Where Technology Means More™

How Threat Intelligence affects Business Risk

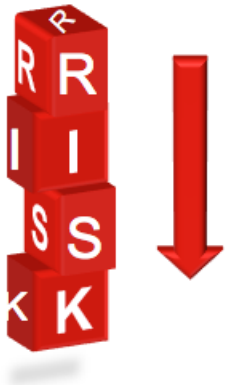
Tom Bowers

Chief Security Strategist

October 2015

Security as Business Risk

- Security is just another business risk similar to:
  - Market risk
  - Customer risk
  - Supply chain risk
  - Compliance risk
  - Legal risk…etc



Until now we've had no way to link business risks to actual threats

Business Risk is Why Threat Intelligence is so Important

Gartner

"Gartner estimates this market will reach almost **$1.5 billion by 2018**, from more than $250 million in 2013"

Ruggero Contu, Rob McMillan
Competitive Landscape: Threat Intelligence Services, Worldwide, 2015
Published: 14 October 2014

Gartner

Strategic Planning Assumption:
"By 2018, **60% of large enterprises globally will utilize commercial threat intelligence services** to help inform their security strategies."

Rob McMillan & Khushbu Pratap
Market Guide for Security Threat Intelligence Services
Published: 14 October 2014

Gartner

"Many vendors can provide raw information, but there are **only a comparative few that provide true intelligence capabilities.**"

Rob McMillan & Kelly Kavanagh
Technology Overview for Security Threat Intelligence Service Providers
Published: 16 October 2013

Slide content courtesy of iSight Partners

Commercial Threat Intelligence is changing Security Programs

Defining Threat Intelligence

Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.

Gartner 16 May 2013 G00249251

Commercial Threat Intelligence Types

- Machine Real Time Intelligence (MRTI) **fed through APIs**
  - Webroot
  - Norse
- Analytical / Contextual (people driven)
  - iSight
  - Crowdstrike

~25 vendors in 2014, 75 in place today (and growing weekly)

Sensitive Data:
Defining the Business Risk

Sensitive Data Identification

- Business leadership discussions
  - C Level
  - Board
- Regulatory
- Compliance

Think big buckets, not detailed data classification
Could be business processes, positive/negative intellectual property…

Sensitive Data Prioritization

- Extinction Level Event (could go out of business)
  - VW ?
  - Cardsystems (payment card processor)
- Major (stock price drop, reputational hit, C-Level job losses)
  - Target
  - OPM
- Minor (PR hit but survivable)
  - TJ Maxx
  - JP Morgan Chase

Where Technology Means More™

Utilizing Threat Intelligence

Implementing an Intelligence Led Security Program

1. **Understand your threat reality**
2. **Create intelligence collection requirements**
3. **Implement a proactive threat intelligence capability** to monitor the relevant threat environment to your business
4. **Integrate threat indicators** delivered from intelligence provider(s) into your security technology, operations, workflow, and communications.
5. **Correlate incident and threat indicators** to the associated threat context to inform impact value and prioritization.
6. **Train like you fight** - Implement a custom training program that emulates the adversaries that pose the greatest risk to your business and **train as a team**.

