README.md

Windows Event Monitoring Guidance

Recommended Events to Collect

Account Usage

User account information can be collected and audited. Tracking local account usage can help detect Pass the Hash activity and other unauthorized account usage. Additional information such as remote desktop logins, users added to privileged groups, and account lockouts can also be tracked. User

accounts being promoted to privileged groups should be audited very closely to ensure that users are in fact supposed to be in a privileged group. Unauthorized membership in privileged groups is a strong indicator that malicious activity has occurred.

Lockout events for domain accounts are generated on the domain controller whereas lockout events for local accounts are generated on the local computer.

	ID	Level	Event Log	Event Source
Account Lockouts	4740	Information	Security	Microsoft-Windows-Security-Auditing
Account Login with Explicit Credentials	4648	Information	Security	Microsoft-Windows-Security-Auditing
Account Name Changed	4781	Information	Security	Microsoft-Windows-Security-Auditing
Account removed from Local Sec. Grp.	4733	Information	Security	Microsoft-Windows-Security-Auditing
Create Profile failed	1518	Error	Application	Microsoft-Windows-User Profiles Service
Credential Authentication	4776	Information	Security	Microsoft-Windows-Security-Auditing
Credentials backed up	5376	Information	Security	Microsoft-Windows-Security-Auditing
Credentials restored	5377	Information	Security	Microsoft-Windows-Security-Auditing

Failed User Account Login	4625	Information	Security	Microsoft-Windows-Security-Auditing
Group Assigned to new Session	300	Information	Microsoft-Windows-LSA/Operational	LsaSrv
Logoff Event	4634	Information	Security	Microsoft-Windows-Security-Auditing
Logon with Special Privs	4672	Information	Security	Microsoft-Windows-Security-Auditing
New User Account Created	4720	Information	Security	Microsoft-Windows-Security-Auditing
New User Account Enabled	4722	Information	Security	Microsoft-Windows-Security-Auditing
Password Hash Accessed	4782	Information	Security	Microsoft-Windows-Security-Auditing
Password Policy Checking API called	4793	Information	Security	Microsoft-Windows-Security-Auditing
Security-enabled Group Created	4731	Information	Security	Microsoft-Windows-Security-Auditing
Security-Enabled group Modification	4735	Information	Security	Microsoft-Windows-Security-Auditing
SID History add attempted on Account	4766	Information	Security	Microsoft-Windows-Security-Auditing

SID History added to Account	4765	Information	Security	Microsoft-Windows-Security-Auditing
Successful User Account Login	4624	Information	Security	Microsoft-Windows-Security-Auditing
Temp Profile Logon	1511	Error	Application	Microsoft-Windows-User Profiles Service
User Account Deleted	4726	Information	Security	Microsoft-Windows-Security-Auditing
User Account Disabled	4725	Information	Security	Microsoft-Windows-Security-Auditing
User Account Unlocked	4767	Information	Security	Microsoft-Windows-Security-Auditing
User Added to Privileged Group	4728, 4732, 4756	Information	Security	Microsoft-Windows-Security-Auditing
User Right Assigned	4704	Information	Security	Microsoft-Windows-Security-Auditing

Application Crashes

Application crashes may warrant investigation to determine if the crash is malicious or benign. Categories of crashes include Blue Screen of Death (BSOD), Windows Error Reporting (WER), Application Crash and Application Hang events. If the organization is actively using the Microsoft Enhanced Mitigation Experience Toolkit (EMET), then EMET logs can also be collected.

	ID	Level	Event Log	Event Source

App Crash	1000	Error	Application	Application Error
App Error	1000	Error	Application	Application Error
App Hang	1002	Error	Application	Application Hang
BSOD	1001	Error	System	Microsoft-Windows-WER-SystemErrorReporting
WER	1001	Information	Application	Windows Error Reporting

Application Whitelisting

Application whitelisting events should be collected to look for applications that have been blocked from execution. Any blocked applications could be malware or users trying to run unapproved software. Software Restriction Policies (SRP) is supported on Windows XP and above. The AppLocker feature is available for Windows 7 and above Enterprise and Ultimate editions only. Application Whitelisting events can be collected if SRP or AppLocker are actively being used on the network.

