ClearSkies™ SaaS NG SIEM

Version 5.9

Incorporating the power of

Big Data Advanced Security Analytics

July 2019

Release Notes

Table of Contents

Overview 4

What's New in v5.9 4

"Analytics" 4

- Big Data Search 4
- User & Entity Behavior Analysis (UEBA) 5

"Threat Intelligence" Service Module 5

- Threat Map 5
- Threat Anticipation 5
- Heat Maps 5

"Preferences" 5

- Network Manager 5

"Endpoint" 6

- Behavior Analysis 6

iCollector High Availability 6

ServiceNow Ticketing integration 6

Microsoft Edge compatibility 6

Enhanced Minimum Resolution 7

Azure Active Directory and Office365 Audit 7

Enhancements 8

"ServiceModules" 8

Event Management 8

Analytics 8

Vulnerability Management 9

Reports 9

Endpoint 10

Performance & Availability 10

Vulnerability Management 10

"Dashboards" 10

"Admin" 10

"Tools" 11

“Preferences” 11
“General” 11
Bug Fixes 13

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 a testament of our pioneering role in the uncharted territory of Big Data Advanced Security Analytics.

What's New in v5.9

Several new features are introduced in this ClearSkies™ SaaS NG SIEM version 5.9:

"Analytics"

- Big Data Search

  The enhanced "**Big Data Search**" application improves user experience by increasing productivity and effectiveness as follows:

  - A query-based event count timeline helps visualize anomalies with more details on an activity during a selected period. When creating a column-based analysis (filter), a bar chart visualization offers a new perspective. Search queries can be bookmarked for future reference.
  - All search queries are now being validated for convenience, and users are now notified if a query is invalid.
  - The search query window carries an auto-complete filter-as-you-type capability, showing suggested search syntax, bookmarked search queries, examples and operators etc. A filtered query regarding assets can now be created directly from the "Search in" dropdown menu.
  - A comprehensive date/time picker was added for providing to the user the ability to perform more time sensitive queries.
  - The new Indicators Of Compromise (IOCs) dropdown menu enables the user to filter out or perform search queries related to probes identify as malicious; selected IOCs are colored red in the queries results.
  - Integration with "Threat Anticipation" application, which provides a visual representation of events identified as malicious.
  - Two breakdown pie charts were added: "Events by category" and "IOC events" for providing to the user the distribution of log and vent data collected.
  - A pie chart visualization depicting query results is now included, with drilldown capabilities executed automatically upon clicking on a chart segment.

- User & Entity Behavior Analysis (UEBA)

  The introduction of an unsupervised machine learning model that keeps track of human-driven network/system activities in order to create a baseline of users' work days and time shifts.

  For any user, the model yields one of three results:

  - The actual working hours
  - Whether it is a shift operation
  - There is not enough data

"Threat Intelligence" Service Module

- Threat Map
  - This new application provides a visualization representation of attacks happening in near real-time against your organization.
- Threat Anticipation
  - With a user-friendly design, this new application anticipates which type of threats targeting your organization might affect the confidentiality, integrity and availability of your information assets. Threats are categorized into different Indicators Of Compromise (IOCs) types, such us Malware, Trojan, ToR Exit Node, Reconnaissance activity etc.
  - The '**network map**' helps users visualize the entire activity, including which assets detected this activity, devices/application/network targeted, action taken by these assets, direction of the activity, type, count, classification of the attack and much more.
  - This powerful '**network map**' provides the associations of IOCs with users, driven by the "User & Entity Behavior Analysis" (UEBA) application, additionally providing a summary with what was observed.
  - Further analysis on each threat allows the user to jump into the "**Big Data Search**" application and view related log and event data.
  - **Unsupervised machine learning model for detecting phishing and malware delivery domains/sites (DNS fast flux**): Utilizing a machine learning model to detect outbound connectivity to malicious domains/sites by analyzing DNS log data.
- Heat Maps
  - This new application presents the density and frequency of attacks by country. It provides a further drilldown of attacks by selecting a desired country on the map. Upon selecting a threat, the application redirects to the "Threat Anticipation" application for a further graphical representation of the threat.

"Preferences"

- Network Manager

  A new tab named "Asset Clustering" was added, which enables the user to perform the following actions:

  - Manage Clusters, Update and delete an asset's clustering.

- Set Name, Description and Type (High Availability, Load Balancing).
- Add and/or remove Assets in/from Cluster.

