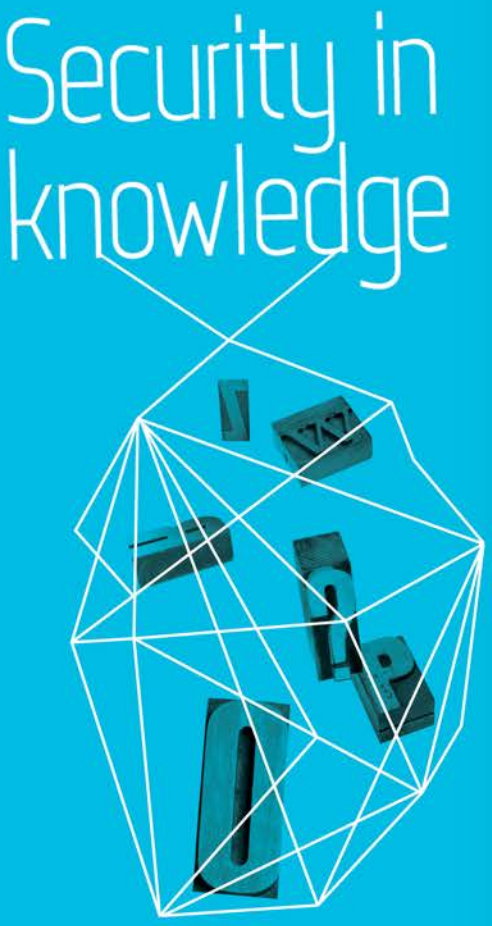
RSA CONFERENCE ASIA PACIFIC 2013



ADVANCED THREATS AND INTELLIGENT DEFENSE

Amit Yoran
Senior Vice President of Products, RSA

Session ID: SEC-T04
Session Classification: Intermediate

Agenda

- Overview of current threats
- Detection and defense

Threat Landscape Overview

- Crimeware as a Service (CaaS)
  - DDoS, Hacking services
- Crimeware Exploit Kits
  - Eleanor, Liberty, Blackhole, Poison Ivy
- Botnets
  - Zeus, Andromeda, SpyEye
- Malicious Code & Content Networks (Malnets)
- Fraud Networks (Fraudnets)
- Laundering Networks
- Spam, Spear Phishing and Targeted Phishing
- Malicious Infector Sites
- Waterholing Sites
- APT campaigns
- SMT campaigns
- Criminal and subnational campaigns

Scams are getting cooler

- Betting on “Rock Paper Scissors”

Usual scam links

Manufacturer DDoSed after Firefox announcement

Mozilla's Firefox OS smartphone to be launched in Japan soon through KDDI

posted on FEBRUARY 25, 2013 by IDA TORRES in TECH

Tales From the Darkside: Firefox OS Phone Manufacturer DDoS'ed

Posted by Fielder Feb 25, 2013

Destination Organization (13 items)
kddi kddi corporation (3,990) - kddi corporation (3,990) - research organization of information and (4) - wakayama prefectural board of education (4) - miyazaki international college (1) - mais(miyazal

Destination City (20 items)
tokyo (862) - osaka (277) - kawasaki (225) - yokosuka (164) - nihon'odori (149) - nagoya (105) - mat

Destination Domain (8 items)
dion.ne.jp (3,990) - bai.ne.jp (30) - it-chiba.ac.jp (25) - sgu.ac.jp (2) - interop.net (2) - hanshin.co.jp (

