Building an intelligence-driven organization

Anastasios Pingios

4 May 2020
FIRST Cyber Threat Intelligence Webinar Series
Disclaimer.

All opinions expressed are my own, and do not represent my employer.
About.

- Principal Security Engineer at Booking.com
- Contributor at MITRE ATT&CK framework
- @xorlgr
- SANS GCTI, RecordedFuture Geopolitical Analyst, Bellingcat OSINT, ISS OSINT, ...
Agenda.

● Definition

● Risk versus threat-based approach

● The 5 phases
Definition.

Threat intelligence
Definition.

Threat intelligence

- Intent
- Opportunity
- Capability
Definition.

Threat intelligence

- Product
- Process
Definition.

Threat intelligence

- Product
- Process

Dissemination and Integration

Planning and Direction

Collection

Analysis and Production

Processing and Exploitation

TLP:WHITE
If you know the enemy and know yourself, you need not fear the result of a hundred battles.

Sun Tzu, The Art of War
Definition.

If you **know the enemy** and know yourself, you need not fear the result of a hundred battles.

*Sun Tzu, The Art of War*
Risk vs threat-based approach.

<table>
<thead>
<tr>
<th>EXAMPLE RISK</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Very High</td>
</tr>
<tr>
<td>Very High</td>
<td>Very High</td>
</tr>
<tr>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Very Low</td>
<td>Medium</td>
</tr>
</tbody>
</table>
**Risk vs threat-based approach.**

<table>
<thead>
<tr>
<th>EXAMPLE RISK</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Very High</td>
</tr>
<tr>
<td>Very High</td>
<td>Very High</td>
</tr>
<tr>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Very Low</td>
<td>Medium</td>
</tr>
</tbody>
</table>

**Risk** = **Impact** × **Likelihood**
Risk vs threat-based approach.
Risk vs threat-based approach.

Threat = Opportunity + Intent + Capability
Risk vs threat-based approach.

<table>
<thead>
<tr>
<th>Risk-based</th>
<th>Threat-based</th>
</tr>
</thead>
<tbody>
<tr>
<td>Covers all cases</td>
<td>Very specific</td>
</tr>
<tr>
<td>Well known</td>
<td>Applicable to all levels</td>
</tr>
<tr>
<td>Standardized</td>
<td>Proactive security</td>
</tr>
</tbody>
</table>
Why?
Why?
Why?

The Sliding Scale of Cyber Security
Robert M. Lee - September 2015
Phase 1: The beginning.

- Typically on spare-time
- No Intelligence Requirements? Start small
- Analysis on past incidents
- Build campaigns & threat actor profiles
- Develop simple products and get lots of feedback (WARNING: DO NOT MAKE THIS AN ECHO CHAMBER)
Phase 1: The beginning.

- **Cyber-security team(s)**
  - TI “team”

- **Products**
  - Past campaigns
  - Past threat actor profiles

- **Customers**
  - Cyber-security team(s)
  - Cyber-security leadership

- **KPIs**
  - Consistency of products
  - Incidents analyzed
Phase 2: External threats.

- Map identified threat actors/groups to external ones
- Track their activities and proactively deploy controls
- Develop processes and focus on quality
- Start measuring key indicators
- Share success stories / develop good reputation
Phase 2: External threats.

Cyber-security team(s)

Products
- Actor/campaign tracking
- External/internal mapping

Customers
- Cyber-security team(s)
- Cyber-security leadership

KPIs
- Incident response from TI
- False positive/negative rate
Phase 3: Formal CTI function.

- Clear mission, vision, and purpose
- Goal-driven intelligence - be a force multiplier
- Quality over quantity!
- Start offering intelligence products for all levels (strategic, tactical, and operational) based on PIRs
- Formal team KPIs
Phase 3: Formal CTI function.

- **Cyber-security team(s)**
  - CTI team

- **Products**
  - Support for RFIs
  - Regular threat updates

- **Customers**
  - Cyber-security team(s)
  - Cyber-security leadership

- **KPIs**
  - Response time on RFIs
  - Quality of products
Phase 4: Intelligence-driven security.

- Expand beyond cyber
- Provide intelligence services to all security teams
- Find links between threats from different domains
- Holistic intelligence reporting
Phase 4: Intelligence-driven security.

**Products**
- Analytical support
- Multi-domain intelligence

**Customers**
- All security teams
- Security leadership

**KPIs**
- Metrics of proactive actions
- Teams utilizing TI resources
Phase 5: Intelligence-driven organization.

- Natural progression
- Build and train specialized intelligence teams
- Moving to the “left side of the boom” collectively
- Wider adoption of threat-based prioritization
- Create an internal intelligence community
Phase 5: Intelligence-driven organization.

- **KPIs**
  - Per domain KPIs
  - Deviations from standards

- **Company**
  - Security
  - Finance
  - Legal
  - R&D
  - Sales

- **Products**
  - Analytical support
  - Domain specific RFIs

- **Customers**
  - All company teams
  - All company leadership

- **Product development**
  - TI teams

- **All company teams**
  - TI teams

- **All company leadership**
  - TI teams

- **Customers**
  - Analytical support
  - Domain specific RFIs
Summary.

**Phase 1:** Beginning

**Phase 2:** External threats

**Phase 3:** Formal CTI function

**Phase 4:** Intelligence-driven security

**Phase 5:** Intelligence-driven organization

**Threat-based**

**Risk-based**
References.

- Conducting Risk Assessments, NIST 800-30
- MITRE ATT&CK framework
- The Sliding Scale of Cyber Security, Robert M. Lee - September 2015
- Left of boom: Do we actually do this?, Anastasios (xorl) Pingios - December 2019