ODYSSEY
Impossible Challenges, Possible Solutions

ClearSkies Version 5.5 Release Notes

March 2017

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

WHAT'S NEW IN V5.5

Three major features are introduced in this **ClearSkies NG SECaaS SIEM** version.

User Entity Behavioral Analysis (UEBA)
This truly innovative feature can be considered as the single most important value delivering addition in this release. Taking behavioral analytics to the next level, UEBA utilizes unsupervised machine learning and advanced behavioral analytics to build out behavioral baselines for User and Asset entities. This capability enables the detection, IN REAL TIME, of insider threats, targeted attacks, and malicious patterns of traffic caused by user behaviors, both normal and malicious in nature.

Enhanced visibility into your security posture
Aware of the critical importance of being in control of your security risk management process, a number of innovative features and enhancements are introduced in this release which, considerably enhance your visibility into your organization's security posture, while considerably improving users' operational experience.

Announcing ClearSkies NG SECaaS SIEM "*Express*"
We could no longer turn a deaf ear to the important and urgent needs of the small and medium businesses. They may be smaller in size but are subject to the same laws and regulations and face the same cybersecurity challenges of their larger counterparts, which most of the time are much more detrimental to their very survival. **ClearSkies NG SECaaS SIEM "*Express*",** a ClearSkies version which offers all powerful features to address small to medium business needs, yet without the complexity that larger organizations may deem necessary. Most importantly, it makes proactive security management affordable to this significant economic sector.

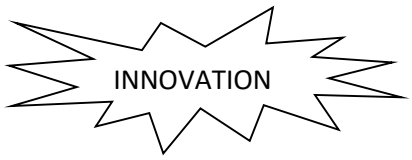
NEW FEATURES

ClearSkies NG SECaas SIEM "*Express*" version

The ClearSkies NG SECaaS SIEM "***Express***" version includes the full functionality of ClearSkies NG SECaaS SIEM, but with the following capacity restrictions:

- Up to 1GB/day log data collection quota
- "Big Data Search" and "Analysis" capbility available based on "LogData" collected during the last seven days
- Up to three months "LogData" retention
- Up to six registered web portal user licenses
- Up to five "Endpoint Agents" licenses
- Minimum license purchase period of three months

Analytics



- **User Entity Behavioral Analysis (UEBA)**, utilizes unsupervised machine learning and advanced behavioural analytics to build behavioral baselines for "User" and "Asset" entities. This capability enables the detection, IN REAL TIME, of insider threats, targeted attacks, and malicious patterns of traffic caused by user behaviors, both normal and malicious in nature. The model allows the organization to choose the security sensitivity that best reflects its risk appetite and disposition towards information security in the form of four different "**Behavioral Moods**" as listed below:
    1. Relaxed
    2. Neutral
    3. Aggressive and
    4. Custom

- **LiveView**: Application deprecated and the "**LiveView**" functionality intergraded within "**Big Data Search**"

Endpoint

- **Management**: Application for centrally scheduling the updating of "ClearSkies NG Endpoint Agents".

  Important Note: For taking advantage of this new feature you should be running Endpoint v4.0 and above.

Admin

- **Assets:** This section has been enhanced with the following features:
    1. Summary Indicators including,
        - Active number of "**Assets/LogSources**"
        - Number of Assets "**Need Attention**"
        - Number of Log Source "**Out of License**"
        - Number of outdated Endpoint Agents "**Out of Date**"
    2. "Asset Group" and "LogSource" type filtering

3. No “LogData” threshold for each “LogSource” type under the “Configuration Gear”
4. “Status” and “Last Contact” columns for Endpoint Agent v4.0
5. Multiple selection of “Assets” for editing common fields
6. “LogSources” belonging to a specific “Asset” are shown in edit mode
7. “Schedule Updating” for outdated Endpoint Agents
8. Edit an “Asset” by selecting the “Asset” after pressing the “View” button
9. Legend information is now shown with mouse over on the grid icons

- **License Overview**: Provides the web portal user with real time license usage information including the following:
    1. Last 24 hours and 30 days’ license overview usage
    2. Summary Indicators based on the period selected
        - Max number of “**Events Per Second**” observed
        - Number of active “**LogSources**”
        - Number of active “**Endpoint Agents**”
        - Number of “**Registered Users**”
        - Number of “**License Violations**”
    3. Top 10 “Assets” generating the highest number of “LogData”
    4. “Events” Generated per “LogSource” category proportionally
    5. Current “License Information”

Tools

- **Resources:** This section provides access to documentation regarding *PortalAdmin*, *UserGuide*, *Big Data Search Query language*, *iCollector initial installation/configuration* and *Device/Asset configuration* for reporting Log Data to the iCollector.
- **Downloads:** This section provides the user with the ability to download the “ClearSkies Endpoint Agent”, in addition to other useful tools and utilities.

