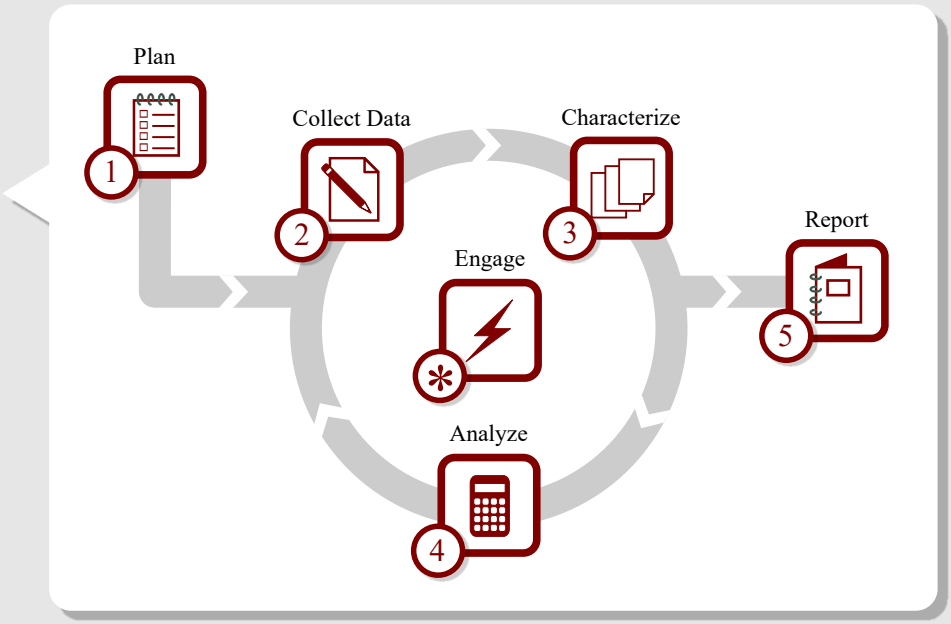
IDART Quick Reference Sheet

The IDART process is Sandia's core red teaming methodology. As such, it provides a framework for a variety of red teaming activities.

An analyst employing the IDART process does not follow a rigid checklist, but instead observes the process shown at right.

This process is as iterative as necessary. An analyst, for example, might find it useful to collect more data after characterizing the target system, or even revisit the project plan after conducting an engagement.

This quick reference sheet complements the RT4PM and RT Metrics quick reference sheets.



Most red team assessments involve engagements, but these are optional and depend upon the specifications of each assessment.

1 Plan

Objective: Confirm customer's security concerns and define the focus, scope, and scale of red teaming project.

Observations:

- The red team uses this phase to elicit customer requirements and expectations.
- These requirements and expectations inform the project plan, which specifies goals, logistics, and nature of the effort.

Pitfalls:

- Depending too heavily on colleagues who have done the customer discovery and relations for guidance in "what the customer wants."
- The red team develops the project plan in a vacuum.

Planning involves understanding what security concerns or questions the analysis is trying to solve, and how the customer will use the red team's deliverables.

Constraints

- Customer's budget and timeline
- Enterprise mission, culture, and policies
- Threat(s)/adversary description(s) the red team will model
- Customer's threat awareness
- Classification and clearances

The red team lead should also consider resources required to successfully execute the project.

Inputs

- Customer's perceived security concerns
- Outputs from RT4PM and RT Metrics considerations
- Initial funding profile
- Customer requirements, which may or may not be additional to perceived security concerns
- Customer negotiations
- Non-disclosure agreement (NDA)
- Statement of work (SOW)
- Project boundaries

Process

- Jointly identify customer's security concerns, aims, and expectations
- Determine type(s) of red teaming to perform
- Determine responsibilities of the red team and project logistics
- Develop project plan and other required documents

Identifying the customer's "nightmare consequences" is a key aspect of capturing the customer's security concerns. What keeps them up at night?

Outputs

- Detailed project plan, including agreements, resources, and capture plans
- Concise, balanced statement(s) defining customer's security concerns
- Rules of engagement (RoE), if required
- Specific threat model, derived from a sound generic threat model
- Identification of primary team members and subject matter experts (SMEs)

2 Collect Data

Objective: Collect data required to characterize the target system in the context of the customer's mission.

