

EC-Council

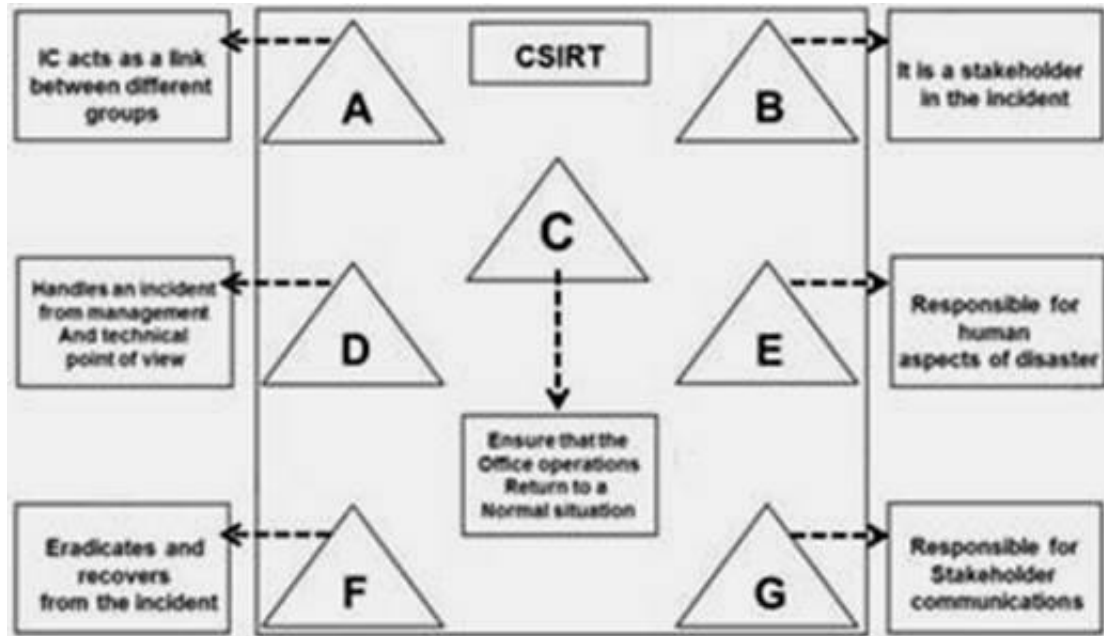
Exam Questions 212-89

EC Council Certified Incident Handler (ECIH v2)



NEW QUESTION 1

The flow chart gives a view of different roles played by the different personnel of CSIRT. Identify the incident response personnel denoted by A, B, C, D, E, F and G.



- A. A-Incident Analyst, B- Incident Coordinator, C- Public Relations, D-Administrator, E- Human Resource, FConstituency, G-Incident Manager
 B. A- Incident Coordinator, B-Incident Analyst, C- Public Relations, D-Administrator, E- Human Resource, FConstituency, G-Incident Manager
 C. A- Incident Coordinator, B- Constituency, C-Administrator, D-Incident Manager, E- Human Resource, FIncident Analyst, G-Public relations
 D. A- Incident Manager, B-Incident Analyst, C- Public Relations, D-Administrator, E- Human Resource, FConstituency, G-Incident Coordinator

Answer: C

NEW QUESTION 2

Quantitative risk is the numerical determination of the probability of an adverse event and the extent of the losses due to the event. Quantitative risk is calculated as:

- A. (Probability of Loss) X (Loss)
 B. (Loss) / (Probability of Loss)
 C. (Probability of Loss) / (Loss)
 D. Significant Risks X Probability of Loss X Loss

Answer: A

NEW QUESTION 3

Risk is defined as the probability of the occurrence of an incident. Risk formulation generally begins with the likeliness of an event's occurrence, the harm it may cause and is usually denoted as Risk = ?(events)X (Probability of occurrence)X?

