SentinelOne - 24.2 Windows Agent Release Notes

April 28, 2025

The purpose of this article is to outline the various improvements in the upcoming SentinelOne agent upgrade. The lists below do not include an exhaustive list of all release notes, but rather a summation of the most notable improvements.

Current Stable version: 24.1.4.257 GA
Target Stable version: 24.2.3.471 GA
OS: Windows
This agent version and its new features have undergone extensive testing and validation by SentinelOne and have been further tested in a lab environment before being identified as stable by the Barracuda XDR Endpoint Security Team.

Upgrade Timeline

The new agent version, 24.2.3.471 was declared GA by SentinelOne on April 2nd, 2025.
This agent upgrade will be pushed out in phases over the next 2-6 weeks across all Managed Endpoint Security partners. The upgrade process is silent, and no interruption, input, or reboot will be needed from our partners.

Reminder – Agent Version Compatibility Changes as of 24.1

As a reminder, Windows Agents 24.1 and higher are compatible **only** with specific 64-bit Windows OS versions and are **not** compatible with 32-bit Windows OS versions.

Windows Agent 24.1+ is compatible only with these Windows versions:

- Windows 8.1 64-bit
- Windows 10 64-bit
- Windows 11 64-bit
- Windows Server/Storage Server 2012 R2 64-bit
- Windows Server/Storage Server/Server Core 2016 64-bit
- Windows Server/Server Core 2019 64-bit
- Windows Server/Storage Server 2022 64-bit

Windows Agent version 24.1+ is **not** supported on:

- Endpoints running 32-bit versions of Windows.
- Endpoints running 64-bit versions of Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8 (not 8.1), and Windows Server 2012 (not R2).
- Endpoints running these OS versions will remain on the latest supported agent build.

Barracuda Managed XDR™

General Agent Enhancements:

- **Enhanced driver-blocking capabilities:** The 24.2.1 Agent has enhanced boot-start driver blocking capabilities. To use these new capabilities, we recommend:
  - If possible, do not configure a driver-blocking Group Policy in Windows, so that the default settings can apply the new driver-blocking capabilities.
  - If a **Boot-Start Driver Initialization Policy** is used in the Group Policy, do not set it to **All**, to allow all of the new driver-blocking capabilities.

Note: This policy is located at *Computer Configuration\Administrative Templates\System\Early Launch Antimalware* in the Group Policy, or at *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Policies\EarlyLaunch\DriverLoadPolicy* on the endpoint's registry.

- **Corrupted database sends the Agent to Rebootless mode**: The Agent recovers to Rebootless mode if the database used by the Agent gets corrupted. In Rebootless mode, most Agent functionality is operational, even if you do not reboot the endpoint. This includes Static detection, Deep Visibility™ events, partial Deep Visibility Storylines, all Agent actions, and all response functions.
  - *Previously, the Agent recovered to Slim mode. In Slim mode, only these Agent engines are enabled: Pre-Execution (blocklist, exclusions), Reputation, and Static AI.*
- **New return codes**: New return codes have been added for when the Windows Task Scheduler folders are inaccessible and the SentinelOne Installer log could not be opened:

Value	Scenario	Status	Detailed Status	Description	Next Step
1009	Install	Failed	Installation aborted	Windows Task Scheduler folders \Sentinel and/or \SentinelOne are inaccessible. For example, if a Task Scheduler task exists at this path.	Delete the existing \Sentinel and/or \SentinelOne folders, or ensure they are accessible (for example, delete the problematic task), then run the installer again.
2031	Upgrade	Failed	Upgrade aborted	Windows Task Scheduler folders \Sentinel and/or \SentinelOne are inaccessible and could not be removed automatically. For example, if a Task Scheduler task exists at this path.	Delete the existing \Sentinel and/or \SentinelOne folders, or ensure they are accessible (for example, delete the problematic task), then run the installer again.
2032	Install or Upgrade			The SentinelOne Installer log could not be opened.	

Barracuda Managed XDR™

Detection Enhancements:

- **Improved Core Impact detection**: Enhanced detection capabilities to identify the Core Impact penetration software agent, which is commonly used by the RocketKitten and WoolenGoldfish Advanced Persistent Threat (APT) groups.
- **SHA-256 support infrastructure**: The Windows 24.2.1 Agent contains the necessary infrastructure to support working with SHA-256 values in the Management Console. We are now able to:
  - Block processes and files based on SHA-256 hash values.
  - Exclude processes and files based on SHA-256 hash values.

