**QUESTION 174**
A security analyst has discovered trial developers have installed browsers on all development servers in the company's cloud infrastructure and are using them to browse the Internet. Which of the following changes should the security analyst make to BEST protect the environment?

A. Create a security rule that blocks Internet access in the development VPC
B. Place a jumpbox m between the developers' workstations and the development VPC
C. Remove the administrator profile from the developer user group in identity and access management
D. Create an alert that is triggered when a developer installs an application on a server

**Correct Answer:** A

**QUESTION 175**
A security analyst has received information from a third-party intelligence-sharing resource that indicates employee accounts were breached. Which of the following is the NEXT step the analyst should take to address the issue?

A. Audit access permissions for all employees to ensure least privilege.
B. Force a password reset for the impacted employees and revoke any tokens.
C. Configure SSO to prevent passwords from going outside the local network.
D. Set up privileged access management to ensure auditing is enabled.

**Correct Answer:** B

**QUESTION 176**
Which of the following attacks can be prevented by using output encoding?

A. Server-side request forgery
B. Cross-site scripting
C. SQL injection
D. Command injection
E. Cross-site request forgery
F. Directory traversal

**Correct Answer:** B

**QUESTION 177**
A host is spamming the network unintentionally. Which of the following control types should be used to address this situation?

A. Operational
B. Corrective
C. Managerial
D. Technical
**Correct Answer:** B

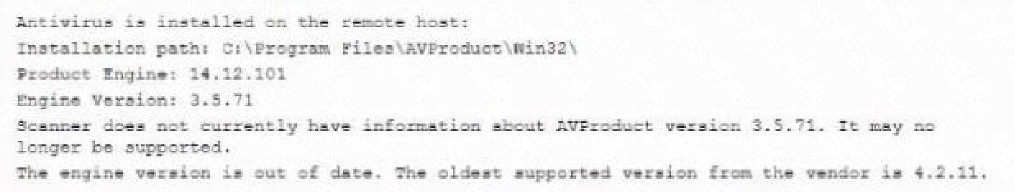
**QUESTION 178**
Ransomware is identified on a company's network that affects both Windows and MAC hosts.

The command and control channel for encryption for this variant uses TCP ports from 11000 to 65000. The channel goes to good1. Iholdbadkeys.com, which resolves to IP address 72.172.16.2. Which of the following is the MOST effective way to prevent any newly infected systems from actually encrypting the data on connected network drives while causing the least disruption to normal Internet traffic?

A. Block all outbound traffic to web host good1 iholdbadkeys.com at the border gateway.
B. Block all outbound TCP connections to IP host address 172.172.16.2 at the border gateway.
C. Block all outbound traffic on TCP ports 11000 to 65000 at the border gateway.
D. Block all outbound traffic on TCP ports 11000 to 65000 to IP host address 172.172.16.2 at the border gateway.

**Correct Answer:** A

**QUESTION 179**
A security analyst is reviewing vulnerability scan results and notices new workstations are being flagged as having outdated antivirus signatures. The analyst observes the following plugin output:



```
Antivirus is installed on the remote host:
Installation path: C:\Program Files\AVProduct\Win32\
Product Engine: 14.12.101
Engine Version: 3.5.71
Scanner does not currently have information about AVProduct version 3.5.71. It may no
longer be supported.
The engine version is out of date. The oldest supported version from the vendor is 4.2.11.
```

The analyst uses the vendor's website to confirm the oldest supported version is correct. Which of the following BEST describes the situation?

A. This is a false positive and the scanning plugin needs to be updated by the vendor
B. This is a true negative and the new computers have the correct version of the software
C. This is a true positive and the new computers were imaged with an old version of the software
D. This is a false negative and the new computers need to be updated by the desktop team

**Correct Answer:** C

**QUESTION 180**
An analyst wants to identify hosts that are connecting to the external FTP servers and what, if any, passwords are being used. Which of the following commands should the analyst use?

