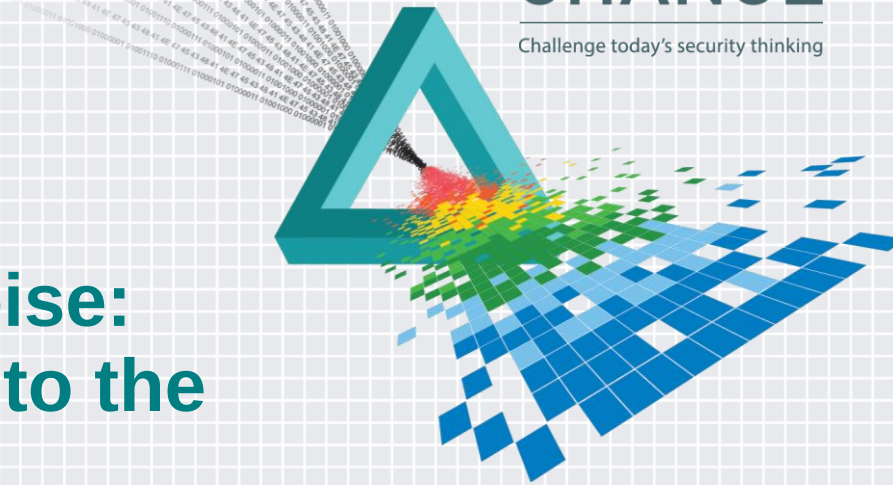
RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking



SESSION ID: SPO2-T09

Separating Signal from Noise: Taking Threat Intelligence to the Next Level

Doron Shiloach

X-Force Product Manager
IBM
@doronshiloach

Agenda

- Threat Intelligence Overview
- Current Challenges
- Solutions
- X-Force
- Questions

The Threat Intelligence Market is growing …

- SANS Cyber Threat Intelligence Summit 2014
  - 3 Courses, 2 Instructors

- SANS Cyber Threat Intelligence Summit 2015
  - 5 courses, 6 instructors

- Threat Intelligence services market size 2013*
  - $250M in 2013

- Threat Intelligence services market size 2018*
  - $1.5B in 2018

*Gartner, Competitive Landscape: Threat Intelligence Services, Worldwide, 2015, October 2014 G00261001

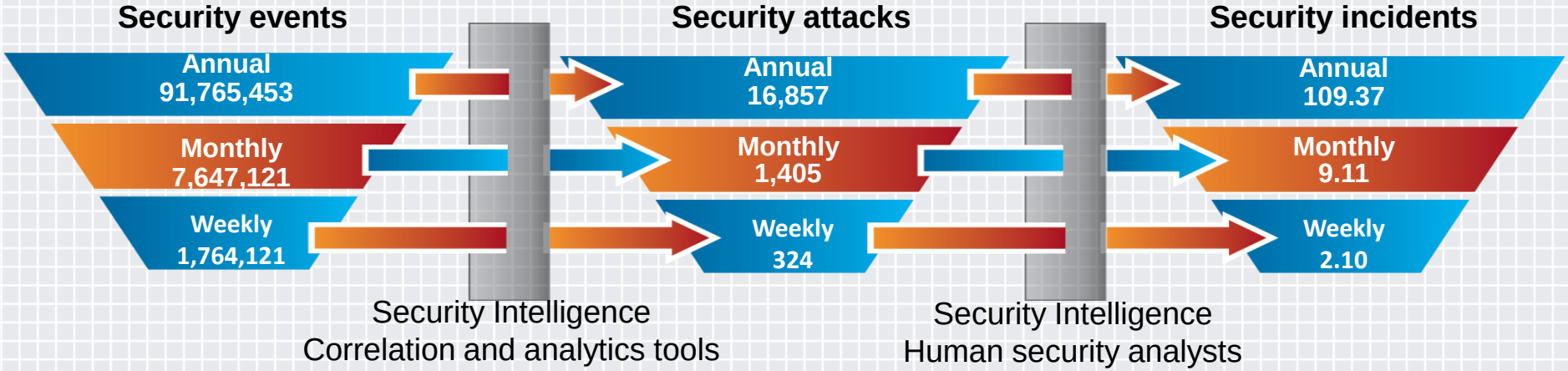
… and maturing from an industry perspective

- Definition of threat intelligence
  - ‘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.
- Importance as part of any organization’s suite of tools
- The criteria for evaluation is coalescing, for example …
  - Where is it sourced from?
  - How often is it updated?
  - Is it vetted by humans?
  - Does it focus on a specific industry?

