25 September 2020

AI IN SECURITY COURSEWARE

COURSE PREPARED BY: PAUL B. ISAAC'S.

1. SECURITY – WHAT IS IT?

A coordinated set of activities to ensure availability, access, validity, authenticity of systems, tools, applications, operations and data being used for the designated purpose, in the right context, by the authorised operator for the rightful purpose.

Activities can include monitoring, auditing, active evaluation, alert mechanisms, response, deflection, redirection, blocking, reactive and proactive defence. Attack.

A. Certification expectations

  i. Attendance is mandatory. Certification is not automatically granted. It must be earned.

  ii. Periodic reviews and training updates necessary to remain relevant.

B. Cybersecurity specialities

  i. Methods

  ii. Best practices

2. ARTIFICIAL INTELLIGENCE – WHAT IS IT?

History – the last 100 years

Intelligence – the ability to make an informed decision within the defined parameters. Utilising computed results but without the need to follow the results. Ability to recognise when to exceed parameters and predetermine the consequences of doing so.

Why a rebellious act is so dangerous.

3. BRUTE FORCE AND INTELLIGENT SELECTION

How raw computational performance is no match for intelligent monitoring.

4. PASSIVE V ACTIVE INTRUSION DETECTION AND HONEYPOTS

Coding practice. Outsmarting the attackers and absentminded operators..

5. THE EXAM

Intelligence – the ability to make an informed decision within the defined parameters. Utilising computed results but without the need to follow the results.

A. Security

- i. Types of security
- ii. Attack vectors
- iii. The Law

B. Artificial Intelligence

- i. History
- ii. Types of AI
    1. *Machine Learning – training & inferencing*
    2. *Artificial Neural Networks*
    3. *Hardware accelerators*
    4. *Spiking neural networks*
    5. *Oscillatory networks*
    6. *Neuromorphics*
- iii. Ethics

C. Coding

- i. Languages used
- ii. Tools available
- iii. Pseudo-code

Day	Topic	Expected Outcome
1	Recap: Security, what is it?	Establish current methods for security attack vectors. The Law.
2	Intro: Artificial Intelligence, what is it?	Understand the history of AI, AI Winters, Machine Learning, Turing test, AGI, ethics
3	Brute force and intelligent selection examples	Practical coding of security examples
4	Passive v active intrusion detection and honeypots	Practical coding continuation

5	Exam prep, exam and feedback.	Pass/Fail certification