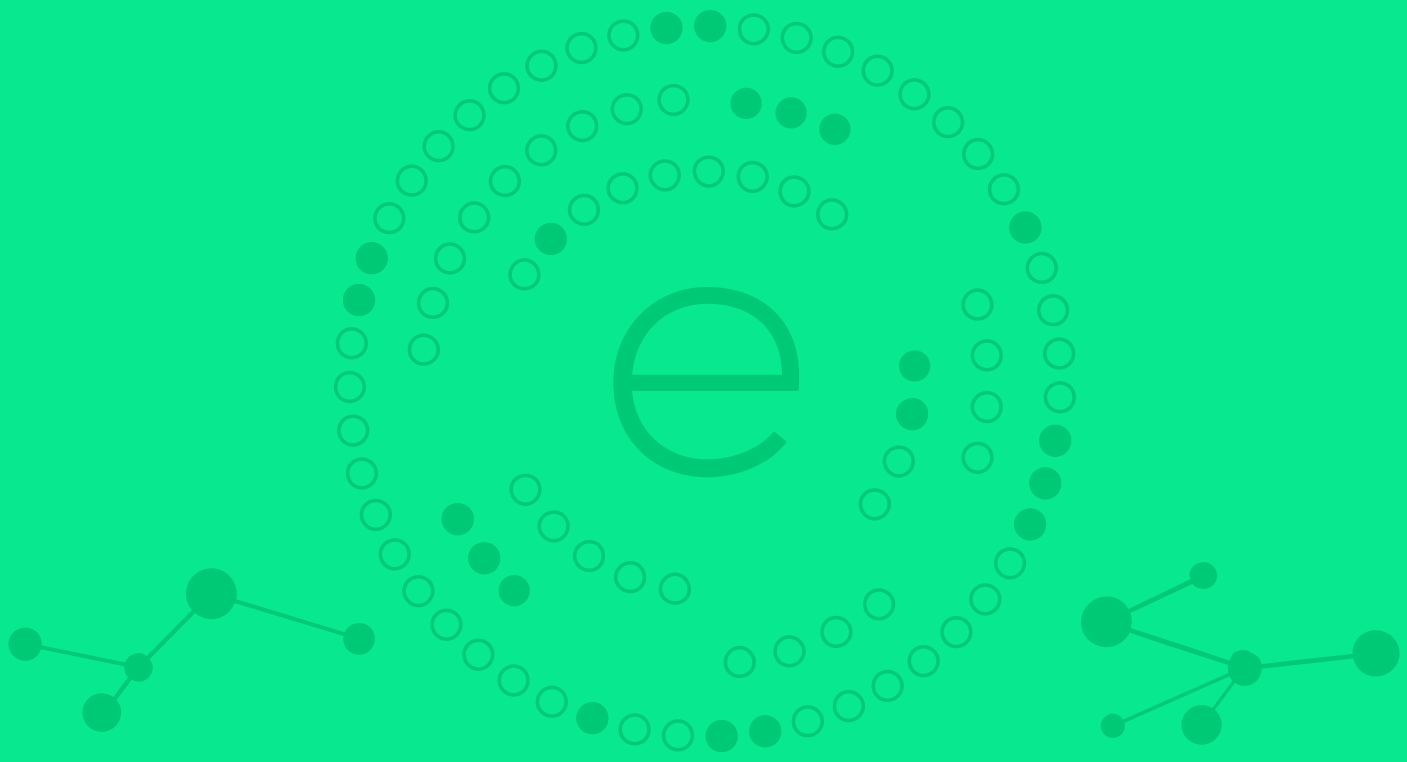
empow

You have it in you.

Artificial Intelligence White Paper



Harnessing the human-like ability to perceive, learn, interact & take action

empow's AI powered SIEM solution autonomously understands the intent behind each piece of data that the existing network infrastructure generates, no matter the data source, and knows to identify if these pieces form or can potentially form a real attack "story" against the organization.

empow's AI is based on machine learning Natural Language Processing (NLP) classifiers. Because the content within the huge number of logs and messages that the network and security tools generate can be described as natural language data, it makes it possible to produce trained NLP classifiers that know how to read and understand the content of these messages, no matter what the source, without human intervention.

