



Improving Information Design Assurance Through Red Teaming

training course fact sheet

Methodology for analyzing system design and implementation from an adversarial point of view

Assessments and red teaming are among the most valuable tools for decision makers in understanding their security risks, vulnerabilities, and defensive posture. Sandia National Laboratories' IDART™ program has developed, and continues to refine, red teaming methodologies for the assessment of high consequence and complex information systems, including those supporting essential security functions, and control. U.S. Military and agencies of the Federal Government have improved their systems using our structured methodology to identify and mitigate vulnerabilities.

Course Objective

This training course is designed to help attendees improve the defensive posture of their information systems by assessing them from an adversarial perspective. The course provides detailed exposure to a red teaming assessment process and contains both lecture and practical application.

Who Should Attend*

Individuals attending this course will have a better understanding of how an *adversary* perceives and approaches attacks against an information system. The course is designed to help analysts apply a systematic approach when assessing information system security. Attendees should include those that will be assessing or red teaming information systems and those that sponsor, specify, manage, or interpret such assessments.



The IDART team generally provides this training at Sandia National Laboratories in Albuquerque, NM. Optionally, we can provide the training at the customer's site. Class size will be managed to ensure an appropriate student to teacher ratio.

This course is typically offered at Sandia's discretion, but may also be scheduled on an as-needed basis.

Course Sessions**

- Introduction to Red Teaming
- Process Overview
- Nightmare Consequences
- Data Collection
- System Characterization/Viewpoints
- Thinking Like a Bad Guy
- Analysis – Vulnerabilities, Exploits & Attacks
- Attack Planning and Metrics
- Improving Design
- Reporting Results
- Case Studies

*This class is provided to external groups at Sandia's sole discretion.

**Course length dependent on customer needs. Our courses may be customized to meet specific customer objectives.



Course Customization

Our courses can be customized to cover different types of IT systems, networks, and infrastructure and industrial control systems. Course content can also be designed to meet the needs of a diverse class composition.

In the last session, students will use the IDART™ Methodology to analyze case studies the sponsoring organization and students provide that are representative of what they will find in the field or in their operational contexts. If desired, we can build an example case study customized to the sponsor's needs.



Trainers and Technical Background

The course trainers are technical staff members of Sandia's Information Design Assurance Red Team (IDART™). IDART is a part of the Information Systems Analysis Center at Sandia National Laboratories.

Our cross cutting teams have a breadth of knowledge and experience in security assessment, system design, secure architectures and cryptography. We apply our unique experience and capabilities to improve the assurance of information and critical infrastructure systems for civilian government agencies, DoD, and industry.



IDART provides red team services for the evaluation of new and innovative information assurance and security technologies under development by the government, military, and commercial sectors.

We routinely assess systems used in oil/gas, power generation/transmission, water, finance, e-commerce, and global enterprise networks. Additionally, our unique capabilities are being applied to analyze and improve software development for our customers.

**For more information contact
Sandia National Laboratories
Raymond C. Parks**

P.O. Box 5800 MS 0671
Albuquerque, NM 87185-0671

Phone: (505) 844-4024

Email: rcparks@sandia.gov

<http://www.idart.sandia.gov/>

