



ZERU

Cybersecurity
Services



Predecir, detectar, contener y responder ante ciberataques

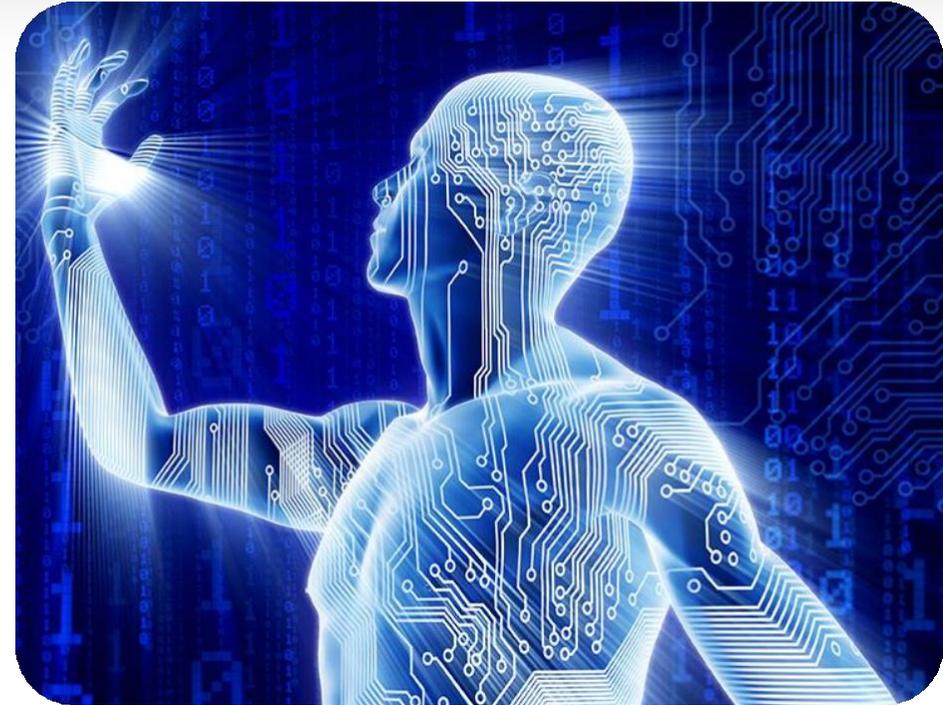


Misión

Proveer a las empresas las capacidades para Prevenir y/o detectar de manera oportuna incidentes de Ciberseguridad, reduciendo el impacto en el negocio, a través del monitoreo 7x24 de sus infraestructuras de seguridad, con un costo adecuado al sector y personal altamente entrenado, comprometido y capacitado.

Visión

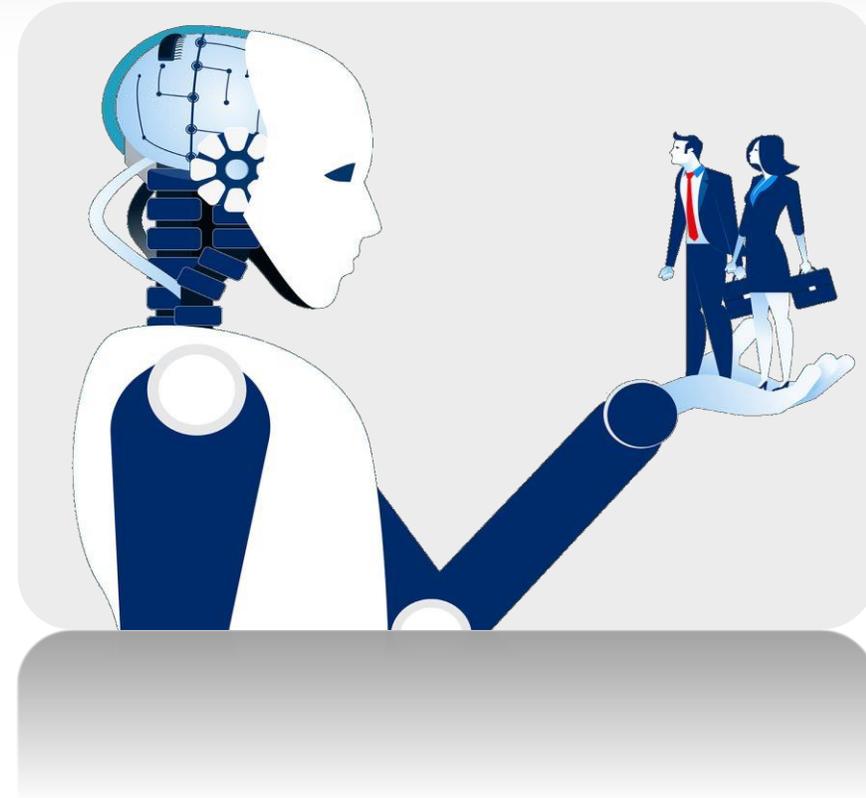
Ser el brazo de Ciberseguridad preferente para las empresas del mercado Venezolano, aportando alto valor en compromiso y experticia.



