Exploring the usage of AI & ML in Cybersecurity

A conversation around how ML can boost security capabilities and its pitfalls

KAIF AHSAN

1068214

SANSKAR AGARWAL

908069

REBEKAH WU

1074412

Agenda

A brief overview of the presentation

01

The security landscape

We get a brief overview on how security is ensured in organisations and it's current challenges

02

Benefits of ML & IBM's product suite

How usage of ML can overcome traditional challenges companies face with cybersecurity and what IBM specifically has to offer.

03

Protecting our privacy

Looking at existing legislation and privacy impacts on our employees and clients. Explore how to achieve security without compromising privacy.

04

Recommendations & drawbacks

Based on the different factors, make high level recommendations and review drawbacks of each approach

The Cyber Landscape

Common Defensive Strategies

A brief overview of defensive mechanisms adopted by companies [1]

SECURITY OPERATION CENTER (SOC)	A dedicated or outsourced team which monitors and deals with security issues through various tools and technologies.
RISK MANAGEMENT AND COMPLIANCE	Comply with national and international regulations to establish a risk management strategy.
SECURITY AWARENESS AND PRACTICES	Establish best security practices and make the wider organisation aware of common security concepts.

What data can we collect for security purposes?

System and sensory information

Key security decisions can be made from application and network traffic data such as IP addresses, cookies etc.

Log & Access Information

Logs and access information are crucial for the security teams to detect intruders in the system.

Behavioral data

User generated content is often utilised by the security team to classify users and detect anomaly.

Limitations of Modern Security

Problems

The common issues that modern security operation centers face

01

Resource intensive

Setting up an effective security program from ground up can be very time consuming and costly.

02

False positives & repetitive

SIEM and SOAR often produces high volume of false positives which are not only time consuming but also repetitive.

03

Hard to scale

If the business grows rapidly the security team will find it hard to keep up due to a high volume of data and logs generated.

Solution - Machine Learning

Automating security using AI & ML can yield a high amount of benefits.[2]

01

Out of the box solutions available

Relatively cheaper third-party solutions from distinguished companies available.

02

Automated and accelerated decision making process

Empowers human engineers to deal with high priority issues by automating routine and repetitive tasks.

03

Make security scalable & reliable

Designed to work across various workloads with reliability. Highly effective in parsing large amount alerts and logs to filter false positives.

