350-201 Dumps

Performing CyberOps Using Core Security Technologies (CBRCOR)

https://www.certleader.com/350-201-dumps.html

NEW QUESTION 1
What is a benefit of key risk indicators?

A. clear perspective into the risk position of an organization
B. improved visibility on quantifiable information
C. improved mitigation techniques for unknown threats
D. clear procedures and processes for organizational risk

Answer: C

NEW QUESTION 2
A European-based advertisement company collects tracking information from partner websites and stores it on a local server to provide tailored ads. Which standard must the company follow to safeguard the resting data?

A. HIPAA
B. PCI-DSS
C. Sarbanes-Oxley
D. GDPR

Answer: D

NEW QUESTION 3
Refer to the exhibit.

```
try
{
    using (MemoryStream memoryStream = new MemoryStream())
    {
        memoryStream.Position = 32L;
        using (AesCryptoServiceProvider aesCryptoServiceProvider = new AesCryptoServiceProvider())
        {
            aesCryptoServiceProvider.KeySize = 128;
            aesCryptoServiceProvider.BlockSize = 128;
            aesCryptoServiceProvider.Mode = CipherMode.CBC;
            aesCryptoServiceProvider.Padding = PaddingMode.PKCS7;
            aesCryptoServiceProvider.Key = key;
            aesCryptoServiceProvider.GenerateIV();
            using (CryptoStream cryptoSream = new CryptoStream(memoryStream, aesCryptoServiceProvider.CreateEncryptor(), CryptoStreamMode.Write))
            {
                memoryStream.Write(aesCryptoServiceProvider.IV, 0, aesCryptoServiceProvider.IV.Length);
                cryptoStream.Write(input, 0, input.Length);
                cryptoStream.FlushFinalBlock();
                using (HMACSHA256 hMACSHA = new HMACSHA256(bytes))
                {
                    byte[] array = hMACSHA.ComputeHash(memoryStream.ToArray(), 32, memoryStream.ToArray().Length - 32);
                    memoryStream.Position = 0L;
                    memoryStream.Write(array, 0, array.Length);
                }
            }
        }
        result = memoryStream.ToArray();
    }
}
catch
{
}
```

An engineer is performing a static analysis on a malware and knows that it is capturing keys and webcam events on a company server. What is the indicator of compromise?

A. The malware is performing comprehensive fingerprinting of the host, including a processor, motherboard manufacturer, and connected removable storage.
B. The malware is a ransomware querying for installed anti-virus products and operating systems to encrypt and render unreadable until payment is made for file decryption.
C. The malware has moved to harvesting cookies and stored account information from major browsers and configuring a reverse proxy for intercepting network activity.
D. The malware contains an encryption and decryption routine to hide URLs/IP addresses and is storing the output of loggers and webcam captures in locally encrypted files for retrieval.

Answer: B

NEW QUESTION 4
An engineer receives an incident ticket with hundreds of intrusion alerts that require investigation. An analysis of the incident log shows that the alerts are from trusted IP addresses and internal devices. The final incident report stated that these alerts were false positives and that no intrusions were detected. What action should be taken to harden the network?

A. Move the IPS to after the firewall facing the internal network
B. Move the IPS to before the firewall facing the outside network
C. Configure the proxy service on the IPS
D. Configure reverse port forwarding on the IPS

Answer: C

NEW QUESTION 5

Refer to the exhibit.

```
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})
```

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

Answer: C

NEW QUESTION 6
A SIEM tool fires an alert about a VPN connection attempt from an unusual location. The incident response team validates that an attacker has installed a remote access tool on a user's laptop while traveling. The attacker has the user's credentials and is attempting to connect to the network.
What is the next step in handling the incident?

A. Block the source IP from the firewall
B. Perform an antivirus scan on the laptop
C. Identify systems or services at risk
D. Identify lateral movement

Answer: C

NEW QUESTION 7
An organization had several cyberattacks over the last 6 months and has tasked an engineer with looking for patterns or trends that will help the organization anticipate future attacks and mitigate them. Which data analytic technique should the engineer use to accomplish this task?