A. tcpdump -X dst port 21
B. ftp ftp.server -p 21
C. nmap -o ftp.server -p 21
D. telnet ftp.server 21

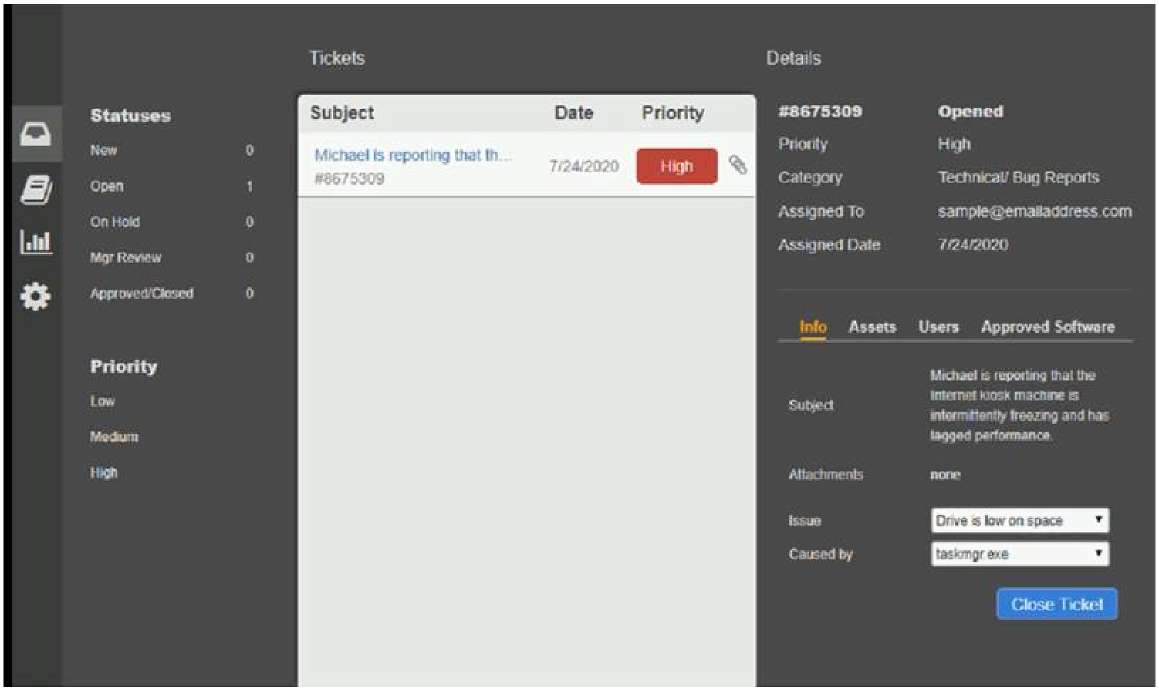
**Correct Answer:** A

**QUESTION 181**
Welcome to the Enterprise Help Desk System. Please work the ticket escalated to you in the desk ticket queue.

INSTRUCTIONS
Click on me ticket to see the ticket details Additional content is available on tabs within the ticket.

First, select the appropriate issue from the drop-down menu. Then, select the MOST likely root cause from second drop-down menu.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



**Statuses**

| | |
|---|---|
| New | 0 |
| Open | 1 |
| On Hold | 0 |
| Mgr Review | 0 |
| Approved/Closed | 0 |

**Priority**

Low
Medium
High

| Subject | Date | Priority |
|---|---|---|
| Michael is reporting that th...<br>#8675309 | 7/24/2020 | High |