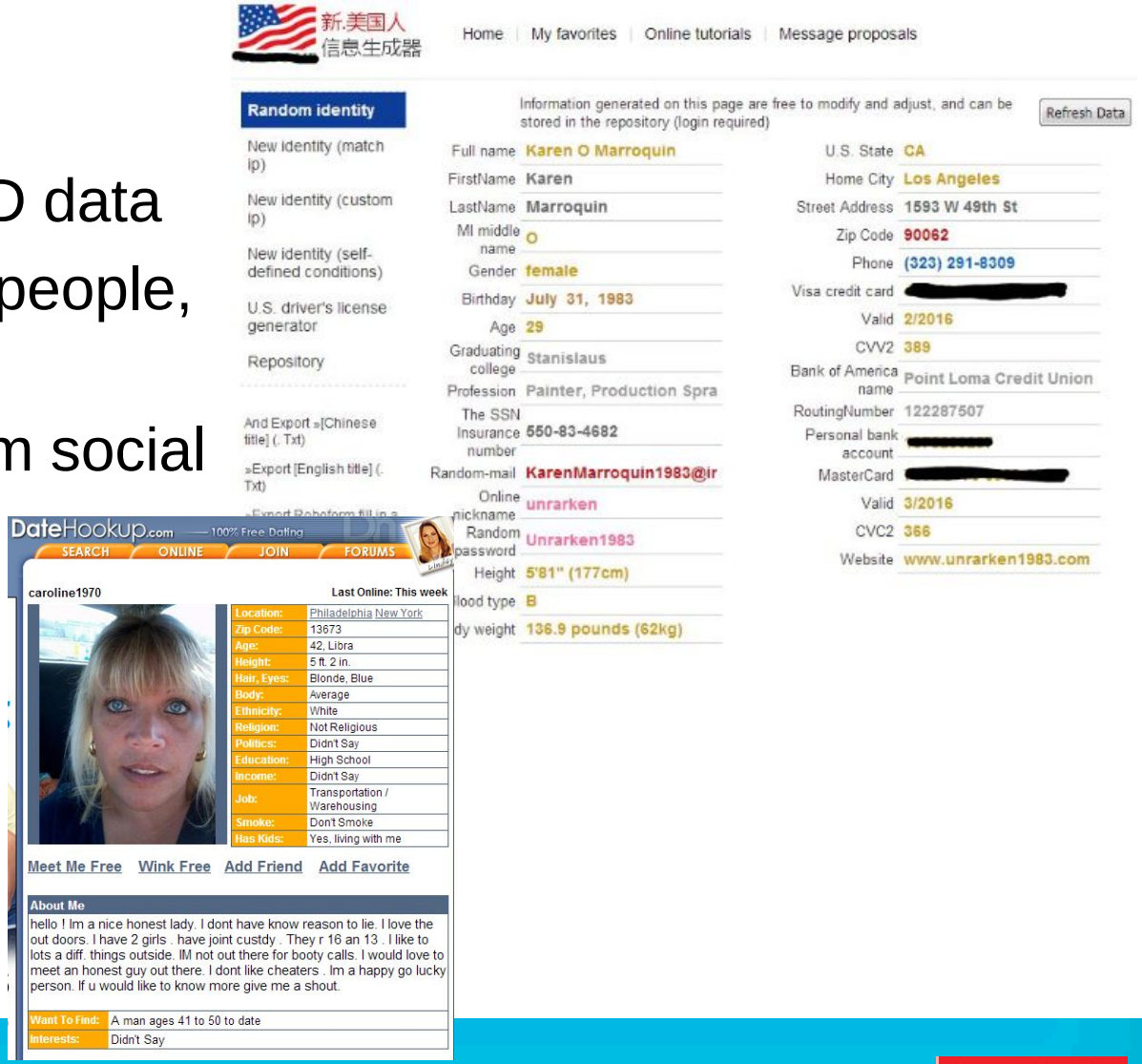
Ethernet Protocol (1 item)
IP (4,277)

IP Protocol (1 item)
ICMP (4,277)

Make sure CISO involved in announcements!

