



The importance of an integrated system for cyber security : Combining proactive and reactive approaches

2016

Chan W. Lee
President
Duzon

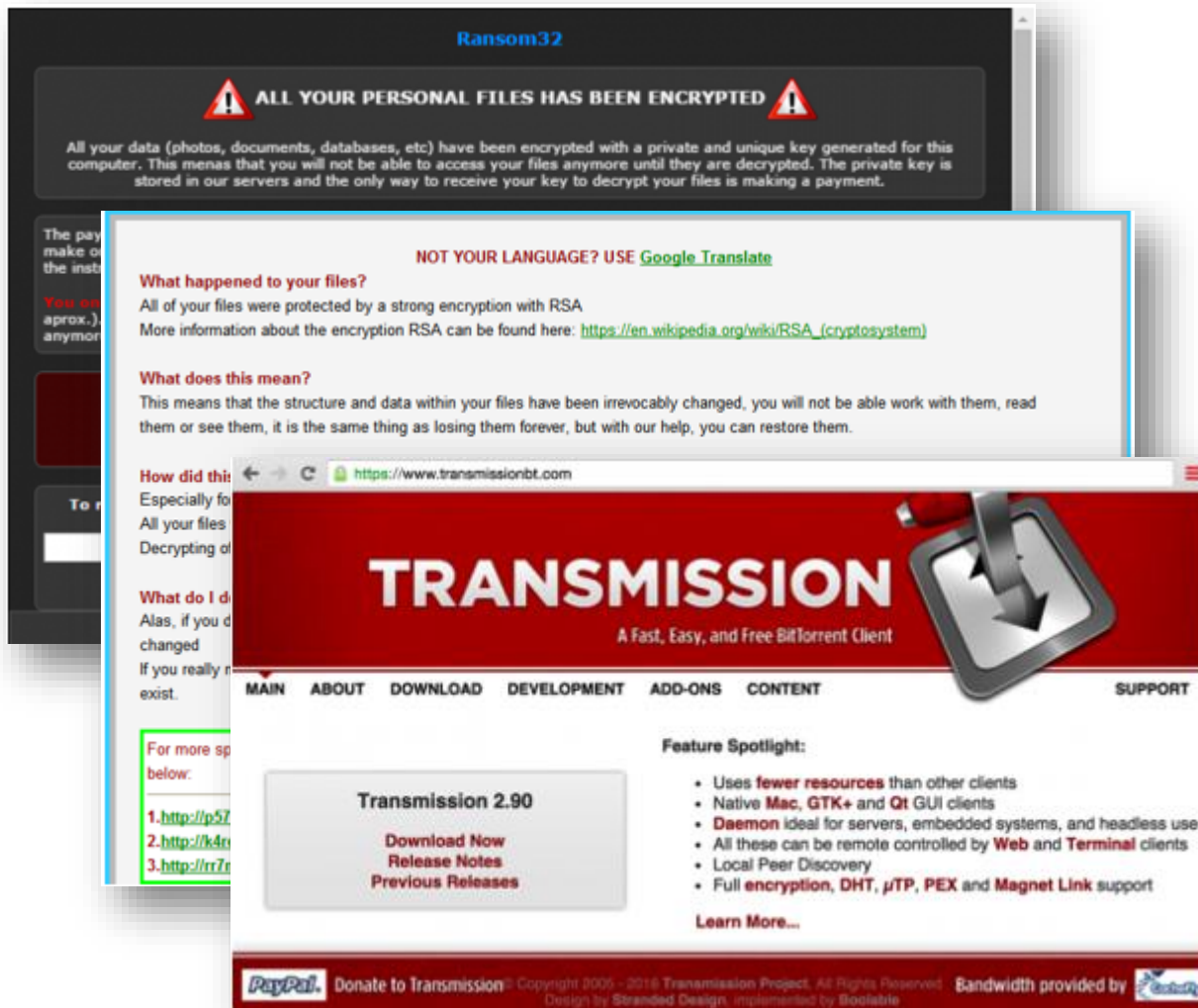
The Blue Heart
That Runs The Company



Everything changes, but nothing changes.



Ransomware



<Impact of Ransomware>

- Temporal or permanent loss of sensitive or proprietary information
- Disruption to regular operations
- Financial losses incurred to restore systems and files
- Potential damage to organization's reputation

Data Breach and IP Theft



<Impact of Ransomware>

- A SVP of LSI Division tried unauthorized carrying out the blueprints of the latest 10 nano tech.
- Chinese firm offered the executives
- A company monitored on him, and seize him on car with the documents at the main gate
- Police arrested and prosecuted him





Cyber Security Trend

Cyber Security



- The term “Cyber Security” is often used interchangeably with the term “Information Security.” The two terms will be used in a way that they have the same meaning though subtle differences they possess.

<Definition>

Cyber Security is the **protection of information systems** from theft or damage to the hardware, the software, and to the information on them, as well as from **disruption or misdirection of the services** they provide.

Information Security (IS) is the **practice of defending self-information or physical and logical assets** from inside and outside illegal actions (e.g. hacking, cracking) or natural disasters.

<Definition source : Wikipedia>

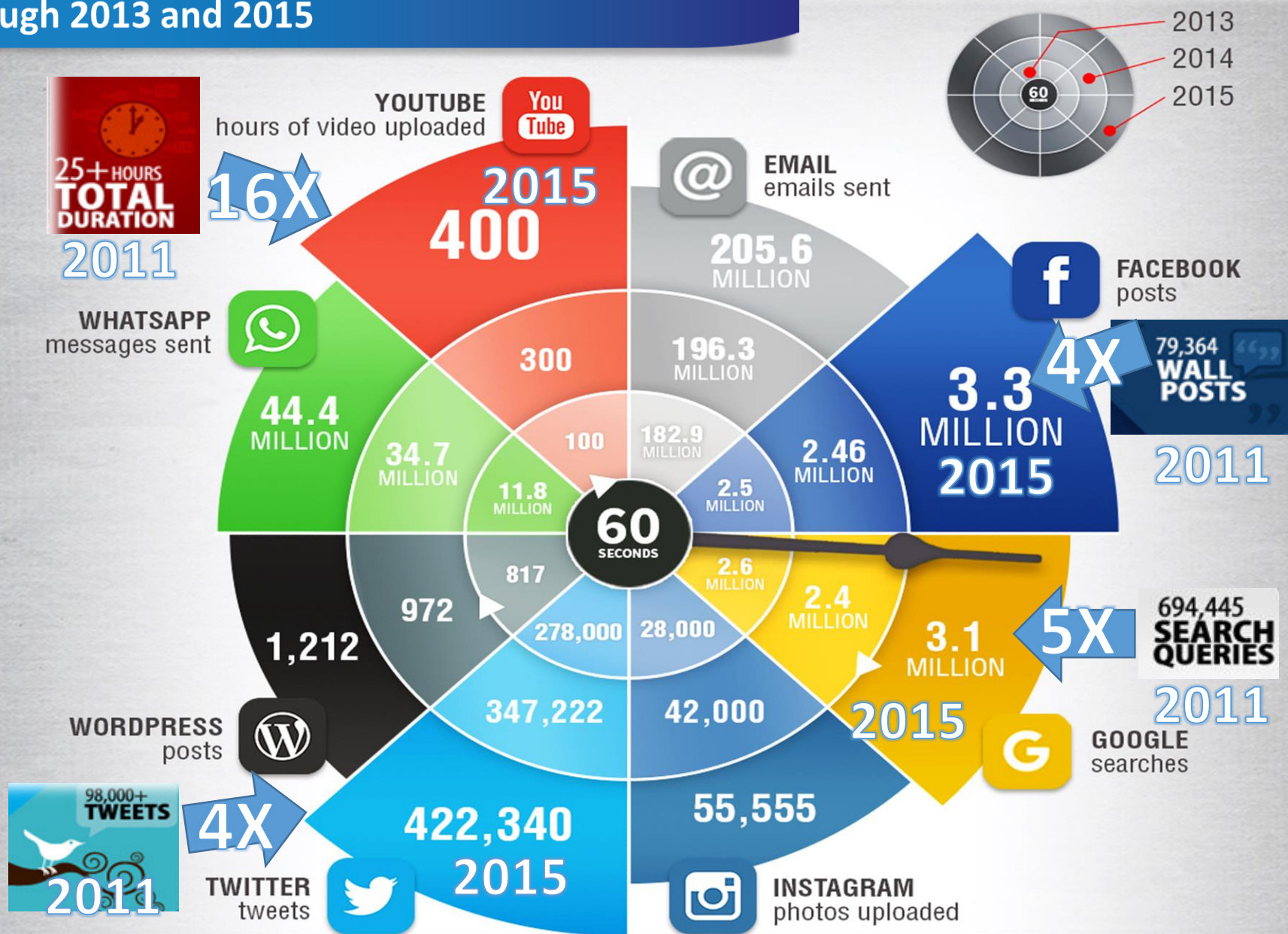
What can be happen in 60 Seconds?



Cyber Security Trend

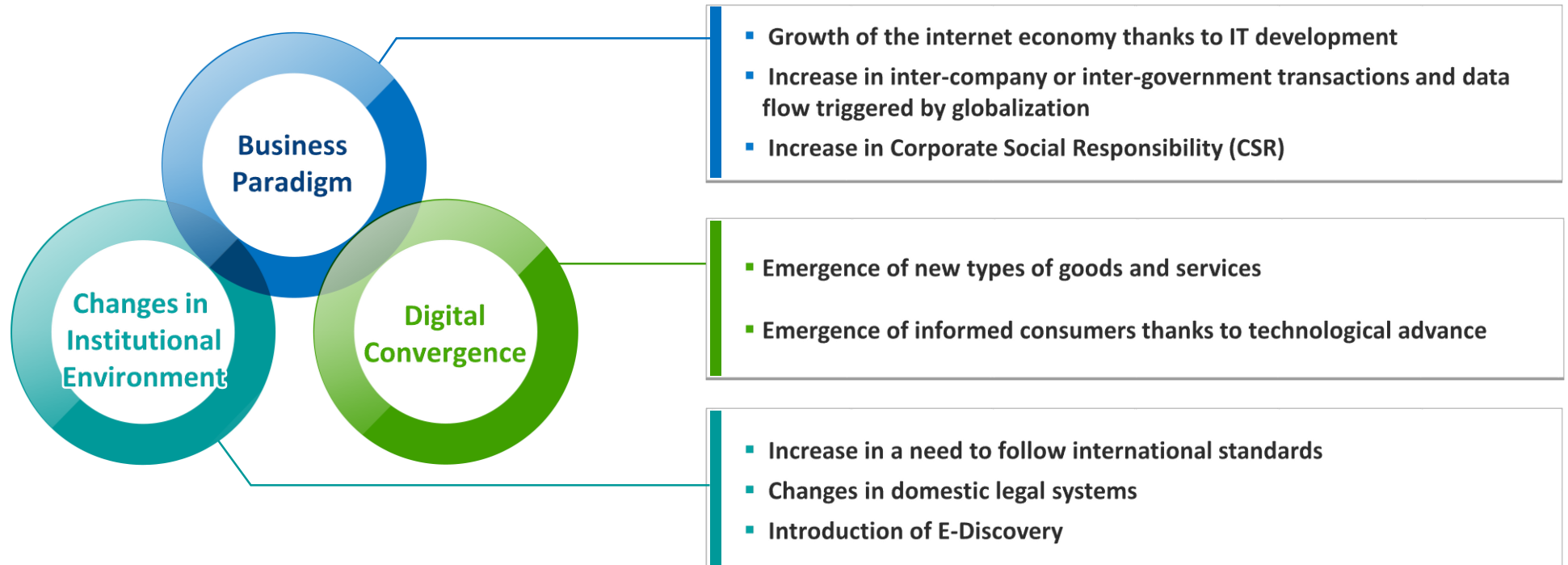


Through 2013 and 2015



Changes in Business Environment

- Institutional environment changes as Corporate Social Responsibility (CSR) and a need to follow national and international legal systems increase
- The Internet economy rapidly grows thanks to IT development
- A number of new types of goods and services with access to the industry rises due to active attitude of consumers



