
WorkED
CYBERSECURITY
JOBS

WorkED

SECURITY ANALYST

Required Education
Bachelor's

Average Annual Salary for Security Analysts: $68,384

Security analysts protect organizations' data from cyberattacks. They typically need a bachelor's degree to enter the profession. The BLS reports that information security analysts earn a median annual salary of $99,730, with a 32% projected increase in jobs from 2018-2028. Security analysts work for public and private sector organizations in business, technology, and finance.

Typical job duties may include installing computer security software, conducting penetration testing, training employees to use secure processes, and developing procedures and policies. These professionals often work with managers, employees, and executives to identify effective security plans and procedures.

Security analyst positions require a bachelor's degree at minimum in a field like computer science or IT. Most security analysts start out as software developers or computer programmers and qualify for security analyst positions after 1-2 years of experience. Earning industry certifications can also help individuals qualify for security analyst jobs.

More Info: https://www.cyberdegrees.org/jobs/security-analyst/

WorkED

SECURITY ADMINISTRATOR

Required Education
Bachelor's required, master's preferred

Average Annual Salary for Security Administrator, IT: $66,969

Security administrators prevent organizations from cybersecurity threats and attacks. These professionals serve in high-level roles, overseeing the IT security efforts of their organizations. With the help of their team, they create policies and procedures, identify weak areas of networks, install firewalls, and respond to security breaches. Security administrators work in nearly every industry that relies on computer networks.

The education requirements for this profession vary by position and employer, but typically include a bachelor's degree in a field like IT, computer science, or information assurance. Management-level positions often require a master's in a field like information systems or business administration. Many security administrators gain professional experience through entry-level IT support jobs. Earning certification can improve career prospects.

Security administrators need advanced technical skills in encryption, firewall and router configurations, operating systems, and protocols. They also benefit from communication, problem-solving, and analytical skills.

More Info: https://www.cyberdegrees.org/jobs/security-administrator/

WorkED

SECURITY SOFTWARE DEVELOPER

Required Education
Bachelor's required

Average Annual Salary for Security Software Developers: $73,788

Security software developers create new technologies for programs and applications. They integrate security protocols into existing programs and applications to ensure software security. Security software developers must possess an advanced understanding of all aspects of software development as they often participate in the entire lifecycle of development.

Their specialized knowledge spans IT security, computer system and network analysis, software design, and programming languages. They may work as members of a software development team or independently. Employers may include government agencies, nonprofit groups, and private businesses.

Education requirements include a bachelor's degree in software engineering, computer science, or a related field. Many security software developers start their careers as general software developers and specialize in security software development over time. Industry certifications, like the global information assurance certification, can offer career benefits to security software developers.

More info: https://www.cyberdegrees.org/jobs/security-software-developer/

WorkED

SECURITY ENGINEER

Required Education
Bachelor's required, master's helpful

Average Annual Salary for Security Engineers: $90,745

Security engineers create IT security systems to protect their organizations' systems and sensitive data from cyberattacks. Their main job duties include building intrusion detection systems and firewalls to stop attacks. Other tasks include conducting security assessments, tests, and risk analyses. They also deliver reports and make recommendations to executives.

A bachelor's degree in cybersecurity, engineering, programming, or computer science represents the typical minimum education requirement for most security engineering positions. In addition to education, security engineers usually need 1-5 years of relevant work experience. Security engineers with a master's degree typically qualify for top-level positions.

Many security engineering positions require industry certifications such as certified ethical hacker or certified information systems security professional. According to PayScale, security engineers earn an average annual salary of $90,745.

More info: https://www.cyberdegrees.org/jobs/security-engineer/

WorkED

PENETRATION TESTER

Required Education
Bachelor's or master's often required

Average Annual Salary for Penetration Testers: $84,605

Penetration testers find vulnerabilities in networks, information systems, and web applications. They test established security systems and try to prevent cyberattacks. Penetration testers identify weaknesses by conducting their own simulated cyberattacks without actually making data vulnerable, a practice sometimes called ethical hacking.

