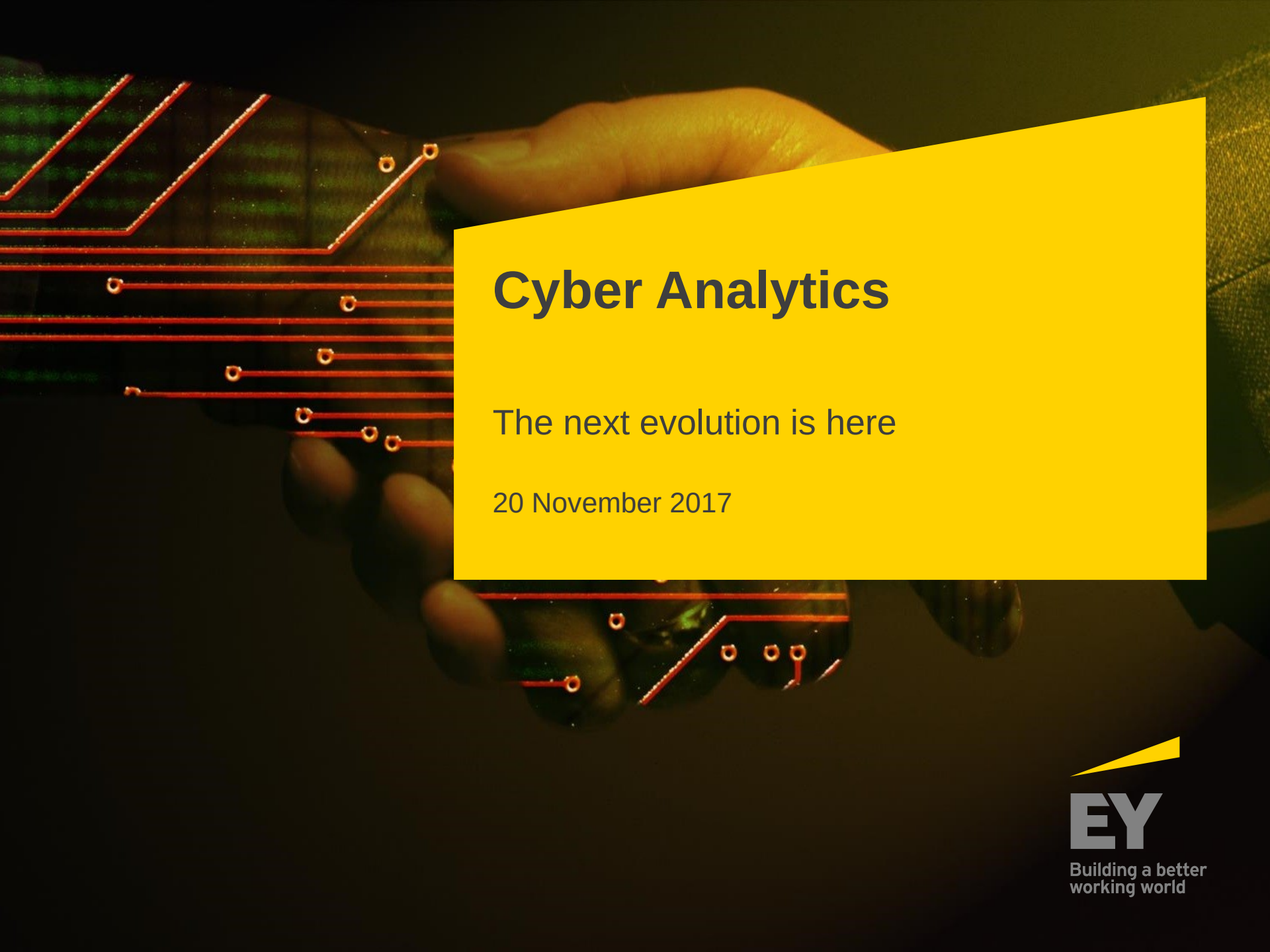


Cyber Analytics

The next evolution is here

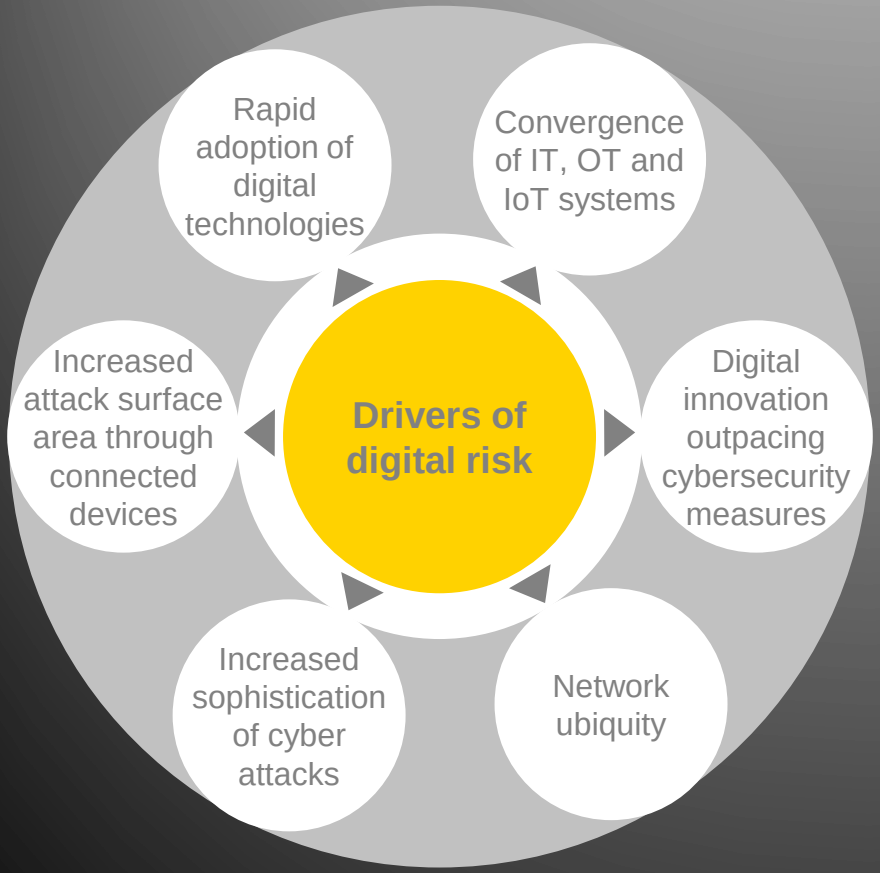
20 November 2017

Building a better working world

Digital transformation

The rapid adoption of digital increase your exposure to cyber attacks

- Digital transparency and assurance is key; enabled through continuous monitoring



