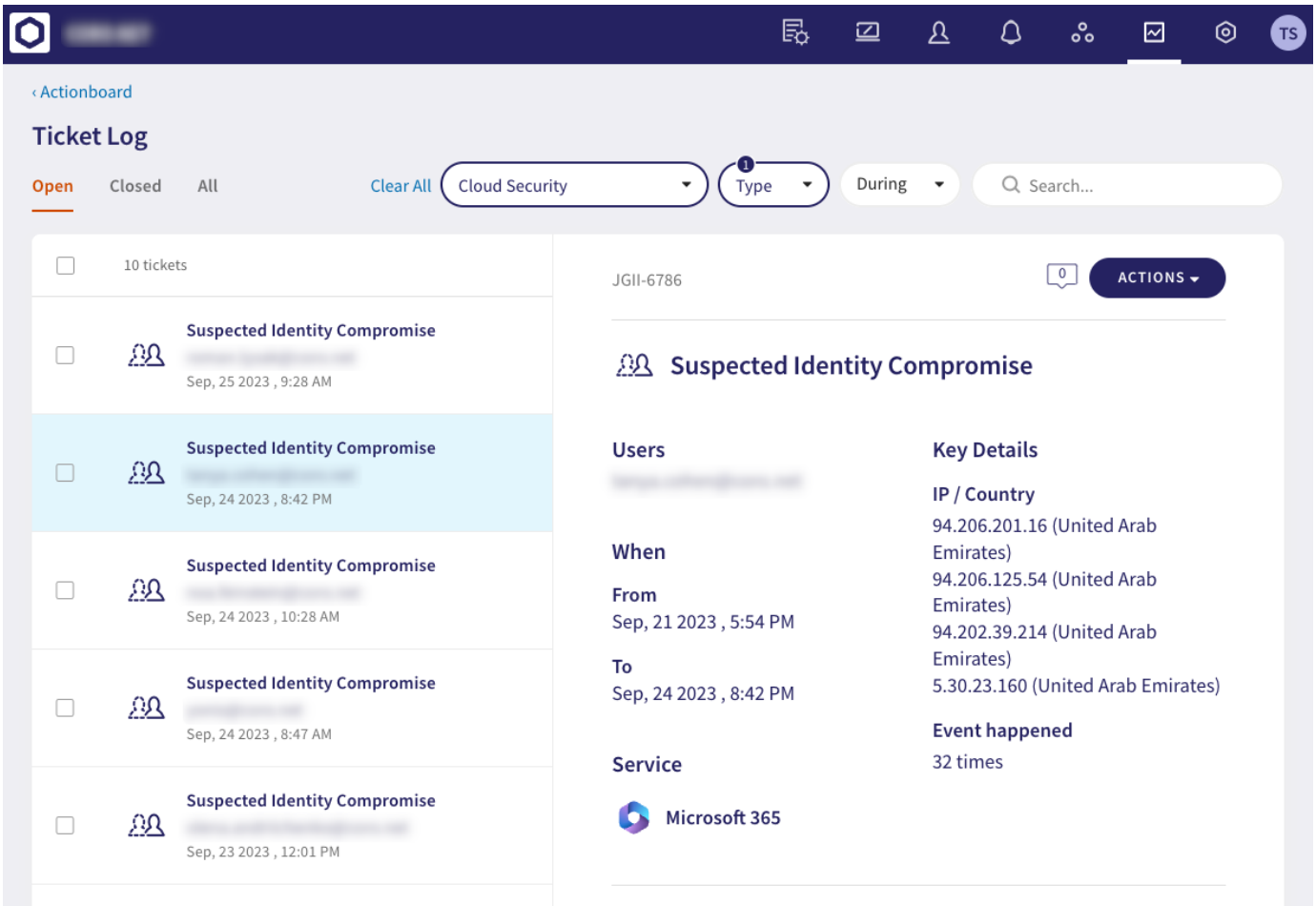
Suspected identity compromise

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:



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