Penetration testing professionals often work for government, healthcare, and finance organizations. They need strong analytical, problem-solving, and hacking skills.

Penetration testers with excellent hacking skills may not need a degree to find employment. However, entry-level positions typically require a bachelor's degree in a field like computer science or cybersecurity and relevant experience. High-level management roles may require as much as 10 years of experience and/or a master's degree.

More Info: https://www.cyberdegrees.org/jobs/penetration-tester/

WorkED

INCIDENT RESPONDER

Required Education
Bachelor's required, master's preferred

Average Annual Salary for Incident Managers: $80,873

The incident responder includes jobs such as response engineer, cyber incident responder, computer network defense incident responder, and forensics intrusion analyst. Most incident response professionals respond to cybersecurity incidents and data breaches.

These professionals improve the overall security, finances, and reputations of organizations. They also provide cybersecurity education to employees and detect threats. Typical job duties include developing systems and plans for identifying security breaches, conducting risk analysis, reverse engineering, and writing reports for law enforcement and/or management.

Some incident responder professionals complete certifications like certified intrusion analyst or certified incident handler, but most hold a bachelor's degree at minimum. Earning a master's degree in cybersecurity, computer forensics, or a related field may open up more career opportunities with greater salary potential.

More Info: https://www.cyberdegrees.org/jobs/incident-responder/

WorkED

CRYPTOGRAPHER

Required Education
Master's or Ph.D. preferred

Average Annual Salary for Cryptologists:
$73,067

Cryptographers help organizations safely and securely communicate and exchange information. As cyberattacks and threats grow, the demand for skilled cryptographers who can protect valuable information may increase. Cryptographers typically work for government agencies, financial institutions, and healthcare organizations. Companies like Amazon, Google, and Apple also hire cryptographers.

Cryptographers develop and crack codes, puzzles, and cryptograms. They encrypt data by writing algorithms, security protocols, and cyphers; break down codes to decrypt data; and create cryptology theories. They also identify weaknesses, vulnerabilities, and potential problems by analyzing encrypted systems.

Professional cryptographers need advanced communication, analytical, and problem-solving skills. They must also possess a variety of technical computer and IT skills. They need to understand algorithms, data structures, multiple programming languages, and various operating systems. The high-level knowledge this career requires means that most employers prefer job applicants with a master's or Ph.D.

More info: https://www.cyberdegrees.org/jobs/cryptographer/

WorkED

VULNERABILITY ASSESSOR

Required Education
Associate required, bachelor's or master's may be helpful

Average Annual Salary for Security Assessors: $102,500

Vulnerability assessors find weaknesses in computer systems and applications. They often present their findings in a formal vulnerability assessment that businesses can consult when making corrections or improvements. Required skills include mastery of multiple operating systems, computer hardware and software systems, and security frameworks.

Typical job tasks include creating a vulnerability assessment database, offering training for systems and network administrators, tracking vulnerability metrics over time, and testing custom scripts and applications. As a highly specialized career, it can be difficult to find salary estimates for vulnerability assessors. However, PayScale reports a $102,500 average annual salary for security assessors.

Junior vulnerability assessors may only need an associate degree and a few years of IT security experience. However, mid- and high-level positions usually require a bachelor's or master's degree and significant professional experience. Specific degree requirements vary by position and employer.

More Info: https://www.cyberdegrees.org/jobs/vulnerability-assessor/

WorkED

FORENSICS EXPERT

Required Education
Bachelor's required

Average Annual Salary for Forensic Computer Analysts: $73,892

Forensics experts investigate computer and cyber crimes and help organizations protect sensitive data and information. Typical job duties may include educating employees about cybersecurity issues, identifying security weaknesses, retrieving data from systems and devices, and reconstructing information systems to understand data breaches. Sometimes forensics experts serve as expert witnesses in trials.

Forensics experts usually work with other IT security professionals. They often deliver security reports to executives, lawyers, and law enforcement personnel. Employers include government agencies, large corporations, and law firms. Individuals with a high level of expertise may work as consultants. Skills required of forensics experts vary by position but typically include advanced understanding of computer software and hardware, programming languages, operating systems, and cryptography.

