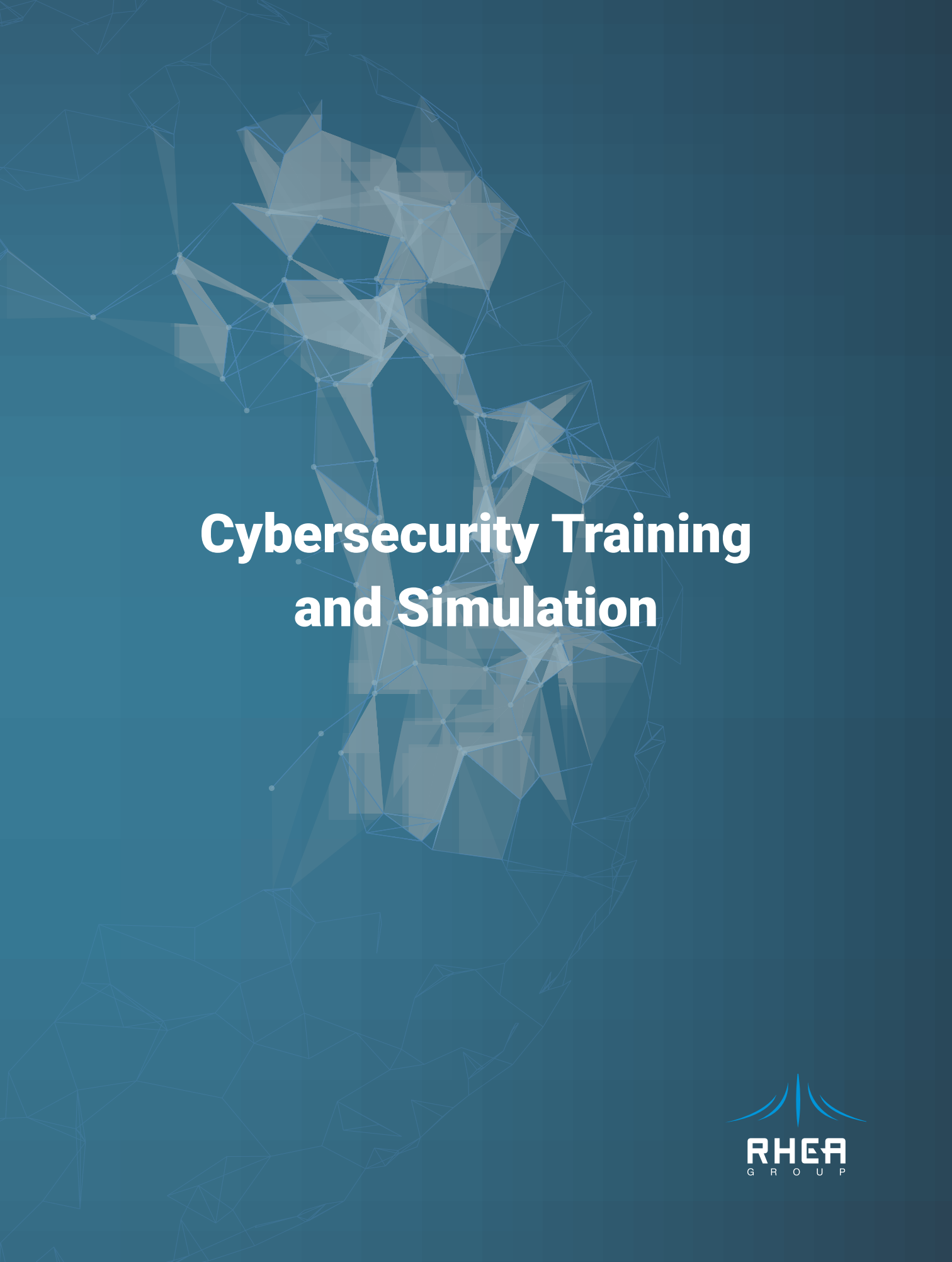


Cybersecurity Training and Simulation

RHEA GROUP

Engineering the world with you

RHEA Group is a world-leading engineering and security company delivering security solutions to large enterprises, governments and institutions in Europe and North America. RHEA Group's experts are certified security engineers offering a comprehensive security portfolio built on a 'security by design' approach.

With more than 25 years of experience in the market, RHEA Group is writing a new chapter in the security industry leveraging its space industry knowledge and capabilities by providing the European Space Agency (ESA) with the first cyber range for space assets.

