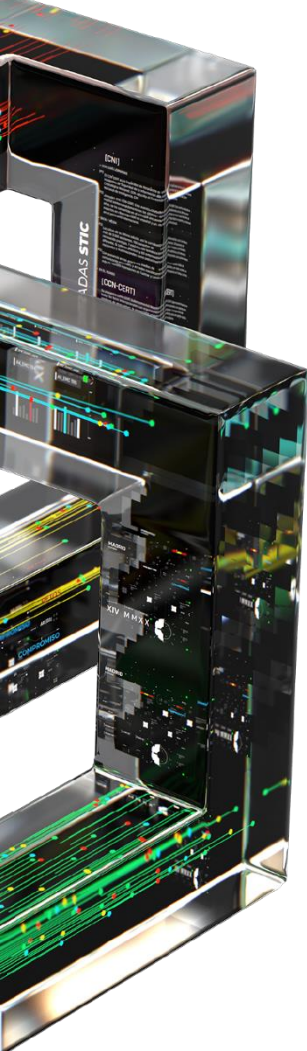
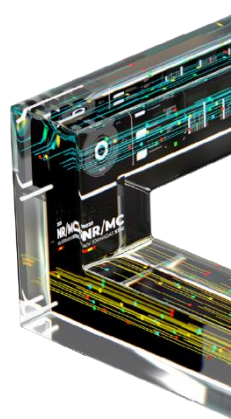




# #XIVJORNADASCCNCERT

## Ciber Resiliencia a través de Machine Learning



# Ciber Resiliencia a través de Machine Learning

**Ramsés Gallego**

**CISM, CGEIT, CISSP, SCPM, CCSK, ITIL, COBIT, Six Sigma Black Belt  
International Chief Technology Officer, Cybersecurity**

