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

DUZON

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

CONTENTS

Cyber Security Trend

DUZON

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.

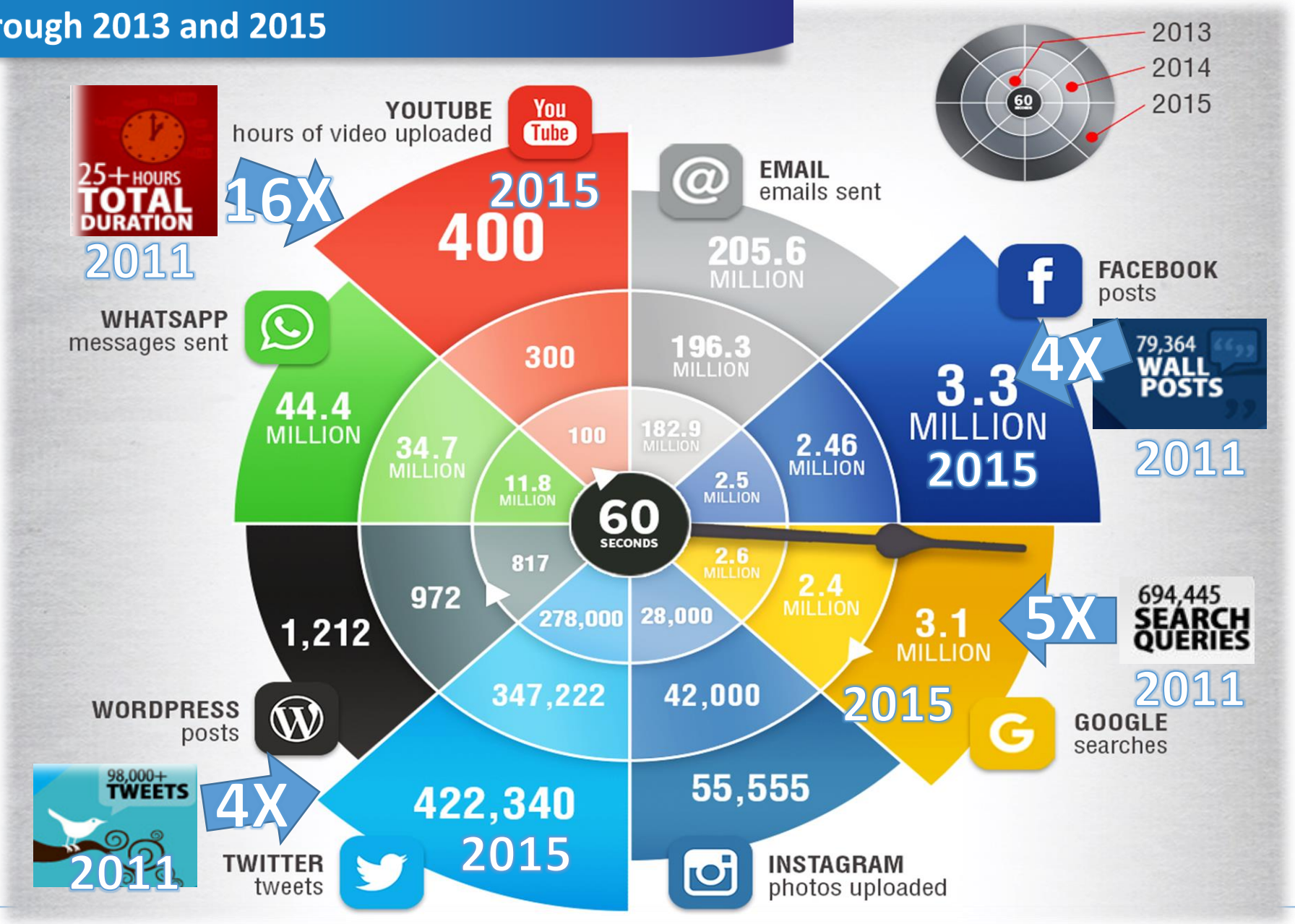
<Definition source : Wikipedia>

What can be happen in 60 Seconds?

Cyber Security Trend

Cyber Security Trend

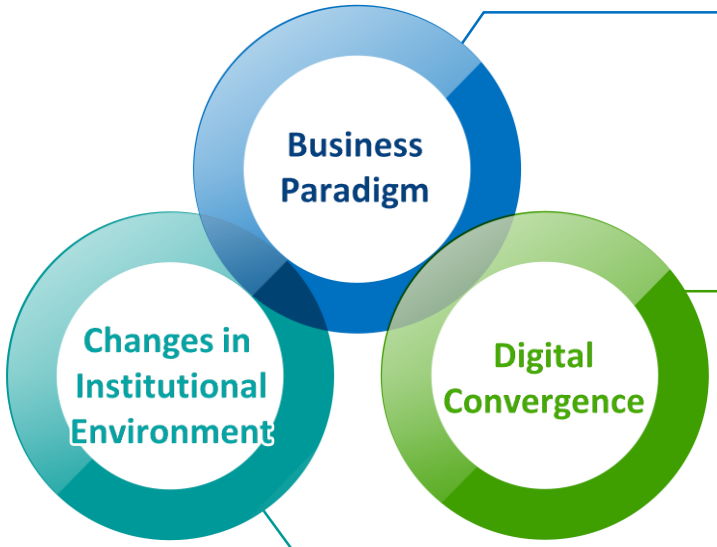
Through 2013 and 2015



Cyber Security Trend

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



- Growth of the internet economy thanks to IT development
- Increase in inter-company or inter-government transactions and data flow triggered by globalization
- Increase in Corporate Social Responsibility (CSR)

- Emergence of new types of goods and services
- Emergence of informed consumers thanks to technological advance

- Increase in a need to follow international standards
- Changes in domestic legal systems
- Introduction of E-Discovery

Cyber Security Trend

Changes in Information Technology Environment

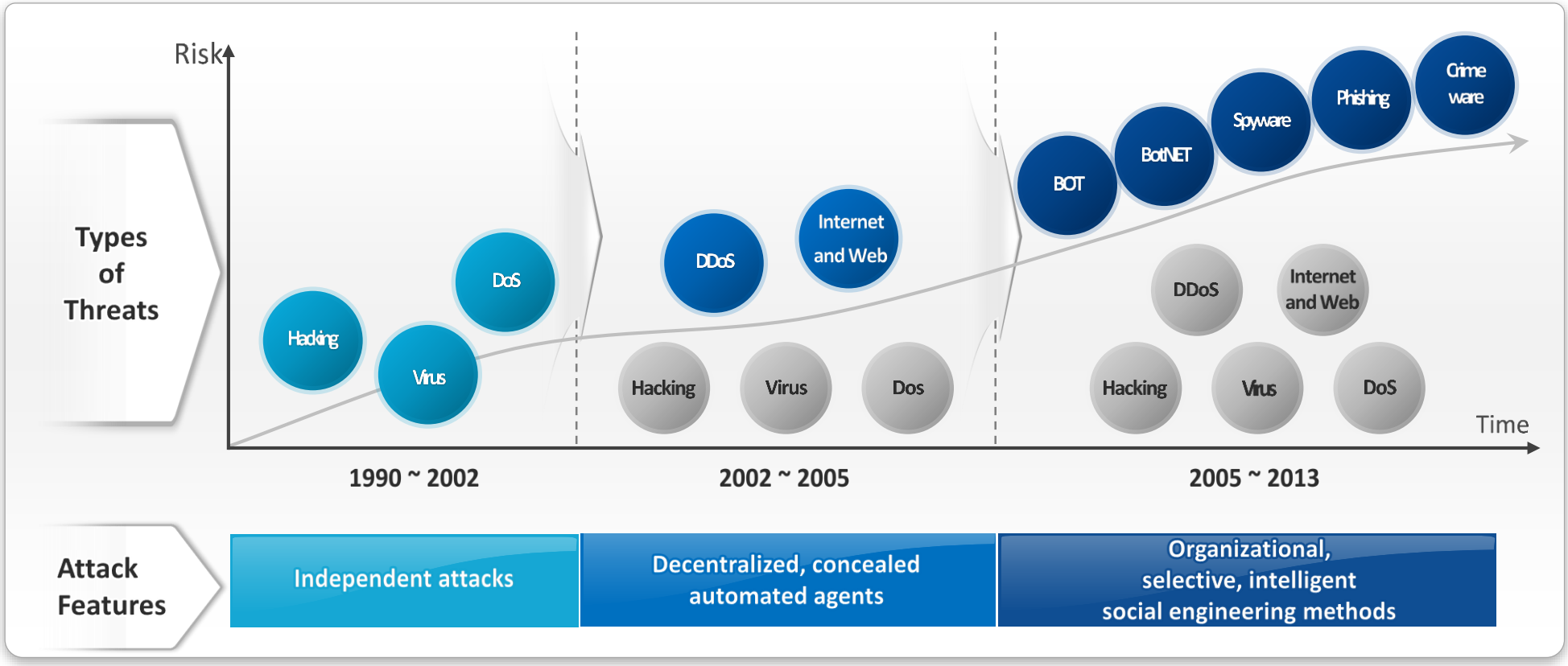
- IT resources, once considered a part of business, are now turning into a business
- User-centric networking devices are equipped with better communications and mobility

