Security in knowledge

USING BIG INTELLIGENCE TO DEFEND AGAINST MODERN ATTACKS

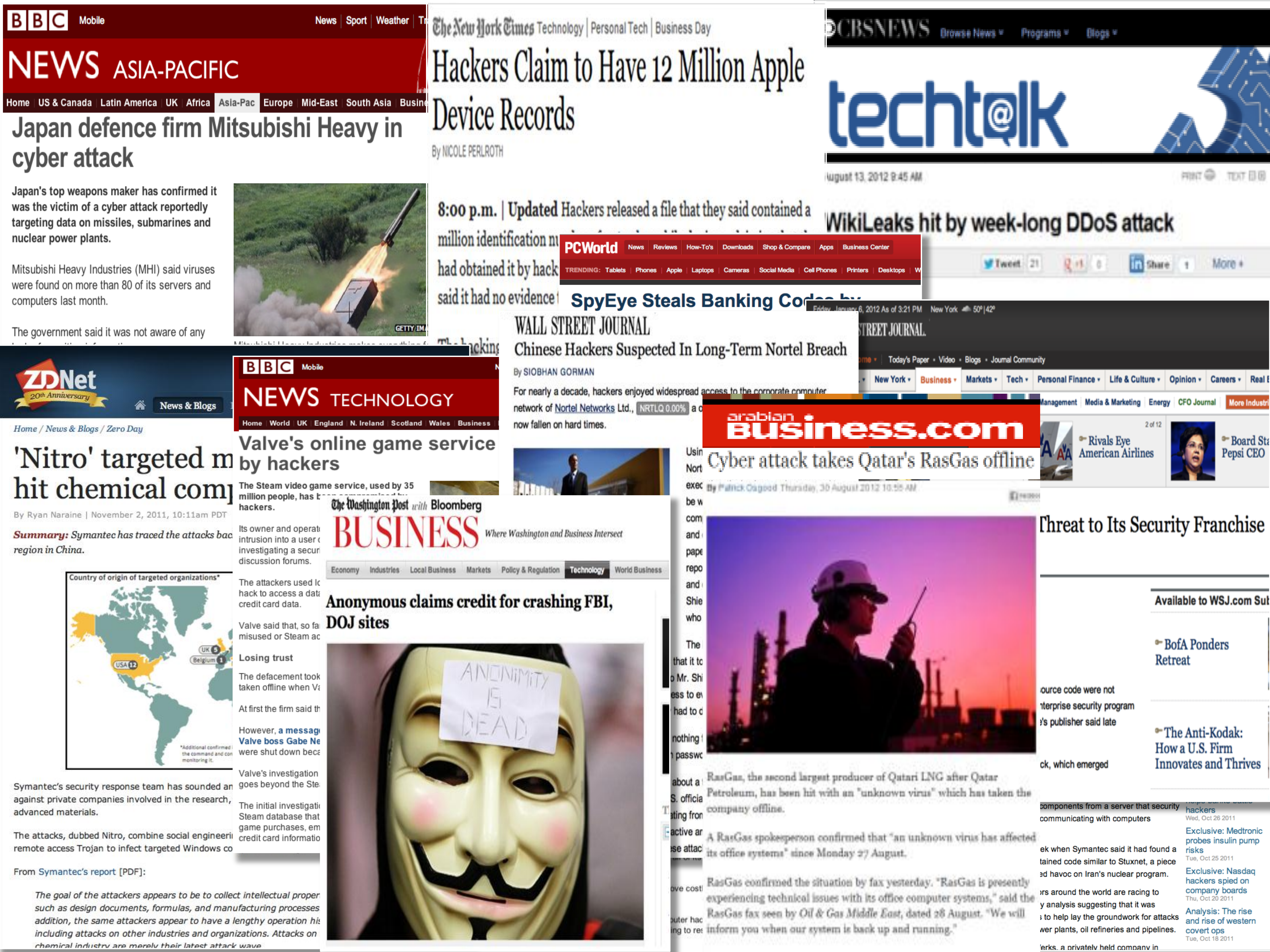
Siân John

Symantec

RSA CONFERENCE EUROPE 2013

Session ID: SPO-W01

Session Classification: Intermediate



BBC Mobile News | Sport | Weather | Tr

NEWS ASIA-PACIFIC

Home | US & Canada | Latin America | UK | Africa | Asia-Pac | Europe | Mid-East | South Asia | Busine

Japan defence firm Mitsubishi Heavy in cyber attack

Japan's top weapons maker has confirmed it was the victim of a cyber attack reportedly targeting data on missiles, submarines and nuclear power plants.

Mitsubishi Heavy Industries (MHI) said viruses were found on more than 80 of its servers and computers last month.

The government said it was not aware of any

GETTY IM

The New York Times Technology | Personal Tech | Business Day

Hackers Claim to Have 12 Million Apple Device Records

By NICOLE PERLROTH

8:00 p.m. | Updated Hackers released a file that they said contained a million identification nu had obtained it by hack said it had no evidence

The hacking

CBSNEWS Browse News ▾ Programs ▾ Blogs ▾

techt@lk

ugust 13, 2012 9:45 AM PRINT TEXT

WikiLeaks hit by week-long DDoS attack

Tweet 21 +1 0 in Share 1 More ▾

PCWorld News | Reviews | How-To's | Downloads | Shop & Compare | Apps | Business Center

TRENDING: Tablets | Phones | Apple | Laptops | Cameras | Social Media | Cell Phones | Printers | Desktops | W

SpyEye Steals Banking Codes by

WALL STREET JOURNAL

Chinese Hackers Suspected In Long-Term Nortel Breach

By SIOBHAN GORMAN

For nearly a decade, hackers enjoyed widespread access to the corporate computer network of Nortel Networks Ltd., NRTLQ 0.00% a c now fallen on hard times.

Usin Nort exec be w com and pape repo and Shie who

The that it to Mr. Shi ess to e had to d

nothing passwo

about a S. officia ting fron active ar se attac

ove cost

puter hac ing to re

Friday, January 6, 2012 As of 3:21 PM New York 50°|42°

TREET JOURNAL.

me ▾ | Today's Paper • Video • Blogs • Journal Community

New York ▾ | Business ▾ | Markets ▾ | Tech ▾ | Personal Finance ▾ | Life & Culture ▾ | Opinion ▾ | Careers ▾ | Real E

anagement | Media & Marketing | Energy | CFO Journal | More Industri

2 of 12

Rivals Eye American Airlines

Board St Pepsi CEO

Threat to Its Security Franchise

ource code were not nterprise security program 's publisher said late

ck, which emerged

components from a server that security communicating with computers

ek when Symantec said it had found a tained code similar to Stuxnet, a piece ed havoc on Iran's nuclear program.

rs around the world are racing to y analysis suggesting that it was to help lay the groundwork for attacks wer plants, oil refineries and pipelines.

erks, a privately held company in

Available to WSJ.com Sub

BofA Ponders Retreat

The Anti-Kodak: How a U.S. Firm Innovates and Thrives

hackers
Wed, Oct 26 2011

Exclusive: Medtronic probes insulin pump risks
Tue, Oct 25 2011

Exclusive: Nasdaq hackers spied on company boards
Thu, Oct 20 2011

Analysis: The rise and rise of western covert ops
Tue, Oct 18 2011

ZDNet 20th Anniversary News & Blogs

Home / News & Blogs / Zero Day

'Nitro' targeted m hit chemical com

By Ryan Naraine | November 2, 2011, 10:11am PDT

***Summary:** Symantec has traced the attacks bac region in China.*

Country of origin of targeted organizations*

*Additional confirmed the command and con monitoring it.

