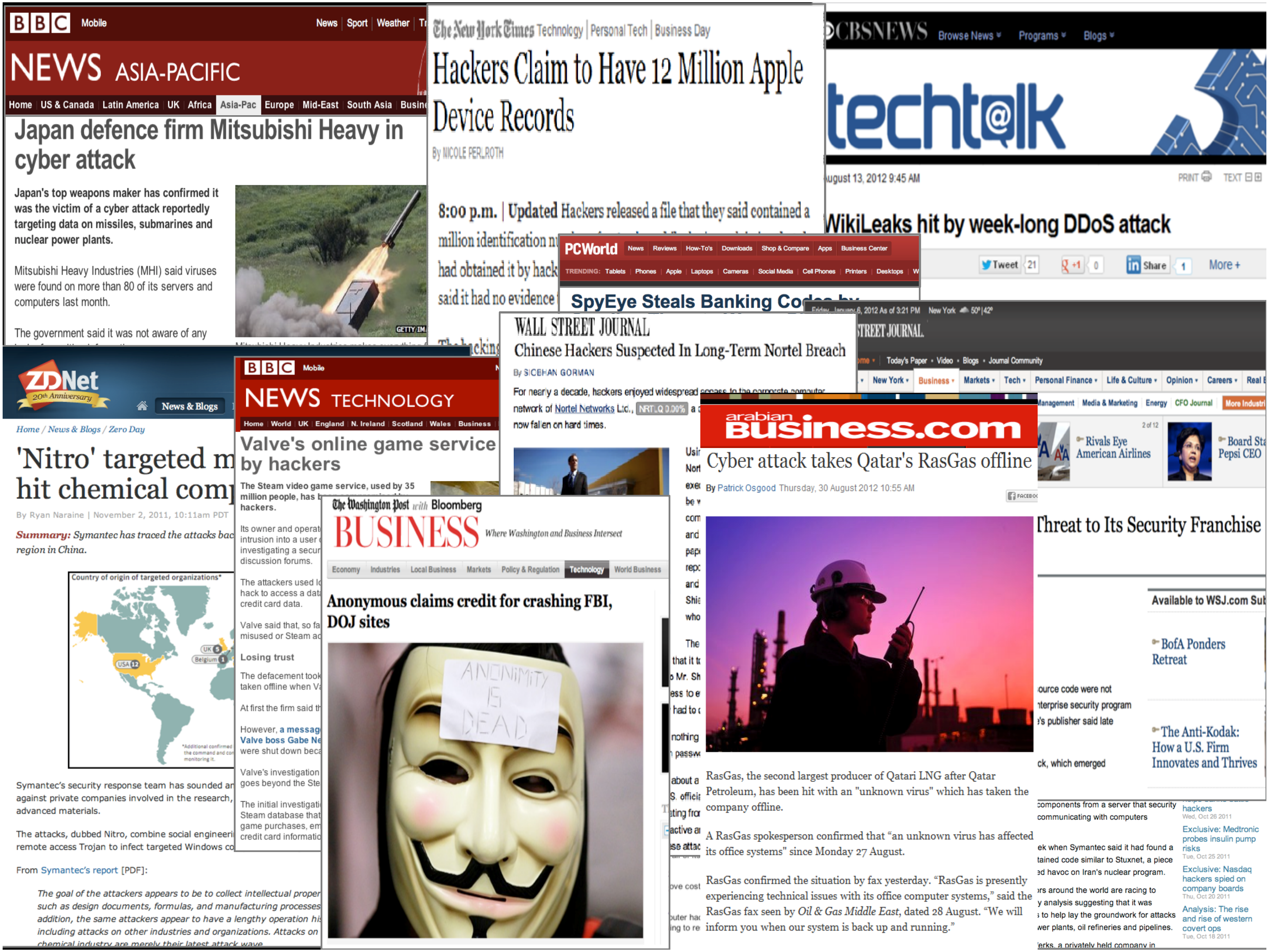
Government of Mauritius

Gregg Gerber

Strategic Engagement, Emerging Markets



BBC Mobile News | Sport | Weather | Tr

NEWS ASIA-PACIFIC

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

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

August 13, 2012 9:45 AM PRINT TEXT

WikiLeaks hit by week-long DDoS attack

Tweet 21 +1 0 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 now fallen on hard times.

Usi Nor exe be com and pap rep and Shi who

The that it t Mr. Sh ess to e had to nothing passw about a S. offici ting fro active a se attac ove cost puter hac ing to re

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

STREET JOURNAL.

ome | Today's Paper • Video • Blogs • Journal Community

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

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

2 of 12

Rivals Eye American Airlines

Board Sta 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*

USA 12 UK 5 Belgium 1

*Additional confirmed the command and co 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 hi 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 dat credit card data.

