INFOSEC Skills

Cybersecurity talent development playbook

12 pre-built training plans to help teams identify, upskill and retain cybersecurity talent

Introduction

There are more than four million open cyber roles worldwide. This shortage of cybersecurity talent is magnified by today's highly competitive job market — causing many organizations to see record-high churn rates, recruitment costs and staff salaries.

Infosec's 2021 IT and Security Talent Pipeline Study found that hiring managers experiencing recruiting success were 44% more likely to consider candidates with no previous experience and 67% more likely to report well-defined cyber roles.

"It is highly unreasonable for companies to expect turn-key hires. There is no one-size-fits-all."

— Jonathan Brandt, Director of Professional Practices and Innovation at ISACA

It's clear that with the right training program, organizations and their teams can greatly reduce the negative impacts felt by the cybersecurity skills gap and the competitive job market. That's why Infosec developed pre-built training roadmaps for 12 of the most in-demand cybersecurity roles. Team leaders can leverage these Infosec Skills Roles to efficiently and effectively:

- Personalize development plans for each employee at every stage of their career
- Upskill and cross-train talent for open cybersecurity positions within their organization
- Boost employee engagement and talent retention

Backed by the research of skills requested by employers and a panel of cybersecurity subject matter experts, each of the 12 Infosec Skills Roles clearly outlines which training and certifications are needed so professionals can spend their limited time on the areas that matter most.

$138K - $184K

Cost to replace a single cybersecurity employee

(Source: Gallup and Payscale)

92%

Hiring managers impacted by the cybersecurity skills gap

(Source: Infosec)

66%

Boost in employee retention when learning and development opportunities are provided

(Source: Salesforce)

Creating a training plan

Role-guided

Developing cybersecurity talent and teams cannot be a one-size-fits-all approach. It is critical to tailor training plans to each employee's job role and level of proficiency. Check out the "Which roles fit your team" section to find the right role for each of your team members.

Measurable

Set your team up for success by identifying and tracking training goals. Every Infosec Skills Role includes a variety of skill assessments and practice exams, helping you to gather baseline scores and report on progress over time.

Personalized

Beyond immediate training goals, provide each employee with a long-term career roadmap. Employees with this insight tend to have greater confidence in their skills, longer retention rates and higher job satisfaction. Twelve sample training plans are provided below to support the long-term career development of each Infosec Skills Role.

Hands-on

We all learn better when we learn by doing. Incorporating elements of hands-on training will deepen your team's engagement, accelerate their skill development and increase their knowledge retention. Explore our Infosec Skills Roles for relevant hands-on training opportunities to move your team from theory to practice.

Engaging

A great way to encourage continuous learning is to gamify the experience with micro-credentials. Small yet tangible milestones will provide your team with the social validation they need to stay motivated. Every time your employee completes a learning path on their training roadmap, they will earn a certificate of completion.

Additional team and skill development resources

"We are finding that retention rates are going up in our cybersecurity roles because people feel like they're being listened to. They're being provided opportunities that they may not have had before."

— James "Slim" Beamon, Dean of the CyberEDGE Academy and Senior Cybersecurity Program Manager at Leidos

2021 IT and Security Talent Pipeline Study

Read Now

2021 Cybersecurity Role and Career Path Clarity Study

Read Now

Developing Cybersecurity Talent and Teams Ebook

Read Now

Talk to Infosec about role-guided training

Book a Meeting

Which roles fit your team?

Infosec Skills role-guided training is designed to be flexible, whether you want to hit the ground running with an out-of-the-box training plan or build a custom plan mapped to the NICE Workforce Framework for Cybersecurity or MITRE ATT&CK® Matrix for Enterprise.

Check out the 12 Roles below and tweak the training plans as necessary to fit your organization's needs.

Cybersecurity Beginner

Cross-train employees and build a baseline of cybersecurity knowledge.

View Plan

SOC Analyst

Build a baseline of incident response skills and prepare junior analysts to progress into more senior positions.

View Plan

Digital Forensics Analyst

Prepare your team to investigate and uncover the true nature of cybersecurity incidents.

View Plan

Penetration Tester

Build your team's skills around uncovering vulnerabilities and other security weaknesses.

View Plan

ICS Security Practitioner

Build your team's operational technology skills and keep your industrial control systems (ICS) secure.

View Plan

Security Engineer

Build your team's technical skills and keep your organization's security controls running smoothly.

View Plan

Cloud Security Engineer

Build your team's cloud security skills and ensure your organization's cloud infrastructure is secure.

View Plan

Security Architect

Upskill your team to better design, implement and maintain secure infrastructure.

View Plan

Information Risk Analyst

Upskill your team and gain a better understanding of how to assess and manage organizational risk.

View Plan

Security Manager

Build your team's management skills and ensure your organization's security aligns with business objectives.

View Plan

Privacy Manager

Build your team's privacy skills and learn to create a strategic and comprehensive privacy program.

View Plan

Secure Coder

Upskill your engineering team and ensure your software and applications are protected from vulnerabilities.

View Plan

Create your free Infosec Skills account to browse all 190+ role-guided learning paths.

Browse All Training

Cybersecurity Beginner

What is a Cybersecurity Beginner?

If you need to get your team up to speed on cybersecurity basics, this is the perfect role for them. The Cybersecurity Beginner Role focuses on the foundational skills and knowledge that will allow anyone to take the first step towards transitioning into a cybersecurity career. No prior knowledge of cybersecurity or work experience is required. The only prerequisite is a passion for technology and cybersecurity.

How this role helps my organization

Finding cybersecurity candidates with the exact background you desire can be challenging. This role provides a proven pathway to quickly upskill employees and certifies they have the baseline of knowledge needed for future success — whether they're external hires with less experience or existing employees from other areas of your organization.

What will my team learn?