Symantec's security response team has sounded an against private companies involved in the research, advanced materials.

The attacks, dubbed Nitro, combine social engineeri remote access Trojan to infect targeted Windows co

From Symantec's report [PDF]:

> *The goal of the attackers appears to be to collect intellectual proper such as design documents, formulas, and manufacturing processes addition, the same attackers appear to have a lengthy operation his including attacks on other industries and organizations. Attacks on chemical industry are merely their latest attack wave*

BBC Mobile

NEWS TECHNOLOGY

Home | World | UK | England | N. Ireland | Scotland | Wales | Business

Valve's online game service by hackers

The Steam video game service, used by 35 million people, has b hackers.

Its owner and operat intrusion into a user investigating a secur discussion forums.

The attackers used l hack to access a data credit card data.

Valve said that, so fa misused or Steam ac

Losing trust

The defacement took taken offline when Va

At first the firm said th

However, a messag Valve boss Gabe Ne were shut down beca

Valve's investigation goes beyond the Ste

The initial investigati Steam database that game purchases, em credit card informatio

The Washington Post with Bloomberg

BUSINESS Where Washington and Business Intersect

Economy | Industries | Local Business | Markets | Policy & Regulation | Technology | World Business

Anonymous claims credit for crashing FBI, DOJ sites

arabian business.com

Cyber attack takes Qatar's RasGas offline

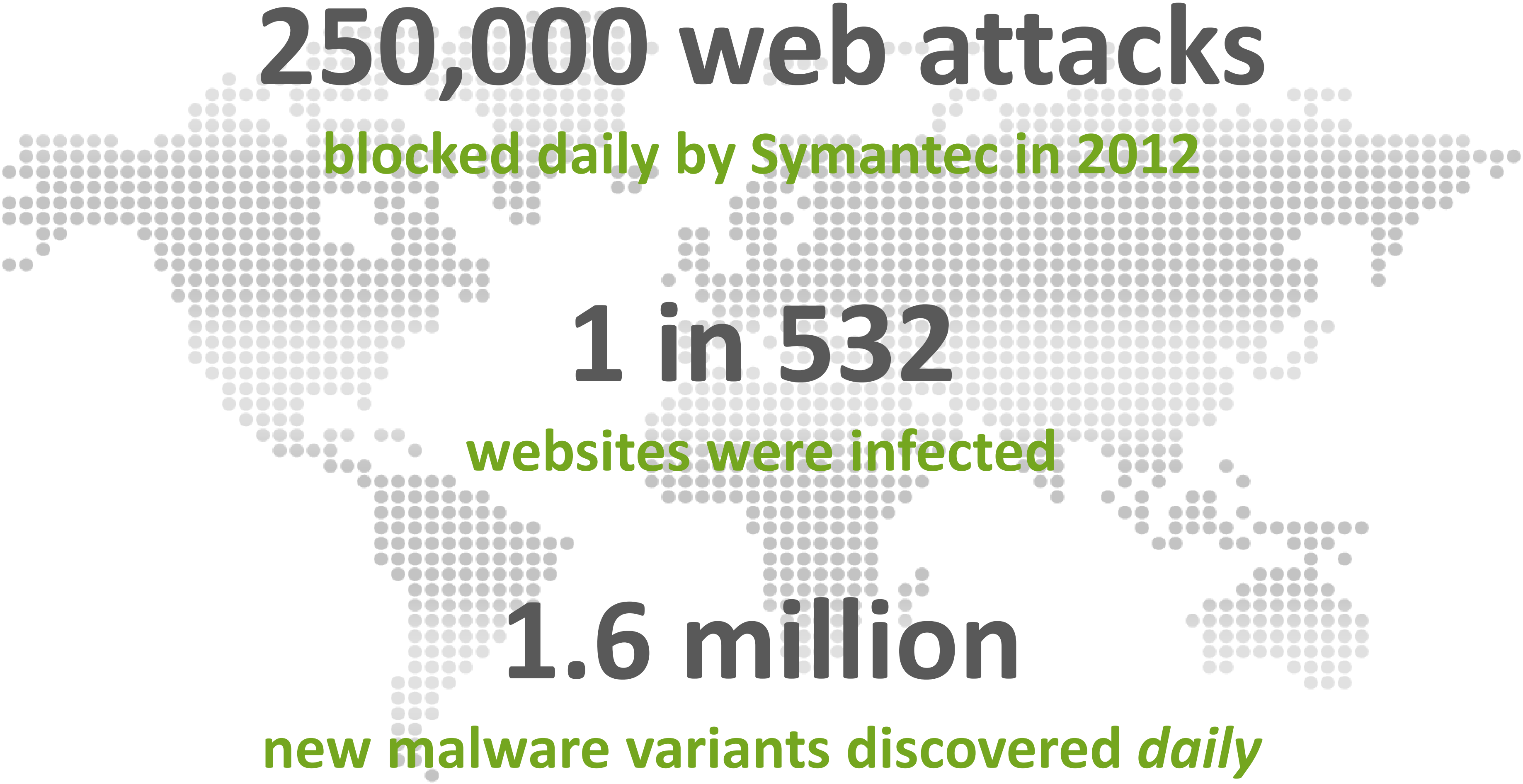
By Patrick Osgood Thursday, 30 August 2012 10:55 AM

RasGas, the second largest producer of Qatari LNG after Qatar Petroleum, has been hit with an "unknown virus" which has taken the company offline.

A RasGas spokesperson confirmed that "an unknown virus has affected its office systems" since Monday 27 August.

RasGas confirmed the situation by fax yesterday. "RasGas is presently experiencing technical issues with its office computer systems," said the RasGas fax seen by *Oil & Gas Middle East*, dated 28 August. "We will inform you when our system is back up and running."