**Executive Vice President, Quantum World Association**

**Past International Vice President, ISACA, Board of Directors**

**Past President, ISACA Barcelona Chapter**

**Privacy by Design Ambassador, Government of Ontario, Canada**

**[ramses.gallego@microfocus.com](mailto:ramses.gallego@microfocus.com)**

 **@ramsesgallego**





# DIGITAL DISRUPTION







## Esto es Seguridad



## Esto es Resiliencia



**GESTIÓN DE IDENTIDAD Y GOBIERNO DE  
LOS ACCESOS**



**PROTECCIÓN DEL PUESTO DE TRABAJO**



**SEGURIDAD DE APLICACIONES**



**OPERACIONES DE SEGURIDAD**



**GOBIERNO DE LOS DATOS Y PROTECCIÓN**



**CONTROL DEL ENTORNO TI HÍBRIDO**

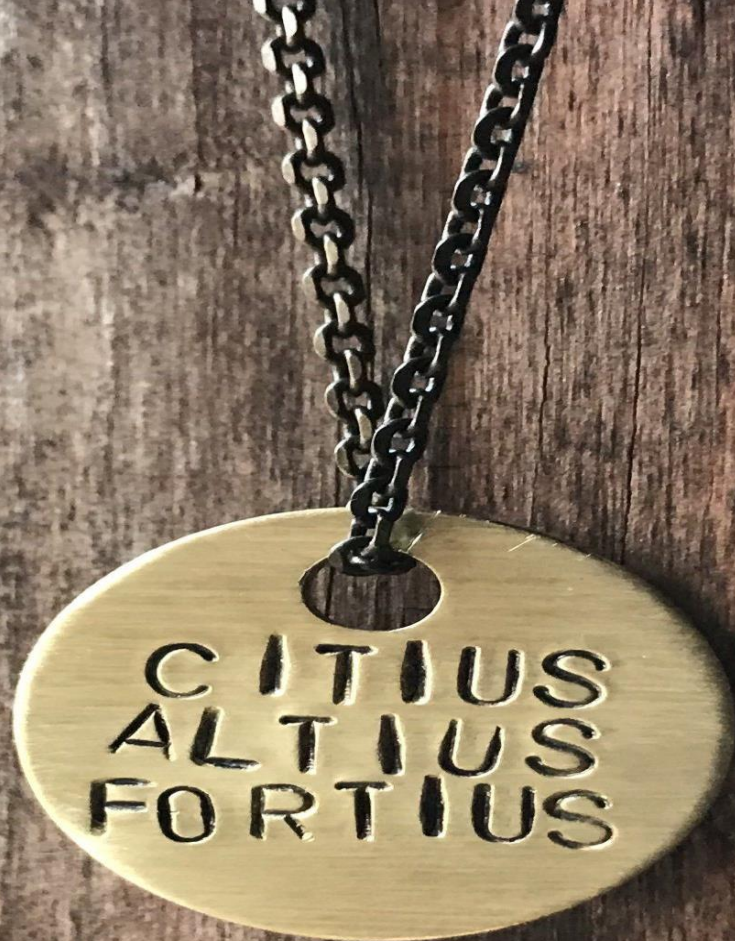


**ANÁLÍTICA Y MACHINE LEARNING**









CITIUS  
ALTIUS  
FORTIUS



- ✓ LEADERSHIP
- ✓ TEAMWORK
- ✓ COMMUNICATION



# INNOVATION



**MITRE**

**ATT&CK™**

Real-Time

ArcSight's next-gen SIEM platform is the fastest way to detect and escalate known threats. The advanced, multi-dimensional and flexible real-time correlation (RTC) engine powers intelligent rules and dashboards that can proactively detect relationships between events in near real-time. Using a wide range of correlation techniques, dynamic rules result in "detection" and "response" times reduced from days or hours to minutes.

Legend

Legend

Technique covered in default content

Technique covered in other content

Not covered content

| Initial Access<br>8           | Execution<br>28               | Persistence<br>13             | Privilege Escalation<br>10    | Defense Evasion<br>30         | Credential Access<br>7        | Discovery<br>9                | Lateral Movement<br>9          | Collection<br>6              | Command and Control<br>11     | Exfiltration<br>4             | Impact<br>4               |  |
|-------------------------------|-------------------------------|-------------------------------|-------------------------------|-------------------------------|-------------------------------|-------------------------------|--------------------------------|------------------------------|-------------------------------|-------------------------------|---------------------------|--|
| Drive-by Compromise           | CMSTP                         | Account Manipulation          | Bypass User Account Contr ... | Bypass User Account Contr ... | Account Manipulation          | Account Discovery             | Component Object Model an ...  | Clipboard Data               | Commonly Used Port            | Data Compressed               | Data Encrypted for Impact |  |
| Exploit Public-Facing App ... | Command-Line Interface        | Create Account                | DLL Search Order Hijackin ... | CMSTP                         | Brute Force                   | File and Directory Discov ... | Exploitation of Remote Se ...  | Data from Local System       | Communication Through Rem ... | Exfiltration Over Alterna ... | Inhibit System Recovery   |  |
| Hardware Additions            | Compiled HTML File            | DLL Search Order Hijackin ... | Exploitation for Privileg ... | Code Signing                  | Credential Dumping            | Network Sniffing              | Pass the Hash                  | Data from Network Shared ... | Connection Proxy              | Exfiltration Over Command ... | Network Denial of Service |  |
| Replication Through Remov ... | Component Object Model an ... | Hooking                       | Hooking                       | Compiled HTML File            | Credentials from Web Brow ... | Password Policy Discovery     | Remote Desktop Protocol        | Email Collection             | Data Encoding                 | Exfiltration Over Physica ... | Service Stop              |  |
| Spearphishing Attachment      | Control Panel Items           | Image File Execution Opti ... | Image File Execution Opti ... | Connection Proxy              | Hooking                       | Query Registry                | Remote File Copy               | Input Capture                | Domain Generation Algorit ... |                               |                           |  |
| Spearphishing Link            | Dynamic Data Exchange         | Kernel Modules and Extens ... | New Service                   | Control Panel Items           | Input Capture                 | Remote System Discovery       | Replication Through Remov ...  | Screen Capture               | Multi-hop Proxy               |                               |                           |  |
| Spearphishing via Service     | Execution through Module ...  | Local Job Scheduling          | Path Interception             | DLL Search Order Hijackin ... | Network Sniffing              | Security Software Discove ... | Third-party Software           | Multiband Communication      |                               |                               |                           |  |
| Valid Accounts                | Exploitation for Client E ... | Modify Existing Service       | Process Injection             | Deobfuscate/Decode Files ...  |                               |                               | Software Discovery             | Windows Admin Shares         | Remote Access Tools           |                               |                           |  |
|                               | Graphical User Interface      | New Service                   | Scheduled Task                | Disabling Security Tools      |                               |                               | System Network Configurati ... | Windows Remote Management    | Remote File Copy              |                               |                           |  |
|                               | InstallUtil                   | Path Interception             | Valid Accounts                | File Deletion                 |                               |                               |                                |                              |                               |                               |                           |  |
|                               | Local Job Scheduling          | Registry Run Keys / Start ... |                               | Image File Execution Opti ... |                               |                               |                                |                              |                               |                               | Web Service               |  |
| Mshhta                        | Scheduled Task                | Indicator Removal on Host     |                               |                               |                               |                               |                                |                              |                               |                               |                           |  |
| PowerShell                    | Valid Accounts                | InstallUtil                   |                               |                               |                               |                               |                                |                              |                               |                               |                           |  |
|                               | Regsvcs/Regasm                |                               |                               |                               | Masquerading                  |                               |                                |                              |                               |                               |                           |  |
|                               | Regsvr32                      |                               | Modify Registry               |                               |                               |                               |                                |                              |                               |                               |                           |  |
|                               | Rundll32                      |                               | Mshhta                        |                               |                               |                               |                                |                              |                               |                               |                           |  |
|                               | Scheduled Task                |                               | Process Hollowing             |                               |                               |                               |                                |                              |                               |                               |                           |  |
|                               | Scripting                     |                               | Process Injection             |                               |                               |                               |                                |                              |                               |                               |                           |  |



