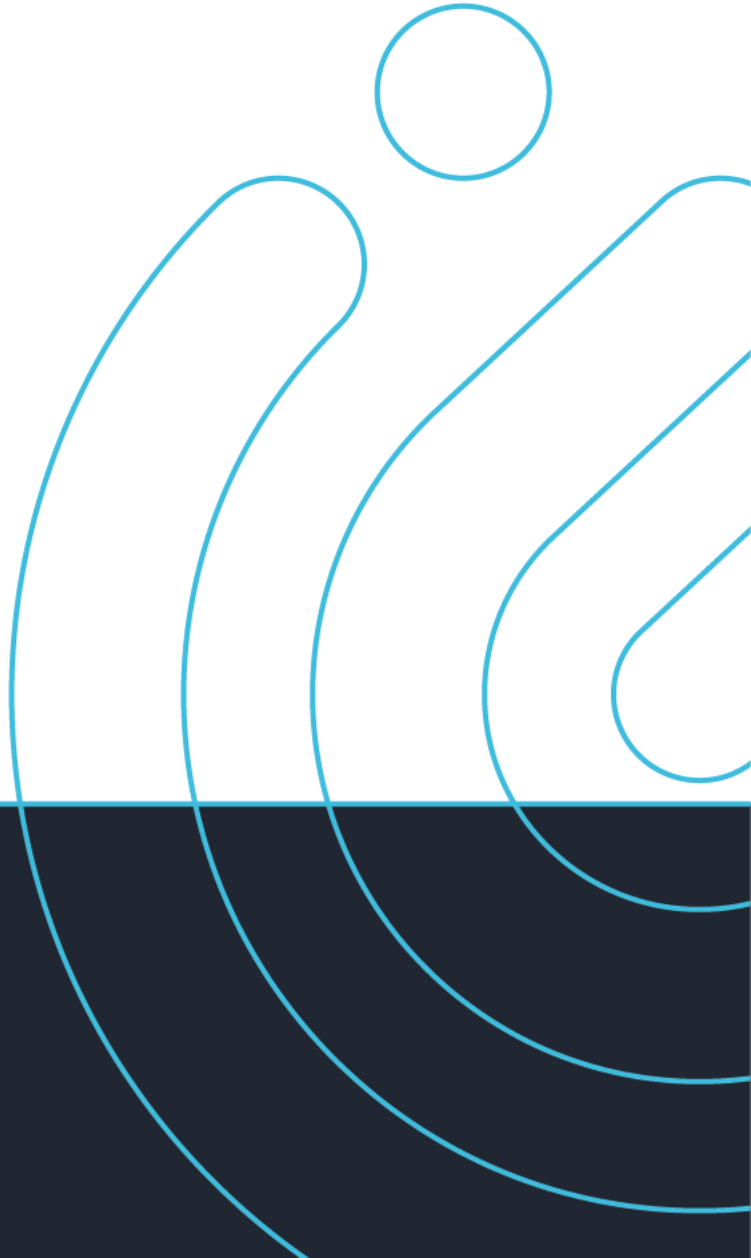
RELEASE NOTES

ClearSkies™ SIEM

Version 6.6.2/ September 2023

"Unlock the Intelligence of Your Data"



ClearSkies™

Table of Contents

Overview

This version release of ClearSkies™ Threat and Vulnerability Platform (T&VP) includes features and enhancements that empower organizations and MSSPs, of any size, in any industry, to effectively anticipate, respond, swiftly recover, and adapt to the emerging threats and vulnerabilities of a dynamically evolving and expanding threat landscape.

What's New in v6.6.2

Several new features, functionality enhancements and bug fixes are introduced in ClearSkies™ T&VP version 6.6.2, including:

- **'Threat Taxonomy' merged with 'Use Case'**: The 'Threat Taxonomy' and 'Use Cases' sections are merged together for simplifying the creation, maintenance and deployment of Correlation rules.
- **Distributed iCollector Architecture:**
  - Provides the ability to deploy multiple collectors, which is suitable for enterprise organizations with remote locations of varying sizes and complexity.
  - Enables the implementation of tailored correlation rules, both specific and broader in scope, at remote locations based on their unique system and network structures.
  - Enhances the collection and processing capacity of log and event data through the use of 'Advanced Forwarders.'
- **Other Enhancements:** Enriched user experience and functionality.

