ReSCIND Performer HSR Dataset
Cover Sheet

ReSCIND

Dataset Details

Dataset Title:	ReSCIND Phase 1 CTF		
Dataset Citation:	Sherouse, P. (2025). IARPA ReSCIND HSR #1 [Data set]. IARPA. https://ieee-dataport.org/open-access/rescind-testing-and-evaluation-ctf-1-cyber-dataset		
Data Format:	GZip files for each major data source	Data Size:	1.3 TB
Dates & Duration:	(see table below)	Time Zone:	Varies
How to access dataset:	ReSCIND Testing and Evaluation CTF 1 Cyber Dataset | IEEE DataPort		
Point of Contact for data questions:	Dr. Perry Sherouse perry.sherouse@iarpa.gov		

CTF Session Batch Number	Session Batch Dates	N
Session Batch 1.1	26 February – 2 March (2025)	1
Session Batch 1.2	3 March – 7 March (2025)	2
Session Batch 1.3	21 March – 23 March (2025)	14
Session Batch 1.4	11 April – 13 April (2025)	9
Total		26

Description of Scenario

Experiment Objectives

This experiment was designed to (1) examine relationships between psychometric data and cyber indicators of task performance (i.e., degree of task success); (2) explore if Performer findings generalize to findings from the CTF which represents a more ecologically valid cyber

environment; and (3) explore if relationships are consistent between selected Performer findings and CTF observed findings.

Experiment Description

The ReSCIND Phase 1 CTF challenges are designed to simulate real-world cyber-attack scenarios with multi-step attack paths against small network topologies.

The CTF contained four challenges, three of which were intended to elicit Cognitive Vulnerabilities (CogVulns) in participants: “Don’t Quote Me” for Loss Aversion Loss Framing, “Marked for Removal” for Loss Aversion Gain Framing, and “Fun House “for Base Rate Neglect. One additional challenge “Access Denied: Party Inside” was intended to serve as a baseline; it included deception technologies and was designed independently from the other three challenges.

Over a series of four scheduled CTF batches running from March through April 2025, T&E collected cyber log data from 26 participants.

Experimental Results

Quick-turn analysis results from this CTF data uncovered several relationships between psychometrics and susceptibility to Loss Aversion (Loss Framing), with the most striking correlation being the strong (and anticipated) link between the ADMC-SC and susceptibility to Loss Aversion (Loss Framing). Despite the overall participant sample demonstrating limited susceptibility to Loss Aversion (Loss Framing), the psychometric analysis revealed that susceptibility to the CogVuln might vary based on psychometric features.

Cyber Environment

The ReSCIND program hosted the Phase 1 CTF via a Cyber Virtual Assured Network (CyberVAN)[1] range, a virtualized, high-fidelity cyber experimentation platform licensed by Peraton Labs.

The CTF contained four challenges designed to simulate real-world cyber-attack scenarios with multi-step attack paths against small network topologies. For each challenge, participants began by reviewing the provided “cover story” on the CTF website; the cover story contained framing information for the challenge, as well as the login credential that they needed to access a designated red Kali Linux [1]

[1] https://www.peratonlabs.com/cybervan.html

workstation in the CyberVAN range specific to that challenge. From there, participants were expected to perform a series of attack techniques related to discovery, lateral movement, privilege escalation, etc. tactics to progress through the network topology to discover the flag.

Within the CyberVAN environment, participants could not access the internet, thus they were unable to install custom tools. The Kali VMs were equipped with the tools needed to complete each challenge. While there was an intended attack path for each challenge, participants had freedom and flexibility to make their own attack path choices, which fostered an ecologically valid experiment design. The participants were not presented with any information about the intended attack path—only framing information and high-level information about the objective. After accessing the Kali Linux workstation, participants were not given any direction on how to proceed with the challenge, allowing them to independently determine their strategy.

The network topologies, intended attack paths, and challenge framing information that were created during the CTF challenge design process are included in the released dataset.

Data

Data Sources

During the ReSCIND Phase 1 CTF, two types of data pertaining the challenges were collected: qualitative self-report data that provide insight into the participants' decision-making processes and cyber log data from which participant intention and attack behaviors could be inferred. Psychometric data was also collected to assess participant characteristics.

This dataset is complementary to the cyber log dataset collected by Lawrence Livermore National Laboratory (LLNL).

Primary Data Sources

Collected directly from the experiment environment.

Category	Data Source	Examples of Select Data Features
Self Report	Cyber Skill Knowledge Test	Six items of varying difficulty (easy, medium, hard), multiple choice response options (ROs)
Self Report	Cyber Expertise Items	3 items, multiple choice response options: Past participation in capture the flag or similar exercises; prior expertise with monitoring/detection software; prior expertise with penetration testing
Self Report	Welcome Questionnaire	Path choice preferences, administered pre-CTF challenges

