**Vendor:**Cisco

**Exam Code:**200-201

**Exam Name:**Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)

**Version:**Demo

**QUESTION 1**

What is a difference between a threat and a risk?

A. A threat can be people, property, or information, and risk is a probability by which these threats may bring harm to the business.

B. A risk is a flaw or hole in security, and a threat is what is being used against that flaw.

C. A risk is an intersection between threat and vulnerabilities, and a threat is what a security engineer is trying to protect against.

D. A threat is a sum of risks, and a risk itself represents a specific danger toward the asset.

Correct Answer: C

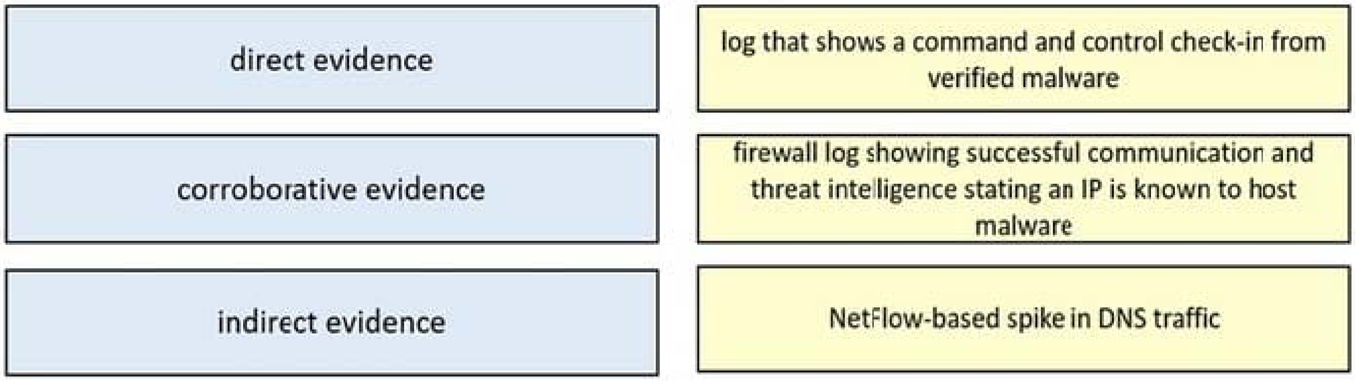
---

**QUESTION 2**

DRAG DROP

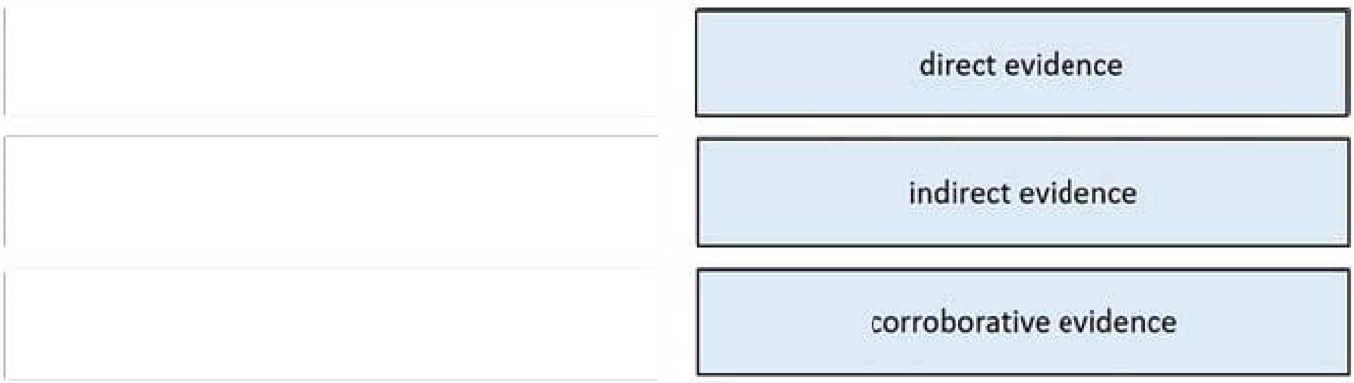
Drag and drop the type of evidence from the left onto the description of that evidence on the right.