Valve said that, so fa misused or Steam ac

Losing trust

The defacement took taken offline when V

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

arabianBusiness.com

Cyber attack takes Qatar's RasGas offline

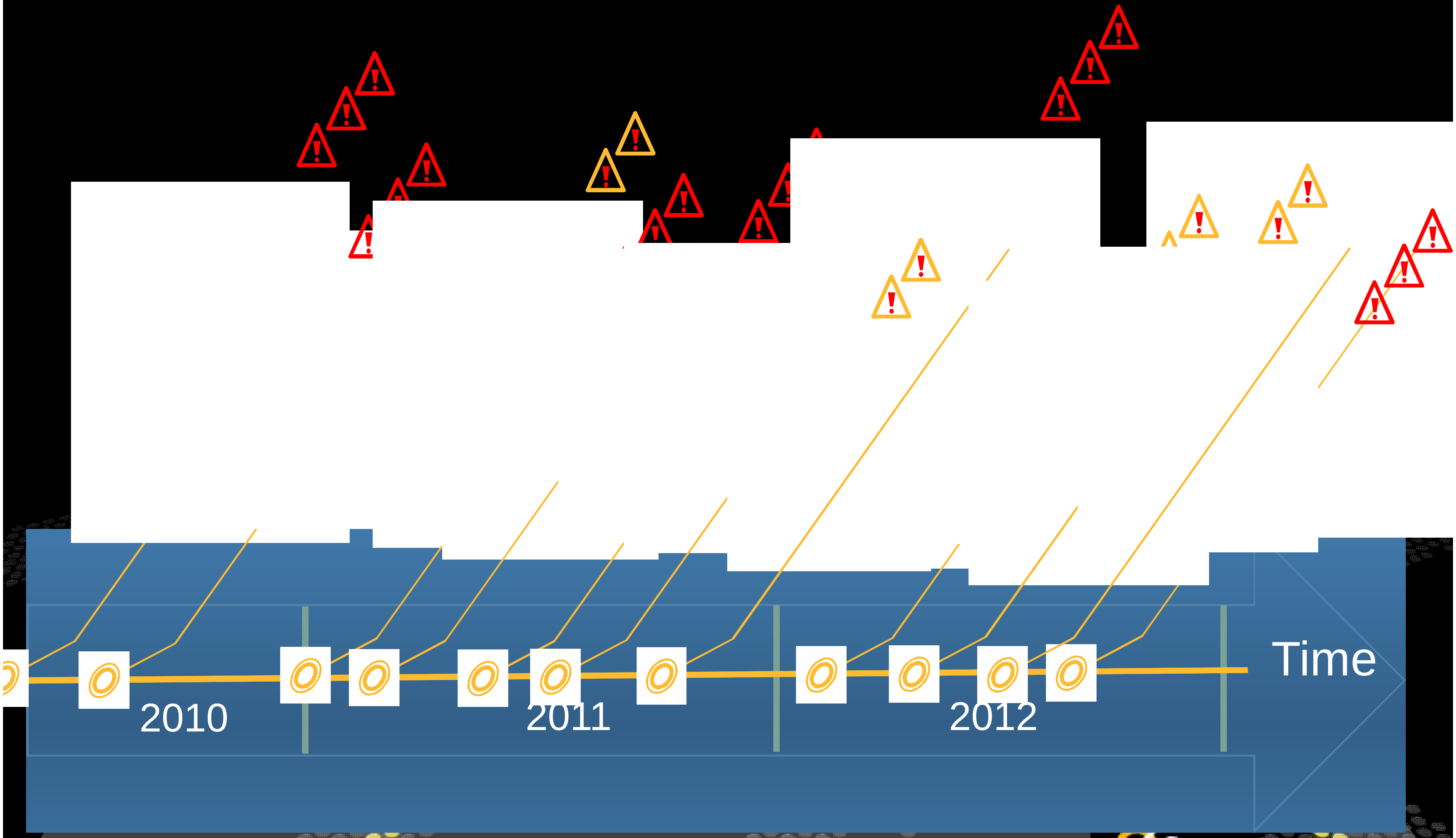
By Patrick Osgood Thursday, 30 August 2012 10:55 AM

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

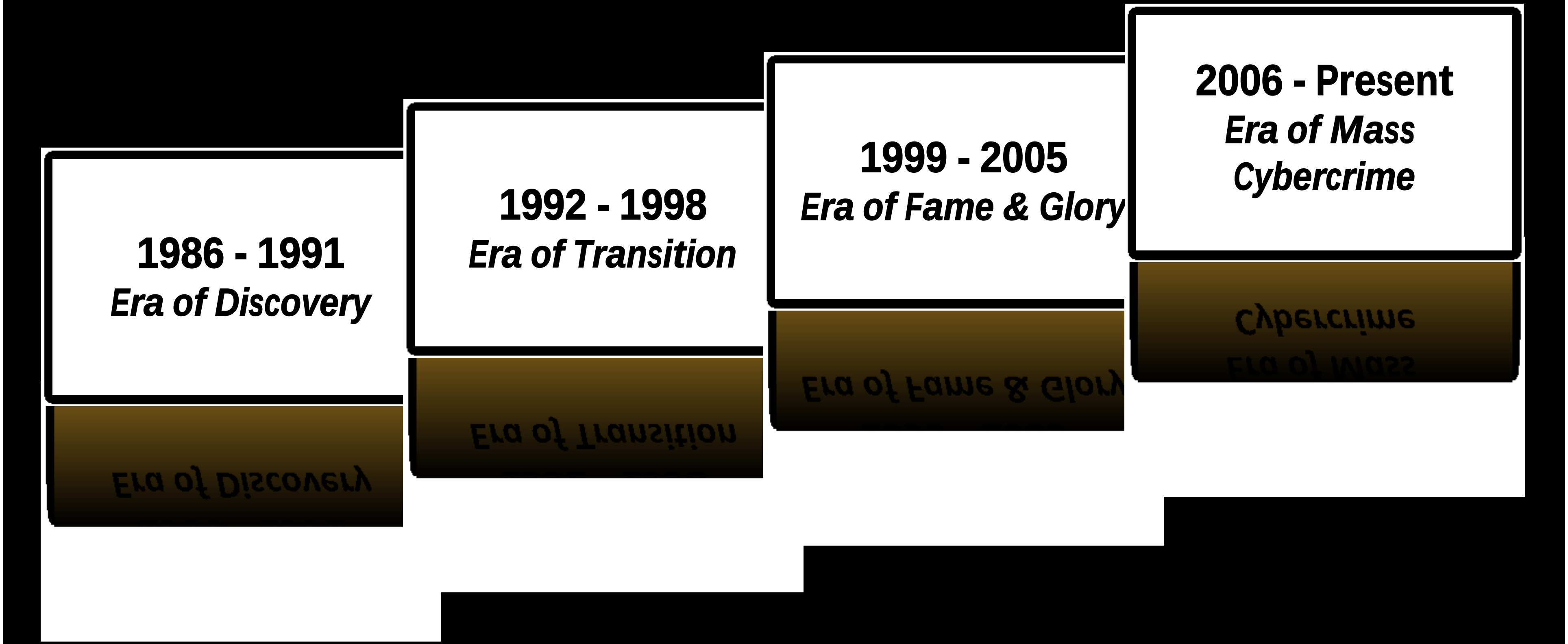
A RasGas spokesperson confirmed that "an unknown virus has affected its office systems" since Monday 27 August.