*Gartner, Definition: Threat Intelligence, Rob McMillan, May 2013, refreshed September 3, 2014, G00249251

Threat intelligence does help

Utilization of threat intelligence can yield a significant reduction in security incidents, as well as speed to respond



Events: up 12% year on year to 91m

Observable occurrences in a system or network

Attacks: Increased efficiencies achieved

More efficiency in security processing to help clients focus on identified malicious events

Incidents: up 22% year on year

Attacks deemed worthy of deeper investigation

Security teams are using multiple sources of intelligence to identify cyber threats

65% of enterprise firms use external threat intelligence to enhance their security decision making

Analysts can glean insights from a wide variety of sources

Data allows analysts to generate alerts

Time spent on analysis can be applied to implementation

Agenda

- Threat Intelligence Overview
- Current Challenges
- Solutions
- X-Force Exchange
- Questions

Security teams are using multiple sources of intelligence to identify cyber threats … the other side

65%

of enterprise firms use external threat intelligence to enhance their security decision making

However, security teams lack critical support to make the most of these resources

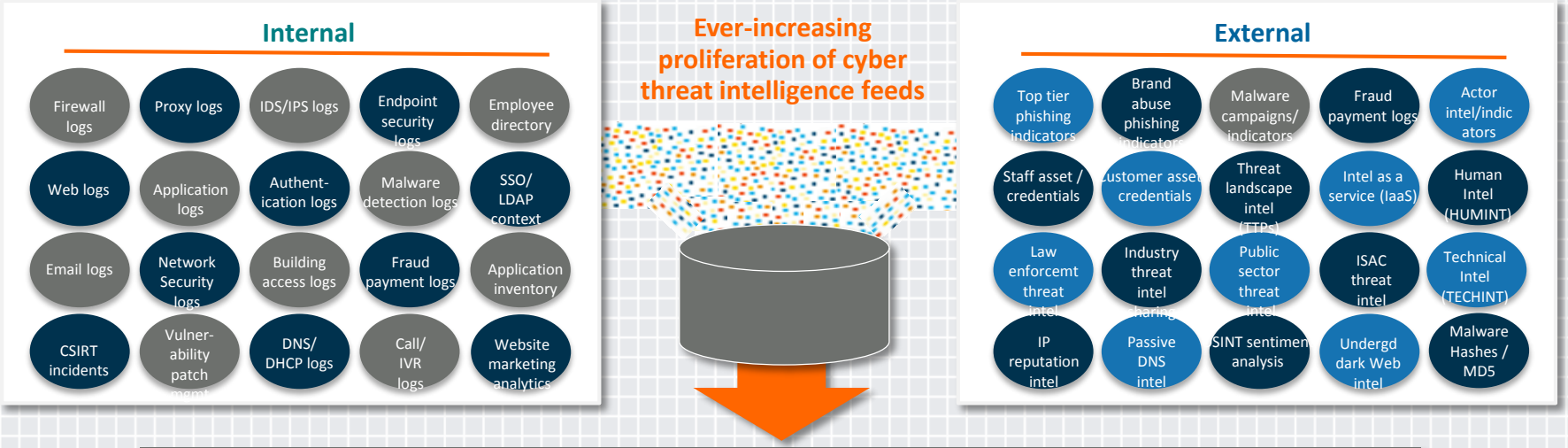
Analysts can't separate the signal from the noise

Data is gathered from untrusted sources

It takes too long to make information actionable

Operationalizing it can be costly and complex

When shopping for intelligence sources, organizations can be overwhelmed by choices as well as the cost and complexity to operationalize and gain a return on investment



Advanced analytics and human intelligence must be applied and integrated into the organization to leverage the value of all the data

Agenda

- Threat Intelligence Overview
- Current Challenges
- Solutions
- X-Force
- Questions

Key capabilities in a solution

- But first, let's think of the ideal requirements
  - Know everything about the particular observable that starts your investigation, i.e. historical information
  - Know everything your colleagues in the same industry know about that particular observable
  - Apply everything you and your colleagues know to the controls that exist in your infrastructure in order to better protect your organization

