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.

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

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™