securonix

Scaling Security Operations

The Answer To The Challenge Of Threat Inflation

Clive McDonald – Director of Sales Engineering (EMEA)

Threat Inflation

Threat Inflation

2017/18 > 16.6%

2018/19 > 32.7 %

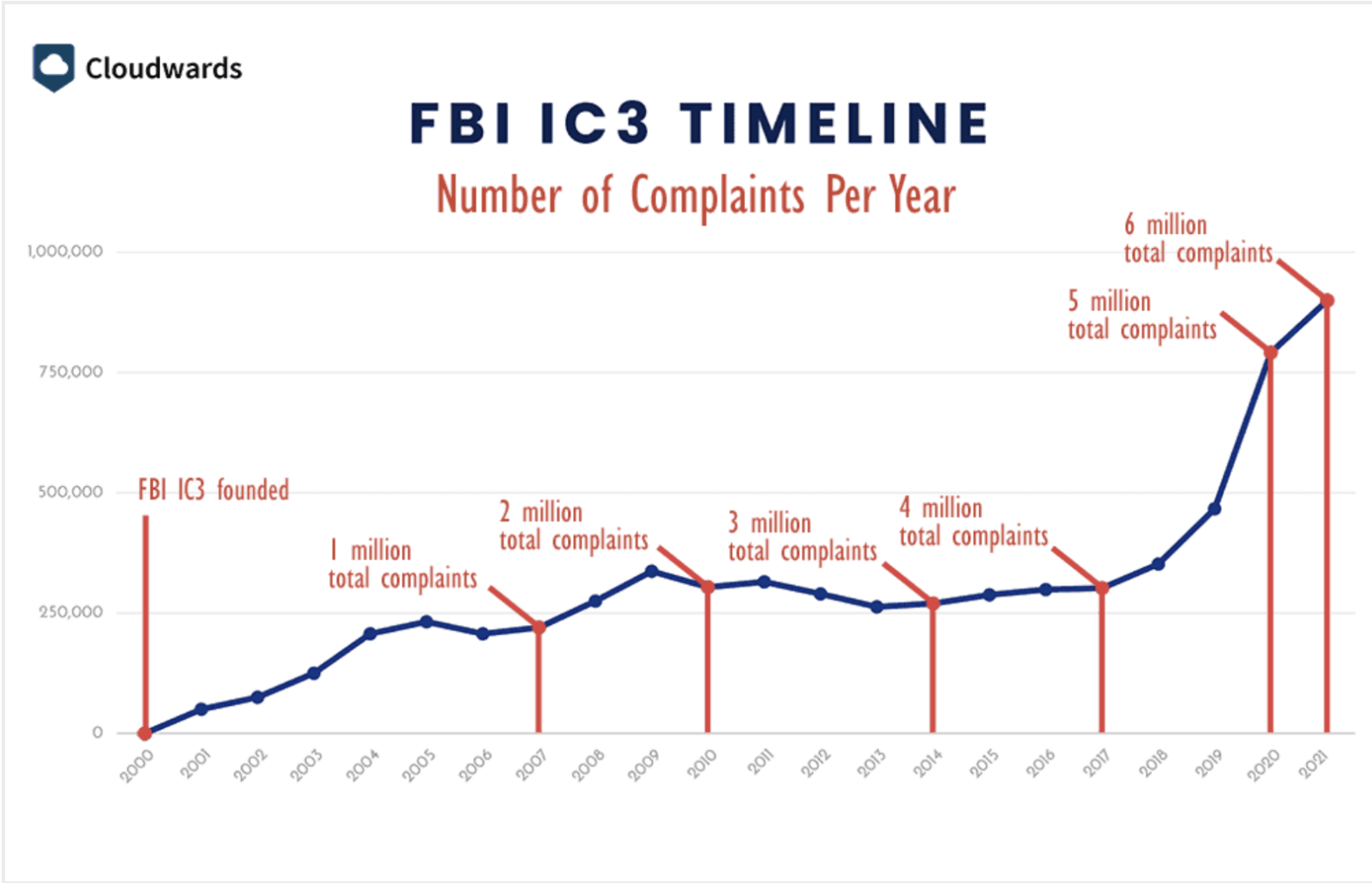
2019/20 > 69.4 %

2020/21 > 7% (Decrease due to CoVID)

2021/22 > (Factor in Geo political tensions and other factors; its skewing towards a 3-digit increase)

Threat inflation

- More threat actors
- Threat actors are more active
- Cyber-espionage and Cyber-war activities by nation-states are more frequent



Our hands are tied

You probably cannot stop or reduce threat inflation

securonix

What have we done about it?