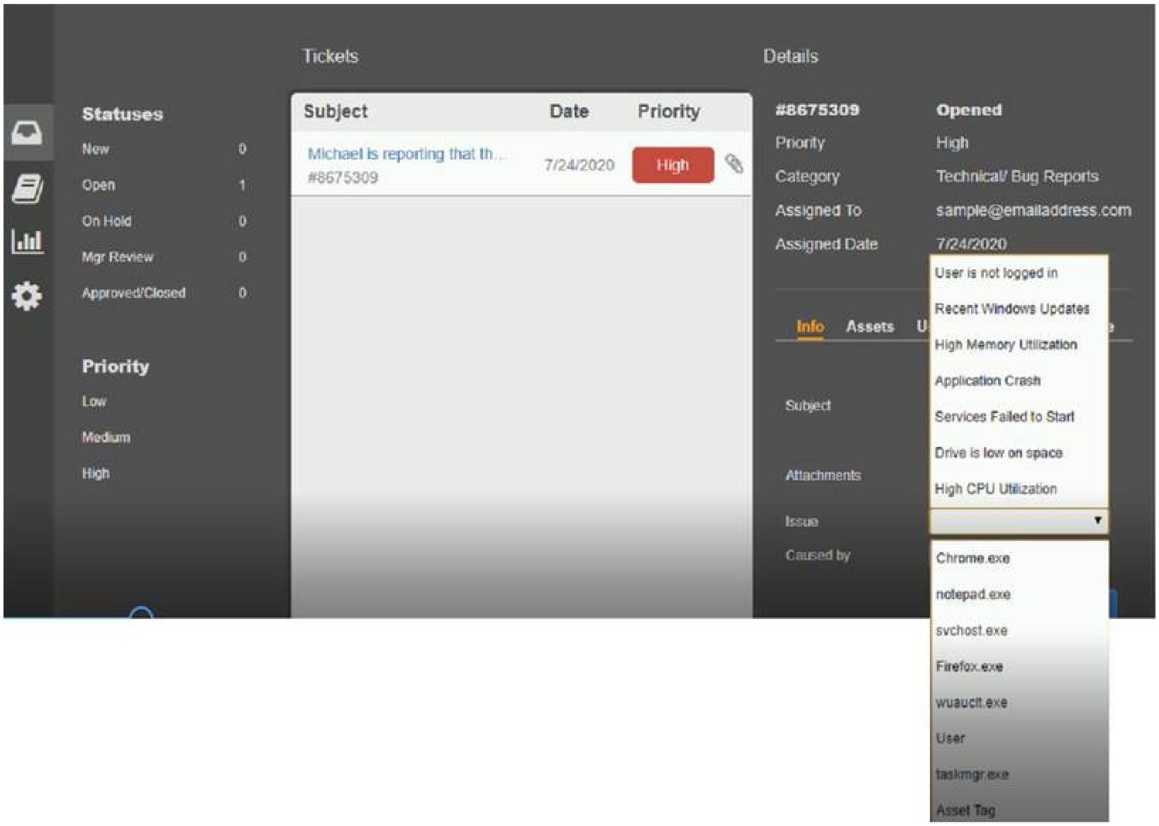
| #8675309 | Opened |
|---|---|
| Priority | High |
| Category | Technical/ Bug Reports |
| Assigned To | sample@emailaddress.com |
| Assigned Date | 7/24/2020 |

Subject: Michael is reporting that the Internet kiosk machine is intermittently freezing and has lagged performance.

Attachments: none

Issue: Drive is low on space ▾

Caused by: taskmgr.exe ▾



| Subject | Date | Priority |
|---|---|---|
| Michael is reporting that th...<br>#8675309 | 7/24/2020 | High |

