**How does machine learning work in security?**

Machine learning (ML)  lets computers to learn without being explicitly programmed and also it learn by experience. Machine learning is a domain within the broader field of artificial intelligence if you can imagine.

In security, machine learning continuously learns by analyzing data to find patterns so we can better detect malware in encrypted traffic, find insider threats, predict where malicious activity are going and make aware of it and those who are online to keep people safe when browsing, or protect data in the cloud by uncovering suspicious user behaviour.

The cyber threat is something which is increasing and new threats are coming every span of time and these are the threat which attacks the important data and to protect from the attack is not handle by only a team of people

This is where machine learning shines as machine learning can recognize patterns and predict threats in larger about of data sets, all at machine speed which is necessary. By automating the analysis, cyber teams can rapidly detect threats and isolate situations that need deeper human analysis.

**Let us know in brief how it works**

The details of machine learning can seem exciting to non-data scientists, so let us know some key terms

Supervised learning calls on sets of training data, called “known truth,” which are correct question-and-answer pairs like key-values. This training helps classifiers, to work around for machine learning analysis, to accurately categorize observations. It also helps algorithms, used to have better classifiers, better analyze new data in the real world. Example of everyday when we upload pic of group of people in Facebook so it recognize people automatically: it is done Classifiers analyzer where they learn the data patterns they are trained it is not like that they are recognizing by your nose or eye in order to correctly tag a unique face amongst many millions of online photos.

**How machine learning helps security; let us know it stepwise**

**Find threats on a network**

Machine learning detects threats by constantly monitoring the behaviour or pattern of the network for anomalies.  Machine learning engines process massive amounts of data in near real time to discover critical incidents or anomalies. These techniques allow for the detection of insider anomalies’, unknown threat & malware, and policy violations.

**Keep people safe when browsing**

Machine learning can predict “bad neighbourhoods”( which can also be stated as abnormal pattern) online to help prevent people from connecting to malicious websites which can steal the information provided Machine learning analyzes Internet activity to automatically identify attack infrastructures staged for current and emergent threats.

**Provide endpoint malware protection**

Algorithms can detect never-seen-before malware that is trying to run on endpoints.  It identifies new malicious files or folder and activity based on the attributes and behaviours of known malware which triing to become one.

**Protect data in the cloud**

Machine learning can protect productivity by tracking doubtful cloud app login or suspicious activity, detecting anomalies by location-based, and conducting IP reputation analysis( to check trustworthiness of source) to identify threats and risks in cloud apps and platforms.

**Detect malware in encrypted traffic**

by analyzing encrypted traffic data elements in common network telemetry machine learning can detect malware in encrypted traffic. Rather than decrypting, machine learning algorithms pinpoint malicious patterns to find threats hidden with encryption which may take some span to analyse.