US 20230231777A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2023/0231777 A1**

McGrew et al. (43) **Pub. Date: Jul. 20, 2023**

(54) **AUTOMATICALLY DETECTING AUTHORIZED REMOTE ADMINISTRATION SESSIONS IN A NETWORK MONITORING SYSTEM**

(71) Applicant: **Cisco Technology, Inc.**, San Jose, CA (US)

(72) Inventors: **David McGrew**, Poolesville, MD (US); **Martin Rehak**, Prague 5 (CZ); **Blake Harrell Anderson**, Chapel Hill, NC (US); **Sunil Amin**, Atlanta, GA (US)

(21) Appl. No.: **18/125,955**

(22) Filed: **Mar. 24, 2023**

Related U.S. Application Data

(63) Continuation of application No. 17/376,924, filed on Jul. 15, 2021, now Pat. No. 11,632,309, which is a continuation of application No. 15/848,101, filed on Dec. 20, 2017, now Pat. No. 11,075,820.

Publication Classification

(51) **Int. Cl.**

H04L 41/28	(2006.01)
H04L 9/40	(2006.01)
H04W 12/12	(2006.01)
G06F 21/55	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 41/28*** (2013.01); ***H04L 63/1425*** (2013.01); ***H04L 63/1441*** (2013.01); ***H04W 12/12*** (2013.01); ***G06F 21/55*** (2013.01); ***H04L 63/14*** (2013.01); *H04L 67/143* (2013.01)

(57) **ABSTRACT**

In one embodiment, a service receives administration traffic data in a network associated with a remote administration session in which a control device remotely administers a client device. The service analyzes the administration traffic data to determine whether any portion of the administration traffic data is resulting from an administration session involving a trusted administrator. The service flags a first portion of the administration traffic data as authorized when the first portion of the administration traffic data is determined to result from an administration session involving a trusted administrator, and a second portion of the administration traffic data is non-flagged. The service assesses the second portion of the administration traffic data using a machine learning-based traffic classifier to determine whether the second portion of the administration traffic data is malicious.