believe in building more than just technical skills—we aim to develop future leaders in AI and Cybersecurity who can think critically, act ethically, and innovate boldly. Whether you're an individual seeking to upskill or an organization striving for excellence, our training pathways are built to support your growth and strategic goals.

Thank you for placing your trust in us. We are honored to be part of your journey toward mastery and impact in two of the most transformative domains of our time.

With sincere regards,
The Founders
Cyber Shield Intelligence

About us
Cyber Shield Intelligence

Cyber Shield Intelligence is a pioneering company specializing in Artificial Intelligence and Cybersecurity consultancy, training, and integrated technology solutions. We offer comprehensive programs in both Arabic and English, designed to equip professionals with the practical skills and strategic insight required to excel in today's rapidly evolving digital landscape.

Our training covers a broad spectrum of critical topics, including AI-powered intrusion detection, incident response, cloud security, and regulatory compliance—tailored for cybersecurity defenders, analysts, operators, and managers. In addition to professional development, we are committed to raising cybersecurity awareness across communities and fostering a culture of digital resilience.

At Cyber Shield Intelligence, we are dedicated to building the next generation of experts, leaders, and innovators in AI and Cybersecurity.

5

Introduction to Artificial Intelligence [5 Days]

Brief Descritpion

In this course, participants will explore the foundations of AI, from basic concepts to practical applications, and gain a comprehensive understanding of this transformative technology.

Throughout the course, participants will engage in lectures, demonstrations, hands-on exercises, and discussions to gain a comprehensive understanding of artificial intelligence fundamentals and applications. Guest speakers from industry and academia may be invited to share their expertise and insights into AI trends and advancements. Participants will also have the opportunity to work on practical AI projects to reinforce their learning and develop practical skills in AI development and implementation.

AI Applications by Industries [4 Days]

Brief Description

This course explores how artificial intelligence is applied across diverse industries—such as healthcare, finance, insurance, and cybersecurity—to solve domain-specific security challenges.

When delivered to specific organizations, the course content and hands-on labs are customized to reflect the unique operational context, risks, and data environments of that industry.

Participants will examine practical use cases including fraud detection, risk analysis, and security automation, while building cross-industry adaptability with AI tools and workflows.

AI Specialization by Industries [5 Days]

Brief Description

Building on the applications course, this advanced program dives deeper into specialized AI techniques as applied in specific industries.

When requested by organizations, the course can be tailored to their domain—healthcare, finance, cyber, or others—to reflect industry-specific challenges, data types, and threat models.

Participants will explore adversarial machine learning, deep learning, federated learning, privircy pre serving and predictive modeling, culminating in the design of robust AI cybersecurity solutions fit for their sector.

The foundations of cybersecurity [3 Days]

Brief Description

In this course, participants will build a solid understanding of key concepts, techniques, and best practices in the cybersecurity field. Participants will explore the fundamentals of risk management, encryption, and network security, equipping themselves with the knowledge to establish a robust foundation for securing digital environments.

Each session will include a combination of lectures, interactive discussions, case studies, and hands-on exercises to reinforce learning objectives. Participants will also have access to relevant resources and materials for further exploration of topics covered in the course.

Cybersecurity Strategy, Leadership, and Management [3 Days]

Brief descritpion

In this course, participants will explore the critical aspects of developing, leading, and managing effective cybersecurity strategies. Participants will gain insights into strategic decision-making, risk management, and leadership skills, empowering them to navigate the complexity of cybersecurity and contribute to the resilience of organizations.

Throughout the course, participants will engage in interactive discussions, case studies, and practical exercises tailored to the UAE cybersecurity landscape. Guest speakers and experts from the UAE cybersecurity industry may be invited to share insights and experiences relevant to the course topics.

Cybersecurity Awareness [3 Days]

Brief Description

This course is crafted to empower participants with the knowledge and skills needed to address common threats effectively. Exploring fundamental principles, offering practical tips, and highlighting best practices, the course ensures participants remain vigilant and play an active role in maintaining a secure digital environment.

Throughout the course, participants will engage in interactive discussions, case studies, and hands-on activities to reinforce cybersecurity awareness principles and best practices. Additionally, real-world examples and scenarios relevant to participants' personal and professional lives will be incorporated to enhance learning outcomes.

