CYBERSECURITY NEXUS™ (CSX) TRAINING PLATFORM

LABS + COURSES PACKAGE

LAB	RELATED COURSE	LAB TYPE	LEVEL	FUNCTIONAL DOMAIN	CPE HOURS	DESCRIPTION
SSH Tunnel Implementation	CSX Advanced Exploitation Course	Instructional	Advanced	Detect	2	In this advanced-level lab, students will learn how to setup an SSH Tunnel, enumerate services through a tunnel, and exploit through a tunnel.
Multiple SSH Tunnel Exploitation Implementation	CSX Advanced Exploitation Course	Instructional	Advanced	Detect	2	Students will learn how to utilize multiple redirectors on multiple ports for scanning, enumeration, and exploitation. They will also learn how to create a reverse tunnel through a network.
Metasploit PortProxy Implementation	CSX Advanced Exploitation Course	Instructional	Advanced	Detect	2	In this lab, students will use Metaploit's PortProxy post-exploitation module to redirect a port scan, an exploit and a backdoor communication.
Metrepreter Autoroute Implementation	CSX Advanced Exploitation Course	Instructional	Advanced	Detect	2	This time, a student will learn how to use Metaploit's AutoRoute Script to redirect a port scan, an exploit and a backdoor communication.
Network Assessment Challenge	CSX Advanced Exploitation Course	Challenge	Advanced	Detect	4	For this final exercise, students will utilize the tunneling and redirection skills learned in this course, as well as all previous training, to gain access to a network and investigate it.
Kali Forensics Environment	CSX Forensic Analysis Course	Instructional	Beginner	Respond	2	Kali Linux provides many utilities to navigate the folder structure, list file, read files, create files, move files, remove files, add directories, and remove directories. As the owner of G's Forensics LLC, you have been curious about using Kali for conducting digital forensic examinations. As a seasoned Forensics Examiner, you know a tool is only as good as the craftsman's hand. And, the craftsmen must master their tools to be successful.
PostgreSQL Configuration	CSX Forensic Analysis Course	Instructional	Beginner	Respond	2	A database is a desirable tool when dealing with documentation and evidence management. It provides structure and compartmentalization of cases and their associated files. As a forensic examiner, it is your job to understand how database management works with your investigations. It is your responsibility to ensure that your environment is configured correctly.
Foreman Configuration	CSX Forensic Analysis Course	Instructional	Beginner	Respond	2	Documentation is a very important aspect of any forensic investigation. Your documents attest to your methodology and provide evidence that you executed with due care and due diligence your responsibilities as a Forensics Examiner.
Final Foreman Setup	CSX Forensic Analysis Course	Instructional	Beginner	Respond	2	In this lab, you will continue your efforts from the previous lab in order to finalize your Foreman forensics case management tool setup using proper documentation.
A New Case	CSX Forensic Analysis Course	Instructional	Beginner	Respond	2	Receiving evidence, continuing the Chain of Custody, and creating exact working copies of the evidence is a major component of the forensics process. You have been contacted by a prosecuting attorney to aid in an important case. Moments ago, a bonded courier arrived at your location with digital evidence. The evidence has been processed and loaded into your Digital Evidence Locker.

CYBERSECURITY NEXUS™ (CSX) TRAINING PLATFORM

LABS + COURSES PACKAGE

LAB	RELATED COURSE	LAB TYPE	LEVEL	FUNCTIONAL DOMAIN	CPE HOURS	DESCRIPTION
My First Case	CSX Forensic Analysis Course	Instructional	Intermediate	Respond	2	Acceptance of a case is it at the discretion of the examiner in charge. The examiner must feel competent in his/her ability to complete the assignment in an unbiased manner. For this scenario, you will play the role of Happy Foreman, newly promoted lead examiner of G's Forensics, LLC. Mr. G has informed you of a new case. This will be your first case as the lead examiner.
A Picture	CSX Forensic Analysis Course	Instructional	Intermediate	Respond	2	In Forensics, pictures are an important factor in evidence. Pictures themselves are a point in time snapshot of what might have been, and they contain a lot more information then what we see during a visual examination. All files, pictures included, contain metadata, which is data about the data.
Data DNA	CSX Forensic Analysis Course	Instructional	Intermediate	Respond	2	Forensics commonly analyzes collections of files in a structured form. In this endeavor, we will start from the lowest level, the partition table, and gradually work our way up.
The Missing Piece	CSX Forensic Analysis Course	Instructional	Intermediate	Respond	2	Now that we have images let's conduct forensic file analysis to start building a case. We'll use built-in file carving and analysis tools that Kali has to offer such as Foremost and Autopsy.
Forensics Challenge	CSX Forensic Analysis Course	Challenge	Advanced	Respond	2	Using the knowledge gained in during this course it's time to catch a bad guy! During this challenge lab you will be required to keep up documentation while discovering evidence for a forensic operation!
Installing Linux	CSX Linux Application and Configuration	Instructional	Beginner	Protect	2	Students will learn how to install and start using Linux Mint, a user-friendly operating system variant.
Shell and Navigation	CSX Linux Application and Configuration	Instructional	Beginner	Identify	1	Students are introduced to basic commands which they can leverage in the Linux command line interface (CLI).
Files, Directories, and Information	CSX Linux Application and Configuration	Instructional	Beginner	Identify	1	Students are provided an opportunity to demonstrate their ability to execute basic Linux terminal commands and navigate different directories.
Files and Standard Input / Output	CSX Linux Application and Configuration	Instructional	Beginner	Identify	2	Students are introduced to the standard input and output capability of the Linux terminal and learn additional commands which will help them leverage Linux effectively.
Using STDIO	CSX Linux Application and Configuration	Instructional	Beginner	Identify	2	Students are presented with an opportunity to demonstrate their ability to leverage STDIO appropriately in a Linux environment.
CLI Tricks	CSX Linux Application and Configuration	Instructional	Beginner	Protect	1	Students learn additional Linux terminal commands which better enable understanding of bash history and environment variables.
Services and Users	CSX Linux Application and Configuration	Instructional	Beginner	Protect	1	Students will learn the how user and group accounts work within the Linux environment and how they impact files and file permissions.
Networking	CSX Linux Application and Configuration	Instructional	Beginner	Protect	2	Students learn various networking commands and gain a deeper understanding of the networking capabilities within Linux.