By doing so, our AI instantly categorizes the huge amount of data into a significantly smaller number of security behavior classes (such as MITRE ATT&CK™ behavior categories). It then knows how to identify cause-and-effect correlations [between the classes] that represent real development of attack and should be prioritized, vs. the overall noise and false positive alerts that should be ignored.

While other SIEM systems require security teams to maintain thousands of static rules, which is a very expensive and reactive approach to cybersecurity, empow's AI engine enables our SIEM platform to detect attacks that are missed by the point solutions (silos), without the need to configure and maintain security alerts and correlation rules.

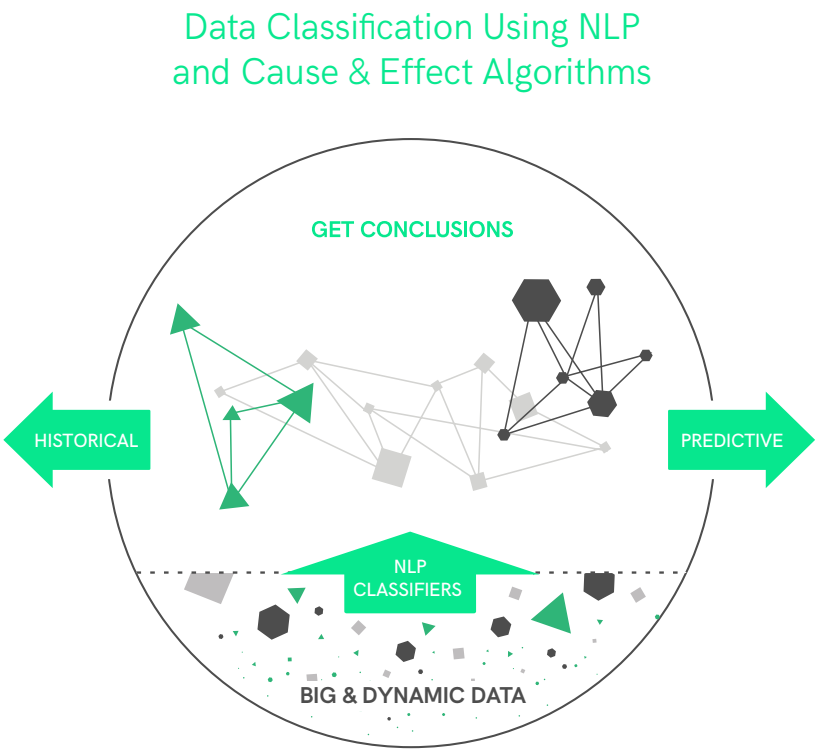


Figure1.

Natural Language Processing- a field of artificial intelligence concerned with the interactions between computers and human (natural) languages.

NLP enables a machine to process structured and unstructured data and to arrive at conclusions.