You can easily customize the training assigned from the Cybersecurity Beginner Role to fit each team member's needs depending on existing knowledge and skills. It includes CompTIA's "core" certifications and other entry-level learning paths that organizations like VetsInTech and other private enterprises have used to build a baseline of knowledge. They'll learn about:

- Hardware, operating systems and mobile device management
- Applications and software development
- Network and cloud infrastructure
- Best practices for troubleshooting
- Common attacks, threats and vulnerabilities
- Introduction to risk and risk management
- Security operations and incident response
- Implementing security best practices

Role at a glance

Core domains

- Foundational cybersecurity

Related job titles

- Beginner
- Newbie
- Entry-level

Related NICE Work Roles

No direct correlation, but this role gives you the foundational knowledge you need for all NICE Work Roles.

View all Cybersecurity Beginner training

View Training

INFOSEC SKILLS SAMPLE TRAINING PLAN

Cybersecurity Beginner

Cross-train employees and build a baseline of cybersecurity knowledge with the Cybersecurity Beginner Role training plan. Use the pre-built training below or customize the plan to meet your organization's goals.

Build your team's skills (Core)

Cybersecurity Foundations
- OS, network & cloud basics
- Risk management basics
- Command line basics

CompTIA A+
- Install, configure & support devices
- Network, virtualization & cloud fundamentals
- Troubleshoot devices & software

CompTIA Security+
- Implement security solutions
- Monitor & secure hybrid environments
- Identify, analyze & respond to incidents

CompTIA Network+
- Network technology & devices
- Implement, monitor & optimize networks
- Harden & troubleshoot networks

Specialize your team's skillsets (Elective)

Linux Fundamentals
- Linux architecture
- Linux jobs & processes
- Linux scripting & automation

The Basics: EC-Council CEH
- Recon & vulnerability analysis
- Web app, wireless & IoT hacking
- Exploitation & exfiltration

Fundamental Privacy Laws & Acts
- U.S. federal privacy legislation
- U.S. healthcare privacy laws
- Global data protection laws

Apply your team's skills (Continuing Ed)

Command Line Basics Cyber Range
- Common Windows tools & utilities
- Common Linux tools & utilities
- System & network admin tasks

Other potential Cybersecurity Beginner training: CompTIA ITF+, Certified Reverse Engineering Analyst Fundamentals, The Basics: CISA, The Basics: CISM and more.

Create your free Infosec Skills account to see all role-guided training

See All Training

Want to speak to someone? Book a meeting now.

SOC Analyst

What is a SOC Analyst?

Security Operations Center (SOC) Analysts are responsible for analyzing and monitoring network traffic, threats and vulnerabilities within an organization's IT infrastructure. This includes monitoring, investigating and reporting security events and incidents from security information and event management (SIEM) systems. SOC Analysts also monitor firewall, email, web and DNS logs to identify and mitigate intrusion attempts.

How this role helps my organization

SOC Analyst is a great role to evaluate junior cybersecurity hires and help them grow into the types of mid-level security employees your company needs. Since this role is typical for many newcomers, it's important to develop a training plan that builds a base foundation of skills to set them up for long-term success — and provides the opportunity to discover future career interests and aptitudes.

What will my team learn?

The SOC Analyst Role in Infosec Skills aligns with 37 Knowledge Statements and eight Skill Statements in the NICE Framework, which primarily roll up to the following competencies:

- Vulnerabilities assessment
- Threat analysis
- Infrastructure design
- Information systems/ network security
- Incident management
- System administration
- Computer network defense
- Business continuity

Common tools and technology

- Wireshark
- Solarwinds Security Event Manager
- Solarwinds Log Analyzer
- Splunk
- Splunk Enterprise Security
- LogRhythm NextGen SIEM
- Alienvault Unified Security Management
- Sumo Logic
- McAfee Enterprise Security Manager
- Trend Micro
- Snort
- Barracuda
- LogDNA
- Datadog

Role at a glance

Core domains

- Cyber defense analysis
- Systems analysis

Related job titles

- Security analyst
- Security specialist
- Incident analyst

Related NICE Work Roles

- Systems security analyst
- Cyber defense analyst
- Vulnerability assessment analyst
- Cyber defense incident responder
- Cyber defense infrastructure support specialist

View all SOC Analyst training

View Training

INFOSEC SKILLS SAMPLE TRAINING PLAN

SOC Analyst

Build a baseline of incident response skills and prepare junior analysts to progress into more senior positions with the SOC Analyst Role training plan. Use the pre-built training below or customize the plan to meet your organization's goals.

Build your team's skills (Core)

CertNexus CyberSec First Responder
- Tools, tactics & procedures
- Evaluate & analyze cybersecurity intel
- Remediate & report incidents

Incident Response
- Incident response stages
- Incident response tool deep dive
- Memory, network & host forensics

Cyber Threat Hunting
- Intelligence gathering
- Investigation techniques
- Remediation methods

Network Traffic Analysis for Incident Response
- Collect & analyze traffic data
- Case studies of extracting intel
- Build network monitoring program

Specialize your team's skillsets (Elective)

Advanced Intrusion Detection
- Open-source tools & use cases
- Prioritize risks with frameworks
- Craft meaningful detections

Cybersecurity Data Science
- Static & dynamic malware analysis
- Building an IDS
- Machine learning use cases

Apply your team's skills (Continuing Ed)

Network Traffic Analysis Cyber Range
- TShark, Scapy & other tools
- Examine capture files & live traffic
- Identify & anlayze abnormal traffic

Cyber Threat Hunting Cyber Range
- Detect port scans
- Find threats in .pcap & .vmem files
- Hunt host-based & network-based threats

Other potential SOC Analyst training: Computer Forensics, Threat Modeling and more.

Create your free Infosec Skills account to see all role-guided training

See All Training

Want to speak to someone? Book a meeting now.

Digital Forensics Analyst

What is a Digital Forensics Analyst?

Digital Forensics Analysts collect, analyze and interpret digital evidence to reconstruct potential criminal events and/or aid in preventing unauthorized actions from threat actors. They help recover data like documents, photos and emails from computer or mobile device hard drives and other data storage devices — such as zip folders and flash drives — that have been deleted, damaged or otherwise manipulated. Digital Forensics Analysts carefully follow chain-of-custody rules for digital evidence and provide evidence in acceptable formats for legal proceedings.