Entry-level positions usually require at least a bachelor's degree in cybersecurity, computer science, or a related field, and some professional experience. Forensics experts may qualify for mid-level and upper-level positions after accumulating more experience, certifications, and education.

More Info: https://www.cyberdegrees.org/jobs/computer-forensics/

WorkED

SECURITY ARCHITECT

Required Education
Bachelor's

Average Annual Salary for Security Architect, IT: $123,687

Security architects design, plan, and supervise systems that thwart potential computer security threats. They must find the strengths and weaknesses of their organizations' computer systems, often developing new security architectures. Job tasks may include budget preparation, allocation of personnel resources, management of IT teams, and report preparation.

These professionals must possess advanced knowledge of software and hardware design, computer programming, risk management, and network and computer systems. Communication, problem-solving, and analytical skills all rank high in importance for this profession. Computer network architects find many opportunities in the computer systems design and telecommunications industries.

Security architects need at least a bachelor's degree in a field like computer science or IT and relevant professional experience. Many enter the field with hacking experience. To advance in the field, they often earn certifications, pursue graduate degrees, and take continuing education classes. PayScale reports an average annual salary of $123,687 for IT security architects.

More info: https://www.cyberdegrees.org/jobs/security-architect/

WorkED

CHIEF INFOSEC OFFICER

Required Education
Bachelor's required, master's recommended

Average Annual Salary for CISOs
$162,037

Chief information security officers occupy high-level roles as they protect their companies' data and manage IT and security issues. They work with other executives and IT security experts. These professionals need advanced business, technical, management, and organizational skills. They must also keep abreast of trends and current issues in information security.

Chief information security officers supervise the operational aspects of data protection and management. They develop information security procedures and policies for organizations and manage teams of professionals who identify and mitigate security threats. Other typical job tasks may include developing budgets, carrying out audits, and making sure that the company complies with relevant laws and regulations.

Most chief information security officers start their careers as IT analysts or specialists with a bachelor's degree in a field like cybersecurity, computer science, or IT.
As they gain experience, certifications, and further education, they can advance to higher-level roles.

More Info: https://www.cyberdegrees.org/jobs/chief-information-security-officer-ciso/

WorkED

CYBERSECURITY JOBS

WorkED

BEST LOCATIONS FOR JOBS IN CYBERSECURITY

The state and city where a professional chooses to live can **affect salary and career outlook in the cybersecurity field**. For example, densely populated major cities typically feature higher costs of living but offer higher salaries than more rural areas.

The presence of certain **high-paying and top-employing industries** also impacts the outlook for cybersecurity jobs in different locations. Cities with large IT, healthcare, and finance sectors may need to hire more skilled cybersecurity experts.

