Guía de inicio del curso Ciber IQ

Onboarding para alumnos N1 y N2

El Concepto

Formación práctica en ciberseguridad defensiva.

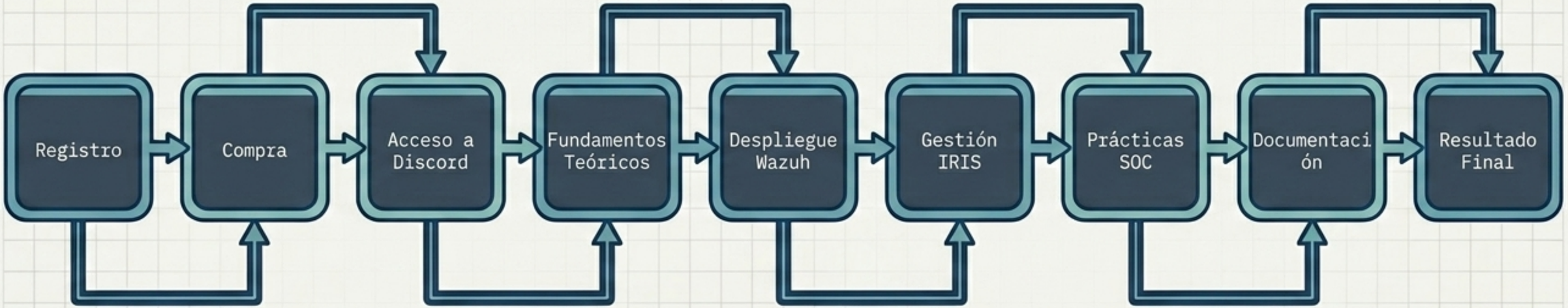
Orientación 100% a operativa real SOC y rol Blue Team.

Desarrollo de criterio técnico integral: desde la detección hasta la documentación.

Tus Objetivos

- Dominar la teoría técnica y estructural.
- Analizar alertas en un laboratorio con eventos reales o simulados controlados.
- Operar con plataformas SIEM líderes en el mercado.
- Gestionar incidentes y documentación profesional SOC.

La Ruta General del Analista



Pasos Siguientes

Post-Registro

- Confirmar correo electrónico.
- Acceder a la plataforma web.
- Ingresar a Discord mediante [URL_DISCORD]
- Leer guía inicial y normativa.

Post-Compra

- Activación automática del plan.
- Asignación de rol de seguridad en Discord.
- Desbloqueo de módulos teóricos.
- Provisión de accesos a Wazuh e IRIS.
- Autorización para inicio de prácticas.

