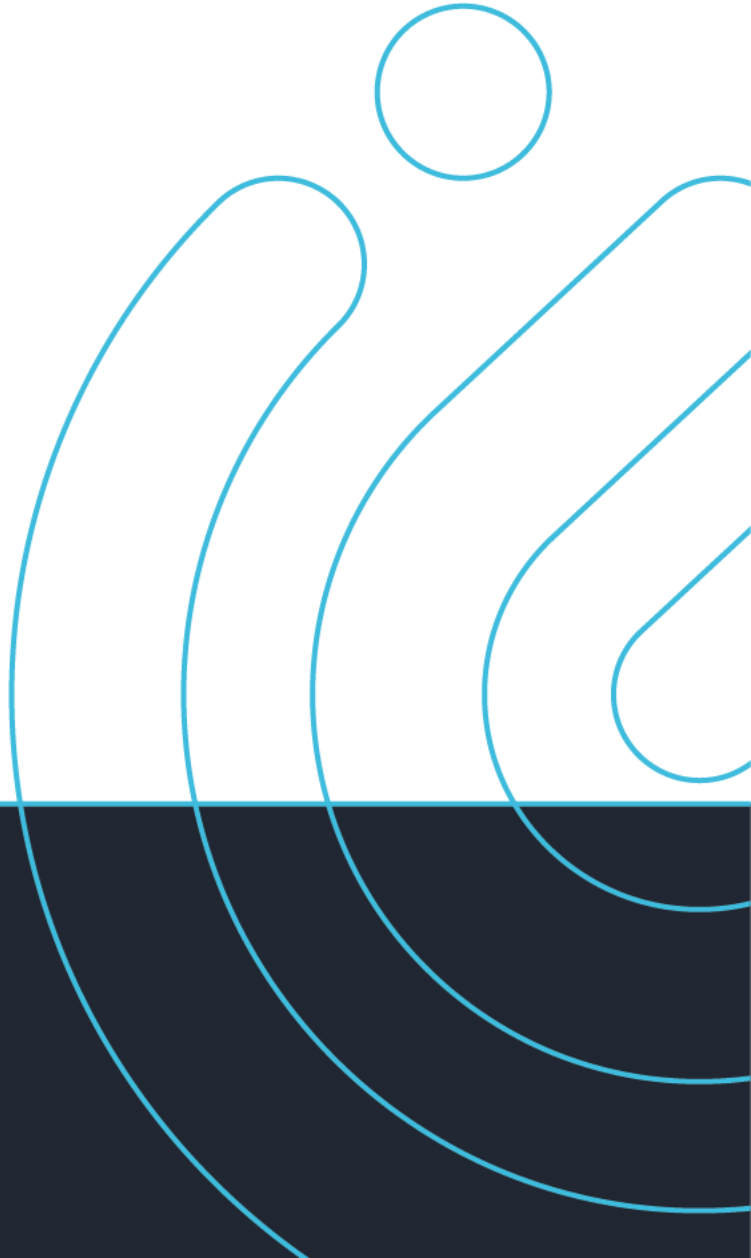
RELEASE NOTES

ClearSkies™

Cloud SIEM

Version 6.5 / January 2022

"Unlock the Intelligence of Your Data"



ClearSkies™

Table of Contents

Overview

This version release of ClearSkies™ Cloud SIEM 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 expanding and unpredictable threat landscape.

What's New in v6.5

Several new features, functionality enhancements and bug fixes are introduced in this ClearSkies™ Cloud SIEM version 6.5, including:

- **Custom Dashboards**: New "Widgets" Sidebar and Dashboard redesign provides a simplified customizable interface, enhancing user experience and productivity.
- **Other Enhancements**: Improved and enriched the effectiveness and usage of existing functionality.

Important Notes

No special considerations applicable for this version.

New Features

"General"

Custom Dashboards

- The "Dashboards" ServiceModule is migrated as Widgets. Dashboard pages are redesigned to provide to users with an easier way to organize their work environment, and have quick access to their most important Tools/Applications. Available Widgets can now be drag-and-dropped across all Dashboard pages. These Widgets can be removed, rearranged and/or relocated to any Dashboard. In addition, each Widget refreshes itself in user-defined time intervals with new and up-to-date data with the use of the "Refresh" dropdown button.

