Sangfor Cyber Command

Release Note

Product Version	3.0.60
Document Version	01
Released on	May. 11, 2022

Disclaimer

Products, services or features described in this document, whether wholly or in part, may be not within your purchase scope or usage scope. The products, services or features you purchase must be subject to the commercial contract and terms as agreed by you and Sangfor. Unless otherwise provided in the contract, Sangfor disclaims warranties of any kind, either express or implied, for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Unless otherwise agreed, this document is used for reference only, and all statements, information, and recommendations therein do not constitute any express or implied warranties.

Technical Support

For technical support, please visit: https://www.sangfor.com/en/about-us/contact-us/technical-support

Send information about errors or any product related problem to tech.support@sangfor.com.

About This Document

This document describes the Release Notes of Sangfor Cyber Command(CCOM) version 3.0.6.0.

Intended Audience

This document is intended for:

- Network design engineers
- O&M personnel

Note Icons

English Icon	Description
	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
	Indicates a hazardous situation, which if not avoided, could result in minor or moderate injury.
	Indicates a hazardous situation, which if not avoided, could result in settings failing to take effect, equipment damage, or data loss. NOTICE addresses practices not related to personal injury.
	Calls attention to important information, best practices, and tips. NOTE addresses information not related to personal injury or equipment damage.

Change Log

Date	Change Description
May. 11, 2022	This is the first release of this document.

Contents

1 New Features and Enhancements

1. **[New]** ATT&CK capability:

- Enhance traffic detection to cover all techniques.
- Allow displaying the asset that hits an attack technique on the ATT&CK Capabilities page.

2. **[New]** SNMP agent:

- Allow sending device information to the SNMP manager via SNMP v1/v2/v3.

3. **[New]** SOAR functionality:

- Implement the built-in version of SOAR 3.1 to fix some issues and improve usability.
- Allow testing connectivity while adding an integrated device.

4. **[Enhanced]** User experience of the Detection module.
5. **[Enhanced]** User experience of the GoldenEye module.
6. **[Enhanced]** Response module.
7. **[Enhanced]** Security event generation.
8. **[Enhanced]** Security detection.
9. **[Enhanced]** Asset identification capability.
10. **[Enhanced]** Loading speed:

- Optimize the underlying architecture to improve the loading speed of the Response module.
- Fix issues to enhance user experience.

11. **[Enhanced]** Update method:

- Allow obtaining update packages and SPs online.

12. **[Enhanced]** Threats module reconstruction.

2 Resolved Issues

[**Fixed**] Fixed some known issues with lower versions.

3 Upgrade Instruction

3.1 Confirmation Before Upgrade

CCOM3.0.60 support upgrade from the following earlier versions:

Cyber Command 3.0.50.

3.2 Update Limitations

Hardware:

1. Memory: None.
2. Disk: None.
3. Disk size: Directory /stmp/ is not smaller than 200 MB.
4. CPU: None.

Software:

Dependent on specific packages:

No**. Immediate Upgrade of Configurations, Logs, and Data.**

Yes. **Impacts on Functions After Upgrade:**

Step 1. SSH process function is disabled by default. However, it can be enabled manually and will be disabled automatically 8 hours later.

Step 2. Firmware Updater is disabled by default. However, if an upgrade is required, it can be enabled together with SSH and will be disabled automatically 8 hours later.

Reboot Required After Upgrade:

Yes.

Time Taken:

30 minutes.

3.3 Upgrade Procedure

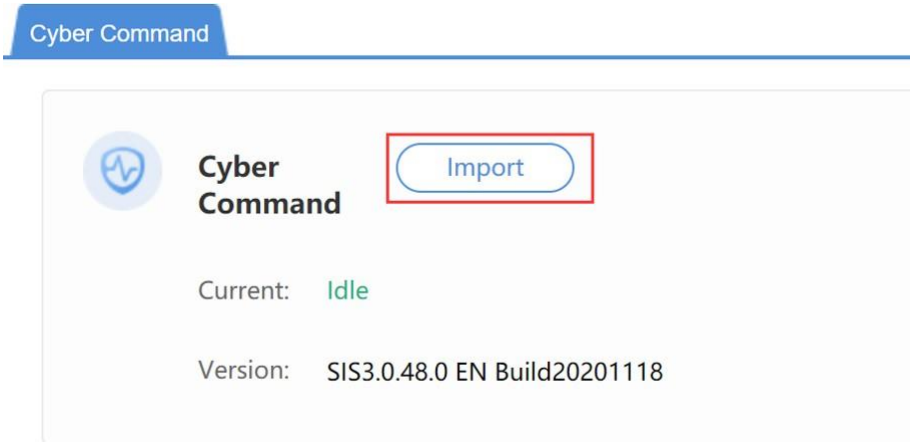
Follow the steps below If you are upgrading from Cyber Command Version 3.0.60c

Before Upgrade:

Step 1. Check the MD5 values of all update packages to ensure they are the same as those in the attachments.

Step 2. Check whether the device has been upgraded to 3.0.50 version.

Step 3. Go to **System** > **Update** > **Cyber Command** and click Import to import the .ssu package.



Step 4. Wait for 30 minutes and log in again. If the version number has changed to 3.0.60, the update is successful.

3.4 Handling of Upgrade Failure

If the upgrade is failed, please get in touch with technical support in time.

4 Precautions

1. A downgrade is not supported.
2. Starting from CCOM 3.0.60, only the bin file upgrade package is supported.
3. The minimum requirement upgrade to CC 3.0.60 required a minimum CC 3.0.50 version, please upgrade to 3.0.50 first if the CCOM firmware is lower than 3.0.50 version.
4. The CC upgrade can only be done via Web Console and Sangfor Updater is not supported because the upgrade file is large.
5. Do not load the upgrade package in the public network during the upgrade. Instead, it is recommended to use an internal PC to upgrade devices.
6. During the upgrade, avoid manual device restart and accidental power failure.
7. Contact customer service if any problems occur during the upgrade, and do not manually restart the device.

SANGFOR