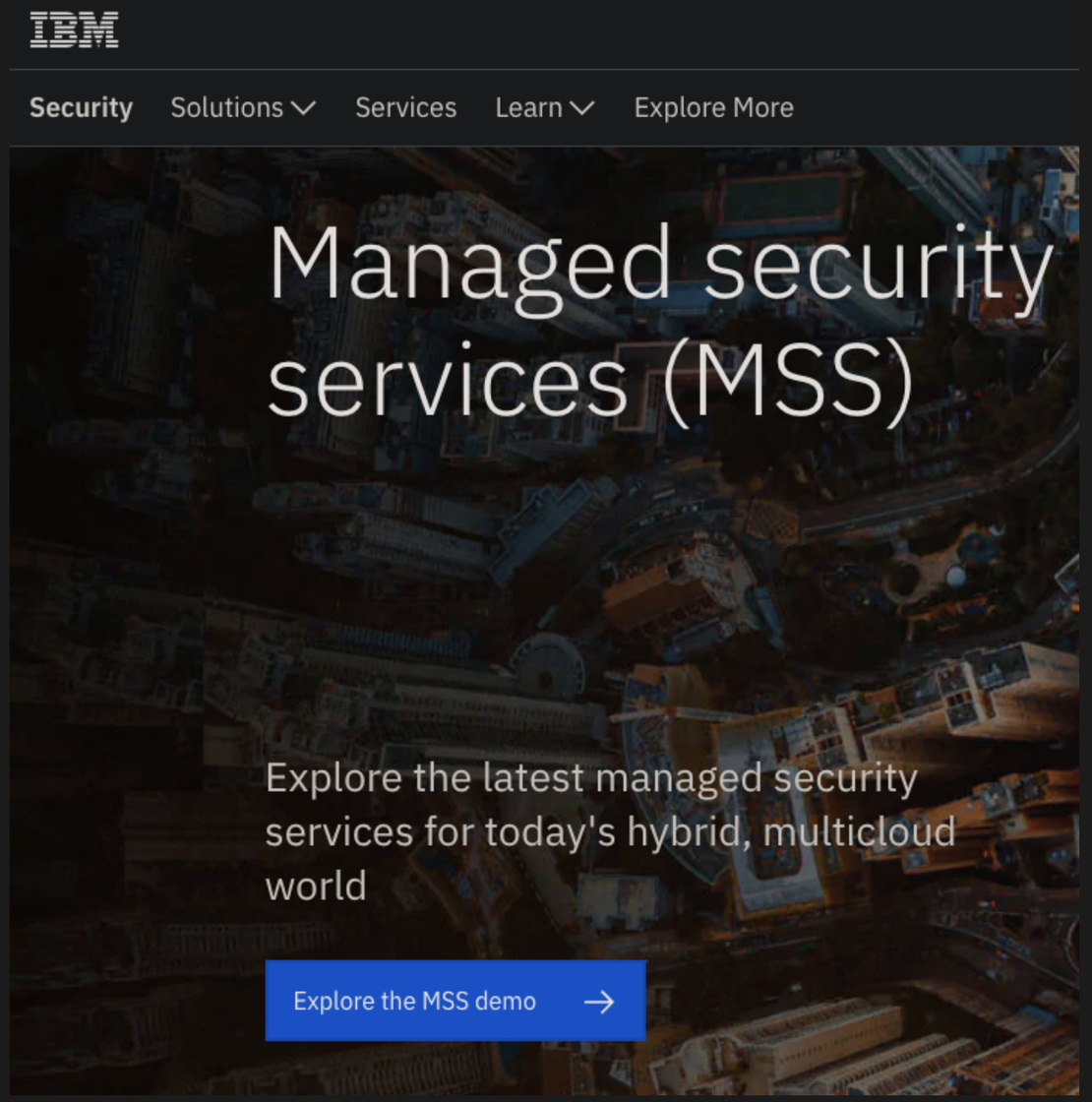
Enter IBM

Outsource security operations

REDUCE UP FRONT COSTS

AI & Automation

ENABLE SCALING WITH LINEARLY INCREASING COSTS



Machine Learning in IBM's Services

Focus on how ML services are integrated within IBM's QRadar Advisor with Watson.[3]

Empower Analysts

Allows their SOC analysts to focus on important tasks by automating repitetive tasks.

Better Investigations

AI powered QRadar Advisor can augment human intelligence to drive consistent investigation.

Reduce response time

Filter through false positives and thousands of alerts to show more actionable items.

How can our security data be repurposed?

How might our existing data contribute to AI powered security services.[4]

SYSTEM LOGS & NETWORK DATA	The ML can learn to distinguish regular traffic from an erratic behaviour by learning the patterns in the traffic information and logs.
EXISTING SECURITY ALERTS AND INFO	ML can be trained on commonly generated alerts to automatically filter out false positives.
BEHVARIORAL INFORAMTION	Collect sensory and behavioural data which can be repurposed to learn user profiles and distinguish an attacker from a regular user.

Exploring and Uplifting Privacy

Existing Regulations

1980 OECD Guidelines on privacy form the backbone of all privacy laws. [5]

Collection Limitation

Collection of personal information should be limited only to what is necessary. If possible this should be done with consent or knowledge of said person.

Purpose Specification

The purpose of collecting personal information should be specified to the individual at the time of collection.

Use Limitation

The personal information collected should only be used for intended purpose unless there is consent or legal authority to do otherwise.

Existing Regulations

Domestic and International Regulations

Private and Data Protection Act 2014 [6]

- Applicable in Victoria
- Protect Private Information with flexible definition open to interpretation
- Has not adapted AI specific regulations

Privacy Act 1988 [7]

- Applicable in Australia
- Governed by 13 Privacy Principle
- Functionally Similar to PDP
- Has not adapted AI specific regulations

General Data Protection Regulation [8]

- Applicable to EU Citizens who may be employees or clients
- Has recognised AI has capabilities to generate new information and are trying to make adaptive amendments

Privacy Implications

Improper Data Collection

Lenient Legislations [9]

Existing legislature is lenient to data collection for cybersecurity purposes and IBM may collect our employee and client data liberally.

Invasive Tools [10]

Sensitive personal data such as employee emails are automatically tracked by SOAR based AI capabilities.

Usage without consent [11]

AI based data collection models collect Data automatically without consent of Individuals via web-tracking and monitoring.

Privacy Implications

Unintended Data Usage

Unintended repurpose of captured data

Organisations typically Issue notices to inform employees of data being collected and its purpose. However, AI has the ability to extract meaning from data beyond initial intended purposes without consent.

Employee behaviour tracking and predictions

Data being collected can be coupled with Narrow AI capabilities to model predictions on the productivity of employees which violates their workplace rights.

Privacy Implications

Risky Data Exposure

IBM will be extracting and maintaining large sets of data of our employees and clients. There is significant risk associated with such exposure.

