Course	Hours	Description
Certified Ethical Hacker (CEH): Hacking and Penetration Testing 1.5 hours	1.5	Hacking involves gaining unauthorized access to a computer system. Penetration testing is performed by ethical hackers using the same hacking techniques as an attacker would use, in order to uncover real and potential security vulnerabilities. In this course we discuss hacking concepts, methods, and penetration testing. An ethical hacker is a person who attacks an organization's security on behalf of its owners in order to discover vulnerabilities. Instead of taking advantage of these vulnerabilities, the ethical hacker reports them to the organization who can then put in place the appropriate countermeasures to protect themselves against malicious hackers. This course is the first in a series of courses which can used in preparation for the Certified Ethical Hacker v8, 312-50, exam. The course has been developed in partnership with EC-Council and is based on their Ethical Hacking and Countermeasures V8 course materials and labs.
Certified Ethical Hacker (CEH): Hacking Wireless Networks 1.5 hours	1.5	Wireless networks pose unique security challenges and any wireless strategy must have security as a central requirement. In this course we look at hacking wireless networks, the associated tools and techniques used, and mitigation strategies. This course is the thirteenth in a series of courses which can used in preparation for the Certified Ethical Hacker v8, 312-50, exam. The course has been developed in partnership with EC-Council and is based on their Ethical Hacking and Countermeasures V8 course materials and labs.
Certified Ethical Hacker (CEH): Malware	2	Malware is malicious software, used by attackers in various ways including disruption, information gathering, and gaining access. In this course we look at how malware is created, the attack vectors, and what countermeasures are available. An ethical hacker is a person who attacks an organization's security on behalf of its owners in order to discover vulnerabilities. Instead of taking advantage of these vulnerabilities, the ethical hacker reports them to the organization who can then put in place the appropriate countermeasures to protect themselves against malicious hackers. In this course we look at malware, how it is created, the attack vectors, and what countermeasures are available. This course is the sixth in a series of courses which can used in preparation for the Certified Ethical Hacker v8, 312-50, exam. The course has been developed in partnership with EC-Council and is based on their Ethical Hacking and Countermeasures V8 course materials and labs.
CISA Domain: IS Operations, Maintenance, and Support - Part 2	2.5	Enterprise network infrastructures and architectures are an integral part of enterprise environments today and are widely unknown to most users. The IS auditor must have a high level knowledge of these frameworks and a clear communication path to those who control them. This course examines the types of networks that are commonly found in enterprises today and the services and components that are commonly used in them. This course also examines disaster recovery strategies and scenarios that must be put in place to deal with any emergency situations that may occur. The Certified Information Systems Auditor (CISA) certification is known world-wide as the standard of achievement for those who assess, audit, control, and monitor an organization's information systems. CISA has been given ISO/IEC 17024:2003 certification by The American National Standards Institute (ANSI). This course will help to prepare learners for the CISA examination and follows the 2014 ISACA Candidate Information Guide.

Course	Hours	Description
CISA Domain: Protection of Information Assets - Part 2	3.5	Securing the network infrastructure is one of the main reasons an IT department exists in an enterprise environment. The role of a CISA is to audit the security measures and to make sure that the most efficient methods are being used to secure the environment. This course examines the components of the network infrastructure, the common threats they face, and how they can be secured. This course also examines the methods used by a CISA to audit and test the IS security and the internal and external security controls that can be used. The Certified Information Systems Auditor (CISA) certification is known world-wide as the standard of achievement for those who assess, audit, control, and monitor an organization's information systems. CISA has been given ISO/IEC 17024:2003 certification by The American National Standards Institute (ANSI). This course will help to prepare learners for the CISA examination and follows the 2014 ISACA Candidate Information Guide.
Cisco ROUTE 2.0: Securing Access	1.5	The need for comprehensive remote access security policies is driven by mobility and consumer trends; configuring remote management access in a secure fashion is of paramount importance to ensure the integrity of networking devices. In this course, you will learn about the AAA security architecture and how to use management access AAA features to secure local and remote access to the network. You will also learn strategies to protect the management plane by limiting access to it, and limiting access to its individual features. How you can use access control lists (ACLs) to filter traffic is also covered.
