AI meets security
Next-generation tools leverage ML

Fran Howarth

Practice leader security

AI or not?

- The stuff of science fiction?
- *"A task performed by a machine that would require a great deal of intelligence if performed by a human."*
- Subsets of AI include machine learning, deep learning, computer vision and natural language processing.

Machine learning

- The use of computers to run algorithms to undertake reasoning that was previously seen as the preserve of humans.
- Come up with better answers that humans can in far less time.
- Calculates the statistical validity of results — prioritise actions.
- Ability to learn from events for predictive capabilities.

How can it help in cybersecurity

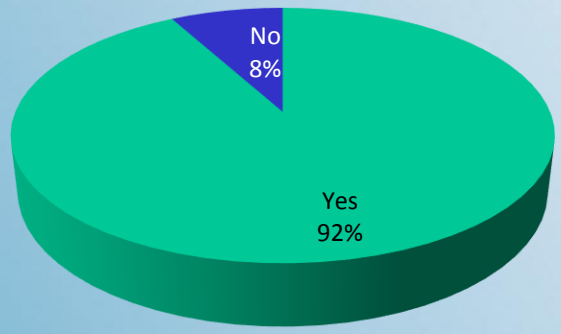
- Better defence against threats, breaches and attacks.
- SIEM was a good foundation, but…
- Provides a higher level of automation for cyber threat response systems.
- Capable of recognising patterns of behaviour and learning from them.
- Prevent, detect, respond.

Benefits of AI for cybersecurity

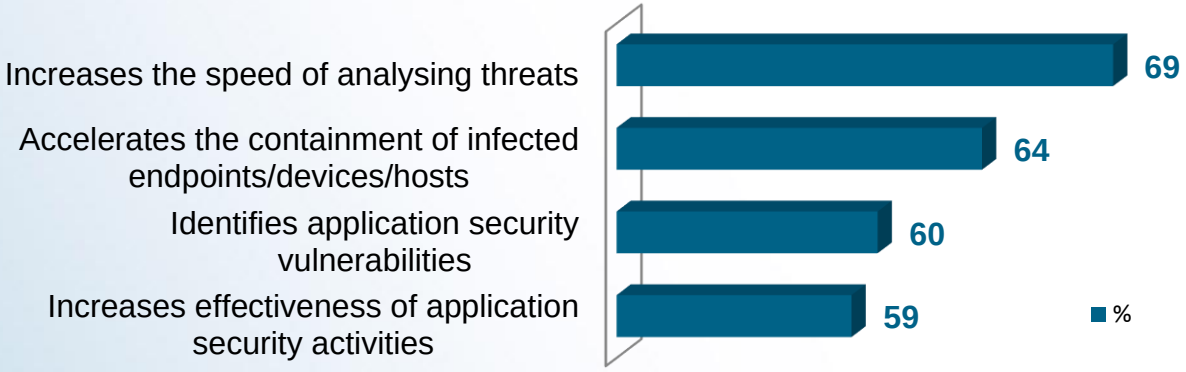
Source:
Osterman Research

Value of AI for cybersecurity

A comprehensive enterprise-wide AI strategy

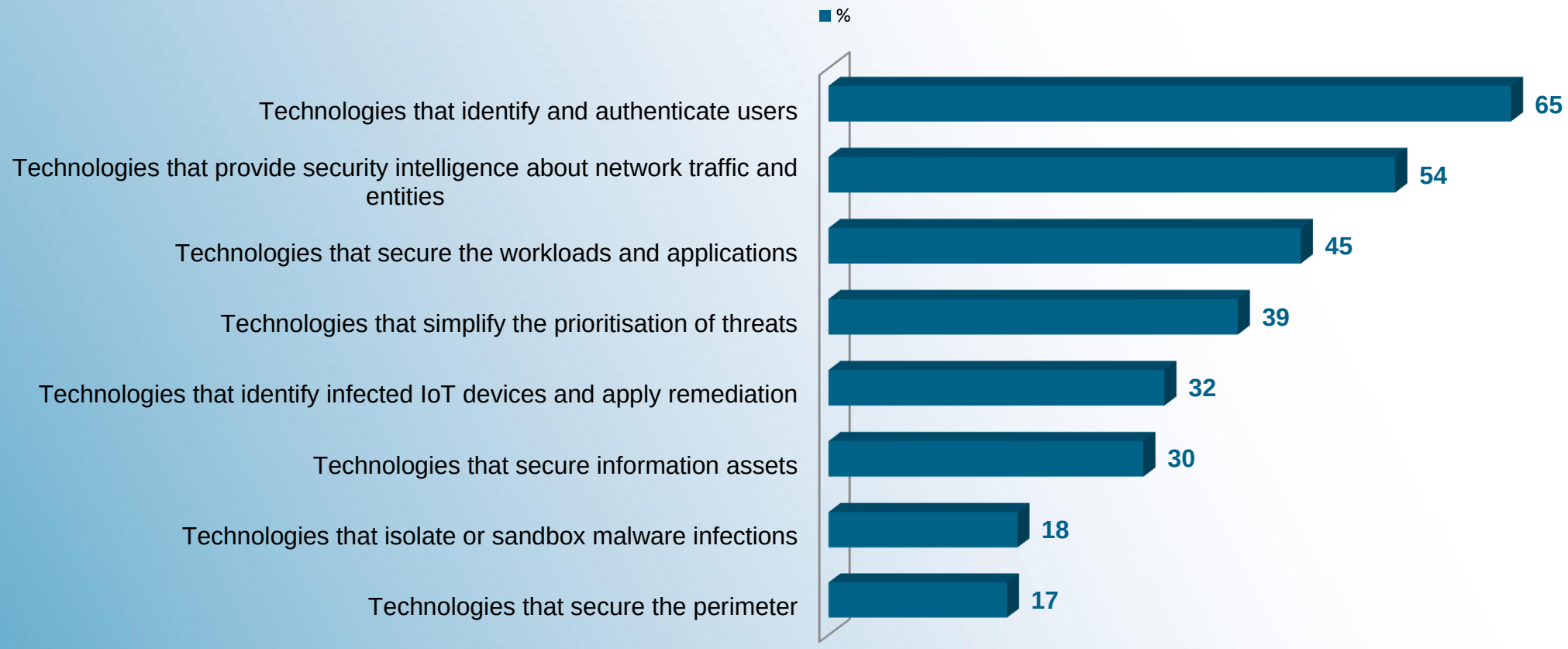


How AI improves security posture



Sources:
Forbes Insights, Ponemon Institute

Technologies used for AI in cybersecurity



Source:
Ponemon Institute

Behavioural analytics

- Focus on identifying patterns of behaviour that appear to be anomalous compared to baselines of expected behaviour.
- Provide detailed contextual information for greater visibility over what is actually happening.
- Weed out false positives, detect insider threats, prevent financial fraud.
- Conduct investigations faster.

SOAR

- Security orchestration, automation and response.
- Enables automation for improved incident response.
- Define, prioritise, standardise and automate incident response functions.

Limitations

- Quality of data
- Need to train system
- Complexity

Conclusions

- First step in the evolution of the use of AI in an evolving cybersecurity landscape.
- AI is no silver bullet.
- Quality will improve over time, with effort.