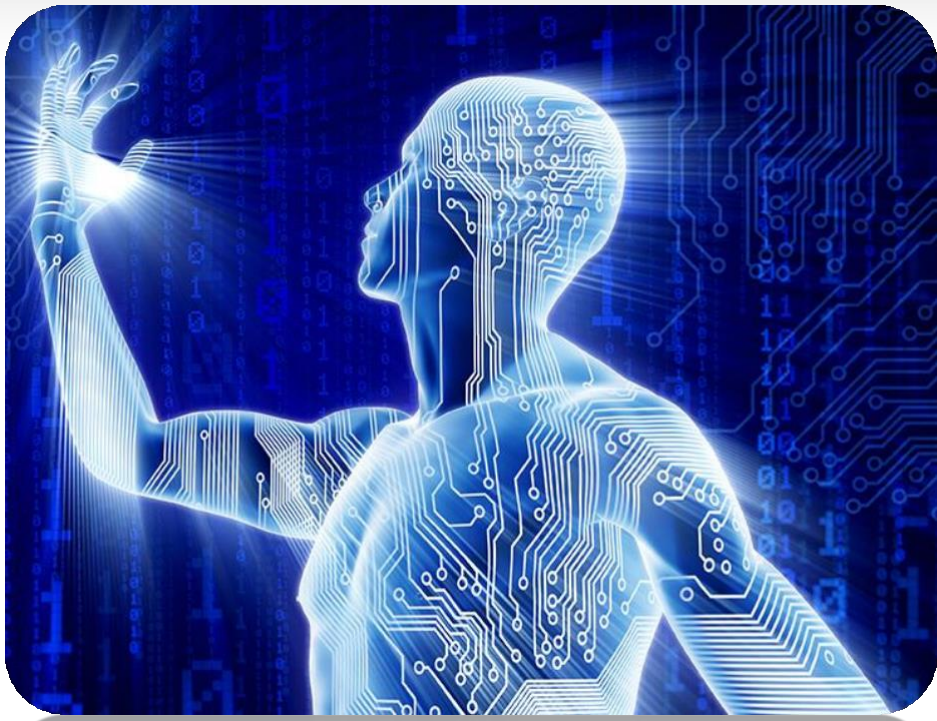
Powered by Corporación Advisor C.A. https://advisor.com.ve

Zeru Cybersecurity Services

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.



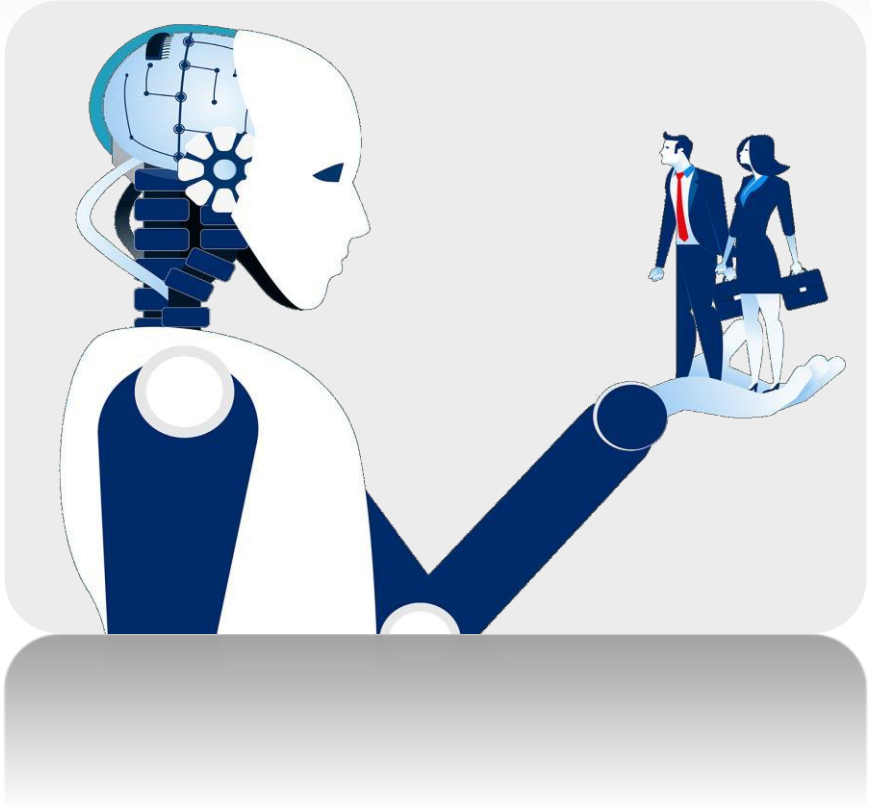
Visión

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.