A. diagnostic
B. qualitative
C. predictive
D. statistical

Answer: C

NEW QUESTION 8
An engineer receives a report that indicates a possible incident of a malicious insider sending company information to outside parties. What is the first action the engineer must take to determine whether an incident has occurred?

A. Analyze environmental threats and causes
B. Inform the product security incident response team to investigate further
C. Analyze the precursors and indicators
D. Inform the computer security incident response team to investigate further

Answer: C

NEW QUESTION 9
A payroll administrator noticed unexpected changes within a piece of software and reported the incident to the incident response team. Which actions should be taken at this step in the incident response workflow?

A. Classify the criticality of the information, research the attacker's motives, and identify missing patches
B. Determine the damage to the business, extract reports, and save evidence according to a chain of custody
C. Classify the attack vector, understand the scope of the event, and identify the vulnerabilities being exploited
D. Determine the attack surface, evaluate the risks involved, and communicate the incident according to the escalation plan

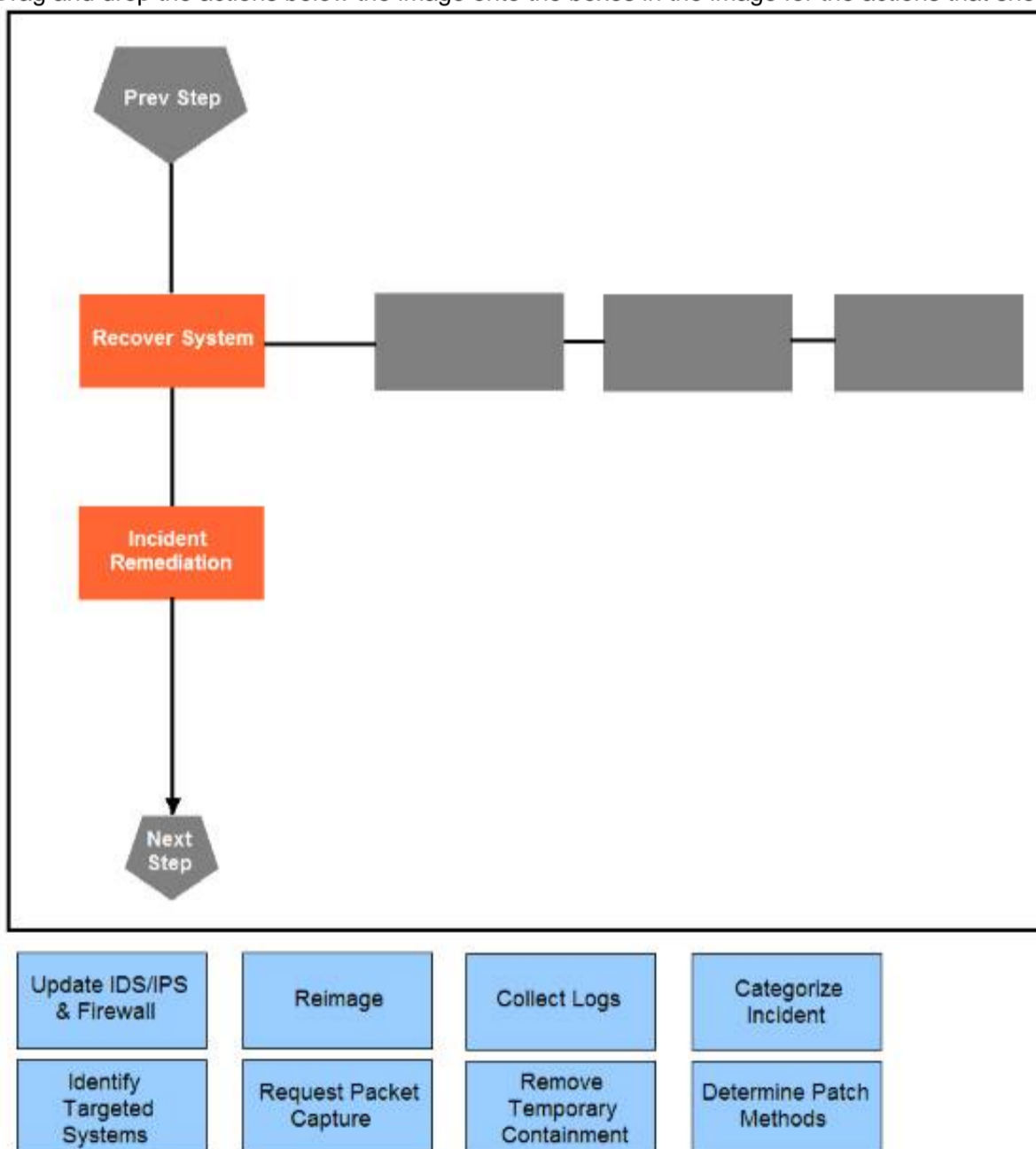**Answer:** B

NEW QUESTION 10
An engineer has created a bash script to automate a complicated process. During script execution, this error occurs: permission denied. Which command must be added to execute this script?

A. chmod +x ex.sh
B. source ex.sh
C. chroot ex.sh
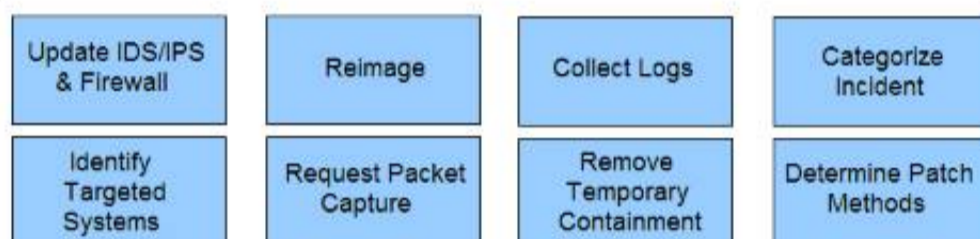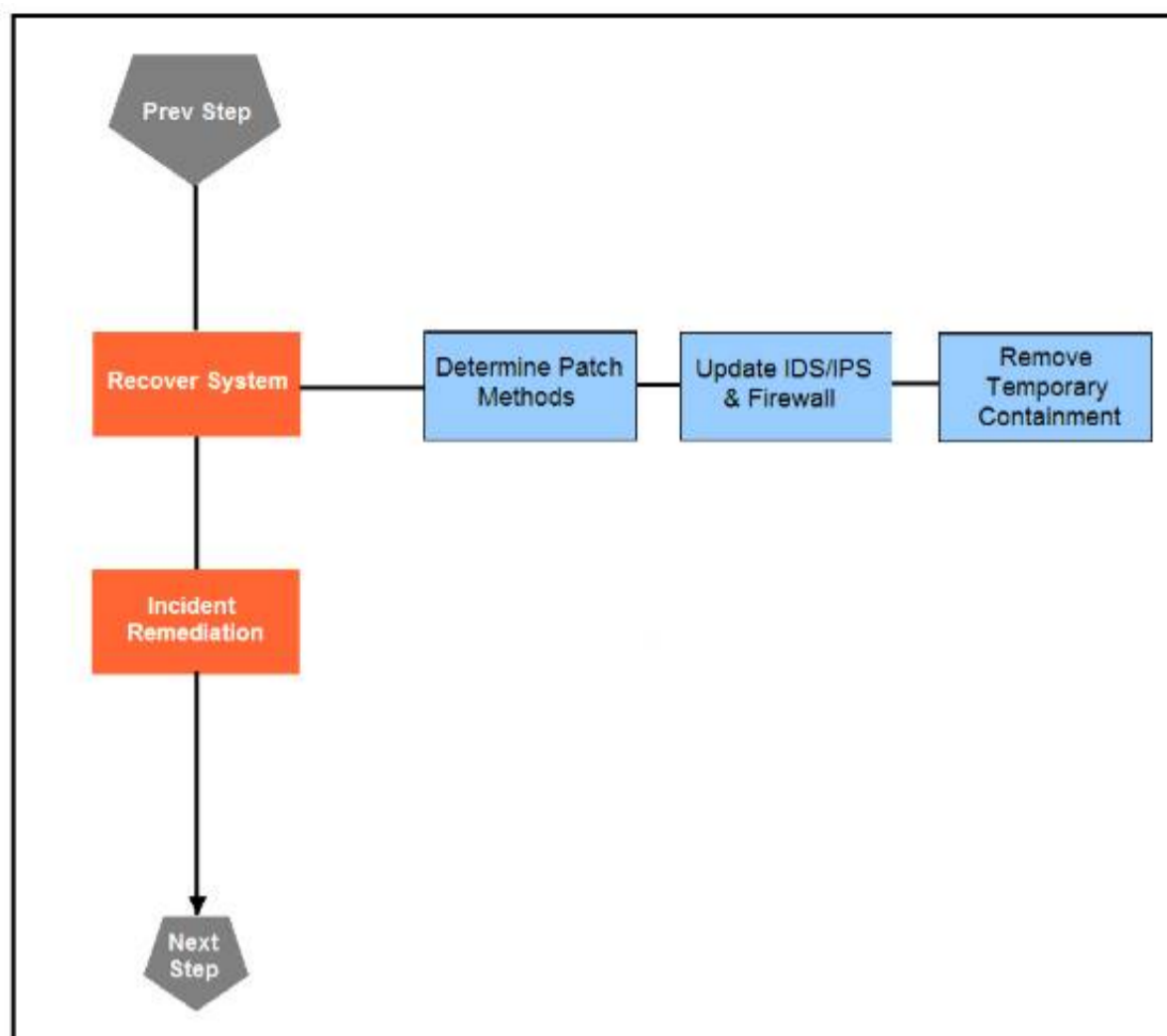D. sh ex.sh

