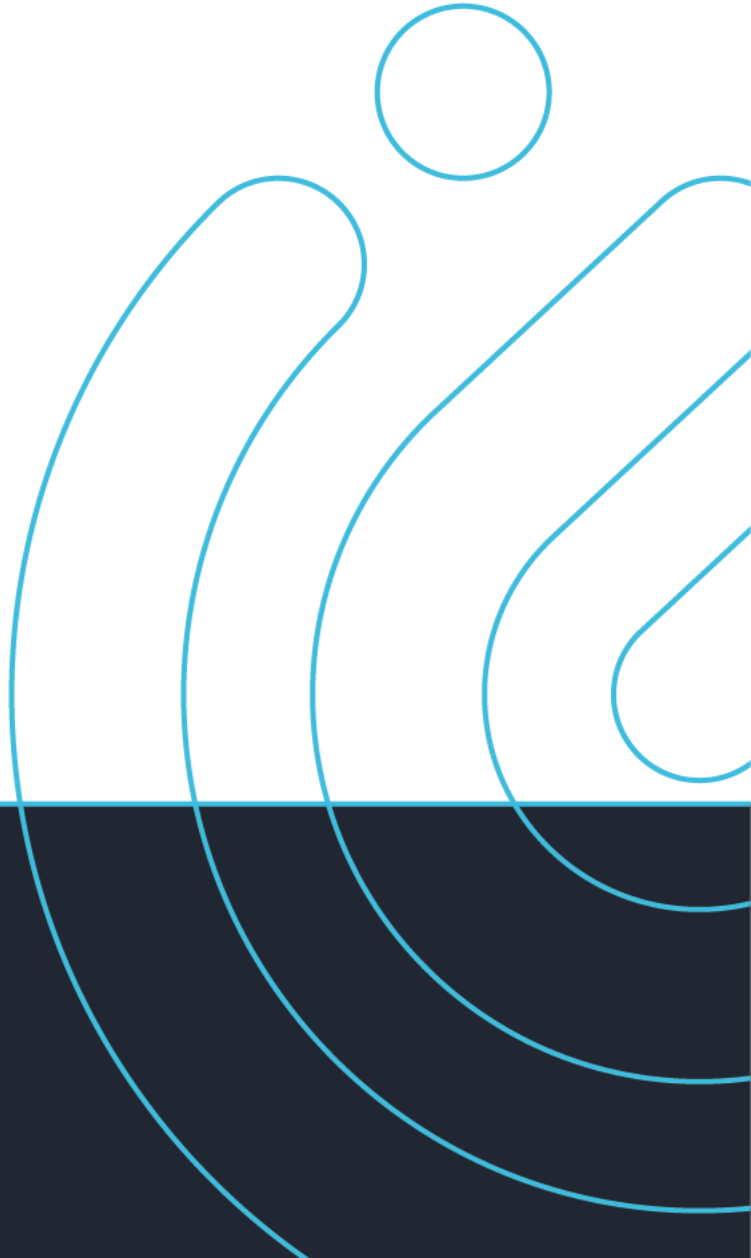
RELEASE NOTES

ClearSkies™

Endpoint Detection & Response (EDR)

Version 6.4 / April 2021



ClearSkies™

Table of Contents

Overview **1**

Important Notes 1

New Features **2**

System Tray (Desktop interface) 2

Active Defense Beacon Traps 2

Enhancement **3**

General 3

Overview

ClearSkies™ EDR Agent v6.4 is a comprehensive Endpoint Detection & Response solution, fully integrated with ClearSkies™ Cloud 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.

Important Notes

No special considerations applicable for this version.

New Features

System Tray (Desktop interface)

To help users keep track of their endpoints' performance and availability, as well as to help with conclusive incident investigations, the "Activity" panel now features the new "Performance" tab, which displays performance metrics (CPU, memory) of the all Windows services related to the ClearSkies™ Endpoint Detection & Response (EDR) Agent. The metrics are taken from averages of 1-minute intervals, and display 24-hour and 1-hour historical charts.

Active Defense Beacon Traps

In conjunction with ClearSkies™ Active Defense, the ClearSkies™ Endpoint Detection & Response (EDR) Agent monitors file system activity of users and applications on beacon traps in an effort to spot suspicious/malicious behavior.

ClearSkies™ Active Defense 'Beacon Traps' use fake information and "poisoned data" as bait to lure threat-actors. This information consists of different file formats and is placed strategically amongst real information to aid in the early detection of suspicious activities related to unauthorized use and/or access.

Fake information may have the form of email accounts, user credentials, financial spreadsheets and document files related to intellectual property or any other valuable information.

Any attempt to copy, access, modify or use this information by threat actors automatically triggers an Alert/Incident, while a similar action involving "real" information/data would have gone unnoticed, allowing the attacker to continue their silent perpetration through the organizational infrastructure.

Enhancement

General

- For easier deployment, the ClearSkies™ Endpoint Detection & Response (EDR) services now start automatically when the Agent configuration files are pre-deployed.
- Endpoint PowerShell scripts are digitally signed to allow their execution on hardened endpoints (workstations and servers).