# Aujas Blog

# Artificial Intelligence - The magic potion to bolster cybersecurity

Carlton Mascarenhas

Sep 22, 2020

SHARE

Remote work is seeing a spike in security threats. Be it backdoor malware, or the abuse of new network protocols such as CoAP, WS-DD, ARMS, Jenkins by DDoS attack vectors or Mobile APTs, prove that hackers have become smarter than ever. The targeted attacks landscape is changing rapidly, and the scare of such attacks might reach a flash point. This fear can push any CISO to ride the wave of uncertainty, making him anxious about how to take on the maverick hacker brain sitting in some corner of this hyper connected world. Hackers are dramatically better, and its time cybersecurity matches up to deliver its promise and not just remain with its grandiose assurances to mitigate threats.

To transcend existing technology limits of managing security for the digital wave of Cloud, IoT, mobile, sweeping the world, and the vast computing resources and oceans of data leveraged by these technologies, enterprises must augment and enhance their security preparedness. Threats have become more intelligent than ever before, and the bitter truth is that these threats must be monitored and responded in real-time to search for every vulnerability across threat span.

In a connected world, where computers are fast becoming the most widely seen objects, they are also the most infected ones with advanced persistent attacks that are high in volume and multidimensional. The threat data generated by these attacks are voluminous, and analyzing the alerts produced by these threats can be tedious and time consuming, if done manually. Legacy security systems are obsolete to manage such tasks and cannot monitor, detect, and respond to threats in real-time.

To take on these tyrannical hackers in the cyber battlefield, security pros must adopt the superpowers of Artificial Intelligence to enhance the chances of winning without any glitch. AI can propel the speed at which systems monitor, detect, and respond to threats. AI can also ingest and process large amounts of threat data to unearth anomalies and automate suitable actions to eradicate the threat rapidly.

AI offers indispensable advantages to transform your security posture and helps you to build and deploy advanced threat protection models.

## Monitoring & identification of attack

The digital world presents a range of vulnerability areas, and anomalies can show up just above anywhere. When a breach happens, the attacks can enact various behaviors as they move across the network. Tracking the attackers' footsteps are the key to know their intentions, how they breached your network, and the pathways taken to access various assets. Revealing and analyzing the route taken can help in faster response and enable you to prevent such attacks in the future. Understanding the attack path is possible only when every single traversing network data is collected, analyzed, and contextualized by leveraging an AI platform.

### Reduce false security alerts

Large number of false positives from rule-based detection systems can mislead security analysts by giving them the impression that every alert is an attack. There can also be a false negative, which is a genuine attack that might go undetected. Analysts have a tough time prioritizing these alerts when even an innocuous alert might look like an aggressive attack. In such cases, AI can augment the analyst's efforts in differentiating the real attacks from the rest. AI can leverage ML methods of clustering, data visualization, pattern recognition, and rule association to segregate and highlight alerts for analysts to examine them further.

### Hunt for threats

Patrolling for threats lurking undetected across the IT infrastructure must be a proactive practice to find any malicious actors that might have slipped past your endpoint defenses. They remain on stealth mode and exercise their intent to look for sensitive data, gather login credentials, and try ways to move laterally across the infrastructure. If you lack AI-driven advanced threat detection capabilities, these adversaries can penetrate and spread across the network. Threat hunting driven by AI can identify unusual patterns, abnormal behaviors, anomalies while augmenting the analyst's cognitive capabilities to investigating the threat. AI can also enable threat data analytics by using ML algorithms to examine any irregularities to pinpoint any abnormalities that might probably be malicious activity.

### Analyze and investigate incidents

Prioritizing alerts and segregating incident symptoms are just not enough, the incidents must be investigated thoroughly to mitigate damage, eliminate any hidden attack spots and attacks, and prevent any upcoming attacks. Security incident investigation solutions that leverage AI provides total real-time visibility and can contextualize threats by leveraging threat intelligence repositories from various security engagements, security event analysis, and endpoint sensors. The solution can also help in conducting deeper forensic analysis to know the impact and behavior of the attacks, including the way they spread. Another important solution feature is security analytics, which can quickly comb through billions of events within seconds to do an event log correlation to uncover any Indicators of Compromise (IoC) within the network.

### Predicting Threats

Anticipating threats is critical, as it can help in knowing the type of threat vector that might hurt the enterprise. AI tools can be used to automate the collection of terabytes of machine-readable threat intelligence data from around the world and contextualize them based on the organization's threat profile. Security analysts can leverage the data to implement remediation's by understanding the topology and tools to protect your enterprise infrastructure.

### Incident Response

One of the biggest challenges of IT teams is the difficulty to interpret and respond to incidents quickly. The challenges include how, or which team or analyst should respond, understanding the relationship between incidents, ensure consistency in response, and gain feedback to improve the security posture for the future. AI, with its incredible ability, can resolve every challenge in incident response through a more predictable and effective approach. AI can contain the attack spread through faster and accurate detection, retrieve affected assets, and improve security posture. Automated remediation is another feature that uses ML for incident response. AI solutions also use application programming interfaces to automate response and remediation through playbooks.

These are just a few critical ways Artificial Intelligence can support security analysts in detecting threat advancements and help them devise new strategies to mitigate complex threats. AI is a powerful resource for user behavior analysis, infer network activity patterns, or recognize any irregularities which are serious security risks to the business. AI can also minimize human security responsibilities through the automation of incident detection, response, and remediation. AI is here to change every traditional security approach and can be considered a magic potion meant to bolster cybersecurity.

**Eager to know how Aujas can help you strengthen your security posture to take on next-gen threats? Please do reach us at contact@aujas.com.**


WRITE TO US

contact@aujas.com

Secure Development

Ecosystem Engineering

CodeSign Platform

Custom Security Development

## Managed Threat Detection And Response

## Company

About us

Careers

Contact us

## Resources

Blog

Collaterals

Case Study