Role of AI In Cybersecurity

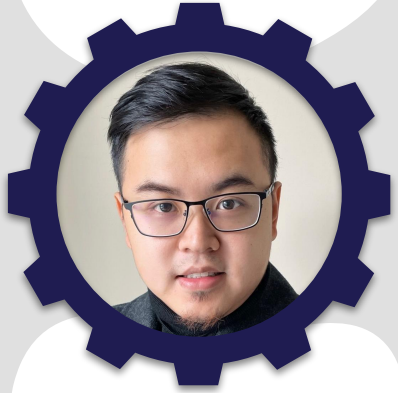
Purple - Team 1

Team Introduction

Abduni Idris

Alyssa Meyer

Ankitha Venkata



Eric Hsu

Sri Telagamsetty

Ujjwal Chauhan

Agenda

01
Cybersecurity Landscape
What are some trends in Cybersecurity?

02
Challenges
What are the some of the main challenges in Cybersecurity?

03
Solutions
How does Artificial Intelligence address these challenges?

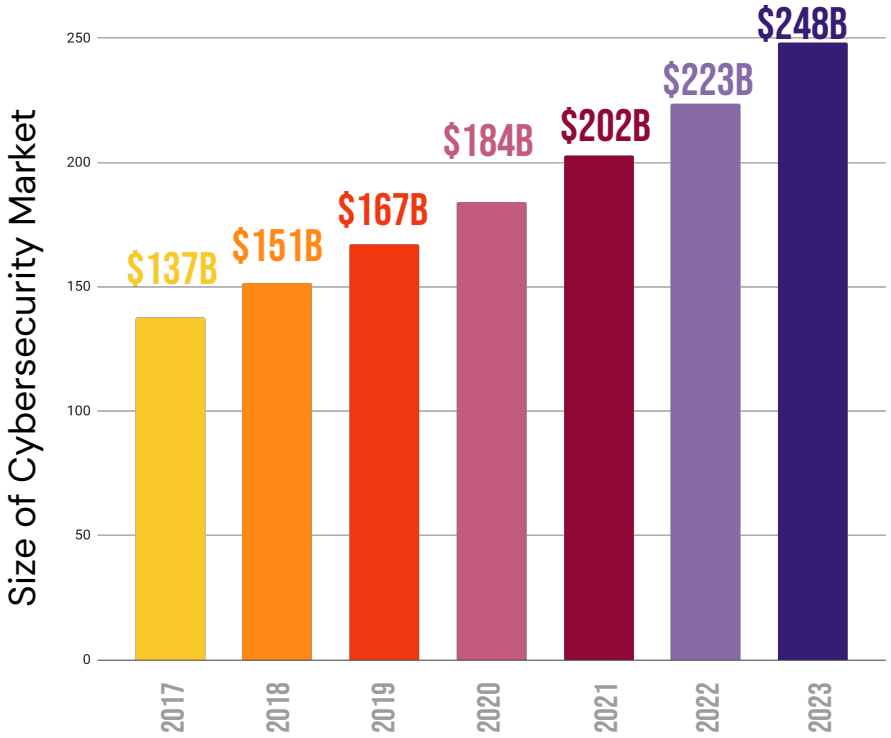
04
Keys for Success
What are some elements that are needed for AI to be effective?

