MIS|TI™ PRESENTS InfoSecWorld Conference & Expo 2018

THE NEW ERA OF CYBER THREATS:
THE SHIFT TO SELF-LEARNING, SELF-DEFENDING NETWORKS

Cameron Armstrong
Regional Director
Darktrace

EVOLVING THREATS IN A NEW BUSINESS LANDSCAPE

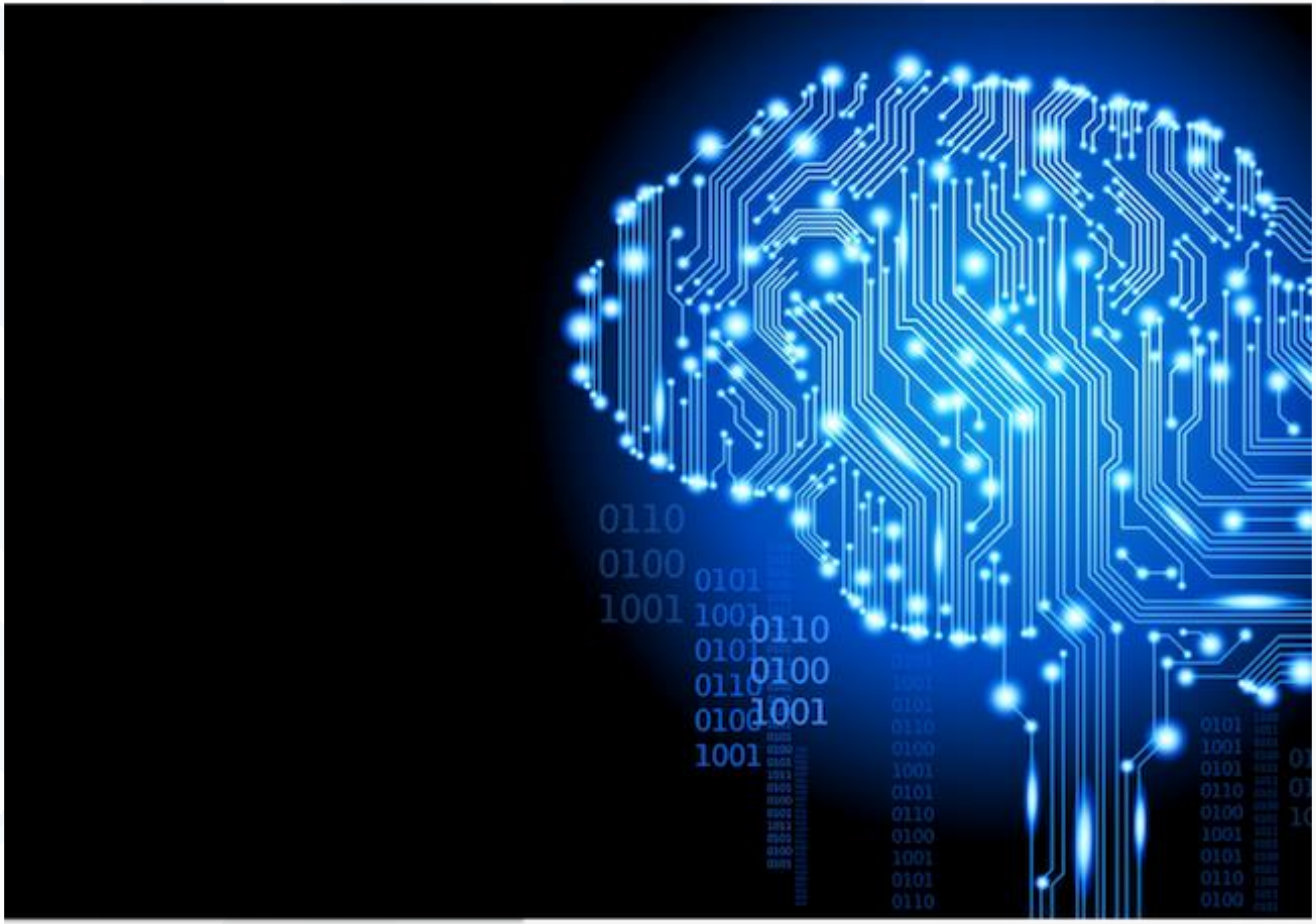
- Outsourced IT, SaaS, cloud, virtual, supply chain, IoT
- Not just data breaches and defaced websites
- Insider threat –malicious and non-malicious
- ‘Trust attacks’ are silent and stealthy
- AI attacks are emerging, leading to highly customized campaigns
- Machine on machine attacks