Important Notes

No special considerations applicable for this version.

New Features

"Correlation"

- The 'Threat Taxonomy' and 'Use Cases' merged to provide a unified view of all available use cases. Users can now easily filter for applicable use cases and choose when and how to deploy them, Furthermore, they create, maintain, and deploy Correlation rules all with just a few clicks. This streamlined process allows users to secure their environment and reduce their risk more efficiently.

"iCollector"

- Introducing the Distributed architecture of ClearSkies™ 'iCollector', which brings enhanced convenience in data loading and improved flexibility. This architecture now supports the provision of multiple collectors for a single project, while maintaining the iCollector's core importance within ClearSkies. Advanced Forwarders are responsible for collecting, normalizing, and processing log data, subsequently forwarding the normalized data to the iCollector for correlation and enrichment with Threat Intelligence. This process effectively enhances the solution's capacity. Furthermore, Syslog Forwarders can be strategically deployed in remote locations to cater to geographically diverse organizations. By harmonizing all these elements, ClearSkies can deliver a personalized solution tailored to the distinct requirements of each organization. This procedure impacts various modules within ClearSkies, including the 'iCollector Management' page, the 'Asset' page, the 'Marketplace' page, and the 'License Overview'.

Enhancements

New enhancements have been implemented to improve functionality and user experience.

"Incidents"

ClearSkies™

- **Configuration Settings**
  - A new configuration was added, now users can keep the current default values of each filter. All filters that are placed in the top toolbar Included In the global configuration panel. Also, it allows the user to select to sort the grid with the preferable column and the sorting order.
  - The settings 'Weekly / Monthly' buttons are now labeled as 'Frequency'.

- **Assets**
  - A new option was included under the "History" tab of the "Maintenance" which is refers to the start, end and duration of an Asset maintenance.

Event Management

- **Correlation**
  - The Correlation module stepper was redesigned to include new sections such as "SOAR configuration" and "Extended Auto-Event configuration".

SOAR

- **New product support**
  - ClearSkies™ SOAR now supports **Sophos XG Firewall API**.

"SWP"

ClearSkies™

- **New functionality added**
  - Now the functionality to export the evidence logs from module "Alerts" on Excel file was added on SWP too.

Bug fixes

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

New Supported Products and Versions

Vendor	Product	Product Category	Product Version	Log Collection Method	Whats New
Aruba	ClearPass NAC CEF	Access Control	6.10.7	Syslog (CEF)	product support
Aruba	ClearPass NAC System CEF	Audit	6.10.7	Syslog (CEF)	product support
BitDefender	BitDefender GravityZone	Endpoint Protection	6.29, 6.40	Syslog (CEF)	product support (6.40)
Cisco	Cisco ASA	Firewall	9.8(2), 9.12	Syslog	version support (9.12)
Cisco	Cisco Email Security CEF	Email Gateway	13.5.3, 14.0.0, 14.2.1	Syslog	version support (14.2.1)
Cisco	Cisco Firepower	IDS - IPS	6.6.1	Syslog	version support
Cisco	Cisco Firepower Management	Health status	6.6.1	Syslog	version support
Cisco	Cisco ISE	Access Control	3.1.0	Syslog	version support
Cisco	Cisco Meraki Events	Network Management	**MX**: 15.42.1, 15.44, 16.16, 17.10, 18.10 **MR**: 28.6.1	Syslog	version support (MX: 17.10, 18.10)
Cisco	Cisco Meraki Flows	Connection Monitoring	**MX**: 15.42.1, 15.44, 16.16, 17.10, 18.10 **MR**: 28.6.1	Syslog	version support (MX: 17.10, 18.10)
Cisco	Cisco Meraki Security Events	IDS - IPS	**MX**: 15.42.1, 15.44, 16.16, 17.10, 18.10 **MR**: 28.6.1	Syslog	version support (MX: 17.10, 18.10)
Cisco	Cisco Meraki URLs	Web Gateway	**MX**: 15.42.1, 15.44, 16.16, 17.10, 18.10 **MR**: 28.6.1	Syslog	version support (MX: 17.10, 18.10)

