The Threat Intelligence EASY Button

January 2020
Once upon a time...

A Story
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
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
<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Requirement</th>
<th>Serial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Security</td>
<td></td>
<td>1.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.3</td>
</tr>
<tr>
<td>Infrastructure Security</td>
<td></td>
<td>2.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.1</td>
</tr>
<tr>
<td>Customer Trust</td>
<td></td>
<td>3.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3.4</td>
</tr>
<tr>
<td>Corporate Security</td>
<td></td>
<td>4.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.5</td>
</tr>
<tr>
<td>Studio InfoSec</td>
<td></td>
<td>5.1</td>
</tr>
<tr>
<td>Device and Content Security</td>
<td></td>
<td>6.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6.3</td>
</tr>
<tr>
<td>Global Content Protection</td>
<td></td>
<td>7.1</td>
</tr>
<tr>
<td>GRIT</td>
<td></td>
<td>8.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8.3</td>
</tr>
<tr>
<td>Open Connect</td>
<td></td>
<td>9.1</td>
</tr>
</tbody>
</table>
The EASY Framework

- Elicit Requirements
- Assess Collection Plan
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

<table>
<thead>
<tr>
<th>Type of Information</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open source or public CTI feeds (DNS, MalwareDomainList.com)</td>
<td>66.2%</td>
</tr>
<tr>
<td>Threat feeds from general security vendors</td>
<td>63.8%</td>
</tr>
<tr>
<td>Community or industry groups such as information sharing and analysis centers (ISACs) and Computer Emergency Readiness Teams (CERTs)</td>
<td>63.4%</td>
</tr>
<tr>
<td>External sources such as media reports and news</td>
<td>63.4%</td>
</tr>
<tr>
<td>Security data gathered from our IDS, firewall, endpoint and other security systems</td>
<td>62.2%</td>
</tr>
<tr>
<td>Threat feeds from CTI-specific vendors</td>
<td>59.8%</td>
</tr>
<tr>
<td>SIEM platform</td>
<td>59.2%</td>
</tr>
<tr>
<td>Vulnerability data</td>
<td>58.6%</td>
</tr>
<tr>
<td>Incident Response and live forensics</td>
<td>55.3%</td>
</tr>
<tr>
<td>Network traffic analysis packet and flow</td>
<td>53.2%</td>
</tr>
</tbody>
</table>
The EASY Framework

- Elicit Requirements
- Assess Collection Plan
- Plan
- Strive for Impact
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)
Intelligence Led Purple Team

Intelligence

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

Continuous Improvement

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).

Strive For Impact
The EASY Framework

- Elicit Requirements
- Assess Collection Plan
- Strive for Impact
- Yield to Feedback
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?
Threat Intelligence Report Feedback

The purpose of this form is to collect your feedback on our threat intelligence reporting. You can always submit new requests for information (RFI) via the RFI portal.

Not you? Switch account

* Required

What was the topic of the product or RFI name? *
The EASY Framework

- Elicit Requirements
- Assess Collection Plan
- Strive for Impact
- Yield to Feedback
Let me leave you with a prediction...
Questions?