TRUST ATTACKS

- ‘Trust attacks’ seek to undermine data integrity
- Characterized by stealth and sophistication
- Seek to manipulate rather than exfiltrate data
- Threat to reputation and stability

AI ATTACKS

- Observe a network in order to blend into the background
- Automatically exploit zero-day vulnerabilities
- Emergence of metamorphic attacks – algorithms fighting algorithms
- Infiltrate malware classification training sets
- Battle is now taking place inside the network



RANSOMWARE ATTACKS

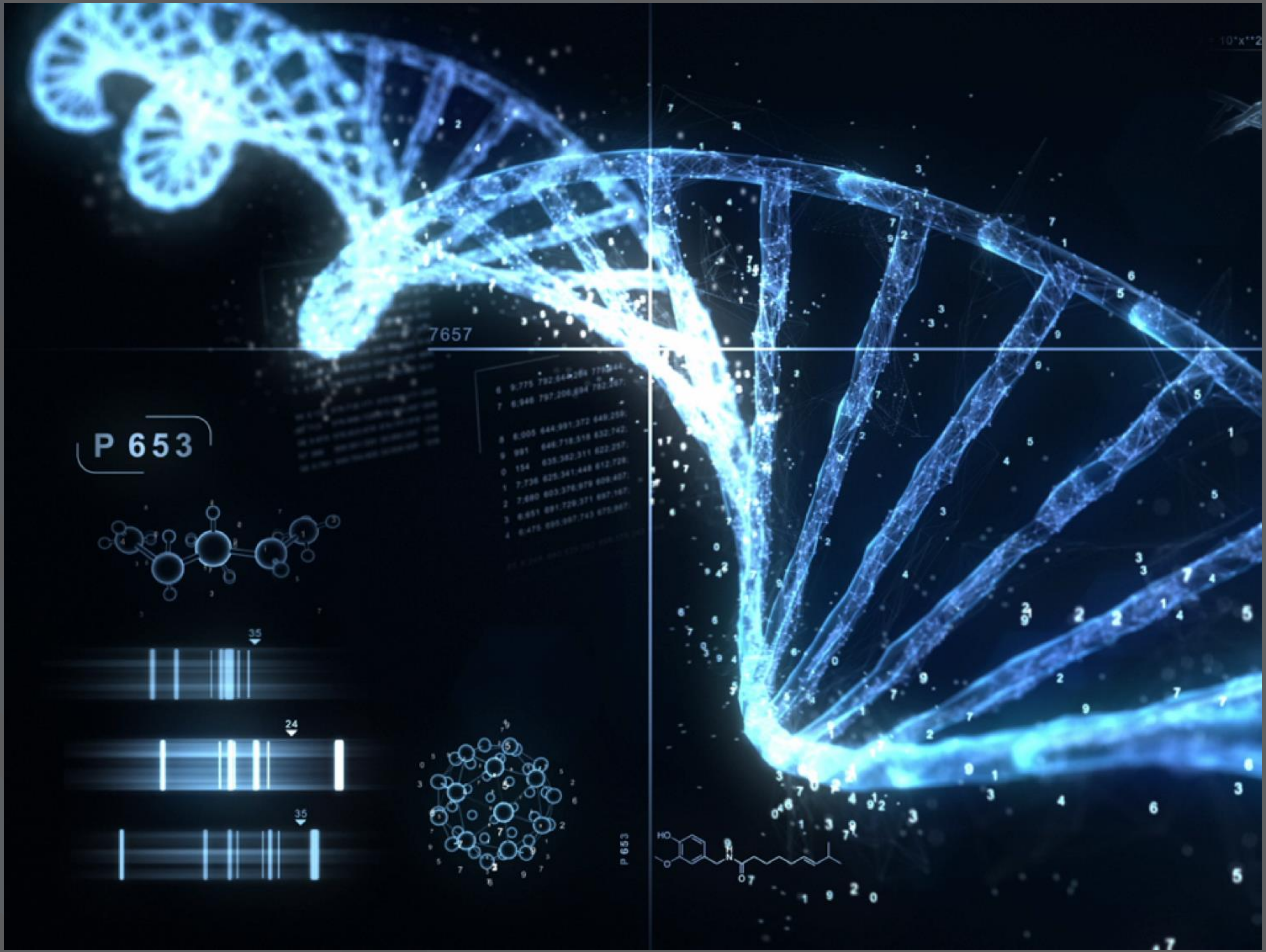
- Capable of encrypting an entire network in a matter of minutes

