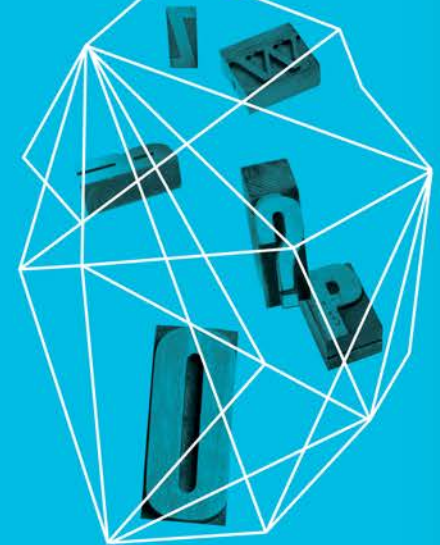


ADVANCED THREATS AND INTELLIGENT DEFENSE

Amit Yoran

Senior Vice President of Products, RSA

Security in
knowledge



— 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”

The screenshot shows a website interface for 'Stone Paper Scissors'. The navigation bar includes links for Home, News, LOTTERY, CBN, Cabinet, Registration, About Us, FAQ, and Contacts. The main content area features a title 'Stone Paper Scissors', a small image of hands in a rock-paper-scissors gesture, and a descriptive paragraph: 'Rock, paper, scissors - (abbreviated as CSS) popular children's game in hand, well-known all over the world. This game is all familiar from childhood, and here you can play it in the money with real players. The game is not with the system and with other users. First you create a game and choose one of the three objects (rock, scissors or paper), and selects the bid.' To the right, there are links for 'Stone Paper Scissors', 'Recommendations', 'Referral system', and 'Regulations'. At the bottom right, there are social media links for 'Твитнуть' (19) and 'Читать @urik09'. A blue advertisement box is overlaid on the bottom left, titled 'Advertising Wmlink.ru', containing a list of scammy offers: 'Investing in the PAMM invest.fondy', 'FreshForeks - Your reliable broker', 'How to earn \$ 200 in 5 minutes!!', 'earn from \$ 100 to \$ 500 a day', 'How to make money online newbie?!', 'Ultimate System earnings from \$ 120 a day! Cn', 'Make your PC to earn.', 'Free system of earnings from \$ 120 a day! ...', 'Work from \$ 2500 a month! Have vacancies!', and 'Earn money online now!'. A red circle highlights this advertisement box, and a yellow arrow points from the text 'Usual scam links' to it.

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(miyazaki)

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 (1)

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

新.美国人 信息生成器

Home | My favorites | Online tutorials | Message proposals

Refresh Data

Information generated on this page are free to modify and adjust, and can be stored in the repository (login required)

Full name	Karen O Marroquin	U.S. State	CA
FirstName	Karen	Home City	Los Angeles
LastName	Marroquin	Street Address	1593 W 49th St
MI middle name	O	Zip Code	90062
Gender	female	Phone	(323) 291-8309
Birthday	July 31, 1983	Visa credit card	[REDACTED]
Age	29	Valid	2/2016
Graduating college	Stanislaus	CVV2	389
Profession	Painter, Production Spr	Bank of America name	Point Loma Credit Union
The SSN	550-83-4682	RoutingNumber	122287507
Insurance number		Personal bank account	[REDACTED]
Random-mail	KarenMarroquin1983@ir	MasterCard	[REDACTED]
Online nickname	unrarken	Valid	3/2016
Random password	Unrarken1983	CVC2	366
Height	5'81" (177cm)	Website	www.unrarken1983.com
Blood type	B		
Body weight	136.9 pounds (62kg)		