CYBERSECURITY NEXUS™ (CSX) TRAINING PLATFORM

LABS + COURSES PACKAGE

LAB	RELATED COURSE	LAB TYPE	LEVEL	FUNCTIONAL DOMAIN	CPE HOURS	DESCRIPTION
Users and Networking	CSX Linux Application and Configuration	Instructional	Beginner	Protect	2	Students will demonstrate their ability to leverage key Linux commands learned thus far in the course, creating users, variables, and network connections.
Package Management, Archives, and Compiling	CSX Linux Application and Configuration	Instructional	Beginner	Protect	2	Students learn how package managers function and how to compress and archive files using TAR. Additionally, they will learn how to compile source code.
Router Familiarization	CSX Network Application and Configuration	Instructional	Beginner	Identify	1	Without understanding the command line interface (CLI) or the graphical user interface (GUI) of an organization's gateway and/or firewall, cyber security analysts find themselves lost in confusion when an incident occurs. This lab will familiarize students with the CLI and GUI of pFsense, one of the preeminently used open-source firewalls available to organizations.
Setting up a LAN and a WAN	CSX Network Application and Configuration	Instructional	Beginner	Protect	2	Understanding the difference between a Wide Area Network (WAN) and Local Area Network (LAN) connection is critical to cyber security analysts and network engineers alike. Regardless of whether an individual is an incident responder or a help-desk technician, it is important to understand the different types of networks and how they impact an organization. In this lab, students will set up and conduct basic configuration of a WAN and LAN interface on a gateway.
Connecting Clients	CSX Network Application and Configuration	Instructional	Beginner	Identify	2	Cyber security professionals understand that most clients do not magically connect to a network unless Dynamic Host Configuration Protocol (DHCP) is involved. Even then, the use of DHCP needs to be established at key points within a network and requires configuration. In this lab, students will work to ensure that clients are able to connect to a network properly.
Initial Configuration	CSX Network Application and Configuration	Instructional	Beginner	Protect	1	Understanding how to configure a firewall and/or gateway for a first use instance is one of the most important elements of establishing a properly functioning network. In this lab, students will set up a pFsense configuration.
Basic Configuration	CSX Network Application and Configuration	Instructional	Beginner	Protect	2	Simply providing connectivity to an organization is insufficient when considering cyber security implications. Ensuring that a firewall is properly configured will guarantee a higher degree of safety when organizational users access network resources. In this lab, students will learn how to navigate a firewall interface to establish appropriate protection mechanisms for organizational users.
Port Forwarding and VPN Setup	CSX Network Application and Configuration	Instructional	Beginner	Protect	2	Many organizations make use of virtual private networks (VPNs) to protect data coming into and leaving the network. Many remote workers, for example, rely on VPNs to ensure that they can securely work on a corporate network from a distance. In this lab, students will set up and perform preliminary configuration of an organizational VPN.