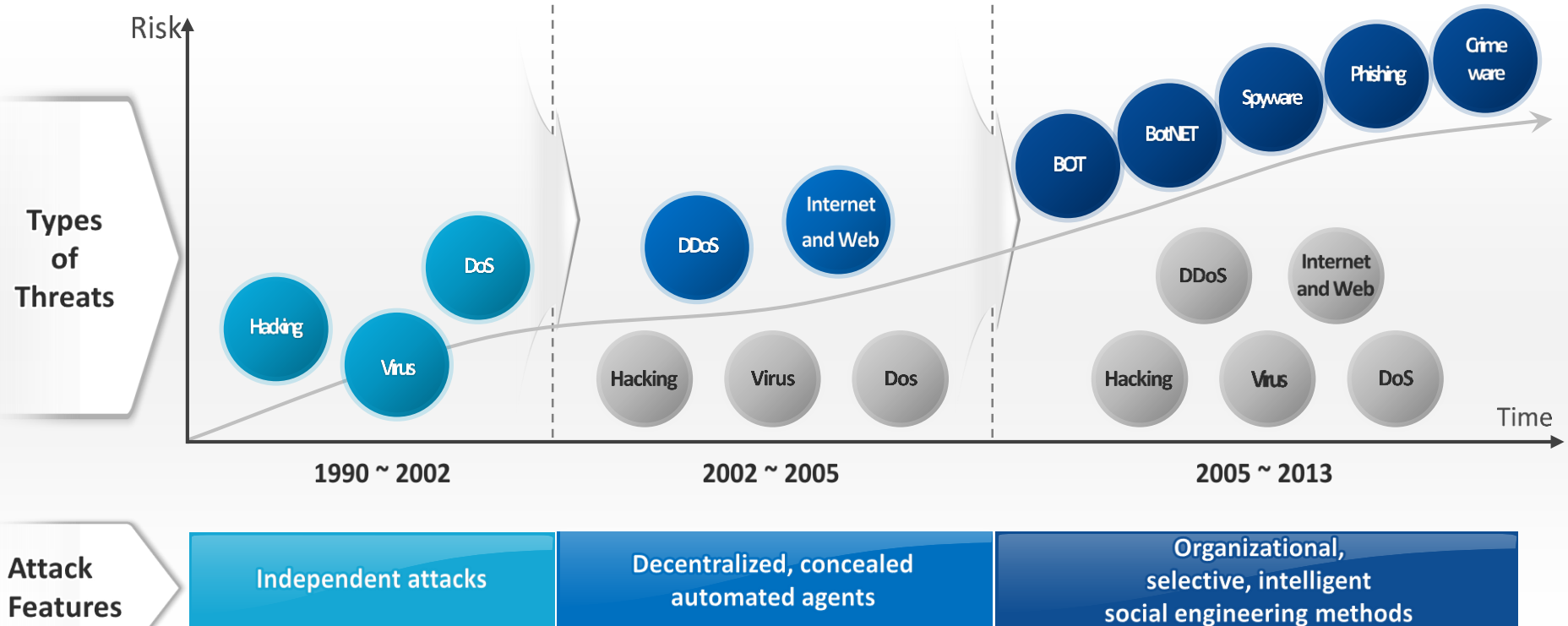
Changes in Information Technology Environment

- > IT resources, once considered a part of business, are now turning into a business
- > User-centric networking devices are equipped with better communications and mobility

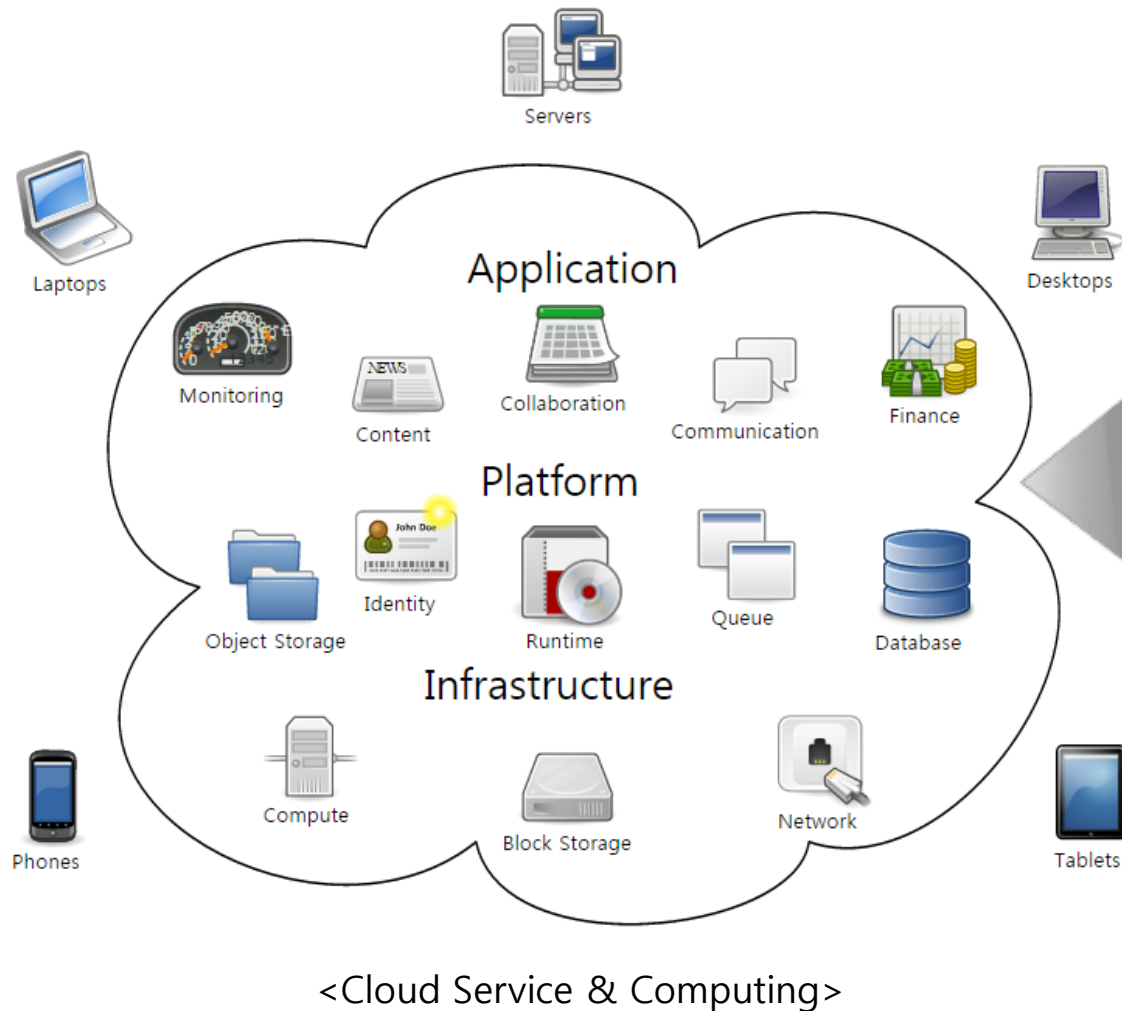
	1990	2000	2010	2020
IT Platform	Dialup	WWW	Mobile	IoT
Hardware	PC	Multimedia	Smartphone	Everything
Network	Modem	Cable ADSL	4G LTE	M2M
Software	DOS	Windows	Android	Cloud OS
Killer App	Chat	Search	Social Media	Machine Learning
Business	Service Charge	Ads	Brokerage	Convergence

Different Threats for Extortion

- Past characteristics of hacking and virus : Independent & Boastful
- Present : Organizational (decentralized, concealed, automated agents), Intelligent (for monetary purposes), Social engineering methods



