Análisis de vulnerabilidades	Escaneo de los activos de la organización en busca de vulnerabilidades en sistemas, red, servicios, software, etc. El objetivo es saber cuál es el estado en materia de ciber seguridad y buscar soluciones. • Interno: auditar activos de la red LAN, el auditor está conectado a la red LAN. • Externo: auditar activos públicos en internet.
Análisis de vulnerabilidades automatizado	Análisis de vulnerabilidades, pero mediante el uso de herramientas automatizadas, al ser un trabajo menos manual se reducen las jornadas necesarias, el valor añadido es la interpretación de los resultados por parte del auditor. Solo está disponible en modalidad interna.
Análisis de vulnerabilidades industrial (ICS/OT)	Análisis de vulnerabilidades de sistemas, red y servicios industriales. El objetivo es saber cuál es el estado de los activos ICS en materia de ciber seguridad y buscar soluciones.
Análisis de vulnerabilidades IoT	Análisis de vulnerabilidades de dispositivos y protocolos IoT “internet of things”, orientado a organizaciones que quieran desarrollar un producto IoT seguro.
Análisis de vulnerabilidades Web CMS	Análisis de vulnerabilidades en Webs construidas con los CMS más comunes como: Wordpress, Joomla, Drupal, etc.
Análisis de vulnerabilidades Web	Análisis de vulnerabilidades de Webs usando la metodología OWASP.
Test de intrusión	El test de intrusión o "pentest", consiste en una prueba de seguridad ofensiva que simula un ciber ataque real en un entorno controlado. El objetivo es identificar las debilidades que podrían ser aprovechadas por un atacante y demostrar así amenazas de robo de información, acceso indebido, caídas de servicios o la instalación de malware, etc. • Interno: el auditor realiza la auditoria conectado a la red LAN. • Externo: el auditor realiza la auditoria desde Internet.
Test de Ingeniería social - estadístico	Test que busca evaluar la concienciación en ciberseguridad de los miembros de una organización usando técnicas de ingeniería social, los resultados del test se recopilan en un informe estadístico.

Test de Ingeniería social - intrusión	Test en el que usando técnicas de ingeniería social trata de simular una intrusión real en la organización, con el fin de demostrar y evaluar las medidas de protección.
Análisis de vulnerabilidades Wifi	Análisis de las vulnerabilidades de las redes Wifi de una organización usando la metodología OWISAM personalizada.
Análisis de código	Análisis del código fuente de forma estática y dinámica para encontrar fallos de seguridad y corregirlos antes de la puesta en producción.
Red Team	Es el ejercicio de ciberseguridad ofensiva más completo y duradero, implica a un equipo de auditores con habilidades múltiples que tienen que cumplir una serie de objetivos de intrusión previamente definidos. Los ejercicios de Red Team son ideales para organizaciones maduras en materia de ciberseguridad. El objetivo es poner a prueba la infraestructura de seguridad y el Blue Team de la organización.