HOW AI EVOLVES DATA INTO OPEN SOURCE INTELLIGENCE

Security teams are responsible for protecting their people, assets, and reputation by staying abreast of major events worldwide. These teams rely on publicly or commercially available information to create Open Source Intelligence (OSINT). OSINT, is the collection and analysis of data gathered from open sources, such as news, blogs, and social media to produce actionable assessments.

TOO MUCH INFORMATION

Where once there was a challenge of not enough information forcing security teams to make judgements with fragments of data, they are now bombarded with the internet's equivalent of basements full of data on any major event. The amount of information created and consumed is only increasing. Statista estimates that by 2025, creation of global data will grow to more than 180 zettabytes; more than ten times the amount produced in 2017. Having too much information is just as paralyzing as not having enough. Modern psychology finds that the human brain can only focus on so much information at a time. As we try to complete more tasks simultaneously, our ability to manage each task diminishes due to "cognitive overload." Information overload leads to less effective analysis and slower decision-making.

DISPARATE TOOLS

Initially security teams had to search for updates on major events directly on social media and news platforms; toggling between screens and constantly refreshing to find the latest information. To help security teams overcome the challenge of multiple platforms and information overload, several tools have been created. Some focus on getting all the open source information into a single searchable platform. With these tools, security teams do not need to toggle between news sites, social media, and deep and dark web forums to find the information they need. These powerful tools are able to get their users thousands of alerts on any given event. So this eliminates the problem of getting all the information about an event in a single pane of glass which helps in making comparisons across platforms. But it leads to another challenge.

NOT ENOUGH TIMELY INTELLIGENCE

What if security teams are grappling with multiple events as will most often be the case? Take the recent Russian invasion of Ukraine and the massive flooding and evacuations in Australia. Even fully staffed Global Security Operation Centers (GSOCs) don't have time to adequately manage tens of thousands of alerts. They can become overloaded, because, while the information may be in one spot, it's not organized or it's not relevant. The information is also duplicative following news cycles. It gets repeated over and over by media and social media accounts. This clutters alert feeds.

To reduce the noise from duplicative and false information, some data aggregation tools utilize human experts on the ground across the globe to verify any reporting before it gets fed into the platform. This verification process is expensive and comes at the additional cost of timeliness. With these tools security teams end up with old information about incidents that happened yesterday when they need to know what's happening now.

AI UNLOCKS THE FULL POTENTIAL OF INFORMATION

Artificial Intelligence (AI) delivers the ability to transform zettabytes of information into OSINT. AI machine learning tools are able to automate the information gathering phase and then inject the raw information into knowledge bases that cluster, curate, and organize it into specific areas of interest. These knowledge bases can be further automated to continuously analyze and self-update with new intelligence reports.

- **Cluster**: ML tools using computer vision (CV) powered image clusters can organize images and videos from across data sources. Computer vision algorithms also tag images and videos to make them searchable by security teams.
- **Curate**: AI can instantly identify and tag key people, organizations, locations, and topics discussed in a datasource. Security teams need information at their fingertips related to where they have people or assets. Advanced AI filters can automatically organize all ingested reports by the location that is mentioned or geotagged in social media.
- **Organize**: NLP engines can now organize and tag information by any number of entities of value to security teams, such as people, organizations, or locations. This allows security teams to separate the latest social media posts related to evacuation routes or infrastructure damage so they can provide updates to their employees in a warzone or dangerous natural event.

After automatically ingesting, tagging and organizing the information, advanced ML algorithms can further filter noisy alert feeds to get rid of disinformation and duplicate reports.

- **Flag disputed information**: AI tools can ingest news and social media feeds and automatically detect, flag, and display the origin and source of disputed information to help users understand its pedigree and evaluate its accuracy.
- **Deduplication**: AI tools can combine duplicate reporting and roll up same or similar information feeds into one. The advanced models can also summarize the text of the combined reports to make it easy for security teams to copy and paste information into their situation reports.

PRIMER COMMAND'S AI ENGINES EMPOWER SECURITY TEAMS

Primer Command is an AI tool that continuously screens news and social media sites for relevant updates, extracts key information—including people, locations, and organizations—using state-of-the-art AI/ML algorithms, and visualizes the results on a dashboard that updates in real-time. Command fills a critical gap in the OSINT toolkits of analysts and operators by giving them unmatched clarity into breaking events and enhanced situational awareness.

But Command can't replace the analysis done by these security teams. Instead, Command allows GSOC's to prioritize their time and focus on the most critical information to help ensure the security of their people and assets. Command, when paired with security teams, turns the challenge of large volumes of data into an advantage by transforming it

Contact us
to learn more

publicsector@primer.ai