



TEKNOLOGISK  
INSTITUT

Online kursus – k72746

---

# Cybersecurity Collection

---

<b>Cloud System Architecture – Concepts and Design</b>	2,20
<b>Cloud Data Security</b>	1,90
<b>Cloud System Security - Platform and Infrastructure</b>	2,00
<b>Cloud Application Security</b>	2,20
<b>Cloud Service – Operations Management</b>	3,00
<b>Cloud Service – Legal and Compliance</b>	2,10
<b>CompTIA Cybersecurity Analyst+ CS0-001: Network Architecture and Reconnaissance</b>	3,10
<b>CompTIA Cybersecurity Analyst+ CS0-001: Threat Identification</b>	2,40
<b>CompTIA Cybersecurity Analyst+ CS0-001: Threat Mitigation</b>	2,20
<b>CompTIA Cybersecurity Analyst+ CS0-001: Reducing Vulnerabilities</b>	2,40
<b>CompTIA Cybersecurity Analyst+ CS0-001: Investigate Security Incidents</b>	2,20
<b>CompTIA Cybersecurity Analyst+ CS0-001: Monitoring for Security Issues</b>	2,30
<b>CompTIA Security+ SY0-501: The Present Threat Landscape</b>	0,90
<b>CompTIA Security+ SY0-501: Types of Malware</b>	0,90
<b>CompTIA Security+ SY0-501: Social Engineering and Related Attacks</b>	0,70
<b>CompTIA Security+ SY0-501: Application and Service Attacks</b>	0,90
<b>CompTIA Security+ SY0-501: Cryptographic and Wireless Attacks</b>	0,80
<b>CompTIA Security+ SY0-501: Penetration Testing and Vulnerability Scanning</b>	0,80
<b>CompTIA Security+ SY0-501: Impacts from Vulnerability Types</b>	0,90
<b>CompTIA Security+ SY0-501: Components Supporting Organizational Security</b>	1,50
<b>CompTIA Security+ SY0-501: Security Assessment Using Software Tools</b>	0,90
<b>CompTIA Security+ SY0-501: Cryptography</b>	2,00
<b>CompTIA Security+ SY0-501: Public Key Infrastructure</b>	1,10
<b>CompTIA Security+ SY0-501: Wireless Security Settings</b>	1,30
<b>CompTIA Security+ SY0-501: Analyzing Output from Security Technologies</b>	1,00
<b>CompTIA Security+ SY0-501: Deploying Mobile Devices Securely</b>	0,50
<b>CompTIA Security+ SY0-501: Implementing Secure Protocols</b>	0,50
<b>CompTIA Security+ SY0-501: Troubleshooting Common Security Issues</b>	0,40
<b>CompTIA Security+ SY0-501: Identity Concepts and Access Services</b>	0,60
<b>CompTIA Security+ SY0-501: Identity and Access Management Controls</b>	0,50
<b>CompTIA Security+ SY0-501: Common Account Management Practices</b>	0,60
<b>CompTIA Security+ SY0-501: Frameworks, Guidelines, and Physical Security</b>	2,00
<b>CompTIA Security+ SY0-501: Implement Secure Network Architecture Concepts</b>	0,80
<b>CompTIA Security+ SY0-501: Secure System and Application Design and Deployment</b>	1,50
<b>CompTIA Security+ SY0-501: Cloud, Virtualization, and Resiliency Concepts</b>	1,10
<b>CompTIA Security+ SY0-501: Policies, Plans, and Procedures</b>	0,80