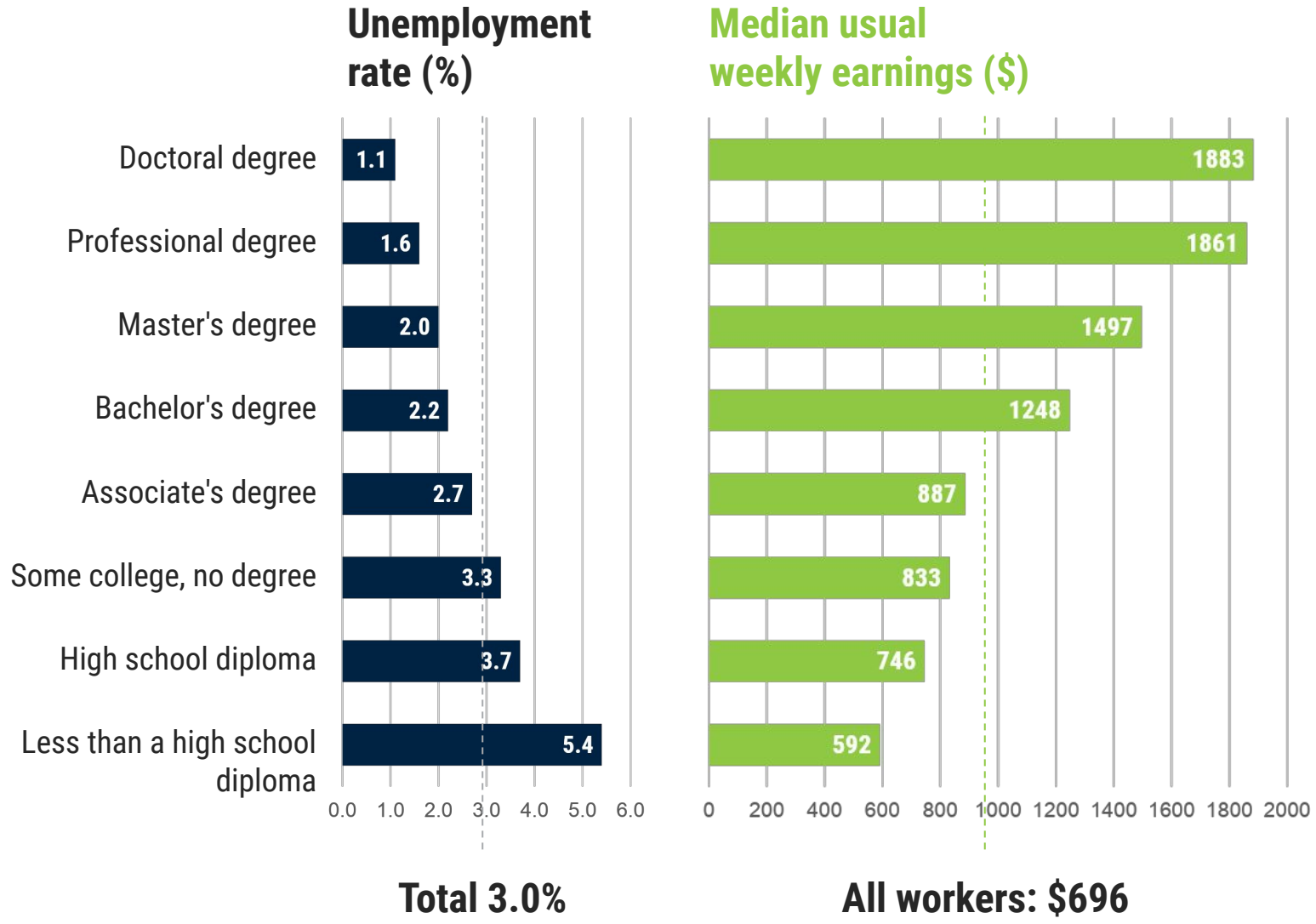
WorkED

CITY - CAREER, PERCENTAGE ABOVE AVERAGE PAY

Arlington, VA
Forensic Computer Analyst, 8%
Atlanta, GA
Incident Manager, 12% Penetration Tester, 1% Security Analyst, 2% Security Director, 10%
Boston, MA
CISO, 20% Forensic Computer Analyst, 8% Security Administrator, IT, 8% Security Architect, 4% IT Auditor, 3% Security Engineer, 1%
Chicago, IL
CISO, 23% Penetration Tester, 12% Security Analyst, 3% Security Architect, 5% Security Engineer, 7% Security Manager, IT, 24%
Columbus, OH
Information Security Specialist, 9%
Dallas, TX
CISO, 15% Incident Manager, 4% Security Administrator, IT, 19% Security Manager, IT, 20%
Houston, TX
Security Analyst, 6% Security Director, 22% Security Manager, IT, 18%
Kirkland, WA
Incident Manager, 39%
New York, NY
CISO, 18% Incident Manager, 61% Security Administrator, IT, 8% Security Architect, 10% IT Auditor, 21% Security Director, 17% Security Engineer, 24% Security Manager, IT, 17% Information Security Specialist, 37%
Philadelphia, PA
Forensic Computer Analyst, 4%
Phoenix, AZ
Information Security Specialist, 50%
Pittsburgh, PA
Security Administrator, IT, 5%
San Francisco, CA
Security Engineer, 42%
Seattle, WA
Incident Manager, 32% Penetration Tester, 16% Security Administrator, IT, 13% Security Analyst, 18% Security Engineer, 20% Information Security Specialist, 13%
Washington, DC
CISO, 6% Forensic Computer Analyst, 31% Penetration Tester, 21% Security Analyst, 12% Security Architect, 19% Security Engineer, 2% IT Auditor, 1% Security Director, 56% Security Manager, IT, 24% Information Security Specialist, 19%