Details

#8675309 Opened

Priority: High

Category: Technical/ Bug Reports

Assigned To: sample@emailaddress.com

Assigned Date: 7/24/2020

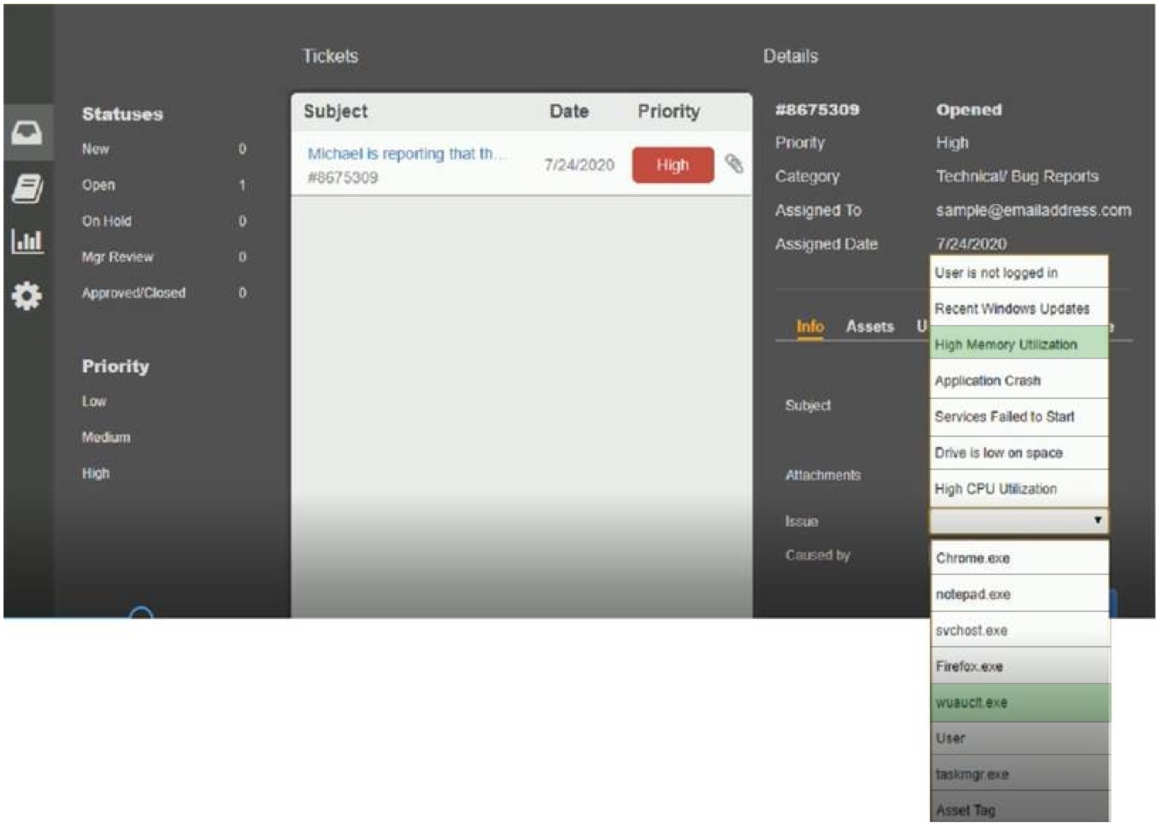
Subject

Attachments

Issue

Caused by

**Correct Answer:**



Statuses

| | |
|---|---|
| New | 0 |
| Open | 1 |
| On Hold | 0 |
| Mgr Review | 0 |
| Approved/Closed | 0 |

Priority

- Low
- Medium
- High

Tickets

| Subject | Date | Priority |
|---|---|---|
| Michael is reporting that th...<br>#8675309 | 7/24/2020 | High |

Details

| | |
|---|---|
| #8675309 | Opened |
| Priority | High |
| Category | Technical/ Bug Reports |
| Assigned To | sample@emailaddress.com |
| Assigned Date | 7/24/2020 |

Subject

Attachments

Issue:
- User is not logged in
- Recent Windows Updates
- High Memory Utilization
- Application Crash
- Services Failed to Start
- Drive is low on space
- High CPU Utilization

Caused by:
- Chrome.exe
- notepad.exe
- svchost.exe
- Firefox.exe
- wuauclt.exe
- User
- taskmgr.exe
- Asset Tag

**QUESTION 182**
Which of following allows Secure Boot to be enabled?

A. eFuse
B. UEFI
C. MSM
D. PAM

**Correct Answer:** C

**QUESTION 183**
A security technician is testing a solution that will prevent outside entities from spoofing the company's email domain, which is comptia.org. The testing is successful, and the security technician is prepared to fully implement the solution. Which of the following actions should the technician take to accomplish this task?

A. Add TXT @ "v=spf1 mx include:_spf.comptiA.org all" to the DNS record.
B. Add TXT @ "v=spf1 mx include:_spf.comptiA.org all" to the email server.
C. Add TXT @ "v=spf1 mx include:_spf.comptiA.org +all" to the domain controller.
D. Add TXT @ "v=spf1 mx include:_spf.comptiA.org +all" to the web server.

**Correct Answer:** A

**QUESTION 184**
A security analyst is evaluating two vulnerability management tools for possible use in an