Cisco	Cisco Nexus Switch	Network Management	**NX-OS:** 7.1, 7.3, 9.7(7a)	Syslog	version support (7.1)
Cisco	Cisco Switch-Router	Network Management	**IOS**: v.15.2 (2) E9, v.15.2(4)E8, 16, 17 **IOS XE**: v.16.09.04, v.16.09.07, v.16.12.3a, v.16.12.04 **SBS** [8]: 1.4.11.5, 2.5.0.90, 2.5.7.85, 3.0.0.69, 3.06	Syslog	version support (SBS 3.06)
Cisco	Cisco Unified Communications Manager	Telephony	14	Syslog	version support
Cisco	Cisco Email Security Management	Audit	13.5.3, 14.0.0, 14.2.1	Syslog, Syslog (SCP)	version support (14.2.1)
Cisco	DUO Authentication Proxy	Access Control	5.4.0, 5.7.3	Syslog	product support
Citrix	Citrix NetScaler	Remote Access	13	Syslog	version support
Cloudflare	Cloudflare Firewall	Application Firewall	-	Syslog	product support
CrowdStrike	CrowdStrike Falcon EDR	Endpoint Protection	1.0	Syslog (CEF)	new event types support
CrowdStrike	CrowdStrike Falcon EDR System	Audit	1.0	Syslog (CEF)	new event types support
Darktrace	Darktrace	Enterprise Immune System	5.0.11, 6.0.17, 6.0.27	Syslog	version support
Darktrace	Darktrace Audit	Enterprise Immune System	5.0.11, 6.0.17, 6.0.27	Syslog	version support
F5 Networks	F5	Load Balancer	15.1.8	Syslog	version support
F5 Networks	F5 BIG-IP Application Security Manager	Application Firewall	15.1, 16.1.32	Syslog	version support, log

					format support
Forcepoint	Email Security	Email Gateway	8.5.5	Syslog (CEF)	product support
Forcepoint	Email Security System	Audit	8.5.5	Syslog (CEF)	product support
Forescout	Forescout CounterAct	Access Control	8.2.0, 8.4.0	Syslog (CEF)	version support (8.4.0)
Fortinet	Fortigate Access Control CEF	Access Control	6.2.3, 6.2.9, 6.4.2, 6.4.3, 6.4.4, 6.4.5, 6.4.6, 6.4.7, 6.4.11, 6.4.12, 7.0.0, 7.0.1, 7.0.3, 7.0.4, 7.0.5, 7.0.8, 7.0.9, 7.2.4	Syslog (CEF)	version support (6.4.12, 7.2.4)
Fortinet	Fortigate Application Control CEF	Application Control	6.2.3, 6.2.9, 6.4.2, 6.4.4, 6.4.5, 6.4.6, 6.4.7, 6.4.8, 6.4.11, 6.4.12, 7.0.0, 7.0.1, 7.0.3, 7.0.4, 7.0.5, 7.0.8, 7.0.9, 7.2.3, 7.2.4	Syslog (CEF)	version support (6.4.12, 7.2.3, 7.2.4)
Fortinet	Fortigate DNS CEF	DNS	6.2.3, 6.2.9, 6.4.2, 6.4.3, 6.4.4, 6.4.5, 6.4.6, 6.4.7, 6.4.8, 6.4.11, 7.0.0, 7.0.1, 7.0.3, 7.0.4, 7.0.5, 7.0.8, 7.0.9, 7.0.10, 7.2.4	Syslog (CEF)	version support (7.0.10, 7.2.4)
Fortinet	Fortigate Firewall CEF	Firewall	5.6.8, 5.6.14, 6.2.3, 6.2.9, 6.4.2, 6.4.3, 6.4.4, 6.4.5, 6.4.6, 6.4.7, 6.4.8, 6.4.11, 6.4.12, 7.0.0, 7.0.1, 7.0.3, 7.0.4, 7.0.5, 7.0.7, 7.0.8, 7.0.9, 7.0.10,	Syslog (CEF)	version support (5.6.8, 5.6.14, 6.4.12, 7.0.7, 7.0.10, 7.2.3, 7.2.4, 7.3.4)

