Release Note
GCenter Version 2.5.3.103

Note version: V1

Translated from original manual version 1

Creation date: January, 2025

Last update: January, 2025

Table of contents

Chapter 1

Presentation of GCenter version 2.5.3.103

This release note provides a description of:

- New features and improvements
- Patches
- Known issues
- Software compatibility
- Hardware compatibility
- Hotfixes
- Upgrade procedure

Chapter 2

New features and improvements

2.1 Detection engines and features

2.1.1 DGA detection engine

A new version of our Domain Generated Algorithm (DGA) detection engine is available featuring:

- An optimized algorithm to reduce false positives
- The possibility of managing the motor sensitivity with six different levels
- A system that helps the analysts to configure the list of domains to be ignored

---

2.1.2 Malcore detection engine

A new version of the Malcore engine is available, improving its performance and stability.

2.1.3 Beacon detect detection engine

A command and control (C&C) infrastructure tag detection engine is now available to detect encrypted communications between an infected host and a C&C server.
A system is available to help the analysts configure the list of IP addresses to be ignored.

2.1.4 Ransomware detect detection engine

A ransomware detection engine is now available to detect the activities of this type of malware over the SMB protocol.
It is possible to:

- Manage the motor sensitivity with six different levels
- Investigate on the basis of an SMB session identifier
- Add IP addresses to a whitelist

2.1.5 GScan detection engine

The GScan engine's interface has been enhanced to provide more details on the files analyzed on demand.

2.1.6 Auto-threshold feature

A new `auto-threshold` feature is available to limit the number of alerts generated by the Sigflow engine.
This feature is based on threshold rules that will be directly applied to the Sigflow engine.
An analyst will be able to use one of the seven existing configuration profiles, or configure a custom profile.

2.1.7 Multitenant feature for network variables

A new feature to improve the support for `multitenant` architectures is available for the Sigflow engine.
This feature allows you to declare:

- A variable with a different configuration per tenant
- A customized `network address` type variable
- A customized `network port` type variable

2.2 Analysts: WebUI and features

2.2.1 Home page improvement

The home page has been enhanced to quickly display the important information for analysts and administrators.

2.2.2 Improved alerts management

The alert management system has been enhanced to:

- Acknowledge the alerts
- Make alerts silent
- Sort the alerts according to different criteria (risk level, name, date, number of occurrences)
- Manage bulk alerts

Alerts that have been acknowledged are excluded from the risk level calculation.

2.2.3 Asset and user filtering

In the search bar, it is now possible to filter assets and users by risk level (`risk_min` and `risk_max`).

2.2.4 Malcore menu

A new interface is available for managing the Malcore engine.
Two options have been added to ignore the alerts based on a file name or those generated by a specific engine.

2.2.5 Powershell and Shellcode detect menu

A new interface is available for managing the Powershell engine and Shellcode detect.

2.2.6 YARA menu

A new interface is available for managing the YARA rules.

2.2.7 Active CTI menu

A new interface is available for managing the CTI.

2.2.8 Sigflow manager menu

The `generate rule file` button has been replaced by a `save` button in the top right-hand corner of the ruleset configuration menu, to save the changes made to the policy applied to the Sigflow engine.

2.3 Administration: WebUI and features

2.3.1 New notification system

A new notification system in the `Health` menu is available to warn the users of malfunctions in certain components of the solution.
A notification can be triggered in many situations:

- Engine update problems
- Configuration problems
- Connection problems between the GCap and the GCenter
- Compatibility problems
- Performance problems

These notifications can be silenced or acknowledged.

2.3.2 History of administrative actions

A new feature has been developed to log user actions.
The events generated can be exported to a Syslog server.

2.3.3 Standardized the event format

A new event format, ECS (Elastic Common Schema), is available for the alerts, metadata and administration events.
A compatibility mode exists for the data export, allowing you to keep the old format, which will be deleted in the next major release.

2.3.4 Improved data export

The data export feature now allows :

- Filter alerts by engine
- Export system events

2.3.5 GCap pairing menu

A new interface is available for managing the pairing of GCap with GCenter.
A help menu has been added to facilitate configuration.

2.3.6 Software update menu

A new interface is available for managing system updates.