	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

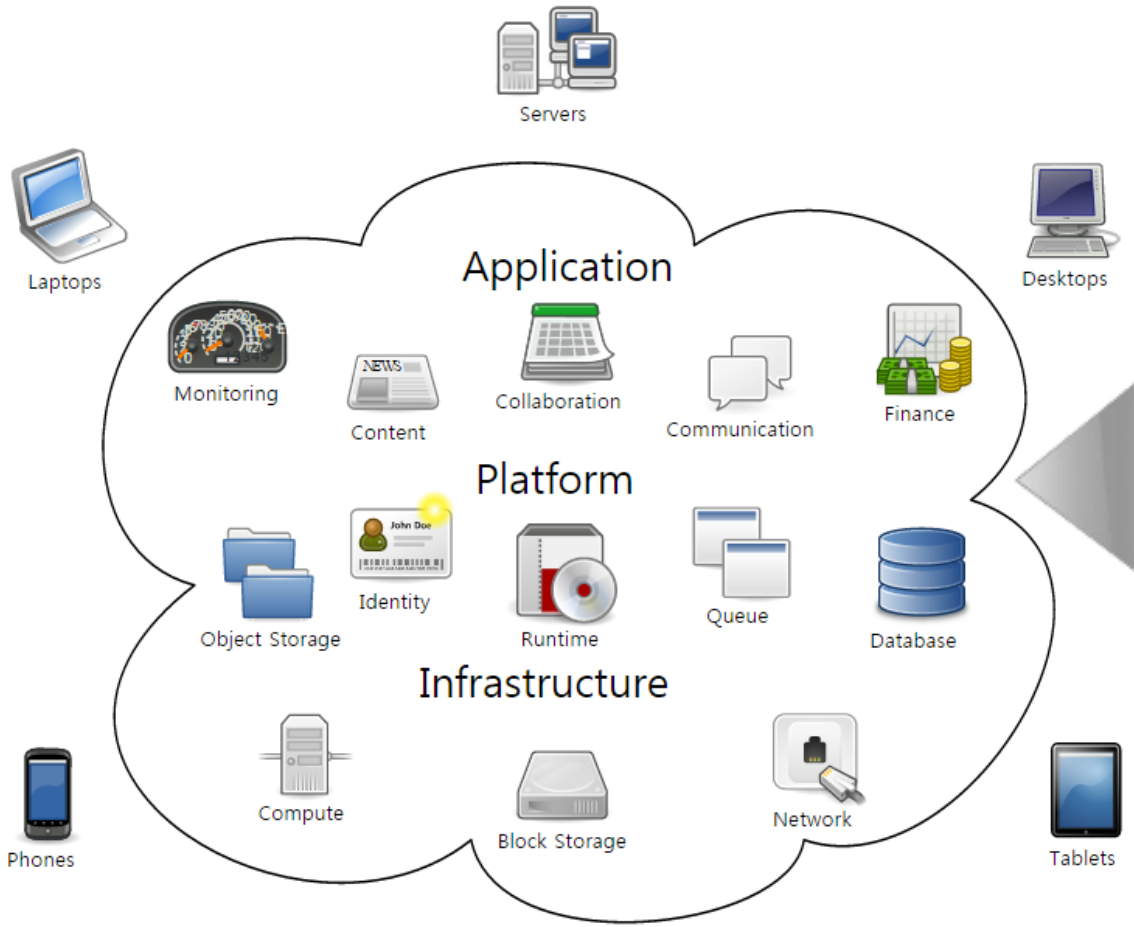
Cyber Security Trend

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

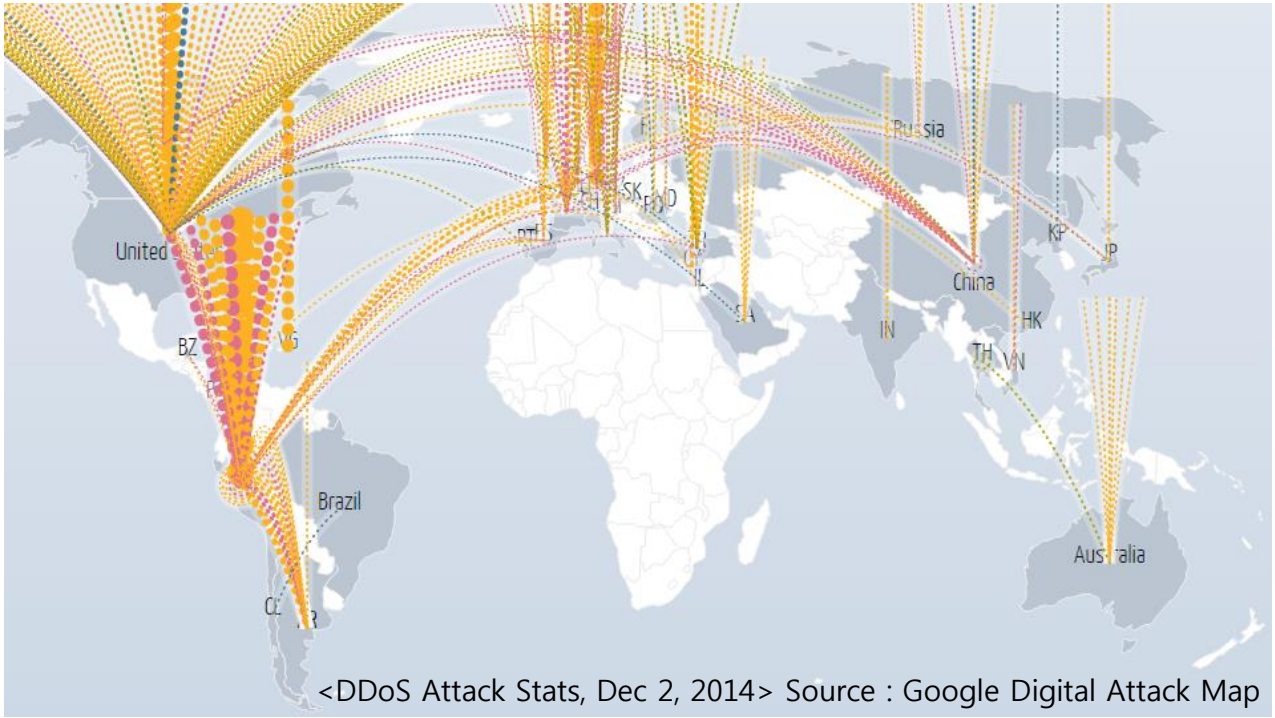


<Cloud Service & Computing>

<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

(day)

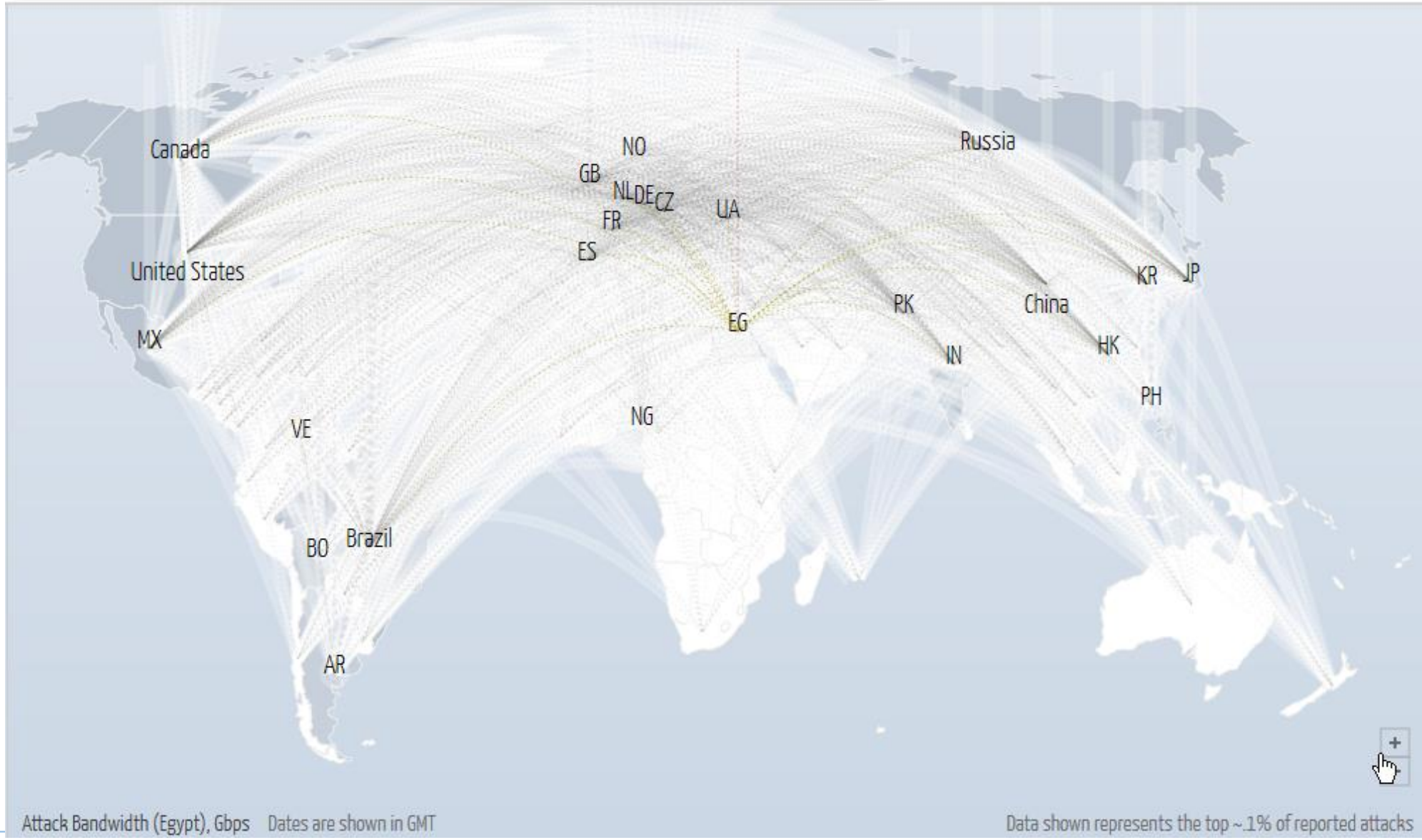
<DDoS Attack Stats, Dec 2, 2014 > Source : Google Digital Attack Map