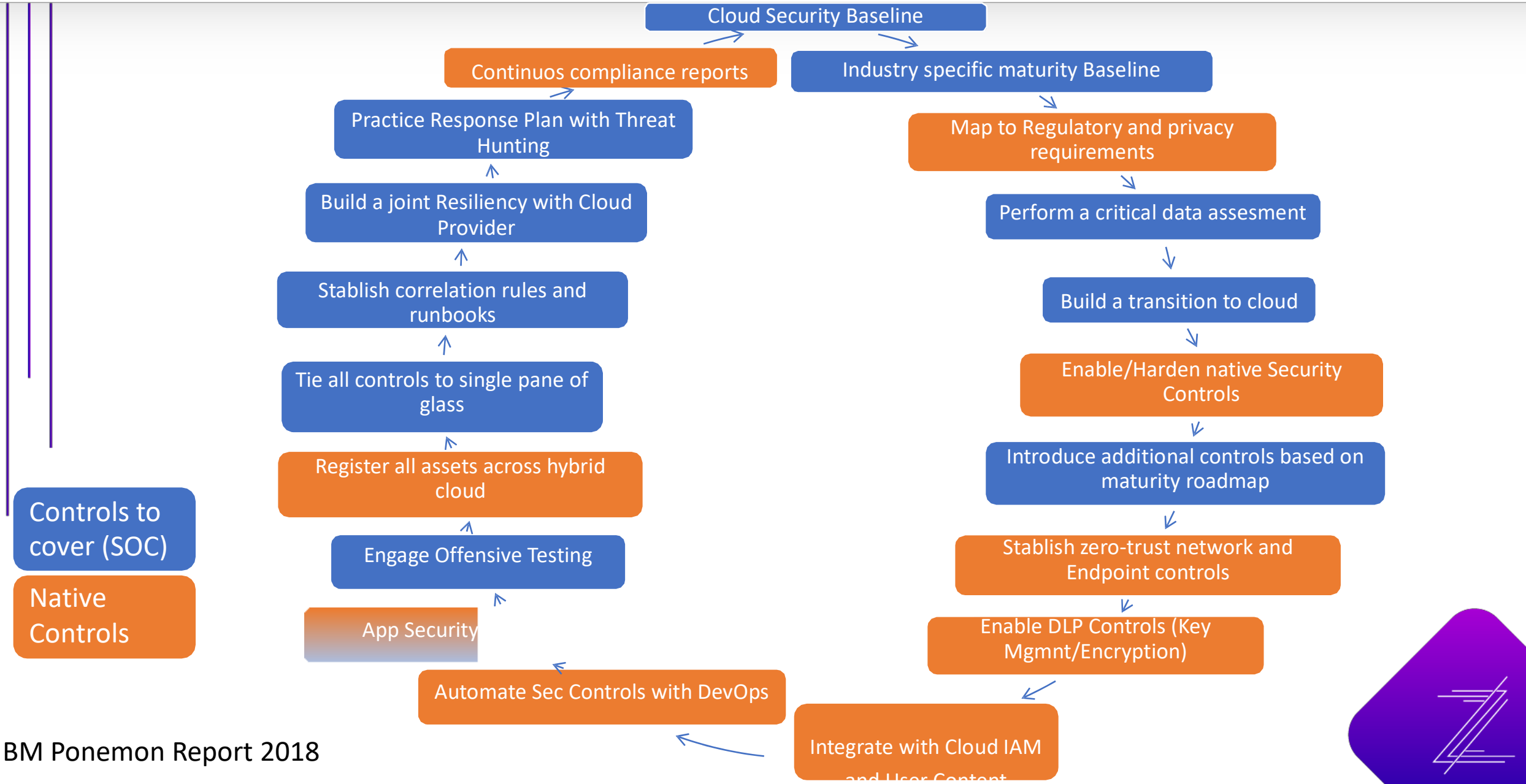


No fracasa quien sufre un ataque de seguridad, es parte del juego, fracasas si no tienes capacidad de respuesta

