ClearSkies™ SaaS NG SIEM

Version 6.0

Incorporating the power of

Big Data Advanced Security Analytics

Nov 2019

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 v6.0

Several new features are introduced in this ClearSkies™ SaaS NG SIEM version 6.0:

"Threat Intelligence"

- Threat Anticipation

  The formula was designed to act as a filter for the different indicators being reported by the "Threat Intelligence" ServiceModule. It operates on a series of variables that were designed and engineered towards capturing the full characteristics of an indicator. Once those variables are derived, the formula evaluates the indicator and assigns it a score. The higher the score, the more important the indicator. Alert generation and incident escalation depend on the score confident level determined by the user.

"Identity & Access"

- Identity & Access

  This new ServiceModule aggregates, visualizes and monitors the statuses of thousands of user accounts, drastically improving the auditing and insider threat detection capabilities of your organization with minimal effort.

  It further integrates with and complements other ClearSkies™ SaaS NG SIEM ServiceModules, such as Advanced Security Analytics (User & Entity Behavior Analysis (UEBA)) and ClearSkies™ NG Endpoint Detection & Response (EDR) agent, for maximal insight generation. It helps to strengthen your security posture against insider threats.

  "Identity & Access" ServiceModule empowers security personnel and upper management to effortlessly spot and timely investigate the following:

  - Inactive user accounts
  - Never-logged-on user accounts
  - Soon-to-expire passwords
  - Disabled accounts
  - Accounts of attention
  - Groups by size
  - Nested groups

- Replication errors
- Operating systems' update status
- Successful and failed logins
- Which user did what from where and when
- User account clutter in need of maintenance

To experience the full capabilities of the "Identity & Access" ServiceModule, download the "Identity & Access" Configuration Guide under Tools→Downloads in the ClearSkies™ Secure Web Portal, and then proceed with the guidelines laid out.

Important note: ClearSkies™ NG Endpoint Detection & Response (EDR) Agent v6.2.0 is a prerequisite to "Identity & Access".

New Supported LogSources

Vendor	Product	Type of Collection
Dell	Dell MXL Switch	Syslog
Symantec	Symantec Data Loss Prevention	Syslog
Symantec	Symantec Endpoint Protection Manager	Syslog
Check Point	Check Point MTA	LEA Application
Microsoft	Azure Audit Logs	Syslog
Oracle	Oracle Audit Vault Database Firewall	Syslog
UNIS	UNIS System	ODBC
Cisco	Cisco Sip	Syslog
Cisco	Cisco ACi	Syslog
Aruba	Aruba WLAN Controller	Syslog
Symantec	Symantec EDR	Syslog
Alcatel	Alcatel Switch	Syslog
Cisco	Cisco Meraki Flows	Syslog
Cisco	Cisco Meraki Events	Syslog
Cisco	Cisco Meraki Security Events	Syslog
Cisco	Cisco Meraki URLs	Syslog
IBM	ISS Network Protection XGS-Self Managed - Firewall	Syslog
IBM	ISS Network Protection XGS-Self Managed - System	Syslog
F5	F5 APM	Syslog
RSA	RSA SecureID Authentication Manager (Admin Audit)	Syslog
RSA	RSA SecureID Authentication Manager (Audit Runtime)	Syslog

Cisco	Cisco Firepower Management	Syslog
Microsoft	Windows DHCP	ClearSkies NG Endpoint agent
Symantec	Symantec DLP Suite System	Syslog
Oracle	Glassfish Web Server	Syslog