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."

(Advanced) Persistent Targeted attacks



Symantec.



1986 - 1991
Era of Discovery

1992 - 1998
Era of Transition

1999 - 2005
Era of Fame & Glory

2006 - Present
Era of Mass Cybercrime

Attackers
Malicious O

State Nation

Insiders
icious and
-Malicious

Hack-tivists
Hacking for

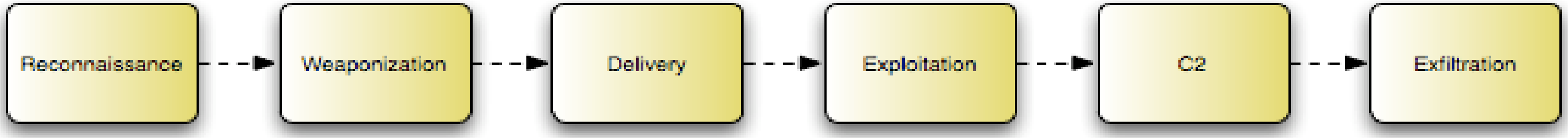
Cyber Criminals

APT	Attacker (Malicious Outsider)	Insider (Malicious and Non-malicious)	Hack-tivist	Cyber Criminals	State Nation
RECON	Free Scanners	Insider Knowledge	Social Networks / Google	Data Mining	Espionage / Collusion
INCURSION	Basic Scripts /MetaSploit	Privileged Access	Social Engineering	Attack Kits / Malcode / Bots / Affiliates	Tailored Malcode / 0-Day
DISCOVERY	Random Targeting	Asset Awareness	Targets of Chance	Targets of Chance / Choice	Targets of Choice
CAPTURE	Visible / Low Value	Critical Assets	Media Worthy Asset or Access	Monetized Assets	High Value IP / Government Secrets
EXFILTRATE	Tagging and Damage	Theft and Damage	DDoS, Theft and Damage	Fraud and Financial Gain	Gain / Maintain Strategic Advantage