05
Our proposal
How can we strategically implement AI?

06
Conclusion
Summary.
Q&A

01 Cybersecurity Landscape

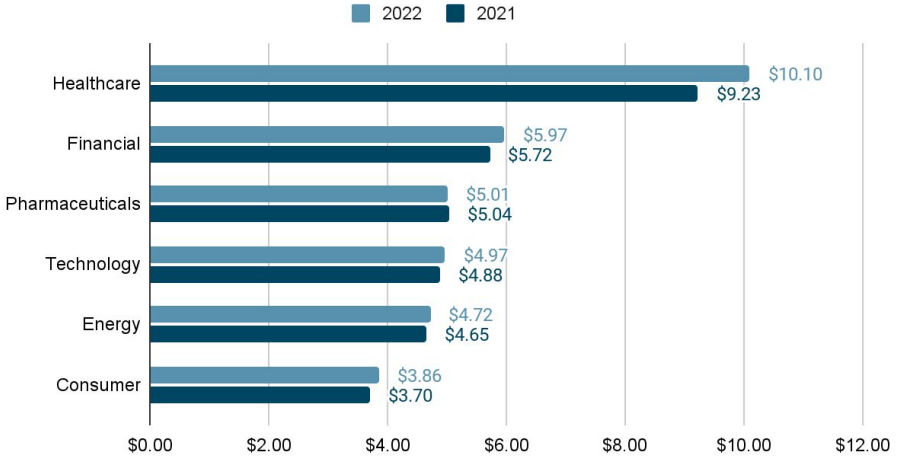
Cybersecurity Market Growth



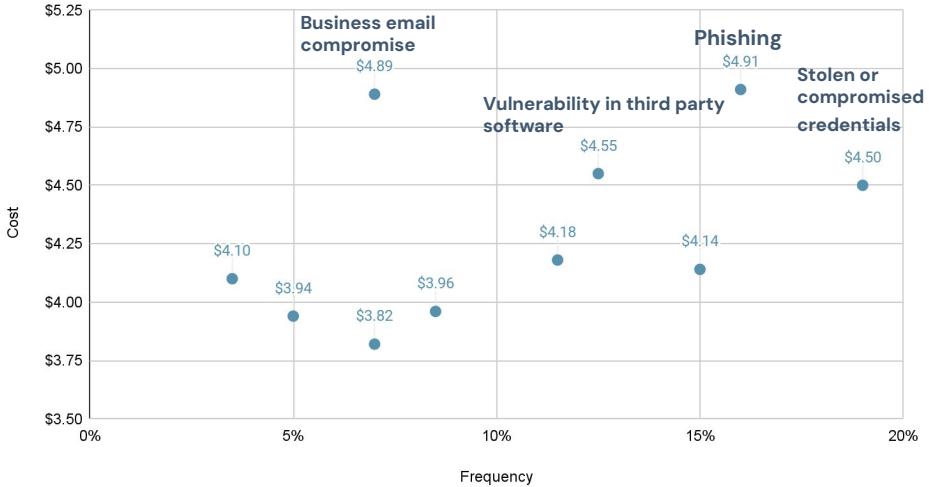
Source: Hackread.com

2022 Average cost of Data Breach ($Millions)

Average cost of a data breach by industry

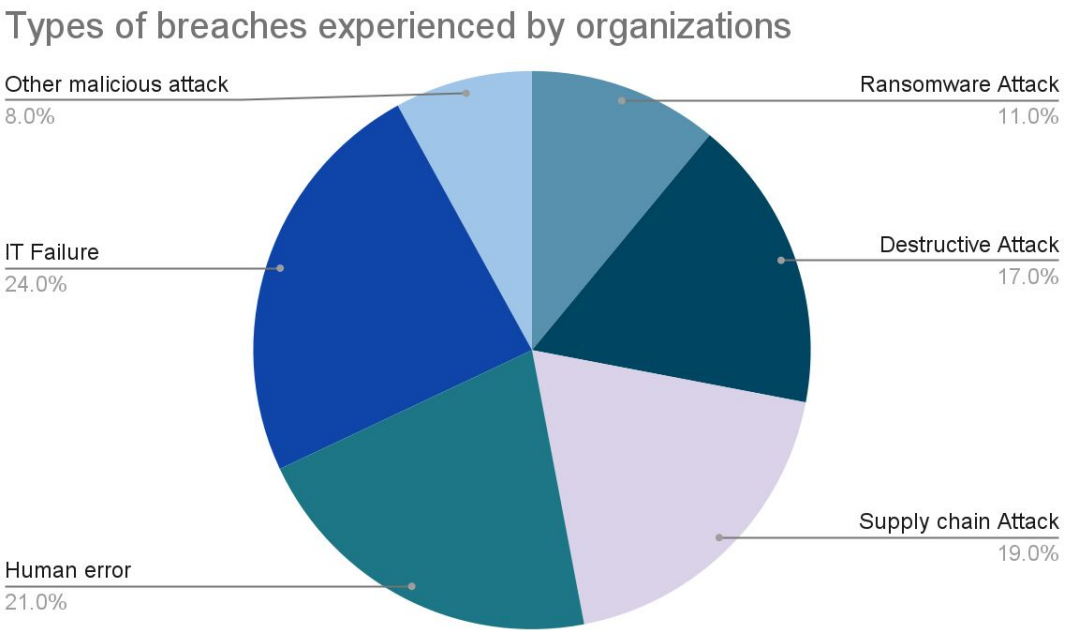


Average Cost and Frequency of Data breaches by initial attack vector



Source: IBM Cost of a data breach report 2022

Different types of Data breaches



Source: IBM Cost of a data breach report 2022

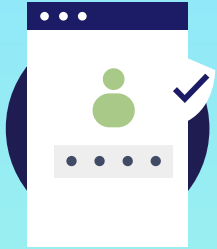
Current Trends

Cyber attacks

There were on average 270 attacks per company over 2021, increase of 31%

