

Practical Applications of AI in Cybersecurity — Threat Detection, Prevention, Containment and Response

Rik Turner

Principal Analyst, Infrastructure Solutions

Ovum

rik.turner@ovum.com

What's going on in Cybersecurity?

1990s

2000s

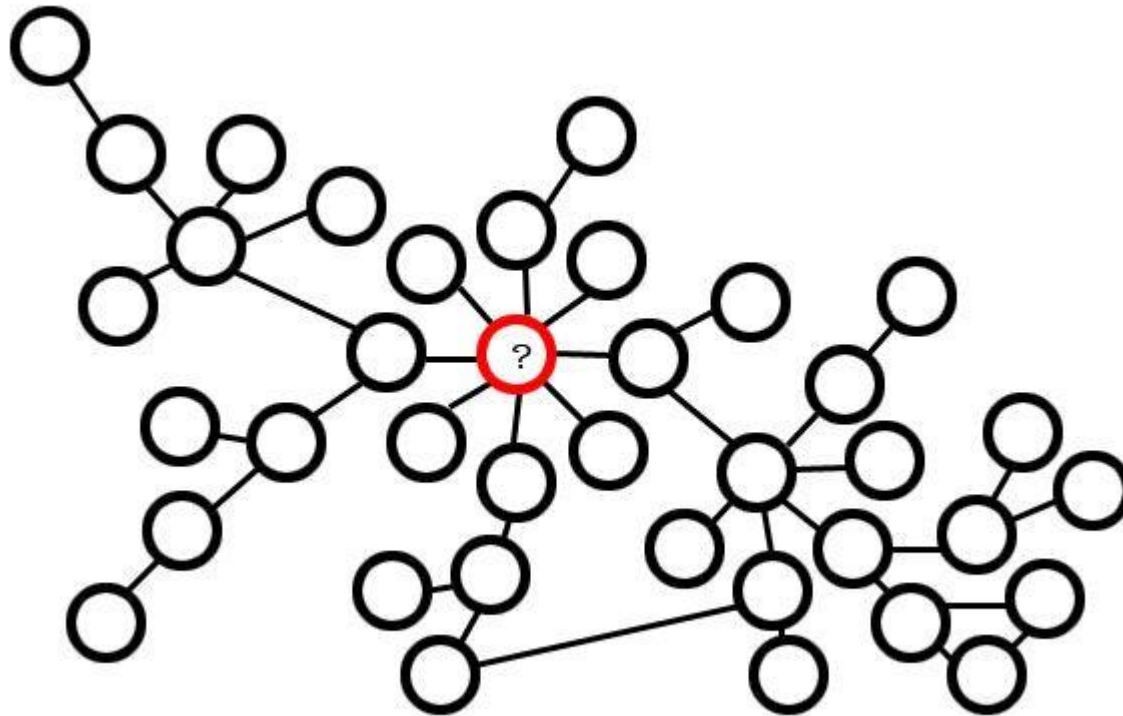
2010s

PREVENT

**DETECT,
MITIGATE &
REMEDiate**



The Signatures-based Paradigm



Find Patient Zero...



The Signatures-based Paradigm



Create an antidote (i.e. a signature)...



