

CYBERSECURITY AND CRITICAL INFRASTRUCTURE

Erka Koivunen @ekoivune
Cyber Security Advisor



VIEWPOINTS TO “CRITICAL”

- Critical Infrastructure Vulnerabilities
 - Critical Dependencies
 - Immature Technology
 - Unnecessary Exposure to threats
 - Target of Deliberate Attacks
- Building Resilience
 - Adopting a Hacker Mindset
 - Knowing Your Enemies
 - Assume Breach
- From Defender's Dilemma to Attacker's Dilemma
- Mandatory Breach Notification

CRITICAL INFRASTRUCTURE VULNERABILITIES



Une panne informatique à l'aéroport d'Orly liée à... Windows 3.1

Le Monde.fr | 11.11.2015 à 14h41 • Mis à jour le 11.11.2015 à 17h04 |

Par Morgane Tual

Abonnez vous à partir de 1 €

👉 Réagir ⭐ Classer 🖨️ ✉

f Partager

🐦 Tweeter



Des milliers de passagers – dont le maire de Bordeaux Alain Juppé – ont été cloués au sol samedi 7 novembre à l'aéroport d'Orly.



DÉCOUVREZ LA NEWSLETTER PIXELS

Chaque semaine, retrouvez l'essentiel de l'actualité « techno » en vous inscrivant à la newsletter Pixels.

Adresse email



☐ Recevoir les informations du Monde

Je m'inscris

Les plus partagés

- 1 Un « triste spectacle » à l'Assemblée, quatre jours après les attentats 16835
- 2 Les restaurateurs se mobilisent pour que Paris reste une fête 9057
- 3 Jonah Lomu, icône néo-zélandaise du rugby, est mort 8165
- 4 Au moins deux morts dans l'assaut à Saint-Denis 7316
- 5 Angela Merkel refuse de se voir en cheffe de guerre 5601

Suivez-nous





BANKING AND FINANCE

European Commission > Banking and finance > Payment Services > Single Euro Payments Area (SEPA)

[Home](#)

Payment Services

[News](#)

[Legislation](#)

[Single Euro Payments Area \(SEPA\)](#)

[Who will benefit, and how?](#)

[Questions and answers](#)

[SEPA Council](#)

[Commission's role](#)

[ECB and EPC](#)

[Card, internet and mobile payments](#)

[Directive on Payment](#)

Single Euro Payments Area (SEPA)

- [What is SEPA?](#)
- [What are the benefits?](#)
- [SEPA Regulation](#)
- [SEPA: a collaborative work](#)
- [SEPA Migration](#)

What is SEPA?

The Single Euro Payments Area (or "SEPA" for short) is where more than 500 million citizens, over 20 million businesses and European public authorities can make and receive payments in euro under the same basic conditions, rights and obligations, regardless of their location.

The introduction of the euro has helped to make cash payments anywhere in the euro area just as easy as at home. But until recently it was not so easy to pay for goods or services electronically in another euro area country, for example with your bank debit card - a



Search on this site



Deadline for SEPA migration

The SEPA Regulation adopted in 2012 set 1 February 2014 as the end-date for the migration to SEPA in the Eurozone. However, as the migration rates for credit transfers and direct debits were not high enough to ensure a smooth transition to SEPA, the Commission adopted a proposal to introduce an additional transition period of six months - until 1 August 2014.

[More information](#)

13/06/2014
23.30.51

CENTRALE IDROELETTRICA DI ABBADIA S.S.

HOME

Utente

Logout

kW **408,3** kVAR **45,0**Hz **50,02** CosFi **0,96**V1 **748**I1 **339,6**V2 **708**I2 **331,2**V3 **743**I3 **334,4**Gruppo VELOCITA' **997**
1001,31Vibrazioni **3,4**

61 quest. reggipinta

41 quest. 1 gen.

acc. 1 **80** **70**acc. 2 **60** **60**acc. 3 **60** **70**

40 quest. 2 gen.

99,0

44,0

43,7

spina 1

regolo pres. olio **92**

Sessante sponsorizzate

Questa era una sessione gratuita sponsorizzata da www.tegview.com.

Le sessioni di Tegnview sono gratuite esclusivamente per utilizzi non professionali.

Grazie per la correzione!