Ransomware

By 2031, its predicted to cost around $265 Billion



Password Attacks

74% increase with an estimated 921 every second

02
Challenges

What are the main Challenges?

Talent

Organizations are low on Talent:

- Alert fatigue is real & prevalent - false positives!
- There are not enough workers - For every 100 cybersecurity roles only 48 candidates.
- Job fatigue due to repetitive work.

USD 550,000

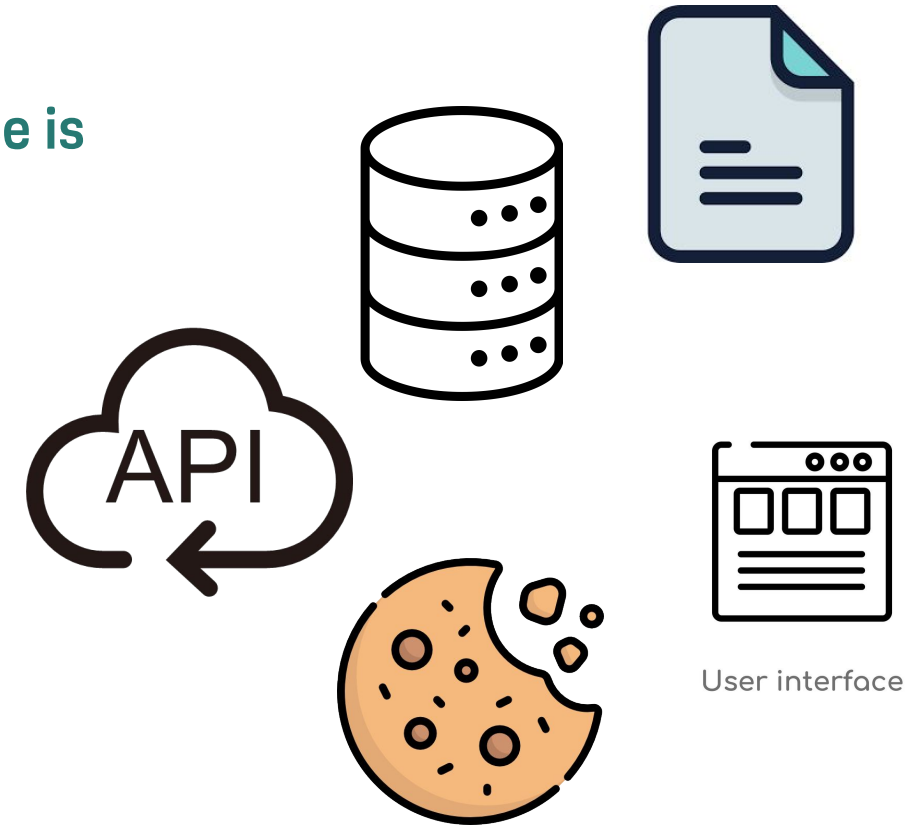
Average data breach cost savings of a sufficiently staffed organization versus insufficiently staffed

Source: https://www.ibm.com/downloads/cas/9EDONM6M

Threat landscape

Organization Risk Attack Surface is Massive!