Showing data for **Last 7 days** from 04 Mar 2020 to 11 Mar 2020

Analytics were run September 9, 2019 on data ingested between September 3 and November 3, 2016

2,312,843  
Events Analyzed793,640  
Anomalies & Violations Found22  
Active Risky Entities

## Productivity

## Case Closure Velocity

Average  
3.5 days  
per case  
18.2% ↓After last annotation  
1.5 days  
per case

## Top Owner

JS

John Smith

Owner Group: Rockers L2

Average  
1.5 days  
per case  
4.6% ↑15  
CLOSED● Catastrophic 7 (40%)  
● Critical 4 (27%)  
● Marginal 3 (20%)  
● Insignificant 1 (7%)

## Productivity by Owner Groups

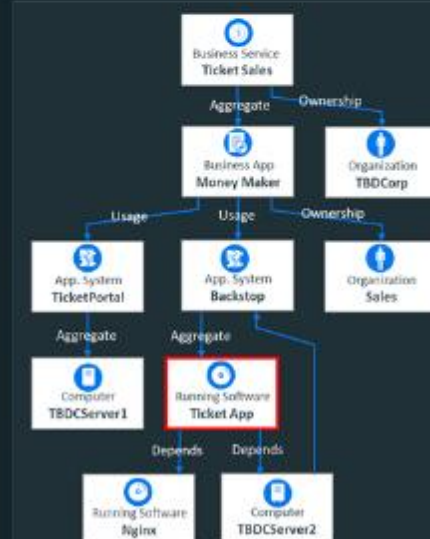
| NAME       | CASE PRODUCTIVITY AVERAGE                            | MOST PRODUCTIVE OWNER                                |
|------------|------------------------------------------------------|------------------------------------------------------|
| Rockers L2 | 2.5 days<br>4.6% ↑ than last week<br>30 Cases Closed | JS John Smith<br>10 Closed   Avg. 1.5 days per case  |
| Eagles     | 2.6 days<br>3.2% ↓ than last week<br>20 Cases Closed | TB Tim Brown<br>7 Closed   Avg. 1.8 days per case    |
| Titans     | 2.7 days<br>8.3% ↑ than last week<br>15 Cases Closed | AP Amanda Perry<br>8 Closed   Avg. 1.7 days per case |

