New Horizons Learning, LLC

APPENDIX C – PRICING INDEX

DIR-CPO-4876

Service Name	Service Description	Unit of Measure	Discount % off
20744 Securing Windows Server 2016	This five-day, instructor-led course teaches IT professionals how they can enhance the security of the IT infrastructure that they administer.	Per Course	40.00%
AS18 IBM I Network and Web Security	This course covers the following TCP/IP network security features: Digital Certificate Manager Securing the IBM i FTP server Securing applications other than HTTP with SSL IBM i IP filters OpenSSH IBM i virtual private networks Single sign-on.	Per Course	5.00%
AWS Security Essentials	This course covers fundamental AWS cloud security concepts, including AWS access control, data encryption methods, and how network access to your AWS infrastructure can be secured. Based on the AWS Shared Security Model, you learn where you are responsible for implementing security in the AWS Cloud and what security-oriented services are available to you and why and how the security services can help meet the security needs of your organization.	Per Course	40.00%

AZ-500T00 Microsoft Azure Security Technologies	In this course students will gain the knowledge and skills needed to implement security controls, maintain the security posture, and identify and remediate vulnerabilities by using a variety of security tools. The course covers scripting and automation, virtualization, and cloud N-tier architecture.	Per Course	40.00%
Certified Cloud Security Professional (CCSP)	The goal of the course is to prepare professionals for the challenging CCSP exam by covering the objectives of the exam based on the six domains as defined in the (ISC)2 CCSP common body of knowledge.	Per Course	40.00%
Certified Information Security Manager (CISM)	In this course, students will establish processes to ensure that information security measures align with established business needs.	Per Course	40.00%
Certified Information Security Systems Professional (CISSP)	In this course, students will expand upon their knowledge by addressing the essential elements of the 8 domains that comprise a Common Body of Knowledge (CBK)® for information systems security professionals.	Per Course	40.00%
Certified Information Systems Auditor (CISA)	In this course, students will evaluate organizational policies, procedures, and processes to ensure that an organizations information systems align with its overall business goals and objectives.	Per Course	40.00%
Check Point Certified Automation Specialist	The goal of this course is to provide an understanding of the advanced concepts and skills necessary to automate and orchestrate tasks relating to managing Check Point Security Policies.	Per Course	5.00%

Check Point Certified Endpoint Specialist	The goal of this course is to provide a comprehensive understanding of Check Point Endpoint Security and how to deploy it within the corporate network environment.	Per Course	5.00%
Check Point Certified Multi-Domain Security Management Specialist	This course provides a comprehensive understanding of the Check Point Multi-Domain Security Management solution and describes how to deploy it within the corporate network environment.	Per Course	5.00%
Check Point Certified Troubleshooting Expert	Provide advanced troubleshooting skills to investigate and resolve more complex issues that may occur while managing your Check Point Security environment.	Per Course	5.00%
Check Point Cyber Security Administrator	The goal of this course is to provide an understanding of basic concepts and skills necessary to configure Check Point Security Gateway and Management Software Blades.	Per Course	5.00%
Check Point Cyber Security Administration and Engineering Bundle	This special CCSA and CCSE bundle covering Check Point Security Administration & Engineering (R80.20) provides you with an understanding of the basic concepts and skills necessary to configure Check Point Security Gateway and Management Software Blades. CCSA-R80.20: The goal of this course is to provide an understanding of basic concepts and skills necessary to configure Check Point Security Gateway and Management Software Blades. CCSE-R80.20: The goal of this course is to provide an understanding and skills necessary to configure and optimally manage Check Point Next Generation Firewalls.	Per Course	5.00%