The security services portfolio includes threats and risk assessments, vulnerability assessments, penetration testing, security by design analysis and support, network monitoring and scanning, cyber forensics, certification and accreditation, and staff training and augmentation.

Headquartered in Belgium, RHEA Group also operates in Canada, Czech Republic, Italy, France, Germany, Spain, Switzerland, The Netherlands, and the United Kingdom.

www.rheagroup.com

Prevention as a means to improve the world

With our security training, we'll tackle all the aspects needed to make your organisation as strong as you envisioned it. We'll equip you to optimize investment decisions and minimize the need for costly technologies.

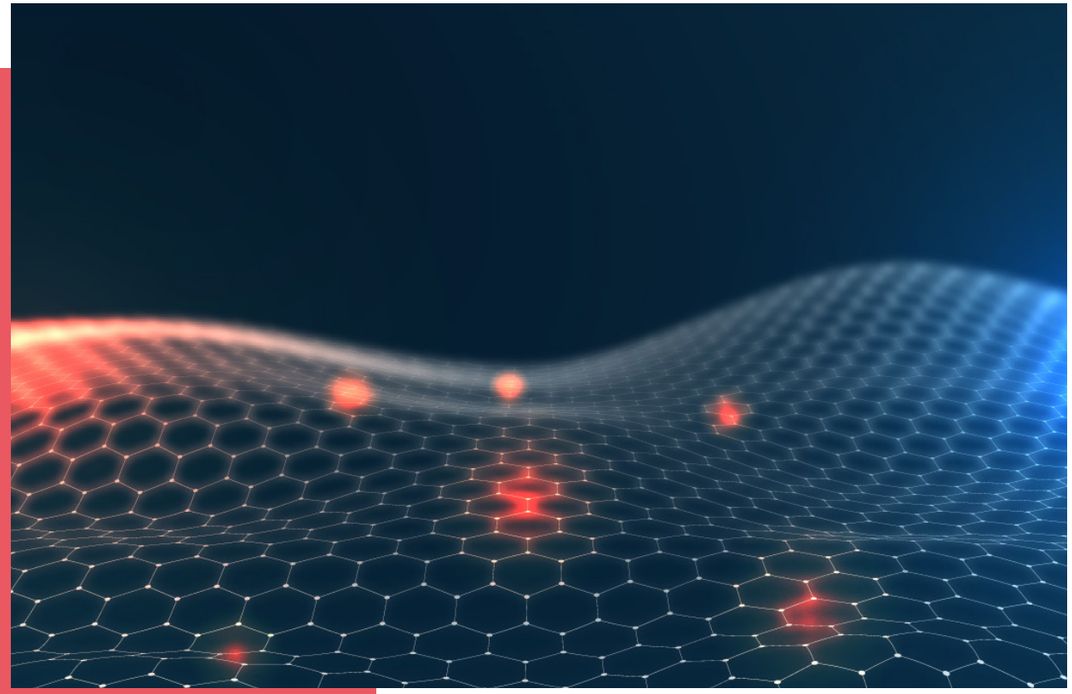
Enhanced security resiliance

Security threats are ever-present and always evolving. With the right training and technologies, you can detect cyber-attacks, minimize operational impacts and enhance your security posture.

The RHEA Group Cyber Security Centre of Excellence (CSCE) training program leverages a virtual simulation environment for hands-on training. Developed from RHEA Group's experience delivering the European Space Agency (ESA) Cyber Range, the simulations involve realistic security risks, equip technical and non-technical staff to recognize and respond to cybersecurity incidents, and ultimately raise awareness of the cybersecurity threats to organisational assets.

It's not just for space
The technologies and methodologies support a variety of industries by emulating their environment and providing realistic feedback about the threats, security requirements and actions needed to be prepared and to manage any threat situation successfully.

Security technologies are only as good as the people managing and operating them. Even the latest security solutions on the market cannot guarantee success in protecting your organisation's assets.



"Cybersecurity should not only be seen as a negative obstacle, but as an opportunity to promote a new generation of products and services that are made and/or delivered with security by design as a central component."

Udo Helmbrecht, Executive Director of the European Union Agency for Network and Information Security.

A comprehensive methodology for our security courses

All our cybersecurity courses were developed for an immersive cyber simulation experience. The CSCE CyFrame offers a responsive simulation platform that can be tailored to industry or organisation specific needs.

A methodology for success

Train with cyber-simulations based technology. Enjoy first-hand experience learning.