			7.2.1, 7.2.3, 7.2.4, 7.3.4		
Fortinet	Fortigate IPS CEF	IDS - IPS	6.2.3, 6.2.9, 6.4.2, 6.4.4, 6.4.5, 6.4.6, 6.4.7, 6.4.8, 6.4.11, 6.4.12, 7.0.0, 7.0.1, 7.0.3, 7.0.4, 7.0.5, 7.0.8, 7.0.9, 7.0.10, 7.2.4	Syslog (CEF)	version support (6.4.12, 7.0.8, 7.0.9, 7.0.10, 7.2.4)
Fortinet	Fortigate System CEF	Audit	5.6.8, 5.6.14, 6.2.3, 6.2.9, 6.4.2, 6.4.3, 6.4.4, 6.4.5, 6.4.6, 6.4.7, 6.4.8, 6.4.11, 6.4.12, 7.0.0, 7.0.1, 7.0.3, 7.0.4, 7.0.5, 7.0.7, 7.0.8, 7.0.9, 7.0.10, 7.2.3, 7.2.4, 7.3.4	Syslog (CEF)	version support (5.6.8, 5.6.14, 6.4.12, 7.0.7, 7.0.10, 7.2.3, 7.2.4, 7.3.4)
Fortinet	Fortigate VOIP CEF	Telephony	6.2.3, 6.2.9, 6.4.2, 6.4.4, 6.4.5, 6.4.6, 6.4.7, 7.0.0, 7.0.1, 7.0.3, 7.0.4, 7.0.5, 7.0.10, 7.2.4	Syslog (CEF)	version support (7.0.10, 7.2.4)
Fortinet	Fortigate WAF CEF	Application Firewall	6.2.3, 6.2.9, 6.4.2, 6.4.4, 6.4.5, 6.4.6, 6.4.7, 6.4.11, 6.4.12, 7.0.0, 7.0.1, 7.0.3, 7.0.4, 7.0.5, 7.08, 7.0.9, 7.2.4	Syslog (CEF)	version support (6.4.12, 7.2.4)
Fortinet	Fortigate WebFilter CEF	Web Gateway	6.2.3, 6.2.9, 6.4.2, 6.4.4, 6.4.5, 6.4.6, 6.4.7, 6.4.8, 6.4.11, 6.4.12, 7.0.0, 7.0.1, 7.0.3, 7.0.4, 7.0.5, 7.08,	Syslog (CEF)	version support (6.4.12, 7.0.10, 7.2.3, 7.2.4)

			7.0.9, 7.0.10, 7.2.3, 7.2.4		
Fortinet	Fortimail Email Gateway	Email Gateway	6.4.4, 6.4.6, 7.0.5, 7.2.2	Syslog	version support (7.0.5)
Fortinet	Fortimail System	Audit	6.4.4, 6.4.6, 7.0.5, 7.2.2	Syslog	version support (7.0.5)
Fortinet	FortiAuthenticator Access Control	Access Control	6.4, 6.4.1, 6.4.6	Syslog	version support (6.4.6)
Fortinet	FortiAuthenticator System	Audit	6.4, 6.4.1, 6.4.6	Syslog	version support (6.4.6)
Fortinet	FortiAnalyzer Fortigate Firewall [7]	Firewall	6.4.7, 7.0.3, 7.2.2	Syslog	version support (7.2.2 - FortiGate Firewall via FortiAnalyzer)
Fortinet	FortiAnalyzer FortiGate Application Control [7]	Web Gateway	6.4.7. 7.2.2	Syslog	product support (FortiGate Application Control via FortiAnalyzer)
Fortinet	FortiAnalyzer FortiGate Web Filter [7]	Web Gateway	6.4.7. 7.2.2	Syslog	product support (FortiGate Web Filter via FortiAnalyzer)
Fortinet	FortiAnalyzer FortiGate DNS [7]	DNS	6.4.7. 7.2.2	Syslog	product support (FortiGate DNS via FortiAnalyzer)
Fortinet	FortiAnalyzer FortiGate System [7]	Audit	6.4.7. 7.2.2	Syslog	product support (FortiGate System

