350-201 Q&As

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

QUESTION 1

How is a SIEM tool used?

A. To collect security data from authentication failures and cyber attacks and forward it for analysis

B. To search and compare security data against acceptance standards and generate reports for analysis

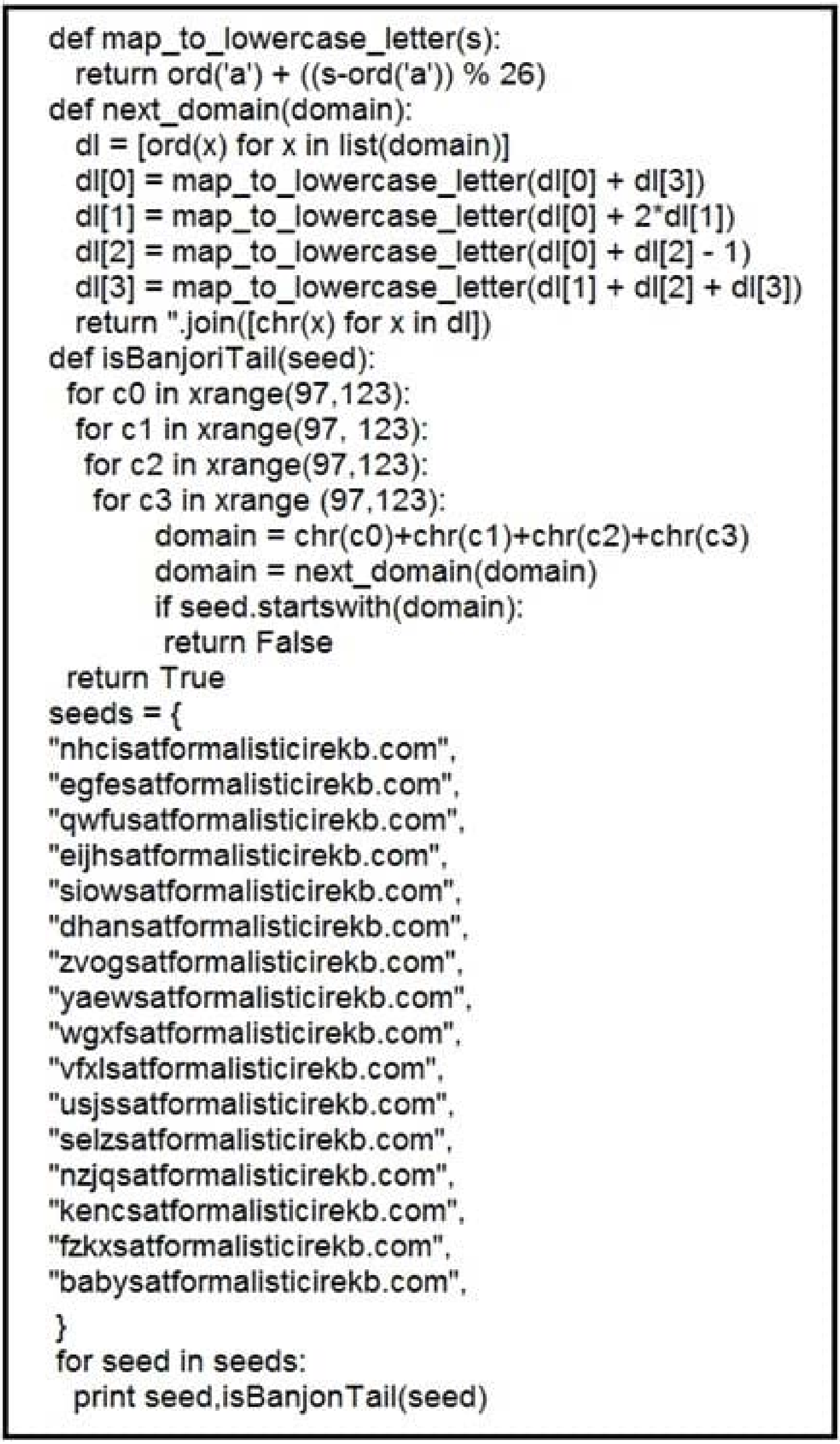
C. To compare security alerts against configured scenarios and trigger system responses

D. To collect and analyze security data from network devices and servers and produce alerts

Correct Answer: D

Reference: https://www.varonis.com/blog/what-is-siem/

QUESTION 2



```
def map_to_lowercase_letter(s):
  return ord('a') + ((s-ord('a')) % 26)
def next_domain(domain):
  dl = [ord(x) for x in list(domain)]
  dl[0] = map_to_lowercase_letter(dl[0] + dl[3])
  dl[1] = map_to_lowercase_letter(dl[0] + 2*dl[1])
  dl[2] = map_to_lowercase_letter(dl[0] + dl[2] - 1)
  dl[3] = map_to_lowercase_letter(dl[1] + dl[2] + dl[3])
  return ''.join([chr(x) for x in dl])
def isBanjoriTail(seed):
 for c0 in xrange(97,123):
  for c1 in xrange(97, 123):
   for c2 in xrange(97,123):
    for c3 in xrange (97,123):
         domain = chr(c0)+chr(c1)+chr(c2)+chr(c3)
         domain = next_domain(domain)
         if seed.startswith(domain):
          return False
 return True
seeds = {
"nhcisatformalisticirekb.com",
"egfesatformalisticirekb.com",
"qwfusatformalisticirekb.com",
"eijhsatformalisticirekb.com",
"siowsatformalisticirekb.com",
"dhansatformalisticirekb.com",
"zvogsatformalisticirekb.com",
"yaewsatformalisticirekb.com",
"wgxfsatformalisticirekb.com",
"vfxlsatformalisticirekb.com",
"usjssatformalisticirekb.com",
"selzsatformalisticirekb.com",
"nzjqsatformalisticirekb.com",
"kencsatformalisticirekb.com",
"fzkxsatformalisticirekb.com",
"babysatformalisticirekb.com",
 }
 for seed in seeds:
   print seed,isBanjonTail(seed)
```

Refer to the exhibit. What results from this script?

A. Seeds for existing domains are checked

B. A search is conducted for additional seeds

C. Domains are compared to seed rules

D. A list of domains as seeds is blocked

Correct Answer: B

QUESTION 3

An organization installed a new application server for IP phones. An automated process fetched user credentials from the Active Directory server, and the application will have access to on-premises and cloud services. Which security threat should be mitigated first?

A. aligning access control policies

B. exfiltration during data transfer

C. attack using default accounts

D. data exposure from backups

Correct Answer: B

QUESTION 4

What is a principle of Infrastructure as Code?

A. System maintenance is delegated to software systems

B. Comprehensive initial designs support robust systems

C. Scripts and manual configurations work together to ensure repeatable routines

D. System downtime is grouped and scheduled across the infrastructure

Correct Answer: B

QUESTION 5

A Mac laptop user notices that several files have disappeared from their laptop documents folder. While looking for the files, the user notices that the browser history was recently cleared. The user raises a case, and an analyst reviews the network usage and discovers that it is abnormally high.

Which step should be taken to continue the investigation?

A. Run the sudo sysdiagnose command

B. Run the sh command

C. Run the w command

D. Run the who command

Correct Answer: A

Reference: https://eclecticlight.co/2016/02/06/the-ultimate-diagnostic-tool-sysdiagnose/