Respuesta al mercado

Las organizaciones cada vez son más complejas, debido al uso de diferentes tecnologías para resolver brechas de seguridad, perdiendo visibilidad de la información que cada una puede generar.

ZERU es la opción para apoyar a las empresas a reducir el riesgo que representa para sus negocios la falta de visibilidad de la seguridad en sus infraestructuras.



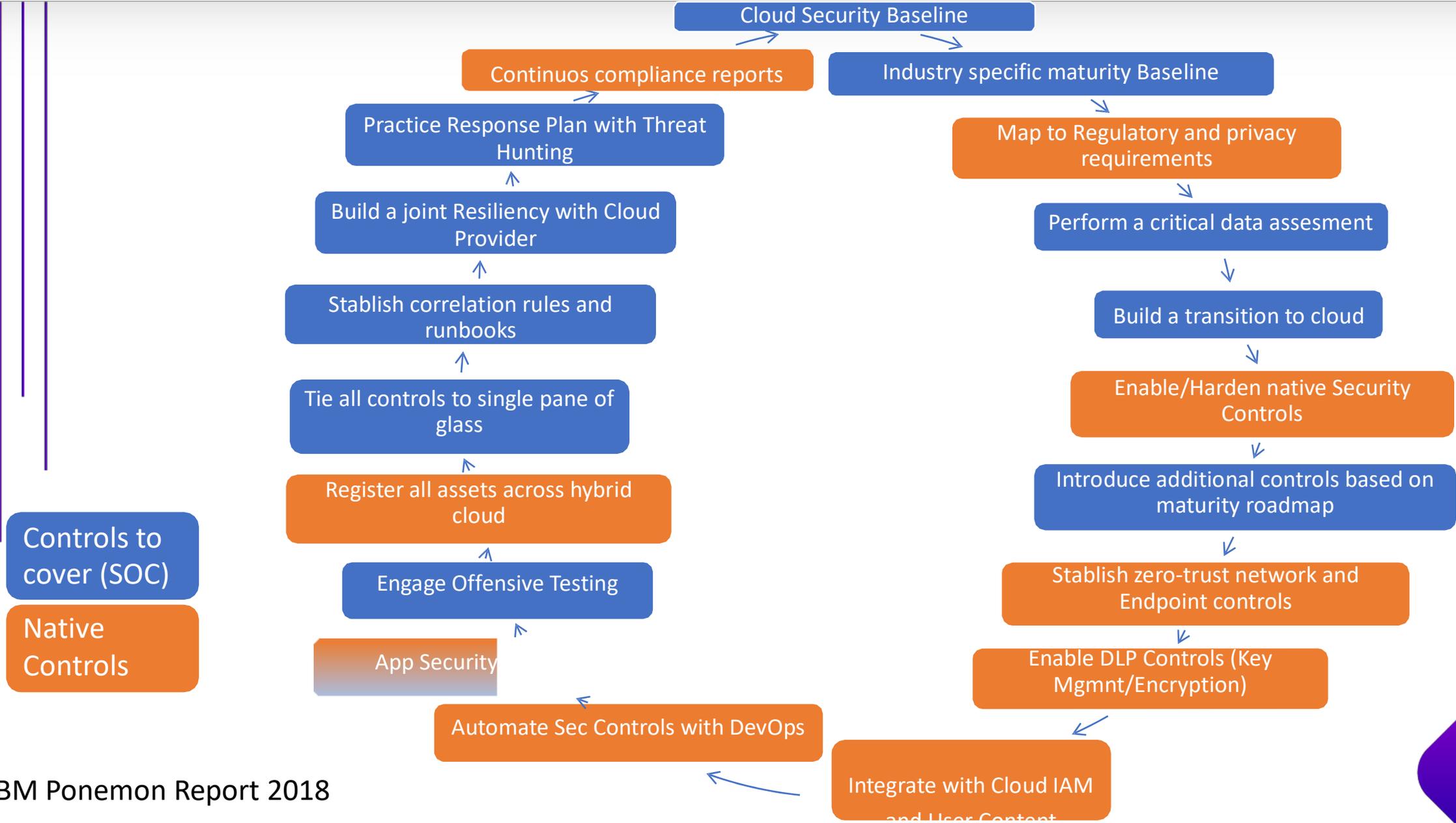


No fracasa quien sufre un ataque de seguridad, es parte del juego, fracasas si no tienes capacidad de respuesta

CHARLES BLAUNIER
CISO, Citigroup



Rapidez para identificar y contener



Controls to cover (SOC)
