Metrics and ATT&CK™

Or how I failed to measure everything.
Introduction

1. IoC != intelligence
2. Small overhead for the analyst
3. Better insights
4. One standard framework
ATT&CK™ as a tool

- Stakeholders Management
- Sources Management
- Track and Improve CTI Maturity
Why ATT&CK™

• Metrics generation

• Standardisation and alignment

• Common language

• Derive new requirements

• Source quality and gaps

• Prioritization and focus

Limitations

• Not always a good fit

• Information loss at requirement mapping

• Limited coverage

• All Techniques are equal
Key to successful integration

- Stakeholder management
- Requirements setting + process
- Understanding your environment and assets
- Valuable intelligence sources
- Mapping to ATT&CK

Easy Right?
**Identify the Stakeholders**

**CISO**
- Bank being compromised
- Get a foothold within the bank perimeter
- Initial access
  - Mapped to ATT&CK

**Incident Responder**
- T1 – T7 – T3
  - T1
  - T3
  - T2
  - T6
  - T7
  - T9
  - Spearphishing Attachment
  - Mapped to ATT&CK

**SOC Analyst**
- T1 – T3 – T9

What she said

What she meant

**METRIC**

<table>
<thead>
<tr>
<th>T1</th>
<th>T3</th>
<th>T2</th>
<th>T6</th>
<th>T7</th>
<th>T9</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

= Technique as req.

= Requirements priority
I’m interested in ways to compromise payment systems

Daruk, Payments team

Initial Access (TA0001)

+ “payments”

Review requirements with stakeholder

Priv. Escalation (TA0004)
Valid Accounts (T1078)

Credential Access (TA0006)
Bash History (T1072)

Collection (TA0009)
Input Capture (T1056)
Mapping to the other frameworks

STRIDE: https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)
<table>
<thead>
<tr>
<th>Initiation</th>
<th>Target Compromise</th>
<th>Perform Fraud</th>
<th>Obtain Fraudulent Assets</th>
<th>Assets Transfer</th>
<th>Monetization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing</td>
<td>Malware</td>
<td>Insider Trading</td>
<td>Compromised payment cards</td>
<td>SWIFT transaction</td>
<td>ATM jackpotting</td>
</tr>
<tr>
<td>Spear Phishing</td>
<td>Account-Checking Services</td>
<td>Business Email Compromise</td>
<td>Compromised account credentials</td>
<td>Fund Transfer</td>
<td>Money Mules</td>
</tr>
<tr>
<td>Vishing</td>
<td>ATM Black Box Attack</td>
<td>Scam</td>
<td>Compromised Personally Identifiable Information (PII)</td>
<td>Cryptocurrency exchange</td>
<td>Fund Transfer</td>
</tr>
<tr>
<td>Social Media Scams</td>
<td></td>
<td>CxO Fraud</td>
<td>Compromised Intellectual Property (IP)</td>
<td></td>
<td>Prepaid Cards</td>
</tr>
<tr>
<td>Smishing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Resell Stolen Data</td>
</tr>
<tr>
<td>ATM Skimming</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ATM Explosive Attack</td>
</tr>
<tr>
<td>ATM Shimming</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>POS Skimming</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Extending ATT&CK™

- Only when malicious
- Pragmatic approach
- Get the experts

First attempt at https://github.com/burritoblue/attck4fraud
Requirements mapping with ATT&CK™

ATT&CK techniques are limited

**SOLUTION**
Get creative. Combine. Extend

**LONG-TERM SOLUTION**
Document and engage MITRE/community
The Threat Actors

Actor Alpha
T2 – T4 – T10 – T12

Actor Beta
T3 – T7 – T12 – T14

Organically linked to
Stakeholders
Sources
Products
Mitigations
Levelling up the Stakeholder relation

CISO

T1 - T2 - T6

Asset 1
T6

Asset 2
T1 – T2

Asset 3
T1

Actor Alpha
The Sources and the Products

Source 1
Source 2
Source 3
OSINT
Closed Group

CISO

T1 - T2 - T6

T1 - T4
T3 - T6 - T10
T5 - T7
T2
T9

Landscape
Flash
Thematic
Daily summary

T1 - T4
T3 - T8
T2 - T6
T10
The big picture

Actors
- Alpha
- Beta
- T3
- T3, T7

Stakeholders
- CSO
- Incident Responder
- SOC Analyst

Products
- Flash
- Landscape
- Thematic
- Daily summary

Sources
- Source 1
- Source 2
- Source 3
- Source 4
- OSINT
# Source coverage

<table>
<thead>
<tr>
<th>Source</th>
<th>Stakeholder c.</th>
<th>Actor c.</th>
<th>Usage</th>
<th>AVG RFI score (1-10)</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>9</td>
<td>5 (14)</td>
</tr>
<tr>
<td>S2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>8 (12)</td>
</tr>
<tr>
<td>S3</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>8</td>
<td>3 (11)</td>
</tr>
<tr>
<td>S4</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>6</td>
<td>2 (8)</td>
</tr>
<tr>
<td>OSINT</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>N/A</td>
<td>2</td>
</tr>
</tbody>
</table>

Number in brackets include avg RFI score for the source. RFI score represent the opinion of the analyst.
Source value