How this role helps my organization

When a cybersecurity incident occurs, Digital Forensics Analysts are the professionals who piece together what happened and the potential impact on your organization. That's why it's important to build a training program that aligns with the types of data and systems they may be tasked with analyzing. The technical and analytical nature of the role is also a good fit for transitioning into future roles like Penetration Tester or Information Risk Analyst.

What will my team learn?

The Digital Forensics Analyst Role in Infosec Skills aligns with 46 Knowledge Statements and 22 Skill Statements in the NICE Framework, which primarily roll up to the following competencies:

- Computer forensics
- Vulnerabilities assessment
- Threat analysis
- System administration
- Legal, government and jurisprudence
- Operating systems
- Information systems/ network security
- Encryption
- Computers and electronics
- Computer network defense`

Common tools and technology

- Kali Linux
- Disk analysis: Autopsy/the Sleuth Kit
- Image creation: FTK imager
- Memory forensics: Volatility
- Windows registry analysis: Registry recon
- Mobile forensics: Cellebrite UFED
- Network analysis: Wireshark
- Linux distributions: CAINE

Role at a glance

Core domains

- Digital forensics

Related job titles

- Incident handler
- Incident responder
- Incident response analyst
- Incident response engineer
- Incident response coordinator
- Intrusion analyst
- Computer network defense incident responder
- Computer security incident response team engineer

Related NICE Work Roles

- Cyber defense forensics analyst
- Cybercrime investigator
- Cyber defense incident responder

View all Digital Forensics Analyst training

View Training

INFOSEC SKILLS SAMPLE TRAINING PLAN

Digital Forensics Analyst

Prepare your team to investigate and uncover the true nature of cybersecurity incidents with the Digital Forensics Analyst training plan. Use the pre-built training below or customize the plan to meet your organization's goals.

Build your team's skills (Core)

Certified Computer Forensics Examiner (CCFE)
- Investigation process
- Legal issues
- Types of forensic artifacts

Network Forensics
- Concepts & techniques
- Firewalls, IDSes & other tools
- Log, protocol, email & traffic analysis

Windows Registry Forensics
- Structure of registry hives
- Investigate different hive files
- Export & interpret data

Windows OS Forensics
- FAT32, exFAT & NTFS systems
- Recover deleted files
- Interpret & validate data

Specialize your team's skillsets (Elective)

Certified Mobile Forensics Examiner (CMFE)
- Android, iOS & other forensics
- Analyze & extract evidence
- Report on findings

Introduction to x86 Disassembly
- Computer architecture basics
- Build & debug x86
- x86 assembly instructions

Cyber Threat Hunting
- Intelligence gathering
- Investigation techniques
- Remediation methods

Certified Reverse Engineering Analyst (CREA)
- Different malware types
- Common malware behavior
- Reversing tools & techniques

CompTIA Advanced Security Practitioner (CASP+)
- Security ops & architecture
- Engineering & cryptography
- Governance, risk & compliance

Apply your team's skills (Continuing Ed)

Computer Forensics Cyber Range
- Create & examine forensic images
- Perform memory forensics
- Use Volatility & Foremost

Cyber Threat Hunting Cyber Range
- Detect port scans
- Find threats in .pcap & .vmem files
- Hunt host-based & network-based threats

Other potential Digital Forensics Analyst training: Incident response, Network Traffic Analysis for Incident Response, CertNexus CyberSec First Responder and more.

Create your free Infosec Skills account to see all role-guided training

See All Training

Want to speak to someone? Book a meeting now.

Penetration Tester

What is a Penetration Tester?

Penetration Testers, or ethical hackers, are responsible for planning and performing authorized, simulated attacks within an organization's information systems, networks, applications and infrastructure to identify vulnerabilities and weaknesses. Findings are documented in reports to advise clients on how to lower or mitigate risk. Penetration Testers often specialize in a number of areas such as networks and infrastructures; Windows, Linux and Mac operating systems; embedded computer systems; web/mobile applications; supervisory control data acquisition (SCADA) control systems; cloud systems and internet of things (IoT) devices.

How this role helps my organization

Penetration Testers require a solid understanding of systems and infrastructure in order to properly uncover all the potential risks facing your organization. A number of tools are available to help automate pentesting tasks, but training programs need to go beyond basic scanning and teach advanced tactics, which is where many of the most important issues are often found. As Penetration Testers' skills grow, they can specialize in certain areas to fit your organization's needs, such as cloud or mobile pentesting.

What will my team learn?

The Penetration Tester Role in Infosec Skills aligns with 70 Knowledge Statements and 15 Skill Statements in the NICE Framework, which primarily roll up to the following competencies:

- Vulnerabilities assessment
- Computer network defense
- Infrastructure design
- Threat analysis
- Information systems/ network security
- Identity management
- Operating systems
- Network management
- Information assurance
- Encryption
- Data privacy and protection

Common tools and technology

- Wireshark
- Hashcat
- John the Ripper
- Hydra
- Aircrack-ng
- Xray
- SimplyEmail
- Zmap
- Powershell-suite
- Burp Suite
- Metasploit
- Nikto

Role at a glance

Core domains

- Exploitation analysis
- Vulnerability assessment and management

Related job titles

- Ethical hacker
- Assurance validator

Related NICE Work Roles

- Exploitation analyst
- Target network analyst
- Threat/warning analyst

View all Penetration Tester training

View Training

INFOSEC SKILLS SAMPLE TRAINING PLAN

Penetration Tester

Build your team's skills around uncovering vulnerabilities and other security weaknesses with the Penetration Tester Role training plan. Use the pre-built training below or customize the plan to meet your organization's goals.

