Ovum

TMT intelligence | informa

Cybersecurity – from Reactive to Predictive

Rik Turner

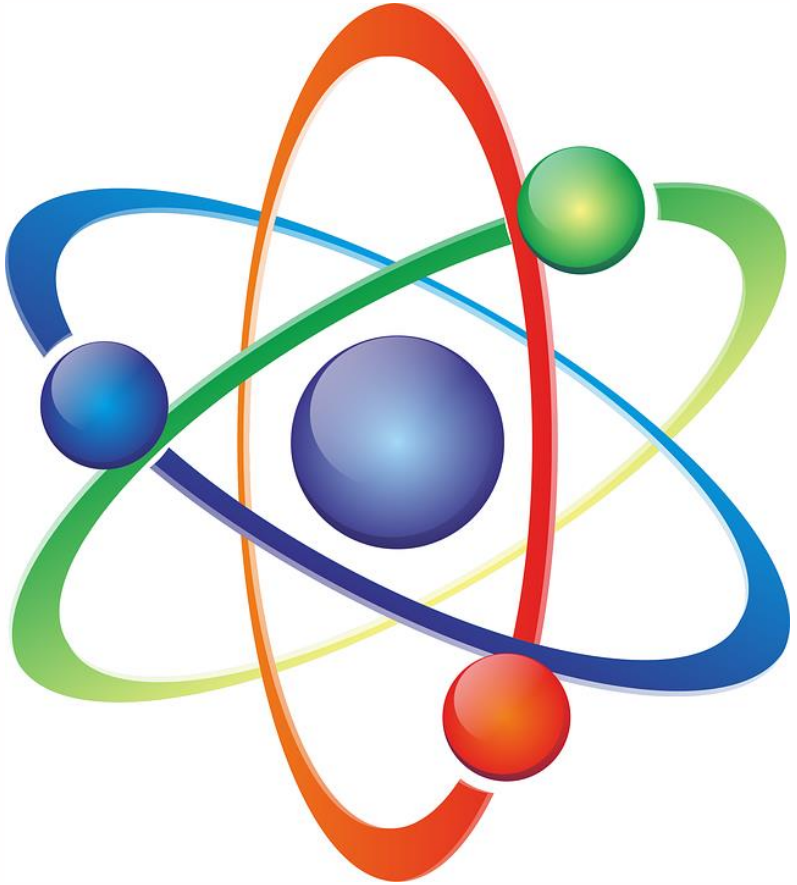
Principal Analyst