Check Point Cyber Security Engineering	The goal of this course is to provide an understanding and skills necessary to configure and optimally manage Check Point Next Generation Firewalls.	Per Course	5.00%
Citrix (Netscaler) ADC 12.x Advanced Concepts - Security, Management and Optimization	Learn how to configure your Citrix networking environment to address application services security requirements with Citrix Web App Firewall; automate and manage network services for scale-out of application architectures with Citrix Application Delivery Management; and optimize Citrix ADC-managed application delivery traffic. This fiveday course for experienced Citrix networking architects, engineers and administrators will teach you to deploy and manage Web App Firewall to protect web applications against different types of attacks. It will also give you a practical understanding of Citrix Application Delivery Management capabilities for centralized management of multiple Citrix ADC platforms, orchestration of changes, transaction reporting, infrastructure visualization and planning.	Per Course	5.00%

Citrix Virtual Apps and Desktops 7 Advanced Deployment, Troubleshooting, Security and Administration	Designed for experienced IT professionals this course builds on the foundational implementation and management skills introducing scalability, redundancy and security configurations. You will learn techniques to investigate many of the common issues that can affect environment health and how to solve issues more effectively in the advanced troubleshooting section. You will leave this course with a good understanding of how to manage more complex solutions such as multi-location environments with configurations around StoreFront, the Delivery Controllers, Cloud Connectors and HDX.	Per Course	5.00%
COBIT 2019 Foundations	COBIT 2019 builds on and integrates more than 25 years of development in this field, not only incorporating new insights from science, but also operationalizing these insights as practice. The heart of the COBIT framework updates COBIT principles while laying out the structure of the overall framework including: New concepts are introduced and terminology is explained—the COBIT Core Model and its 40 governance and management objectives provide the platform for establishing your governance program. The performance management system is updated and allows the flexibility to use maturity measurements as well as capability measurements. Introductions to design factors and focus areas offer additional practical guidance on flexible adoption of COBIT 2019, whether for specific projects or full implementation. From its foundation in the IT audit community, COBIT has developed into a broader and more comprehensive information and technology (I&T) governance and management framework and continues to establish itself as a generally accepted framework for I&T governance.	Per Course	40.00%

CompTIA Advanced Security Practitioner (CASP+)	In this course, students will examine advanced security concepts, principles, and implementations that pertain to enterprise level security.	Per Course	40.00%
CompTIA Cybersecurity Analyst (CySA+)	The course introduces tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate the organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur.	Per Course	40.00%
CompTIA Penetration Tester+ (PenTest+)	Security remains one of the hottest topics in IT and other industries. It seems that each week brings news of some new breach of privacy or security. As organizations scramble to protect themselves and their customers, the ability to conduct penetration testing is an emerging skill set that is becoming ever more valuable to the organizations seeking protection, and ever more lucrative for those who possess these skills. In this course, you will be introduced to some general concepts and methodologies related to pen testing, and you will work your way through a simulated pen test for a fictitious company.	Per Course	40.00%
CompTIA Security+ Certification	In this course, students will build on their knowledge of and professional experience with security fundamentals, networks, and organizational security as you acquire the specific skills required to implement basic security services on any type of computer network.	Per Course	40.00%

CRISC Certified In Risk and Information Systems Control	The CRISC course is designed for those who have experience with risk identification, assessment, and evaluation; risk response; risk monitoring; information systems control design and implementation; and information systems control monitoring and maintenance.	Per Course	40.00%
CWS-313 Citrix Virtual Apps and Desktops 7 Advanced Deployment, Troubleshooting, Security and Administration	Students will learn techniques to investigate many of the common issues that can affect environment health and how to solve issues more effectively in the advanced troubleshooting section. Students will leave this course with a good understanding of how to manage more complex solutions such as multi-location environments with configurations around StoreFront, the Delivery Controllers, Cloud Connectors and HDX.	Per Course	5.00%
Cybersafe Extended Edition 2019	Regardless of your computer experience, this class will help you become more aware of technology-related risks and what you can do to protect yourself and your organization from them. This course will help you to understand security compliance considerations, social engineering, malware, and various other data security-related concepts. In this course, you will explore the hazards and pitfalls and learn how to use technology safely and securely.	Per Course	40.00%