Cisco SWITCH 2.0: Campus Network Security I	2	Layer 2 security implementation is often forgotten. However, you should take the basic security measures to guard against a host of attacks that can be launched at a switch and its ports. Two common security measures are implementing port security and port access lists. Network or host misconfigurations, host malfunctions, or intentional DoS attacks may flood the network with traffic storms. Cisco IOS switches provide the storm control feature to limit the impact of traffic storms and, if necessary, take appropriate actions. In this course you'll learn what a traffic storm is and how to control it, you'll also learn how to configure storm control and verify its behavior. In addition, this course will introduce the importance of switch security, and describe all the recommended practices for securing a switch. Lastly, you'll learn how to configure and verify simple port security, configure and verify port security by using sticky MAC address, what can cause ports to become error-disabled and how to recover from this state as well as how to define and configure port access lists. This course offers the official training for the Implementing Cisco IP Switched Networks 2.0 certification exam which is a component exam for the CCNP and CCDP certifications. Passing this exam will also refresh CCNA certification, which expires after three years
CISM: Information Security Governance (Part 2)	2	Many companies realize that their information security is not in the state that it should be. As an information security manager, it will be your role to guide your organization to where information-related risks are controlled and sound information security processes are being followed by each and every employee. In order to move a company from a current state, to a desired state, there are many steps that must be taken. This course examines what an information security strategy is, frameworks and models you can use to build your strategy, who the strategy participants are, and constraints that may stand in your way. This course prepares you for the Certified Information Security Manager (CISM) exam and follows the 2015 ISACA Candidate Information Guide.

Course	Hours	Description
CISM: Information Security Incident Management (Part 1)	2.5	Managing incidents, and the response that is put forward by an organization falls directly under the duties of a CISM. Organizations must have a plan in place, and must know the steps they will take to deal with incidents when they occur. This course examines what incident management is, how responses are prepared, and concepts and technologies that are used when dealing with incidents. This course also looks at the principles, importance of, and outcomes of incident management and how the information security manager, with the approval of senior management, prepares the people and the resources of the organization to deal with incidents when they occur. Finally, this course explains the steps for conducting a business impact analysis as technique used in effective incident management. This course prepares you for the Certified Information Security Manager (CISM) exam and follows the 2015 ISACA Candidate Information Guide.
CISM: Information Security Incident Management (Part 2)	2	Preparing incident response and recovery plans is a very important part of a CISM's role. This course examines how to identify the current state of incident response capability, identifies the elements of incident response and recovery plans, and discusses principles for effectively managing the plans. This course also examines the importance of testing, documentation, and how to physically prepare recovery sites and related offsite resources. This course prepares you for the Certified Information Security Manager (CISM) exam and follows the 2015 ISACA Candidate Information Guide.
CISM: Information Security Program Development and Management (Part 3)	1.5	Information security managers are responsible for all administrative activities related to the development and management of an information security program. Those activities include such things as assigning and training security personnel, overseeing the creation and distribution of policies and other documentation, and monitoring the effectiveness of the security program itself. This course examines the many activities that an information security manager is responsible for and the skills required to perform them. This course prepares you for the Certified Information Security Manager (CISM) exam and follows the 2015 ISACA Candidate Information Guide.
CISSP: Asset Security	1.5	The substantial increase in the amount of digitized data over the past few years requires an equal response in attention to the security of that data. In this course, you'll learn about asset security best practices including classification techniques and asset security ownership. This course also covers privacy protection considerations, including data remanence and collection limitations. Finally, you'll explore best practices for media, hardware and personnel retention, and techniques for determining the most appropriate data security controls like scoping, tailoring and cryptography. This course is one of a series in the Skillsoft learning path that covers the objectives for the Certified Information Systems Security Professional (CISSP) exam.