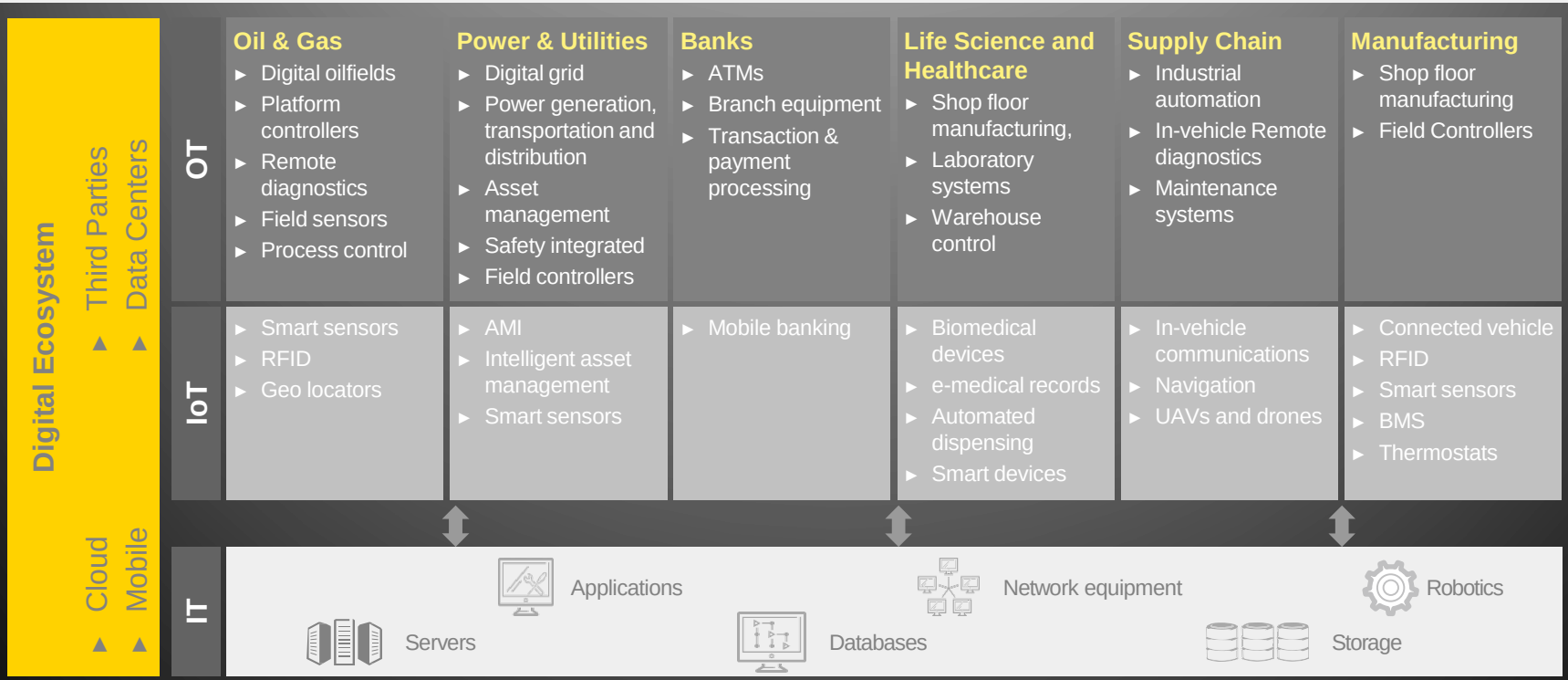
Measures to address digital risk

- Ecosystem visibility
- Digital risk governance
- Understand threat environment
- Cyber threat intelligence
- Establish 24x7 threat detection and response approaches
- Monitor & secure IT, OT & IoT systems
- Resilience for service continuity
- Manage behavioral & cultural change effectively

Digital risk in convergence of IT, OT and IoT

Each industry is facing ever increasing cyber risks

- Digital convergence is generating business opportunities and benefits — cost, performance and flexibility
- Risk vs. Award — Increased online presence, Mass mobile adoptions, Cloud services, Data collection, Third Party



Current cyber security operations challenges

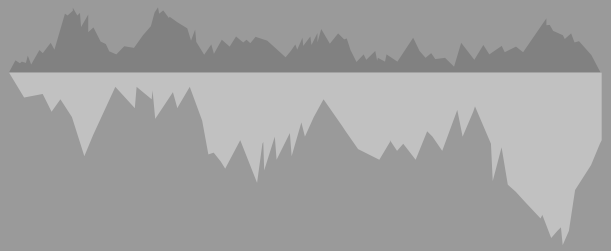
Traditional cyber is failing to detect threats

44%*

of respondents say they do not have a Security Operations Center (SOC)

30%**

of SOCs are failing to meet their most basic security operations requirements



"… there are also unknown unknowns"
Donald Rumsfeld

Commercial off-the-shelf product timelines are slow

You cannot protect what you cannot see — Indexing large data volumes is expensive

Cannot interrogate large volumes of historical data — Too much "noise"