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

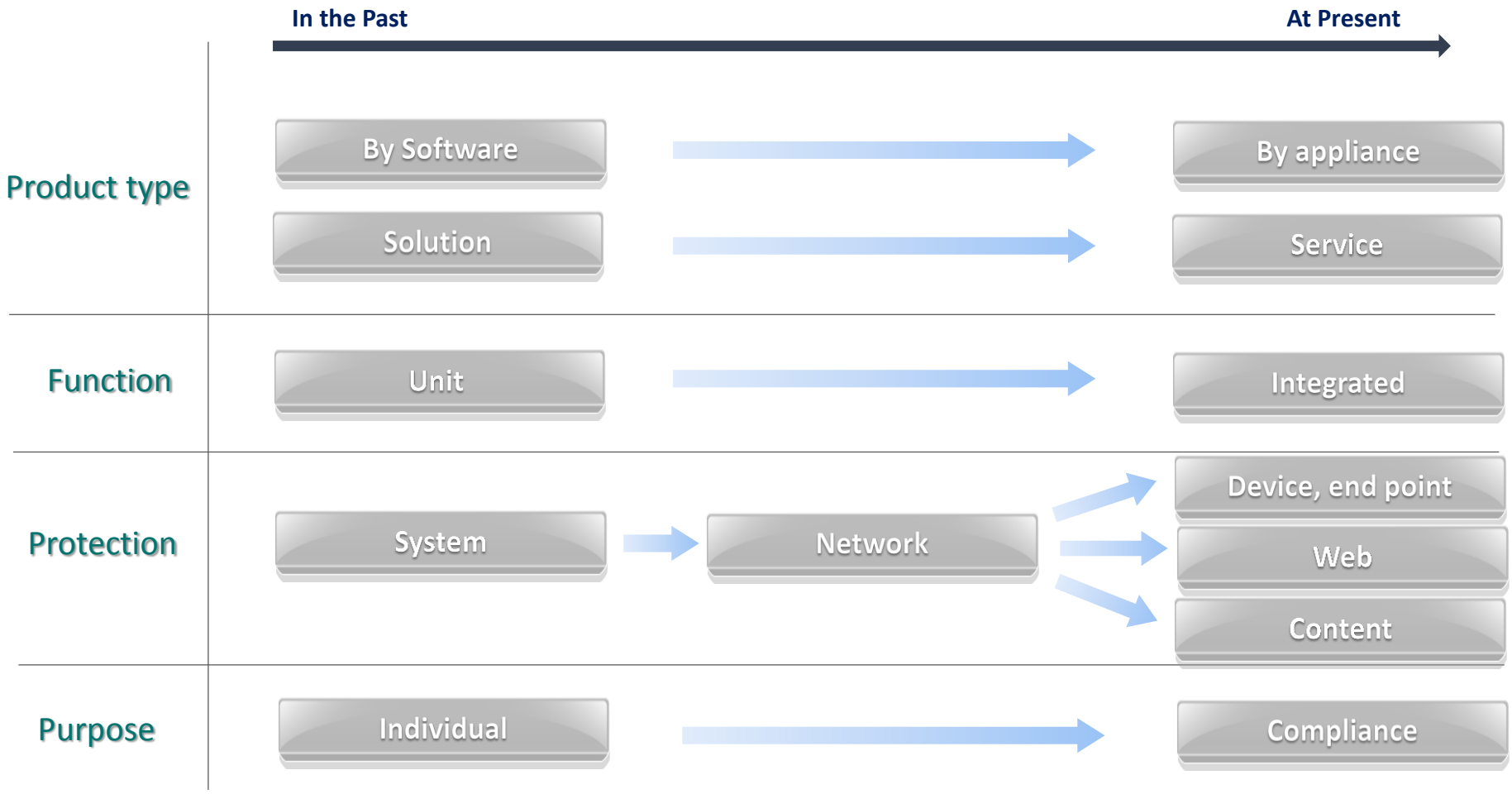
Cyber Security Trend

DDoS Attack on Egypt : 20th Sep 2016



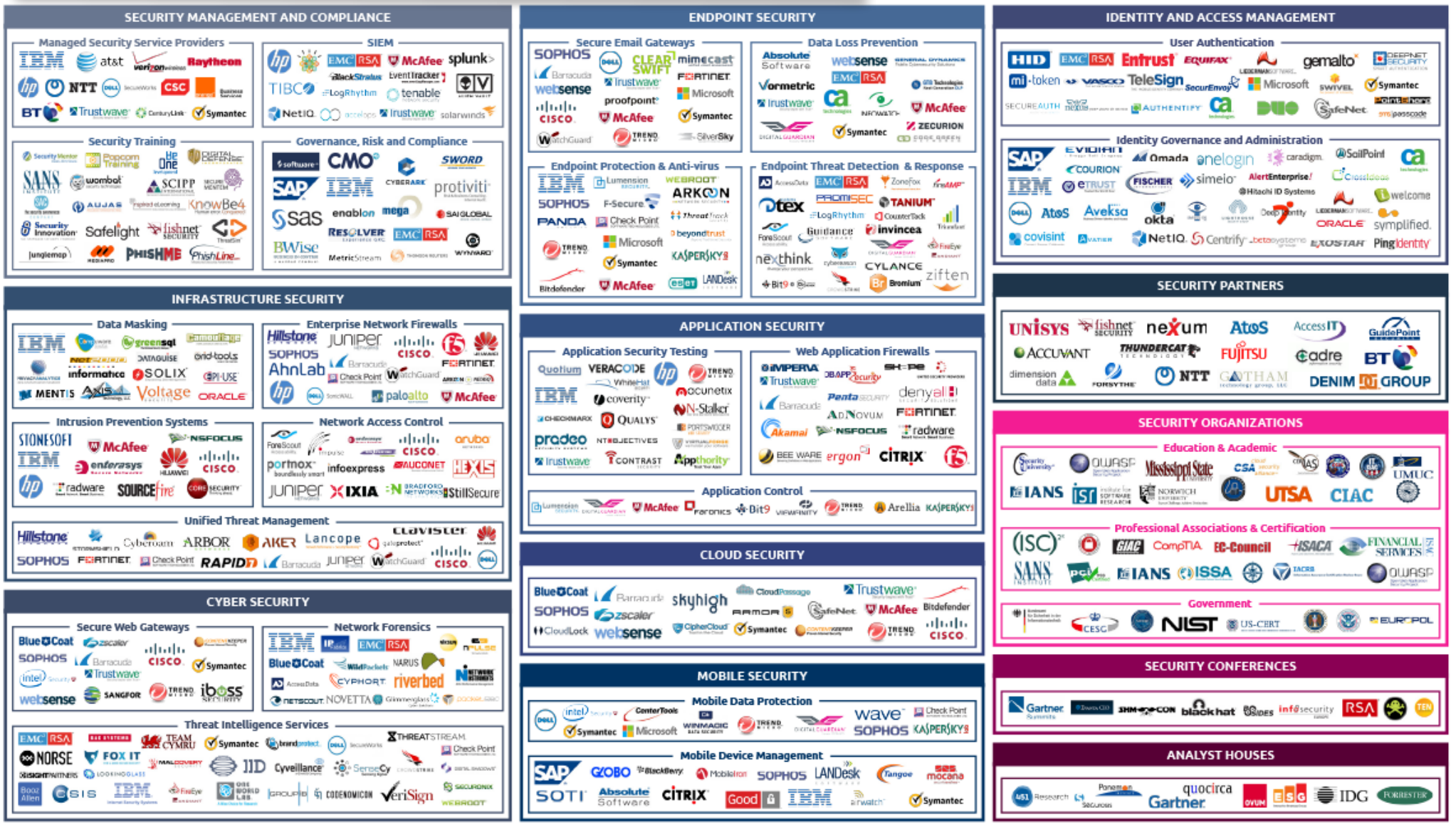
Cyber Security Trend

Cyber Security Technology Trend



Cyber Security Trend

Cyber Security Technology Industry



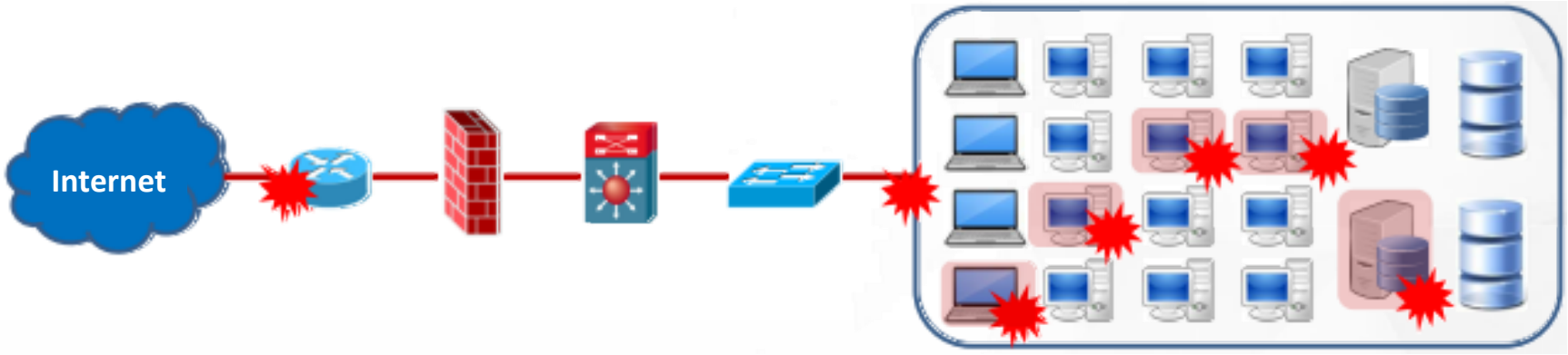
Cyber Attack Paradigm Shift

"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.