DateHookup.com — 100% Free Dating

SEARCH ONLINE JOIN FORUMS

caroline1970 Last Online: This week

Location:	Philadelphia New York
Zip Code:	13673
Age:	42, Libra
Height:	5 ft. 2 in.
Hair, Eyes:	Blonde, Blue
Body:	Average
Ethnicity:	White
Religion:	Not Religious
Politics:	Didn't Say
Education:	High School
Income:	Didn't Say
Job:	Transportation / Warehousing
Smoke:	Don't Smoke
Has Kids:	Yes, living with me

Meet Me Free Wink Free Add Friend Add Favorite

About Me

hello ! im a nice honest lady. I dont have know reason to lie. I love the out doors. I have 2 girls . have joint custdy . They r 16 an 13 . I like to lots a diff. things outside. IM not out there for booty calls. I would love to meet an honest guy out there. I dont like cheaters . Im a happy go lucky person. If u would like to know more give me a shout.

Want To Find: A man ages 41 to 50 to date

Interests: Didn't Say

From APTs to SMTs

▶ Evolution of advanced threats

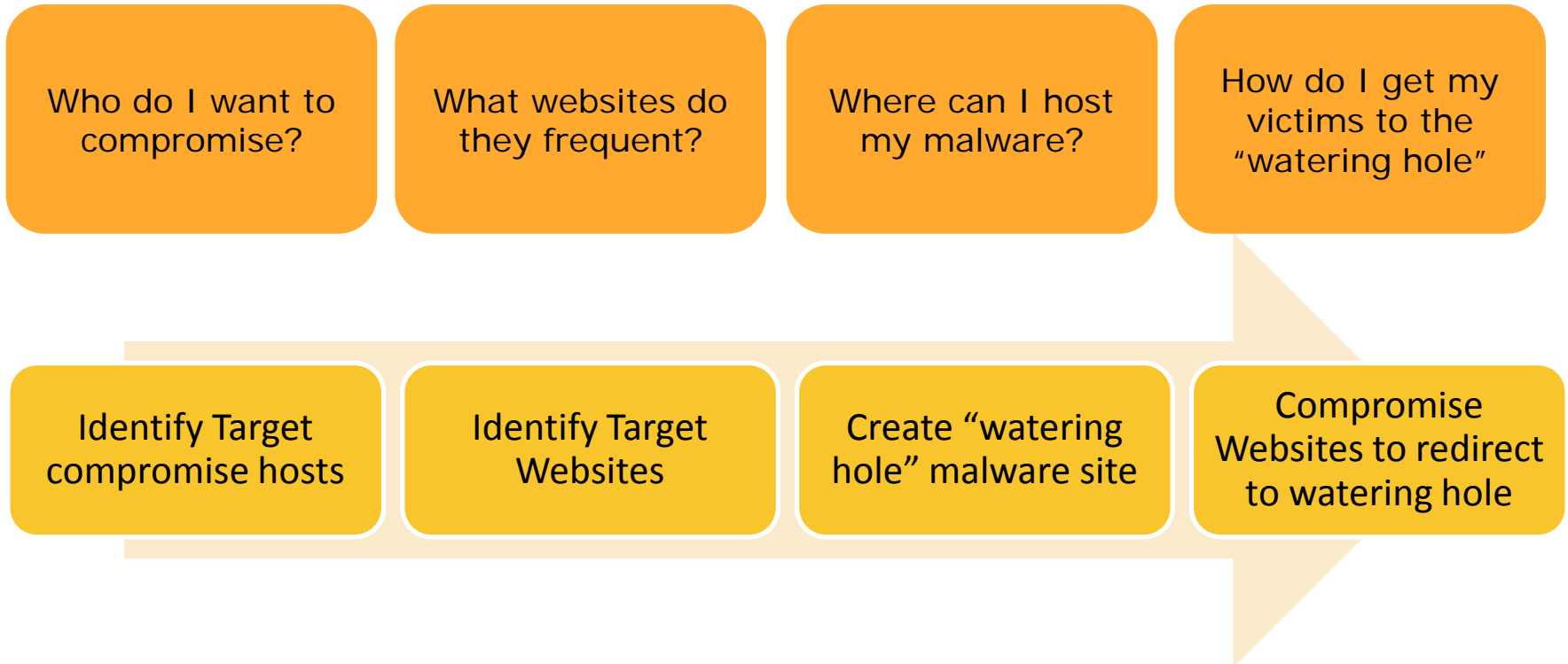
	Advanced Persistent Threat	Subversive Multivector Threat
Target	Military, Intelligence, DIB	Much wider realm – media, financial services
Methods	Largely exploits technical vulnerability	Union of technical, people and process weaknesses
Adaptability	Largely linear in nature until goal is reached	Highly 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](http://www.xxxxxxxxtrust.com)
- ▶ [hxxp://xxxxxxxcountymd.gov](http://xxxxxxxcountymd.gov)
- ▶ [hxxp://xxxxxxxcenter.org](http://xxxxxxxcenter.org)
- ▶ [hxxp://xxxxxxxpolitics.com](http://xxxxxxxpolitics.com)
- ▶ [hxxp://www.xxxxxantennas.com](http://www.xxxxxantennas.com)