Increasing:

- Budgets
- Teams
- Technology stack

It doesn’t scale

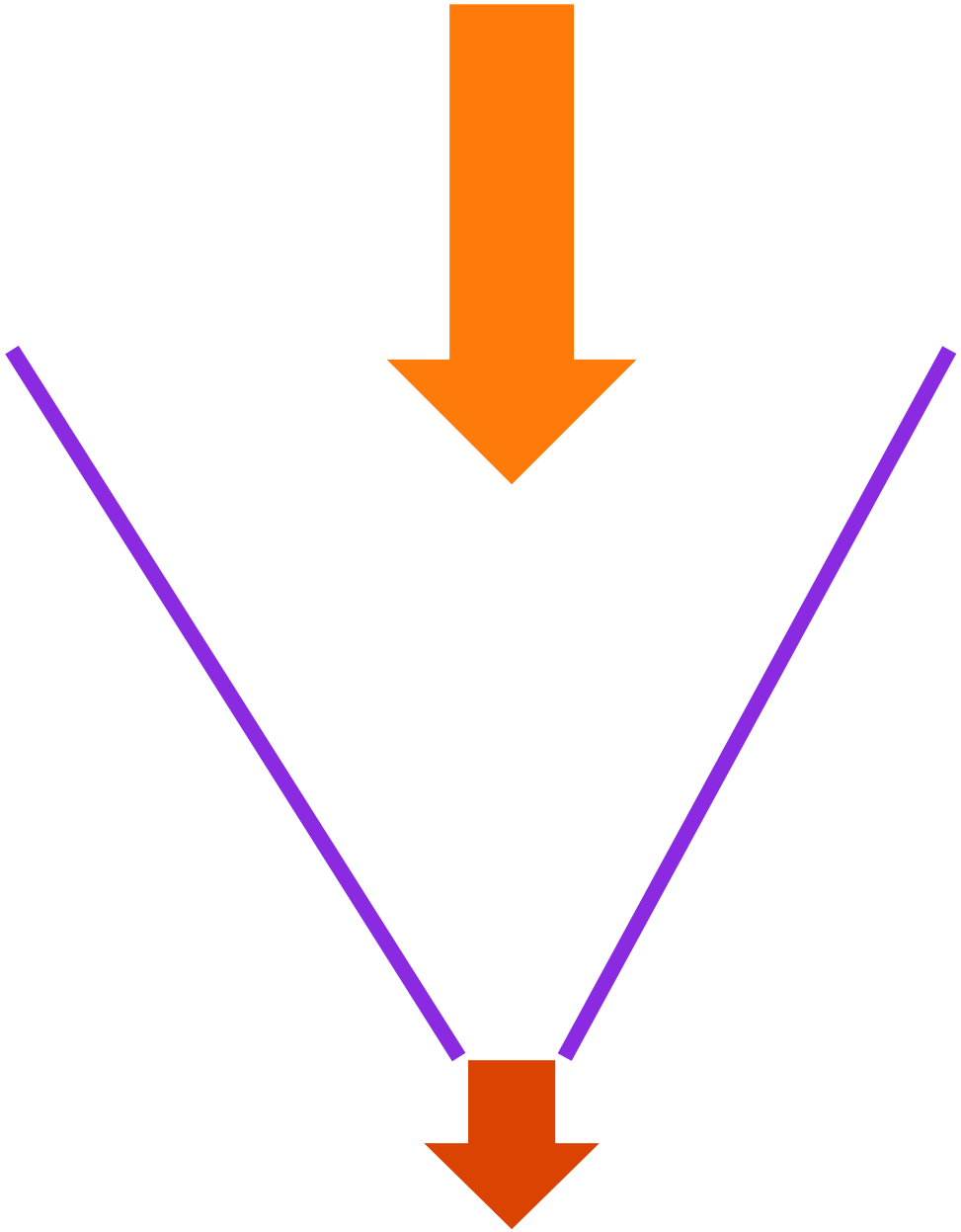
Security operations must scale

securonix

How to scale threat detection and response?

