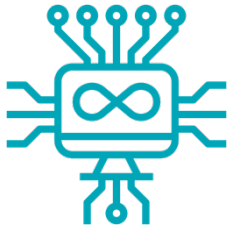
THE NATURE OF THE PROBLEM



Technology

Verses

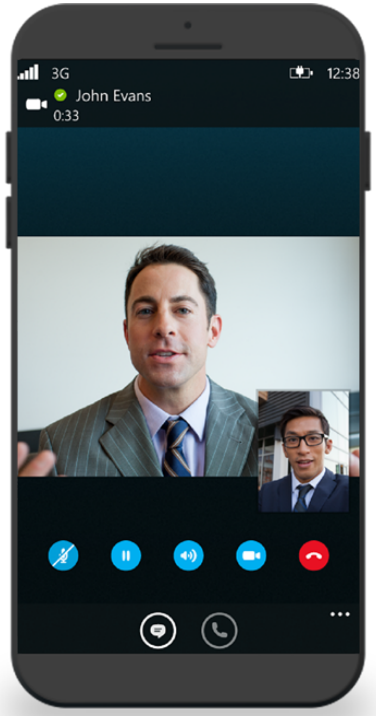
People

Adversary is a computer program.	Adversary is a person using a computer program.
Find the solution and repeat it.	Creativity and strategy.
A product will solve the problem.	People need to solve the problem.