Build your team's skills (Core)

EC-Council Certified Ethical Hacker
- Tools, systems & programs
- Procedures & methodology
- Hacking ethics

Web Application Pentesting
- OWASP Top Ten
- Tool setup & useage
- Pentesting dos & don'ts

Python for Pentesters
- Python basics
- Common vulnerabilities
- Network & web app attacks

Cloud Penetesting
- AWS pentesting
- Azure pentesting
- Tools & techniques

Specialize your team's skillsets (Elective)

Mobile Application Pentesting
- iOS pentesting
- Android pentesting
- Tools & techniques

Advanced Cybersecurity Concepts
- Reverse engineering
- Web app pentesting
- Privilege escalation

Offensive Bash Scripting
- Bash & Python basics
- Reconnaissance & scanning
- Privilege escalation

Certified Mobile & Web App Penetration Tester
- Pentesting methodoliges
- Pentesting tools
- Mobile & web app attacks

Machine Learning for Red Team Hackers
- Hack CAPTCHA systems
- Write evolutionary fuzzer
- Evade malware detection

Certified Expert Penetration Tester
- Create Windows exploits
- Create Linux exploits
- Advanced techniques

Apply your team's skills (Continuing Ed)

Purple Team Web App Cyber Range
- Remote code execution
- LFI vulnerabilitity
- Web app firewall

Common Attack Types Cyber Range
- Cross-site scripting
- Cross-site request forgery
- Injection attacks

Resource Development Cyber Range
- Build custom tools
- Malicious APK & Linux packages
- C&C, keyloggers & webshells

Other potential Penetration Tester training: CompTIA PenTest+, Cyber Threat Hunting, Reconnaissance Cyber Range and more.

Create your free Infosec Skills account to see all role-guided training

See All Training

Want to speak to someone? Book a meeting now.

ICS Security Practitioner

What is an ICS Security Practitioner?

Industrial Control System (ICS) Security Practitioners are responsible for securing mission-critical SCADA and ICS information systems. They are responsible for restricting digital and physical access to ICS devices, such as PLCs and RTUs, to maximize system uptime and availability. Extensive knowledge of OT and IT protocols, incident response, Linux and Windows OS, configuration management, air-gapped or closed networks, insider threats and physical security controls are important competencies for any ICS Security Practitioner.

How this role helps my organization

Solid networking skills are foundational to many ICS roles. ICS systems also tend to have significantly more restrictions around patching, so it's important for teams to have excellent planning skills and be proactive around security updates. An effective training plan should include a solid understanding of what's most important to your organization and guidance on how your systems, policies and procedures help balance those priorities against potential cyber risks.

What will my team learn?

The ICS Security Practitioner Role in Infosec Skills aligns with 23 Knowledge Statements and nine Skill Statements in the NICE Framework, which primarily roll up to the following competencies:

- Computer network defense
- Information systems/ network security
- Vulnerabilities assessment
- Infrastructure design
- System administration
- Information assurance
- Incident management
- Encryption

Common tools and technology

- Tripwire
- FireEye IOC Editor
- FireEye IOC Finder
- Symantec Anomaly Detection for ICS
- DarkTrace ICS
- AlienVault Unified Security Management SIEM
- McAfee
- Nessus
- Nextnine ICS Shield
- Snort
- Splunk
- Symantec Anomaly Detection for ICS

ICS SECURITY PRACTITIONER

Role at a glance

Core domains

- System administration
- Systems architecture

Related job titles

- Information security engineer
- Cybersecurity engineer
- Security systems engineer
- IT security engineer
- IS architect

Related NICE Work Roles

- Systems testing and evaluation specialist
- Technical support specialist
- Network operations specialist
- System administrator
- Cyber infrastructure support specialist
- Information systems security developer
- Security architect

View all ICS Security Practitioner training

View Training

INFOSEC SKILLS SAMPLE TRAINING PLAN

ICS Security Practitioner

Build your team's operational technology skills and keep your industrial control systems (ICS) secure with the ICS Security Practitioner Role training plan. Use the pre-built training below or customize the plan to meet your organization's goals.

Build your team's skills (Core)

ICS/SCADA Security Analyst
- SCADA security frameworks
- Assess ICS/SCADA risk
- SCADA security controls

Network Traffic Analysis for Incident Response
- Collect & analyze traffic data
- Case studies of extracting intel
- Build network monitoring program

Certified SCADA Security Architect (CSSA)
- SCADA security best practices
- Authentication & authorization
- Detecting cyber incidents

Identity & Access Management
- Design & implement IAM system
- IAM security considerations
- IAM federal standards

Specialize your team's skillsets (Elective)

Writing Secure Code in C++
- Common C/C++ vulnerabilities
- Safely use variables & strings
- Error handling

Cyber Threat Hunting
- Network traffic anomalies
- Identify & remediate malware
- Attack simulators

Apply your team's skills (Continuing Ed)

SCADA Cyber Range
- Reconnaissance & scanning
- Attacks & exploits
- CTF exercises

Cyber Threat Hunting Cyber Range
- Detect port scans
- Find threats in .pcap & .vmem files
- Hunt host-based & network-based threats

Other potential ICS Security Practitioner training: CompTIA Security+, Incident Response and more.

Create your free Infosec Skills account to see all role-guided training

See All Training

Want to speak to someone? Book a meeting now.

Security Engineer

What is a Security Engineer?

Security Engineers are responsible for implementing and continuously monitoring security controls that protect computer assets, networks and organizational data. They often design security architecture and develop technical solutions to mitigate and automate security-related tasks. Technical knowledge of network/web protocols, infrastructure, authentication, log management and multiple operating systems and databases is critical to success in this role.

How this role helps my organization

The day-to-day tasks of a Security Engineer vary depending on the organization, but strong technical skills and a solid understanding of system architecture will set employees on a path to success. Although it's usually not an entry-level role, you can build a solid pipeline of talent by identifying employees in more junior technical roles and creating training plans specific to your organization's cybersecurity engineering needs.

What will my team learn?

