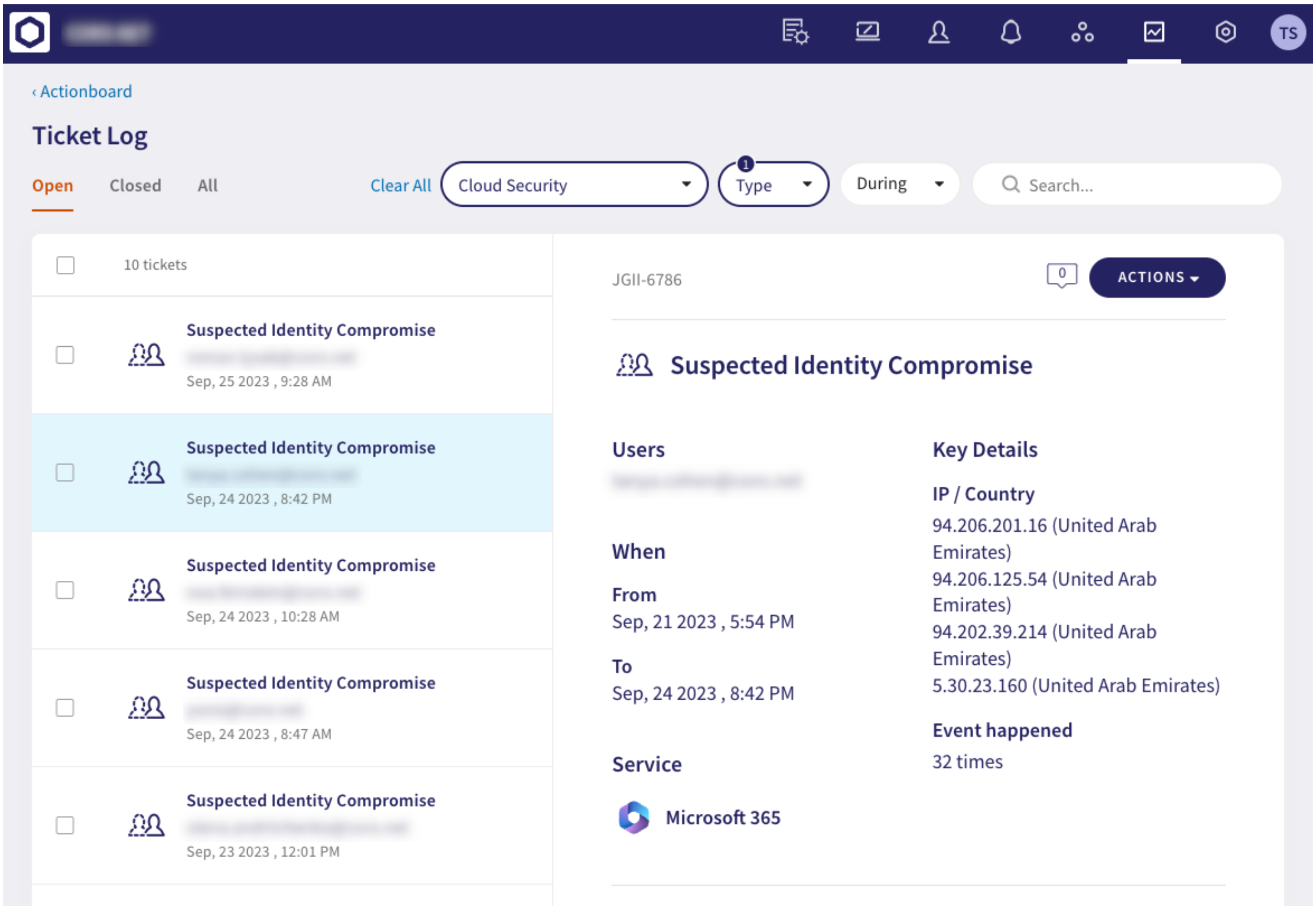
# Suspected identity compromise

**Suspected Identity Compromise** tickets report instances of potential user account breaches and abnormal admin activity, focusing on actions that pose a significant threat to customer data.

These tickets present key details of the event, including the access point location and descriptions of the specific activities deemed suspicious:



Ticket Log

□ 10 tickets

□ Suspected Identity Compromise
[redacted]
Sep, 25 2023 , 9:28 AM

□ Suspected Identity Compromise
[redacted]
Sep, 24 2023 , 8:42 PM

□ Suspected Identity Compromise
[redacted]
Sep, 24 2023 , 10:28 AM

□ Suspected Identity Compromise
[redacted]
Sep, 24 2023 , 8:47 AM

□ Suspected Identity Compromise
[redacted]
Sep, 23 2023 , 12:01 PM

JGII-6786

Suspected Identity Compromise

Users
[redacted]

When

From
Sep, 21 2023 , 5:54 PM

To
Sep, 24 2023 , 8:42 PM

Service
Microsoft 365

Key Details

IP / Country
94.206.201.16 (United Arab Emirates)
94.206.125.54 (United Arab Emirates)
94.202.39.214 (United Arab Emirates)
5.30.23.160 (United Arab Emirates)

Event happened
32 times

> **Note**
>
> **Suspected Identity Compromise** tickets are classified as suggested for review, and are automatically closed after a review period of two weeks.

The **Full Details** section provides references to normative actions taken in close proximity to suspected activities. The suspected activities use a red indicator, while the presumably normative activities use a green indicator. In the example