Security through compliance.	Unique, morphing defenses.
Technology solves the problem.	***People supported by tech solves the problem.***

COMMODITIZATION OF TECHNOLOGY

Overtime technology becomes cheaper and easier to use.

Video conferencing from 1990's



Video conferencing Today

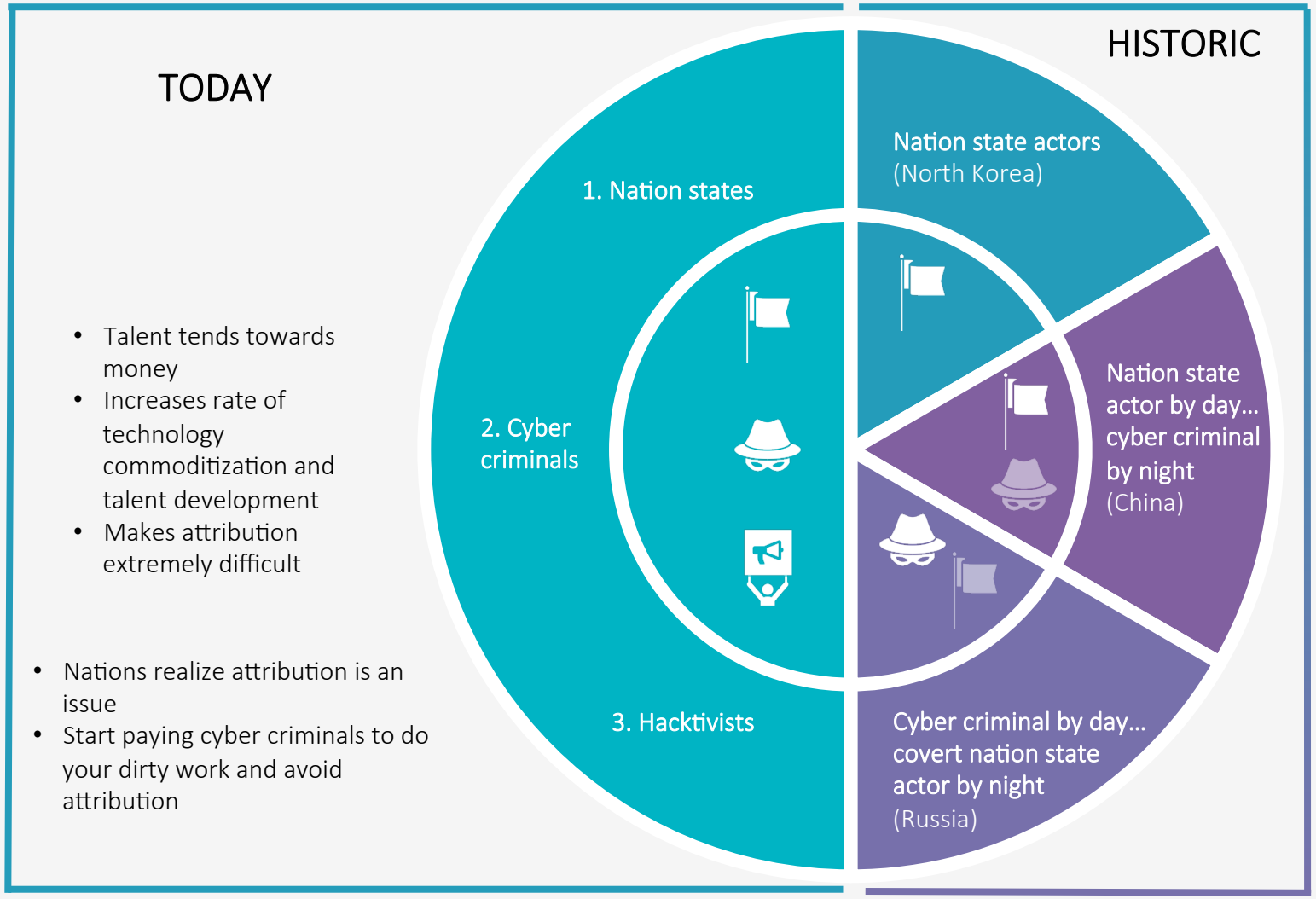
Hacking technology is no different.