Observations:

- Data collection is used to derive adversary goals.
- The data collected serves as the basis for characterization, attack brainstorming, and target system analysis.
- Data collection is not limited to this phase and is likely required in other process phases.
- Collected data will influence and can, in some instances, alter the project plan.

Pitfalls:

- Inadequate access to target system data due to technical or administrative realities.
- Pushback from customer stakeholders that may view the red team as a threat.

Collect data as early as possible. Be considerate of the data providers, as this could become time-intensive. Data collection may be considered an engagement.

Constraints

- Budget and timeline
- Relative availability of information
- Agreements between customer and red team
- Target system fragility
- Level of cooperation between red and blue teams as dictated by project objectives

The aggregation of data performed in this phase often becomes the best available on the target system(s).

Inputs

- Project plan, including scope and scale of the effort
- Customer's security concerns
- Target system context(s)
- Interfaces between target system and external systems
- System documentation
- Open-source information
- Data from site visits

Process

- Identify likely data sources
- Elicit data from these sources
- Validate and deconflict data
- Review system documentation; ask for more as needed
- Conduct anonymous open-source intelligence (OSINT) searches
- Undertake external and internal data collection engagement(s)
- Conduct personnel interviews

Outputs

- System description(s) and mission(s)
- Concept of operations
- Additional "nightmare consequences"
- Raw data to be collated, analyzed, and catagorized into views

3 Characterize

Objective: Assemble collected data into views, which the red team can use to understand, analyze, and identify potential vulnerabilities in the target system.

Observations:

- The collection of views provides the basis for system analysis.
- Views validate the red team's understanding of the target system and help identify single points of failure, high-value nodes, and unexpected attack opportunities.
- Common views include system, functional, logical, temporal, lifecycle, and consequence.
- Input data is always incomplete; make and document assumptions based on expert opinion.

Pitfalls:

- Skipping this phase altogether.
- Failure to validate and deconflict data used to generate the views.
- Including too much information in a single view, rather than developing multiple simpler views.

Views often increase the customer's understanding of their system and its dependencies.

Constraints

- Budget and schedule
- Relative availability of information
- Agreements between customer and red team
- Level of cooperation between red and blue teams as dictated by the objectives

Critical success factors are closely related to dependencies and consequences, and are used to derive target opportunities.

Inputs

- Collected data
- Existing target system diagrams/schematics
- Consequences
- Target system dependencies and interdependencies
- Target system description, functions, and mission(s)
- Critical success factors

Do not consider customer knowledge as complete or accurate, as it is often biased.

Process

- Determine necessary views based on target system nature, red team requirements, and available data
- Distribute view creation tasks amongst red team members
- Choose existing view types, or develop new types as needed
- Choose an appropriate communications medium
- Characterize target system dependencies
- Identify target system's "critical success factors", or the actions, factors, and assumptions required for target system to fulfill its mission
- Validate views with customer
- Document assumptions made when generating views

Outputs

- One or more of system, physical/spatial, functional/logical, temporal, lifecycle, and consequence views
- Other views as indicated by target subject
- Single points of failure
- High-value nodes (from attacker's perspective)
- Assumptions and questions related to views constructed

4 Analyze

Objective: Analyze the target system using characterization views to identify, explore, and prioritize possible attacks.

Observations:

- The analysis process must be structured and should generate replicable results.
- The red team should consider customer "nightmare consequences" and target system vulnerabilities, attacks, and security performance.
- The red team should strive to think outside the box for potential vulnerabilities in unexpected places, such as dependencies and lifecycle opportunities.
- Look for resources or events the red team can leverage to increase efficiency or impact of attacks.
- Decompose adversary objectives into mission, attack, and exploitation goals.

Pitfalls:

- Failure to generate answers to address customer's security concerns.
- Attempting to perform analysis on raw data.
- Failing to bring in SMEs.
- Lack of creative thinking.
- Failure to identify simple and elegant attacks.

During this phase, the red team seeks to address the customer's security concerns with replicable results.

Constraints

- Available time and budget
- Adversary model and associated capabilities and characteristics
- Assessment rules of engagement, if applicable (for attack selection)
- Other constraints agreed upon by customer and red team

Consider target system performance before, during, and after an attack. Assess for mission continuity/recovery, attack detection and response, and extent of damage inflicted.

