Cybersecurity Summer School Program
CyberFuture

22-24 November 2023, Cape Town, South Africa

DAY 1: Wednesday, 22nd November 2023
Cyber Foundations

8:00 – 9:00:	Registration, Opening and Welcome
9:00 – 10:15 Session 1	**Embarking on a Digital Odyssey: Exploring Cybersecurity** The summer school begins with an overview of the aims and objectives, focusing on providing a comprehensive understanding of cybersecurity principles and core concepts. We start by understanding risk, exploring threats, vulnerabilities, and impacts. Then, the focus shifts to the basics of network infrastructure, setting the stage for a discussion on securing the network and empowering the attendees to protect their digital assets.
10:15 – 10:45	Networking Break
10:45 – 13:00 Session 2	**Behind Enemy Lines: Tactics and Motivations of Modern Cyber Threat Actors** In this engaging session, we delve into the rising menace of organized cybercrime groups, exploring both cyber-enabled and cyber-dependent crimes. Participants are guided through the intricacies of social engineering, ransomware, and other malicious software, while uncovering emerging threats and attack vectors. The discussion moves to advanced persistent threats (APTs) and targeted attacks, emphasizing the importance of cybersecurity awareness. We then introduce cloud computing models and outline best practices for securing cloud-based systems and data, reinforcing the need for vigilance in today's rapidly evolving digital landscape.
13:00 – 14:00	Lunch
14:00 – 16:45 Session 3	**Cracking the Code: Delving into the Intriguing World of Classical Cryptography** In this enlightening session, participants delve into the fascinating world of cryptography, a cornerstone of modern cybersecurity. Although often treated as a 'black-box' by many professionals, the session illuminates the basic concepts and techniques underpinning cryptographic protocols. The narrative introduces traditional cryptography, transitioning to various modern systems, including DES, 3DES, PKI, Digital Signatures, DHKE, RSA, ECDSA, and blockchain. Attendees are provided with a solid foundation in cryptography's history and its vital role in contemporary communication. Through exploring different types of ciphers, their workings, and methods to break them, participants gain a thorough understanding of the strengths and weaknesses of diverse cryptographic systems.

DAY 2: Thursday, 23rd November 2023
Cyber Strategies

9:00 – 9:30	Recap day one and preview of the day ahead
9:30 – 10:15 Session 4	**Steering the Cyber Ship: Navigating the Challenges of Effective Cybersecurity Management** In this session participants navigate the challenges of effective cybersecurity management. The program delves into securing access to digital resources, discussing access control models, password policies, biometric authentication, and identity management. The narrative emphasizes the importance of response plans, stakeholder roles, disaster recovery, and business continuity planning. The course also explores SIEM systems, their selection, and cybersecurity frameworks like NIST, ISO 27001, and CIS Controls. Participants learn to integrate multiple frameworks for a cohesive strategy. Additionally, the program empowers attendees with the skills to develop and present comprehensive cybersecurity strategies, covering risk assessment, threat modelling, stakeholder engagement, and budgeting.
10:15 – 10:45	Networking Break

10:45 – 13:00 Session 5	**Guardians of the Digital Realm: Mastering Privacy and Data Protection in the Information Age** In this comprehensive session, participants delve into the complex regulatory landscape of data privacy and protection on regional and global scales. We cover topics such as the EU's GDPR, South Africa's POPIA, and other regional frameworks. Attendees learn about key principles, requirements, cross-border data transfer challenges, and non-compliance implications. The session also focuses on Computer Emergency Response Teams (CERTs), equipping participants with the skills to establish and operate effective CERTs. It delves into the intricate relationship between cybersecurity legislation, stakeholder engagement, and the balance between security and privacy, providing attendees with an in-depth understanding of the legislative impact on the cybersecurity landscape.
13:00 – 14:00	Lunch
15:30 – close Session 6	**Mysterious Destinations: An Exclusive Cybersecurity Site Visit** A visit is planned to a major IT installation in Cape Town. The visit will conclude with a sponsored cocktail party.

DAY 3: Friday, 24th November 2023
Cyber Futures

9:00 – 9:30	Recap day two and preview of the day ahead
9:30 – 12:00 Session 7	**Fortifying the Digital Frontier: Exploring AI-Powered Cybersecurity Strategies** This captivating session delves into the application of AI and Machine Learning for threat detection, prevention, and anomaly detection, including Natural Language Processing for phishing detection. The narrative explores AI-driven, risk-based authentication methods that adapt security measures based on user behaviour and context. Participants are encouraged to ponder the ethical implications, potential risks, and privacy concerns associated with AI technologies in cybersecurity. The discussion also encompasses the role of AI in securing the metaverse, autonomous blockchain applications, and speculates on the future of cybersecurity in an AI-driven world.
12:00 – 13:00	Lunch
13:00 – 15:30 Session 8	**Quantum Leaps in Cybersecurity: Unravelling the Potential of Quantum Computing for Next-Generation Defence** In a world increasingly plagued by cyberattacks and data breaches, this session explores the potential of quantum computing to revolutionize next-generation defence mechanisms. Delving into quantum computing fundamentals, the session examines concepts such as qubits, superposition, entanglement, and quantum gates, including the enigmatic notion of quantum entanglement. We introduces quantum cryptography and Quantum Key Distribution (QKD) as revolutionary secure communication methods. The session also investigates quantum computing's impact on blockchain security and the development of quantum-resistant technologies. As quantum computers advance, the narrative underscores the need for investment in research, development, and implementation of quantum-resistant technologies, as well as education and training in quantum computing and cryptography. We also addresses the threats quantum computing poses to classical cryptography and highlight the importance of Post-Quantum Cryptography (PQC).
15:30 – 16:00	Close Out and the way forward

The Cybersecurity Summer School has been conceptualised and developed by:

- Professor Manoj Maharaj, School of School of Management, IT and Governance UKZN
- Professor Bruce Watson, School of Data Science and Computational Thinking, Stellenbosch University
- Dr Kiru Pillay, School of Data Science and Computational Thinking, Stellenbosch University

Held in conjunction with

THREAT CYBERFUTURE 2023 Government Academia Industry