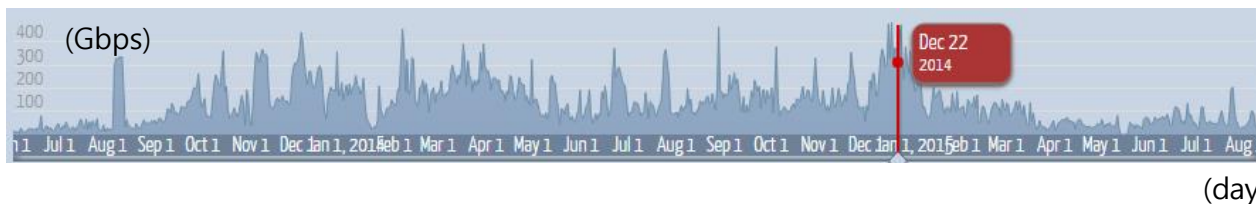
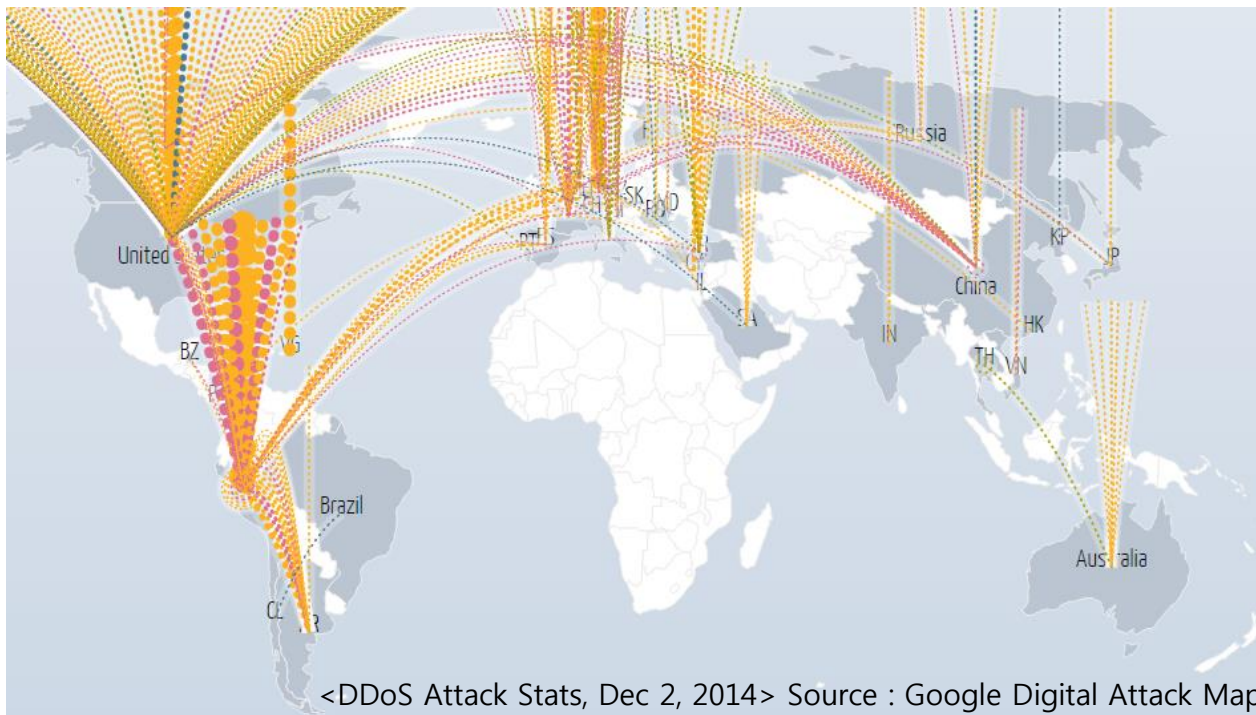
Threats to a Cloud Service



<9 Worst Cloud Security Threats>

1. Data Breach
2. Data Loss
3. Account or Service Traffic Hijacking
4. Insecure APIs
5. Denial of Service
6. Malicious Insiders
7. Abuse of Cloud Services
8. Insufficient Due Diligence
9. Shared Technology

DDoS Attack Statistics

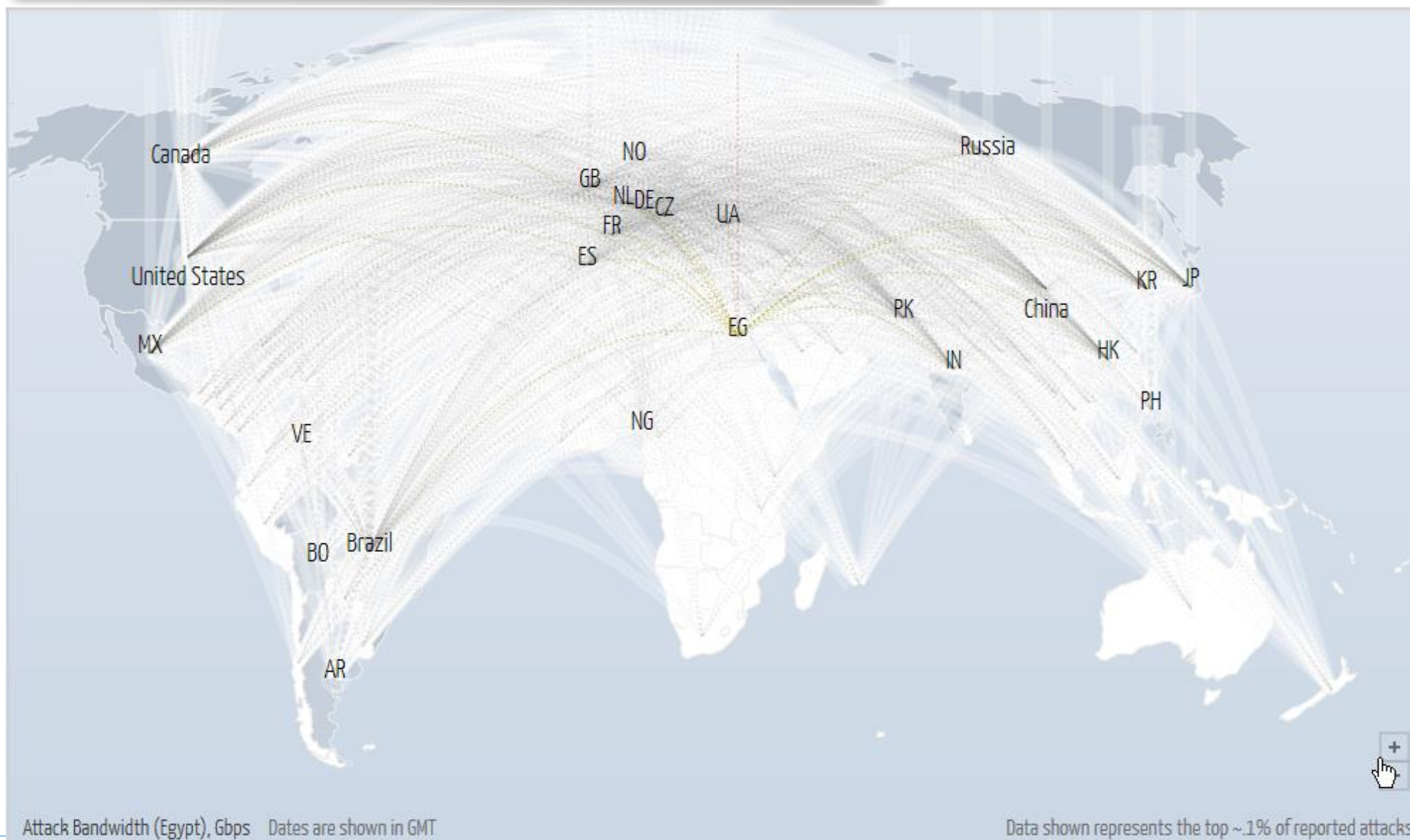


<DDoS Attack Stats, Dec 2, 2014 > Source : Google Digital Attack Map

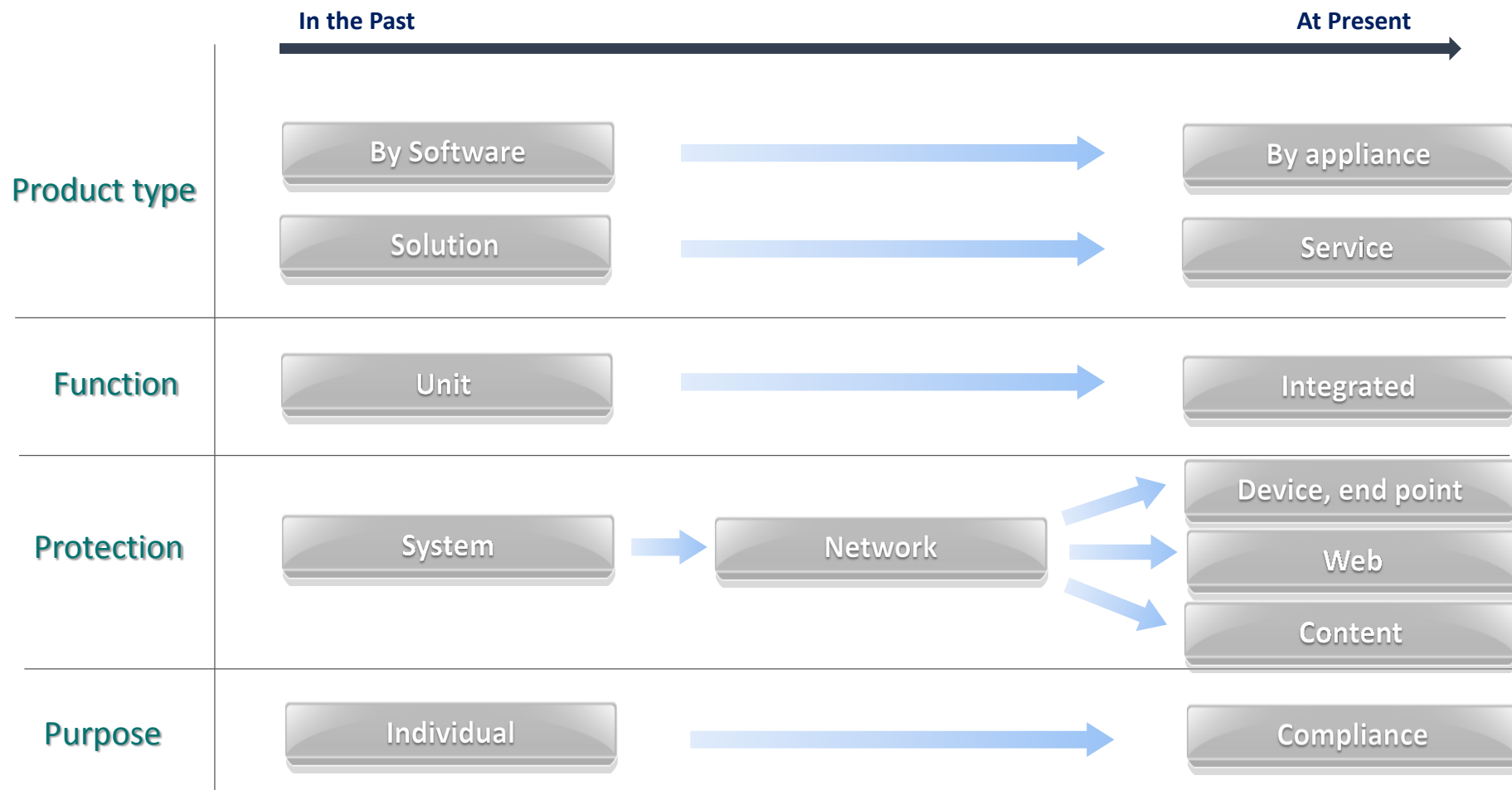
DoS Attacks Comparison in 2013 and 2014

- 47% increase in total DDoS attacks
- 69% increase in infrastructure attacks
- 133% increase in average peak bandwidth
- Target based DDoS attacks

