How to Get Promoted: Developing metrics to show how threat intel works

Toni Gidwani
Director of Research
@t_gidwani

Marika Chauvin
Senior Threat Intelligence Researcher
@MarSChauvin
Who are we?

Toni Gidwani
Side gig as a Georgetown professor
Maker of gelato

Marika Chauvin
Research nerd
King cake aficionado
The problem: showing value

Classes of metrics

Examples by maturity
How do I show that threat intel provides value to my org?
“Building a Threat Intel Program” Survey Respondents

- Manager / Senior manager
- Director / VP / SVP
- President / CEO / C-Level Exec / Owner
- Other (please specify):
What’s the 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

36%
Disconnect: Just how mature are we?

Executives self-rate maturity much higher

- Analyst: 26%
- Manager / Senior Manager: 29%
- Director / VP / SVP: 47%
- President / CEO / C-Level Exec / Owner: 55%
The problem

When we’re not on the same page...
“Metrics”

60% OF THE TIME

IT WORKS EVERY TIME
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

Measure task completion and efficiency

Am I doing things right?

Measures of Effectiveness

Measure what is accomplished and whether goals are being met

Am I doing the right things?
Measures of Performance

Types of Metrics

Useful for:
- Impact of automation/efficiencies
- Process improvement
- Utilization of resources
- Incentivizing a baseline step

Examples:
- Total alerts issued
- Total Intel 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
Types of Metrics

...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
Self-Reported Money Saved

• 77% saved a significant sum of money in the last year
  ○ Least mature: ~$2k
  ○ Mid-level programs: $1.7 million
  ○ Well-Defined programs: $10 million
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

© 2018 ThreatConnect, Inc. All Rights Reserved.
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
## Key Takeaways: All Metrics aren’t Created Equal

<table>
<thead>
<tr>
<th>Easy</th>
<th>Difficult</th>
</tr>
</thead>
<tbody>
<tr>
<td>Least Valuable</td>
<td>Most Valuable</td>
</tr>
<tr>
<td></td>
<td><strong>Mean cost of breach</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Revenue saved</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Incident criticality impacted by TI</strong></td>
</tr>
<tr>
<td></td>
<td><strong>False positive ratio</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Countermeasures enacted</strong></td>
</tr>
<tr>
<td></td>
<td><strong>New incidents from TI</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Number of reports</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Number of IOCs</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Number of ingested feeds</strong></td>
</tr>
<tr>
<td></td>
<td><strong>AV detections</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Number of reports</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Number of IOCs</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Number of ingested feeds</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Incidents worked</strong></td>
</tr>
<tr>
<td></td>
<td><strong>AV detections</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Incidents worked</strong></td>
</tr>
</tbody>
</table>
Thank You

www.ThreatConnect.com