Native Controls



Zeru SOC & MDR Services



Paquetes de Servicio

Platino

Oro

Plata



Add-on

Plata

Monitoreo 24x7

Respuesta a Incidentes
Ciberseguridad

Shadow IT Cloud
Discovery

CISO coaching
sessions

Workshop ISO
27001

Boletín de
ciberseguridad

Oro

Análisis de
Vulnerabilidades

Análisis
comportamiento
usuarios (UEBA)

Respuesta a
vulnerabilidades

Azure/AWS Threat
Management

Security Awareness
& Training

Platino

Analisis de
compromiso

Vulnerability
Coaching
Remediation

BaaS

DRPaaS

Add-ons

Analisis de código

CISOaaS

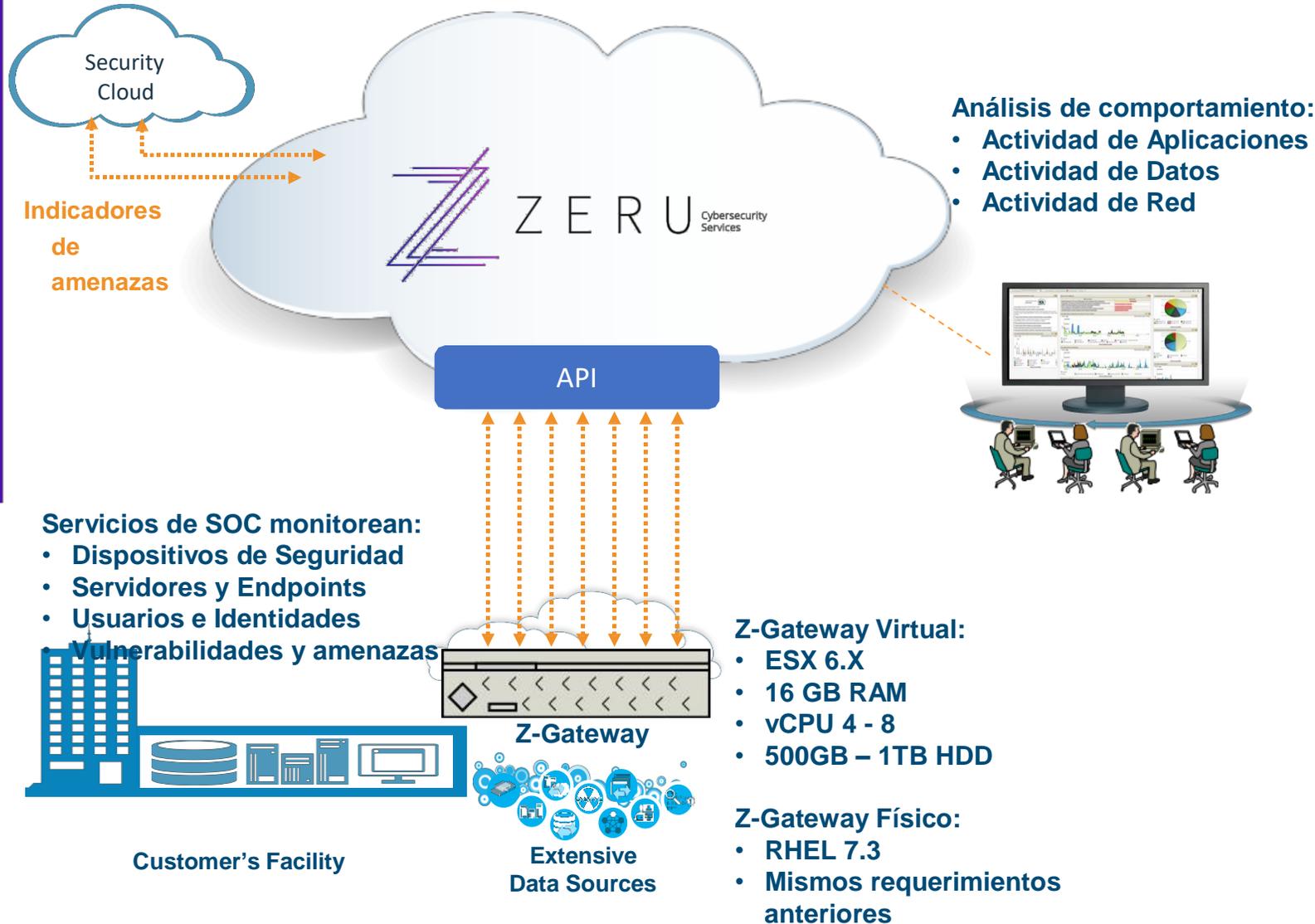
Ethical Hacking
(Pentest)