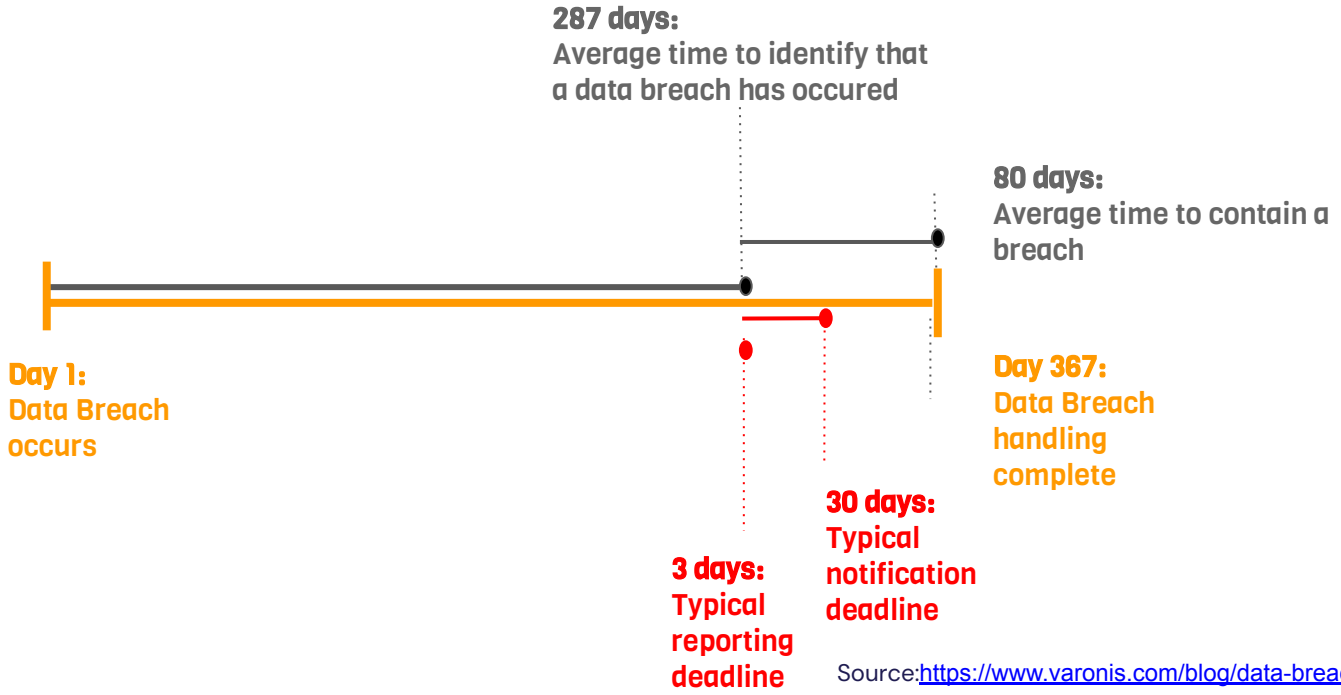
- Threat landscape is constantly evolving
- In some cases, potentially up to a billion!!
- Staying ahead of attackers is a constant battle



Source: https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/

Time

When Dwelling times are too long - it can cost Money!