Strategy Rethink: Anatomy of an attack

1. Research
2. Incursion
3. Discovery
4. Capture
5. Exfiltrate

Risk Posture and Policies



Reconnaissance → Weaponization → Delivery → Exploitation → C2 → Exfiltration

IT Security pressures – changing world

Time
- to enable
- to respond

User demands
- Social Networking
- Fav technology

Reduce costs

Information
- Supply chain
- De-perimeterisation

New Tech adoption

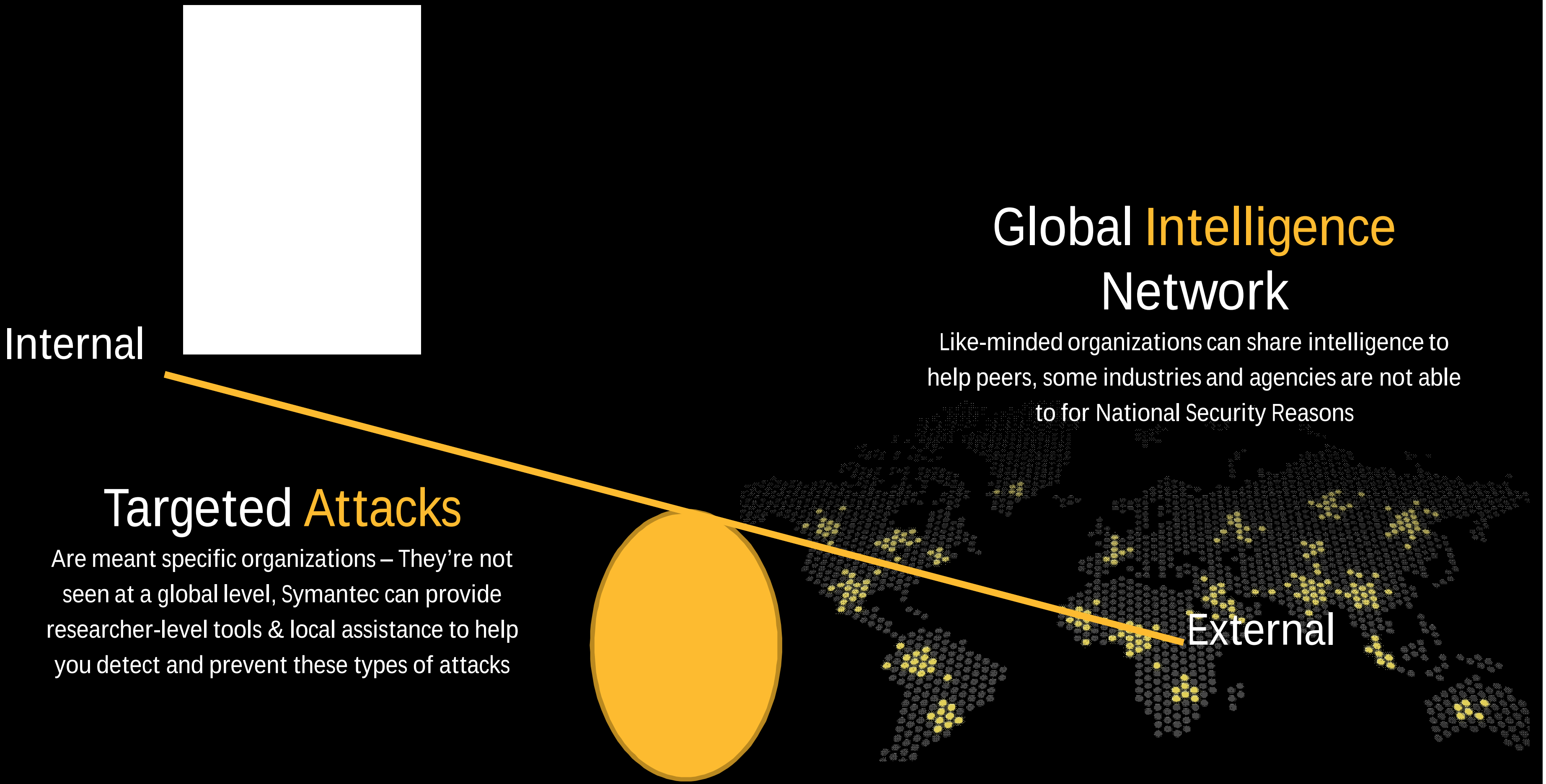
Governance

Compliance

Security Complexity (More controls)

Threats
- Volume
- Type

Where Does Your Threat Intelligence Reside?



Internal

External

Global Intelligence Network

Like-minded organizations can share intelligence to help peers, some industries and agencies are not able to for National Security Reasons

Targeted Attacks

Are meant specific organizations – They're not seen at a global level, Symantec can provide researcher-level tools & local assistance to help you detect and prevent these types of attacks

Symantec Cyber Threat Intelligence

Cyber Awareness

Cyber Briefing Center | Strategist Advisories
Cyber Risk Assessments | Cyber Training
Cyber Readiness Assessments

Cyber Preparedness

Security Base lining | Threat Intelligence Reports
Reputation Analysis | Business Risk Modeling

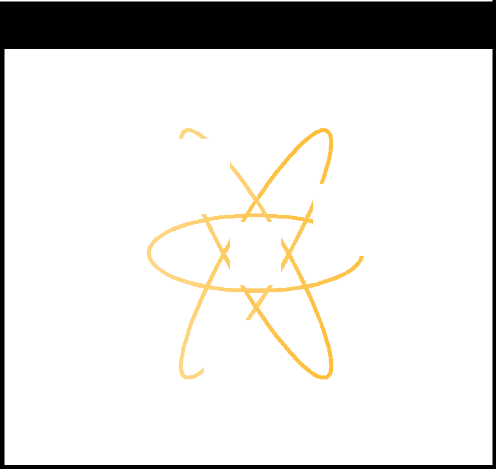
Cyber Forensics

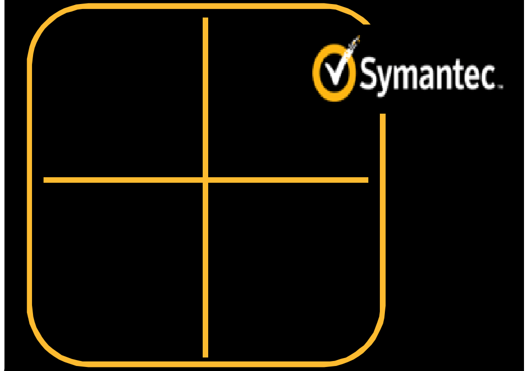
Security Base lining
Incident & Event Management
Threat Analysis & Response
Threat Impact Assessment

Cyber Response

Product & Threat Analysis Support
Cyber Incident Advice
Cyber Threat Response | Scribe

What Makes Symantec Unique?