CONTENTS

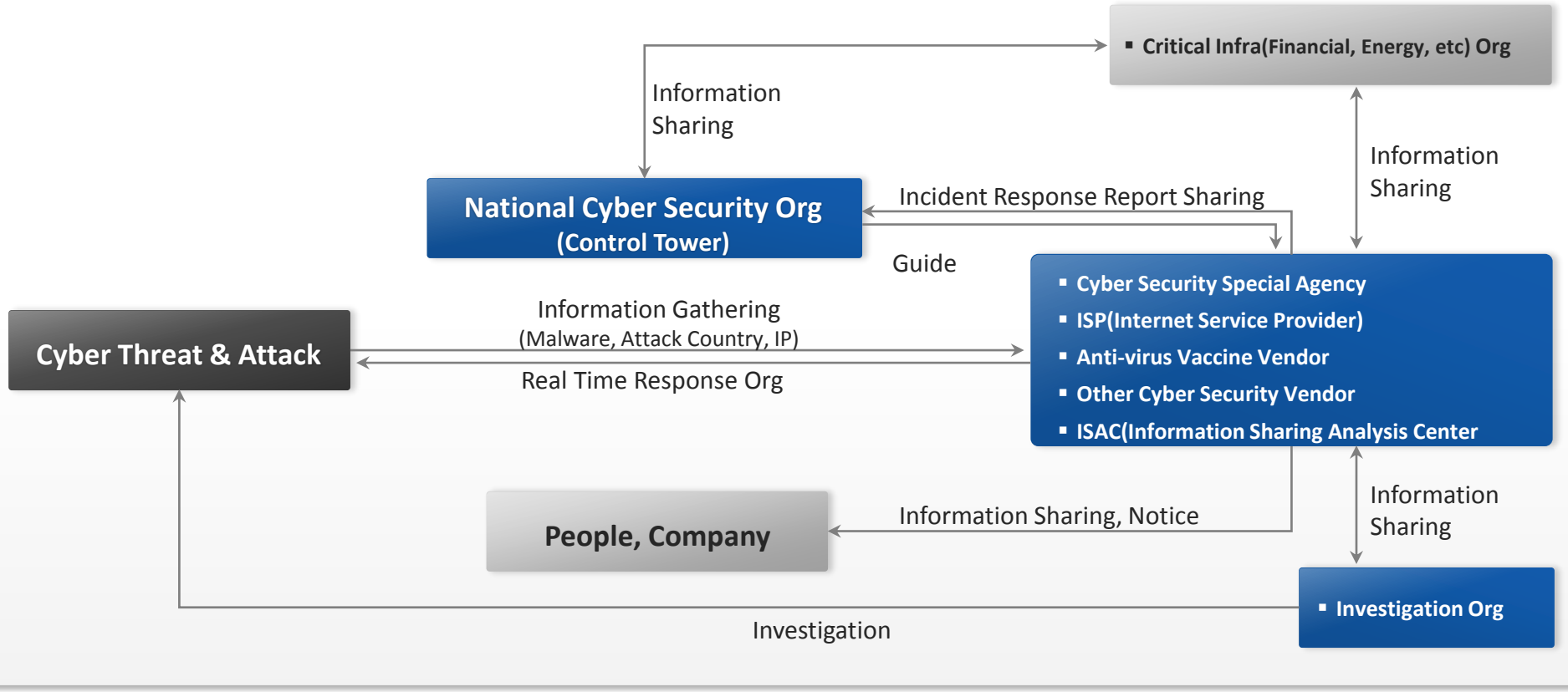
Cyber Security Response

DUZON

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.**



Cyber Security Response

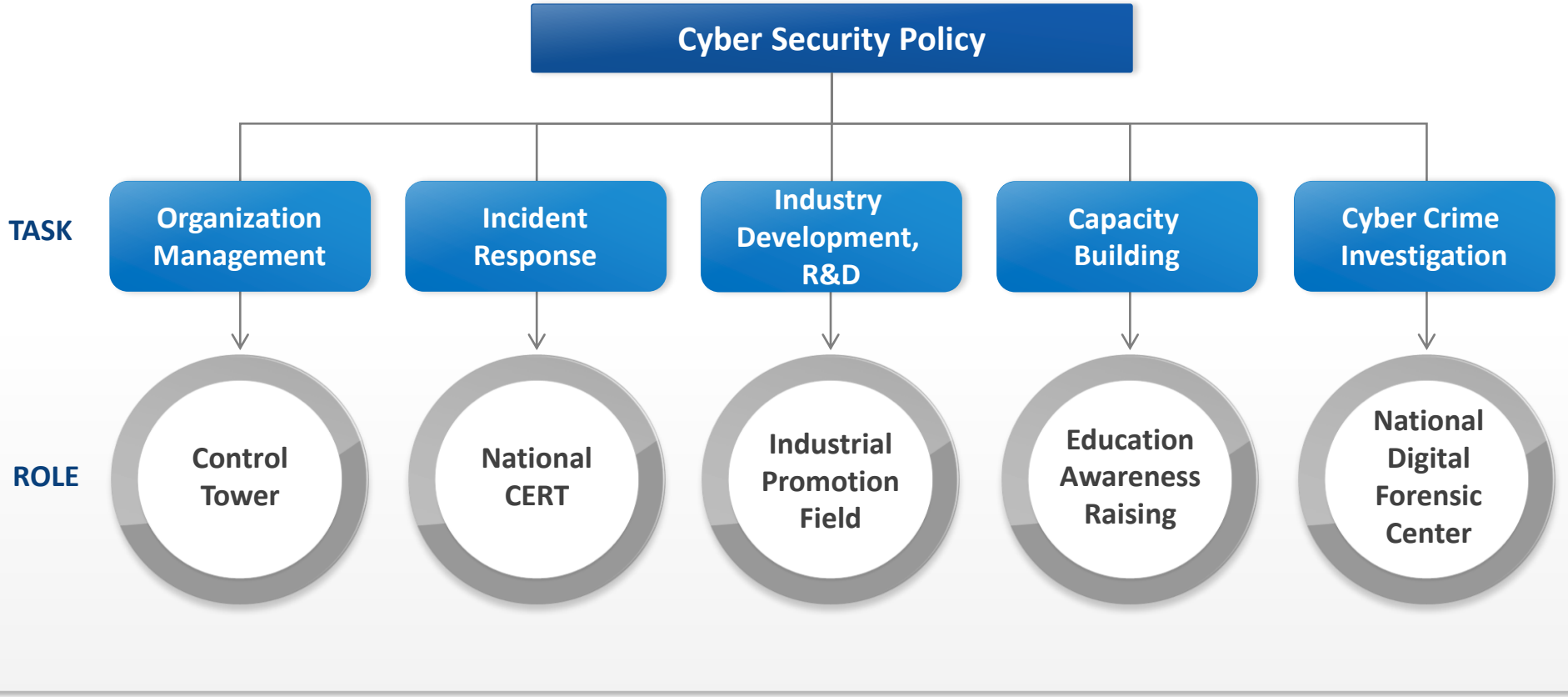
Organization by Role & Responsibility

☑ **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.**

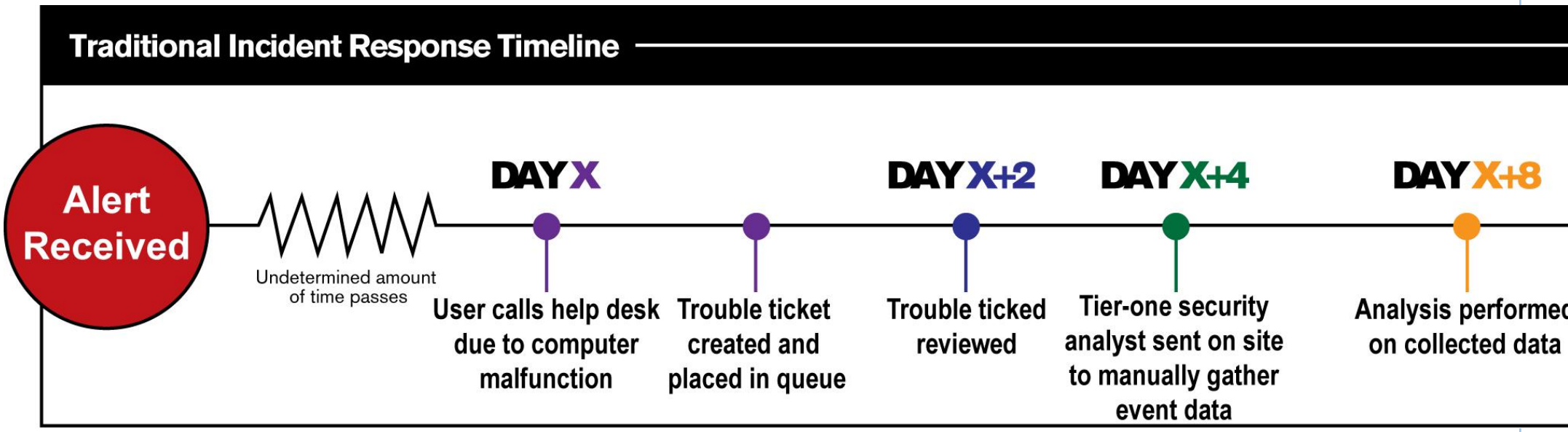
Cyber Security Response

Organization by Policy

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

