How to Define and Build Threat Intelligence Capability

Prof. Claudio Cilli, CISA, CISM, CGEIT, CRISC, CSX-P
University of Rome, Italy
claudio.cilli@uniroma1.it
http://wwwusers.di.uniroma1.it/~cilli
https://www.linkedin.com/in/claudiocilli/

Agenda

Why threat intelligence?

What exactly is threat intelligence?

What Threat Intel Does: Situational Awareness

Threat Intelligence Capability

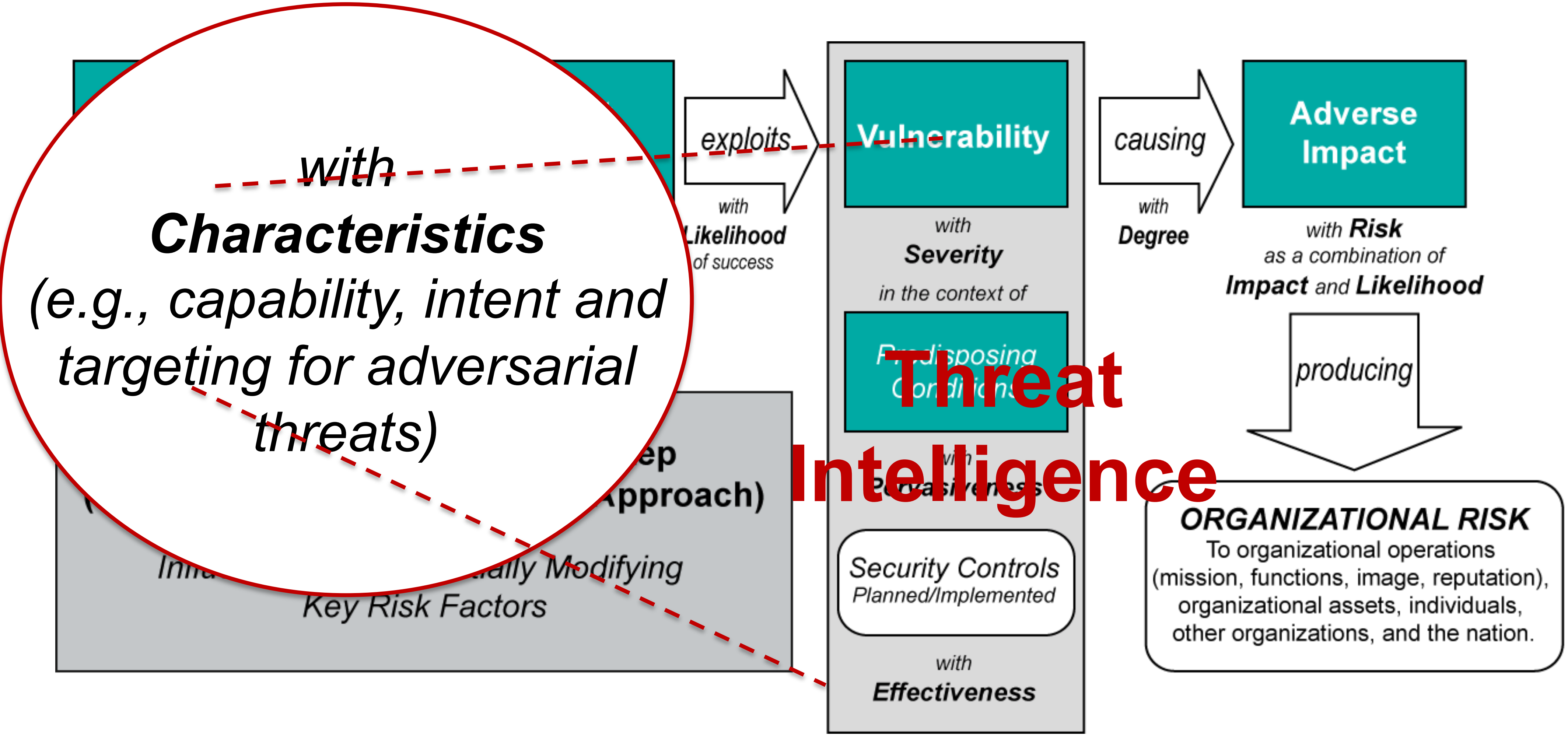
OSINT & Other sources

Proliferation of cyber-weapons

Conclusion

Why Threat Intelligence?

The NIST Risk Management Framework



with **Characteristics** *(e.g., capability, intent and targeting for adversarial threats)*

exploits with **Likelihood** of success

Vulnerability with **Severity** in the context of *Predisposing Conditions* with **Pervasiveness**

Security Controls *Planned/Implemented* with **Effectiveness**

causing with **Degree**

Adverse Impact with **Risk** as a combination of **Impact** and **Likelihood**

producing

ORGANIZATIONAL RISK
To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the nation.

ep **Approach)**

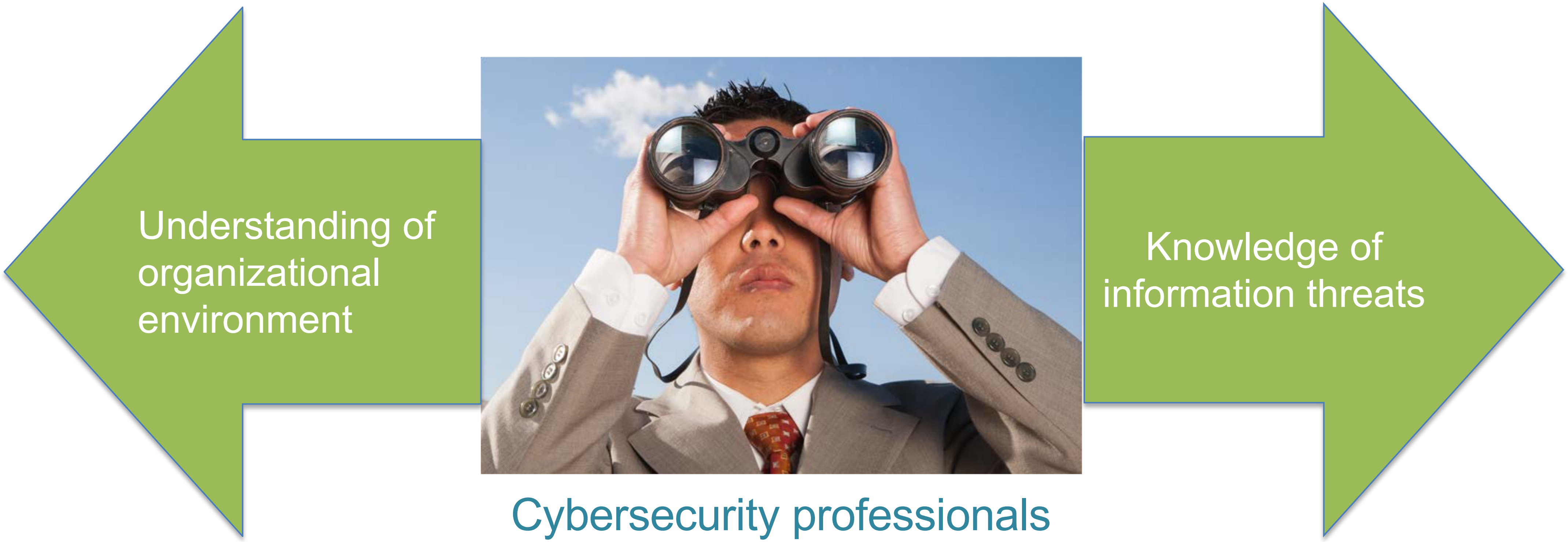
Infl... ally Modifying Key Risk Factors

Threat Intelligence

Source: “Generic Risk Model with Key Risk Factors,” National Institute of Standards and Technology (NIST), Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments,* USA, September 2012

Situational Awareness

Understanding **real** threats and **comprehensive** organizational environment represents the fundation of Threat Intelligence



Understanding of organizational environment

Knowledge of information threats

Cybersecurity professionals

What exactly is threat intelligence?

Forrester’s definition

“Details of the motivations, intent, and capabilities of *internal* and *external* threat actors. Threat intelligence includes specifics on the tactics, techniques, and procedures of these adversaries. *Threat intelligence's primary purpose is to inform business decisions regarding the risks and implications associated with threats.*”

Gartner’s definition

“Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard to assets that *can be used to inform decisions regarding the subject’s response to that menace or hazard.*”

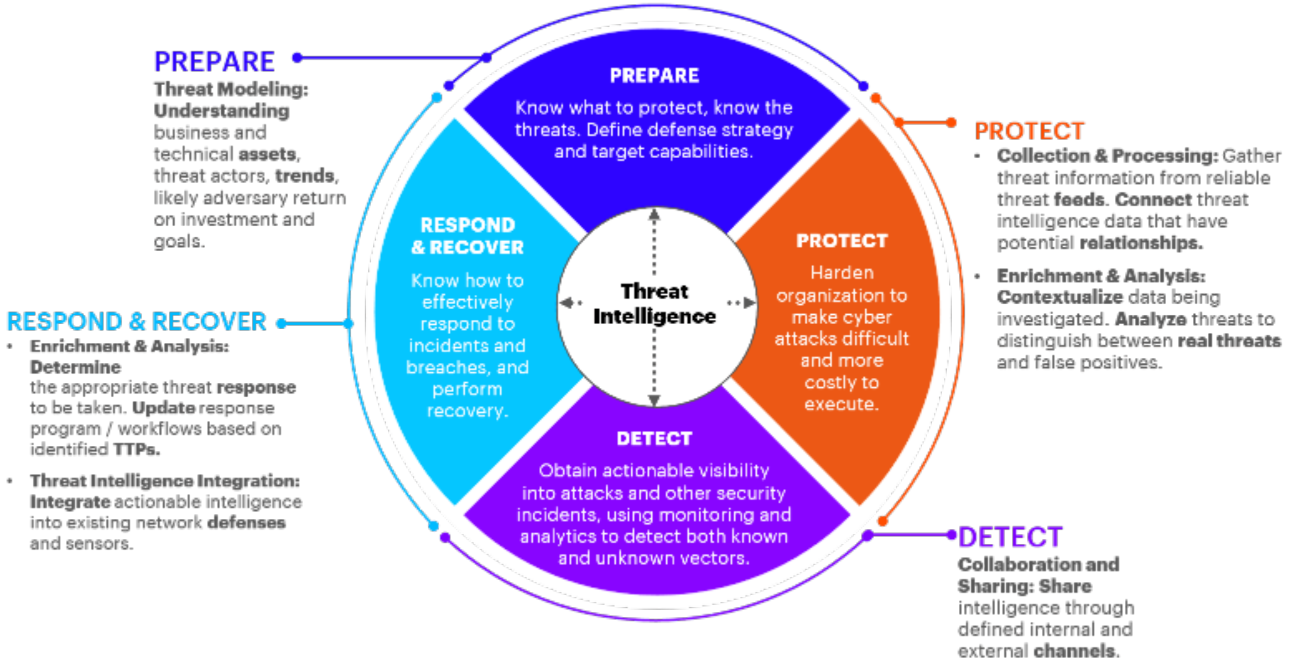
Threat Intel (TI) =

Strategic:

- **Context**
- Motivations
- Capabilities
- Implications
- **Actionable** Advice

Operational:

- **Context**
- Mechanisms
- Indicators
- **Tactics**
- **Techniques**
- **Procedures**



PREPARE

Threat Modeling: Understanding business and technical **assets**, threat actors, **trends**, likely adversary return on investment and goals.

RESPOND & RECOVER

- **Enrichment & Analysis: Determine** the appropriate threat **response** to be taken. **Update** response program / workflows based on identified **TTPs.**
- **Threat Intelligence Integration: Integrate** actionable intelligence into existing network **defenses** and sensors.

PREPARE

Know what to protect, know the threats. Define defense strategy and target capabilities.

RESPOND & RECOVER

Know how to effectively respond to incidents and breaches, and perform recovery.

Threat Intelligence

PROTECT

Harden organization to make cyber attacks difficult and more costly to execute.

DETECT

Obtain actionable visibility into attacks and other security incidents, using monitoring and analytics to detect both known and unknown vectors.

PROTECT

- **Collection & Processing:** Gather threat information from reliable threat **feeds. Connect** threat intelligence data that have potential **relationships.**
- **Enrichment & Analysis: Contextualize** data being investigated. **Analyze** threats to distinguish between **real threats** and false positives.

DETECT

Collaboration and Sharing: Share intelligence through defined internal and external **channels.**

What Threat Intel Does:

Situational Awareness

Situational Awareness

Strategic:

- Risk Management
- Vulnerability Management
- Threat Modeling

↑

Prevention

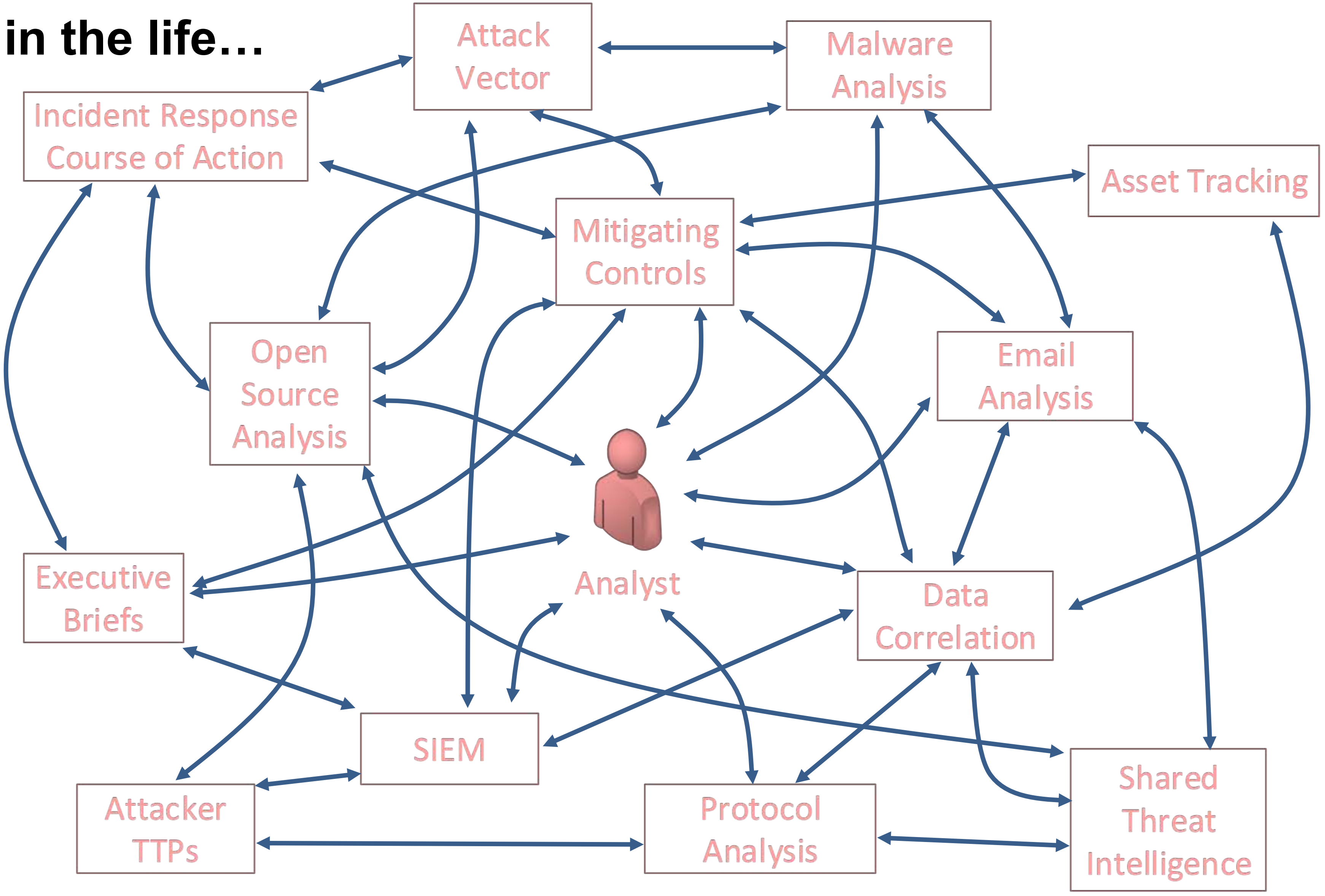
Tactical:

- Proactive/Reactive IR
- Threat Communications
- Breach Discovery

↑

Detection

Day in the life…



Attack Vector

Malware Analysis

Incident Response Course of Action

Asset Tracking

Mitigating Controls

Open Source Analysis

Email Analysis

Analyst

Executive Briefs

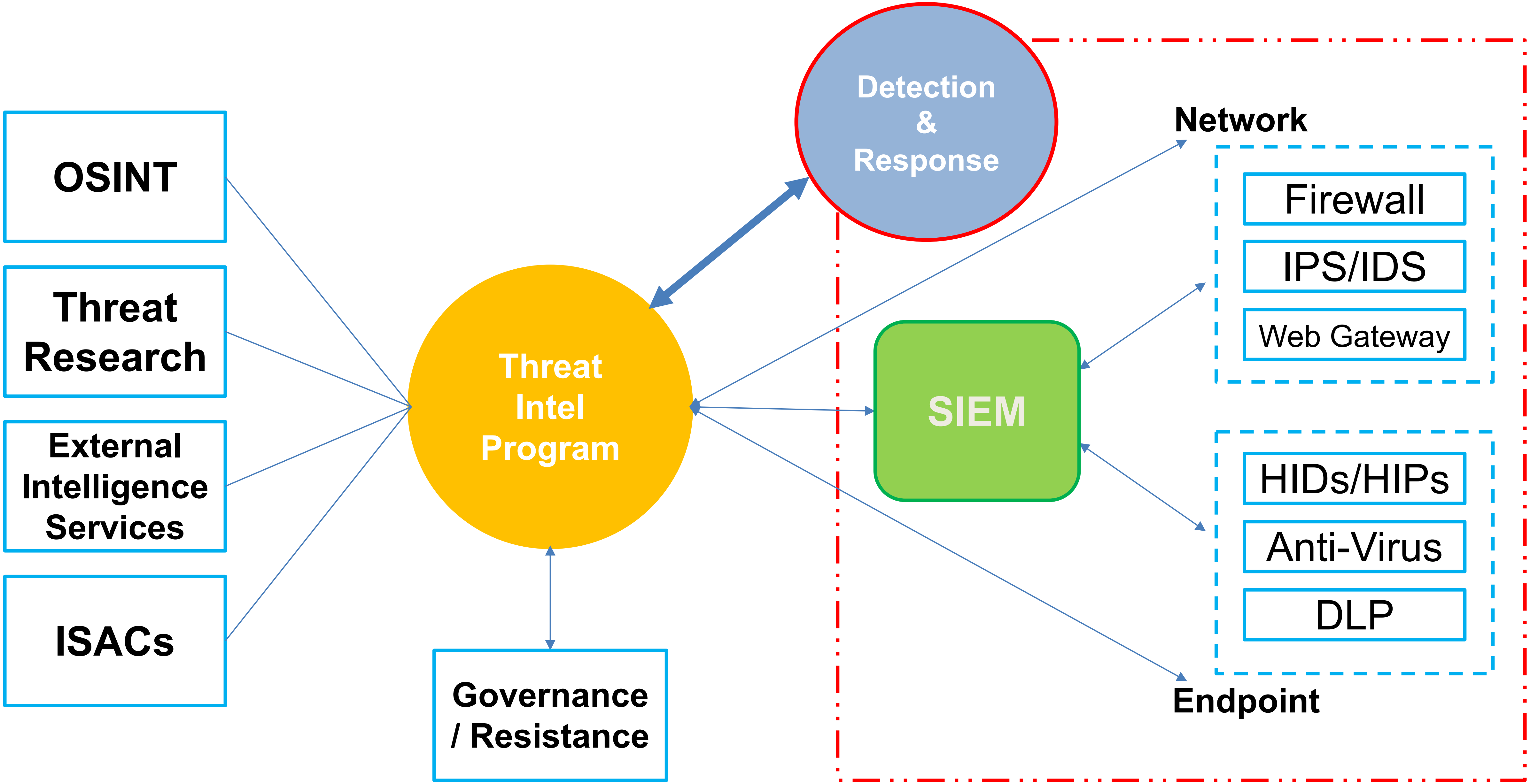
Data Correlation

SIEM

Attacker TTPs

Protocol Analysis

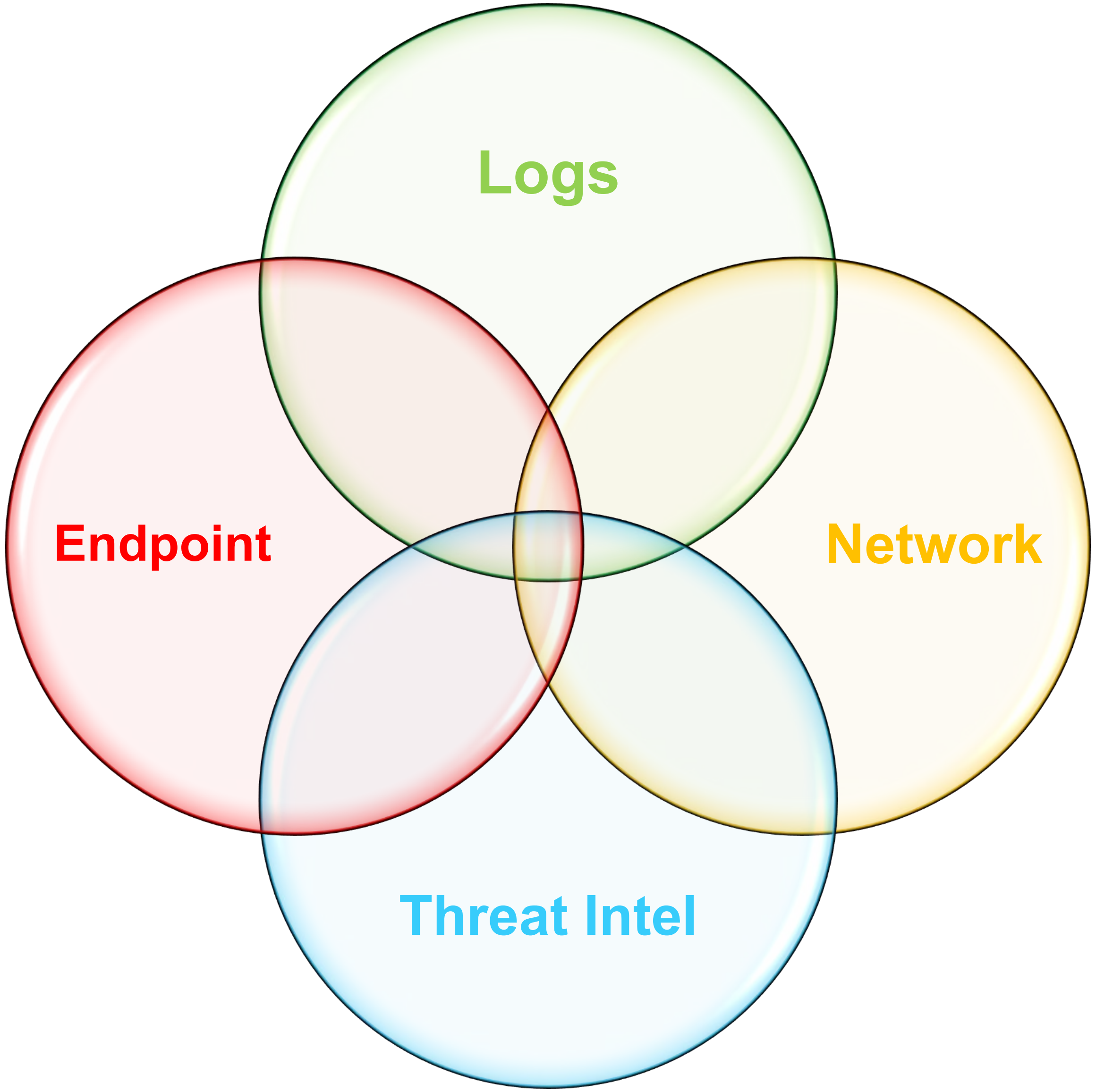
Shared Threat Intelligence


OSINT
Threat Research
External Intelligence Services
ISACs
Threat Intel Program
Governance / Resistance
Detection & Response
SIEM
Network
Firewall
IPS/IDS
Web Gateway
HIDs/HIPs
Anti-Virus
DLP
Endpoint

TI/IR Focal Points

Focal points:

- Logs
- Network
- Endpoint
- Threat Intel



Threat Intelligence Capability

Corporate Cyber Threat Intelligence

“If you **know the enemy** and know yourself you
need not fear the results of a hundred battles” (SunTzu)

Purpose: Enable risk reduction

Three Levels:

- **Tactical** – Improve defense against today’s attacks
- **Operational** – Focus security engineering and resiliency
- **Strategic** – Improve corporate risk decisions going forward

Value of Corporate Threat Intelligence Practice

- **Tactical**: Improve the ability of NOC/SOC and other corporate security personnel to anticipate prevent & mitigate cyber attacks across a wide spectrum
  - Including amateurs, fraud, APT, DDOS and insiders
  - Will involve activities that reaches across security functions

- **Operational**: Improve ability of CISO, CIO, CTO to evolve use of IT / Cyber for both protection and response
  - Understand threat to improve security engineering
  - Improve training/exercise programs – improve people

- **Strategic**: Improve CRO, CEO and Board decisions about cyber risk
  - Inform decision about where to operate facilities and people
  - Improve security management of vendors and supply chain

Initiating a Threat Intelligence Practice

- Understanding Your Adversaries and Risks
- Establish the Level of Corporate Commitment
  - Mission & Responsibilities -> Resources
- Management
  - Who’s in Charge & Organization
  - Concept of Operation -> Implementation Plan
- Skilled People
  - Ninjas plus Positions
- Sources of Information
  - Internal and External
- Tools and Technical Processes
  - Development of an Analytical Engine

Understand Mission > Assess Current Capabilities > Evolve to Strategic Approach

Map Your Adversaries

Risk	*Potential Adversary*	*Description & Intent*	*Example*	*Applicability*
High	Organized crime	Independent or collective hackers that collect information that can be sold for a profit or used directly for fraud and extortion; may be for hire for non-state actors	2011 Unknown criminal syndicate (Fidelity Information Service) 2013 Eastern European criminals (World Health Organization)	Seek access to client data; target organization to hold data hostage in order to make money
	Hacktivist/ advocacy groups	Decentralized group that targets sectors of interest to disrupt productivity and cause reputational damage or advance specific causes through information gathering	2007 Albert Gonzales (Heartland Payment Systems, others) 2010 Anonymous (HBGary, OWS, etc.)	Expose confidential info, inject misinformation into news stream, use website to send a message
Med.	Disgruntled Employees/ Contractor Access	(may be used by other adversaries) Trying to damage the company/make money	2007-9 Samarth Agrawal (SocGen) 2009-11 Chunlai Yang (Chicago Mercantile Exchange) 2010 Rodney Reed Caverly (Bank of America)	Provide code to others – enable disruption to use as intellectual property; emplace software bugs to cause major systems disruption
	State sponsored entity	Well resourced, operational teams with goals to damage competitor interests/impact critical infrastructure operations/track dissidents	2006- China (comprehensive) 2007- Russia (Estonia, Georgia) 2009- US/Israel (Iran) 2012- Iran (financial services)	Disrupt ability to provide accurate trading data to shut down markets; get at news investigators
Low	Corporate competitors	Other corporate entities that want to understand inner workings of others or steal intellectual property for internal use	2008, Starwood sues Hilton for theft of thousands of pages of company data, $75M in damages	Competition for various tools or tradecraft might be of value to competitors, likely to hire ex-employees to get this data
	Opportunists	Unaffiliated hackers (usually young) looking for bragging rights and hacker community recognitions, and may target information could be of value to sell or use	1998 Kazakh nationals (Michael R. Bloomberg) 2013 Syrian Group (Associated Press Twitter)	Unaffiliated parties take advantage of security gaps, able to dig around to find information, or other actions