CHARLES BLAUNIER

CISO, Citigroup

Rapidez para identificar y contener



IBM Ponemon Report 2018

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

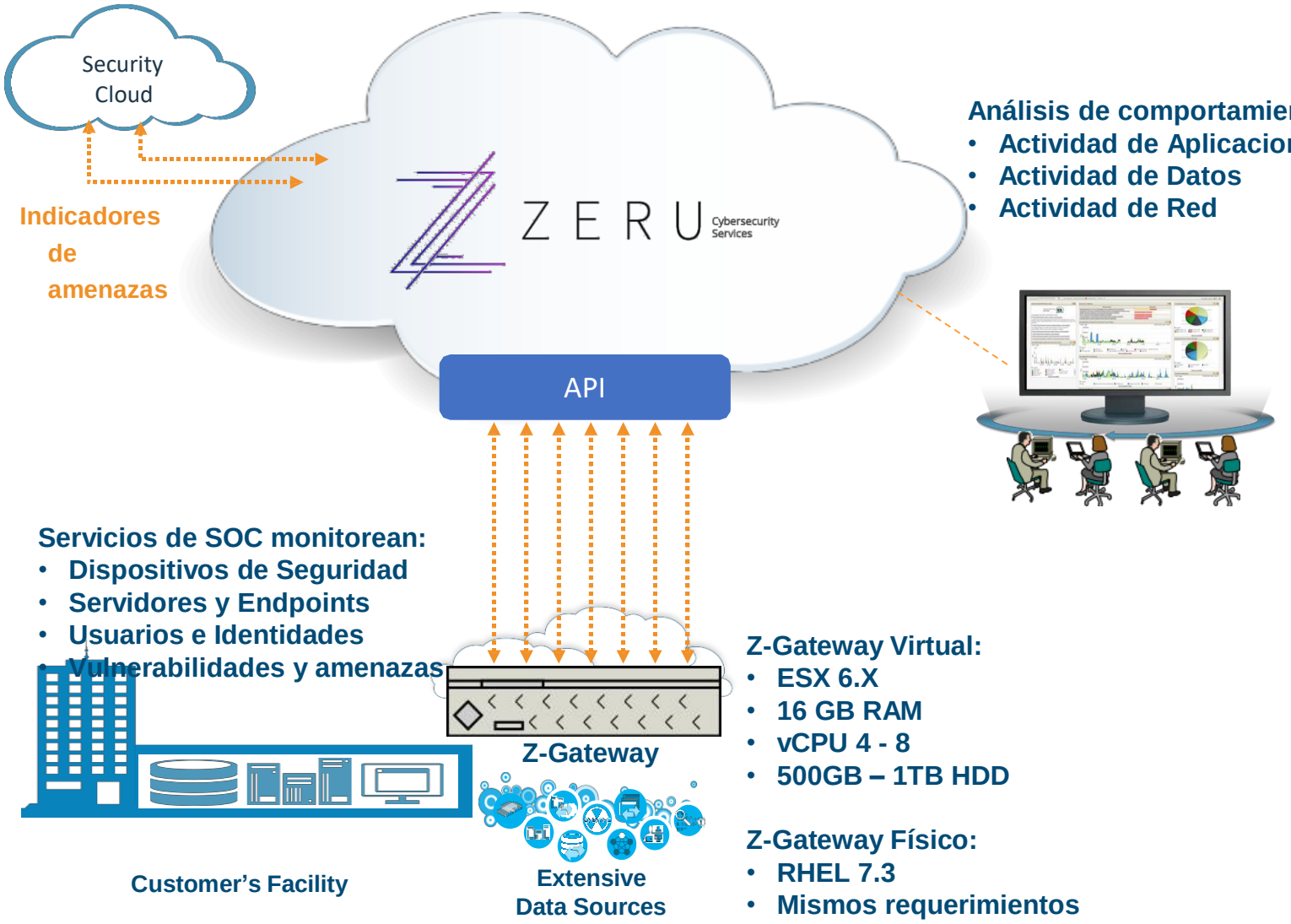
- Analisis de compromiso
- Vulnerability Coaching Remediation
- BaaS
- DRPaaS