Troubleshooting

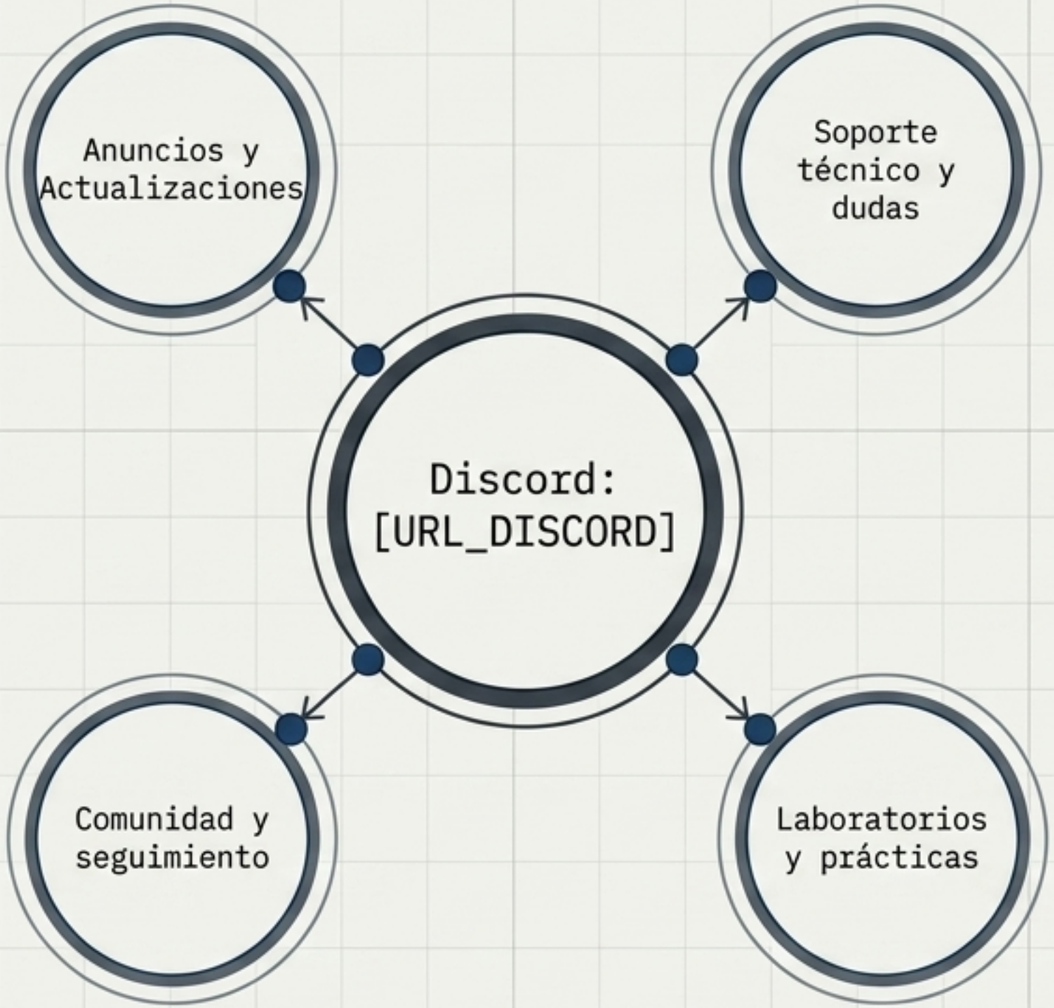
¿No ves el correo de confirmación? Revisa las carpetas de Spam o Promociones.
Soporte: [CANAL_SOPORTE] con [RESPONSABLE_SOPORTE]

Comparativa Táctica: Plan N1 vs Plan N2

Base Técnica (Ambos Planes)	Plan N1	Plan N2
Acceso a teoría, Discord, Wazuh e IRIS	✓	✓
Prácticas SOC y Análisis de alertas	✓	✓
Casos de uso, Dashboards y eventos	✓	✓
Documentación SOC y Soporte comunitario	✓	✓
Capa de Empleabilidad (Solo N2)		
Sesión 1:1 personalizada		✓
Revisión de CV y Optimización de LinkedIn		✓
Orientación laboral y Preparación para candidaturas SOC		✓

Plan N1 = Maestría Técnica Operativa | Plan N2 = Maestría Técnica + Posicionamiento Profesional