Source:https://www.varonis.com/blog/data-breach-statistics

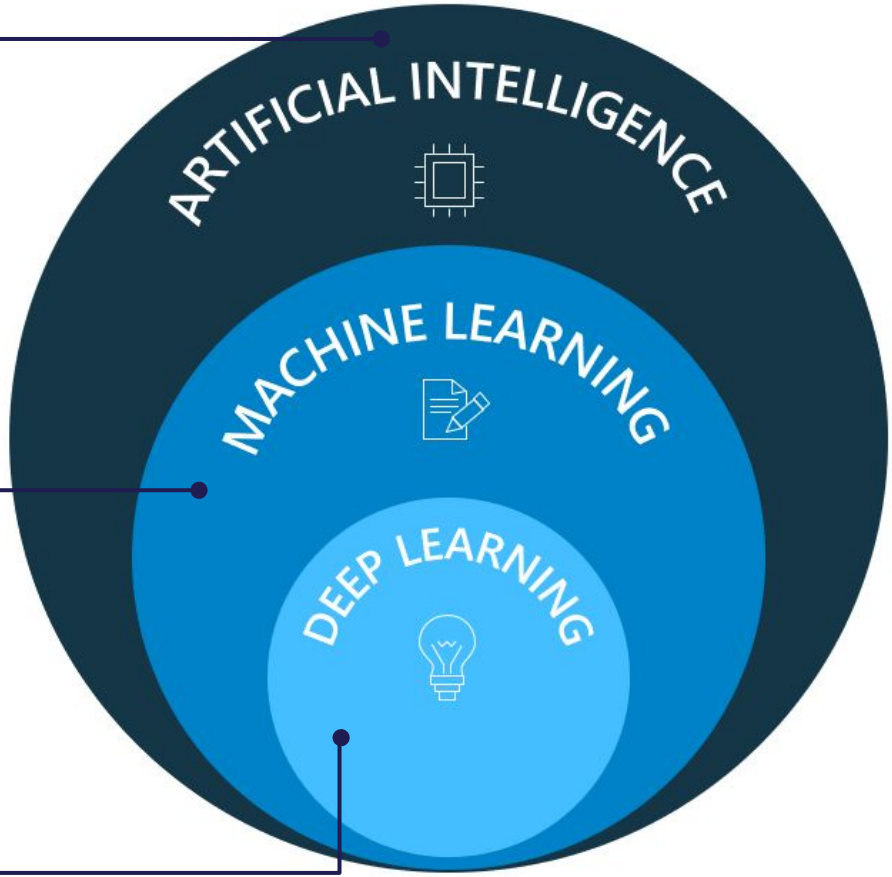
03
Solutions

What is AI?

Artificial intelligence refers to systems or machines that mimic human intelligence to perform tasks.
e.g. If-then rules.

Machine Learning use data to infer the unknown.
e.g. group and predict things.

Deep learning is part of machine learning methods. It is more suitable for unstructured data.
e.g. images, sounds



Value of AI

01 Chain different potential incidents together, automatically.

02 Solve people problem.

03 Drive consistent and deeper investigations, every time.

Value of AI

04 Conduct more thorough and consistent investigations in a short time.

05 Focus on the most important alerts first.

06 Have a robust and automated incident response (IR).

Highlights of Benefits

01 Automate Repetitive Tasks

02 Avoid False Positives

03 Identifies Threats Faster

04 Continuously Learns

04 Keys for Success

How to create effective AI solutions

Data

To insure accurate models you must have a large amount of quality data

Vulnerabilities of AI

With the developments of AI capabilities, the security of AI systems themselves is often overlooked

People

AI is not a replacement for cyber analysts, instead it enables defenders to effectively scale their protection capabilities

05
Our Proposal

Steps towards
Championing
Cybersecurity

Current challenges

Major struggles that our security team face:

- Our security team is understaffed and overworked
- CISO has to critically balance his decisions to prevent becoming a business blocker at the same time managing security priorities
- Current AI implementations are underutilized and not in sync with our processes
- Lack of AI experts on staff to consult our security team on best practices