Answer: A

NEW QUESTION 10
Drag and drop the actions below the image onto the boxes in the image for the actions that should be taken during this playbook step. Not all options are used.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 13
Refer to the exhibit.

```
{
    "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"
        }
    ]
}
```

Which indicator of compromise is represented by this STIX?

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

Answer: C

NEW QUESTION 15
Refer to the exhibit.

```
URIs:

    • /invoker/JMXInvokerServlet
    • /CFIDE/adminapi
    • /?a=<script>alert%28%22XSS%22%29%3B</script>&b=UNION+SELECT+ALL+FROM+information
      _schema+AND+%27+or+SLEEP%285%29+or+%27c=../../../../etc/passwd
```

At which stage of the threat kill chain is an attacker, based on these URIs of inbound web requests from known malicious Internet scanners?

A. exploitation
B. actions on objectives
C. delivery
D. reconnaissance

Answer: C

NEW QUESTION 20
The incident response team was notified of detected malware. The team identified the infected hosts, removed the malware, restored the functionality and data of infected systems, and planned a company meeting to improve the incident handling capability. Which step was missed according to the NIST incident handling guide?

A. Contain the malware
B. Install IPS software
C. Determine the escalation path
D. Perform vulnerability assessment

Answer: D

NEW QUESTION 23
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

Answer: AB

NEW QUESTION 28
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

Answer: C

NEW QUESTION 33
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

Answer: D

NEW QUESTION 37
The incident response team receives information about the abnormal behavior of a host. A malicious file is found being executed from an external USB flash drive. The team collects and documents all the necessary evidence from the computing resource. What is the next step?