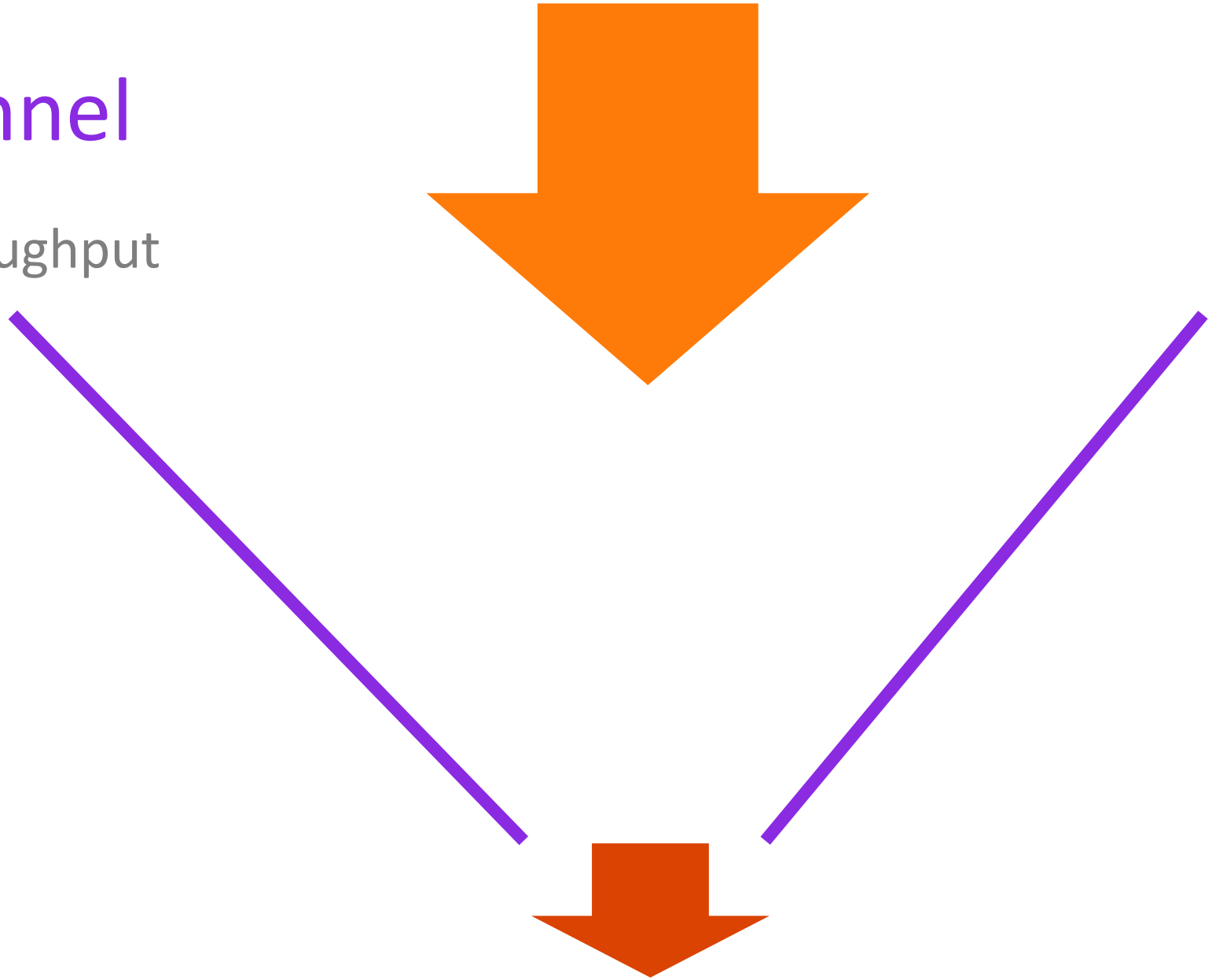
- We operate TDR as a funnel
- Telemetry gets in, alerts go out
- But many of these funnels have problems:
  - Throughput
  - Too much output
- How can we fix our funnels?