The Signatures-based Paradigm

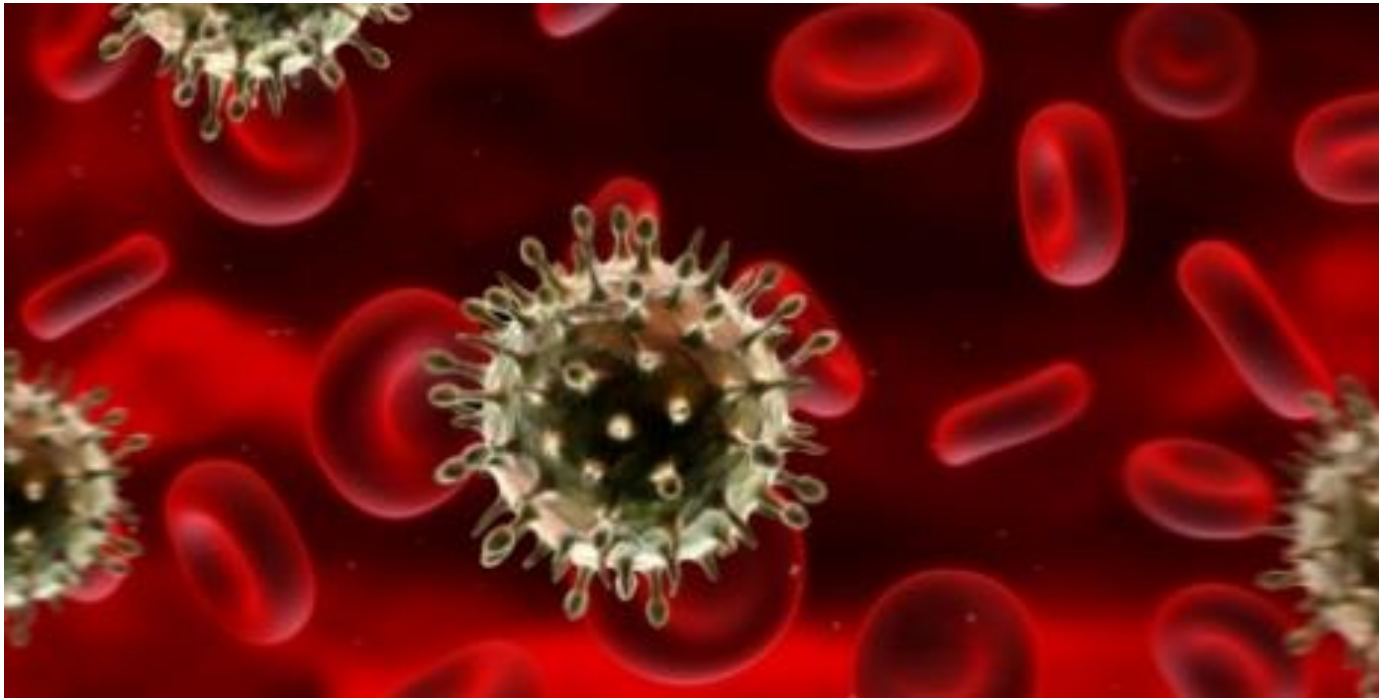


...and disseminate to immunise all other machines



But now...

Anti-virus signatures catch no more than 30%-40% of malwares



Why?