▶ Water Hole site (redacted)

- ▶ [hxxp://xxxxxxxcurling.com](http://xxxxxxxcurling.com)

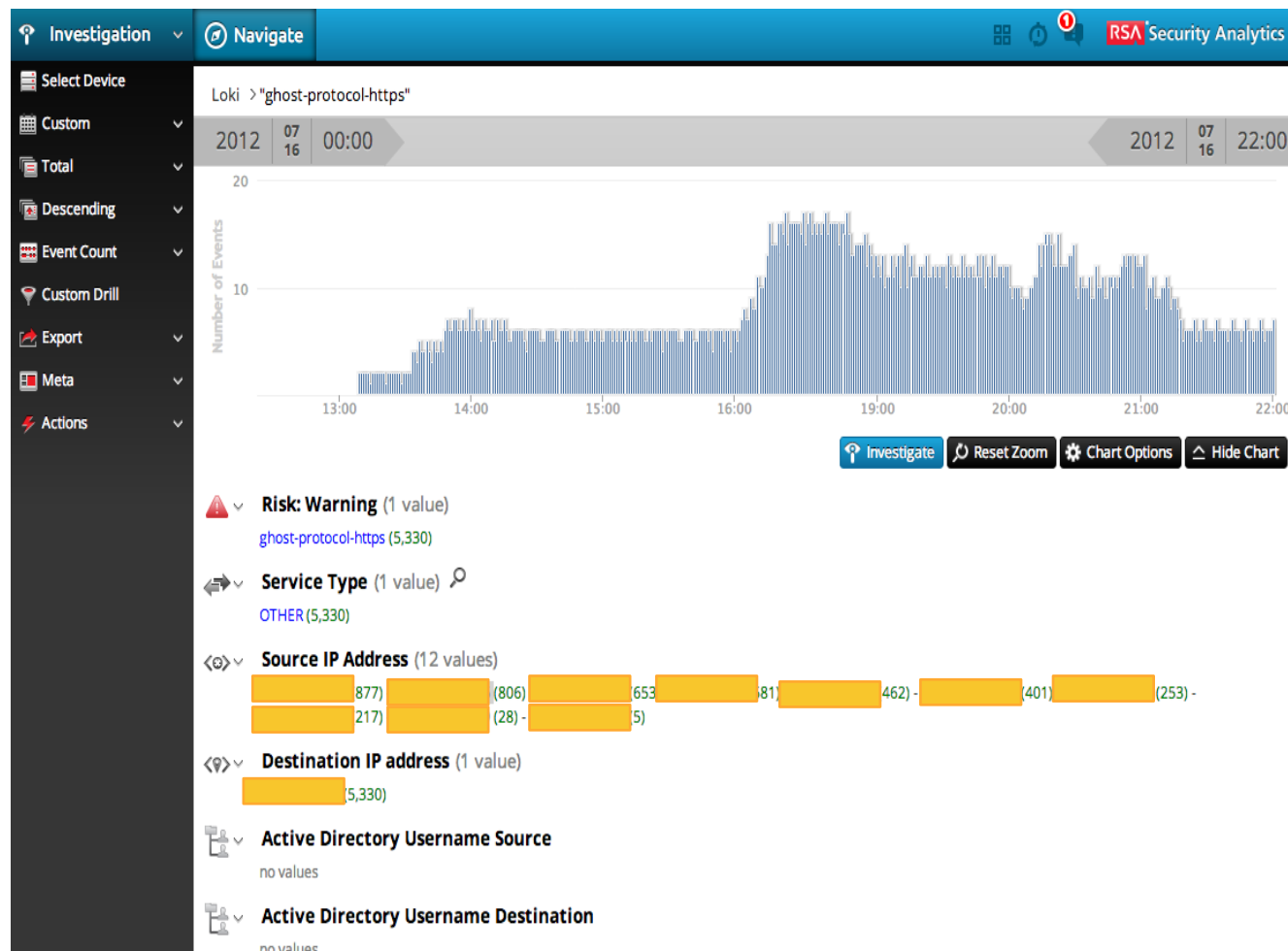


Detection Scenario

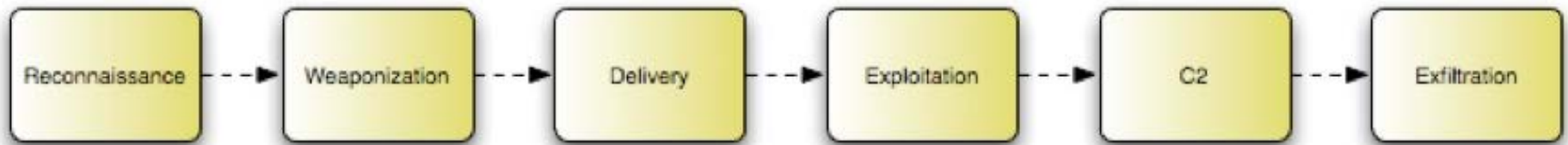
- ▶ Look for communication with blacklisted hosts
 - ▶ Known C2 sites
 - ▶ Known malware domains
- ▶ Look for suspect network traffic
 - ▶ “Gh0st” or “HTTPS” in first 5 packets of non-RFC compliant session
 - ▶ Use of web redirect using xKungFoo script

