# SECURITY AUTOMATION / MACHINE LEARNING

**by Jason Lorenz, VTS Program Services Coordinator**

## INTRODUCTION

While many industries are struggling amid the coronavirus pandemic, both the IT industry and the broader trend of transition to remote work have revealed many areas where traditional approaches to managing businesses create unnecessary waste. Still, data science and its subdivision – machine learning – reveal that such expansion is nearly limitless. [1]

When it comes to giving cyber security experts the tools they need to take action, automation and machine learning (ML) can make a big difference. Many companies are working with high volumes of data, and types and variants of attack are always growing and changing. It can become too much for people to process in a meaningful time frame. But security automation and machine learning-based early triage can reduce data volumes. [2]

## SECURITY AUTOMATION

So what is security automation exactly? Security automation is the machine-based execution of security actions with the power to programmatically detect, investigate, and remediate cyber threats with or without human intervention by identifying incoming threats, triaging and prioritizing alerts as they emerge, then responding to them in a timely fashion.

Security automation does most of the work for your security team, so they no longer have to weed through and manually address every alert as it comes in. Among other things, security automation can:

- Detect threats in your environment.
- Triage potential threats by following the steps, instructions, and decision-making workflow taken by security analysts to investigate the event and determine whether it's a legitimate issue.
- Determine whether to take action in response.
- Contain and resolve the issue.

## SIGNS THAT AN ORGANIZATION NEEDS SECURITY AUTOMATION

There are several signs indicating that your organization needs security automation, including a breach, lagging response times, overwhelming false positives, and a need for more efficient and cost-effective operations.

---

1 https://artificialintelligence-news.com/2021/03/03/five-common-use-cases-where-machine-learning-can-make-a-big-difference/
2 https://securityintelligence.com/posts/security-automation-enterprise-defense/

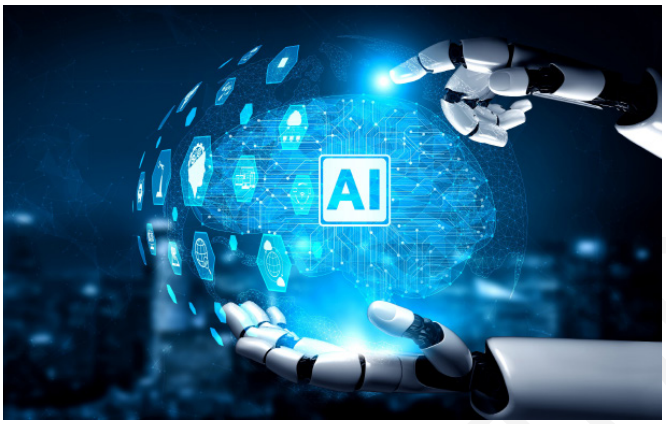


14900 Conference Center Dr,
Suite 200
Chantilly, Virginia 20151

info@vtscyber.com
Jason Lorenz - jlorenz@vtscyber.com
703.498.2150 703.498.2149

While it's safe to say that most organizations could benefit from security automation, they're more likely to require or adopt it if:

- **A breach has occurred.** Billions of people and countless businesses have been affected by data breaches. In 2018, breaches cost roughly $148 per lost or stolen record – nearly $4 million overall per incident. Organizations can't afford to be lax when it comes to security measures.
- **Incident response times are lagging.** Security analysts can only investigate a fraction of the alerts that come in, so responding in real time is rarely possible. Organizations need solutions and practices that allow them to resolve incidents faster, reducing overall time spent per incident.
- **False positives are overwhelming the security team.** False positives are only revealed as false after each is investigated as a real threat. These incidents steal security analysts' focus and prevent them from addressing genuine threats.
- **Security teams want to operate more effectively, efficiently, and cheaply.** If security analysts are wasting time on repetitive tasks and false positives, they aren't maximizing their value to the organization. [3]




## MACHINE LEARNING

The pandemic has accelerated the imperative for businesses to invest in Artificial Intelligence (AI) and Machine Learning (ML) so they can replace guesswork with data-powered certainty to reorient strategy and optimize operations for success in an uncertain future. The ability to make fast, data-driven decisions has never been more valuable as businesses grapple with the shift toward hyper-personalization, driven by rapidly changing customer behaviors and expectations.

Nevertheless, enterprises often struggle to integrate these technologies at scale and monetize the benefits. Stumbling blocks typically include challenges associated with cost, lack of investment protection, undefined business outcomes, lengthy timeframes from development to deployment, lack of expertise, and the complexities of the regulatory landscape.

There's no one size fits all. MLOps implementation should be governed by business priorities and current levels of AI/ML adoption. That said, establishing a robust MLOps framework is fundamental to streamlining the process from model creation through training to deployment so companies can reap value from AI/ML much faster. [4]

## FIVE CASES WHERE MACHINE LEARNING CAN MAKE A DIFFERENCE

Machine learning uses powerful algorithms to discover insights based on real-world data that can then be used to make predictions about future outcomes. As new data comes available, machine learning

[3] https://www.splunk.com/en_us/data-insider/what-is-security-automation.html
[4] https://www.cio.com/article/3609525/stop-experimenting-with-ai-and-machine-learning.html

14900 Conference Center Dr,
Suite 200
Chantilly, Virginia 20151

info@vtscyber.com
Jason Lorenz - jlorenz@vtscyber.com
703.498.2150 703.498.2149

programs can automatically adapt and produce updated predictions. As with any tool, machine learning is not a silver bullet. However, there are many situations in which the technology can outperform linear and statistical algorithms.

Here are five of the most common use cases where machine learning can make a big difference:

- When engineers can't code rules for certain problems.
- When you need to scale a solution to millions of cases.
- When you can do it manually, but it's not cost-efficient.
- When you have a massive dataset without obvious patterns.
- When you live in an ever-changing universe (adaptive). [5]

## CONCLUSION

Threats in the digital world evolve so quickly that no amount of training and manpower can effectively catch or detect any kind of malware or virus that could indicate of a security breach. With industries struggling with the coronavirus pandemic, there is now more than ever, a greater threat within organizations without the use of manpower. Using security automation and machine learning will give an organization the ability to limit the amount of threats within cyber security while limiting the amount of manpower needed to do so.



[5] https://artificialintelligence-news.com/2021/03/03/five-common-use-cases-where-machine-learning-can-make-a-big-difference/