	ID	Level	Event Log	Event Source
Application Installed	8023	Information	Microsoft-Windows-AppLocker/Packaged app-Deployment	Microsoft-Windows-AppLocker
Application Ran	8020	Information	Microsoft-Windows-AppLocker/Packaged app-Execution	Microsoft-Windows-AppLocker
AppLocker Block	8002	Information	Microsoft-Windows-AppLocker/EXE and DLL	Microsoft-Windows-AppLocker
AppLocker Block	8003	Error	Microsoft-Windows-AppLocker/EXE and DLL	Microsoft-Windows-AppLocker
AppLocker Block	8004	Warning	Microsoft-Windows-AppLocker/EXE and DLL	Microsoft-Windows-AppLocker
AppLocker Warning	8006	Error	Microsoft-Windows-AppLocker/MSI and	Microsoft-Windows-AppLocker

			Script	
AppLocker Warning	8007	Warning	Microsoft-Windows-AppLocker/MSI and Script	Microsoft-Windows-AppLocker
Process Created	4688	Information	Security	Microsoft-Windows-Security-Auditing
Process Terminated	4689	Information	Security	Microsoft-Windows-Security-Auditing
Script or Installer ran	8005	Information	Microsoft-Windows-AppLocker/MSI and Script	Microsoft-Windows-AppLocker
SRP Block	865, 866, 867, 868, 882	Warning	Application	Microsoft-Windows-SoftwareRestrictionPolicies

Boot Events

	ID	Level	Event Log	Event Source
Shutdown Initiate Failed	1074	Warning	User32	User32
Windows Shutdown	13	Information	System	Microsoft-Windows-Kernel-General
Windows Startup	12	Information	System	Microsoft-Windows-Kernel-General

Certificate Services

Certificate Services receives requests for digital certificates over RPC or HTTP. For organizations that do not rely upon external certification authorities, policies and settings can be customized in order to support the organization's requirements. The below events can be collected to ensure expected use.

Additional Information can be found at the TechNet article titled Certificate Services Lifecycle Notifications and the Microsoft Secure blog post titled New Guidance for Securing Public Key Infrastructure

	ID	Level	Event Log	Event Sourc
CA Permissions Corrupted or Missing	95	Error	Application	Microsoft-Windows-CertificationAuthority
CA Services Request	4886	Information	Security	Microsoft-Windows-S Auditing
Certificate Manager Settings Changed	4890	Information	Security	Microsoft-Windows-S Auditing
Certificate Request Attributes Changed	4874	Information	Security	Microsoft-Windows-S Auditing
Certificate Request Extension Changed	4873	Information	Security	Microsoft-Windows-S Auditing
Certificate Revoked	4870	Information	Security	Microsoft-Windows-S Auditing
Certificate Services approved request	4887	Information	Security	Microsoft-Windows-S Auditing
Certificate Services Audit Filter Changed	4885	Information	Security	Microsoft-Windows-S Auditing

Certificate Services Configuration Changed	4891	Information	Security	Microsoft-Windows-S Auditing
Certificate Services denied request	4888	Information	Security	Microsoft-Windows-S Auditing
Certificate Services Loaded Template	4898	Information	Security	Microsoft-Windows-S Auditing
Certificate Services Permissions Changed	4882	Information	Security	Microsoft-Windows-S Auditing
Certificate Services Property Changed	4892	Information	Security	Microsoft-Windows-S Auditing
Certificate Services Started	4880	Information	Security	Microsoft-Windows-S Auditing
Certificate Services Stopped	4881	Information	Security	Microsoft-Windows-S Auditing
Certificate Services Template Security Updated	4900	Information	Security	Microsoft-Windows-S Auditing
Certificate Services	4899	Information	Security	Microsoft-Windows-S Auditing

Template Updated				
Entries Removed from Certificate Database	4896	Information	Security	Microsoft-Windows-S Auditing
Import Certificate	1006	Information	Microsoft-Windows-CertificateServicesClientLifecycle-System/Operational	Microsoft-Windows-CertificateServicesClie System
Remove Certificate	1004	Information	Microsoft-Windows-CertificateServicesClientLifecycle-System/Operational	Microsoft-Windows-CertificateServicesClie System
Exported Certificate	1007	Information	Microsoft-Windows-CertificateServicesClientLifecycle-System/Operational	Microsoft-Windows-CertificateServicesClie System
Certificate close to expiration	1003	Warning	Microsoft-Windows-CertificateServicesClientLifecycle-System/Operational	Microsoft-Windows-CertificateServicesClie System
Replace Certificate	1001	Information	Microsoft-Windows-CertificateServicesClientLifecycle-System/Operational	Microsoft-Windows-CertificateServicesClie System
Expired Certificate	1002	Error	Microsoft-Windows-CertificateServicesClientLifecycle-System/Operational	Microsoft-Windows-CertificateServicesClie System

Clearing Event Logs

It is unlikely that event log data would be cleared during normal operations and it is likely that a malicious attacker may try to cover their tracks by clearing an event log. When an event log gets cleared, it is suspicious. Centrally collecting events has the added benefit of making it much harder for an attacker to cover their tracks. Event forwarding permits sources to forward multiple copies of a collected event to multiple collectors thus enabling redundant event collection. Using a redundant event collection model can minimize the single point of failure risk.