Infrastructure Solutions

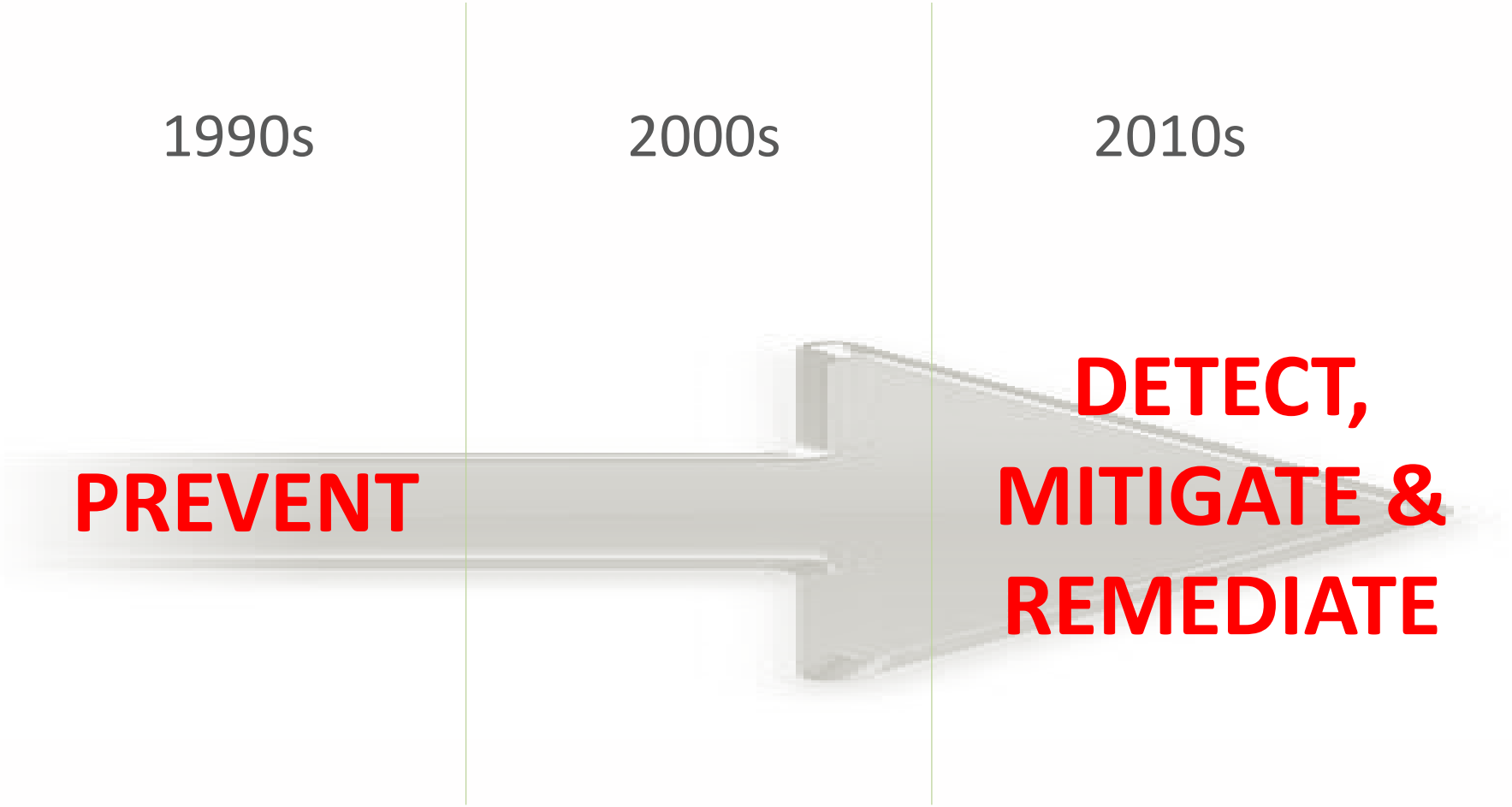
Ovum

Agenda

1. Where We Are Now
2. What Has Changed
3. Tech Responses
4. Prediction