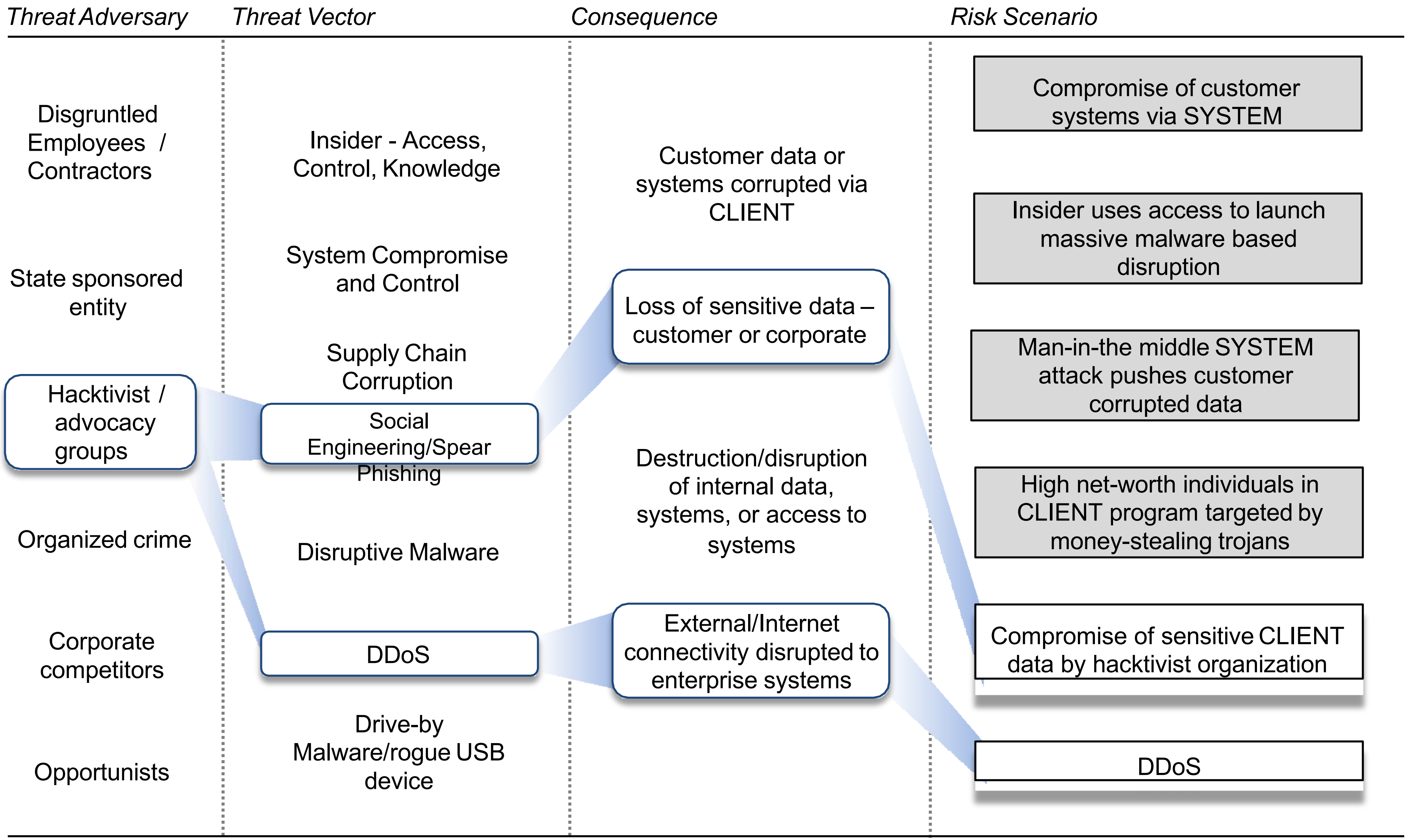
Analyze Your Potential Attack Vectors

Threat Vectors	*Description*	*Example*	*Applicability*
Insider - Access, Control, Knowledge	Has legitimate access to networks, systems, code and data	2011, Citigroup employee steals $750k over 8 years by subverting monitoring and audit capabilities	Disgruntled employee accesses customer databases and sells them to competitors; steals payment
Cloud-based, Mobile Assets & Social Media	Compromise data stored outside the corporate network, and potentially outside corporate security monitoring	DROPBOX Social Media Mobile Attacks	Information data can be stolen quietly over time; potential lack of clarity on who is responsible for incident response
System Compromise and Control	Take over specific cyber assets and able to control them; used to exfiltrate data or disrupt operations	2010, Night Dragon report of Chinese APT targeting financial docs related to oil/gas and bids	Theft activities of data over long periods of time; theft of operating processes and other intellectual property
Supply Chain Corruption	Compromised hardware/software that allows for attacker access – could be foothold	2008-present, counterfeit router gear from China presents access risk to infrastructures	Footholds introduced into the environment without traditional infiltration forensic log data
Social Engineering/Spear Phishing	Through human action gain access/foothold & may lead to targeted exploit; top APT vector	2013, Syrian Electronic Army socially engineers The Onion to take over its Twitter accounts	Attacker gets help desk/HR to open malware; Tangential risk of subsidiaries and other third-party vendor networks
Disruptive Malware	Malware leveraging access to disrupt/destroy data integrity and/or access to systems	Aramco and 30,000 computers wiped; threats of recce on US energy industry	Custom virus written and implanted to erase systems/corrupt customer databases
DDoS	Disrupt Internet/public facing services	2013, MasterCard, PayPal and others targeted in a major DDoS attack requiring active responses	Attack against egress points, denying users/field personnel access to corporate information
Drive-by Malware/rogue USB device	User inadvertently installs; attacker gains foothold; e.g.. criminals harvesting PII for fraud or resale	Fake AV and other variants trick users into providing information or allowing hackers to access system	Employee finds USB device and inserts it, or visits drive- by web site, causing system infection

Assess Potential Consequences to Your Corporation

Consequence	*Description*	*Impact*
Reputational Damage	Negative perception by customers, media, public due to publicized issues	Organization could experience negative publicity, lose customers, revenue, confidence and potentially be targeted by other cyber adversaries
Reduction of competitive edge with direct competitors	Theft of intellectual property (e.g. corporate processes, customer databases, privileged communications)	Customers could be contacted by competitors and entice with slightly better deals, tradecraft could be analyzed allowing competitors to improve upon it
Loss of data or systems	Destruction of data, systems, or access to systems through willing or accidental means; physical loss of mobile devices	Adversaries could alter or destroy data in databases, making it very difficult or impossible for operations to work and requiring incident response/data recovery functions to be enacted
Data breach disclosure	Compromise of internal integrity and public disclosure of privileged communications or customer data	Posting of sensitive information (e.g. communications, PII, payment information) publicly can not only damage an organization, but create a problem for customers and partners
Loss of customers	Customer's loss of confidence in services offered	Customers might simply leave the company for another, regardless of cost, in order to distance themselves from fallout from a catastrophic cyber incident

Mapping Threat/Vector/Consequence to Risk



Threat Adversary

Disgruntled Employees / Contractors

State sponsored entity

Hacktivist / advocacy groups

Organized crime

Corporate competitors

Opportunists

Threat Vector

Insider - Access, Control, Knowledge

System Compromise and Control

Supply Chain Corruption

Social Engineering/Spear Phishing

Disruptive Malware

DDoS

Drive-by Malware/rogue USB device

Consequence

Customer data or systems corrupted via CLIENT

Loss of sensitive data – customer or corporate

Destruction/disruption of internal data, systems, or access to systems

External/Internet connectivity disrupted to enterprise systems

Risk Scenario

Compromise of customer systems via SYSTEM

Insider uses access to launch massive malware based disruption

Man-in-the middle SYSTEM attack pushes customer corrupted data

High net-worth individuals in CLIENT program targeted by money-stealing trojans

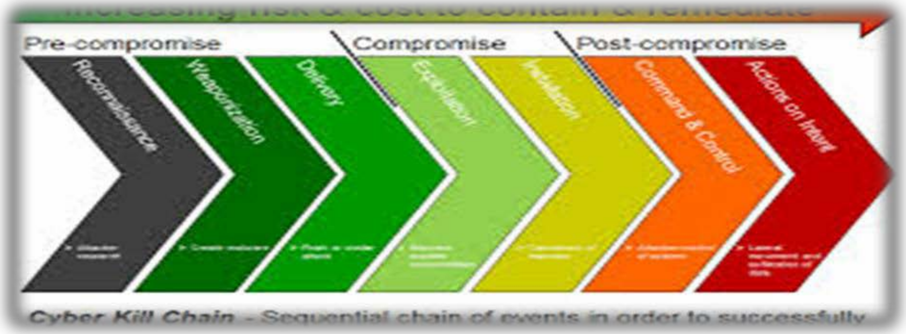
Compromise of sensitive CLIENT data by hacktivist organization

DDoS

Helps Build Illustrative Threat Scenarios (see CObIT Implementaion)

Establishing Operational Level Analysis

- Drive proactive changes to IT Infrastructure and net defense posture through understanding adversary, TTP and rhythms



- Drive training, exercise and range environments based on realistic adversary replication – people are the greatest asset

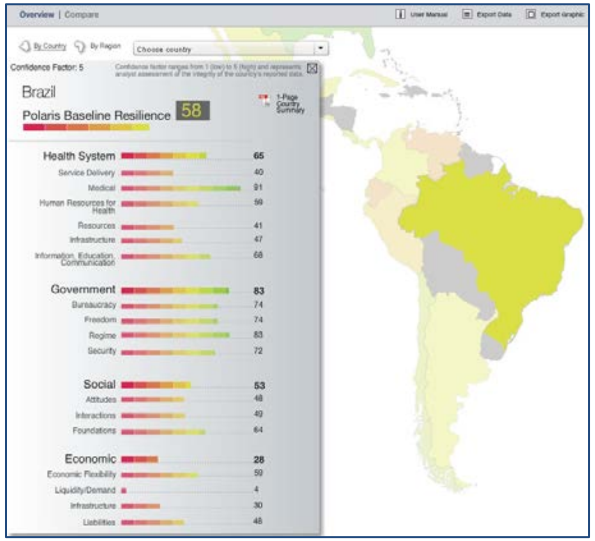
Establishing Strategic Level Analysis

- Adversary Evolution
  - Improved Capability of Cyber Guerilla Forces
  - Emergence of Cyber Weapons focus on RF access & disruption
- Geo-Cyber Risk Analysis
  - Exposures to facilities, people, data flows
- Business Evolution, Mergers & Acquisitions
  - Cyber security posture of new business operations
- Supply Chain and Vendors
  - Increasing the threat vector of sophisticated attackers
  - Integrate into vendor management process
- Technology Evolution

Geocyber Risk Assessment

The Meaning of Geocyber Risk

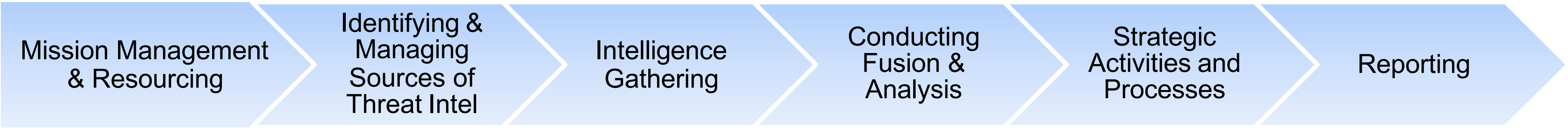
- Despite the Internet's global presence, cyber threats occur within localized environments
- Companies with global operations face diverse cyber threats depending on where the company operates
- By tailoring operational security to in- country risk, companies can efficiently allocate resources and prioritize protection of its most vulnerable operational centers



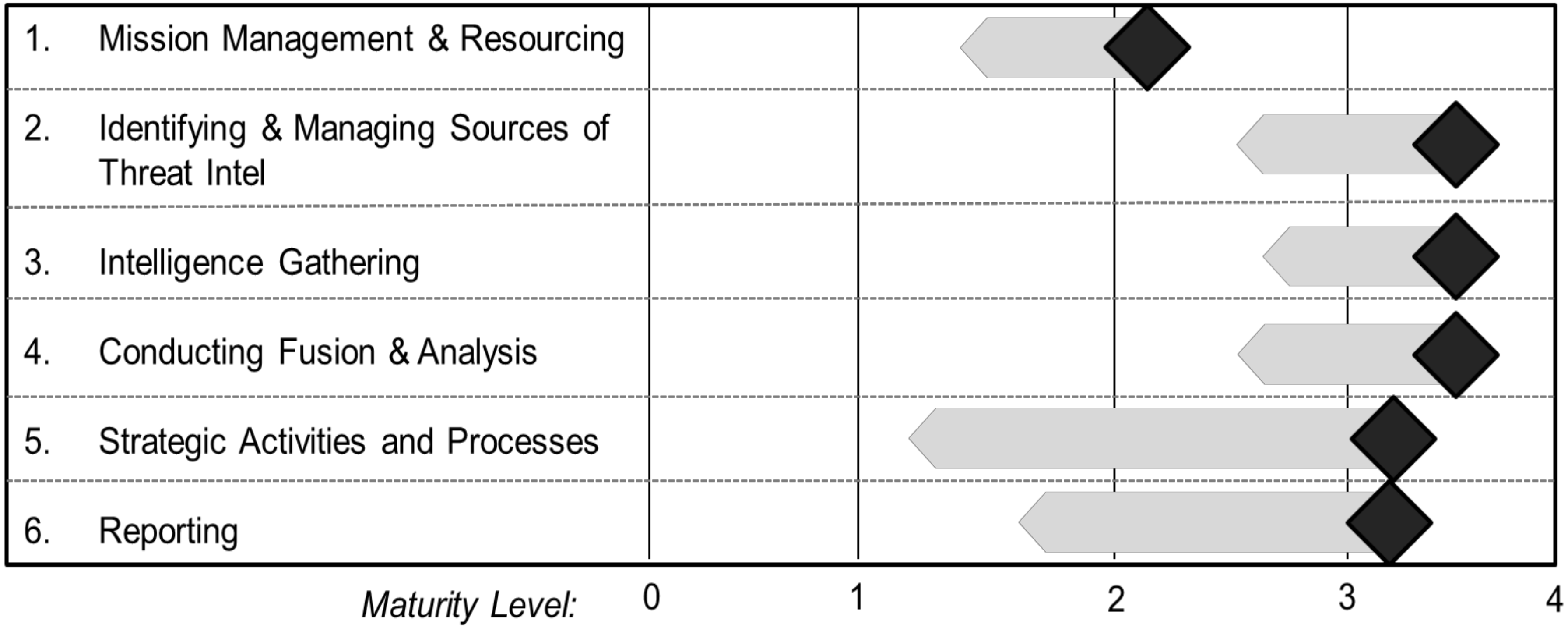
Examples of Geocyber Risk

- **Human Enabled Cyber Activities**
  - Device access (Cell phones, Laptops, USBs, etc.) – theft or spyware infection
  - Physical access to networks, infrastructure, other opportunities
  - Origins of spear phishing attacks – email spoofing targeted at specific individuals or organizations
- **Activity of Specific Actors enabled by Proximity**
  - Patriot hackers such as the Honker's Union of China and mercenaries like Hidden Lynx
  - Government-run groups such as Unit 61398 aka APT
- **Poor Cyber Hygiene in Operating Environment**
  - High amount of pirated software and Operating Systems; pirates wary of system updates due to chance of being locked out of own pirated software
  - Poor operating/security practices of local businesses
  - High malware infection rate
- **Governmental Climate**
  - Permissive industrial and intelligence service espionage or cyber dissents
  - Policies that exacerbate poor hygiene, environmental & supply chain conditions

Benchmark Program & Establish Improvement Goals


Mission Management & Resourcing
Identifying & Managing Sources of Threat Intel
Intelligence Gathering
Conducting Fusion & Analysis
Strategic Activities and Processes
Reporting

Our Rating of the Recommended Goals



Example Metrics for Cyber Threat Intel Practice

More Qualitative

- **Strategic:** CRO determinations of corporate risk are impacted based upon threat intelligence outputs
  - *Indicative of a well informed CRO, fed by information gleaned at all stages of threat intelligence.*

- **Operational:** Time to respond to a known high severity intrusion
  - *Indicative of change in capability (people/process/technology) in intrusion response.*
  - *Time should be from detection to containment of intrusion.*

- **Tactical:** Number of threats detected in a given month
  - *Indicative of the quality of detection capability within an organization.*
  - *Similar metrics exist for prevention, and response.*

More Quantitative

OSINT & Other sources

What is OSINT?