WorkED

UNEMPLOYMENT RATES AND EARNINGS BY EDUCATIONAL ATTAINMENT, 2019



Note: Data are for persons age 25 and over. Earnings are for full-time wage and salary workers.
Source: U.S. Bureau of Labor Statistics, Current Population Survey.

WorkED

LIFETIME EARNINGS BY DEGREE
(IN MILLIONS DOLLARS)

OCCUPATION	LESS THAN HIGH SCHOOL	HIGH SCHOOL DIPLOMA	SOME COLEEGE	ASSOCIATE'S	BACHELOR'S	MASTER'S / PROFESSIONAL / DOCTORAL
Human Resources. Training, and Labor Relations Specialists	-	1.7	1.9	1.9	2.3	2.9
Management Analysts	-	-	2.2	-	2.9	3.5
Other Business Operations Specialists	-	1.6	1.8	-	2.3	3.1
Accountants and Auditors	-	1.5	1.7	1.6	2.4	3.0
Appraisers and Assessors of Real Estate	-	-	-	-	2.0	-
Budget, Credit, Financial Analysts	-	-	-	-	2.7	3.8
Personal Financial Advisors	-	-	2.0	-	3.1	3.8
Insurance Underwriters	-	-	-	-	2.7	-
Financial Examiners, Financial Specialists, all other	-	-	-	-	2.7	-
Loan Counselors and Officers	-	1.6	1.8	-	2.4	2.9
Tax Examiners, Collectors, Revenue Agents, and Preparers	-	-	-	-	2.2	-
Computer Scientists and Systems Analysts	-	2.2	2.4	2.3	3.0	3.5
Computer Programmers	-	-	2.6	2.7	3.0	3.3
Computer Software Engineers	-	-	3.1	3.0	3.6	3.9
Computer Support Specialists	-	1.9	2.1	2.0	2.4	2.6
Database Administrators	-	-	-	-	3.0	-
Network and Computer Systems Administrators	-	-	2.5	2.5	2.9	3.3
Network Systems and Data Communications Analysts	-	-	2.4	2.5	2.7	3.4

WorkED

WHAT ARE IT CERTIFICATIONS?

A formal process to make certain that an individual is qualified in terms of particular knowledge or skills.