Cybersecurity Risk Management and Business Continuity [5 Days]

Brief Description

In this course, participants will navigate the complex landscape of digital threats and ensure organizational resilience. Participants will learn strategic risk assessment, mitigation strategies, and business continuity planning to secure critical assets and maintain operational integrity in the face of cyber challenges.

Throughout the course, participants will engage in lectures, case studies, group discussions, and practical exercises to reinforce key concepts and skills related to cybersecurity risk management and business continuity. Guest speakers and experts may be invited to share insights and experiences relevant to the course topics.

Cyber Crimes, Cyber Terrorism, and Cyber Warfare [3 Days]

Brief Description

In this course, participants will explore a wide range of criminal activities, terrorism, and state-sponsored warfare in the cyber domain. Participants will gain insights into the motives, tactics, and preventive measures to protect against and respond to the diverse challenges posed by cyber threats.

Throughout the course, participants will engage in lectures, case studies, group discussions, and simulations to deepen their understanding of cyber crimes, cyber terrorism, and cyber warfare. Practical exercises and scenarios will be used to explore preventive measures and response strategies to combat cyber threats effectively.

National Policy Analysis [3 Days]

Brief Descritpion

In this course, participants will gain a comprehensive understanding of crafting, evaluating, and implementing policies at the national level. Participants will explore the intersection of cybersecurity, governance, and national security, developing the expertise needed to contribute to effective policy frameworks.

Digital Transformation and Cyber Resilience [5 Days]

Brief Description

In this course, participants will explore the synergy between technological evolution and cybersecurity readiness. Participants will learn to implement resilient cybersecurity measures when navigating to the digital world, ensuring that their organizations thrive in the everchanging technological advancement. Throughout the course, participants will engage in lectures, case studies, group discussions, and hands-on exercises to deepen their understanding of digital transformation and cyber resilience. Guest speakers and industry experts may be invited to share insights and practical experiences relevant to the course topics. Participants will also have the opportunity to apply their learning through practical exercises and develop actionable plans to enhance cyber resilience in their organizations.

Introduction to Cryptography [5 Days]

Brief Description

Throughout the course, participants will engage in lectures, demonstrations, practical exercises, and discussions to gain a comprehensive understanding of cryptographic principles and techniques. Guest speakers from industry and academia may be invited to share their expertise and insights into cryptography trends and advancements. Participants will also have the opportunity to work on practical cryptographic projects to reinforce their learning and develop practical skills in cryptography.

Cyber Threat Intelligence [3 Days]

Brief Description

Throughout the course, participants will engage in lectures, case studies, hands-on exercises, and discussions to develop their skills in cyber threat intelligence analysis and operationalization. Guest speakers from industry and government may be invited to share real-world experiences and insights into threat intelligence practices. Participants will also have the opportunity to apply their knowledge through practical exercises and scenarios simulating threat intelligence analysis and response.

Metaverse Security [5 Days]

Brief Description

Throughout the course, participants will engage in lectures, case studies, hands-on exercises, and discussions to develop their skills in metaverse security. Guest speakers from industry, academia, and virtual reality communities may be invited to share their expertise and insights into metaverse security practices and challenges. Participants will also have the opportunity to apply their knowledge through practical exercises and scenarios simulating metaverse security threats and responses.

Wireless Security [5 Days]

Brief Description:

Throughout the course, participants will engage in lectures, demonstrations, hands-on exercises, and discussions to develop their skills in wireless security. Guest speakers from industry and academia may be invited to share their expertise and insights into wireless security practices and challenges. Participants will also have the opportunity to apply their knowledge through practical exercises and scenarios simulating wireless security threats and responses.

Web Security [5 Days]

Brief Description:

Throughout the course, participants will engage in lectures, demonstrations, hands-on exercises, and discussions to develop their skills in web security. Guest speakers from industry and academia may be invited to share their expertise and insights into web security practices and challenges. Participants will also have the opportunity to apply their knowledge through practical exercises and scenarios simulating web security threats and responses.

Artificial Intelligence (AI) and Cybersecurity [5 Days]

Brief Description:

Throughout the course, participants will engage in lectures, hands-on exercises, case studies, and discussions to develop their skills in using AI for cybersecurity. Guest speakers from industry and academia may be invited to share their expertise and insights into AI-driven cybersecurity solutions. Participants will also have the opportunity to apply their knowledge through practical exercises and simulations simulating AI-powered threat detection, incident response, vulnerability management, and threat intelligence analysis.