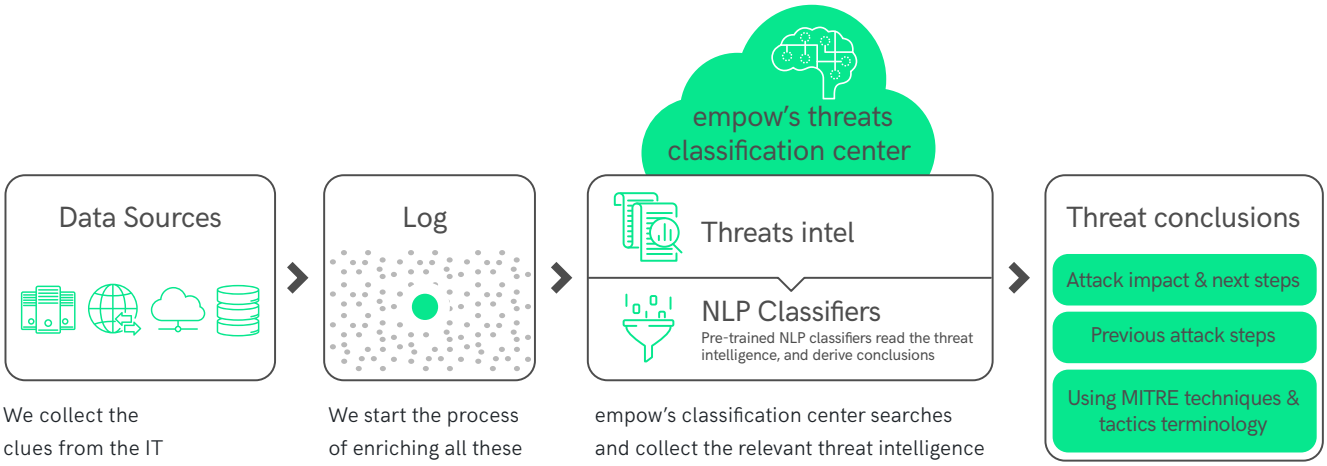
NLP - How It Works

NLP is a field in artificial intelligence that focuses on understanding and converting natural language into workable data. In our context, NLP enables to automatically classify signals from natural language (like threat intelligence content) into potential attack stages, tactics, and techniques.

Some logs (or clues) already include natural language, which describes them. However, many do not.

The good news is that threat intelligence data in the form of natural language is all around us. Threat Intelligence data is updated on an hourly basis by the good guys as well as the bad ones and is constantly documented and updated. Threat Intelligence data sources such as virus total, commercial threat intel. centers (TIPs), security blogs, security research centers such as Microsoft, TrendMicro, Symantec, and many more, including "bad guy" blogs.

The following process illustrates the flow to collect and use threat intelligence and NLP for automating the process of logs classification into classes of attack tactics and techniques which represent attacker intent, as well as into classes of possible root causes of the attack.



We collect the clues from the IT infrastructure, the logs.

We start the process of enriching all these logs with threat intelligence, written in natural language, via empow's NLP-based classification center

empow's classification center searches and collect the relevant threat intelligence data based on clues inside the logs (e.g., object hash, malware name, intrusion name, CVE and more), and erchied each log with it.

Pre-trained NLP classifiers read the threat intelligence, and derive conclusions

Figure 2

In this way we can enrich ALL logs (especially the ones which lack a natural language description) into natural language. The beauty of NLP is that it liberates us from having to read and process the entirety of the sentences and paragraphs. describing the threat or the attacker intent. The result is a log that is enriched with information that is used by the security analyst to accelerate the process of alert validation, and to investigate the possible impact and next steps of the attack, as well as the root cause..

Training process – it comes ready …

NLP classifiers are trained to read and understand the security language inside messages, including logs, intelligence data-feeds, security articles and reports etc.

The training process is conducted at empow's cloud classification center and is hosted on AWS. In order to continuously train the classifiers, the classification center is fed with millions of data and samples including 3rd party threat center security reports.

As part of the NLP classifiers creation and optimization process, empow's security research team provides its classification inputs and feedback. This process allows to test the performance of each classifier until it is optimized to a level that can classify new (previously unseen) data with a very high degree of accuracy.

