ODYSSEY
Impossible Challenges, Possible Solutions

ClearSkies™ NG SIEM Version 5.6 Release Notes

July 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 V5.6

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

Risk Index & Responsiveness Score

- **Risk Index**
  Displays an indicative assessment of the Information Risk the organization is exposed to. The assessment is based on a number of key indicators including:
  - The number and type of Log Data collected over a specific time period
  - The users' responsiveness in reviewing Alerts and closing raised Incidents on time based on their classification.

- **Responsiveness Score**
  Displays each user's responsiveness in reacting to assigned Alerts and Incidents.

Integration with STIX/TAXII cybersecurity situational awareness

Supports automated information sharing for cybersecurity situational awareness, real-time network defense and sophisticated threat analysis with the integration of STIX/TAXII. Intelligent cyber-threat information extracted from TAXII such as malicious Emails, URLs, Domains and IP addresses, can be utilized during the "Analysis" phase, as well as during the creation of correlation rules.

Meet and validate compliance with PCI DSS, ISO 27001, FISMA and HIPAA

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 FIM features with related compliance criteria found under PCI DSS, ISO 27001, FISMA and HIPAA.

NEW FEATURES

TopMenu

- **Risk Index**

  Displays an indicative assessment of the Information Risk the organization is exposed to. The assessment is based on a number of key indicators including:
  - The number and type of Log Data collected over a specific time period
  - The users' responsiveness in reviewing Alerts and closing raised Incidents on time based on their classification.

  A relevant "**Risk Index" email notification** is sent either weekly or monthly to designated users.

- **Responsiveness Score**

  Displays each user's responsiveness in reacting to assigned Alerts and Incidents.
  A relevant "Responsiveness" email notification is sent either weekly or monthly to each user describing their performance.

  Note: The Time/Date when the email is sent is configurable from a user with a "Portal Admin" privilege.

Event Management

- **Alert Filtering (Application)**

  False-Positive alerts may be filtered out, so that related correlation rules would not fire. An option to quickly add an alert filter has also been added in the "Alerts-Application".

- **Alert -> Actions -> Merge Alerts**

  With this capability, a user may manually merge new Alerts into an outstanding Incident, if it is determined that they are related. This association can be established based on the following criteria:
  - Incident ID,
  - Search for keywords within "Comments" found in an Incident,
  - Asset Name,
  - Correlation rule ID

- **Incidents -> Configuration-Gear**

  The "Configuration-Gear" provides to a user with "Portal-Admin" privilege the ability to set:
  - An Incident's response grace period based on its severity.
  - The Time/Date when a status report regarding the "Risk-Index" and "Responsiveness Score" will be sent out by email to the designated users/roles.

Admin

- **Asset Configuration**

  Provides to the user with "Portal-Admin" privilege the ability to integrate LDPA directory services for retrieving user and group related information for use within the "User Entity Behavior Analysis" model.

Endpoint (ClearSkies™ NG Endpoint Agent v5.0)

- **Enterprise Agent**

  This version complements the early detection of malicious activity and/or abnormal behavior on critical servers by combining File Integrity Monitoring (FIM) for meeting regulatory compliance requirements. It also incorporates other vital security capabilities such as Malware, Zero-Day and Advanced Persistence Threats (APTs) detection.

Threat Intelligence

- **Evidence-Based Knowledge (provided by IthacaLabs™)**

  Supports automated information sharing for cybersecurity situational awareness, real-time network defense and sophisticated threat analysis with the integration of STIX/TAXII. Intelligent cyber-threat information extracted from TAXII such as malicious Emails, URLs, Domains and IP addresses, can be utilized during the “Analysis” phase, as well as during the creation of correlation rules.

Compliance

- **PCI DSS, ISO 27001, FISMA and HIPAA**

  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 FIM features with related compliance criteria found under PCI DSS, ISO 27001, FISMA and HIPAA.

ENHANCEMENTS

Reports

- **Create**
  1. Introduces the ability to apply filter to the columns “Created Date” and “Modified Data”
  2. The option to create report for variables with null values has been added

- **Results**
  1. Paging on grid has been introduced

Event Management

- **Correlation**
  1. To add more user clarity, the size of the “Filter” area has been expanded when creating a correlation rule in Step 2
  2. A new warning message has been added, displayed when a title is missing during the creation process of a correlation rule in Step 2
  3. A warning message is displayed when a correlation rule cannot be validated (as a result enforced from the correlation engine)
  4. The ability to apply the same correlation rule on multiple iCollectors™ has been added.
  5. Missing correlation category will be created automatically if it does not exist during the process of creating a new correlation rule