Analisis de Trafico
red

Procesos de
Seguridad ISO 27k

Antimalware IA





Aspectos relevantes:

- Correlación histórica y en tiempo real de activos, eventos y vulnerabilidades
- Capacidades de AI para manejar eventos de seguridad
- Detección de amenazas avanzadas
- Reportes periódicos y bajo demanda
- Soporta integraciones de más de 450 soluciones de seguridad y TI
- ROI en menor tiempo

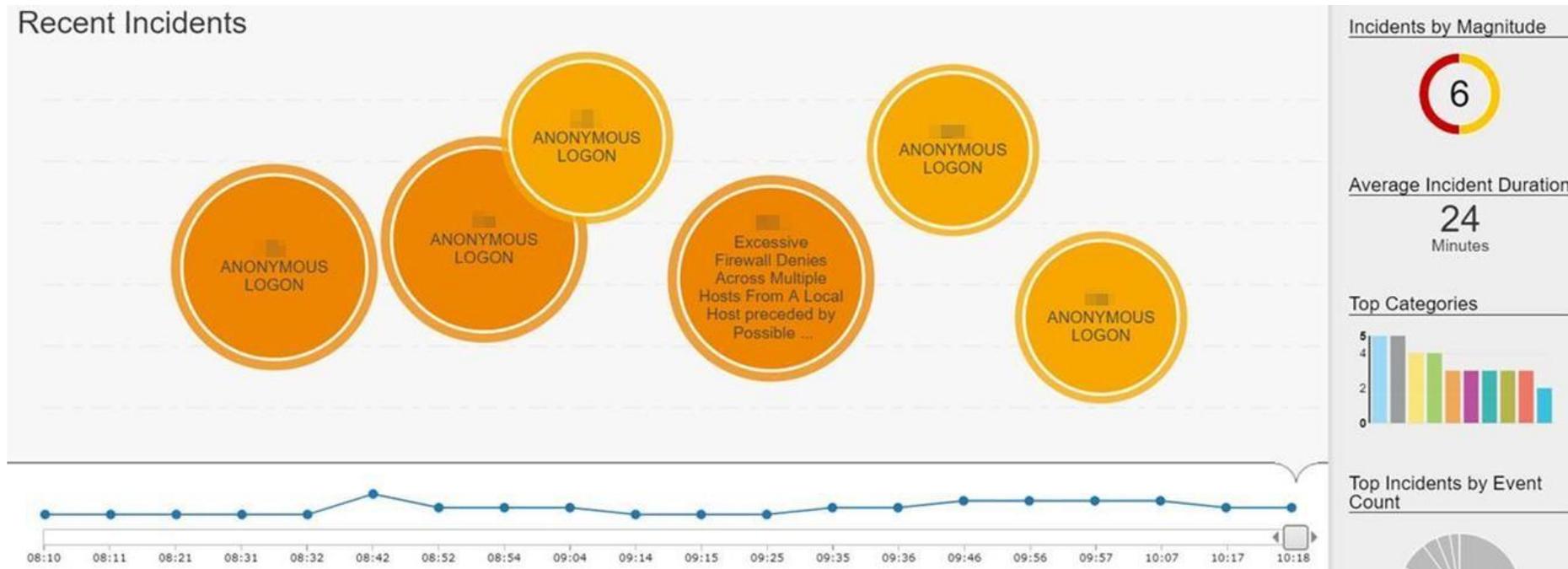
Valor añadido:

- Seguridad especializada para detección de amenazas
- Sin licencia basada en Appliances
- Orígenes de Logs en Cloud (Azure, O365 y AWS)
- Monitoreo 24/7
- Reglas de seguridad a medida
- Ráfagas de EPS bajo demanda
- Monitoreo de Shadow IT
- Análisis de Vulnerabilidades y Aplicaciones desde el Cloud
- Descubrimiento de índices de compromiso (IoC)





- **Reportes de Incidentes Automatizados:** no solo tendrán un reporte de un potencial incidente, sino también el tipo, origen/destino y afectación. Todos estos parámetros son configurables para adaptarse a las necesidades de la organización.



Zeru Cybersecurity Services



- **User Behavior Analytics**: le garantizamos visibilidad total de potencial comportamiento no deseado y/o compromiso de cuentas que puedan representar un riesgo para su organización.

The dashboard provides a comprehensive view of user behavior and risk. Key components include:

- Dashboard Overview:** Shows 66 Monitored Users, 4 High Risk Users (6% of monitored users), and 16 Users Discovered from Events (24% of monitored users).
- User Details (Shirley Pollack):** Active status, Overall Risk Score of 1.4K, and Risk last Interval of 0. Includes a search bar for the user.
- Recent Offenses:** Lists offenses such as "Multiple Login Failures for the Same User preceded by Login Failures Followed By Success from the same Username containing Authcrypt" (3 days ago) and "Multiple Login Failures for the Same User preceded by Login Failures Followed By Success from the same Username containing Login attempt - failed" (9 days ago).
- Risk Category Breakdown (Last Hour):** A donut chart showing the distribution of risk categories.
- Timeline:** A bar chart showing user events and risky events from Mar 9 to Mar 13.
- Summary Metrics (Mar 13):** 210 Risk, 4 Use Cases, 44 Risky Events, 17 Log Devices, 180 Event IDs, 486 URLs, and 1 Aliases.
- Table of Use Cases:**

Count	Use Cases	Risk
40	Detect Insecure Or Non-Standard Protocol	200
2	Abnormal increase in User activity	10
1	Deviation from learned peer group	5
1	Deviation from normal activity patterns	5





- **Shadow IT Discovery:** usted y su empresa tendrán visibilidad total de los servicios de nube que utilizan sus empleados, obtendrán un reporte con servicios de Cloud que puedan representar un riesgo para su organización.

Dashboard Offenses Log Activity Network Activity Assets Reports Admin **Cloud Discovery**

Quick Insights Last updated on Sep 26, 2017, 3:29:23 PM

Risky Users **29** Critical Violations **12** Risky Applications **9**

Top Risky Applications [All Applications](#)

Score ↓	Type	Application Name	Severity
24.6		Putlocker	
12.67		4shared	
7.77		Box	

Cloud Applications Insights



Top Risky Users [All Users](#)

Score ↓	User	Severity
7.3	[blurred]	
6.03	[blurred]	
4.82	[blurred]	
4.46	[blurred]	
3.14	[blurred]	

Top Violations [All Violations](#)

Score ↓	Violation	Severity
19.64	User accessing unapproved cloud application	
17.64	High risk application accessed by user	
5.01	Large unapproved download from cloud applications	
3.06	New application discovered with threats	
2.96	Large unapproved upload to cloud applications	





- **Azure/AWS Threat Management:** ganará tiempo al tratar los incidentes de su plataforma de Cloud de una manera más simple, con mayor efectividad y con total visibilidad de potenciales eventos maliciosos.