Levels of Attacks are Increasing



250,000 web attacks

blocked daily by Symantec in 2012

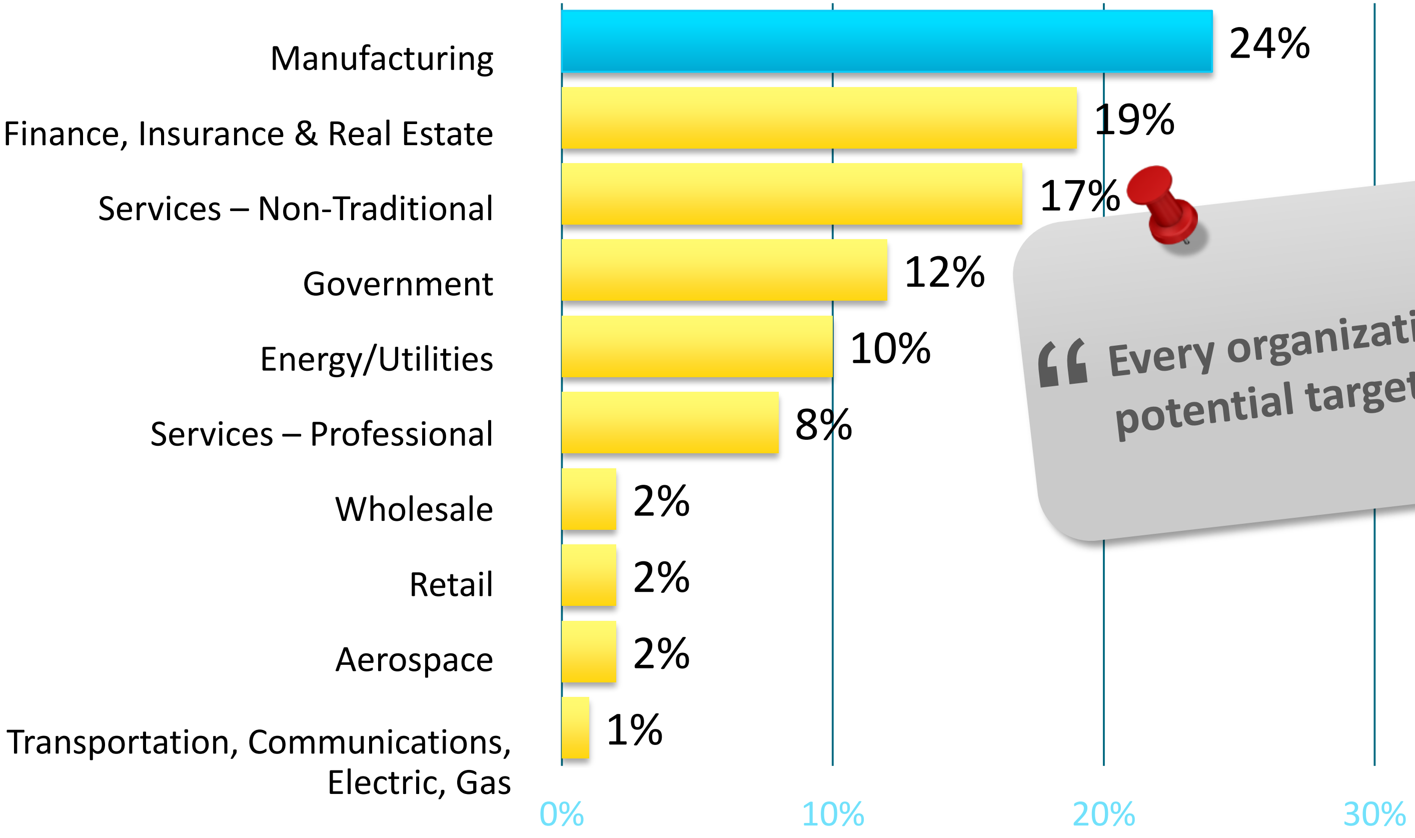
1 in 532

websites were infected

1.6 million

new malware variants discovered *daily*

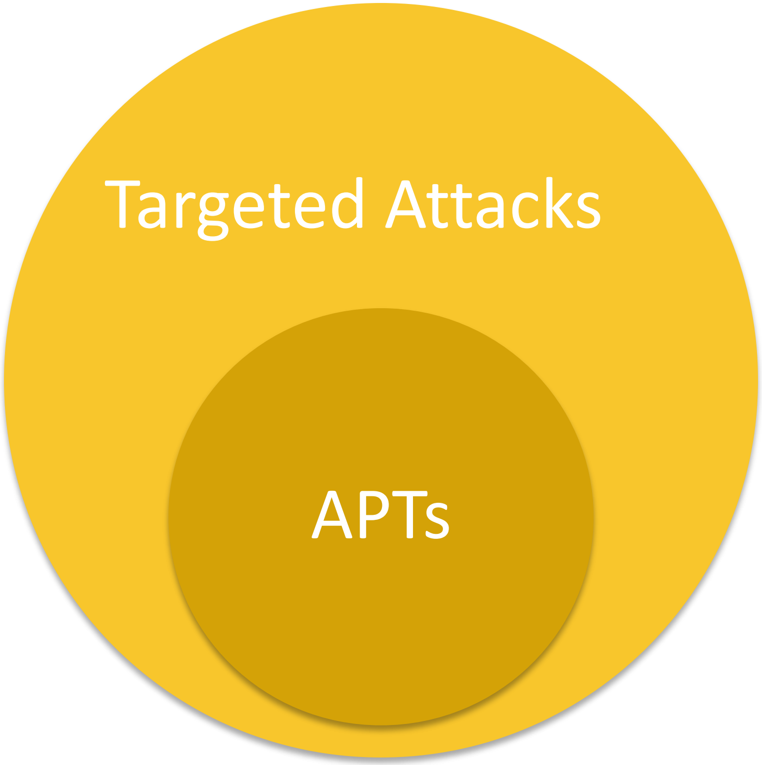
Targeted Attacks are Widening



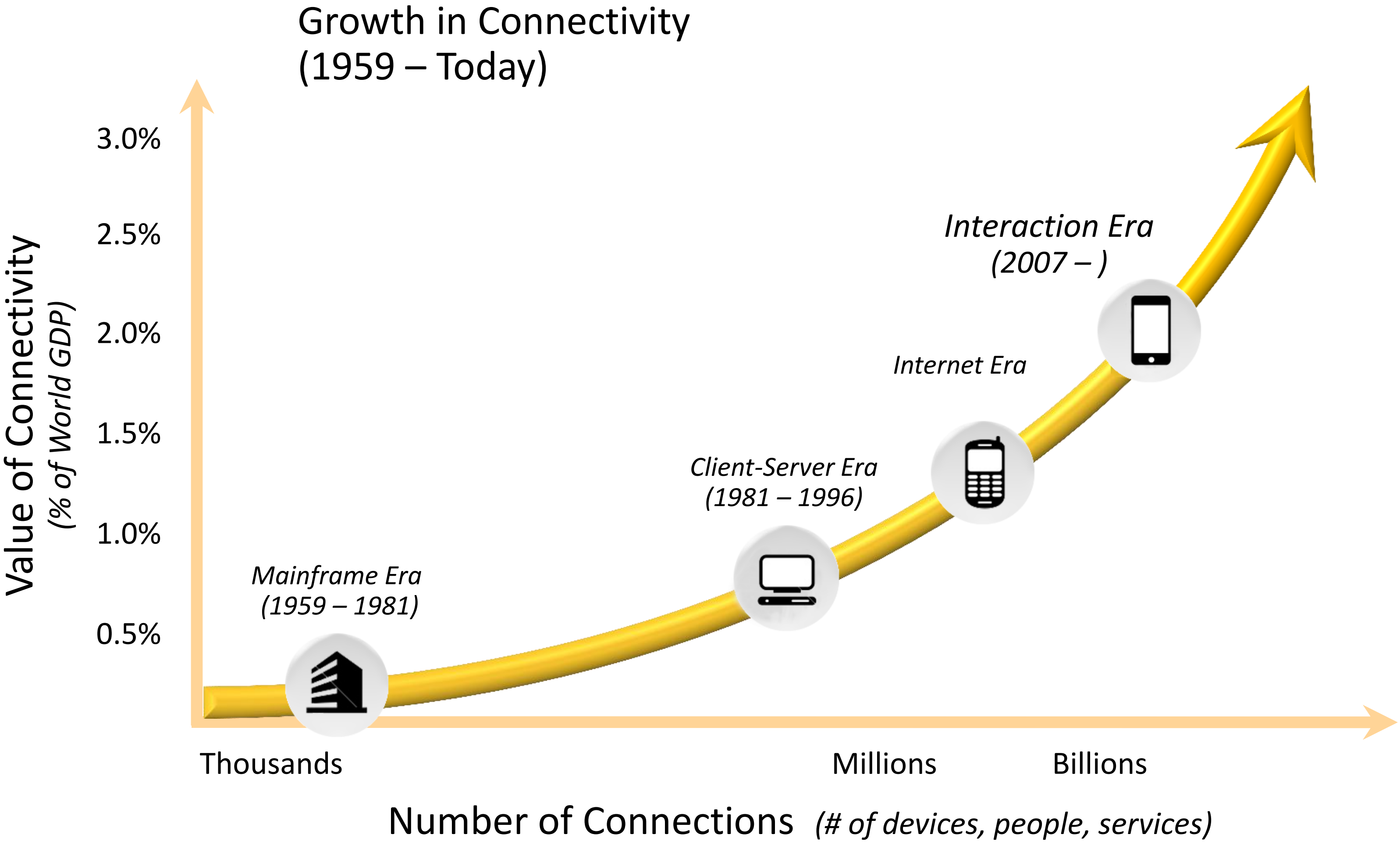
> “Every organization is a potential target”

