RELEASE NOTES

ClearSkies™

TDIR Platform

Version 6.8 / March 2025

SEE BEYOND THE NOISE, RESPOND WITH INTELLIGENCE & CONFIDENCE

ClearSkies™

Contents

Copyright & Legal Information

Copyright Notice

Trademarks

Refer to the Copyright page http://www.clearskiessa.com/copyright for a list of our trademarks.

Feedback

Odyssey Consultants is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments to erratum@clearskiessa.com

Overview

ClearSkies™ TDIR – Optimized for Faster Detection and Response

The latest release of ClearSkies™ Threat Detection, Investigation, and Response (TDIR) is designed to help organizations and MSSPs drastically **reduce Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR)** — two critical factors **in minimizing the impact of modern cyber threats.** By automating detection and response workflows, enriching alerts with real-time intelligence, and **providing clear investigative guidance**, **ClearSkies™ TDIR** empowers your SecOps team to contain threats faster, limit damage, and maintain operational continuity.

Highlights

AI-Powered SecOps Intelligent Assistant

Augment the capabilities of your SecOps team by automating time-consuming tasks, provide context to complex cyber threats, improve threat detection, and enable faster and more accurate response actions to stay ahead of evolving threats — especially from AI-Powered adversaries.

Native Playbook Capabilities

Helping your SecOps team streamline detection and incident response with predefined, automated workflows for sophisticated AI-driven threats like malware, phishing, unauthorized access, and anomalous behavior.

MITRE ATT&CK Integration

Aligns with MITRE ATT&CK, automatically mapping incidents to adversary tactics, techniques, and detection methods and provides the common language for SecOps team, threat hunters, and executives to discuss threats.

What's New in v.6.8

AI-Powered SecOps Intelligent Assistant Agent for Alert Analysis

A **new AI Assistance Agent** enhances alert analysis with AI-generated insights. With a simple right-click on any alert, analysts can **instantly access structured analysis and recommendations**, **accelerating investigations** and **improving response** times.

Key Benefits:

1. **Automated Alert Analysis:** Automatically analyzes and enriches alerts from multiple sources, reducing manual effort and accelerating initial triage.
2. **Faster, Smarter Decision-Making**: Provides analysts with real-time context, recommended investigation steps, and AI-driven insights to guide faster and more accurate responses.
3. **Prioritized Threat Response:** Assesses severity, relevance, and context of each alert, helping teams focus on the most critical threats first.
4. **Improved Detection Accuracy:** Leverages AI to detect patterns and anomalies that may be missed manually, reducing false positives and highlighting genuine threats.
5. **Seamless Integration:** Fully embedded within the TDIR platform, ensuring consistent analysis across all data sources for a unified, centralized view of your security landscape.
6. **Continuous Learning & Adaptation:** AI models continuously evolve, learning from new data and attack techniques to enhance future detections and response actions.

Native Playbook Capabilities

ClearSkies™ TDIR Platform now offers **native playbook capabilities**, helping you streamline detection and incident response with predefined, automated workflows for **sophisticated AI-driven threats** like malware, phishing, unauthorized access, and anomalous behavior. These automated workflows **enhance response speed, accuracy, and consistency** while remaining fully customizable to match your organization's unique needs.

Key Benefits:

1. **Standardized Incident Response:** Provides a structured approach to handling threats, reducing reliance on ad-hoc decision-making.
2. **Automation & Efficiency:** Automates repetitive tasks (e.g., enrichment, containment, remediation), allowing analysts to focus on high-value activities.
3. **Faster Threat Mitigation:** Enables rapid response by executing predefined actions, minimizing the impact of cyber threats.
4. **Contextualized Decision-Making:** Integrates threat intelligence and historical data to guide analysts through informed, data-driven responses.
5. **Cross-Team Collaboration:** Ensures seamless coordination between teams by providing clear, documented steps for investigation and resolution.
6. **Regulatory Compliance & Auditability:** Helps meet compliance requirements by enforcing consistent incident-handling procedures and maintaining an audit trail.

MITRE ATT&CK Integration

ClearSkies™ TDIR platform now fully aligns with the **MITRE ATT&CK framework**, providing **enhanced visibility into adversary tactics, techniques, and detection methods**. Incidents are **automatically** mapped to the framework, enabling your team to **understand attack patterns, identify potential gaps in your defenses, and prioritize response actions** with greater precision — all contributing to a stronger, more proactive security posture.

