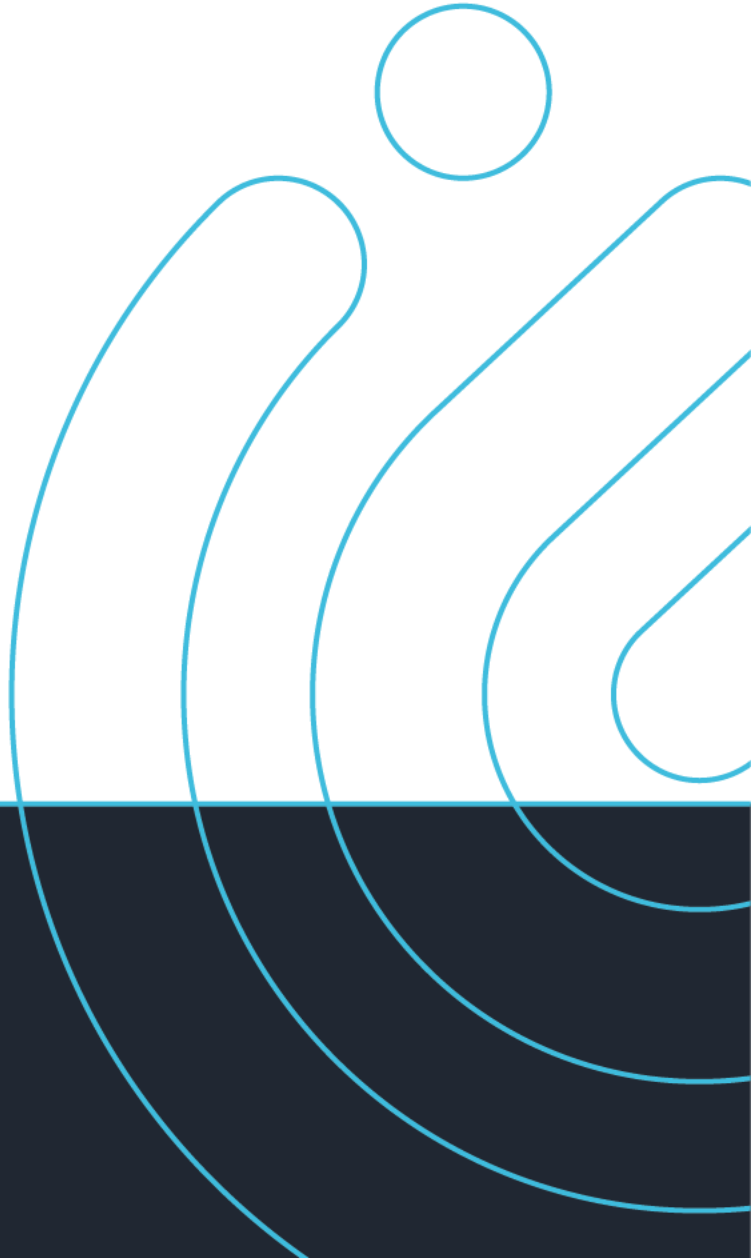
RELEASE NOTES

ClearSkies™
Cloud SIEM
Version 6.4 / July 2021



ClearSkies™

Table of Contents

Overview 1

What's New in v6.4 1

Important Notes 1

New Features 2

"ServiceModules" 2

"General" 2

Enhancements 4

"ServiceModules" 4

"TopMenu" 4

Bug fixes 6

New Supported LogSources 7

Overview

Digital Transformation is changing the world, and we are constantly staying ahead of the curve to anticipate the digital risks emanating from the rapid expansion of the information-threat landscape.

In keeping with our principle “to fulfil our clients’ needs and exceed their expectations”, we are continuously revamping our platform with new innovative features and enhancements.

Such features and enhancements are testament to our pioneering role in the uncharted territory for the early detection of and response to targeted attacks, data breaches and user suspicious/malicious behavior, by utilizing the power of Big Data Advanced Analytics.