Targeted Attacks and APTs

An APT is always a targeted attack, but…
a targeted attack is not necessarily an APT

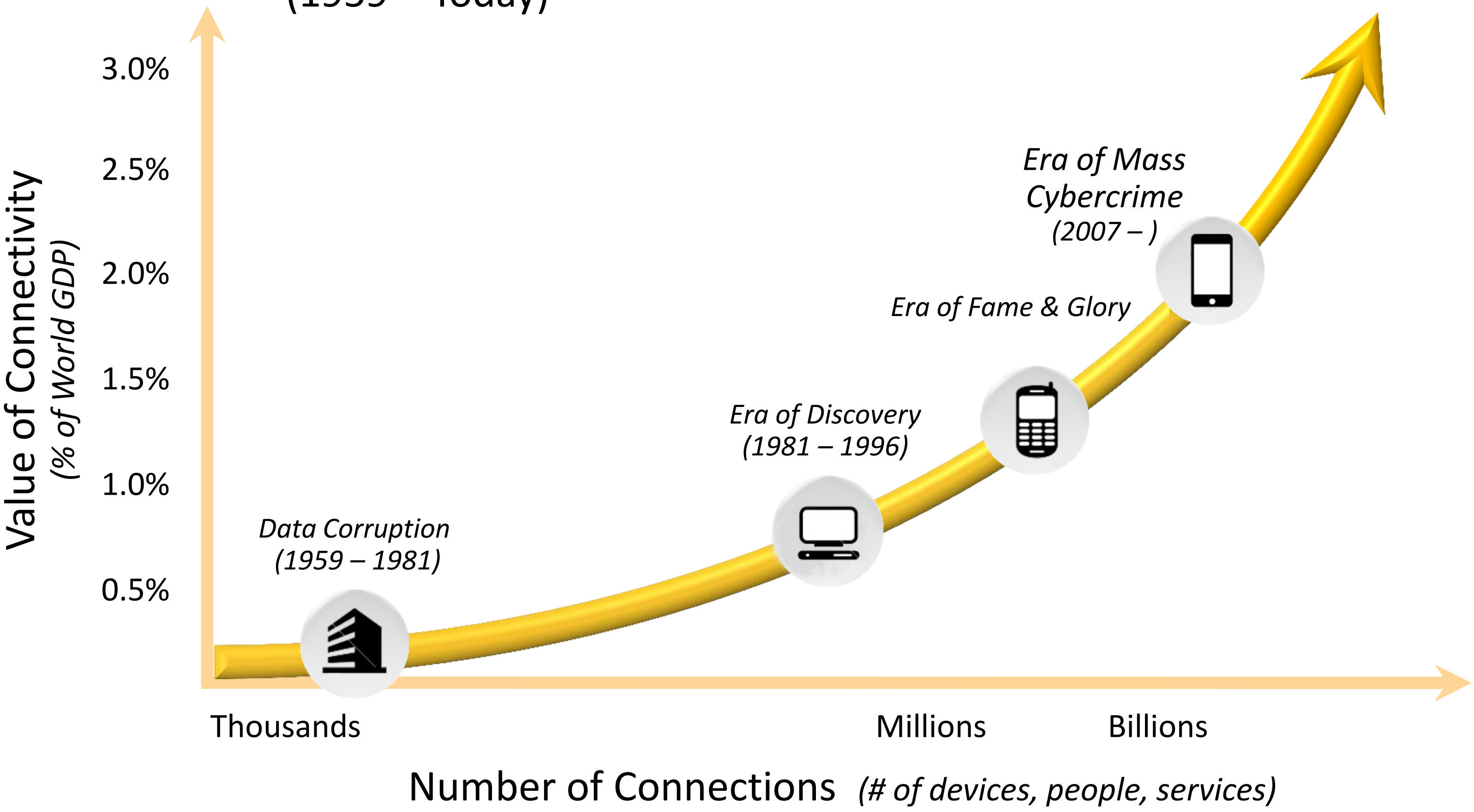


IT Trends are Driving Increased Productivity



Which is Driving the Threat Landscape

Changes in Threat Landscape
(1959 – Today)



#RSAC

Actors Driving the Market

State Actors
Government Sponsored

Attackers
Malicious Outsiders

Insiders
Malicious and Non-Malicious

Hack-tivists
Hacking for a Cause

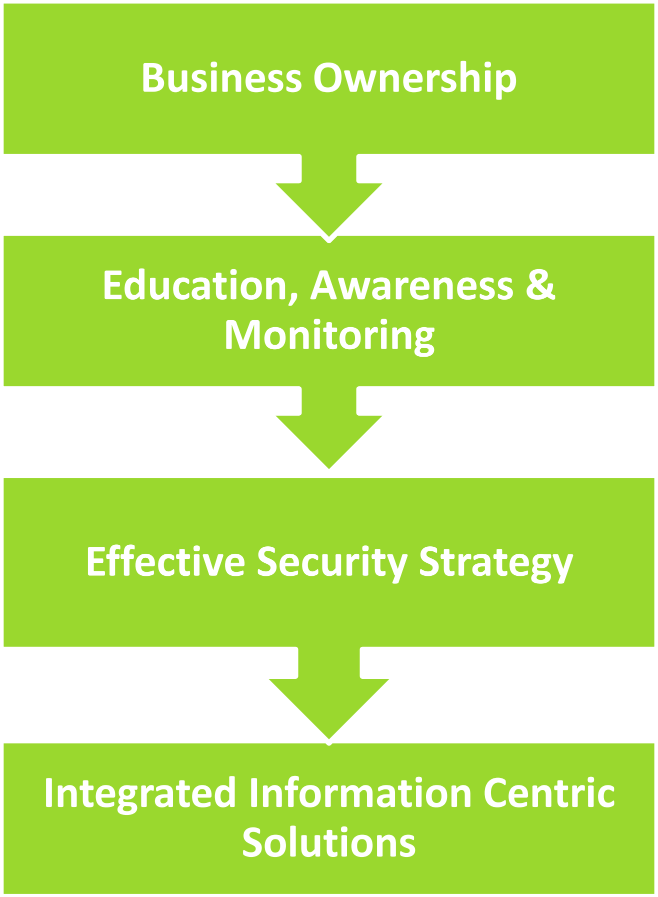
Cyber Criminals
Hacking for Profit

Modern Threat Landscape Drives Cyber

Cyber Risk Challenges

Lack of Business Ownership	•Organisational ownership does not support the desired level of cyber resilience
People & Process	•Poor cyber security appreciation, inappropriate staff behaviours & non compliance to security policies
Evolving Technologies	•Evolving IT Trends (Cloud, mobility, virtualisation & Web 2.0) increase complexity & cost to defend against cyber risks
Security Architecture	•Weakly integrated security architectures & disparate security technologies provide opportunities for targeted cyber attacks
Lack of Visibility	•Lack of situational awareness results in poor incident visibility