- A. Magnitude
 B. Probability
 C. Consequences
 D. Significance

Answer: A

NEW QUESTION 4

An audit trail policy collects all audit trails such as series of records of computer events, about an operating system, application or user activities. Which of the following statements is NOT true for an audit trail policy:

- A. It helps calculating intangible losses to the organization due to incident
 B. It helps tracking individual actions and allows users to be personally accountable for their actions
 C. It helps in compliance to various regulatory laws, rules,and guidelines
 D. It helps in reconstructing the events after a problem has occurred

Answer: A

NEW QUESTION 5

Multiple component incidents consist of a combination of two or more attacks in a system. Which of the following is not a multiple component incident?

- A. An insider intentionally deleting files from a workstation
 B. An attacker redirecting user to a malicious website and infects his system with Trojan
 C. An attacker infecting a machine to launch a DDoS attack
 D. An attacker using email with malicious code to infect internal workstation

Answer: A

NEW QUESTION 6

The network perimeter should be configured in such a way that it denies all incoming and outgoing traffic/ services that are not required. Which service listed

below, if blocked, can help in preventing Denial of Service attack?

- A. SAM service
- B. POP3 service
- C. SMTP service
- D. Echo service

Answer: D

NEW QUESTION 7

A US Federal agency network was the target of a DoS attack that prevented and impaired the normal authorized functionality of the networks. According to agency's reporting timeframe guidelines, this incident should be reported within two (2) HOURS of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate the activity. Which incident category of the US Federal Agency does this incident belong to?

- A. CAT 5
- B. CAT 1
- C. CAT 2
- D. CAT 6

Answer: C

NEW QUESTION 8

Identify a standard national process which establishes a set of activities, general tasks and a management structure to certify and accredit systems that will maintain the information assurance (IA) and security posture of a system or site.

- A. NIASAP
- B. NIAAAP
- C. NIPACP
- D. NIACAP

Answer: D

NEW QUESTION 9

A threat source does not present a risk if NO vulnerability that can be exercised for a particular threat source. Identify the step in which different threat sources are defined:



- A. Identification Vulnerabilities
- B. Control analysis
- C. Threat identification
- D. System characterization

Answer: C

NEW QUESTION 10

Which of the following incident recovery testing methods works by creating a mock disaster, like fire to identify the reaction of the procedures that are implemented to handle such situations?

- A. Scenario testing
- B. Facility testing
- C. Live walk-through testing
- D. Procedure testing

Answer: D

NEW QUESTION 10

An incident is analyzed for its nature, intensity and its effects on the network and systems. Which stage of the incident response and handling process involves auditing the system and network log files?

- A. Incident recording
- B. Reporting
- C. Containment
- D. Identification

Answer: D

NEW QUESTION 14

Which among the following CERTs is an Internet provider to higher education institutions and various other research institutions in the Netherlands and deals with all cases related to computer security incidents in which a customer is involved either as a victim or as a suspect?

- A. NET-CERT
- B. DFN-CERT
- C. Funet CERT
- D. SURFnet-CERT

Answer: D

NEW QUESTION 19

One of the main objectives of incident management is to prevent incidents and attacks by tightening the physical security of the system or infrastructure. According to CERT's incident management process, which stage focuses on implementing infrastructure improvements resulting from postmortem reviews or other process improvement mechanisms?

- A. Protection
- B. Preparation
- C. Detection
- D. Triage

Answer: A

NEW QUESTION 22

The insider risk matrix consists of technical literacy and business process knowledge vectors. Considering the matrix, one can conclude that:

- A. If the insider's technical literacy is low and process knowledge is high, the risk posed by the threat will be insignificant.
- B. If the insider's technical literacy and process knowledge are high, the risk posed by the threat will be insignificant.
- C. If the insider's technical literacy is high and process knowledge is low, the risk posed by the threat will be high.
- D. If the insider's technical literacy and process knowledge are high, the risk posed by the threat will be high.