The Security Engineer Role in Infosec Skills aligns with 65 Knowledge Statements and 14 Skill Statements in the NICE Framework, which primarily roll up to the following competencies:

- System administration
- Infrastructure design
- Identity management
- Operating systems
- Information systems/ network security
- Enterprise architecture
- Data privacy and protection
- Information technology assessment
- Software development
- Risk management
- Information assurance
- Encryption
- Vulnerabilities assessment
- Systems integration
- Network management

Common tools and technology

- Wireshark
- Nmap
- Ncat (previously Netcat)
- Metasploit
- Nikto
- Burp Suite
- Kali Linux
- Web vulnerability scanning tools
- Network security monitoring tools
- Encryption tools
- Network defense wireless tools
- Packet sniffers

Role at a glance

Core domains

- System administration
- Systems architecture

Related job titles

- Information security engineer
- Cybersecurity engineer
- Security systems engineer
- IT security engineer
- IS architect

Related NICE Work Roles

- Systems testing and evaluation specialist
- Technical support specialist
- Network operations specialist
- System administrator
- Cyber infrastructure support specialist
- Information systems security developer
- Security architect

View all Security Engineer training

View Training

INFOSEC SKILLS SAMPLE TRAINING PLAN

Security Engineer

Build your team's technical skills and keep your organization's security controls running smoothly with the Security Engineer Role training plan. Use the pre-built training below or customize the plan to meet your organization's goals.

Build your team's skills (Core)

(ISC)² Certified Information Systems Security Professional (CISSP)

- Security operations
- Network, asset & software security
- Security assessment & testing

Security Engineering

- Implement security controls
- Manage processes & tools
- Vulnerability & risk management

Enterprise Security Risk Management

- Risk metrics & frameworks
- Security governance & policies
- Risk mitigation & response

Identity & Access Management

- Design & implement IAM system
- IAM security considerations
- IAM federal standards

Specialize your team's skillsets (Elective)

Advanced Intrusion Detection

- Linux architecture
- Linux jobs & processes
- Linux scripting & automation

Database Security

- Laws & regulations
- Data in use, in transit & at rest
- Standards & disaster recovery

Threat Modeling

- Defense-in-depth
- Conceptual frameworks
- Rapid Threat Model Prototyping

CompTIA Advanced Security Practitioner (CASP+)

- Security operations
- Security architecture
- Governance, risk & compliance

Windows Server Security

- Best practices
- Update services
- Backups & disaster recovery

DevSecOps

- Source control management
- Secure CI/CD pipeline
- Container security

Apply your team's skills (Continuing Ed)

Advanced Adversary Tactics Cyber Range

- MITRE ATT&CK® Matrix for Enterprise
- Tactics & techniques
- Offensive & defensive measure

Other potential Security Engineer training: CISSP-ISSEP, Identity and Access Management, Advanced Adversary Tactics, Web Application Security and more.

Create your free Infosec Skills account to see all role-guided training

See All Training

Want to speak to someone? Book a meeting now.

Cloud Security Engineer

What is a Cloud Security Engineer?

Cloud Security Engineers design, develop, manage and maintain a secure infrastructure leveraging cloud platform security technologies. They use technical guidance and engineering best practices to securely build and scale cloud-native applications and configure network security defenses within the cloud environment. These individuals are proficient in identity and access management (IAM), using cloud technology to provide data protection, container security, networking, system administration and zero-trust architecture.

How this role helps my organization

The duties of a Cloud Security Engineer will vary depending on where your organization is on its cloud journey. Organizations often employ junior, senior and lead Cloud Security Engineers, but even "junior" employees should have experience in multiple security domains. Identifying employees with a solid baseline of experience and creating a training plan to build their cloud skills will ensure a smooth transition — no matter what stage of your journey.

What will my team learn?

The Cloud Security Engineer Role in Infosec Skills aligns with 70 Knowledge Statements and 14 Skill Statements in the NICE Framework, which primarily roll up to the following competencies:

- System administration
- Infrastructure design
- Identity management
- Operating systems
- Information systems/ network security
- Enterprise architecture
- Data privacy and protection
- Information technology assessment
- Software development

Common tools and technology

- Amazon Cloudwatch
- Microsoft Cloud Monitoring
- AppDynamics
- BMC TrueSight Pulse
- DX Infrastructure Manager (IM)
- New Relic
- Hyperic
- Solarwinds
- CrowdStrike Falcon Horizon
- eSentire esCLOUD
- Jenkins
- Docker

Role at a glance

Core domains

- System administration
- Systems architecture

Related job titles

- Information security engineer
- Cybersecurity engineer
- Security systems engineer
- IT security engineer
- IS architect

Related NICE Work Roles

- Systems testing and evaluation specialist
- Technical support specialist
- Network operations specialist
- System administrator
- Cyber infrastructure support specialist
- Information systems security developer
- Security architect

View all Cloud Security Engineer training

View Training

INFOSEC SKILLS SAMPLE TRAINING PLAN

Cloud Security Engineer

Build your team's cloud security skills and ensure your organization's cloud infrastructure is secure with the Cloud Security Engineer Role training plan. Use the pre-built training below or customize the plan to meet your organization's goals.

Build your team's skills (Core)

(ISC)² Certified Cloud Security Professional (CCSP)

- Cloud architecture & design
- Data, platform & app security
- Legal, risk & compliance

Identity & Access Management

- Design & implement IAM system
- IAM security considerations
- IAM federal standards

Azure Security Engineer Associate

- Logging & monitoring
- Infrastructure security
- Data protection

AWS Certified Security Specialist

- Implement platform protection
- Manage security operations
- Secure data & apps

Specialize your team's skillsets (Elective)

Cloud Service Providers (CSP) Security Features

- CSP responsibilities
- Native security controls
- AWS, Azure & GCP

Container Security

- Container basics
- Docker security
- Kubernetes security

Microsoft Windows & Virtualization Fundamentals

- Command-line interface
- PowerShell
- VLANs & cloud computing

Apply your team's skills (Continuing Ed)

Offensive Bash Scripting Project

- Attack virtual machine
- SQL injection
- Python reverse shell

Container Security Project

- Review images
- Docker image best practices
- Scan for vulnerable software

Identity & Access Management Project

- Password policies
- Access control & authentication
- PKI systems

Other potential Cloud Security Engineer training: AWS Essentials and Solutions Architect Associate and more.

Create your free Infosec Skills account to see all role-guided training

See All Training

Want to speak to someone? Book a meeting now.

Security Architect

What is a Security Architect?

Security Architects are responsible for planning, designing, testing, implementing and maintaining an organization's computer and network security infrastructure. Security Architects develop information technology rules and requirements that describe baseline and target architectures and support enterprise mission needs. Advanced technical knowledge of network/web protocols, infrastructure, authentication, enterprise risk management, security engineering, communications and network security, identity and access management, and incident response is critical to success in this role.

