Log Number	1	7
Category	6	1
	Provider Lifecycle	1
ComputerName	sandbox	1
EventCode	600	-
EventIdentifier	600	-
EventType	3	1
Logfile	Windows PowerShell	
Message	Provider "Variable" is Started.	
	Details: ProviderName=Variable NewProviderState=Started	
	SequenceNumber=11	
	HostName=ConsoleHost HostVersion=5.1.22621.169 HostId=0ed7b684-e68a-45c6-bc00-6b6d9f8a7161 HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=	
RecordNumber	4095	
SourceName	PowerShell	
TimeGenerated	2022-10-04T08:06:11.674531Z	
TimeWritten	2022-10-04T08:06:11.674531Z	
Туре	Information	
User	N/A	
Log Number	2	Ī

Log Number	3
User	N/A
Туре	Information
TimeWritten	2022-10-04T08:06:12.232165Z
TimeGenerated	2022-10-04T08:06:12.232165Z
SourceName	PowerShell
RecordNumber	4096
	ScriptName= CommandPath= CommandLine=
	CommandType= ScriptNamo-
	CommandName=
	PipelineId=
	RunspaceId=294ed587-7265-4bfa-bcf7-ba74259544cd
	EngineVersion=5.1.22621.169
	HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe
	HostVersion=5.1.22621.169 HostId=0ed7b684-e68a-45c6-bc00-6b6d9f8a7161
	HostName=ConsoleHost
	SequenceNumber=13
	PreviousEngineState=None
	NewEngineState=Available ProviousEngineState=None
	Details:
Message	Engine state is changed from None to Available.
Logfile	Windows PowerShell
EventType	3
EventIdentifier	400
EventCode	400
ComputerName	
CategoryString	Engine Lifecycle