- "Dashboards" ServiceModule is redesigned as Widgets, allowing for enhanced interface customization. ServiceModule Widgets can be drag-and-dropped onto any of the Custom Dashboards, providing users with the ability to organize and have quick access to their most important Tools/Applications.

Widgets sidebar

New "Widgets" (left) sidebar introduced in "Custom Dashboards" screen for quick and easy access to the organization's most important figures. Widgets can be selected from ServiceModules and TopMenu items dropdown lists, and drag-and-dropped onto the Custom Dashboards. Upon mouse hover-over a Widget element, related drilldown figures displayed.

Enhancements

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

"ServiceModules"

Real Time Analysis

"Analytics" ServiceModule renamed as "Real Time Analysis" ServiceModule, granting access to "Big Data Search" Tool/Application enabling search through billions of current and/or historical log and event data. "Real Time Analysis" provides users with the ability to identify behavioral patterns, enhancing the discovery of suspicious and/or malicious activities critical for fending off threat actors and responding to threats.

UEBA (User & Entity Behavior Analysis)

- "UEBA" Tool/Application redesigned as separate ServiceModule for enhanced navigation and user experience. It provides users with the ability to profile and baseline user-related/host/network/application activities to detect suspicious/malicious behavior by identifying meaningful anomalies and deviations from "usual" behavioral patterns.
- Tile design of "Identity & Access", "Active Defense", "ClearSkies Endpoint" ServiceModules revamped to include "Premium" banner as add-on ServiceModules.

ClearSkies™ Endpoint

- **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.

Event Management

- **Correlation**

  - New "Soft Isolation" type added in "Isolation Type" dropdown list under the "SOAR" step in "New Correlation" and/or "Edit" window of "Rules" tab. "Soft Isolation" allows users to block all IP connections to isolate the Endpoint from the network, except the ones to the "iCollector", and can be deactivated to restore connections.

Reports

- **Create**

  - In "New Report" window, "Summary" final row introduced, appearing when selecting "Count" at the end of result set, calculating the sum of the aggregation of all counts.
  - "Sort (Direction)" column introduced in "Field Selector" of "Properties" tab in "Edit" and/or "New Report" window of "Log Data Reports" and "Portal Data Reports" tabs for enhanced sorting.
  - "Period" span of reports in "Schedule" tab in "Edit" and/or "New Report" window of "Log Data" and "Portal Data" tab limited to 6 months.
  - New "Category" option titled "License" added under "Categorization" section in "Edit" and/or "New Report" window of the "Portal Data" tab for improved reporting according to License type. Additionally, new columns in "Field Selector" and criteria in "Criteria Selector" added.

SOAR

- **Management**

  - In "Add EDR Isolation" and/or "Edit" of "EDR Isolation" page in the "Management" Tool/Application, new "Soft Isolation" selection introduced in "Isolation Type" dropdown list. "Soft Isolation" blocks all Endpoints' connections to isolate the Endpoint from the network, excluding the connection to the iCollector, and can be deactivated reinstating severed connections.

“General”

Widgets

New “Top 5 Assets (License Consumption in MBs since last reset)”, and “Top 5 Logsources (License Consumption in MBs since last reset)” widgets introduced providing customers with easy access to their Top 5 Assets, and Logsources according to their License consumption.

License Consumption

Warning pop-up messages regarding License Consumption at 60% and 70% of the total available License introduced. Switching Licenses automatically resets the warning thresholds according to the new License scheme. In addition, all blocked Logsources due to expiration of License coverage are unblocked on License change.

Asset Ownership Icon

“Odyssey” Asset Ownership icon renamed “SOC” Asset Ownership icon in all corresponding platform sections.

