ClearSkies™ NG Endpoint Detection & Response (EDR)

Agent Version 6.3

Incorporating the power of

Big Data Advanced Security Analytics

Jul 2020

Release Notes

Table of Contents

Overview

ClearSkies™ NG EDR Agent v6.3 is a comprehensive Endpoint Detection & Response solution, fully integrated with ClearSkies™ SaaS NG SIEM. It complements the detection of and response to never-before-seen targeted attacks and insider threats with the use of Behavioral Monitoring and Analysis (BMA), and by leveraging Advanced Security Analytics complemented by Threat Intelligence and signature-based detection.

What's New in v6.3:

New Features:

- Detection of missing/recommended security patches as well as related vulnerabilities that could impact the integrity and availability of information assets
- Automatic updating of policy changes and related updates using an encrypted tunnel when working remotely
- Collection and analysis of SQL Trace (Audit) Events
- Correlation of DHCP log and event data within UEBA
- And many more that improve effectiveness and user experience…

Important note:

To avoid operational conflicts between any other antivirus/antimalware agents that might be running on the in-scope assets make sure that you whitelist the following folders paths on those products prior to installation.

The folder paths to whitelist:

- C:\Program Files (x86)\Odyssey\ClearSkies NG Endpoint
- C:\ProgramData\Odyssey Consultants

Enhancements

Several major new enhancements are introduced in this new ClearSkies™ NG Endpoint Detection & Response (EDR) Agent version 6.3:

Behavioral Analysis Tool/Application

- Redesigned and upgraded graphical user interface
- Watchdog service enhancement/upgrade:
  - Improved detection capability through refined Sysmon configurations
  - Performance enhancements
- File Integrity Monitoring (FIM) enhancements:
  - Redesigned and upgraded graphical user interface
  - No file count and file size restrictions
  - Capability to monitor entire drive volumes
  - Improved performance

Management Tool/Application

- Redesigned and upgraded graphical user interface:
  - New overview page illustrating important metrics
  - Global iCollector and Incident/Alert settings can now only be configured in the 'Policies' page
  - Policies can now only be scheduled in the 'Policies' page
  - Versions can now only be scheduled in the 'Schedules' page
  - Schedules can now be deleted
  - Endpoints that exhibit loss of communication with the iCollector for more than 30 days are automatically removed, and they can reappear when they become active
- New information logsource prerequisites are now displayed in the agent policy configuration screen

General

- Log and event data forwarding to the iCollector using SFTP now uses higher compression:
  - The Agent compresses and forwards log and event data via SFTP to the iCollector for improved performance and bandwidth utilization
- Redesign of the Agent's services architecture:
  - The Agent now supports the collection of logsources and other functionalities contained in multiple services for improved service integrity and performance

Bug Fixes

This version resolves a number of stability and performance issues identified.

Previous Versions Highlights

Version 6.0.2

- Support for SWIFT Alliance Entry
- LogFile Forwarder support for compressed files. File Types supported: AR, ARJ, CAB, CHM, CPIO, CramFS, DMG, EXT, FAT, GPT, GZip, HFS, IHEX, ISO, LZH, LZMA, MBR, MSI, NSIS, NTFS, QCOW2, RAR, RPM, SquashFS, UDF, UEFI, VDI, VHD, VMDK, WIM, XAR, Z, Zip
- Performance fixes and improvements

Version 6.0.3

- Support for OSI Soft Pi Historian

Version 6.1

- Automated Response Actions (Simulated Block, Block, Quarantine)
- Signature-Based Analysis
- Application Control
- Operational Status and Configuration Interface
- Real-Time Visibility of Suspicious and/or Malicious Activities
- New Log Sources Supported
  - Microsoft DNS logs client/server
  - W3C logs
- Enhanced Reporting Capabilities
- Online and Offline Protection
- Behavioral Monitoring & Analysis (Watchdog)
- Built-In Threat Intelligence
- User & Entity Behavior Analysis (UEBA)

Version 6.1.4

- Active Directory information forwarding.
- Enhanced W3C logs support.
- Log File Forwarder customization.
- Improved automated response logic.
- Windows OS & Patches.

Version 6.2

- Watchdog performance enhancements
- Log File Forwarder bug fixes

Version 6.2.1

- Removed “Discarding old log” functionality pertaining to old IIS logs
- New log message in IIS logs when date and time fields are absent

Version 6.2.2

- Support for IIS nested folders
- DNS analytical performance enhancements

Version 6.2.3

- New functionality for Agent services to detect and workaround .Net Runtime errors
- Windows module configuration bug fixes

Appendix: Minimum system requirements

The minimum system requirements for ClearSkies™ NG Endpoint Detection & Response (EDR) Agent v6.3 are as follows:

CPU: Intel quad core or equivalent processor

Memory (RAM): 8 GB

Available free hard disk space: 20 GB free space