Indicators Defined To Help Identify Attack

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

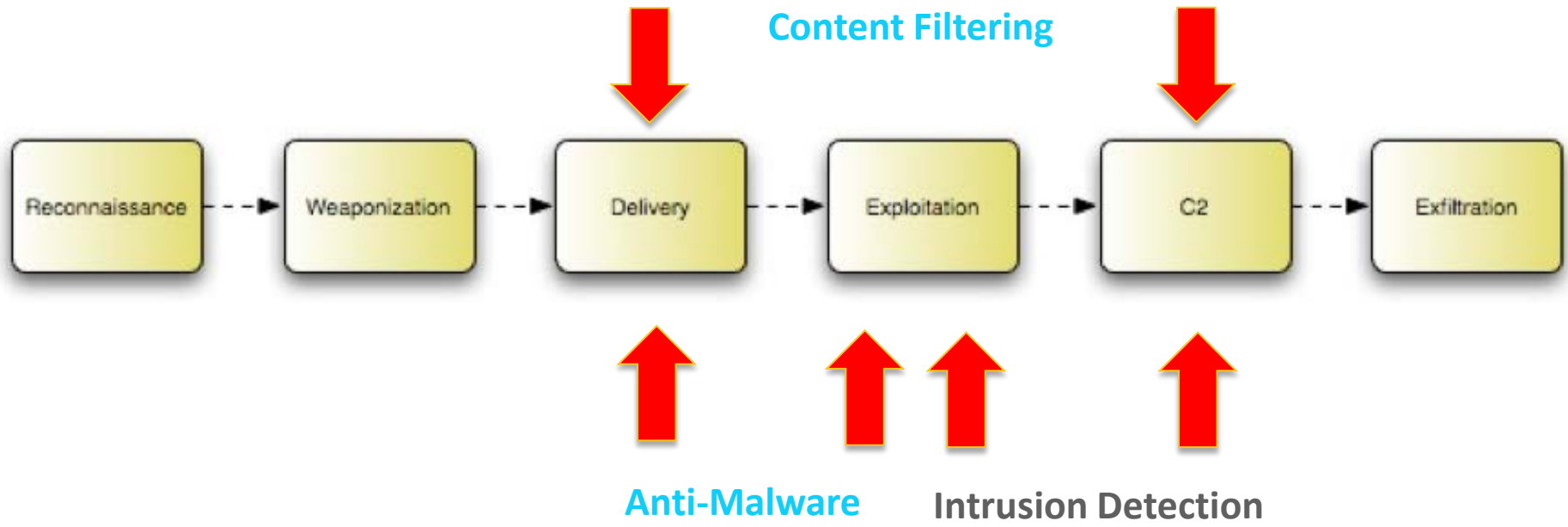


The Cyber Kill Chain



Attribution: Lockheed Martin

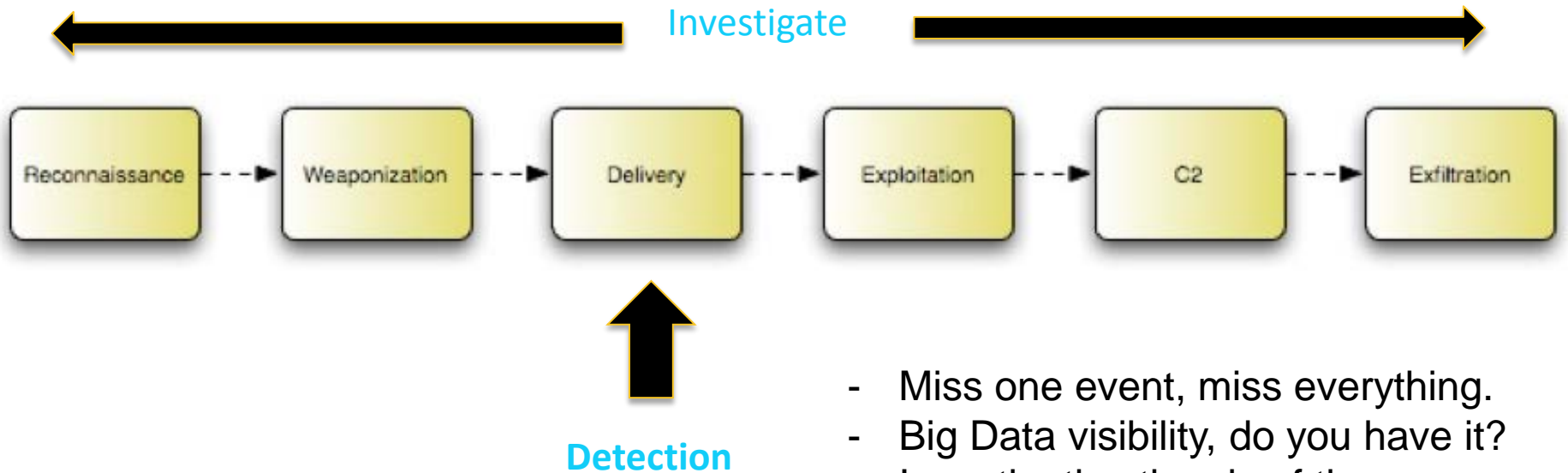
The Traditional Security Paradigm



“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”

