УДК 004.8
Nikita Zuy[1], Nataliia Zhukova[2]
[1]student of group CST-510, National University «Zaporizhzhia Polytechnic»
[2]PhD (Philology), assistant prof. National University «Zaporizhzhia Polytechnic»

AI/ML APPLIED TO CYBERSECURITY

Cybersecurity is one of the multiple uses of Artificial Intelligence. A report by Norton showed that the global cost of typical data breach recovery is $3.86 million. The report also indicates that companies need 196 days on average to recover from any data breach. For this reason, application of AI and machine learning (ML) to cybersecurity is essential.

Machine learning and Artificial Intelligence in cybersecurity is much more than a mere application of the algorithms. It can be used to analyze cyber threats better and respond to security incidents. There are a few other significant benefits of machine learning:

1. detecting malicious activities and putting end to cyber attacks;

2. analyzing mobile endpoints for cyber threats (Google is already using ML for this purpose);

3. improving human analysis – from malicious attack detection to endpoint protection;

4. automating mundane security tasks;

5. eliminating zero-day vulnerabilities.

Traditional security techniques use signatures or indicators of compromise to identify threats. These methods might work well for previously encountered threats, but they are not effective for threats that have not been discovered yet.

Signature-based techniques can detect about 90% of threats. Replacing traditional techniques with AI can increase the detection rates up to 95%. The best solution would be to combine both traditional methods and AI. This can result in 100% detection rate and minimize false positives.

While traditional vulnerability databases are critical to manage and contain known vulnerabilities, AI and ML techniques like User and Event Behavioral Analytics (UEBA) can analyze baseline behavior of user accounts, endpoint and servers, and identify anomalous behavior that might signal a zero-day unknown attack. This can help protect organizations even before vulnerabilities are officially reported and patched.

The purposes of a remote attack are to abuse and take touchy information from the framework or to harm by presenting a noxious computer program. Remote exploitation can happen in different ways.

Denial of service attack. Typically, a procedure to form the server inaccessible for clients by flooding the servers with untrue client demands. It makes a tremendous utilization spike which makes servers solidify and preoccupies them with a huge number of pending demands to continue.

DNS poisoning. DNS servers are frameworks that interpret human-memorable space names like facebook.com to compare numeric IP addresses. DNS frameworks are utilized to distinguish and approve assets on the web. Harming DNS servers fundamentally implies deceiving them to acknowledge misrepresented information beginnings as true and clients who are getting to those harmed DNS servers are diverted to locales that unwittingly download malevolent programs or infections into the framework.

Port scanning. Computer ports are utilized to send and get information. Port scanners can be utilized to distinguish vulnerabilities of information and pick up get to control computers by abusing those vulnerabilities.

Artificial Intelligence/Machine learning algorithms can be utilized to analyze framework behavior and recognize anomalous occasions that do not match the ordinary behavior. Algorithms can be prepared for different information sets so that they can track down a misuse payload in advance.