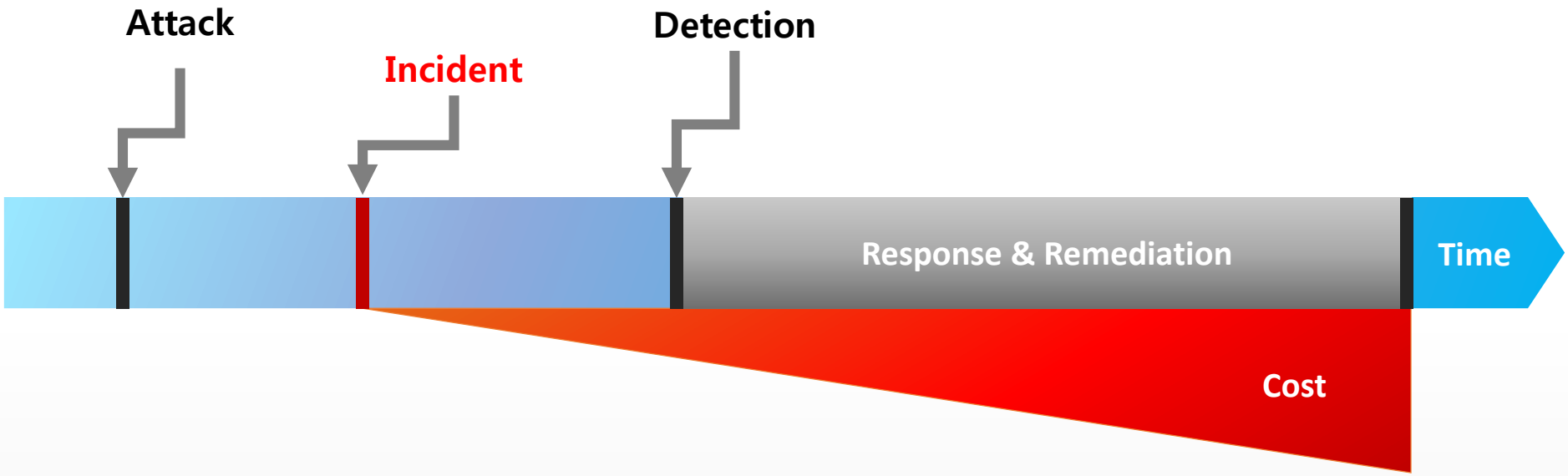


Traditional Incident Response Timeline



Cyber Security Response

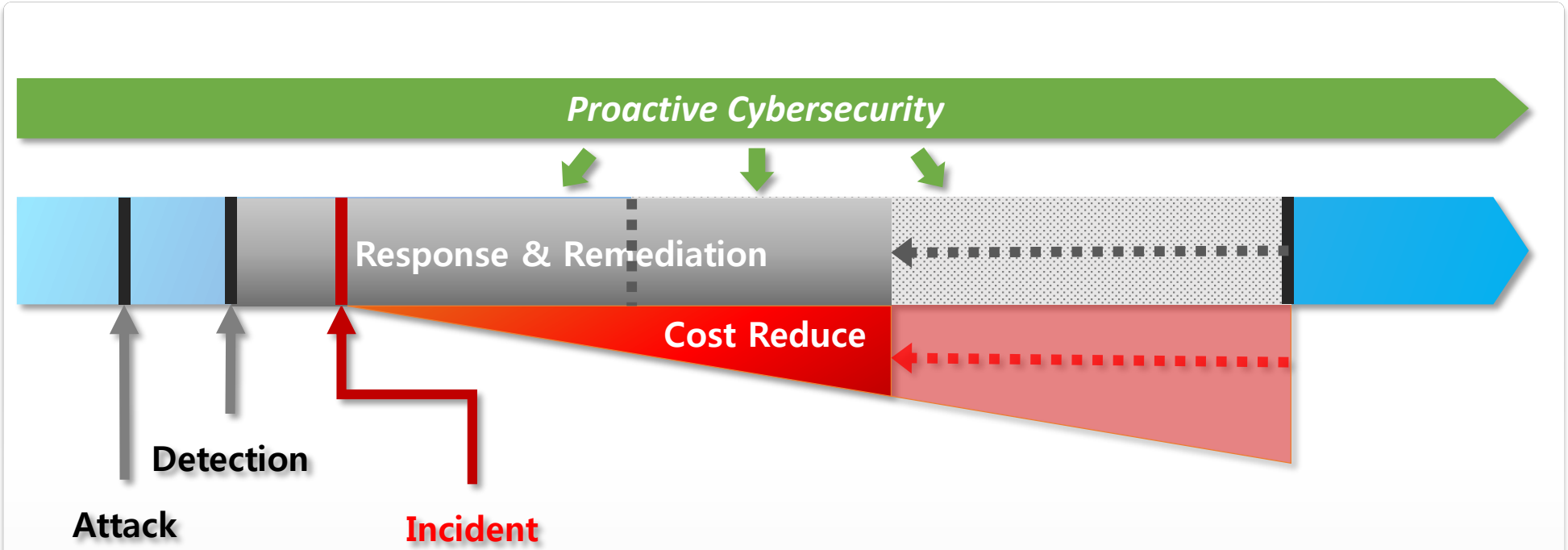
Incident Metrics



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

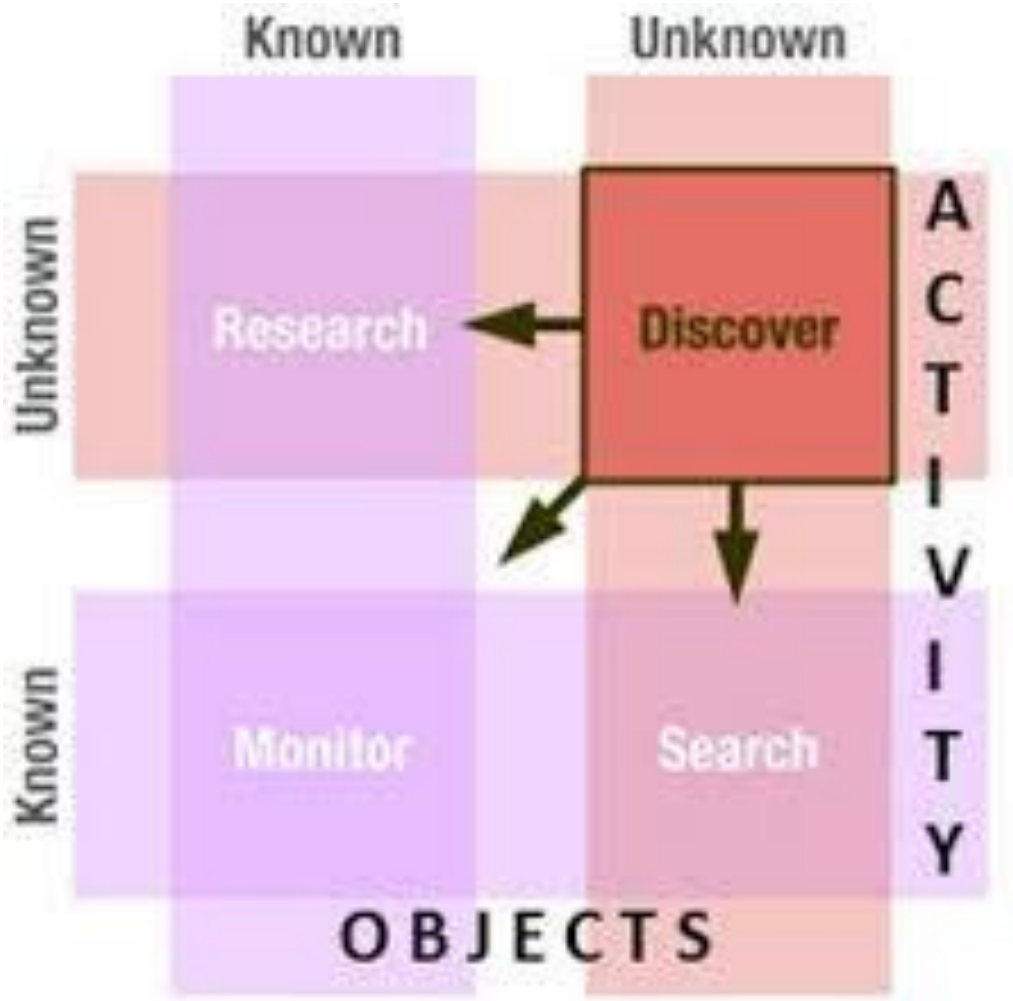
Cyber Security Response

Incident Metrics



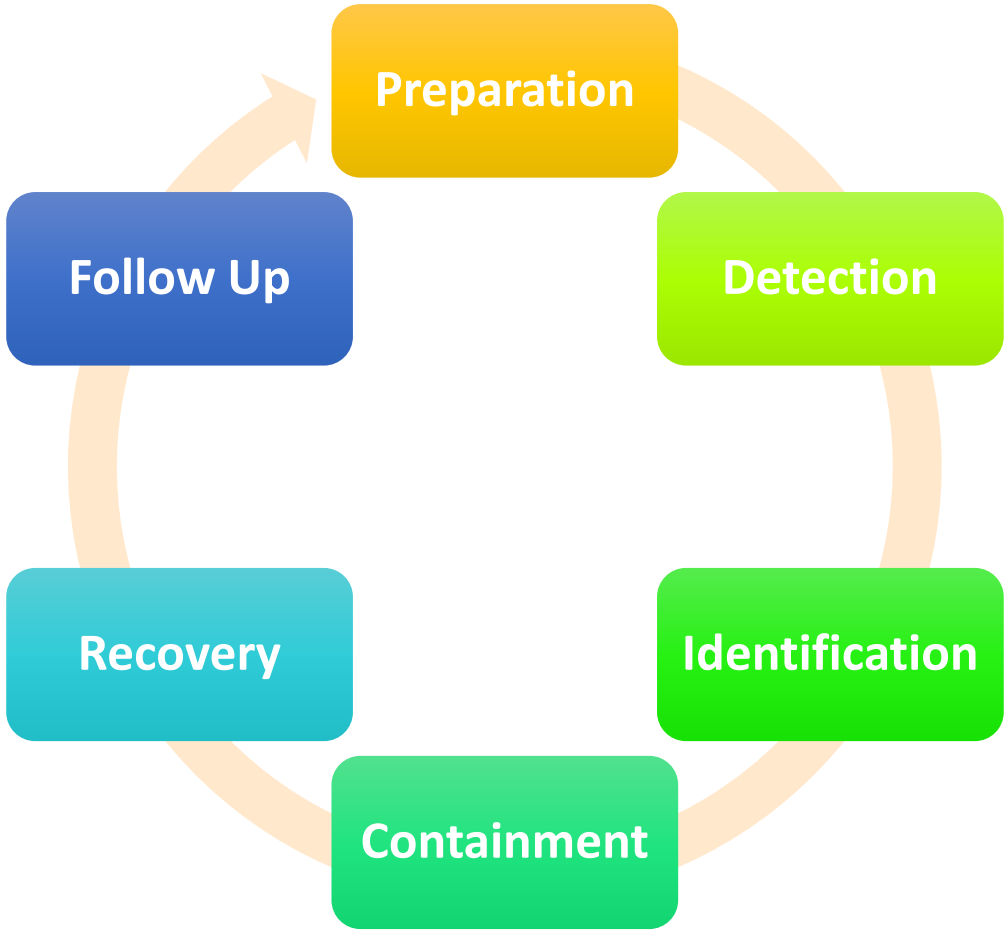
Successful proactive approach detecting the attack before incident will reduce total cost