Requirements for Cyber Resilience


Business Ownership
Education, Awareness & Monitoring
Effective Security Strategy
Integrated Information Centric Solutions

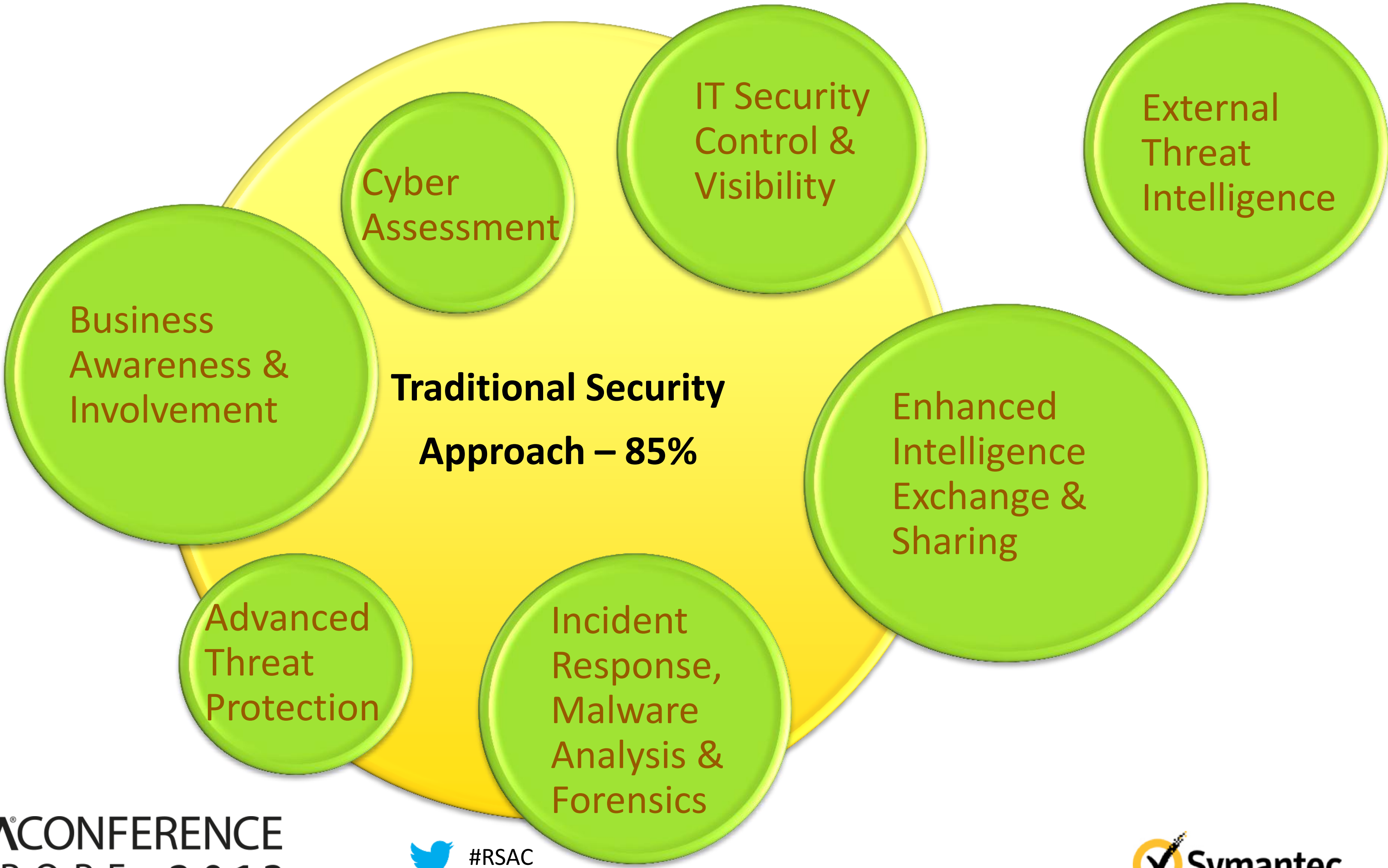
HOW CAN WE IDENTIFY AND PRIORITIZE THE KEY THREATS WHEN THERE ARE SO MANY?

IF AN ATTACK IS SUCCESSFUL HOW CAN WE RESPOND QUICKLY TO CONTAIN THE IMPACT AND RECOVER?

HOW CAN WE MEASURE AND DEMONSTRATE THE VALUE OF OUR SPENDING ON SECURITY?

HOW CAN WE BEST USE THE RESOURCES AND CAPABILITIES WE HAVE TO PROTECT OUR ORGANIZATION?

Expanding our Approach to Security



Traditional Security Approach – 85%

Cyber Assessment
IT Security Control & Visibility
External Threat Intelligence
Business Awareness & Involvement
Enhanced Intelligence Exchange & Sharing
Advanced Threat Protection
Incident Response, Malware Analysis & Forensics

