ThreatConnect

How to Get Promoted

Developing metrics to show how threat intel works

ThreatConnect.com

Who are we?

Toni Gidwani @t_gidwani

Director of Research

Side gig as a Georgetown professor

Maker of gelato

Marika Chauvin @MarSChauvin

Senior Threat Intelligence Researcher

Research junkie

Stress baker

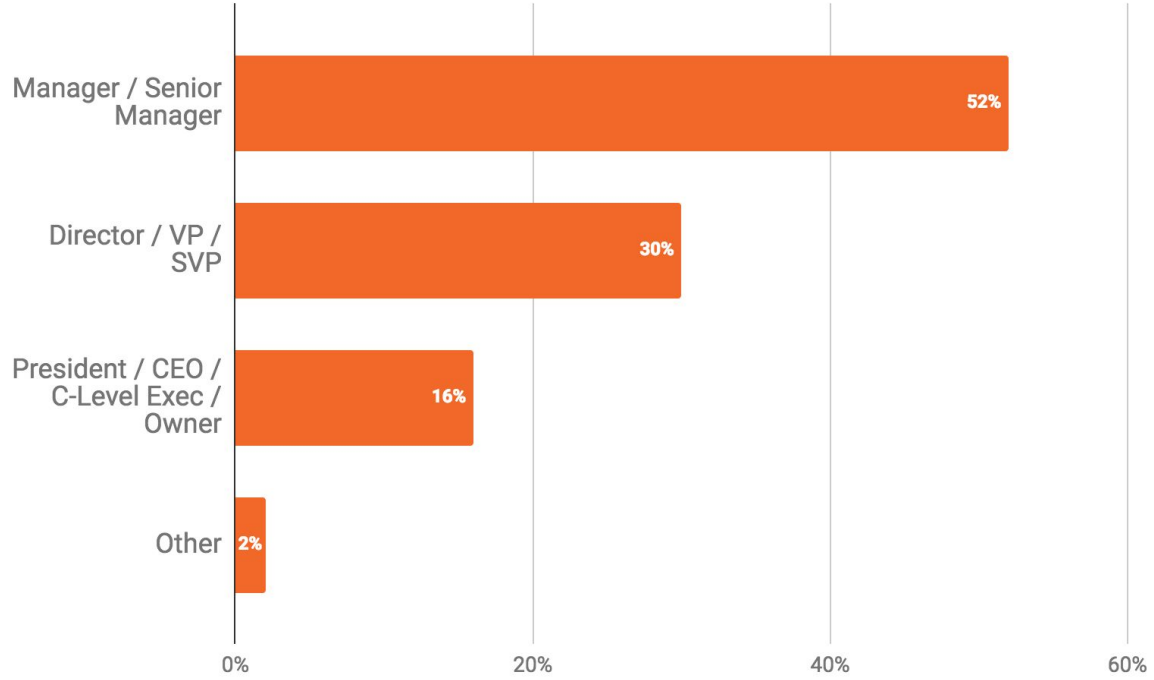
ThreatConnect

Contents

Problem

How do I show that threat intel provides value to my org?