CYBERSECURITY NEXUS™ (CSX) TRAINING PLATFORM

LABS + COURSES PACKAGE

LAB	RELATED COURSE	LAB TYPE	LEVEL	FUNCTIONAL DOMAIN	CPE HOURS	DESCRIPTION
Exploitation Identification and Response	CSX Network Application and Configuration	Instructional	Beginner	Detect/Respond	2	Identifying when an exploitation is on a network is one of the key abilities separating a cyber security professional from other IT work roles. Identifying when an exploit is sending data out of a network of responsibility and stopping the data leakage ensures that organizations can safely commence disaster recovery proceedings without losing additional data. In this lab, students will learn how to identify and block an exploitation on their network of responsibility.
Establishing a Network	CSX Network Application and Configuration	Challenge	Intermediate	Identify	2	Cyber security professionals should be able to set up and backup router and firewall configurations in the event of an incident. Ensuring that these backups are on hand is critical, yet, more important is that they exist in the first place. Students will implement what they have learned thus far to ensure that a network is established and a backup of it is secured.
Detecting, Responding, Recovering from a Network Attack	CSX Network Application and Configuration	Challenge	Intermediate	Detect/Respond/ Recover	2	Students have learned a myriad of networking skills throughout this course and this final challenge will require them to critically apply all of their newfound talents to an incident occurring on their network of responsibility.
Protocol Parsing	CSX Packet Analysis Course	Instructional	Intermediate	Identify	1	Students will leverage Wireshark to identify basic information from a packet capture.
ARP Analysis	CSX Packet Analysis Course	Instructional	Intermediate	Identify	1	Students will leverage Wireshark to identify dissect and understand ARP packets.
Initial Connection	CSX Packet Analysis Course	Instructional	Intermediate	Identify	1	Students will leverage Wireshark to identify dissect and understand the type of network activity associated with Internet Control Messaging Protocol (ICMP) and traceroute activity.
Interesting Searches	CSX Packet Analysis Course	Instructional	Intermediate	Identify	1	Students will learn how to conduct packet analysis to identify the types of searches which devices are executing on their network.
Additional Pets	CSX Packet Analysis Course	Challenge	Intermediate	Identify	1	Based on what students have learned, thus far, they are challenged to conduct preliminary analysis on a provided packet capture in order to ascertain information about the device and individual using it.
GET Request and Response Dissection	CSX Packet Analysis Course	Instructional	Intermediate	Identify	1	Understanding the user-agent affiliated with devices allow analysts to assess what kind of devices are on their network of responsibility. This lab will show students how to properly evaluate a user-agent and characterize a system. Additionally, it will illustrate how to gain contextual information from GET Requests and server responses.
Nefarious Employee	CSX Packet Analysis Course	Challenge	Intermediate	Identify	1	Using the skills learned thus far in the course, students will characterize the traffic and device of a potentially nefarious employee, suspected of selling company secrets.

CYBERSECURITY NEXUS™ (CSX) TRAINING PLATFORM

LABS + COURSES PACKAGE

LAB	RELATED COURSE	LAB TYPE	LEVEL	FUNCTIONAL DOMAIN	CPE HOURS	DESCRIPTION
Playing Around	CSX Packet Analysis Course	Instructional	Intermediate	Identify	1	This lab leverages all of the Wireshark filters and methods presented in the course thus far to show a student how to characterize network traffic and an individual on the network.
Probe Request Analysis	CSX Packet Analysis Course	Instructional	Intermediate	Identify	1	This lab leverages demonstrates how to analyze a probe request. Students learn what key information can be pulled out of a probe request about a device and a wireless network.
Beacon Analysis	CSX Packet Analysis Course	Challenge	Intermediate	Identify	1	This lab leverages requires students to leverage the skills and filters learned in the probe request lab and use them to analyze a captured beacon packet.
Network Topology	CSX Packet Analysis Course	Instructional	Intermediate	Identify	1	Understanding how to create a network map from a provided packet capture is important for individuals desiring to gain a better understanding of a network, but are prohibited from disrupting the network by introducing packets into the medium.
Wireless Network Topology	CSX Packet Analysis Course	Challenge	Intermediate	Identify	1	Testing all the skills learned in the Packet Analysis course and labs, this challenge requires students to create a network topology (netmap) of the 192.168.1.0 network in the provided packet capture.
Blaster Worm Analysis	CSX Packet Analysis Course	Instructional	Intermediate	Identify	1	Understanding how systems become infected and recognizing affiliated packets is an important skill for incident responders and IT personnel. In this lab, students will analyze a Blaster worm infection's affiliated packets.
Rouge AP and Mobile Analysis	CSX Packet Analysis Course	Challenge	Intermediate	Identify	1	Students will identify and characterize the rouge access point that is connected to a network of responsibility. They will also assess the traffic on the access point to determine what type of device is using it and what that device is doing.
Complete Netmap and Device Characterization	CSX Packet Analysis Course	Challenge	Intermediate	Identify	2	Students will leverage all of the skills learned in the Packet Analysis course and labs to provide in-depth analysis of a provided capture. Final submissions will include a complete network topology and a fully characterized device.
Linux Shell and Commands	CSX Penetration Testing Overview	Instructional	Beginner	Identify	2	The Unix bourne-again shell, also known as Bash, is a command processor that runs in the Kali Linux terminal. Bash scripting and command execution is the foundation of penetration testing.
TCP/IP Basics	CSX Penetration Testing Overview	Instructional	Beginner	Identify	2	In Linux, viewing and configuring network connections is not only a fundamental aspect of computer and network security, but it is also an essential piece of the penetration testing infrastructure.
Packet Inquiry	CSX Penetration Testing Overview	Instructional	Beginner	Identify	2	Wireshark is a free and open source network protocol analyzer that is both efficient and effective. In Kali Linux, packets are captured in Wireshark by penetration testers and cybersecurity professionals on a daily basis.