How this role helps my organization

A Security Architect is usually a more senior role in an organization as they are tasked with implementing the infrastructure on which an organization's security is built. It requires a thorough understanding of security components, how to implement those components to meet your organization's needs and how risk is managed within your organization. An effective training plan should cover all three aspects.

What will my team learn?

The Security Architect Role in Infosec Skills aligns with 85 Knowledge Statements and 15 Skill Statements in the NICE Framework, which primarily roll up to the following competencies:

- Infrastructure design
- Information assurance
- Enterprise architecture
- Systems integration
- Encryption
- Information systems/ network security
- Vulnerabilities assessment
- Data privacy and protection
- Technology awareness
- System administration

Common tools and technology

- Wireshark
- Nmap
- Ncat (previously Netcat)
- Metasploit
- Nikto
- Burp Suite
- Kali Linux
- Security orchestration
- Automation, and response (SOAR) tools
- Security information and event management (SIEM) tools
- Web vulnerability scanning tools
- Network security monitoring tools

Role at a glance

Core domains

- System administration
- Systems architecture

Related job titles

- Enterprise architect
- Solutions architect
- Enterprise security architect
- Infrastructure architect
- Data architect
- Cloud solutions architect

Related NICE Work Roles

- Enterprise architect
- Solutions architect
- Enterprise security architect
- Infrastructure architect

View all Security Architect training

View Training

INFOSEC SKILLS SAMPLE TRAINING PLAN

Security Architect

Upskill your team to better design, implement and maintain secure infrastructure with the Security Architect Role training plan. Use the pre-built training below or customize the plan to meet your organization's goals.

Build your team's skills (Core)

(ISC)² Certified Information Systems Security Professional (CISSP)
- Security operations
- Network, asset & software security
- Security assessment & testing

Security Architecture
- Frameworks & processes
- Threat modeling
- Design for security

Enterprise Security Risk Management
- Risk metrics & frameworks
- Security governance & policies
- Risk mitigation & response

Cloud Security Architecture
- Design requirements
- Data, app & infrastructure security
- Legal & compliance

Specialize your team's skillsets (Elective)

NIST DoD RMF
- NIST RMF phases
- Security authorization processes
- Statutory & regulatory requirements

AWS Essentials & Solutions Architect Associate
- Resilient architectures
- High-performing architectures
- Secure apps & architectures

Certified SCADA Security Architect
- SCADA security best practices
- Authentication & authorization
- Detecting cyber incidents

SIEM Architecture & Process
- Bring structure to data
- Gain visibility into your environment
- Build content for threat detection

Web Server Protection
- Infrastructure concepts
- Design & installation
- Monitoring & active defense

Incident Response
- Incident response stages
- Incident response tool deep dive
- Memory, network & host forensics

Apply your team's skills (Continuing Ed)

SIEM Architecture & Process Project
- Dashboard visualization
- Enrich data
- Create alerts

Web Server Protection Project
- Implement network filtering
- Harden host OS
- Identify tampered files

Incident Response Project
- Wireshark, Zeek & Volatility
- Watering hole attack
- SQL injection attack

Other potential Security Architect training: Threat Modeling, Incident Response, CISSP-ISSAP and more.

Create your free Infosec Skills account to see all role-guided training

See All Training

Want to speak to someone? Book a meeting now.

Information Risk Analyst

What is an Information Risk Analyst?

Information Risk Analysts conduct objective, fact-based risk assessments on existing and new systems and technologies, and communicate findings to all stakeholders within the information system. They also identify opportunities to improve the risk posture of the organization and continuously monitor risk tolerance.

How this role helps my organization

Managing risk is crucial for every organization, and Information Risk Analysts must have the knowledge, skills and authority to match the high stakes. An effective training plan should build that expertise and align with how your organization measures risk. This role also requires solid communication skills so that leadership can make informed decisions on whether to accept the risk, avoid it, transfer it or mitigate it.

What will my team learn?

The Information Risk Analyst Role in Infosec Skills aligns with 76 Knowledge Statements and 14 Skill Statements in the NICE Framework, which primarily roll up to the following competencies:

- Vulnerabilities assessment
- Information assurance
- Information systems/ network security
- Infrastructure design
- Data privacy and protection
- Risk management
- Enterprise architecture
- Systems integration
- System administration
- Encryption
- Information technology assessment
- Systems testing and evaluation

Common tools, frameworks and documentation

- NIST Cybersecurity Framework
  - NIST SP 800-53
  - NIST SP 800-37
  - NIST SP 800-171
- Vulnerability scanning tools
- Log management tools
- Security technical implementation Guides (STIGs)
- Security content automation protocol (SCAP)
- Compliance checker (SCC)
- Knowledge of information assurance vulnerability alerts (IAVAs)

Role at a glance

Core domains

- Risk management
- Vulnerability assessment

Related job titles

- ISSO
- Cybersecurity auditor
- Cybersecurity assessor
- Security analyst
- Risk analyst
- Security controls assessor

Related NICE Work Roles

- Security controls assessor
- System security analyst

View all Information Risk Analyst training

View Training

INFOSEC SKILLS SAMPLE TRAINING PLAN

Information Risk Analyst

Upskill your team and gain a better understanding of how to assess and manage organizational risk with the Information Risk Analyst Role training plan. Use the pre-built training below or customize the plan to meet your organization's goals.

