CCI RESULTS - RANKED BY IMPORTANCE

	IMP	IMP	DIFF	DIFF	TIME	TIME
	μ	σ	μ	σ	μ	σ
Given a scenario, identify attacks against confidentiality, authentication, integrity, and availability.	8.7	1.3	7.5	1.3	8.9	1
Given a scenario or vulnerability, devise a defense.	8.6	1.1	7.5	0.7	8.2	0.8
Given a scenario, identify potential vulnerabilities and potential failures.	8.5	1.2	7.6	0.8	8.8	0.8
Given a scenario, identify potential targets and attackers.	8.2	1.6	5.2	0.9	8.5	1
Given a scenario, devise an attack.	8.1	1.1	7.8	0.7	7.8	0.7
Given a scenario, identify the security goals.	7.9	1.8	5.9	0.9	8.5	1.3
Given a scenario, identify risky behaviors.	7.5	1.4	6.4	1	7	1.1
Given a scenario, devise a social engineering attack.	7.5	1.2	5.6	1.4	7.5	0.9
Given a breach, explain how to recover from it.	7.5	0.9	7.6	0.6	7.9	0.9
Given a scenario, explain why a failure happened.	7.4	1.4	6.9	0.9	7.7	1
Given a scenario and change to it, identify new vulnerabilites caused by the change.	7.4	0.9	7.8	0.6	8	0.7
Given two security solutions, compare their pros and cons.	7.4	0.8	6.9	0.7	7.7	1
Given a scenario with faulty functionality or incorrect assumption, identify vulnerabilities caused by that faulty functionality or incorrect assumptio	7.2	0.7	7.4	0.5	7.5	0.5
Given a scenario, identify vulnerabilities based on usability issues.	7.2	1.7	6.6	1.3	7	0.7
Given a list of assumptions made by a system, identify which assumptions are most likely to be exploitable.	7.2	1.1	7.5	0.6	6.9	1.1
Given a scenario, assess the risk of acting and of not acting.	7.1	0.9	7.1	0.8	7.3	1
Given a scenario, rank a set of vulnerabilities.	7	0.9	7.5	0.8	7.1	0.9
Given a scenario, assess the difficulty of various attacks.	6.9	0.7	7.1	0.3	7.1	0.5
Given a description of a system, list assumptions the system makes implicitly.	6.9	2	7.6	0.7	8	0.9
Given a scenario, rank a set of possible corrective actions.	6.9	0.9	7	0.9	7.2	0.8
Given a protocol, identify a vulnerability.	6.8	1.8	8.5	1.1	7.6	0.6
Given a system, devise attacks that exploit the role of actors and information outiside of the system.	6.8	0.8	7.1	1	7.2	0.5
Given a scenario, devise a security plan.	6.6	1.2	6.9	1.3	8.1	1.1
Given a scenario, identify vulnerabilites based on gaps between theory and practice.	6.6	1.5	7.7	1.2	6.9	0.9
Given a scenario, identify where technological solutions can help versus policy solutions.	6.6	1.5	7	1.2	7.1	0.8
Given a scenario, assess the risks for two different types of users.	6.6	1	6.9	0.7	7	0.7
Given a scenario, identify and classify vulnerabilities by categories.	6.5	0.9	5.8	1	6.7	1.3
Given a policy, devise way to evade it.	6.4	1.8	6.8	1.3	6.8	1.4
Given a scenario, rank the relative risks of certain possible actions.	6.3	1.9	6.7	1.6	6.6	1.5
Given an example of software, explain how to exploit one of its vulnerabilities.	6.2	1.4	7.9	1.1	6.6	1.2
Given a scenario, identify ways to influence people.	6.1	0.9	5.4	1.2	6.7	1.1
Given an example of software, idenitify its vulnerabilities.	6.1	1.6	8	1.1	6.6	1.3
Given a network scenario, explain how to exploit traffic analysis.	5.8	0.9	6.7	1	6	0.9
Given a malware example, characterize its behavior.	5.7	1.1	8.1	0.9	5.9	1.3
Given a multi-party protocol, identify vulnerabilities based on people cheating.	5.6	1.2	8.4	0.9	6.8	1.4
Identify possible phishing emails from a set of samples.	5.6	2	4.4	1.6	4.8	1.6
Solve a puzzle requiring "out-of-the-box" thinking.	5.4	1.9	7.4	2	6.2	1.8
Given a scenario, devise an attack that analysts can't identify.	4.9	1.7	9.4	0.8	5.8	1