Leaders in Threat Research & Technology

The Biggest Organisations Trust our People & Services

Provide Risk-Based Perspective

Market Validation

Symantec Cyber Threat Intelligence Summary

Government Engagement

Participation in National Cyber Strategies

Security Intelligence Group

Our Global Intelligence Network and Reputation Feeds add Threat Context to YOUR Infrastructure

Highly Targeted Threat Analysis

The Symantec's Threat Analysis Tools Used by Our Researchers Are Also Available to You to Analyze Highly Targeted Attacks

Leverage Existing Investments

Our Modular Approach means we can Leverage Investments in Your Existing Security Controls, and Demonstrate Where to allocate resources With Risk Modeling

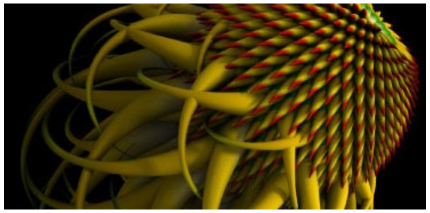
Cyber Readiness Programs

We Help you understand YOUR risks and Prepare for Cyber Threats

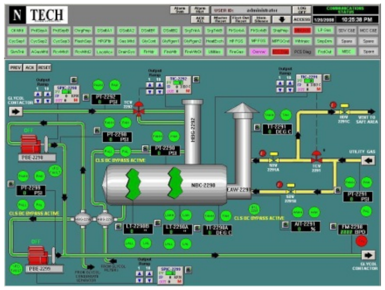
Attack Scenarios

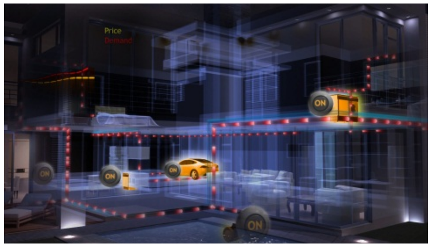
Targets - Depend on the objective of the attacker

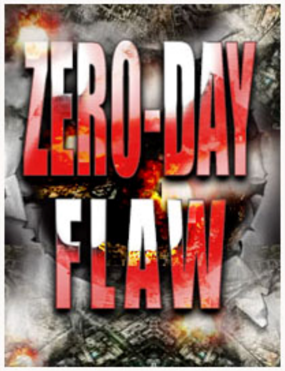
Modus operandi



Modus operandi







Specifically on defense

5th Domain of Warfare

Land

Sea

Air

Space

Cyber

Merge of EW and SIGINT with cyber

Specifically on defense

Makes sense from a military point of view

VS.

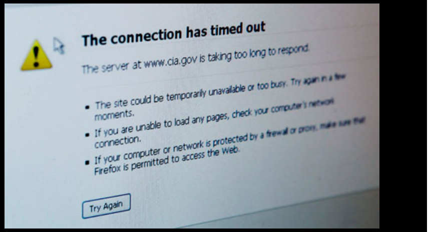
Sensors, communications and robotics technologies dominating future battlefield

Specifically on defense

Historically listen to information & deny access to information

access denied...

...unauthorized request

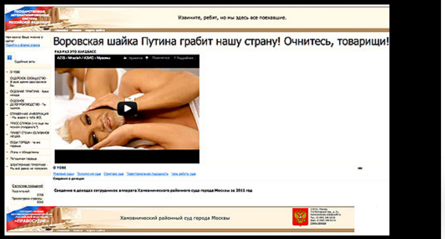


The connection has timed out

The server at www.cia.gov is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

New paradigms include modifying information to create a false operational picture and damage the infrastructure, or remotely control it



Извините, ребят, но мы здесь все поехавшие.

Воровская шайка Путина грабит нашу страну! Очнитесь, товарищи!

О СУДЕ

Сведения о доходах сотрудников аппарата Хамовнического районного суда города Москвы за 2015 год

Хамовнический районный суд города Москвы

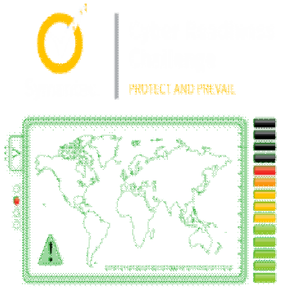
Cyber Awareness

Strategist Cyber Advisories

Summary business reports defining best practices for mitigating the attack

Cyber Training

Cyber threat detection and incident response course (10day)



Cyber Briefing Center

Briefing on the latest threats
Understand the processes and techniques required to deal with today's cyber attacks