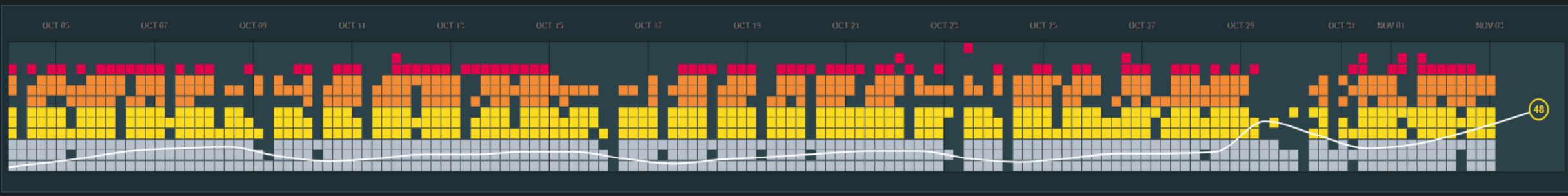
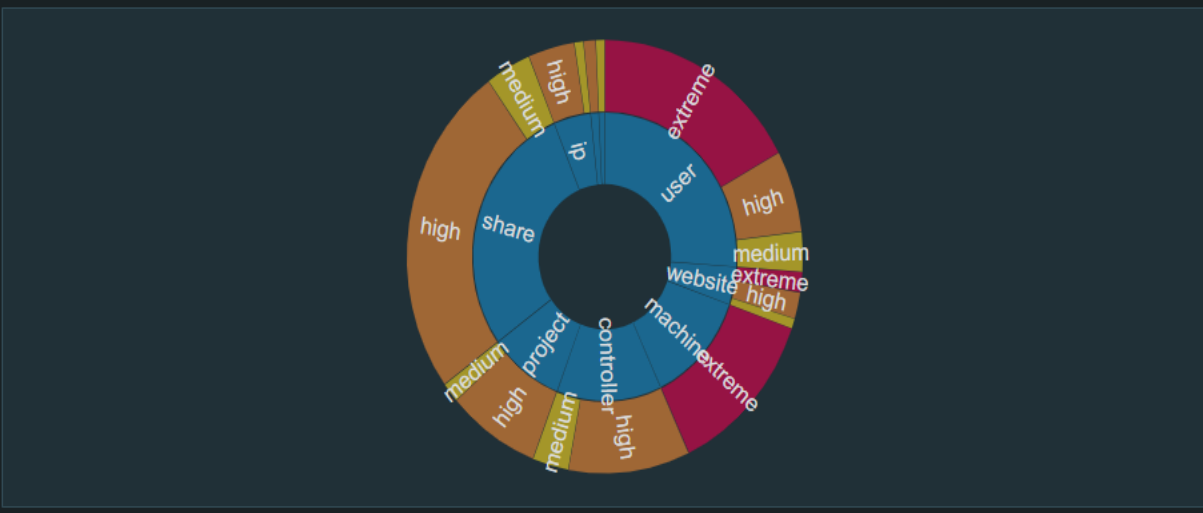
## Average KPI for Events



## Average KPI for Cases

Cases by Stage







People

Find People

List

Profile

Activity



Brad Buchanan

Infrastructure Manager  
Information Technology  
bbuchana@tbdcorp.com  
+1(212)555-3214