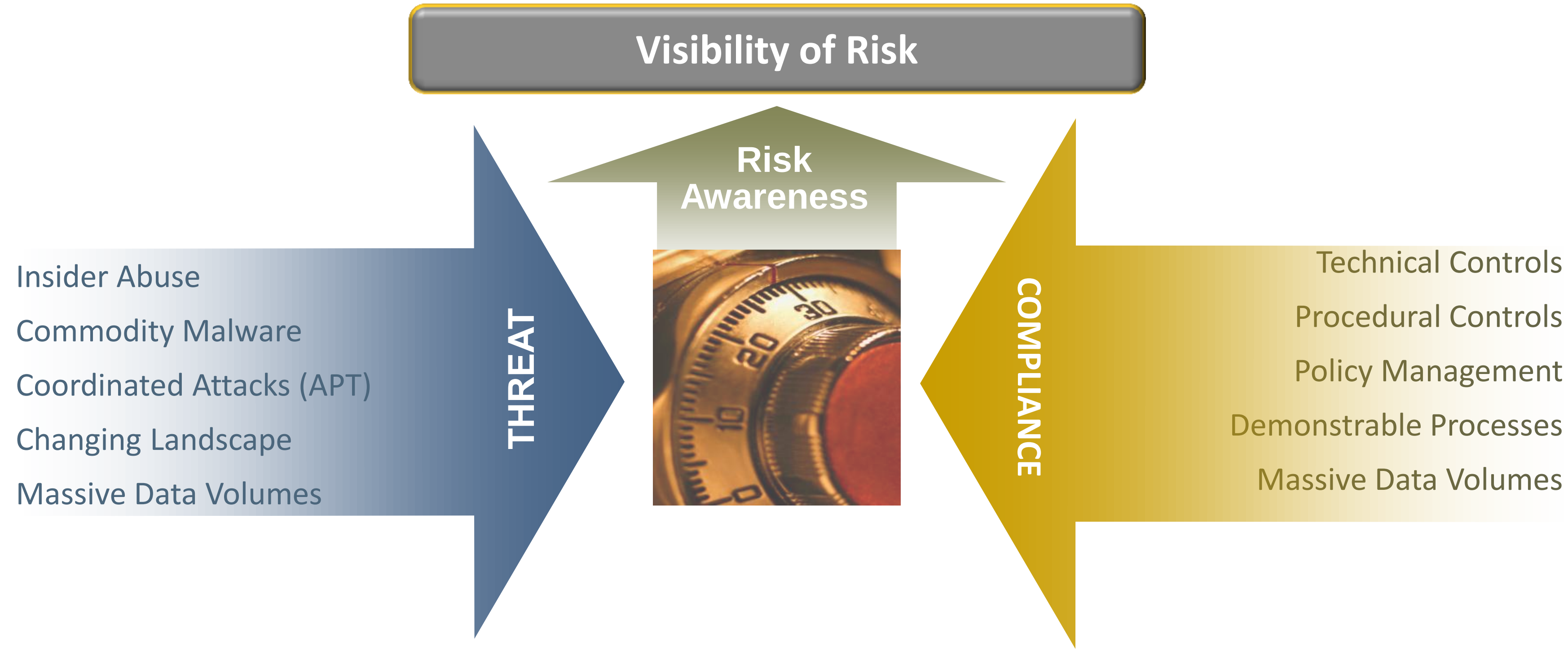
Cyber – Moving from IT to the Business

IT & IT Security

The Business

Technology alone cannot fix this…

Addressing Cyber Risk



Visibility of Risk

Risk Awareness

THREAT

Insider Abuse

Commodity Malware

Coordinated Attacks (APT)

Changing Landscape

Massive Data Volumes

COMPLIANCE

Technical Controls

Procedural Controls

Policy Management

Demonstrable Processes

Massive Data Volumes

Stay ahead of threats

Complete visibility

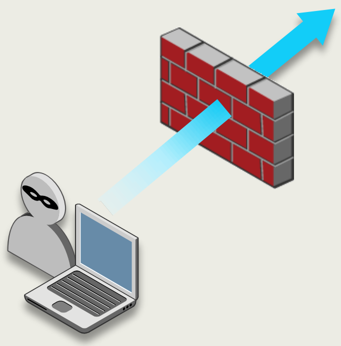
Focus on top priorities

Build a sustainable program

Present in business context

Symantec Anatomy of a Breach

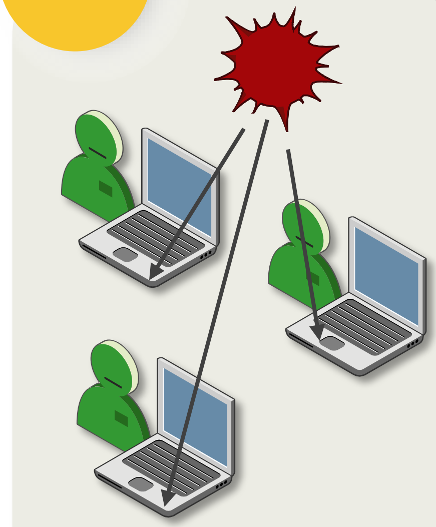
1



INCURSION

Attacker breaks into the network by delivering targeted malware to vulnerable systems and employees

2

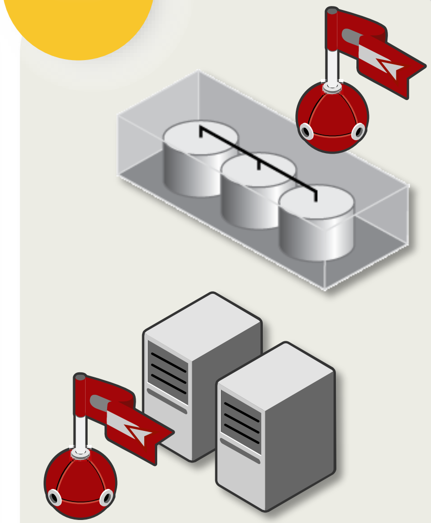


DISCOVERY

Hacker then maps organization's defenses from the inside

Creates a battle plan

3

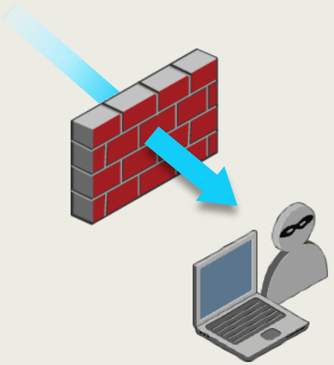


CAPTURE

Accesses data on unprotected systems

Installs malware to secretly acquire data or disrupt operations

4

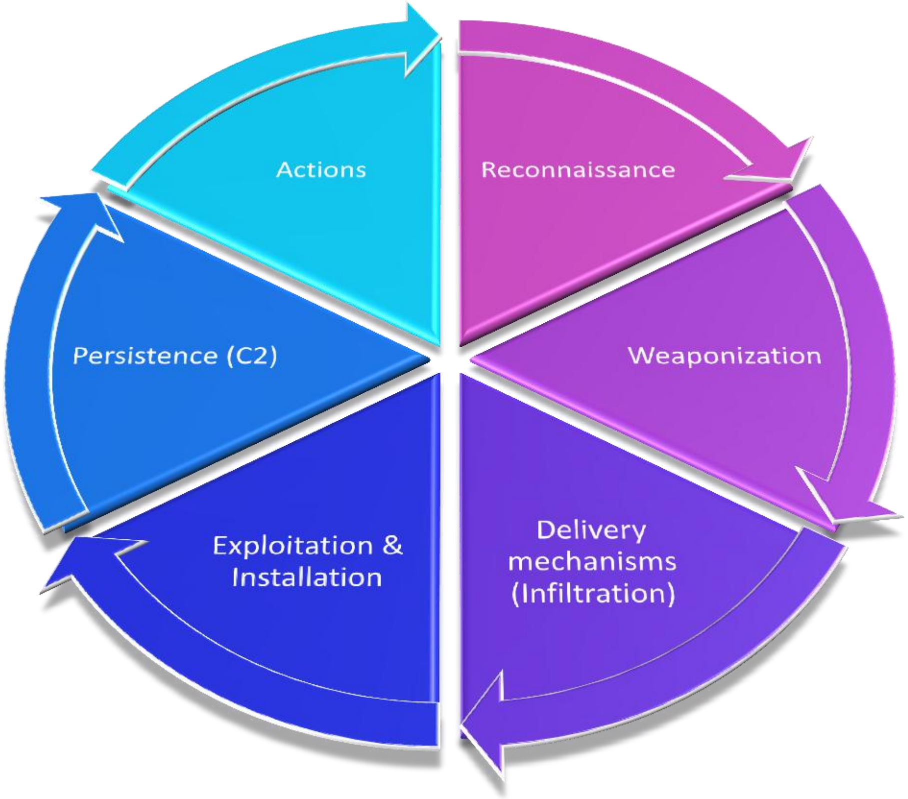


EXFILTRATION

Data sent to enemy's "home base" for analysis and further exploitation/fraud

Cyber Kill Chain

Identifying Overlapping Indicators at Different Levels


Reconnaissance
Weaponization
Delivery mechanisms (Infiltration)
Exploitation & Installation
Persistence (C2)
Actions

The State of Security Intelligence Data

Legacy Security Models

- Numerous data sets, multiple owners
- Multiple:
  - Physical locations
  - Database platforms
  - Data standards
- Limited data fusion
- Feature or function focused

Big Data Security Models

- Centralized storage/analysis of refined data
- Common database platform
- Codified common data standards
- Designed with data fusion in mind – correlation and analysis