Digital Forensics and Investigation [5 Days]

Brief Description

Throughout the course, participants will engage in lectures, hands-on exercises, case studies, and discussions to develop their skills in digital forensics and investigation. Guest speakers from industry and law enforcement may be invited to share their expertise and insights into digital forensic practices. Participants will also have the opportunity to apply their knowledge through practical exercises and simulations simulating digital forensic investigations and incident response scenarios.

Access Control System Design and Planning [5 Days]

Brief Description

Throughout the course, participants will engage in lectures, case studies, hands-on exercises, and discussions to develop their skills in access control system design and planning. Guest speakers from industry and security consulting may be invited to share their expertise and insights into access control best practices. Participants will also have the opportunity to apply their knowledge through practical exercises and simulations simulating access control system design and planning scenarios.

Red Team [3 Days]

Brief Description

Throughout the course, participants will engage in lectures, hands-on labs, group discussions, and practical exercises to reinforce their understanding of red team operations and techniques. Real-world scenarios and case studies will be used to illustrate concepts and demonstrate the application of red team methodologies. Guest speakers with experience in red teaming may be invited to share insights and best practices.

Cloud Security [5 Days]

Brief Description

Throughout the course, participants will engage in lectures, hands-on labs, group discussions, and case studies to reinforce their understanding of cloud security concepts and best practices. Real-world scenarios and examples will be used to illustrate concepts and demonstrate practical application.

Penetration Testing [5 Days]

Brief Description

Throughout the course, participants will engage in lectures, hands-on labs, group discussions, and practical exercises to reinforce their understanding of penetration testing concepts and techniques. Real-world scenarios and case studies will be used to illustrate concepts and demonstrate practical application.

IT-OT-IoT Monitoring [5 Days]

Brief Description

Throughout the course, participants will engage in lectures, hands-on labs, group discussions, and case studies to reinforce their understanding of IT-OT-IoT monitoring concepts and techniques. Real-world scenarios and examples will be used to illustrate concepts and demonstrate practical application. Participants will also have access to resources and tools to support their learning journey in IT-OT-IoT monitoring.

Blue Team [3 Days]

Brief Description

Throughout the course, participants will engage in lectures, hands-on labs, group discussions, and practical exercises to reinforce their understanding of blue team operations concepts and techniques. Real-world scenarios and examples will be used to illustrate concepts and demonstrate practical application. Participants will also have access to resources and tools to support their learning journey in blue team operations.

Crisis Management [3 Days]

Brief Description

Throughout the course, participants will engage in lectures, group discussions, case studies, and tabletop exercises to reinforce their understanding of crisis management concepts and techniques. Real-world scenarios and examples will be used to illustrate concepts and demonstrate practical application.

Monitoring and Operations [4 Days]

Brief Description

Throughout the course, participants will engage in lectures, hands-on labs, group discussions, and practical exercises to reinforce their understanding of security monitoring and operations concepts and techniques. Real-world scenarios and examples will be used to illustrate concepts and demonstrate practical application. Participants will also have access to resources and tools to support their learning journey in monitoring and operations.

Compliance in Depth [3 Days]

Brief Description

Throughout the course, participants will engage in lectures, case studies, group discussions, and practical exercises to reinforce their understanding of compliance concepts and techniques. Real-world scenarios and examples will be used to illustrate concepts and demonstrate practical application. Participants will also have access to resources and tools to support their learning journey in compliance management.

Security Architecture and Engineering [5 Days]

Brief Description

Throughout the course, participants will engage in lectures, case studies, group discussions, and practical exercises to reinforce their understanding of security architecture and engineering concepts and techniques. Real-world scenarios and examples will be used to illustrate concepts and demonstrate practical application. Participants will also have access to resources and tools to support their learning journey in security architecture and engineering.

Security Orchestration, Automation & Response (SOAR) [5 Days]

Brief Description

Throughout the course, participants will engage in lectures, hands-on labs, group discussions, and practical exercises to reinforce their understanding of SOAR concepts and techniques. Real-world scenarios and examples will be used to illustrate concepts and demonstrate practical application. Participants will also have access to resources and tools to support their learning journey in security orchestration, automation, and response.

