RSAConference2017
Abu Dhabi | 7–8 November | Emirates Palace

POWER OF OPPORTUNITY

SESSION ID: SPO2-T08A

Cutting through the AI Noise: How my prevention is better than yours

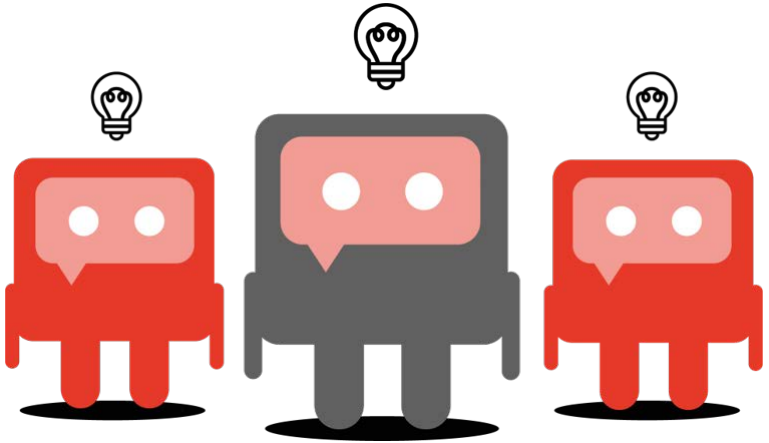
Sameh Sabry
Associate Vice President
Spire Solutions
@samehysabry

Welcome to RSA

- First product to use Deep Learning!
- AI-powered NGAV thwarts all cyber theft!
- Patented Machine Learning-based agent replaces the need for human analysts!
- Replace everything you have with pure math!
- AI sprinkles tiny magical unicorns all over your endpoints and makes your problems go away!

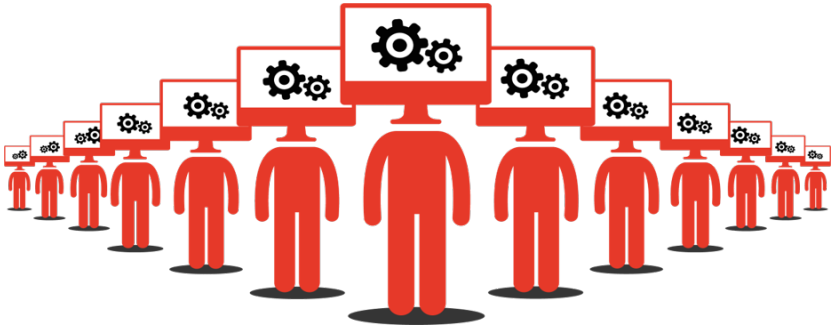
What is AI and Machine Learning?

- Artificial Intelligence is a machine acting in a way that seems smart
- Most applications in security refer to some aspect of Machine Learning, a branch of AI
  - Give a machine lots of data
  - Letting it learn how to predict things



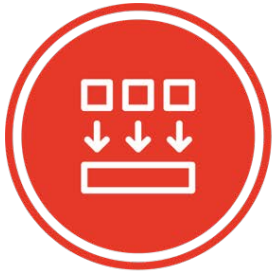
Common Misperceptions in Security

- AI drastically reduces the need for skilled employees
- AI is better than humans
- In AI, algorithms are the most important thing
- AI in security is all about detection



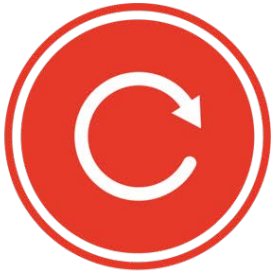
Advantages to Machine Learning in Security

Generalization



Scale & Automation

Infrequent Updates



Deep Insights

Transparency

Considerations when building and using ML

Garbage in, Garbage out

Burn-in Time

Misleading Metrics

Compute Requirements

Users Do Things

Overfitting

Bottom Line

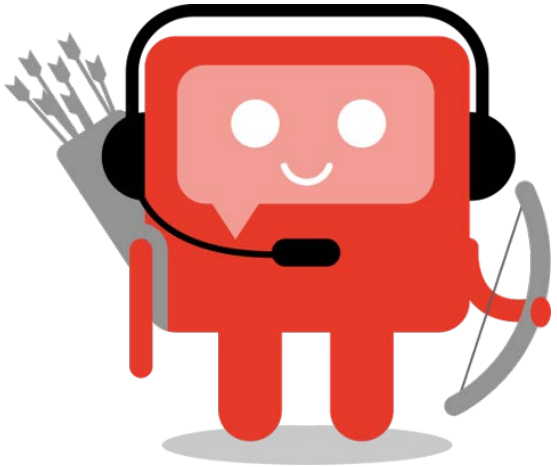
- AI/ML can be a powerful detection tool
- It is a challenge to do correctly
- Products can augment ML with known effective techniques
  - Heuristics
  - Runtime analysis (preferably inline)
  - Domain expertise

Is Detection Everything?

Is it even your biggest problem?

You need to know:

- How do I triage this?
- Is it actually bad?
- Where else is this?
- Where did this come from?
- What should I do about it?
- How should my teams collaborate?



Cutting through the Nonsense!

- Is AI/ML the answer to all our problems?
  - No
- Will AI replace all my employees?
  - No
- Is AI/ML always better?
  - No! No! No!
- Is AI/ML useful in security?
  - Yes!

Things to ask your vendor

- How are you generating these metrics and what do they mean?
- How do you incorporate domain knowledge and generalize to emergent threats?
- Has your detection been evaluated by a reputable third party?
- Why did you choose ML to solve this problem?
- Can I talk to a customer who has run this ML in a real environment?

RSA Conference 2017

Abu Dhabi

Thank You