Naveen:

1.

Microsoft Intune and Defender for Endpoint (Soto, 2023) provide a number of features that can help you to manage and secure a variety of Windows endpoint devices, regardless of their age or operating system version.

1. Use security baselines

Security baselines are predefined sets of security configurations that can be applied to devices to help protect them from common threats. Microsoft provides a number of security baselines for different Windows operating systems and versions, and you can also create your own custom baselines.

To apply a security baseline to devices using Intune, go to Endpoint security > Security baselines. Then, select the baseline that you want to apply and click Create profile. In the Create profile pane, specify the devices that you want to apply the baseline to and click Create.

2. Use attack surface reduction (ASR) rules

ASR rules are advanced security configurations that can help to reduce the attack surface of your devices and make them less vulnerable to attack. Microsoft provides a number of pre-configured ASR rules, and you can also create your own custom rules.

To deploy ASR rules to devices using Intune, go to Endpoint security > Attack surface reduction. Then, select the rule that you want to deploy and click Create profile. In the Create profile pane, specify the devices that you want to deploy the rule to and click Create.

3. Use device compliance policies

Device compliance policies allow you to define the security requirements that devices must meet in order to access your corporate resources. You can use device compliance policies to enforce the use of security baselines, ASR rules, and other security settings.

To create a device compliance policy, go to Compliance > Policies > Create policy. In the Create policy pane, select Device compliance and click Create. Then, specify the security requirements that you want devices to meet and click Create.

4. Use conditional access

Conditional access allows you to control whether devices can access your corporate resources based on a variety of factors, such as the device's operating system version, security posture, and location.

To use conditional access to control access to corporate resources, go to Azure Active Directory > Security > Conditional access. Then, create a new conditional access policy and specify the conditions that devices must meet in order to access corporate resources.

Intune and Defender for Endpoint can also be used to manage and secure other types of endpoints, such as macOS devices, Android devices, and iOS devices.

Intext citation:

"Microsoft Intune and Defender for Endpoint provide a number of features that can help you to manage and secure a variety of Windows endpoint devices, regardless of their age or operating system version." (Soto, 2023)

Citation:

Soto, S. (2023). Hardening clients with microsoft Intune and defender for endpoint. Tech Community. <https://techcommunity.microsoft.com/t5/security-compliance-and-identity/hardening-windows-clients-with-microsoft-intune-and-defender-for/ba-p/3807378>

2. "Microsoft Defender for Endpoint automatically investigates all the incidents' supported events and suspicious entities in the alerts, providing you with auto response and information about the important files, processes, services, and more." (Microsoft, 2023). To find evidence of system changes on an endpoint, you can start by looking at the following:

* Event logs: Event logs contain information about all of the events that have occurred on a system, including system changes. You can view event logs using the Event Viewer tool.
* Security logs: Security logs contain information about all of the security-related events that have occurred on a system, including system changes made by malicious actors. You can view security logs using the Security Event Log Viewer tool.
* System Restore points: System Restore points are snapshots of the system state at a specific point in time. You can use System Restore to restore the system to a previous point in time if it becomes compromised.

Specifically, you can look for the following in the event logs:

* Events that indicate that files modification.
* Events that indicate that registry keys modification.
* Events that indicate that system settings modification.

To find evidence of system changes through the command line, you can use the following commands:

* eventquery: This command allows you to query event logs for specific events.
* Get-WinEvent: This cmdlet allows you to query event logs for specific events using PowerShell.
* wevtutil: This command-line tool allows you to manage event logs.

Once you have identified the events related to system changes, you can investigate them further to determine when the machine was possibly compromised. For example, you can look for events that indicate that new files were created or modified, or that new registry keys were created. You can also look for events that indicate that system settings were changed.

Citation:

Microsoft. (2023). Investigate incidents in microsoft defender for endpoint. Microsoft. <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/investigate-incidents?view=o365-worldwide>

3. Microsoft has moved server certification to the Azure platform (Microsoft, 2016). it's move to Azure for all server instances will likely increase the usage of the MS CLI, as it is the primary tool for managing Azure resources. The MS CLI is available for both Windows and Linux, so users will not need to learn new skills to use it in the cloud.

They made the decision to use a Linux subshell in the MS CLI. Which will likely increase the demand for Linux skills among users who are currently PowerShell proficient. However, the MS CLI will continue to support PowerShell commands, so users will not need to completely abandon PowerShell.

Overall, Microsoft's move to Azure and Linux will likely have a positive impact on MS CLI usage. The MS CLI is a powerful tool for managing Azure resources, and the move to Linux will make it more accessible to a wider range of users.

Citation:

Microsoft (2016/12/05). Azure and linux: a match made in hybrid cloud to deliver innovation options to aussie developers. (Microsoft News Center). <https://news.microsoft.com/en-au/2016/12/05/azure-and-linux-a-match-made-in-hybrid-cloud-to-deliver-innovation-options-to-aussie-developers/>

Bindu F

1.

To handle the various MS endpoint varieties that you may be exposed to, you should:

* Identify the different endpoint varieties that you need to support. This includes identifying the different operating systems, versions, and architectures of the devices that you need to manage
* Develop a plan for how you will support each endpoint variety. This may involve developing different policies and profiles for different types of devices.

For example, you may need to develop different security policies for devices that are running different versions of Windows.

* Test your plan to ensure that it works as expected. You can use tools such as Microsoft Endpoint Manager to test your policies and profiles on different devices (Microsoft,2023).

Microsoft. (2023). Endpoint management documentation.Microsoft.com <https://learn.microsoft.com/en-us/mem/>

2.

