Free Questions for 350-201 by ebraindumps

Shared by Bailey on 06-06-2022

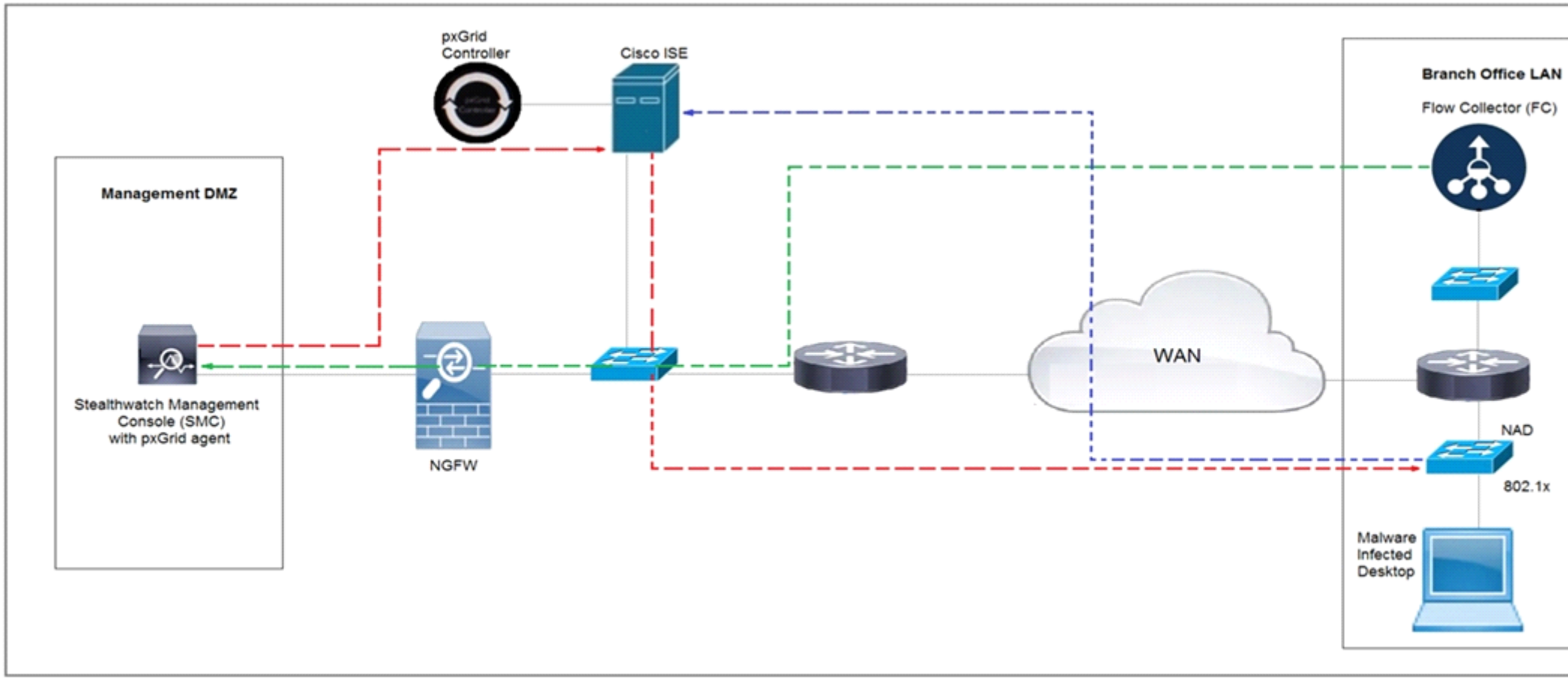
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit.



Rapid Threat Containment using Cisco Secure Network Analytics (Stealthwatch) and ISE detects the threat of malware-infected 802.1x authenticated endpoints and places that endpoint into a quarantine VLAN using Adaptive Network Control policy. Which method was used to signal ISE to quarantine the endpoints?

Options:

A- SNMP

B- syslog

C- REST API

D- pxGrid

Answer:

C

Question 2

Question Type: **MultipleChoice**

After a recent malware incident, the forensic investigator is gathering details to identify the breach and causes. The investigator has isolated the affected workstation. What is the next step that should be taken in this investigation?

Options:

A- Analyze the applications and services running on the affected workstation.

B- Compare workstation configuration and asset configuration policy to identify gaps.

C- Inspect registry entries for recently executed files.

D- Review audit logs for privilege escalation events.