CISSP: Communication & Network Security Design	2	Securing network communications is a key activity in managing the security of any IT system, and the network is a common and potent vector for attack. In this course, you'll learn about the design and components of network systems, how to implement secure systems, and how to mitigate common attacks. This course is one of a series in the Skillsoft learning path that covers the objectives for the Certified Information Systems Security Professional (CISSP) exam.

Course	Hours	Description
CISSP: Identity and Access Management	2	Identity and access management is at the heart of security management and is key to the CISSP examination. Compromising identity is the main aim of most attacks on data confidentiality. In this course, you'll learn about physical and logical access control, the proper management of identity and identification of the identity lifecycle, and attacks to access control and their mitigation. You'll also learn about the design and components of network systems, how to implement secure systems, and how to mitigate common attacks. This course is one of a series in the Skillsoft learning path that covers the objectives for the Certified Information Systems Security Professional (CISSP) exam.
CISSP: Risk Management	1.5	Risk management is an integral part of overall information systems security. In this course, you'll learn about personnel security best practices, risk management concepts, and risk analysis techniques. You'll also be introduced to threat modeling best practices, countermeasure selection, and implementing risk controls. Finally, this course covers risk monitoring and reporting best practices. This course is one of a series in the Skillsoft learning path that covers the objectives for the Certified Information Systems Security Professional (CISSP) exam.
CISSP: Security Assessment and Testing	1.5	The time spent planning and establishing security controls isn't worth much if you don't spend time ensuring that those security designs work. In this course, you'll learn how to design and validate security control assessment and test strategies, and perform vulnerability assessments. This course also covers how to perform log reviews, code reviews and tests, and perform penetration testing to test security controls. Finally, you'll learn about best practices for collecting security test data, and analyzing test outputs so you can identify gaps and implement any further required security controls in the overall security design. This course is one of a series in the Skillsoft learning path that covers the objectives for the Certified Information Systems Security Professional (CISSP) exam.
CISSP: Security Engineering Part 1	2	Integrating comprehensive security controls into information systems planning and design activities is vital for establishing IS architecture that has necessary functionality combined with the ability to fend off both internal and external threats. In this course, you'll learn best practices for implementing and managing secure engineering processes, including applying underlying security principles in IS architecture design. This course also introduces you to systems security evaluation models selecting appropriate controls and countermeasures. Finally, you'll learn about IS security capabilities and vulnerabilities and how to capitalize both for establishing security of the overall IS architecture. This course is one of a series in the Skillsoft learning path that covers the objectives for the Certified Information Systems Security Professional (CISSP) exam.
CISSP: Security Engineering Part 2	2	Even in an age of digitized data, securing the physical environment is still a critical part of security engineering. In this course, you'll learn about security threats, both natural and man-made, and techniques for preventing loss from these threats. You'll also learn about site and facility design considerations, restricted work area security, and best practices for crime prevention through secure design of the physical environment. This course is one of a series in the SkillSoft learning path that covers the objectives for the Certified Information Systems Security Professional (CISSP) exam.

Course	Hours	Description
CISSP: Security Operations Part 1	2	The day to day security activities in an organization are the heart of security operations. In this course, you'll learn techniques for performing general security operations activities such as security investigations, including best practices and requirements for the types of investigations that security professionals typically take part in. This course also introduces you to techniques for using logging and monitoring activities for security purposes, establishing secure resource provisioning, and applying general security concepts such as least privilege to all security operations activities. This course is one of a series in the Skillsoft learning path that covers the objectives for the Certified Information Systems Security Professional (CISSP) exam.
CISSP: Security Operations Part 2	1.5	One of the primary activities within security operations is detecting and responding to security-related incidents. In this course, you'll learn incident management techniques including incident detection, response, mitigation, reporting, and recovery best practices. This course also covers how to use preventative measures such as firewalls, whitelisting and blacklisting, sandboxing, and anti-malware. In addition, you'll be introduced to patch and vulnerability management activities such as patch testing, installation, and deployment. Finally, this course covers change management processes that security professionals regularly take part in as part of security operations, including versioning, baselining, and security impact analyses. This course is one of a series in the Skillsoft learning path that covers the objectives for the Certified Information Systems Security Professional (CISSP) exam.