The real value of threat intelligence lies in its application to your business – to turn insight into action

Without insight, organizations struggle to understand and stay ahead of the threat

- Potential attacks can be overlooked if the attacker's methods and motives are unknown
- Armed with this intelligence, organizations can take action ahead of threat to proactively adapt security strategy, remediate vulnerabilities and monitor for impact
- By applying intelligence upfront, an organization can optimize security resources, increase efficiencies, reduce costs and improve risk management

Threat intelligence sharing has become essential

- The bad guys are doing it
- It helps provide insight, context, and confidence with respect to the information that is being observed, i.e. an isolated attack or part of a broader industry-wide attack
- It benefits both the organization and the broader community
- Ranges from technical information on a particular piece of malware to more strategic, unstructured content

The current state of threat intelligence sharing

- E-mail and informal gatherings
- ISACs – Information Sharing and Analysis Center
  - Financial Services, National Health, Information Technology
- Threat Intelligence Platforms
  - Dynamic market with both established players and startups
- Machine Readable Threat Intelligence
  - STIX - Structured Threat Information Expression
  - TAXII – Trusted Automated Exchange of Indicator Information
  - Cybox – common structure for cyber observables

Agenda

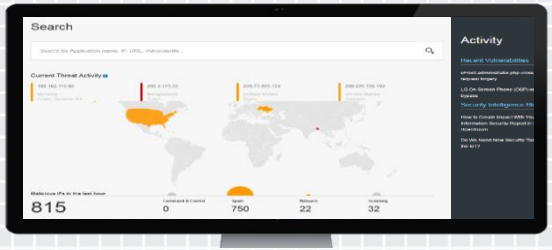
- Threat Intelligence Overview
- Current Challenges
- Solutions
- X-Force
- Questions

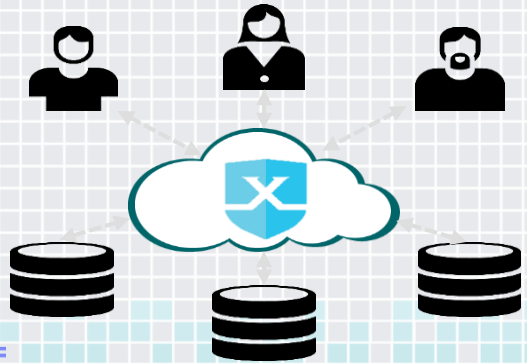
X-Force: Advanced Security & Threat Research

The mission of X-Force

- **Monitor** and evaluate the rapidly changing threat landscape
- **Research** new attack techniques and develop protection for tomorrow's security challenges
- **Educate** our customers and the general public
- **Distribute** Threat Intelligence to make IBM solutions smarter

Access to a broad range of threat intelligence data





Threat indicators

- IPs, URLs, vulnerabilities, web applications, malware
- Additional context
  - Passive DNS, historical information
  - Pivoting on each observable
- Anonymized customer information

Sources

- Machine-generated intelligence from crawler robots, honeypots, darknets, and spamtraps
- Multiple third party and partner sources of intelligence

Additional correlation is key to insights

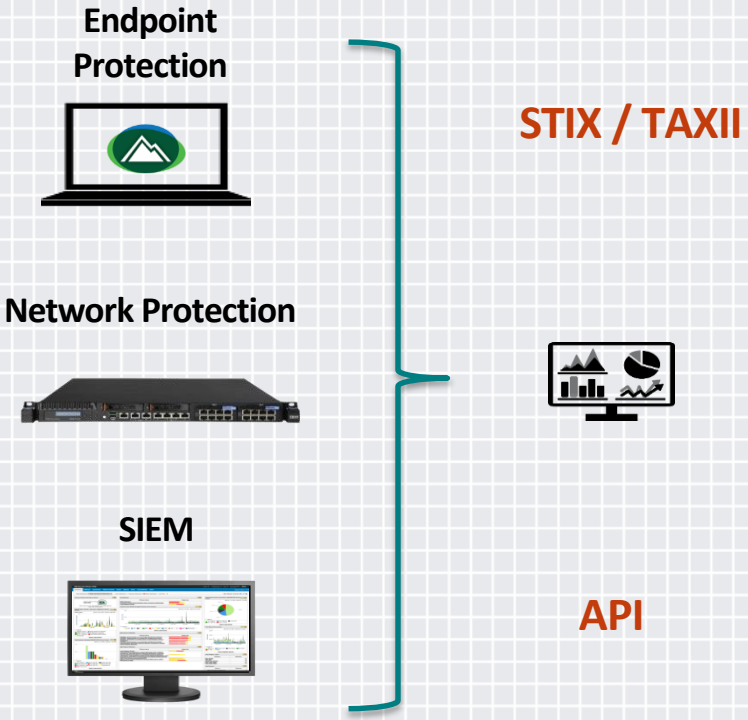
Cross-reference the following information

