In the following pages you will see:

- Suggested course outlines for Cyber Security
- Emeritus Pedagogy, Instruction Format, and Curriculum
- Program timeline
- How will we setup the training program for success, including assessments, pre-course work and tracking success
- Delivery Methodology

20.1.1 CYBER SECURITY

About this course: Specific learning objectives and technology stack will be established when Emeritus conducts a requirements inception on the engaging organization's environment.

Goal:
The goal of this training is to provide students with skills necessary to join a cybersecurity community of practice as an entry level individual contributor.

Duration:
12 weeks, full-time. Each week students would be expected to read material, take part in the lecture and complete hands-on projects that derive from work in the lectures and reading material.

Course overview:
Successful cybersecurity analysts need to combine core skills literacy related to network and system administration with an awareness and understanding of the continual threat landscape that businesses face on a day-to-day basis. This course will train individuals to assess the threat landscape, develop protective policies and procedures for enhancing security, and identify and react to security anomalies in the systems they are trained to protect. This course provides a breadth first look at the field of cybersecurity and will prepare graduates to productively contribute to a community of practice at an entry level.

20.1.1.1 PRE-REQUISITES

Students should have a degree in computer science which includes command line scripting capability, and some familiarity with networking and system administration.

20.1.1.2 WEEKLY COURSE WORK SCHEDULE

Week 1:
Introduction to Cybersecurity - This unit introduces the course, and the skills that common to cybersecurity analysts. An overview of networking and system administration, modern network topologies, the threat landscape that faces analysts, and the tools that they have at their disposal to address threats and attacks are introduced in this lesson.

Networking Fundamentals - This unit introduces fundamental concepts and tools needed to manage and surveille a corporate network as well as operating with

machines on the internet. Ping, IPConfig, Tracert, NSLookup, NetStat and PuTTY are reviewed and experimented with during this lesson.

Week 2:
Windows Troubleshooting - This lesson focuses on the tools necessary to assess, identify and respond to security threats that are presented on Windows workstations and servers. Tools covered include RELI, PSR, PathPing, MTR, Sysinternals and GodMode.

Exploring Networks with Nmap - This unit makes heavy use of Nmap to explore ports, protocols, services, and OS characteristics of machines that are connected to a network. Zenmap (the GUI interface for NMap) is also covered.

Week 3:
Managing Vulnerabilities - The vulnerability management lifecycle is explored in this lesson and how it forms the basis for a program of continuous assessment. OpenVAS, the Nexpose community and strategies for vulnerability remediation are also covered.

Log Based Intrusion Detection - This lesson focuses on the use of OSSEC (Open-Source Security) to monitor and detect intrusions to corporate networks. Agents and log analysis techniques are covered in detail.

Week 4:
Securing Wireless Networks - This unit explores the 802.11 network protocol, tools like inSSIDer and Wireless Network Watcher that monitor activity on networks, Hamachi and other VPN services, and onion routing tools like TOR are covered.

Week 5:
Wireshark - This module covers the wireshark network monitoring tool in detail including the OSI model, capture capabilities, how to filter and tag captured data, and strategies for inspection.

Access Management - Policy development and specific skills around authentication, authorization and auditing are covered in this module. Concepts like least privilege and single signon are covered as well. The Jumpcloud service is also introduced.

Week 6:
Log Management Strategies - Windows event viewer, powershell, baretail, syslog, and Solarwinds Kiwi are among the tools covered in this unit. Strategies are presented for how to gain valuable knowledge from OS and network logging.

Week 7:
MetaSploit - Metasploit is often considered to be a red team tool, however it can be used for reconnaissance on your own network to identify vulnerabilities that offensive hackers could use to exploit your systems. This unit looks at how blue team members can use this tool to their advantage.

Week 8:
Web Application Security - Many companies expose their networks and data via public web applications. These systems are a common vector of attack by malevolent actors, so they need to be properly secured. This unit explores strategies for surveillance and monitoring of web applications. Offensive tools like the Burp Suite are explored as well.

Week 9:
Patching and System Maintenance - Patching and configuration management are key to limiting your company's threat landscape. This module explores tools like ManageEngine Desktop Central and Clonezilla and helps students learn to craft sensible maintenance policies.

Week 10:
Social Engineering - The human factor in security can be the weakest link in an otherwise strong security chain. This unit explores social engineering attacks, human nature, the role of education and presents a toolkit for managing OSI **layer 8.**

Week 11:
Kali Linux - Kali is a linux distribution that is designed for security analysts and contains over 600 penetration testing tools including all the tools covered in this class (Metasploit, Nmap, Wireshark, Burp, etc.). This unit covers an introduction to the distribution, how to run it from virtualization or from a boot thumb drive, and how to optimize it for your own use.

Week 12:
CIS Basic Controls - CISv7 outlines several policy controls that will help you audit your approach to security. This unit covers the most important controls including those related to hardware assets, software assets, vulnerability management, administrative privilege, configuration, maintenance, monitoring and audits.