- **Many more malware actors:**

Criminal gangs

Hacktivists

State-sponsored groups

- **An active market for malware on the Dark Web**
- **The Cloud**



So now... **NEW DETECTION TECHNOLOGIES**

Sandboxing



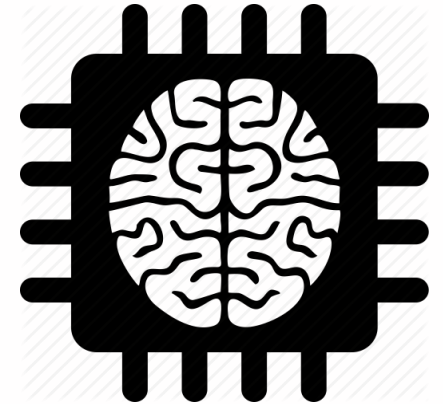
UEBA



EDR

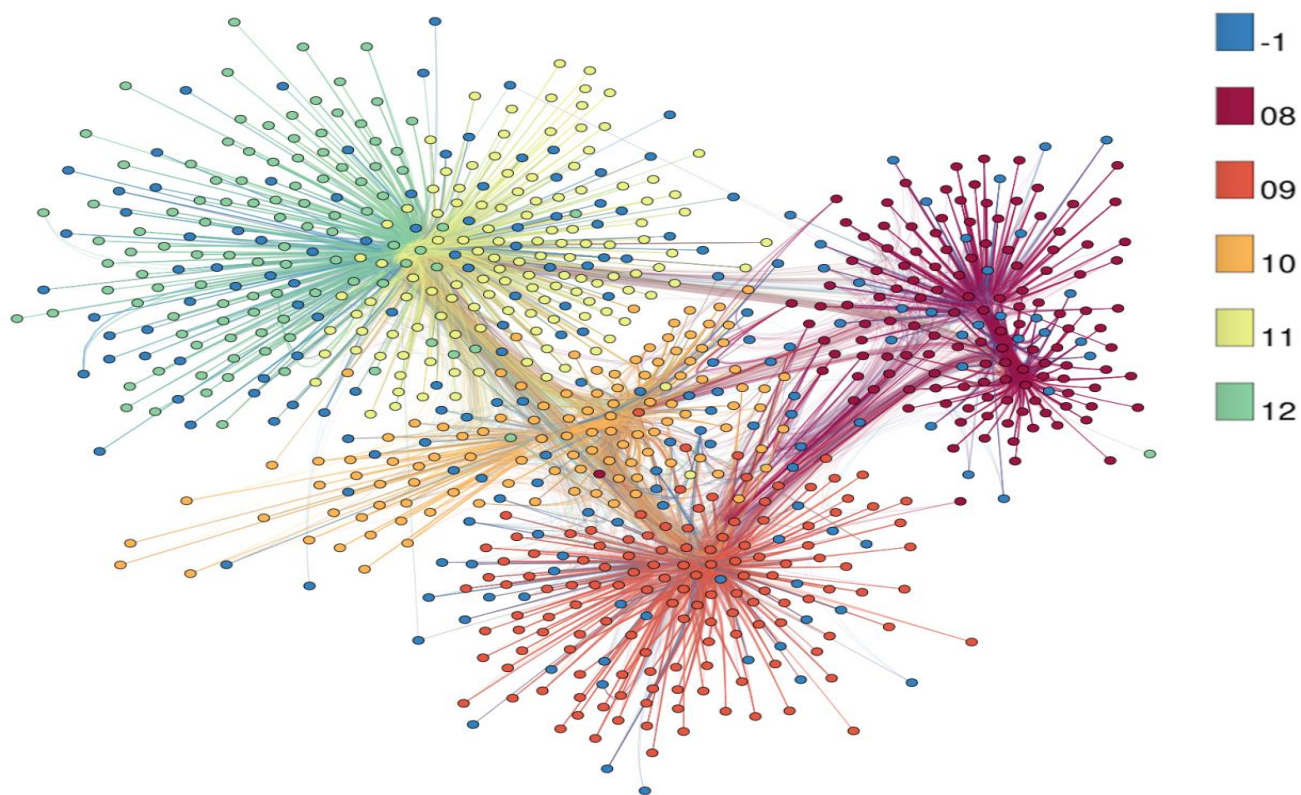


AI / Machine Learning



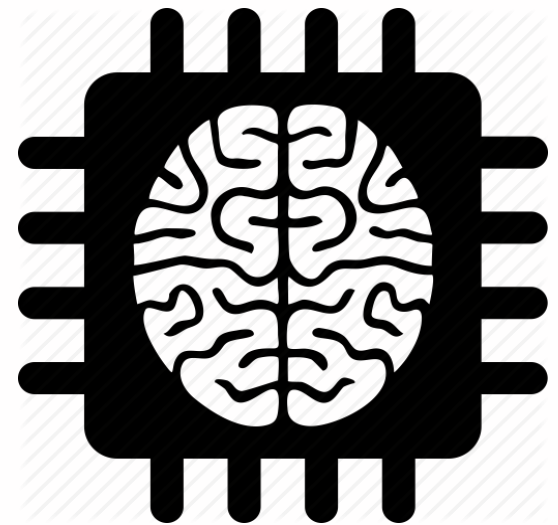
NEW DETECTION TECHNOLOGIES (cont'd)...

Threat Intelligence



Tasks for AI/Machine Learning in Cybersecurity

1. Model “Normal” to Alert on “Abnormal”
2. Filter out the noise in Threat Intel
3. Find hidden trends



Copyright notice and disclaimer

The contents of this product are protected by international copyright laws, database rights and other intellectual property rights. The owner of these rights is Informa Telecoms and Media Limited, our affiliates or other third party licensors. All product and company names and logos contained within or appearing on this product are the trademarks, service marks or trading names of their respective owners, including Informa Telecoms and Media Limited. This product may not be copied, reproduced, distributed or transmitted in any form or by any means without the prior permission of Informa Telecoms and Media Limited.

Whilst reasonable efforts have been made to ensure that the information and content of this product was correct as at the date of first publication, neither Informa Telecoms and Media Limited nor any person engaged or employed by Informa Telecoms and Media Limited accepts any liability for any errors, omissions or other inaccuracies. Readers should independently verify any facts and figures as no liability can be accepted in this regard - readers assume full responsibility and risk accordingly for their use of such information and content.

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Informa Telecoms and Media Limited.