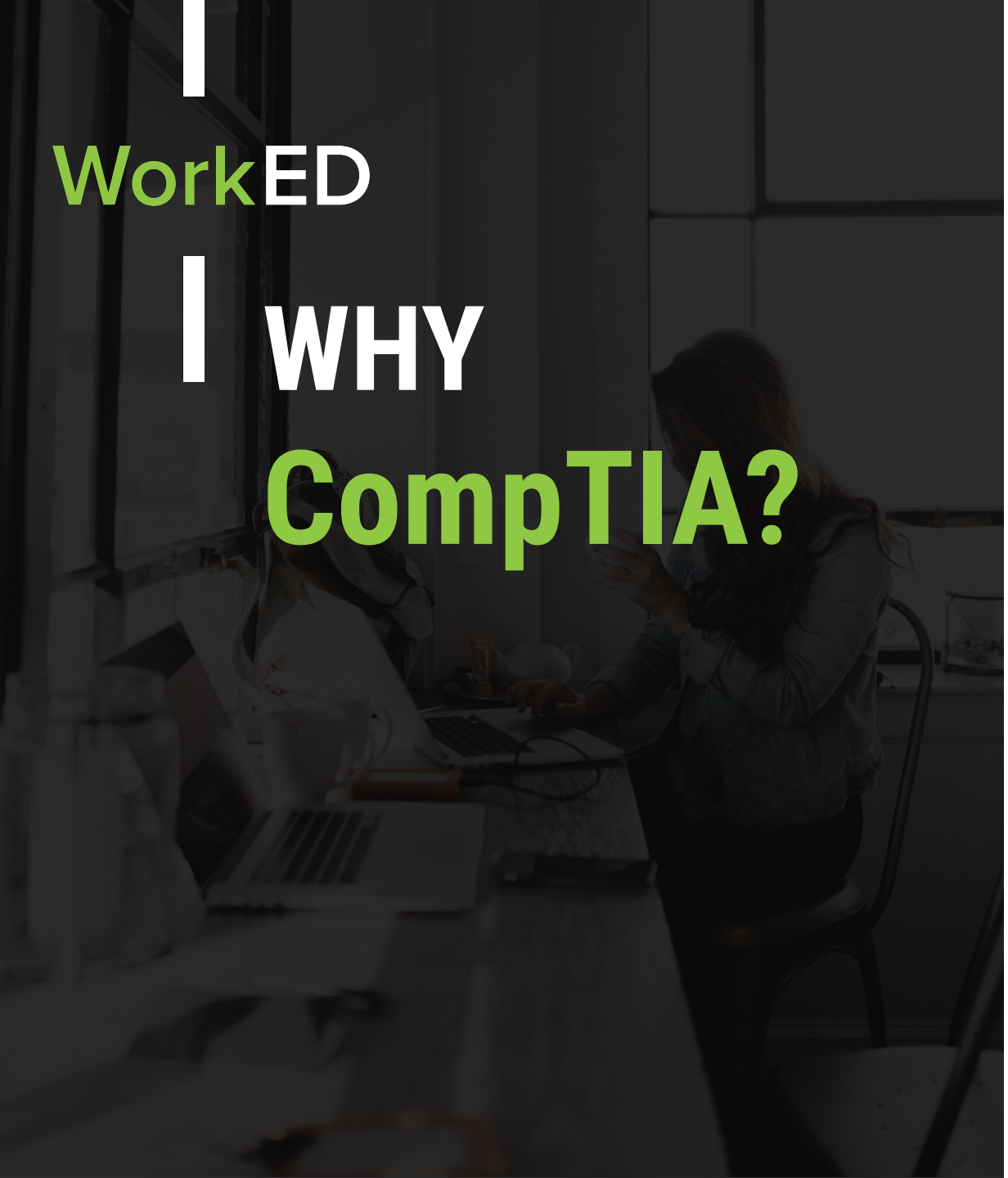
Time Effective

Cost Effective

Networking

Flexible Educational Requirements

Gain Practical Skills
Benefits of Certification



WorkED

WHY CompTIA?

- Vender Neutral
- Established since 1993
- Aligned to real-world skills IT Professionals Need
- Stays relevant with current industry standards
  - Training
  - Additional Certifications
  - Continuing Education

