C.A.R F.C
ALINEACÍON SOC

CLASIFICATORIAS COPA SEGURIDAD DIGITAL 2030
ESTADIO: BLACK HAT ARCHEYPE

EL ENEMIGO NUNCA DUERME
NOSOTROS TAMPOCO
SEGURIDAD DIGITAL

¿Por qué el equipo de fútbol es exitoso con la alineación SOC?

Revisan sus partidos y entrenan continuamente para mejorar su desempeño. Se centran en la comunicación y colaboración entre los jugadores para ejecutar estrategias de manera efectiva. Responden rápidamente a las tácticas del oponente, ha sido crucial en los partidos ganados. Siempre están atentos, defendiendo su portería y atacando cuando es posible para ganar el partido.

DT : DIRECTOR DE CIBERSEGURIDAD

¿QUÉ HACE CADA JUGADOR DEL EQUIPO?

PERFIL DEL JUGADOR

23 GERENTE SOC
Defie la visión del equipo. Evalua las cuestiones presupuestarias y de recursos.

7 ESPECIALISTA RED-TEAM
Busca activamente lagunas en la red/sistema/configuración

15 LÍDER DEL SOC
Coordina con todos los miembros del equipo. Definie y documenta el proceso. Ejecuta las operaciones.

13 ANALISTA DE SEGURIDAD SENIOR
Segunda línea de seguimiento. Con más experiencia en análisis de seguridad.

10 INGENIERO SIEM
Configura, ajusta y mantiene la solución SIEM

8 ESPECIALISTA EN CONFORMIDAD Y AUDITORÍA
Asegura que la organización cumpla con todas las normativas, regulaciones y estándares de seguridad aplicables.

9 ANALISTA DE SEGURIDAD
Primera línea de monitoreo. Monitorea en pantalla. Análisis básico, siguiendo procedimientos operativos estándar (SOP) y guías de actuación (playbooks).

20 CAZADOR DE AMENAZAS
Explora activamente los datos SIEM para buscar actividades sospechosas, especialmente amenazas desconocidas o de día cero.

3 INVESTIGADOR DE INTELIGENCIA SOBRE AMENAZAS
Busca activamente información sobre amenazas y correlacionarla con los activos que pertenecen a la organización.

17 GESTOR DE INCIDENTES
Remedia los incidentes de seguridad lo antes posible según el análisis realizado por su compañero el analista de seguridad.

2 ESPECIALISTA FORENCSE
Analiza en profundidad los incidentes de seguridad. Colabora en la investigación de delitos cibernéticos.

ARBITRAJE

ANALISTA DE NOC

RIVAL DE PATIO

CLUB DEPORTIVO MALWARE

BALÓN DEL PARTIDO

BALL LOG

Suplentes 1: Ingeniero DevSecOps 2: Administrador de Seguridad de Redes 3: Arquitecto de Seguridad 3. Mesa de ayuda 4. Fabricantes

BHA