RELEASE NOTES

ClearSkies™

Endpoint Detection & Response (EDR)

Version 6.6 / January 2022

ClearSkies™

Table of Contents

Overview **1**

Important Notes 1

What's New in v6.6 .... **1**

New Features **2**

YARA 2

Management 2

Enhancements **3**

Behavior Analysis 3

Management 3

Log File Forwarder 3

Active Directory 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 v6.6

- **YARA support:** Out-of-the-box rules and packages that contribute to the early detection and response based on textual and/or binary patterns of threats related to malware families.
- **Other Enhancements**: Improved user experience via enriched effectiveness of existing functionality.

.

New Features

YARA

“YARA” Tool/Application introduced in “ClearSkies^{TM} Endpoint” ServiceModule granting access to “YARA Rules” and “YARA Packages”, enhancing EDR detection mechanisms. “YARA” facilitates threat hunting by providing users with the ability to manually create new or utilize preconfigured out-of-the-box YARA rules and packages.

This functionality enhances the Extended Detection and Response (XDR) capabilities of ClearSkies^{TM} “Threat & Vulnerability” platform, that unifies all ClearSkies^{TM} line of products into a cohesive security operations platform for the early Detection, Response and Threat Hunting.

Management

Endpoint Engine supports EDR Soft Isolation SOAR requests forwarded by ClearSkies^{TM} SIEM. The EDR agent blocks all IP connections to isolate the Endpoint from the network, except the ones to the “iCollector”. Soft Isolation can be deactivated to restore connections.

Enhancements

Behavior Analysis

New “Type” and “Activity” buttons added in “Activities” pie charts for enhanced filtering capabilities according to type of activity or specific activity.

Management

- New “Detection Categories” tab added in “Global Settings” window of the “Overview” page for enhanced malware detection configuration.
- “YARA Rules Modifications (Last 30 Days)”, and “YARA Packages Modifications (Last 30 Days)” introduced in “Overview” page of the “Management” Tool/Application for easy access to the latest modifications in the “YARA” page.

Log File Forwarder

- “Programs” dropdown list introduced in “Log File Forwarder Configuration” window of the “Settings” for simplified program selection for synced or custom programs.

- NXLog Configuration enhanced for optimized CPU and Memory performance.

- The number of files of monitored folders was limited to 30.000 to ensure optimal performance and memory usage.

Active Directory

The Endpoint agent now detects if the Endpoint is an Active Directory Domain Controller and that no PowerShell scripts are executed on workstations for improved overview and configuration.

Bug fixes

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