The CSCE CyFrame provides an advanced virtualization environment where relevant situations may be simulated to provide a realistic setup for hosting the cybersecurity training courses.

The CSCE CyFrame supports instantiation of all aspects of the organisation environment relevant to the cyber scenarios. In the specific case of ESA's security training program, the simulation is tailored to include a full mission environment including mission control system simulation; ground station and satellite simulators; data segments; and corporate and development networks.

Working on a simulated scenario allows flexible insertion of attack sequences that are being used throughout the training.
Our methodology is built on the principle of familiarizing students with incident detection and management tools along with forensics capabilities hosted in the virtual environment.

The curriculum is designed not only to present content that is relevant and specific to the cybersecurity needs of the organization, but also to provide practical experience in how to detect, respond and report when security is breached.

Be trained by the team of experts who developed and continue to deliver the curriculum for the ESA Cyber Range.

The security training offering

Particular needs, targeted solutions. If you can't find here what your organization needs, we can tailor the security training according to your specific requirements. Benefit from a training methodology and simulation technologies to enhance a hands-on training experience.

Hands-on Cyber Awareness

Get hands-on experience on how to handle cyber-risk with a real-life simulation environment.

Duration
16 hours over two days.

Cyber-First Responder

Gain the capability to identify potential cyber incidents and contribute to incident response.

Duration
24 hours over three days

Applied Incident Response and Forensics Investigation

Analyze incidents in-depth and propose measures to prevent similar events of occurring in the future.

Duration
40 hours over five days.

Cyber security for programs and projects

Master the risk management practices and security controls to be applied from the early stages of project delivery.

Duration
16 hours over two days.

Blue / Red team Cyber Exercise

Learn to defend your organization network from real-time attacks in the safety of a virtual environment.

Duration
40 hours over five days.

Enroll and read more about the courses

products.rheagroup.com/cybersecurity-training

Hands-on Cyber-risk Awareness Training (HoCAT)

Get hands-on experience on how to handle cyber-risk with a real-life simulation environment.

Participate in cyber-attacks simulations that facilitate hands-on activities and role-playing training exercises.

The course is a cyber-risk awareness course, applied as much as possible to your operational environment. It is intended for personnel at any level, from higher management to entry-level staff. The goal is to have a good mix of students working at different locations, within different departments, having different backgrounds, and from different levels of the decision making hierarchy. These different viewpoints and experiences will foster discussions about the role of the individual versus the role of the organization, current security practices and how they could be improved, the constraints different stakeholders have to deal with, and how these impact information security of your organization's operations.

Course content

HANDS-ON CYBER-RISK AWARNESS TRAINING

- Introduction to ISO/IEC 27001
- Security Threats, Vulnerabilities, and Controls
- Social engineering and personnel security
- Incident management
- Risk management
- Access controls
- Forensic investigation

What you will learn
Become an active contributor to protecting the security of your organization. Learn how to identify and deal with typical security threats with a hands-on approach to actively tackle these situations in an emulated environment. For each scenario a link will be made to the corresponding sections of the ISO/IEC 27001 standard, as well as your security regulations and directives.

Location
RHEA Group CSCE Security Training Facility located at the European space Security and Education Centre in Redu, Belgium.

Prerequisites
None.

Duration
16 hours over two days

Places available
20 people

More information
Learn more about course and how to enroll at products.rheagroup.com/cybersecurity-training

Cyber First Responder Training (CyFRT)

Gain the capability to identify potential cyber incidents and contribute to incident response.

Get hands-on experience with the latest methods currently available to detect and address cyber-attack incidents.

The course is intended for employees with a technical background, but who are not necessarily involved in systems management. In other words, this course is designed for technically oriented personnel from different disciplines. For example, members of technical development teams, software developers, system engineers, system administrators, system operators, and operations managers, among others.

Course content

CYBER FIRST RESPONDER TRAINING

- Advanced awareness principles (HoCAT review)
- Windows Forensics
- Linux Forensics
- Network Forensics
- USB infections
- Intrusion Detection
- Incident Response
- Acquisition, development and maintenance of information systems

What you will learn
Get the basic notions about incident management and forensics. Having this basis, you will gain an understanding of means and methods to detect and recognize events that may indicate a cyber-attack incident as early on as possible and understand appropriate reactions to a possible incident in such a manner to avoid destroying any evidence that might be relevant to future forensic analysis.

Location
RHEA Group CSCE Security Training Facility located at the European space Security and Education Centre in Redu, Belgium.