- Human security teams cannot keep up with such fast-moving attacks

- Autonomous response has become vital in today’s threat landscape

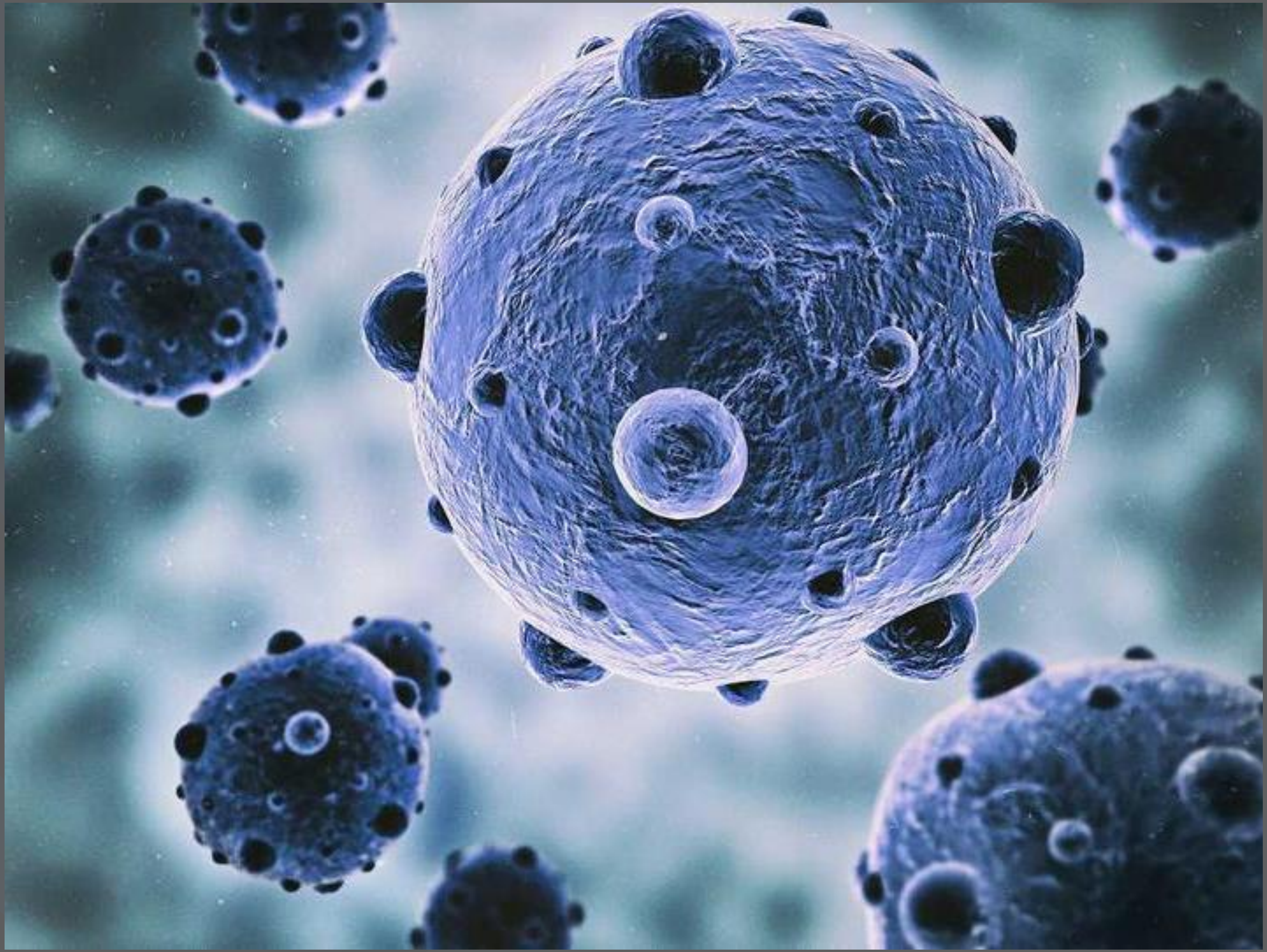
A NEW APPROACH IS NEEDED

- Legacy tools are being constantly outpaced
- Tools that rely on rules and signatures can’t catch never before seen threats
- IoT expanding endpoint
- Security teams struggling to keep up with fast-moving threats



AUTONOMOUS RESPONSE

- Automatically produces real-time active responses to potential threats
- Does not rely on predefined signatures or prior knowledge
- Slows down or stops the progress of novel threats within the network
- Gives security team critical time to catch up



MACHINE LEARNING IS HARD TO GET RIGHT

- Cannot rely on training sets of data
- Needs to work without customer configuration or tuning of models
- No AI expertise necessary
- Must deliver value immediately, but keep learning and adapting as it goes
- Can work remotely and support small form factors

EVALUATING MACHINE LEARNING TECHNOLOGY

- What does the machine learning do?

- Is the technology proven? Who uses it?
-
- Do you need the mathematicians to support it?

- Is machine learning at the technology’s core or used as a feature?

- Does it require model tuning?
-

  Can it be used on premises and in the cloud?

AUGMENTING & AUTOMATING THE ANALYST

- Introducing supervised machine learning and deep learning
- Continued research and development into automating and assisting the human analyst
- Classify unusual activity into benign or potential threat
- Perform greater analysis of multiple weak indicators to raise increasingly subtle threats above the threshold

Alamy