CyberSec First Responder-Threat Detection & Response	This course covers the duties of those who are responsible for monitoring and detecting security incidents in information systems and networks, and for executing a proper response to such incidents. Depending on the size of the organization, this individual may act alone or may be a member of a cybersecurity incident response team (CSIRT). The course introduces tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate the organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur. Ultimately, the course promotes a comprehensive approach to security aimed toward those on the front lines of defense. This course is designed to assist students in preparing for the CyberSec First Responder™ (Exam CFR-310) certification examination. What you learn and practice in this course can be a significant part of your preparation.	Per Course	40.00%

EC-Council Certified Application Security Engineer (CASE).net	The Certified Application Security Engineer (CASE) credential is developed in partnership with large application and software development experts globally. The CASE credential tests the critical security skills and knowledge required throughout a typical software development life cycle (SDLC), focusing on the importance of the implementation of secure methodologies and practices in today's insecure operating environment. The CASE certified training program is developed concurrently to prepare software professionals with the necessary capabilities that are expected by employers and academia globally. It is designed to be a hands-on, comprehensive application security course that will help software professionals create secure applications. The training program encompasses security activities involved in all phases of the Software Development Lifecycle (SDLC): planning, creating, testing, and deploying an application. Unlike other application security trainings, CASE goes beyond just the guidelines on secure coding practices and includes secure requirement gathering, robust application design, and handling security issues in post development phases of application development. This makes CASE one of the most comprehensive certifications on the market today. It is desired by software application engineers, analysts, testers globally, and respected by hiring authorities.	Per Course	5.00%
EC-Council Certified Chief Information Security Officer (C-CISO)	In this course, students will learn in-depth content in each of the 5 CCISO Domains	Per Course	40.00%

EC-Council Certified Ethical Hacker (CEH)	CEH provides an in-depth understanding of ethical hacking phases, various attack vectors, and preventative countermeasures. It will teach you how hackers think and act maliciously so you will be better positioned to setup your security infrastructure and defend against future attacks. An understanding of system weaknesses and vulnerabilities helps organizations strengthen their system security controls to minimize the risk of an incident. CEH was built to incorporate a hands-on environment and systematic process across each ethical hacking domain and methodology, giving you the opportunity to work towards proving the required knowledge and skills needed to achieve the CEH credential. You will be exposed to an entirely different posture toward the responsibilities and measures required to be secure. Now in its 11th version, CEH continues to evolve with the latest operating systems, tools, tactics, exploits, and technologies.	Per Course	40.00%
EC-Council Certifeid Network Defender (CND)	Certified Network Defender (CND) is a vendor-neutral, hands-on, instructor-led comprehensive network security certification training program. It is a skills-based, lab intensive program based on a job-task analysis and cybersecurity education framework presented by the National Initiative of Cybersecurity Education (NICE). The course has also been mapped to global job roles and responsibilities and the Department of Defense (DoD) job roles for system/network administrators. The course is designed and developed after extensive market research and surveys.	Per Course	40.00%

EC-Council Computer Hacking Foresnics Investigator (CHFI)	This course will provide participants the necessary skills to identify an intruders footprints and to properly gather the necessary evidence to prosecute in the court of law.	Per Course	40.00%
F5 Networks - Configuring BIG-IP ASM - Application Security Manager V13.X	The BIG-IP Application Security Manager course provides participants with the expertise needed to detect, mitigate, and prevent HTTP-based attacks on web applications.		5.00%
Implementing and Operating Cisco Security Core Technologies (SCOR)	In this course, Implementing and Operating Cisco Security Core Technologies (SCOR), students will master the skills and technologies needed to implement core Cisco security solutions to provide advanced threat protection against cybersecurity attacks. Students will learn security for networks, cloud and content, endpoint protection, secure network access, visibility and enforcements. They will get extensive hands-on experience deploying Cisco Firepower Next-Generation Firewall and Cisco ASA Firewall; configuring access control policies, mail policies, and 802.1X Authentication; and more. Students will also get introductory practice on Cisco Stealthwatch Enterprise and Cisco Stealthwatch Cloud threat detection features. This course will help you prepare to take the Implementing and Operating Cisco Security Core Technologies (350-701 SCOR) exam. It also helps you prepare for the CCNP Security and CCIE Security certifications and for senior-level security roles featuring Cisco security solutions.	Per Course	5.00%

