



ZERU

Cybersecurity
Services



Predcir, detectar, contener y responder ante ciberataques



ADV INTEGRADORES Y CONSULTORES S.A de C.V.

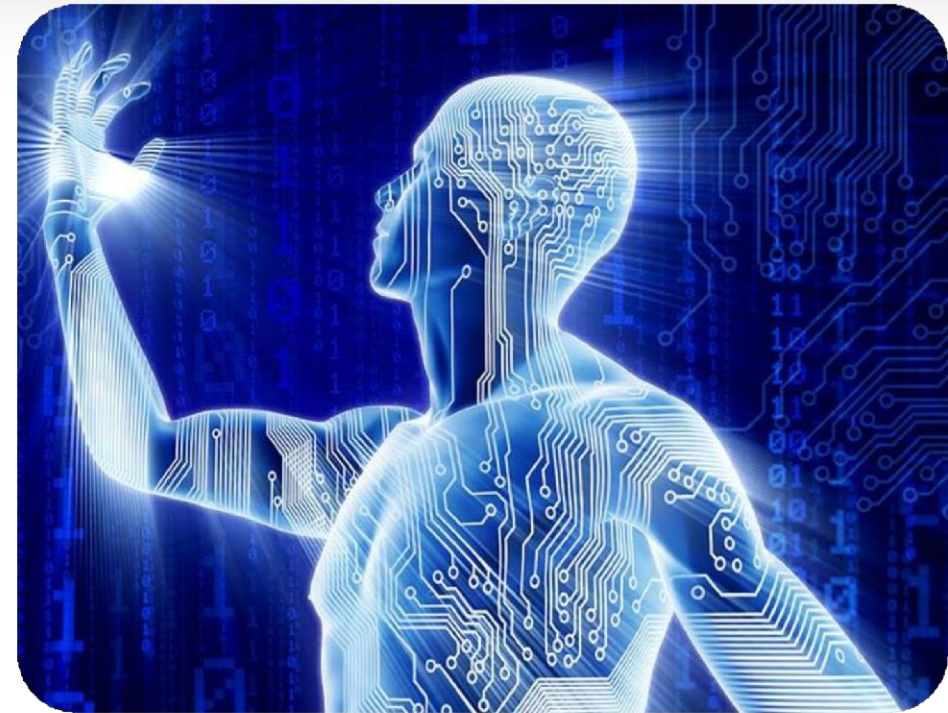


Misión

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.

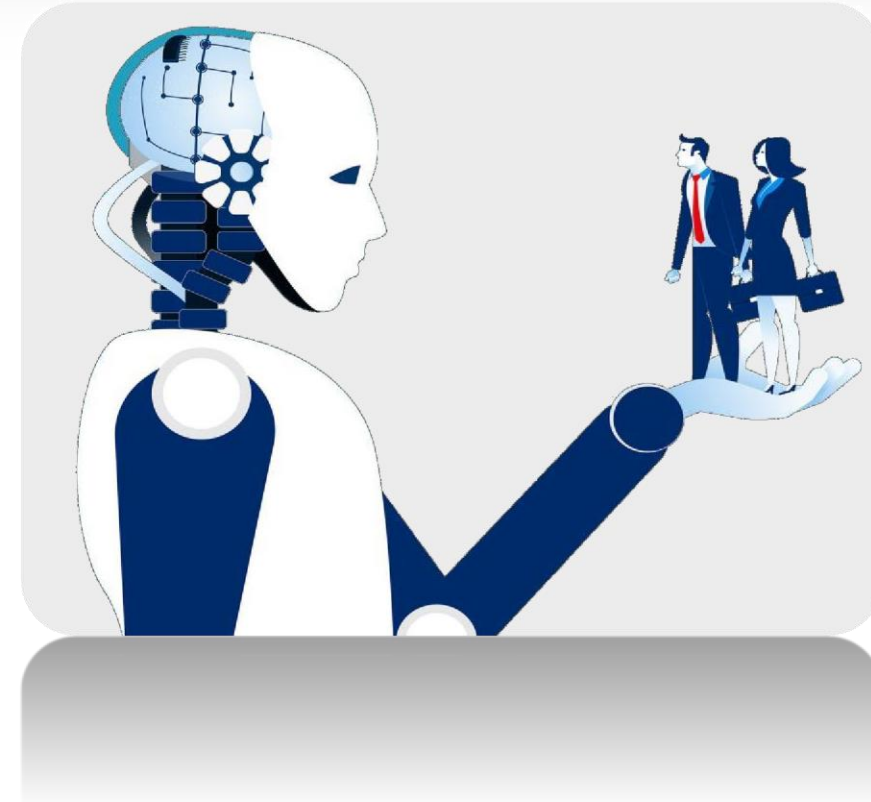




Respuesta al mercado

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.

