ClearSkies™ SaaS NG SIEM

Version 6.2

Incorporating the power of

Big Data Advanced Security Analytics

Sep 2020

Release Notes

Table of Contents

Overview

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 Security Analytics.

What's New in v6.2

Several new features and functionality enhancements are introduced in this ClearSkies™ SaaS NG SIEM version 6.2 including:

New Features

- **Chatbot**: Your friendly and intelligent virtual assistant "Argos[1]" embodies the new insightful chatbot functionality, promising not only to help customers accomplish more using ClearSkies™ SaaS NG SIEM and ClearSkies™ EDR Agent, but also to provide them with real-time live access to our helpdesk, including support engineers, Professional Services and Managed Security Services (MSS) analysts. Argos has the intelligence to guide users and empower them to make the most out of ClearSkies™ products.
- **New Help Module:** A vastly restructured and enhanced Help module offering comprehensive search capability covering detailed help topics pertaining to the comprehensive functionality of the ClearSkies™ SaaS NG SIEM and ClearSkies™ EDR Agent.
- **Login Page Redesign:** Redesigned from the ground up for a more pleasant look and feel.

Functionality Enhancements

- **Configuration Wizard**: For facilitating initial and ongoing configuration and maintenance of ClearSkies™ SaaS NG SIEM, the Configuration Wizard was expanded to include access to more capabilities in this centralized control panel.
- And more…

[1] In Homer's epic "The Odyssey", Argos is Odysseus's faithful dog who symbolizes loyalty.

Important Notes

No special considerations applicable for this version.

New Features

"Home Page"

- Chatbot

The "Chatbot" functionality was added as a floating drag-and-drop icon globally throughout the ClearSkies™ Secure Web Portal (SWP) interface. "Argos" functions as a virtual assistant, helping users accomplish more using ClearSkies™ SaaS NG SIEM and ClearSkies™ EDR Agent, while also providing them with real-time live access to our helpdesk, including support engineers, Professional Services and Managed Security Services (MSS) analysts. Argos is fully integrated with the latest guides, helping users/admins become experts in ClearSkies™ services with little effort.

The Chatbot is fully integrated with admin-user guides for comprehensive and targeted search results, as well as with WhatsApp for an additional live chat channel with our helpdesk, (support engineers, Professional Services, Managed Security Services (MSS) analysts).

Specifically, users can do the following when using Live Chat:

- Converse with "Argos" the chatbot to carry out searches using keywords that correspond to section headings (anchors) and/or tags.
- Have real-time chat with support engineers, Professional Services and Managed Security Services (MSS) analysts
- Leave a message to our Helpdesk to be contacted at a later time, if in a hurry.
- Call us using WhatsApp while remaining online.

"Top Menu"

- Help

The Help module was redesigned from the ground up and enhanced, providing sidebar navigation through detailed help topics (search section headings (anchors) and/or content body keywords) pertaining to the comprehensive functionality of the ClearSkies™ Secure Web Portal (SWP).

- "Magnifying Glass" Search

ClearSkies™ SaaS NG SIEM users can now carry out searches via the search "magnifying glass" TopMenu item using keywords that correspond to section headings (anchors) and/or tags.

“Login Page”

- Login

  The Login page were redesigned and enhanced with an animated background and improved look for an upgraded user experience. Additionally, the security questions in the initial sign up process have now become part of the Configuration wizard.

“About”

- About

  The “About” page (accessible through the ClearSkies clickable logo) was redesigned from the ground up and enhanced, providing sidebar navigation for an improved visualization and with updated information.

Enhancements

"ServiceModules"

Event Management

- Incidents
  - In the "Alerts" tab of the "Evidence Logs" tab, all the information in an alert listing can now be selected/highlighted and copied to be pasted as text.

Reports

- Create
  - In the "Portal Data Reports" tab, under the "Incidents" category (in the "Categorization" section), the "asset" and "logsource" fields were added under the "Field Selector" and "Criteria Selector" sections.
  - The number of maximum results in "Log Data" and "Portal Data" Reports was increased to 100000.

Identity & Access

- Identity & Access
  - When selecting a Domain Controller, the "Monitoring Services Status" chart was replaced with the "Missing Patches" chart.
    Important Note: ClearSkies™ NG Endpoint Detection & Response (EDR) Agent **v6.3.0** is a prerequisite for this chart to display correct data.

"Admin"

- Groups
  - In the "Users" and "Assets" tabs, in a user's and/or asset's "View" settings, when the "Set as default" action is clicked, a pop-up message was added asking for confirmation (Yes/No).
- Asset Configuration
  - The user can now upload files (key, password, configuration etc. files carrying additional information) on certain Asset Configurations.
- iCollector Management
  - The "RAW LOGS" settings were moved to the new "Raw Logs and Backup Methods" page.
  - iCollector Administration and Configuration in HA (High Availability) mode is now supported.
- License Overview
  - In the "Type of Service" section, the label "LogData (Last Completed Day)" was renamed to "LogData for the current day".

"Top Menu"

- Show me how
  - "Show me how" was removed and replaced by the content of the new "HELP" TopMenu item.

- Configuration Wizard
  - The "Compliance" step was redesigned. Additionally, in the second page, the new checkbox named "Enable" and the new fields named "Disclaimer" and "Image" were added.
  - In the first page of the "Users" step, a new column named "Portal Admin" was added. Additionally, in the second page, in "Details" section, a new checkbox named "Portal Admin" was added.
  - A new mandatory step named "Images & Disclaimers" was added.
  - In the third page of the "Reports" step, in the "Classification" section, a new field named "Image" was added.
  - A new mandatory step named "Security Questions" was added.
  - The following enhancements were implemented in the "Portal Admin" step:
    1. The "Personal Information" section was renamed to "Details".
       - The ordering of the fields was changed.
       - The "Email" field was brought to this section.
    2. The "Contact Information" section was renamed to "Phones".
       - The fields named "Email", "Home Phone", "Mobile Phone", "Work Phone", "Street", "Area", "Postal Code", "Country" and "City" were removed from this section.
    3. A new section named "Primary Login Location" was added containing the fields "Street", "Area", "Postal Code", "Country" and "City".
    4. The "Alternative Logins" section was renamed to "Alternative Login Location".

- Feedback button
  - The feedback button was removed as it was made redundant by the Chatbot.

"General"

- Several changes/enhancements were implemented in order to support an updated version of Checkpoint Threat Emulation Logs, Reports and Portlets.

Bug Fixes

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

New Supported LogSources

Vendor	Product	Type of Collection
Cisco	Cisco Email Security (CEF)	Syslog
Cisco	Cisco Firepower IDS (eStreamer)	Syslog
Imagicle	Application Suite	Syslog
Arista	Arista Switches	Syslog
GoAnywhere	Managed File Transfer (MFT)	Syslog
Sophos	Web Application Firewall (WAF)	Syslog
Sophos	Advanced Threat Protection (ATP)	Syslog
Sophos	Sophos Antivirus	Syslog
Sophos	Sophos Anti-Spam	Syslog