LAB	RELATED COURSE	LAB TYPE	LEVEL	FUNCTIONAL DOMAIN	CPE HOURS	DESCRIPTION
Network Discovery	CSX Penetration Testing Overview	Instructional	Beginner	Identify	2	Again, Wireshark is a free and open source network protocol analyzer that is both efficient and effective. It is necessary for penetration testers to understand the packets that are traversing through a network segment while discovering network hosts and navigating to websites.
Service Enumeration	CSX Penetration Testing Overview	Instructional	Beginner	Identify	2	The CLI tool, nmap, and its GUI counterpart, Zenmap, are both extremely important when it comes to identifying and enumerating network hosts, ports and services, and more.
Network Vulnerability Identification	CSX Penetration Testing Overview	Instructional	Beginner	Identify	2	Metasploit is a software project that is arranged for penetration testing. Metasploit provides essential information about computer and network security vulnerabilities and helps users exploit machines.
Network Vulnerability Exploitation	CSX Penetration Testing Overview	Instructional	Beginner	Identify	2	Using the results of an exploit to enable another exploit is something penetration testers do on a daily basis. Once their exploits take them deep enough into a remote system, using MySQL syntax to navigate a MySQL database can be a crucial skill when they're in search of information.
Evidence Removal	CSX Penetration Testing Overview	Instructional	Beginner	Recover	2	Removing evidence, also known as covering your tracks, is the last step in penetration testing. Although it is the last step, it is by far not the least important.
CPTO Challenge 1	CSX Penetration Testing Overview	Challenge	Beginner	Identify	2	This challenge is based on the first four labs of this series. This lab reflects the Identify domain of penetration testing.
CPTO Challenge 2	CSX Penetration Testing Overview	Challenge	Beginner	Detect	2	This challenge is based on the last four labs of this series. This lab reflects the Identify, Detect, and Recover domains of penetration testing.
Asset Identification	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Identify	2	Understanding how to perform basic asset identification is an important skill for any cybersecurity practitioner. Leveraging Nmap, students will learn how to scan a network and determine the identity of computers for which they are responsible.
Data Flow Identification	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Identify	2	In order to capture and analyze data flow, it is important to understand how to use Wireshark and Tshark, two critical tools in the packet analysis field. This lab helps students use these tools to map endpoints on the network.
Enterprise Asset Identification	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Identify	2	In addition to small networks, it is also just as important to practice working with large networks. Using Nmap and zenmap, students will identify assets on an enterprise network in order to build a topology.
Data Flow Analysis	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Identify	2	In this lab, students will be identifying packets with Wireshark. Due to the fact that data loss is a prevalent aspect of technology, students will learn to recover the packet identification data using the tool Foremost.

CYBERSECURITY NEXUS™ (CSX) TRAINING PLATFORM

LABS + COURSES PACKAGE

LAB	RELATED COURSE	LAB TYPE	LEVEL	FUNCTIONAL DOMAIN	CPE HOURS	DESCRIPTION
Enterprise Data Flow Analysis	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Identify	2	Since Wireshark cannot handle large amounts of data, students will be using SiLK for this lab. SiLK is a command line network protocol analyzer designed to help users map out endpoints within a network.
Identify Challenge	CSX Practitioner Exam Prep Course	Challenge	Intermediate	Identify	2	In this exercise, students will utilize their skills learned during the Identify module to complete a challenge mapping their network and identifying an attack on a local machine.
Firewall Setup	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Protect	2	Students will learn to create firewall rules for a pfSense firewall based on their network's layout.
Backup and Restore Points	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Protect	2	Students will learn how to create a Windows restore point and backup Linux servers from a baseline functioning. In addition, they will create a task with Windows Task Scheduler.
File System Protections	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Protect	2	Students will learn how to set file permissions on a Windows Server, as well as an Ubuntu machine, in this lab.
OS Baseline	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Protect	2	In this lab, students will get more practice with MBSA, as well as be introduced to the Linux tools Tiger and Lynis.
Protect Challenge	CSX Practitioner Exam Prep Course	Challenge	Intermediate	Protect	2	In this exercise, students will utilize skills learned during the Protect module to complete a challenge.
Sec Onion Setup and Testing	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Detect	2	In the first lab of the Detect module, students will learn how to set up a standalone Security Onion Server and explore and test its functionality.
Snort Rules	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Detect	2	In this lab, students will learn to construct simple SNORT rules and use Kibana to conduct post-attack analysis.
Event Detection	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Detect	2	An investigation is needed for an intrusion detection system alert. In this lab, students must find out what is occurring in the network.
Data and Network Analysis	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Detect	2	Students will use WireShark to conduct a live packet capture while they are under attack. Using WireShark, students will identify the attacker's IP, type of attack, and isolate anomalous packets related to the attack.
Vulnerability Analysis	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Detect	2	This lab focuses on the security of the local area network. Vulnerability scans are critical when maintaining strong security within a network. In this lab, students will conduct vulnerability assessments.
Detect Challenge	CSX Practitioner Exam Prep Course	Challenge	Intermediate	Detect	2	In this exercise, students will utilize skills learned during the Detect module to complete a challenge.
Incident Correlation	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Respond	2	SecOnion has reported a possible threat to the network. Students will investigate the tripped SNORT rule and the system logs of the possible affected systems via Kibana.
Network Forensics	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Respond	2	After snort reported a network issue, students must conduct network forensics on the compromised system to identify and isolate the possible malware during this lab.