DDoS Attack on Egypt : 20th Sep 2016



Cyber Security Technology Trend



Cyber Security Technology Industry

SECURITY MANAGEMENT AND COMPLIANCE



INFRASTRUCTURE SECURITY



CYBER SECURITY



ENDPOINT SECURITY



APPLICATION SECURITY



CLOUD SECURITY



MOBILE SECURITY



IDENTITY AND ACCESS MANAGEMENT



SECURITY PARTNERS



SECURITY ORGANIZATIONS



SECURITY CONFERENCES



ANALYST HOUSES



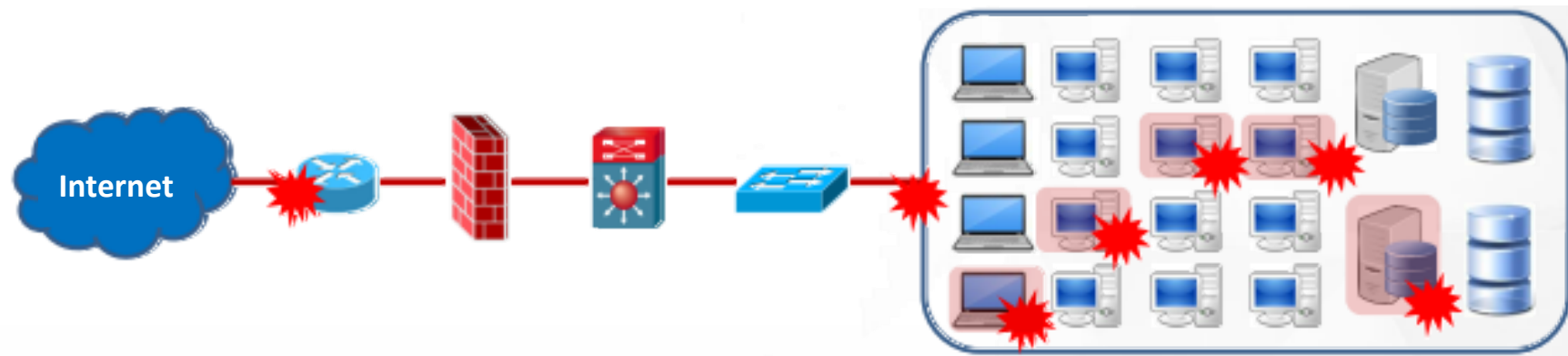
Cyber Attack Paradigm Shift

“The security industry has long been overly focused on prevention.

Let’s keep preventing, but enhance our ability to detect threats that slip through our defenses (which they will inevitably do).”

■ RSA

Cyber Attack Lateral Movement



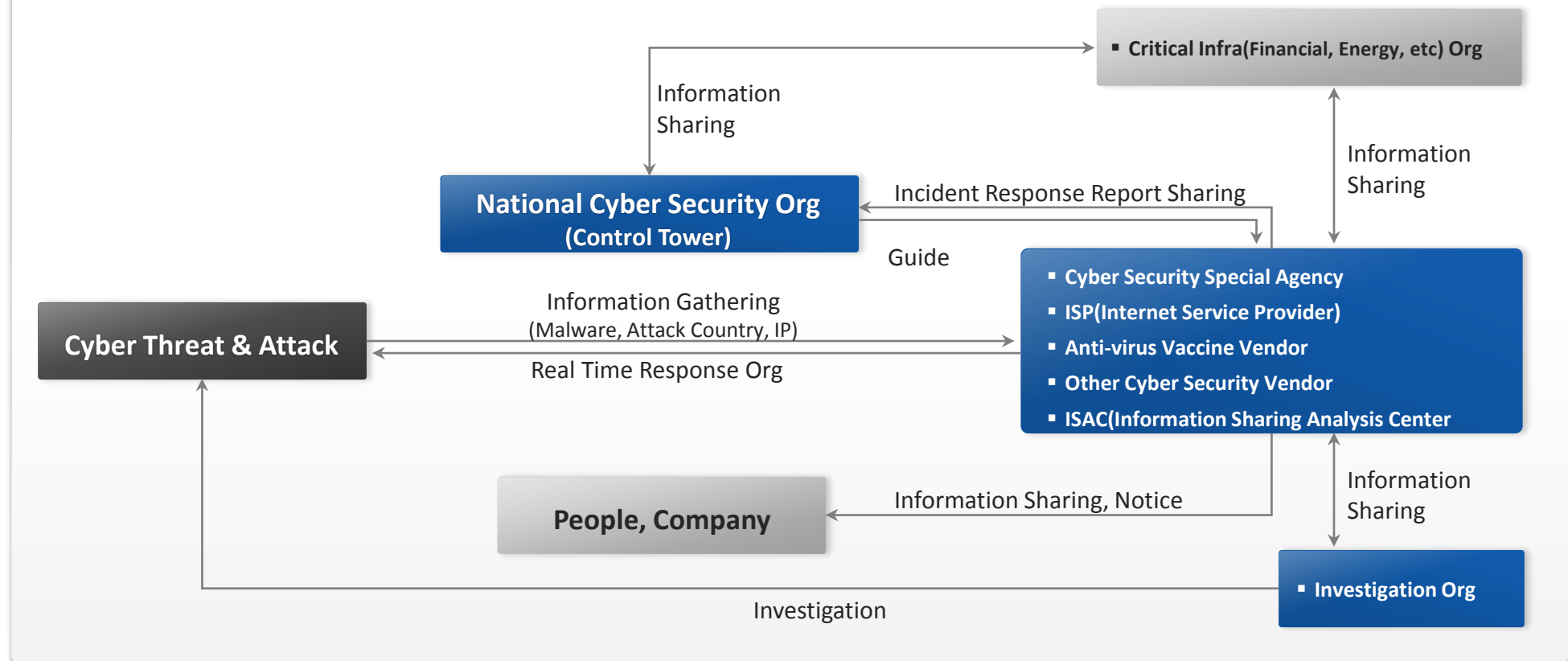
Attack the insecure target first, then move into the critical point step by step. Even CIP and SCADA systems are reachable by the internet connected PC.



Cyber Security Response

Cyber Security Response Structure

- ✓ Information Security organizations can be divided into a variety of configurations according to the cyber security strategy. In general, Information Security strategies, policies, correspondence, etc.



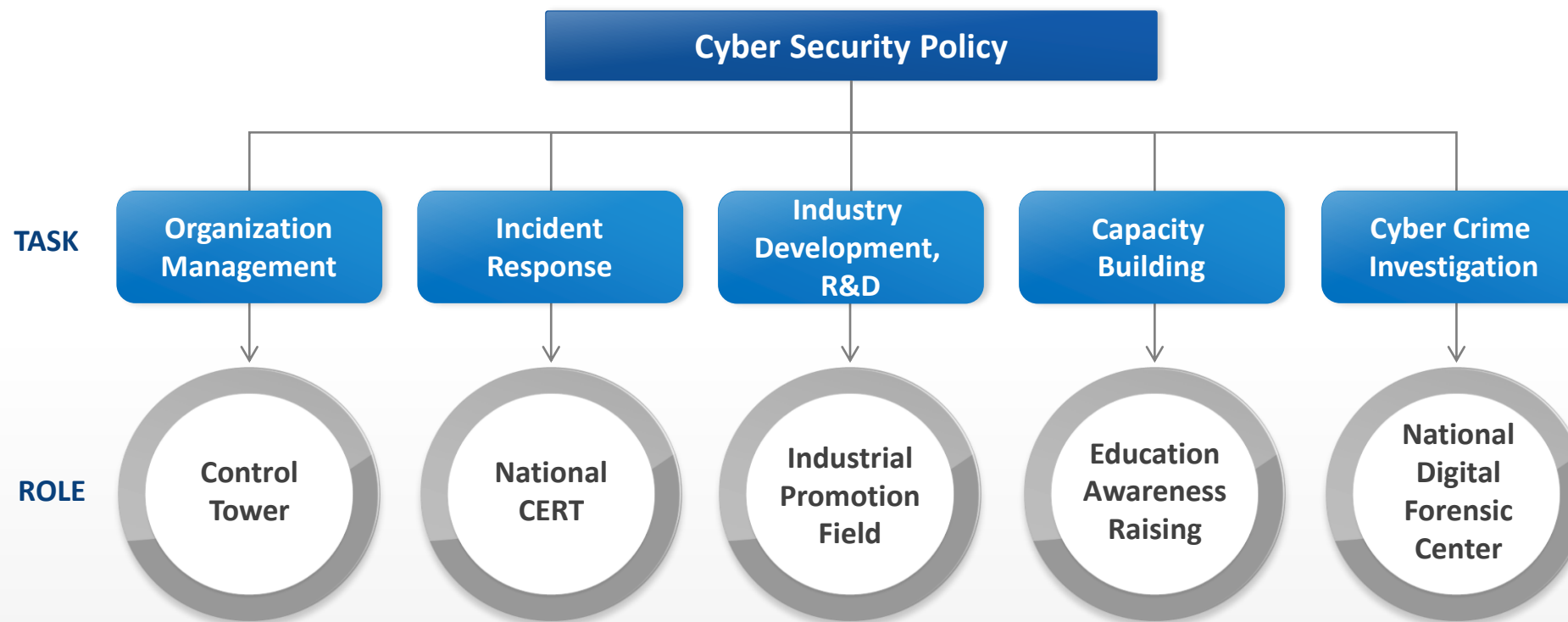
Organization by Role & Responsibility

- ✓ Information Security Organizations can be divided into a variety of configurations according to the cyber security strategy. In general, Information Security strategies, policies, correspondence, etc.

