US 20240214348A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2024/0214348 A1**

Benameur et al. (43) **Pub. Date: Jun. 27, 2024**

(54) **APPLICATION PROGRAMMING INTERFACE (API) SECURITY**

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

(72) Inventors: **Azzedine Benameur**, Fairfax, VA (US); **Yun Shen**, Bristol (GB)

(73) Assignee: **NetApp, Inc.**, San Jose, CA (US)

(21) Appl. No.: **18/303,359**

(22) Filed: **Apr. 19, 2023**

Related U.S. Application Data

(60) Provisional application No. 63/477,105, filed on Dec. 23, 2022.

Publication Classification

(51) **Int. Cl.**

H04L 9/40 (2006.01)

G06F 9/54 (2006.01)

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

CPC ***H04L 63/0236*** (2013.01); ***G06F 9/547*** (2013.01); ***H04L 63/1425*** (2013.01)

(57) **ABSTRACT**

Systems and methods for enhancing API security by identifying anomalous activities in a cloud environment are provided. In one embodiment, the lack of awareness of an external API with respect to how calls to the external API may affect a cluster of a container orchestration platform is addressed. For instance, the views of the external and internal APIs may be combined to achieve better API security by correlating external API calls with undesirable behavior or other anomalies arising in the internal API. Responsive to identifying such undesirable behavior, information (e.g., a host, a source IP, a user, a specific payload) associated with the offending external API call may be added to a network security feature (e.g., a deny list, an IPS, or a WAF) utilized by the external API to facilitate performance of enhanced filtering of subsequent external API calls by the external API on behalf of the internal API.