Fake identities still big business

- Generates fake ID data
- Based upon real people, real data formats
- Data gleaned from social networking sites



From APTs to SMTs

- Evolution of advanced threats

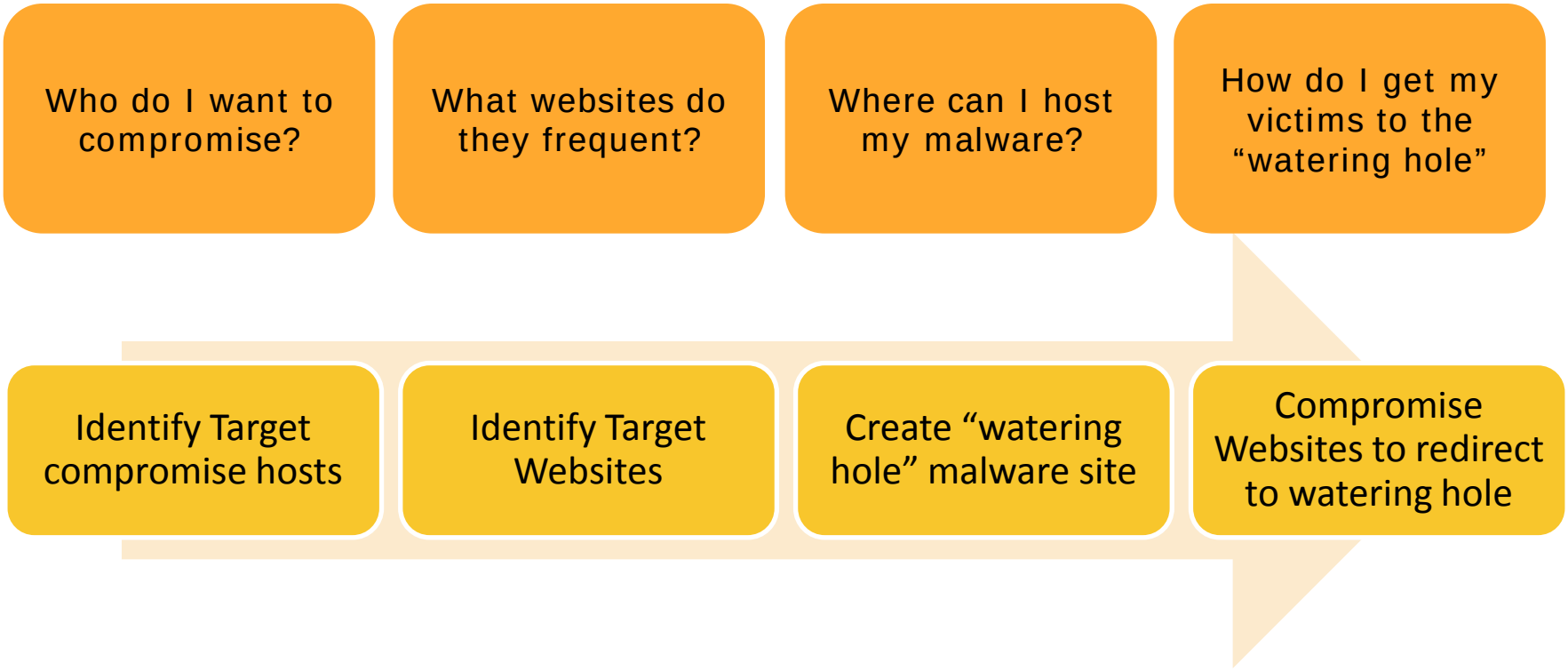
	Advanced Persistent Threat	Subversive Multivector Threat
Target	Military, Intelligence, DIB	Much wider realm – media, financial services
Methods	Largely exploits technical vulnerability	Union of technical, people and process weaknesses
Adaptability	Largely linear in nature until goal is reached	Highly dynamic based upon path of least resistance

Attribution: Gragido/Pirc

Example: The VOHO Campaign?

