YOUR FILES HAVE BEEN ENCRYPTED
What happened?
Your organization has been targeted by Cyber Liberation

CYBER RANGE

Fraunhofer
SIT

FRAUNHOFER INSTITUTE FOR
SECURE INFORMATION TECHNOLOGY

The contiuous progress of digitalization leads to a rising danger of cyber attacks. At the same time, attackers are increasingly automating and professionalizing their attacks on IT systems and infrastructures. Organisations particularly affected by the resulting threat landscape are

- Financial institutes and insurance companies
- Operators of critical infrastructures (hospitals, energy suppliers, media houses, etc.)
- Technology and innovation leaders in medtech, pharmaceuticals and engineering
- Public authorities and institutions
- IT companies and IT service providers
- Research organizations
- Suppliers and service companies working with the above mentioned

In order to meet the daily challenges, to distinguish false alarms from real attacks, and to quickly decide on adequate countermeasures security teams should prepare as best as they can. The Fraunhofer Cyber Range training can raise the level of experience of security staff and enhance advance its cyber expertise and further enhance their strategic competence.

Unique Training Opportunity

The Fraunhofer Cyber Range is the world's first defense training that combines the advantages of a hyper-realistic simulation platform with the latest findings from the world of applied science. Practical training in a deeply engineered virtual environment with insights into the latest developments in hacking and technology make a unique combination. It facilitates the rapid development of practical cyber security skills and provides knowledge and experience that is required to successfully face future threats.

Under Attack

Participants are placed in a complex network situation where they face real life attacks. They have to stop the killchain and minimize damages. Apache take down and website defacement are just the warm up for more advanced attack scenarios. After the attack the teams discuss their performance and identify possible improvements.The curriculum is complemented by case studies and technology talks, which provide valuable insights into relevant topics like malware analysis, hacking techniques but also security of Internet infrastructures.

Companies need to always win.

Attackers just once.

Practitioners, Hackers and Experts

Apart from the training team participants meet practitioners and security experts from one of Germany's leading research Institutes with special expertise in software analysis, mobile security, cryptography, IT Forensics and Insights from Security Operation Center and PKI Center for the Fraunhofer-Gesellschaft and its over 70 institutes. The Institute also runs different hacking teams that publish various vulnerabilities and advisories on a regular basis at the world's leading conferences like Black Hat or Defcon.

Who can train?

- Network administrators
- Cybersecurity analysts
- Cybersecurity defense specialists, authorities and public institutions
- SOC analysts
- Threat hunters
- CERT & NOC teams
- Intelligence analysts
- Forensic analysts
- Incident response consultants

For further information, dates and prices please check out our website under https://cyberrange.sit.fraunhofer.de

For customized trainings, scenario development and other topics for joint research and development please send an email to cyberrange@sit.fraunhofer.de.

Goethe-University Frankfurt

Fraunhofer Institute for Secure
Information Technology SIT

Contact:
Prof. Dr. Haya Shulman
Rheinstraße 75
64295 Darmstadt
Germany

cyberrange@sit.fraunhofer.de
www.cyberrange.sit.fraunhofer.de