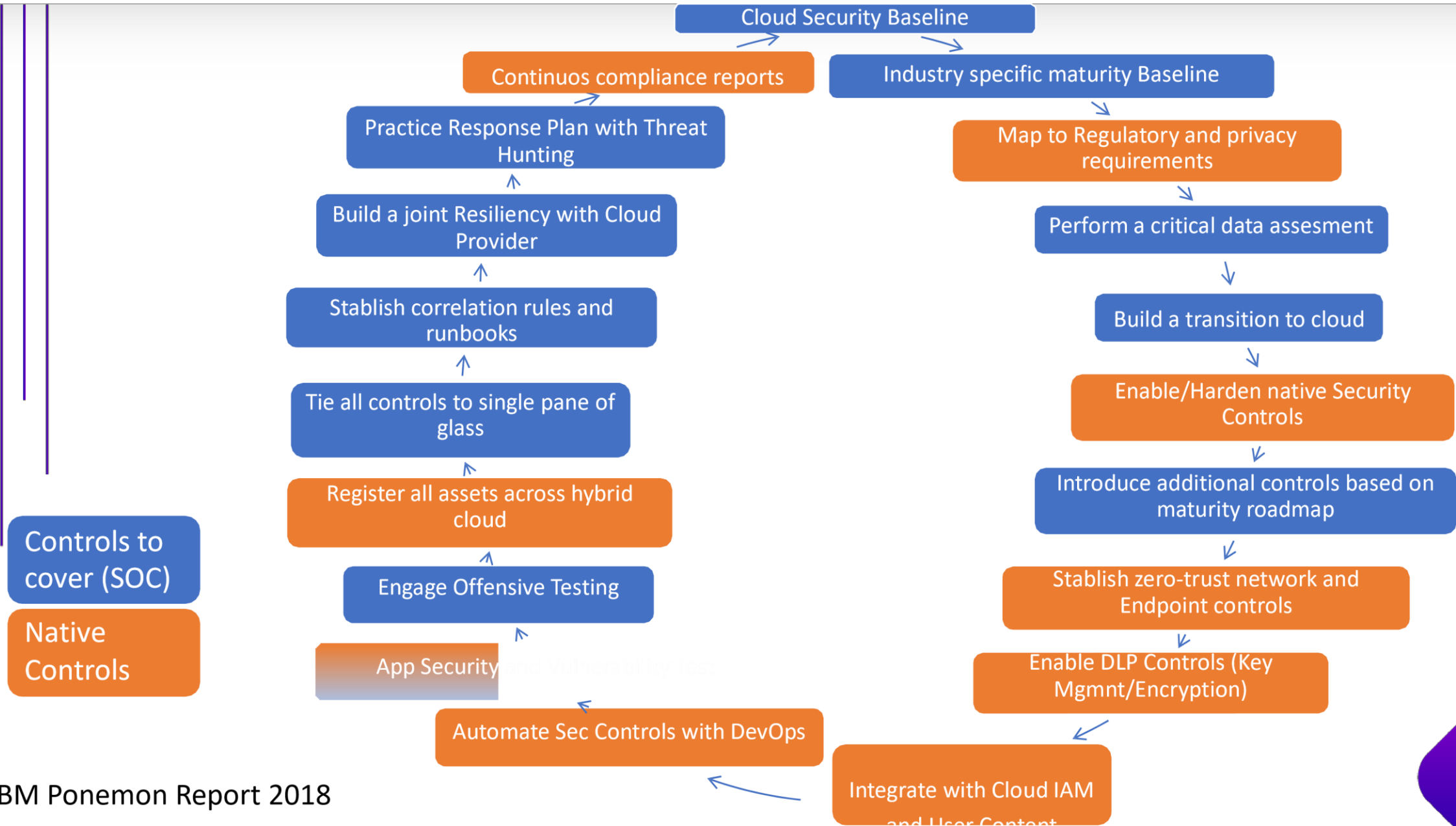




No fracasa quien sufre un ataque de seguridad, es parte del juego, fracasas si no tienes capacidad de respuesta