	ID	Level	Event Log	Event Source
Event Log Service Shutdown	1100	Information	Security	Microsoft-Windows-EventLog
Event Log was Cleared	104	Information	System	Microsoft-Windows-Eventlog
Event Log was Cleared	1102	Information	Security	Microsoft-Windows-Eventlog

DNS/Directory Services

Malicious or misused software can often attempt to resolve blacklisted or suspicious domain names. The collection of DNS queries and responses are recommended in order to enable discovery of compromise or intrusion through security analytics.

A number of the below event IDs will only be recorded with enhanced auditing enabled. See Network Forensics with Windows DNS Analytical Logging for more information.

	ID	Level	Event Log	Event Source
Directory service created	5137	Information	Security	Microsoft-Windows-Security-Auditing
Directory service deleted	5141	Information	Security	Microsoft-Windows-Security-Auditing
Directory service modified	5136	Information	Security	Microsoft-Windows-Security-Auditing
Directory service moved	5139	Information	Security	Microsoft-Windows-Security-Auditing
Directory service recovered	5138	Information	Security	Microsoft-Windows-

				Security-Auditing
DNS Query Complete	3008	Information	Microsoft-Windows-DNS-Client/Operational	Microsoft-Windows-DNS-Client
DNS Request/Response	256, 257	Information	Microsoft-Windows-DNSServer/Analytical	Microsoft-Windows-DNSServer
DNS Response Complete	3020	Information	Microsoft-Windows-DNS-Client/Operational	Microsoft-Windows-DNS-Client

External Media Detection

Detection of USB device (e.g., mass storage devices) usage is important in some environments, such as air gapped networks. This section attempts to take the proactive avenue to detect USB insertion at real-time. Event ID 43 only appears under certain circumstances. The following events and event logs are only available in Windows 8 and above.

Microsoft-Windows-USB-USBHUB3-Analytic is not an event log per se; it is a trace session log that stores tracing events in an Event Trace Log (.etl) file. The events created by Microsoft-Windows-USB-USBHUB3 publisher are sent to a direct channel (i.e., Analytic log) and cannot be subscribed to for event collection. Administrators should seek an alternative method of collecting and analyzing this event (43).

	ID	Level	Event Log	Event Source
New Device Information	43	Information	Microsoft-Windows-USB-USBHUB3-Analytic	Microsoft-Windows-USB-USBHUB3
New Mass Storage Installation	400, 410	Information	Microsoft-Windows-Kernel-PnP/Device Configuration	Microsoft-Windows-Kernel-PnP

Group Policy Errors

Management of domain computers permits administrators to heighten the security and regulation of those machines with Group Policy. The inability to apply a policy due to a group policy error reduces the

aforementioned benefits. An administrators should investigate these events immediately.

	ID	Level	Event Log	Event Source
Generic Internal Error	1126	Error	System	Microsoft-Windows-GroupPolicy
Group Policy Application Failed due to Connectivity	1129	Error	System	Microsoft-Windows-GroupPolicy
Internal Error	1125	Error	System	Microsoft-Windows-GroupPolicy

Kernel Driver Signing

Introduction of kernel driver signing in the 64-bit version of Windows Vista significantly improves defenses against insertion of malicious drivers or activities in the kernel. Any indication of a protected driver being altered may indicate malicious activity or a disk error and warrants investigation.

	ID	Level	Event Log	Event Source
Code Integrity Check	3001, 3002, 3003, 3004, 3010, 3023	Warning, Error	Microsoft-Windows-CodeIntegrity/Operational	Microsoft-Windows-CodeIntegrity
Detected an invalid image hash of a file	5038	Information	Security	Microsoft-Windows-Security-Auditing
Detected an invalid page hash of an image file	6281	Information	Security	Microsoft-Windows-Security-Auditing
Failed Kernel Driver	219	Warning	System	Microsoft-Windows-

Loading				Kernel-PnP

Microsoft Cryptography API

The Microsoft CryptoAPI can be used for certificate verification and encryption/decryption of data. There are a number of interesting events that should be logged for suspicious behavior or for future auditing.

