

Title (en)

INTRUSION FILTER FOR AN INTRUSION DETECTION SYSTEM

Title (de)

INTRUSIONSFILTER FÜR EIN INTRUSIONSERKENNUNGSSYSTEM

Title (fr)

FILTRE ANTI-INTRUSION POUR UN SYSTÈME DE DÉTECTION D'INTRUSION

Publication

EP 4237975 A1 20230906 (EN)

Application

EP 20835841 A 20201222

Priority

EP 2020087720 W 20201222

Abstract (en)

[origin: WO2022135706A1] Embodiments of the invention relate to an intrusion filter (100) for Detection Prevention Systems (DPS) and Intrusion Detection Prevention Systems (IDPS). Embodiments of the invention also relate to a detection subsystem (300) and a collection and investigation system (400) comprising such an intrusion filter. The intrusion filter filters anomaly indications such that an anomaly indication identified as a false positive anomaly indication is discarded. Otherwise, the anomaly indication will be provided to a collection and investigation system (400) for further processing. Thereby, e.g. reduced computational load on the system is achieved. Furthermore, embodiments of the invention also relate to corresponding methods and a computer program.

IPC 8 full level

G06F 21/55 (2013.01); **H04L 9/40** (2022.01)

CPC (source: EP)

G06F 21/55 (2013.01); **H04L 63/1416** (2013.01)

Citation (search report)

See references of WO 2022135706A1

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

Designated extension state (EPC)

BA ME

Designated validation state (EPC)

KH MA MD TN

DOCDB simple family (publication)

WO 2022135706 A1 20220630; CN 116671066 A 20230829; EP 4237975 A1 20230906

DOCDB simple family (application)

EP 2020087720 W 20201222; CN 202080107762 A 20201222; EP 20835841 A 20201222