



# 212-89<sup>Q&As</sup>

EC-Council Certified Incident Handler

## Pass EC-COUNCIL 212-89 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/212-89.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





### QUESTION 1

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.

Correct Answer: D

---

### QUESTION 2

The most common type(s) of intellectual property is(are):

- A. Copyrights and Trademarks
- B. Patents
- C. Industrial design rights and Trade secrets
- D. All the above

Correct Answer: D

---

### QUESTION 3

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

Correct Answer: C

---

### QUESTION 4

Incident prioritization must be based on:

- A. Potential impact



- B. Current damage
- C. Criticality of affected systems
- D. All the above

Correct Answer: D

---

#### QUESTION 5

The process of rebuilding and restoring the computer systems affected by an incident to normal operational stage including all the processes, policies and tools is known as:

- A. Incident Management
- B. Incident Response
- C. Incident Recovery
- D. Incident Handling

Correct Answer: C

[212-89 Practice Test](#)

[212-89 Study Guide](#)

[212-89 Exam Questions](#)