“Building a Threat Intel Programme” Survey Respondents

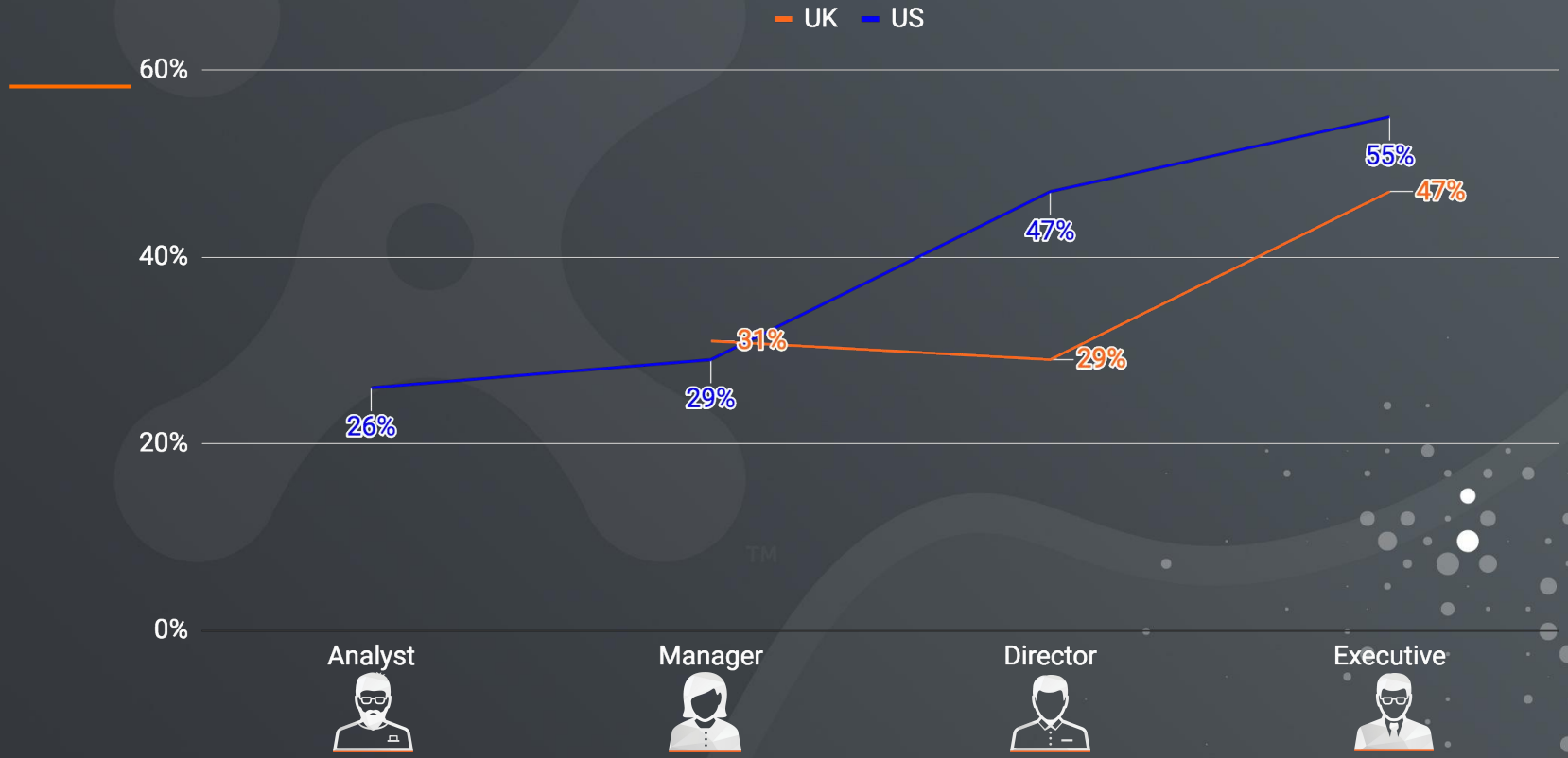


ThreatConnect

Most Important Success Factor

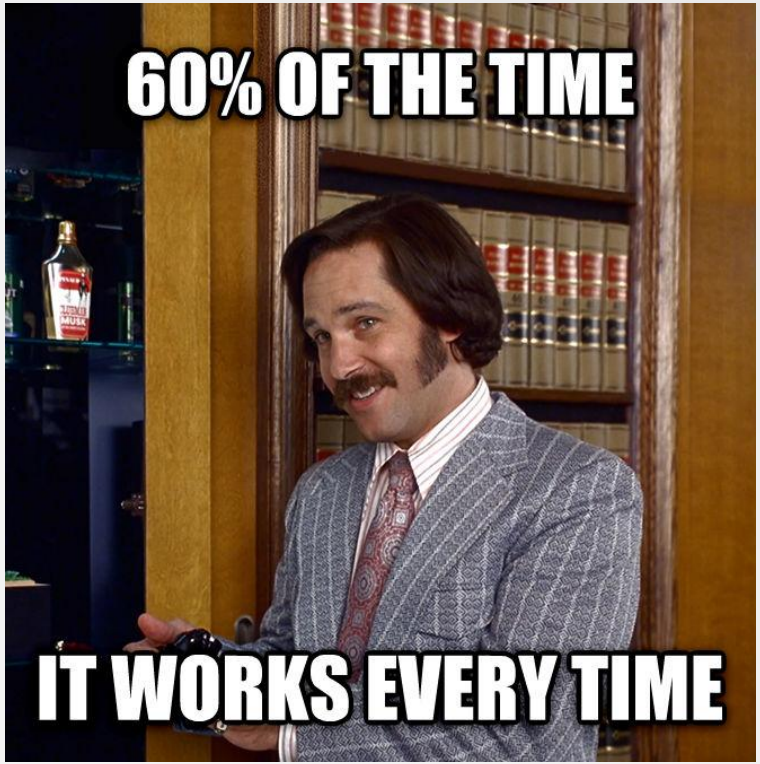
- Remove risks from cybercrime activities
- **Protect personal client information**
- Protect monetary assets of the organization
- Increase productivity for other parts of the organization
- Revenue generated for the organization
- Prevent service interruption for core business functions
- Avoid embarrassing public disclosures of information

Disconnect: Executives Self-rate Maturity Much Higher



The Problem When We're Not on the Same Page...