Adjusting the funnel



Adjusting the funnel

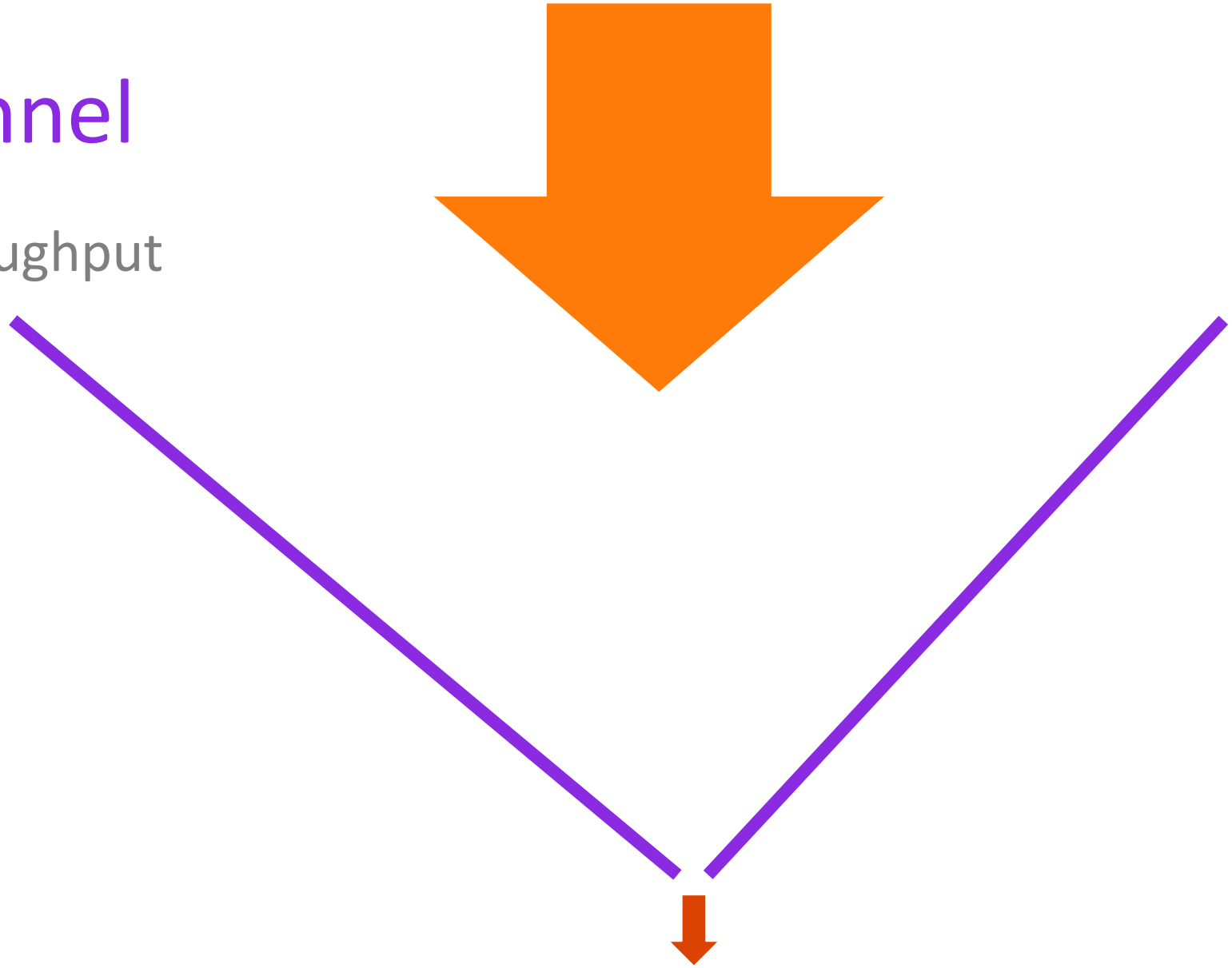
- Cloud increases the throughput



Adjusting the funnel

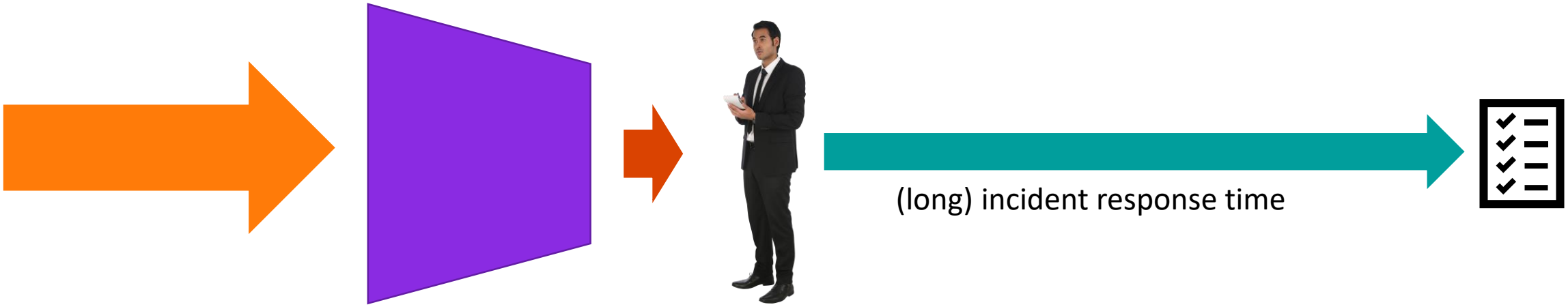
- Cloud increases the throughput
- Advanced analytics reduces the output

Is the problem solved?