<b>CompTIA Security+ SY0-501: Business Impact Analysis and Risk Management</b>	1,10
<b>CompTIA Security+ SY0-501: Incident Response, Forensics, and Disaster Recovery</b>	1,10
<b>IT Security for End Users: IT Security Fundamentals</b>	0,90
<b>IT Security for End Users: Using Corporate Devices Securely</b>	0,80
<b>IT Security for End Users: Secure Corporate Communications and Networking</b>	0,80
<b>Microsoft SharePoint Server 2013 - Developing Core Solutions: Implementation Security</b>	1,60
<b>IINS 3.0: Introduction to Cisco Security</b>	0,80
<b>IINS 3.0: SIEM Technology and Security Terminology</b>	1,20
<b>IINS 3.0: Introduction to Network Attacks</b>	1,10
<b>IINS 3.0: Specific Network Attacks</b>	0,60
<b>IINS 3.0: Malware and Data Loss</b>	1,20
<b>IINS 3.0: Encryption Methods</b>	0,90
<b>IINS 3.0: Cryptographic Key Exchange</b>	1,00
<b>IINS 3.0: Network Topologies</b>	1,20
<b>IINS 3.0: Secure Device Management</b>	0,50
<b>IINS 3.0: Auto Secure</b>	0,80
<b>IINS 3.0: Management Plane Access</b>	0,90
<b>IINS 3.0: Simple Network Management Protocol</b>	0,60
<b>IINS 3.0: Network Time Protocol</b>	0,80
<b>IINS 3.0: SCP and AAA Technologies</b>	1,00
<b>IINS 3.0: TACACS+</b>	0,90
<b>IINS 3.0: Network Access Control</b>	1,00
<b>IINS 3.0: Port Based Access Control, BYOD, and MDM</b>	1,00
<b>IINS 3.0: IPsec and VPN</b>	1,00
<b>IINS 3.0: Clientless SSL VPN &amp; ASDM</b>	0,60
<b>IINS 3.0: AnyConnect VPN Using ASDM</b>	1,10
<b>IINS 3.0: IPSec Site-to-Site VPN</b>	1,00
<b>IINS 3.0: Secure CLI Access</b>	0,60
<b>IINS 3.0: OSPF and EIGRP Authentication</b>	1,10
<b>IINS 3.0: Attack Mitigation</b>	1,50
<b>IINS 3.0: Control Plane Policing</b>	0,50
<b>IINS 3.0: PVLANs and VLAN Security</b>	1,00
<b>IINS 3.0: Firewall Technology</b>	0,60
<b>IINS 3.0: Network Address Translation</b>	0,90
<b>IINS 3.0: Zone-Based Firewall Configuration</b>	0,80
<b>IINS 3.0: ASA Security and Policies</b>	1,40
<b>IINS 3.0: Firewall Features</b>	0,60
<b>IINS 3.0: IPS Deployment Configuration</b>	1,10
<b>IINS 3.0: Configuring Cisco IPS</b>	0,90
<b>IINS 3.0: Threat Mitigation for Email, Web, and Endpoints</b>	1,30
<b>CompTIA PenTest+: Planning for an Engagement</b>	0,90
<b>CompTIA PenTest+: Scoping an Engagement</b>	0,90