CISSP: Security Operations Part 3	1.5	Security professionals are required to anticipate, plan for, respond to, and recover from security incidents quickly and appropriately as part of security operations for the overall organization. In this course, you'll learn how to develop and implement recovery strategies, including specific strategies for backup storage, recovery sites, multiple processing sites, and system resilience and fault tolerance requirements. This course also covers best practices for disaster recovery activities, including response, personnel, communications, assessment, restoration, and training and awareness considerations. Finally, you'll learn about organizational safety measures such as business continuity planning, managing physical security of the premises, and addressing personnel safety concerns like employee monitoring and privacy policies. This course is one of a series in the Skillsoft learning path that covers the objectives for the Certified Information Systems Security Professional (CISSP) exam.
CompTIA CASP CAS-002: Advanced Network Design, Management, and Controls	2.5	Network design plays a significant role in the security of an organization, as do the management strategies and the control mechanisms that are put in place. In this course, you'll learn about advanced network design concepts such as VPNs, RDP, VNC and IPv6. This course will also examine security devices, application aware technologies, and security controls. This course is one of a series in the Skillsoft learning path that covers the objectives for the CompTIA Advanced Security Practitioner (CAS-002) certification exam.
CompTIA CASP CAS-002: Privacy Policies & Procedures and Incident Recovery	1.5	Creating strong privacy polices and procedures will aid in securing organizational assets. If an event does occur, it is important to have proper procedures in place to make sure that recovery occurs as quickly and as efficiently as possible. In this course, you'll learn about the policies, procedures, and business documents that are used when creating a secure network environment. You will also examine the incident response and recovery procedures that are used when security breaches occur. This course is one of a series in the Skillsoft learning path that covers the objectives for the CompTIA Advanced Security Practitioner (CAS-002) certification exam.

Course	Hours	Description
CompTIA CASP CAS-002: Research, Analysis and Assessment	2.5	Research and testing are the backbone of introducing new technologies and devices into your network. It is important to make sure none of the new changes will compromise network security. In this course, you'll learn about research methods to determine industry trends and their impact to the enterprise.You will also explore methods of securing an enterprise environment, and you will select methods or tools appropriate to conduct an assessment and analyze the results. This course is one of a series in the Skillsoft learning path that covers the objectives for the CompTIA Advanced Security Practitioner (CAS-002) certification exam.
CompTIA CASP CAS-002: Security Controls for Hosts	2	Host security plays a tremendously important role in network security. Even if all your network links are secured, improperly secured hosts can leave your organization open to attack. In this course, you'll learn about end point security solutions, security controls and host hardening techniques, boot protection mechanisms, and finally you will learn about securing virtualized and cloud environments. This course is one of a series in the Skillsoft learning path that covers the objectives for the CompTIA Advanced Security Practitioner (CAS-002) certification exam.
CompTIA CASP CAS-002: Technical Integration of Enterprise Components	1.5	Tying all the security mechanisms in your organization together is extremely important, as it will bring the overall security into effect. In this course, you'll learn about integrating hosts, storage, networks and applications into a secure enterprise architecture. You will also examine ways to integrate advanced authentication and authorization technologies to support enterprise objectives. This course is one of a series in the Skillsoft learning path that covers the objectives for the CompTIA Advanced Security Practitioner (CAS-002) certification exam.
CompTIA Mobility+ MB0-001: Security	1.5	The chief concern for organizations entering the world of BYOD and mobile device is security. With greater flexibility, the mobile nature of devices, and the ownership issues of BYOD, the potential for security issues has never been greater. This course covers security concepts and risks, and strategies for mitigating those risks in a connected, mobile world. This course is one of a series of courses that cover the objectives for CompTIA Mobility+ (MB0-001).
CompTIA Network+ N10-006: Network Operations Part 1	1.5	Managing and monitoring are routine tasks performed on every network, regardless of its size. Proper management and monitoring of a network can forestall many problems that commonly occur in a network environment, as well as make troubleshooting problems that do arise that much easier. In this course, you'll learn about the methods and tools used in the operations of your network, including tools used in network monitoring, monitoring data analysis, configuration management, and network segmentation. This course is one of a series in the SkillSoft learning path that covers the objectives for certification exam CompTIA Network+ N10-006.