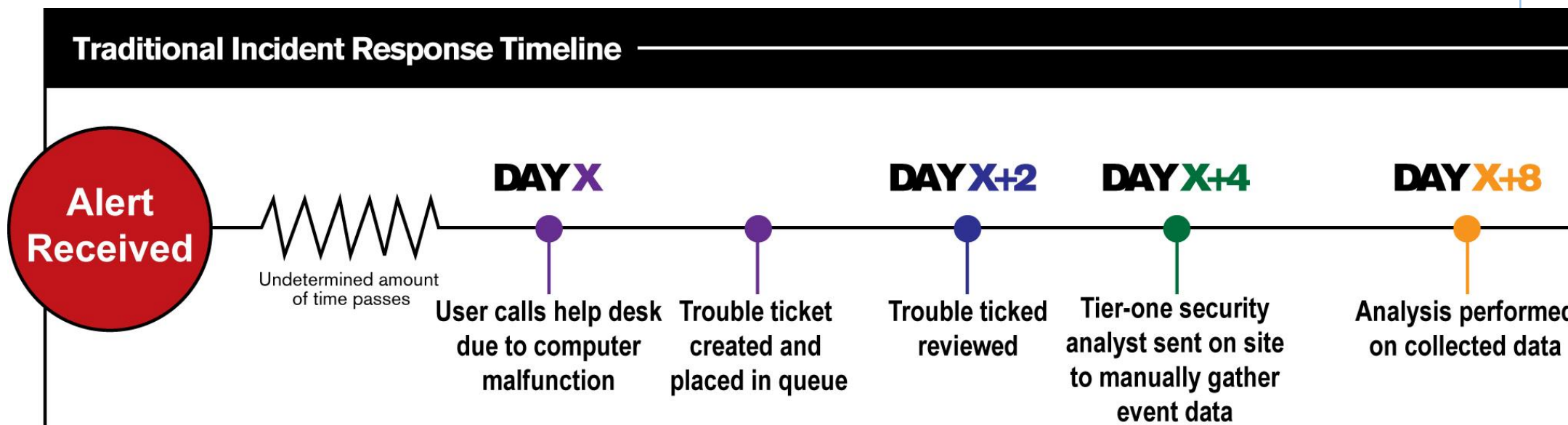


Organization by Policy

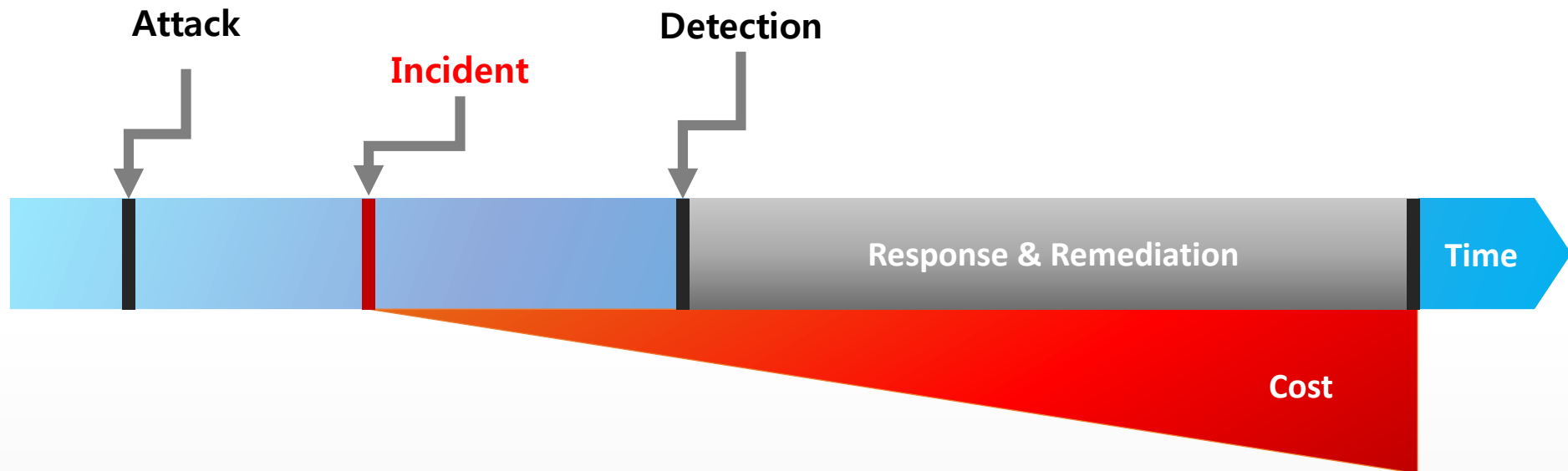
✓ Depending on the cyber security strategy, Variety of role separation is existing.



Traditional Incident Response Timeline

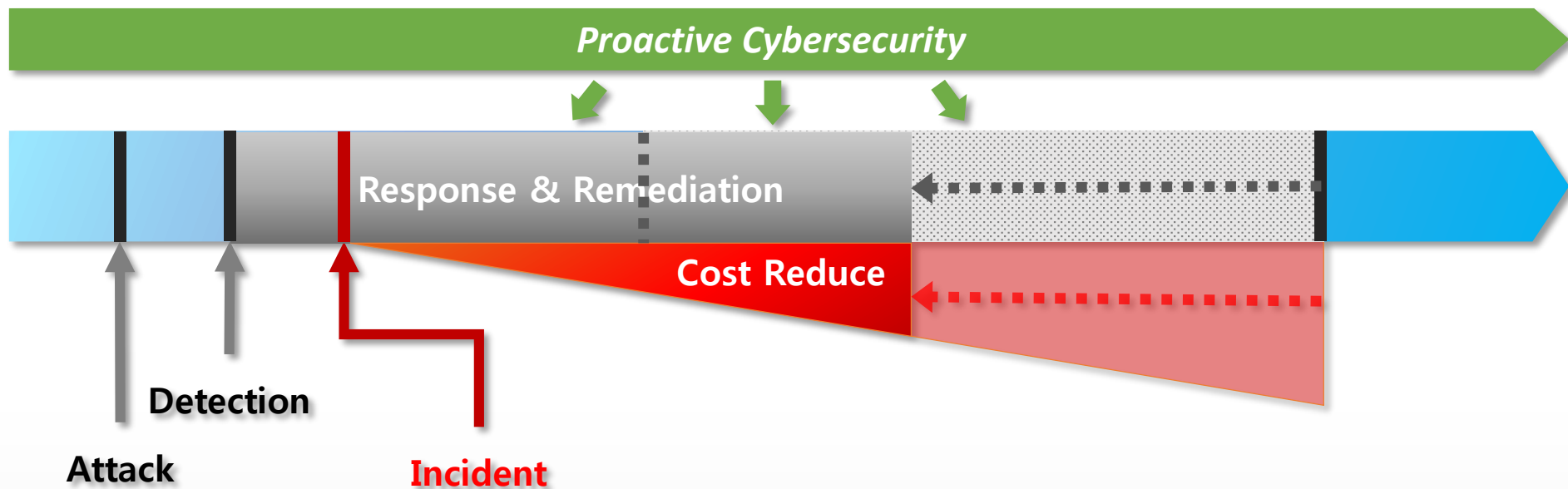


Incident Metrics



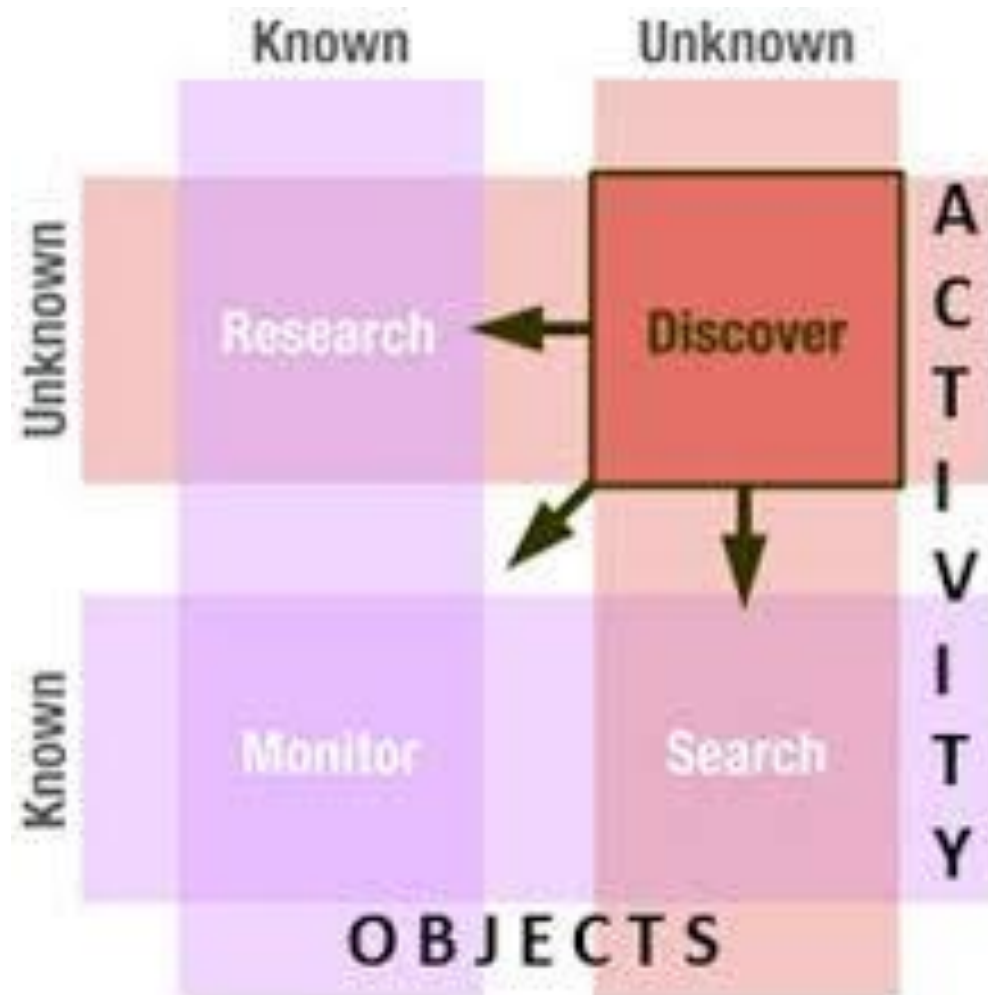
As detection, response, and remediation efforts slide to the right, the level of effort and expense to resolve the incident increase dramatically.