Integración con la Comunidad Táctica



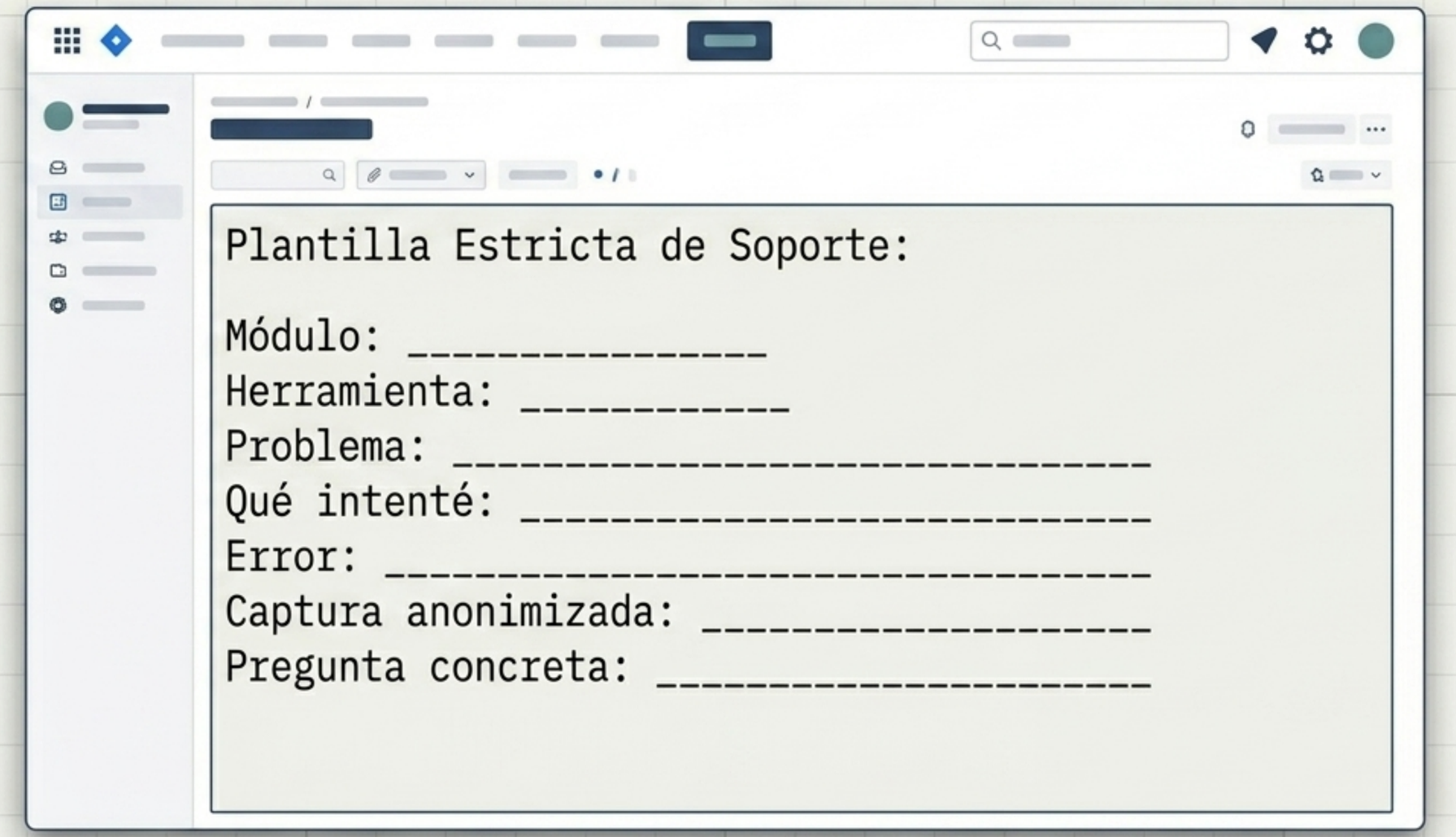
Canales Prioritarios

Bienvenida | Normas | Guía del servidor | Anuncios | Actualizaciones | Soporte por módulos | Laboratorios y práctica | Análisis de alertas

Protocolo de Presentación

Indica:
Nombre/Alias, Nivel actual, Background (IT, redes, desde cero), Objetivo, Plan (N1/N2)

Protocolo de Escalado y Soporte



El uso de esta plantilla es obligatorio para mantener el estándar de la industria en la resolución de incidentes.

Arsenal Defensivo: Wazuh (SIEM Principal)

- [x] Monitorización mediante alertas y eventos.
- [x] Despliegue y gestión de agentes.
- [x] Revisión de reglas y mapeo con MITRE ATT&CK.
- [x] Filtrado de eventos y análisis de IPs/Hosts.
- [x] Interpretación de severidad de amenazas.
- [x] Investigación y documentación de hallazgos.

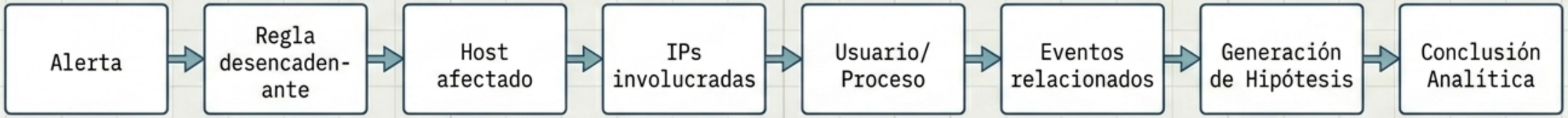
Operativa Wazuh: Acceso y Flujo de Análisis

