ClearSkies™ NG SIEM

Version 5.8 & 5.8.1

Incorporating the power of

Big Data Advanced Security Analytics

June 2018

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 Advanced Security Analytics.

What's New in v5.8 & 5.8.1

Sensitivity Level of User activity

Each UEBA user may be assigned a different sensitivity level (Relaxed, Neutral and Aggressive) which is determined based on his/her behavioral activity in combination with the criticality of information this user has access to. Sensitivity levels describe how a user's activities may be classified into suspicious or malicious.

Enhance the detection of sophisticated attacks and insider threats using UEBA

- Enhance the detection of sophisticated threats or unusual behavior using Machine Learning Models.
- Introduction of global and per user activity "Whitelisting" for minimizing false positive alerts.
- Full integration with Active Directory for analysing and correlating host-related activity based on user properties and permissions.
- Expand the analysis regarding host, network and application user activities for enchasing its behavioral profile.
- Introduction of forensic audit trail for further investigation of identified suspicious and malicious activities and abnormal user behavior.

Meet and validate compliance with GDPR

Delivers the GDPR 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 GDPR.

New Features

Sensitivity Level of User activity

Each UEBA user may be assigned a different sensitivity level (Relaxed, Neutral and Aggressive) which is determined based on his/her behavioral activity in combination with the criticality of information this user has access to. Sensitivity levels describe how a user's activities may be classified into suspicious or malicious.

Analytics (User and Entity Behavior Analysis)

- Enhance the detection of sophisticated threats or unusual behavior using Machine Learning Models.
- Introduction of global and per user activity "Whitelisting" for minimizing false positive alerts.
- Full integration with Active Directory for analysing and correlating host-related activity based on user properties and permissions.
- Expand the analysis regarding host, network and application user activities for enchasing its behavioral profile.
- Introduction of forensic audit trail for further investigation of identified suspicious and malicious activities and abnormal user behavior.

Compliance (GDPR)

Delivers the GDPR 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 GDPR.

Event Management (Alerts)

Ability of the user to create custom Alerts and Incidents based on his/her observation of unrelated events detected.

Enhancements

"ServiceModules"

Event Management

- Incidents
  - Enabled the "Final review" state to be reset back to "Normal State".
  - Corrected the different audit inserted for Incidents created by the MSS/MDR team and the Customer.
  - Added the "Incident Title" in the main grid and a button that allows the title modification.
  - Added an audit entry for the "No LogData" in the "History" tab.

- Correlation
  - Added an "Enable/Disable" button.
  - Assigned the "Incident title" to be set to the Correlation rule name when the "Auto-Incident" option is turned ON.

- Alerts
  - Added paging on "View Logs" option under the "More Info" dropdown menu.
  - Added a field to insert an incident title when raising an Incident.

- Alert Filtering
  - Added the "Created Date", "Modified Date" and "Modified by" fields in the main grid.

- Alerts / Incident Geolocation
  - Added the "Asset Name" in the main grid.

Vulnerability Management

- Manage Scans
  - Increased the file upload size from 5 MB to 20 MB.
  - Increased the number of hosts allowed in a scan from 20 to 100.

- Review Results
  - Changed the "Low" vulnerability classification type to "Informative".

Analytics

- Asset Behavioral Analysis
  - Application deprecated.

Reports

- Create
  - Added the "View" button.
  - Added an "Enable/Disable" button.
  - Added more fields for the “LogSources” category in “Portal Data” reports, like “Asset Name”, “IP Address”, “Last Updated”, “Category”, “License Status”, “Monitored By” and "Created Date".
  - Enabled the "Portal Data" reports to allow you to find "Not Configured" LogSources for the "Sending Logs" option in the "LogSources" Category.
  - Added the "Incident Title" and "Raised By" fields in "Portal Data" reports for the "Incident" Category.
  - Increased the number of results in “Portal Data” Reports from 1000 to 5000.
  - Enabled the display of all allowed SubCategories even if a LogSource does not have License.

- Results
  - Added the "View" button.