OSINT: *Open Source Intelligence; publicly available information. i.e., information that any member of the public could lawfully obtain by request or observation, as well as other unclassified information that has limited public distribution or access.*

- OSINT represents a constant threat to any organization or mission and can account for up to 80% of actionable intelligence, which is generally not protected and not classified
- In most cases, it's legal to obtain information in this way. This means that despite the high potential for harm, this critical information may be obtained at little or no risk

Definitions:

- Open Source Data (**OSD**): the raw print, broadcast or information in any other form from a primary source. This can include photographs, tape recordings, satellite imagery, personal letters, online postings, etc.
- Open Source Information (**OSIF**): Generic information generally intended for wide dissemination that combines multiple pieces of data using some level of validation. Examples include books, newspapers and news reports
- Validated Open Source Intelligence (**OSINT-V**): Information to which a high degree of certainty can be attributed. This includes two categories:
  - Information which comes from an established reliable source and/or can be validated by comparing to other data
  - Information which can be established as valid in its native format. i.e., news reports showing a state leader's speech. This, of course, must consider the possibility of manipulation or forgery

OSINT Sources

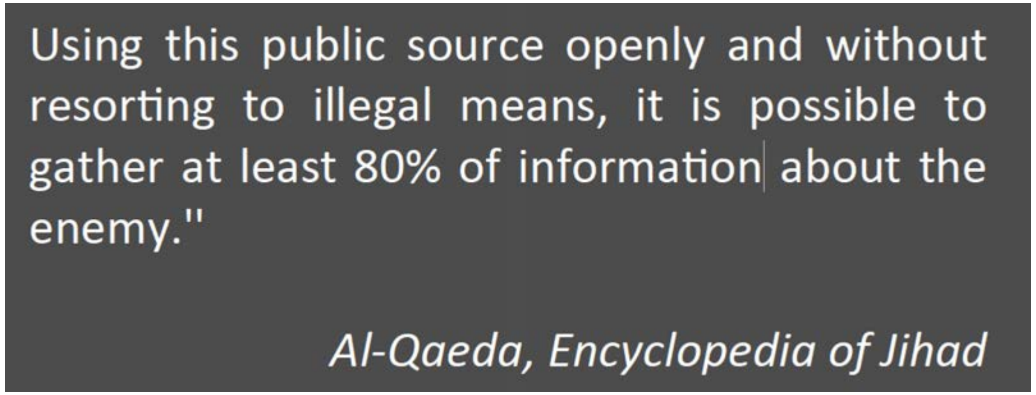
Intelligence can be gathered from a broad range of publicly available sources

- Media
  - Television, radio, newspaper, magazines
- Internet
  - Search engines
    - Google, Bing, Yahoo
  - User-generated content
    - Blogs, forums, social-networking, wikis
  - RSS feeds
  - Peer to Peer (P2P)
- Geographic
  - Maps and environmental and navigational data
- Observation
  - Camera, video recorder, reporting
- Academia
  - Experts, research, conferences

OSINT

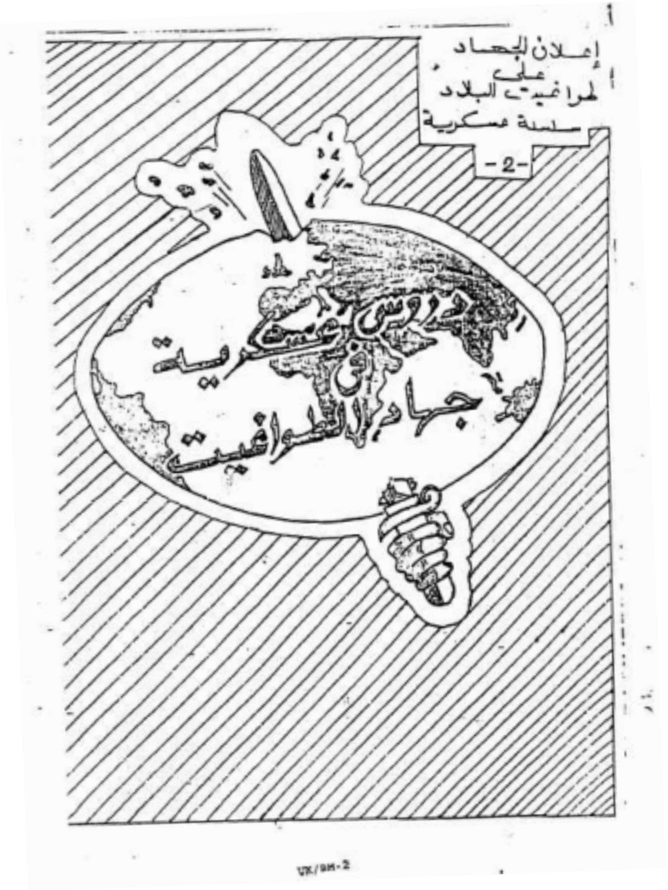
"… using **public sources** in an open manner, **without making use of illegal means** it's possible to get at least the **80% of needed information about our enemy.** It's possible to gain such information through newspapers, magazines, books, periodicals, official publications and various genre radio/tv transmissions…"

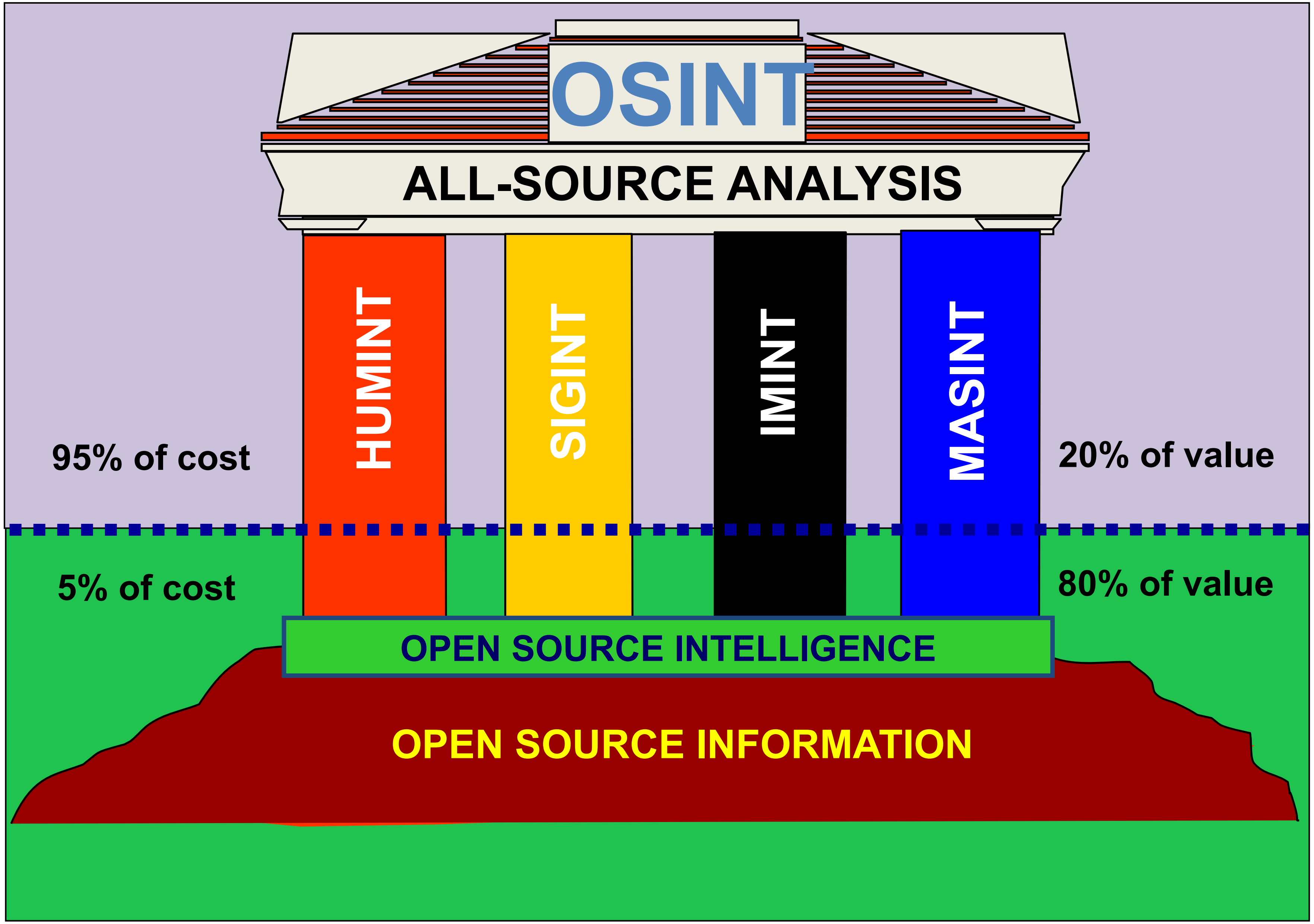
From the Al-Qaeda manual



Using this public source openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy."

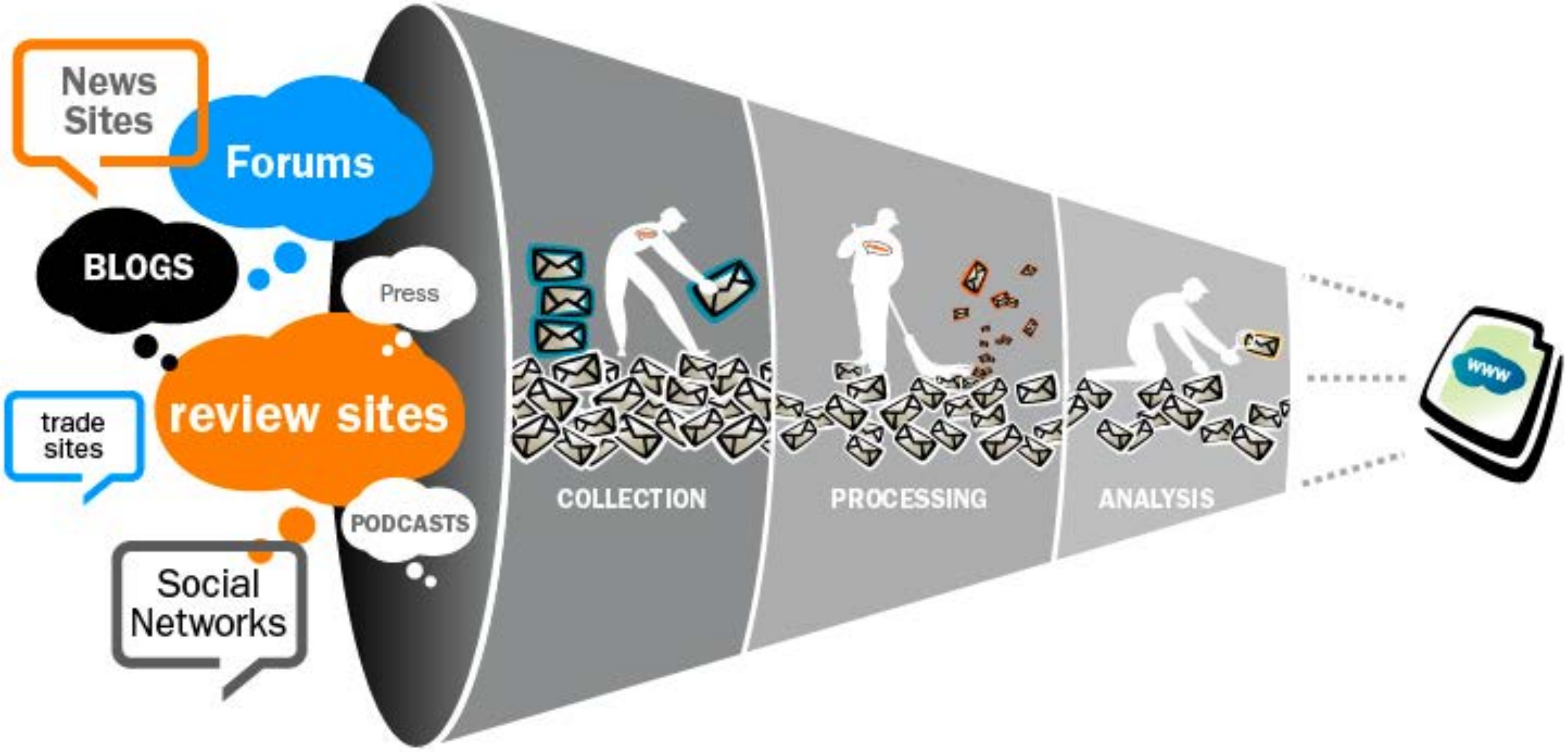
Al-Qaeda, Encyclopedia of Jihad





HUMINT = HUMan INTelligence
SIGINT = SIGnals INTelligence
MASINT = Measurement and Signature Intelligence
IMINT = IMagery INTelligence

OSINT – The sources



What is the value of OSINT?

OSINT has incredible value, and it’s the fundamental of Threat Intelligence:

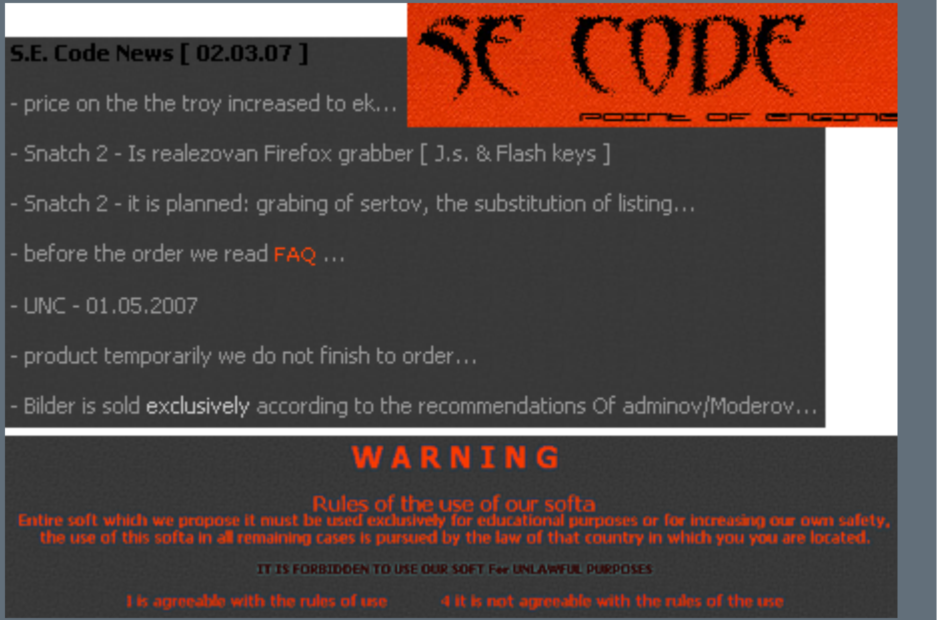
- OSINT gives context to classified information. Generally, only select information meets the criteria for classification, with unclassified sources of information filling the gaps.
- OSINT gives a starting point and additional resources necessary to leverage further defense capability or counter-attack
- OSINT reveals the intent of friendly or adversarial forces
- OSINT reveals current status, capabilities or other contemporary information

Proliferation of cyber-weapons

C2C: Malware/Phishing Kit – “Arms Suppliers”

Criminal to Criminal – C2C

- Selling malware for "research only“
- Manuals, translation
- Support / User forums
- Language-specific
- Bargains on mutation engines and packers
- Referrals to hosting companies
- Generally not illegal
- Operate in countries that shield them from civil actions
- Makes it easy to enter the cybercrime market



S.E. Code News [02.03.07]

- price on the the troy increased to ek...
- Snatch 2 - Is realezovan Firefox grabber [J.s. & Flash keys]
- Snatch 2 - it is planned: grabing of sertov, the substitution of listing...
- before the order we read FAQ ...
- UNC - 01.05.2007
- product temporarily we do not finish to order...
- Bilder is sold exclusively according to the recommendations Of adminov/Moderov...