Inputs

- Characterization views
- SME inputs
- Customer's "nightmare consequences"
- RT Metrics considerations

Process

- Perform consequence analysis using adversary goals for guidance
- Assess target system's performance in face of attack
- Analyze target system for both weaknesses and strengths
- Brainstorm attacks
- Develop and apply a basic set of metrics by which all attacks are graded/ranked
- Apply necessary attack filters
- Identify enabling attack resources to support engagements, if applicable
- Validate attack steps for viability against target system design
- Review adversary metrics for reality in light of system design
- Save complete attack graph
- Apply adversary capability filter(s) to produce subsets of the complete attack graph(s)
- Apply RoE filter to attack graph; identify in-bounds and out-of-bounds attacks
- Identify and document critical attack steps and paths
- Present identified set of attacks to customer
- Assess identified attacks for mitigation options
- Develop attacks for engagements, as needed

Outputs

- Fully characterized and filtered set of attacks that meet attacker's goals
- Attack graph (preferred) or tree, textual descriptions, and/or attack flow charts, based on customer needs identified during planning
- Target system strengths and weaknesses
- Mitigation strategies for identified attacks of concern

5 Report

Objective: Report findings, observations, and recommendations clearly and intuitively.

Observations:

- The report should build a case for the assessment project.
- Reporting is made easier when documentation is generated in each phase of the process.

Pitfalls:

- Revealing sensitive data unnecessarily or inappropriately.
- Failing to record progress, findings, and observations as the project plays out.

The report provides the customer with a record of the analysis.

Constraints

- Available time and budget
- Customer's technical background and preferences
- Classification and clearance issues
- Customer-imposed dissemination restrictions

Avoid putting all information into the body of the report. Detailed material often fits best in appendices or separate supporting documents.

Inputs

- All materials generated during the IDART process, including chronologies and data logs

Process

- Collect materials generated throughout the project
- Determine type(s) of information the customer requires
- Write a report answering customer's security questions
- Develop other required deliverables negotiated during planning

Outputs

- Deliverables tailored to customer's needs that adequately documents results from the red team's analysis
- Lessons-learned to improve red team processes and capabilities

Engage

Objective: Perform target system testing activities that supply needed data, support or refute a hypothesis, demonstrate feasibility or consequences of an attack, verify one or more vulnerabilities, or test one or more mitigations.

Observations:

- Besides tests, demonstrations, exercises, and experiments, other kinds of live system engagements might be needed, such as for data collection.
- Data collection engagements require RoE, which must be ready by the end of Planning.
- Characterization engagements expand upon data collection.
- Analysis engagements include experiments, demonstrations, tests, and exercises.
- Experiments occur when the red team implements an attack plan to gather data to support or refute a hypothesis.
- Demonstrations occur when the red team implements an attack plan to show how an adversary might exploit a vulnerability.
- Tests and exercises occur when the red team implements an attack plan to verify existence of a vulnerability or mitigation.
- Engagements can yield unexpected outcomes.

Pitfalls:

- Damage or disruption to an out-of-bounds operational system, or worse, the customer's mission.
- Performing engagements of live systems without a full recovery plan.

"Murphy" frequently disrupts engagements. Strong planning will counter the potential for fatal disruptions and minimize foreseeable consequences.

Constraints

- Time and budget
- Location (travel)
- Adversary model
- Specific authorizations
- OPSEC and classification
- Risks associated with engaging an operational system

The red team must have authorization to perform live engagement activities, and it must perform them with the highest degree of professionalism and discretion.

Inputs

- Customer objectives: what the customer wants to learn/achieve
- Red team objectives: collect data, characterize the system, or test target system security performance
- Required resources from both the customer and red team

Process

- Clearly define purpose and goals of engagement
- Plan, develop, and, as necessary, test engagement activities in a representative, low-risk environment
- Develop comprehensive operation plan including RoE, attack descriptions, targets, points of contact, a full recovery plan, OPSEC, and legal authorizations
- Conduct customer in-brief
- Perform engagement and collect resulting data
- Conduct customer out-brief
- Restore target system back to its original state using the recovery plan, if necessary
- Perform lessons-learned review of engagement activities

Outputs

- Results to support customer and/or red team objectives
- Unexpected outcomes that may alter the project plan
- Lessons-learned to improve future engagements

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

IDART Information Design Assurance Red Team