MENA
INFORMATION SECURITY
CONFERENCE 2018

Leveraging Machine Learning & AI in Cyber Defense

James Blake

Operationalising Analytics

VIRTUPORT

@VirtuPortMEA

www.menaisc.com

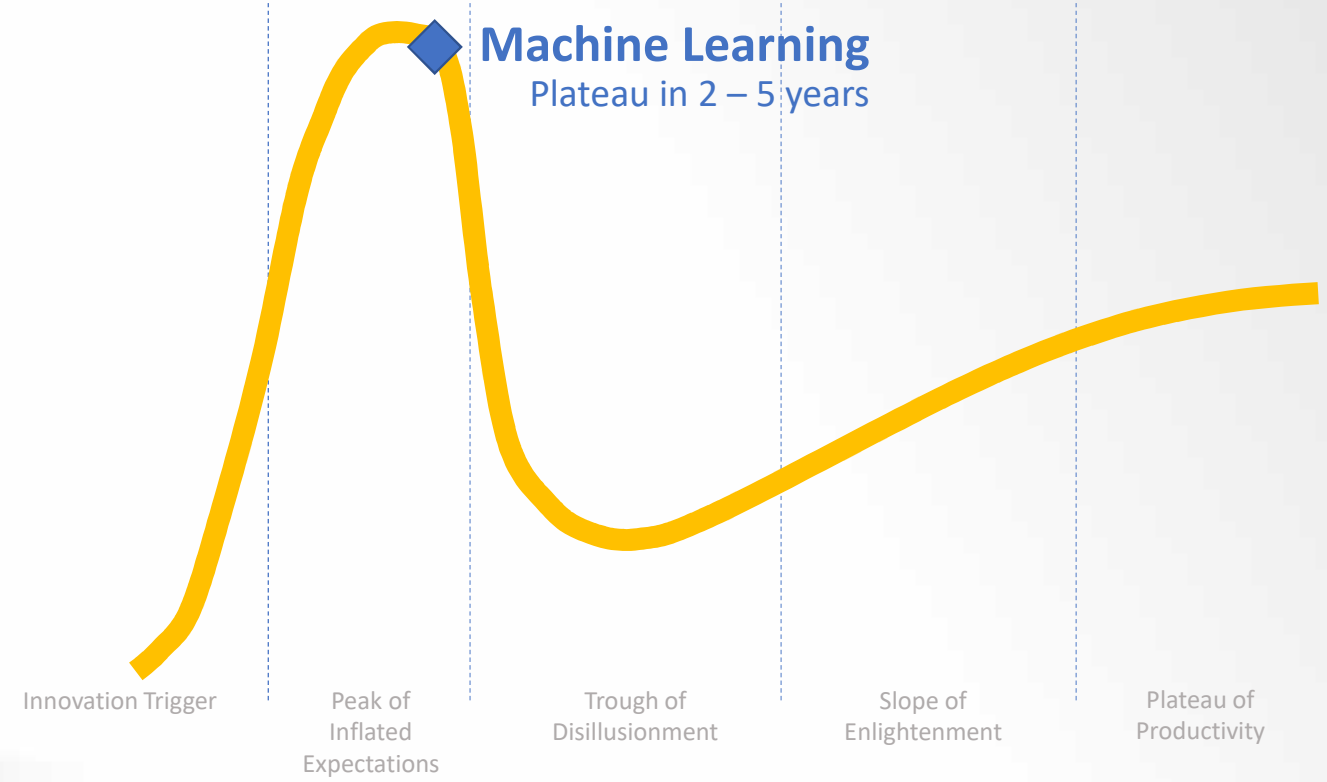
Dr James Blake GCIH CISSP CCSK CCISO CEH ITIL-F CCTIA CISM

- **Global Strategist, Micro Focus Cyber Security**
  Team built end-to-end cyber operations capability for 91 organisations. Evaluated over 200.
- **Former Global Head of Cyber Security Integration**
  JPMorgan Chase
- **Former Chief Information Security Officer**
  Mimecast
- Background in building and running operations, not product