	ID	Level	Event Log	Event Source
Cert Trust Chain Build Failed	11	Information	Microsoft-Windows-CAPI2/Operational	Microsoft-Windows-CAPI2
Private Key Accessed	70	Information	Microsoft-Windows-CAPI2/Operational	Microsoft-Windows-CAPI2
X.509 Object	90	Information	Microsoft-Windows-CAPI2/Operational	Microsoft-Windows-CAPI2

Mobile Device Activities

Wireless devices are ubiquitious and the need to record an enterprise's wireless device activities may be critical. A wireless device could become compromised while traveling between different networks, regardless of the protocol used for communication (e.g., 802.11 or Bluetooth). Therefore, the tracking of which networks mobile devices are entering and exiting is useful to prevent further compromises. The creation frequency of the following events depend on how often the device disconnects and reconnects to a wireless network. Each event below provides mostly similar information with the exception that additional fields have been added to certain events.

	ID	Level	Event Log	Event Source
Disconnect from Wireless connection	8003	Information	Microsoft-Windows-WLAN-AutoConfig/Operational	Microsoft-Windows-WLAN-AutoConfig
Network Connection and Disconnection Status (Wired and Wireless)	10000, 10001	Information	Microsoft-Windows-NetworkProfile/Operational	Microsoft-Windows-NetworkProfile

Starting a Wireless connection	8000, 8011	Information	Microsoft-Windows-WLAN-AutoConfig/Operational	Microsoft-Windows-WLAN-AutoConfig
Successfully connected to a Wireless connection	8001	Information	Microsoft-Windows-WLAN-AutoConfig/Operational	Microsoft-Windows-WLAN-AutoConfig
Wireless Association Status	11000, 11001	Information	Microsoft-Windows-WLAN-AutoConfig/Operational	Microsoft-Windows-WLAN-AutoConfig
Wireless Association Status	11002	Error	Microsoft-Windows-WLAN-AutoConfig/Operational	Microsoft-Windows-WLAN-AutoConfig
Wireless Authentication Started and Failed	12011, 12012	Information	Microsoft-Windows-WLAN-AutoConfig/Operational	Microsoft-Windows-WLAN-AutoConfig
Wireless Authentication Started and Failed	12013	Error	Microsoft-Windows-WLAN-AutoConfig/Operational	Microsoft-Windows-WLAN-AutoConfig
Wireless Connection Failed	8002	Error	Microsoft-Windows-WLAN-AutoConfig/Operational	Microsoft-Windows-WLAN-AutoConfig
Wireless Security Started, Stopped, Successful, or Failed	11004, 11005	Information	Microsoft-Windows-WLAN-AutoConfig/Operational	Microsoft-Windows-WLAN-AutoConfig

Wireless Security Started, Stopped, Successful, or Failed	11010, 11006	Error	Microsoft-Windows-WLAN-AutoConfig/Operational	Microsoft-Windows-WLAN-AutoConfig

Network Host Activities

Monitoring network activities can be performed in multiple ways ranging from a network sensor detecting the traffic directly to collecting indirect artifacts generated by a client or server performing network activities. Windows hosts generate log artifacts pertaining to network activities to assist with network troubleshooting and detection of unusual network traffic occurring by or against a host such as lateral movement, unauthorized network policy change, unauthorized network connections, and unusual manipulation of network resources (e.g., unexpected file share being quickly created and deleted). The following events require the enabling of the **Audit Other Policy Change**, **Audit Authentication Policy Change**, **Audit Kerberos Service Ticket Operations**, **Audit Network Policy Server**, **Audit File Share**, **Audit Certification Services**, **Audit Policy Change**, and **Audit Other Logon/Logoff Events** group policies.