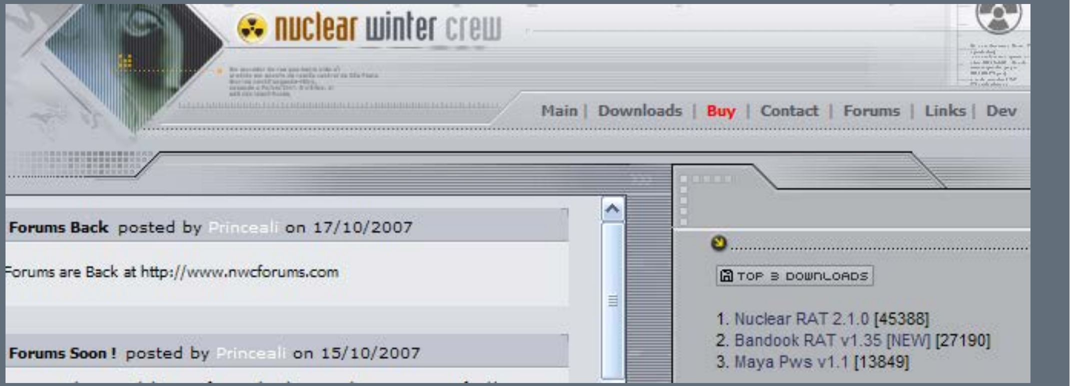
WARNING

Rules of the use of our softa

Entire soft which we propose it must be used exclusively for educational purposes or for increasing our own safety, the use of this softa in all remaining cases is pursued by the law of that country in which you you are located.

IT IS FORBIDDEN TO USE OUR SOFT For UNLAWFUL PURPOSES

I is agreeable with the rules of use   4 it is not agreeable with the rules of the use

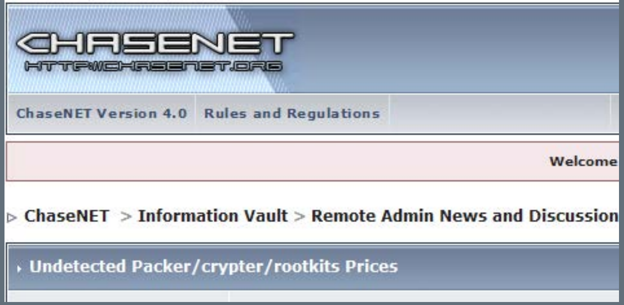


Forums Back posted by Princeali on 17/10/2007

Forums are Back at http://www.nwcforums.com

Forums Soon ! posted by Princeali on 15/10/2007

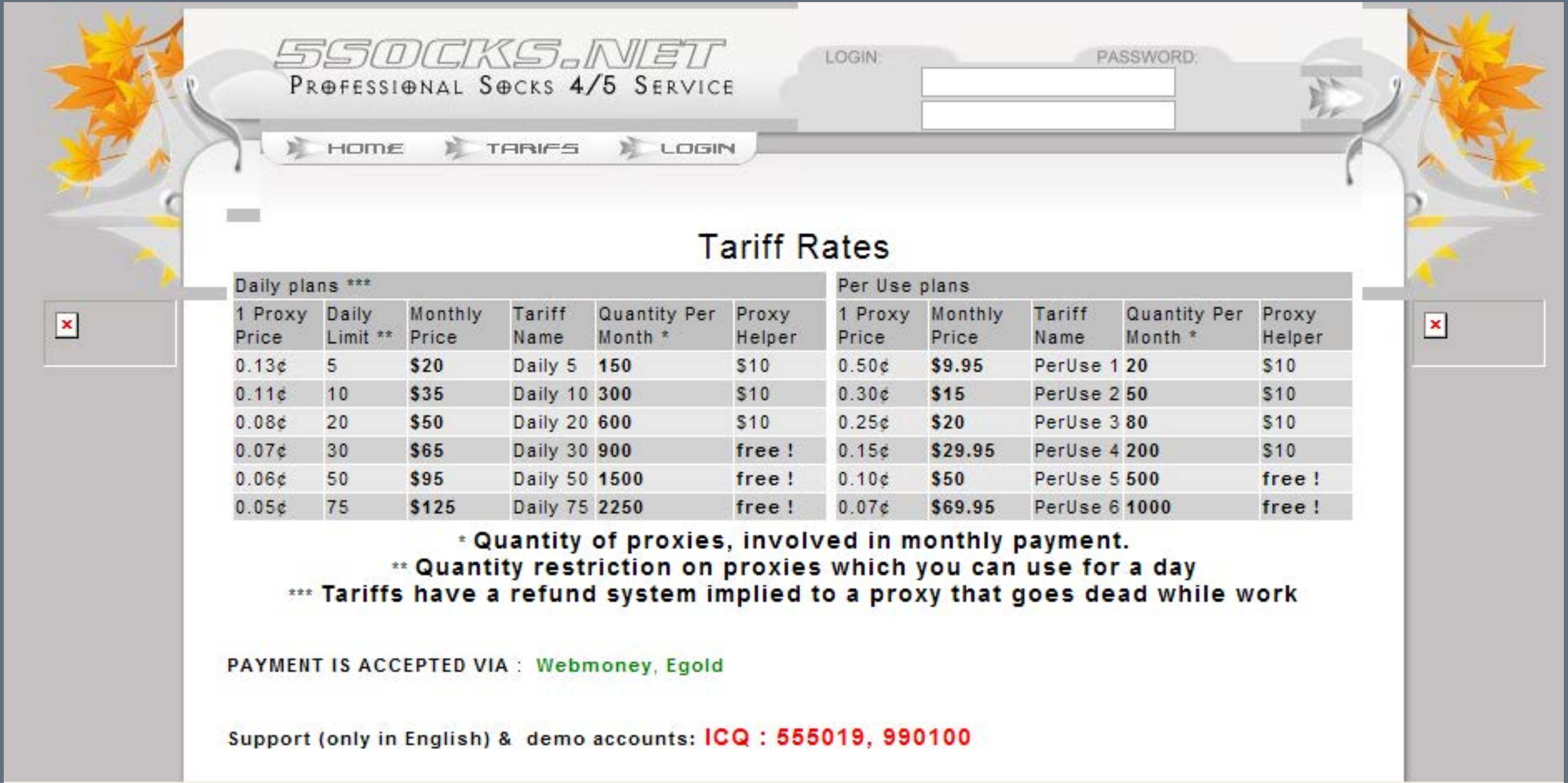
1. Nuclear RAT 2.1.0 [45388]
2. Bandook RAT v1.35 [NEW] [27190]
3. Maya Pws v1.1 [13849]



ChaseNET > Information Vault > Remote Admin News and Discussion

Undetected Packer/crypter/rootkits Prices

C2C – Distribution & Delivery – “Force Suppliers”



Tariff Rates

Daily plans ***					
1 Proxy Price	Daily Limit **	Monthly Price	Tariff Name	Quantity Per Month *	Proxy Helper
0.13¢	5	**$20**	Daily 5	**150**	$10
0.11¢	10	**$35**	Daily 10	**300**	$10
0.08¢	20	**$50**	Daily 20	**600**	$10
0.07¢	30	**$65**	Daily 30	**900**	**free !**
0.06¢	50	**$95**	Daily 50	**1500**	**free !**
0.05¢	75	**$125**	Daily 75	**2250**	**free !**

Per Use plans				
1 Proxy Price	Monthly Price	Tariff Name	Quantity Per Month *	Proxy Helper
0.50¢	**$9.95**	PerUse 1	**20**	$10
0.30¢	**$15**	PerUse 2	**50**	$10
0.25¢	**$20**	PerUse 3	**80**	$10
0.15¢	**$29.95**	PerUse 4	**200**	$10
0.10¢	**$50**	PerUse 5	**500**	**free !**
0.07¢	**$69.95**	PerUse 6	**1000**	**free !**

* **Quantity of proxies, involved in monthly payment.**

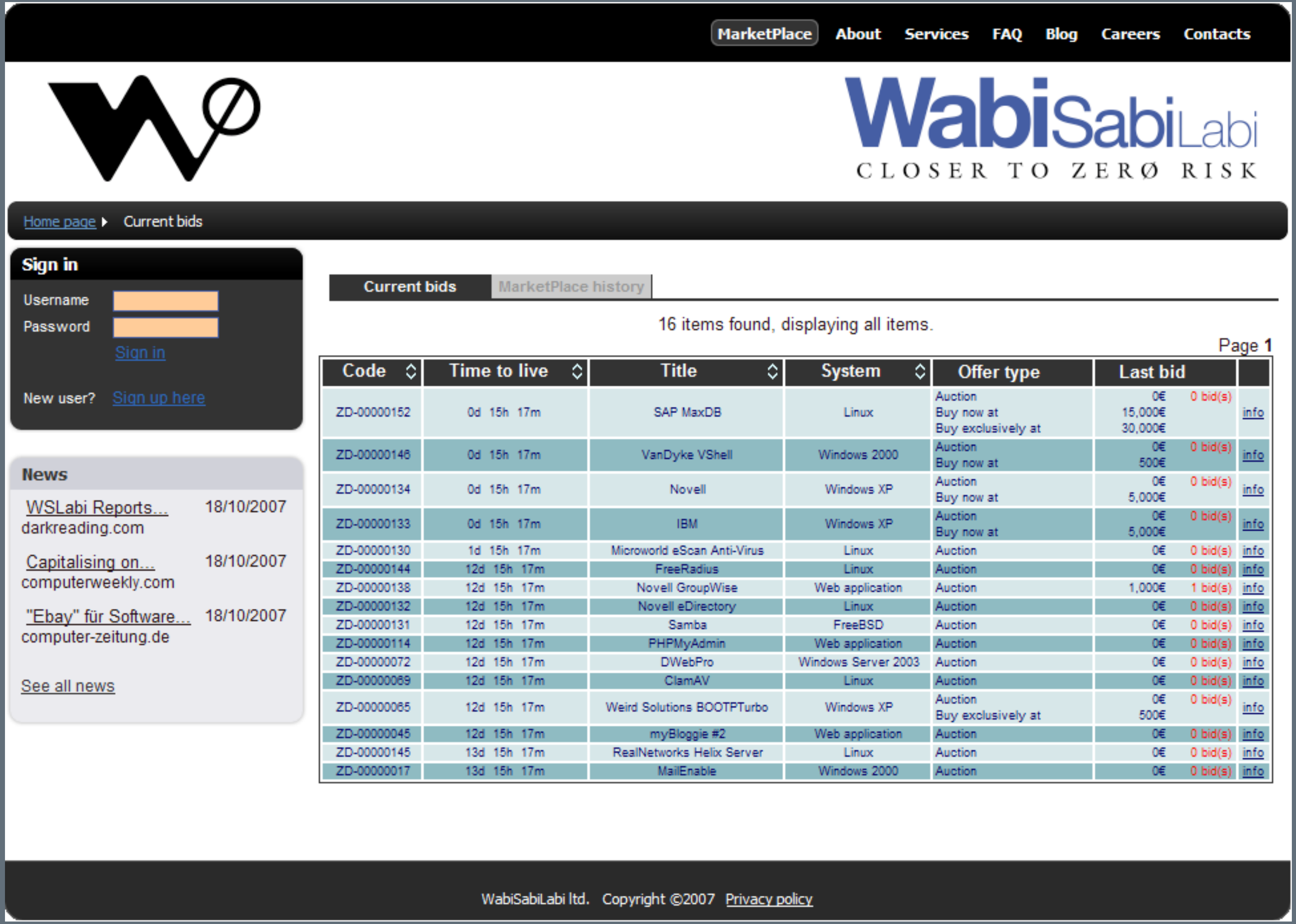
** **Quantity restriction on proxies which you can use for a day**

*** **Tariffs have a refund system implied to a proxy that goes dead while work**

PAYMENT IS ACCEPTED VIA : Webmoney, Egold

Support (only in English) & demo accounts: **ICQ : 555019, 990100**

C2C – Exploit – “Intelligence



News

WSLabi Reports... 18/10/2007
darkreading.com

Capitalising on... 18/10/2007
computerweekly.com

"Ebay" für Software... 18/10/2007
computer-zeitung.de

See all news

16 items found, displaying all items.