If IBM were to undergo a breach or accidentally leak this data online security of our organisation and its people would face significant risk.

Achieving Both Privacy & Security

Consented Data Collection

Employees should be made aware of data collection and should ideally be done in an ‘unforced consent’ model.

Using Data

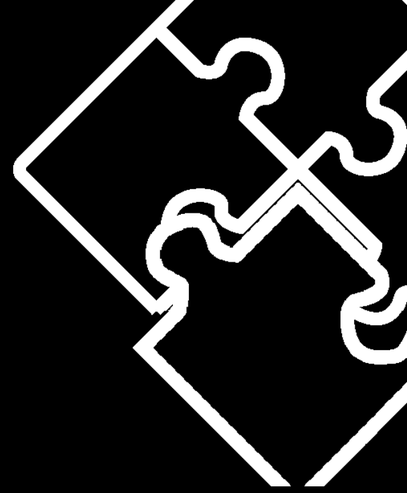
Regulations should exist that define the boundaries of usage of data. This would prevent data from being used for unethical purposes.

Protecting Data

Insurance should be sought against breaches or data leakages. Action plan should be sought incase of possible breaches and leakages.

Recommendations

Based on solutions and drawbacks -



TIERED ADOPTION	Adopt to IBM's AI based SOAR and monitoring capabilities gradually.
FILTERS AND RESTRICTIONS	Filter out Personally identifiable data (PII) and have restrictions on third party access.
REGULATIONS	Set up policies in regards to the prevention of IBM's collection and use of personal data for purposes other than monitoring the company's cybersecurity and ensure they comply with public legislated.

Novel legislation proposals

How we can legalise our security and privacy

Enhanced privacy laws

Key policies akin to 'Right to be forgotten' of the GDPR could be established for Australian consumers and businesses.

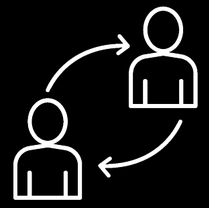
Restrict data misuse

Stricter laws can be established to ensure collected data can only be used for the intended purpose

Business Plan

AI specific laws as they have capabilities to synthesise meaning out of data and can create loopholes in existing laws.

Possible tradeoffs



Chained effect

If IBM's data is breached, the company and the employees' data would also be at risk of being exposed to the attackers.

However, we can trust IBM based on their track records and industry experience.

Up-front cost

There is upfront cost in establishing a process to extract PII and sensitive information in an automated manner.

However, it's lower than establishing a program of our own.

Slower adoption rates

There is a possibility that the employees might not feel comfortable performing tasks with the knowledge that they are tracked and monitored by an external third party