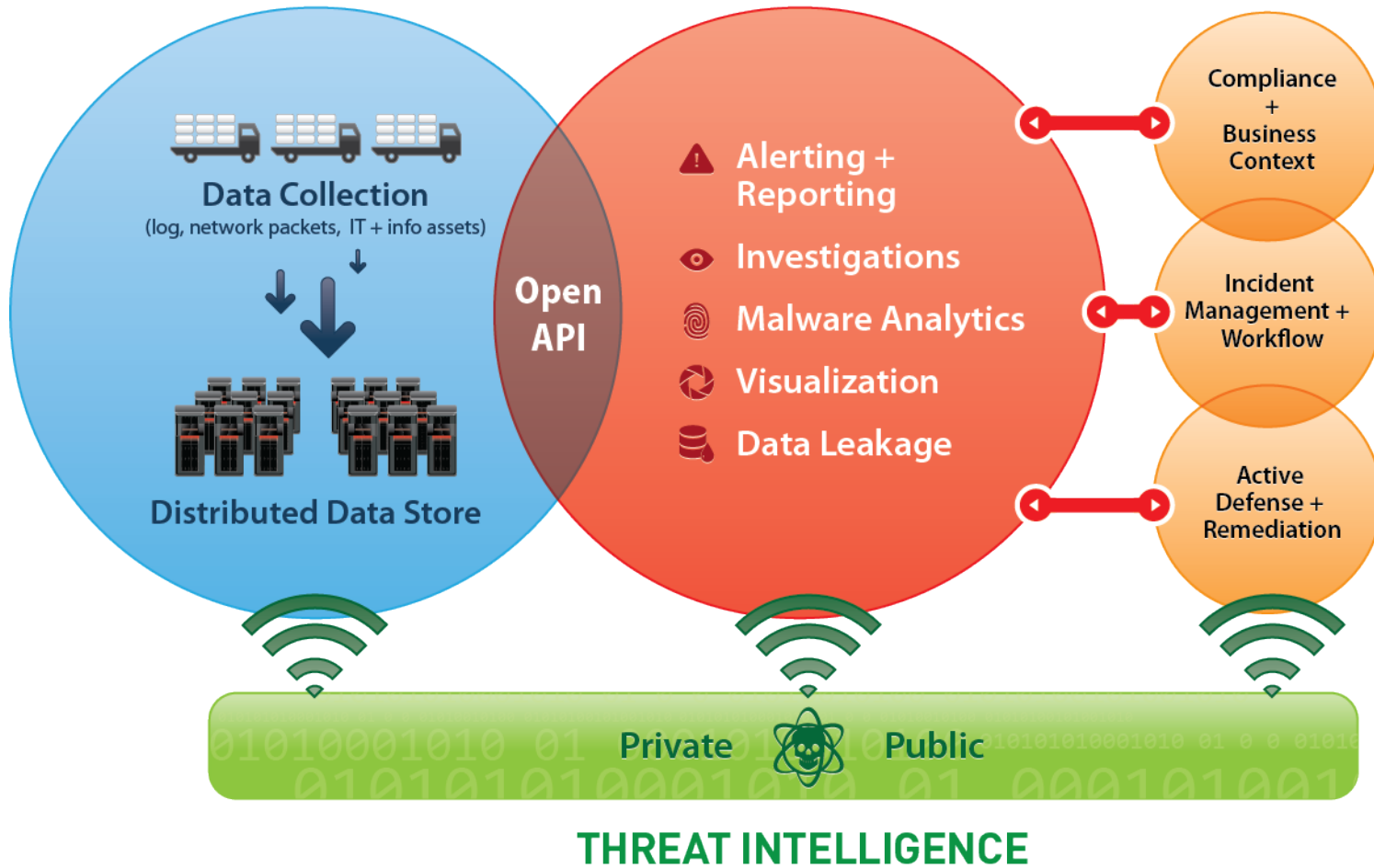


Defense Architecture

BIG DATA

ANALYTICS

GOVERNANCE



Summary

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