	ID	Level	Event Log	Event Source
Encrypted Data Recovery Policy Changed	4714	Information	Security	Microsoft-Windows-Security-Auditing
Kerberos Policy Changed	4713	Information	Security	Microsoft-Windows-Security-Auditing
Kerberos Service Ticket Req. Failed	4769	Information	Security	Microsoft-Windows-Security-Auditing
Network Policy Server Denied Access	6273	Information	Security	Microsoft-Windows-Security-Auditing
Network Policy Server Discarded Accounting Request	6275	Information	Security	Microsoft-Windows-Security-Auditing

Network Policy Server Discarded Request	6274	Information	Security	Microsoft-Windows-Security-Auditing
Network Policy Server Granted Access	6272	Information	Security	Microsoft-Windows-Security-Auditing
Network Policy Server Granted Full Access	6278	Information	Security	Microsoft-Windows-Security-Auditing
Network Policy Server Granted Probationary Access	6277	Information	Security	Microsoft-Windows-Security-Auditing
Network Policy Server Locked Account	6279	Information	Security	Microsoft-Windows-Security-Auditing
Network Policy Server Quarantined User	6276	Information	Security	Microsoft-Windows-Security-Auditing
Network Policy Server Unlocked Account	6280	Information	Security	Microsoft-Windows-Security-Auditing
Network share accessed	5140	Information	Security	Microsoft-Windows-Security-Auditing
Network Share Checked	5145	Information	Security	Microsoft-Windows-Security-Auditing
Network Share Created	5142	Information	Security	Microsoft-Windows-Security-Auditing
Network Share Deleted	5144	Information	Security	Microsoft-Windows-Security-Auditing

New Trust for Domain	4706	Information	Security	Microsoft-Windows-Security-Auditing
Outbound TS Connect Attempt	1024	Information	Microsoft-Windows-TerminalServices-RDPClient/Operational	Microsoft-Windows-TerminalServices-ClientActiveXCore
RADIUS User assigned IP	20250	Success	RemoteAccess	Microsoft-Windows-MPRMSG
RADIUS User Authenticated	20274	Success	RemoteAccess	Microsoft-Windows-MPRMSG
RADIUS User Disconnected	20275	Success	RemoteAccess	Microsoft-Windows-MPRMSG
Role Separation Enabled	4897	Information	Security	Microsoft-Windows-Security-Auditing
System Audit Policy Changed	4719	Information	Security	Microsoft-Windows-Security-Auditing
Trusted Domain Information Modified	4716	Information	Security	Microsoft-Windows-Security-Auditing
TS Session Disconnect	4779	Information	Security	Microsoft-Windows-Security-Auditing
TS Session Reconnect	4778	Information	Security	Microsoft-Windows-Security-Auditing
Wireless 802.1X Auth	5632	Information	Security	Microsoft-Windows-Security-Auditing

Pass the Hash Detection

Tracking user accounts for detecting Pass the Hash (PtH) requires creating a custom view with XML to configure more advanced filtering options. The event query language is based on XPath. The recommended **QueryList** below is limited in detecting PtH attacks. These queries focus on discovering lateral movement by an attacker using local accounts that are not part of a domain. The **QueryList**

captures events that show a local account attempting to connect remotely to another machine not part of the domain. This event is a rarity so any occurrence should be treated as suspicious.

These XPath queries below are used for the Event Viewer's **Custom Views**.

The successful use of PtH for lateral movement between workstations would trigger event ID 4624, with an event level of Information, from the Security log. This behavior would be a **LogonType** of 3 using NTLM authentication where it is not a domain logon and not the ANONYMOUS LOGON account. To clearly summarize the event that is being collected, see event 4624 below.

In the **QueryList** below, substitute the section with the desired domain name.

A failed logon attempt when trying to move laterally using PtH would trigger an event ID 4625. This would have a **LogonType** of 3 using NTLM authentication where it is not a domain logon and not the ANONYMOUS LOGON account. To clearly summarize the event that is being collected, see event 4625 below.

```
<QueryList>
  <Query Id="0" Path="Forwarded Events">
    <Select Path="ForwardedEvents">
      *[System[(Level=4 or Level=0) and (EventID=4624)]]
      and
      *[EventData[Data[@Name='LogonType'] and (Data='3')]]
      and
      *[EventData[Data[@Name='TargetUserName'] != 'ANONYMOUS LOGON']]
      and
      *[EventData[Data[@Name='TargetDomainName'] != '<DOMAIN NAME>']]
    </Select>
  </Query>
</QueryList>
<QueryList>
  <Query Id="0" Path="Forwarded Events">
    <Select Path="ForwardedEvents">
      *[System[(Level=4 or Level=0) and (EventID=4625)]]
      and
      *[EventData[Data[@Name='AuthenticationPackageName'] and (Data='3')]]
      and
      *[EventData[Data[@Name='TargetUserName'] != 'ANONYMOUS LOGON']]
      and
      *[EventData[Data[@Name='TargetDomainName'] != '<DOMAIN NAME>']]
    </Select>
  </Query>
</QueryList>
```

Event ID	Log	Level	LogonType	Authentication Pkg Name
4624	Security	Information	3	NTLM
4625	Security	Information	3	NTLM

PowerShell Activities

PowerShell events can be interesting as Powershell is included by default in modern Windows installations. If a PowerShell script is failing, it may indicate misconfiguration, missing files, or malicious activity. Use of the Get-MessageTrackingLog cmdlet can be used to enumerate Exchange Server mail metadata, returning detailed information about the history of each mail message traveling through the server.