Build your team's skills (Core)

(ISC)² Certified Authorization Professional (CAP)
- Risk management program
- Security & privacy controls
- Continuous monitoring

Enterprise Security Risk Management
- Risk metrics & frameworks
- Security governance & policies
- Risk mitigation & response

ISACA CRISC
- Governance
- IT & security principles
- Risk assessment, response & reporting

Vulnerability Assessment
- Discover, classify & prioirtize
- Create remediation plan
- Document & maintain assessment

Specialize your team's skillsets (Elective)

NIST DoD RMF
- NIST RMF phases
- Security authorization processes
- Statutory & regulatory requirements

Implementing Controls for HIPAA Compliance
- HIPAA models & protocols
- HIPAA controls
- HIPAA security incidents

NIST Cybersecurity Framework
- Legal guidelines
- NIST CSF implementation
- CSF components & processes

Apply your team's skills (Continuing Ed)

Vulnerability Assessment Project
- JDK 11, Maven 3.6.3 & Git
- Identify & rate CWEs & CVEs
- Discover appropriate mitigations

Secure Coding Fundamentals Project
- Identify vulnerabilities in code
- How exploits work
- Injection, overflow & XSS attacks

NIST Cybersecurity Framework Project
- Perform a gap analysis
- FIPS 199 & NIST SP 800-60
- NIST SP 800-53 controls

Other potential Informatiion Risk Analyst training: ISACA CISA, CompTIA Cloud+, NIST 800-171 and more.

Create your free Infosec Skills account to see all role-guided training

See All Training

Want to speak to someone? Book a meeting now.

Security Manager

What is a Security Manager?

Security Managers develop security strategies that align with the organization's goals and objectives. In addition, they direct and monitor security policies, regulations and rules that the technical team implements. Knowledge in areas like information security governance, program development and management, incident response and risk management are important to success in any security management role.

How this role helps my organization

Security Managers often come from two primary backgrounds: technical cybersecurity roles or business and project management roles. No matter their background, Security Managers require solid relationship-building skills to make sure your organization's security is aligned with your business strategy. An effective training program should provide the frameworks, strategies and metrics needed to help them meet that objective.

What will my team learn?

The Security Manager Role in Infosec Skills aligns with 68 Knowledge Statements and three Skill Statements in the NICE Framework, which primarily roll up to the following competencies:

- Vulnerabilities assessment
- Systems integration
- Risk management
- Infrastructure design
- Information systems/ network security
- Data privacy and protection
- Project management
- Network management
- Legal, government and jurisprudence
- Information technology assessment
- Information assurance
- Incident management
- Contracting/procurement
- Business continuity

Common frameworks and documentation

- NIST Cybersecurity Framework
  - NIST 800-30
  - NIST 800-37
  - NIST 800-53
  - NIST 800-171
- ISO/IEC 27001
- CMMC (Federal)

Role at a glance

Core domains

- Cybersecurity management
- Leadership

Related job titles

- Chief information security officer (CISO)
- Chief security officer (CSO)
- Head of cybersecurity
- VP of cybersecurity
- Information security director
- Information technology manager

Related NICE Work Roles

- Information systems security manager
- Authorizing official
- Program manager
- Privacy officer/compliance manager
- IT project manager

View all Security Manager training

View Training

INFOSEC SKILLS SAMPLE TRAINING PLAN

Security Manager

Build your team's management skills and ensure your organization's security aligns with business objectives with the Security Manager Role training plan. Use the pre-built training below or customize the plan to meet your organization's goals.

Build your team's skills (Core)

(ISC)² Certified Information Systems Security Professional (CISSP)

- Security operations
- Network, asset & software security
- Security assessment & testing

Cybersecurity Administration

- Industry cybersecurity risks
- Measure & control risks
- Integrate technologies

Enterprise Security Risk Management

- Risk metrics & frameworks
- Security governance & policies
- Risk mitigation & response

Cybersecurity Management

- Security metrics & controls
- Incident response & recovery
- Security activities & architecture

Specialize your team's skillsets (Elective)

NIST DoD RMF

- NIST RMF phases
- Security authorization processes
- Statutory & regulatory requirements

Cybersecurity Leadership & Management

- Align security with strategy
- Align trust with regulations
- Align stability with operations

Information Privacy Essentials

- Global data protection laws
- U.S. laws & regulations
- Frameworks & standards

(ISC)² Certified Authorization Professional (CAP)

- Risk management program
- Security & privacy controls
- Continuous monitoring

Cloud Security Management

- Design requirements
- Platform, data & app security
- Legal & compliance

IAPP Certified Information Privacy Manager (CIPM)

- Company vision & team
- Implement privacy program
- Measure & communicate

Other potential Security Manager training: ISACA Certified Information Security Manager (CISM), ISACA Certified in Risk and Information Systems Control (CRISC), NIST Cybersecurity Framework and more.

Create your free Infosec Skills account to see all role-guided training

See All Training

Want to speak to someone? Book a meeting now.

Privacy Manager

What is a Privacy Manager?

A Privacy Manager is responsible for the development, creation, maintenance and enforcement of the privacy policies and procedures of an organization. They ensure compliance with all privacy-related laws and regulations. The Privacy Manager takes an active lead role when a privacy incident or data breach occurs and will start the investigation. They will then monitor, track and resolve any privacy issues. The Privacy Manager builds a strategic and comprehensive privacy program for their organization that minimizes risk and ensures the confidentiality of protected information.

How this role helps my organization

Privacy Managers come from a variety of backgrounds ranging from technical practitioners to legal experts to people managers. Regardless of their background, they require a training plan that builds their knowledge and skills around understanding legal requirements, translating external requirements into policies and procedures, and managing processes.

What will my team learn?

The Privacy Manager Role in Infosec Skills aligns with 15 Knowledge Statements and four Skill Statements in the NICE Framework, which primarily roll up to the following competencies:

- Legal, government and jurisprudence
- Vulnerabilities assessment
- Data privacy and protection
- Business continuity
- TPO (third party oversight)
- Threat analysis
- Telecommunications
- Risk management
- Requirements analysis
- Organizational awareness
- Onfrastructure design
- Information systems/ network security

Common frameworks and documentation

- NIST Privacy Framework
- Privacy impact assessments (PIA)
- Knowledge of data protection laws and regulations
  - GDPR
  - FERPA
  - The Privacy Act of 1974
- Incident response
- Risk Management Framework
  - NIST SP 800-53
  - NIST SP 800-37
  - NIST SP 800-60

Role at a glance

Core domains

- Oversee and govern
- Legal advice and advocacy

Related job titles

- Compliance officer
- Privacy officer
- Compliance manager
- Privacy leader
- Data protection officer

Related NICE Work Roles

- Privacy officer/privacy compliance manager

View all Privacy Manager training

View Training

INFOSEC SKILLS SAMPLE TRAINING PLAN

Privacy Manager

Build your team's privacy skills and learn to create a strategic and comprehensive privacy program with the Privacy Manager Role training plan. Use the pre-built training below or customize the plan to meet your organization's goals.