Credenciales Seguras

URL: [URL_WAZUH]
Usuario: [USUARIO]
Clave: [CONTRASEÑA_TEMPORAL]

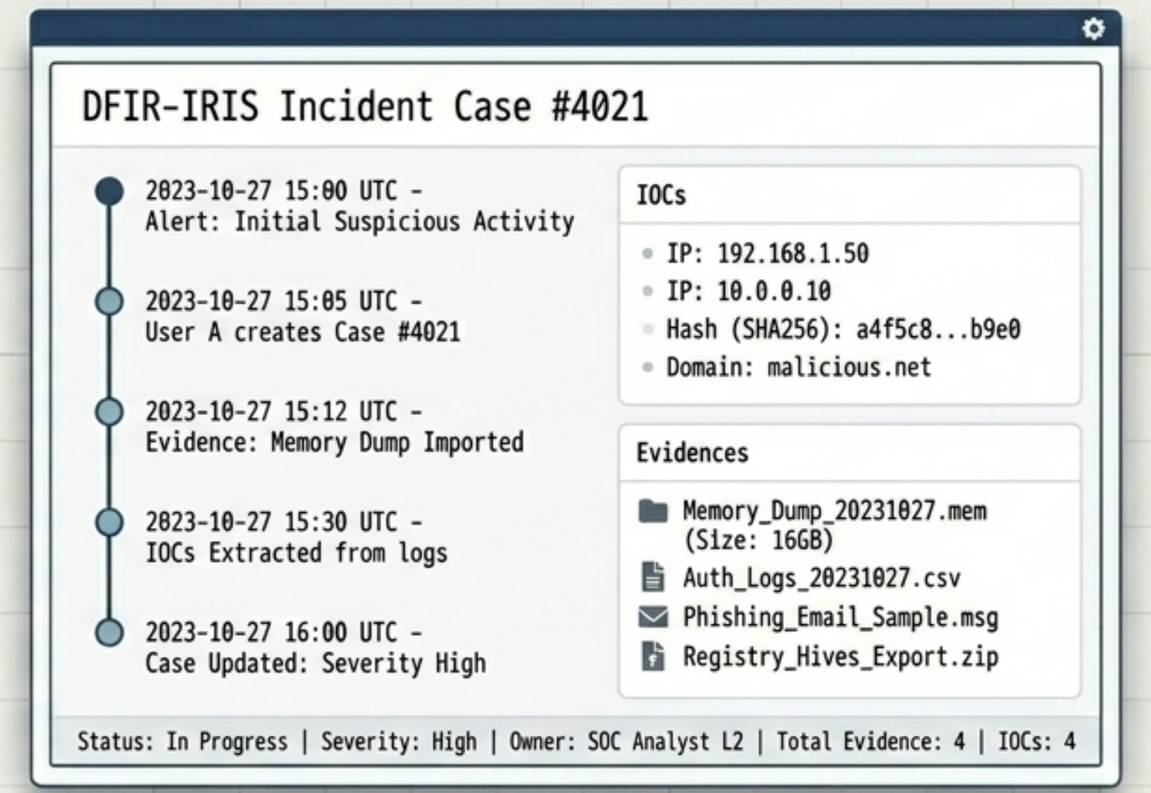
Las credenciales definitivas se entregan por canal seguro.

Triage Pipeline



Arsenal Defensivo: DFIR-IRIS (Gestión de Incidentes)

- Plataforma para transformar alertas en casos documentados.
- Creación integral de casos y cierre.
- Inserción y validación de evidencias.
- Documentación del Timeline del ataque.
- Registro y análisis de IOCs.
- Clasificación de criticidad y simulación de escalado.