Vi piace

Acquista licenza

OK

Linea V1 **16010** I1 **0,0**V2 **16102** I2 **0,0**V3 **16074** I3 **0,0**Pot **0,0**Rea **-0,0**Cos fi **0,99**Freq **50,02**Tratto gruppo imposta
spina
manualeby-pass per prova teste Partello Portata l/s **159,6**livello **777,064** SET + **777,100** SET - **777,060**Pressione Condotta **285,6** Turbina **280,3**Rendimento **+0,881**

ON/OFF

STOP

RESET

AUT. MAN.

AUTOMATICO

LOCALE

REMOTO

HOME

GENERATORE

TURBINA

PARAMETRI

ARCHIVIO ALLARMI

ALLARMI 4TH

PRODUZIONE

Tutti i giorni

Pagina servizi base



115 batshit stupid things you can put on the internet in as fast as I can go by Dan Tentler



DEVONX PR
20 YEARS OF JAVA
JUST THE BEGINNING

~~100-115~~ 121 batshit stupid things
you can put on the internet
in as fast as I can go, someone
get me a drink.

With your host:
Viss



OX
IUM



0:17 / 1:03:18





Search Twitter



Have an account? Log in



Erka Koivunen

@ekoivune



Follow

Q: How to abbreviate Industrial Devices and Internet of Things without stealing light from an old IoT joke?