Select and Place:



| | |
|---|---|
| direct evidence | log that shows a command and control check-in from verified malware |
| corroborative evidence | firewall log showing successful communication and threat intelligence stating an IP is known to host malware |
| indirect evidence | NetFlow-based spike in DNS traffic |

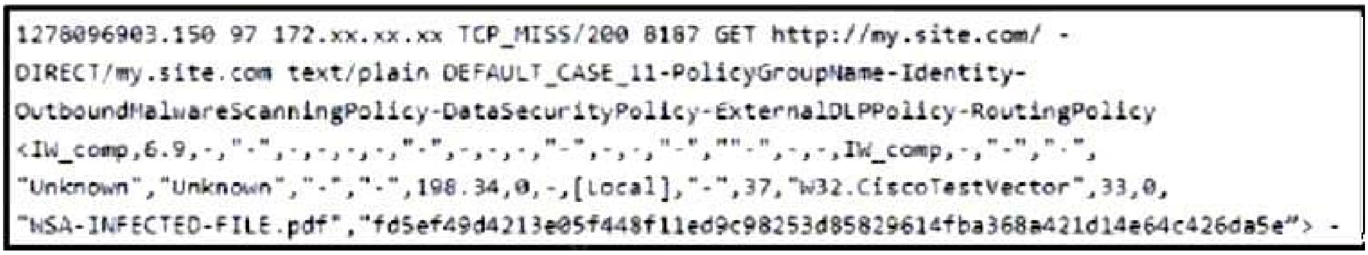
Correct Answer:



---

**QUESTION 3**

Refer to the exhibit.



```
1278096903.150 97 172.xx.xx.xx TCP_MISS/200 8187 GET http://my.site.com/ -
DIRECT/my.site.com text/plain DEFAULT_CASE_11-PolicyGroupName-Identity-
OutboundMalwareScanningPolicy-DataSecurityPolicy-ExternalDLPPolicy-RoutingPolicy
<IW_comp,6.9,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","""-",-,-,IW_comp,-,"-","-",
"Unknown","Unknown","-","-",198.34,0,-,[Local],"-",37,"W32.CiscoTestVector",33,0,
"WSA-INFECTED-FILE.pdf","fd5ef49d4213e05f448f11ed9c98253d85829614fba368a421d14e64c426da5e"> -
```

Which technology produced the log?

A. antivirus

B. IPS/IDS

C. firewall

D. proxy

Correct Answer: B

---

**QUESTION 4**

Which two elements are used for profiling a network? (Choose two.)

A. session duration

B. total throughput

C. running processes

D. listening ports

E. OS fingerprint

Correct Answer: AB

A network profile should include some important elements, such as the following:

Total throughput the amount of data passing from a given source to a given destination in a given period of time Session duration the time between the establishment of a data flow and its termination Ports used a list of TCP or UDP processes that are available to accept data Critical asset address space the IP addresses or the logical location of essential systems or data Profiling data are data that system has gathered, these data helps for incident response and to detect incident Network profiling = throughput, sessions duration, port used, Critical Asset Address Space Host profiling = Listening ports, logged in accounts, running processes, running tasks,applications

---

**QUESTION 5**

An analyst received a ticket regarding a degraded processing capability for one of the HR department\\'s servers. On the same day, an engineer noticed a disabled antivirus software and was not able to determine when or why it occurred. According to the NIST Incident Handling Guide, what is the next phase of this investigation?

A. Recovery

B. Detection

C. Eradication

D. Analysis

Correct Answer: B

Reference: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

---

**QUESTION 6**

What is the difference between a threat and an exploit?

A. An exploit is an attack path, and a threat represents a potential vulnerability.

B. An exploit is an attack vector, and a threat is a potential path the attack must go through.

C. A threat is a potential attack on an asset, and an exploit takes advantage of the vulnerability of the asset.

D. A threat is a result of utilizing flow in a system, and an exploit is a result of gaining control over the system.

Correct Answer: C

---

**QUESTION 7**

What describes the concept of data consistently and readily being accessible for legitimate users?

A. integrity

B. availability

C. accessibility

D. confidentiality

Correct Answer: B

---

**QUESTION 8**

What are two denial of service attacks? (Choose two.)

A. MITM

B. TCP connections

C. ping of death

D. UDP flooding

E. code red

Correct Answer: CD

---

**QUESTION 9**

What causes events on a Windows system to show Event Code 4625 in the log messages?

A. The system detected an XSS attack

B. Someone is trying a brute force attack on the network

C. Another device is gaining root access to the system

D. A privileged user successfully logged into the system

Correct Answer: B

---

**QUESTION 10**

Why is HTTPS traffic difficult to screen?

A. HTTPS is used internally and screening traffic (or external parties is hard due to isolation.

B. The communication is encrypted and the data in transit is secured.

C. Digital certificates secure the session, and the data is sent at random intervals.

D. Traffic is tunneled to a specific destination and is inaccessible to others except for the receiver.

Correct Answer: B

**QUESTION 11**

What is a description of a social engineering attack?

A. fake offer for free music download to trick the user into providing sensitive data

B. package deliberately sent to the wrong receiver to advertise a new product

C. mistakenly received valuable order destined for another person and hidden on purpose

D. email offering last-minute deals on various vacations around the world with a due date and a counter

Correct Answer: D

**QUESTION 12**

Which metric in CVSS indicates an attack that takes a destination bank account number and replaces it with a different bank account number?

A. integrity

B. confidentiality

C. availability

D. scope

Correct Answer: A