A. Conduct a risk assessment of systems and applications
B. Isolate the infected host from the rest of the subnet
C. Install malware prevention software on the host
D. Analyze network traffic on the host's subnet

Answer: B

NEW QUESTION 42
An engineer wants to review the packet overviews of SNORT alerts. When printing the SNORT alerts, all the packet headers are included, and the file is too large to utilize. Which action is needed to correct this problem?

A. Modify the alert rule to "output alert_syslog: output log"
B. Modify the output module rule to "output alert_quick: output filename"
C. Modify the alert rule to "output alert_syslog: output header"
D. Modify the output module rule to "output alert_fast: output filename"

Answer: A

NEW QUESTION 45
Refer to the exhibit.

| TCP	192.168.1.8:54580	vk-in-f108:imaps	ESTABLISHED
TCP	192.168.1.8:54583	132.245.61.50:https	ESTABLISHED
TCP	192.168.1.8:54916	bay405-m:https	ESTABLISHED
TCP	192.168.1.8:54978	vu-in-f188:5228	ESTABLISHED
TCP	192.168.1.8:55094	72.21.194.109:https	ESTABLISHED
TCP	192.168.1.8:55401	wonderhowto:http	ESTABLISHED
TCP	192.168.1.8:55730	mia07s34-in-f78:https	TIME WAIT
TCP	192.168.1.8:55824	a23-40-191-15:https	CLOSE_WAIT
TCP	192.168.1.8:55825	a23-40-191-15:https	CLOSE_WAIT
TCP	192.168.1.8:55846	mia07s25-in-f14:https	TIME_WAIT
TCP	192.168.1.8:55847	a184-51-150-89:http	CLOSE_WAIT
TCP	192.168.1.8:55853	157.55.56.154:40028	ESTABLISHED
TCP	192.168.1.8:55879	atl14s38-in-f4:https	ESTABLISHED
TCP	192.168.1.8:55884	208-46-117-174:https	ESTABLISHED
TCP	192.168.1.8:55893	vx-in-f95:https	TIME_WAIT
TCP	192.168.1.8:55947	stackoverflow:https	ESTABLISHED
TCP	192.168.1.8:55966	stackoverflow:https	ESTABLISHED
TCP	192.168.1.8:55970	mia07s34-in-f78:https	TIME_WAIT
TCP	192.168.1.8:55972	191.238.241.80:https	TIME_WAIT
TCP	192.168.1.8:55976	54.239.26.242:https	ESTABLISHED
TCP	192.168.1.8:55979	mia07s35-in-f14:https	ESTABLISHED
TCP	192.168.1.8:55986	server11:https	TIME_WAIT
TCP	192.168.1.8:55988	104.16.118.182:http	ESTABLISHED

A security analyst needs to investigate a security incident involving several suspicious connections with a possible attacker. Which tool should the analyst use to identify the source IP of the offender?