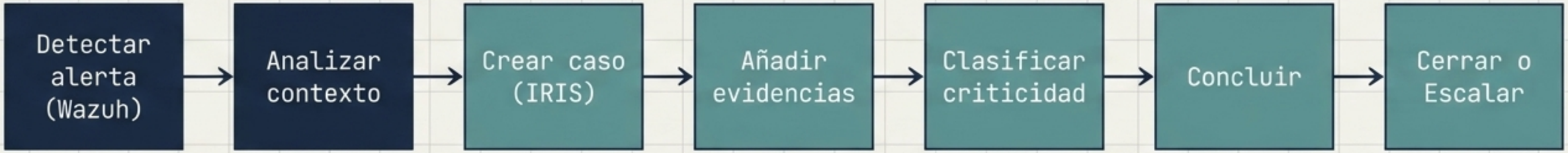
Operativa IRIS: Acceso y Puente Wazuh-IRIS

Credenciales Seguras

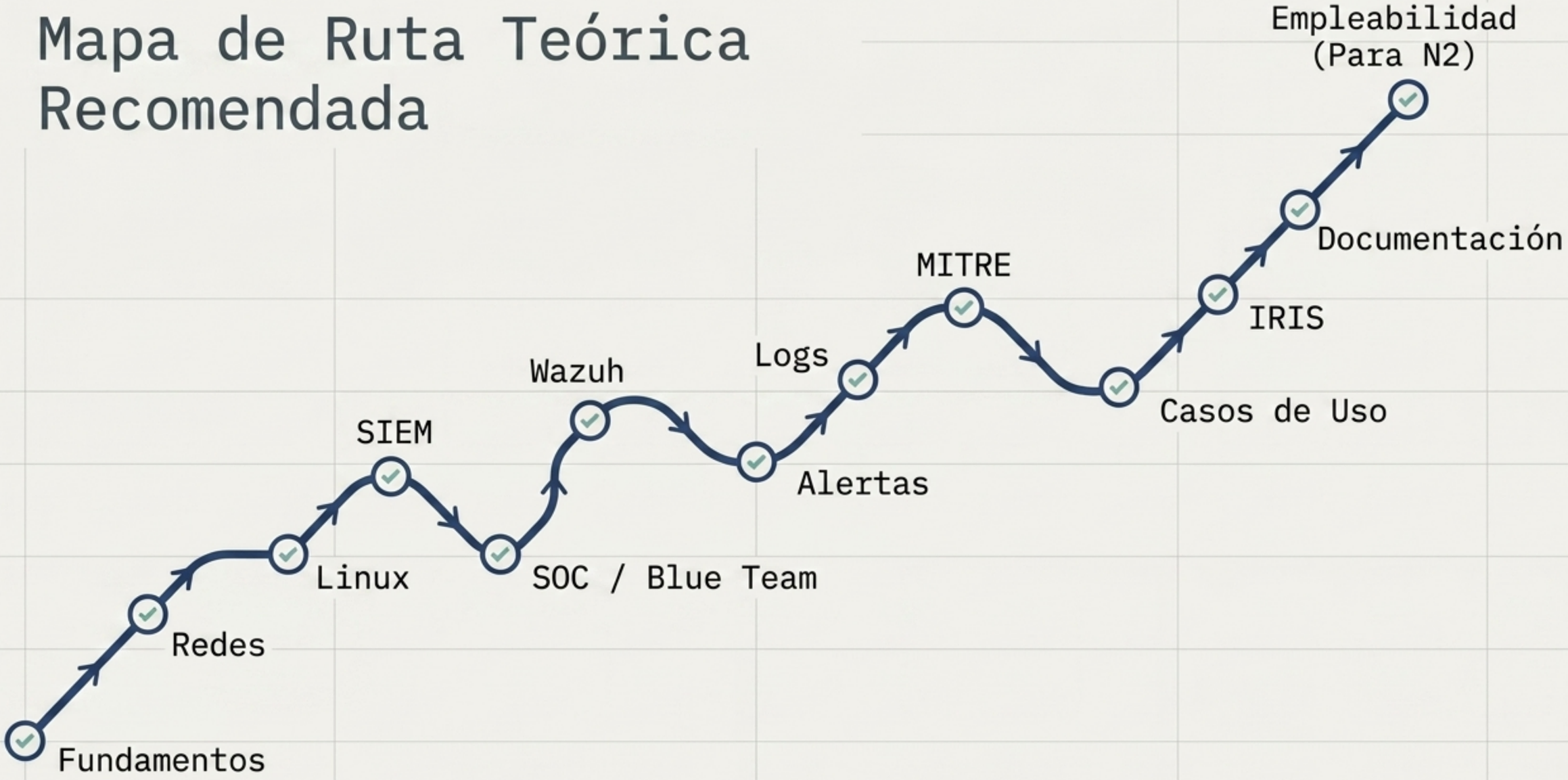
URL: [URL_IRIS]
Usuario: [USUARIO]
Clave: [CONTRASEÑA_TEMPORAL]

Acceso entregado por canal privado o sistema seguro.