CHARLES BLAUNIER
CISO, Citigroup







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

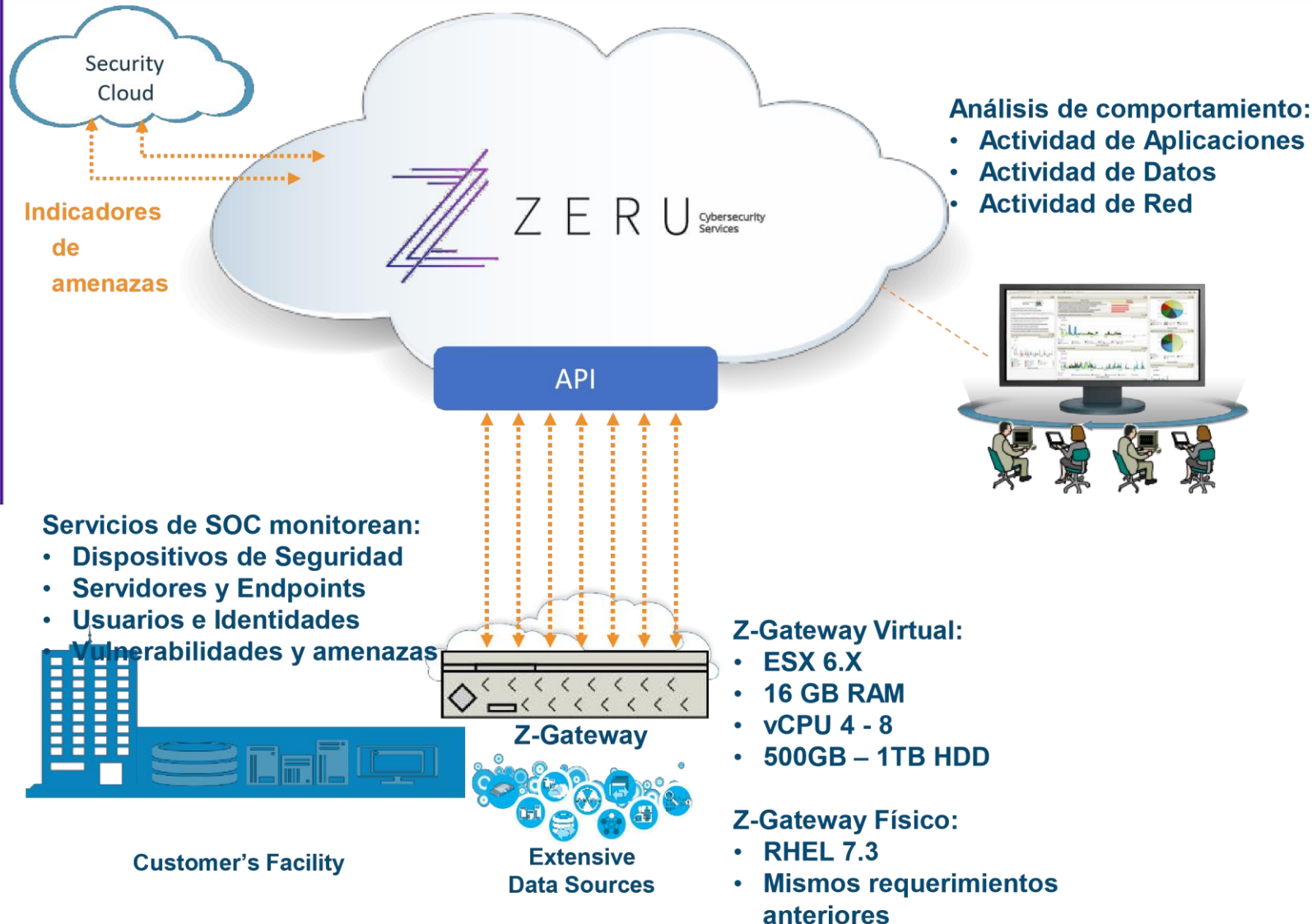
Ethical Hacking (Pentest)