- Customers targeted
- Industries affected, i.e. % of healthcare, financial, manufacturing, etc.
- Attack sequence and tools
- Vulnerabilities affected

Benefits

- Reduction of false positives by validating against multiple criteria
- Prioritization of attacks

An integrated solution helps tie information to action



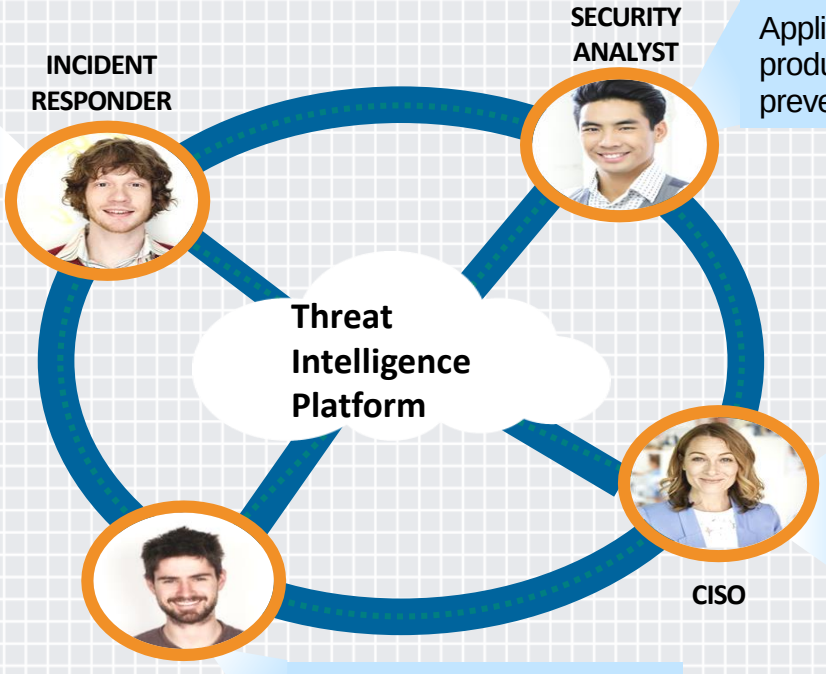
The foundation for integration

- Threat intelligence dynamically updated on a minute-by-minute basis
- Each product/service can access information from the others

Examples

- SIEM products can act on and get context from threat intelligence
- APIs provide technical users the ability to build the proper solutions, with the most flexibility

Share information among teams



Collects latest new indicators of compromise

Applies IOC information to products to remediate and prevent intrusions

Understands high-level threat landscape and status of issues via dashboard of information

Communicate with clients and provide information

Human intelligence is the difference

- Different perspectives on the same set of information
- Each user has own requirements/use cases

Steps you can take today … on tools

- Understand your threat intelligence
  - Relevance
  - Integration
  - Efficiency in sharing among products and teams

- Understand machine readable threat intelligence
  - STIX – stix.mitre.org
  - TAXII – taxii.mitre.org
  - Cybox – cybox.mitre.org
  - APIs – RESTful, JSON, XML, etc.

Steps you can take today … on processes

- At a security team level
  - Identify information you have
  - Collaborate effectively
    - Within the organization
    - With other colleagues in the industry, i.e. ISACs

- At a company level
  - Team with CIO/CISO
  - Understand and address silos and legal issues

*Source: Rick Holland, Forrester Research

Agenda

- Threat Intelligence Overview
- Current Challenges
- Solutions
- X-Force
- Questions