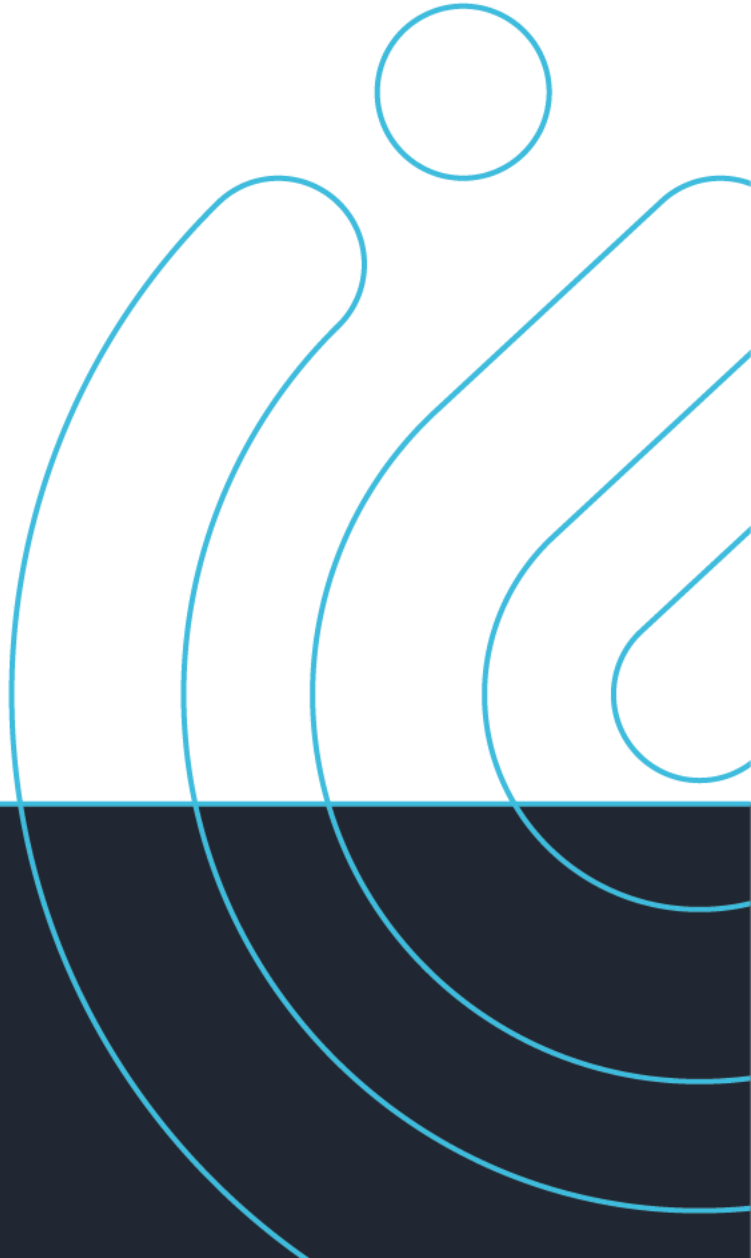
RELEASE NOTES

ClearSkies™

SWP Threat Detection, Investigation and Response (TDIR)

Version 6.6.3/ November 2023

"Unlock the Intelligence of Your Data"



ClearSkies™

Table of Contents

Copyright Notice **1**

Trademarks **1**

Feedback **1**

Overview **2**

What's New in v6.6.3 ..... **2**

Important Notes 2

New Features **3**

Support of New Assets 3

Threat Intelligence 3

Security Orchestration Automation and Response 3

Bug fixes **3**

Appendix A: New Supported Vendor/Products **4**

Appendix B: SOAR New Integrations **5**

Copyright 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™ SWP 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 v6.6.3

Several new features and enhancements are introduced in ClearSkies™ SWP Threat Detection, Investigation and Response (TDIR) platform version 6.6.3, including:

- **Assets:** Support the collection and analysis of log and event data from a plethora of new Vendor/Products.
- **SOAR**: Integration with a number of diverse products.
- **Threat Intelligence**: Support of a new threat intelligence feed.
- **Other Enhancements:** Enriched user experience and functionality.

Important Notes

No special considerations applicable for this version.

New Features

ClearSkies™ SWP Threat Detection, Investigation and Response (TDIR) platform Marketplace data enrichment, provides seamless integration of disparate 3rd-party technologies for broader and deeper real-time visibility, detection and analysis of what transpires in your networks and systems.

Support of New Assets

- Supports a plethora of new vendors/products of already supported products> Refer to Appendix A – "New supported Products/Vendors".

Threat Intelligence

- Integration with SOCRadar XTI.

Security Orchestration Automation and Response

- Provides the ability to Orchestrate and Automate responses with BitDefender (GravityZone) and SonicWall OS, Refer to Appendix B – "New SOAR Integrations". This integration enhances the orchestration, automate and response actions, such as block the communication of specific malicious and suspicious hosts or entire IP addresses/subnets.

Bug fixes

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

Appendix A: New Supported Vendor/Products

Vendor	Product	Product Category	Product Version	Log Collection Method	What's New
OneSpan	Identikey Authentication Server	Access Control	3.23.1	Syslog	Product support
Hewlett Packard	HP Switch	Network Management	15.11	Syslog	Version support
Aruba	Switch	Network Management	15.11	Syslog	Version support
Symantec	BlueCoat ProxySG	Web Gateway	7.3	Syslog	Version support
Trend Micro	Deep Discovery Email Inspector	Email Gateway	5.1	Syslog (CEF)	Product support as standalone
IBM	IBM Storwize	Data Storage	6.2	Syslog	Version support
Cimcor	Cimcor Cimtrak	File Integrity Monitoring	4.1.2	Syslog	Version support
Juniper	Juniper Switch	Network Management	21	Syslog	Version support
Juniper	Juniper	Firewall	21	Syslog	Version support
VMWare	VMWare	Virtualization	7.3	Syslog	Version support
VMWare	vSAN	Audit	7.3	Syslog	Version support
Sophos	Sophos XG Firewall	Firewall	19.5.3	Syslog	Version update

Appendix B: SOAR New Integrations

Vendor	Product	Product Category	Product Version	Communication Method	What's New
BitDefender	GravityZone	Endpoint	N/A	API	Product support
SonicWall	SonicOS	Firewall	7.0	API	Product support