350-201 Q&As

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Pass Cisco 350-201 Exam with 100% Guarantee

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

https://www.geekcert.com/350-201.html

100% Passing Guarantee
100% Money Back Assurance

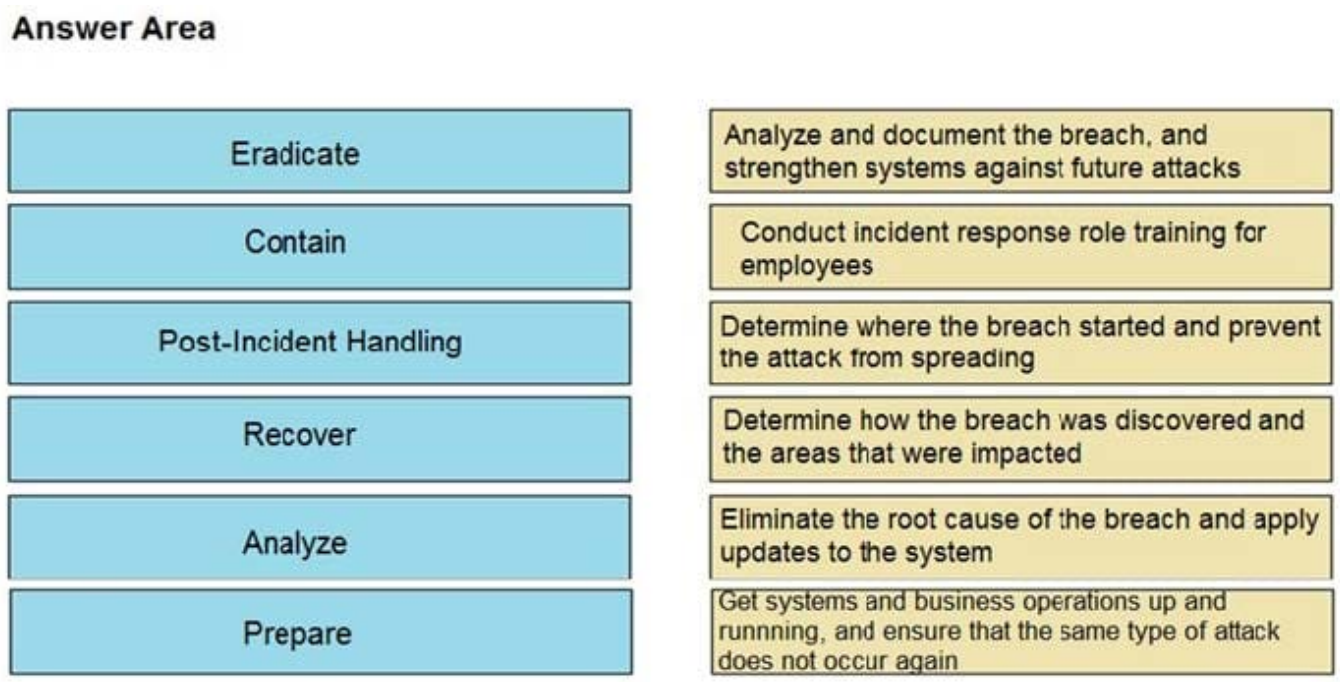
Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

DRAG DROP

Drag and drop the NIST incident response process steps from the left onto the actions that occur in the steps on the right.

Select and Place:



Correct Answer:

Reference: https://www.securitymetrics.com/blog/6-phases-incident-response-plan

QUESTION 2

An engineer is investigating several cases of increased incoming spam emails and suspicious emails from the HR and service departments. While checking the event sources, the website monitoring tool showed several web scraping alerts overnight.

Which type of compromise is indicated?

A. phishing

B. dumpster diving

C. social engineering

D. privilege escalation

Correct Answer: C

QUESTION 3

```
def get_umbrella_dispos(domains):
      # put in right format to pass as argument in POST request
      values = str(json.dumps(domains))
      req = requests.post(investigate_url, data=values, headers=headers)
      # time for timestamp of verdict domain
      time = datetime.now().isoformat()
      # error handling if true then the request was HTTP 200, so successful
      if(req.status_code == 200):
        print("SUCCESS: request has the following code: 200\n")
        output = req.json()
        [                                                                    ]
        [                                                                    ]
        [                                                                    ]
        [                                                                    ]
        if(domain_status == -1):
          print("The domain %(domain)s is found MALICIOUS at %(time)s\n" % {'domain': domain, 'time': time})
        elif(domain_status == 1):
          print("The domain %(domain)s is found CLEAN at %(time)s\n" %
           {'domain': domain, 'time': time})
        else:
          print("The domain %(domain)s is found UNDEFINED / RISKY at %(time)s\n" %
           {'domain': domain, 'time': time})
    else:
      print("An error has occurred with the following code %(error)s, please consult the following link:
      https://docs.umbrella.com/investigate-api/"%
            {'error': req.status_code})
```

Refer to the exhibit. Which code snippet will parse the response to identify the status of the domain as malicious, clean or undefined?

A.
```
for domain in domains[]:
        domain_status = domain_output["status"]
```

B.
```
while domain in domains:
    domain_status = domain_output["status"]
```

C.
```
for domain in domains:
    domain_output = output[domain]
    domain_status = domain_output["status"]
```

D.
```
while domains in domains:
    domain_output = output[domain]
    domain_status = domain_output["status"]
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: C

QUESTION 4

An engineer is developing an application that requires frequent updates to close feedback loops and enable teams to quickly apply patches. The team wants their code updates to get to market as often as possible. Which software development approach should be used to accomplish these goals?

A. continuous delivery

B. continuous integration

C. continuous deployment

D. continuous monitoring

Correct Answer: A

QUESTION 5

An employee who often travels abroad logs in from a first-seen country during non-working hours. The SIEM tool generates an alert that the user is forwarding an increased amount of emails to an external mail domain and then logs

out. The investigation concludes that the external domain belongs to a competitor.

Which two behaviors triggered UEBA? (Choose two.)

A. domain belongs to a competitor

B. log in during non-working hours

C. email forwarding to an external domain

D. log in from a first-seen country

E. increased number of sent mails

Correct Answer: AB