Answer: D

NEW QUESTION 27

Which policy recommends controls for securing and tracking organizational resources:

- A. Access control policy
- B. Administrative security policy
- C. Acceptable use policy
- D. Asset control policy

Answer: D

NEW QUESTION 32

Which one of the following is the correct sequence of flow of the stages in an incident response:

- A. Containment - Identification - Preparation - Recovery - Follow-up - Eradication
- B. Preparation - Identification - Containment - Eradication - Recovery - Follow-up
- C. Eradication - Containment - Identification - Preparation - Recovery - Follow-up
- D. Identification - Preparation - Containment - Recovery - Follow-up - Eradication

Answer: B

NEW QUESTION 36

Organizations or incident response teams need to protect the evidence for any future legal actions that may be taken against perpetrators that intentionally attacked the computer system. EVIDENCE PROTECTION is also required to meet legal compliance issues. Which of the following documents helps in protecting evidence from physical or logical damage:

- A. Network and host log records
- B. Chain-of-Custody
- C. Forensic analysis report
- D. Chain-of-Precedence

Answer: B

NEW QUESTION 40

Except for some common roles, the roles in an IRT are distinct for every organization. Which among the following is the role played by the Incident Coordinator of an IRT?

- A. Links the appropriate technology to the incident to ensure that the foundation's offices are returned to normal operations as quickly as possible
- B. Links the groups that are affected by the incidents, such as legal, human resources, different business areas and management
- C. Applies the appropriate technology and tries to eradicate and recover from the incident
- D. Focuses on the incident and handles it from management and technical point of view

Answer: B

NEW QUESTION 42

In a qualitative risk analysis, risk is calculated in terms of:

- A. (Attack Success + Criticality) –(Countermeasures)
- B. Asset criticality assessment – (Risks and Associated Risk Levels)
- C. Probability of Loss X Loss
- D. (Countermeasures + Magnitude of Impact) – (Reports from prior risk assessments)

Answer: C

NEW QUESTION 46

A computer virus hoax is a message warning the recipient of non-existent computer virus. The message is usually a chain e-mail that tells the recipient to forward it to every one they know. Which of the following is NOT a symptom of virus hoax message?

- A. The message prompts the end user to forward it to his / her e-mail contact list and gain monetary benefits in doing so
- B. The message from a known email id is caught by SPAM filters due to change of filter settings
- C. The message warns to delete certain files if the user does not take appropriate action
- D. The message prompts the user to install Anti-Virus

Answer: A

NEW QUESTION 47

In which of the steps of NIST's risk assessment methodology are the boundary of the IT system, along with the resources and the information that constitute the system identified?

- A. Likelihood Determination
- B. Control recommendation
- C. System characterization
- D. Control analysis

Answer: C

NEW QUESTION 50

Incident handling and response steps help you to detect, identify, respond and manage an incident. Which of the following helps in recognizing and separating the infected hosts from the information system?

- A. Configuring firewall to default settings
- B. Inspecting the process running on the system
- C. Browsing particular government websites
- D. Sending mails to only group of friends

Answer: B

NEW QUESTION 54

The type of relationship between CSIRT and its constituency have an impact on the services provided by the CSIRT. Identify the level of the authority that enables members of CSIRT to undertake any necessary actions on behalf of their constituency?

- A. Full-level authority
- B. Mid-level authority
- C. Half-level authority
- D. Shared-level authority

Answer: A

NEW QUESTION 59

Which of the following incidents are reported under CAT -5 federal agency category?