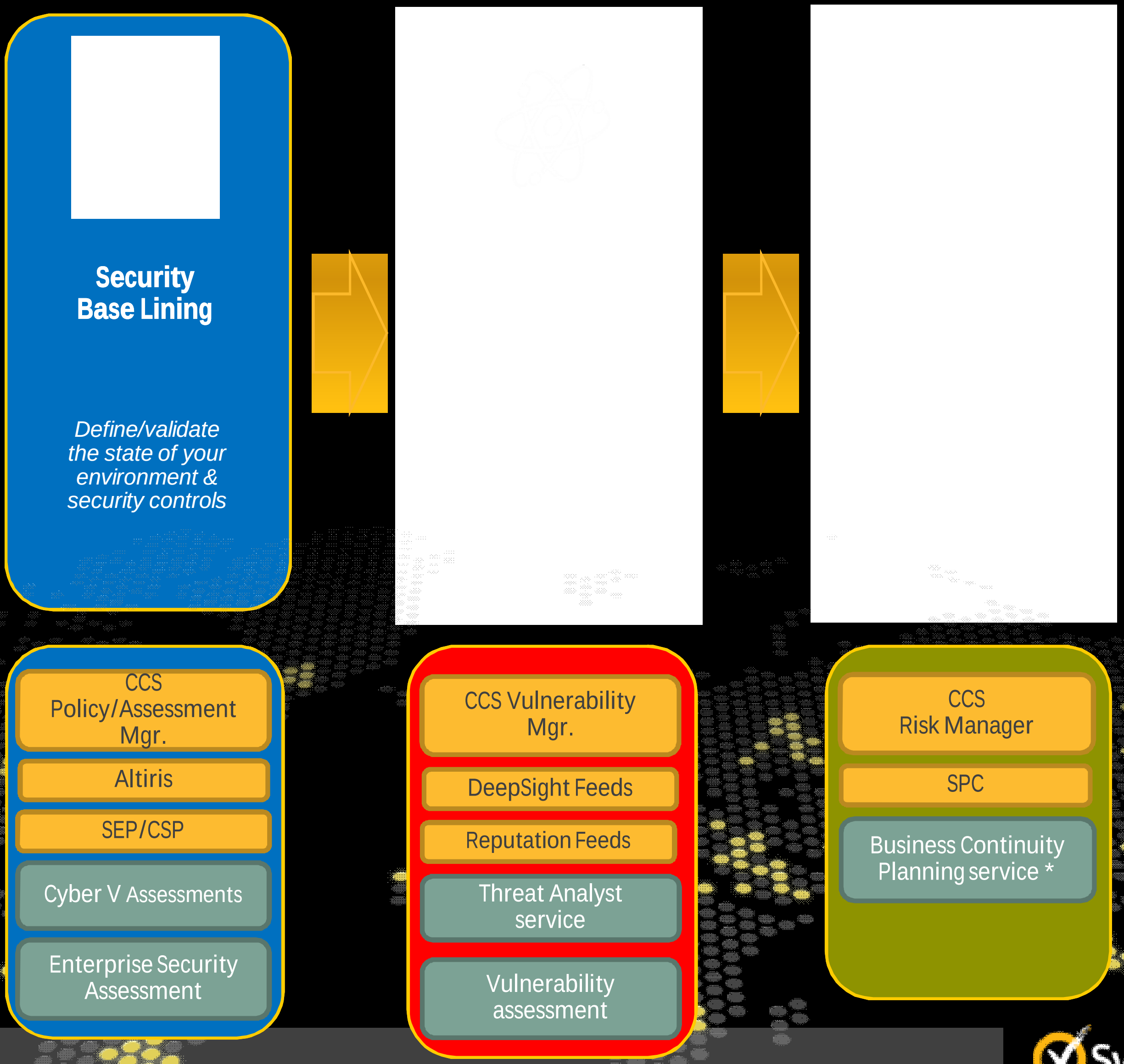
Cyber Risk Assessments

Information risk assessments, cyber security policy assessments

Cyber Readiness

Join in Symantec's Cyber war games to test and develop your skills and capability

Cyber Preparedness



Security Base Lining

Define/validate the state of your environment & security controls

CCS Policy/Assessment Mgr.

Altiris

SEP/CSP

Cyber V Assessments

Enterprise Security Assessment

CCS Vulnerability Mgr.