DN

CN=bbuchanan, OU=IT,  
OU=New York

Given Name

Brad

Surname

Buchanan

Manager

Meike Winzen

Customer ID

1234

Source Identity

5000

Vault Name

eDirectory

Workforce ID

000001

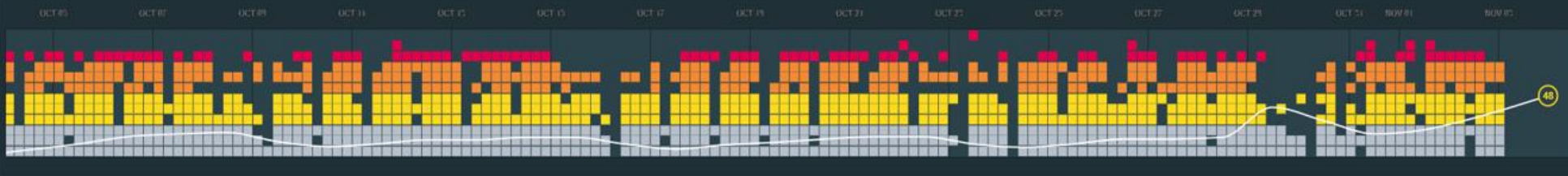
Mobile

+1(212)555-7792

Brad Buchanan Accounts

- Active Directory buchananb
- Mainframe bcb1542
- AS/400 BB1234

Event Actions



| Application | App Contributed Revenue | Calculated Operating Risk | Avg. Cost Of Breach | Calculated Likelihood of Breach |
|-------------|-------------------------|---------------------------|---------------------|---------------------------------|
| TicketApp   | \$800M                  | \$71.3M                   | \$1.2B              | 5.94%                           |

| Risk Level         | Data Encryption | Vulnerability Management | Authentication Management | Automated Access Control |
|--------------------|-----------------|--------------------------|---------------------------|--------------------------|
| Compensating Value | 30%             | 10%                      | 20%                       | 20%                      |
| High               | ✓               | ✓                        | ✓                         | ✓                        |
| MED                | ✓               |                          | ✓                         | ✓                        |
| LOW                | ✓               |                          |                           |                          |

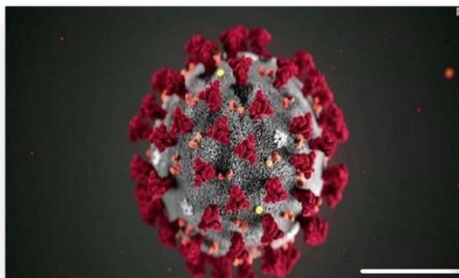
| END_TIME              | ACTIVE_CHANNEL | ATTACKER_GEO_COUNTRY_CODE | CATEGORY_CUSTOM_FORMAT_FIELD               | CATEGORY_DEVICE_GROUP         | DEVICE_PRODUCT | DEVICE_SEVERITY | DEVICE_VENDOR | FILE_NAME                      | NAME                           |
|-----------------------|----------------|---------------------------|--------------------------------------------|-------------------------------|----------------|-----------------|---------------|--------------------------------|--------------------------------|
| 11/4/2016, 9:01:57 AM | Mitre Attack   | JP                        | /Attack Life Cycle/Exploit                 | /IDS/Network                  | Arc Sight      | Warning         | Arc Sight     | Exploit Attempt Detected by... | Exploit Attempt Detected by... |
| 11/4/2016, 6:10:31 AM | Mitre Attack   | JP                        | /Attack Life Cycle/Exploit                 | /IDS/Network                  | Arc Sight      | Warning         | Arc Sight     | Exploit Attempt Detected by... | Exploit Attempt Detected by... |
| 11/4/2016, 5:19:21 AM | Mitre Attack   | CN                        | /Attack Life Cycle/Exploit                 | /IDS/Network                  | Arc Sight      | Warning         | Arc Sight     | Exploit Attempt Detected by... | Exploit Attempt Detected by... |
| 11/4/2016, 3:30:59 AM | Mitre Attack   | TH                        | /Attack Life Cycle/Exploit                 | /IDS/Network                  | Arc Sight      | Warning         | Arc Sight     | Exploit Attempt Detected by... | Exploit Attempt Detected by... |
| 11/4/2016, 3:12:32 AM | Mitre Attack   |                           | /Attack Life Cycle/Activities/Expand Ac... | /Security Information Manager | Arc Sight      | Warning         | Arc Sight     | Successful Brute Force Login   | Successful Brute Force Logi    |