Future Roadmap

How we can safely adopt ML into our company

FIRST STAGE

Tiered Adoption

SECOND STAGE

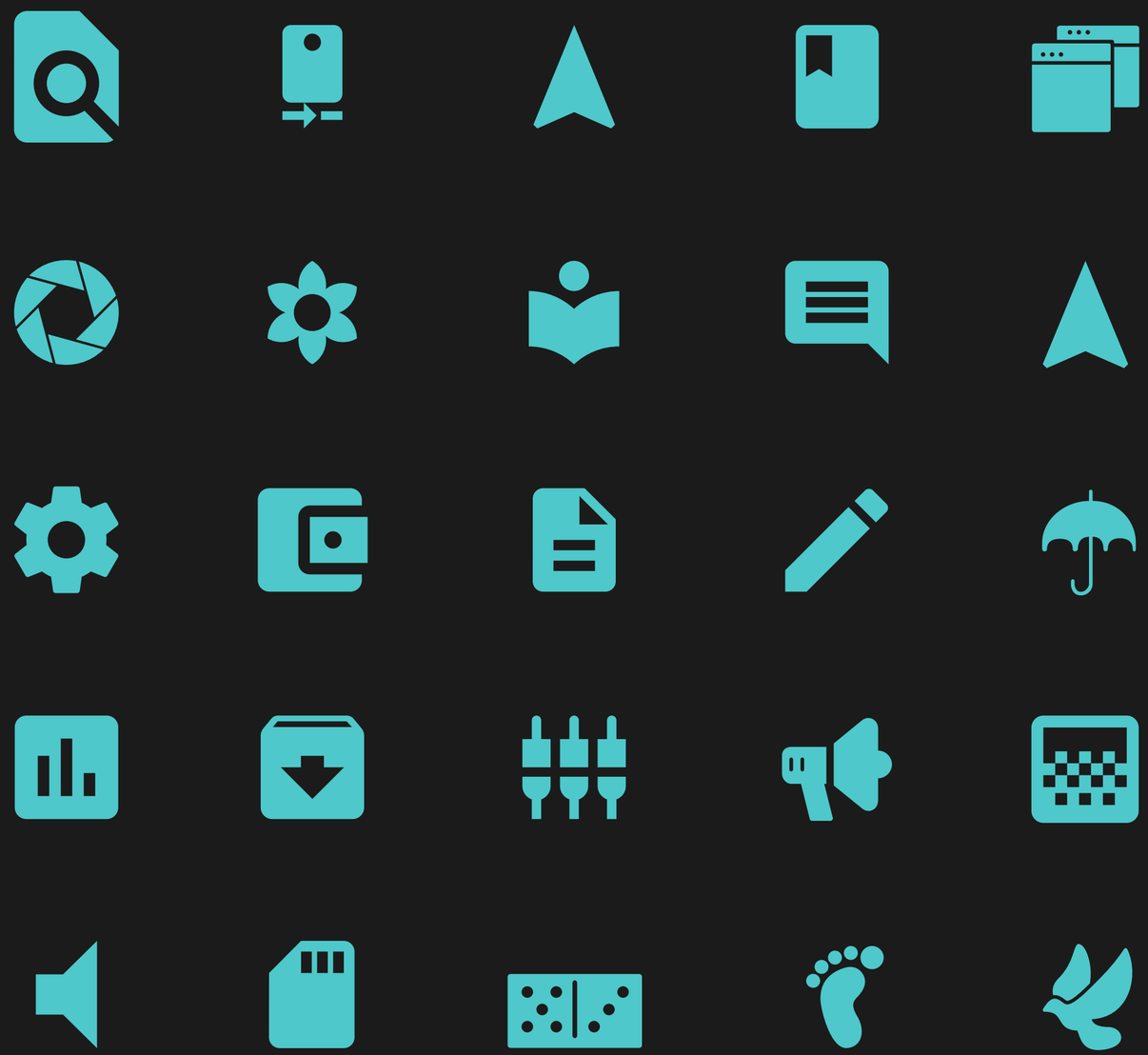
Verify initial results

THIRD STAGE

Full-fledge adoption

Thank you!

Any questions?



References

[1] Australian Government. (2021, August 3). Protect your business from cyber threats. Business.Gov.Au. https://business.gov.au/online/cyber-security/protect-your-business-from-cyber-threats

[2] Jackson, B. W. (2019). Cybersecurity, Privacy, and Artificial Intelligence: An Examination of Legal Issues Surrounding the European Union General Data Protection Regulation and Autonomous Network Defense. Minnesota Journal of Law, Science & Technology, 21(1), 169.

[3] IBM. (2021). IBM Security QRadar. https://www.ibm.com/au-en/security/security-intelligence/qradar

[4] Jackson, B. W. (2019). Cybersecurity, Privacy, and Artificial Intelligence: An Examination of Legal Issues Surrounding the European Union General Data Protection Regulation and Autonomous Network Defense. Minnesota Journal of Law, Science & Technology, 21(1), 169.

[5] Office of Victorian Information Commissioner(2021). ARTIFICIAL INTELLIGENCE AND PRIVACY – ISSUES AND CHALLENGES. Ovic.Vic.Gov.Au. https://ovic.vic.gov.au/privacy/artificial-intelligence-and-privacy-issues-and-challenges/?fbclid=IwAR1UpIpewCFK7bukmbbKOWGRKhCmtt_u5_xMy0hOMMOnBLDW_aZs3r7McPI

[6] Victorian Legislation. (2021). Privacy and Data Protection Act 2014. https://www.legislation.vic.gov.au/in-force/acts/privacy-and-data-protection-act-2014/027

References

[7] Australian Federation Government. (2021, June 29). Privacy Act 1988. Federal Register of Legislation. https://www.legislation.gov.au/Details/C2021C00242

[8] European Data Protection Regulation. (2016, April 27). General Data Protection Regulation. General Data Protection Regulation. https://gdpr-info.eu/

[9] Jackson, B. W. (2019). Cybersecurity, Privacy, and Artificial Intelligence: An Examination of Legal Issues Surrounding the European Union General Data Protection Regulation and Autonomous Network Defense. Minnesota Journal of Law, Science & Technology, 21(1), 169.

[10]IBM. (2021). IBM Security SOAR Platform - Overview. Australia | IBM. https://www.ibm.com/au-en/products/soar-platform

[[11]Escott, E. (2017, October 24). What are the 3 types of AI? A guide to narrow, general, and super artificial intelligence. Codebots. https://codebots.com/artificial-intelligence/the-3-types-of-ai-is-the-third-even-possible