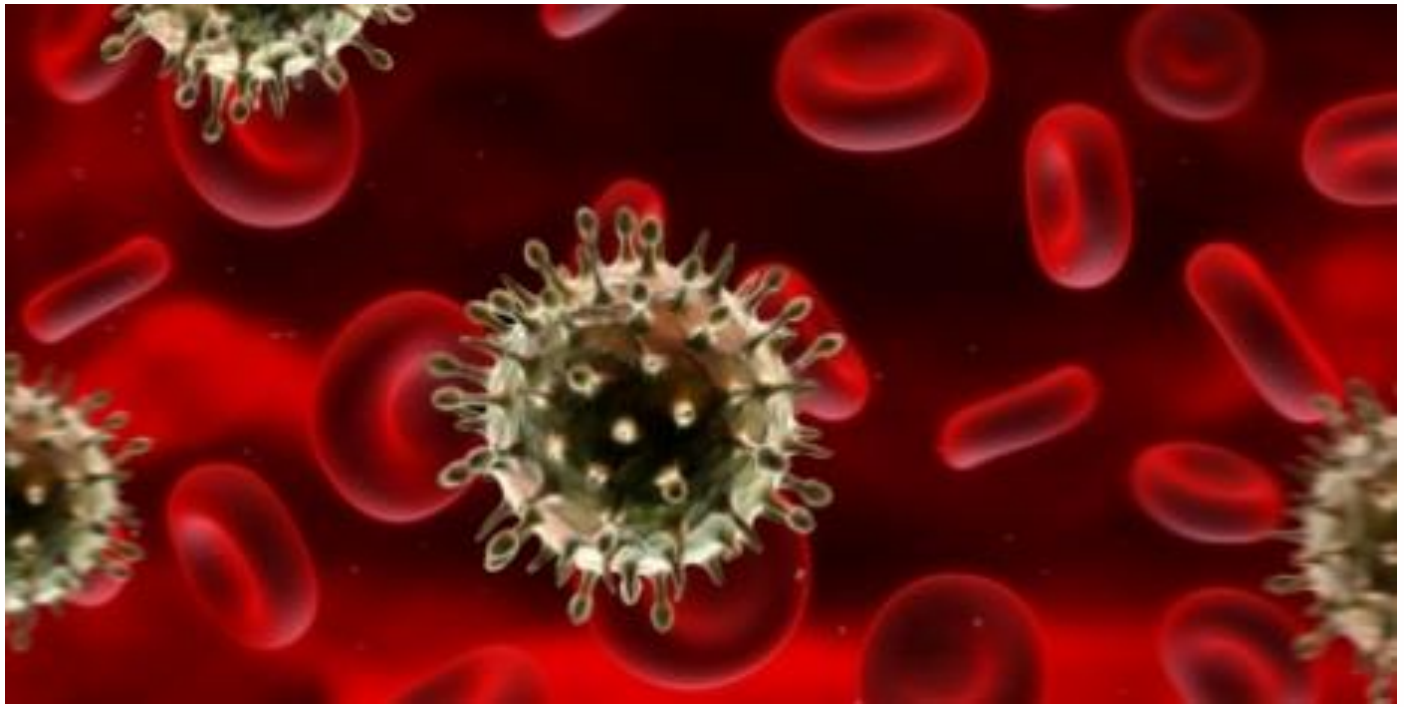


Where we are now in Cybersecurity



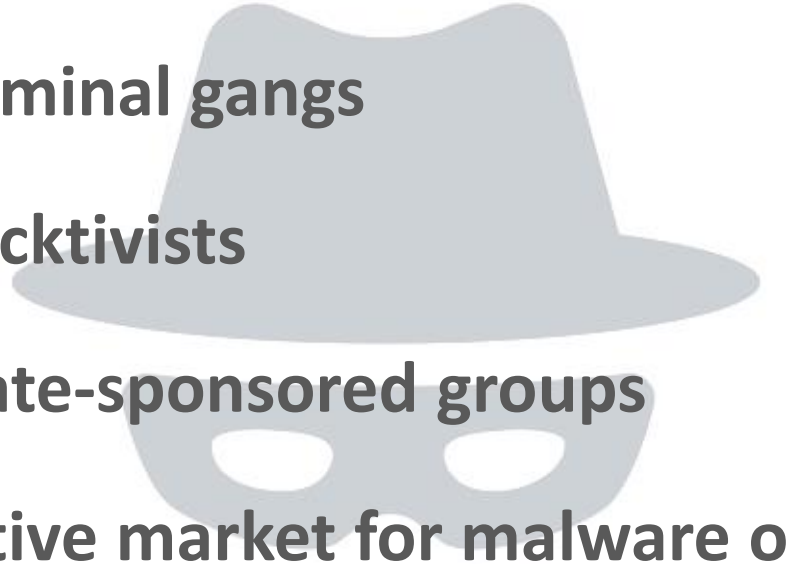
What has changed - Signatures on the wane