Prerequisites
The participants should have good knowledge of Windows system configuration, networking protocols and basic Linux commands.

Duration
24 hours over three days

Attendance limit
20 people

More information
Learn more about course and how to enroll at products.rheagroup.com/cybersecurity-training

Applied Incident Response Forensic Investigation Training (AIRFIT)

Analyze incidents in-depth and propose measures to prevent similar events of occurring in the future.

Advance your cyber incident response and forensic investigation skills.

The course is oriented to staff members working in systems support functions or supporting applications. These people may be called upon when there is a suspected incident and therefore need to have the necessary skills to be able to quickly identify a cyber-incident and react appropriately while correctly preparing for a forensic analysis.

Course content

APPLIED INCIDENT RESPONSE FORENSIC INVESTIGATION TRAINING

- Intrusion Detection and Incident Handling
- Advanced windows Forensics
- Advanced Linux Forensics
- Advanced Network Forensics
- Establishing incident timeline
- Third-party code management
- Acquisition, development and maintenance of information systems

What you will learn
Advance your understanding of concepts related to cyber incident management and forensics so you can contribute to a more in-depth analysis of a cyber-incident. This includes, for instance, the ability to assess damage, define indicators of compromise, or propose system / software measures to prevent similar events of occurring in the future.

Location
RHEA Group CSCE Security Training Facility located at the European space Security and Education Centre in Redu, Belgium.

Prerequisites
The participants should have good knowledge of Windows system configuration, networking protocols and basic Linux commands.

Duration
40 hours over 5 days

Places available
20 people

More information
Learn more about course and how to enroll at products.rheagroup.com/cybersecurity-training

Cyber security for programs and projects

Master the risk management practices and security controls to be applied from the early stages of project delivery.

Gain hands-on experience with risk assessment tools applied to relevant project development processes.

The course is intended for Program and Project planners. It focuses on the necessity for consideration of security requirements from the early stages of design. It will help you understand the need for integrated security controls targeting an appropriately secured and resilient outcome for a given cost. The students will have the opportunity to see the methodology and the advantages of a security-by-design approach utilizing efficient tools.

Course content

CYBER SECURITY FOR PROGRAMS AND PROJECTS TRAINING

- Introduction to ISO/IEC 27001 and ISO/IEC 27005
- Security Threats, Vulnerabilities, and Controls
- Security risk management processes
- Identification and selection of security controls
- Software assisted risk assessment procedures

What you will learn
Understand the benefits of a security-by-design approach from the early design phases. Learn risk management best-practices and how to select the appropriate security controls to mitigate the risks according to the needs of your specific programs or projects.

Location
RHEA Group CSCE Security Training Facility located at the European space Security and Education Centre in Redu, Belgium.

Prerequisites
The participants should have basic understanding of project management processes and project oriented risk assessment. Knowledge of project development and delivery lifecycle concept is also helpful.

Duration
16 hours over two days

Places available
20 people

More information
Learn more about course and how to enroll at products.rheagroup.com/cybersecurity-training

Blue / Red team cyber exercise

Learn to defend your organization from real-time attacks in the safety of a virtual environment.

Understand and improve your ability to respond during a cyber-attack in the safety of a simulated environment.

This course provides lifelike experience in incident response and forensics investigation. The real-time attacks in the advanced simulation environment of RHEA Group's cyber range will help prepare students for real-life events. The course is intended for technical personnel who would like to enhance their capabilities for incident handling by allowing them to practice their skills and organizational procedures during real-time events.

Course content

BLUE / RED TEAM CYBER EXERCISE

- Intrusion Detection review
- Incident response review
- Forensics investigation review
- Tools and environment introduction and familiarization
- 1-day dry-run exercise
- 2-days exercise participation

What you will learn
Defend your network under the stress of response timing. The attacks are executed in real-time and you need to act fast. Use tools and procedures introduced in the first days to achieve an effective defence to minimize the attack impact. The hands-on labs and the one-day dry-run of the scenario will help you prepare for the "big battle". Are you ready?

Location
RHEA Group CSCE Security Training Facility located at the European space Security and Education Centre in Redu, Belgium.

Prerequisites
The participants should have good knowledge of Intrusion Detection, Incident Response and Forensics concepts. Hands-on experience in Windows and Linux system at an intermediate level is also required.

Duration
40 hours over 5 days

Places available
8 people

More information
Learn more about course and how to enroll at products.rheagroup.com/cybersecurity-training

products.rheagroup.com/cybersecurity-training