



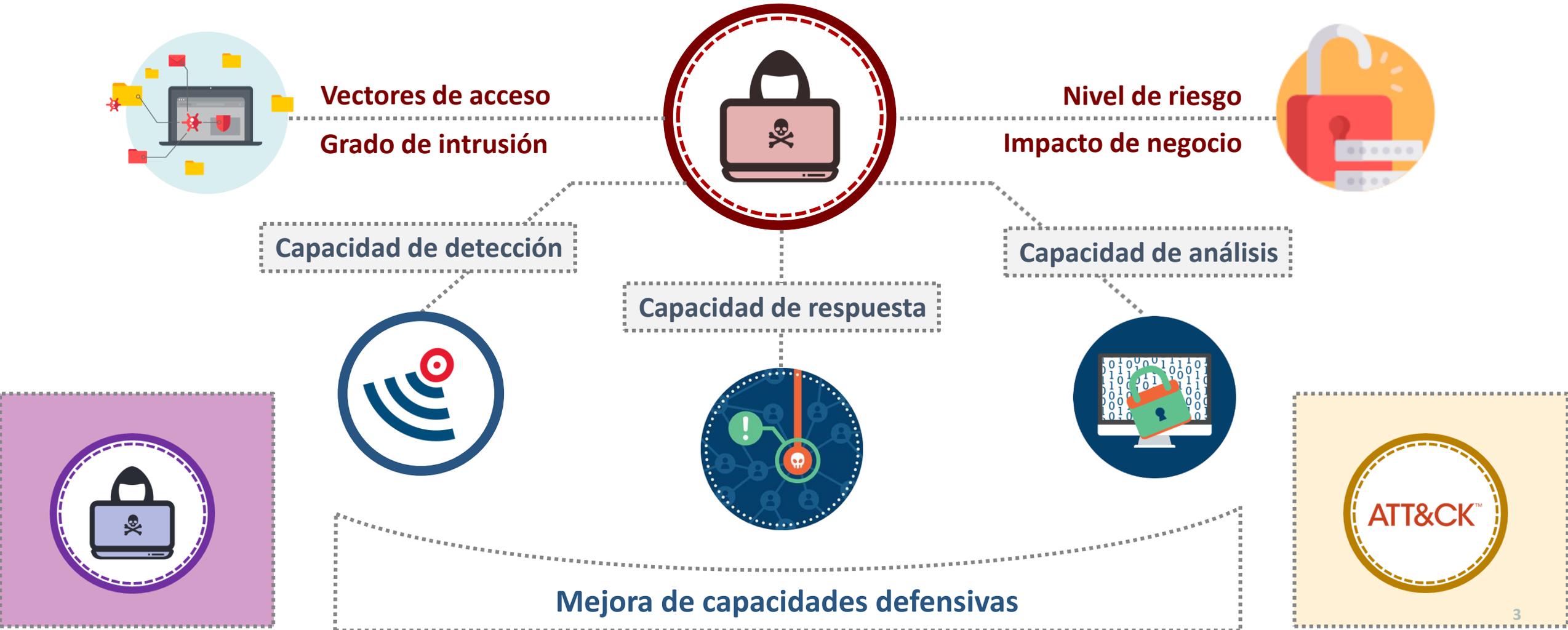
Innotec

SECURITY

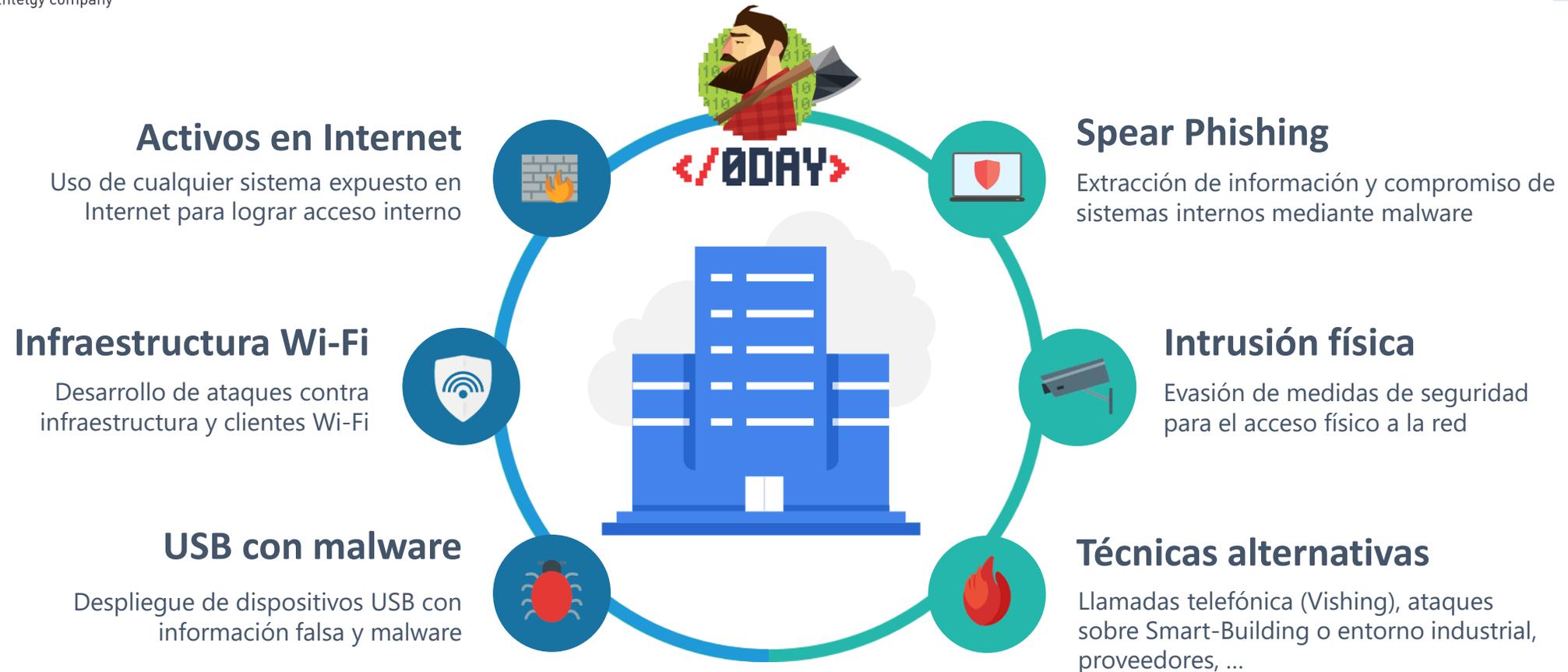
An Entelgy company

Enfoques y aspectos clave en ejercicios Red Team

EVOLUCIÓN FRENTE A ATAQUES DIRIGIDOS







- Modelo de evolución
- Combinación de vectores
- Vector de acceso interno



Intrusión interna

- Infraestructura (VPS)
- Binarios sin firma
- Sistema de trazabilidad
- Acciones manuales
- Análisis interno
- Backdoors alternativas



Obtención documentos

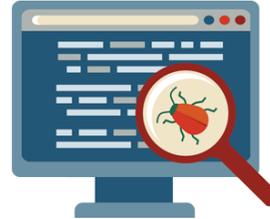
Extracción de metadatos

Identificación matriculas

Creación diccionario

Fuerza bruta contra VPN

Acceso a la red interna



Preparación pretexto

Envío ratón USB

Inyección de pulsaciones

Ejecución de PowerShell

Conexión a OneDrive

Ejecución remota

Extracción credenciales

Acceso vía VPN



Búsqueda teléfonos

Preparación pretexto