Add-ons

- Analisis de código
- CISOaaS
- Ethical Hacking (Pentest)
- Analisis de Trafico red
- Procesos de Seguridad ISO 27k
- Antimalware IA

Zeru Cybersecurity Services

Arquitectura



Aspectos relevantes:

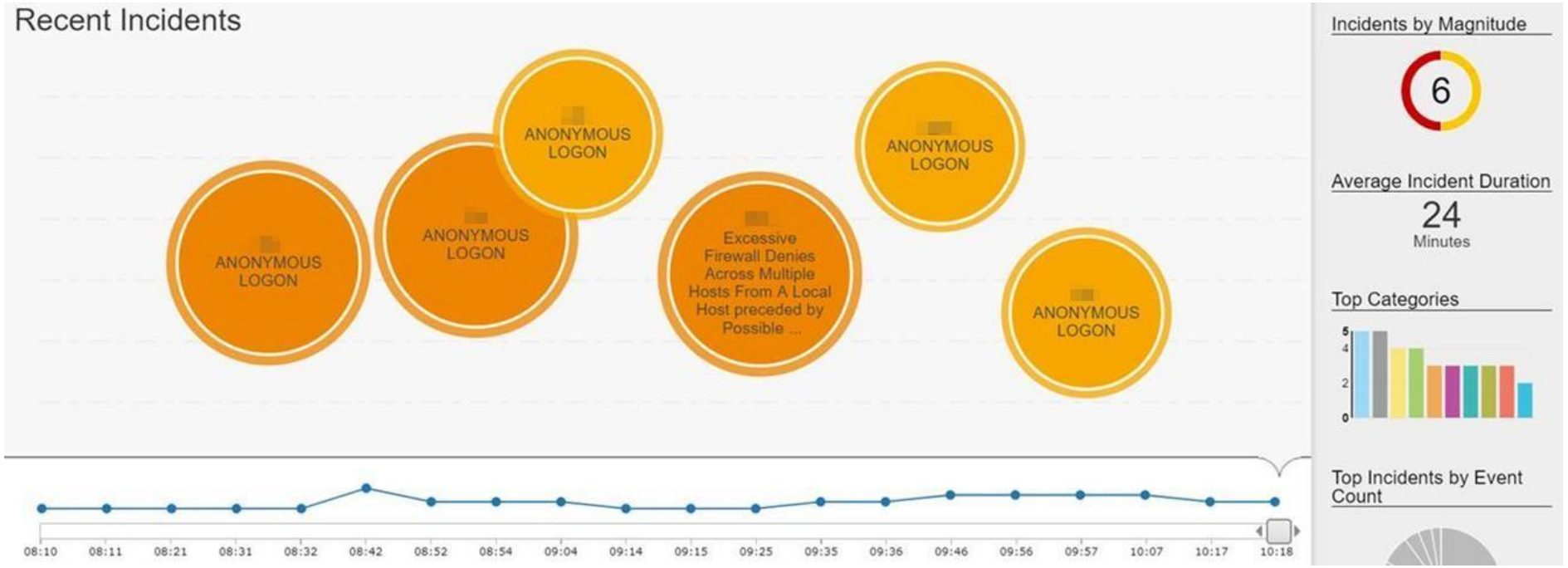
- Correlación histórica y en tiempo real de activos, eventos y vulnerabilidades
- Capacidades de AI para manejar eventos de seguridad
- Detección de amenazas avanzadas
- Reportes periódicos y bajo demanda
- Soporta integraciones de más de 450 soluciones de seguridad y TI
- ROI en menor tiempo