Bridge Pipeline



Mapa de Ruta Teórica Recomendada

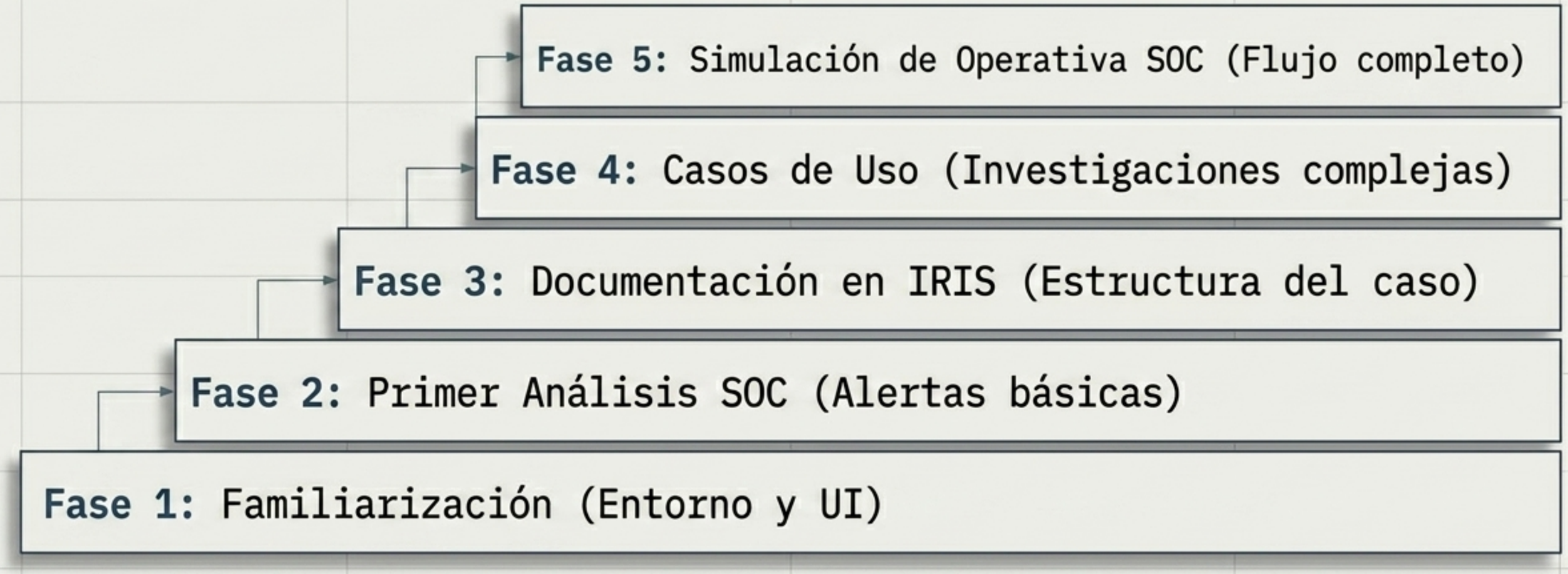


Criterios de Validación para Fase Práctica

Antes de acceder al laboratorio con eventos controlados, debes comprender con exactitud:

	1. Qué es un evento (Raw data).
	2. Qué es una alerta (Detección y trigger).
	3. Qué es una regla (Lógica condicional).
	4. Qué es una severidad (Nivel de impacto).
	5. Qué es un falso positivo (Ruido operativo).
	6. Qué es una conclusión SOC (Veredicto final).

Despliegue de Práctica por Fases



Initializing Mission...

Terminal Output - /bin/bash

```
> Ejecutar paso 1: Confirma tu registro web.
> Ejecutar paso 2: Accede a [URL_DISCORD].
> Ejecutar paso 3: Lee y acepta la normativa de seguridad.
> Ejecutar paso 4: Inicia el primer módulo teórico.
```

Bienvenido al Blue Team. La misión comienza ahora.