Incident Metrics

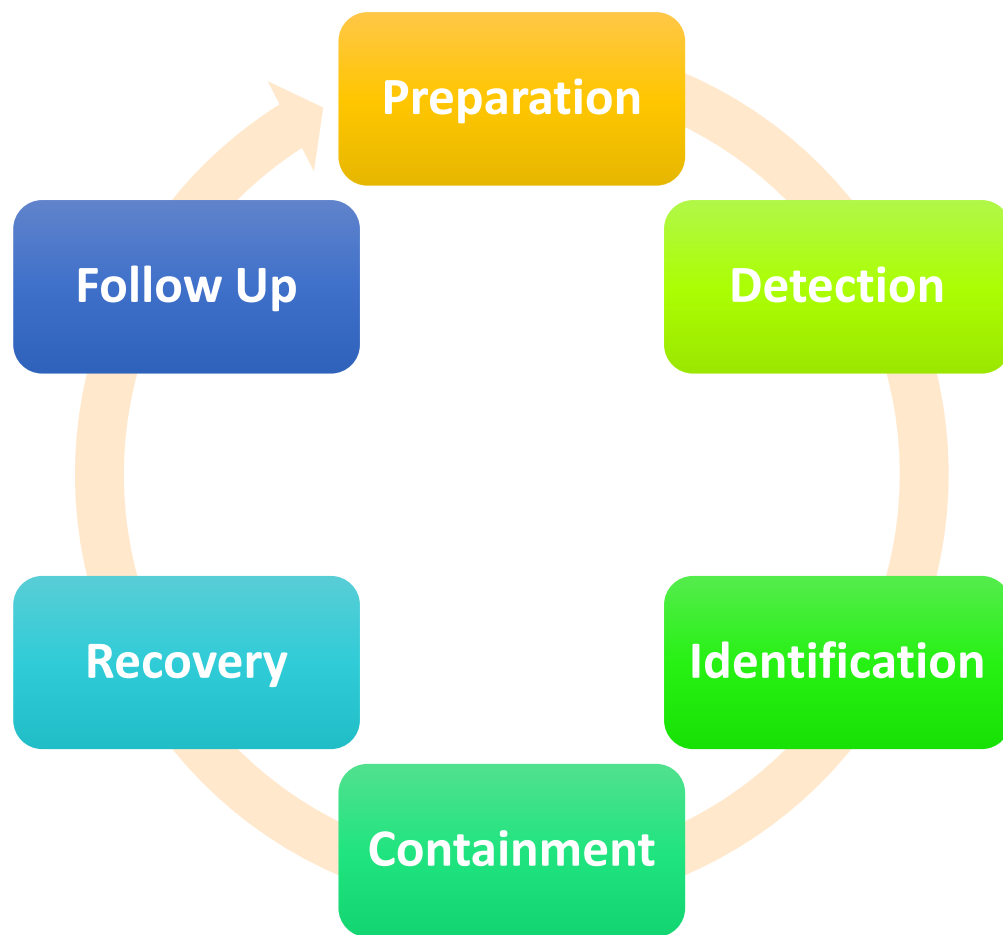


Successful proactive approach detecting the attack before incident will reduce total cost

Detection : Discover, Search, Research, Monitor



Identification and Containment



**Identification
requires
100% accuracy
through
Digital Forensics**

MTTI and MTTC

Mean time to identify (MTTI)



The time it takes to detect that an Incident has occurred

(total cost, in millions)

\$3.23

MTTI < 100 days

\$4.38

MTTI ≥ 100 days

Mean time to contain (MTTC)

\$3.18

MTTC < 30 days

\$4.35

MTTC ≥ 30 days

The time it takes to resolve a situation and ultimately restore service

(total cost, in millions)

※ source : 2016 Cost of Data Breach Study : Global Analysis / Ponemon
※ source : <http://www.slideshare.net/ibmsecurity/the-2016-ponemon-cost-of-a-data-breach-study>



Digital Forensics for Identification/Containment



Law Enforcement

Digital Forensics is the **acquiring** and **scientific examination** and analysis of **data** retrieved from computer or other **digital devices** (mobile phones, games consoles, memory sticks, etc) in such a way that the information can be **used in a court of law**.



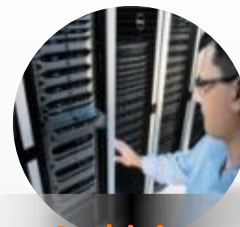
Devices & Data



Forensic Experts



Analysis

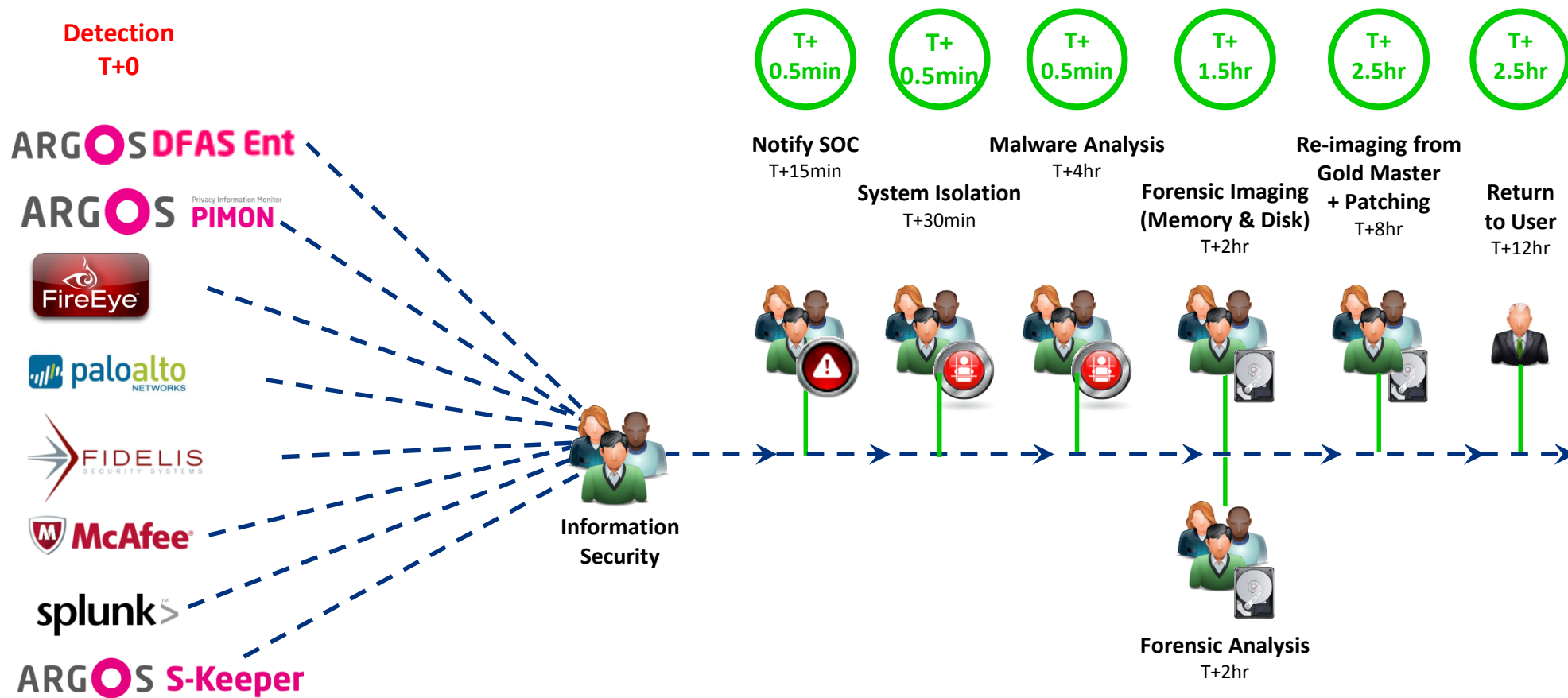


Archiving



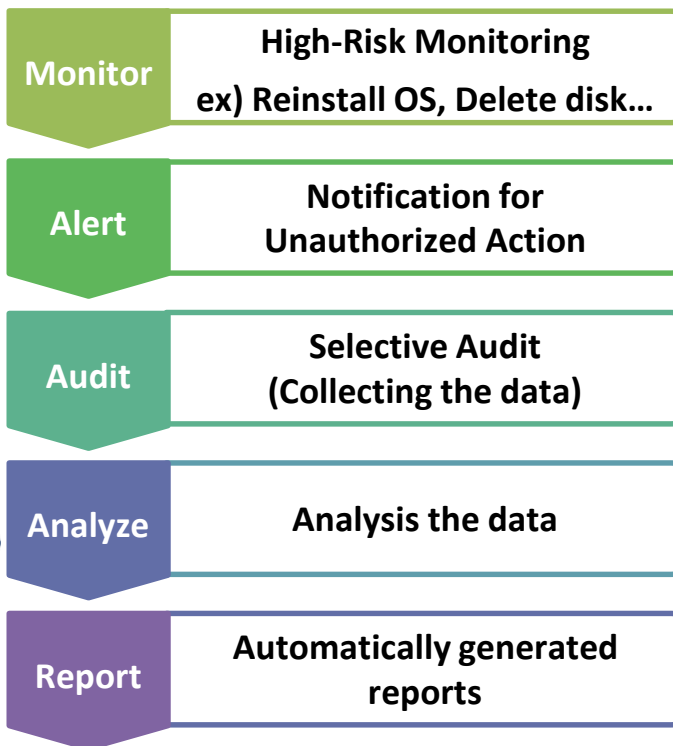
Court
Presentation

Combining Proactive and Reactive Response



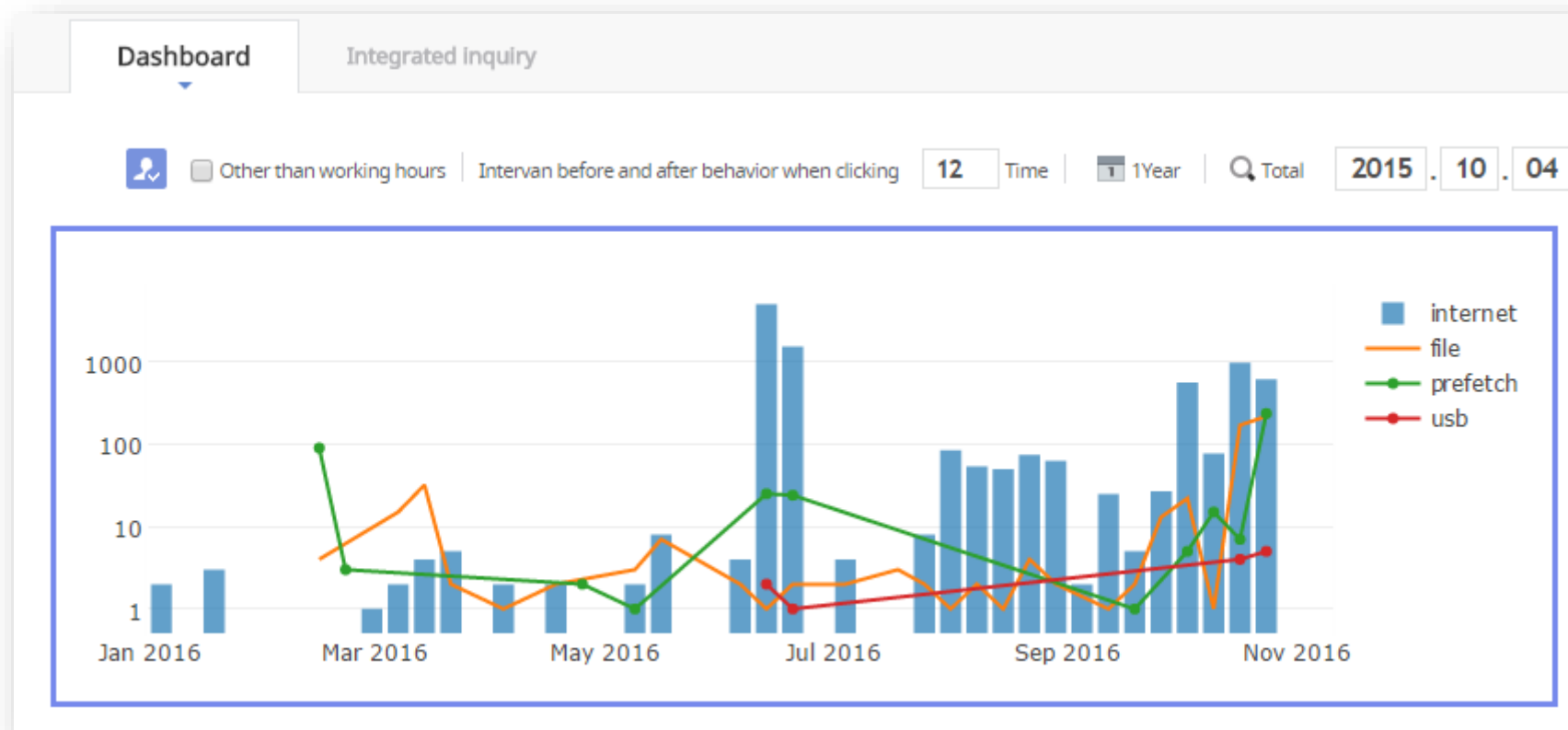
Remote Digital Forensics

You can simply execute the information audit in anytime and everywhere by just clicking the DFAS Enterprise.