“Endpoint”

- Behavior Analysis

  ClearSkies™ NG EDR Agent v6.1 is a comprehensive Endpoint Detection & Response solution, fully integrated with ClearSkies™ SaaS NG SIEM. It complements the detection and prevention of never-before-seen targeted attacks and insider threats with the use of Behavioral Monitoring and Analysis (BMA) and by leveraging Advanced Security Analytics complemented by Threat Intelligence and signature-based detection. Several new features are included:

- Next-Gen Behavioral Monitoring and Analysis
- Integrated Threat Intelligence
- Application Control
- Automated Response Actions

For more information, refer to the ClearSkies™ NG Endpoint Detection & Response (EDR) Agent v6.1 Release Notes.

iCollector High Availability

All physical iCollectors now support a high-availability option where a second iCollector acts as a fail-over system in case the primary iCollector goes down. They both share a virtual IP where all traffic from the in-scope assets is forwarded, ensuring minimum data loss and continuation of all operations as normal. In terms of the collecting applications, they too are taken care of, as they resume the collection from the secondary iCollector. All the rest (Correlation Engine, Reports, Big Data Search, Dashboard et al.) then work as expected, this way creating an invisible layer between the iCollector and the ClearSkies™ Secure Web Portal.

ServiceNow Ticketing integration

ServiceNow Security Incidents has now been integrated into ClearSkies™ Big Data Advanced Security Analytics Platform. This enables your organization to further extend the capabilities of the ClearSkies™ **“Incidents”** application for a more creative use of ServiceNow. With this integration, you can maintain your internal workflow while being able to assign ServiceNow Security Incidents beyond ClearSkies™ users. Once an Incident is raised in ClearSkies™, an Incident is also raised in ServiceNow, complete with bi-directional synchronization in terms of the Incident status and comments added on either side. Refer to “ServiceNow (v. Kingston) Security Incidents Integration” document found on the ClearSkies™ Secure Web Portal.

Microsoft Edge compatibility

Microsoft Edge web browser is now supported.

Enhanced Minimum Resolution

The minimum resolution supported is now 1600 x 900.

Azure Active Directory and Office365 Audit

ClearSkies™ now supports log and event data from Office365 and Azure Active Directory. The following content types are supported: Azure Active Directory, Exchange, SharePoint, General Audit and DLP events.

Enhancements

“ServiceModules”

Event Management

- Correlation
  - ➢ The Correlation Rule Templates are now filtered based on the Asset groups a user is associated with. A template is only visible to a user if all associated LogSources are viewable by a specific user.

- Alerts
  - ➢ Upon Custom Alert creation, the LogSource field is now disabled. Upon selecting an asset, the LogSource field is enabled and the relevant Assets are shown in alphabetical order based on User/Asset permissions. In addition, fields are enhanced with a filter-as-you-type capability.
  - ➢ The icons categorization in the Alerts left-hand side panel can now be configured in Preferences → Network Manager.

- Incidents
  - ➢ When alerts merge automatically via a correlation rule, an audit line was added to the Incident “History” tab.
  - ➢ When the Incidents application first opens, the open incidents of the last 360 days are now being displayed.
  - ➢ The “messageid” field in the “Evidence Logs” tab was enlarged.
  - ➢ The ID column was removed from Evidence Logs.

Analytics

- User & Entity Behavior Analysis (UEBA)
  - ➢ Two new UEBA Flags, “Unusual Network Activity – Destination IP addresses” and “Unusual Network Activity – Destination Ports”, which are volumetric multivariate anomaly detection methods, were applied onto network logs collected from firewall LogSources.
  - ➢ A hyperlink was added to malicious IoCs in the UEBA Flags Analysis table linking to Threat Anticipation.
  - ➢ Additional filtering parameters were added to the Shortcut function.
  - ➢ The User & Entity Behavior Analysis (UEBA) mechanism was integrated with Threat Anticipation.
  - ➢ The current anomaly detection framework was enriched and optimized by a supervised model. Its purpose is to reduce false positives by classifying the anomalous point(s).

- Big Data Search
  - ➢ When using the range of values and IP address range with the CIDR notation, the IP addresses are now highlighted in the results.
  - ➢ Additional filtering parameters were added to the Shortcut function.

- In page numbering, the capability to type a number page in the field provided and jump to that specific page was added, instead of only having the option to click on the next/previous buttons. This functionality is not available when the number of the results is more than 15000.
- New conditions (<, >, >=, <=) are now available for numeric fields.
- Values of fields "sourceport" and "destinationport" are now highlighted in results for conditions (<, >, >=, <=).

Vulnerability Management

- Manage Scans
  - The maximum number of hosts was increased for Nessus files from 100 to 1024.