Bug fixes

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

New Supported Products and Versions

Vendor	Product	Product Category	Product Version	Type of Collection	What's New
Cisco	Cisco ASA	Firewall	9.8 (2)	Syslog	Version support
Cisco	Cisco Meraki Events	Network Management	15.42.1, 15.44	Syslog	Version support
Cisco	Cisco Meraki Flows	Connection Monitoring	15.42.1, 15.44	Syslog	Version support
Cisco	Cisco Meraki Security Events	IDS – IPS	15.42.1, 15.44	Syslog	Version support
Cisco	Cisco Meraki URLs	Web Gateway	15.42.1, 15.44	Syslog	Version support
Cisco	Cisco Nexus Switch	Network Management	**NX-OS**: v.7.3, v.9.7 (7a)	Syslog	Version support
Cisco	Cisco Switch-Router	Network Management	**IOS**: v.15.2 (2) E9, V.15.2 (4) E8 **IOS XE**: v.16.09.04, v.16.09.07, v.16.12.3a, v.16.12.04	Syslog	Version support

Cisco	Cisco Web Security Appliance	Web Gateway	10.1.3-054t, 11.8.0.453, 12.0.3-007	Syslog	Version support
Cisco	Cisco Wireless LAN Controller	Network Management	**AirOS**: 8.5.160.0, 8.9.111.0	Syslog	Version support
Cisco	Cisco Email Security Management	Audit	M100V (Async-OS v.13.8.1, 14.0.0-404)	Syslog	Version support
Cynet	Cynet360	Endpoint Protection	3.7.4.158, 4.2.10.10495, 4.2.12.11749	Syslog (CEF)	Version support
Cynet	Cynet360 Audit	Audit	3.7.4.158, 4.2.10.10495, 4.2.12.11749	Syslog (CEF)	Version support
Ecessa	Ecessa PowerLink	Network Management	v.11.1.2, v.12.0.1	Syslog	Version support
Hewlett Packard	HP Switch	Network Management	PD 02.06	Syslog	Version support
McAfee	McAfee WebGateway	Web Gateway	9.2.8, 10.2.4	Syslog	Version support
McAfee	McAfee WebGateway Audit	Audit	9.2.8, 10.2.4	Syslog	Version support

Mikrotik	Mikrotik Router	Network Management	6.48.1, 6.48.5	Syslog	Product support
Oracle	Oracle Cloud	Audit	-	API	Product support
Oracle	Oracle Cloud	Firewall	-	API	Product support
Palo Alto Networks	Palo Alto Access Control CEF	Access Control	8.1.5 - 10.0.2	Syslog (CEF)	Version support
Palo Alto Networks	Palo Alto Firewall CEF	Firewall	8.1.5 - 10.0.2	Syslog (CEF)	Version support
Palo Alto Networks	Palo Alto IPS CEF	IDS – IPS	8.1.5 - 10.0.2	Syslog (CEF)	Version support
Palo Alto Networks	Palo Alto System CEF	Audit	8.1.5 - 10.0.2	Syslog (CEF)	Version support
Palo Alto Networks	Palo Alto URL Filtering CEF	Web Gateway	8.1.5 - 10.0.2	Syslog (CEF)	Version support
Palo Alto Networks	Palo Alto Packet Inspection CEF	Audit	10.0.2	Syslog (CEF)	Version support
Palo Alto Networks	Palo Alto Data Filtering CEF	Anti Virus	10.0.2	Syslog (CEF)	Version support
Sophos	Sophos Email Filtering	Email Gateway	18.0.4, 18.5.1	Syslog	Version support
Sophos	Sophos Firewall Event	Audit	18.0.4, 18.5.1	Syslog	Version support
Sophos	Sophos IDS – IPS	IDS – IPS	18.0.4, 18.5.1	Syslog	Version support
Sophos	Sophos System Health	Health Status	18.0.4, 18.5.1	Syslog	Version support
Sophos	Sophos WAF	Application Firewall	18.0.4	Syslog	Version support

Sophos	Sophos XG Firewall	Firewall	18.0.4, 18.5.1	Syslog	Version support
Sophos	Sophos XG Web Filtering	Web Gateway	18.0.4, 18.5.1	Syslog	Version support
Symantec	Symantec EDR	Endpoint Protection	4.3.0, 4.6.7	Syslog (CEF)	Product Support
Symantec	Symatec EDR System	Audit	4.3.0, 4.6.7	Syslog (CEF)	Product Support
VMWare	VMWare Horizon	Application Management	v.7.11.0	Syslog	Version support