Building a Threat Intelligence Program

Michael Smith, CISSP-ISSEP
APJ Security CTO
mismith@akamai.com
@rybolov

Straw Poll: What Is Threat Intelligence?

Data feeds for purchase

Big Data, Big Data, Big Data

OSINT

Output from a SIEM

Tools dumps

Executive reports

Reporting from your vendors

Blogs and RSS

Things that if you ignore you're now negligent

Too much noise, not enough signal

The greatest thing since Hainanese Chicken Rice

Akamai CSIRT

Customer Security Incident Response Team (CSIRT):

Incident Response for Akamai customers

HTTP(s), DNS, and the infrastructure

Threat briefs

Out of scope: APT, endpoints, email, authentication

We collect and provide information:

OSINT

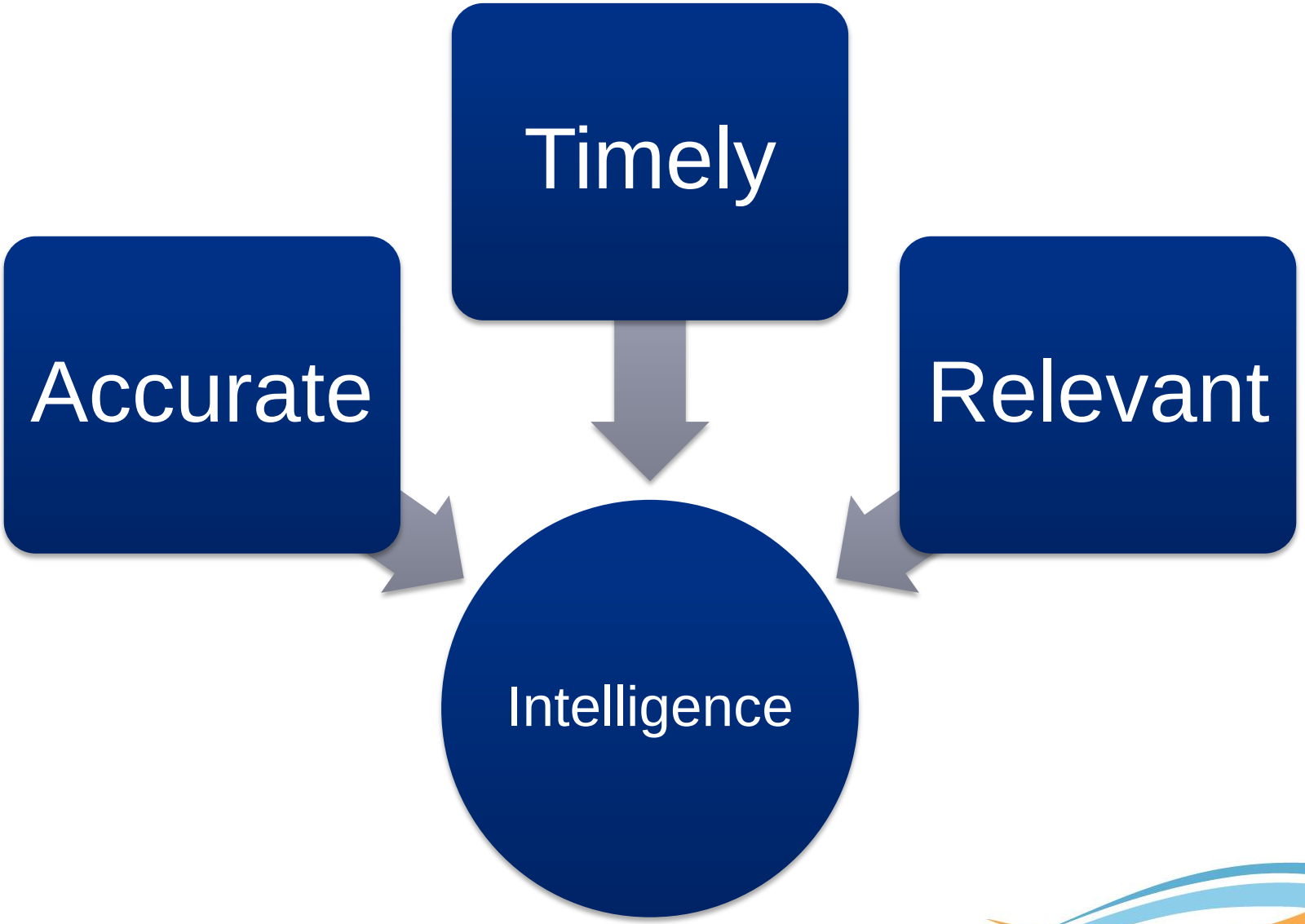
Coordination with peer CERT/SIRT/SOC

Threat intelligence

Discussions with policy-makers

Customer outreach (internal and direct)

Qualities of Good Intelligence



How the Intelligence World Does It

Intelligence Requirements
(questions to answer)

Indicators
(which data points can prove/disprove the question)

Coverage
(how to find out the data points)

Akamai CSIRT's Intelligence Requirements

Which customers need our help as incident responders?

- Which active or future campaigns target our customers?
- Have any customers been impacted by an attack?
- Are their any attacks that could spread to other targets?

Are there any additional things that we can do to protect our customers?

- Are there any new tools that evade our controls set?
- Are there any attack indicators that we should be looking for temporarily during an event?
- Have we seen any new types of attacks?
- Are there activities associated with particular attacks that we should also look for?

My Sources

Incident response activities: alerts and investigations

OSINT

- Scumblr
- Site scraping
- “Is it a customer?” tool

Email lists

ISACs

- Financial Services
- Communications

Big Data

- WAF
- Firewall

Selective data feeds

The Big Ugly Web Attack Tool Search

(xss | "cross site scripting" | csrf | xsrf | "cross site request forgery" | sqli | "sql injection" | "remote code execution" | RFI | "remote file include" | LFI | "local file include" | "command injection") (site:pastebin.com | site:gist.github.com)