Home Screen

- **Customize:** Provides the user with the ability to rearrange “ServiceModules”, “Applications” and “Menu” Items tiles.
- **Tiles shake gesture**: For capturing user’s attention on important messages/information within “ServiceModules”, “Applications” and “Menu” items are shaking.
- **Notification counter**: Indicates the number of pending important messages/information within “ServiceModules” and “Applications” on mouse over.
- **New tag**: New “ServiceModules” and “Applications” are indicated by the “New” flag shown in the upper left corner of the tile.

General

- **Messaging Center:** The ability to send important ad-hoc messages as a pop-up window to web portal users.
- **Copy**: Ability to copy text found with in grids in different sections of the web portal.
- **Syslog Relay**: Ability to process, store and analyse log data forwarded from syslog relays, including third party SIEMs, to the iCollector.

ENHANCEMENTS

Reports

- **Create**
  1. "User Groups" and "Asset Groups" are shown in the initial Grid
  2. Caption corrections between Graph and Chart
  3. Scheduled status is shown for "Scheduled Reports"
  4. Scheduling is disabled for reports not related to "Asset Groups"
  5. Extra columns added for "Assets" (Dates, LogSources, Monitored by, OS etc)
  6. Data Callouts added on charts
  7. Extra columns added within "Incidents" (Dates, Correlation Rule and Observation)

Event Management

- **Correlation**
  1. "Correlation Rules" that are not validated are ignored
  2. Average function added based on filter window
  3. A "Correlation Rule Category" is automatically created when not found
  4. "Correlation Rule Templates" filtering added
- **Incidents**
  1. When searching using an "Incident ID" all the other filters are disabled
  2. Users are allowed to copy text from "Incident" comments
- **Alerts**
  1. Incident Severity is proposed based on the alerts severity
  2. Observation text is improved based on the factors of the alert

Admin

- **Users**
  1. A warning message is shown when the number of web portal users is reached
  2. "User Role" is mandatory when creating a new web portal user
  3. A warning message is shown when the "Escalation Order" is enabled and no phone numbers are defined
  4. A checkbox added for enabling the "Escalation Order"
  5. SMS and Push settings on web portal user creation are unchecked by default

- **User Roles**
  1. A warning message is shown when the maximum number of "Custom User Roles" is reached.
  2. Duplicating an existing "User Role"

- **Assets**
  1. "No LogData" threshold is set by default to all new LogSources
  2. "Monitored By" option added for "Asset" ownership

- **No LogData**

  This service provides to the web portal user the ability to define which "LogSources" report LogData to the iCollector. If the "No LogData" service is enabled for a specific "LogSource", the following configuration options are provided to the web portal user:

1. “Generate Alert”: Define whether “Alerts” will be issued if conditions are met
2. “Threshold”: Define the time interval for no LogData reported from a specific “LogSource” to the iCollector
3. “Suppression”: Define the sleep interval before the next “Alert” will be issued for a “LogSource” which continues not reporting “LogData” to the iCollector

Important Note: When a “No LogData” incident is raised and the status is “Open”, the “Correlation Engine” stops issuing “No LogData” Alerts

General

- **Shortcut creation**: A warning message is displayed when the maximum number of “Shortcut” tiles is reached when adding a new “Shortcut” tile.

BUG FIXES

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

NEW SUPPORTED LOGSOURCES

Vendor	Product	Version Supported	Type of Collection
Blue Coat	Web Gateway	4.x-6.x	Syslog
Fortinet	FortiAnalyzer	All	Syslog
IBM ISS	XGS (Standalone)	All	Syslog
ObserveIT	ObserveIT Enterprise	All	ODBC
RioRey	DDoS Protection	RIOS 5.0, 5.1, 5.2	API
RioRey	DDoS Protection	RIOS 5.0, 5.1, 5.2	Syslog
Trend Micro	Deep Discovery	All	Syslog
Vasco	Identity Key	3.x	Syslog
Vormetric	Data Security	4.x	Syslog
Checkpoint	Management Audit Logs	R75 and higher	LEA
Fortinet	FortiWeb	All	Syslog
Radware	LinkProof	All	Syslog

CYPRUS
1 Lefkos Anastasiades str.,
2012 Strovolos
Nicosia
Tel.: +357 22463600
Fax: +357 22463563

OFFICES

GREECE **SERBIA** **DUBAI** **USA** **SOUTH AFRICA**