- **Incidents**
  1. An Incident workflow is introduced as follows: An incident first should be assigned to a user or to a group of users first for further investigation and resolution and then for closure.
  2. Assigned -> Under Investigation -> Close
  3. “Summary Indicators” have been added, including New, Unsigned, Under Investigation, Final Review, Overdue, for user clarity
  4. When an Incident raised relates to Events with CVE, the following information is displayed:
     - Classification
     - Severity
     - Exploitability and
     - Impact Factors

- **Alerts**
  1. The action buttons “Ignore alert(s)”, “Monitor alert(s)” and “Raise Incident” have been moved under the “Actions” button
  2. The “Actions” button has been renamed to “More Info”
  3. Similar Log Data is grouped together, when creating an Incident

Admin

- **Users**
  1. Format validation when entering phone numbers has been added

2. More user clarity is being introduced with the addition of "**Summary Indicators**", including Registered, Active, Portal-Admins and Locked
3. Client site validation when entering user related information has been added
4. A warning message is displayed if user license limit has been reached

- **User Roles**
  1. Column added to display the user role type

- **License**
  1. The timeline graphs colors have changed
  2. The "**Summary Indicators**" colors have changed

- **License Overview**
  1. Added the Log Data volume of the last completed day
  2. Enterprise Endpoints license is displayed
  3. The type of service acquired (Express, Standard, Plus, Premium) is displayed

- **Groups**
  1. Assets: In view/edit of a group under the "Assets Association", the legend and text from icons have been removed. Information is now displayed via a mouse-over
  2. Users: In view/edit of a group, a "Refresh" button is been added in the "Asset Groups Association" in order for new changes to be visible
  3. Assets: In view/edit of a group, counters display the number of groups in which an asset belongs to

- **Assets**
  1. When adding a new Asset, the user adding this Asset should select group(s) to associate with-that this Asset should belong to

Analytics

- **Big Data Search**
  1. Alphabetic sorting on filters has been added
  2. The "Asset Name" and Asset "IP Address" in the results have been added
  3. When applying a filter on facet value the number of distinct values returned increased from 100 to 1,000

Vulnerability Management

- **Manage Scans**
  1. In the Vulnerabilities of an Asset, the "Delete" button has been renamed to "Remove"

General

- **Notifications**
  1. Pop-Up messages/Slider notifications are displayed based on user's role access permissions

2. Pop-Up message does not animate if not acknowledged
3. Exploitability and Impact Factors related to the Incident raised have been added

- Subcategory “Linux Services” has been renamed to “Unix Services”
- The user could type or use the up/down arrows for specifying date values
- **New LogSources**
  1. The “Not Sending Logs” status on newly created LogSources is set based on the “No LogData configuration” found under the Assets -> Configuration-Gear
- “Help appearance has been improved
- Tool-Tip on mouse-over remains visible until the mouse pointer is removed
- **Shortcut creation**
  1. A notification message is displayed when the user tries to add a new shortcut to the “HomeScreen” once the maximum allowed shortcuts has been reached
- **New Password page**
  1. Changed caption on new password title and disabled the browser autofill

BUG FIXES

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

NEW SUPPORTED LOGSOURCES

Vendor	Product	Version Supported	Type of Collection
Riorey	rWeb	RIOS 5.x and higher	SMTP
McAfee	McAfee Host Protection	7.0 and higher	ODBC
McAfee	McAfee Data Loss Prevention	7.0 and higher	ODBC
McAfee	McAfee Virus Scan Enterprise	7.0 and higher	ODBC
McAfee	McAfee Solidifier	7.0 and higher	ODBC
McAfee	McAfee VirusScan Enterprise for Linux	7.0 and higher	ODBC
McAfee	McAfee Security for MS Exchange	7.0 and higher	ODBC
Fortinet	Fortigate Fortianalyzer	All	Syslog
Fortinet	Fortigate App Control	All	Syslog
Fortinet	Fortigate DLP	All	Syslog
Fortinet	Fortigate System	All	Syslog
Fortinet	Fortigate User	All	Syslog
Fortinet	Fortigate Virus	All	Syslog
Fortinet	Fortigate VPN	All	Syslog
Fortinet	Fortigate WAD	All	Syslog
Fortinet	Fortigate Traffic	All	Syslog
Fortinet	Fortigate Email Filtering	All	Syslog
Fortinet	Fortigate IPS	All	Syslog
Fortinet	Fortinet FortiWeb	All	Syslog
F5 Networks	F5 Analytics	All	Syslog
Check Point	CheckPoint HTTPS Inspection	R77.30 and higher	LEA
Check Point	CheckPoint Antimalware	R77.30 and higher	LEA
Check Point	CheckPoint New Antivirus	R77.30 and higher	LEA
Check Point	CheckPoint Security Gateway	R77.30 and higher	LEA
Linux	Nailslogd	-	Syslog

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

OFFICES

GREECE **SERBIA** **U.A.E.** **USA** **SOUTH AFRICA**