- A. Exercise/ Network Defense Testing
- B. Malicious code
- C. Scans/ probes/ Attempted Access
- D. Denial of Service DoS

Answer: C

NEW QUESTION 63

Incident management team provides support to all users in the organization that are affected by the threat or attack. The organization's internal auditor is part of the incident response team. Identify one of the responsibilities of the internal auditor as part of the incident response team:

- A. Configure information security controls
- B. Perform necessary action to block the network traffic from suspected intruder
- C. Identify and report security loopholes to the management for necessary actions
- D. Coordinate incident containment activities with the information security officer

Answer: C

NEW QUESTION 67

An assault on system security that is derived from an intelligent threat is called:

- A. Threat Agent
- B. Vulnerability
- C. Attack
- D. Risk

Answer: C

NEW QUESTION 71

Incidents such as DDoS that should be handled immediately may be considered as:

- A. Level One incident
- B. Level Two incident
- C. Level Three incident
- D. Level Four incident

Answer: C

NEW QUESTION 75

If the loss anticipated is greater than the agreed upon threshold; the organization will:

- A. Accept the risk
- B. Mitigate the risk
- C. Accept the risk but after management approval
- D. Do nothing

Answer: B

NEW QUESTION 80

A payroll system has a vulnerability that cannot be exploited by current technology. Which of the following is correct about this scenario:

- A. The risk must be urgently mitigated
- B. The risk must be transferred immediately
- C. The risk is not present at this time
- D. The risk is accepted

Answer: C

NEW QUESTION 83

Overall Likelihood rating of a Threat to Exploit a Vulnerability is driven by :

- A. Threat-source motivation and capability
- B. Nature of the vulnerability
- C. Existence and effectiveness of the current controls
- D. All the above

Answer: D

NEW QUESTION 87

What is correct about Quantitative Risk Analysis:

- A. It is Subjective but faster than Qualitative Risk Analysis
- B. Easily automated
- C. Better than Qualitative Risk Analysis
- D. Uses levels and descriptive expressions

Answer: B

NEW QUESTION 89

Which of the following is a risk assessment tool:

- A. Nessus
- B. Wireshark
- C. CRAMM
- D. Nmap

Answer: C

NEW QUESTION 94

Performing Vulnerability Assessment is an example of a:

- A. Incident Response
- B. Incident Handling
- C. Pre-Incident Preparation
- D. Post Incident Management

Answer: C

NEW QUESTION 98

What is the best staffing model for an incident response team if current employees' expertise is very low?

- A. Fully outsourced
- B. Partially outsourced
- C. Fully insourced
- D. All the above

Answer: A

NEW QUESTION 99

Incident response team must adhere to the following:

- A. Stay calm and document everything
- B. Assess the situation
- C. Notify appropriate personnel
- D. All the above

Answer: D

NEW QUESTION 102

Removing or eliminating the root cause of the incident is called:

- A. Incident Eradication
- B. Incident Protection
- C. Incident Containment
- D. Incident Classification

Answer: A

NEW QUESTION 105

Which of the following is a correct statement about incident management, handling and response:

- A. Incident response is on the functions provided by incident handling
- B. Incident handling is on the functions provided by incident response
- C. Triage is one of the services provided by incident response
- D. Incident response is one of the services provided by triage

Answer: A

NEW QUESTION 110

Incident Response Plan requires

- A. Financial and Management support
- B. Expert team composition
- C. Resources
- D. All the above

Answer: D

NEW QUESTION 112

The service organization that provides 24x7 computer security incident response services to any user, company, government agency, or organization is known as:

- A. Computer Security Incident Response Team CSIRT
- B. Security Operations Center SOC
- C. Digital Forensics Examiner
- D. Vulnerability Assessor

Answer: A

NEW QUESTION 113

The role that applies appropriate technology and tries to eradicate and recover from the incident is known as:

- A. Incident Manager
- B. Incident Analyst
- C. Incident Handler
- D. Incident coordinator

Answer: B

NEW QUESTION 116

CERT members can provide critical support services to first responders such as:

- A. Immediate assistance to victims
- B. Consolidated automated service process management platform
- C. Organizing spontaneous volunteers at a disaster site
- D. A + C

Answer: D

NEW QUESTION 120

CSIRT can be implemented at:

- A. Internal enterprise level
- B. National, government and military level
- C. Vendor level
- D. All the above

