Tickets in Coro

Tickets play a central role in Coro. They serve as records for detected events or a series of events where Coro identifies suspicious behavior.

For example, if you set up Coro to protect users against email phishing attacks, a ticket is generated each time a phishing attempt is detected.

The detection process is based on three principles:

Workspace settings detection

- Admin users define the expected behavior of users and devices in the organization. For example, enabling firewall features on endpoint devices or restricting access to Microsoft 365 accounts from outside a specific country.
- These detections are predefined based on the configuration set by Admin users in the Coro console.

Best practice detection

- Coro follows industry best practices for deletion, modification, and remediation. For example, it verifies the authenticity of email servers used for specific domains.
- It also detects malware fingerprints based on best practices, even if not explicitly specified by an admin user.

Data driven detection

- Coro employs adaptive data-driven or artificial intelligence (AI) driven decisions for detection, alerting, and remediation. For example, text classification for email phishing detection or anomaly analysis for identifying suspicious access to cloud app accounts.