DeepSight Feeds

Reputation Feeds

Threat Analyst service

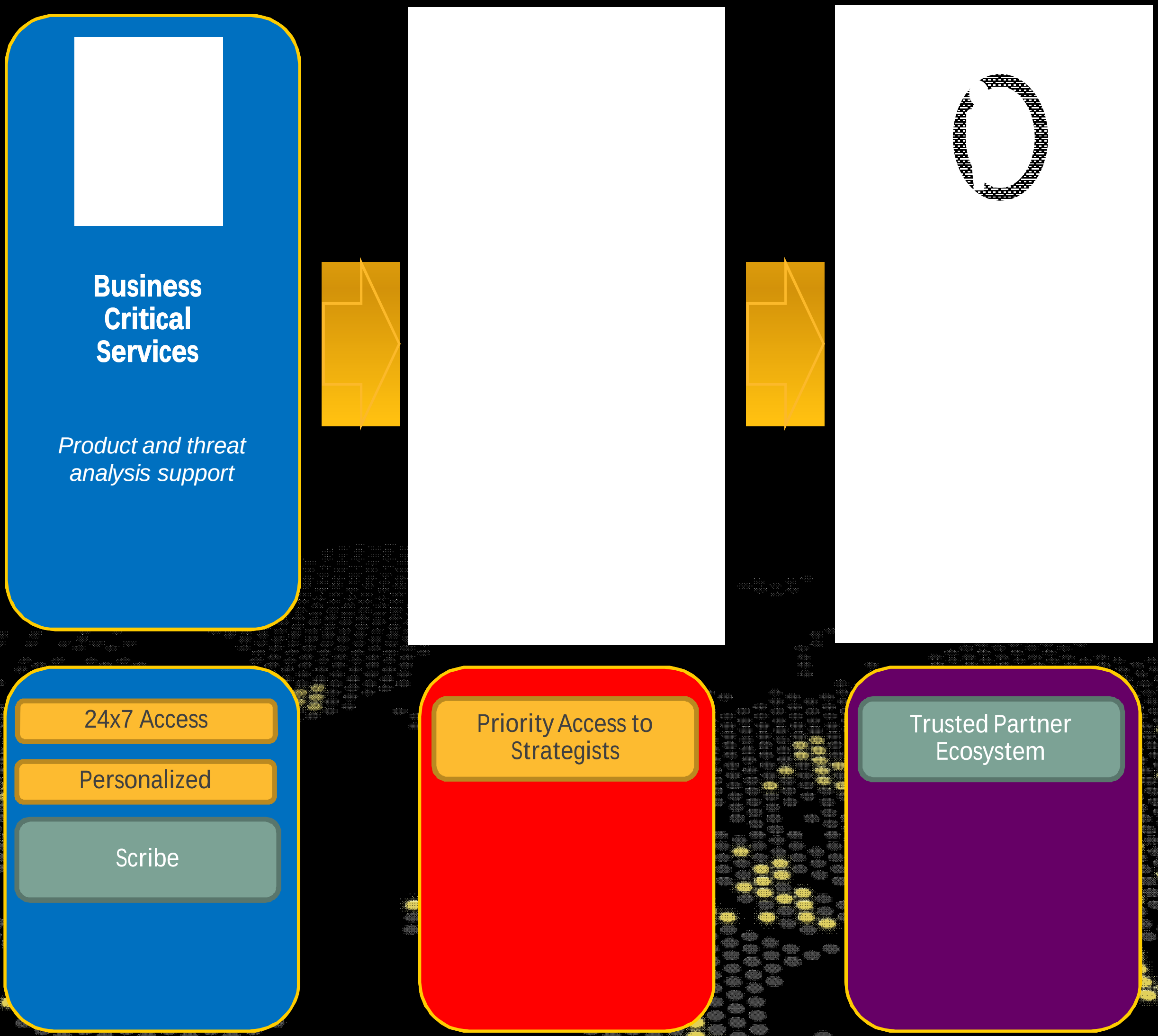
Vulnerability assessment

CCS Risk Manager

SPC

Business Continuity Planning service *

Cyber Response



Business Critical Services

Product and threat analysis support

24x7 Access

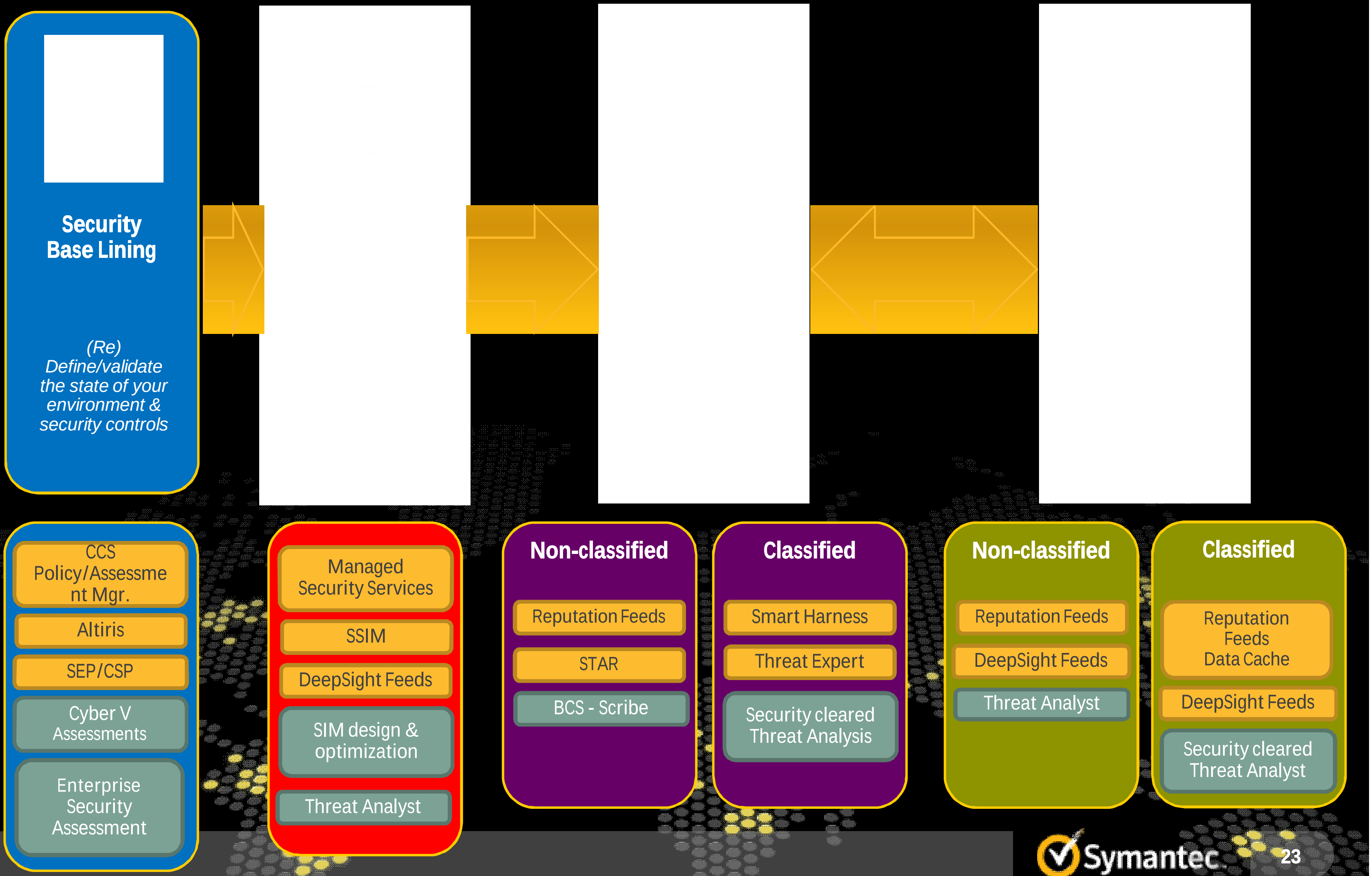
Personalized

Scribe

Priority Access to Strategists

Trusted Partner Ecosystem

Cyber Forensics – In-Progress & Post Incident



Security Base Lining

(Re) Define/validate the state of your environment & security controls

- CCS Policy/Assessment Mgr.
- Altiris
- SEP/CSP
