Threat Intelligence Buyer’s Guide

SANS CTI Summit, 10 February 2014

Rick Holland
@rickhholland
Principal Analyst
Last year

“If it bleeds we can kill it” Leveraging CTI to take the fight to the adversary

Rick Holland, Senior Analyst
March 22, 2013
@rickholland
This year, Arnold’s back!!
Agenda

› Threat intelligence trends
› Evaluating threat intelligence
› Recommendations
Forrester defines threat intelligence as:

- Details of the motivations, intent, and capabilities of internal and external threat actors. Threat intelligence includes specifics on the tactics, techniques, and procedures of these adversaries. *Threat intelligence's primary purpose is to inform business decisions regarding the risks and implications associated with threats.*
Threat intelligence trends

75% report that establishing or improving threat intel capabilities is a top priority.

Which of the following initiatives are likely to be your firm's top IT security priorities over the next 12 months?

Source: Forrsights Security Survey, Q2 2013

Threat Intelligence Salary Data

Source: Indeed.com
Actionable intel meet Terry Tate

“The leading provider of actionable intelligence ...”
Challenges

- Gleaning intelligence from a multitude of feeds and data
- Dealing with variances in data quality and relevancy
- Validating third-party intelligence
- Tactical focus of intelligence programs
Operationalizing intelligence = cat herding
Operationalizing intelligence
Threat intelligence sharing

- We share at about the same speed that George R.R. Martin writes novels, which is slow
- Quid pro quo and relationship driven
- You cannot automate trust
Sharing standards adoption

› FS-ISAC & DHS are driving adoption of STIX/TAXII
  • STIX (Structured Threat Information eXpression)
  • TAXII (Trusted Automated Exchange of Indicator Information)

› FS-ISAC members are pushing vendors to support them
My threat intel can beat up your threat intel

Have you ever been in a vendor meeting and heard the vendor extol the greatness of their threat intelligence? You may have ever seen a slide that looks similar to this:

Unparalleled World Class Threat Intelligence

The vendor probably proceeded to highlight the key differentiators that make their threat intelligence network stand second to none. Bullet points containing statistics like this surely followed:

- Global coverage, in well over 100 countries
- 50 million network devices
- 50 billion web queries each month
- 30 billion emails a month
- 100 million users
Crowded market place – research preview
Intelligence providers deliver

Examples:
- Threat indicator feeds (host/network)
- Cryptolocker analysis

Examples:
- Executive briefs
- Campaign analysis
- Industry specific threat assessments
Agenda

› Threat intelligence trends
› Evaluating threat intelligence
› Recommendations
Before we start
Before we start, **STOP**
You have to have an actual strategy

Jerry “the owner” isn’t happy with Jerry “the general manager”
Before we start, stop

› What is your mission?
› What are your intelligence requirements?
› Develop requirements:
  • What threat actors target you?
  • What are they after?
  • Do you know your organization's priorities?
  • Do you know the risks to your business?
Align with business risks

Interruptions in our supply chain or increased commodity prices and supply chain costs could adversely affect our gross margins, expenses and results of operations.

We are dependent on our vendors to supply merchandise in a timely and efficient manner. If a vendor fails to deliver on its commitments, whether due to financial difficulties or other reasons, we could experience merchandise out-of-stocks that could lead to lost sales. In addition, a large portion of our merchandise is sourced, directly or indirectly, from outside the United States, with China as our single largest source. Political or financial instability, trade restrictions, the outbreak of pandemics, labor unrest, transport capacity and costs, port security, weather conditions, natural disasters or other events that could slow port activities and affect foreign trade are beyond our control and could disrupt our supply of merchandise and adversely affect our results of operations. In addition, changes in the costs of procuring commodities used in our merchandise or the costs related to our supply chain, including labor, fuel, tariffs, and currency exchange rates could have an adverse effect on gross margins, expenses and results of operations.

Failure to address product safety concerns could adversely affect our sales and results of operations.