Expanding threat horizon

Nation States

Hacktivists

Organized crime

Trusted insiders

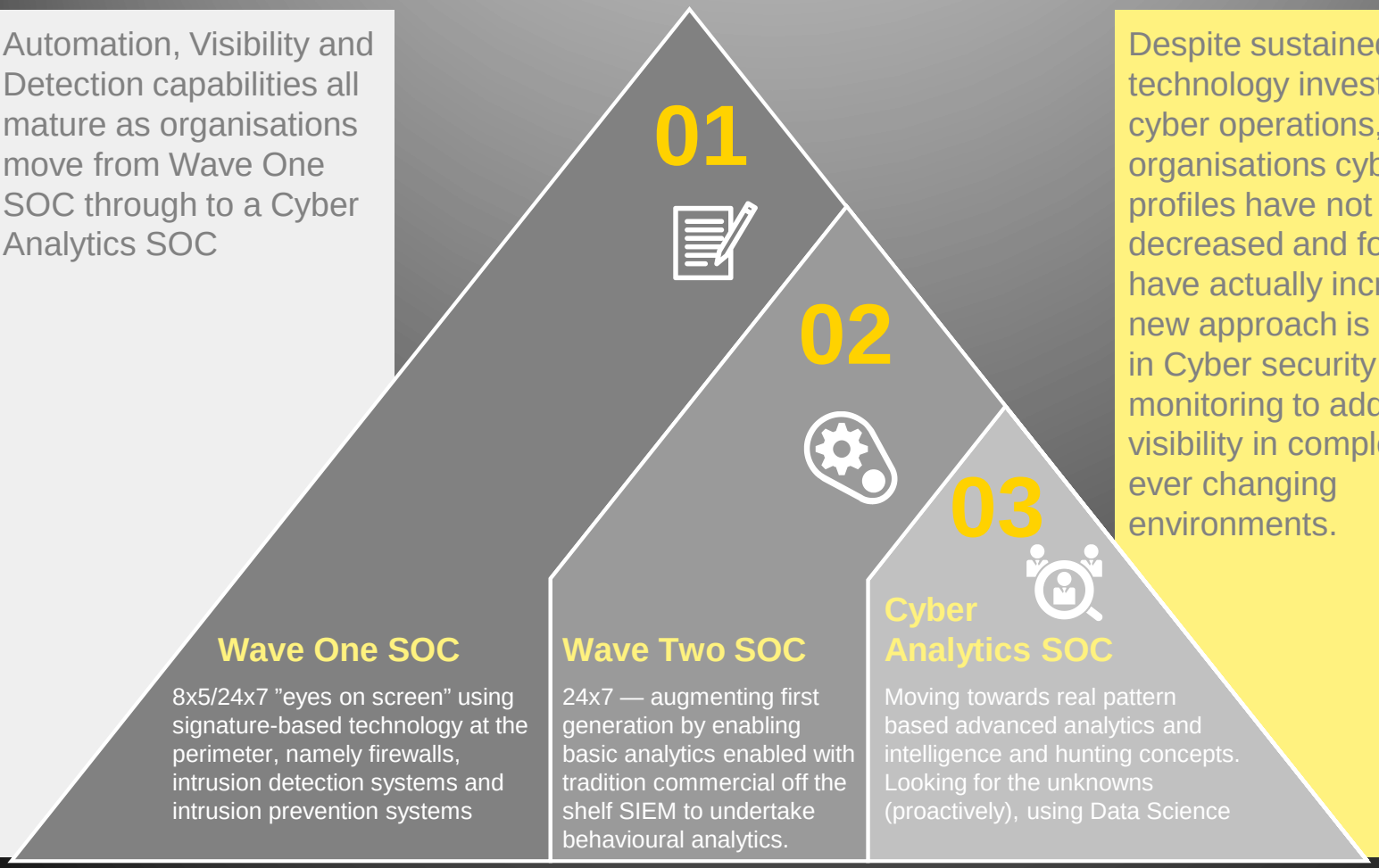
Difficult to innovate at the speed of threat attackers