Focus Areas for AI implementation

Automated Incident Response Workflow

Vulnerability Management

User and Event Behavior Analytics

Enhancing Network Security

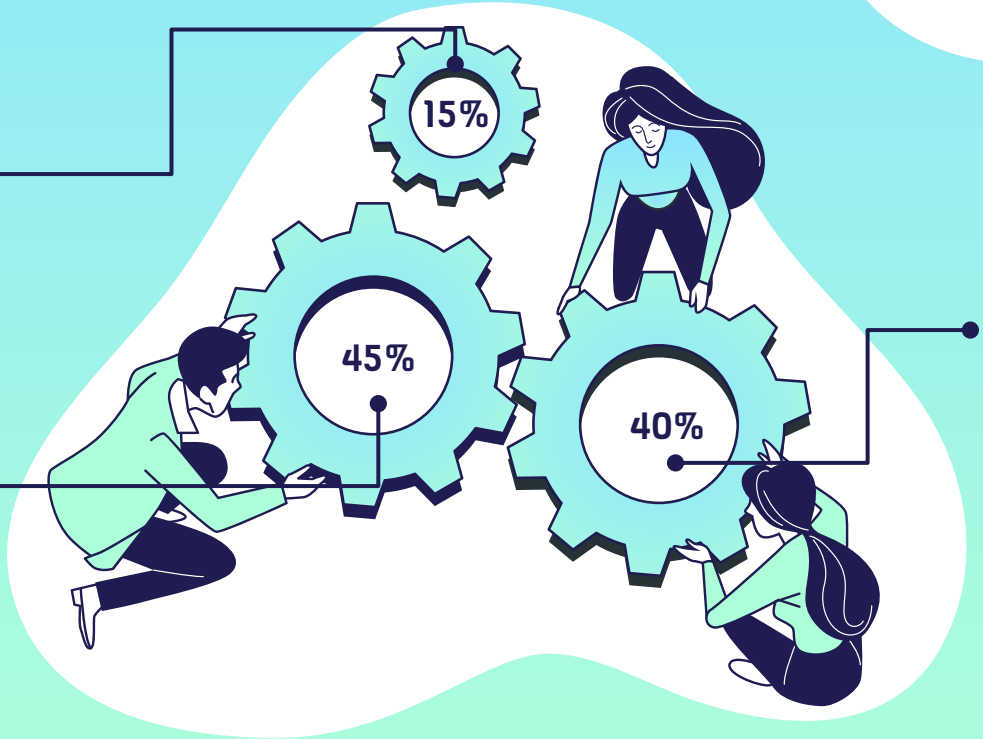
Workload reduction for security team

Investment overview

$2.5M
Total projected first year investment

External Consultation

New Technology Implementation



Security team Expansion

$1.5M
Subsequent yearly investment

Implementation Plan

Kick Off

- External consultants
- Solicitation for new technology
- Recruitment for internal team

3 Month Milestones

- Automation of manual security tasks
- Onboarding of new internal security team

6 Month Milestones

- Deployment of Automated Incident Response Workflow
- Cross training of security staff on AI practices

9 Month Milestones

- New Vulnerability Management adoption
- Deployment of AI based User and Event Behavior Analytics reporting

1 year Milestones

- We have fully deployed AI solutions in all areas of concerns
- We are **Security Champion!**