Detection : Discover, Search, Research, Monitor



Cyber Security Response

Identification and Containment



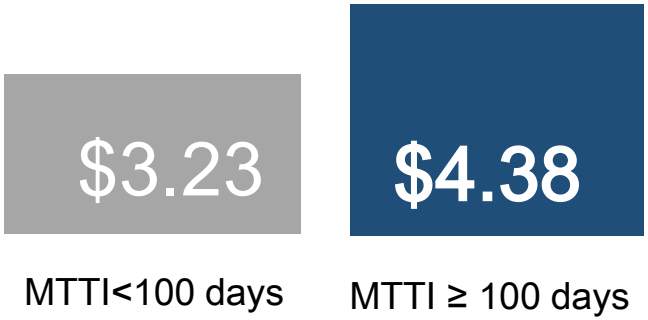
Identification requires 100% accuracy through Digital Forensics

MTTI and MTTC

Mean time to identify (MTTI)

The time it takes to detect that an Incident has occurred

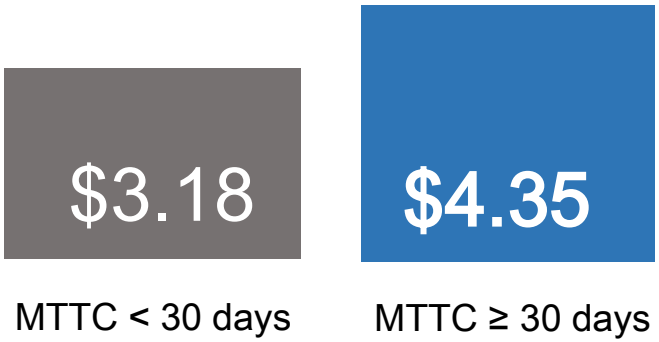
(total cost, in millions)



Mean time to contain (MTTC)

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

(total cost, in millions)



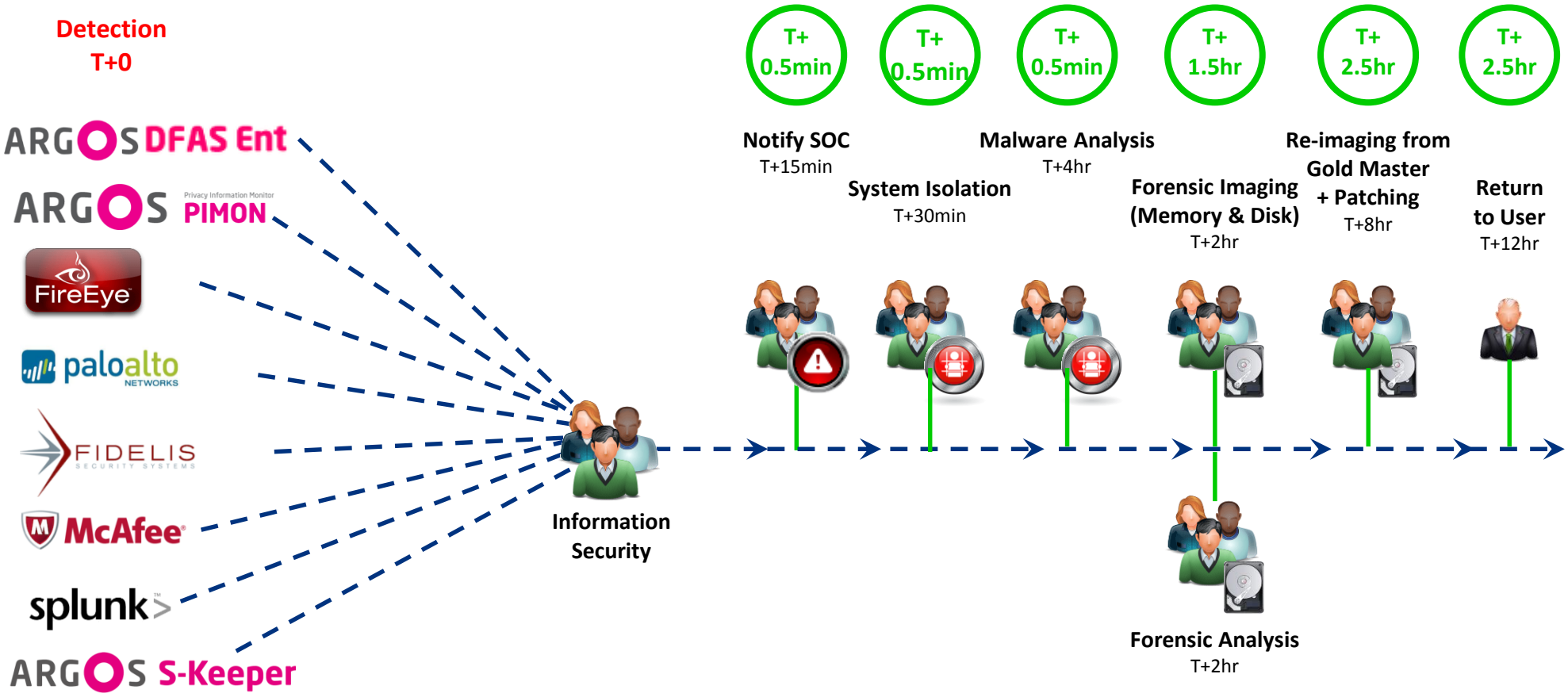
※ source : 2016 Cost of Data Breach Study : Global Analysis / Ponemon
※ source : http://www.slideshare.net/ibmsecurity/the-2016-ponemon-cost-of-a-data-breach-study

Digital Forensics for Identification/Containment

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.

Cyber Security Response

Combining Proactive and Reactive Response



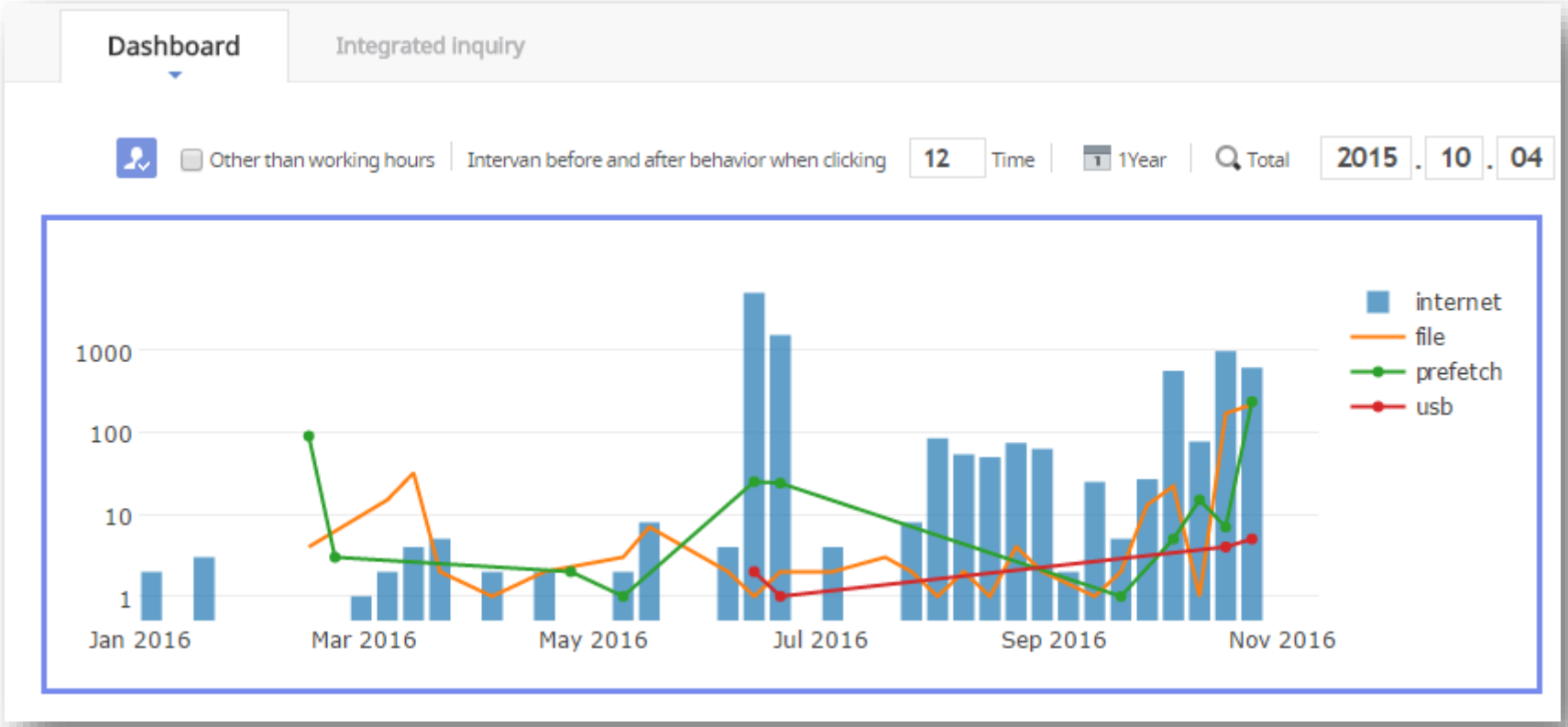
Remote Digital Forensics

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

Monitor	High-Risk Monitoring ex) Reinstall OS, Delete disk…
Alert	Notification for Unauthorized Action
Audit	Selective Audit (Collecting the data)
Analyze	Analysis the data
Report	Automatically generated reports