Answer:

C

Question 3

Question Type: MultipleChoice

A security incident affected an organization's critical business services, and the customer-side web API became unresponsive and crashed. An investigation revealed a spike of API call requests and a high number of inactive sessions during the incident. Which two recommendations should the engineers make to prevent similar incidents in the future? (Choose two.)

Options:

A- Configure shorter timeout periods.

B- Determine API rate-limiting requirements.

C- Implement API key maintenance.

D- Automate server-side error reporting for customers.

E- Decrease simultaneous API responses.

Answer:

B, D

Question 4

Question Type: **MultipleChoice**

Engineers are working to document, list, and discover all used applications within an organization. During the regular assessment of applications from the HR backup server, an engineer discovered an unknown application. The analysis showed that the application is communicating with external addresses on a non- secure, unencrypted channel. Information gathering revealed that the unknown application does not have an owner and is not being used by a business unit. What are the next two steps the engineers should take in

this investigation? (Choose two.)

Options:

A- Determine the type of data stored on the affected asset, document the access logs, and engage the incident response team.

B- Identify who installed the application by reviewing the logs and gather a user access log from the HR department.

C- Verify user credentials on the affected asset, modify passwords, and confirm available patches and updates are installed.

D- Initiate a triage meeting with department leads to determine if the application is owned internally or used by any business unit and document the asset owner.

Answer:

A, D

Question 5

Question Type: MultipleChoice

A cloud engineer needs a solution to deploy applications on a cloud without being able to manage and control the server OS. Which type of cloud environment should be used?

Options:

A- IaaS

B- PaaS

C- DaaS

D- SaaS

Answer:

A

Question 6

Question Type: **MultipleChoice**

A SOC team receives multiple alerts by a rule that detects requests to malicious URLs and informs the incident response team to block the malicious URLs requested on the firewall. Which action will improve the effectiveness of the process?

Options:

A- Block local to remote HTTP/HTTPS requests on the firewall for users who triggered the rule.

B- Inform the user by enabling an automated email response when the rule is triggered.

C- Inform the incident response team by enabling an automated email response when the rule is triggered.

D- Create an automation script for blocking URLs on the firewall when the rule is triggered.

Answer:

A

Question 7

Question Type: **MultipleChoice**

Refer to the exhibit.

```
HttpWebRequest httpWebRequest = (HttpWebRequest)WebRequest.Create("http://freegeoip.net/xml/");
httpWebRequest.UserAgent = "Mozilla/5.0 (Windows NT 6.3; rv:48.0) Gecko/20100101 Firefox/48.0";
httpWebRequest.Proxy = null;
httpWebRequest.Timeout = 10000;
using (HttpWebResponse httpWebResponse = (HttpWebResponse)httpWebRequest.GetResponse())
{
    using (Stream responseStream = httpWebResponse.GetRepsonseStream())
    {
        using (StreamReader streamReader = new StreamReader(responseStream))
        {
            string xml = streamReader.ReadToEnd();
            XmlDocument xmlDocument = new XmlDocument();
            xmlDocument.LoadXml(xml);
            string innerXml = xmlDocument.SelectSingleNode("Response//IP").InnerXml;
            string innerXml2 = xmlDocument.SelectSingleNode("Response//CountryName").InnerXml;
            string innerXml3 = xmlDocument.SelectSingleNode("Response//CountryCode").InnerXml;
            string innerXml4 = xmlDocument.SelectSingleNode("Response//RegionName").InnerXml;
            string innerXml5 = xmlDocument.SelectSingleNode("Response//City").InnerXml;
            string innerXml6 = xmlDocument.SelectSingleNode("Response//TimeZone").InnerXml;
```

An engineer is performing static analysis of a file received and reported by a user. Which risk is indicated in this STIX?

Options:

A- The file is redirecting users to a website that requests privilege escalations from the user.

B- The file is redirecting users to the website that is downloading ransomware to encrypt files.

C- The file is redirecting users to a website that harvests cookies and stored account information.

D- The file is redirecting users to a website that is determining users' geographic location.

Answer:

D

Question 8

Question Type: MultipleChoice

An engineer received multiple reports from users trying to access a company website and instead of landing on the website, they are redirected to a malicious website that asks them to fill in sensitive personal dat

a. Which type of attack is occurring?

Options:

A- Address Resolution Protocol poisoning

B- session hijacking attack

C- teardrop attack

D- Domain Name System poisoning

Answer:

D