If our merchandise offerings, including food, drug and children’s products, do not meet applicable safety standards or our guests’ expectations regarding safety, we could experience lost sales and increased costs and be exposed to legal and reputational risk. All of our vendors must comply with applicable product safety laws, and we are dependent on them to ensure that the products we buy comply with all safety standards. Events that give rise to actual, potential or perceived product safety concerns, including food or drug contamination, could expose us to government enforcement action or private litigation and result in costly product recalls and other liabilities. In addition, negative guest perceptions regarding the safety of the products we sell could cause our guests to seek alternative sources for their needs, resulting in lost sales. In those circumstances, it may be difficult and costly for us to regain the confidence of our guests.

If our efforts to protect the security of personal information about our guests and team members are unsuccessful, we could be subject to costly government enforcement actions and private litigation and our reputation could suffer.

The nature of our business involves the receipt and storage of personal information about our guests and team members. We have a program in place to detect and respond to data security incidents. To date, all incidents we have experienced have been insignificant. If we experience a significant data security breach or fail to detect and appropriately respond to a significant data security breach, we could be exposed to government enforcement actions and private litigation. In addition, our guests could lose confidence in our ability to protect their personal information, which could cause them to discontinue usage of REDcards, decline to use our pharmacy services, or stop shopping with us altogether. The loss of confidence from a significant data security breach involving team members could hurt our reputation, cause team member recruiting and retention challenges, increase our labor costs and affect how we operate our business.
The Intelligence Cycle

› Use the Intelligence Cycle as a framework to evaluate intelligence sources
1) Planning and direction

- How does the provider develop intel requirements?
- How do the provider’s intelligence requirements align with yours?
  - Threat actor, vertical specific, malware, geopolitical
- How does the provider work with you? What feedback mechanisms exist?
2) Collection

★ What are providers collection capabilities?
  • OSINT, HUMINT, language coverage, geos
  • P2P, honeypots, Tor, crawlers, professional service engagements, vendor products footprint

★ Do collection capabilities align with your intelligence requirements?

★ Overcome the “sources and methods” challenge
2) Collection continued

› Collection management should be a function within your intelligence team
› You must be able to identify your collection gaps
› Then you can make a build versus buy decision
3) Processing

- Raw data is transformed into information for analysis
- What platform is used for processing?
- How does processing enable *timely* intelligence production?
- How do you prioritize processing based on intelligence requirements?
4) **Analysis and production**

› Understand the analytic methodology used to derive intelligence (Diamond)

› What analysis platform is used? (Is it available to customers?)

› Who is doing the analysis? Background and skillsets?
  - Intelligence community
  - Incident responders
  - Malware analysts
4) Analysis and *production* continued

<table>
<thead>
<tr>
<th>Common intelligence products</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability analysis</td>
</tr>
<tr>
<td>Campaign analysis</td>
</tr>
<tr>
<td>Periodic summaries</td>
</tr>
<tr>
<td>(weekly/monthly)</td>
</tr>
<tr>
<td>Brand monitoring</td>
</tr>
<tr>
<td>Custom products</td>
</tr>
</tbody>
</table>
## Measuring intelligence

<table>
<thead>
<tr>
<th>Characteristics of valuable intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accurate</td>
</tr>
<tr>
<td>Timely</td>
</tr>
<tr>
<td>Relevant</td>
</tr>
<tr>
<td>Tailored</td>
</tr>
<tr>
<td>Predictive</td>
</tr>
<tr>
<td>Actionable</td>
</tr>
</tbody>
</table>

© 2014 Forrester Research, Inc. Reproduction Prohibited
# Measuring intelligence

## Characteristics of valuable intelligence

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accurate</td>
<td>Pretty obvious</td>
</tr>
<tr>
<td>Timely</td>
<td>Meh, stale indicators</td>
</tr>
<tr>
<td>Relevant</td>
<td>Aligned with intelligence requirements</td>
</tr>
<tr>
<td>Tailored</td>
<td>Audience appropriate (tactical/strategic)</td>
</tr>
<tr>
<td>Predictive</td>
<td>Anticipates threat activity</td>
</tr>
<tr>
<td>Actionable</td>
<td>Can be <strong>easily</strong> integrated into security controls</td>
</tr>
</tbody>
</table>

Do you actually get hits? Compare with peer orgs.
5) Dissemination

› How do you help me make the intelligence actionable?
5) Dissemination

› How do you help me make the intelligence actionable?
  