12548

Category

CategoryString Special Logon ComputerName sandbox EventCode 4672 EventIdentifier 4672 EventType 4 Logfile Security Message Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeSecurityPrivilege SeLoadDriverPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeAuditPrivilege SeAuditPrivilege SeAuditPrivilege SeSeutityPrivilege SeSeutityPrivilege SeSeutityPrivilege SeNestorePrivilege SeNestorePrivilege SeNestorePrivilege SeNestorePrivilege SeSuppersonatePrivilege SeSeutityPrivilege SeSuppersonatePrivilege SeNestorePrivilege SeSuppersonatePrivilege SeSuppersonatePrivilege SeNestoreTrivilege SeVentile Privilege SeSuppersonatePrivilege SeVentile Privilege SeVentile Privil		
EventCode 4672 EventIdentifier 4672 EventType 4 Logfile Security Message Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeSecurityPrivilege SeSecurityPrivilege SeBackupPrivilege SeBackupPrivilege SeRestorePrivilege SeRestorePrivilege SeSystemEnvironmentPrivilege SeSystemEnvironmentPrivilege SeloplegateSessionUserImpersonatePrivilege RecordNumber 17079 SourceName Microsoft-Windows-Security-Auditing TimeGenerated 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category 0 CategoryString N/A	CategoryString	Special Logon
EventType 4 Logfile Security Message Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeSecurityPrivilege SeSecurityPrivilege SeBackupPrivilege SeRestorePrivilege SeRestorePrivilege SeAuditPrivilege SeAuditPrivilege SeAuditPrivilege SeSuppersonatePrivilege SeUppersonatePrivilege SeUpperso	ComputerName	sandbox
EventType 4 Logfile Security Message Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeSecurityPrivilege SeLoadDriverPrivilege SeRackupPrivilege SeRestorePrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeImpersonatePrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege RecordNumber 17079 SourceName Microsoft-Windows-Security-Auditing TimeGenerated 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category 0 CategoryString N/A	EventCode	4672
Logfile Security Message Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeSecurityPrivilege SeSecurityPrivilege SeBackupPrivilege SeBackupPrivilege SeRestorePrivilege SePestorePrivilege SePebugPrivilege SeSystemEnvironmentPrivilege SelmpersonatePrivilege SelpegateSessionUserImpersonatePrivilege SeDebugAtiPrivilege SeVerentary SelpegateSessionUserImpersonatePrivilege RecordNumber 17079 SourceName Microsoft-Windows-Security-Auditing TimeGenerated 2022-10-05T02:53:54.702543Z TimeWritten 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category O CategoryString N/A	EventIdentifier	4672
Message Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeSecurityPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SePabugPrivilege SePabugPrivilege SePabugPrivilege SeSystemEnvironmentPrivilege SeSystemEnvironmentPrivilege SeDelegateSessionUserImpersonatePrivilege RecordNumber 17079 SourceName Microsoft-Windows-Security-Auditing TimeGenerated 2022-10-05T02:53:54.702543Z TimeWritten 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category O CategoryString N/A	EventType	4
Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeSecurityPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeBackupPrivilege SePastorePrivilege SePauditPrivilege SePauditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeblegateSessionUserImpersonatePrivilege RecordNumber 17079 SourceName Microsoft-Windows-Security-Auditing TimeGenerated 2022-10-05T02:53:54.702543Z TimeWritten 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category 0 CategoryString	Logfile	Security
Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeBackupPrivilege SeBackupPrivilege SeBackupPrivilege SeBackupPrivilege SePebpugPrivilege SeSystemEnvironmentPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege RecordNumber 17079 SourceName Microsoft-Windows-Security-Auditing TimeGenerated 2022-10-05T02:53:54.702543Z TimeWritten 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category 0 CategoryString N/A	Message	Special privileges assigned to new logon.
Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeSecurityPrivilege SeIakeOwnershipPrivilege SeBackupPrivilege SeBackupPrivilege SeBackupPrivilege SeBackupPrivilege SePebpugPrivilege SeSystemEnvironmentPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege RecordNumber 17079 SourceName Microsoft-Windows-Security-Auditing TimeGenerated 2022-10-05T02:53:54.702543Z TimeWritten 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category 0 CategoryString N/A		
Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeBackupPrivilege SeBackupPrivilege SeBackupPrivilege SeBackupPrivilege SePebpugPrivilege SeSystemEnvironmentPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege RecordNumber 17079 SourceName Microsoft-Windows-Security-Auditing TimeGenerated 2022-10-05T02:53:54.702543Z TimeWritten 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category 0 CategoryString N/A		Subject
Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeBackupPrivilege SeBackupPrivilege SeBackupPrivilege SeBackupPrivilege SePauditPrivilege SePauditPrivilege SeSystemEnvironmentPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege RecordNumber 17079 SourceName Microsoft-Windows-Security-Auditing TimeGenerated 2022-10-05T02:53:54.702543Z TimeWritten 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category 0 CategoryString N/A		
Logon ID: 0x3E7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeSecurityPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeBackupPrivilege SeRestorePrivilege SeAuditPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege RecordNumber 17079 SourceName Microsoft-Windows-Security-Auditing TimeGenerated 2022-10-05T02:53:54.702543Z TimeWritten 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category 0 CategoryString N/A		
Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeSecurityPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege RecordNumber 17079 SourceName Microsoft-Windows-Security-Auditing TimeGenerated 2022-10-05T02:53:54.702543Z TimeWritten 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category 0 CategoryString N/A		Account Domain: NT AUTHORITY
SeTcbPrivilege SeSecurityPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeBackupPrivilege SeRestorePrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SelmpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege RecordNumber 17079 SourceName Microsoft-Windows-Security-Auditing TimeGenerated 2022-10-05T02:53:54.702543Z TimeWritten 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category 0 CategoryString N/A		Logon ID: 0x3E7
SeTcbPrivilege SeSecurityPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeBackupPrivilege SeRestorePrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SelmpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege RecordNumber 17079 SourceName Microsoft-Windows-Security-Auditing TimeGenerated 2022-10-05T02:53:54.702543Z TimeWritten 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category 0 CategoryString N/A		
SeTcbPrivilege SeSecurityPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeBackupPrivilege SeRestorePrivilege SePebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SelmpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege RecordNumber 17079 SourceName Microsoft-Windows-Security-Auditing TimeGenerated 2022-10-05T02:53:54.702543Z TimeWritten 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category 0 CategoryString N/A		Privileges: SeAssignPrimaryTokenPrivilege
SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeRestorePrivilege SeDebugPrivilege SeDebugPrivilege SeSudditPrivilege SeSystemEnvironmentPrivilege SelmpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege RecordNumber 17079 SourceName Microsoft-Windows-Security-Auditing TimeGenerated 2022-10-05T02:53:54.702543Z TimeWritten 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category 0 CategoryString N/A		
SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SePebugPrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SelmpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege RecordNumber 17079 SourceName Microsoft-Windows-Security-Auditing TimeGenerated 2022-10-05T02:53:54.702543Z TimeWritten 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category 0 CategoryString N/A		
SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege RecordNumber 17079 SourceName Microsoft-Windows-Security-Auditing TimeGenerated 2022-10-05T02:53:54.702543Z TimeWritten 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category 0 CategoryString N/A		SeTakeOwnershipPrivilege
SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege RecordNumber 17079 SourceName Microsoft-Windows-Security-Auditing TimeGenerated 2022-10-05T02:53:54.702543Z TimeWritten 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category 0 CategoryString N/A		
SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege RecordNumber 17079 SourceName Microsoft-Windows-Security-Auditing TimeGenerated 2022-10-05T02:53:54.702543Z TimeWritten 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category 0 CategoryString N/A		
SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege RecordNumber 17079 SourceName Microsoft-Windows-Security-Auditing TimeGenerated 2022-10-05T02:53:54.702543Z TimeWritten 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category 0 CategoryString N/A		- Control of the cont
SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege RecordNumber 17079 SourceName Microsoft-Windows-Security-Auditing TimeGenerated 2022-10-05T02:53:54.702543Z TimeWritten 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category 0 CategoryString N/A		
SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege RecordNumber 17079 SourceName Microsoft-Windows-Security-Auditing TimeGenerated 2022-10-05T02:53:54.702543Z TimeWritten 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category 0 CategoryString N/A		
SeDelegateSessionUserImpersonatePrivilege RecordNumber 17079 SourceName Microsoft-Windows-Security-Auditing TimeGenerated 2022-10-05T02:53:54.702543Z TimeWritten 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category 0 CategoryString N/A		
SourceName Microsoft-Windows-Security-Auditing TimeGenerated 2022-10-05T02:53:54.702543Z TimeWritten 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category 0 CategoryString N/A		
TimeGenerated 2022-10-05T02:53:54.702543Z TimeWritten 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category 0 CategoryString N/A	RecordNumber	17079
TimeWritten 2022-10-05T02:53:54.702543Z Type Audit Success User N/A Log Number 4 Category 0 CategoryString N/A	SourceName	Microsoft-Windows-Security-Auditing
Type Audit Success User N/A Log Number 4 Category 0 CategoryString N/A	TimeGenerated	2022-10-05T02:53:54.702543Z
User N/A Log Number 4 Category 0 CategoryString N/A	TimeWritten	2022-10-05T02:53:54.702543Z
Log Number 4 Category 0 CategoryString N/A	Туре	Audit Success
Category 0 CategoryString N/A	User	N/A
CategoryString N/A	Log Number	4
	Category	0
ComputerName sandbox	CategoryString	N/A
	ComputerName	sandbox

