



# Startel

*Dé IT-opleider*

## Certified Cybersecurity Analyst (CCSA) E-Learning and Exam

This self-study package from Mile2 contains: Course video, e-book, e-prep Guide, E-lab Guide, Exam Simulator, 1 week Cyberrange, 1 Year Courseware Access and 1 Year Exam Voucher.

### Algemene omschrijving

This self-study package from Mile2 contains: Course video, e-book, e-prep Guide, E-lab Guide, Exam Simulator, 1 week Cyberrange, 1 Year Courseware Access and 1 Year Exam Voucher.

Companies and organizations today are scrambling to keep up with protection against the latest threats. This course is going to help a candidate prepare from the ground up.

Often, network architecture creates a fundamental issue when attempting to monitor. The CCSA course will analyze the entire architecture to better prepare for today's monitoring. Our Certified Cyber Security Analyst courseware helps the candidate prepare an organization to create a complete end to end solution for proactively monitoring, preventing, detecting, and mitigating current threats as they arise in real time. This course maps to the Mile2 Certified Cyber Security Analyst Exam as well as the [CompTIA CySA+CS0-001](#) certification exam.

Do not fool yourself, this course is far more advanced and will move at a fast pace for a well-rounded enjoyable experience. Be ready to dig deep into the details of security analysis for today's needs!

This course assumes that you have a fairly in-depth knowledge of security principles, forensics, incident handling and some ethical hacking skills. The candidate is not required to be an expert in these areas but 2 or more years of experience is recommended.

### Doelgroep

Security Professional, Incident Handling Professionals, anyone working in a Security Operations Center, Forensics Experts & anyone that needs a deep understanding of proactive security analysis on networks and systems.

### Leerdoelen

Upon completion, the **Certified Cyber Security Analyst** candidate will not only be able to competently take the **CCSA** exam, they will also be ready to prepare an organization for proactive

defense against today's hackers. The candidate will be able to setup and deploy state of the art open source and for purchase analysis tools, intrusion detection tools, syslog servers, SIEMs, along with integrating them for the entire company to find and in many cases prevent today's exploits.

## Voorkennis

[Certified Security Principles](#), [Certified Digital Forensics Examiner](#), [Certified Incident Handling Engineer](#), [Certified Professional Ethical Hacker](#)/[Certified Penetration Testing Engineer](#) or equivalent knowledge.

## Onderwerpen

- **Module 1** – Blue Team Principles.
- **Module 2** – Digital Forensics.
- **Module 3** – Malware Analysis.
- **Module 4** – Traffic Analysis.
- **Module 5** – Assessing the Current State of Defense with the Organization.
- **Module 6** – Leveraging SIEM for Advanced Analytics.
- **Module 7** – Defeating the Red Team with Purple Team Tactics.

Labs:

- **Lab 1** – Establishing Ips and Logging into the VMs.
- **Lab 2** – Blue Team Principles.
- **Lab 3** – Digital Forensics.
- **Lab 4** – Malware Analysis.
- **Lab 5** – Traffic Analysis.
- **Lab 6** – Assessing Current State of Defense within an Organization.
- **Lab 7** – Leveraging SIEM for Advanced Analytics.
- **Lab 8** – Defeating the Red Team with Purple Team Tactics.