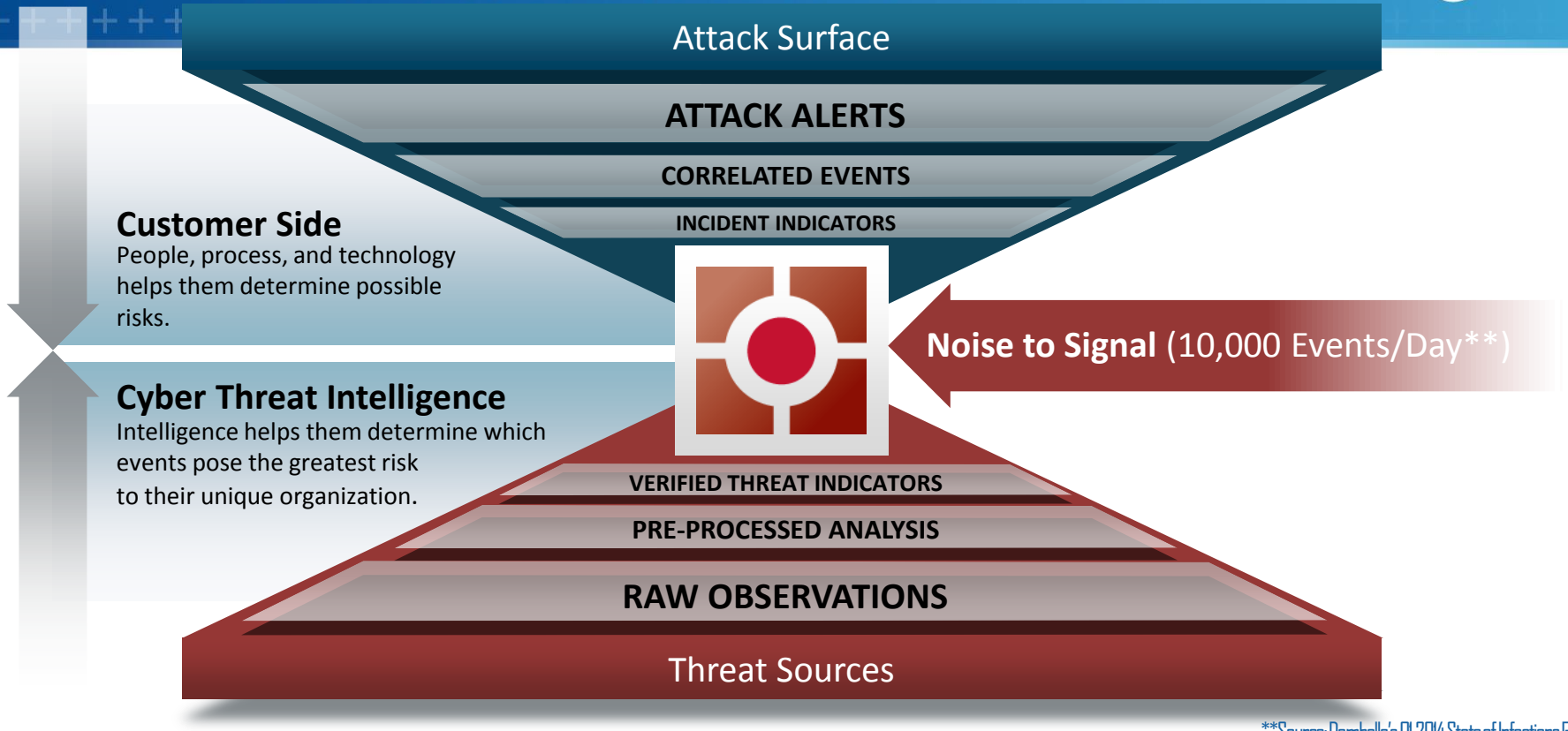
Slide content courtesy of iSight Partners

Two years to fully operationalize this program

Phase	Effort	Elapsed time
Identify and assess complex risk	1 month	1 month
Strategize and agree options with line of business	2 months	3 months
Write business case	3 months	6 months
Wait for executive committee slot to get approval	3 months	9 months
Wait for funding	4+ months	13+ months
Start the project	1 month	14+ months
Implementation (example)	6 months	20+ months

Gartner

Shrink the Problem and Improve Prioritization



**Source: Damballa's Q1 2014 State of Infections Report

Benefits to Threat Intelligence

- Focused security spending on actual threats to your business
  - **Versus the current perceived threat model**
- Instantaneously **reactive** and improving **predictive** business risk threat response
- Improved business risk threat mitigation metrics (is your security program effective?)

tbowers@eplus.com