EventCode	16394
EventIdentifier	-1073725430
EventType	3
Logfile	Application
Message	Offline downlevel migration succeeded.
RecordNumber	7422
SourceName	Microsoft-Windows-Security-SPP
TimeGenerated	2022-10-05T02:53:56.774261Z
TimeWritten	2022-10-05T02:53:56.774261Z
Туре	Information
User	N/A

Log Number	5
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3
Logfile	Windows PowerShell
Message	Provider "Registry" is Started.
	Details:
	ProviderName=Registry
	NewProviderState=Started
	SequenceNumber=1
	HostName=ConsoleHost
	HostVersion=5.1.22621.169
	HostId=4cea8f63-8b91-448c-b01c-64f1cdac22da
	HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe
	EngineVersion=
	RunspaceId=
	PipelineId=

CommandName= CommandType= ScriptName= CommandLine= RecordNumber 4246 SourceName PowerShell TimeGenerated 2022-10-05T02:54:37.588841Z TimeWritten 2022-10-05T02:54:37.588841Z Type Information User N/A Log Number 6 Category 6 Category 6 Category Frovider Lifecycle ComputerName sandbox EventCode 600 EventIdentifier 600 EventType 3 Logfile Windows PowerShell Message Provider "Function" is Started. Details: ProviderName=Function NewProviderState=Started SequenceNumber=9			
CommandLine= RecordNumber 4246 SourceName PowerShell TimeGenerated 2022-10-05T02:54:37.588841Z TimeWritten 2022-10-05T02:54:37.588841Z Type Information User N/A Log Number 6 Category 6 Category 6 CategoryString Provider Lifecycle ComputerName sandbox EventCode 600 EventIdentifier 600 EventType 3 Logfile Windows PowerShell Message Provider "Function" is Started. Details: ProviderName=Function NewProviderState=Started		CommandType= ScriptName=	
SourceName PowerShell TimeGenerated 2022-10-05T02:54:37.588841Z TimeWritten 2022-10-05T02:54:37.588841Z Type Information User N/A Log Number 6 Category 6 Category Frovider Lifecycle ComputerName sandbox EventCode 600 EventIdentifier 600 EventType 3 Logfile Windows PowerShell Message Provider "Function" is Started. Details: ProviderName=Function NewProviderState=Started			
TimeGenerated 2022-10-05T02:54:37.588841Z TimeWritten 2022-10-05T02:54:37.588841Z Type Information User N/A Log Number 6 Category 6 Category Provider Lifecycle ComputerName sandbox EventCode 600 EventIdentifier 600 EventType 3 Logfile Windows PowerShell Message Provider "Function" is Started. Details: ProviderName=Function NewProviderState=Started	RecordNumber	4246	1
TimeWritten 2022-10-05T02:54:37.588841Z Type Information User N/A Log Number 6 Category 6 CategoryString Provider Lifecycle ComputerName sandbox EventCode 600 EventIdentifier 600 EventType 3 Logfile Windows PowerShell Message Provider "Function" is Started. Details: ProviderName=Function NewProviderState=Started	SourceName	PowerShell	
Type Information User N/A Log Number 6 Category 6 CategoryString Provider Lifecycle ComputerName sandbox EventCode 600 EventIdentifier 600 EventType 3 Logfile Windows PowerShell Message Provider "Function" is Started. Details: ProviderName=Function NewProviderState=Started	TimeGenerated	2022-10-05T02:54:37.588841Z	
User N/A Log Number 6 Category 6 CategoryString Provider Lifecycle ComputerName sandbox EventCode 600 EventIdentifier 600 EventType 3 Logfile Windows PowerShell Message Provider "Function" is Started. Details: ProviderName=Function NewProviderState=Started	TimeWritten	2022-10-05T02:54:37.588841Z	
Log Number 6 Category 6 CategoryString Provider Lifecycle ComputerName sandbox EventCode 600 EventIdentifier 600 EventType 3 Logfile Windows PowerShell Message Provider "Function" is Started. Details: ProviderName=Function NewProviderState=Started	Туре	Information	
Category CategoryString Provider Lifecycle ComputerName sandbox EventCode 600 EventIdentifier 600 EventType 3 Logfile Windows PowerShell Message Provider "Function" is Started. Details: ProviderName=Function NewProviderState=Started	User	N/A	
CategoryString Provider Lifecycle ComputerName sandbox EventCode 600 EventIdentifier 600 EventType 3 Logfile Windows PowerShell Message Provider "Function" is Started. Details: ProviderName=Function NewProviderState=Started	Log Number	6	
ComputerName sandbox EventCode 600 EventIdentifier 600 EventType 3 Logfile Windows PowerShell Message Provider "Function" is Started. Details: ProviderName=Function NewProviderState=Started	Category	6	
EventCode 600 EventType 3 Logfile Windows PowerShell Message Provider "Function" is Started. Details: ProviderName=Function NewProviderState=Started	CategoryString	Provider Lifecycle	
EventType 3 Logfile Windows PowerShell Message Provider "Function" is Started. Details: ProviderName=Function NewProviderState=Started	ComputerName	sandbox	
EventType 3 Logfile Windows PowerShell Message Provider "Function" is Started. Details: ProviderName=Function NewProviderState=Started	EventCode	600	
Logfile Windows PowerShell Message Provider "Function" is Started. Details: ProviderName=Function NewProviderState=Started	EventIdentifier	600	
Message Provider "Function" is Started. Details: ProviderName=Function NewProviderState=Started	EventType	3	
Details: ProviderName=Function NewProviderState=Started	Logfile	Windows PowerShell	
ProviderName=Function NewProviderState=Started	Message	Provider "Function" is Started.	
NewProviderState=Started		Details:	
SequenceNumber=9		NewProviderState=Started	
		SequenceNumber=9	
HostName=ConsoleHost HostVersion=5.1.22621.169			
HostId=4cea8f63-8b91-448c-b01c-64f1cdac22da			
		HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe)
EngineVersion=			
RunspaceId= PipelineId=			
CommandName=	1	i ipointoid-	

