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.pass2lead.com/350-201.html

100% Passing Guarantee
100% Money Back Assurance

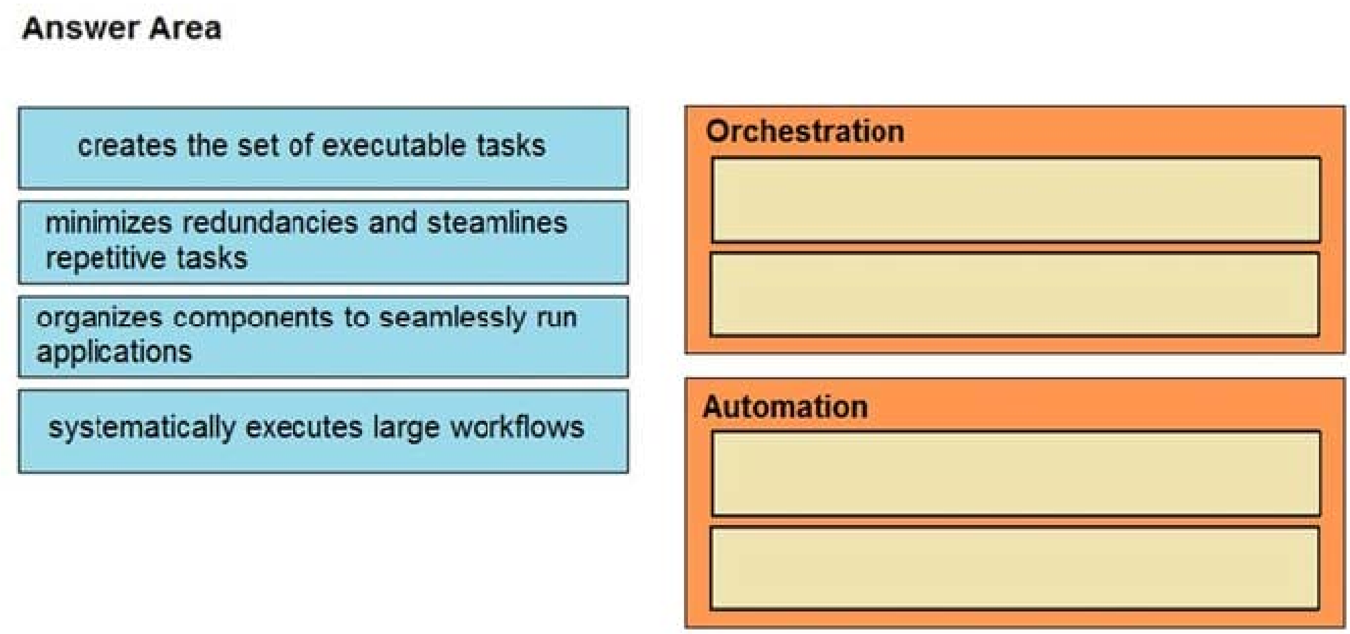
Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

DRAG DROP

Drag and drop the function on the left onto the mechanism on the right.

Select and Place:



Answer Area

creates the set of executable tasks

minimizes redundancies and steamlines repetitive tasks

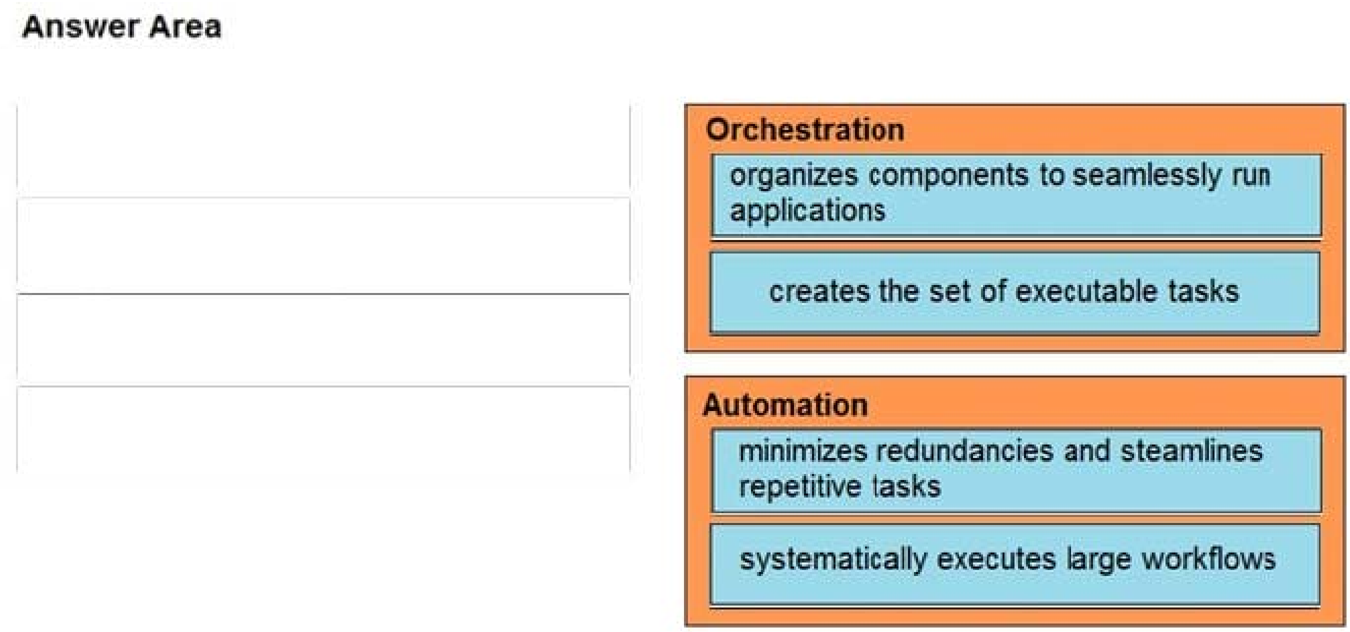
organizes components to seamlessly run applications