Key Benefits:

1. **Enhanced Threat Detection:** Maps adversary behavior to tactics, techniques, and detection methods to improve detection accuracy and identify early-stage threats before they escalate.
2. **Context-Driven Investigations:** Provides a structured framework to understand attack progression, correlating security events with known techniques to enable faster triage and threat prioritization.
3. **Improved Response & Mitigation:** Aligns response playbooks with MITRE ATT&CK techniques to ensure targeted, effective countermeasures, allowing SecOps teams to proactively disrupt attack chains by addressing known adversary behaviors.
4. **Cross-Team Collaboration & Reporting:** Provides a common language for analysts, threat hunters, and executives to align on threats, while enabling data-driven security decisions by visualizing attack patterns and identifying security coverage gaps.
5. **Continuous Security Improvement:** Help organizations identify detection gaps and refine their security posture while supporting red and purple teaming exercises to test defenses against real-world adversary behaviors.

Extended iCollector Support for Google Cloud

Gain seamless visibility across multi-cloud environments with **expanded iCollector integrations**. Centralize log collection, monitor cloud-native services**,** and detect threats **from assets deployed on Google Cloud**. Cloud activities are correlated with other data sources to provide a unified view of the **security posture, enhancing threat detection, compliance monitoring, and incident response**.

Key Benefits:

1. **Centralized Log Collection**: Collect and analyze security logs from Google Cloud deployed resources for full visibility.
2. **Enhanced Compliance Monitoring**: Centralized visibility helps ensure audit-ready reporting and simplifies compliance management across multi-cloud environments**.**
3. **Faster Incident Response**: Real-time log ingestion and analysis provides immediate insights, enabling security teams to quickly investigate and respond to emerging threats.

Important Notes

No special considerations applicable for this version.

Enhancements

Category	Enhancement	Details
Backend	Enhanced Elastic indexing performance and improved real-time search responsiveness.	Improved the performance of Elastic indexing to enhance real-time search capabilities, ensuring faster data retrieval and indexing efficiency.
Backend	Optimized initial loading of Projects with fetch-on-login implementation.	Applied fetch-on-login mechanism to optimize the initial loading of Projects, reducing wait times and improving user experience
Backend	Optimized memory usage for Sigma Template Rule Parser scheduled tasks.	Enhanced memory management for scheduled tasks related to Sigma Template Rule Parser to improve overall system stability.
Backend	Converted GetAlertLogsTablenames endpoint to an asynchronous job.	Reworked the GetAlertLogsTablenames endpoint to function asynchronously, enhancing system responsiveness during data retrieval.
Backend	Added support for "one of" operator and circuit breaker functionality in Sigma Rules parser.	Extended Sigma Rules parser to include "one of" operator support and added a circuit breaker mechanism for better performance control.
Backend	Enhanced Custom Alerts to properly filter deleted log sources.	Improved Custom Alerts filtering logic to ensure deleted log sources are excluded, maintaining data accuracy.
Backend	Implemented Fortiguard Threat Intelligence filtering capabilities.	Added filtering capabilities to leverage Fortiguard Threat Intelligence, enhancing threat detection accuracy.

Backend	Improved Activation Key validation error messages.	Enhanced the clarity and detail of Activation Key validation error messages for better user guidance.
Backend	Added header parameters in Swagger documentation.	Updated Swagger documentation to include header parameters, improving API documentation completeness.
Backend	Enhanced email settings management in Portals.	Improved email settings management in Portals for greater flexibility and easier configuration.
Backend	Migrated UEBA Engine database cleaning process.	Transferred UEBA Engine's database cleaning process to a more efficient framework, improving performance and reliability.
Backend	Enhanced JSON field escaping to preserve file format integrity.	Improved JSON field handling to ensure proper escaping, preserving file structure and compatibility.
Backend	Improved Notifications Engine thread handling.	Enhanced the Notifications Engine to better manage threading, improving performance and reducing potential issues.
Backend	Enhanced ModelUtilCore Elastic bulk insert functionality.	Optimized the ModelUtilCore bulk insert process into Elastic, enhancing throughput and reducing latency.
iCollector	Implemented Dual Mode for Correlation Engine.	Developed and introduced Dual Mode functionality for Correlation Engine to enhance flexibility and processing capabilities.
iCollector	Improved error reporting for Azure AD & Office 365 authentication.	Enhanced error reporting for Azure AD and Office 365 authentication flows, providing clearer diagnostic information.
iCollector	Developed Oracle OCI iCollector functionality.	Created and integrated new Oracle OCI iCollector functionality for expanded data collection support.