In the early 2010s, Endpoint Detection and Response (EDR) emerged as a crucial solution to counter the escalating complexity and volume of cyber threats confronting organizations (Cyborg Security, 2023). To discern signs of system alterations on an endpoint, crucial areas to investigate include event logs, security logs, and System Restore points. Event logs encompass a comprehensive record of system events, offering insights into system changes. The Security logs, specifically tailored for security-related events, aid in identifying alterations made by potential malicious actors. Furthermore, System Restore points serve as snapshots of the system state at specific times, enabling restoration to a previous secure state if needed.

For command-line analysis of system changes, essential commands include "eventquery" for targeted event log inquiries and "Get-WinEvent" cmdlet in PowerShell for precise event log querying. Additionally, "wevtutil," a versatile command-line tool, facilitates efficient management of event logs. Following the identification of events associated with system modifications, a thorough investigation can help pinpoint potential compromises, examining events indicative of new file or registry key creation, as well as alterations in system settings.

Cyborg Security. (2023). Edr: endpoint detection and response. Security Boulevard. <https://securityboulevard.com/2023/01/edr-endpoint-detection-and-response/>

3. Microsoft's move to Azure for all server instances is likely to increase the usage of the Azure CLI, as it is the cross-platform command-line tool for managing Azure resources. This is because the Azure CLI offers the same commands on all platforms, including Windows, Linux, and Mac. This will make it easier for administrators to manage Azure resources, regardless of their platform of choice.

However, Microsoft's move to using a Linux subshell versus PowerShell will affect those who are currently PowerShell proficient but lacking in Linux skills. This is because the Linux subshell provides access to a different set of commands and tools than PowerShell. This may require administrators to learn new commands and tools in order to manage their Azure resources.

Overall, the impact of Microsoft's move to Azure for all server instances on MS CLI usage and those who are currently PowerShell proficient but may be lacking in Linux skills is likely to be mixed. The Azure CLI is likely to become more popular, as it is the cross-platform command-line tool for managing Azure resources. However, those who are currently PowerShell proficient but may be lacking in Linux skills may need to learn new commands and tools in order to manage their Azure resources.

Microsoft. (2023). Azure command-line interface (cli) documentation. Microsoft.com. <https://learn.microsoft.com/en-us/cli/azure/>

Bindu

1.

Handling the diverse array of Microsoft (MS) endpoint varieties is a crucial challenge for anyone in the field of computer science, especially for recent graduates like myself. Firstly, staying informed and continuously learning about the evolution of MS operating systems is essential. This includes following tech news, subscribing to relevant online communities, and engaging in continued education programs.

Understanding the different versions of Windows (Pcmag,2023) is vital. Familiarity with legacy systems like Windows 98/XP/2000 and contemporary ones like Windows 10 and 11 is necessary. Learning to navigate, troubleshoot, and manage these versions through hands-on experience is invaluable.

Additionally, gaining proficiency in virtualization technologies is beneficial. Utilizing virtual machines allows us to simulate various Windows environments for testing and experimentation without needing physical hardware. This can aid in understanding the nuances and challenges associated with each version.

Collaborating with peers and mentors is also key. Joining professional groups or forums enables knowledge sharing and exposure to real-world scenarios, further enhancing our skills in managing diverse MS endpoints.

Citation:

Pcmag. (2023). Windows versions. PCmag.com. <https://www.pcmag.com/encyclopedia/term/windows-versions>

2. To look for evidence of system changes on an endpoint, you can start by looking at the Windows Event Logs and Firewall Logs (Willems, 2018). These logs contain detailed information about all system activity, including changes to files, folders, and settings.

To view the Windows Event Logs, you can use the Event Viewer application.

To view the Firewall Logs, you can use the Windows Firewall Control Panel.

Specifically, you should look for events that indicate that files were created, modified, or deleted, or that settings were changed. You should also look for events that indicate that there was network activity that is unusual or suspicious.

To find out what changes occurred and when using the command line, you can use the following command:

wevtutil el /f:"\*%SystemRoot%\System32\winevt\Logs\System.evtx"

This command will list all of the events in the System log, including the date and time of each event.

You can also use the following command to filter the results and only show events that indicate that files were created, modified, or deleted:

wevtutil el /f:"\*%SystemRoot%\System32\winevt\Logs\System.evtx" /q:"(EventID=11459 OR EventID=11460 OR EventID=11461)"

This command will only show events with the EventIDs 11459, 11460, or 11461, which are the EventIDs for file creation, modification, and deletion events.

Citation:

Willems, M. (2018). Recognize indicators of compromise with complete endpoint visibility. LogRhythm. <https://logrhythm.com/blog/integrated-threat-discovery-and-response-with-logrhythm-and-cylance-dashboard/>

3.

The move to Azure for all server instances is unlikely to have a significant impact on MS CLI usage, as the CLI is already widely used for managing Azure resources (Rothman, 2010). However, it may lead to increased demand for skills in managing Azure resources using the CLI, as well as skills in using the Linux subshell, which is used in the Azure CLI.

For those who are proficient in PowerShell but lacking in Linux skills, this move may present some challenges. However, there are a number of resources available to help users learn Linux, including online tutorials, books, and courses. Additionally, the Azure CLI provides a number of commands that are similar to PowerShell commands, making it easier for PowerShell users to learn the Azure CLI.

**Citation:**

Rothman, M. (2010). Esf: endpoint incident response. Securosis Research. <https://securosis.com/blog/esf-endpoint-incident-response>