

# INFOSEC™

# Build your cybersecurity workforce.



## Closing your skills gap

The shortage of cybersecurity professionals has grown to nearly three million globally, with 498,000 openings in North America. There are simply not enough trained professionals to fill the current demand. Organizations are clamoring for fresh talent, but where can you find those individuals — and how can you get them up to speed quickly and effectively?

Luckily for you, a proven pathway has been established. At Infosec, we've been helping organizations close their cybersecurity skills gaps for more than 15 years. Follow their well-trodden path, and before you know it, you'll have a fresh batch of cybersecurity professionals ready to carry the workload — and be on your way to a more secure organization.



## 3 steps to jumpstart your cybersecurity workforce



### 1. CompTIA A+

Build your team's foundation of knowledge and skills related to entry-level technical support roles.



### 2. CompTIA Network+

Expand your team's skills by teaching them how to configure, troubleshoot and oversee networks.



### 3. CompTIA Security+

Establish a baseline of security concepts and practical skills for your team that will aid them throughout their careers.

# VetsInTech

## No experience, no problem

In 2019, we partnered with VetsInTech to help train veterans for cybersecurity roles using the same getting started in cybersecurity model outlined above. The program includes three weeks of intense training focused on building the skills required to earn the A+, Network+ and Security+ certifications.

Many who attended began with little or no IT experience; nevertheless, the program has seen a 100% pass rate and 95% employment rate. It's provided a model for individuals looking to jumpstart their cybersecurity careers — and a path forward for organizations looking to upskill employees for entry-level cybersecurity roles.



## Security+

### Springboard for security careers

If your employees are starting without any cybersecurity experience, they're not alone. According to our "2019 Cybersecurity Industry Report," only 8% of cybersecurity professionals began their careers directly in an information security role. But the report also found common ground: Security+ was by far the most commonly held certification. By identifying talented employees and training them towards Security+, you'll establish a new generation of cybersecurity talent within your organization. They'll have a broad range of entry-level knowledge, including:

- » Common cyber threats and vulnerabilities
- » Popular security technologies and tools
- » Best practices for secure networks and systems
- » Technical controls, such as identity management and cryptography
- » Impact of cyber risks on businesses

Once a baseline of knowledge and skills is established, those employees can pursue a variety of skills and career paths unique to your organization.

## Cybersecurity careers:

### By the numbers



**3.5 million**

Number of projected unfilled cybersecurity positions by 2021



**32% growth**

Expected increase in cybersecurity jobs from 2018-2028



**92% of infosec pros**

Spend at least a few hours each month learning new skills



**500,000+**

Number of Security+ certification holders

# Common cybersecurity careers:

## Which path is right for your team?

### Entry-level

#### Cybersecurity specialist

Perform essential duties, such as network security, vulnerability assessments and intrusion detection.

[Learn More](#)

#### Cybercrime analyst

Understand how malware compromises a system and the methodologies behind digital forensics.

[Learn More](#)

#### Incident analyst

Understand security operations and a range of technical and communication skills.

[Learn More](#)

#### IT auditor

Understand internal auditing procedures, risk assessments and compliance requirements.

[Learn More](#)



### Mid-level

#### Cybersecurity analyst

Implement more complex aspects of security, including security operations, cyber threat analysis and cryptography.

[Learn More](#)

#### Cybersecurity consultant

Evaluate and communicate an organization's cybersecurity risk and how it relates to security standards and frameworks.

[Learn More](#)

#### Penetration tester

Understand pentesting methodologies and vulnerability assessments, exploiting systems and communicating findings.

[Learn More](#)



### Advanced

#### Cybersecurity manager

Advanced understanding of information security concepts, security operations and information assurance as well as project and risk management.

[Learn More](#)

#### Cybersecurity engineer

Advanced understanding of information security principles, including network security, authentication, cryptography, and project and risk management.

[Learn More](#)

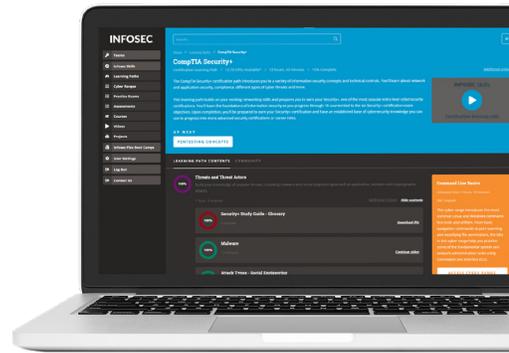
#### Cybersecurity architect

Advanced understanding of technical security as well as a thorough understanding of systems development and project and risk management.

[Learn More](#)

# Stay ahead of technology change with hands-on cybersecurity education

Skill up and get certified with hands-on cybersecurity training for you and your team. Train on your team's schedule with unlimited access to 100s of courses and hands-on cyber ranges — or upgrade to a boot camp for live, instructor-led training guaranteed to certify your team on their first attempt.



Guide development with 700+ courses mapped to the Workforce Framework



Build practical skills with cloud-hosted cyber ranges and hands-on projects



Identify and fill knowledge gaps with technical skill assessments



Gauge exam readiness with customizable certification practice exams



Fast-track certification with 100+ live, instructor-led boot camps

[Download Course Catalog](#)

## Certify your team — guaranteed

IT and security certification is often more than a goal — it's a business requirement. That's why we offer over 100 certification boot camps taught by industry experts with 10+ years of experience. Here's how we guarantee your certification success:

- » **Exam Pass Guarantee:** Students who don't pass their exam on the first attempt get a second attempt free. Includes the ability to re-sit the course for free for up to one year.
- » **100% Satisfaction Guarantee:** Students who are not 100% satisfied with their boot camp at the end of day one may enroll in a different online or in-person course.
- » **Knowledge Transfer Guarantee:** If your employee leaves within three months of obtaining certification, we will train a different employee tuition-free for up to one year.

## About Infosec

At Infosec, we believe knowledge is the most powerful tool in the fight against cybercrime. We provide the best certification and skills development training for IT and security professionals, as well as employee security awareness training and phishing simulations. Learn more at [infosecinstitute.com](https://infosecinstitute.com).