<b>CompTIA PenTest+: Information Gathering</b>	0,90
<b>CompTIA PenTest+: Vulnerability Identification</b>	0,70
<b>CompTIA PenTest+: Social Engineering and Specialized System Attacks</b>	0,90
<b>CompTIA PenTest+: Network-Based Exploits</b>	1,30
<b>CompTIA PenTest+: Application-Based Vulnerabilities</b>	0,90
<b>CompTIA PenTest+: Local Host Vulnerabilities</b>	0,60
<b>CompTIA PenTest+: Post-Exploitation and Facilities Attacks</b>	0,70
<b>CompTIA PenTest+: Penetration Testing Tools</b>	1,40
<b>CompTIA PenTest+: Analyzing Tool and Script Output</b>	0,90
<b>CompTIA PenTest+: Reporting and Communication</b>	0,60
<b>SECFND: Overview and Network Models</b>	0,60
<b>SECFND: Network Models</b>	0,90
<b>SECFND: Basic Networking Protocols</b>	1,00
<b>SECFND: Basic Networking Services</b>	1,00
<b>SECFND: Network Devices Operations &amp; Security</b>	1,20
<b>SECFND: Network Addressing</b>	0,90
<b>SECFND: VLANS and Data Visibility</b>	0,50
<b>SECFND: ACLs &amp; Filtering</b>	0,90
<b>SECFND: Filtering and Packet Capture</b>	1,00
<b>SECFND: Packet Analysis</b>	0,80
<b>SECFND: Data Loss &amp; Defense in Depth</b>	0,90
<b>SECFND: Security Concepts</b>	0,90
<b>SECFND: Security Management Part 1</b>	0,80
<b>SECFND: Security Management Part 2</b>	0,50
<b>SECFND: Cryptography</b>	0,90
<b>SECFND: Digital Signatures</b>	1,30
<b>SECFND: SSL/TLS Components</b>	1,00
<b>SECFND: Cryptographic Hashing Algorithms</b>	0,50
<b>SECFND: Cryptographic Encryption Algorithms</b>	1,00
<b>SECFND: Windows Host Terminology</b>	0,60
<b>SECFND: Linux Host Terminology</b>	0,90
<b>SECFND: Endpoint Security</b>	0,50
<b>SECFND: Interpreting Log Data</b>	0,80
<b>SECFND: Network Data Types</b>	1,00
<b>SECFND: Network Data Types and Security Monitoring</b>	0,90
<b>SECFND: Network Monitoring</b>	0,90
<b>SECFND: Next Generation Firewalls</b>	0,40
<b>SECFND: Monitoring Network Protocols</b>	0,90
<b>SECFND: Security Attack Concepts</b>	0,50
<b>SECFND: Network and Web Attacks</b>	0,80
<b>SECFND: Attacks and Evasion</b>	0,90
<b>SECOPS: Analyzing Threat Mitigation Reports</b>	1,50
<b>SECOPS: Scoring with CVSS 3.0</b>	1,50
<b>SECOPS: Securing File Systems</b>	1,30

<b>SECOPS: Identifying Forensic Evidence</b>	1,10
<b>SECOPS: Interpreting Regular Expressions</b>	1,00
<b>SECOPS: Protocol Header Security</b>	1,50
<b>SECOPS: IP Header Security</b>	1,40
<b>SECOPS: ICMP Intrusion</b>	0,90
<b>SECOPS: ICMP Intrusion Part 2</b>	0,90
<b>SECOPS: Transport Layer Headers</b>	1,20
<b>SECOPS: HTTP Headers</b>	1,20
<b>SECOPS: Identifying NetFlow v5 Records</b>	0,90
<b>SECOPS: Examining Intrusion Events</b>	0,40
<b>SECOPS: Intrusion Event Technologies</b>	1,20
<b>SECOPS: Analyzing Intrusion Impact</b>	1,00
<b>SECOPS: Responding to Incidents</b>	1,00
<b>SECOPS: CSIRT Goals and Cybersec Elements</b>	0,90
<b>SECOPS: Data Normalization and 5-Tuple Correlation</b>	0,60
<b>SECOPS: Firepower Management Console and Analysis Methods</b>	0,90
<b>SECOPS: Categorize and Classify Intrusions</b>	1,10
<b>SECOPS: Handling Incident Events and Evidence</b>	1,30
<b>Mentoring Certified Information Systems Security Professional (CISSP)</b>	0,00
<b>Mentoring Systems Security Certified Practitioner (SSCP)</b>	0,00
<b>Oracle Database 11g Release 2: Storage Structures and User Security</b>	1,50
<b>Oracle Database 11g Release 2: Oracle Partitioning and Security Features</b>	2,00
<b>Oracle Database 11g Release 2: Oracle Scheduler and Secure Backup</b>	1,00
<b>Defensive Coding Fundamentals for C#</b>	2,10
<b>Defensive Coding for C#</b>	1,90
<b>Defensive Programming in Android: Input and Methods</b>	1,50
<b>Defensive Programming in Android: Using Standards</b>	1,50
<b>Defensive Programming in Android: Errors, Exceptions, and Testing</b>	1,90
<b>Defensive Programming in Android: Network Access and Java Defensive Techniques</b>	1,60
<b>Thinking Defensively about Functions, Methods, and Input</b>	1,90
<b>Managing Network Interaction</b>	2,20
<b>Errors, Exceptions, and Testing</b>	2,30
<b>Protecting Data in iOS Apps</b>	2,20
<b>Defensive Coding Fundamentals for JavaScript and HTML5</b>	1,70
<b>Defensive Coding for JavaScript and HTML5</b>	1,20
<b>Introduction to Secure Programming</b>	0,70
<b>Secure Programming for C/C++</b>	1,40
<b>Securing C/C++ Applications</b>	1,10
<b>CISA: The Process of Auditing Information Systems - Part 1</b>	1,30
<b>CISA: The Process of Auditing Information Systems - Part 2</b>	1,50
<b>CISA: Governance and Management of IT - Part 1</b>	1,60
<b>CISA: Governance and Management of IT - Part 2</b>	1,50

