Release announcement - ESET Connect 2.13

2025-01-23 - Steef | ESET Nederland - Comments (0) - Feature release

Changelog:

•IMPROVED: Infrastructure & security.

•ADDED: Additional Syslog outgoing IP addresses for EU, US, JPN, CA & DE regions.

We are reaching out with important updates regarding Syslog Export functionality and event severity classification for ESET PROTECT & ESET Inspect (cloud versions).

1. **Firewall Configuration for Syslog Server**

To ensure uninterrupted Syslog Export functionality, please configure your Syslog server's firewall to allow incoming Syslog Export events only from the updated IP ranges. These changes will take effect on **February 25th, 2025**.

For the latest information, please visit our support page: Syslog Security restrictions and limits.

2. **Event Severity Classification in LEEF Format**

As per the official IBM documentation (Predefined LEEF Event Attributes):

- 1 represents the lowest event severity.
- 10 represents the highest event severity.Hardware inventory for all platforms

Please note that ESET's implementation of event severity in LEEF format was previously inverted. To align with the standard, we kindly request you to adapt your configurations accordingly for proper functionality. If you have any questions or need further assistance, please do not hesitate to contact our support team.