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



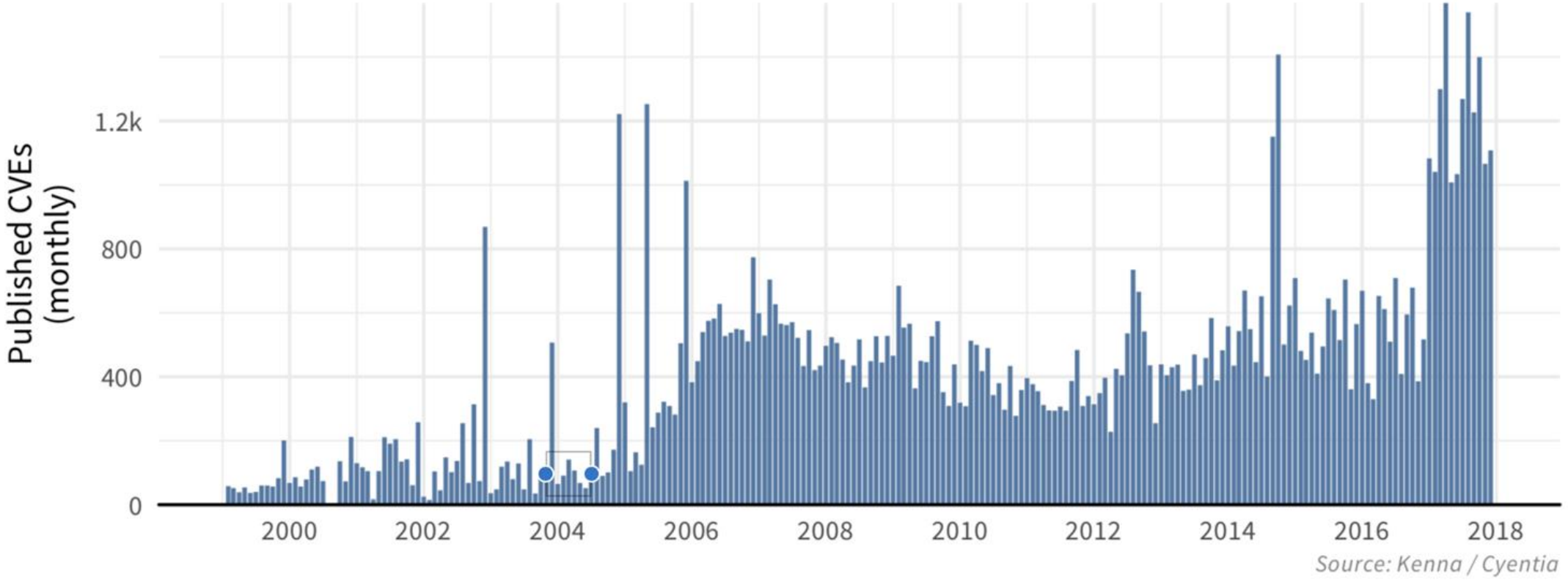
What has changed - Why?

- **Many more malware actors:**
  - **Criminal gangs**
  - **Hacktivists**
  - **State-sponsored groups**
- **An active market for malware on the Dark Web**
- **The Cloud**



What has changed - Vulnerability Volume increasing

Volume of published CVEs from 1999 through 2017



[1]For discussion of these biases and other CVE-related issues, see 2013 BlackHat presentation titled "Buying into the Bias: Why Vulnerability Statistics Suck" from Brian Martin and Steve Christy.

What has changed - Attack Velocity increasing

Average Days from
Publish to Exploit

(639 / 8%):

19.68

Days

Average Days from
Publish to Event

(36 / 0.5%):

27.36

Days

Shortest Average Window:
Adobe Reader (days)

Longest Average Window:
IE Edge (months)