- Discovered in July 2012 by RSA FirstWatch
  - Infrastructure was shared for multiple threat campaigns
  - Trojan payload via browser-based exploits to delivers exploits to website visitors
- At first glance appeared to be “garden variety” drive by attack
  - However, victims seemed to be geographically clustered
- Further research found campaign used brand new attack approach utilizing ‘water holing’ method
- Multistage Campaign: Redirection with a heavy dependency on JavaScript on two specific domains for majority of promulgation

VOHO Waterholing Attack Flow



VOHO Watering Hole Leveraged

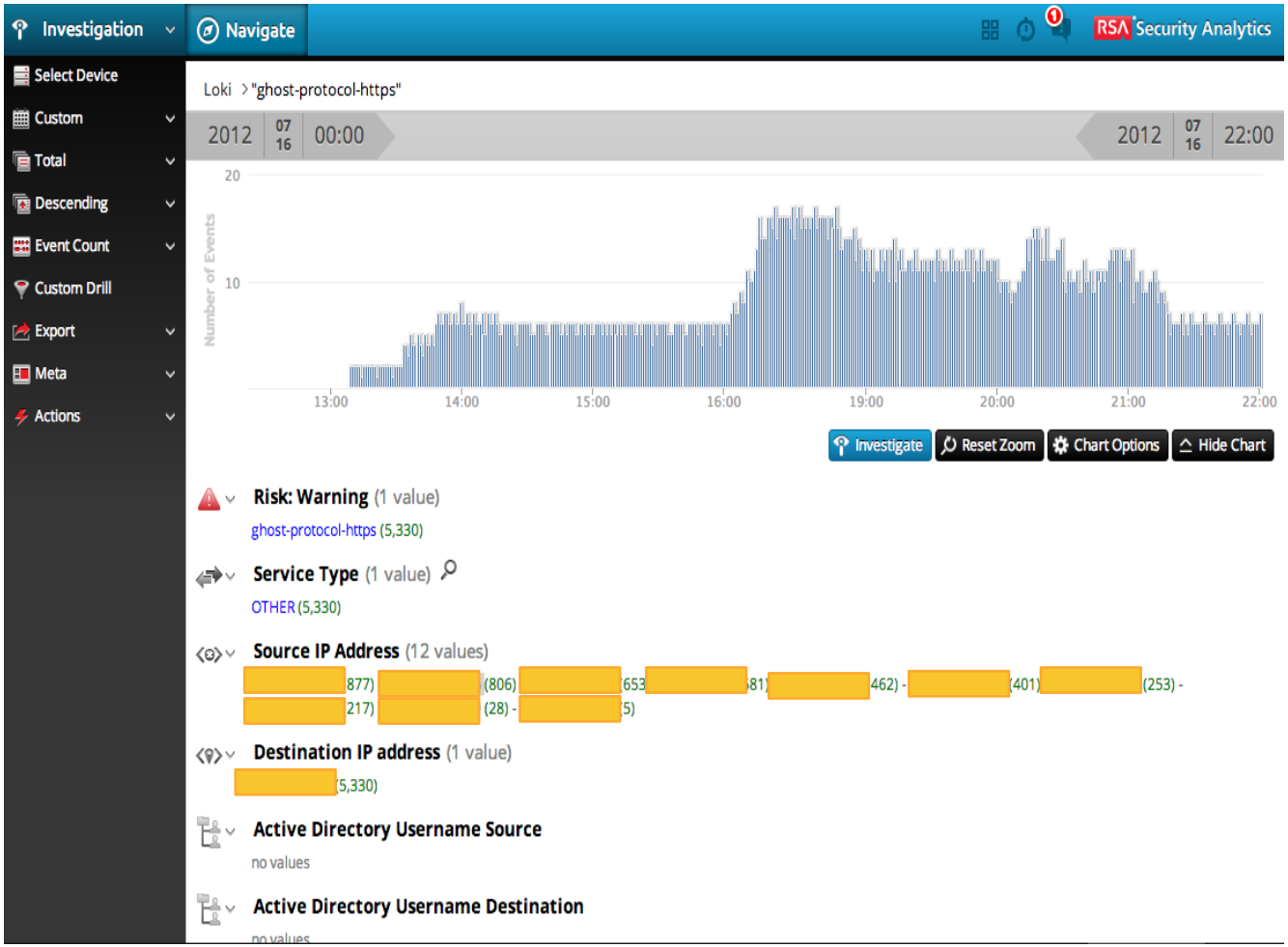
- Sample targeted websites (redacted)
  - hxxp://www.xxxxxxxxtrust.com
  - hxxp://xxxxxxxxxcountymd.gov
  - hxxp://xxxxxxcenter.org
  - hxxp:/xxxxxxxpolitics.com
  - hxxp://www.xxxxxantennas.com
- Water Hole site (redacted)
  - hxxp://xxxxxxxcurling.com