OSINT Search for Impacts

site:google.com/newspapers (site|website|web) (hacktivist|hacked|ddos|defaced|"data breach") –”to death”

Then We Started Using Traffic Light Protocol

Classification and Information Types

TLP Classification	What It Contains
Red	Non-public data breach of or attack on a specific customer or prospect listed by name. Non-public blocking rules, the disclosure of which would severely impact our ability to protect our customers. Example attack code. Information derived from classified (Top Secret, Secret, Confidential, etc) or government sources. Information such as attacker physical addresses which could be acted upon that would let the attackers know that they are under surveillance or being investigated. Data which could expose the aformentioned information types through a simple google search.
Amber	Tactics, techniques, and procedures for a specific threat actors or group thereof. Blocking rules such as IP blacklists or custom WAF rules.
Green	General trends. High-level blocking rules such as standard (ie, Core Rule Set) WAF rules and the application thereof. General Akamai platform capabilities normally releasable under NDA. Any information of which the public and inadvertent disclosure of would not impact customers or Akamai's ability to protect them from attackers.
White	Marketing materials. News articles. Blog posts.

Two Views of Sharing Communities

Hub and Spoke	**Peer to Peer**
ISAOs	Event-centric
Regulators	Less-developed
Government-sponsored	Cross-industry
Industry-specific	Cross-discipline

How We Share Threat Intelligence

Case Study: Login Abuses

Actively worked October 2012-May 2013 and then again later

35+ customers initially affected

Created TLP-Red advisory with all the details

Internal release to security operators

Removed “naughty bits” to make it TLP-Green

Outreach to industries

Corporate blog

Putting it all Together

Start with what you know now

Questions to answer

Use existing tools

Get coverage that you can process

Join/build a community with your peers

Share what you can

Thank You!

mismith@akamai.com

@rybolov