Asking for friend. @mikko

RETWEETS

10

LIKES

11



7:52 AM - 18 Jan 2016



10



11

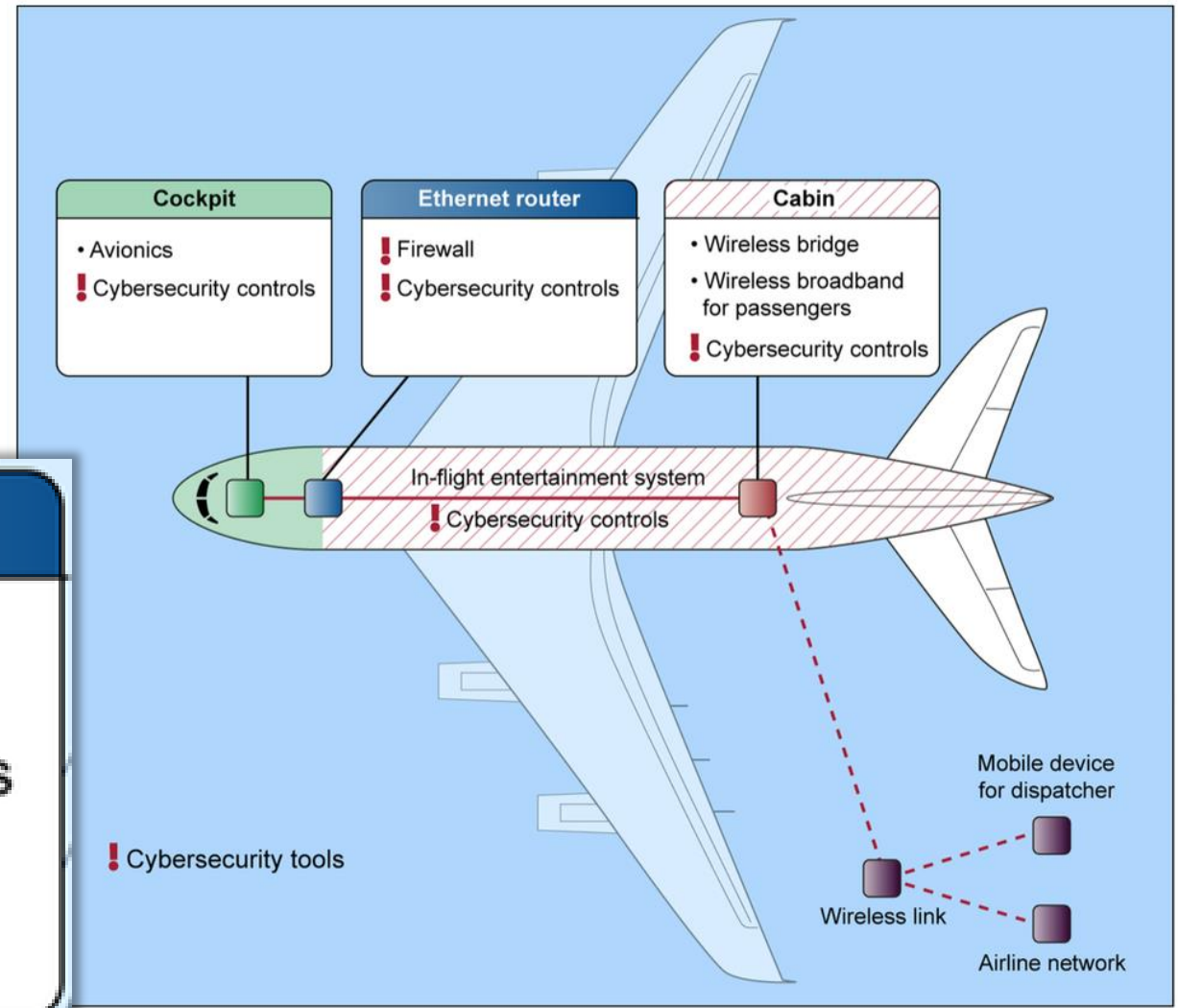


April 2015

AIR TRAFFIC
CONTROLFAA Needs a More
Comprehensive
Approach to AddressC
A
N

Ethernet router

- ! Firewall
- ! Cybersecurity controls

Figure 4: Aircraft Diagram Showing Internet Protocol Connectivity Inside and Outside of Aircraft

Source: GAO. | GAO-15-370

Heist 1

Bangladesh → Philippines
\$81 Million dollars

Heist 2

Unknown bank
Unknown amount

Heist 3

Ecuador → Hong Kong
\$12 Million

Heist 4

Vietnam → Slovenia
Failed

Heists 5 →
Ukraine → ?