iCollector	Enhanced Sophos Central API integration.	Improved the integration with Sophos Central API, ensuring more reliable data collection and processing.
iCollector	Resolved Oracle Cloud Infrastructure connectivity issues.	Addressed and resolved Oracle Cloud Infrastructure connectivity issues to ensure stable data ingestion.
iCollector	Enhanced CTI integration requests with detailed application logs.	Improved CTI integration requests to log detailed application-level information for better troubleshooting.
iCollector	Enhanced database synchronization logging to reduce Collector Logs volume.	Optimized logging in database synchronization processes to reduce unnecessary Collector Logs volume.
iCollector	Implemented server worker for iCollector table synchronization.	Added a dedicated server worker to handle iCollector table synchronization processes for improved performance.
iCollector	Updated iCollector Management Network Scripts.	Revised and updated network management scripts used by iCollector for better compatibility and automation.
UI/UX	Searchable sidebar for SWP.	Added a sidebar with search functionality in SWP, allowing for quicker navigation and improved user experience.
UI/UX	Resolved Module Alerts limitation issues.	Fixed limitations related to Module Alerts, ensuring alerts display consistently and accurately.
UI/UX	Enhanced time frame search functionality in the Incidents module.	Improved the time frame search feature in the Incidents module for more precise filtering and usability.
UI/UX	Optimized MSSP screen loading to prevent redundant refreshes.	Enhanced MSSP screen logic to avoid unnecessary refreshes, improving performance and responsiveness.
UI/UX	Refined Marketplace configuration deletion process.	Simplified and refined the process for deleting configurations within the Marketplace module.

UI/UX	Resolved SOAR inconsistencies when creating Correlation Rules based on Templates.	Addressed inconsistencies in SOAR when creating Correlation Rules using Templates, ensuring accurate rule creation.
UI/UX	Removed unused code from SOAR Management Window Pop Up.	Cleaned up unused code from the SOAR Management window popup for improved maintainability.
UI/UX	Enhanced information display in the "About" module.	Improved the content and layout of the "About" module to provide clearer product information.
UI/UX	Improved Projects date field functionality.	Enhanced date field handling within Projects, ensuring consistent date selection and display.
UI/UX	Refined Asset Discovery scheduling with improved iCollector selection.	Enhanced the Asset Discovery scheduling process with better iCollector selection logic for improved accuracy.
UI/UX	Enhanced Alerts and Reports with Correlation Rule dropdown.	Added Correlation Rule dropdown filters to Alerts and Reports for easier filtering and better visibility.

Bug fixes

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

Important Note: This release brings substantial performance, usability and effectiveness capabilities with the introduction of new vendor/product integrations.

Thank you for your continued support, insights and valuable feedback.

Appendix A: New Supported Vendor/Products

Vendor	Product	Product Category	Product Version	Log Collection Method
Forcepoint	DLP	Data Loss Prevention	10.0	Syslog
Veeam	Veeam Backup & Replication	Audit	12.1	Syslog
Nextron Systems	ASGARD Management Center	Audit	2.17.2	Syslog
Nextron Systems	ASGARD Analysis Cockpit	Audit	3.10.4	Syslog
Fortinet	FortiDeceptor	Deception	6.1	Syslog
Delinea	PAM	Access Control	2024.x	Syslog
Proofpoint	Proofpoint Email Protection	Email Gateway	8.x	Syslog
Haltdos	Haltdos ADC	Load Balancer	2.0	API
Infoblox	Infoblox	DNS	9	Syslog
Airllock Digital	Airlock Digital	Endpoint Protection	5.x	Syslog

ClearSkies™

Contact Us

Cyprus (Headquarters)

1 Lefkos Anastasiades Street,
2012 Strovolos, Nicosia

T +357 22 463600
F +357 22 463563

www.clearskies.io

OFFICES CYPRUS | GREECE | UK | KSA | ITALY