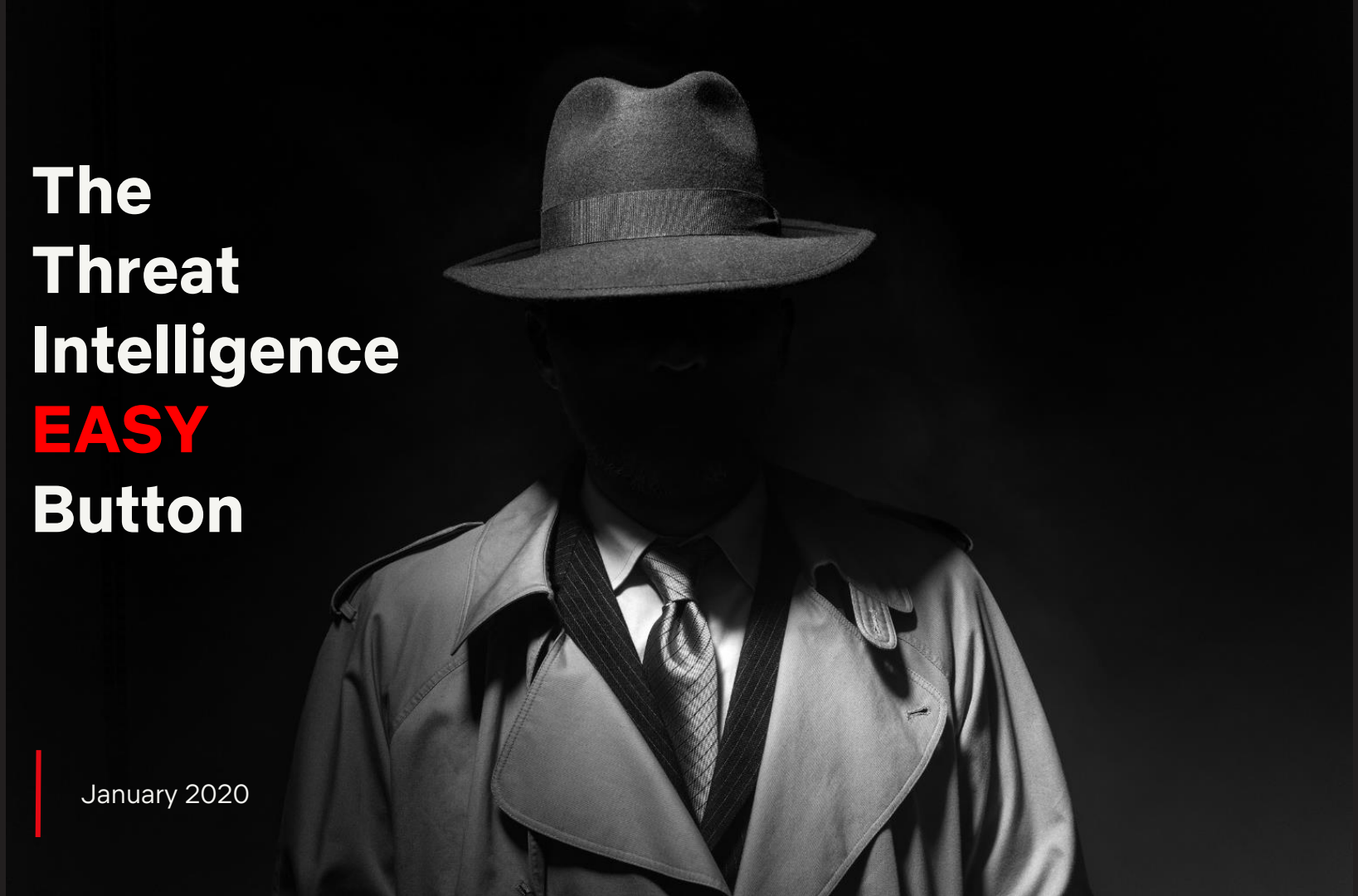
The Threat Intelligence EASY Button



January 2020

A Story

Once upon a time...