Build your team's skills (Core)

IAPP Certified Information Privacy Professional/U.S. (CIPP/US)

- Private-sector data use
- Government & court data access
- Federal, state & workplace laws

IAPP Certified Information Privacy Manager (CIPM)

- Company vision & team
- Implement privacy program
- Measure & communicate

NIST Cybersecurity Framework

- Legal guidelines
- NIST CSF implementation
- CSF components & processes

Information Privacy Essentials

- Global data protection laws
- U.S. laws & regulations
- Frameworks & standards

Specialize your team's skillsets (Elective)

Cybersecurity Audit Fundamentals

- Governance & due diligence
- Security operations components
- Digital assets & controls

Cybersecurity Management

- Security metrics & controls
- Incident response & recovery
- Security activities & architecture

Implementing Controls for HIPAA Compliance

- HIPAA models & protocols
- HIPAA controls
- HIPAA security incidents

(ISC)² Certified Information Systems Security Professional

- Security operations
- Network & asset security
- Security assessment & testing

Apply your team's skills (Continuing Ed)

SIEM Architecture & Process Project

- Perform a gap analysis
- FIPS 199 & NIST SP 800-60
- NIST SP 800-53 controls

Web Server Protection Project

- Wireshark, Zeek & Volatility
- Watering hole attack
- SQL injection attack

Incident Response Project

- Identify vulnerabilities in code
- How exploits work
- Injection, overflow & XSS attacks

Other potential Privacy Manager training: CIPP/Europe (CIPP/E), Certiifed Information Privacy Technologist (CIPT) and more.

Create your free Infosec Skills account to see all role-guided training

See All Training

Want to speak to someone? Book a meeting now.

Secure Coder

What is a Secure Coder?

Secure coders are responsible for developing and writing secure code in a way that protects against security vulnerabilities like bugs, defects and logic flaws. They take proactive steps to introduce secure coding methodologies before the application or software is introduced into a production environment, often following recommendations from the Open Web Application Security Project (OWASP) Foundation.

How this role helps my organization

If it's true that every company is a software company, then Secure Coders are the backbone that keeps your organization running securely. An effective training program should include both widely applicable secure coding methodologies as well as training related to specific coding languages within your organization.

What will my team learn?

The Secure Coder Role in Infosec Skills aligns with 44 Knowledge Statements and 14 Skill Statements in the NICE Framework, which primarily roll up to the following competencies:

- Software development
- Computer languages
- Vulnerabilities assessment
- Risk management
- Infrastructure design
- Systems testing and evaluation
- Information systems/ network security
- Information assurance
- Data privacy and protection
- Identity management

Common tools and technology

- VisualCodeGrepper
- Coverity
- Veracode
- Cppcheck
- Clang
- RIPS
- Flawfinder
- DevBug
- SonarQube
- PVS-Studio
- Kiuwan
- Kritika
- Gamma
- Code Compare
- Parasoft

Role at a glance

Core domains

- Software development
- Vulnerability assessment

Related job titles

- Security software developer
- Software testing engineer

Related NICE Work Roles

- Software developer
- Secure software assessor

View all Secure Coder training

View Training

INFOSEC SKILLS SAMPLE TRAINING PLAN

Secure Coder

Upskill your engineering team and ensure your software and applications are protected from vulnerabilities with the Secure Coder Role training plan. Use the pre-built training below or customize the plan to meet your organization's goals.

Build your team's skills (Core)

CertNexus Cyber Secure Coder
- Implement common protections
- Test software & fix defects
- Maintain deployed software

Secure SDLC
- Secure design, build & deployment
- Test & validate software
- Incidents during code lifecycle

Writing Secure Code in PHP
- PHP best practices
- Environment & cryptography principles
- Mitigate against common attacks

OWASP Top Ten
- Common web app risks
- Risk severity & ranking
- How to prevent risks

Specialize your team's skillsets (Elective)

DevSecOps
- Source control management
- Secure CI/CD pipeline
- Container security

Developing in Splunk
- Splunk basics
- Build Splunk apps
- Splunk REST API

Database Security
- Laws & regulations
- Data in use, in transit & at rest
- Standards & disaster recovery

Container Security
- Container basics
- Docker security
- Kubernetes security

Software Security Testing
- Methodology & processes
- Identify & exploit vulnerabilities
- Break security systems

Offensive Bash Scripting
- Bash & Python basics
- Reconnaissance & scanning
- Privilege escalation

Apply your team's skills (Continuing Ed)

Secure Coding Cyber Range
- Javascript
- Java
- C/C++, PHP & Python

Python Code Security Cyber Range
- Common issues
- Perform control flow analysis
- Recognize vulnerabilities

C++ Code Security Cyber Range
- Common issues
- Perform control flow analysis
- Recognize vulnerabilities

Other potential Secure Coder training: Writing Secure Code for Android, Writing Secure Code for iOS, HTML5 Security, PCI DSS for Developers and more.

Create your free Infosec Skills account to see all role-guided training

See All Training

Want to speak to someone? Book a meeting now.

Additional resources

Defeat cybercrime through education

- Upskill your IT, security and engineering teams
- Educate employees with security awareness
- Talk to someone about cybersecurity training

More free resources from Infosec

- 2021 IT and Security Talent Pipeline Study
- 2021 Cybersecurity Role and Career Path Clarity Study
- Developing Cybersecurity Talent and Teams Ebook
- Security Awareness, Behavior Change and Culture Ebook
- Cyber Work Podcast
- Infosec webcasts and events
- Infosec YouTube channel
- Infosec Resources blog

About Infosec

Infosec believes knowledge is power when fighting cybercrime. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and privacy training to stay cyber-safe at work and home. It's our mission to equip all organizations and individuals with the know-how and confidence to outsmart cybercrime.

Learn more at infosecinstitute.com

INFOSEC™