Compliance

- General
  - Adjusted the "Status" and "Severity" to be shown in the “History” tab.

Admin

- Users
  - Enabled the "User Roles" to be shown in alphabetic order when adding a User.
  - Added the "View" button.

- User Roles
  - Added the "View" button.
  - Allowed the total number of 20 “User Roles”.
  - Renamed the "Access Permission" for "Monitor Alert" to "Suspicious".
  - Added icons on the tree in "Access Permissions" for "Admin" items.
  - Removed the notification options for “LogSources” – Sending/Not Sending Logs.

- Groups
  - Enabled the display of the number of “User Groups” and “Users” associated with an “Asset Group” in the "Assets" tab.
  - Added the "View" button.
  - Added a different highlight for “Users” or “Assets” that exist only in one Group.

- Password Policies
  - Added the "View" button.
  - Enabled the user "Idle timeout" in the password policies to be controlled by the "Portal Admin".

- Assets
  - The "Asset Groups" are displayed alphabetically in the filter dropdown menu.
  - Added a mouse-over message showing possible reasons when the "Request to monitor" button is disabled.
  - Enabled an “Asset” not to be closed when a license is Applied/Revoked.
  - Added an information icon in the “Configurations Gear” next to “Alert” in the grid that shortly explains the behavior of the “No LogData” alert.

- Asset Configuration
  - Added the "View" button.
  - Added the option to filter Gateways in “Check Point Lea” configuration.

"TopMenu"

- Moved the "User Menu" to open on the right hand side.

"Tools"

- Alias Manager
  - Added the "View" button.
- Data Masking
  - Added the "View" button.
- Tile Manager
  - Added the "View" button.
- Classifications/Disclaimers
  - Added the "View" button.
- Downloads
  - Adjusted "Download a file" so that it doesn't need another tab to open.

"Preferences"

- Network Manager
  - Added the "View" button.

"General"

- Notifications
  - Added notifications for when a LogSource is updated.
  - Updated the signature, which also includes an image with a link.
  - Changed the "From" field in emails to the "@clearskiessa.com" domain.
  - Included the user's "Salutation" and the "Last Name" in the body of emails sent.
- User Preferences
  - Added the option to set an "Alternative Login Location".
  - Added an "Information" icon next to the "City" field in "Business Address".

- Indicators
  - Enabled the full original value to be displayed on mouse-over if the value was rounded.

- Location-based authentication
  - Enabled the validation of users with IP address.

What's New in v5.8.1

Enhancements

Admin

- User Roles
  - Added grid filtering in Access Permissions and notifications.
  - Access permissions for editing Predefined 1 and 2 Dashboards transferred to "Portal Admin".

- Asset Configuration
  - Applied small UI changes and ability to find an Asset/Asset Group by just starting to type its name.
  - Added the option to filter Gateways in Check Point Lea configuration.

- Groups
  - Value groups created by Odyssey are now not editable, but can be copied.

- Password Policies
  - When the Idle timeout is set to 0, it means that there is no idle timeout.

Performance & Availability

- Health Status
  - Updated the iCollector engine so as to support connection checks on UDP services.

- TopMenu
  - Icons are now clickable, and are highlighted (greyed) with mouse over.

Event Management

- Correlation
  - Value groups created by each side are shown in the filter configuration (step 3).
  - Added support to count "Distinct" values.

- Alerts
  - The "Actions" dropdown menu is now hidden if the user has no access permissions.

Dashboards

- User-Defined

➢ Added a new Portlet named "Events per 5 min from all LogSources".
➢ Added a new Portlet named "Events per hour from all LogSources".
➢ Added a new Portlet named "Top 10 Users by # of Events".
➢ Added a new Portlet named "NetFlow events by Asset".
➢ Added a new Portlet named "User successful logons by Asset".
➢ Added a new Portlet named "Failed and successful attempts based on Active Directory".

Reports

- Create

➢ Empty values in criteria are now disallowed.