A Story

Once upon a time...

In a land called Netflix...

Chris Cochran

- Former Active Duty Marine
- Leading Intelligence @ NETFLIX
- Co-Host of Hacker Valley Studio

The EASY Framework

The EASY Framework

Elicit Requirements

- **Requirements start with the stakeholder, not prior engagements or training**

Elicit Requirements

- **Requirements start with the stakeholder, not prior engagements or training**

- **Sit down with your stakeholder to understand their function, intelligence needs, and to build the relationship**

Elicit Requirements

- Requirements start with the stakeholder, not prior engagements or training
- Sit down with your stakeholder to understand their function, intelligence needs, and to build the relationship
- If your stakeholder does not know what they need from intelligence, use this as an opportunity to develop requirements together

Elicit Requirements

Intel Requirements

File Edit View Insert Format Data Tools Add-ons Help Last edit was on August 23, 2019

100% $ % .0 .00 123 Default (Ari... 10

fx Stakeholder

	A	B	C	D
1	Stakeholder	Requirement	Serial	
2	Application Security		1.1	
3			1.2	
4			1.3	
5	Infrastructure Security		2.1	
6	Customer Trust		3.1	
7			3.2	
8			3.3	
9			3.4	
10	Corporate Security		4.1	
11			4.2	
12			4.3	
13			4.4	
14			4.5	
15	Studio InfoSec		5.1	
16	Device and Content Security		6.1	
17			6.2	
18			6.3	
19	Global Content Protection		7.1	
20	GRIT		8.1	
21			8.2	
22			8.3	
23	Open Connect		9.1	
24				

The EASY Framework

Assess Collection Plan

- Identify internal and external information sources

Assess Collection Plan

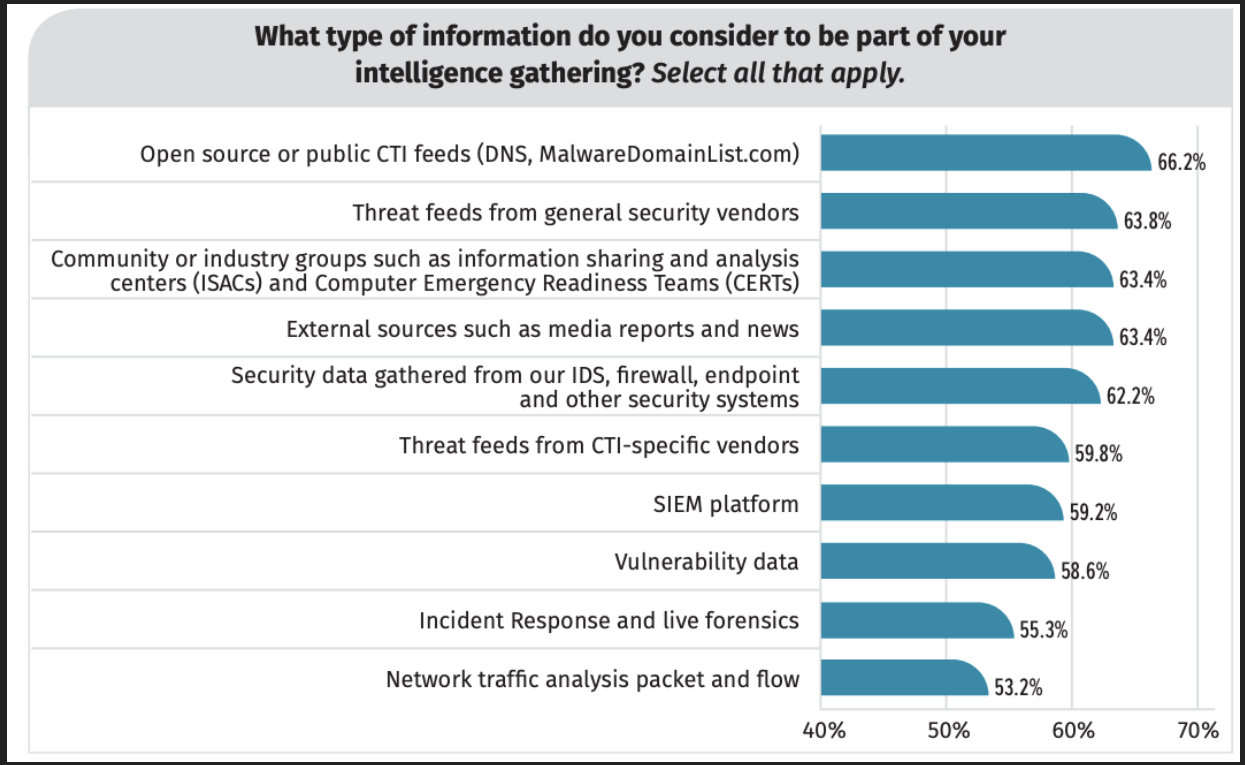
- Identify internal and external information sources
- As your requirements change, reassess your collection plan to ensure coverage

