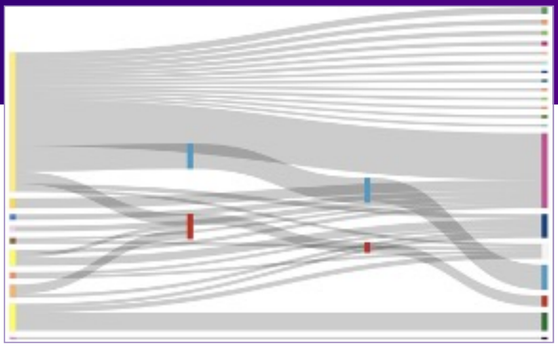
HUMAN

Preventing Inventory Sniping and Content Scraping

HUMAN helps boutique Hospitality Chain identify Account Takeover fraud designed to snipe inventory in lucrative destinations and scrape exclusive member prices.

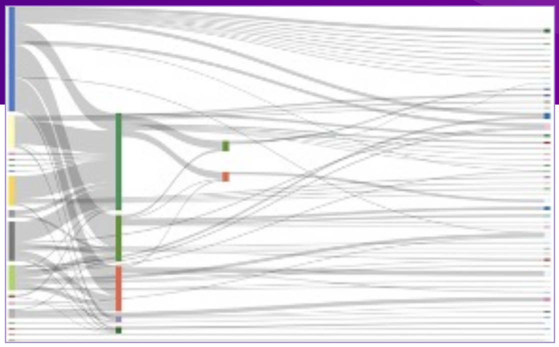
DATA CONTAMINATION FROM AUTOMATED FRAUD

SUSPICIOUS



Automated traffic patterns typically demonstrate more clustered user flow, identifying key areas of potential fraud. When unchecked, fake traffic contaminates real data and result in non-trivial infrastructure costs.

HUMAN



Human traffic patterns typically demonstrate diverse user flow. Clean data can be used to optimize site for profitability, measuring critical business metrics, and more.

Findings:

- **Security Risk:** 14% of traffic to the login page was fraudulent, attempting to login to the reservation system.
- **Threat Insights**: Once logged in, the bots were navigating to specific high-value hotels and attempting to complete a booking.
- **Content Scraping**: Exclusive member rates were being scraped for potentially competitive/predatory pricing.

Without the HUMAN verification platform, **~80% of Account Takeover Logins are successful.**

Threat Category		Total Events
BOT - BOT	Sophisticated Bot	15%
NSD - ANO_DEV	Anomalous Device	7%
NSD - ANO_USR	Anonymized User	3%
BOT - ENT_BVR	Abnormal Entity Behavior	2%

Deploy a **single line of code** and know who’s real.