* EY Global Information Security Survey 2016
** HPE State of Security

Evolution of SOCs

A SOC power by cyber analytics provides comprehensive visibility

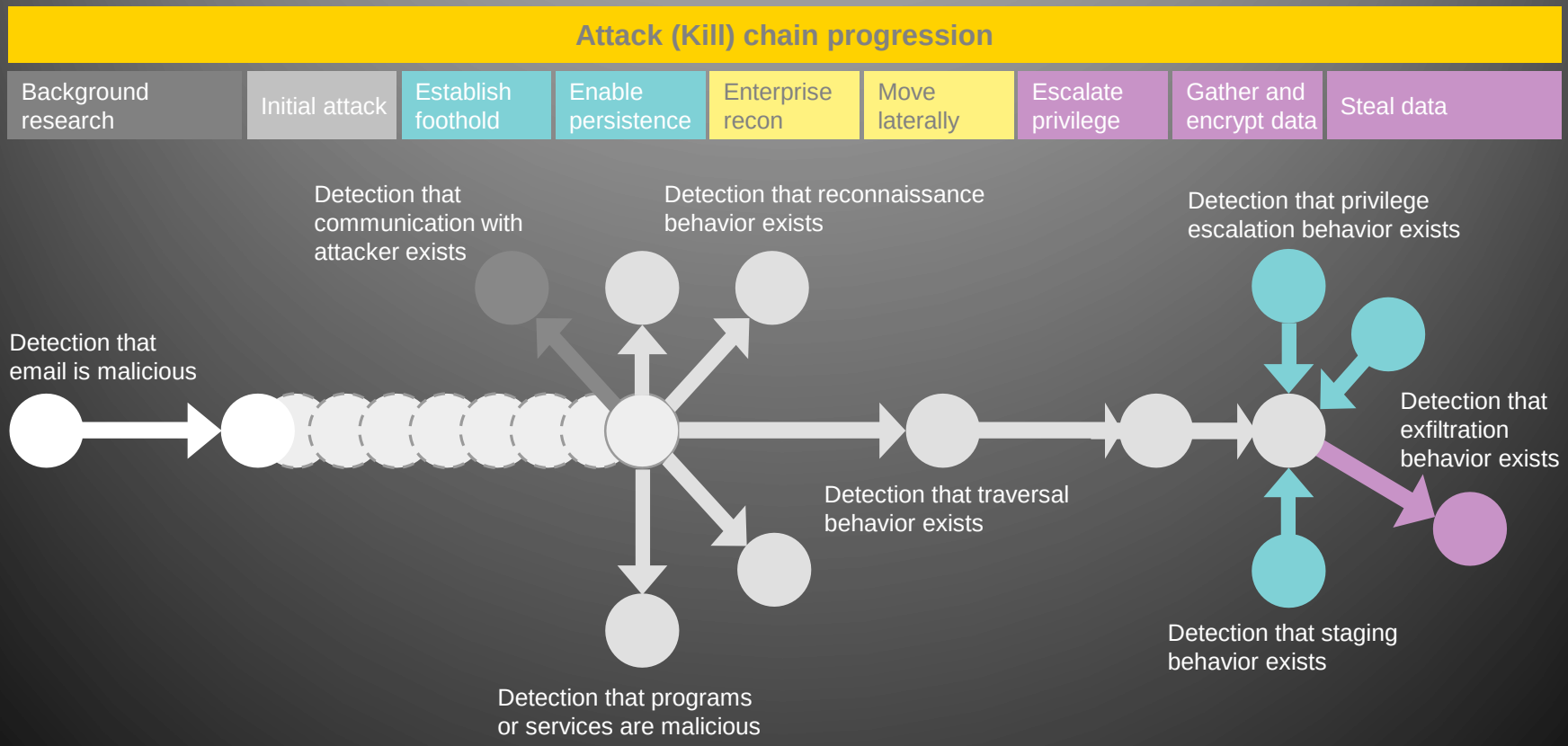
Automation, Visibility and Detection capabilities all mature as organisations move from Wave One SOC through to a Cyber Analytics SOC



Despite sustained technology investment in cyber operations, organisations cyber risk profiles have not decreased and for many have actually increased. A new approach is required in Cyber security monitoring to address visibility in complex and ever changing environments.