systematically executes large workflows

Orchestration

Automation

Correct Answer:



Answer Area

Orchestration

organizes components to seamlessly run applications

creates the set of executable tasks

Automation

minimizes redundancies and steamlines repetitive tasks

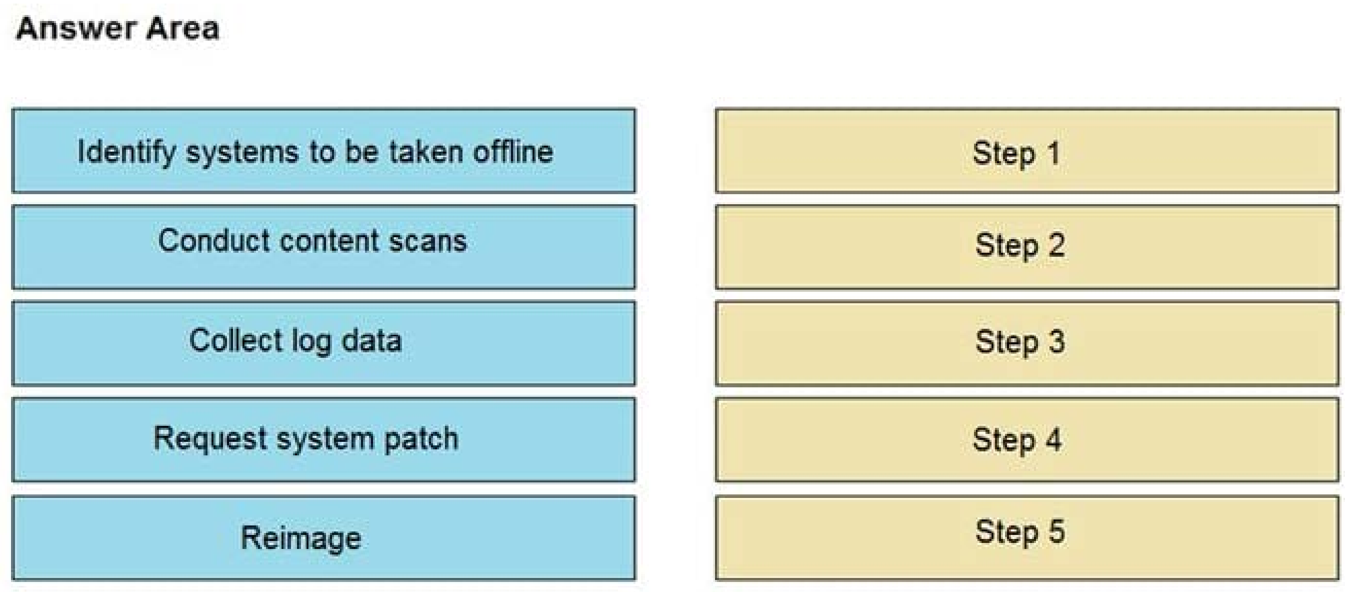
systematically executes large workflows

QUESTION 2

DRAG DROP

An engineer notices that unauthorized software was installed on the network and discovers that it was installed by a dormant user account. The engineer suspects an escalation of privilege attack and responds to the incident. Drag and drop the activities from the left into the order for the response on the right.