Answer: D

NEW QUESTION 123

The typical correct sequence of activities used by CSIRT when handling a case is:

- A. Log, inform, maintain contacts, release information, follow up and reporting
- B. Log, inform, release information, maintain contacts, follow up and reporting
- C. Log, maintain contacts, inform, release information, follow up and reporting
- D. Log, maintain contacts, release information, inform, follow up and reporting

Answer: A

NEW QUESTION 124

Common name(s) for CSIRT is(are)

- A. Incident Handling Team (IHT)
- B. Incident Response Team (IRT)
- C. Security Incident Response Team (SIRT)
- D. All the above

Answer: D

NEW QUESTION 126

The free, open source, TCP/IP protocol analyzer, sniffer and packet capturing utility standard across many industries and educational institutions is known as:

- A. Snort
- B. Wireshark
- C. Cain & Able
- D. nmap

Answer: B

NEW QUESTION 130

Installing a password cracking tool, downloading pornography material, sending emails to colleagues which irritates them and hosting unauthorized websites on the company's computer are considered:

- A. Network based attacks
- B. Unauthorized access attacks
- C. Malware attacks
- D. Inappropriate usage incidents

Answer: D

NEW QUESTION 135

Changing the web server contents, Accessing the workstation using a false ID and Copying sensitive data without authorization are examples of:

- A. DDoS attacks
- B. Unauthorized access attacks
- C. Malware attacks
- D. Social Engineering attacks

Answer: B

NEW QUESTION 139

To respond to DDoS attacks; one of the following strategies can be used:

- A. Using additional capacity to absorb attack
- B. Identifying none critical services and stopping them
- C. Shut down some services until the attack has subsided
- D. All the above

Answer: D

NEW QUESTION 141

The very well-known free open source port, OS and service scanner and network discovery utility is called:

- A. Wireshark
- B. Nmap (Network Mapper)
- C. Snort
- D. SAINT

Answer: B

NEW QUESTION 145

In a DDoS attack, attackers first infect multiple systems, which are then used to attack a particular target directly. Those systems are called:

- A. Honey Pots
- B. Relays
- C. Zombies
- D. Handlers

Answer: C

NEW QUESTION 147

A Malicious code attack using emails is considered as:

- A. Malware based attack
- B. Email attack
- C. Inappropriate usage incident
- D. Multiple component attack

Answer: D

NEW QUESTION 148

A malware code that infects computer files, corrupts or deletes the data in them and requires a host file to propagate is called:

- A. Trojan
- B. Worm
- C. Virus
- D. RootKit

Answer: C

NEW QUESTION 149

A malicious security-breaking code that is disguised as any useful program that installs an executable programs when a file is opened and allows others to control the victim's system is called:

- A. Trojan
- B. Worm
- C. Virus
- D. RootKit

Answer: A

NEW QUESTION 152

The message that is received and requires an urgent action and it prompts the recipient to delete certain files or forward it to others is called:

- A. An Adware
- B. Mail bomb
- C. A Virus Hoax
- D. Spear Phishing

Answer: C

NEW QUESTION 153

The free utility which quickly scans Systems running Windows OS to find settings that may have been changed by spyware, malware, or other unwanted programs is called:

- A. Tripwire
- B. HijackThis
- C. Stinger
- D. F-Secure Anti-virus

Answer: B

NEW QUESTION 157

A software application in which advertising banners are displayed while the program is running that delivers ads to display pop-up windows or bars that appears on a computer screen or browser is called:

- A. adware (spelled all lower case)
- B. Trojan
- C. RootKit
- D. Virus
- E. Worm

Answer: A

NEW QUESTION 161

The sign(s) of the presence of malicious code on a host infected by a virus which is delivered via e-mail could be:

- A. Antivirus software detects the infected files
- B. Increase in the number of e-mails sent and received
- C. System files become inaccessible
- D. All the above