Script block logging can be enabled with PowerShell 5.0+ and PowerShell 4.0 with patches enabled. For more information:

- https://docs.microsoft.com/en-us/powershell/wmf/5.0/audit_script
- https://blogs.msdn.microsoft.com/powershell/2015/06/09/powershell-the-blue-team/
- https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html

	ID	Level	Event Log	Event Source
Get-MessageTrackingLog cmdlet	800	Information	Powershell	Microsoft-Windows-Powershell
Remote Connection	169	Information	Powershell	Microsoft-Windows-Powershell
Exception Raised	4103	Information	Microsoft-Windows-Powershell/Operational	Microsoft-Windows-Powershell
Script block contents	4104	Information	Microsoft-Windows-Powershell/Operational	Microsoft-Windows-Powershell
Script block start	4105	Information	Microsoft-Windows-Powershell/Operational	Microsoft-Windows-

				Powershell
Script block end	4106	Information	Microsoft-Windows-Powershell/Operational	Microsoft-Windows-Powershell

Printing Services

Document printing is essential for daily operations in many environments. The vast amount of printing requests increases the difficulty in tracking and identifying which document was printed and by whom. Documents forwarded to a printer for processing can be recorded for logging purposes in multiple ways. Each printing job can be logged either by a printing server, the printer itself, or the requesting machine. The logging of these activities permits early detection of printing certain documents. The following event is generated on the client machine requesting to print a document. This event should be treated as a historical record or an additional piece of evidence rather than an auditing record of printing jobs.

This operational log is disabled by default and requires the log to be enabled to capture this event.

	ID	Level	Event Log	Event Source
Printing Document	307	Information	Microsoft-Windows-PrintService/Operational	Microsoft-Windows-PrintService

Remote Desktop Logon Detection

Remote Desktop account activity events are not easily identifiable using the Event Viewer GUI. When an account remotely connects to a client, a generic successful logon event is created. A custom **Query Filter** can aid in clarifying the type of logon that was performed. The query below shows logins using Remote Desktop. Remote Desktop activity should be monitored since only certain administrators should be using it, and they should be from a limited set of management workstations. Any Remote Desktop logins outside of expected activity should be investigated.

The XPath queries below are used for the Event Viewer's **Custom Views**. Event ID 4624 and Event ID 4634 respecively indicate when a user has logged on and logged off with RDP. A LogonType with the value of 10 indicates a Remote Interactive logon.

```
<QueryList>
  <Query Id="0" Path="ForwardedEvent">
```

```
    <Select Path="ForwardedEvents">
    <!-- Collects Logon and Logoffs in RDP -->
    <!-- Remote Desktop Protocol Connections -->
      *[System[(Level=4 or Level=0) and (EventID=4624 or EventID=4634)]]
      and
      *[EventData[Data[@Name='LogonType']='10')]]
      and
    (*[EventData[Data[5]='10')]]
      or
      *[EventData[Data[@Name='AuthenticationPackageName'] = 'Negotiate']])
    </Select>
  </Query>
</QueryList>
```

Event ID	Log	Level	LogonType	Authentication Pkg Name
4624	Security	Information	10	Negotiate
4634	Security	Information	10	N/A

Software and Service Installation

As part of normal network operations, new software and services will be installed, and there is value in monitoring this activity. Administrators can review these logs for newly installed software or system services and verify that they do not pose a risk to the network.

It should be noted that an additional Program Inventory event ID 800 is generated daily on Windows 7 at 12:30 AM to provide a summary of application activities (e.g., number of new application installations). Event ID 800 is generated on Windows 8 as well under different circumstances. This event is beneficial to administrators seeking to identify the number of applications that were installed or removed on a machine.