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)

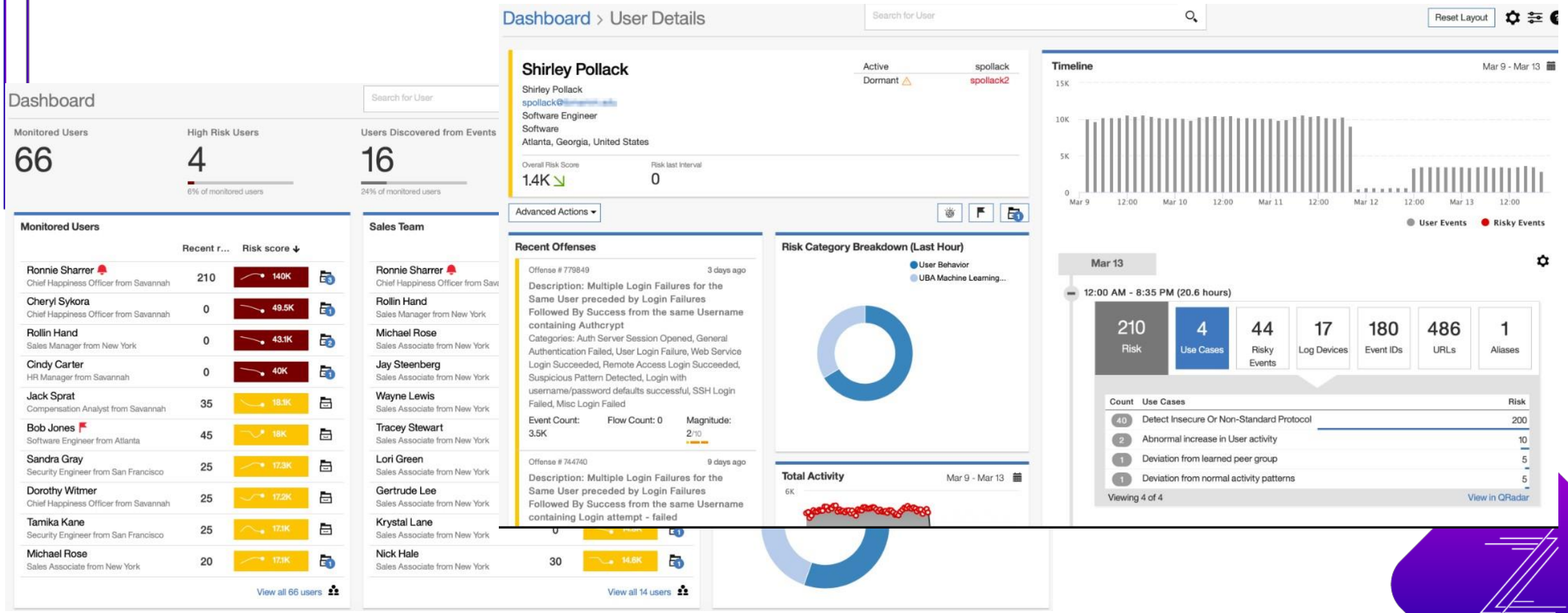
Zeru Cybersecurity Services

- **<u>Reportes de Incidentes Automatizados:</u>** 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.