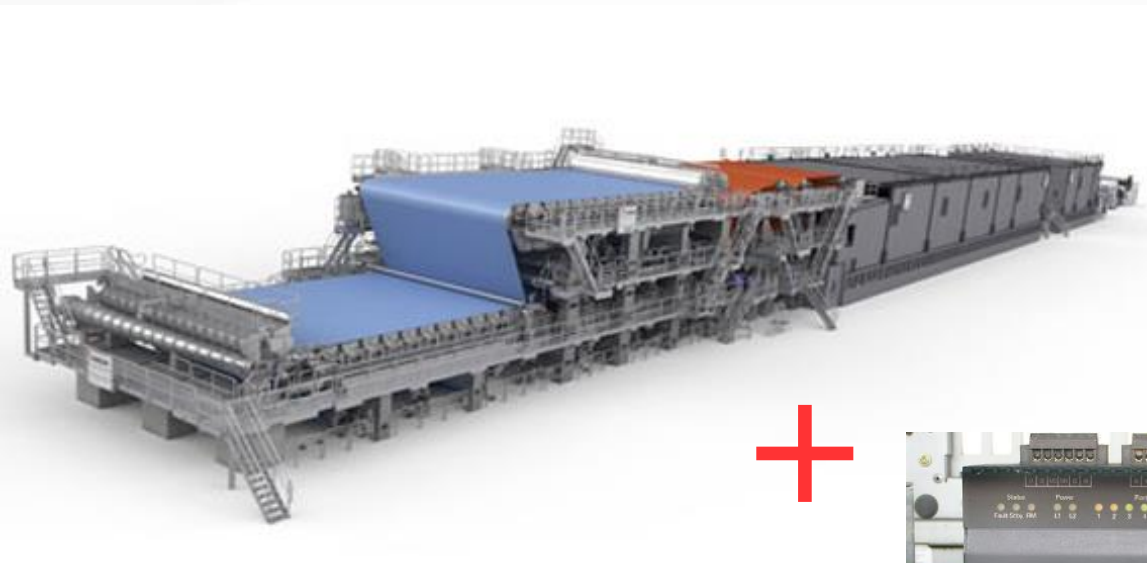
PRYKARPATTYA OBLENERGO





BUILDING RESILIENCY





INDUSTRIAL CONTROL SYSTEMS

CORPORATE IT



**WE ARE NO LONGER
SECURING
COMPUTERS,
WE ARE SECURING
SOCIETY**

HACKING
IS AN ATTACK
AGAINST
ASSUMPTIONS

Eye of the Tiger

WOT WEISS

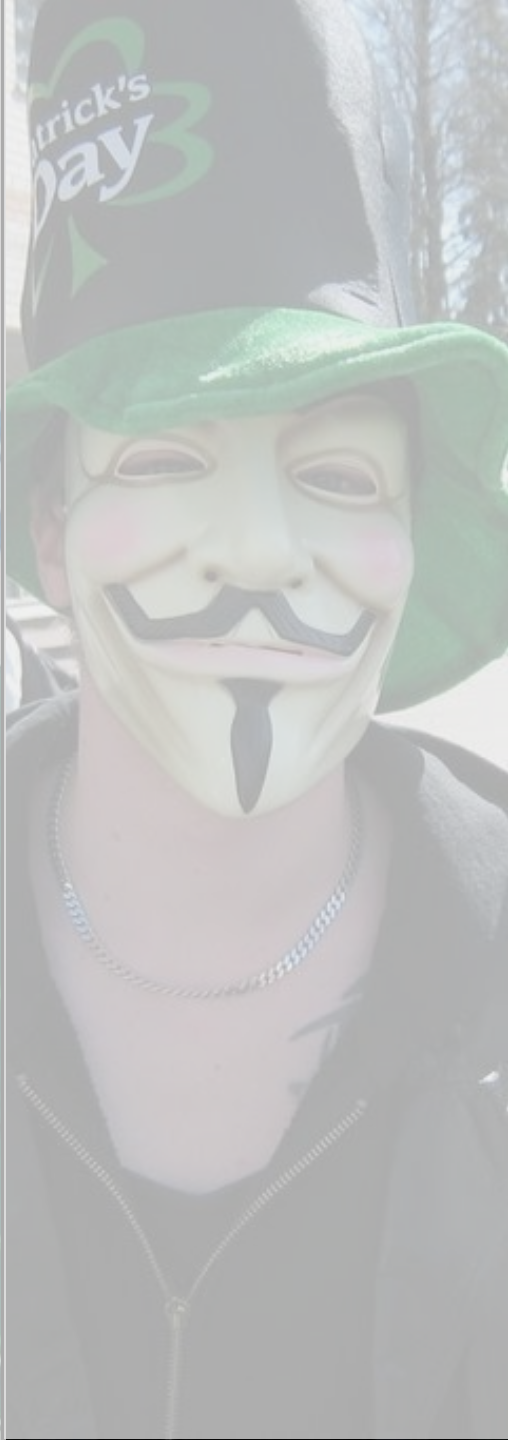
7753

• Genuine EPSON ribbon cartridge recommended

• All warranties are voided if not used



KNOW YOUR ADVERSARIES





ASSUME BREACH

PREPARE FOR THE INEVITABLE



An aerial photograph of a city, likely New York City, with a network of lines and dots overlaid, suggesting a digital or communication network. The text 'DEFENDER'S DILEMMA?' is prominently displayed in the center in a bold, red, sans-serif font. Faint, semi-transparent IP addresses are visible in the background, including '160.120.20.2', '126.5.68.5', '56.80.21.10', and '38.20.20.5'.

DEFENDER'S DILEMMA?