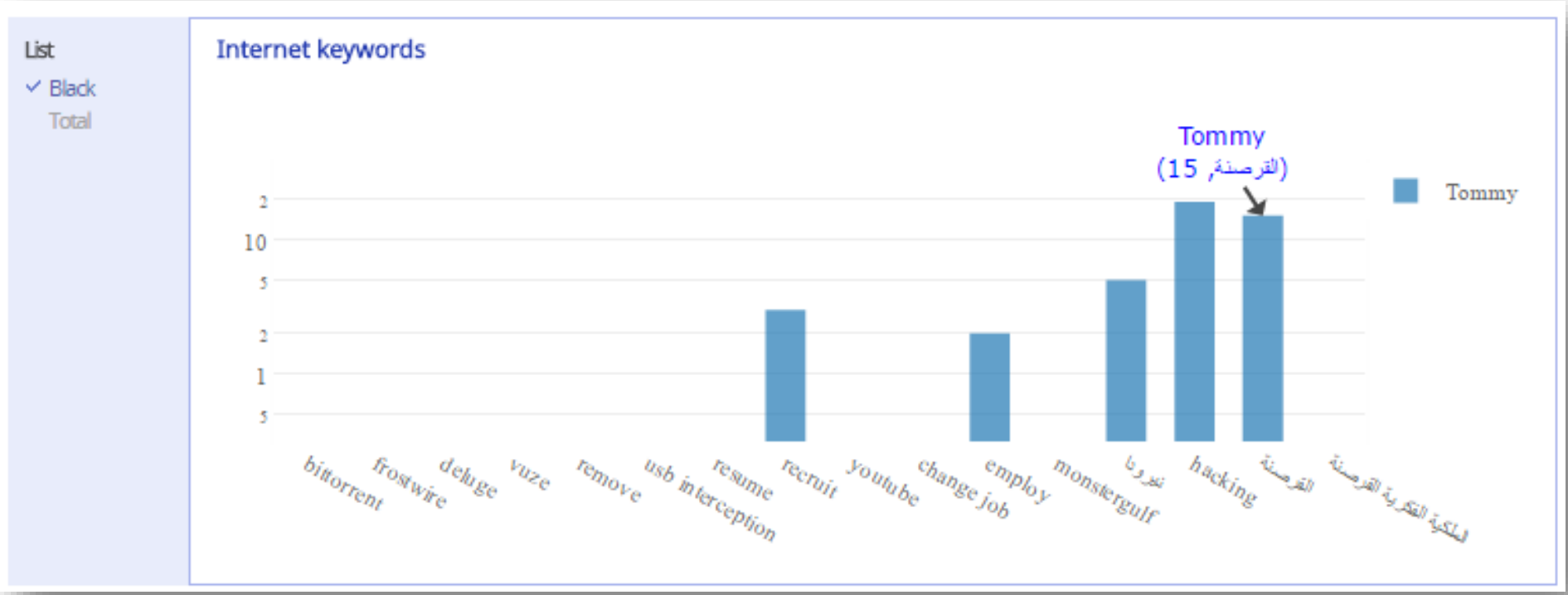
Case Study

Endpoint User Activity



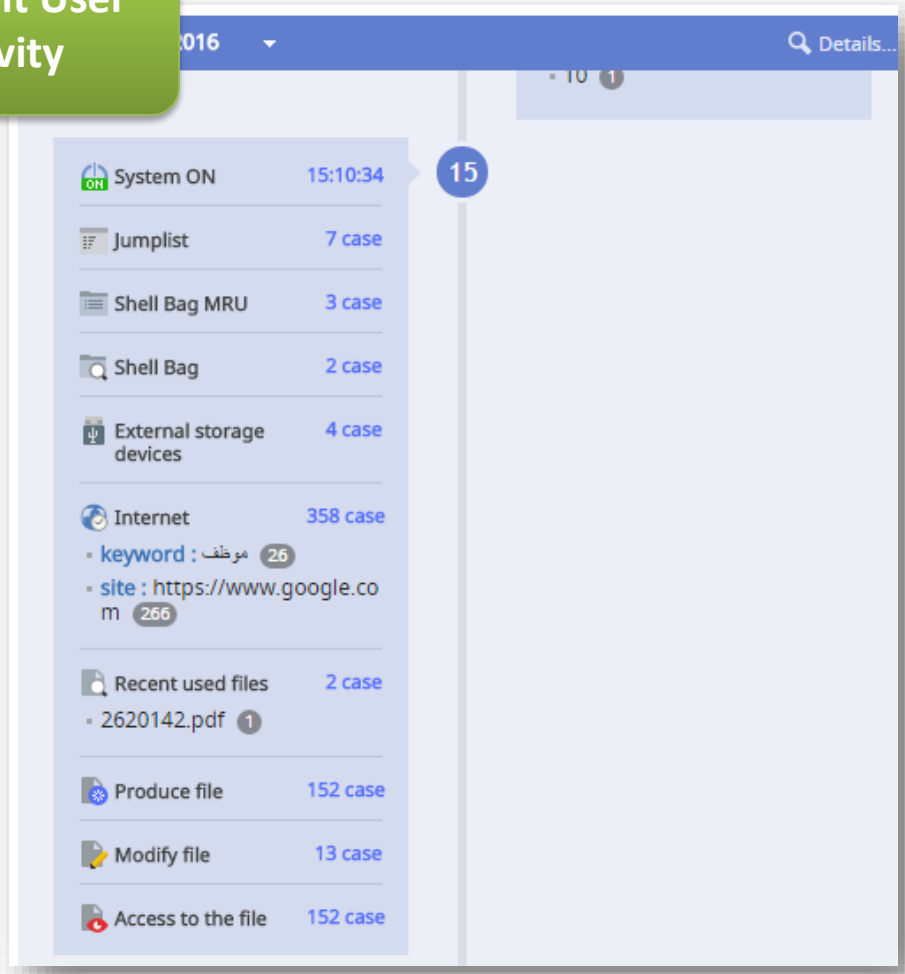
Case Study

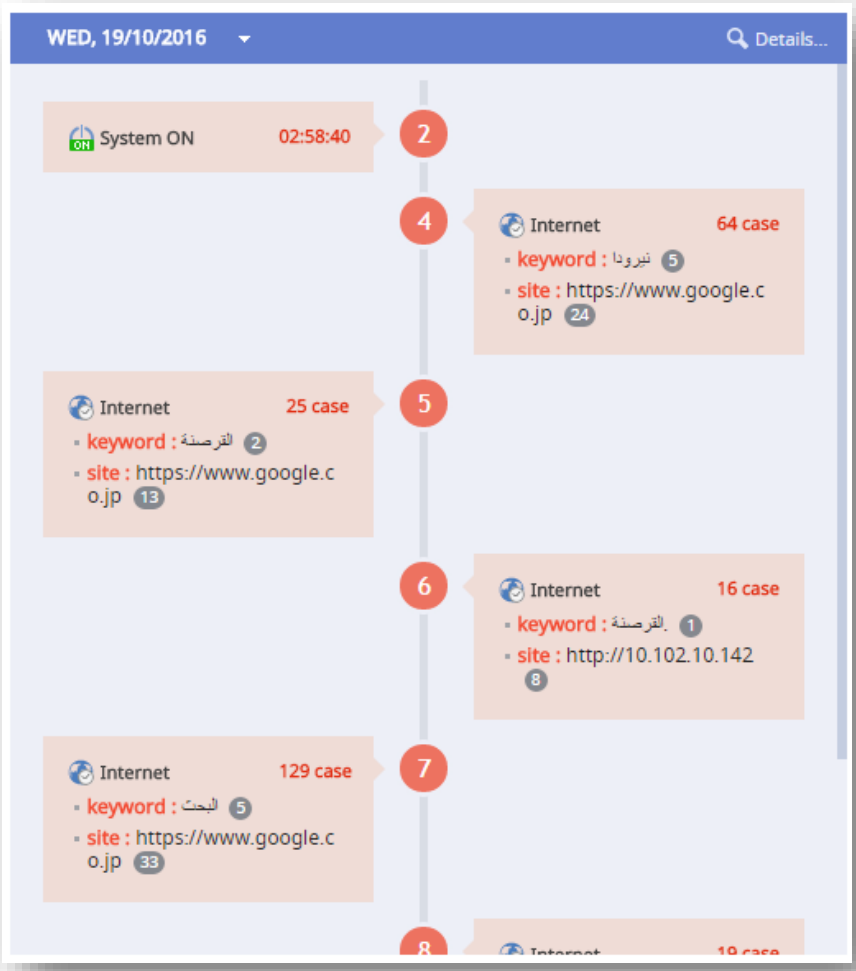
Endpoint User Activity



Case Study

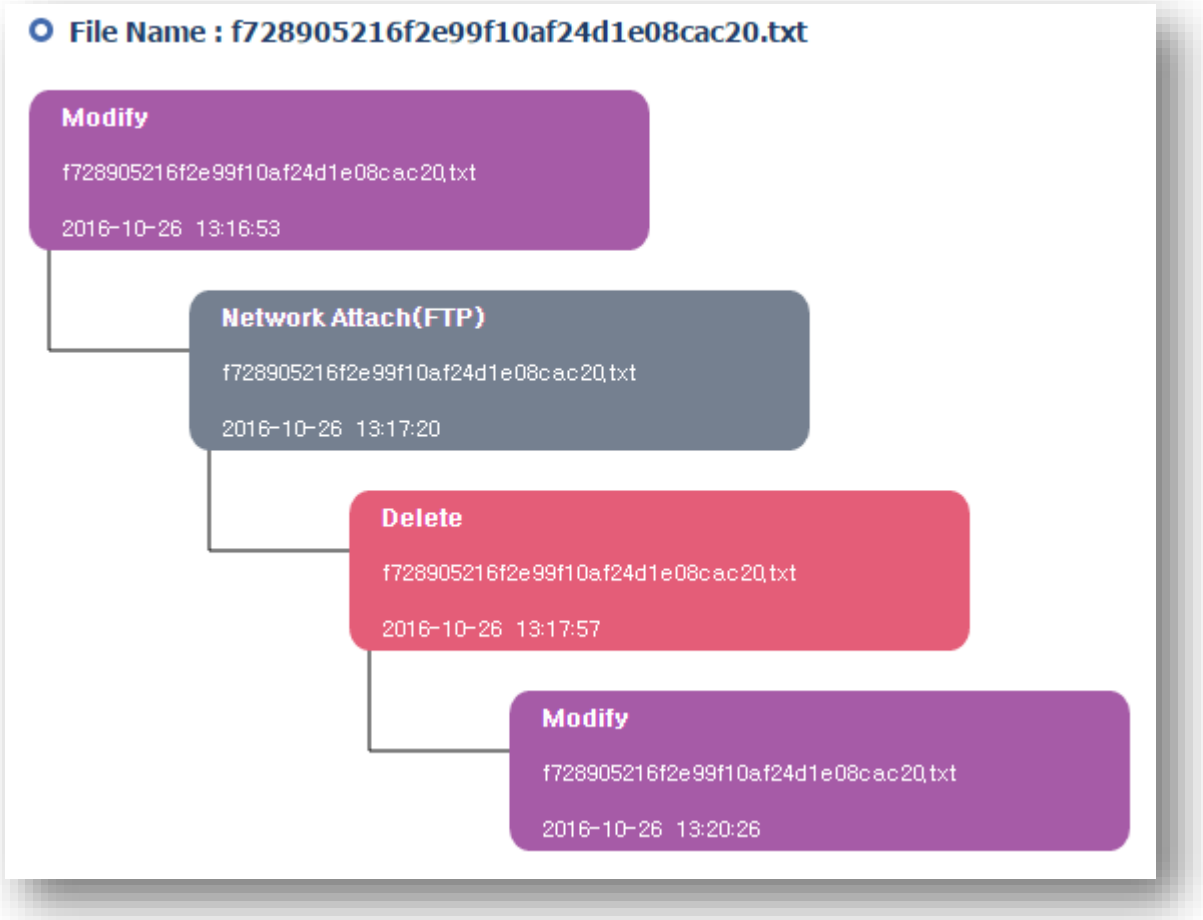
Endpoint User Activity





Case Study

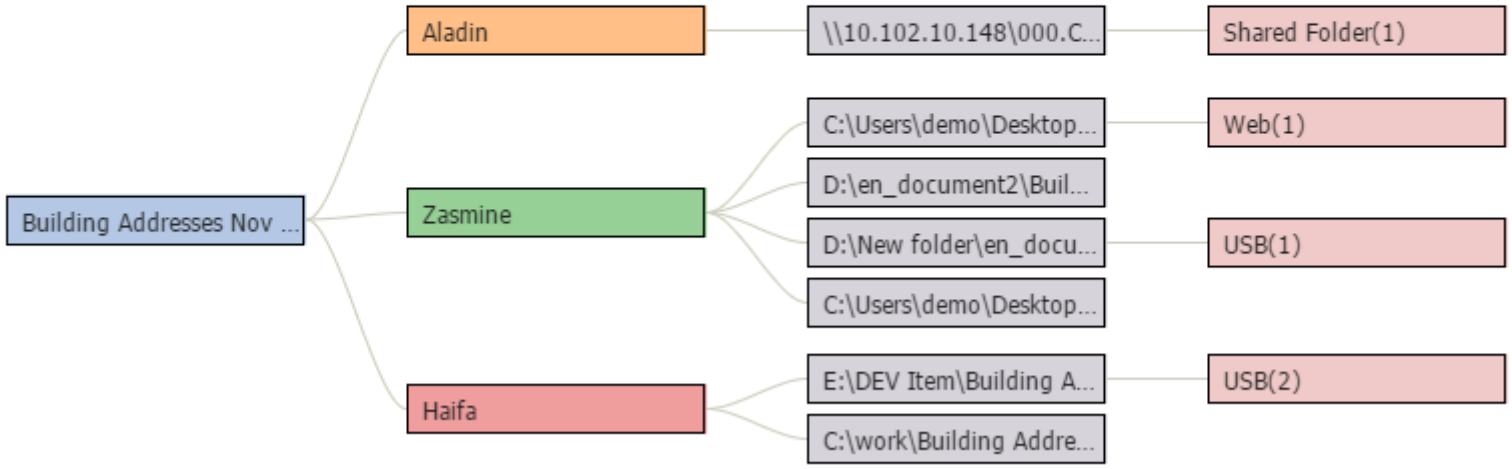
Breach Detection



Case Study