MENA INFORMATION SECURITY CONFERENCE 2018

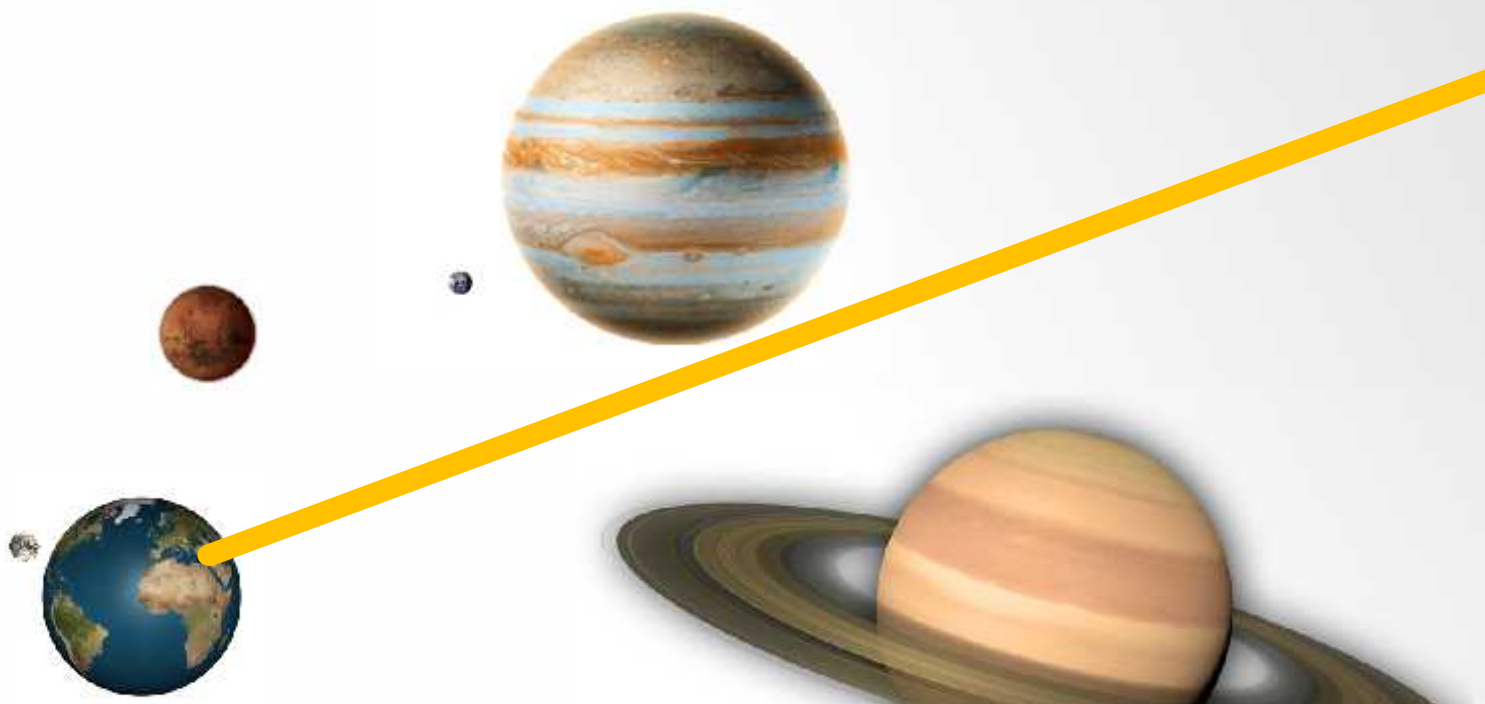
- **Enabling technology, not a product**
- **Not New**
- **Trust us, because math**
- **Lots of marketing, little detail**

Gartner Machine Learning Hype Cycle



Source: Gartner Hype Cycle 2017

Machine Learning Hype Cycle: Reality



Dr. Anton Chuvakin

Gartner

Research Vice President and Distinguished Analyst

“Q: How do you know that a security vendor REALLY uses AI in their product?

A: If they say they do it, then you know they don’t.”

"Not only [machine learning] can be wrong, but it's also harder to ascertain, and, as people say in security, harder to triage what it means. Are we in real trouble? Are we in, somewhat of a trouble or are we not in trouble at all?"

"Not only are the systems not always explainable, but to actually tune the product to operate effectively, you have to have skills that most security operations teams don't have."