CCI RESULTS - RANKED BY DIFFICULTY

	IMP	IMP	DIFF	DIFF	TIME	TIME
	μ	σ	μ	σ	μ	σ
Given a scenario, devise an attack that analysts can't identify.	4.9	1.7	9.4	0.8	5.8	1
Given a protocol, identify a vulnerability.	6.8	1.8	8.5	1.1	7.6	0.6
Given a multi-party protocol, identify vulnerabilities based on people cheating.	5.6	1.2	8.4	0.9	6.8	1.4
Given a malware example, characterize its behavior.	5.7	1.1	8.1	0.9	5.9	1.3
Given an example of software, idenitify its vulnerabilities.	6.1	1.6	8	1.1	6.6	1.3
Given an example of software, explain how to exploit one of its vulnerabilities.	6.2	1.4	7.9	1.1	6.6	1.2
Given a scenario, devise an attack.	8.1	1.1	7.8	0.7	7.8	0.7
Given a scenario and change to it, identify new vulnerabilites caused by the change.	7.4	0.9	7.8	0.6	8	0.7
Given a scenario, identify vulnerabilites based on gaps between theory and practice.	6.6	1.5	7.7	1.2	6.9	0.9
Given a scenario, identify potential vulnerabilities and potential failures.	8.5	1.2	7.6	0.8	8.8	0.8
Given a breach, explain how to recover from it.	7.5	0.9	7.6	0.6	7.9	0.9
Given a description of a system, list assumptions the system makes implicitly.	6.9	2	7.6	0.7	8	0.9
Given a scenario, identify attacks against confidentiality, authentication, integrity, and availability.	8.7	1.3	7.5	1.3	8.9	1
Given a scenario or vulnerability, devise a defense.	8.6	1.1	7.5	0.7	8.2	0.8
Given a list of assumptions made by a system, identify which assumptions are most likely to be exploitable.	7.2	1.1	7.5	0.6	6.9	1.1
Given a scenario, rank a set of vulnerabilities.	7	0.9	7.5	0.8	7.1	0.9
Given a scenario with faulty functionality or incorrect assumption, identify vulnerabilities caused by that faulty functionality or incorrect assumptio	7.2	0.7	7.4	0.5	7.5	0.5
Solve a puzzle requiring "out-of-the-box" thinking.	5.4	1.9	7.4	2	6.2	1.8
Given a scenario, assess the risk of acting and of not acting.	7.1	0.9	7.1	0.8	7.3	1
Given a scenario, assess the difficulty of various attacks.	6.9	0.7	7.1	0.3	7.1	0.5
Given a system, devise attacks that exploit the role of actors and information outiside of the system.	6.8	0.8	7.1	1	7.2	0.5
Given a scenario, rank a set of possible corrective actions.	6.9	0.9	7	0.9	7.2	0.8
Given a scenario, identify where technological solutions can help versus policy solutions.	6.6	1.5	7	1.2	7.1	0.8
Given a scenario, explain why a failure happened.	7.4	1.4	6.9	0.9	7.7	1
Given two security solutions, compare their pros and cons.	7.4	0.8	6.9	0.7	7.7	1
Given a scenario, devise a security plan.	6.6	1.2	6.9	1.3	8.1	1.1
Given a scenario, assess the risks for two different types of users.	6.6	1	6.9	0.7	7	0.7
Given a policy, devise way to evade it.	6.4	1.8	6.8	1.3	6.8	1.4
Given a scenario, rank the relative risks of certain possible actions.	6.3	1.9	6.7	1.6	6.6	1.5
Given a network scenario, explain how to exploit traffic analysis.	5.8	0.9	6.7	1	6	0.9
Given a scenario, identify vulnerabilities based on usability issues.	7.2	1.7	6.6	1.3	7	0.7
Given a scenario, identify risky behaviors.	7.5	1.4	6.4	1	7	1.1
Given a scenario, identify the security goals.	7.9	1.8	5.9	0.9	8.5	1.3
Given a scenario, identify and classify vulnerabilities by categories.	6.5	0.9	5.8	1	6.7	1.3
Given a scenario, devise a social engineering attack.	7.5	1.2	5.6	1.4	7.5	0.9
Given a scenario, identify ways to influence people.	6.1	0.9	5.4	1.2	6.7	1.1
Given a scenario, identify potential targets and attackers.	8.2	1.6	5.2	0.9	8.5	1
Identify possible phishing emails from a set of samples.	5.6	2	4.4	1.6	4.8	1.6