Bug Fixes:

- Upgrades from Windows 10 to Windows 11 sometimes failed.
- Running dism.exe and sfc.exe when KB5052093 was installed on the Windows 11 preview caused an error message to appear. Microsoft has subsequently reverted the changes introduced in this KB.
- Installation sometimes failed if the system product information could not be queried using Windows Management Instrumentation (WMI).
- Upgrades from Windows 10 to Windows 11 sometimes failed when Anti-tamper was enabled in the policy.
- Installation sometimes took significantly longer than expected.
- An interoperability issue with third-party boot drivers sometimes caused boot devices to be inaccessible or to fail.
- On-demand scan could not be executed after an on-demand scan was completed on an optical drive.
- If a custom data folder was used for SentinelOne Installer installation, the cleaner sometimes failed to delete it when cleaning.
- The Agent sometimes crashed on system start when one of the Agent services experienced a timeout.
- Resolved issue where disabled agents failed to enable.
- VSS snapshots could be deleted, causing system error.
- VSS snapshots created by third-party applications could be deleted.
- Installation error log was not sent and no return code was provided to the user. A new return code, 2032, was added for failures to access the log file created by SentinelOne Installer.
- Agent installation or upgrade failed due to registry key permissions.
- Interoperability issue with Symantec.
- Interoperability issues with Paint.NET 5.0.13.
- Interoperability issue with Citrix shell servers.
- Interoperability issue with Powershell 7.5.
- An interoperability issue prevented the installation of Proxy Pro Host.
- No sufficient disk space reservation for Agent logs.
- The Agent consumed a significant portion of the CPU on virtual machines hosted on Amazon EC2.

Barracuda Managed XDR™

False Positive Fixes:

- Detection of NinjaOne software.
- Detection on kavfswh.exe.
- Detections on Slack.
- Detections on SCCM installed software.
- Detections on Duo Security product.
- Detection on IP-Guard.
- Detection on cmd.exe.

New AI detection and visibility:

Description	Behavioral Indicator
Detects threats that attempt to modify an EFI system partition file for AV evasion.	AntiVirusEvasionModifyEfiSystemPartitionFile
Detects User Account Control (UAC) bypass by dccw.exe through PowerShell	UacBypassUsingDccwByPowershell
Detects a process registered a custom extension.	SuspiciousCustomExtension
Detects file encode/decode operation by renamed CertUtil.	FileDecodeByRenamedCertUtil
Detects attempt to bypass User Account Control (UAC).	UACBypassGeneric
Detects access token manipulation by script.	AccessTokenManiuplationByScript
Detects indirect command execution by pcalua.exe.	IndirectCommandExecutionPcalua
Detects that a process created a deceptive directory.	FakeFileName
Detects UAC bypass by mocking trusted directory.	UACBypassMockingTrustedDirectory
Detects proxy execution by pubprn.vbs script.	ProxyExecutionByPubPrn
Detects that a forbidden powershell process was launched via an Outlook Web Access IIS instance.	ForbiddenOWARemotePowershell
Detects that an encoded PowerShell process was launched via an Outlook Web Access IIS instance.	EncodedOWARemotePowershell
Detects that an obfuscated powershell process was launched via an Outlook Web Access IIS instance.	ObfuscatedOWARemotePowershell

Barracuda
Managed XDR™

Description	Behavioral Indicator
Detected a loop that continuously modifies the system time.	SystemTimeModificationLoop
Extended logic for Raspberry Robin. Detects the Msiexec process downloading a suspicious payload.	MsiexecPayloadDownload
Detects hook removal after unsigned processes or LOLBins read Kernel32/KernelBase from disk	HookRemovalAttemptAfterKernelDllReadByUnsignedProcess
Detects hook removal after unsigned processes or LOLBins read NTDLL from disk	HookRemovalAttemptAfterNtdllReadByUnsignedProcess
Detects when a process attempts to bypass User Account Control (UAC) using auto-elevated binary	UACBypassAutoElevation
Detects the first stage SocGholish Attack pattern	SuspiciousSocGholish
Detects persistence registration by a process related to a downloaded archive file	PersistenceFromDownloadedArchive
Detects suspicious RunDLL execution behavior from a shortcut in an external drive	RunDLLFromExternalLnk
Detects suspicious RunDLL execution behavior from a shortcut in an ISO drive	RunDLLFromLnkInIso
Suspicious Powershell behavior from external drive.	PowershellFromExternalLnk
Detects the execution of a malicious multi-stage PowerShell dropper	MaliciousPowershellChainedInterpreterDropper
Detects scheduled task registered with LOLBins execution from shortcut in ISO drive	PersistentForbiddenScheduledTaskFromIso
Detects scheduled task registered by shortcut in ISO drive	PersistentScheduledTaskFromIso
Detects Core Impact framework was executed	CoreImpact
Detects a process created a symbolic link from a file with a network path to a file in the system directory which then might be used for LPE exploits	SymlinkFromSystemPathToNetworkPath
Detected a process created a symbolic link to a file in the system directory which might be used for LPE exploits	SymlinkWithSystemPath
Detects the execution of services.exe with an unusual parent process	SuspiciousServicesExecution