	ID	Level	Event Log	Event Source
New Application Installation	903, 904	Information	Microsoft-Windows-Application-Experience/Program-Inventory	Microsoft-Windows-Application-Experience
New Kernel Filter Driver	6	Information	System	Microsoft-Windows-FilterManager

New MSI File Installed	1022, 1033	Information	Application	MsiInstaller
New Windows Service	7045	Information	System	Microsoft-Windows-FilterManager
Removed Application	907, 908	Information	Microsoft-Windows-Application-Experience/Program-Inventory	Microsoft-Windows-Application-Experience
Service Start Failure	7000	Error	System	Service Control Manager
Summary of Software Activities	800	Information	Microsoft-Windows-Application-Experience/Program-Inventory	Microsoft-Windows-Application-Experience
Update Packages Installed	2	Information	Setup	Microsoft-Windows-Servicing
Updated Application	905, 906	Information	Microsoft-Windows-Application-Experience/Program-Inventory	Microsoft-Windows-Application-Experience
Windows Update Installed	19	Information	System	Microsoft-Windows-WindowsUpdateClient

System Integrity

System Integrity ensures the trustworthiness of a host in the presence of manipulation. The ability to identify unusual changes to a host can hinder additional integrity compromises and possibly prevent such changes. The **Audit Registry** and **Audit Security State Change** group policies must be enabled. The Registry Modification event will not be generated unless a SACL is applied to a desired registry key or value (see the Windows 10 and Windows Server 2016 security auditing and monitoring reference). A non-exhaustive list identifying individual or sets of registry keys and values to monitor may be found at

Microsoft's Threat Protection article titled Use Windows Event Forwarding to help with intrusion detection Appendix B, Microsoft's Securing PKI TechNet article on Registry Values to Monitor, SwiftOnSecurity's GitHub project titled sysmon-config, Specter Ops's Subverting Trust Windows white paper, and Cylance's Windows Registry Persistence, Part 1: Introducing, Attack, Phases and Windows Services blog post.

	ID	Level	Event Log	Event Source
Registry Modification	4657	Information	Security	Microsoft-Windows-Security-Auditing
System Time Changed	1	Information	System	Microsoft-Windows-Kernel-General
System Time Changed	4616	Information	Security	Microsoft-Windows-Security-Auditing

A non-exhaustive registry key and value list to potentially monitor

Registry key / value
HKLM\SYSTEM\CurrentControlSet\Services\Ntmssvc\
HKLM\SYSTEM\CurrentControlSet\Services\NWCWorkstation\
HKLM\SYSTEM\CurrentControlSet\Services\Nwsapagent\
HKLM\SYSTEM\CurrentControlSet\Services\SRService\
HKLM\SYSTEM\CurrentControlSet\Services\WmdmPmSp\
HKLM\SYSTEM\CurrentControlSet\Services\LogonHours\
HKLM\SYSTEM\CurrentControlSet\Services\PCAudit\
HKLM\SYSTEM\CurrentControlSet\Services\helpsvc\
HKLM\SYSTEM\CurrentControlSet\Services\uploadmgr\
HKLM\SYSTEM\CurrentControlSet\Services\FastUserSwitchingCompatibility\
HKLM\SYSTEM\CurrentControlSet\Services\Ias\

HKLM\SYSTEM\CurrentControlSet\Services\Nla\
HKLM\SYSTEM\CurrentControlSet\Services\Wmi\
HKLM\SYSTEM\CurrentControlSet\Services\Irmon\
HKLM\SYSTEM\CurrentControlSet\Control\Cryptography\Configuration\
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SecurityProviders
HKLM\SOFTWARE\Microsoft\Cryptography\OID\
HKLM\SOFTWARE\Microsoft\Cryptography\Providers\Trust\
HKLM\SOFTWARE\Microsoft\WOW6432Node\Microsoft\Cryptography\OID\
HKLM\SOFTWARE\Microsoft\WOW6432Node\Microsoft\Cryptography\Providers\Trust
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32\
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Font Drivers\

System or Service Failures

System and Services failures are interesting events that may need to be investigated. Service operations normally do not fail. If a service fails, then it may be of concern and should be reviewed by an administrator. If a Windows service continues to fail repeatedly on the same machines, then this may indicate that an attacker is targeting a service.

	ID	Level	Event Log	Event Source
Windows Service Fails or Crashes	7022, 7023, 7024, 7026, 7031, 7032, 7034	Error	System	Service Control Manager

Task Scheduler Activities

Scheduled tasks can be maliciously created or deleted. The Task Scheduler can be used, for instance, to create tasks that wait for certain preconditions before downloading malicious files or to load malicious software into memory.