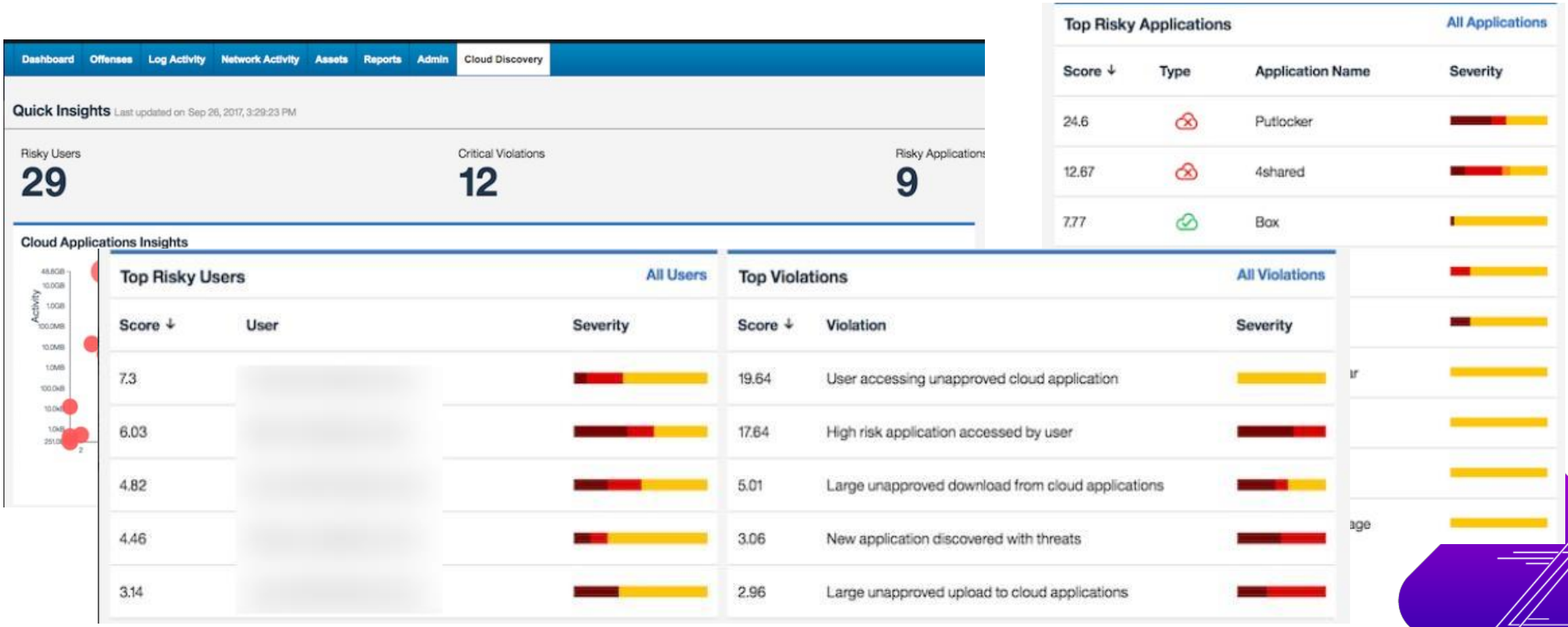
Zeru Cybersecurity Services

- **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.



