

Cyber Training Academy Security Expert Course

While you can read a book or leverage a sea of information on the internet to increase your cyber security knowledge, it is not until you have experienced a cyber incident that the understanding becomes real. Today's state-of-the-art cyber training is about creating real-world scenarios and immersing both individuals and the team which would have to deal with them. For security experts, training needs to involve complex scenarios with hands-on resolution to make it worthwhile.

Business Challenges

Cyber-attacks are becoming increasingly sophisticated and often enter an organization with no signs of threat until it is too late. First-hand experience of dealing with an attack is not something which many individuals have, so being able to detect an attack and understand how it will impact an organization becomes a challenge. However, it is through hands-on experience when people learn the most. A poorly handled response to a cyber incident can result in damaged business reputation and while the leadership team handles the communication aspects of an attack, it is up to IT security experts to immediately manage the incident, reduce the impact and ultimately remove the risk.

Solution

RUAG Cyber Training Academy offers multiple specialist training courses aimed at upskilling IT security personnel to expert level. The training courses cover real-world scenarios applicable to all organizations (e.g. phishing, ransomware, trojans and advanced persistent threats) through to industry specific threats, including sophisticated SCADA based attacks. Simulations are used to provide a real-life experience of what can happen, what to look for, what actions to take, and importantly, how to mitigate an incident occurring again. Sessions are recorded so that they can be analyzed to optimize understanding, knowledge and ultimately skills.

Key Features and Benefits

- Expert Trainers deliver courses in state-of-the-art Training Centers using the latest in simulation technology
- Training locations: Bern - Switzerland, Berlin - Germany, or if requested, on-site
- SCADA and Internet based cyber-attack simulations
- Realistic worst-case scenarios based on real events
- Learn how to recognize approaching threats and how to mitigate them
- Understand immediate actions to take to minimize damage to the organization and its reputation
- Learn how to retain and interpret evidence for future use
- Recognize attack patterns to understand the attacker motivation
- Team response optimization
- Monitored and recorded sessions for analysis playback
- Full simulation provides insight on individuals and teams under pressure
- Focus on building individual and team skills
- Identify critical assets and understand the potential threats towards them
- Sector specific modules and scenarios
- Specialist knowledge improves risk posture for the whole organization

About RUAG

RUAG develops trailblazing innovations and internationally sought after cutting-edge technology in the fields of aerospace and defence. By combining outstanding technological expertise with a high degree of foresight and responsibility, it creates the foundations for security and progress within society.

For more information:

www.ruag.com

Other Relevant Services

- Incident Response and eForensics
- Cyber Academy Training
- IT Emergency Planning
- Security Health Check

Primary Offices

RUAG Cyber Security

RUAG Schweiz AG
Stauffacherstrasse 65
3000 Bern 22
Switzerland
T: +41 31 376 68 42

RUAG Cyber Security

Repräsentanz Berlin
Leipziger Platz 14
10117 Berlin
Germany
T: +49 3020 61 68810

RUAG Cyber Security (Clearswift)

1310 Waterside
Arlington Business Park
Theale
Reading
Berkshire RG7 4SA
United Kingdom
T: +44 118 903 8300

Email for more information:

info@ruagcybersecurity.com

Scenarios

There are currently 14 different scenarios which can be used for expert training delivered by our specialists, which include:

Phishing and Ransomware

Designing, building and executing a ransomware attack helps participants uncover vulnerabilities and weaknesses in their own organization. Working through the process from crafting a phishing email, identifying vulnerabilities, building an exploit and finally enacting it. While on the other side of the activity looking at how to detect phishing emails, ensuring that no known vulnerabilities can be exploited and deploying appropriate processes to deal with a successful attack.

SCADA Device

While Internet based attacks are frequent, those against SCADA (Supervisory Control and Data Acquisition, aka industrial control systems) are on the rise. The impact of hacking into industrial systems such as oil pipelines or wind turbines would be devastating. Understanding what it takes to shut off an attack while minimizing the potential disruption to devices or infrastructure is key. An attack / defense scenario gives team members the opportunity to pit their wits against each other, without putting anyone at real risk.

Trojan Based Privilege Escalation

Today malware can infect IT infrastructure and remain undetected for months or even years. These Advanced Persistent Threats (APTs) often begin with a Trojan which then moves through the environment to create an account with administrative privileges which in turn enables access to all the data held, such that it can be exfiltrated. Learning how the attack takes place enables the expert to detect and ultimately neutralize the threat in their own organization.

Pricing

Pricing depends on the level of customization and number of scenarios required. A standard expert training course lasting 1 day, costs 10'000 CHF (up to 5 people).

Why RUAG Cyber Security Services

RUAG Cyber Security Services have grown out of high profile engagements with the Swiss Government, operating in highly secure environments with specialist personnel. A consistent approach to projects of all sizes ensures a high-quality, on-time, on-budget deliverable which is tailored to the customer's specific needs.

Customers for Cyber Academy Courses include government departments, manufacturers, telecommunication providers, finance (Bank & Insurance), transportation, logistics, food manufacturers.



RUAG Cyber Security