Page **1**

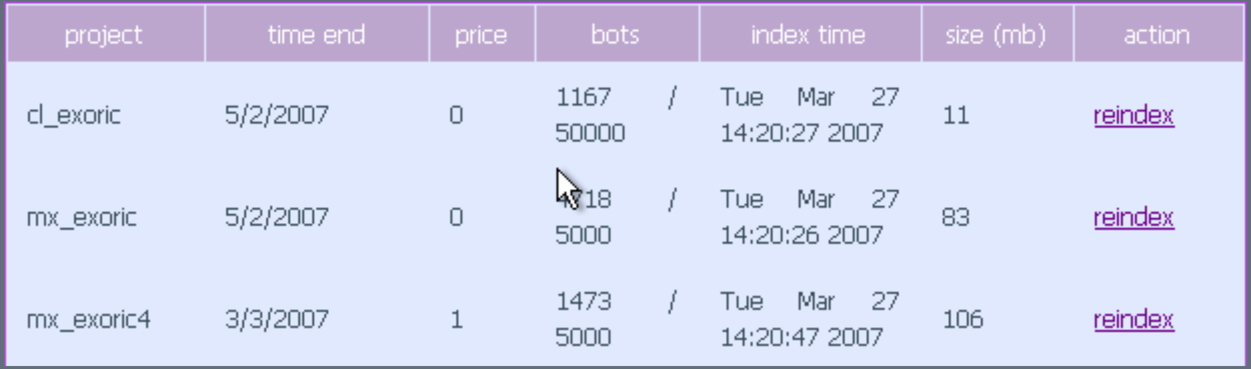
Code	Time to live	Title	System	Offer type	Last bid		
ZD-00000152	0d 15h 17m	SAP MaxDB	Linux	Auction Buy now at Buy exclusively at	0€ 15,000€ 30,000€	0 bid(s)	info
ZD-00000146	0d 15h 17m	VanDyke VShell	Windows 2000	Auction Buy now at	0€ 500€	0 bid(s)	info
ZD-00000134	0d 15h 17m	Novell	Windows XP	Auction Buy now at	0€ 5,000€	0 bid(s)	info
ZD-00000133	0d 15h 17m	IBM	Windows XP	Auction Buy now at	0€ 5,000€	0 bid(s)	info
ZD-00000130	1d 15h 17m	Microworld eScan Anti-Virus	Linux	Auction	0€	0 bid(s)	info
ZD-00000144	12d 15h 17m	FreeRadius	Linux	Auction	0€	0 bid(s)	info
ZD-00000138	12d 15h 17m	Novell GroupWise	Web application	Auction	1,000€	1 bid(s)	info
ZD-00000132	12d 15h 17m	Novell eDirectory	Linux	Auction	0€	0 bid(s)	info
ZD-00000131	12d 15h 17m	Samba	FreeBSD	Auction	0€	0 bid(s)	info
ZD-00000114	12d 15h 17m	PHPMyAdmin	Web application	Auction	0€	0 bid(s)	info
ZD-00000072	12d 15h 17m	DWebPro	Windows Server 2003	Auction	0€	0 bid(s)	info
ZD-00000069	12d 15h 17m	ClamAV	Linux	Auction	0€	0 bid(s)	info
ZD-00000065	12d 15h 17m	Weird Solutions BOOTPTurbo	Windows XP	Auction Buy exclusively at	0€ 500€	0 bid(s)	info
ZD-00000045	12d 15h 17m	myBloggie #2	Web application	Auction	0€	0 bid(s)	info
ZD-00000145	13d 15h 17m	RealNetworks Helix Server	Linux	Auction	0€	0 bid(s)	info
ZD-00000017	13d 15h 17m	MailEnable	Windows 2000	Auction	0€	0 bid(s)	info

WabiSabiLabi ltd. Copyright ©2007 Privacy policy

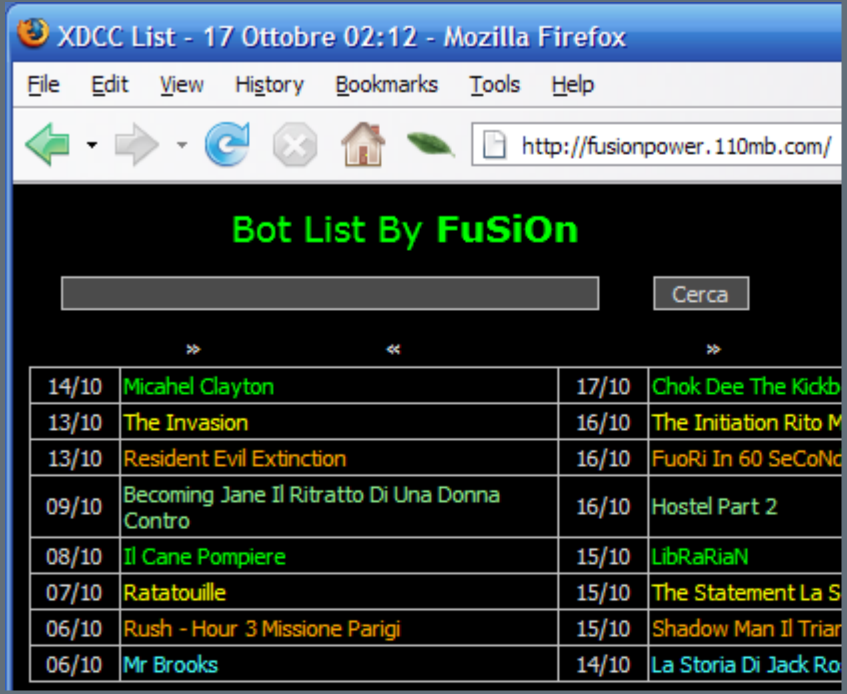
C2C: Bot Management– “Turn Key Weapons Systems”

76service, Nuklus Team

Botnet Dashboards

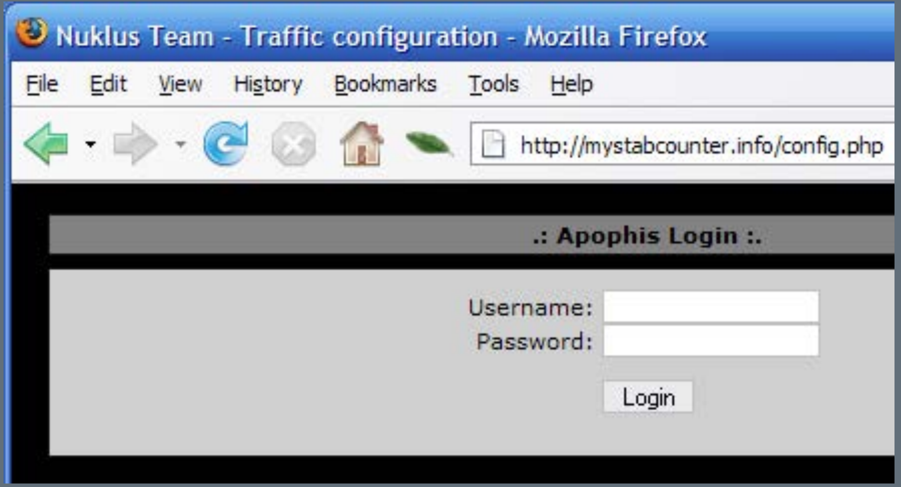


project	time end	price	bots	index time	size (mb)	action
cl_exoric	5/2/2007	0	1167 / 50000	Tue Mar 27 14:20:27 2007	11	reindex
mx_exoric	5/2/2007	0	4718 / 5000	Tue Mar 27 14:20:26 2007	83	reindex
mx_exoric4	3/3/2007	1	1473 / 5000	Tue Mar 27 14:20:47 2007	106	reindex


XDCC List - 17 Ottobre 02:12 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://fusionpower.110mb.com/
Cerca
» « »

Bot List By FuSiOn

14/10	Micahel Clayton	17/10	Chok Dee The Kickb
13/10	The Invasion	16/10	The Initiation Rito M
13/10	Resident Evil Extinction	16/10	FuoRi In 60 SeCoNc
09/10	Becoming Jane Il Ritratto Di Una Donna Contro	16/10	Hostel Part 2
08/10	Il Cane Pompiere	15/10	LibRaRiaN
07/10	Ratatouille	15/10	The Statement La S
06/10	Rush - Hour 3 Missione Parigi	15/10	Shadow Man Il Triar
06/10	Mr Brooks	14/10	La Storia Di Jack Ro


Nuklus Team - Traffic configuration - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://mystabcounter.info/config.php
Login

.: Apophis Login :.

Username:

Password:

Driving Factors Behind Cyber CrimeProfitable

Low risk

New services to exploit

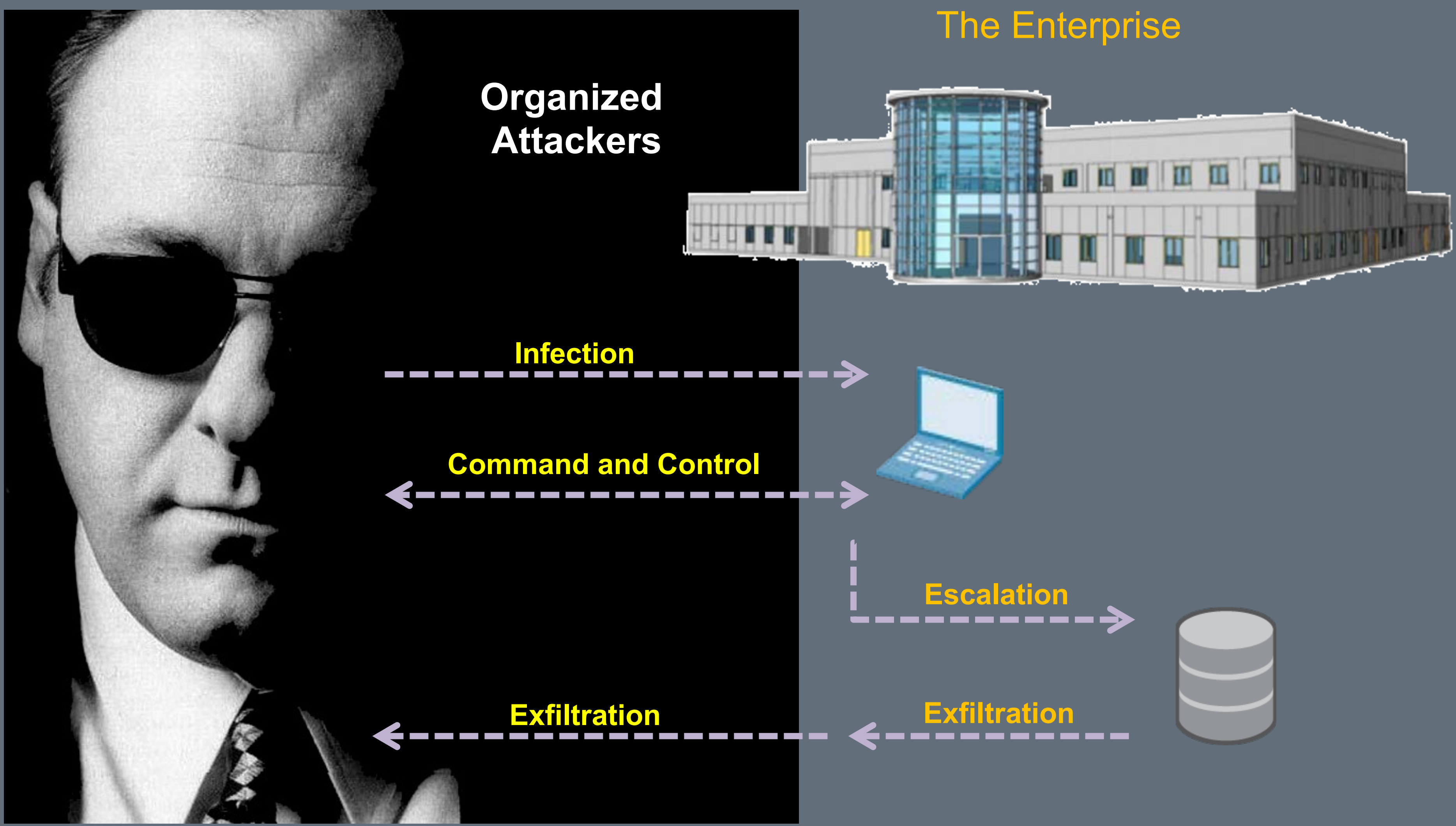
Easy (technically)

Easy (morally – you never meet the victim)

Picture provided by
“energizer” hacking group
90-day project take
$300,000 - $500,000

Conclusion

Security Perimeter Paradigm



The Enterprise

Organized Attackers

Infection

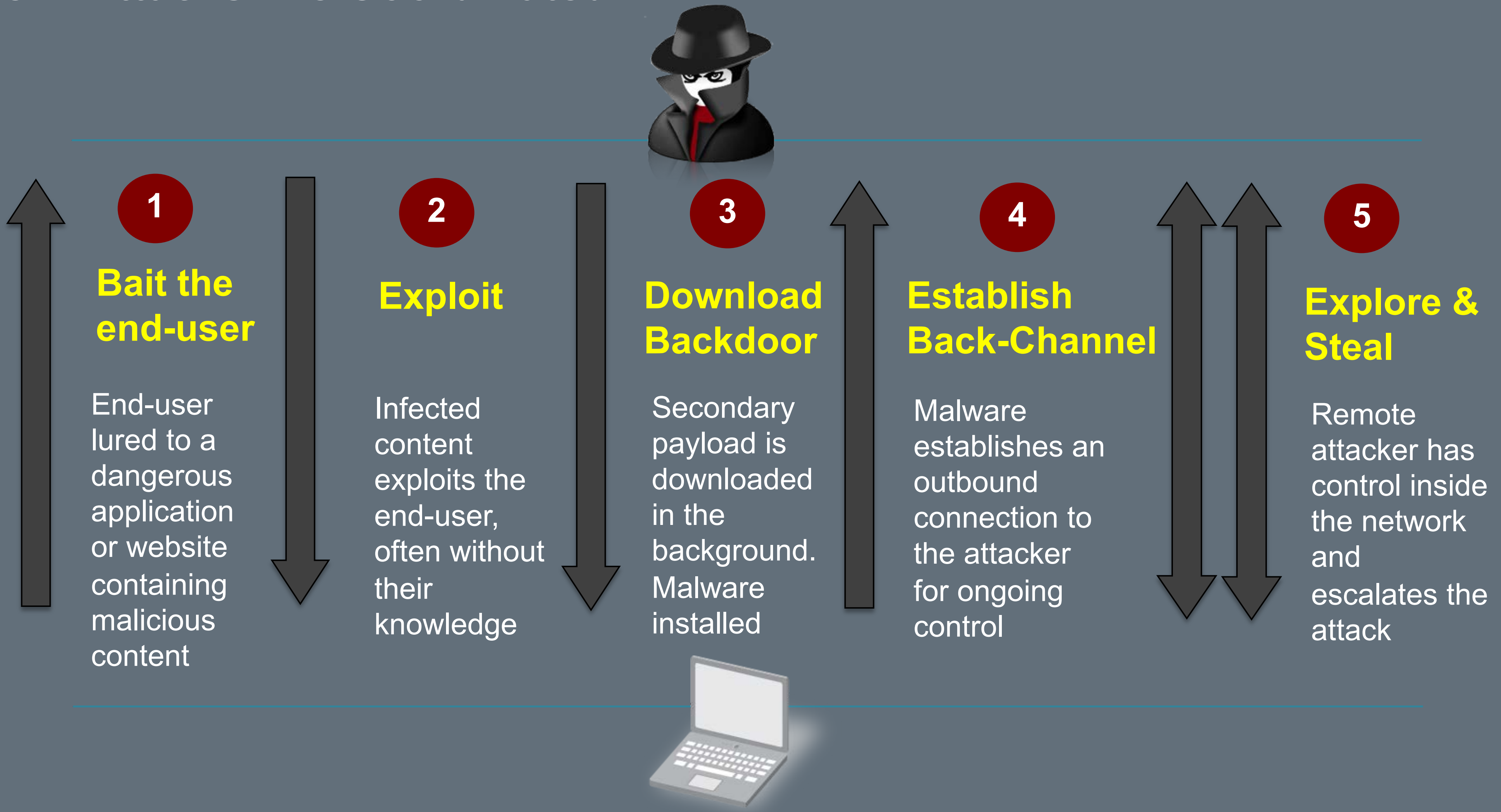
Command and Control

Escalation

Exfiltration

Exfiltration

Modern Attacks Are Coordinated



1 **Bait the end-user**

End-user lured to a dangerous application or website containing malicious content

