ClearSkies™ SaaS NG SIEM

Version 6.1

Incorporating the power of

Big Data Advanced Security Analytics

Mar 2020

Release Notes

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 and malicious behaviour, utilizing the power of Big Data Advanced Security Analytics.

What's New in v6.1

Several new features and functionality enhancements are introduced in this ClearSkies™ SaaS NG SIEM version 6.1:

- **Executive Report/Dashboard** (Birds-eye view of the current "Risk Exposure" of the organization)
- **ENISA's Threat Taxonomy now integrated with Use Cases/Correlation rules** (Improves threat investigation in order to help organizations choose defenses most appropriate to their context)
- **Attack prioritization** (Focus on analyzing events of importance)
- **Configuration Wizard** (Ongoing configuration optimization for increased effectiveness)
- **iCollector™ Management** (Providing centralized overview and control of deployed iCollectors)

New Features

"Threat Intelligence"

- ### Threat Anticipation (Attack Prioritization)

  The '**Threat Confidence Level**' configuration option enables you to select, based on your "Security Appetite", which Indicators of Attack (IOAs) will be escalated to Incident status for further analysis.

  The '**Threat Confidence Level**' provides a scale of 1 to 10, which spans across four different classifications (Informative, Medium, High and Critical). This configuration can be set through the global settings of the "**Threat Anticipation**" tool/application.

  This way, events that do not meet the criteria of the selected classification will not be escalated to incidents status, thus allocated resources can focus on analyzing events of importance.

  The classification of each Indicator of Attack (IOA) is calculated using a Machine Learning algorithm that takes into consideration a number of observables, including frequency, type, complexity of the current activity.

  Note: The default **Confidence Level** value is 7.

"Event Management"

- ### ENISA Threat Taxonomy integrated with Use Cases/Correlation Rules

  The newly added support for the ENISA Threat Taxonomy, which functions as an analysis mechanism for collecting and sorting cyber-threat information, helps organizations improve the investigation of incidents raised, and choose defenses most appropriate to their context.

"Top Menu"

- ### Configuration Wizard

  The new '**Configuration Wizard**' mirrors and consolidates configuration settings from different "**ServiceModules**" and global configuration parameters of the SWP into a user-friendly centralized step-by-step graphical user interface for increased effectiveness.

  What's more is the 'Use Cases' configuration panel with added support for the ENISA Threat Taxonomy, as mentioned above.

  The end result is the ongoing optimization of configuration settings in a more efficient, effective and transparent management process for an optimal use of **ClearSkies™ SaaS NG SIEM**.

  The mandatory areas need input from the user are indicated, leaving no room for system configuration omissions.

  The following areas require input from the user:

- Portal Admin*
- Users*
- Asset Groups*
- Asset Clustering*
- Asset Classification*
- No Log and Event Data*
- Incidents Grace Period*
- Encryption Passphrase*
- Use Cases
- Reports
- Attack Prioritization
- EDR Configuration
- UEBA Configuration
- SNMP Configuration
- Health Status
- Compliance

* indicates mandatory areas to be completed for proceeding any further.

- Risk Exposure Dashboard

The '**Risk Index**' was replaced with the "**Risk Exposure**" dashboard, which opens by default every time you log in to the SWP. This new dashboard is an insightful real-time birds-eye view of your current "**Risk Exposure**". Its intuitive interface is comprised of a collection of dynamic graphical visualizations and insightful charts representing organizational security posture as a whole, with regards to:

- The number and frequency of log and event Data collected
- Alerts fired and Incidents raised
- Top Indicators of Attack **(IOAs)** identified
- Alerts forecasting
- Detection Deficit by Incident severity
- Number and severity of Outstanding Incidents
- Trend Analysis of log and events collected, alerts fired, and incidents raised

Note: The '**Risk Index**' email notifications are no longer available.

- Risk Exposure Report

This executive report helps upper level management assess their organization's risk exposure to '**Cyber Risk**' during a reporting period (weekly, monthly, quarterly, semiannually, yearly) by presenting the different types of attacks, vulnerabilities, configuration weaknesses and the impact of targeted attacks and data breaches.