A. packet sniffer
B. malware analysis
C. SIEM
D. firewall manager

Answer: A

NEW QUESTION 46
Refer to the exhibit.
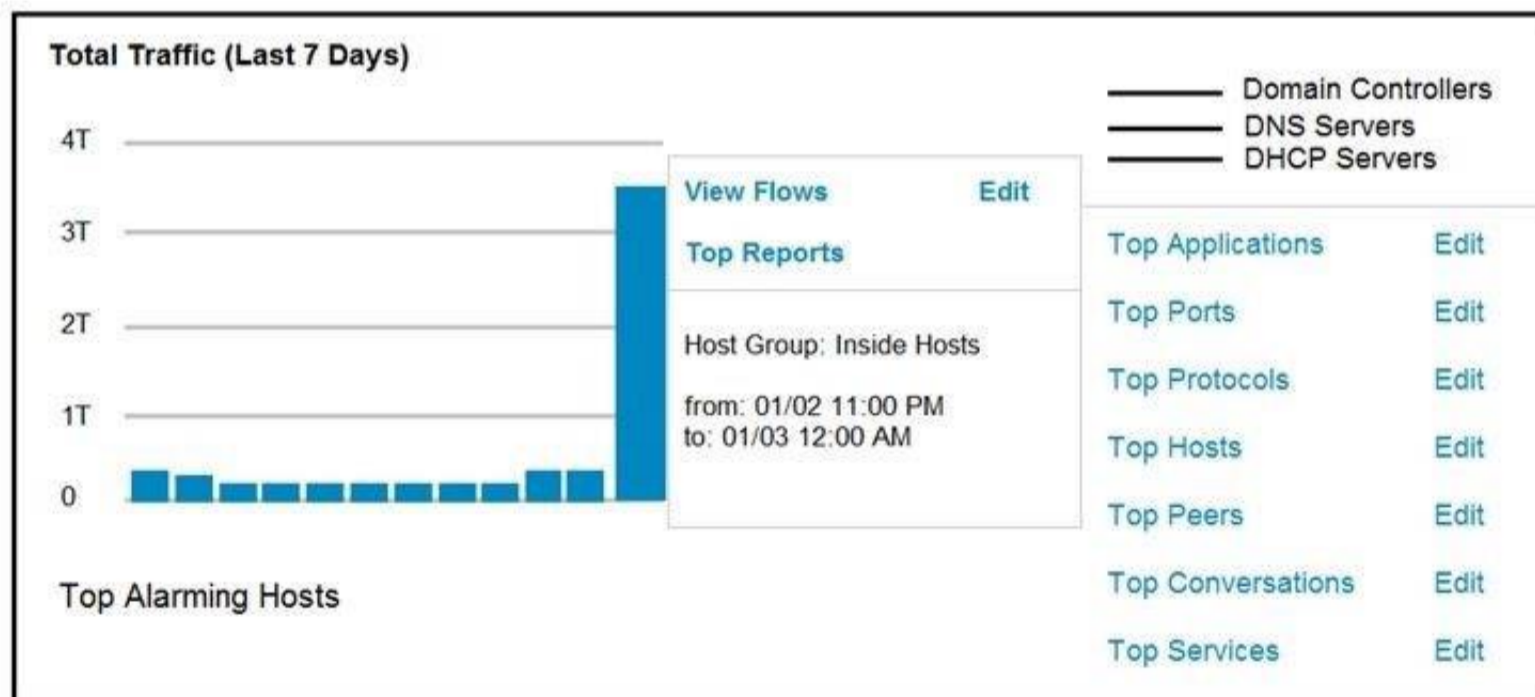
An engineer notices a significant anomaly in the traffic in one of the host groups in Cisco Secure Network Analytics (Stealthwatch) and must analyze the top data transmissions. Which tool accomplishes this task?

A. Top Peers
B. Top Hosts
C. Top Conversations
D. Top Ports

Answer: B

NEW QUESTION 49
Refer to the exhibit.

The Cisco Secure Network Analytics (Stealthwatch) console alerted with "New Malware Server Discovered" and the IOC indicates communication from an end-user desktop to a Zeus C&C Server. Drag and drop the actions that the analyst should take from the left into the order on the right to investigate and remediate this IOC.

Answer Area

Execute rapid threat containment	Step 1
Investigate and classify the exposure	Step 2
Investigate infected hosts	Step 3
Search for infected hosts	Step 4
Examine returned results	Step 5

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Execute rapid threat containment	Search for infected hosts
Investigate and classify the exposure	Investigate infected hosts
Investigate infected hosts	Investigate and classify the exposure
Search for infected hosts	Examine returned results
Examine returned results	Execute rapid threat containment

NEW QUESTION 50
......

Thank You for Trying Our Product

* 100% Pass or Money Back

    All our products come with a 90-day Money Back Guarantee.

* One year free update

    You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

    We currently serve more than 30,000,000 customers.

* Shop Securely

    All transactions are protected by VeriSign!

100% Pass Your 350-201 Exam with Our Prep Materials Via below:

https://www.certleader.com/350-201-dumps.html