2 **Exploit**

Infected content exploits the end-user, often without their knowledge

3 **Download Backdoor**

Secondary payload is downloaded in the background. Malware installed

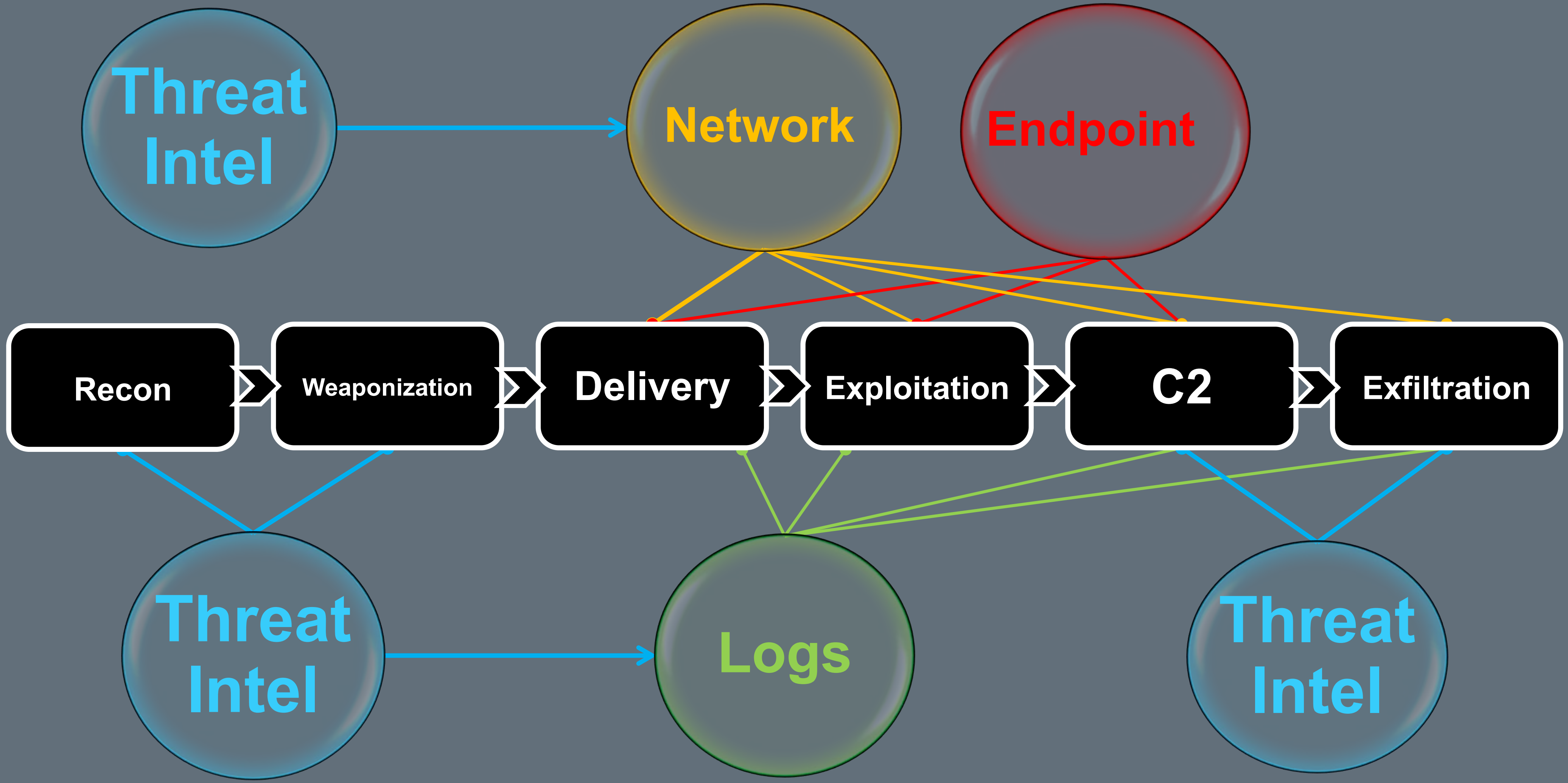
4 **Establish Back-Channel**

Malware establishes an outbound connection to the attacker for ongoing control

5 **Explore & Steal**

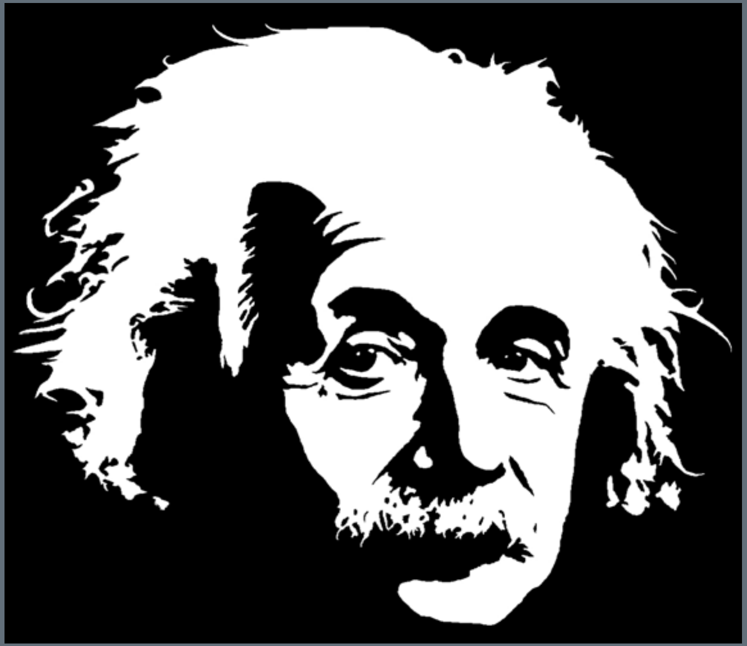
Remote attacker has control inside the network and escalates the attack

Kill Chain & Focal Points



Fighting cybercrime

Today’s approach to IT Security is **Falling Behind**



“Two things are infinite: The universe and human stupidity, and I’m not so sure about the former”

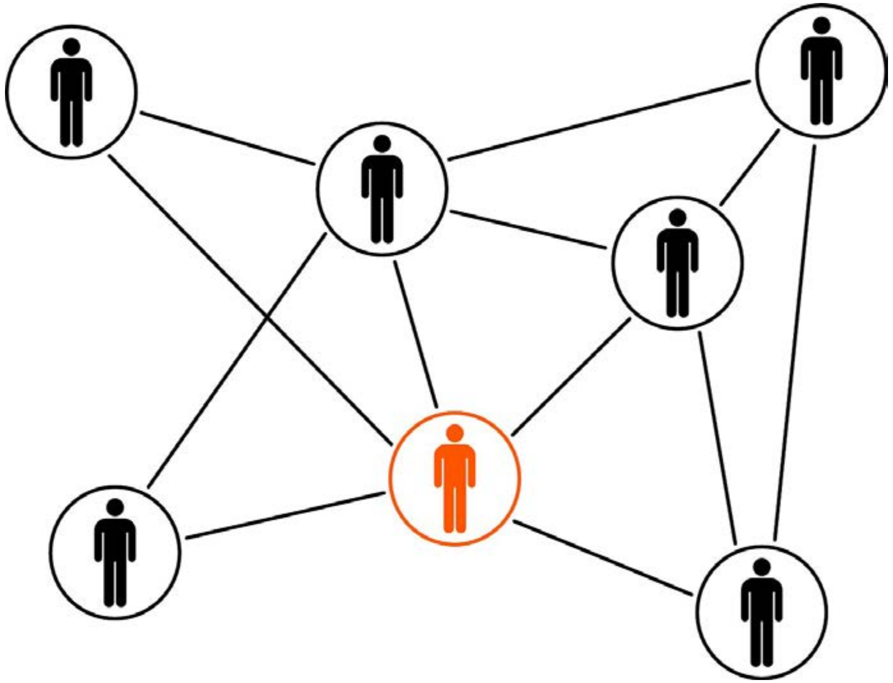
- Albert Einstein

Defending from a Cyber Attack: Web Intelligence

Today all criminal activity goes throughout the web, both secret message and intention

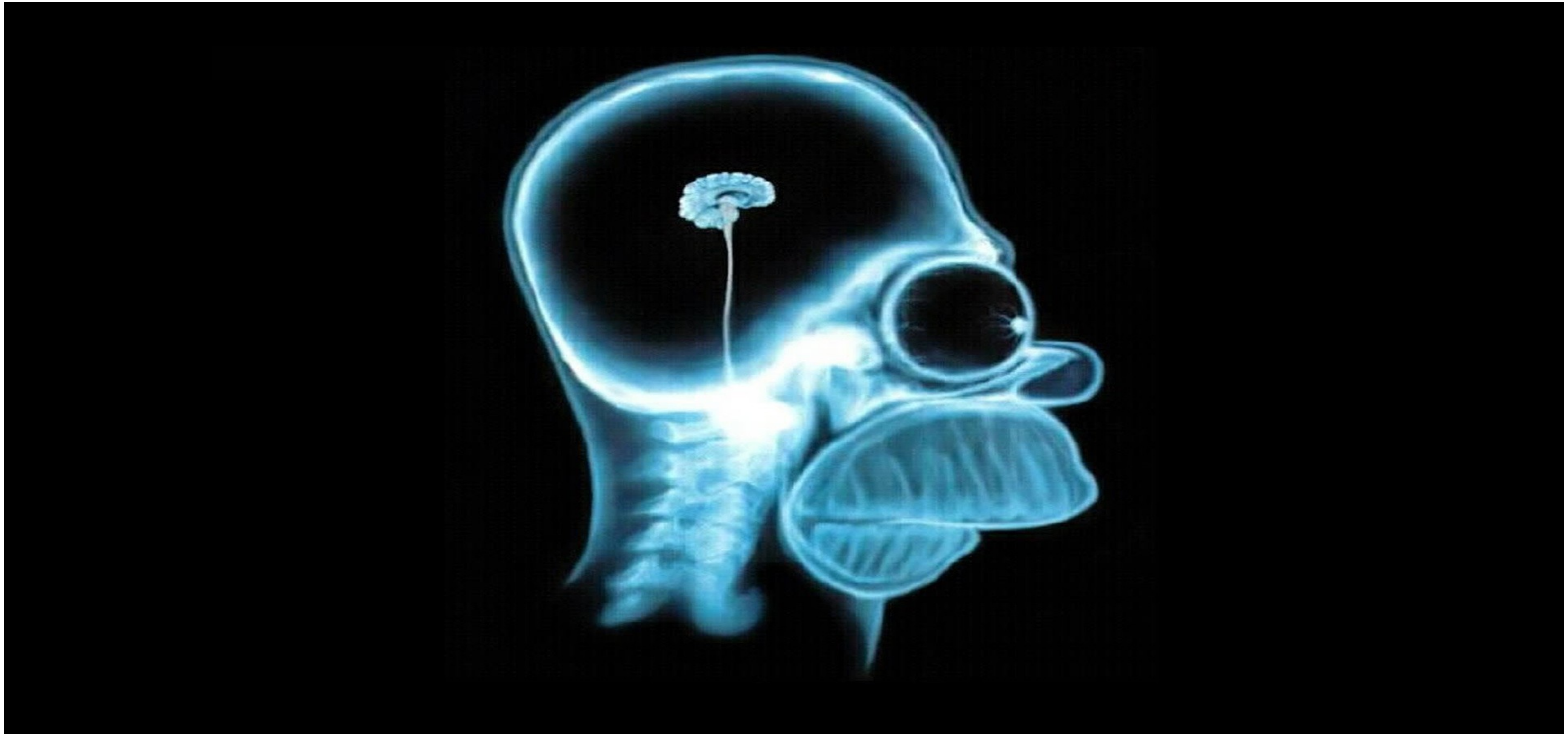
Web Intelligence is the **art of reading and collecting** all this signals allowing to understand and anticipate terrorist's plans and projects or criminal activity, to help the organizations to prevent and intercept the attacks

Web-Intelligence is a mix of instruments and techniques: **Cyber-HUMINT and SOCMINT, Text-Mining Distillation Approach, Multi language Support, Sentiment Analysis**



The main approach is to build secrets Avatar for penetrating in stealth way in the groups, close forum and in the dark-web, for monitoring the malicious activities

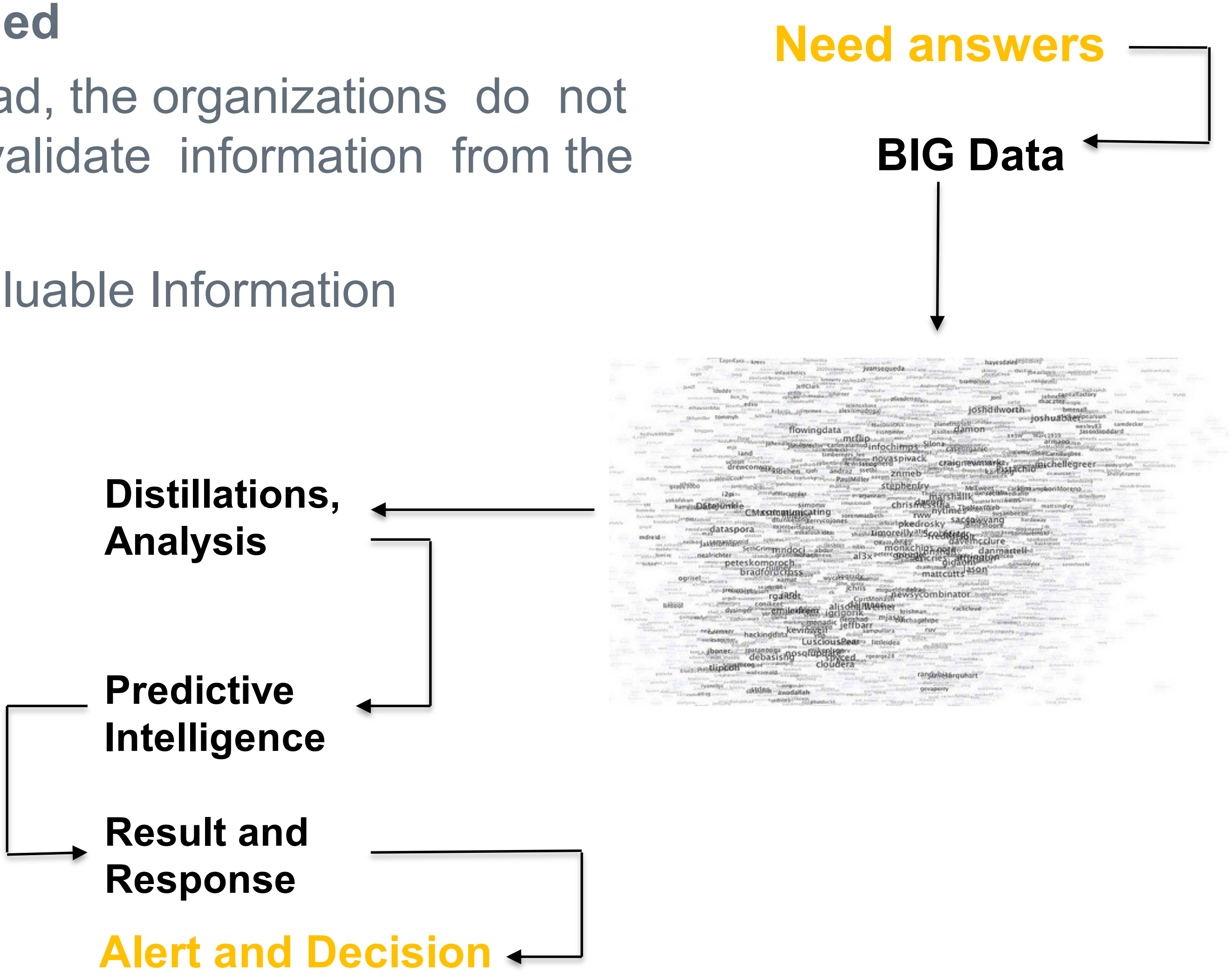
What is social engineering?