Intelligence Extraction and Analysis

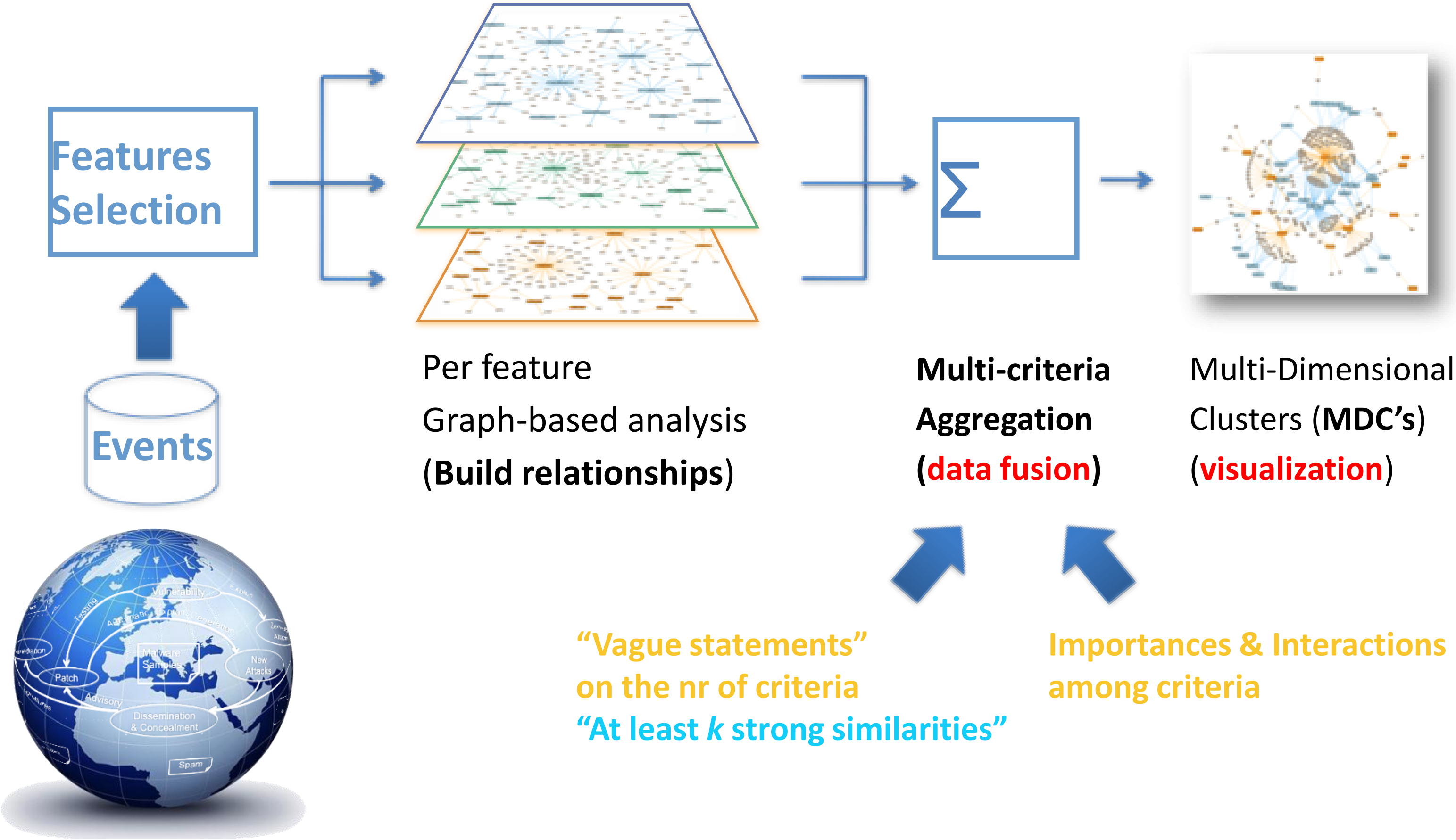
- Strategic Campaign Analysis
  - Determine the patterns and behaviors of the intruders, i.e., their tactics, techniques, and procedures
  - How attackers operate rather than what they do
  - Challenge: Intrusions sourced by the same attackers may have **varying** degrees of correlation
- Effective detection mechanisms for new threats relies on a **detailed understanding** of the threat and how the attackers operate
  - What is the modus operandi of attackers?
  - Who are the targets?
  - What are key indicators for these intrusions?

TRIAGE

- **Data analytics framework for *attack attribution***
  - Find *systematically* groups of events (intrusions) likely due to the same root cause
  - Identifies (varying) set of commonalities between attackers "fingerprints"
  - Enable the analysis of attackers *modus operandi*
- **Combines various approaches**
  - Graph Clustering techniques (unsupervised)
  - Multi-Criteria Decision Analysis (MCDA)
  - **Leverages Visual analytics (VIS-SENSE)**

THE TRIAGE APPROACH

- → Data clustering based on **M**ulti-**C**riteria **D**ecision **A**nalysis (MCDA)
- → Automatic grouping of elements likely to share the same root causes



Per feature
Graph-based analysis
(**Build relationships**)

Multi-criteria Aggregation
(**data fusion**)

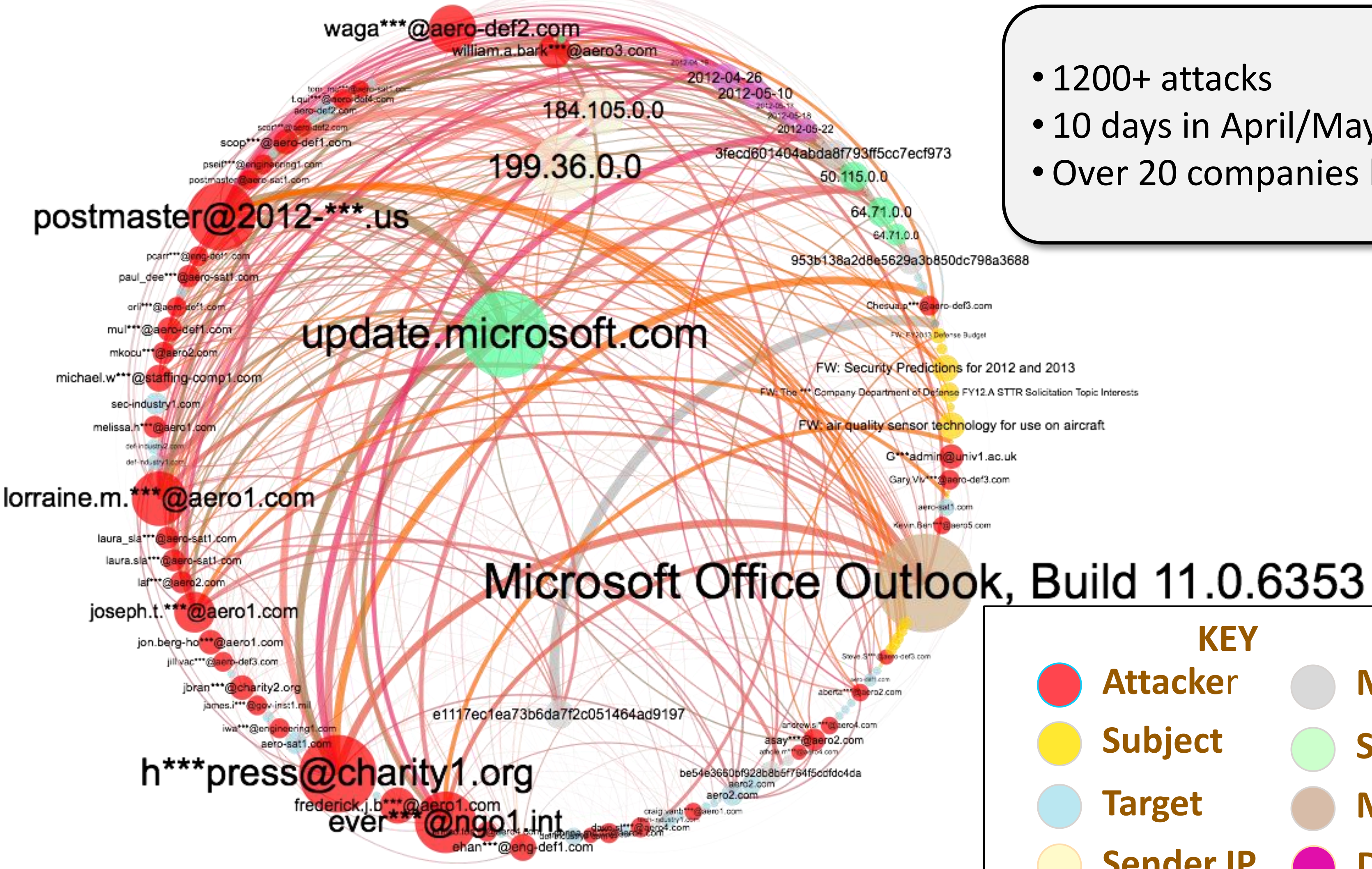
Multi-Dimensional Clusters (**MDC's**)
(**visualization**)