Example - Visibility throughout the kill chain

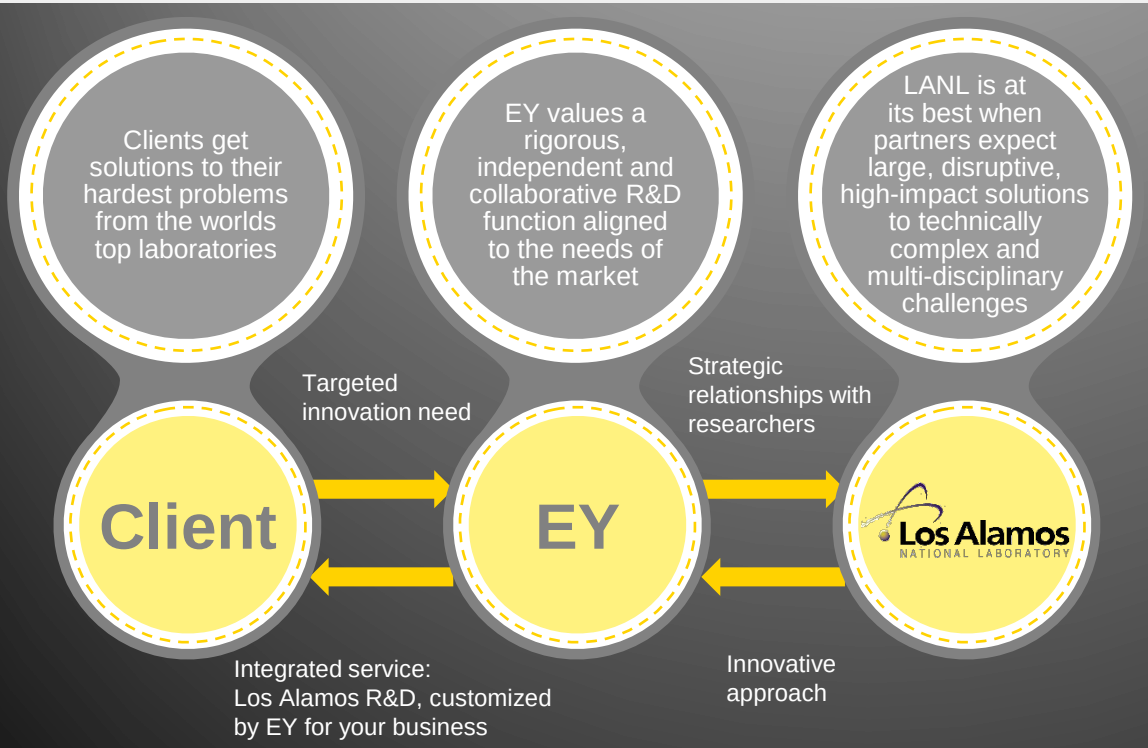
- Vectra report “120 participating organizations, 117 detected at least one of these behaviours (reconnaissance, lateral movement or data exfiltration) during each month of the study”



EY and Los Alamos National Laboratory (LANL)

Los Alamos NATIONAL LABORATORY

2016 R&D 100 WINNER



www.ey.com/losalamos

Cyber Security Experience

National Security Laboratory

- Focused on security science to protect the nation

Long history of networking

- First connected to Arpanet in 1983

Long history of cyber security

- First attack in 1983
- Over 15 years of data collected
- Many nation state and criminal attacks