Self Report	Post-challenge Questionnaires	Path choice preferences, administered post-CTF challenge
Self Report	Final Questionnaire	Post-challenge feedback. 1 item, free response
Flag Data	PysberQuest-flags-consolidated	All flags submitted to the PsyberQuest CTF website during the competition. Features include user ID, flag type, flag status, data, CTF session.
Network Data	PCAP	Raw pcap as collected from taps at various locations within each challenge environment
	IDS – Zeek [2]	Zeek logs associated with a default configuration, including connection, DNS, and HTTP logs, as well as others. Logs provided as both .log and timestamped-and-gzipped files. Available logs may include: stderr, stdout, stats,telemetry, workerstatus_workerstatus, capture_loss, conn, conn-summary, dns, weird, ssh, ldap_search, ldap, kerberos, dce_rpc, smb_mapping, notice, files, smb_files, analyzer, known_services, known_hosts, software, loaded_scripts, packet_filter, dpd, disable_syslog, ntlm, reporter, http, ssl, rdp, rfb, x509, ftp, irc, known_certs, snmp, mysql, sip, pe, websocket, dhcp, ntp
	IDS - Suricata [3]	Suricata alerts generated by the emerging.rules signature set [4]. Available logs may include: fast, suricata, stats, eve
Kali Host Data	Keylog	Text file containing all of the keypresses performed by the participant, in order, no timestamps. Each keylog file represents a single session, where the log starts when participant connects to the challenge environment and the log ends when they disconnect.
	Screen Recording	MP4 video recording of the participant's screen. Each recording file represents a single session, where the video starts when participant connects to the challenge environment and the log ends when they disconnect
	Terminal Histories	All commands, as entered into the kali terminal, by the participant. Terminal history logs are stored within the messages log and can be identified by the prefix 'MMM dd hh:mm:ss kali bash: HISTORY'
	Host Data	As listed below under the Linux Host Data category

Windows Host Data	Wintap [5	Parquet-formatted windows host logs generated by Wintap. Not all logs exist for all systems. Available logs may include: eventlogevent, file, focuschange, host, imageload, kernelapicall, macip, microsoftwindowsgrouppolicy, process, processstop, registry, sessionchange, tcp_process_conn_incr, udp_process_conn_incr, waitcursor, wmiactivity
Linux Host Data	Syslog	Logs generated by the host's system and services as sent by the system to a local syslog server. Not all logs exist for all systems. System logs may commonly include: messages, secure, maillog, spooler, boot, cron, kern

Derivative Data Sets

Datasets created from aggregating, analyzing, curating, and labeling the source data.

Category	Data Source	Examples of Select Data Features
Session Data	all_CTF_session_data	Interpreted Guacamole Session Data. Features include challenge count, challenge sequence, context switching.
Psychometric/Cyber	CTF_quickturn_cyber_combined	Aggregated psychometric and cyber data per participant for all CTF sessions. Features include user, DQM_Kelog_Lines, DQM_PATH_A_Nonbiased_Choices, DQM_PATH_B_Biased_Choice.
Cyber	CTF_1.<N>_Challenge_Data	Interpreted Cyber Log Data for CTFs 1.1, 1.2, 1.3, 1.4. These include a variety of checkpoint measurements for each of the three CogVuln-based challenges. Features include event message, attempted login, search string, Path_A_Dwatson_Logon, Path_B_Server_Access.

Research

Hypotheses

Quick-turn analysis results from this CTF data uncovered several relationships between psychometrics and susceptibility to Loss Aversion (Loss Framing), with the most striking correlation being the strong (and anticipated) link between the ADMC-SC and susceptibility to Loss Aversion (Loss Framing).

Despite the overall participant sample demonstrating limited susceptibility to Loss Aversion (Loss Framing), the psychometric analysis revealed that susceptibility to the CogVuln might vary based on psychometric features.

The main findings of the quick-turn analysis, intended to test top level CogVuln hypotheses per challenge, are summarized in figure below. While few hypotheses were supported or could be examined due to small sample sizes, there were several noteworthy relationships between psychometric variables and susceptibility to Loss Aversion (Loss Framing). Additionally, the qualitative data provided some valuable insights into the decision-making processes of participants.

Challenge	Hypothesis	Was the Hypothesis Supported?	If not, what did we find instead?
DQM (LA: Loss Frame)	Participants would choose the risky path	No	Participants chose the less risky path
	ADMC-RF (reverse scored) would correlate with choosing the risky path	No	ADMC-SC correlated with choosing the risky path, supporting secondary hypothesis
M4R (LA: Gain Frame)	Participants would choose the certain gain	Yes	---
	ADMC-RF (reverse scored) would correlate with choosing the certain gain	No*	Not enough cyber data to conclude*. We did not look at correlations between psychometric and self-reported data
Fun House (Base Rate Neglect)	Participants would fall foul to base rate neglect	No	Cyber norms may outweigh presented base rate framing
	CRT3-i would correlate with falling foul to BRN	No*	Not enough cyber data to conclude*. We did not look at correlations between psychometric and self-reported data

Figure 1: Summary of findings for top level CogVuln hypotheses

References

References

[1] g0tmi1k. “What Is Kali Linux?: Kali Linux Documentation.” Kali Linux, 18 June 2025, www.kali.org/docs/introduction/what-is-kali-linux/.

[2] The Zeek Project. “About Zeek.” About Zeek - Book of Zeek, 21 Aug. 2025, docs.zeek.org/en/master/about.html.

[3] OISF. “What Is Suricata.” What Is Suricata - Suricata 8.0.1-Dev Documentation, docs.suricata.io/en/latest/what-is-suricata.html. Accessed 21 Aug. 2025.

[4] Proofpoint. “Emergingthreats.” Proofpoint Emerging Threats Rules, rules.emergingthreats.net/open/suricata-5.0.0/emerging.rules.tar.gz.

[5] LLNL. “LLNL/Wintap: An Extensible Host-Based Agent for Windows.” Wintap Github Repository, github.com/LLNL/Wintap. Accessed 21 Aug. 2025.