Tech responses - New Detection Technologies

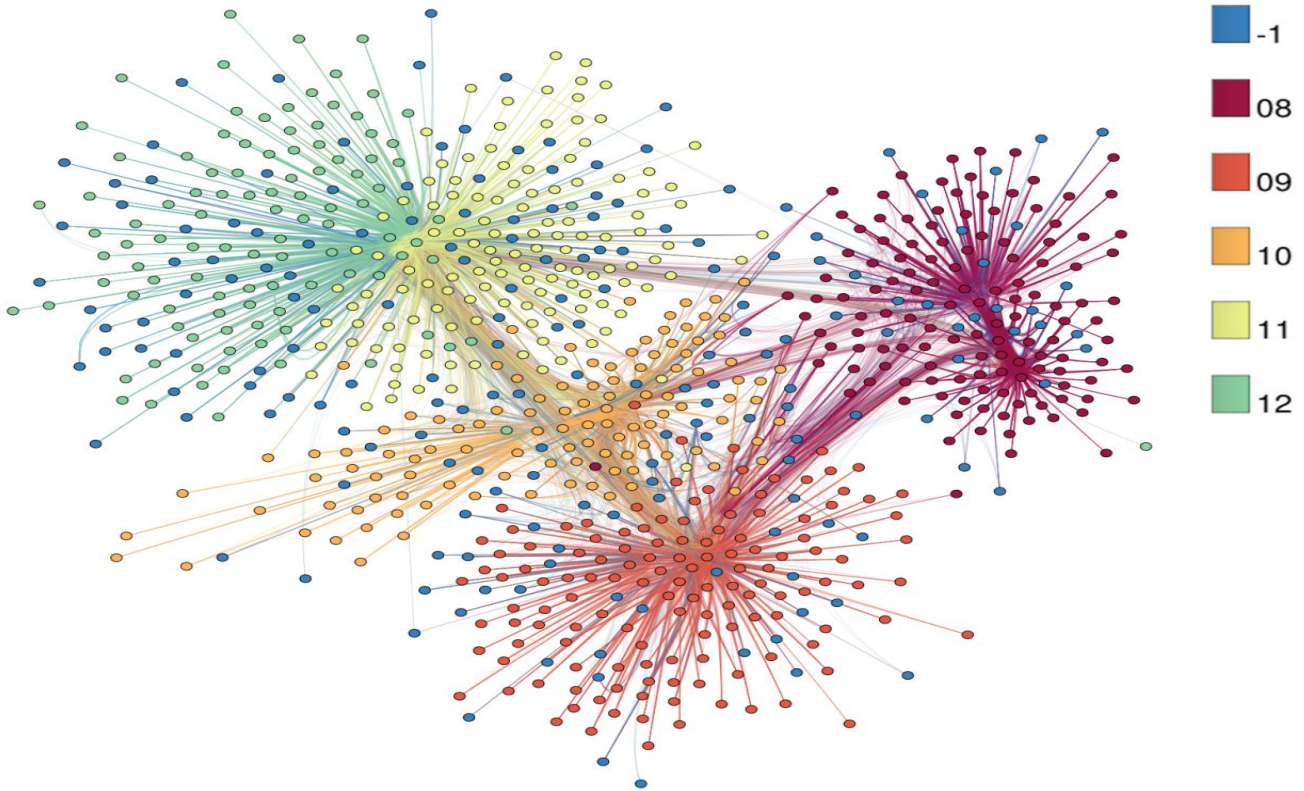
Sandboxing

UEBA

EDR

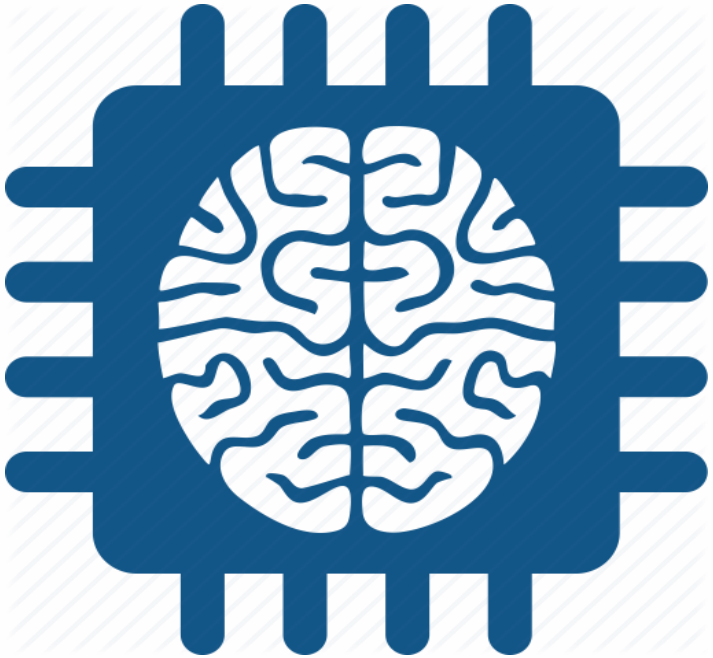
Tech responses

Threat Intelligence



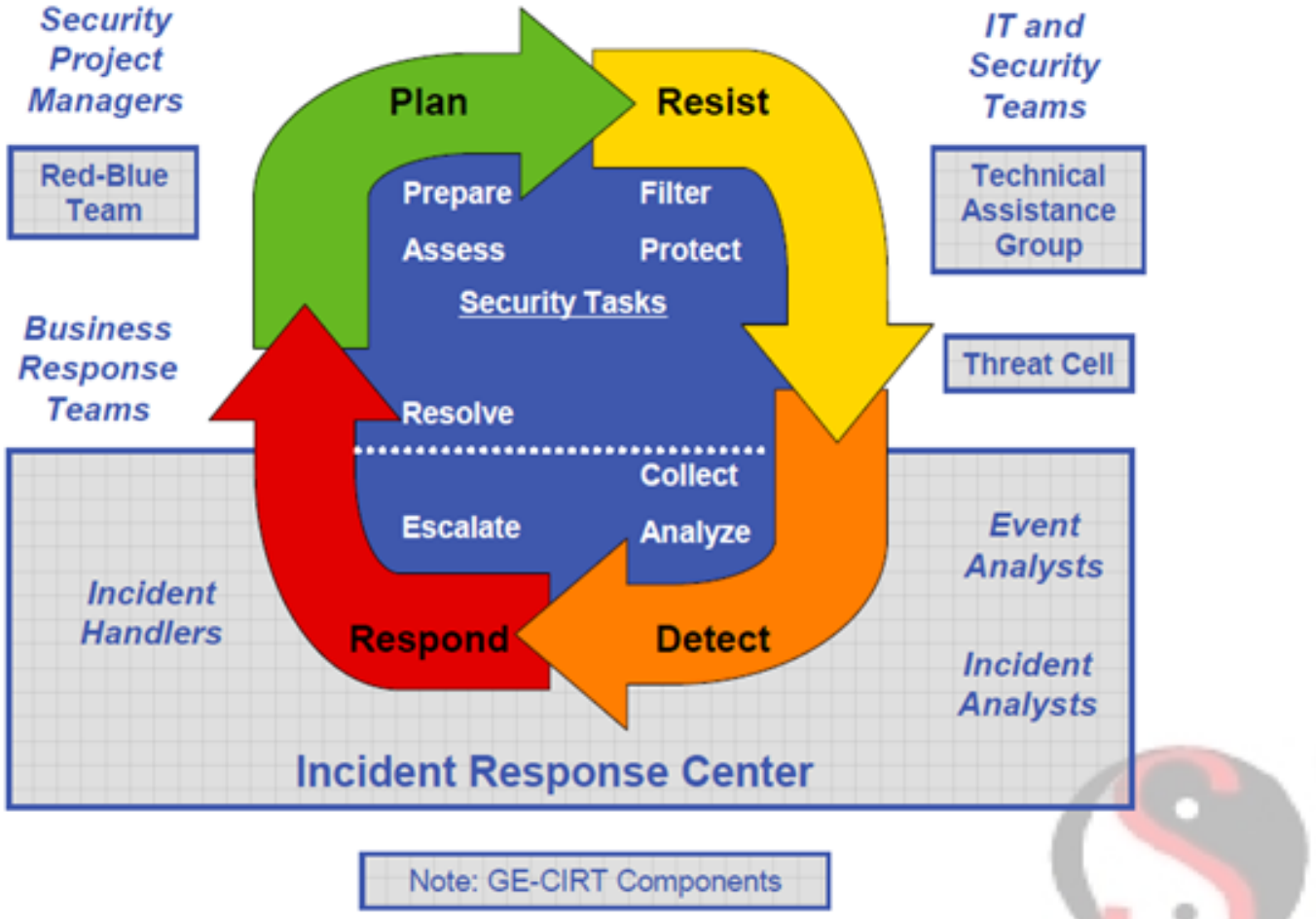
Tech responses

AI / Machine Learning



The Evolution of Incident Response

SOAR tools etc..



Source: Richard Bejtlich, *CIRT-Level Response to Advanced Persistent Threat*

Less clairvoyance…

Prediction

…more Data Science