Detection Scenario

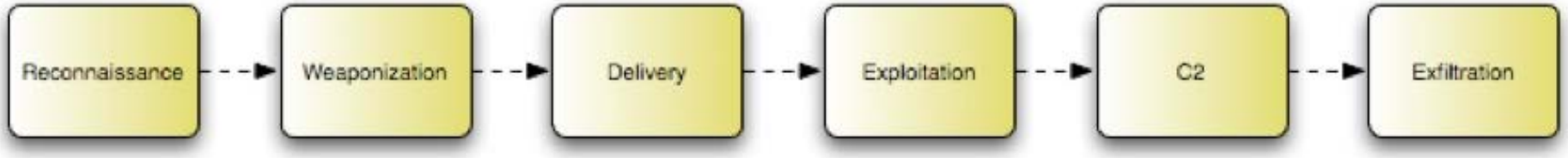
- Look for communication with blacklisted hosts
  - Known C2 sites
  - Known malware domains
- Look for suspect network traffic
  - “Gh0st” or “HTTPS” in first 5 packets of non-RFC compliant session
  - Use of web redirect using xKungFoo script

Indicators Defined To Help Identify Attack

- Look for Command and Control (C2) IP addresses
- Look for Control Channel IP addresses
- Parser created

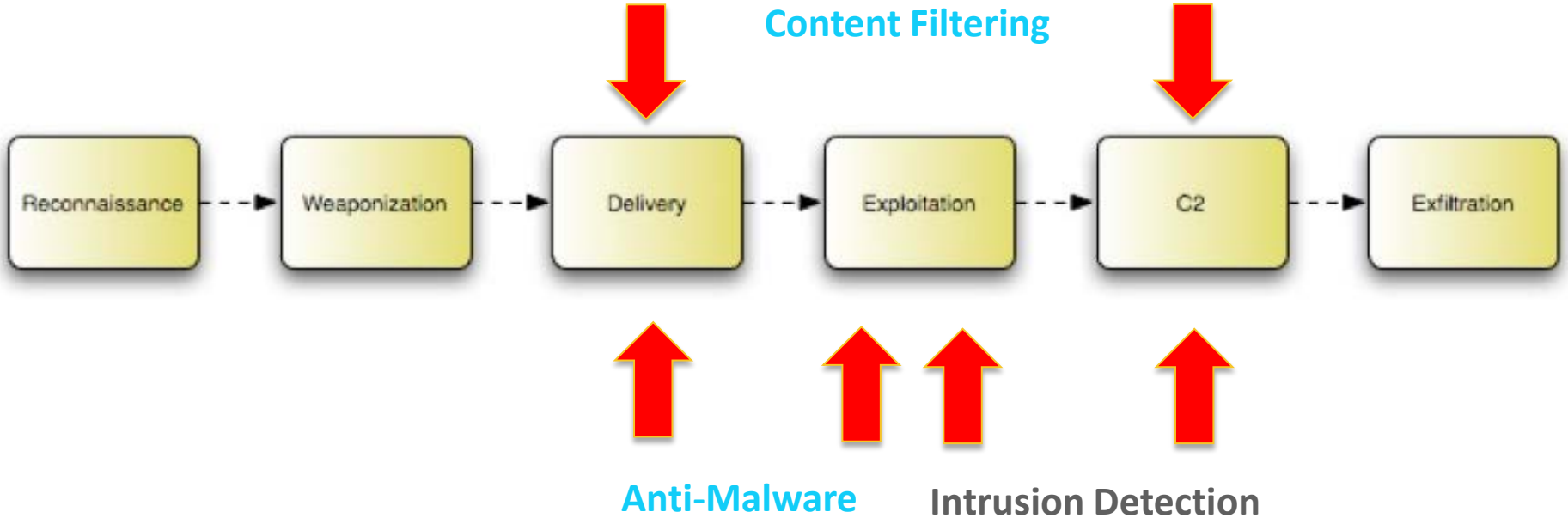