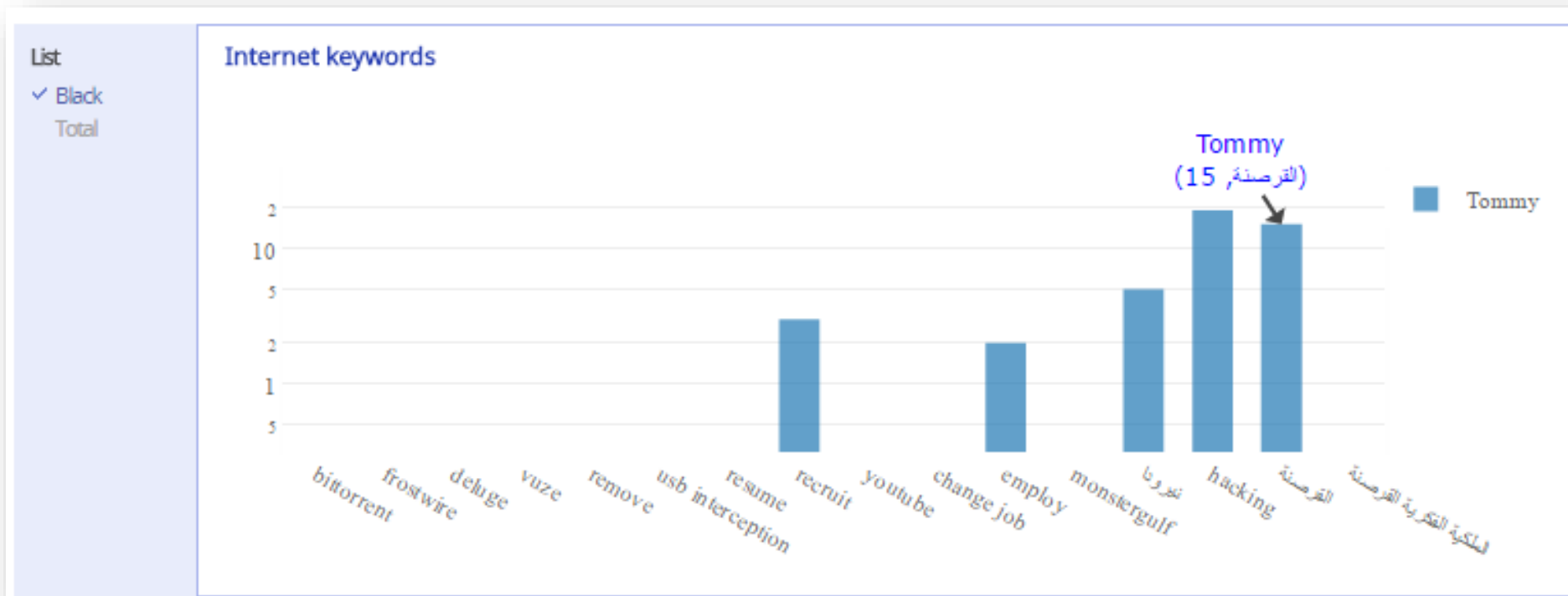
Case Study

Endpoint User Activity



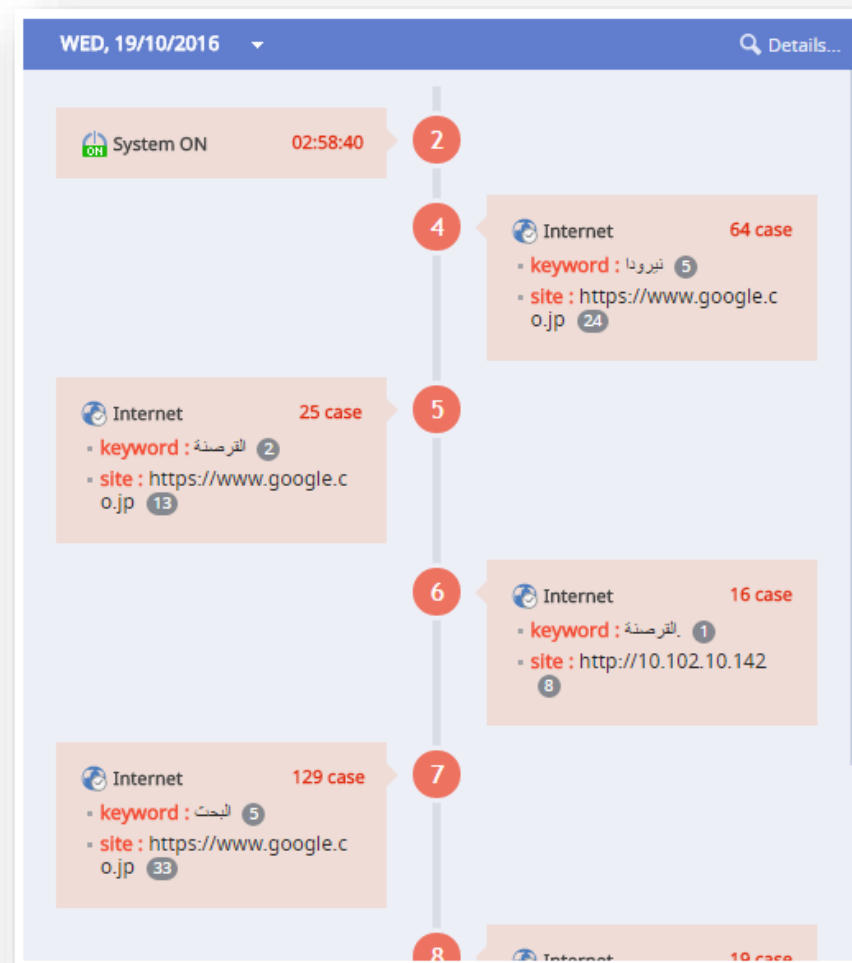
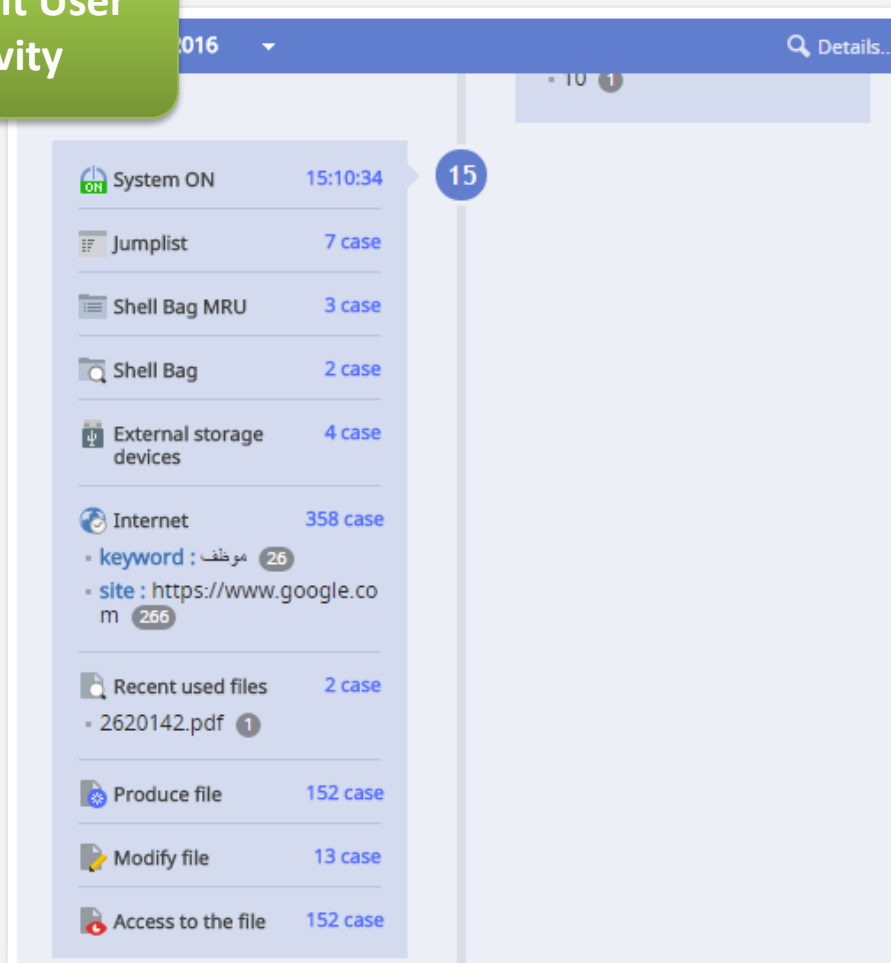
Case Study