		_
	CommandType= ScriptName= CommandPath= CommandLine=	
RecordNumber		
SourceName	PowerShell	
TimeGenerated	2022-10-05T02:54:37.599284Z	
TimeWritten	2022-10-05T02:54:37.599284Z	1
Туре	Information	1
User	N/A	
Log Number	7	Ī
Category	6	
CategoryString	Provider Lifecycle	
ComputerName	sandbox	1
EventCode	600	1
EventIdentifier	600	
EventType	3	
Logfile	Windows PowerShell	
Message	Provider "Registry" is Started.	
	Details: ProviderName=Registry NewProviderState=Started SequenceNumber=1	
	HostName=ConsoleHost HostVersion=5.1.22621.169 HostId=cd635701-06a7-4607-8626-f422cd2a174b HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType=	:

	_
ScriptName=	
CommandPath=	
CommandLine=	
4253	
PowerShell	
2022-10-05T02:58:07.36052Z	
2022-10-05T02:58:07.36052Z	
Information	
N/A	
8	Ī
6	
Provider Lifecycle	
sandbox	
600	
600	
3	
Windows PowerShell	
Provider "Alias" is Started.	
D. (4.9).	
NewProviderState=Started	
SequenceNumber=3	
HostName=ConsoleHost	
EngineVersion=	
RunspaceId=	
PipelineId=	
CommandName=	
CommandType=	
ScriptName=	
	CommandPath= CommandLine= 4253 PowerShell 2022-10-05T02:58:07.36052Z 2022-10-05T02:58:07.36052Z Information N/A B B G Provider Lifecycle sandbox 500 500 500 3 Windows PowerShell Provider "Alias" is Started. Details: ProviderName=Alias NewProviderState=Started SequenceNumber=3 HostName=ConsoleHost HostVersion=5.1.22621.169 HostId=cd635701-06a7-4607-8626-f422cd2a174b HostApplication=C:\WiNDOWS\System32\WindowsPowerShell\v1.0\powershell.exe Engine Version= Engine Ve

	CommandPath=	
	CommandLine=	-
RecordNumber	4254	
SourceName	PowerShell	
TimeGenerated	2022-10-05T02:58:07.361018Z	
TimeWritten	2022-10-05T02:58:07.361018Z	
Туре	Information	
User	N/A	
Log Number	9	
Category	6	
CategoryString	Provider Lifecycle	
ComputerName	sandbox	
EventCode	600	
EventIdentifier	600	
EventType	3	
Logfile	Windows PowerShell	
Message	Provider "Function" is Started.	
	Details:	
	ProviderName=Function NewProviderState=Started	
	SequenceNumber=9	
	HostName=ConsoleHost	
	HostVersion=5.1.22621.169	
	HostId=cd635701-06a7-4607-8626-f422cd2a174b	
	HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe	
	EngineVersion=	
	RunspaceId=	
	PipelineId= CommandName=	
	CommandType=	
	ScriptName=	
	CommandPath=	

	CommandLine=
RecordNumber	4257
SourceName	PowerShell
TimeGenerated	2022-10-05T02:58:07.401071Z
TimeWritten	2022-10-05T02:58:07.401071Z
Туре	Information
User	N/A

Туре	Information
User	N/A
Log Number	10
Category	12544
CategoryString	Logon
ComputerName	sandbox
EventCode	4624
EventIdentifier	4624
EventType	4
Logfile	Security
Message	An account was successfully logged on.
	Subject: Security ID: S-1-5-18 Account Name: SANDBOX\$
	Account Name: SANDBOA\$ Account Domain: WORKGROUP
	Logon ID: 0x3E7
	Logon Information: Logon Type: 5 Restricted Admin Mode: - Remote Credential Guard: - Virtual Account: No Elevated Token: Yes
	Impersonation Level: Impersonation
	New Logon:

Security ID: S-1-5-18

Account Name: SYSTEM

Account Domain: NT AUTHORITY

Logon ID: 0x3E7
Linked Logon ID: 0x0
Network Account Name: Network Account Domain: -

Process Information: Process ID: 0x304

Process Name: C:\Windows\System32\services.exe

Network Information: Workstation Name: -

Source Network Address: -

Source Port: -

Detailed Authentication Information:

Logon Process: Advapi

Authentication Package: Negotiate

Transited Services: -

Package Name (NTLM only): -

Key Length: 0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

The New Logon fields indicate the account for whom the new logon was

	created, i.e. the account that was logged on.
	The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.
	The impersonation level field indicates the extent to which a process in the logon session can impersonate.
	The authentication information fields provide detailed information about this specific logon request.
	 Logon GUID is a unique identifier that can be used to correlate this event with a KDC event.
	- Transited services indicate which intermediate services have participated in
	this logon request Package name indicates which sub-protocol was used among the NTLM protocols.
	- Key length indicates the length of the generated session key. This will be 0 if
	no session key was requested.
RecordNumber	17318
SourceName	Microsoft-Windows-Security-Auditing
TimeGenerated	2022-10-05T15:57:05.586776Z
TimeWritten	2022-10-05T15:57:05.586776Z
Туре	Audit Success
User	N/A
Log Number	11
Category	0
CategoryString	N/A
ComputerName	sandbox
EventCode	10016
EventIdentifier	10016
EventType	2
Logfile	System
Message	The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID

	{2593F8B9-4EAF-457C-B68A-50F6B8EA6B54} and APPID {15C20B67-12E7-4BB6-92BB-7AFF07997402} to the user sandbox\guru SID (S-1-5-21-3249831223-3918070856- 2126610958-1001) from address LocalHost (Using LRPC) running in the application container Unavailable SID (Unavailable). This security permission
Doggard Normale and	can be modified using the Component Services administrative tool.
	7205 Microsoft-Windows-DistributedCOM
SourceName	2022-10-05T16:38:37.724846Z
TimeWritten	2022-10-05T16:38:37.724846Z 2022-10-05T16:38:37.724846Z
Type User	Warning sandbox\quru
	sandbox\guru
Log Number	12
Category	12292
CategoryString	Other System Events
ComputerName	
EventCode	5058
EventIdentifier	5058
EventType	4
Logfile	Security
Message	Key file operation. Subject: Security ID: S-1-5-21-3249831223-3918070856-2126610958-1001 Account Name: guru Account Domain: sandbox Logon ID: 0xC7B7D6A
	Process Information: Process ID: 14592 Process Creation Time: ?2022?-?10?-?05T11:08:37.273091600Z Cryptographic Parameters: Provider Name: Microsoft Software Key Storage Provider

Algorithm Name: ECDSA_P256
Key Name: Microsoft-Edge-TB-test-key
Key Type: User key.
Key File Operation Information:
File Path:
C:\Users\guru\AppData\Roaming\Microsoft\Crypto\Keys\53caafca80232173a709de019
f770-4829-8e8b-55f975dac4a9
Operation: Delete key file.
Return Code: 0x0
17335
Microsoft-Windows-Security-Auditing
2022-10-05T16:38:40.787809Z
2022-10-05T16:38:40.787809Z
Audit Success
N/A
13
6
Provider Lifecycle
sandbox
600
600
3
Windows PowerShell
Provider "Alias" is Started.
Details:
ProviderName=Alias NewProviderState=Started
NewProviderState=Started
SequenceNumber=3
Gequencer variber = 0
HostName=ConsoleHost
HostVersion=5.1.22621.169

	HostId=0ed7b684-e68a-45c6-bc00-6b6d9f8a7161
	HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe
	EngineVersion=
	RunspaceId=
	PipelineId=
	CommandName=
	CommandType=
	ScriptName=
	CommandPath=
	CommandLine=
RecordNumber	4091
SourceName	PowerShell
TimeGenerated	2022-10-04T08:06:11.653928Z
TimeWritten	2022-10-04T08:06:11.653928Z
Туре	Information
User	N/A
Log Number	14
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3
Logfile	Windows PowerShell
Message	Provider "Environment" is Started.
	Details:
	ProviderName=Environment NewProviderState=Started
	NewProviderState=Started
	SequenceNumber=5
	HostName=ConsoleHost
	HostVersion=5.1.22621.169
	HostId=0ed7b684-e68a-45c6-bc00-6b6d9f8a7161

	HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe
	EngineVersion=
	RunspaceId=
	PipelineId=
	CommandName=
	CommandType=
	ScriptName= CommandPath=
	CommandLine=
RecordNumber	
SourceName	PowerShell
TimeGenerated	2022-10-04T08:06:11.655681Z
TimeWritten	2022-10-04T08:06:11.655681Z
Туре	Information
User	N/A
Log Number	15
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3
Logfile	Windows PowerShell
Message	Provider "FileSystem" is Started.
	Details:
	ProviderName=FileSystem
	NewProviderState=Started
	SequenceNumber=7
	HeatNema Canada Heat
	HostVersion=5.1.23621.160
	HostVersion=5.1.22621.169 HostId=0ed7b684-e68a-45c6-bc00-6b6d9f8a7161
	HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe
	Trock (pphoditori—0.///////DOV/0/oterrioz///////////////////////////////////

	EngineVersion=]
	RunspaceId=	
	PipelineId=	
	CommandName=	
	CommandType=	
	ScriptName=	
	CommandPath=	
	CommandLine=	
RecordNumber	4093	
SourceName	PowerShell	
TimeGenerated	2022-10-04T08:06:11.671192Z	
TimeWritten	2022-10-04T08:06:11.671192Z	
Туре	Information	
User	N/A	

0001	1.77
Log Number	16
Category	12544
CategoryString	Logon
ComputerName	sandbox
EventCode	4624
EventIdentifier	4624
EventType	4
Logfile	Security
Message	An account was successfully logged on.
	Subject:
	Security ID: S-1-5-18
	Account Name: SANDBOX\$
	Account Domain: WORKGROUP
	Logon ID: 0x3E7
	Logon Information:
	Logon Type: 5
	Restricted Admin Mode: -
	Remote Credential Guard: -
	Virtual Account: No
	Elevated Token: Yes

Impersonation Level: Impersonation

New Logon:

Security ID: S-1-5-18

Account Name: SYSTEM

Account Domain: NT AUTHORITY

Logon ID: 0x3E7
Linked Logon ID: 0x0
Network Account Name: Network Account Domain: -

Process Information: Process ID: 0x304

Process Name: C:\Windows\System32\services.exe

Network Information:

Workstation Name: -

Source Network Address: -

Source Port: -

Detailed Authentication Information:

Logon Process: Advapi

Authentication Package: Negotiate

Transited Services: -

Package Name (NTLM only): -

Key Length: 0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.

The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.

The impersonation level field indicates the extent to which a process in the logon session can impersonate.

The authentication information fields provide detailed information about this specific logon request.

- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event.
- Transited services indicate which intermediate services have participated in this logon request.
- Package name indicates which sub-protocol was used among the NTLM protocols.
- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

	, ,
RecordNumber	17080
SourceName	Microsoft-Windows-Security-Auditing
TimeGenerated	2022-10-05T02:53:54.924526Z
TimeWritten	2022-10-05T02:53:54.924526Z
Туре	Audit Success
User	N/A

Log Number	17
Category	12548
CategoryString	Special Logon
ComputerName	sandbox

Log Number	18
User	N/A
Туре	Audit Success
TimeWritten	2022-10-05T02:53:54.924539Z
TimeGenerated	2022-10-05T02:53:54.924539Z
SourceName	Microsoft-Windows-Security-Auditing
RecordNumber	17081
	SeDelegateSessionUserImpersonatePrivilege
	SeImpersonatePrivilege
	SeSystemEnvironmentPrivilege
	SeAuditPrivilege
	SeDebugPrivilege
	SeBackupPrivilege SeRestorePrivilege
	SeLoadDriverPrivilege SeRoekupPrivilege
	SeTakeOwnershipPrivilege
	SeSecurityPrivilege
	SeTcbPrivilege
	Privileges: SeAssignPrimaryTokenPrivilege
	Logon ID: 0x3E7
	Account Domain: NT AUTHORITY
	Account Name: SYSTEM
	Security ID: S-1-5-18
	Subject:
Message	Special privileges assigned to new logon.
Logfile	Security
EventType	4
EventIdentifier	4672
EventCode	4672

Log Number	18
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600

EventType	3
Logfile	Windows PowerShell
Message	Provider "Alias" is Started.
	Details:
	ProviderName=Alias
	NewProviderState=Started
	SequenceNumber=3
	HostName=ConsoleHost
	HostVersion=5.1.22621.169
	HostId=4cea8f63-8b91-448c-b01c-64f1cdac22da
	HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe
	EngineVersion= RunspaceId=
	PipelineId=
	CommandName=
	CommandType=
	ScriptName=
	CommandPath=
	CommandLine=
RecordNumber	4247
SourceName	PowerShell
TimeGenerated	2022-10-05T02:54:37.58953Z
TimeWritten	2022-10-05T02:54:37.58953Z
Туре	Information
User	N/A
Log Number	19
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3

Logfile	Windows PowerShell
Message	Provider "Variable" is Started.
	Details:
	ProviderName=Variable
	NewProviderState=Started
	SequenceNumber=11
	HostName=ConsoleHost
	HostVersion=5.1.22621.169
	HostId=4cea8f63-8b91-448c-b01c-64f1cdac22da
	HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion=
	RunspaceId=
	PipelineId=
	CommandName=
	CommandType=
	ScriptName= CommandPath=
	CommandLine=
RecordNumber	4251
SourceName	PowerShell
TimeGenerated	2022-10-05T02:54:37.600602Z
TimeWritten	2022-10-05T02:54:37.600602Z
Туре	Information
User	N/A
Log Number	20
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3
Logfile	Windows PowerShell

Message	Provider "Environment" is Started.
	Details:
	ProviderName=Environment
	NewProviderState=Started
	SequenceNumber=5
	HostName=ConsoleHost
	HostVersion=5.1.22621.169
	HostId=cd635701-06a7-4607-8626-f422cd2a174b
	HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion=
	RunspaceId=
	PipelineId=
	CommandName=
	CommandType=
	ScriptName=
	CommandPath= CommandLine=
RecordNumber	
SourceName	PowerShell
TimeGenerated	
TimeWritten	2022-10-05T02:58:07.361271Z
Туре	Information
User	N/A
Log Number	21
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3
Logfile	Windows PowerShell
Message	Provider "Variable" is Started.

	Details:
	ProviderName=Variable
	NewProviderState=Started
	SequenceNumber=11
	HostName=ConsoleHost
	HostVersion=5.1.22621.169
	HostId=cd635701-06a7-4607-8626-f422cd2a174b
	HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe
	EngineVersion=
	RunspaceId=
	PipelineId=
	CommandType
	CommandType= ScriptName=
	CommandPath=
	CommandLine=
RecordNumber	4258
SourceName	PowerShell
TimeGenerated	2022-10-05T02:58:07.403133Z
TimeWritten	2022-10-05T02:58:07.403133Z
Туре	Information
User	N/A
Log Number	22
Category	4
CategoryString	Engine Lifecycle
ComputerName	sandbox
EventCode	400
EventIdentifier	400
EventType	3
Logfile	Windows PowerShell
Message	Engine state is changed from None to Available.

		-
	Details:	
	NewEngineState=Available	
	PreviousEngineState=None	
	SequenceNumber=13	
	HostName=ConsoleHost	
	HostVersion=5.1.22621.169	
	HostId=cd635701-06a7-4607-8626-f422cd2a174b	
	HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe	:
	EngineVersion=5.1.22621.169	
	RunspaceId=40acef8c-09e8-431e-be19-d3ee00dd6498	
	PipelineId=	
	CommandName= CommandType=	
	ScriptName=	
	CommandPath=	
	CommandLine=	
RecordNumber	4259	1
SourceName	PowerShell	
TimeGenerated	2022-10-05T02:58:07.922265Z	
TimeWritten	2022-10-05T02:58:07.922265Z	
Туре	Information	
User	N/A	
Log Number	23	Ī
Category	6	
CategoryString	Provider Lifecycle	
ComputerName	sandbox	
EventCode	600	
EventIdentifier	600	
EventType	3	
Logfile	Windows PowerShell	
Message	Provider "Registry" is Started.	1