Barracuda Managed XDR™

Description	Behavioral Indicator
Detects attempt to evade monitoring with an indirect syscall executation and unexpected function	IndirectSyscallThroughUnexpectedFunction
Detects use of ransomware indicators by unsigned process	KnownRansomwareFilesByUnsignedProcess
Detects ransomware artifacts created by unsigned process	RansomwareArtifactsDroppedByUnsignedProcess
Detects suspicious use of regsvr from LNK files	SuspiciousRegsvrFromLnk
Detects suspicious regsvr execution behavior from a shortcut in an external drive	RegsvrFromExternalLnk
Detects suspicious regsvr execution behavior from a shortcut in an ISO drive	RegsvrFromLnkInIso
Detects suspicious regsvr execution behavior from a shortcut in a network share	RegsvrFromLnkInNetworkShare
Detects execution of malicious interpreter from WMI by a remote process	MaliciousInterpreterFromWmiExecutedRemotely
Detects execution of malicious cmd from WMI by a remote process	MaliciousCmdFromWmiExecutedRemotely
Detects execution of cmd from a scheduled task by a remote process	ScheduledTaskCmdCommandExecutedRemotely
Detects cmd service creation by a remote process	RemoteServiceCreatedForCmd
Detects service creation for cmd	ServiceCreatedForCmd
Detects cmd command service creation by a remote process	RemoteServiceCreatedForCmdWithArgs
Detects accesses (web-surfing) to an IIS web-shell	IISWebshell
Detects the creation of a process from an IIS web-shell	ForbiddenProcessFromIISWebshell
Detects the creation of a process from an IIS web-shell	ForbiddenProcessFromNewThreadFromIISWebshell
Detects the creation of a process from an IIS web-shell	ForbiddenAliveProcessFromIISWebshell
Detects NTDS.dit harvesting from direct volume access tools (such as Invoke-NinjaCopy)	DirectVolumeNtdsHarvesting
Detects when a process dumped Kerberos tickets through the LsaCallAuthenticationPackage API	TicketDumping

Barracuda
Managed XDR™

Description	Behavioral Indicator
Detects when an unknown process with an Agent token was created	UnknownProcessWithAgentTokenCreated
Detects when the store of plaintext passwords in memory was disabled or enabled	EnableMemoryPlaintextPasswords
Detects code injection to other process memory space via unknown usermode callback	UnknownUserCallback
Detects a process attempted a kerberos attack using Rubeus	PotentialKerberosAttackAttempt
Detects LSASS loaded an unknown extension library	LsassUnknownSspLibraryLoad
Detected suspicious process disabled event log channel	SuspiciousETWChannelTampering
Detects LOLBins chained together from file in ISO drive	LolbinChainingFromIso
Detected process registered as a logon process with a name associated with Rubues	RubeusLogonProcess
Detects a PowerShell encoded command executed rundll32.exe	RundllFromEncodedPowershellCommand
Detects LSASS memory dumping with the registration of SSP packages	RegisteredUnknownSSP
Detects scheduled task registered from content with Mark-of-the-Web	ScheduledTaskFromMarkOfTheWeb
Detects direct attempts to bypass security measures and dump LSASS	DirectSSPRegistration
Detects LSASS loaded an unknown and invalid SSP package	LsassMissingSSPExport
Detected scheduled task with long malicious command line	MaliciousScheduledTaskLongCommandLine
Detects registration of scheduled task with long command line	ScheduledTaskLongCommandLine
Detects DLL loading into LSASS with undocumented registry keys	SuspiciousRegistryNtdsSSPRegistrationPersistence
Detects a reverse TCP shell was created with PowerShell	PowershellReverseTcpShell
Detects a process registered malicious registry autorun entry for persistence	ForbiddenRegistryPersistence
Detects NTDS harvesting from VSS	VssNtdsHarvestingFromRead
Detects SAM harvesting from VSS	VssSamHarvestingFromRead