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

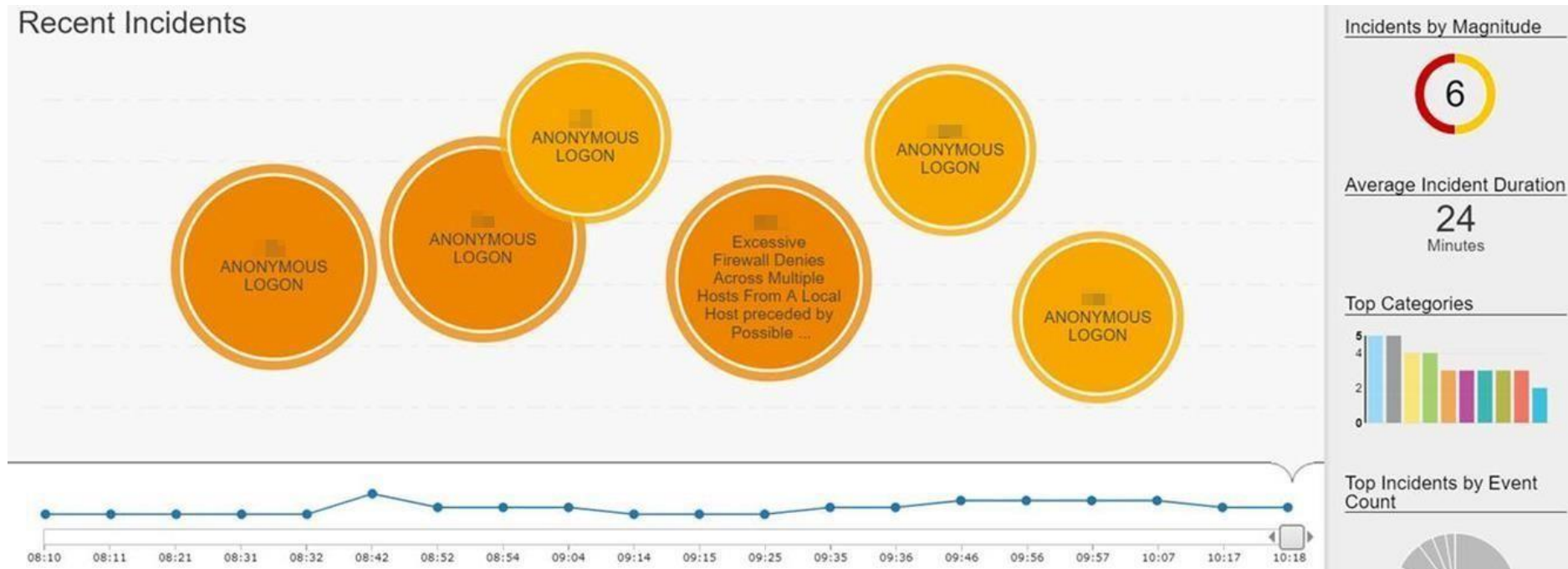
Valor añadido:

- 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)