CYBERSECURITY NEXUS™ (CSX) TRAINING PLATFORM

LABS + COURSES PACKAGE

LAB	RELATED COURSE	LAB TYPE	LEVEL	FUNCTIONAL DOMAIN	CPE HOURS	DESCRIPTION
Malware Investigation and Evaluation	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Respond	2	This lab has students utilize various tools (ClamAV, strings, PDF Parser, and PDF Toolkit), to not only investigate, but also evaluate, possible malware that has been attached to emails in the form of PDFs. In addition, the tool cron will come into play while students conduct their investigation.
Notification and Escalation	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Respond	2	Students will learn to properly document and preserve evidence of an attack, and notify the appropriate personnel in accordance with the Incident Response Plan.
Response Challenge	CSX Practitioner Exam Prep Course	Challenge	Intermediate	Respond	2	Using Security Onion, SGUIL, Snort, SSH, and ClamAV, students will put their Respond domain skills to the test to complete this challenge.
Re-Imaging	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Recover	2	In this lab, students will restore a Linux server from an image. Students will use Clonezilla in order to restore the Linux system to its baseline.
Restore Points	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Recover	2	Students will learn to restore a Windows Server using the restore point created in Lab 2.2 "Restore and Backup" in this lab.
Footprinting	CSX Vulnerability and Exploitation Course	Instructional	Intermediate	Detect	2	This lab instructs students on the basics of open source researching a target domain.
Initial Vulnerability Scanner Setup	CSX Vulnerability and Exploitation Course	Instructional	Intermediate	Detect	2	OpenVAS is a popular open-source vulnerability scanner and management tool. One of the tools included with OpenVAS is the Greenbone Security Assistant (GSA), a web application which connects to the OpenVAS manager daemon to provide a GUI for vulnerability management. In this lab, you'll become familiar with how these tools work and how to use them.
Vulnerability Analysis	CSX Vulnerability and Exploitation Course	Instructional	Intermediate	Detect	2	Conducting a vulnerability scan is important. In this lab, students will learn how to interpret the results from the vulnerability scans.
Initial Exploitation	CSX Vulnerability and Exploitation Course	Instructional	Intermediate	Detect	2	It's important to realize not all exploits require scripted code and payloads. Sometimes a simple Nmap scan - coupled with a Telnet connection and a clever username - is all you need.
Privilege Escalation	CSX Vulnerability and Exploitation Course	Instructional	Intermediate	Detect	2	Privilege escalation exploits are one of the most common exploit types. By exploiting flaws in the OS, this type of exploit allows a user to elevate their level of system access. Once elevated, a user can make permanent changes and gain control of the vulnerable system.
Backdoor Implementation	CSX Vulnerability and Exploitation Course	Instructional	Intermediate	Detect	2	This lab will take students through creating backdoors in systems as well as implementing inadvertent backdoors and exploitations.
Covering Tracks	CSX Vulnerability and Exploitation Course	Instructional	Intermediate	Detect	2	When a system is accessed, either by normal or clandestine operations, evidence is left behind in log files. Sanitation of those log files is important to cover up any activity that had taken place.

CYBERSECURITY NEXUS™ (CSX) TRAINING PLATFORM

LABS + COURSES PACKAGE

LAB	RELATED COURSE	LAB TYPE	LEVEL	FUNCTIONAL DOMAIN	CPE HOURS	DESCRIPTION
Deeper Exploitation	CSX Vulnerability and Exploitation Course	Instructional	Intermediate	Detect	2	Once a system has been compromised with administrator level access all sensitive system information is available to the attacker. In this lab, we'll take you through obtaining that system information.
CVEC Challenge	CSX Vulnerability and Exploitation Course	Challenge	Intermediate	Detect	2	This is a challenge lab based on the materials covered in the previous 8 labs.
Finding the Lost Web Server	Labs Volume 1	Instructional	Beginner	Identify	2	Students will leverage network discovery and diagnostic capabilities to identify what happened to a corporate webserver severely damaged during an attack.
Network Scanning	Labs Volume 1	Instructional	Beginner	Identify	2	Students will leverage network scanning tools to identify nodes and services on an internal network. The end goal is to create an up to date network map of their company's internal network for troubleshooting, analysis, and future reference.
HTTP Packet Analysis	Labs Volume 1	Instructional	Beginner	Detect	2	Conducting basic packet analysis is a key skill for anyone working in the cyber security field. Students will learn how to filter and parse packets to detect if corporate intellectual property is being stolen from their organization.
Data Integrity	Labs Volume 1	Instructional	Beginner	Protect	2	Students will learn the importance of data integrity through comparative analysis of hash algorithm output. Leveraging hashing tools, students will learn how to ensure that data is not compromised post-incident.
Web Server Backup	Labs Volume 1	Instructional	Beginner	Recover	2	Maintaining copies of non-compromised data and files are paramount to the incident response and disaster recovery process. This lab ensures that students understand how to archive and hash non-compromised data and back it up to a safe location.
DNS Packet Analysis	Labs Volume 1	Instructional	Beginner	Detect	2	Cyber security practitioners understand the importance of Domain Name System (DNS) packets and how they enable the flow of data across the Internet. They also understand that the subversion of DNS services on a network is a common attack seen in cyber security. In this lab, students will learn how to detect odd DNS activity and isolate samples of the traffic.
Scripts with Nmap	Labs Volume 1	Instructional	Beginner	Identify	2	Understanding if a system's ports are open and exposed is only half the battle of fully identifying and understanding an asset. You must also assess which services may be running on the asset. Every cyber security practitioner should understand how to leverage tools to understand which services are running on their networks. Students will leverage Nmap to see which services their computers are running.