Bruce Schneier

NYT Best Selling Author / CTO Resilient

Resilient
an IBM Company

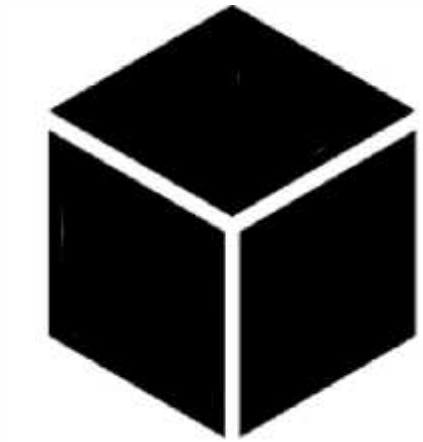
“You can only automate what you're certain about, and there is still an enormous amount of uncertainty in cybersecurity. Automation has its place in incident response, but the focus needs to be on making the people effective, not on replacing them

"Incident response needs to be dynamic and agile, because you are never certain and there is an adaptive, malicious adversary on the other end. You need a response system that has human controls and can modify itself on the fly. Automation just doesn't allow a system to do that to the extent that's needed in today's environment."

PRODUCT

PLATFORM

Black-Box Analytics Products



+ Quick(er) to deploy

- What algorithms?

- Limited tuning opportunities

- Reliant on vendor to adapt

- Often focused on one problem statement

- **May alert in isolation**
  - **…or you could still use a SIEM and/or SOAR platform**
- **Still needs Analysts (called ICE now)**