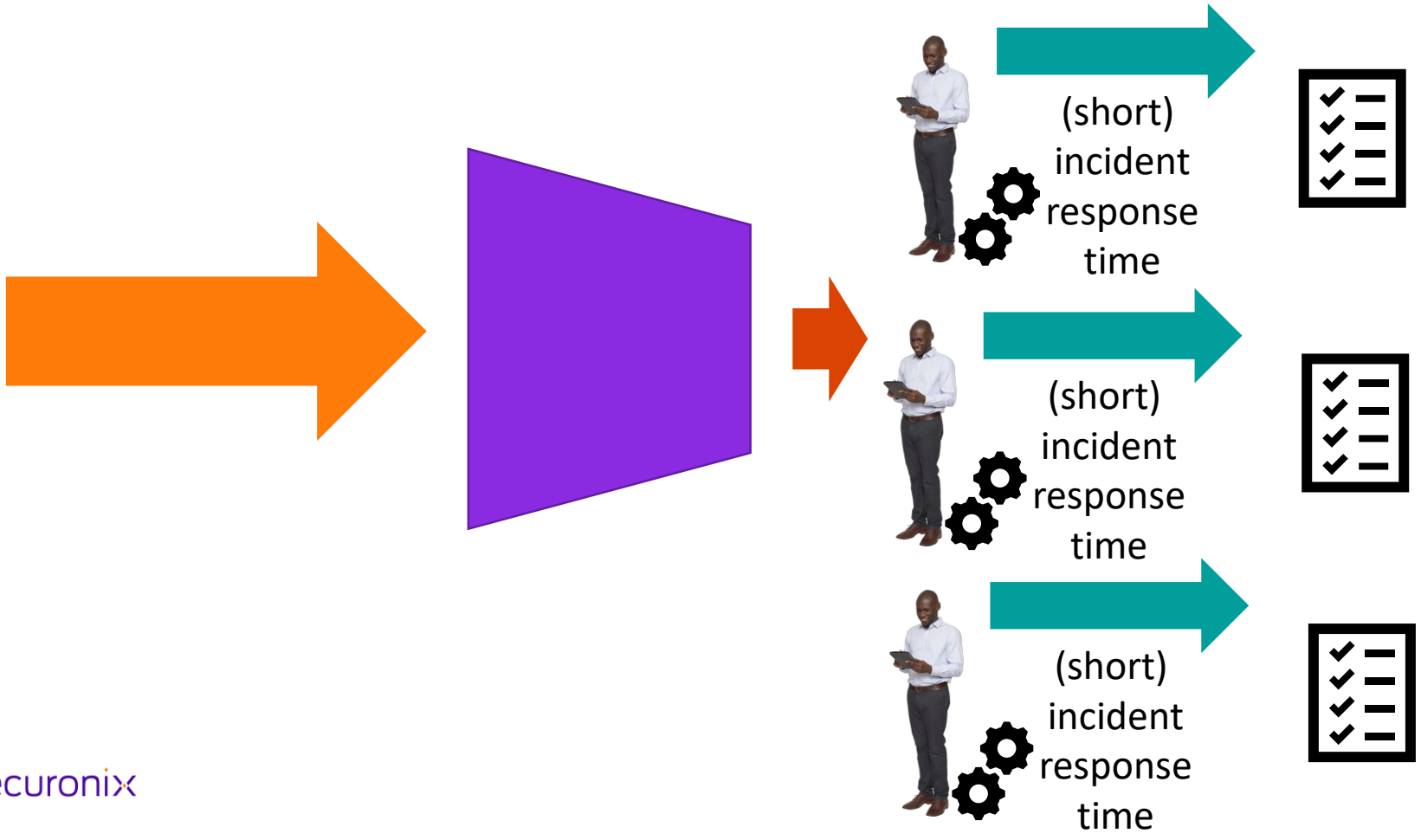
After the funnel

- The output of the funnel – the alerts – are still treated manually, by humans



Time for automation

- Automation reduces incident response time and add scale



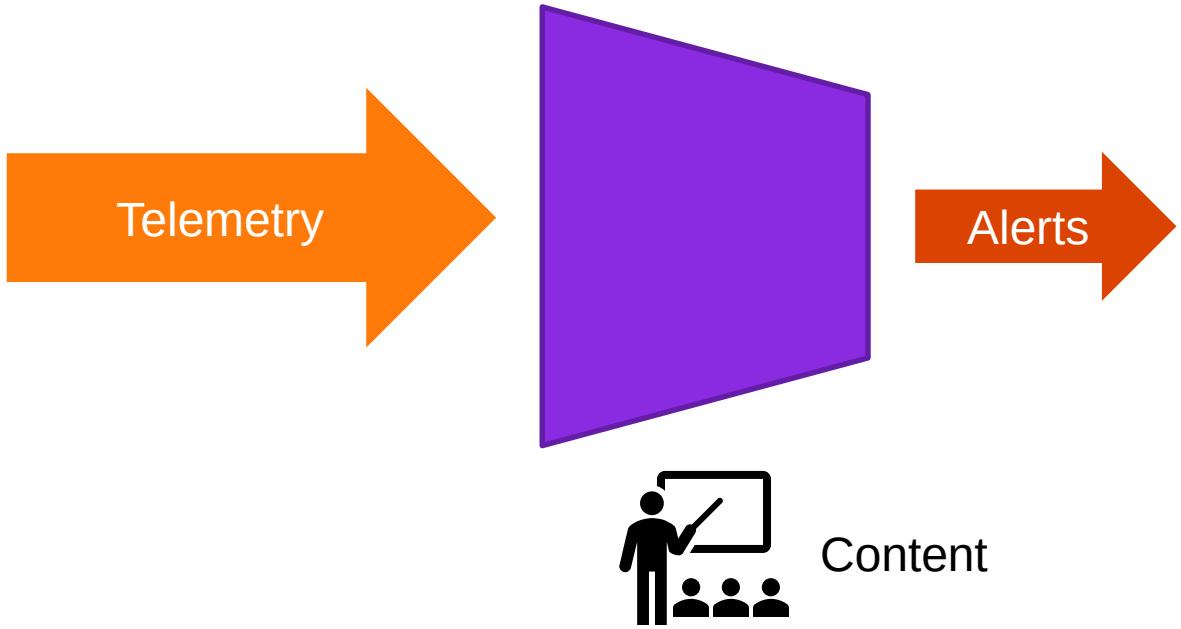
securonix

There is another (hidden) funnel

securonix

How do you know what to look for?

- What tells your funnel what should go out through the other side?



Content production is hard

Threat Intelligence

What to look for

Expensive

Hard to find

Skills

Transform TI in content

securonix

How to scale content production?

Services

Vendors and service providers produce content that will be used by many customer

The classic “1 to many” relationship

Fixing the security operations scale challenge

Cloud Native Technology

Provides scalability with cost efficiency

Powerful Analytics

Provides the tools required to find threats

Top-Notch Threat Detection Content

Reduced time to value and economy of scale

securonix

Thank You
@apbarros