"Vague statements" on the nr of criteria
"At least *k* strong similarities"

Importances & Interactions among criteria

Mass-scale Targeted Attack Campaign

- 1200+ attacks
- 10 days in April/May 2012
- Over 20 companies hit



KEY

🔴	Attacker	●	MD5
🟡	Subject	●	Server
●	Target	🟤	Mailer
●	Sender IP	🟣	Date

Global Intelligence Network

Worldwide Coverage — **Global Scope and Scale** — 24x7 Event Logging

Rapid Detection

Threat Activity
- •240,000+ sensors
- •200+ countries

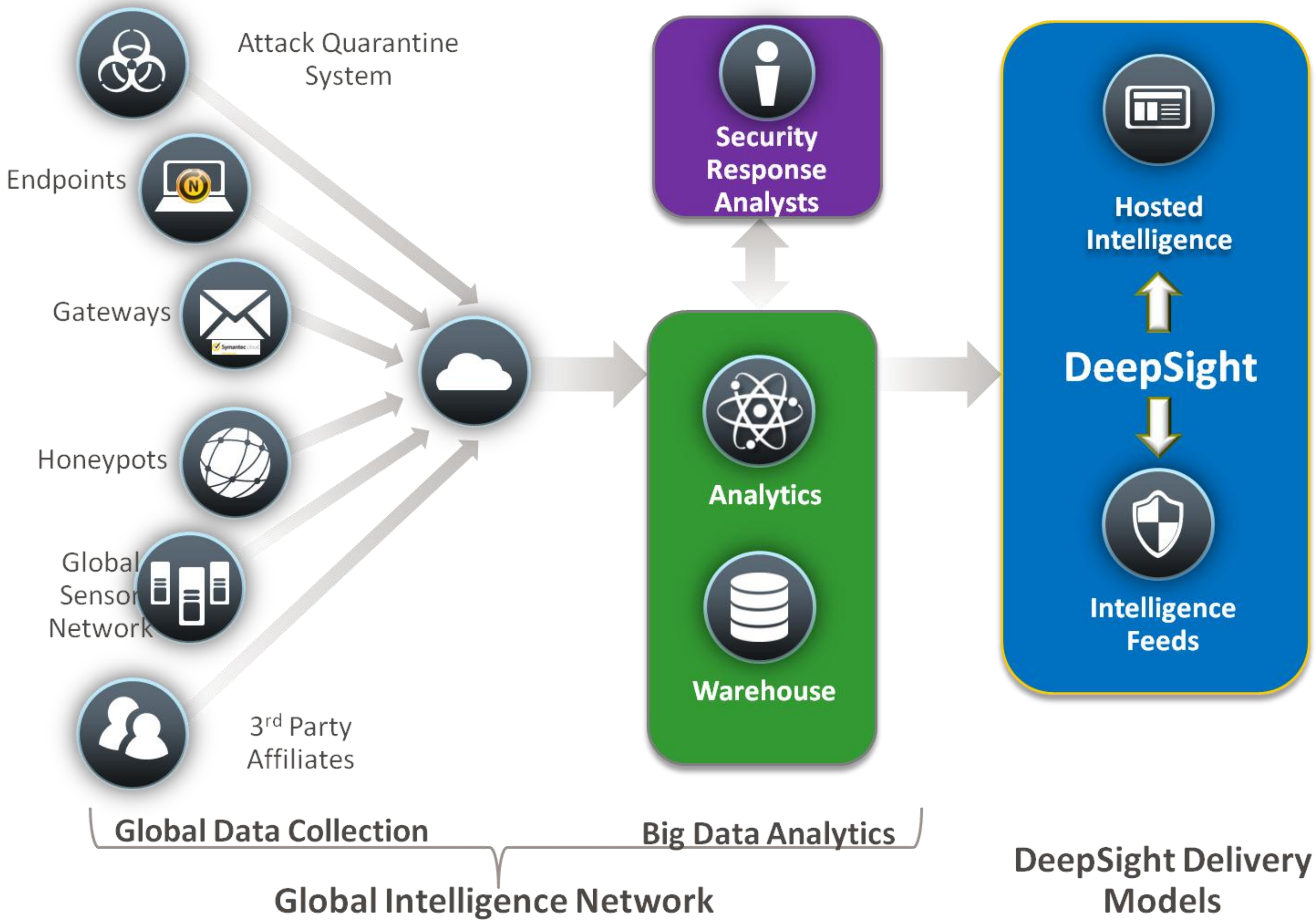
Malcode Intelligence
- •133M client, server, gateways
- •Global coverage

Vulnerabilities
- •40,000+ vulnerabilities
- •14,000 vendors
- •105,000+ technologies

Spam/Phishing
- •5M decoy accounts
- •8B+ email messages/daily
- •1B+ web requests/daily

Preemptive Security Alerts — **Information Protection** — Threat Triggered Actions

Symantec Data Analytics Platform



Security Intelligence Lifecycle Management

Planning

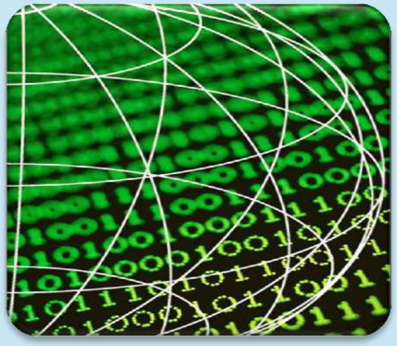
What needs to be tracked and analyzed

Client Directive or Symantec provided

Collection

Capturing relevant source data

Symantec Mission



Analysis

Integrating, collating, evaluating, and analyzing data

Symantec Mission

Dissemination

Providing the results of processing Data into Information

Client Directive or Symantec provided

Security in knowledge

Thank you!

Siân John

Symantec

@sbj24

sian_john@symantec.com

www.symantec.com