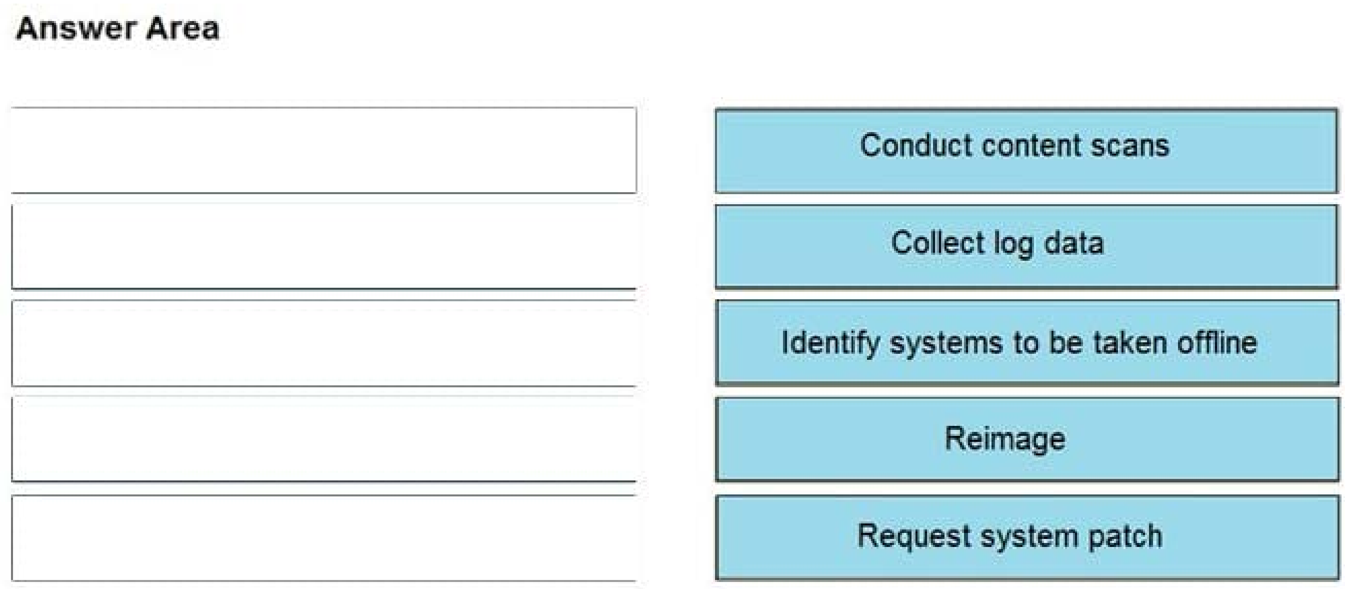
Select and Place:



Answer Area

Identify systems to be taken offline	Step 1
Conduct content scans	Step 2
Collect log data	Step 3
Request system patch	Step 4
Reimage	Step 5

Correct Answer:



Answer Area

	Conduct content scans
	Collect log data
	Identify systems to be taken offline
	Reimage
	Request system patch

QUESTION 3

An employee abused PowerShell commands and script interpreters, which lead to an indicator of compromise (IOC) trigger. The IOC event shows that a known malicious file has been executed, and there is an increased likelihood of a breach.

Which indicator generated this IOC event?