CompTIA Network+ N10-006: Network Security	2.5	A network's security is only as strong as the security of its individual systems. Before connecting individual computers to the network, you need to ensure that the computers are secured using proper security mechanisms. Identifying the appropriate steps and measures you can implement to protect your systems and keeping your resources and revenue safe from potential attacks is a key aspect of securing systems on your network. This course explores the different security concepts and common threats, and vulnerabilities of a network. It also covers network hardening, physical security, firewalls, Network Access Control models, and forensics. This course is one of a series in the SkillSoft learning path that covers the objectives for certification exam CompTIA Network+ N10-006.

Course	Hours	Description
CompTIA Security+ SY0-401: Authentication, Biometrics, and Security Controls	0.5	CompTIA Security+ is a vendor neutral security certification that tests foundation knowledge of security skills in a computer environment. This course covers account management, risk reduction, and LDAP. The course will also cover best practices, mitigation techniques, as well as strategies to reduce overall risk. This is the fifth course of the security+ SY0-401 certification training path.
CompTIA Security+ SY0-401: Continuity, Disaster Recovery, and Computer Forensics	2	CompTIA Security+ is a vendor neutral security certification that tests foundation knowledge of security skills in a computer environment. This course covers account management, risk reduction, and LDAP. The course will also cover best practices, mitigation techniques, as well as strategies to reduce overall risk. This is the fifth course of the security+ SY0-401 certification training path.
CompTIA Security+ SY0-401: Control Fundamentals and Security Threats	1.5	Comptia Security+ is a vendor neutral security certification that tests foundation knowledge of security skills in a computer environment. This course exams control fundamentals and the CIA traid, along with the types of malware that can affect computer systems and the mechanisms and applications that can be used to combat this malware. This is the first course of the security+ SYO-401 certification training path.
CompTIA Security+ SY0-401: Creating Secure Networks	1.5	CompTIA Security+ is a vendor neutral security certification that tests foundation knowledge of security skills in a computer environment. This course exams router and switch configurations, along with firewall types and configurations, and how IDS and IPS are used to secure a network environment. This course also examines other security mechanisms such as proxy servers, all-in-one security devices, flood guards, and unified security management. Finally, this course examines: layered security, Defense in depth, subnetting, DMZ, and NAT. This is the third course of the security+ SYO-401 certification training path.
CompTIA Security+ SY0-401: Network Protocols, Attacks, and Defenses	2	Comptia Security+ is a vendor neutral security certification that tests foundation knowledge of security skills in a computer environment. This course examines common network protocols, the fundamentals and dangers of network attacks, implementation of network security, and available tools and devices used to secure networks. This is the second course of the security+ SYO-401 certification training path.
CompTIA Security+ SY0-401: Remote Access, Mobile, and Wireless Security	1	CompTIA Security+ is a vendor neutral security certification that tests foundation knowledge of security skills in a computer environment. This course examines remote authentication services and mobile security implementation. It also discusses how to secure a wireless network and how to prevent wireless security attacks. This is the seventh course of the security+ SY0-401 certification training path.
CompTIA Security+ SY0-401: Vulnerability Assessment and Penetration Testing	1	Comptia Security+ is a vendor neutral security certification that tests foundation knowledge of security skills in a computer environment. This course exams penetration testing methods and technologies, along with vulnerability assessment technologies and tools. This is the fourth course of the security+ SYO-401 certification training path.