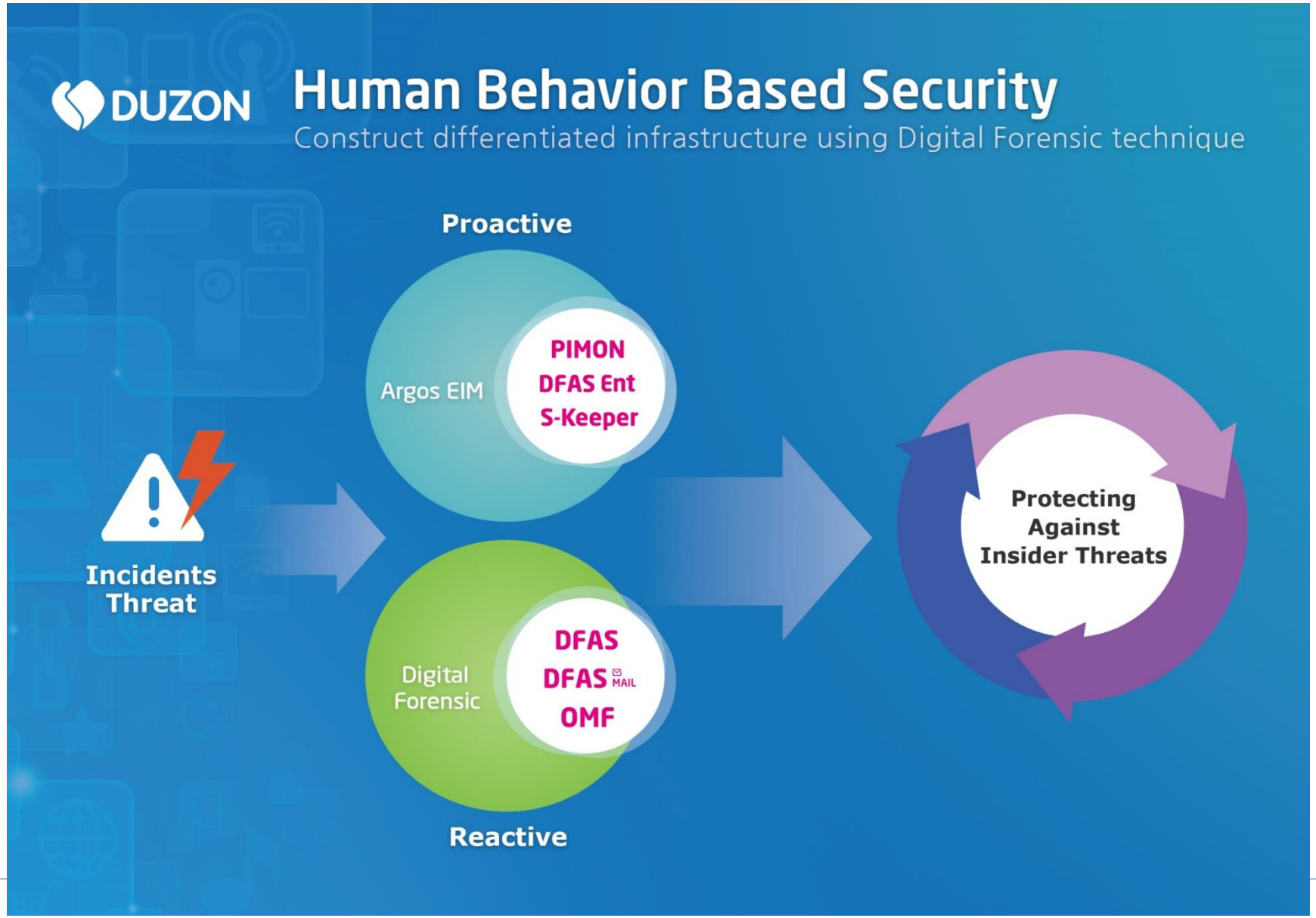
Breach Detection

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



Cyber Security Response

Incident Detection



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

About Duzon

Oman NDFL Project

شكرا جزيلا

http://www.d-forernsic.com

forensic@duzon.com

DUZON

Duzon Forensic Center
E-mail : forensic@duzon.com