	ID	Level	Event Log	Event Source
New Task Registered	106	Information	Microsoft-Windows-TaskScheduler/Operational	Microsoft-Windows-TaskScheduler
Task Deleted	141	Information	Microsoft-Windows-TaskScheduler/Operational	Microsoft-Windows-TaskScheduler
Task Disabled	142	Information	Microsoft-Windows-TaskScheduler/Operational	Microsoft-Windows-TaskScheduler
Task Launched	200	Information	Microsoft-Windows-TaskScheduler/Operational	Microsoft-Windows-TaskScheduler

Windows Defender Antivirus Activities

Spyware and malware remain a serious problem and Microsoft developed an antispyware and antivirus, Windows Defender, to combat this threat. Any notifications of detecting, removing, or preventing these malicious programs should be investigated. In the event Windows Defender fails to operate normally, administrators should correct the issue immediately to prevent the possibility of infection or further infection. If a third-party antivirus and antispyware product is currently in use, the collection of these events is not necessary.

	ID	Level	Event Log	Event Source
Action on Malware Failed	1008	Error	Microsoft-Windows-Windows Defender/Operational	Microsoft-Windows-Windows Defender
Detected Malware	1006, 1116	Warning	Microsoft-Windows-Windows Defender/Operational	Microsoft-Windows-Windows Defender
Failed to remove item from quarantine	1010	Error	Microsoft-Windows-Windows Defender/Operational	Microsoft-Windows-Windows Defender

Failed to update engine	2003	Error	Microsoft-Windows-Windows Defender/Operational	Microsoft-Windows-Windows Defender
Failed to update signatures	2001	Error	Microsoft-Windows-Windows Defender/Operational	Microsoft-Windows-Windows Defender
File Restored from Quarantine	1009	Information	Microsoft-Windows-Windows Defender/Operational	Microsoft-Windows-Windows Defender
Malware Removal Error	1118	Information	Microsoft-Windows-Windows Defender/Operational	Microsoft-Windows-Windows Defender
Malware Removal Fatal Error	1119	Error	Microsoft-Windows-Windows Defender/Operational	Microsoft-Windows-Windows Defender
Malware Removed	1007, 1117	Information	Microsoft-Windows-Windows Defender/Operational	Microsoft-Windows-Windows Defender
Real-Time Protection failed	3002	Error	Microsoft-Windows-Windows Defender/Operational	Microsoft-Windows-Windows Defender
Reverting to last known good set of signatures	2004	Warning	Microsoft-Windows-Windows Defender/Operational	Microsoft-Windows-Windows Defender

Scan Failed	1005	Error	Microsoft-Windows-Windows Defender/Operational	Microsoft-Windows-Windows Defender
Unexpected Error	5008	Error	Microsoft-Windows-Windows Defender/Operational	Microsoft-Windows-Windows Defender

Windows Firewall

If client workstations are taking advantage of the built-in host-based Windows Firewall, then there is value in collecting events to track the firewall status. For example, if the firewall state changes from on to off, then that log should be collected. Normal users should not be modifying the firewall rules of their local machine. The below events for the listed versions of the Windows operating system are only applicable to modifications of the local firewall settings.

	ID	Level	Event Log	Event Source
Firewall Failed to load Group Policy	2009	Error	Microsoft-Windows-Windows Firewall With Advanced Security/Firewall	Microsoft-Windows-Windows Firewall With Advanced Security
Firewall Rule Add	2004	Information	Microsoft-Windows-Windows Firewall With Advanced Security/Firewall	Microsoft-Windows-Windows Firewall With Advanced Security
Firewall Rule Change	2005	Information	Microsoft-Windows-Windows Firewall With Advanced Security/Firewall	Microsoft-Windows-Windows Firewall With Advanced Security
Firewall Rules Deleted	2006, 2033	Information	Microsoft-Windows-Windows Firewall With Advanced Security/Firewall	Microsoft-Windows-Windows Firewall With Advanced Security

Windows Update Errors

A machine must be kept up to date to mitigate known vulnerabilities. Although unlikely, these patches may sometimes fail to apply. Failure to update issues should be addressed to avoid prolonging the existence of an application issue or a vulnerability in the operating system or an application.

	ID	Level	Event Log	Event Source
Hotpatching Failed	1009	Information	Setup	Microsoft-Windows-Servicing
Windows Update Failed	20, 24, 25, 31, 34, 35	Error	Microsoft-Windows-WindowsUpdateClient/Operational	Microsoft-Windows-WindowsUpdateClien