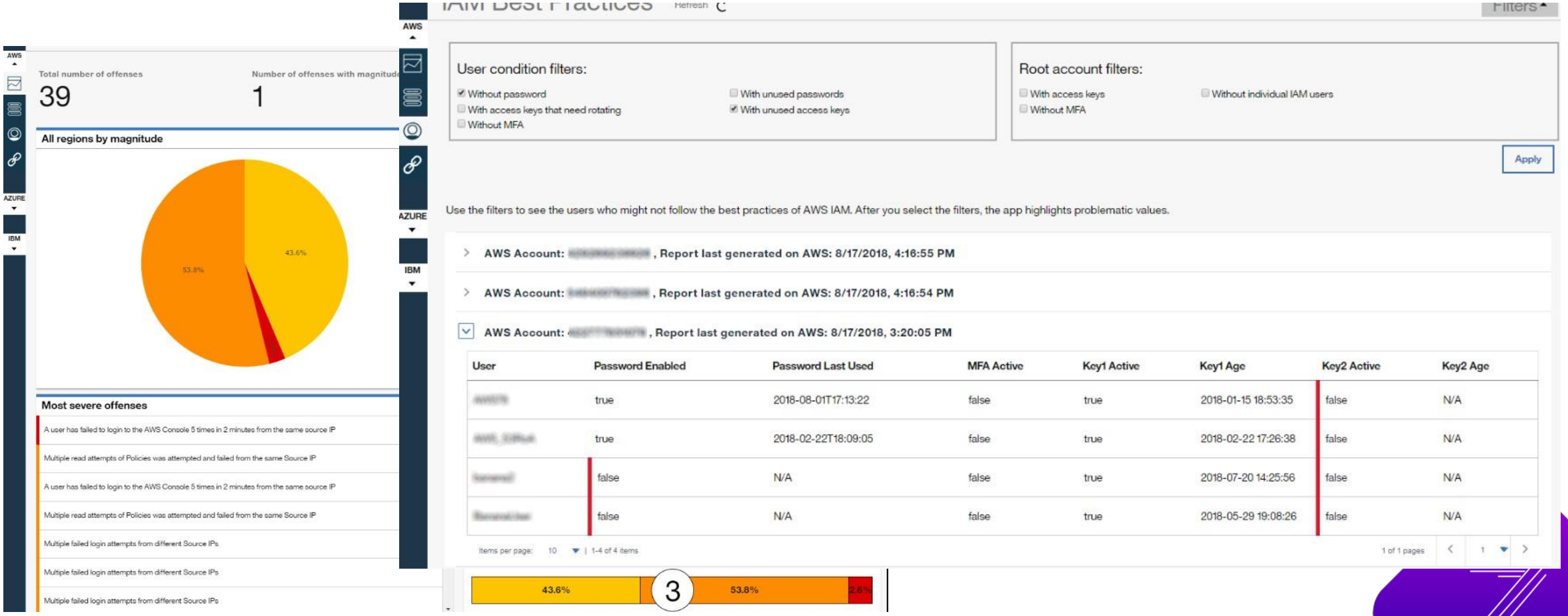
Zeru Cybersecurity Services

- **<u>Shadow IT Discovery:</u>** 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.



Zeru Cybersecurity Services

- **<u>Azure/AWS Threat Management:</u>** 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.

