CUSTOMER STORY

imply

Superhuman Capabilities: HUMAN expedites bot detections and investigations by 10X

About HUMAN

The Internet is flooded with automated traffic from sources such as search engines, virtual assistants, and chatbots. This traffic is both benevolent and malicious.

While basic bots simply gather publicly available data or perform necessary functions, more sophisticated bots attack vulnerable applications to steal unprotected and sensitive data. In addition, sophisticated bots can mimic human behavior. Attackers constantly create, buy, and modify bots, so bot behavior, objectives, and sophistication levels vary greatly. HUMAN's sophisticated bot management tools determine the intent of automated traffic in real-time to distinguish between good bots and bad bots.

Challenge

HUMAN developed an advanced bot detection and identification engine called - Human Verification Engine (HVE). HVE layers a variety of techniques to detect bots including ML models and statistical analysis of user behavior.
HVE makes "bot" or "not" decisions on trillions of digital events. The decisions need to be made in less than 12 milliseconds. HVE makes more than 10 trillion decisions per week.

HUMAN analysts maintain oversight on the new and evolving threats by carefully selecting a subset of traffic data to manually analyze and incorporate the learnings to the HVE engine.

HUMAN needed a database and visualization layer which can ingest and visualize the data at a massive scale without being cost-prohibitive. Another key requirement was to use a solution that did not require analysts to write complex SQL queries.

Before Imply, analysts would either write complex Snowflake queries or run automated pre-written Jupyter notebooks to query and analyze the data. The data analysis was slow and required a learning curve to surface the insights from underlying data.

Solution

Imply forms the first line of defense for HUMAN to keep its customers secure.

HUMAN

HUMAN is a cybersecurity company that protects applications, APIs, and digital media from bot attacks, preventing losses and improving the digital experience for real humans.

Challenge

The bot detection team needed a scalable database and sub-second latency visualization layer to perform ad-hoc data analysis to identify new and sophisticated bot attacks.

Solution

Imply is used by the detection team performing investigations and identifying new botnets and recent attacks.

Highlights

- Increased investigation efficiency by up to 10X
- Enhanced reporting and analysis on new attacks
- Improved customer experiences

Analysts use Imply Pivot for Threat Research & Investigations:

Analysts built dashboards in Imply Pivot to look at different interesting signals or characteristics to evaluate a subset of the traffic and make decisions if the traffic is from the “bot” or “not”. These characteristic patterns are then fed into the detection team’s library of known bots to detect those or similar attacks automatically in the future.

DataOps & Solution Architects use Imply to identify anomalies and share insights behind those anomalies with customers:

- **Improved Investigations:** Solution architects can see an interesting signal and dig deep into the signal and all of the associated data.
- **Enhanced Reporting & Analysis:** DataOps now not only discovers attacks, traffic spikes, and the reasons behind them but also shares this visual analysis with other team members for reporting which was not possible before.
- **Better Customer Experience:** The Data Ops team can answer customer questions quicker than ever before.

Customer Quote

“Imply helps me make decisions 10X faster. It’s been a game-changer because we are making decisions way quicker in terms of our investigations.”

- Marion, Senior Data Ops, Mobile Traffic

“The whole idea of dragging and dropping something, and then immediately seeing the answer in a visual format that is stimulating to the user and allows deeper questions to be asked quickly—that’s the advantage.”

- H, Senior Software Engineer, DAIT (Detection, Analysis and Investigation Tools)

Ready. Set. Go.

HUMAN now ingests three months’ worth of data from Snowflake to Imply to make data available for ad-hoc visual analysis in Imply Pivot.

Currently about 50 users use Imply regularly to perform various data analysis.

Results

Imply helps the Human analysts discover new and undetected bots at about 10X the speed of their previous solutions.

With Imply Pivot, analysts now drag and drop the dimensions on canvas to visualize the underlying massive data within milliseconds.

This has been a game changer to analysts in improving their productivity while shining light on new kinds of bot attacks or behaviors resulting in the
following key benefits:

- Investigate 10-15 new leads per week
- Complete in-depth threat research to detect and identify bots that are too sophisticated for simple detection
- Improve the core HUMAN Verification Engine by feeding the complete data analysis behind newly identified malicious bots for automated detection in future
- Build dashboards to alert on anomalous data

imply

For more information visit us at imply.io