SIEM With Tactical Analysis [3 Days]

Brief Description

Throughout the course, participants will engage in lectures, hands-on labs, group discussions, and practical exercises to reinforce their understanding of SIEM concepts and techniques. Real-world scenarios and examples will be used to illustrate concepts and demonstrate practical application. Participants will also have access to resources and tools to support their learning journey in SIEM with tactical analysis.

Advanced IR & Threat Hunting Bootcamp [3 Days]

Brief Description

Throughout the course, participants will engage in lectures, hands-on labs, group discussions, and scenario-based exercises to reinforce their understanding of advanced incident response and threat hunting concepts and techniques. Real-world scenarios and examples will be used to illustrate concepts and demonstrate practical application. Participants will also have access to resources and tools to support their learning journey in advanced IT and threat hunting.

Intrusion Detection [3 Days]

Brief Description

Throughout the course, participants will engage in lectures, hands-on labs, group discussions, and practical exercises to reinforce their understanding of intrusion detection concepts and techniques. Real-world scenarios and examples will be used to illustrate concepts and demonstrate practical application. Participants will also have access to resources and tools to support their learning journey in intrusion detection.

Purple Team [3 Days]

Brief Description

Throughout the course, participants will engage in lectures, hands-on labs, group discussions, and practical exercises to reinforce their understanding of purple teaming concepts and techniques. Real-world scenarios and examples will be used to illustrate concepts and demonstrate practical application. Participants will also have access to resources and tools to support their learning journey in purple teaming.

CompTIA Network+ [5 Days]

Brief Description

Throughout the course, participants will engage in lectures, hands-on labs, group discussions, and practice exams to reinforce their understanding of networking concepts and prepare for the CompTIA Network+ certification exam. Guest speakers with industry expertise may be invited to share insights and real-world examples. Participants will also have access to study materials and resources to support their certification preparation journey.

CompTIA A+ [5 Days]

Brief Description

Throughout the course, participants will engage in lectures, hands-on labs, group discussions, and practice exams to reinforce their understanding of computer hardware, software, networking, and security concepts and prepare for the CompTIA A+ certification exam. Guest speakers with industry expertise may be invited to share insights and real-world examples. Participants will also have access to study materials and resources to support their certification preparation.

CompTIA Security+ [5 Days]

Brief Description

Throughout the course, participants will engage in lectures, hands-on labs, group discussions, and practice exams to reinforce their understanding of cybersecurity concepts and prepare for the CompTIA Security+ certification exam. Guest speakers with industry expertise may be invited to share insights and real-world examples. Participants will also have access to study materials and resources to support the possible certification preparation.

CompTIA PenTest+ [5 Days]

Brief Description

Throughout the course, participants will engage in lectures, hands-on labs, group discussions, and practical exercises to reinforce their understanding of penetration testing concepts and prepare for the CompTIA PenTest+ certification exam. Guest speakers with industry expertise may be invited to share insights and real-world examples.

Certified Ethical Hacker (CEH) [5 Days]

Brief Description

Throughout the course, participants will engage in lectures, hands-on labs, group discussions, and practical exercises to reinforce their understanding of ethical hacking concepts and prepare for the CEH certification exam. Guest speakers with industry expertise may be invited to share insights and real-world examples. Participants will also have access to study materials and resources to support their certification preparation.

Certified Cloud Security Professional (CCSP) [5 Days]

Brief Description

Throughout the course, participants will engage in lectures, hands-on labs, group discussions, and case studies to reinforce their understanding of cloud security concepts and prepare for the CCSP certification exam. Guest speakers with industry expertise may be invited to share insights and real-world examples.

AI Programmable Robots [5 Days]

Brief Description

Throughout the course, participants will learn how to design, program, and operate intelligent robots. It combines theoretical knowledge with practical, hands-on exercises. Learners gain skills in automation, problem-solving, and AI applications. The program prepares participants to implement robotics solutions effectively.

Cybersecurity War Games [5 Days]

Brief Description

Throughout the course, participants will engage in cybersecurity war games that simulate real-world attacks and defenses. They learn to identify vulnerabilities, respond to threats, and strengthen system security. The training combines theoretical concepts with hands-on exercises. Participants gain practical skills to protect and defend organizational networks effectively.

Cyber Shield Intelligence
CSI

2025
Abu Dhabi

Contact Us
+97150-690-65-65
cybershieldintelligencellc@gmail.com