CCI RESULTS - RANKED BY TIMELESSNESS

	IMP	IMP	DIFF	DIFF	TIME	TIME
	μ	σ	μ	σ	μ	σ
Given a scenario, identify attacks against confidentiality, authentication, integrity, and availability.	8.7	1.3	7.5	1.3	8.9	1
Given a scenario, identify potential vulnerabilities and potential failures.	8.5	1.2	7.6	0.8	8.8	0.8
Given a scenario, identify the security goals.	7.9	1.8	5.9	0.9	8.5	1.3
Given a scenario, identify potential targets and attackers.	8.2	1.6	5.2	0.9	8.5	1
Given a scenario or vulnerability, devise a defense.	8.6	1.1	7.5	0.7	8.2	0.8
Given a scenario, devise a security plan.	6.6	1.2	6.9	1.3	8.1	1.1
Given a scenario and change to it, identify new vulnerabilites caused by the change.	7.4	0.9	7.8	0.6	8	0.7
Given a description of a system, list assumptions the system makes implicitly.	6.9	2	7.6	0.7	8	0.9
Given a breach, explain how to recover from it.	7.5	0.9	7.6	0.6	7.9	0.9
Given a scenario, devise an attack.	8.1	1.1	7.8	0.7	7.8	0.7
Given a scenario, explain why a failure happened.	7.4	1.4	6.9	0.9	7.7	1
Given two security solutions, compare their pros and cons.	7.4	0.8	6.9	0.7	7.7	1
Given a protocol, identify a vulnerability.	6.8	1.8	8.5	1.1	7.6	0.6
Given a scenario with faulty functionality or incorrect assumption, identify vulnerabilities caused by that faulty functionality or incorrect assumptio	7.2	0.7	7.4	0.5	7.5	0.5
Given a scenario, devise a social engineering attack.	7.5	1.2	5.6	1.4	7.5	0.9
Given a scenario, assess the risk of acting and of not acting.	7.1	0.9	7.1	0.8	7.3	1
Given a system, devise attacks that exploit the role of actors and information outiside of the system.	6.8	0.8	7.1	1	7.2	0.5
Given a scenario, rank a set of possible corrective actions.	6.9	0.9	7	0.9	7.2	0.8
Given a scenario, rank a set of vulnerabilities.	7	0.9	7.5	0.8	7.1	0.9
Given a scenario, assess the difficulty of various attacks.	6.9	0.7	7.1	0.3	7.1	0.5
Given a scenario, identify where technological solutions can help versus policy solutions.	6.6	1.5	7	1.2	7.1	0.8
Given a scenario, assess the risks for two different types of users.	6.6	1	6.9	0.7	7	0.7
Given a scenario, identify vulnerabilities based on usability issues.	7.2	1.7	6.6	1.3	7	0.7
Given a scenario, identify risky behaviors.	7.5	1.4	6.4	1	7	1.1
Given a scenario, identify vulnerabilites based on gaps between theory and practice.	6.6	1.5	7.7	1.2	6.9	0.9
Given a list of assumptions made by a system, identify which assumptions are most likely to be exploitable.	7.2	1.1	7.5	0.6	6.9	1.1
Given a multi-party protocol, identify vulnerabilities based on people cheating.	5.6	1.2	8.4	0.9	6.8	1.4
Given a policy, devise way to evade it.	6.4	1.8	6.8	1.3	6.8	1.4
Given a scenario, identify and classify vulnerabilities by categories.	6.5	0.9	5.8	1	6.7	1.3
Given a scenario, identify ways to influence people.	6.1	0.9	5.4	1.2	6.7	1.1
Given an example of software, idenitify its vulnerabilities.	6.1	1.6	8	1.1	6.6	1.3
Given an example of software, explain how to exploit one of its vulnerabilities.	6.2	1.4	7.9	1.1	6.6	1.2
Given a scenario, rank the relative risks of certain possible actions.	6.3	1.9	6.7	1.6	6.6	1.5
Solve a puzzle requiring "out-of-the-box" thinking.	5.4	1.9	7.4	2	6.2	1.8
Given a network scenario, explain how to exploit traffic analysis.	5.8	0.9	6.7	1	6	0.9
Given a malware example, characterize its behavior.	5.7	1.1	8.1	0.9	5.9	1.3
Given a scenario, devise an attack that analysts can't identify.	4.9	1.7	9.4	0.8	5.8	1
Identify possible phishing emails from a set of samples.	5.6	2	4.4	1.6	4.8	1.6