- Attacks executed by nation states 5 years ago are now executed by cyber criminals and hacktivists.
- NSA leaks lead to WannaCry and Bad Rabbit ransomware.

COMMODITIZATIO
N
OF TALENT

Five years ago, there was a distinct hierarchy of attackers.

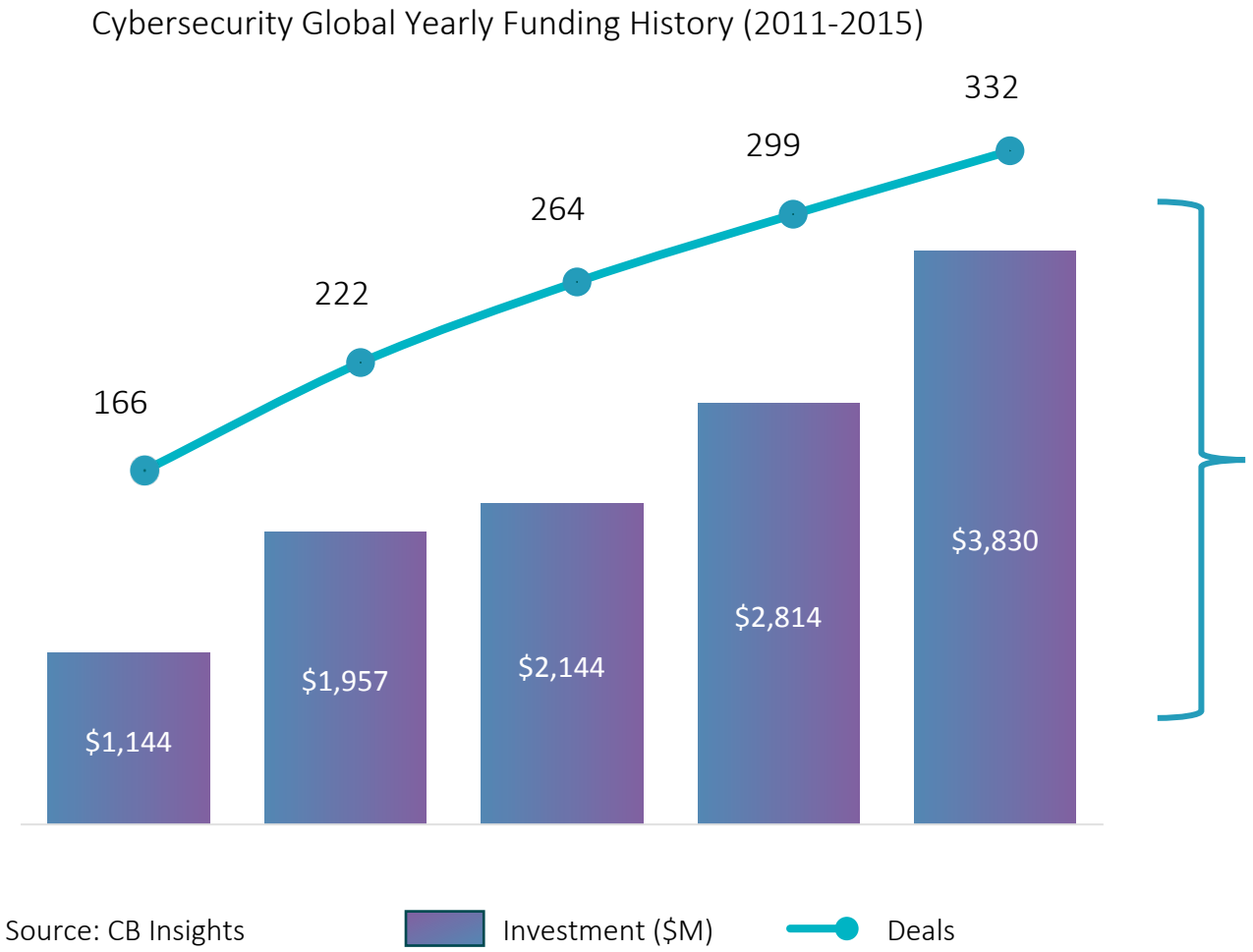
Today, the lines are blurred.



- Talent tends towards money
- Increases rate of technology commoditization and talent development
- Makes attribution extremely difficult

- Nations realize attribution is an issue
- Start paying cyber criminals to do your dirty work and avoid attribution

HOW TO RESPOND



- A LOT OF PEOPLE TRYING TO GET YOUR ATTENTION AND YOUR $$$: A lot of investment and a lot of marketing
- WHAT ARE WE HEARING?: Technology will solve the problem. Regulation of the right processes will solve the problem. Talented people will solve the problem
- WHAT IS THE TRUTH? WHAT WORKS?

KEY MEASURES OF A SECURITY PROGRAM

Compliance metrics

First thing first, meet the basics. Are your auditors happy and can you continue to do business?

Detect time

How long does it take to identify both automated and advanced attacks?

Containment time

Once an attack is detected, how long before the attacker is neutralized?