Endpoint User Activity



Case Study

Endpoint User Activity



Case Study

Breach Detection

File Name : f728905216f2e99f10af24d1e08cac20.txt

Modify

f728905216f2e99f10af24d1e08cac20.txt

2016-10-26 13:16:53

Network Attach(FTP)

f728905216f2e99f10af24d1e08cac20.txt

2016-10-26 13:17:20

Delete

f728905216f2e99f10af24d1e08cac20.txt

2016-10-26 13:17:57

Modify

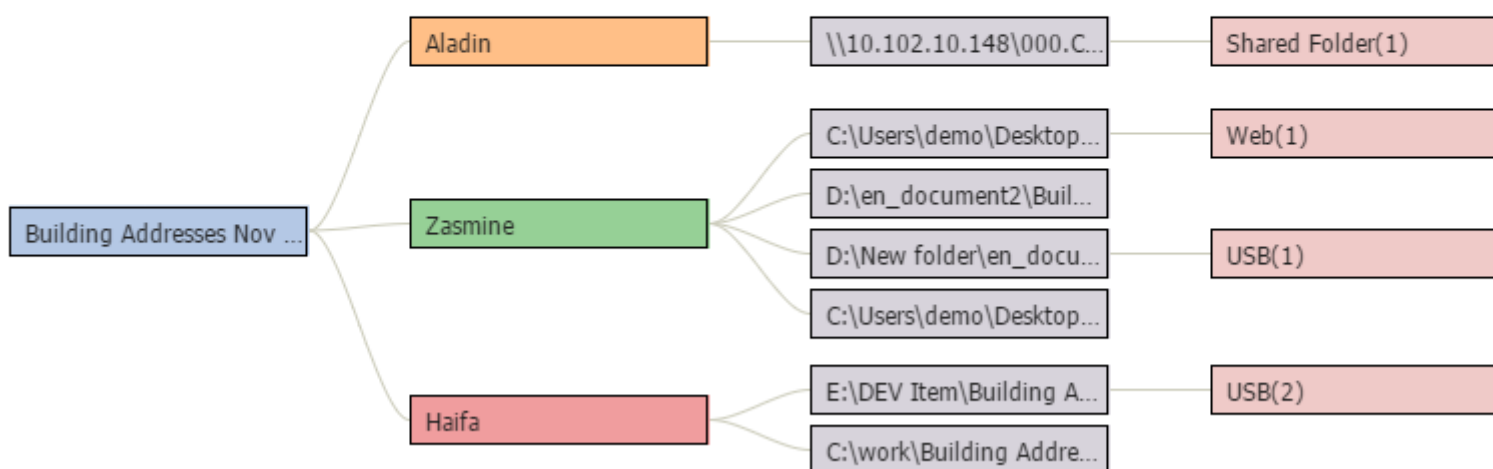
f728905216f2e99f10af24d1e08cac20.txt

2016-10-26 13:20:26

Case Study

Breach Detection

File Name : Building Addresses Nov 2010.xlsx and 6 Others

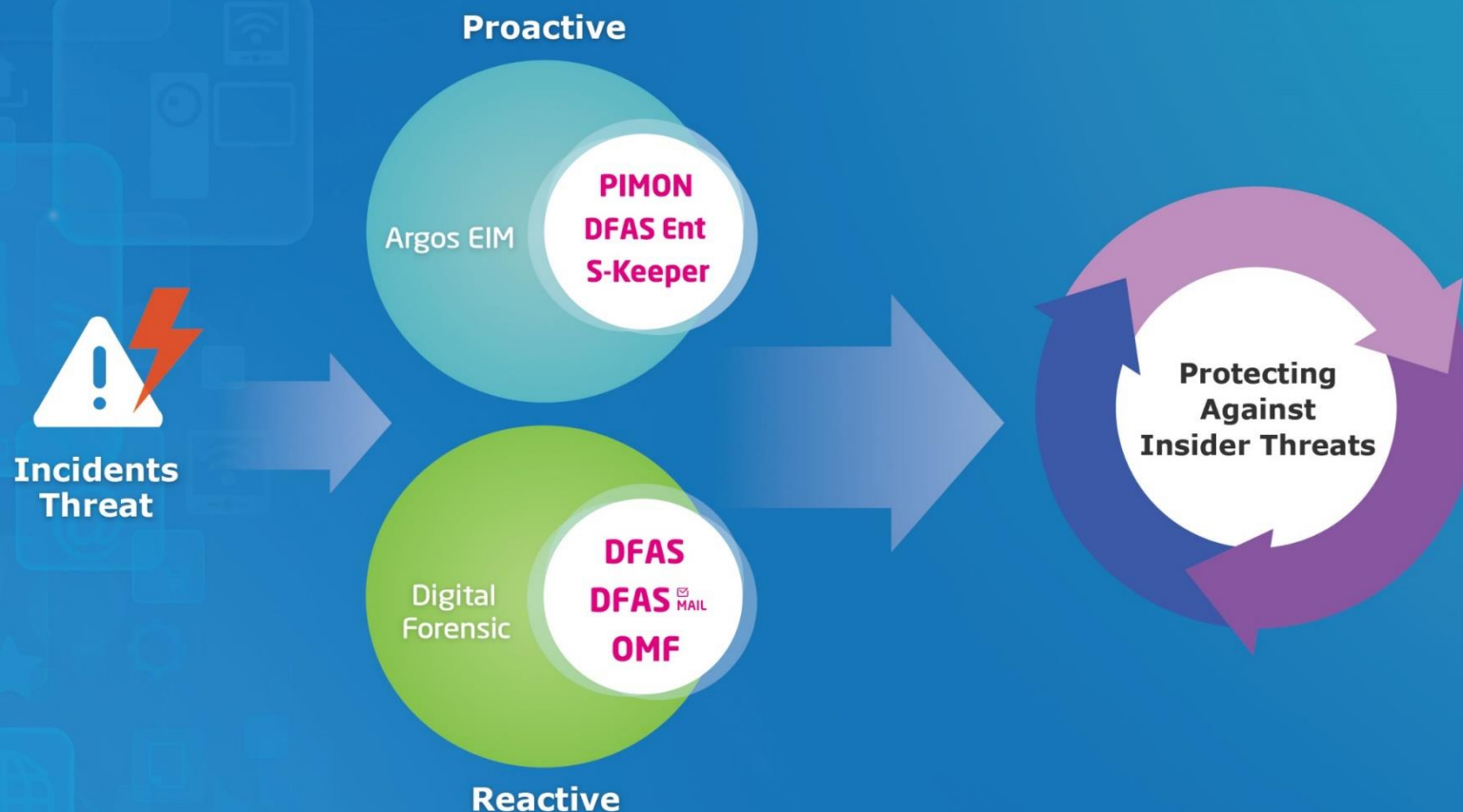


Incident Detection



Human Behavior Based Security

Construct differentiated infrastructure using Digital Forensic technique



About Duzon

Leading IT and Security Solution & Service Provider in Korea

Established : 1997

Employee : 1300+ (700+ R&D)

Customer : 140,000+ (IT) 15,000+ (Security & Digital Forensics)



About Duzon

Oman NDFL Project

National Digital Forensics Laboratory: 2 years of project establishment and management:
Solutions & Equipment, Facilities, and Training

ITA signs a national digital forensic lab contract
30 Dec 2014



The Information Technology Authority (ITA) has signed a contract with the Korean Internet and Security Agency (KISA) to build a national digital forensic laboratory in Oman. Dr. Salim Sultan Al Ruzaiqi, CEO of ITA, signed the contract along with Mr. Chanwoo Lee from KISA.

The idea behind establishing a national digital forensic laboratory is to help detect cybercrimes in order to serve the law and justice. This will also help in producing qualified experts in digital forensics and work along with the law enforcement institutions in investigating cybercrimes to justice especially in cases related to the Information Communications Technology (ICT).

The national digital forensic lab in Oman aims to obtain an international recognition which would enhance the credibility of the lab and its evidence, especially with regard to cybercrimes from outside the country.

It is worth mentioning that the Sultanate, represented by the Information Technology Authority (ITA) had signed a previous memorandum of understanding with the Korean Internet and Security Agency (KISA) including interests related to digital evidence and cyber-security incidents caused by cybercrimes.

Task	Start	Finish
Computer Forensics	Sun 15-09-11	Thu 15-09-17
Preparation	Sun 15-05-31	Wed 15-08-19
Deployment and Test	Sun 15-06-07	Thu 15-08-06
Lab Management Establishment (Data Center)	Sun 15-06-07	Thu 15-08-06
AD Lab Establishment (Data Center)	Mon 15-07-13	Thu 15-08-20
Computer Forensic Lab (KOM4)	Sun 15-08-16	Thu 15-09-03
UAT from ITA	Sun 15-09-06	Thu 15-09-10
Milestone Approval from ITA	Sun 15-09-13	Thu 15-09-17
Data Recovery	Sun 15-06-14	Mon 15-10-05
Preparation	Sun 15-06-14	Wed 15-08-26
Deployment and Test	Sun 15-06-09	Thu 15-09-17
UAT from ITA	Sun 15-09-20	Mon 15-09-28
Milestone Approval from ITA	Tue 15-09-29	Mon 15-10-05
Mobile Forensics	Sun 15-06-21	Sun 15-10-18
Preparation	Sun 15-06-21	Sun 15-08-30
Deployment and Test	Sun 15-09-13	Thu 15-10-01
UAT from ITA	Sun 15-10-04	Thu 15-10-08
Milestone Approval from ITA	Sun 15-10-11	Sun 15-10-18
Audio/Video Forensics	Sun 15-06-28	Thu 15-11-05
Preparation	Sun 15-06-28	Thu 15-10-01
Deployment and Test	Sun 15-10-04	Thu 15-10-22
UAT from ITA	Sun 15-10-25	Thu 15-10-29
Milestone Approval from ITA	Sun 15-11-01	Thu 15-11-05

MUSCATDAILY.COM

DIGITAL FORENSIC LAB ADDS EDGE TO ANTI-CYBERCRIME MEASURES



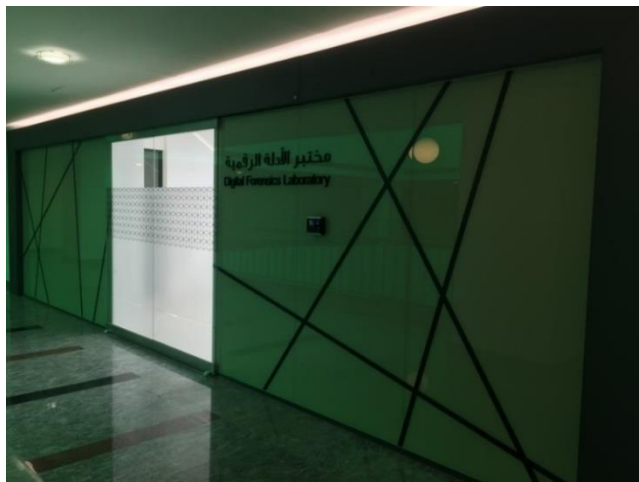
Haitham presides over National Digital Forensic Lab opening



The laboratory was inaugurated under the auspices of His Highness Sayyid Haitham bin Tariq Al Said Minister of Heritage and Culture at Knowledge Oasis Muscat. -Supplied photo

About Duzon

Oman NDFL Project



شکرا جزیرا

<http://www.d-forensic.com>

forensic@duzon.com