Creación red Wi-Fi

Llamada telefónica

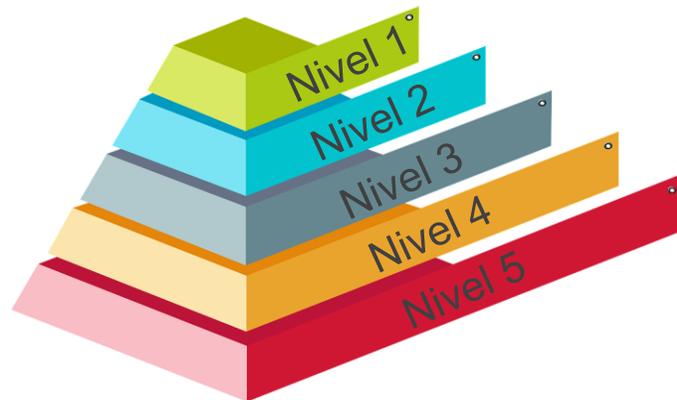
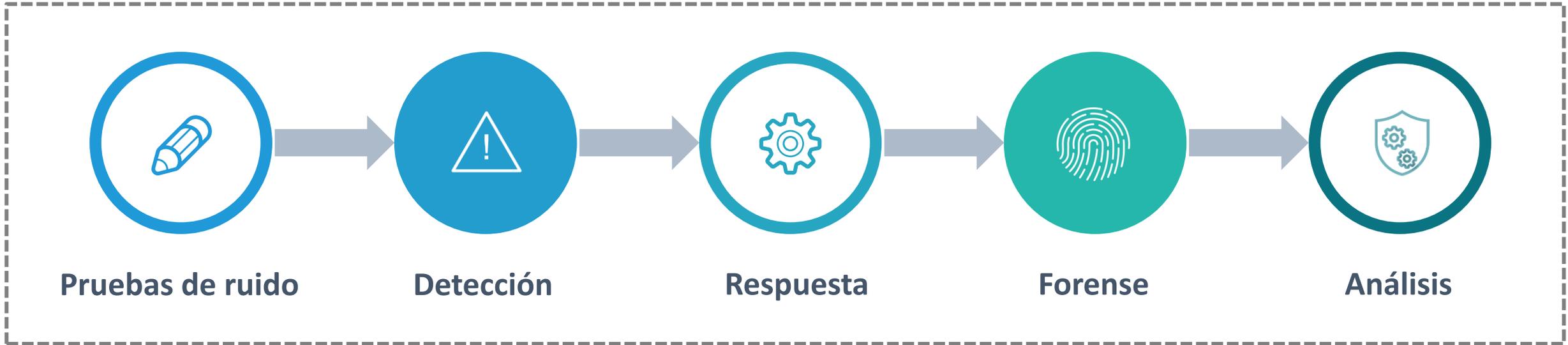
Captura de credenciales

Acceso remoto a equipo

Conexión inversa (DNS)



Análisis de capacidades



Desarrollo de pruebas sobre ámbitos internos:

- Directorio activo
- Seguridad en sistemas
- Seguridad en red
- Seguridad en ICS
- Exfiltración de información

01. Resultados del ejercicio

Presentación de riesgos, resultados y recomendaciones del ejercicio

03. Análisis y ataque

Workshop para el análisis de la infraestructura y ataque sobre ella

05. Planes de actuación

Workshop para la revisión y definición de planes de acción



02. Formación ofensiva

Exposición de Técnicas, Tácticas y Procedimientos de ataque habituales.

04. Simulaciones - Wargame

Workshop con ejercicios teóricos de ataque - defensa



¡Muchas gracias!
¿Preguntas?