What’s New in v6.4

Several new features, functionality enhancements and bug fixes are introduced in this ClearSkies™ Cloud SIEM version 6.4 including:

- **Automated Security Orchestration, Automation and Response (SOAR) capabilities** are now integrated across all ClearSkies™ line of products, providing users with the ability to orchestrate and automate responses.
- **Improved User Experience** through dynamic dashboards.
- **Expanded Vulnerability Management capabilities** with the integration of IthacaLabs™ Vulnerability Assessment tool.
- **Time-saving functionality** of reverting deleted assets.
- **Improved real-time situational awareness** with the use of Widgets which gives timely information from your favorite “ServiceModules-Applications” at a glance.
- **Complement UEBA behavioral access monitoring** with location awareness.
- Other improvements that enhance User Experience.

Important Notes

No special considerations applicable for this version.

New Features

"ServiceModules"

SOAR (Security Orchestration, Automation and Response) Service Module

SOAR functionality is now integrated across all ClearSkies™ line of products, providing users with the ability to orchestrate and automate responses, such as blocking the communication of specific IP subnet/address from and/or using the ClearSkies™ EDR Agent to isolate from the network workstations designated as suspicious/malicious.

In the upcoming release of ClearSkies™ (scheduled end of September 2021), the SOAR functionality will be integrated within the Event Management ServiceModule that will allow users to orchestrate and automate responses based on the outcome of a correlation rule.

Supported products for Orchestration and Automation:

- Check Point Firewalls
- Cisco ASA
- FortiGate Firewalls
- Palo Alto Firewalls (w/ Panorama)
- ClearSkies™ EDR

Analytics

- Complement UEBA behavioral access monitoring with location awareness
    - The User & Entity Behavior Analysis (UEBA) is enhanced with a new analytical model. The Geolocation Login model detects anomalies in regards to the physical location of the user during login attempts to the organization, raising attention for further investigation.

"General"

Dynamic Dashboards

Dynamic screen sliding capability added between the ISRE dashboard, the Home Screen and the Widgets screen for improved workflows. Additionally, the ISRE icon in the center of the TopMenu was replaced with the icon of the organization.

Widgets

A Widgets screen was added containing various metrics related to your organizational posture, providing easy access to the figures more important to your organization such as:

- EDR responses
- EDR Activities
- Top 10 Indicator Categories
- Geolocation of Inbound Traffic

- Enterprise Endpoints
- Outdated Endpoints
- Events by Category
- Threat Alert Level
- Log & Event Data Timeline

Widgets can be drag-and-dropped onto any location in the Home Screen.

Enhancements

A number of enhancements were made for improved functionality and user experience.

“ServiceModules”

Vulnerability Management

- Manage Scans
    - Support for XML Report by IthacaLabs™. Odyssey’s IthacaLabs™ Threat Research & Assessment services help you assess your organization’s readiness, resilience, risk level and response capabilities in stopping, containing and mitigating targeted attacks.

Endpoint

- Management
    - “.NET Framework” dropdown list in “Edit” and/or “New schedule” window of the “Schedules” page removed for simplicity.

Reports

- Create
    - In the “Information Security Risk Exposure”, monthly ISRE report now set by default.

“TopMenu”

Admin

- Assets
    - “Active Status” dropdown menu for filtering main grid results according to available options “Active”, “Pending” and “Deleted” assets. Ability to revert a deleted asset to active status was added by selecting an asset, clicking “View”, and then clicking the new “Revert Back” button.
    - New column "Last logged" added to the “Logsources section of an asset’s “View” details window, indicating the time the last log was forwarded.

Tools

- Downloads
    - The “Md5 hash” column now hidden by default and can be reinstated through the column sorting and filtering options. Additionally, new “File Name” column introduced.