“Metrics”



Metrics: Can’t live with them, can’t live without them

Good metrics

- Clear
- Measurable
- Correlate to business outcomes

Common pitfalls

- What we can count
- Output, not impact
- Too tactical for your boss’ boss

Types of Metrics

Measures of Performance

Measures task completion and efficiency

Am I doing this right?

Measures of Effectiveness

Measure what is accomplished and whether goals are being met

Am I doing the right things?

Measures of Performance

Useful for:

- Impact of automation/efficiencies
- Process improvement
- Utilization of resources
- Incentivising a baseline step

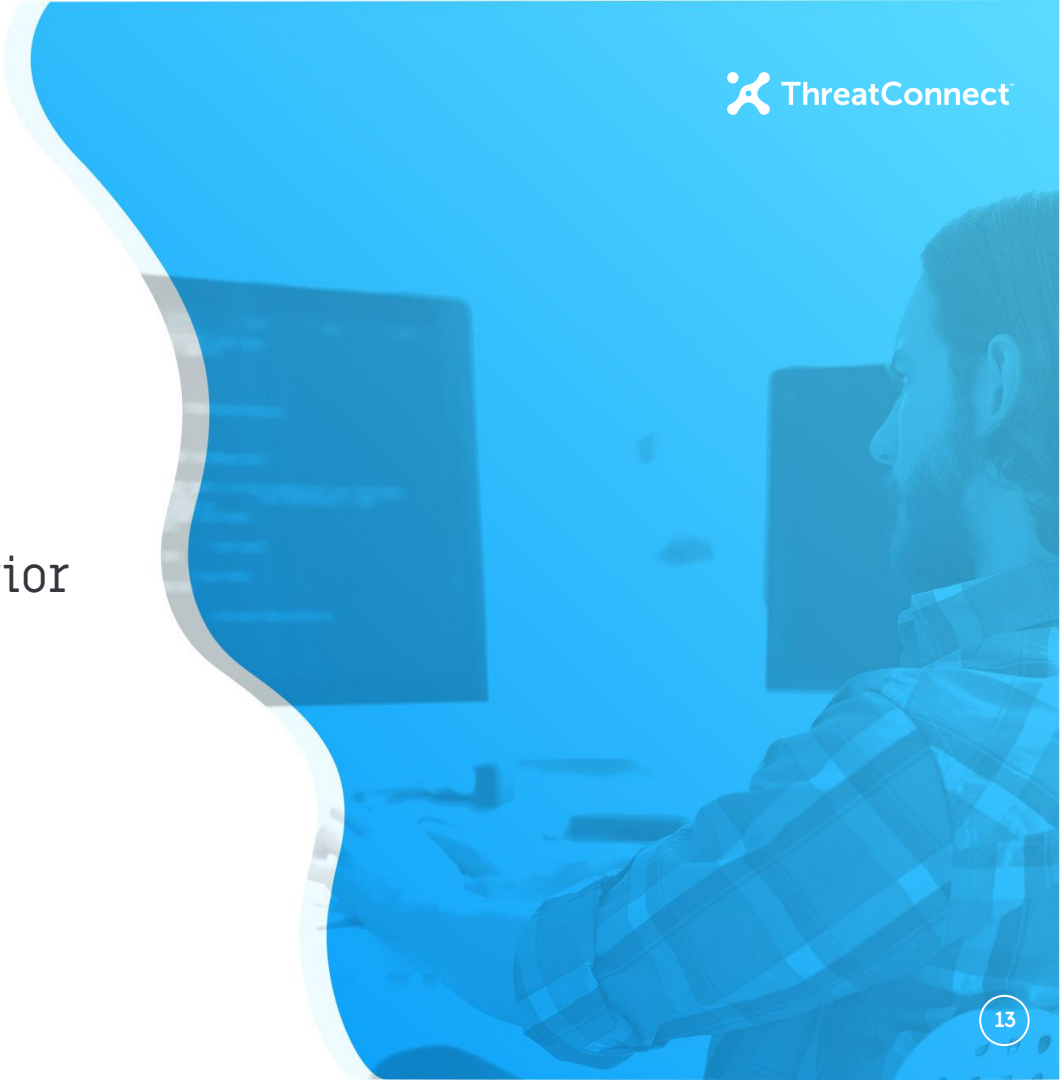
Examples:

- Total alerts issued
- Total items reviewed/parsed
- % of malware samples detonated
- IOCs shared with community

… But

Limitations:

- Less useful for senior leaders
- Risk incentivizing poor behavior
- Less useful over long-term



Measures of Effectiveness

Useful for:

- Conveying program value to senior leaders
- Can be qualitative or quantitative
- Drive data collection
- Drive process development

Examples:

- Incidents discovered from TI
- Countermeasures enacted
- Total proactive blocks
- Mean time to detection
- Savings generated

...But

Cons:

- More difficult to generate
- Not as easily countable
- Often require interaction and input from other teams

Key Takeaway

Measures of Effectiveness are more compelling to your boss' boss

Showing Value at Different Maturity Levels

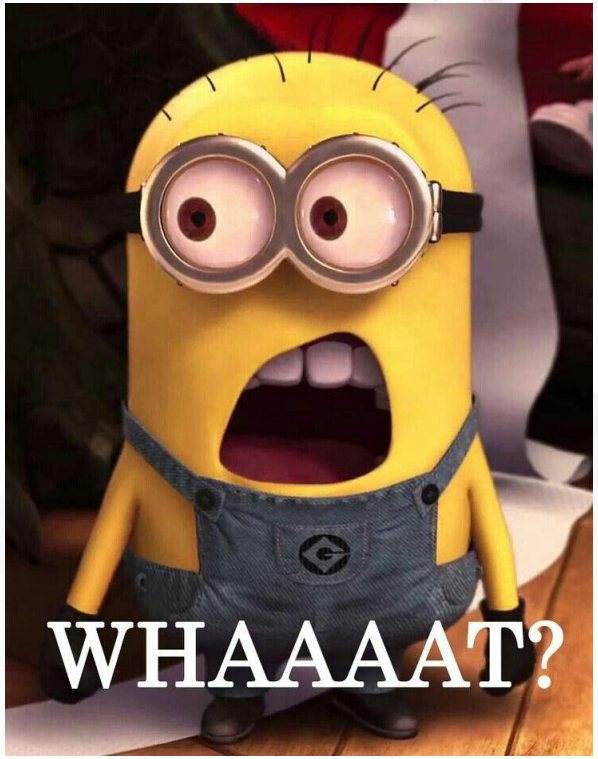
…because I can’t wait 5 years

ThreatConnect™

Self-Reported Money Saved

60% saved a significant sum of money in the last year

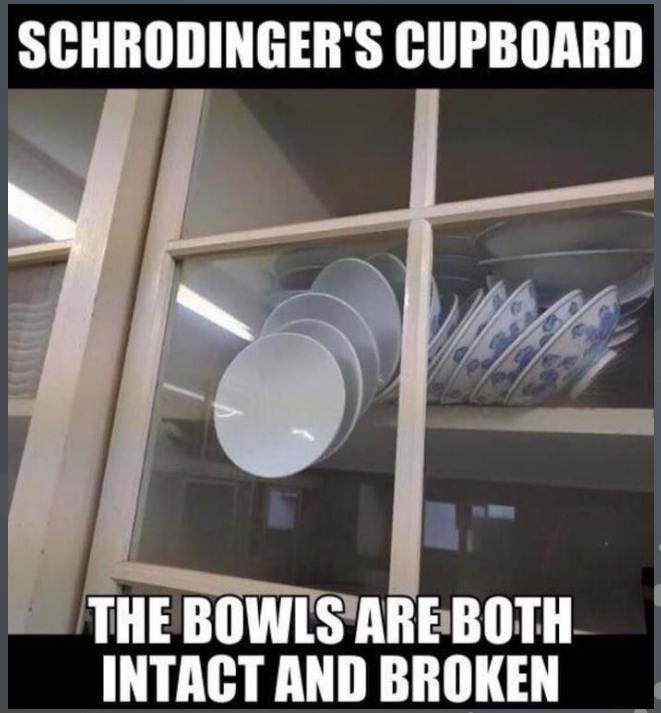
- Least mature: **~ £333**
- Mid-level programmes: **£5.9 million**
- Well-defined programmes: **£14.5 million**



Schrodinger's Breach: When Getting Better Looks Worse

Gains for lower maturity programs come first from:

- Improving visibility
- Understanding the threat
- Enhanced detection



Metrics to Tell if Improving or Everything is on Fire

Getting started?