Assess Collection Plan

- Identify internal and external information sources
- As your requirements change, reassess your collection plan to ensure coverage
- Evaluate your sources for impact to the mission
  - Metrics are your friend

Assess Collection Plan

The Evolution of Cyber Threat Intelligence (CTI): 2019 SANS CTI Survey Rebekah Brown and Robert M. Lee



https://www.sans.org/reading-room/whitepapers/analyst/evolution-cyber-threat-intelligence-cti-2019-cti-survey-38790

The EASY Framework

Strive For Impact

- Producing for the sake of production doesn’t help anyone

Strive For Impact

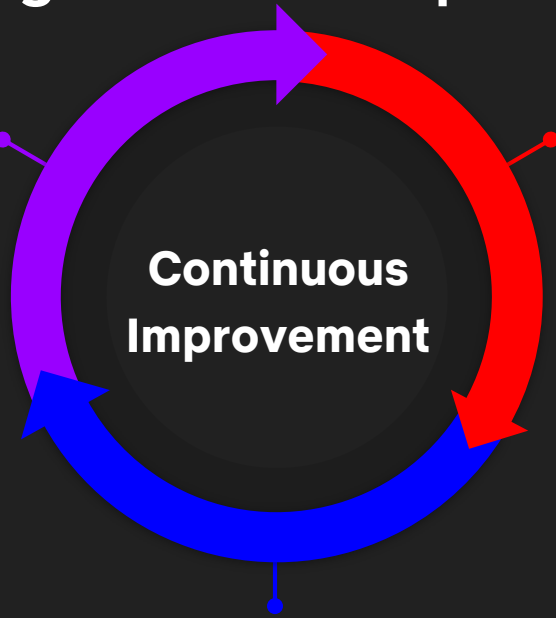
- Producing for the sake of production doesn’t help anyone
- Frame intelligence to help the stakeholder make a decision or execute actions to improve security

Strive For Impact

- Producing for the sake of production doesn’t help anyone
- Frame intelligence to help the stakeholder make a decision or execute actions to improve security
- Capture actions taken by stakeholders based on intelligence
  - Metrics are your friend (again)

Strive For Impact

Intelligence Led Purple Team



Intelligence

Feeds relevant TTPs to the red team for emulation and to the blue team for context

Red Team

Emulates attacks and attempts to circumvent prevention and detection measures

Blue Team

Looks for evil where we do not have conventional mitigations, closes gaps, and aspires to automate hunts (Detection)

The EASY Framework

Yield to Feedback

- If the stakeholder has a criticism for your intelligence or the program, something needs to be adjusted