  • A .pdf file?
  • An email list?
  • A portal I have to login to?
5) Dissemination

› How do you help me make the intelligence actionable?
  • A .pdf file?
  • An email list?
  • A portal I have to login to?

› Terry Tate is still out there
5) Dissemination

› How do you help me make the intelligence actionable?
   • A .pdf file?
   • An email list?
   • A portal I have to login to?

› Terry Tate is still out there

› XML, JSON, STIX, IODEF, OpenIOC are better answers
5) Dissemination continued

Vendors must make APIs available to:
  • Permit enterprises with development skills/bandwidth customization capabilities (1%ers)

Better living through integrations
  • Those without software development skills will have to rely upon product integrations
  • NetCitadel has an interesting offering that automates (or semi-automates) responses to firewalls and proxies
The Intelligence Cycle repeats
Agenda

- Threat intelligence trends
- Evaluating threat intelligence
- Recommendations
Recommendations

1) Avoid Expense in Depth
Expense in Depth – Are you more secure?
The 80s called, they want their security strategy back

Don’t blindly invest in intelligence

Instead:

- Let intelligence requirements drive investment
- Invest based on collection gaps
- Measure your intelligence sources effectiveness
- And continue to do so periodically
Recommendations

2) Focus on the Intelligence Analysis Platform
Orchestrate your intelligence activities

› Quarterbacks orchestrate on the field
Orchestrate your intelligence activities

› Quarterbacks orchestrate on the field
Orchestrate your intelligence activities

› Quarterbacks orchestrate on the field
An Intelligence Analysis Platform is your quarterback
Intelligence Analysis Platform capabilities

- Rate intelligence source value
- Manage threat indicators
- Asset aware
- Have an API for making intelligence actionable
- Enables analysis (visualization, pivoting)
- Provide enrichment
  - Active DNS, GeoIP, Maltego, Passive DNS, VirusTotal
# Intelligence Analysis Platforms

<table>
<thead>
<tr>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Squared ThreatConnect</td>
</tr>
<tr>
<td>Detica CyberReveal</td>
</tr>
<tr>
<td>IBM i2 Analyst's Notebook</td>
</tr>
<tr>
<td>Lockheed Martin Palisade</td>
</tr>
<tr>
<td>Lookingglass ScoutPlatform</td>
</tr>
<tr>
<td>Maltego</td>
</tr>
<tr>
<td>MITRE CRITs (Collaborative Research Into Threats)</td>
</tr>
<tr>
<td>Palantir</td>
</tr>
</tbody>
</table>
Recommendations

3) *Have an actual strategy*
Final thoughts

› Don’t be Jerry Jones, proceed wisely
› Develop intelligence requirements that focus both internally and externally
› Manage collection capabilities
You must demonstrate value

An intelligence led defense has significant operating costs:

• $100k analysts (How many does your org have?)
• Hundreds of thousands to millions of dollars in technology investment

How to show value

• Produce strategic intelligence products for executives
• Use intelligence for portfolio management
• Decrease dwell time metrics
• Communicate cost avoidance (Leverage financial impact data from public companies in your sector i.e. TGT 10K)
Free research

› Follow me on Twitter for updates on upcoming research
  • Previewed today: *Market Overview: Threat Intelligence Service Providers* (May)
  • Forrester's Targeted Attack Hierarchy Of Needs (April)

› Participate in a research interview and get the final report for free (anonymous)

› Provide input that can drive vendor strategy
My favorite
Thank you

Rick Holland
+1 469.221.5300
rholland@forrester.com
@rickholland

forrester.com