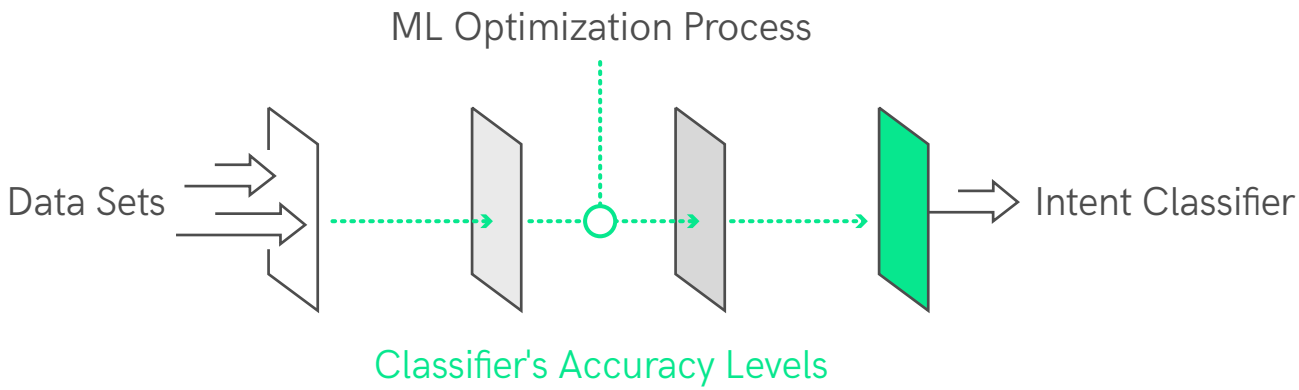


Figure3.

How does your solution deal with false positives and other AI modules?

empow's solution integrates with the existing network and security infrastructure and includes a number of internal layers that work together in order to filter out noise and false positives from the organization's entire security system. These layers are:

NLP ML Classifiers

Automatically select only the logs and data feeds that are associated with threats that are in focus for the organization/business. In this way, they prevent duplicates (merge logs and data feeds that mean the same thing), and remove logs that are not relevant.

Cause-and-Effect Algorithms

Collects all the classified logs, analyzes them, identifies cause-and-effect relationships and, if these exist, creates an "attack story". Logs that cannot be correlated with others are considered lower priority (noise or false positives) and are filtered out accordingly.

Automated Investigation

Conducts two types of investigative actions, in the context of the developed "attack story", in order to prioritize the detected threats and further remove false positives and noise:

- Root-cause forensics analysis that searches for historical "supportive events" and can validate the "attack story" (i.e. an incident) accordingly.
- Predictive – anticipates the possible next steps (the potential effect), provides the user with these next steps to conduct prevention action, as well as strengthens the decision in case a next action does actually occur.

How often must your AI models be refreshed?
How do you update your AI models?

empow's AI classification center refreshes the NLP classifiers every few months (typically 4-6 months) and updates our solution with the classifiers automatically.

As the "security language" doesn't change so often (terms remain pretty steady), only the content does, our classifiers can remain relevant for this length of time with no updates.

Summary

empow is the first cybersecurity company to take advantage of the tremendous progress made by the data science community in NLP algorithms to develop a solution that automatically classifies and understands the huge amount of data that security tools and the network infrastructure generate, without human intervention.

empow's patented, data-source agnostic AI technology deciphers the intent behind each log and data feed that the network infrastructure generates. The AI algorithms emulate actions done today by the security analyst, including: Reading the textual logs and data feeds, seeking out more relevant information from third party threat research centers, understanding the intent behind the data and identifying cause-and-effect relationships between all the clues, which can potentially form a real "attack story".

Customers choose empow's AI because it:

Reduces the noise & false positives in the security system.

Its data-agnostic AI technology translates into seamless and faster integration with more organizational data sources.

Detects advanced threats missed by point solutions - Instantly correlates the data from the silos and identifies security incidents missed by point solutions, quickly.

Reduces time to respond by automating the process of triage, correlation and root-cause investigation.

Maximizes existing and future security investments – creates a security ecosystem that maximizes the security value of the existing infrastructure, while reducing the overall TCO.

This all translates into fast and optimal incident response, while at the same time simplifying security operations and eliminating maintenance overhead.

empow
You have it in you.

Tel: +1-877-647-4361
129 Newbury Street, 2nd Floor
Boston, MA 02116, United States

Tel: +972-3-519-5517
Hayetzira 29, Ramat Gan,
Israel 5252171

www.empow.co
info@empow.co