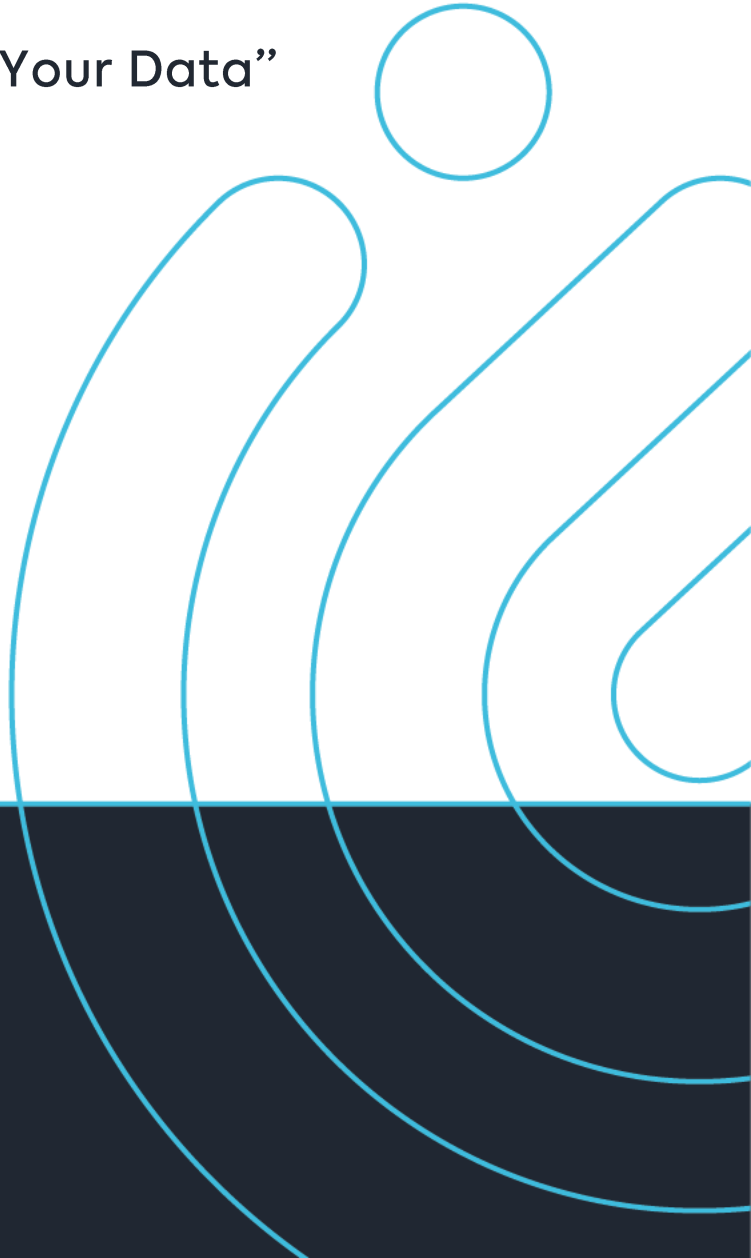
RELEASE NOTES

ClearSkies™

Endpoint Detection & Response (EDR)

Version 6.7 / July 2022

“Unlock the Intelligence of Your Data”



ClearSkies™

Table of Contents

Overview **1**

Important Notes 1

What's New in v6.7 ..... **1**

New Features **2**

Behavior Analysis 2

Enhancements **3**

Behavior Analysis 3

Bug fixes **4**

Overview

This version release of ClearSkies™ EDR includes features and enhancements which empower the detection and response of cyber, insider and third-party threats by utilizing Behavioral Monitoring and Analysis (BMA) which leverages ClearSkies™ advanced security analytics and Threat Intelligence.

Important Notes

Please refer to "New Features" and "Enhancements" sections for further information.

What's New in v6.7

- **New Functionality:**
  - Enhanced the detection and response capabilities with the introduction of:
    - Process Tampering,
    - DNS traffic monitoring for detecting C&C (Command and Control), malware and web sites hosting exploits and/or scam/phishing campaigns,
    - Critical files deletion detection, and
    - Office macro commands execution detection.
- **Other Enhancements**:
  - Improved performance and as a result the user experience with re-engineering of critical services of the EDR agent:
    - Sysmon v13.33 update
    - Watchdog Performance enhancement.

New Features

Behavior Analysis

- Endpoint Agent updated to Sysmon v13.33, now supporting 3 new Detection Events vastly enhancing detection capabilities:
  - DNS Query
  - Process Tampering
  - File Delete Detected

Enhancements

Behavior Analysis

- "Network Connections" and "DNS Queries" events toggle button introduced in the "Behavior Configuration" of "LogSources" in the "iCollector Configuration" enhancing the configuration of Behavioral LogSources.
- New "Office Macro Command Execution" malicious activity introduced in "Activity Configuration" of a Policy detecting macro command execution by Microsoft Office Products.
- New "Sysmon eventID" field introduced in behavioral process LogSources.
- Watchdog performance enhanced.

Bug fixes

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