RELEASE NOTES

ClearSkies™ TDIR Platform Version 6.7 / June 2024

“Unlock the Intelligence of Your Data”

Table of Contents

Copyright Notice

While every precaution has been taken in the preparation of this document, Odyssey Consultants LTD assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

Trademarks

Refer to the Copyright page http://www.clearskiessa.com/copyright for a list of our trademarks.

Feedback

Odyssey Consultants is engaged in a continuous effort to improve its documentation. Please help us by sending your comments to erratum@clearskiessa.com

Overview

This version release of ClearSkies™ Threat Detection, Investigation and Response (TDIR) includes features and enhancements that empower organizations and MSSPs of any size, in any industry, to effectively anticipate, respond, swiftly recover and adapt to the emerging threats and vulnerabilities of a dynamically evolving and expanding threat landscape.

What’s New in v6.7

Several new features, functionality enhancements, and bug fixes are introduced in ClearSkies™ TDIR platform version 6.7, including:

- **Multilingual Support**: ClearSkies MSSP and SWP portals now and in Arabic. The support of Arabic language demonstrates our ongoing commitment to better serve our customers in different geographic regions.
- Expanded SOAR Capabilities with the support of:
  - SentinelOne
  - SophosCentral
  - Microsoft Defender for Endpoint
- Enhanced Threat Intelligence feeds with the support of:
  - RST Cloud Threat Intelligence

Important Notes

No special considerations applicable for this version.

New Features

- **Multilingual Capabilities**:
    - **MSSP and SWP Portals**: Allows you to preselect the preferable language on the login screen and within the MSSP and SWP portals.

Marketplace New Integrations

- **SentinelOne**: Enhance endpoint protection and threat detection capabilities.
- **SophosCentral API**: Streamlined access to Sophos security services.
- **RST Cloud Threat Intelligence Feed**: Integration with RST Cloud Threat Intelligence Feed to enhance threat detection, investigation and response.
- **MS Defender**: Enhance endpoint threat detection and response.

TDIR Platform Enhancements

- **CVE Severity Appearance**: To reduce user confusion and enhance clarity.
- **SOCRadar Integration**: To enhance threat detection, investigation and response..
- **Microsoft Sentinel Performance improvement**: To improve performance .
- **Correlation Engine**: To enhance Alert Filtering to improve alert management.
- **SOAR Engine Logging Optimizations**: To improve performance .
- **Correlation Engine Log Memory Optimizations**: To improve performance
- **Field Selector Enhancement**: For selecting multiple fields in the “Field Selector” when creating and customizing reports.
- **Enhanced Error Reporting**: To provide more detailed and actionable error information related to “ManageEngine ServiceDesk Plus” platform.
- **Check Point SOAR Integration**: For providing more flexibility and control during configuration.

MSSP Platform Enhancements

- **Correlation rules (Use Cases) deployment:** Flagged Correlation Rules / Use Cases only can be edited only from MSSP portal admins to ensure better management and maintenance.
- **Performance Overview** : To improve the performance and user experience.
- **Incident Management:** Ability to open multiple Incidents in separate windows, to improve incident management.

Bug fixes

- **Indicators**: Resolved a visual slash issue on Mac systems.
- **Reports - Portal Data**: Fixed an issue where the asset IP field sometimes returned hostnames instead of IPs.
- **Multiple Collectors**: Corrected the top path display of the module when the hostname is too long.
- **Escalation Order**: Removed an extra column in the escalation order.
- **Threat Level Manager**: Enhanced CVEs search by description validation.
- **Row Number Columns**: Fixed an issue with hidden row numbers.
- **Assets Module**: Adjusted spacing between SNMP and Netflow dropdowns.
- **Identity and Access - Global (UI)**: Resolved a multi-site domain issue in the user interface.
- **Identity and Access - Global (Webservices)**: Fixed a multi-site domain issue affecting web services.
- **Alias Manager**: Ensured the correct pop-up appears when saving with errors.
- **Notifications**: Fixed an issue preventing pop-up messages from appearing after acknowledging notifications.
- **Assets Module**: Added missing tooltips on the iCollector field.
- **Automation**: Addressed an issue stopping scheduled tasks.
- **ISRE Reports**: Fixed sorting issues in ISRE reports.
- **Report Creation**: Resolved a non-functional create change page.
- **ISRE Graphs**: Corrected issues with graphs under the Responding to Reported Incidents section.
- **Report Portal Data**: Fixed a casting issue in the ReportPortalData.
- **Report Modules**: Aligned icons in the report modules columns.
- **SOAR IP Policies**: Fixed a response filter issue with SOAR IP policies.
- **Active Defense Management**: Resolved an interface filter issue.
- **Group Module**: Fixed data export issues.
- **Wizard Reports**: Corrected the number of selected items displayed in the dropdown.
- **Group Values**: Fixed a UI issue with the edit component on the grid.
- **Async Processing**: Ensured previous calls are aborted properly.
- **Localization and Locale**: Fixed reference issues between localization and locale.
- **Start Menu**: Resolved a search icon issue in the start menu.
- **Active Defense Beacon Traps**: Fixed export issues for policies and schedules.
- **Active Directory**: Corrected export issues in the overview grid (Enabled field).
- **Report Export**: Fixed export issues in the Managed By column in Create Log Data Reports.
- **UI**: Fixed paging issues in the Incidents module.
- **UI**: Resolved a datepicker hover issue.
- **UI**: Fixed an export file issue related to maintenance status in the Asset Module.
- **UI**: Addressed horizontal scrolling issues in Alerts > View Logs.
- **Data Masking**: Fixed inconsistencies in data masking functionality.
- **UI**: Resolved path arrow inconsistencies in the sidebar, widgets, and toolbar.
- **UI**: Fixed issues with disabled reports pop-up messages during report creation.
- **UI**: Ensured the iCollector toolbar path remains after navigating to SOAR and Endpoint Management.
- **Report Generation**: Addressed various issues with report generation.

Important Note: This release brings substantial performance, usability and effectiveness capabilities with the introduction of new vendor/product integrations.

Thank you for your continued support, insights and valuable feedback.

Appendix A: New Supported Vendor/Products

Vendor	Product	Product Category	Product Version [5]	Log Collection Method
One Identity	PAM - Safeguard for Privileged Passwords	Access Control	7.3	Syslog CEF
One Identity	PAM - Safeguard for Privileged Sessions (Management)	Access Control	7.1.1	Syslog CEF