Barracuda Managed XDR™

Description	Behavioral Indicator
Detects sensitive information from McAfee was accessed without permission	McAfeeSiteListInfoSteal
Detects scheduled task registered with reflective loader command	ReflectiveScheduledTask
Detects a signed process was hijacked by a suspicious DLL	DllHijackKnownProcess
Detects process attempted to bypass User Account Control (UAC) using auto-elevated binary	UACBypassAutoElevation
Detects hook removal after unsigned processes or LOLBins read Kernel32/KernelBase from disk	HookRemovalAttemptAfterKernelDllReadByUnsignedProcess
Detects hook removal after unsigned processes or LOLBins read NTDLL from disk	HookRemovalAttemptAfterNtdllReadByUnsignedProcess

New AI indicators for analysis and threat hunting:

Description	Behavioral Indicator
Detects execution of potentially malicious JavaScript files downloaded from the internet.	SuspiciousDownloadedJS
Detects ScareCrow shellcode loader.	HackTool_ScareCrow
Detects the creation of a process from a non-standard IIS web-shell.	ForbiddenProcessFromOtherIISWebshell
Detects the creation of a process from a non-standard Apache web-shell.	ForbiddenProcessFromOtherApacheWebshell
Detects the creation of a process from a non-standard Apache Tomcat web-shell.	ForbiddenProcessFromOtherApacheTomcatWebshell
Detects the creation of a process from a non-standard IIS web-shell.	ForbiddenProcessFromNewThreadFromOtherIISWebshell
Detects the creation of a process from a non-standard Apache web-shell.	ForbiddenProcessFromNewThreadFromOtherApacheWebshell
Detects the creation of a process from a non-standard Apache Tomcat web-shell.	ForbiddenProcessFromNewThreadFromOtherApacheTomcatWebshell

Barracuda
Managed XDR™

Description	Behavioral Indicator
Detects the creation of a process from a non-standard IIS web-shell.	ForbiddenAliveProcessFromOtherIISWebshell
Detects the creation of a process from a non-standard Apache web-shell.	ForbiddenAliveProcessFromOtherApacheWebshell
Detects the creation of a process from a non-standard Apache Tomcat web-shell.	ForbiddenAliveProcessFromOtherApacheTomcatWebshell
Detects dumping of LSASS memory using registration of remote SSP packages.	RemoteSSPRegistration
Detects dumping of LSASS memory using direct registration of remote SSP packages.	DirectRemoteSSPRegistration
Detects persistence registration by a process related to a downloaded archive file.	PersistenceFromDownloadedArchive
Detects persistence registration by an LNK process or root LNK process.	PersistenceFromLnk
Detects pseudo-console creation by a forbidden spawn	PseudoConsoleCreatedByForbiddenSpawn
Detects pseudo-console creation by an unsigned process.	UnsignedProcessCreatedPseudoConsole
Detects pseudo-console creation.	PseudoConsoleCreated
Detected a process hogging memory in an attempt to blind EDR.	MemoryHogger
Detects when a process changes the system time multiple times.	MultipleSystemTimeChanges
Detects changes made to the AutodialDLL registry value that may establish persistence privileges	AutodialDllPersistence
Detects the InternalMologue attack using fabricated NTLM challenges	InternalMonologue
Detects when a process modifies the registry to enable NTLMv1. This is used by the Internal Monologue attack.	NtlmDowngrade
Detects Ekko's Sleep Mask packer	EkkoSleepMask
Detects Foliage's Sleep Mask packer	FoliageSleepMask

Barracuda Managed XDR™

Description	Behavioral Indicator
Detects Foliage's SleepMask packer with obfuscation using trampolines	ObfuscatedFoliageSleepMask
Detects when a process attempts to bypass User Account Control (UAC)	UACBypassGeneral
Detects when a process loads an unallowed DLL to bypass defenses	PreloadDllLoaded
Detects remote installation using msiexec	RemoteMsiInstallation
Detects a process attempt to bypass User Account Control (UAC) by using Scheduled Task	UACBypassScheduledTask
Detects when a Mavinject process is created	MavinjectExecution
Detects when the Windows Event Log service thread is terminated	EventLogServiceThreadTerminated
Detects process manipulation that aims to bypass detection from EDR vendors. Detects the EtwTi tampering bypass technique.	EtwtiTampering
Detects the usage of LetMeowIn in LSASS dumps	LetMeowIn
Detects remote Sam harvesting from VSS	VssSamHarvestingRemote
Detects remote Ntds harvesting from VSS	VssNtdsHarvestingRemote

Contact the SOC if you have any questions.

Thank you.