ClearSkies™ NG SIEM Version 5.7

Incorporating the power of

Big Data Security Analytics

November 2017

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

What's New in v5.7

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

Meeting and validating compliance with SWIFT

Delivers the framework for helping you meet and validate regulatory compliance. With no effort on your part, since these criteria are designed into the ClearSkies™ NG SIEM "**Compliance - ServiceModule**", you can validate complex compliance requirements in an efficient and cost-effective manner.

Furthermore, it associates ClearSKies™ NG Endpoint Agent FIM features with related compliance criteria found under SWIFT.

Location-based two-factor authentication

As an additional security measure, when a ClearSkies™ NG Secure Web Portal user attempts to login from a different location (city/country) than the default one, a time-based one-time password will be sent automatically to the user's registered email address or mobile number complementing his/her existing password for logging in.

Asset/Application Health Status

This "Application" monitors the Asset/Application status and performance trends over time by querying running service ports, i.e http, SMTP, and alerts you when there is a status change.

New Features

"ServiceModules"

Performance & Availability

- **Asset/Application Health Status**

  This "Application" monitors the Asset/Application status and performance trends over time by querying running service ports, i.e http, SMTP, and alerts you when there is a status change.

  By default the "Application" will send ICMP probes to determine the status of the Asset if no services are configured or if they fail to respond. The highly customizable dashboard provides real-time Asset performance and availability status, current and historical.

- **Bandwidth Utilization**

  This "Application" provides the functionality to monitor network inbound/outbound bandwidth usage trends over time with the use of SNMP on routers and switches.

Compliance

- **Meet and validate compliance with SWIFT**

  Delivers the framework for helping you meet and validate regulatory compliance. With no effort on your part, since these criteria are designed into the ClearSkies™ NG SIEM "**Compliance - ServiceModule**", you can validate complex compliance requirements in an efficient and cost-effective manner.

  Furthermore, it associates ClearSKies™ NG Endpoint Agent FIM features with related compliance criteria found under SWIFT.

Event Management

- **Alerts**

  For a better management of Alerts and for users' convenience, the "**Monitored**" alerts have been renamed to "**Suspicious**". In addition, a new feature has been added to 'auto-ignore' "Suspicious" alerts after a duration of one week if no action was taken.

Copyright ©2017 Odyssey Consultants LTD. All rights reserved

"TopMenu"

Admin

- **Assets**
  An actual count of LogSources that have no license is shown based on attached SKU's on each project.

Tools

- **Asset Discovery**
  The Asset Discovery is now using the newly released nmap version 7.1 that allows for higher results accuracy and also supports the discovery of Windows 10.

"General"

- **Location-based two-factor authentication**
  As an additional security measure, when a ClearSkies™ NG Secure Web Portal user attempts to login from a different location (city/country) than the default one, a time-based one-time password will be sent automatically to the user's registered email address or mobile number complementing his/her existing password for logging in.

Copyright ©2017 Odyssey Consultants LTD. All rights reserved

Enhancements

"ServiceModules"

Event Management

- Incidents
  - The user shown on the "Last Comment By" field is the one who last modified the correlation rule
  - The user shown in "Audit" as the one who created the incident is the one who last modified a correlation rule
  - Added "Audit" for assigning action on Auto-Incidents
  - Added grid filtering for the "Severity" field
  - Displaying [Odyssey] under "Assigned From" for MSS-raised Incidents
  - Disabled "Request for assistance" button for Incidents raised by the Customer (Hybrid)

- Correlation
  - A "View" button was added when selecting a rule to add more clarity
  - Automatically ignoring correlation rules with validation issues

- Alert Filtering
  - Added filtering for the "Expiration" column

Vulnerability Management

- Manage Scans / Review
  - Renamed "Delete" button to "Remove"
  - Renamed "Low" vulnerabilities to "Informative"

Performance & Availability

- SNMP
  - Data from pre-calculated tables is retrieved

Reports

- Create
  - Customers are allowed to edit compliance reports
  - A new tab was added for the Compliance ServiceModule when scheduling a report
  - Added the Asset name in the available fields
  - The user is allowed to edit the presentation of reports created by Odyssey

- Results
  - The Report name is displayed on top of the results

Copyright ©2017 Odyssey Consultants LTD. All rights reserved

- The report number column width was increased

Compliance

- All applications
  - Added notifications for parents and parent requirements
  - A notification appears if an application is not enabled

Analytics

- Big Data Search
  - Search query is case-insensitive
  - Facet results export is set to 1000

Copyright ©2017 Odyssey Consultants LTD. All rights reserved

"TopMenu"

Admin

- Users
  - Added "Information" icon (i) next to Role
  - Added sorting for columns "Role" and "User Groups"
  - The user is not allowed to close the "User Project" panel if no action is taken

- Assets
  - The "Last Updated" field is updated when a new LogSource is added under an asset
  - When an asset is deleted, the user/asset group association is set to Default

- User Roles
  - Removed permissions for Endpoint schedule from Portal Admin

- Asset Configuration
  - Removed "OPSEC Application" and "Activation Key" from existing configurations

"General"

Notifications

- Added notifications for Alert Filtering actions

Pop-Up messages

- Added a link icon to clickable notification messages

Copyright ©2017 Odyssey Consultants LTD. All rights reserved

Bug Fixes

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

Copyright ©2017 Odyssey Consultants LTD. All rights reserved

New Supported LogSources

Vendor	Product	Version Supported	Type of Collection
Fortinet	Fortigate Router	All	Syslog
Fortinet	Fortigate VOIP	All	Syslog
Fortinet	Fortigate FortiSandbox	All	Syslog
Cisco	Cisco Unified Communications Manager	11.0 and higher	Syslog
Zimbra	Zimbra Email Server	All	Syslog
Linux	DNS Queries	All	Syslog
Check Point	Check Point Syslog	All	LEA
Imperva	Imperva Database Firewall	All	Syslog
OSISoft	PI System Audit	All	ODBC
OSSEC	OSSEC HIDS Security	All	Syslog
Society for Worldwide Interbank Financial Telecommunication (*SWIFT*)	Swift Alliance	All	SNMP
Aruba Networks	ClearPass for NAC	All	Syslog
Synology Inc.	ISCSI Storage	All	Syslog

Copyright ©2017 Odyssey Consultants LTD. All rights reserved