The screenshot displays the AWS IAM Best Practices console interface. On the left, a sidebar shows navigation options for AWS, AZURE, and IBM. The main content area is divided into several sections:

- Summary:** Total number of offenses: 39; Number of offenses with magnitude: 1.
- All regions by magnitude:** A pie chart showing the distribution of offenses across regions: 53.8% (orange), 43.6% (yellow), and 2.8% (red).
- Filters:** Two filter panels are visible. The 'User condition filters' panel includes options for 'Without password', 'With access keys that need rotating', 'Without MFA', 'With unused passwords', and 'With unused access keys'. The 'Root account filters' panel includes options for 'With access keys', 'Without MFA', and 'Without individual IAM users'. An 'Apply' button is located at the bottom right of the filter panels.
- Table of Users:** A table listing users and their compliance status. The table has columns for User, Password Enabled, Password Last Used, MFA Active, Key1 Active, Key1 Age, Key2 Active, and Key2 Age. The 'Password Enabled' and 'Key2 Active' columns have red vertical bars indicating non-compliance for some users.
- Most severe offenses:** A list of specific security events, such as 'A user has failed to login to the AWS Console 5 times in 2 minutes from the same source IP'.

At the bottom of the console, a progress bar shows the overall compliance status: 43.6% (yellow), 3 (circled in white), 53.8% (orange), and 2.8% (red).

- **Geolocalización:** a través de las herramientas del SOC podremos determinar el país y reputación de una potencial conexión, enriqueciendo los IOC de potenciales conexiones maliciosas.



	80.82.	
	94.102	
	89.248	
	89.248	
	36.91.	
	117.102.	
	179.95.	
	36.72.	
	181.193.	
	45.249.	
	117.193.	
	101.108	
	14.163	
	177.238.	
	14.192.	
	183.82.	





- **Correlación de eventos:** de una manera simple podemos determinar en segundos la relación entre eventos, determinando la posibilidad de un compromiso real y tomando acciones en el dispositivo (de ser necesario).

```
AutoID: [redacted] AutoGUID: [redacted] ServerID: [redacted] ReceivedUTC: "2019-[redacted]" DetectedUTC: "2019-[redacted]"
AgentGUID: [redacted] Analyzer: [redacted] "VirusScan Enterprise" AnalyzerVersion: "8.8"
AnalyzerHostName: [redacted] AnalyzerIPV4: [redacted] AnalyzerIPV6: [redacted] AnalyzerMAC: [redacted] AnalyzerDATVersion:
"9146.0000" AnalyzerEngineVersion: "6000.8403" AnalyzerDetectionMethod: [redacted] SourceHostName: " " SourceIPV4: [redacted] SourceIPV6:
[redacted] SourceMAC: [redacted] SourceUserName: [redacted] SourceProcessName: [redacted] SourceURL: [redacted] TargetHostName: [redacted]
TargetIPV4: [redacted] TargetIPV6: [redacted] TargetMAC: [redacted] TargetUserName: [redacted] TargetPort: [redacted] TargetProtocol:
[redacted] TargetProcessName: [redacted] TargetFileName: "E:[redacted]VEGAS 12+PATCH.rar\vegas.pro.12.-patch.exe" ThreatCategory:
"av.pup" ThreatEventID: [redacted] ThreatSeverity: "2" ThreatName: "Generic PUP" ThreatType: "app_pua" ThreatActionTaken: "access denied" ThreatHandled: [redacted]
TheTimestamp: [redacted] TenantId: [redacted]
```

[redacted]	92	6
[redacted]	84	3
NT AUTHORITY\SYSTEM	2	12

Top 5 Categories

Name	Magnitude	Local Destination Count	Events/Flows	First Ever
Virus Detected		0	178	Jan 29, 2019, 11

Last 10 Events

Event Name	Magnitude	Log Source	Category
Unwanted program, clean error, denie...		McAfee ePO	Virus Detected
file infected. Undetermined clean er...		McAfee ePO	Virus Detected
Unwanted program, clean error, denie...		McAfee ePO	Virus Detected
file infected. Undetermined clean er...		McAfee ePO	Virus Detected
Infected file deleted		McAfee ePO	Virus Detected
Infected file deleted		McAfee ePO	Virus Detected
Infected file deleted		McAfee ePO	Virus Detected
Infected file deleted		McAfee ePO	Virus Detected
Unwanted program, clean error, denie...		McAfee ePO	Virus Detected
Unwanted program, clean error, denie...		McAfee ePO	Virus Detected



- **Incumplimiento de Políticas:** reducimos sus tiempos de remediación en incumplimiento de políticas, para que pueda corregir de manera orgánica toda desviación potencial.