Cost Benefits

USD 3.05 million

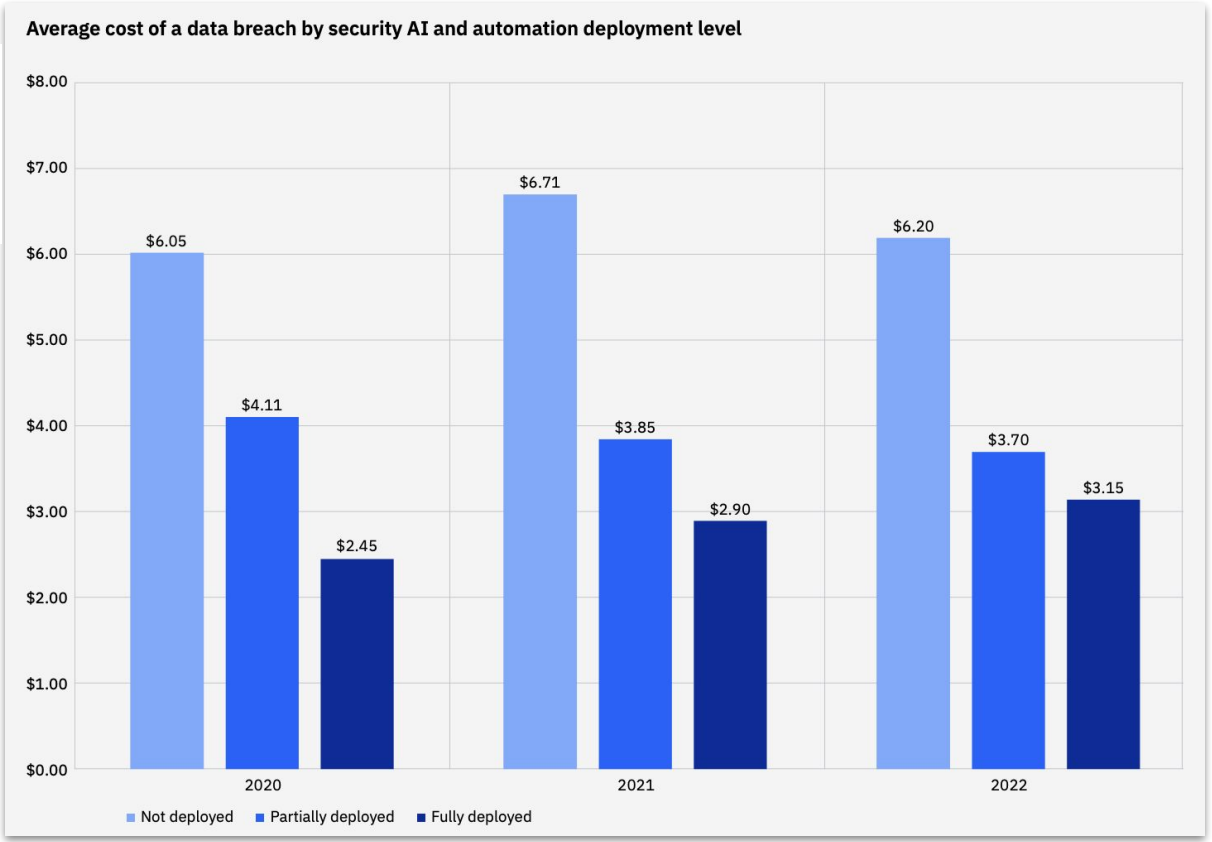
Average cost savings associated with fully deployed security AI and automation

83%

of organizations studied have had more than one data breach.

Therefore, minimum potential indirect costs savings with a fully deployed AI system =