- Cyber V Assessments
- Enterprise Security Assessment

- Managed Security Services
- SSIM
- DeepSight Feeds
- SIM design & optimization
- Threat Analyst

Non-classified

- Reputation Feeds
- STAR
- BCS - Scribe

Classified

- Smart Harness
- Threat Expert
- Security cleared Threat Analysis

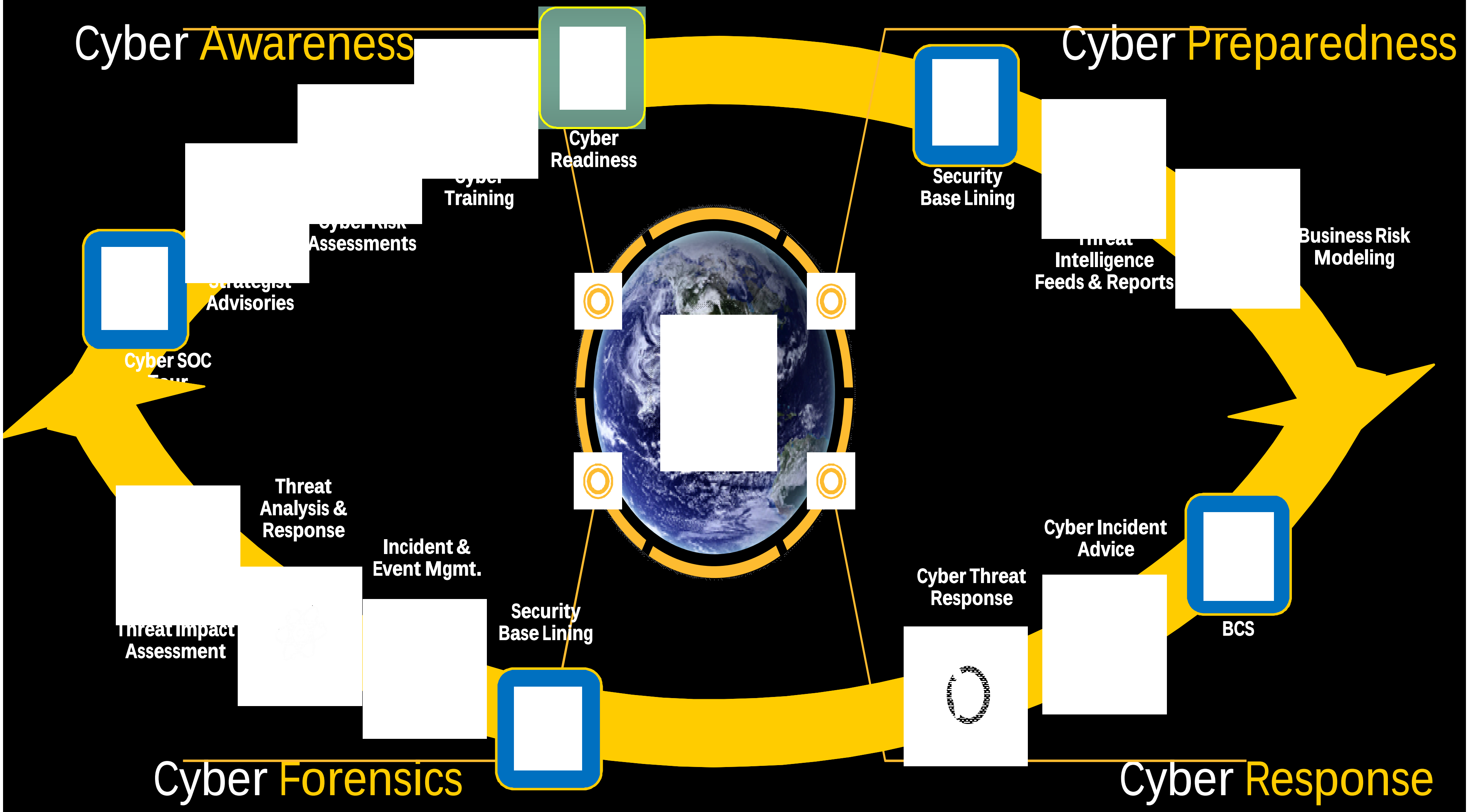
Non-classified

- Reputation Feeds
- DeepSight Feeds
- Threat Analyst

Classified

- Reputation Feeds Data Cache
- DeepSight Feeds
- Security cleared Threat Analyst

Symantec Cyber Lifecycle Offering



Thank You

Gregg Gerber

Gregg_gerber@symantec.com

gregg_gerber