Answer: D

NEW QUESTION 165

Which of the following is NOT one of the common techniques used to detect Insider threats:

- A. Spotting an increase in their performance
- B. Observing employee tardiness and unexplained absenteeism
- C. Observing employee sick leaves
- D. Spotting conflicts with supervisors and coworkers

Answer: A

NEW QUESTION 166

Keyloggers do NOT:

- A. Run in the background
- B. Alter system files
- C. Secretly records URLs visited in browser, keystrokes, chat conversations, ...etc
- D. Send log file to attacker's email or upload it to an ftp server

Answer: B

NEW QUESTION 167

Which is the incorrect statement about Anti-keyloggers scanners:

- A. Detect already installed Keyloggers in victim machines
- B. Run in stealthy mode to record victims online activity
- C. Software tools

Answer: B

NEW QUESTION 170

Which of the following is NOT a digital forensic analysis tool:

- A. Access Data FTK
- B. EAR/ Pilar
- C. Guidance Software EnCase Forensic
- D. Helix

Answer: B

NEW QUESTION 175

The Linux command used to make binary copies of computer media and as a disk imaging tool if given a raw disk device as its input is:

- A. "dd" command
- B. "netstat" command
- C. "nslookup" command
- D. "find" command

Answer: A

NEW QUESTION 176

The individual who recovers, analyzes, and preserves computer and related materials to be presented as evidence in a court of law and identifies the evidence, estimates the potential impact of the malicious activity on the victim, and assesses the intent and identity of the perpetrator is called:

- A. Digital Forensic Examiner
- B. Computer Forensic Investigator
- C. Computer Hacking Forensic Investigator
- D. All the above

Answer: D

NEW QUESTION 181

Any information of probative value that is either stored or transmitted in a digital form during a computer crime is called:

- A. Digital evidence
- B. Computer Emails
- C. Digital investigation
- D. Digital Forensic Examiner

Answer: A

NEW QUESTION 182

Which of the following is NOT one of the Computer Forensic types:

- A. USB Forensics
- B. Email Forensics
- C. Forensic Archaeology
- D. Image Forensics

Answer: C

NEW QUESTION 186

The correct order or sequence of the Computer Forensic processes is:

- A. Preparation, analysis, examination, collection, and reporting
- B. Preparation, collection, examination, analysis, and reporting
- C. Preparation, examination, collection, analysis, and reporting
- D. Preparation, analysis, collection, examination, and reporting

Answer: B

NEW QUESTION 187

The person who offers his formal opinion as a testimony about a computer crime incident in the court of law is known as:

- A. Expert Witness
- B. Incident Analyzer
- C. Incident Responder
- D. Evidence Documenter

Answer: A

NEW QUESTION 188

Electronic evidence may reside in the following:

- A. Data Files
- B. Backup tapes
- C. Other media sources
- D. All the above

Answer: D

NEW QUESTION 192

The steps followed to recover computer systems after an incident are:

- A. System restoration, validation, operation and monitoring
- B. System restoration, operation, validation, and monitoring
- C. System monitoring, validation, operation and restoration
- D. System validation, restoration, operation and monitoring

Answer: A

NEW QUESTION 196

The product of intellect that has commercial value and includes copyrights and trademarks is called:

- A. Intellectual property
- B. Trade secrets
- C. Logos
- D. Patents

Answer: A

NEW QUESTION 198

According to the Fourth Amendment of USA PATRIOT Act of 2001; if a search does NOT violate a person's "reasonable" or "legitimate" expectation of privacy then it is considered:

- A. Constitutional/ Legitimate
- B. Illegal/ illegitimate
- C. Unethical
- D. None of the above

Answer: A

NEW QUESTION 201

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

212-89 Practice Exam Features:

- * 212-89 Questions and Answers Updated Frequently
- * 212-89 Practice Questions Verified by Expert Senior Certified Staff
- * 212-89 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * 212-89 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 212-89 Practice Test Here](#)