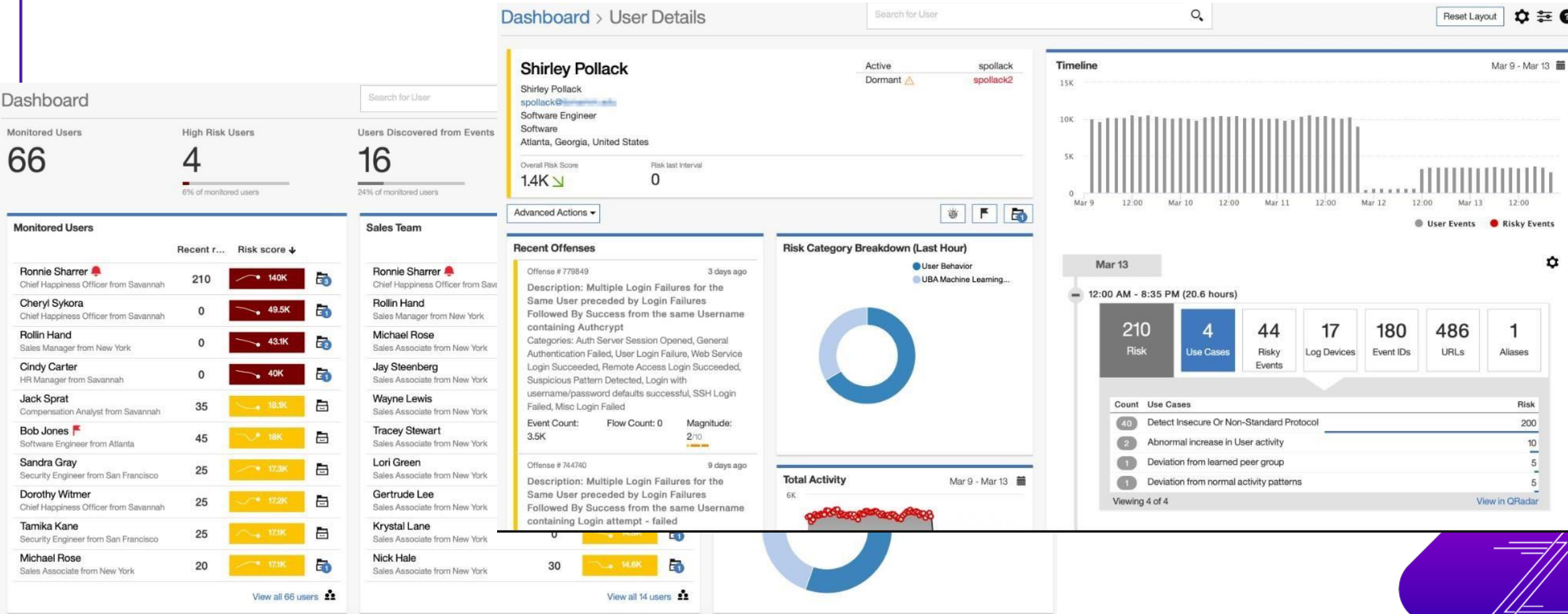


- **Reportes de Incidentes Automatizados:** no solo tendrán un reporte de un potencial incidente, sino también el tipo, origen/destino y afectación. Todos estos parámetros son configurables para adaptarse a las necesidades de la organización.





- 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.





- **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.



Top Risky Applications				All Applications
Score ↓	Type	Application Name	Severity	
24.6		Putlocker		
12.67		4shared		
7.77		Box		





- **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.

AWS

AZURE

IBM

39

1

All regions by magnitude

Most severe offenses

A user has failed to login to the AWS Console 5 times in 2 minutes from the same source IP

Multiple read attempts of Policies was attempted and failed from the same Source IP

A user has failed to login to the AWS Console 5 times in 2 minutes from the same source IP

Multiple read attempts of Policies was attempted and failed from the same Source IP

Multiple failed login attempts from different Source IPs

Multiple failed login attempts from different Source IPs

Multiple failed login attempts from different Source IPs

Filters

User condition filters:

☒ Without password

☐ With unused passwords

☐ With access keys that need rotating

☒ Without MFA

☒ With unused access keys

Root account filters:

☐ With access keys

☐ Without individual IAM users

☒ Without MFA

Apply

Use the filters to see the users who might not follow the best practices of AWS IAM. After you select the filters, the app highlights problematic values.

