Effective Threat
Intel
Value of Threat Intelligence

- Threat Intelligence supports:
  - Operations - *What do I do when I detect Threat* X
  - Strategy - *What Threats* should I spend my limited security *budget on*
  - Detection - *How do I detect Threat* X

*Where Threats are actors, malware, and techniques*
True vs False Positives

IoC Matches

% of Matches

Month

Aug Sept Oct

True Positive  False Positive
Non-Actionable matches

IoC Matches

% of Matches

Month

Aug  Sept  Oct

True Positive  Non-Actionable  False Positive
Goal: All IoCs are actionable
- have context
IoC Discovery: Malware vs. Indicator Based

Selected Anomali Malware IoC feeds

Selected Anomali Indicator Expansion feeds

© 2016 Anomali Confidential
The Ultimate Detection Metric: *Reductions in Dwell Time*

<table>
<thead>
<tr>
<th>ORGANIZATIONS MORE VIGILANT ABOUT DISCOVERY</th>
</tr>
</thead>
<tbody>
<tr>
<td>In 2015, the median time from compromise to discovery was cut by 59 days, down from 205 days.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TIME FROM COMPROMISE TO DISCOVERY</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEDIAN</td>
</tr>
<tr>
<td>EXTERNAL NOTIFICATION</td>
</tr>
<tr>
<td>INTERNAL DISCOVERY</td>
</tr>
</tbody>
</table>

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DAYS</td>
<td>DAYS</td>
<td>DAYS</td>
<td></td>
</tr>
<tr>
<td>146</td>
<td>320</td>
<td>56</td>
<td></td>
</tr>
</tbody>
</table>

Source: *M-Trends 2016, FireEye*
IoC Age

Measured IoC Age - $\Delta(Dreg - Ding)$

- Dreg = Domain Registration Creation Date
- Ding = Domain ingest to detection/protection
IoC Age

Median Dwell Time (146 days): Our number to beat

- This Feeds Median Time
- Internal Median Time (56 days)
- External Median Time (320 days)
IoC Age
Effective Detections

- **IoCs**
  - Hash Values
  - IP Addresses
  - Domain Names
  - Network/Host Artifacts
  - Tools
  - TTPs

- **Signatures & Analytics**
  - Tough!
  - Challenging
  - Annoying
  - Simple
  - Easy
  - Trivial

© 2016 Anomali Confidential
Tactical Signatures

**Malware Family - Multiple IoCs**

```
alert tcp any any -> any any (msg:"OilRig backdoor headers order"; content:"Cookie|3A|"; content:"Content-Type|3A| binary|3B| charset|3D|utf-8"; within:512; content:"Content-Length|3A|"; content:"User-Agent|3A| Mozilla/5.0 (compatible|3B| MSIE 9.0|3B| Windows NT 6.1|3B| Trident|2F|5.0"; within:144; content:"Cache-Control: no-cache"; within:64; sid:1236; rev:1;)
```

path:C:\Users\*ntoskrnl.exe
Strategic Signatures

Tactics, Techniques, Procedures - Multiple Families

Window of Exploitation
Technique Detected
Technique Protected

process_name:ntoskrnl.exe AND -path:C:\Windows\System32\ntoskrnl.exe
Event ID 5136, a directory service object was modified can be filtered to give you insight on Kerb PreAuth changes/malicious edits.
Coverage

- establish “trends” / “baseline”
- measure against baseline
  - pattern of life
  - volumetric
<table>
<thead>
<tr>
<th>Goal</th>
<th>Action</th>
</tr>
</thead>
</table>
| Reduce Dwell Time    | ● **Good:** *Measure IoC Age*  
                      ● *Malware and Intrusion data provides proof*  
                      ● *but Orient towards Indicator Expansion methods*  
                      ● **Better:** Tactical Signatures  
                      ● **Best:** Strategic Signatures / Analytics |
| Ensure Coverage      | ● Establish Baseline of “Threat”  
                      ● Measure % Captured vs. Baseline |
| Useful Detections    | ● Measure Enrichment via reduction in Non-Actionable  
                      ● Measure Accuracy via True-Positive vs. False-Positive |

- Collected IoCs / Malware / Signatures != activity on the ground
  - *but OSint is useful to orient around and prioritize*
## Detection Utility

<table>
<thead>
<tr>
<th>Focal Point</th>
<th>Reduces Dwell Time for life of IoC Specific Sample or Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tactical</td>
<td>Specific Toolkit</td>
</tr>
<tr>
<td>Strategic</td>
<td>General Techniques</td>
</tr>
</tbody>
</table>