The report gives perspective on the organization's '**Risk Tolerance**' and likelihood to address or absorb risk in conjunction with its current risk management culture.

"Admin"

- iCollector Management

  This feature was relocated from the "**TopMenu**" to the '**Admin**' menu, and it was enhanced to provide greater control over deployed **iCollectors** through intuitive visualizations and insights on resource utilization, (number of events per hour, CPU usage, memory usage and disk usage), appliance status and license usage.

  Moreover, it introduces remote storage configuration settings for archiving raw log & event data collected.

  iCollector™ Management essentially bestows upon the user the ability to change or add configurations to the **iCollector™** itself directly from the ClearSkies™ Secure Web Portal interface. Through this feature, the Portal Admin may configure the following **iCollector™** settings:

  - Set the archive location of raw log and event data
  - set the time-zone for each **iCollector™**
  - Set or change the passphrase of archived raw log & event data

- Assets

  Global configuration (stopped receiving log and event data)

  In order to reduce the number of false positive alerts related to Assets having stopped sending log and event data to the **iCollector™**, we have associated the time elapsed with the Asset severity. So, if an Asset is categorized as critical, it will inherit the set threshold. When the set threshold is met, an Alert is fired.

  Local configuration (stopped receiving log and event data)

  The user is now able to customize locally, for each Asset's LogSource individually, the Alert generation criteria for when log and event data stop being forwarded.

"Endpoint"

- Behavior Analysis
  - Overview

  The '**Overview**' tab of the **Behavior Analysis** 'Tool/Application' was re-engineered to provide greater visibility over user and asset behavioral analysis of identified events. This includes the following charts and graphs with drilldown capability:

  - breakdown of activities by type,
  - classification of malicious/suspicious indicators,
  - enriched response actions ("simulated blocked", "blocked" and "quarantined"),
  - highlights of missing security and recommended patches on workstation and servers the agent is installed, and

- breakdown of **FIM** activity.

View

The graph activity visualization now includes missing/recommended updates as well as **FIM** activity, enabling you to get a more complete picture of what transpires on each endpoint.

FIM

The **File Integrity Monitoring (FIM)** was re-engineered to have no limitation on the number and size of folders and files monitored.

- Application Control

  The Endpoint '**Management**' Tool/Application was redesigned and enhanced to simplify the administration and maintenance of ClearSkies™ EDR Agents deployed on your network.

Enhancements

"ServiceModules"

Event Management

- Incidents
  - Incident "Severity" flag colors were changed as follows:
    - Informative (Blue color)
    - Medium (Yellow color)
    - High (Orange color)
    - Critical (Red color)
  - In "Configuration – Global Settings", the Incidents' grace periods were changed as follows:
    High: 1 day, 2 days, 3 days, 4 days. Default value: 2 days.
    Medium: 5 days, 6 days, 7 days, 8 days. Default value: 6 days.
    Critical: 6 hours, 12 hours, 18 hours, 24 hours. Default value: 12 hours.
  - Multiple selection and a "select all" option were added to the main grid, allowing the user to select and perform actions on multiple incidents simultaneously.

- Correlation
  - Filtering options were added to columns "Created Date" and "Modified Date".
  - Additional filtering parameters were added to the Shortcut function.
  - In the "Auto-Incident" tab, in the "Notification Suppression" field, the options "Hour(s)" and "Day(s)" were added, with maximum allowed duration of 7 days.

Endpoint

- Management
  - Only the Portal Admin role can now inherit Endpoint Management actions.

- Behavior Analysis
  - In "Overview" page grid, the "Classification" flag colors were changed as follows:
    - Low (Blue color)
    - Medium (Yellow color)
    - High (Orange color)
    - Critical (Red color)

Reports

- Create
  - In the "Portal Data Reports" tab, under the "Assets" category, the "incidents" field was added under "Field Selector" and Criteria Selector" sections.