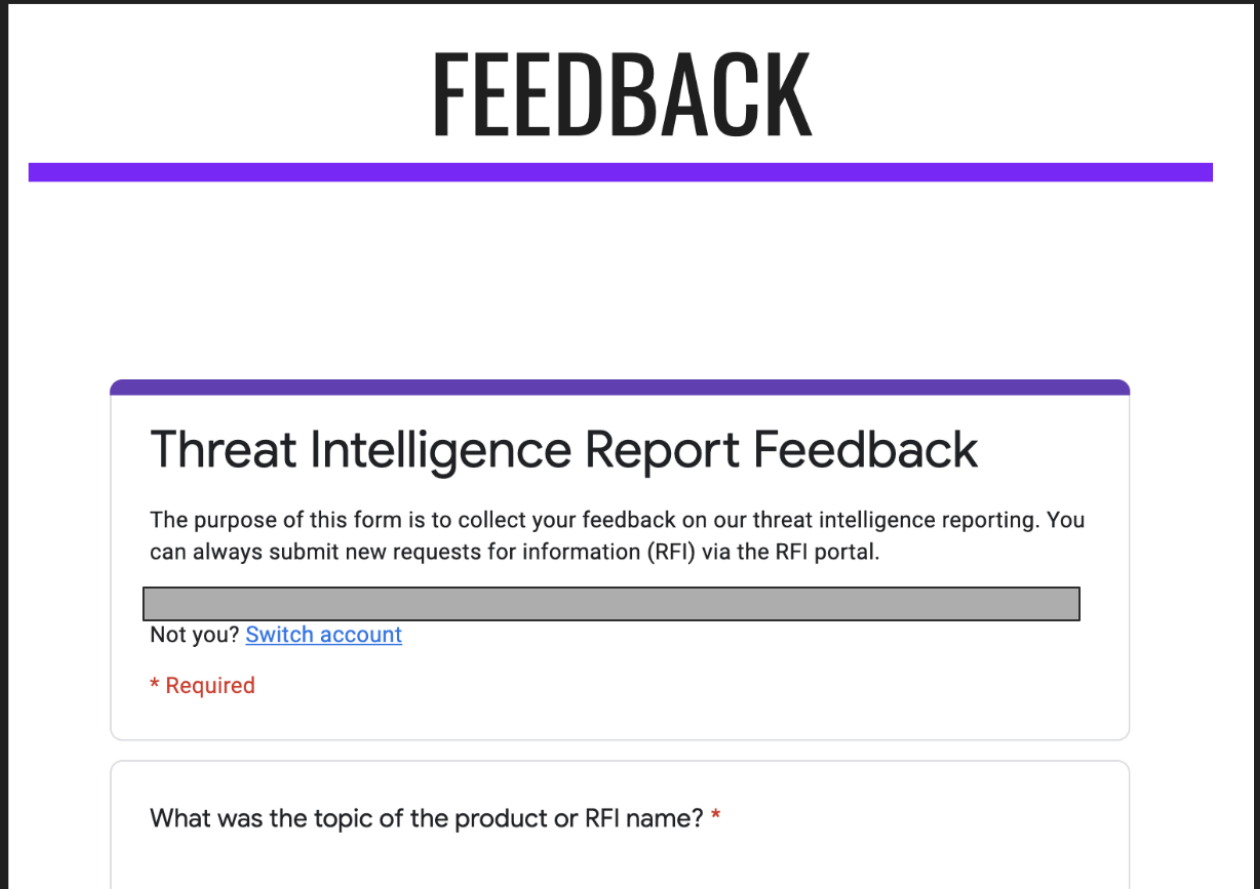
Yield to Feedback

- If the stakeholder has a criticism for your intelligence or the program, something needs to be adjusted
- Make it easy for the stakeholder to submit feedback

Yield to Feedback

- If the stakeholder has a criticism for your intelligence or the program, something needs to be adjusted
- Make it easy for the stakeholder to submit feedback
- Use feedback to set goals for the program
  - Did I ever mention metrics are your friend?

Yield to Feedback



The EASY Framework

Let me leave you with a prediction...

Questions?