DEFENDERS: STOP FEELING PITIFUL

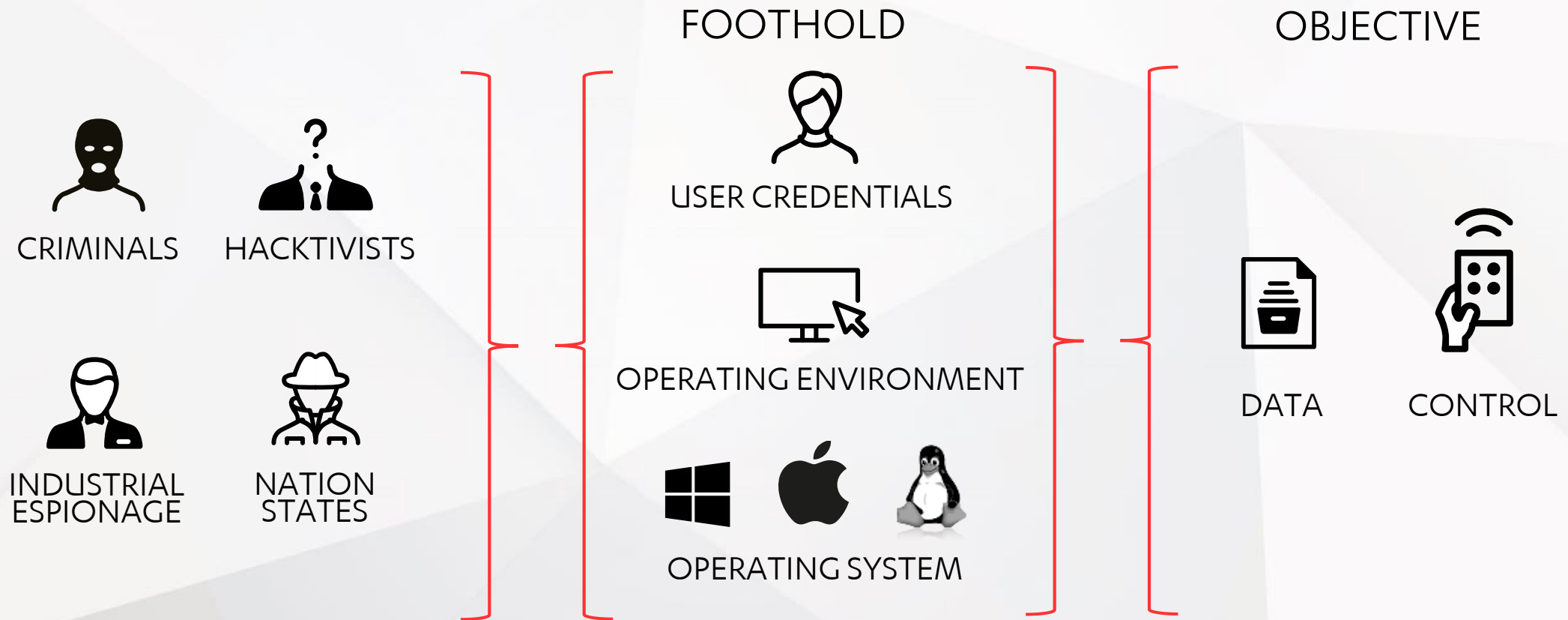
■ DEFENDER'S DILEMMA

- The intruder only needs to **exploit one of victim's vulnerabilities** in order to compromise the enterprise.

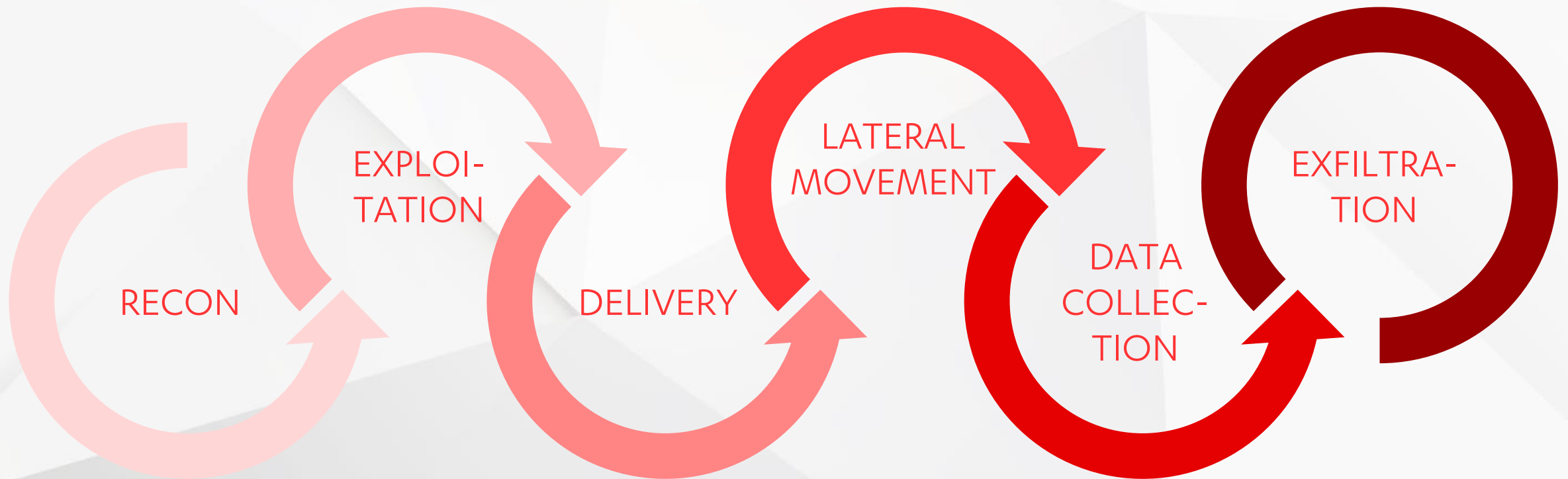
■ INTRUDER'S DILEMMA

- The defender only needs to **detect one of the indicators** of intruder's presence in order to initiate incident response within the enterprise.