Course	Hours	Description
CompTIA Server+ SK0-004: Networking and Disaster Recovery	2.5	Almost everywhere you go, from large businesses to people's homes, networks are in place to facilitate the movement of data between computers and other devices, such as printers or the Internet. The network infrastructure services, ports, protocols, and cabling involved in networking can be complicated, which can make troubleshooting issues that arise complicated as well. It is important that server administrators are very familiar with server networking concepts. Also, without a well-thought-out plan in place, all the best equipment and well trained personnel in the world will be useless in the event of a disaster. Disasters can be man-made or natural, and both types can cause short delays or major business disruptions.In this course, you will learn about IP addressing and network infrastructure services. This course also compares various ports and protocols, and covers how to install and implement proper cable management procedures. In addition, you will learn about backup strategies and procedures for restoring data. You'll also explore various types of backup, such as full, incremental, and differential, along with the common media used for backup such as hard disks and optical media. Finally, you'll explore disaster planning and the implementation of a disaster recovery plan. This course is one of a series in the Skillsoft learning path that maps to CompTIA's Server+ exam, SK0-004, and covers the following exam objectives: 5.1 Given a scenario, configure servers to use IP addressing and network infrastructure services, 5.2 Compare and contrast various ports and protocols, 5.3 Given a scenario, install cables and implement proper cable management procedures, 6.1 Explain the importance of disaster recovery principles, and 6.2 Given a scenario, implement appropriate backup techniques.
CompTIA Server+ SK0-004: Security	2.5	Because so much work is done electronically, businesses and governments generate vast amounts of information, most of which needs to be safe. Security technologies have improved with the growth of data requirements. This course introduces the methods and concepts involved in physically protecting this data. As well, you'll learn about the different server hardening techniques, the different types of network security systems and protocols, as well as logical access control methods. This course also covers how to securely dispose storage and how to implement proper environmental controls in your server room. This course is one of a series in the SkillSoft learning path that maps to CompTIA's Server+ exam, SK0-004, and covers the following exam objectives: 4.1 Compare and contrast physical security methods and concepts, 4.2 Given a scenario, apply server hardening techniques, 4.3 Explain basic network security systems and protocols, 4.4 Implement logical access control methods based on company policy, 4.5 Implement data security methods and secure storage disposal techniques, and 4.6 Given a scenario, implement proper environmental controls and techniques.
CSSLP: Secure Software Concepts	2	A fundamental understanding of the potential risks, vulnerabilities and exposures throughout the software lifecycle is the basis for ensuring overall software security. In this course, you'll learn about the core concepts of confidentiality, integrity, authentication, and authorization. You'll also be introduced to security design principles such as least privilege, separation of duties, fail safe, and economy of mechanism. Finally, this course covers best practices for governance, risk, and compliance throughout the software lifecycle. This course is one of a series in the Skillsoft learning path that covers the objectives for the Certified Secure Software Lifecycle Professional (CSSLP) exam.

Course	Hours	Description
CSSLP: Secure Software Design	2.5	Security practices must be integrated in every aspect of software design. In this course, you'll explore secure software design processes such as attack surface evaluation, threat modeling, control identification, and prioritization. You'll also be introduced to specific design considerations to keep in mind like addressing core security concepts and interconnectivity. Finally, this course covers best practices for securing commonly used architecture and technologies like virtualization, database, and the programming language environment. This course is one of a series in the Skillsoft learning path that covers the objectives for the Certified Secure Software Lifecycle Professional (CSSLP) exam.
CSSLP: Secure Software Implementation and Coding	2	Building security controls within software implementation and coding is vital for end-product software security. In this course, you'll learn about declarative versus programmatic security, how to use Open Web Application Security Project or OWASP and Common Weakness Enumeration or CWE as great security sources, and some defense coding practices and controls such as configuration, error handling, and session management. This course also covers some essential secure coding techniques such as versioning, peer-based code reviews, code analysis, and anti-tampering techniques. This course is one of a series in the Skillsoft learning path that covers the objectives for the Certified Secure Software Lifecycle Professional (CSSLP) exam.
CSSLP: Secure Software Requirements	1	Integrating security into the software development process and identifying key security objectives is paramount to successful secure software development. In this course, you'll learn about internal and external security requirements and how to classify and categorize data. You'll also explore functional requirements such as role and user definitions, the role of the deployment environment on requirements, and sequencing and timing requirements. Finally, this course covers operational requirements such as deployment and management solutions. This course is one of a series in the Skillsoft learning path that covers the objectives for the Certified Secure Software Lifecycle Professional (CSSLP) exam.