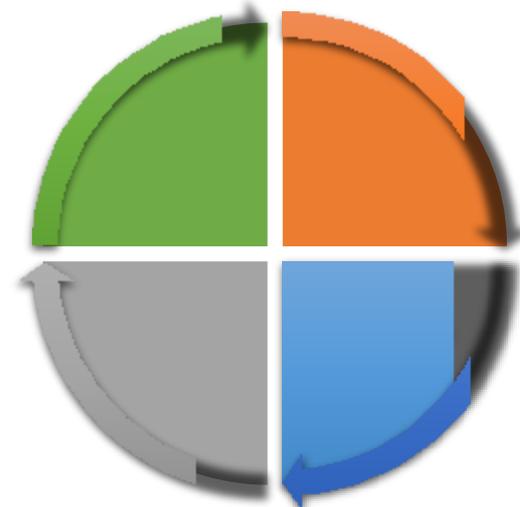
Event Name	Success Audit: An account was successfully logged on		
Low Level Category	User Login Success		
Event Description	Success Audit: An account was successfully logged on.		
Magnitude		(7)	Relevance 7
Username	ANONYMOUS LOGON		
Start Time		Storage Time	



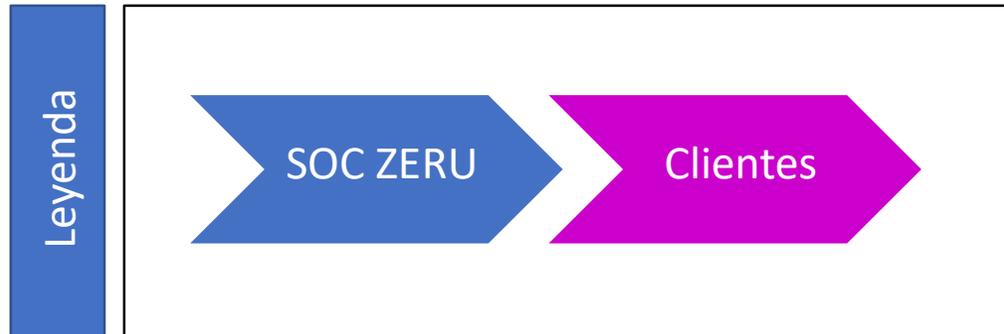
Qué incluye el Servicio?



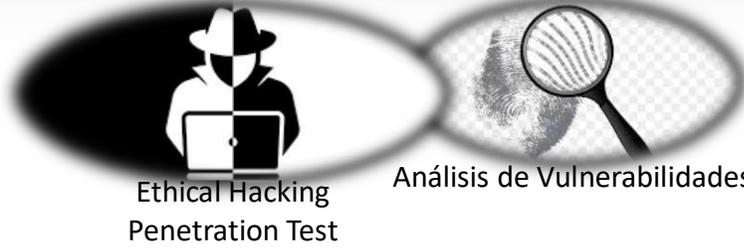
- Monitoreo 7x24
 - AWS
 - Azure
 - O365
 - Firewall
 - Active Directory
 - Anti Virus Console
- SIEM Management
- Gestión de incidentes:
 - Detección
 - Triage
 - Escalamiento
 - Reportes Mensuales
 - Tendencias
- Análisis de vulnerabilidades
- User Behavior Analytics
- Shadow IT
- Respuesta a Vulnerabilidades
- CISO Coaching Session
- Cybersecurity Workshop
- Boletín de Seguridad



Gestión de Incidentes



Zeru Cybersecurity Services



Corporación Advisor Services





ZERU Cybersecurity
Services



Le ofrecemos soluciones
integrales para aspectos críticos.

Su ciberseguridad es lo más importante.



ZERU

Cybersecurity
Services



Predecir, detectar, contener y responder ante ciberataques



Zer0 Malware
Zer0 Ataques
100% Prevención
<https://advisor.com.ve>