2.3.7 Threat DB update menu

A new interface is now available for managing detection engine updates.
Several options have been added:

- Manage the frequency of GCap updates
- The ability to download updates in several parts
- The option of using a local HTTPS server

2.3.8 Retention policy menu

A new interface is available for managing the retention of data stored in Elastic Search.
It is now possible to manage the space allocated for the alerts, metadata and administration events.

2.3.9 Network settings menu

A new interface is available for viewing the network configuration parameters.

2.3.10 Licensing menu

A new interface is now available for the license management.

2.3.11 Diagnostics menu

A new interface is available for generating system logs and tech support.

2.4 WebUI – Kibana dashboards

2.4.1 Improvements of the existing dashboards

The existing dashboards have been restructured to improve the visibility and facilitate the investigation.

2.4.2 New Beacon detect dashboard

A new dashboard is available for viewing the events from the Beacon detect engine.

2.4.3 New Ransomware detect dashboard

A new dashboard is available for viewing the events from the Ransomware detect engine.

2.4.4 New Relations dashboard

A dashboard showing the relationships between the various IP addresses in the solution is available in the `Hunting > Network Metadata > Relations` menu.

2.4.5 New Administration dashboard

A new dashboard is available for viewing the administration events.

2.5 System

2.5.1 Update of the operating system

The operating system was updated to the latest Long-Term Support (LTS) version.

2.5.2 Update of the kernel

The operating system kernel was updated to the latest Long-Term Support (LTS) version.

2.5.3 Update of the components

The various operating system components have been updated.

2.5.4 Virtualization

GCenter is officially supported on VMware ESXi hypervisors.

2.5.5 ECDSA certificates

The ECDSA certificates are supported to secure the access to the GCenter web interface.

2.5.6 GCenter configuration tool

The GCenter configuration tool has been enhanced to facilitate the network setup and to add SSH keys to the "setup" user.

2.6 Other improvements

2.6.1 Contextual help

A contextual help is available on the GCenter web interface.

2.6.2 Reflex Interoperability

A new menu is available to interconnect with the Reflex solution.

2.6.3 API improvement

New API points have been added to automate certain actions.

2.6.4 PCI-DSS compliance

A new option has been added to replace the credit card numbers with a specific keyword.

2.6.5 LDAP authentication

When connecting using an LDAP server for authentication, if the account used is present in the GCenter's local database, it is deactivated to avoid conflicts.

2.7 Other changes

2.7.1 Renaming `active-hunt` in `active-cti`

The classtype of suricata rules generated by active CTI is renamed to `active-cti`.

2.7.2 Interoperability withdrawal

Interconnections with the following solutions have been removed:

- Intelligence
- Hurukai

2.7.3 IDMEF format

The IDMEF format is no longer supported when exporting events to a Syslog server.

Chapter 3

Patches

Section intentionally left blank

Chapter 4

Known problems and limitations

4.1 Active-CTI / RetroHunt - Post-update problem

In some cases, Active-CTI and RetroHunt (available with the LIS license) may not work optimally.

Workaround: contact the Gatewatcher technical support.

4.2 GCenter Backup/Restore - Error management

If the user has made a mistake while applying the restore procedure, the menu progress bar (`Admin-Backup/Restore - Backup operations` screen) remains blocked and no error message is visible in the WebUI.

Workaround: no solution.

4.3 GCenter Backup/Restore - Pairing the GCap

Following a GCenter backup, if the GCap pairing is deleted, then restoring the backup will not enable restoring the connection with the previously deleted GCap.

Workaround: reapply the pairing.

4.4 Incorrect GCap status after updating the GCenter

The status of the GCap may be erroneous following the GCenter update (Last update = unknown / Status: Online but update outdated)

Workaround: reapply the ruleset configuration at the GCap level.

4.5 Sigflow Manager - Transform Category

Applying a Transform category raises a 500 error if no ruleset is available on GCenter.

Workaround: create a ruleset.

4.6 Sigflow Manager - Error 500 when adding a rule to a custom source

Adding a rule raises a 500 error if the following conditions are present:

- The rule is added by editing a custom source
- The rule already exists in another custom source (same SID)

Workaround: change the rule's SID that is to be added in order to avoid the SID conflict.