The Cyber Kill Chain



Attribution: Lockheed Martin

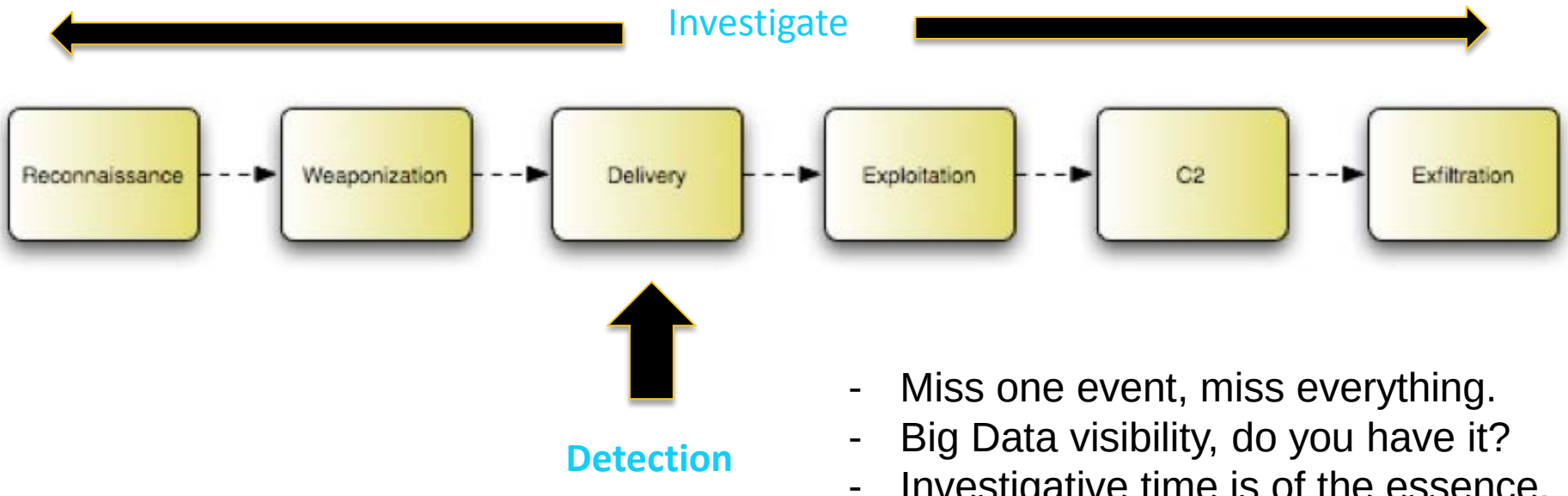
The Traditional Security Paradigm



"Single events are rarely indicative of the scope of an event, and also easily obfuscated."

The “Complex Event” Paradigm

Forensic Use Case



- Miss one event, miss everything.
- Big Data visibility, do you have it?
- Investigative time is of the essence.
- Time proven methodology, but the ability to connect kill chain points has lacked, high potential for failure.