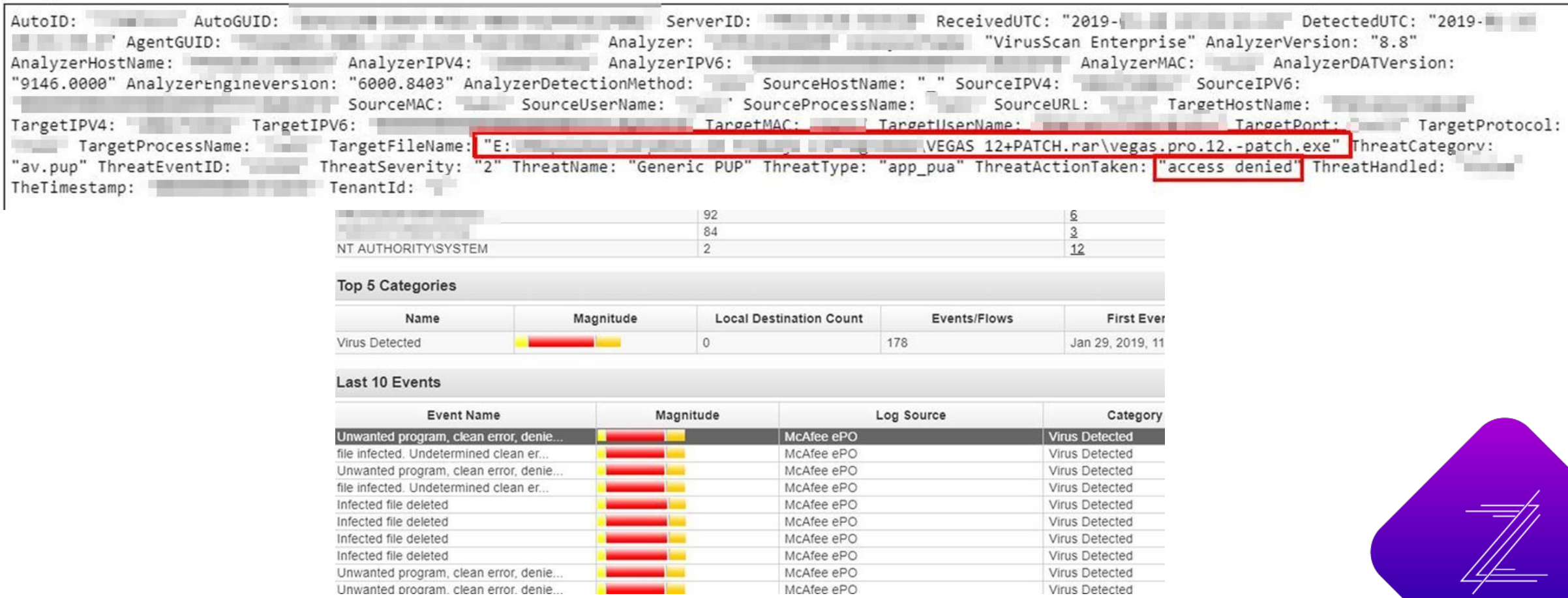


Zeru Cybersecurity Services

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

Zeru Cybersecurity Services

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

	92	6
	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

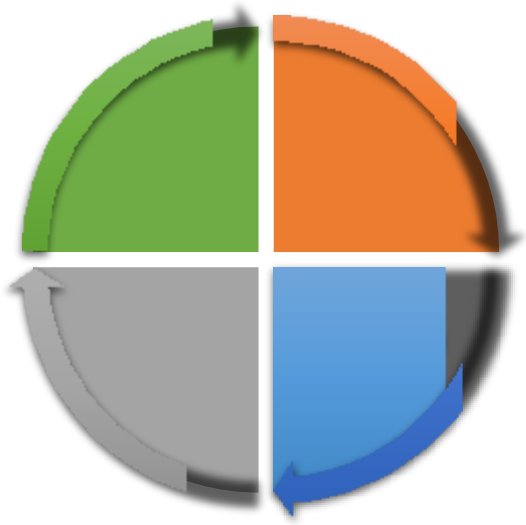
- **Incumplimiento de Políticas:** reducimos sus tiempos de remediación en incumplimiento de políticas, para que pueda corregir de manera orgánica toda desviación potencial.

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**	

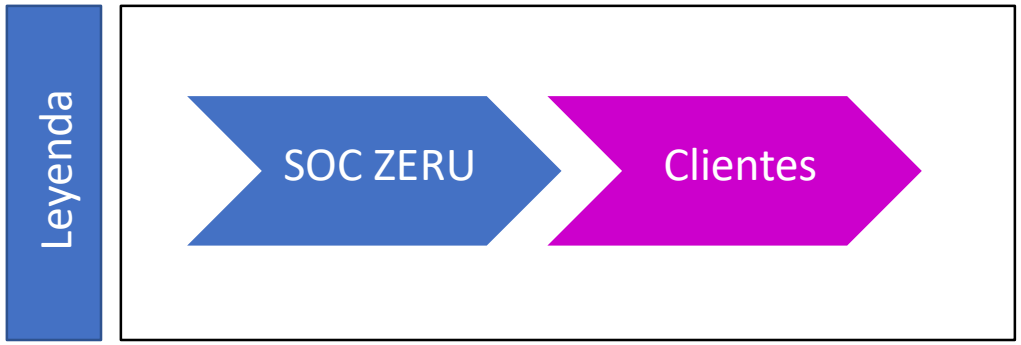
Qué incluye el Servicio?

- Monitoreo 7x24
  - AWS
  - Azure
  - O365
  - Firewall
  - Active Directory
  - Anti Virus Console
- SIEM Management
- Gestión de incidentes:
  - Detección
  - Triaje
  - 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

- Reconocimiento
- Construcción del Payload
- Entrega
- Explotación
- Instalación
- Comando y Control
- Acciones!

Ejercicio de Ingeniería Social

Ethical Hacking
Penetration Test

Análisis de Vulnerabilidades

Corporación Advisor Services

Manejo de Parcheo y Actualizaciones

Respaldo y Recuperación de Datos

Protección del Endpoint

Tratamiento de incidentes

Detección y Contención de Amenazas

Acompañamiento para Remediación

ZERU
SOC Services

ZERU

Cybersecurity Services

Powered By ADV

Le ofrecemos soluciones
integrales para aspectos críticos.

Su ciberseguridad es lo más importante.

Zer0 Malware

Zer0 Ataques

100% Prevención

https://advisor.com.ve