A. ExecutedMalware.ioc

B. Crossrider.ioc

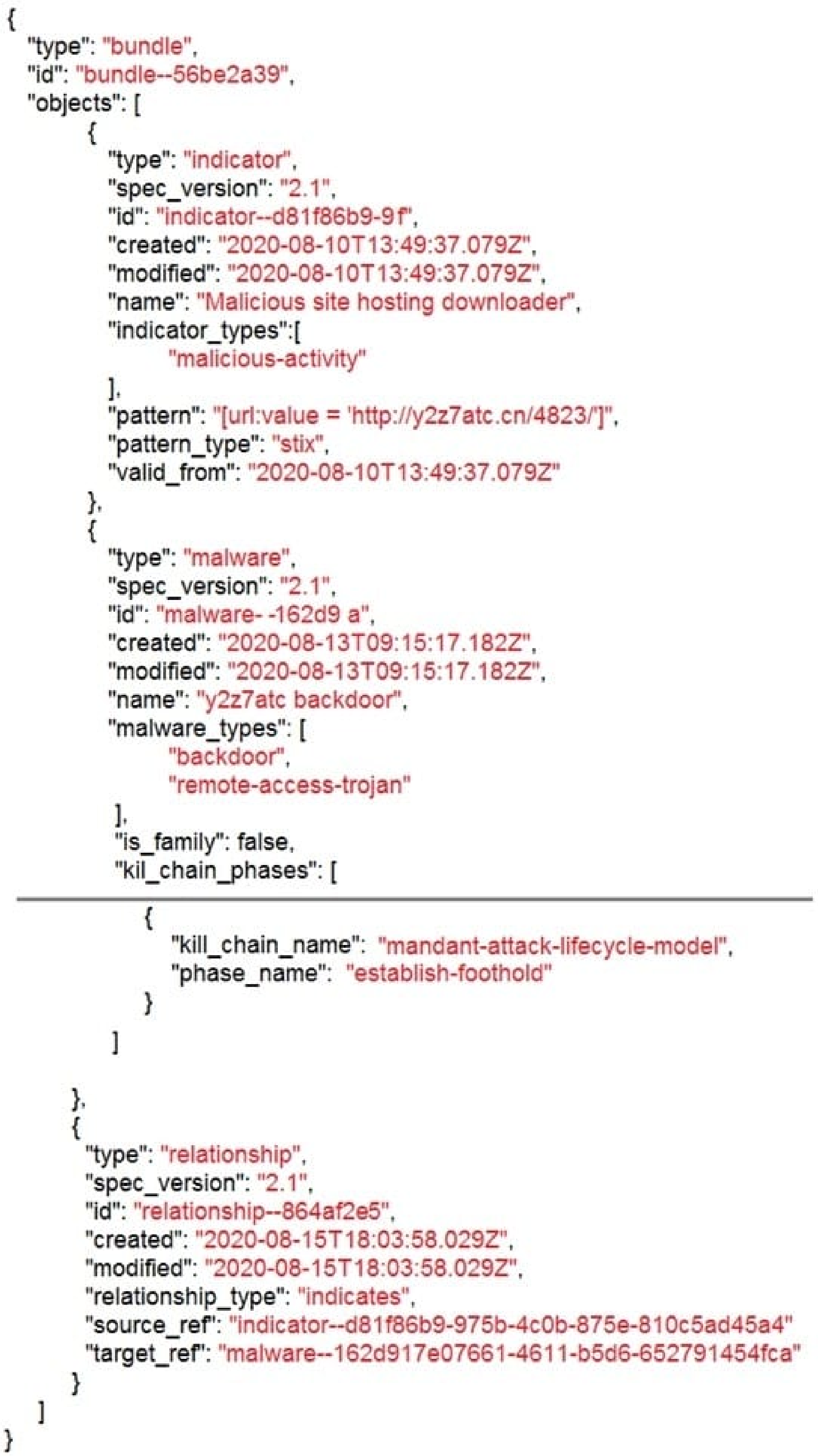
C. ConnectToSuspiciousDomain.ioc

D. W32 AccesschkUtility.ioc

Correct Answer: D

QUESTION 4

Refer to the exhibit. Which indicator of compromise is represented by this STIX?



```
{
  "type": "bundle",
  "id": "bundle--56be2a39",
  "objects": [
        {
          "type": "indicator",
          "spec_version": "2.1",
          "id": "indicator--d81f86b9-9f",
          "created": "2020-08-10T13:49:37.079Z",
          "modified": "2020-08-10T13:49:37.079Z",
          "name": "Malicious site hosting downloader",
          "indicator_types":[
                "malicious-activity"
          ],
          "pattern": "[url:value = 'http://y2z7atc.cn/4823/']",
          "pattern_type": "stix",
          "valid_from": "2020-08-10T13:49:37.079Z"
        },
        {
          "type": "malware",
          "spec_version": "2.1",
          "id": "malware- -162d9 a",
          "created": "2020-08-13T09:15:17.182Z",
          "modified": "2020-08-13T09:15:17.182Z",
          "name": "y2z7atc backdoor",
          "malware_types": [
                "backdoor",
                "remote-access-trojan"
           ],
           "is_family": false,
           "kil_chain_phases": [
              {
                 "kill_chain_name":  "mandant-attack-lifecycle-model",
                 "phase_name":  "establish-foothold"
              }
           ]

      },
      {
        "type": "relationship",
        "spec_version": "2.1",
        "id": "relationship--864af2e5",
        "created": "2020-08-15T18:03:58.029Z",
        "modified": "2020-08-15T18:03:58.029Z",
        "relationship_type": "indicates",
        "source_ref": "indicator--d81f86b9-975b-4c0b-875e-810c5ad45a4"
        "target_ref": "malware--162d917e07661-4611-b5d6-652791454fca"
      }
   ]
}
```

A. website redirecting traffic to ransomware server

B. website hosting malware to download files

C. web server vulnerability exploited by malware

D. cross-site scripting vulnerability to backdoor server

Correct Answer: C

QUESTION 5

Which bash command will print all lines from the “colors.txt” file containing the non case-sensitive pattern “Yellow”?

A. grep -i “yellow” colors.txt

B. locate “yellow” colors.txt

C. locate -i “Yellow” colors.txt

D. grep “Yellow” colors.txt

Correct Answer: A