RFI feedback not included; Example data
## Product quality

<table>
<thead>
<tr>
<th>Product</th>
<th>Stakeholder covered</th>
<th>Actor covered</th>
<th>Source used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flash</td>
<td>1</td>
<td>1</td>
<td>S2, S3</td>
</tr>
<tr>
<td>Landscape</td>
<td>3</td>
<td>2</td>
<td>S1</td>
</tr>
<tr>
<td>Thematic</td>
<td>3</td>
<td>0</td>
<td>S2, OSINT</td>
</tr>
<tr>
<td>Daily summary</td>
<td>0</td>
<td>1</td>
<td>S2</td>
</tr>
</tbody>
</table>

Combine to actual feedback

= **Product quality**

<table>
<thead>
<tr>
<th>Product</th>
<th>Stakeholder c.</th>
<th>Actor c.</th>
<th>Feedback (1-10)</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flash</td>
<td>1</td>
<td>1</td>
<td>8</td>
<td>10</td>
</tr>
</tbody>
</table>
Level up the team

- Number of technique never covered by a product
- Number of covered tactics/techniques for an actor
- Threat = Capability + Intent + **Coverage**
Because metrics matter

<table>
<thead>
<tr>
<th>Theme</th>
<th>Metric</th>
<th>Implementation complexity</th>
<th>Added value</th>
<th>Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stakeholders</td>
<td>Number of stakeholders on boarded (formally/informally)</td>
<td>low</td>
<td>low</td>
<td>Program sponsor</td>
</tr>
<tr>
<td></td>
<td>Number of intel requirements</td>
<td>medium</td>
<td>medium</td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td>Number of unique intel requirements</td>
<td>medium</td>
<td>medium</td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td>Number of issued products per stakeholder</td>
<td>low</td>
<td>medium</td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td>Number of products within deadline</td>
<td>low</td>
<td>low</td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td>Number of products meeting the initial scope</td>
<td>low</td>
<td>low</td>
<td>Team</td>
</tr>
<tr>
<td></td>
<td>Number of incoming RFI per stakeholder</td>
<td>low</td>
<td>high</td>
<td>Team</td>
</tr>
<tr>
<td></td>
<td>Average score per stakeholder (e.g. success/fail)</td>
<td>medium</td>
<td>high</td>
<td>Program sponsor</td>
</tr>
</tbody>
</table>
Because metrics matter

<table>
<thead>
<tr>
<th>Theme</th>
<th>Metric</th>
<th>Implementation complexity</th>
<th>Added value</th>
<th>Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Products</strong></td>
<td>Number of issued products not linked to a requirement</td>
<td>high</td>
<td>medium</td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td>Number of products issued per requirement</td>
<td>high</td>
<td>high</td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td>Number of requirements without a product</td>
<td>high</td>
<td>high</td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td>Number of issued products per intelligence level (operational, tactical and strategic)</td>
<td>low</td>
<td>medium</td>
<td>Team</td>
</tr>
<tr>
<td></td>
<td>Number of IoC per ATT&amp;CK tactic (via Feed)</td>
<td>high</td>
<td>medium</td>
<td>Team</td>
</tr>
<tr>
<td></td>
<td>Number of IoC per ATT&amp;CK technique (via Feed)</td>
<td>high</td>
<td>medium</td>
<td>Team</td>
</tr>
<tr>
<td></td>
<td>Number of IoC per requirement (via Feed)</td>
<td>high</td>
<td>medium</td>
<td>Team</td>
</tr>
<tr>
<td></td>
<td>Number per issued product type and average score</td>
<td>medium</td>
<td>low</td>
<td>Program sponsor</td>
</tr>
<tr>
<td><strong>Intel sources</strong></td>
<td>Number of requirements satisfied by a source</td>
<td>high</td>
<td>medium</td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td>Number of products making use of a source (which sources are used the most)</td>
<td>low</td>
<td>high</td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td>Average score of outgoing RFIs per source</td>
<td>low</td>
<td>high</td>
<td>Management</td>
</tr>
</tbody>
</table>
## Because metrics matter

<table>
<thead>
<tr>
<th>Theme</th>
<th>Metric</th>
<th>Implementation complexity</th>
<th>Added value</th>
<th>Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Team</td>
<td>Number of alerts handled</td>
<td>low</td>
<td>low</td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td>Average saving thanks to met requirement</td>
<td>medium</td>
<td>medium</td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td>Average time taken to create a report/product (report cycle - days)</td>
<td>low</td>
<td>low</td>
<td>Team</td>
</tr>
<tr>
<td></td>
<td>Number of actors on the watch list</td>
<td>low</td>
<td>low</td>
<td>Program sponsor</td>
</tr>
<tr>
<td></td>
<td>Number of actors on the watch list per actor sophistication</td>
<td>low</td>
<td>low</td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td>Number of actors on the watch list per actor label</td>
<td>low</td>
<td>low</td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td>Number of incidents/action taken created directly from product</td>
<td>high</td>
<td>high</td>
<td>Program sponsor</td>
</tr>
</tbody>
</table>
Final thoughts

• Use your TIP + reporting
• Clear set of stakeholders’ requirements
• Not always a good fit
• Valuable measurable data

Not a silver bullet...but still a bullet!