- IOCs observed
- Incidents discovered from TI
- Qualitative feedback loop
- Countermeasures enacted

Metrics to Tell if Improving or Everything is on Fire

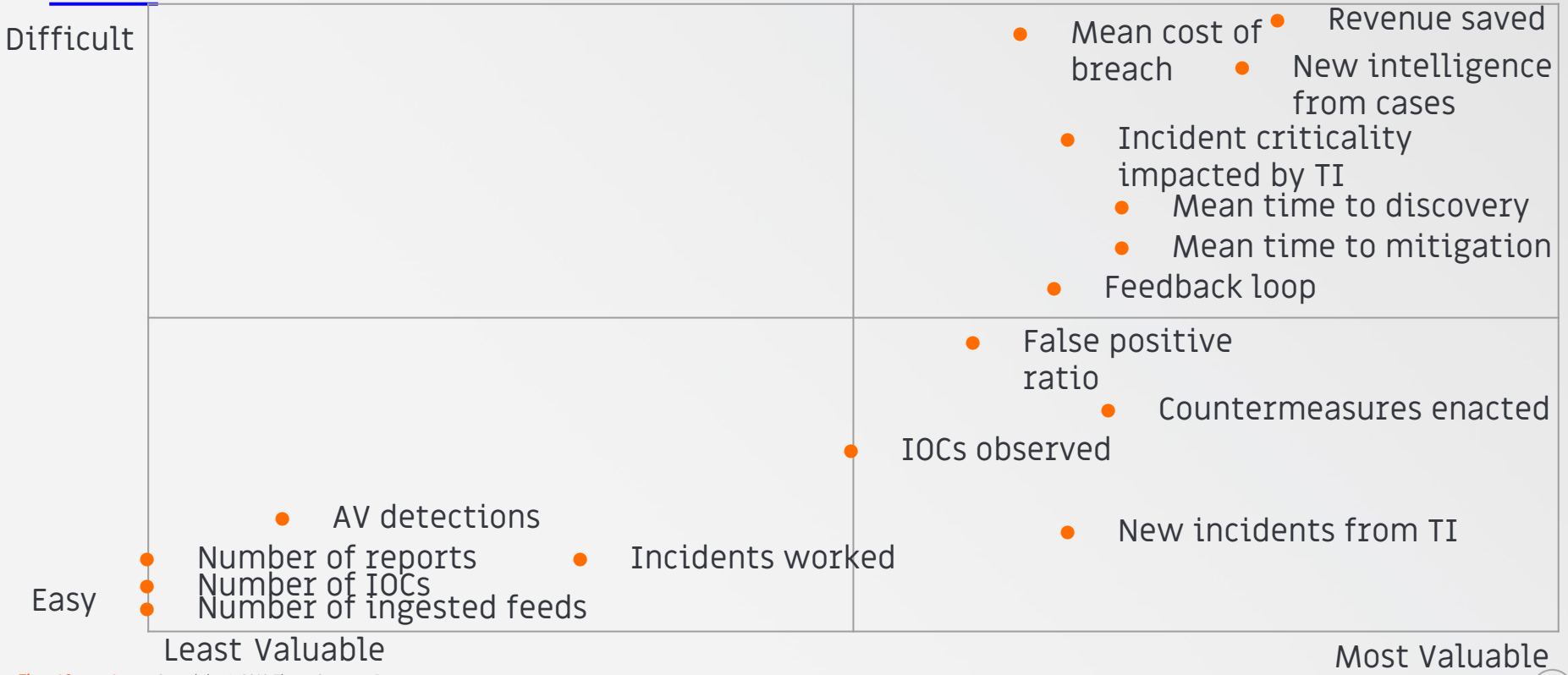
More mature?

- False positive ratio
- Impact year over year
  - **Mean time to detection**
  - **Mean time to respond**
- New intelligence from cases
- Incident criticality impacted by TI

Quantifying value

- Mean cost of breach
  - Downtime
  - Additional resources to address breach (consultants, identity theft protection, etc)
- Feedback loop can be used to justify salary, team budget, and direct analysis efforts
- IBM Cost of a Data Breach Calculator

Metrics to Tell if Improving or Everything is on Fire



Thank You

ThreatConnect.com

ThreatConnect™