<b>CISA: Information Systems Acquisition, Development, and Implementation</b>	2,40
<b>CISA: Information Systems Operations, Maintenance, and Service Management</b>	2,30
<b>CISA: Protection of Information Assets - Part 1</b>	1,50
<b>CISA: Protection of Information Assets - Part 2</b>	2,20
<b>Cryptography Fundamentals: Defining Cryptography</b>	1,50
<b>Cryptography Fundamentals: Applying Cryptography</b>	1,80
<b>Securing Mobile Devices in the Enterprise: Mobile Security Threats</b>	2,00
<b>Securing Mobile Devices in the Enterprise: Mobile Security Technologies</b>	1,70
<b>Securing Mobile Devices in the Enterprise: Mobile Security Threat Mitigation</b>	1,60
<b>Securing Mobile Devices in the Enterprise: Configuring Enterprise-level Security</b>	1,30
<b>Attack Vectors and Mitigations</b>	1,40
<b>Vulnerabilities and Exploits</b>	1,00
<b>Android Architecture, Protection, and Development Best Practices</b>	2,70
<b>Android Security Vulnerabilities, Testing, and Enterprise Considerations</b>	2,00
<b>iOS Security Architecture and Application Data Protection</b>	1,50
<b>Securing Against Threats, Securing for Enterprise, and Jailbreaking Devices</b>	1,40
<b>OWASP Overview</b>	1,00
<b>OWASP Top 10: List Item Overview</b>	1,10
<b>OWASP A8 and A3: Cross-Site Attacks</b>	0,90
<b>OWASP A7 and A6: Leaky and Unprepared Applications</b>	1,10
<b>OWASP A4 and A2: Broken Applications</b>	1,20
<b>OWASP A5 and A1: Security and Injection</b>	1,20
<b>OWASP A10 and A9: API and Component Attacks</b>	0,90
<b>CSSLP: Secure Software Concepts</b>	2,20
<b>CSSLP: Secure Software Requirements</b>	1,30
<b>CSSLP: Secure Software Design</b>	2,50
<b>CSSLP: Secure Software Implementation and Coding</b>	2,10
<b>CSSLP: Secure Software Testing</b>	1,50
<b>CSSLP: Software Acceptance, Deployment, Operations, Maintenance, and Disposal</b>	1,40
<b>CSSLP: Supply Chain and Software Acquisition</b>	1,90
<b>Securing User Accounts: Fundamental Security Concepts</b>	2,60
<b>Securing User Accounts: Authorization, Registration, and Passwords</b>	2,10
<b>Securing User Accounts: Logon, Logoff, Account Changes, and Attack Mitigation</b>	1,90
<b>Systems Security Certified Practitioner: Access Controls</b>	1,00
<b>Systems Security Certified Practitioner: Security Operations</b>	0,80
<b>Systems Security Certified Practitioner: Security Administration</b>	0,90
<b>Systems Security Certified Practitioner: Risk Management</b>	0,90
<b>Systems Security Certified Practitioner: Incident Response and Recovery</b>	1,00

<b>Systems Security Certified Practitioner: Cryptography</b>	1,10
<b>Systems Security Certified Practitioner: Network and Communications Security</b>	1,73
<b>Systems Security Certified Practitioner: Systems and Application Security</b>	2,10
<b>Advanced Windows Store Apps with C# in Visual Studio 2013: Security &amp; Optimizing</b>	1,50
<b>Programming in C#: Debugging and Security Implementation</b>	1,10
<b>TestPrep 300-208 Implementing Cisco Secure Access Solutions (SI-SAS)</b>	1,50