## Seguimiento de la propagación del coronavirus mediante el uso de IDOL

Solicite una demostración en vivo



### Información general

El nuevo Coronavirus fue identificado por primera vez en diciembre de 2019 en Wuhan, China, y desde entonces se ha propagado rápidamente de un país a otro, trayendo consigo una devastación en forma de enfermedades y muertes masivas debido a la enfermedad ocasionada por el COVID-19. Micro Focus IDOL, un motor de inteligencia artificial perfectamente posicionado para ayudar a rastrear y saber cómo se propaga el virus, y la escala del impacto en los servicios de salud pública y la economía provocados por este virus. Nunca antes se había visto algo así en tiempos de paz y actualmente tanto gobiernos como organizaciones se esfuerzan en una lucha por entender la propagación de la enfermedad y cómo poder frenarla.

IDOL obtiene conocimientos contextuales y conceptuales a partir de numerosas

### Seguimiento de la evolución del coronavirus a través de artículos de noticias

IDOL utiliza un espectrógrafo para seguir la evolución de los temas de interés a través del tiempo. Ahora estamos publicando en directo a través de nuestro sitio web News Spectrum que muestra la propagación del coronavirus #COVID-19 día a día. El grosor de las líneas entre los temas de las noticias indica el volumen de los artículos de noticias que reflejan esos temas. También puede ver cómo un tema determinado se ramifica en subtemas relacionados a medida que evoluciona la complejidad de los efectos del coronavirus en nuestras sociedades.



### Investigar y comprender los datos del coronavirus

Una versión de demostración de Micro Focus IDOL indexa todos los días un subconjunto limitado de información sobre la propagación del brote del coronavirus (COVID-19) mediante el análisis de artículos de noticias, la difusión de noticias de varios canales de televisión, Twitter y canales RSS, y ya ha capturado e indexado más de 22 millones de documentos. IDOL puede obtener conocimientos a partir de la información visual y textual, también conocida como "datos no

## Cómo IDOL puede ayudar a rastrear el coronavirus

Al escribir la palabra clave "Coronavirus" en la herramienta BUSCAR, IDOL puede identificar y agrupar rápidamente los conceptos relacionados, los cuales se identifican automáticamente mediante análisis estadístico como importantes en el corpus de datos dentro del índice. La imagen muestra una presentación visual de esto, conocida como "Topic Map" (mapa del tema), que permite a un analista ver una instantánea de toda la información relacionada con el tema en cuestión y favorece la detección de nuevos grupos de información.



## Uso de geoetiquetado para rastrear la actividad del coronavirus

Mediante el uso de las capacidades de geoetiquetado de IDOL de texto sin estructurar, somos capaces de trazar un mapa de la información de las ciudades de todo el mundo afectadas por los casos de COVID-19. El mapa muestra las menciones de la enfermedad en toda la web asignando ubicaciones geográficas ya sea a partir de los metadatos o extrayendo los nombres de lugares a los que se hace referencia en esas menciones.