LAB	RELATED COURSE	LAB TYPE	LEVEL	FUNCTIONAL DOMAIN	CPE HOURS	DESCRIPTION
Updating Firewall Rules	Labs Volume 1	Instructional	Intermediate	Protect	2	Cyber security professionals are often responsible for implementing acceptable use policies on their networks of responsibility. Thanks to the constant change of application usage and computing platforms, incident responders and technical professionals find themselves updating these policies regularly. In this lab, students learn how to change firewall rules to block unacceptable traffic.
Man-in-the-Middle Detection	Labs Volume 1	Instructional	Intermediate	Detect	2	One of the most common attacks in the field of cyber security is the Man-in-the-Middle (MitM) attack. Students taking this lab will learn how to detect when a potential MitM attack is occurring.
Threat Detection	Labs Volume 1	Instructional	Intermediate	Detect	2	Cyber security professionals are often given vague declarations of discontent from end-users experiencing technical difficulties. Understanding how to take minimal information and implement tools from their suite of capabilities to further understand the potential problems is key to proficiency. In this lab, students will implement typical network diagnostic tools to determine the type of issue an end user is having.
Cleaning Up After an Attack	Labs Volume 1	Instructional	Intermediate	Recover	2	Cyber security professionals understand that simply detecting and responding to an incident is not enough to adequately protect an organization's business processes and corporate assets. Therefore, it is important that practitioners understand how to recover from an incident. In this lab, students will learn how to ensure no backdoors or additional compromises exist on a system after an attack.
Browser Attacks	Labs Volume 1	Instructional	Advanced	Detect	2	Phishing attacks are the lynchpin of many organizational breaches and exploitations. Cyber security professionals that understand this also understand that many of these attacks are successful due to lack of understanding by end users. This course will teach cyber security professionals how to perform a phishing attack and illustrate the importance of cyber security awareness when browsing the internet.
Restoring Data with Secure Copy	Labs Volume 1	Instructional	Advanced	Recover	2	Every cybersecurity professional should understand the importance of obtaining, maintaining, and implementing a baseline of key system element in case of an incident. During the recovery process, pushing out clean baselines is paramount to restore system operations. In this lab, students will learn how to restore important, unaltered information by leveraging secure copy.
Testing Web Applications	Labs Volume 1	Instructional	Advanced	Protect	2	Part of a comprehensive defense-in-depth implementation includes testing new capabilities and applications before implementing them into an organizations production network. This course illustrates how students can conduct testing against newly developed web applications to ensure they do not pose a risk to organizational assets.

CYBERSECURITY NEXUS™ (CSX) TRAINING PLATFORM

LABS + COURSES PACKAGE

LAB	RELATED COURSE	LAB TYPE	LEVEL	FUNCTIONAL DOMAIN	CPE HOURS	DESCRIPTION
Malware Analysis	Labs Volume 1	Instructional	Advanced	Respond	2	Part of combating an incident or ensuring that an incident does not re-occur includes conducting in-depth analysis on the elements which compromised the network of the system. Thus, malware analysis has become a key capability which is applied during and after an incident. In this lab, students will gain an understanding of how to conduct malware analysis.
Scanning and Enumeration Challenge	Labs Volume 1	Challenge	Advanced		2	In this challenge, you will have to utilize some of the knowledge you acquired in the previous labs to complete a few tasks. Please make sure to read all instructions carefully and save all results or reports into the specified files. These files are case sensitive and can change results
Integrity and Malware Analysis Challenge	Labs Volume 1	Challenge	Advanced		2	In this challenge, you will have to utilize some of the knowledge you acquired in the previous labs to complete a few tasks. Please make sure to read all instructions carefully and save all results or reports into the specified files. These files are case sensitive and can change results
Forensics 1: Imaging	Labs Volume 2	Instructional	Beginner	Recover	2	The first step in computer forensics is obtaining a copy of the computers hard drive in question. This lab will guide students through that process.
Forensics 2: File Recovery	Labs Volume 2	Instructional	Intermediate	Recover	2	Once an image of the device in question has been obtained, file and recovery forensics can be attempted. In this lab, students will take the image created in a previous lab to investigate a possible data breach in their company.
Firewall Setup 2	Labs Volume 2	Instructional	Intermediate	Protect	2	Once the initial firewall setup has been completed it's time to start adding some rules to protect specific network devices from potential threats.
Mobile Forensics	Labs Volume 2	Instructional	Intermediate	Recover	2	This lab takes students through the nuances of mobile forensics. Mobile Applications, or Apps, utilize very specific technologies to store user data and configurations.
SQL Injection	Labs Volume 2	Instructional	Advanced	Detect	2	In this lab, students will be exposed to SQL injection attacks and learn how to implement the elements of prevention.
Firewall Setup 1	Labs Volume 2	Instructional	Advanced	Detect	2	Firewall routers will help protect your network from external and internal threats. This lab takes students through the first step of setting up a firewall.
Data Leakage	Labs Volume 3	Instructional	Intermediate	Identify	2	In this lab, students will interact with a username and password leak from a web app.
DDoS Detection	Labs Volume 3	Instructional	Advanced	Detect	2	Students will experience the different components of a distributed denial of service attack.
Session Hijacking	Labs Volume 3	Instructional	Advanced	Detect	2	Students will identify web application cookies, interact with Burp, and a MITM attack.
Insider Threat Identification	Labs Volume 3	Instructional	Beginner	Detect	2	This lab takes students through a situation where a former employee poses a serious threat to the company network.
Packet Construction and Kernel Hardening	Labs Volume 3	Instructional	Intermediate	Protect	2	In this lab, students will analyze a flood script built with Scapy, then configure their Linux kernel to detect flooding attacks.