	Details:	7
	ProviderName=Registry	
	NewProviderState=Started	
	SequenceNumber_1	
	SequenceNumber=1	
	HostName=ConsoleHost	
	HostVersion=5.1.22621.169	
	HostId=0ed7b684-e68a-45c6-bc00-6b6d9f8a7161	
	HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe	
	EngineVersion=	
	RunspaceId=	
	PipelineId=	
	CommandName=	
	CommandType=	
	ScriptName=	
	CommandPath=	
	CommandLine=	
RecordNumber	4090	
SourceName	PowerShell	
TimeGenerated	2022-10-04T08:06:11.649372Z	
TimeWritten	2022-10-04T08:06:11.649372Z	
Туре	Information	
User	N/A	
Log Number	24	
Category	6	
CategoryString	Provider Lifecycle	
ComputerName	sandbox	
EventCode	600	
EventIdentifier	600	
EventType	3	
Logfile	Windows PowerShell	
Message	Provider "Function" is Started.	
	Details:	
	<u> </u>	<u>_</u>

	ProviderName=Function NewProviderState=Started	
	New Tovider Stated	
	SequenceNumber=9	
	HostName=ConsoleHost	
	HostVersion=5.1.22621.169	
	HostId=0ed7b684-e68a-45c6-bc00-6b6d9f8a7161	
	HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.	.exe
	EngineVersion=	
	RunspaceId= PipelineId=	
	CommandName=	
	CommandType=	
	ScriptName=	
	CommandPath=	
	CommandLine=	
RecordNumber	4094	
SourceName	PowerShell	
TimeGenerated	2022-10-04T08:06:11.672918Z	
TimeWritten	2022-10-04T08:06:11.672918Z	
Туре	Information	
User	N/A	
Log Number	25	
Category	100	
CategoryString	N/A	
ComputerName	sandbox	
EventCode	105	
EventIdentifier	105	
EventType	3	
Logfile	System	
Message	Power source change.	
RecordNumber	7112	
SourceName	Microsoft-Windows-Kernel-Power	
TimeGenerated	2022-10-05T02:53:53.526809Z	

TimeWritten	2022-10-05T02:53:53.526809Z
Туре	Information
User	NT AUTHORITY\SYSTEM
Log Number	26
Category	12544
CategoryString	Logon
ComputerName	sandbox
EventCode	4624
EventIdentifier	4624
EventType	4
Logfile	Security
Message	An account was successfully logged on.
	Subject: Security ID: S-1-5-18 Account Name: SANDBOX\$ Account Domain: WORKGROUP Logon ID: 0x3E7 Logon Information: Logon Type: 5 Restricted Admin Mode: - Remote Credential Guard: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation
	New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Linked Logon ID: 0x0 Network Account Name: -

Network Account Domain: -

Process Information: Process ID: 0x304

Process Name: C:\Windows\System32\services.exe

Network Information:

Workstation Name: -

Source Network Address: -

Source Port: -

Detailed Authentication Information:

Logon Process: Advapi

Authentication Package: Negotiate

Transited Services: -

Package Name (NTLM only): -

Key Length: 0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.

The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some

	cases.
	The impersonation level field indicates the extent to which a process in the logon session can impersonate.
	The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
RecordNumber	17078
SourceName	Microsoft-Windows-Security-Auditing
TimeGenerated	2022-10-05T02:53:54.702531Z
TimeWritten	2022-10-05T02:53:54.702531Z
Туре	Audit Success
User	N/A
Log Number	27
Category	0
CategoryString	N/A
ComputerName	sandbox
EventCode	15
EventIdentifier	15
EventType	3
Logfile	Application
Message	Updated Windows Defender status successfully to SECURITY_PRODUCT_STATE_ON.
RecordNumber	7421
SourceName	SecurityCenter
TimeGenerated	2022-10-05T02:53:55.800172Z
TimeWritten	2022-10-05T02:53:55.800172Z

Туре	Information
User	N/A
Log Number	28
Category	0
CategoryString	N/A
ComputerName	sandbox
EventCode	16384
EventIdentifier	1073758208
EventType	3
Logfile	Application
Message	Successfully scheduled Software Protection service for re-start at 2122-09-10T21:24:34Z. Reason: RulesEngine.
RecordNumber	7423
SourceName	Microsoft-Windows-Security-SPP
TimeGenerated	2022-10-05T02:54:34.880793Z
TimeWritten	2022-10-05T02:54:34.880793Z
Туре	Information
User	N/A
Log Number	29

Log Number	29
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3
Logfile	Windows PowerShell
Message	Provider "Environment" is Started.
	Details:
	ProviderName=Environment
	NewProviderState=Started
	SequenceNumber=5

HostName=ConsoleHost HostVersion=5.1.22621.169
10317 5131011-0. 1.2202 1. 103
HostId=4cea8f63-8b91-448c-b01c-64f1cdac22da
HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe
EngineVersion=
RunspaceId=
PipelineId=
CommandName=
CommandType= ScriptName=
CommandPath=
CommandLine=
PowerShell
2022-10-05T02:54:37.589936Z
2022-10-05T02:54:37.589936Z
nformation
N/A
30
3
Provider Lifecycle
sandbox
600
600
3
Windows PowerShell
Provider "FileSystem" is Started.
Details:
ProviderName=FileSystem
NewProviderState=Started

	HostName=ConsoleHost HostVersion=5.1.22621.169 HostId=4cea8f63-8b91-448c-b01c-64f1cdac22da HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType=
	ScriptName= CommandPath= CommandLine=
RecordNumber	
SourceName	PowerShell
TimeGenerated	2022-10-05T02:54:37.59774Z
TimeWritten	2022-10-05T02:54:37.59774Z
Туре	Information
User	N/A
Log Number	31
Category	4
CategoryString	Engine Lifecycle
ComputerName	sandbox
F	400
EventCode	400
EventIdentifier	400
EventIdentifier	400
EventIdentifier EventType	400 3
EventIdentifier EventType Logfile	400 3 Windows PowerShell
EventIdentifier EventType Logfile	400 3 Windows PowerShell Engine state is changed from None to Available. Details: NewEngineState=Available
EventIdentifier EventType Logfile	400 3 Windows PowerShell Engine state is changed from None to Available. Details:

	HostName=ConsoleHost
	HostVersion=5.1.22621.169
	HostId=4cea8f63-8b91-448c-b01c-64f1cdac22da
	HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe
	EngineVersion=5.1.22621.169
	RunspaceId=67503dfb-db10-4832-a25a-86a1f432a8e3
	PipelineId=
	CommandType-
	CommandType= ScriptName=
	CommandPath=
	CommandLine=
RecordNumber	4252
SourceName	PowerShell
TimeGenerated	2022-10-05T02:54:37.973293Z
TimeWritten	2022-10-05T02:54:37.973293Z
Туре	Information
User	N/A
Log Number	32
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3
Logfile	Windows PowerShell
Message	Provider "FileSystem" is Started.
	Details:
	ProviderName=FileSystem
	NewProviderState=Started
	SequenceNumber=7
	HostName=ConsoleHost

ostVersion=5.1.22621.169	
·	exe
ommandName=	
ommandType=	
criptName=	
ommandPath=	
ommandLine=	
256	
owerShell	
022-10-05T02:58:07.3984Z	
022-10-05T02:58:07.3984Z	
formation	
/A	
3	
2548	
pecial Logon	
andbox	
672	
672	
ecurity	
pecial privileges assigned to new logon.	
uhioat	
ccount Name: 31312M	
ogon ID: 0x3E7	
ogon ID: UX3E7	
rivileges: SeAssignPrimaryTokenPrivilege eTcbPrivilege	
0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0	stid=cd635701-06a7-4607-8626-f422cd2a174b stApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.gineVersion= nspaceId= nsp

		7
	SeTakeOwnershipPrivilege	
	SeLoadDriverPrivilege	
	SeBackupPrivilege	
	SeRestorePrivilege	
	SeDebugPrivilege	
	SeAuditPrivilege	
	SeSystemEnvironmentPrivilege SeImpercentePrivilege	
	SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege	
	SeDelegateSessionUserImpersonatePrivilege 17319	-
	Microsoft-Windows-Security-Auditing	
	2022-10-05T15:57:05.586789Z	_
	2022-10-05T15:57:05.586789Z	_
	Audit Success	_
71	N/A	
Log Number	34	
_	12292	
	Other System Events	
ComputerName	sandbox	
EventCode	5058	
EventIdentifier	5058	
EventType	4	
Logfile	Security	
Message	Key file operation.	
	Subject:	
	Security ID: S-1-5-21-3249831223-3918070856-2126610958-1001	
	Account Name: guru	
	Account Domain: sandbox	
	Logon ID: 0xC7B7D6A	
	Process Information:	
	Process ID: 14592	
	Process Creation Time: ?2022?-?10?-?05T11:08:37.273091600Z	
	<u> </u>	

	Cryptographic Parameters: Provider Name: Microsoft Software Key Storage Provider Algorithm Name: ECDSA_P256
	Key Name: Microsoft-Edge-TB-test-key
	Key Type: User key.
	Key File Operation Information: File Path:
	C:\Users\guru\AppData\Roaming\Microsoft\Crypto\Keys\53caafca80232173a709de019a
	f770-4829-8e8b-55f975dac4a9
	Operation: Write persisted key to file.
	Return Code: 0x0
RecordNumber	17333
SourceName	Microsoft-Windows-Security-Auditing
TimeGenerated	2022-10-05T16:38:40.785665Z
TimeWritten	2022-10-05T16:38:40.785665Z
Туре	Audit Success
User	N/A
Log Number	35
Category	12290
CategoryString	System Integrity
ComputerName	sandbox
EventCode	5061
EventIdentifier	5061
EventType	4
Logfile	Security
Message	Cryptographic operation.
Message	Cryptographic operation.
Message	
Message	Subject:
Message	Subject: Security ID: S-1-5-21-3249831223-3918070856-2126610958-1001
Message	Subject:
Message	Subject: Security ID: S-1-5-21-3249831223-3918070856-2126610958-1001 Account Name: guru
Message	Subject: Security ID: S-1-5-21-3249831223-3918070856-2126610958-1001 Account Name: guru Account Domain: sandbox
Message	Subject: Security ID: S-1-5-21-3249831223-3918070856-2126610958-1001 Account Name: guru Account Domain: sandbox

	Provider Name: Microsoft Software Key Storage Provider	
	Algorithm Name: ECDSA_P256	
	Key Name: Microsoft-Edge-TB-test-key	
	Key Type: User key.	
	Cryptographic Operation:	
	Operation: Create Key.	
	Return Code: 0x0	
RecordNumber	17334	
SourceName	Microsoft-Windows-Security-Auditing	
TimeGenerated	2022-10-05T16:38:40.786997Z	
TimeWritten	2022-10-05T16:38:40.786997Z	
Туре	Audit Success	
User	N/A	
Log Number	36	
Category	0	
CategoryString	N/A	
ComputerName	sandbox	
EventCode	16	
EventIdentifier	16	
EventType	3	
Logfile	System	
Message	The access history in hive	
	\??\C:\Users\guru\AppData\Local\Packages\Microsoft.ScreenSketch_8wekyb3d8	3bbwe\s
- INTrombor	was cleared updating 2 keys and creating 1 modified pages.	
	7206	
SourceName	Microsoft-Windows-Kernel-General	
	2022-10-05T16:39:07.931254Z	
TimeWritten	2022-10-05T16:39:07.931254Z	
Type	Information	