LETS LOOK AT HOW ATTACKERS OPERATE AND WHAT THEY ARE AFTER



ATTACK IN STAGES



ATTACKERS WILL ALWAYS LEAVE FOOTPRINTS SOMEWHERE (SOMETIMES VERY SUBTLE ONES, THOUGH)



CRIMINALS



HACKTIVISTS



INDUSTRIAL
ESPIONAGE



NATION
STATES



USER CREDENTIALS



OPERATING ENVIRONMENT



OPERATING SYSTEM



USER LEVEL
FOOTPRINTS



APPLICATION
LEVEL FOOTPRINTS



NETWORK LEVEL
FOOTPRINTS



OPERATING
ENVIRONMENT
FOOTPRINTS



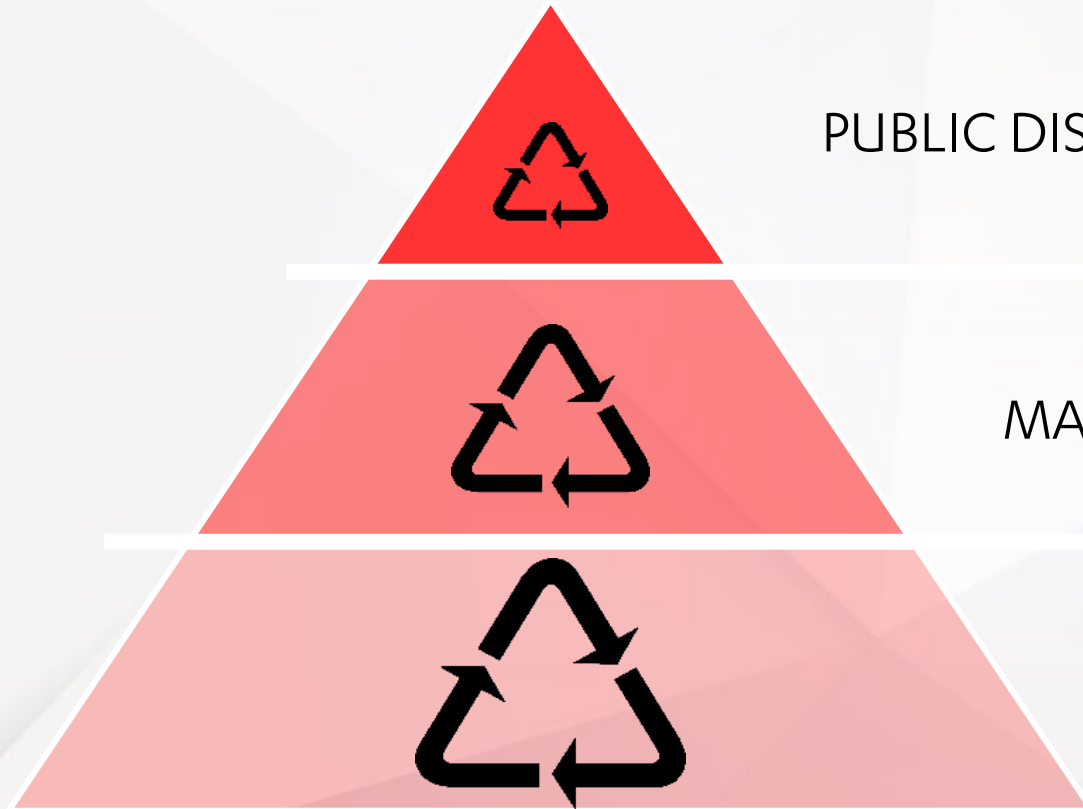
OS LEVEL FOOTPRINTS



MANDATORY BREACH NOTIFICATION



MANDATORY REPORTING



PUBLIC DISCLOSURE – Silence is Not an Option

MANDATORY REPORTING – Supervised by Authorities

MINOR BREACHES – Internal Incident Handling Process



F-Secure®