					via FortiAnalyzer)
Fortinet	FortiAnalyzer FortiGate Email Filtering [7]	Email Gateway	7.2.2	Syslog	product support (FortiGate Email FIltering via FortiAnalyzer)
Fortinet	FortiAnalyzer FortiGate Access Control [7]	Access Control	7.2.2	Syslog	product support (FortiGate Access Control via FortiAnalyzer)
Fortinet	FortiAnalyzer FortiGate IPS [7]	IDS - IPS	7.2.2	Syslog	product support (FortiGate IPS via FortiAnalyzer)
Fortinet	FortiAnalyzer Fortigate WAF	Application Firewall	7.2.2	Syslog	product support (FortiGate WAF via FortiAnalyzer)
Fortinet	FortiEDR	Endpoint Protection	5.2.0	Syslog	product support
Fortinet	FortiEDR System	Audit	5.2.0	Syslog	product support
Genian	NAC Enterprise	Access Control	5.0	Syslog (CEF)	product support
Hewlett Packard	HP iLO	Lights Out Management	2.72, 2.78	Syslog	version support (2.78)
IBM	zSecure Alert	Audit	2.4.0	Syslog (CEF)	product support
Kaspersky	Kaspersky Security Center	Endpoint Protection	11.0.0.1131, 13.2.0.1511, 14.0	Syslog	version support
LibreNMS	LibreNMS	Health status	23.4.1	Syslog	product support

Manage Engine	Manage Engine ADAudit Plus	Audit	4.2, 7.1.1	Syslog (CEF)	version support
Palo Alto Networks	Palo Alto Firewall CEF	Firewall	8.1.5 - 10.0.2, 10.1, 10.2.3, 11.0	Syslog (CEF)	version support (11.0)
Palo Alto Networks	Palo Alto IPS CEF	IDS - IPS	8.1.5 - 10.0.2, 10.1, 10.2.3, 11.0	Syslog (CEF)	version support (11.0)
SonicWall	SonicWallOS Access Control	Access Control	6.5.1.5-6n, 7.0.1	Syslog (CEF)	version support (7.0.1)
SonicWall	SonicWallOS Antivirus	Anti Virus	6.5.1.5-6n, 7.0.1	Syslog (CEF)	version support (7.0.1)
SonicWall	SonicWallOS Application Control	Application Control	6.5.1.5-6n, 7.0.1	Syslog (CEF)	version support (7.0.1)
SonicWall	SonicWallOS DNS	DNS	6.5.1.5-6n, 7.0.1	Syslog (CEF)	version support (7.0.1)
SonicWall	SonicWallOS Firewall	Firewall	6.5.1.5-6n, 7.0.1	Syslog (CEF)	version support (7.0.1)
SonicWall	SonicWallOS IPS	IDS - IPS	6.5.1.5-6n, 7.0.1	Syslog (CEF)	version support (7.0.1)
SonicWall	SonicWallOS System	Audit	6.5.1.5-6n, 7.0.1	Syslog (CEF)	version support (7.0.1)
SonicWall	SonicWallOS VPN	VPN	6.5.1.5-6n, 7.0.1	Syslog (CEF)	product support
SonicWall	SonicWallOS Web Gateway	Web Gateway	6.5.1.5-6n, 7.0.1	Syslog (CEF)	product support
Sophos	Sophos UTM Web Filter	Web Gateway	9.7.13	Syslog	version support
Sophos	Sophos XG Firewall	Firewall	17.5.15, 18.0.3, 18.0.4, 18.0.5, 18.5.1, 19.0	Syslog	version support (17.5.15, 18.0.5)
Sophos	Sophos UTM Firewall	Firewall	9.0, 9.7.13	Syslog	version support
Sophos	Sophos UTM System	Audit	9.0, 9.7.13	Syslog	version support
Sophos	Sophos Central	Endpoint Protection	1	API	product support (CR coverage will be

					concluded after 2-3 weeks)
Sophos	Sophos UTM IPS	IDS - IPS	9.7.13	Syslog	version support
Symantec	Symantec Messaging Gateway	Email Gateway	10.7.0	Syslog	version support
Trend Micro	Smart Protection Server	Endpoint Protection	-	Syslog (CEF)	product support
Trend Micro	Deep Security Manager	Endpoint Protection	-	Syslog (CEF)	product support