4.7 Sigflow Manager - Inconsistency in the display of the number of categories and rules of a category

The `Sigflow > Sources` homepage shows the number of categories and rules contained in each source.
It is possible that the information displayed is inconsistent with the sources' actual content.
This situation may occur after editing a custom source or an update.

Workaround: no workaround.

4.8 Sigflow configuration - custom source name cannot contain space

In the `Config - Sigflow/sources` screen of the legacy web UI, it is possible to define a custom source of signatures for the Sigflow detection engine.
During the addition procedure, the source name must be entered.
This name must not contain any space otherwise it will generate an error.

Workaround: change name by removing the spaces.

4.9 GCenter Backup/Restore - error with FQDN

In v2.5.3.103, when restoring a backup, if the FQDN of the target GCenter is different then an error occurs.

Workaround: need to change the target GCenter FQDN and restart.

4.10 Kibana - Error code 500 after the modification of the storage media for ES data

Following the change of ES data storage media, a temporary 500 error may appear when accessing Kibana.

Workaround: wait few minutes.

Chapter 5

Software compatibility

5.1 Compatibility with the GCap

GCenter version	GCap version	Compatibility
2.5.3.103	2.5.3.105	Unsupported configuration: GCap is to be migrated in advance of the GCenter update
2.5.3.103	2.5.4.0 (or +)	Configuration ok

Chapter 6

Hardware compatibility

The version 2.5.3.103 is compatible with every hardware version of the GCenter.

GCENTER Reference	Local storage	Other storage	Interface network	Power supply
GCENT8100r2	2 x 960GB RAID1	2 x 2 TB RAID1	4 x RJ45	2 x 750W
GCENT9100r2	4 x 480GB RAID5	2 x 2 TB RAID1	4 x RJ45	2 x 750W
GCENT9900r2	10 x 480GB RAID5	4 x 2 TB RAID5	4 x RJ45	2 x 1100W
GCENT10500r2	12 x 480GB RAID5	4 x 2 TB RAID5	4 x RJ45	2 x 1100W

Chapter 7

Hotfix

Section intentionally left blank

Chapter 8

V102 to V103 upgrade procedure

8.1 Prerequisites

To install the **V2.5.3.103** update:

- The GCenter must be running **V2.5.3.102-HF3** or higher
- The GCap will need to be version **V2.5.4.0** or higher
- If you have any questions about these items, please contact the Gatewatcher Technical Support

Important:

It is highly recommended to have an iDRAC type connection in order to be able to connect post-upgrade if a problem occurs during the process. Otherwise, you'll need a physical access to the equipment (screen, keyboard).

Important:

Before proceeding with the update, it is strongly recommended to backup the GCenter configuration in the `Administrators > Backup / Restore > Operations` menu and save the file to an external server in a directory indicating the current GCenter version (example: 2.5.3.102-XXXX-HFX).

8.2 Retained data

All the GCenter configuration and data are retained.

8.3 Installation procedure with data retention

1. Make sure the GCap probes are in version **V2.5.4.0** or higher, otherwise refer to the following update procedure: https://releases.gatewatcher.com/en/gcap/2.5.4/V0/8_upgrade_procedure.html
2. Download the newly available version of the GCenter and the associated sha256 on the https://update.gatewatcher.com/upgrade/ platform (directory 2.5.3.103).
3. Check the image with the associated sha256.
4. Connect to the GCenter WebUI and go to the menu `Admin > GUM > Software update`.

5. In the `Uploading a new software update` section, click on the `Click to upload` button, select the new GCenter version previously uploaded and click `Submit`.
6. Connect to the GCap with the SSH account **setup**.
7. Shut down the monitoring engine with the following command: `monitoring-engine stop`.
8. Change the compatibility mode using the following command: `set compatibility-mode 2.5.3.103`.
9. Start the monitoring engine with the following command: `monitoring-engine start`.
10. In the `Saved package list` section, at the location of the previously sent update, click on the `Apply` button.
11. Once the operation is complete, restart the GCenter by connecting via SSH with the **setup** account and then going to the `Restart` menu.
12. Once the GCenter is restarted, connect to the WebUI and check whether new events appear in the `Hunting` section (Kibana interface).

`PDF Release Note`