Reports

- Create
  - The number of results in "Log Data" Reports and "Portal Data" Reports was increased to 10000.
  - In the Portal Data Reports tab, in the "Criteria Selector" section of a report's properties dialogue box tab, the "correlation rule" field values dropdown menu is now sorted alphabetically. Additionally, in the "Categorization" section, the "Category" field values dropdown menu is now sorted alphabetically also.
  - In the Portal Data Reports tab, in the "Criteria Selector" section of a report's properties dialogue box tab, icons were added in the dropdown menu in the "correlation rule" field values depicting by whom the correlation rule is being managed (Odyssey, Customer etc.).
  - In the Portal Data Reports tabs, the new fields "first comment date", "final review date", "final review date (first)" and "final review date (last)" were added in the "Field Selector" and "Criteria Selector" sections.
  - In the Log Data Reports tab, a new section named "Aggregation Criteria Selector was created. The user is now able to define the desired criteria of the aggregation count.
  - Additional filtering parameters were added to the Shortcut function.
  - The fields "year", "month", "day", "hour", "minute" were added as separate fields in the Portal Data Reports tab's properties (only under Alerts categorization).
  - In both the Log Data Reports and Portal Data Reports tabs, the value "None" was added in "Image" field, and is now set as the default value of this field.
  - When a schedule is added in a report, the "Compliance" section is now active by default.
  - When a default value is set in Preferences → Classifications/Disclaimers, that value is shown as default in the corresponding "Classification" and "Disclaimer" fields in the Presentation section when a new report is created.
  - Column Filtering was added for "Name" in the "Field Selector" and "Criteria Selector" sections of a report's "Properties" tab.

- Results
  - ➢ Pagination (paging) was added to results shown in the portal. Each page now shows up to 100 results and also supports grid filtering.
  - ➢ Additional filtering parameters were added to the Shortcut function.
  - ➢ Only one year's worth of instances are now shown.
  - ➢ Handling of numeric fields when exporting to a file is now enabled on reports.

Endpoint

- Behavior Analysis
  - ➢ Several enhancements were implemented in this page in order to accommodate the new features of the Endpoint. For more information refer to the ClearSkies™ NG Endpoint Detection & Response (EDR) Agent v6.1 Release Notes document.

Performance & Availability

- SNMP
  - ➢ Additional filtering parameters were added to the Shortcut function.

- Bandwidth Utilization
  - ➢ Support for SNMP metrics from Virtual Instances was added. Currently the only vendor supported is Check Point.
  - ➢ Additional filtering parameters were added to the Shortcut function.

- Health Status
  - ➢ Additional filtering parameters were added to the Shortcut function.

Vulnerability Management

- Manage Scans
  - ➢ The number of hosts allowed in a single file scan was increased from 100 to 1024.

"Dashboards"

- User Defined
  - ➢ Several new portlets were added under the Events category for Check Point Threat Emulation, Check Point Antibot, McAfee Web Gateway and ISS NS Proventia G.

"Admin"

- Assets
  - ➢ A new field "Role" was added. The user can now define a descriptive role to each asset.
  - ➢ Asset clustering information is now displayed in Assets.
  - ➢ The Health Status option now displays the ICMP check.
  - ➢ A multiple asset deletion option was added. Also, a warning message now accompanies the option, indicating that the assets selected for deletion contain 'x' LogSources. Lastly,

when an asset with LogSources is deleted, the asset as well as its LogSources are now marked as deleted.

- ➢ Additional filtering parameters were added to the Shortcut function.
- ➢ A new field named “Description” was added to the “Details” section.

- Users
  - ➢ Text labels in each field were added in the “Phones” section.
- Groups (Values tab)
  - ➢ A new “Upload” action was added in the “Values” section in each Group’s dialogue box. Clicking the “Upload” button now opens a dialog box for browsing and adding a file. In the same section, pagination (paging) was added to the values list. Each page now shows up to 25 values and supports grid filtering. Upon saving, the total number of duplicates (if any) are shown in a popup message, and may be removed by selecting the option “Yes”.
- License Overview
  - ➢ The chart data is now grouped in 30-minute intervals.
  - ➢ A notification email, SMS, and pop-up notification is now sent when EPS or Volume violations occur.

“Tools”

- Alias Manager
  - ➢ Aliasing can now be applied based on asset ownership.

“Preferences”

- Classifications/Disclaimers
  - ➢ A new setting named “Set As Default” was added. In addition, the columns “Created By”, “Created Date”, “Modified By”, “Modified Date” and “Default” were added in the grid.

“General”

- ➢ The field names are now shown in lowercase for “Big Data Search”, “Alerts, “Reports”, “Correlation Rules” etc.
- ➢ The visual for the Risk Index indicator was changed.
- ➢ Each user’s columns setup and order for each Application grid are now maintained for future use into the portal.
- ➢ Blank spaces typed when populating fields (space, tab, new line) are now not taken into consideration in service modules and/or applications Correlation Engine, Alert Filtering, Reports and Value Groups.
- ➢ New notifications were added when an Asset Configuration is added, edited and deleted.
- ➢ The top bar of the Portal was redesigned.
- ➢ The maximum allowed characters of the feedback message was increased. In addition, a file can now be uploaded via the feedback dialogue box.

- The parsing of logs from multiple Email Gateways (Symantec, Cisco) was enhanced.

Bug Fixes

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