CSSLP: Secure Software Testing	1.5	It's not enough to integrate secure coding into your software designs; it's equally important to test that your controls function properly. In this course, you'll learn best practices for testing for security and quality insurance, including artifact testing, functional and nonfunctional testing, and bug tracking. This course also covers some of the essential testing types such as penetration testing, scanning, simulation testing, failure testing, and cryptographic validation. Finally, you'll explore options for dealing with test results, such as the importance of impact assessments and corrective actions you can take with less than perfect results. This course is one of a series in the Skillsoft learning path that covers the objectives for the Certified Secure Software Lifecycle Professional or CSSLP exam.

Course	Hours	Description
CSSLP: Software Acceptance, Deployment, Operations, Maintenance, and Disposal	1	Regardless of how encompassing your software designs are, there's always a possibility that vulnerabilities still exist in the software or new vulnerabilities will be discovered later in the software development lifecycle. In this course, you'll learn different pre- and post-release activities to address these such as the pre-release testing process, completion criteria, risk acceptance practices, post-release plans, and independent testing options. You'll also be introduced to installation and deployment controls that you can use to mitigate vulnerabilities such as bootstrapping, configuration management practices, and release management. Finally, this course will cover operations and maintenance best practices for managing vulnerabilities such as incident and problem management, change management, and software disposal planning and execution for end-of-phase iterations. This course is one of a series in the Skillsoft learning path that covers the objectives for the Certified Secure Software Lifecycle Professional or CSSLP exam.
CSSLP: Supply Chain and Software Acquisition	1.5	Software lifecycle activities regularly extend beyond the internal environment. Outsourced software development, acquisition, and procurement activities require specific attention to ensure security is integrated into the end software product or service. In this course, you'll learn about supplier risk assessment considerations, including intellectual property, code reuse, and legal compliance complexities. This course also introduces some considerations to make with supplier sourcing like contractual integrity controls, vendor technical integrity controls, and service-level agreements or SLAs. Finally, this course also introduces software delivery and maintenance best practices like publishing and dissemination controls, product deployment and sustainment controls, and supplier transitioning requirements. This course is one of a series in the Skillsoft learning path that covers the objectives for the Certified Secure Software Lifecycle Professional or CSSLP exam.
IT Security for End Users: Using Corporate Devices Securely	0.5	Knowing how to use corporate computers and devices in a secure way helps ensure you don't jeopardize your work, your organization, or your personal security. In this course you'll learn about common threats to corporate computers, including malicious attacks, and best practices for using your computer in ways that prevent these attacks. This course also covers some of the security threats you might face when using corporate mobile devices, and techniques you can use to protect your device and yourself.
Juniper Networks Junos Essentials: Routing Policy & Firewall Filters	1.5	A robust routing policy has a number of positive effects on your network, from lowering utilization and improving responsiveness, to assisting with security. Security is a primary issue for modern networks, and Junos OS routing devices come with sophisticated firewall filter functionality. This course covers Junos OS routing devices routing policy concepts and configuration, and firewall filter concepts and configuration to help you in configuring a robust, performant, and secure network. This course is one of a series of Skillsoft courses that cover the objectives for Juniper Networks exam JN0-102. This exam completes the requirement for the certification Juniper Networks Certified Associate - Junos (JNCIA-Junos).

Course	Hours	Description
Microsoft Security Fundamentals: Network Security	1	One of the building blocks of successful IT security practices is a fundamental understanding of network security. This course introduces key concepts about dedicated firewalls and methods including packet filtering, circuit-level, application-level, and stateful multilevel firewalls. This course also covers types of inspection, and stateful v. stateless inspection. Finally, this course covers best practices for Network Access Protection, network isolation methods, and protocol security concepts including common network attack methods. This course is one of a series in the Skillsoft learning path that covers the objectives for the Microsoft Security Fundamentals: MTA 98-367 exam.