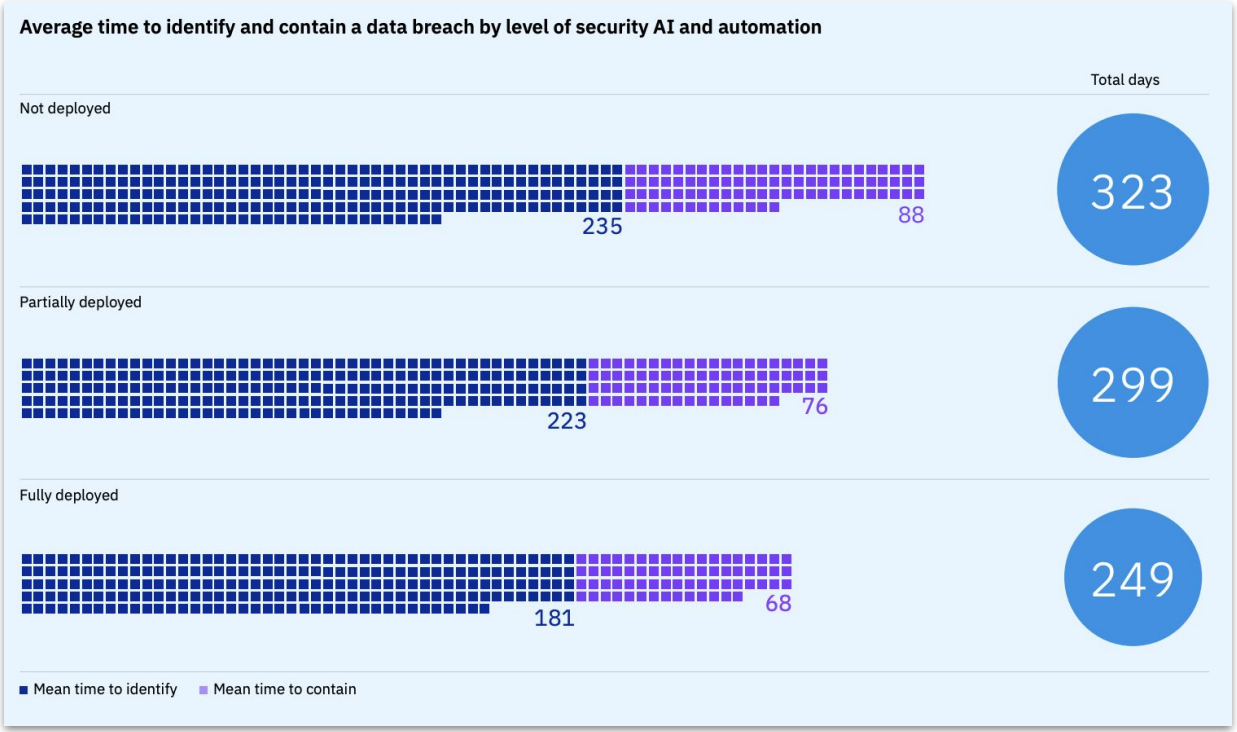
$6.1M



Source: IBM Cost of a data breach report 2022

Other benefits

- **Faster response:**
  Organizations with fully deployed security AI and automation were able to detect and contain a breach much more quickly.
- **Greater security talent retention:**
  Automated workflows will relieve our security professionals from monotonous work, boosting morale within the team
- **Better analytics for CISO's decisions:**
  Improved metrics and detailed reports will be available for our security leadership team to base their decisions.



Source: IBM Cost of a data breach report 2022

06 Conclusion

Conclusion

Security teams need to focus on 3 main actions:

- PROTECT
- DETECT
- RESPOND

These actions can be effectively tackled with AI implementation that comes with the requirements of:

AI Model requirements

TRAIN
Right data used for modeling

REMOVE BIAS
Model tested to remove bias

ROBUST
Tested for robustness

Results produced

ACCURATE
Higher accuracy in detection

ACCELERATED
Faster response to cyber attacks

AUTOMATED
Automation of tasks & responses

Thanks!

Shoot away with your questions.

References

- Accenture report: https://www.accenture.com/us-en/insights/artificial-intelligence/synthetic-data-speed-security-scale
- IBM 2022 report: https://www.ibm.com/reports/data-breach
- Cybercrime magazine https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/
- CNBC: https://www.cnbc.com/2022/09/13/
- Sailpoint article https://www.sailpoint.com/identity-library/how-ai-and-machine-learning-are-improving-cybersecurity/
- Youtube: https://www.youtube.com/watch?v=d31eg547Uuo
- Written statement from eric horvitz: https://www.erichorvitz.com/Testimony_Senate_AI_Cybersecurity_Eric_Horvitz.pdf
- Slide template: https://slidesgo.com/