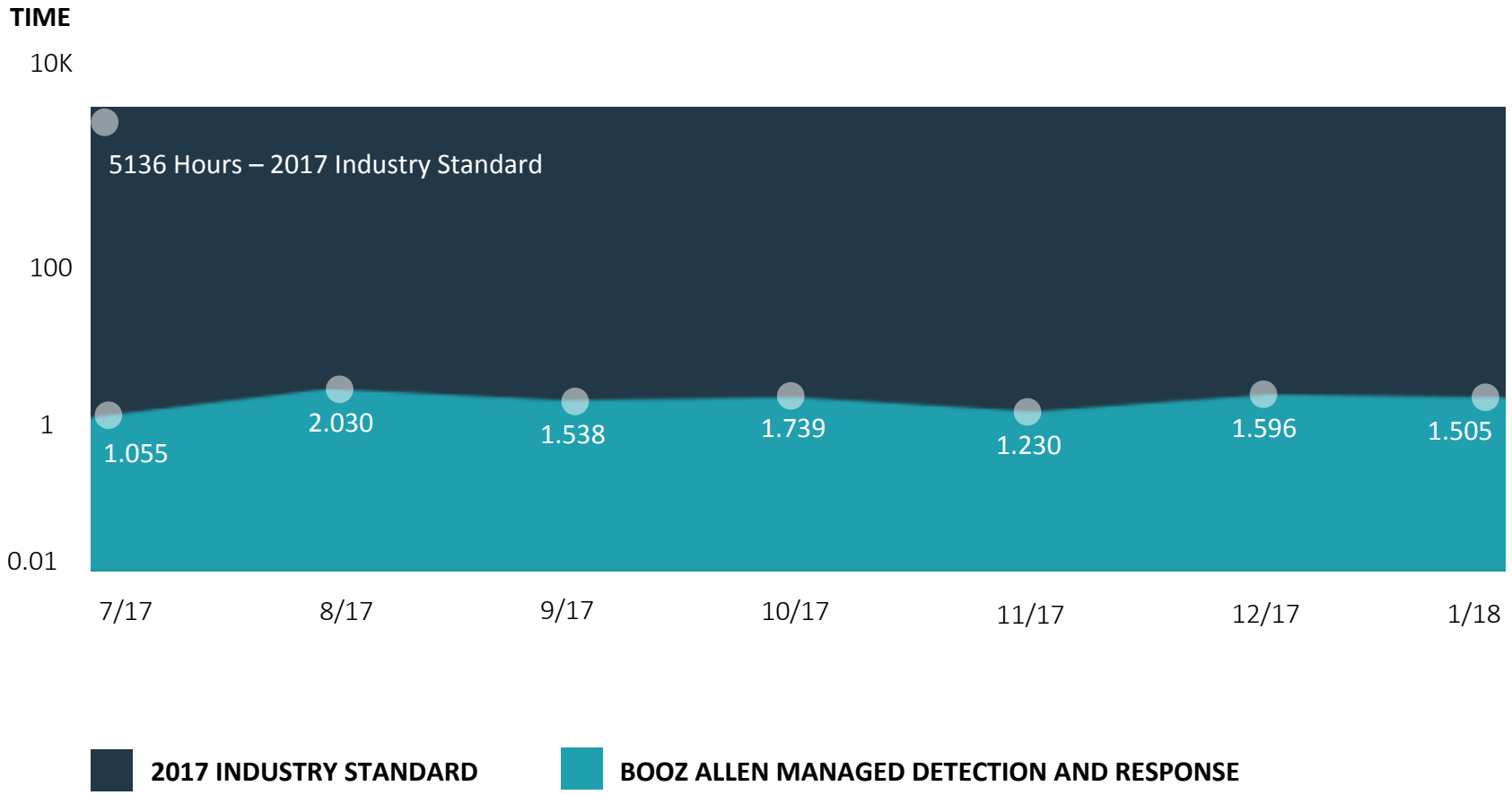
Remediation time

How long was the business impacted?

Dwell time

How long was the attacker able to take action within your systems?

MEAN TIME TO DETECT



DETECTION DELIVERED

1 HOUR

FROM INDUSTRY AVG. OF

5136 HOURS*

MEAN TIME TO DETECT

THE MOST CRITICAL SECURITY METRIC

You cannot defend against what you cannot detect. A critical metric for modern cyber security programs is how quickly they detect attacks. Mean Time to Detect (MTTD) is the metric that measures how long it takes defenders to detect. Across the industry, companies take an average of 214 days to detect attacks. This means that attackers have an extended period of time in which they can take actions on their objectives before security teams even begin to contain and remediate attacks. Contrast this with the Booz Allen Hamilton MDR service which take 60 minutes to detect. By vastly shrinking the MTTD, Booz Allen's MDR offerings demonstrably improves client's security while also limiting attackers.

* Ponemon Institute

QUESTIONS