Microsoft Security Fundamentals: Operating System Security	1.5	One of the building blocks of successful IT security practices is a fundamental understanding of operating system security. This course provides an introduction to the concept of user authentication, including multifactor and Remote Authentication Dial-In User Service (RADIUS) authentication. This course also covers key concepts of permissions, such as file, Active Directory, share, and group permissions. Finally, this course covers fundamental security policies including password and audit policies, as well as encryption and malware best practices. This course is one of a series in the Skillsoft learning path that covers the objectives for the Microsoft Security Fundamentals: MTA 98-367 exam.
Microsoft Security Fundamentals: Security Layers	1	One of the building blocks of successful IT security practices is a fundamental understanding of security layers. This course introduces learners to some of the main core concepts in IT security including confidentiality, integrity, and availability. This course also covers foundational information on physical, Internet, and wireless security, including keylogging, browser settings and zones, and service set identifier, or SSID, and media access control, or MAC, filters. This course is one of a series in the Skillsoft learning path that covers the objectives for the Microsoft Security Fundamentals: MTA 98-367 exam.
Microsoft Security Fundamentals: Security Software	1	One of the building blocks of successful IT security practices is a fundamental understanding of security software. This course introduces learners to client protection practices, including methods for dealing with malware, antivirus for client protection, and using User Account Control, or UAC. This course also includes fundamental best practices for e-mail protection and server protection, including server hardening. This course is one of a series in the Skillsoft learning path that covers the objectives for the Microsoft Security Fundamentals: MTA 98-367 exam.
Protecting Windows 7 Against Malware and Vulnerabilities	1.5	This course provides the desktop support technician with guidelines for preventing the infection of client systems by malicious software, how to identify possible infections, and an overview of the tools available to resolve any infection. It will also detail how Windows Firewall can be used to block unwanted content, but allow needed programs and services to be accessed. Also covered are the configuration options provided by the Advanced Security Snap-In, which provides advanced rules and monitoring settings for remote or standalone client systems but can also be configured through Group Policy in the Enterprise environment. To ensure overall vulnerability management of the operating system this course also stresses the importance of the Windows Update process, and provides the information needed to configure Windows Update, verify installed updates, or remove troublesome updates. This course is one of a series in the SkillSoft learning path that covers the objectives for the Microsoft exam: 70-685 Pro: Windows 7, Enterprise Desktop Support Technician. Passing this exam will earn the learner Microsoft Certified IT Professional: Windows 7, Enterprise Desktop Support Technician certification.

Course	Hours	Description
Securing User Accounts: Authorization, Registration, and Passwords	2	Without the ability to gain entry to a network, hackers are powerless, so establishing effective authorization protocols is vital. In this course, you'll learn about key authentication concepts and best practices such as identification, user authentication components, the user logon process, and how to effectively manage user account credentials. This course also covers registration security, including how to use Completely Automated Public Turing test to tell Computers and Humans Apart or CAPTCHA, and enabling two-step verification. Finally, this course introduces password security best practices, including establishing password strength, complexity, and age criteria.
Securing User Accounts: Fundamental Security Concepts	2.5	Online user accounts, when not properly secured, are one of easiest entry points for savvy hackers. In this course, you'll learn about the fundamental security concepts of authenticity, integrity, and confidentiality, and what role they play in establishing effective user account policies. You'll also learn why and how most common user account breaches happen. Finally, this course covers some general security practices, such as privilege management, permissions, and account settings, to help protect against potential intrusions via user accounts.
Securing User Accounts: Logon, Logoff, Account Changes, and Attack Mitigation	1.5	You can probably think of at least one major account security breach you've heard about. When a security breach happens, it puts your customers, assets, and entire reputation at risk, so knowing how to identify and respond to potential attacks can be the difference between an organization's continued success or complete failure. In this course, you'll learn about enhancing user account security by establishing logon, logoff, and advanced password management protocols. You'll also learn about safe and secure policies for advanced user account management such as account change and reset practices. Finally, this course covers effective best practices for handling user account security breaches, such as neutralizing attacks, and safely handling compromised systems to limit any further damage to your systems, network, and other user assets.