LAB	RELATED COURSE	LAB TYPE	LEVEL	FUNCTIONAL DOMAIN	CPE HOURS	DESCRIPTION
System Baselining	Labs Volume 3	Instructional	Beginner	Protect	2	Students will get more practice with MBSA, as well as be introduced to the Linux Tiger IDS in this lab.
CSX Volume 3, Challenge 1	Labs Volume 3	Challenge	Intermediate	Protect/Detect	2	As part of this challenge, students must capture packets with Wireshark, configure their firewalls, and use Burp to intercept traffic.
CSX Volume 3, Challenge 2	Labs Volume 3	Challenge	Intermediate	Protect/Detect	2	Students will detect and respond to a cyber attack.
Spectre Mitigation	Labs Volume 4	Instructional	Intermediate	Protect	2	Spectre exploits crucial and vital susceptibilities in today's processors. Spectre uses speculative execution on processors using branch prediction. In other terms, Spectre takes advantages of the processors' performance techniques.
Meltdown Mitigation	Labs Volume 4	Instructional	Intermediate	Protect	2	Meltdown exploits crucial and vital susceptibilities in today's processors. Meltdown is similar to Spectre but there are some differences. Meltdown allows access to ANY data that is mapped to current memory space.
Chrome Extension Testing	Labs Volume 4	Instructional	Intermediate	Detect	2	In early 2018, security researchers discovered several nefarious Chrome extensions that were making unwanted calls to ad servers. This resulted in the removal of these Chrome extensions from the Google Extension Store and a heightened awareness to the possible effects of Chrome extensions on business networks.
Linux Baseline with Lynis	Labs Volume 4	Instructional	Beginner	Identify	2	Lynis is a security auditing tool designed specifically for Linux systems. Lynis is an open-source product that runs on the host itself and is essential when it comes to obtaining knowledge on Linux baselining.
Securing Web Browsers	Labs Volume 4	Instructional	Intermediate	Protect	2	Ensuring web browsing security is an integral part of cybersecurity as a whole. Google Chrome and Mozilla Firefox are both used in this lab.
Malware Detection and Removal with Baseline	Labs Volume 4	Challenge	Advanced	Respond	2	In addition to Lynis, this lab features Difference, ClamAV, and other vital Linux tools. This lab fuses these essentials together in order to present a challenge.
Domain Detection	Labs Volume 4	Challenge	Advanced	Detect	2	This challenge lab will be testing your packet analysis and domain detections skills.
Script Construction and Execution	Labs Volume 5	Instructional	Beginner	Identify	2	Assuming the role of a network security expert, who is responsible for creating, executing and then examining the output of a bash script and a batch file, students will learn the basics of scripting using both the Kali Linux bash and the Windows 10 command prompt.
Passive Computer Forensics	Labs Volume 5	Instructional	Intermediate	Recover	2	Leveraging the Kali and Clonezilla Linux distributions, students will image a file system, inspect identified files and leverage tools to identify nefarious deleted emails.
Intrusion Detection System Implementation and Testing	Labs Volume 5	Instructional	Beginner	Detect	2	Students will evaluate the functionality and applicability of IDS tools provided by the Security Onion Linux distribution, by identifying incidents and responding to alerts within the network of responsibility.