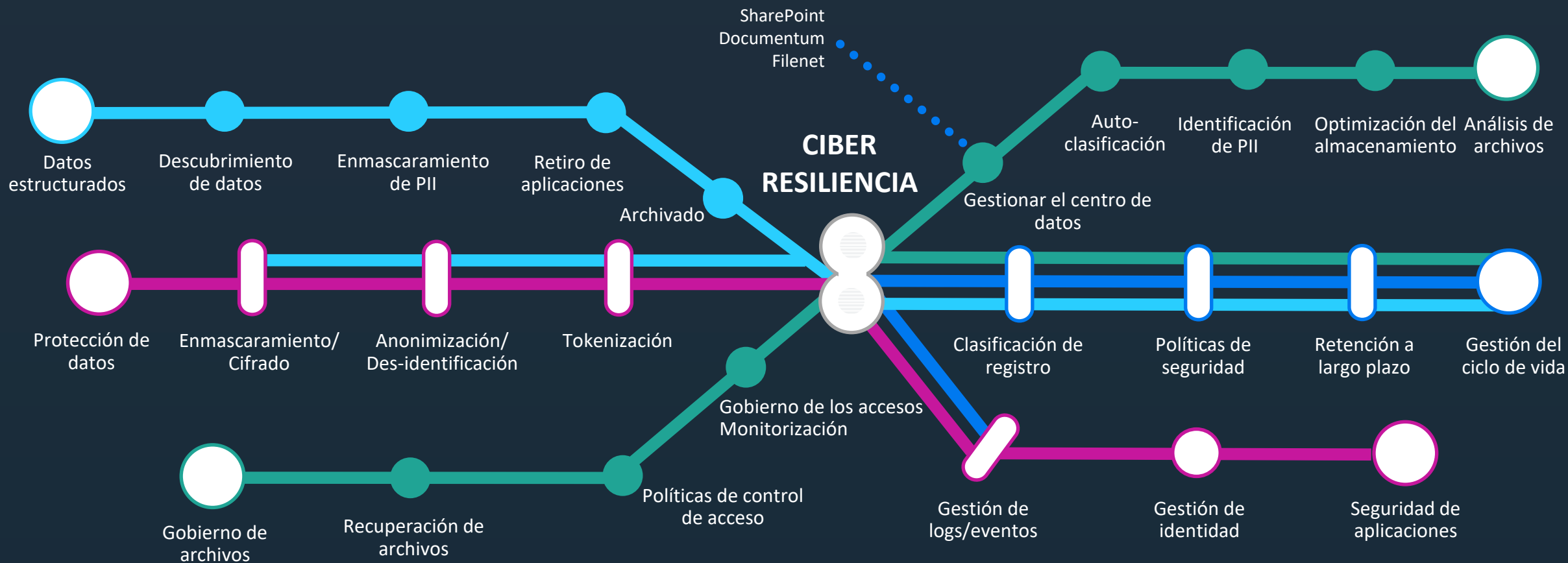


WAYNE GRETZKY

"You Miss 100% Of The Shots You Don't Take"

WINTER

THE BOX



1

LÍNEA DE DATOS ESTRUCTURADOS

2

LÍNEA DE DATOS NO ESTRUCTURADOS

S

LÍNEA DE SEGURIDAD EMPRESARIAL

L

LÍNEA DE GESTIÓN DEL CICLO DE VIDA

point of view.

**Trust** [trʌst] n

confidence in

dependence v

contingent a

# GRACIAS

## Ciber Resiliencia a través de Machine Learning

**Ramsés Gallego**

**CISM, CGEIT, CISSP, SCPM, CCSK, ITIL, COBIT, Six Sigma Black Belt  
International Chief Technology Officer, Cybersecurity**

**Executive Vice President, Quantum World Association**

**Past International Vice President, ISACA, Board of Directors**

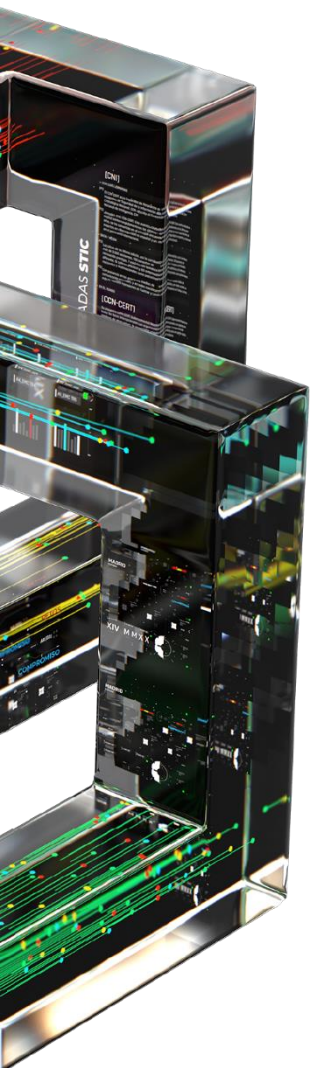
**Past President, ISACA Barcelona Chapter**

**Privacy by Design Ambassador, Government of Ontario, Canada**

**[ramses.gallego@microfocus.com](mailto:ramses.gallego@microfocus.com)**

 **[@ramsesgallego](https://twitter.com/ramsesgallego)**





**MUCHAS GRACIAS**  
**#XIVJORNADASCCNCERT**