> AWS Account: [redacted], Report last generated on AWS: 8/17/2018, 4:16:55 PM

> AWS Account: [redacted], Report last generated on AWS: 8/17/2018, 4:16:54 PM

☒ AWS Account: [redacted], Report last generated on AWS: 8/17/2018, 3:20:05 PM

User	Password Enabled	Password Last Used	MFA Active	Key1 Active	Key1 Age	Key2 Active	Key2 Age
[redacted]	true	2018-08-01T17:13:22	false	true	2018-01-15 18:53:35	false	N/A
[redacted]	true	2018-02-22T18:09:05	false	true	2018-02-22 17:26:38	false	N/A
[redacted]	false	N/A	false	true	2018-07-20 14:25:56	false	N/A
[redacted]	false	N/A	false	true	2018-05-29 19:08:26	false	N/A

Items per page: 10

1-4 of 4 items

1 of 1 pages

43.6%

3

53.8%

2.6%



- **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	2023-01-01 00:00:00	Storage Time	2023-01-01 00:00:00





- **Monitoreo 7x24**

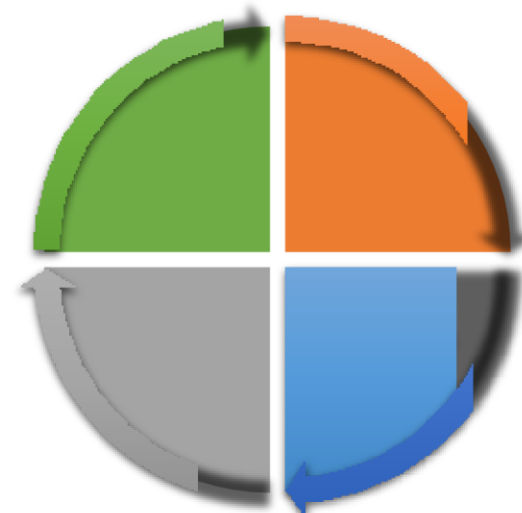
- AWS
- Azure
- O365
- Firewall
- Active Directory
- Anti Virus Console

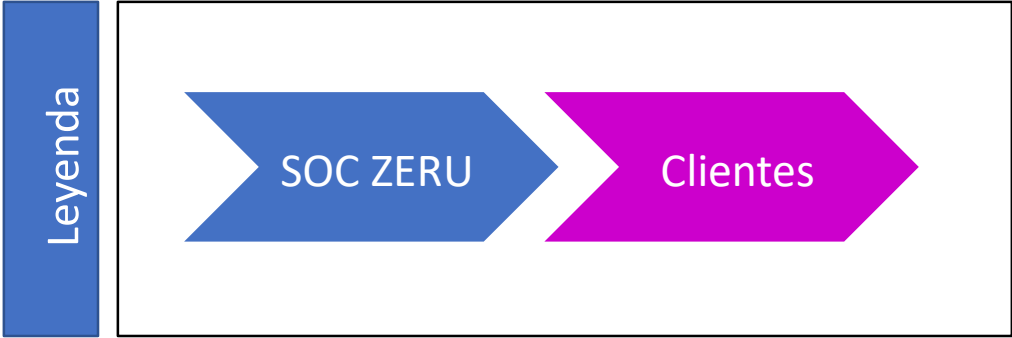
- **SIEM Management**

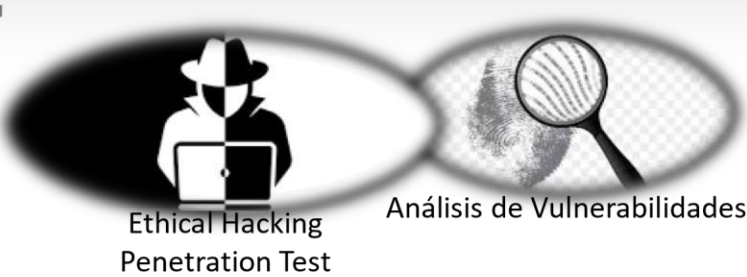
- **Gestión de incidentes:**

- 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



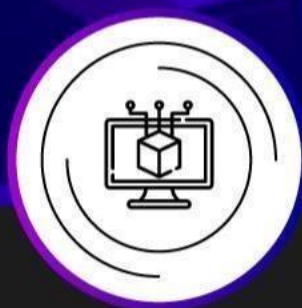






ZERU Cybersecurity
Services

Powered By  ADV
Advisor Company



Le ofrecemos soluciones
integrales para aspectos críticos.

Su ciberseguridad es lo más importante.



ZERU

Cybersecurity
Services



Predicir, detectar, contener y responder ante ciberataques



Zer0 Malware
Zer0 Ataques
100% Prevención

Powered by ADV INTEGRADORES Y CONSULTORES S.A de C.V.