Cyber Intelligence & Strategy Short Course

12-16 AUGUST 2019

CENTURION, GAUTENG

Security Institute for Governance & Leadership in Africa

Stellenbosch University

1918 · 2018

Cyber Intelligence & Strategy Short Course

Security Institute for Governance & Leadership in Africa

Stellenbosch University

Presented by SIGLA, Stellenbosch University, this course is designed to create awareness and build competencies and practical skills within the Cyber Intelligence domain. Topics include

- the Cyber Security environment
- attack methods
- finding information in the open and closed domain relative to an established profile
- effectively selecting and utilizing data gathering and analysis techniques and tools to provide intelligence to upper analysis and operational levels
- Cyber Criminology (especially threat actors active in different economic domains)
- Compiling an intelligence strategy to provide proactive solutions to cyber threats.

The target audience includes cyber analysts, managers within the cyber space, board members and persons active within a cyber program.

Presenters

Prof Elmarie Biermann, Director Cyber Security Institute
Extraordinary Professor, Dept of Strategic Studies, Stellenbosch University
About the Cyber Security Institute**.** **www.cybersecurityinstitute.co.za**
Noëlle Cowling, Dept Strategic Studies, Stellenbosch University
Lead SIGLA Cyber **http://www.sun.ac.za/english/faculty/milscience/sigla**

Scope

The evolution of threats and exploits within the Cyber domain compels organizations and governments to move from a reactive to a proactive environment in a quest to tamp attacks on data and services. Proactive solutions rely on actionable intelligence regarding threat actors, threat vectors and toolkits utilized to provide value within every step of the cyber kill chain. Intelligence encompasses not only threat profiling and understanding attacker behaviours and toolsets but also the processes followed together with the criminology aspect. This in turn then assists in identifying indicators of compromise, allowing managers and practitioners to make informed decisions. Ultimately an understanding of the threat profile and how threat actors access and move around inside networks leads to better threat hunting.

Objective

The purpose of the course is to create awareness and build competencies and practical skills within the Cyber Intelligence domain.

Course Outcomes

Understand the Cyber Security environment and identify attack methods.
Source information in the open and closed domains relative to an established profile.
Effectively choose and utilize data gathering and analysis techniques and tools to provide intelligence to upper analysis and operational levels.
Study cyber criminology, especially threat actors active in different economic domains.
Be able to effectively apply intelligence at every step of the attack process.
Compile an intelligence strategy to provide proactive solutions to cyber threats.

Stellenbosch University Short Course Certificate

Certificates of competence to be issued on successful completion of the course. Successful completion requires continuous attendance and a minimum achieved mark of at least 70%.

Course Outline

Day 1: Cyber Security Environment

- Cyber Landscape
- Cyber threats and exploits
- Cyber Actors & Criminology aspects
- Attack methods & tools Criminal networks (Structure, Crime as a service, etc.)

Day 2: Obtaining Data

- Source of Data
- Collection operations
- Applications, Tools and Services
- Sensors (IoT)
- Big Data
- Scraping Information

Day 3: Analysis

- Analysis of cybercriminals' modus operandi
- Analysis Techniques (Data to Information)
- Indicators of Compromise
- Tactics, Techniques and Procedures Cyber kill chain and CCVs
- Tools & Services

Day 4: Cyber Intelligence

- Cyber Intelligence Lifecycle & Practices
- Types of intelligence (External, Military, Institutional, Open, Closed, HUMINT, etc.)

- Intelligence platforms, applications and services.
- Data – Information – Intelligence
- Collective and Counterintelligence
- Psychology of Intelligence Analysis

Day 5: Intelligence Strategy

- Incident management
- Cyber warfare
- Political and commercial risks
- Consuming and applying intelligence
- Developing an Intelligence driven strategy
- Strategic and Tactical Intelligence function
- Risk management

Details

Duration

Five (5) Full Days Contact Classes

Cost and Registration

R15490-00

https://shortcourses.sun.ac.za/courses/c-15.html

Venue

Centurion, Gauteng

Includes course packs, tools, refreshments and lunches