Analytics

- User and Entity Behavior Analysis

➢ Updated the "User's Activity Breakdown" graph in a User's Profile with a new one, and changed the name to "Activity".
➢ Added the option for the "Portal Admin" to set the sensitivity on different users via the configuration gear icon.
➢ Added a cellphone icon in the "User Profile" under the user's graph in case the cellphone is connected to an MDM device.
➢ Set the default view of the application to "Last 24 Hours".
➢ The application is integrated with an Active Directory and creates as Entities all discovered users.
➢ When clicking an IP address in the "Analysis for Malicious Endpoint Activity flags" a direction is now performed to the "Behavior Analysis" application.
➢ Updated the "Suspicious/Malicious Flags" graph to show a percentage number based on what it was detected within the organization.

- Big Data Search

➢ Renamed the tab names in Source IP filters from "Internal" to "LAN", and from "External" to "Internet".

Bug Fixes

These versions resolve a number of stability and performance issues identified.

New Supported LogSources

Vendor	Product	Version Supported	Type of Collection
Check Point	Check Point Syslog	R77.30	LEA
Check Point	Check Point Antivirus & FW	R77.30	LEA
Check Point	Check Point Other	R77.30	LEA
BIND	DNS Queries	v.9	Syslog
Zimbra	Zimbra Email Server	ALL	Syslog
Cisco	Cisco Unified Communications Manager	Cisco iOS	Syslog
Fortigate	Fortigate Router	FortiOS 5.x	Syslog
Fortigate	Fortigate VOIP	FortiOS 5.x	Syslog
Fortigate	Fortigate FortiSandbox Results	FortiOS 5.x	Syslog
Fortigate	Fortigate Endpoint Control	FortiOS 5.x	Syslog
Fortigate	Fortigate DNS	FortiOS 5.x	Syslog
OSSEC	OSSEC HIDS	ALL	Syslog
Imperva	Imperva Database Firewall	v.10	Syslog
Imperva	Imperva System Events	v.10	Syslog
TrendMicro	Trend Micro Control Manager CEF	ALL	Syslog
Bluecoat	Bluecoat Gateway	ALL	Syslog
Palo Alto	Palo Alto Traffic CEF	PANOS v.5.x	Syslog
Palo Alto	Palo Alto Threat CEF	PANOS v.5.x	Syslog
Arbor	Arbor DDoS Protection	ALL	Syslog
IBM	IBM Storwize	ALL	Syslog
McAfee	McAfee WebGateway Audit	v.7.x	Syslog

McAfee	McAfee Agent	ePO v5.3.3	ODBC
McAfee	McAfee AutoUpdate	ePO v5.3.3	ODBC
McAfee	McAfee Virus Scan Enterprise (syslog)	ePO v5.3.3	ODBC
McAfee	McAfee Virus Scan Enterprise for Linux (syslog)	ePO v5.3.3	ODBC
McAfee	McAfee Drive Encryption	ePO v5.3.3	ODBC
McAfee	McAfee Endpoint Encryption	ePO v5.3.3	ODBC
McAfee	McAfee DLP Host	ePO v5.3.3	ODBC
McAfee	McAfee Solidifier (syslog)	ePO v5.3.3	ODBC
McAfee	McAfee System Prep	ePO v5.3.3	ODBC
McAfee	McAfee Active Response	ePO v5.3.3	ODBC
McAfee	McAfee AntiSpyware Enterprise	ePO v5.3.3	ODBC
F5	F5 BIG-IP Application Security Manager	ALL	Syslog
Juniper	JunOS Pulse Secure	ALL	Syslog
Symantec	Symantec Endpoint Protection	SEP v.11	ODBC
IBM	IBM Security Identity Management	ALL	Syslog
Odyssey	PassiveDNS	ALL	Syslog
Oracle	Oracle GoldenGate	ALL	Syslog
KEMP	KEMP LoadBalancer	ALL	Syslog
RedHat	JBoss Application Server	ALL	Syslog
Cisco	Cisco Firepower	v.6.x	Syslog
Ecessa	Ecessa PowerLink	ALL	Syslog