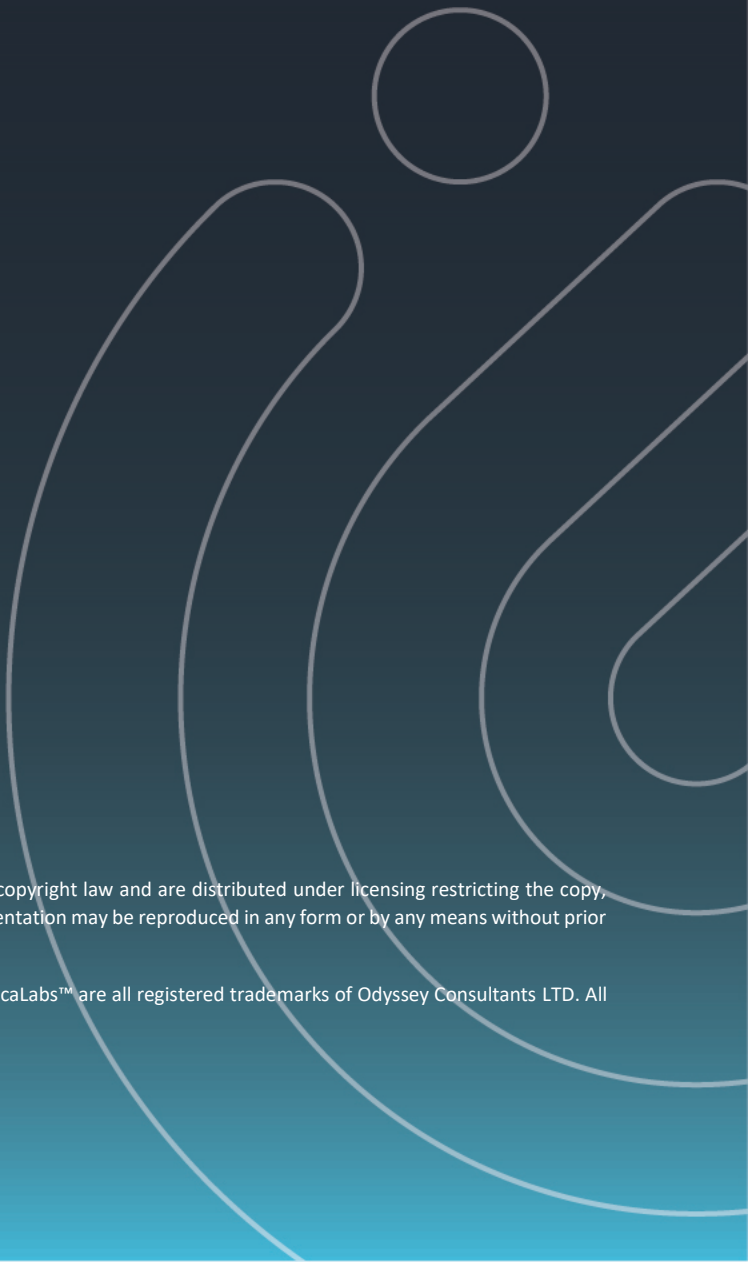
- Resources
    - The “Md5 hash” column now hidden by default and can be reinstated through the column sorting and filtering options. Additionally, new “File Name” column introduced.

Bug fixes

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

New Supported LogSources

Vendor	Product	Product Category	Version	Type of Collection
Huawei	Huawei Switch	Network Management	firmware V200R019C10	Syslog



© 2021 Odyssey Consultants LTD.

All rights reserved. This product and related documentation are protected by copyright law and are distributed under licensing restricting the copy, distribution, and reverse-engineering. No part of this product or related documentation may be reproduced in any form or by any means without prior written permission from Odyssey Consultants LTD.

Trademarks © 2021 Odyssey Cybersecurity™, ClearSkies™, iCollector™ and IthacaLabs™ are all registered trademarks of Odyssey Consultants LTD. All other marks mentioned herein are trademarks of their respective companies.

Copyright © 2021 Odyssey Consultants LTD. All Rights Reserved.