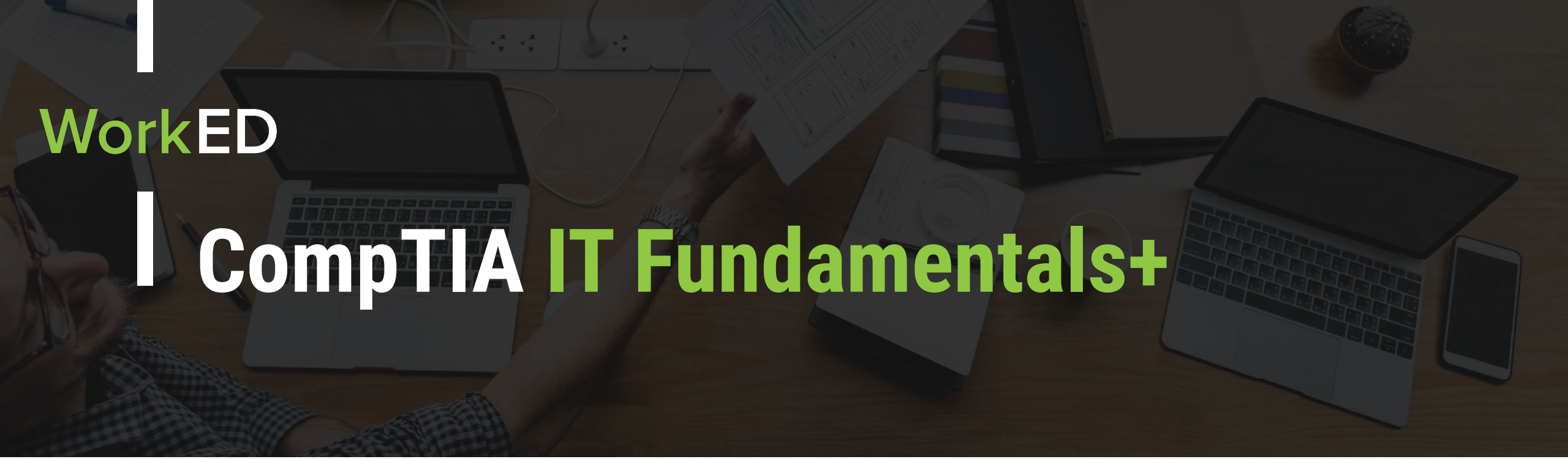
WorkED

CERTIFICATIONS

CompTIA A+
CompTIA Network+,
CompTIA Cybersecurity Analyst (CySA+),
CompTIA PenTest+
CompTIA Advanced Security Practitioner (CASP)
CompTIA Security+

Certified Ethical Hacker (CEH)
Certified Information System Security Professional (CISSP)
Certified Information Security Manager (CISM)
Certified Information Systems Auditor (CISA)
NIST Cybersecurity Framework (NCSF)
Certified Cloud Security Professional (CCSP)
Computer Hacking Forensic Investigator (CHFI)
Cisco Certified Network Associate (CCNA)

https://www.newhorizons.com/article/the-best-cybersecurity-certifications-to-boost-your-career-in-2018
https://cybersecurityventures.com/10-hot-cybersecurity-certifications-for-it-professionals-to-pursue-in-2019/
https://hackr.io/blog/best-cybersecurity-certification
https://www.cyberdegrees.org/resources/certifications/



WorkED

CompTIA IT Fundamentals+

- **Entry-level** IT certification
- Demonstrates your readiness for the digital workplace, covering networking and cybersecurity essentials to hardware and software basics.

WorkED

CompTIA A+

- CompTIA A+ is the **Globally Recognized industry standard** for getting a job in technical support and establishing an IT career.
- More than one million IT professionals hold the A+ certification. A+ is required for Dell, Intel and HP service technicians and is recognized by the U.S. Department of Defense.
- **Jobs**: Technical Support Specialist, IT Support Technician, Field Service Technician
- The median annual wage for computer user support specialists was **$53,100** in May 2016.

WorkED

CompTIA Network+

- CompTIA Network+ verifies that you have the **essential knowledge and skills in networking** central to careers in IT infrastructure and cybersecurity.
- **Jobs**: Network Field Technician, Network Support Specialist, Network Administrator, Network Analyst, Technical Support
- The median annual wage for Network and Computer Systems Administrators was **$79,700** in May 2016

WorkED

CompTIA Security+

- CompTIA Security+ validates the **baseline skills necessary to perform core security functions** and pursue an IT security career.
- **Jobs**: Security Architect, Security Engineer, Security Consultant, Security Specialist, Security or Systems Administrator
- The median annual wage for information security analysts was **$92,600** in May 2016.

WorkED

SOME CERTIFICATION OPTIONS

App Development with Swift

Associate of (ISC)² Designation

(International Information System Security

Certification Consortium)

C++ Certified Associate Programmer (CPA)

Google

Internet and Computing Core Certification (IC3)

Microsoft Technology Associate (MTA)

Oracle

Unity Certified Programmer

WD Certified Web Design Certification

WorkED

CYBERSECURITY JOBS

QUESTIONS?

THANK YOU