White-Box Analytics Platforms

+ Full control over algorithm choice

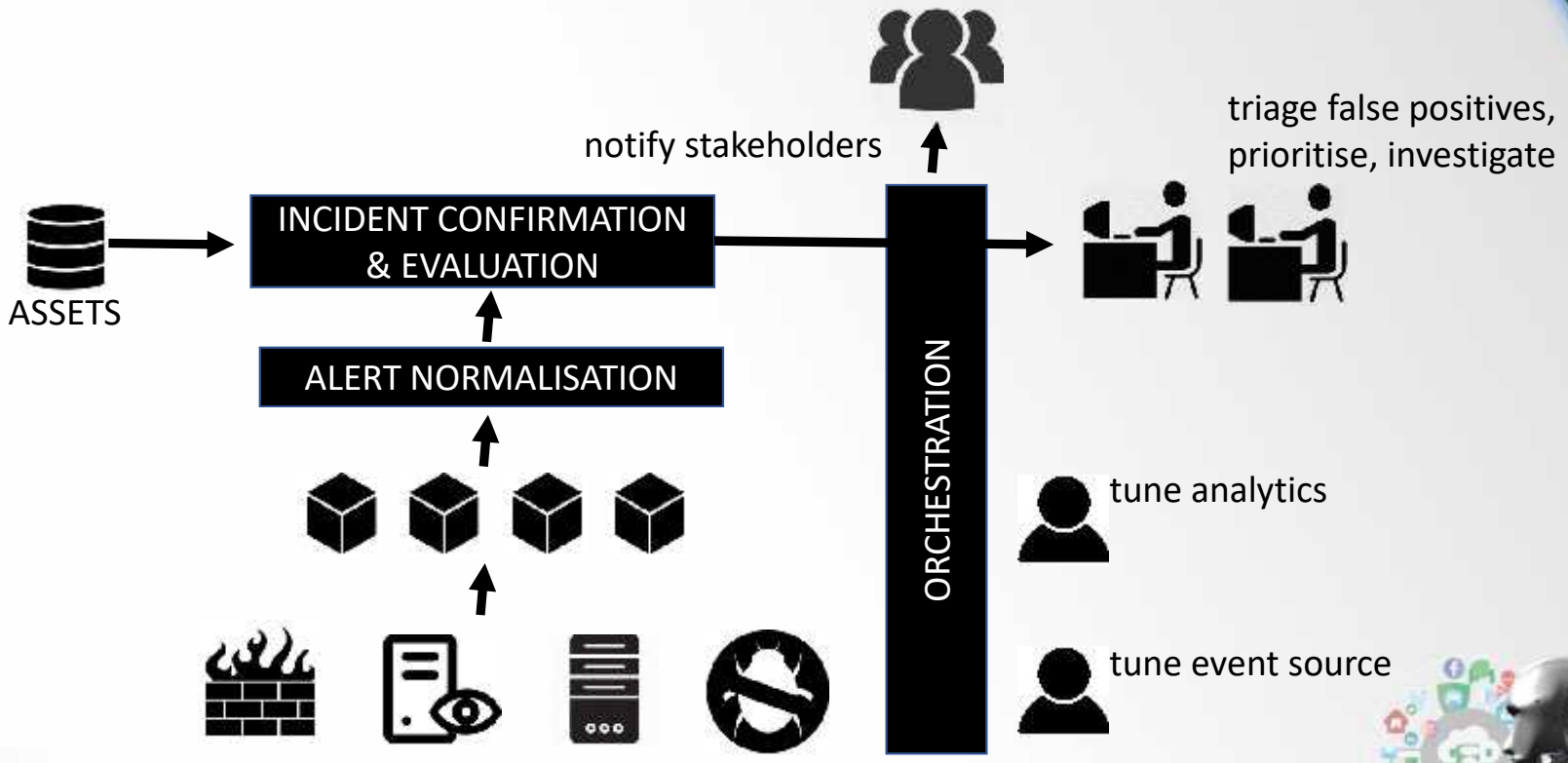
+ Full tuning capability

+ One platform for multiple problem statements

+ Alert to a common taxonomy

- Needs hard-to-find Data Science expertise

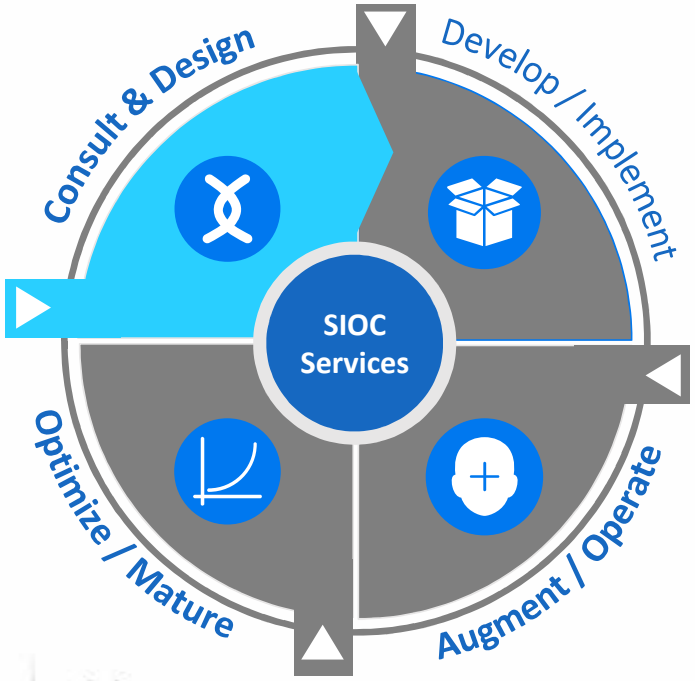
There is still process, people and technology



Avoiding the trough

- Focus on **operational outcomes**, not technology
- Think about **all** your technology in a holistic way
- Ensure you have the right **skills** and **processes** in place
- Even with Machine Learning you can't avoid
  - understanding your **business**
  - understanding your **assets**
  - understanding your **adversaries**

Micro Focus



MENA INFORMATION SECURITY CONFERENCE 2018

Experience

The **most experienced consultancy team** in the World for building and maturing **Security Intelligence & Operations** capabilities, encompassing **Threat Intelligence**, **Hunt Teams**, **Machine Learning Analytics, Analysis** and **Incident Response**, for customers in all verticals.

- > 93 SOCs and MSSPs built end-to-end, operated & transferred
- > 215 SOCs and MSSPs assessed and transformed

Expertise

- 65+ Consultants globally
- Over 275 years of cumulative operational SOC experience
- Operational experience in every vertical market

Methodology

- Proven **methodology** & extensive **intellectual capital**
- **Accelerate time-to-value** and **de-risk** SOC projects
- **Unlock demonstrable value** in existing SIEM & SOC investments
- **Capability**, not technology, **focused**

MENA
INFORMATION SECURITY
CONFERENCE 2018

Leveraging Machine Learning &
AI in Cyber Defense

Q&A

VIRTUPORT

@VirtuPortMEA

www.menaisc.com