CYBERSECURITY NEXUS™ (CSX) TRAINING PLATFORM

LABS + COURSES PACKAGE

LAB	RELATED COURSE	LAB TYPE	LEVEL	FUNCTIONAL DOMAIN	CPE HOURS	DESCRIPTION
Triaging Incidents	Labs Volume 5	Instructional	Intermediate	Respond	2	Students will generate malicious traffic, examine the generated traffic, and respond to the incidents based upon their order of importance. These actions will enable the student to understand an incident from an attacker's perspective, as well as a responder.
IOT Device Indicators	Labs Volume 5	Instructional	Intermediate	Detect	2	Students will analyze a collection of IOT device communications packets and correlate the timing of data spikes with IOT user habits.
Home Automation Device Patterns	Labs Volume 5	Instructional	Intermediate	Detect	2	This lab will teach a student how to analyze wireless data collection in order to map and characterize a network and the devices resident upon said network.
Incident Response Script Implementation	Labs Volume 5	Challenge	Advanced	Respond	2	This lab will challenge students to create scripts and appropriately leverage tools within Security Onion to enhance IDS implementation and response times.
Forensic Data Recovery and Analysis	Labs Volume 5	Challenge	Advanced	Detect	2	This lab will challenge students to leverage tools such as Photorec and Wireshark to conduct forensic analysis in order to identify potential malicious activity indicators.
Implementing Database Management	Labs Volume 6	Instructional	Intermediate	Identify	2	MySQL uses the Structured Query Language to provide a free and open source RDBMS. As an employee new to the database management team, it is your responsibility to understand the essentials of the Structured Query Language. You will be using MySQL to create a database, create a table, and insert valuable data in order to get a basic understanding of database management.
Testing Intrusion Detection Systems	Labs Volume 6	Instructional	Intermediate	Identify	2	Cybersecurity Practitioners must understand how intrusion detection systems work and how they can be fine-tuned for a specific organizations needs. This lab will teach students how to create Snort rules for web-based attacks and how to manage alerts in Sguil.
Initializing Honeypots	Labs Volume 6	Instructional	Intermediate	Detect	2	Honeypots are used as bait against hackers wanting unauthorized access into networks. As a network security expert, it is your responsibility to set up honeypots on different machines in order to see its benefits. You will then save, read, and copy the logs for further investigation.
Generating and Analyzing Logs	Labs Volume 6	Instructional	Intermediate	Respond	2	As a network security expert, it is your responsibility to know how to use various tools within the Security Onion system. You will generate an attack within Kali Linux in order to trip alerts in Sguil and Kibana. You will need to be able to navigate through the Elastic Stack to investigate logs in order to be a blue team practitioner.

CYBERSECURITY NEXUS™ (CSX) TRAINING PLATFORM
LABS + COURSES PACKAGE

LAB	RELATED COURSE	LAB TYPE	LEVEL	FUNCTIONAL DOMAIN	CPE HOURS	DESCRIPTION
Identifying Cryptojacking Processes	Labs Volume 6	Instructional	Advanced	Identify	2	Using a small amount of JavaScript code, websites can utilize your computers CPU and GPU resources, without your knowledge, to mine cryptocurrencies. This type of cyber attack, referred to as "Cryptojacking", saw an 8,500% increase in occurrences throughout 2017. This lab will teach students how to identify these types of attacks through system resource monitoring.
Protecting Against VPNFilter	Labs Volume 6	Instructional	Advanced	Detect	2	VPNFilter malware was detected on over 500,000 devices in the US by the FBI in May of 2018. As a network security expert, it's crucial you are able to identify the presence of malware on your network. This lab will teach students how to identify the presence of VPNFilter on their network by using Snort to create alerts for traffic associated with the malware.
Administering Databases and Honeypots	Labs Volume 6	Challenge	Advanced	Detect	2	As a cybersecurity practitioner, it is your job to use the lessons learned in the Implementing Database Management and Initializing Honeypots labs in order to complete a new challenge.
Applying Snort Rules and Classifying Processes	Labs Volume 6	Challenge	Advanced	Detect	2	Using knowledge from the Cryptojacking Identification, Testing Intrusion Detection Systems, and Protecting Against VPNFilter labs, students will complete this final challenge lab for Volume 6.

CSX SKILLS ASSESSMENT TOOL	Exclusive to the CSX platform, the CSX Skills Assessment Tool allows you to assess the technical abilities and current skill levels of both your current employees and potential hires. Each assessment provides an on-the-spot evaluation of an individual's cyber strengths and weaknesses, allowing you to make informed hiring, promotional, and development decisions.
CSX CYBERSECURITY FUNDAMENTALS COURSE	For those just getting started in cybersecurity, or who need a refresher on foundational concepts, we have included our popular Cybersecurity Fundamentals Course in your package. This non-technical, self-paced course helps students build their knowledge of core cybersecurity concepts, techniques, roles and terminology. A perfect course to quickly train entry-level employees and professionals in related IT roles needing to understand more about cybersecurity concepts.

AVAILABLE FOR ADDITIONAL PURCHASE TO SUPPLEMENT YOUR PACKAGE:

CSX CYBERSECURITY FUNDAMENTALS CERTIFICATE EXAM	This remote-proctored, online exam is available as an add-on or separate purchase to your Training Platform package. Those passing the exam will earn the CSX Cybersecurity Fundamentals Certificate – a professional, globally-recognized certificate in the foundational concepts and principles that frame cybersecurity.