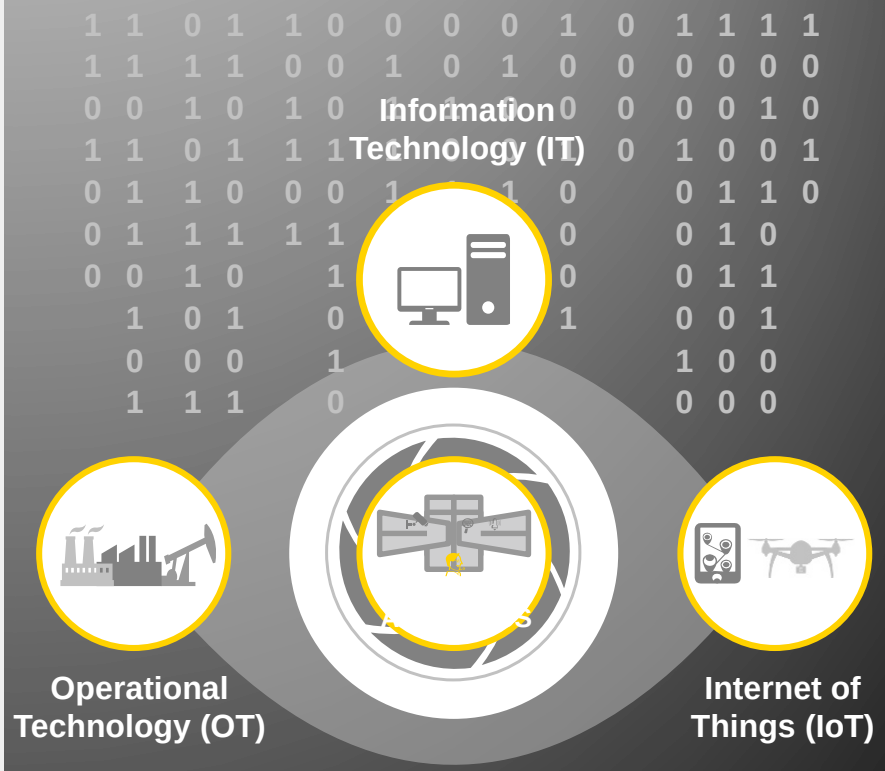
Long history of cyber R&D

- For defense of LANL's network and US DOD networks
- Strong analytics program

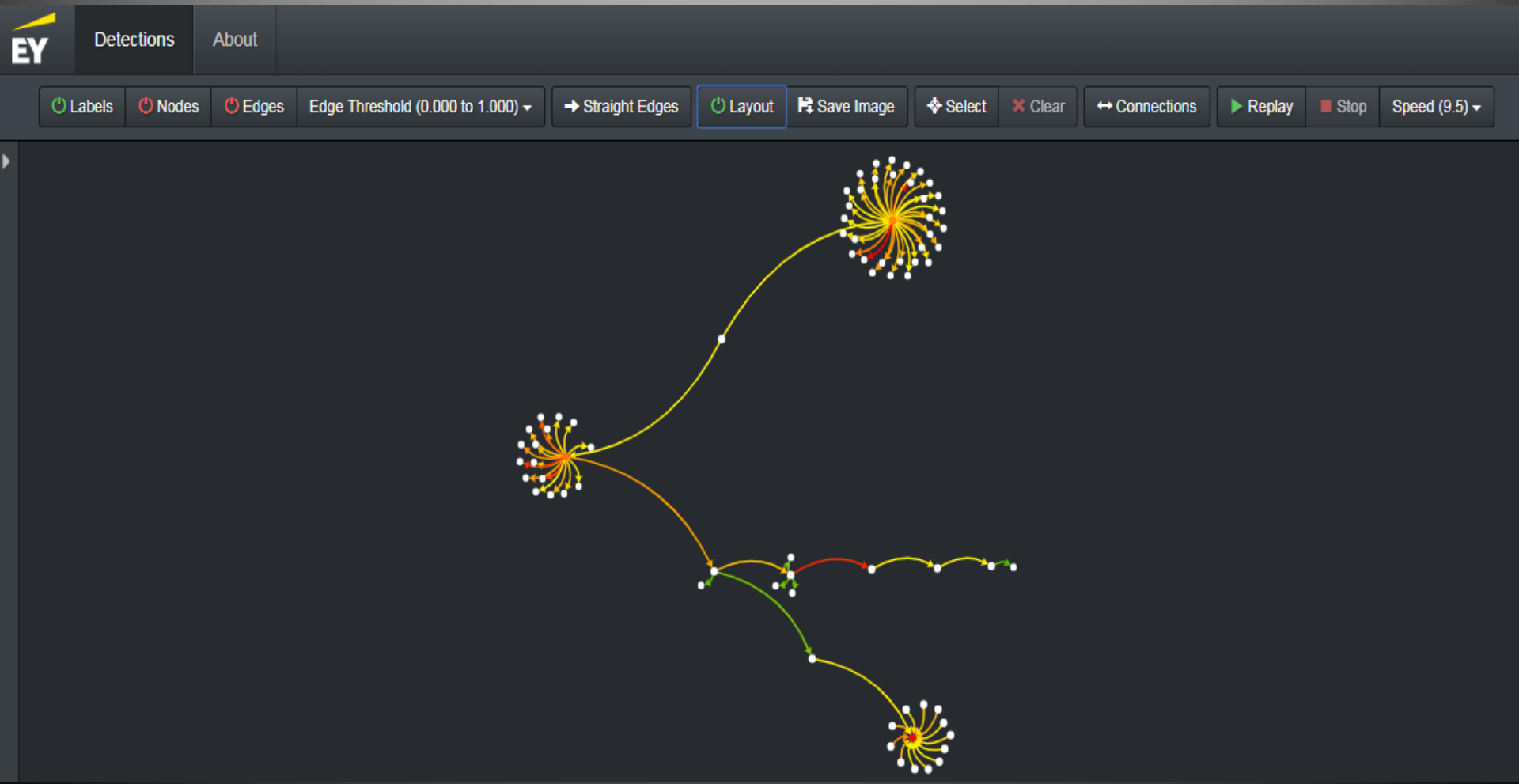
EY

Cyber Analytics - the goal

- Provides monitoring of Digital ecosystem (IT, OT & IoT)
- Accelerated deployment
- Detect advanced attacks
- Ability to actively follow an attack & forensic support – Threat Intelligence
- Augment existing Cybersecurity controls
- Threat focused analysis
- Scalable and flexible
- Remove false positives



EY Cyber Analytics



Questions & Thanks