BIG Data = Difficult to evaluate and choose

The world becomes hyper-informed

- The problem: information overload, the organizations do not have the time to search and validate information from the large amount available
- The solution: Relevant and Valuable Information



Need answers

BIG Data

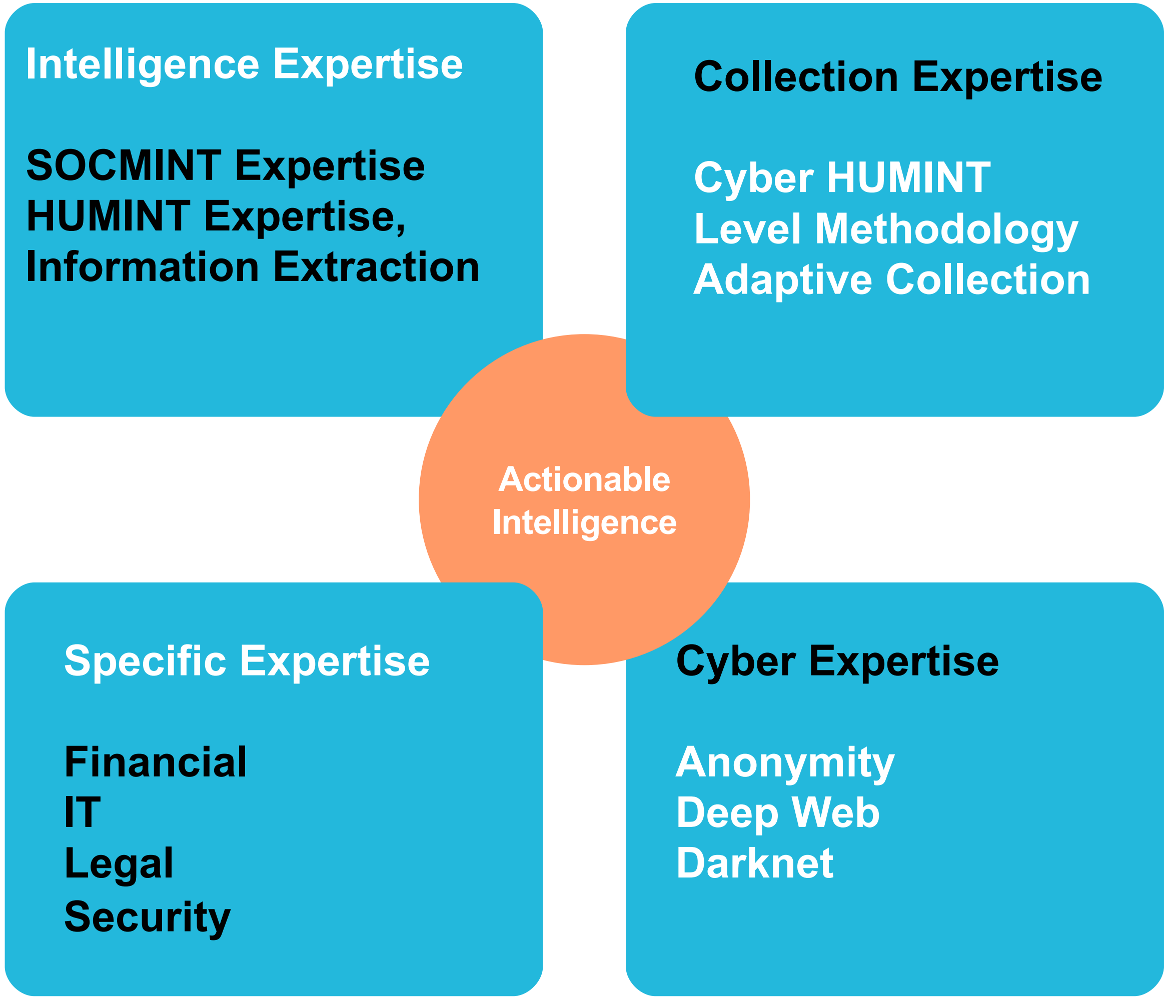
Distillations, Analysis

Predictive Intelligence

Result and Response

Alert and Decision

Many competencies required



Intelligence Expertise

SOCMINT Expertise
HUMINT Expertise,
Information Extraction

Collection Expertise

Cyber HUMINT
Level Methodology
Adaptive Collection

Actionable Intelligence

Specific Expertise

Financial
IT
Legal
Security

Cyber Expertise

Anonymity
Deep Web
Darknet

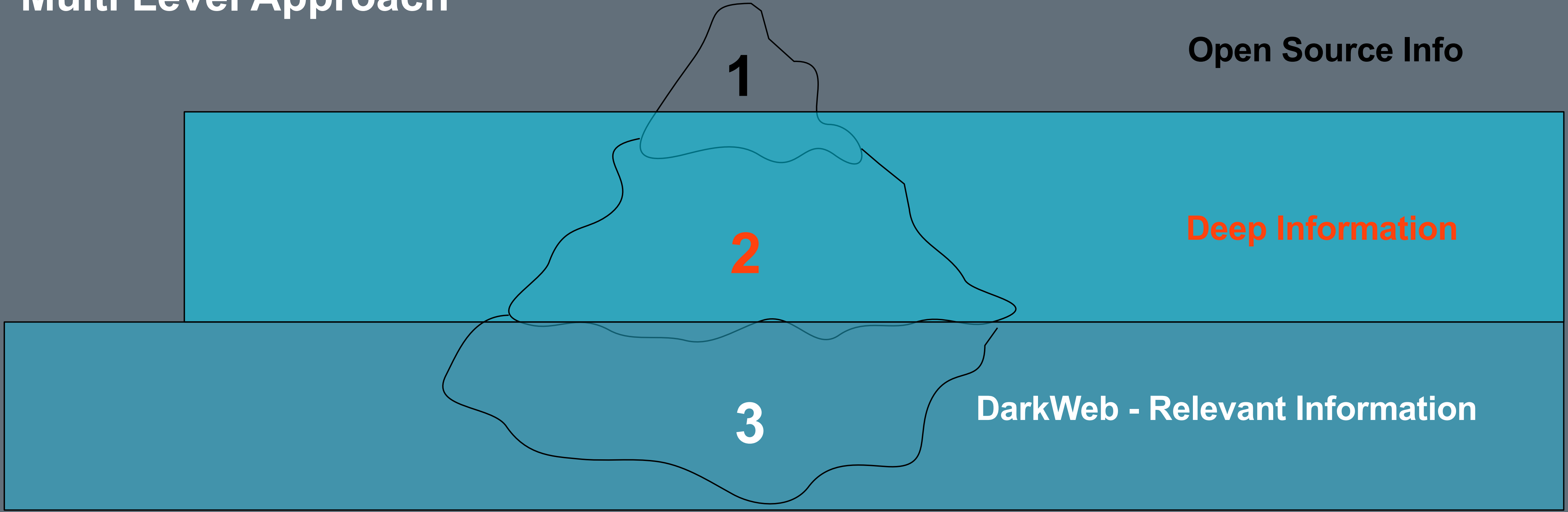
Linguistic & Cultural

Methodology

Technology

Legal Financial & Regulatory

Multi Level Approach



Level 1 – Open source intelligence, open social platforms, public and professional databases and more

Level 2 – Cyber Ops, Social engineering operation techniques along with cyber expertise to generate lawful access, and extraction of the required information from the right sources

Level 3 – Cyber HUMINT techniques and capabilities in the real 'physical' world. In this level various cover identities and stories tailored to the operation at hand, must be adopted in order to gain lawful access to the required information

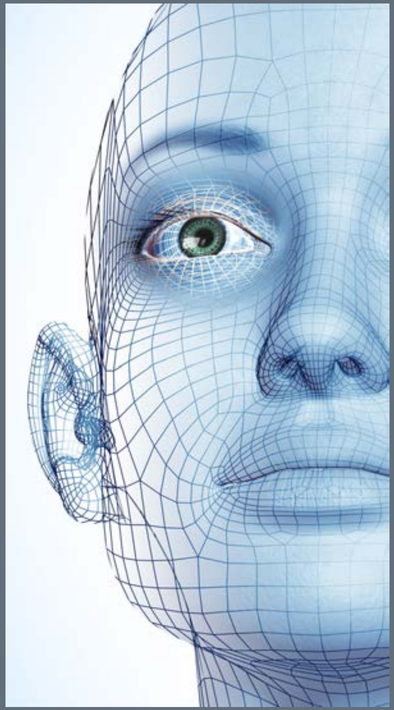
Cyber Intelligence

- **Who needs these**
- **Government Intelligence**
- **Intelligence units**

Law Enforcement

Cyber Crime unit

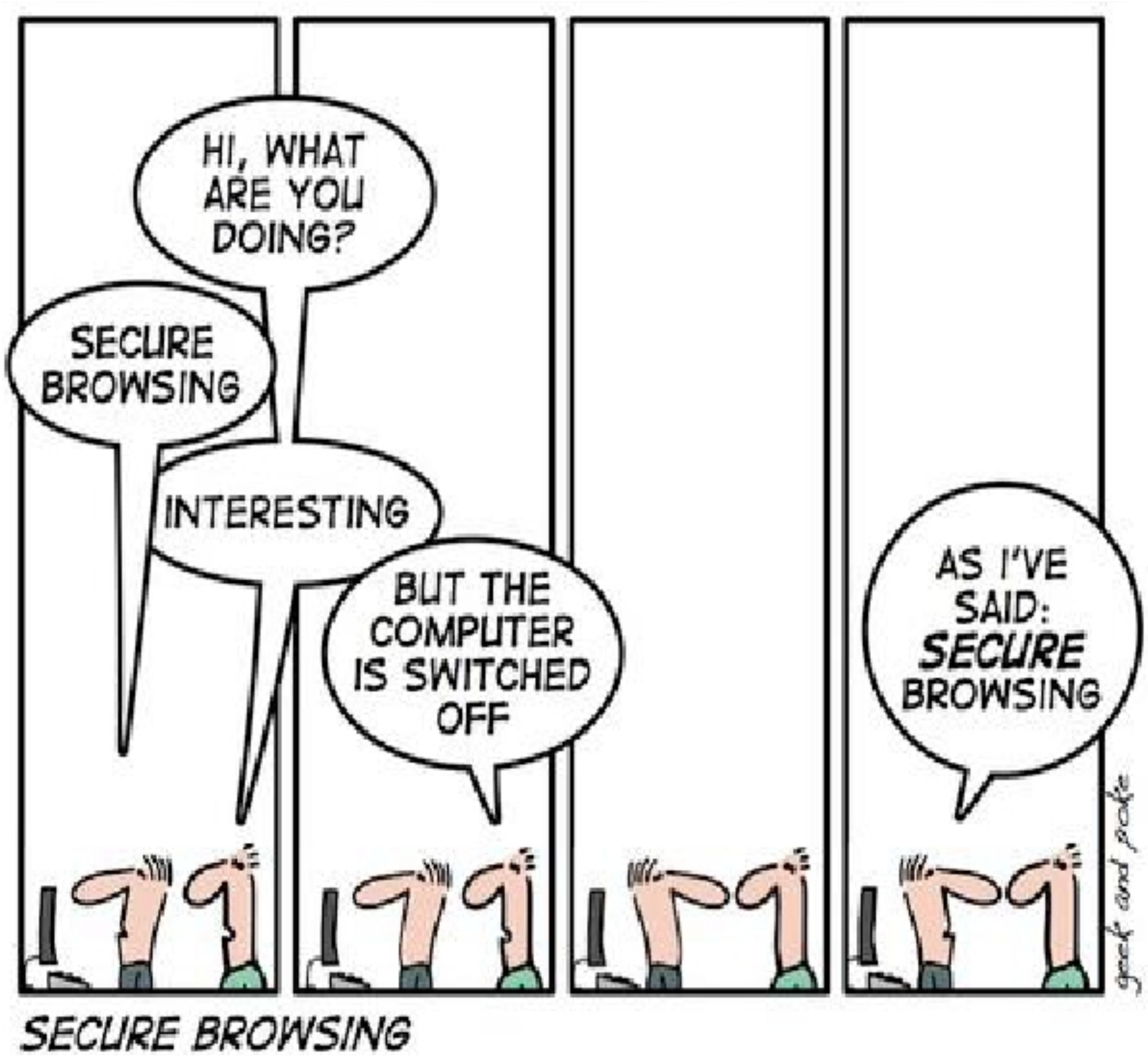
Financial Crime unit



Cyber Intelligence for who?

Company - Financial – Mass Media – Government – Critical Infrastructure

Threat	Response	Solution
Malware	Intelligence on Malware	Report
DDOS Attack by Criminal	Intelligence Operations	Report
Exposure Sensitive Information	Monitoring – Alerting	Report-Service
Lack of Awareness	Training	Training
Deface Site, Reputation Damage	Intelligence Operations	Report
Post-Attack	Response and Analysis	Service


HI, WHAT ARE YOU DOING?
SECURE BROWSING
INTERESTING
BUT THE COMPUTER IS SWITCHED OFF
AS I'VE SAID: *SECURE* BROWSING
geek and poke
SECURE BROWSING

Thanks for your attention!

Prof. Claudio Cilli,
CISA, CISM, CGEIT, CRISC

University of Rome, Italy

claudio.cilli@uniroma1.it

http://dsi.uniroma1.it/~cilli

https://www.linkedin.com/in/claudiocilli/

Questions?