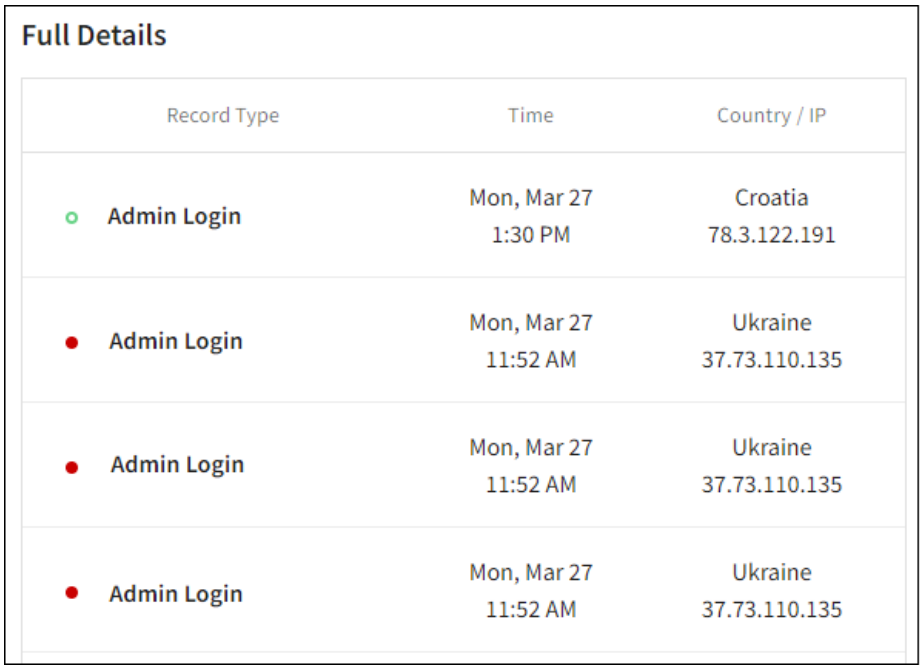
Abnormal admin activity

The **Full Details** section for **Abnormal Admin Activity** tickets is similar to that of **Suspected Identity Compromise** tickets.

Coro displays a log of admin activity, listing the time and location for each event. Suspected activities are indicated in red, while typical activities are in green. In the example below, an "Admin Login" is marked suspicious because it occurred from different IP addresses within a short time span.



Coro detects suspected identity compromise for both regular and Admin user accounts by analyzing data from all customers, specific customers, and specific users behind a ticket. Coro then creates normative behavior models from which anomalies can be detected. These models range from simple statistical anomaly models to more complex models that cross-correlate data from various sensors throughout the system, uncovering evidence of abnormal behavior.

Note

Abnormal Admin Activity tickets are classified as suggested for review and are automatically closed after a review period of four weeks.