- Results
  - The new "Cyber Risk Exposure" tab was added, listing Executive Reports Results.

Performance & Availability

- Bandwidth Utilization
  - Graph scaling is now dynamic for optimal visualization.

Threat Intelligence

- Threat Alert
  - Additional filtering parameters were added to the Shortcut function.
- Latest Threats
  - Additional filtering parameters were added to the Shortcut function.

Identity & Access

- Identity & Access (all pages)
  - Additional filtering parameters were added to the Shortcut function.

Dashboards

- User Defined
  - Under the "Intelligence" category, in the "Portlet Selector" the following portlets were removed: "IP Reputation (10 Newly added)", "Top 10 IPs with Bad Reputation (last 24h)" and "Newly Malicious Ips".

"Admin"

- Assets
  - In "No LogData Configuration – Global Settings", The "Configuration" section was renamed to "No Logs Settings".
  - In the "LogSources" section of an Asset Details tab, under a LogSource details tab, the "No LogData Configuration" section was renamed to "No Logs Settings".
  - In the "Details" section, the "Classification" field was renamed to "Severity", and a new field, with completely new values, named "Classification" was added.
  - The fields "Classification", "Cluster Mode" and "Version" were removed from the LogSource "Details" section.
  - All dropdown lists are now sorted alphabetically.
  - "Severity" flag colors were changed as follows:
    - Low (Blue color)
    - Medium (Yellow color)
    - High (Orange color)
    - Critical (Red color)
  - In the "No LogData configuration – Global Settings", in the "No Logs Settings" section, the default values were set as follows:
    - For "Low" Asset Severity: Threshold set to "40" minutes and Suppression to "160" minutes.
    - For "Medium" Asset Severity: Threshold set to "20" minutes and Suppression to "80" minutes.

- For “High” Asset Severity: Threshold set to “10” minutes and Suppression to “40” minutes.
- For “Critical” Asset Severity: Threshold set to “5” minutes and Suppression to “20” minutes.

- Asset Configuration
  - The new columns “Created Date”, “Created By”, “Modified Date” and “Modified By” were added to the main grid. Also, column filtering was included these columns.

- Users
  - In the “Password Policy” section, the “Password Policy Name list” is now sorted alphabetically.
  - The “Status” filtering values are now sorted alphabetically.
  - Additional filtering parameters were added to the Shortcut function.

“Tools”

- Asset Discovery
  - All dropdown lists are now sorted alphabetically.
- Alias Manager
  - “Duplicate” actions in the main grid can now only be duplicated once.

“General”

- Support for CVEs provided by NIST was updated. More information can be found here: https://nvd.nist.gov/vuln/data-feeds.
- In the Login screen, the note specifying supported browsers for ClearSkies™ SaaS NG SIEM now includes Microsoft Edge.
- In the “User Preferences” page, in “Password Policy” section, “Password Policy Name list” is now sorted alphabetically.
- In the “Responsiveness” page, in the “Incidents” grid, “Severity” flag colors were changed as follows:
  - Informative (Blue color)
  - Medium (Yellow color)
  - High (Orange color)
  - Critical (Red color)
- New “Export” button was added to the main grid’s top toolbar, enabling the exporting of all grid’s data to an Excel file, only for the following:
  - **Event Management ServiceModule:** for “Incidents” and Alert “Evidence Logs” tab, “Alerts” and “Correlation” applications.
  - **Reports ServiceModule:** for all applications.
  - **Endpoint ServiceModule:** for all applications.
  - **Compliance ServiceModule:** for all applications.
  - **Admin TopMenu item**: for “Assets”, “Users” and “User Roles” sections.

Bug Fixes

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

New Supported LogSources

Vendor	Product	Type of Collection
Aruba	ClearPass Session	Syslog
Aruba	ClearPass System	Syslog
Aruba	ClearPass Insight	Syslog
Aruba	ClearPass Audit	Syslog
F5	DDOS Protection	Syslog
Avigilon	Control Center	Syslog
Cimcor	Cimtrak	Syslog
Cynet	Cynet 360	Syslog