CASE STUDY:

A smart fish tank left a casino vulnerable to hackers

- "Someone used the fish tank to get into the network, and once they were in the fish tank, they scanned and found other vulnerabilities and moved laterally to other places in the network."

- High-end fish tank configured to use an individual VPN

- Transfer of 10GB outside the network was deemed highly unusual by Darktrace's AI algorithms

- This was a clear case of data exfiltration, but more subtle than typical attempts at data theft

CASE STUDY:

Data Exfiltration from Video Conferencing Device

- This device was the only internal computer connecting externally via Telnet
- The anomalously large volumes of information were uploaded to six rare external computers
- A back-door Trojan had been uploaded to the device before Darktrace was installed
- External servers that the company otherwise never contacted were connecting to the camera via FTP, Telnet and HTTP

[80]
CHAIN OF ANOMALIES:
PUBLIC WEB EXPOSURE
DATA TRANSFER
TRANSFER DESTINATION

CASE STUDY:

Autonomous Response Against Ransomware

- Employee circumvented corporate policy to check her personal email
- Inadvertently downloaded a malicious ZIP file containing a ransomware payload

CASE STUDY:

Internal Data Theft From the Cloud

- Customer database held on a third-party cloud to enable flexible working and reduce costs
- IT manager downloaded contact details and credit card numbers, then transfers to a home server
- The employee was likely intending to sell the information for a substantial profit

Customer Database
CREDIT CARD
0000 1234 6789 1011
HERE TO HELP

Q&A

MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!