MS-101T00 Microsoft 365 Mobility and Security	This course covers three central elements of Microsoft 365 enterprise administration – Microsoft 365 security management, Microsoft 365 compliance management, and Microsoft 365 device management. In Microsoft 365 security management, you will examine all the common types of threat vectors and data breaches facing organizations today, and you will learn how Microsoft 365's security solutions address these security threats. You will be introduced to the Microsoft Secure Score, as well as to Azure Active Directory Identity Protection and much more.	Per Course	40.00%
MS-500 Microsoft 365 Security Adminstrator	This four-MOC packaged set aligned to Microsoft 365 Exam: Microsoft 365 Security Administrator contains courseware that helps prepare students for Exams MS-500. Passing this exam is required to earn the Microsoft 365 Security Administrator certification.	Per Course	40.00%
NIST Cyber Security Professional (NCSP) Foundation	This course is targeted at IT and Cybersecurity professionals looking to become certified on how to operationalize the NIST Cybersecurity Framework (NCSF) across an enterprise and its supply chain.	Per Course	20.00%
NIST Cyber Security Professional (NCSP) Practitioner	This course is targeted at IT and Cybersecurity professionals looking to become certified on how to operationalize the NIST Cybersecurity Framework (NCSF) across an enterprise and its supply chain.	Per Course	20.00%

Red Hat Security - Linux in Physical, Virtual	This course is ideal for security administrators and system administrators who need to manage the secure operation of servers running Red Hat® Enterprise Linux®, whether deployed on physical hardware, as virtual machines, or as cloud instances. Maintaining security of computing systems is a process of managing risk through the implementation of processes and standards backed by technologies and tools. In this course, you will discover and understand the resources that can be used to help you implement and comply with your security requirements. This course is based on Red Hat Enterprise Linux 7.5, Red Hat Satellite 6.3, Red Hat Ansible® Engine 2.5, Red Hat Ansible Tower 3.2, and Red Hat Insights.	Per Course	5.00%

Understanding Cisco Cybersecurity Operations Fundamentsl (CBROPS)	The Understanding Cybersecurity Operations Fundamentals (CBROPS) v1.0 course teaches an understanding of the network infrastructure devices, operations, and vulnerabilities of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. You will learn basic information about security concepts, common network application operations and attacks, the Windows and Linux operating systems, and the types of data used to investigate security incidents. After completing this course, you will have the basic knowledge required to perform the job role of an associate-level cybersecurity analyst in a threat-centric security operations center to strengthen network protocol, protect your devices and increase operational efficiency. This course prepares you for the Cisco Certified CyberOps Associate certification. New – Recommended as preparation for the following exams: 200-201 - CBROPS Understanding Cisco Cybersecurity Operations Fundamentals Please note that this course is a combination of Instructor-Led and Self-Paced Study - 5 days in the classroom and approx. 1 day of self-study. The self-study content will be provided as part of the digital courseware that you will receive at the beginning of the course and should be part of your preparation for the exam.	Per Course	5.00%
Self Paced IT Cybersecurity Library	Self-Paced On Demand training is available online 24 hours a day, 7-days a week. Libraries can be purchased individually or in bulk. Customized learning plans can be built for each of your individual employees as well. This product offers the lowest entry cost to maximize your investment.	Per Course	35.00%

End of Appendix C