To Defend you need

Big Data Infrastructure

"Need a fast and scalable infrastructure to conduct short term and long term analysis"

Comprehensive Visibility

"See everything happening in my environment and normalize it"

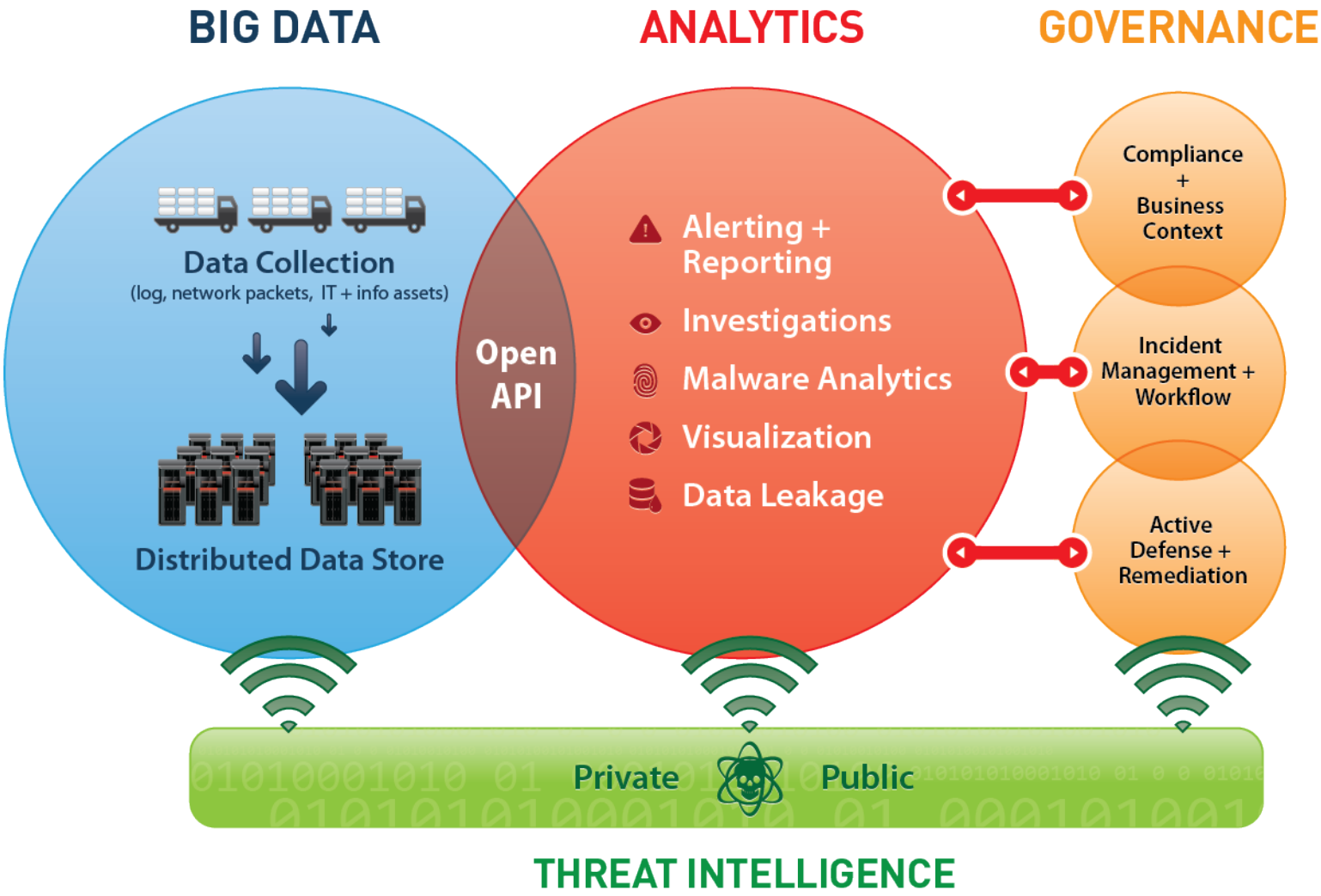
High Powered Analytics

"Give me the speed and smarts to discover and investigate potential threats in near real time"

Integrated Intelligence

"Help me understand what to look for and what others have discovered"

Defense Architecture



Summary

- Adversary is getting smarter
- Threats evolving to complex mix of technology people and process
- Defense is a combination of
  - Visibility
  - Analytics
  - Intelligence
  - Response