TECNOideas2.0 ciberseguretat i formació

PRESENTACIÓ

TECNOideas2.0 es una empresa que presta serveis de ciberseguretat, tant industrial com informàtica.

Què fem?

- Test d'intrusió —físics, sistemes o webs— en sistemes informàtics.
- Auditoria de seguretat en la industria 4.0.
- Anàlisi forense juntament amb perícia judicial.
- Consultoria legal en tecnologies de la informació.
- Formació. Cursos de seguretat per a empleats; per a directius d'empreses en general i també una formació més tècnica per a personal de tecnologies de la informació.

TECNOideas2.0 té més de deu anys d'experiència.

Vam néixer **a l'any 2009** oferint serveis informàtics generals, com venda i manteniment de xarxes i equips, gestió de projectes, etc. a tota mena de clients i en sectors molt diversos.

En el 2018 decidim especialitzar-nos en ciberseguretat, per l'augment de la demanda en aquests serveis per part dels nostres clients i per l'experiència **del nostre personal.**

TECNOideas2.0 posseeix personal qualificat.

El nostre personal **és especialista en ciberseguretat** i posseeix una dilatada experiència en els àmbits tecnològic, informàtic, industrial i empresarial.

Per a impartir formació, tenim **docents reconeguts**. Els nostres experts no sols tenen els coneixements tècnics, sinó que són **professors universitaris i del Basque Cybersecurity Center** i

dicten conferències en els millors esdeveniments de ciberseguretat d'Espanya.

A TECNOideas2.0 tenim un mètode propi de treball.

El nostre sistema es basa en els principis del hacking ètic, creixent i nodrint-nos de les fallades i el coneixement compartit. Investiguem l'entorn, busquem els defectes i forats dels sistemes; en definitiva ens posem en la pell d'un delinqüent.

Els nostres mètodes en auditories informàtiques **no inclouen l'ús de grans plataformes de programari (software),** però per a la indústria podem seguir llistats de ISOs, recomanacions sectorials, governamentals o qualsevol altra que sigui conforme amb les necessitats del client.

Fem ***pentesting*** (test de penetració) y qualsevol acció dins del **hacking ètic**, per a provar els seus sistemes. I repetim totes les auditories quan se suposen solucionades les fallades, per a la seva total seguretat i confiança.

A TECNOideas2.0 som ètics.

Hem enfocat la nostra visió empresarial en aquesta paraula.
Analitzem i detectem les fallades en els sistemes dels nostres clients.
Els informe del que han de fer.
Proposem les empreses que poden realitzar-ho. Solen ser empreses que també ens presten aquests serveis, o que consumim nosaltres, ja que l'exemple és la millor demostració de qualitat.

Per què? Creiem que no és ètic indicar als clients els problemes que tenen, solucionar-los i després certificar que ho hem solucionat.

No obstant això, sempre ajudem als clients en aquesta etapa. Busquem els millors professionals i solucions, ens comprometen a fer un seguiment i anar de la mà amb ells en tot el procés.

A TECNOideas2.0 parlem el vostre idioma.

Ens agrada que els client sens entenguin. **Claredat de conceptes**. Per això volem definir tres paraules que es repeteixen constantment en aquest sector:

Hacker: des de sempre s'ha desfigurat aquesta definició i se la fa sinònim de delinqüents informàtics.
Un *hacker* és algú que busca coneixement, provar-se dia a dia, compartir-ho i demostrar on ha arribat. Per exemple, mostrant-li a una empresa on té vulnerabilitats en els seus sistemes perquè li posin solució.

Si ho fa per a benefici propi, segrestant dades, fent que una empresa no pugui treballar o, en definitiva, buscant un lucre econòmic, és un **ciberdelinqüent**.
Si el que fa és vulnerar un programari (software) o maquinari (hardware), per a copiar-ho i revendre-ho pel seu compte, és un ***cracker***.

Test d'intrusió o pentesting o test de penetració: son un conjunt d'atacs simulats dirigits a un sistema informàtic per a detectar possibles febleses o vulnerabilitats, perquè siguin corregides i no puguin ser explotades.

***Hacking ètic*:** anàlisi en el qual es realitzen una sèrie de proves acordades amb el client, amb la finalitat de descobrir fallades de seguretat que puguin afectar a l'empresa i a la seva producció.

CIBERSEGURETAT INDUSTRIAL

- **Indústria 4.0**

La ciberseguretat industrial ja no pot ignorar-se.

Els responsables de IT/OT **necessiten avaluar la seguretat dels sistemes de control industrial i sistemes conjunts** (Entorns IT clàssics).

La quarta revolució industrial ja ha arribat, i inclou dispositius digitals i de comunicacions en l'entorn productiu o logístic.
Aquests dispositius són essencials per al bon funcionament industrial, són **elements crítics i en estar connectats a Internet, també són vulnerables.**

A TECNOideas2.0 som experts en dispositius industrials i posseïm la màxima certificació per a això.

Què oferim?
Serveis de ciberseguretat industrial que milloren i s'adapten als més exigents requeriments de qualitat.

Apliquem normatives i estàndards nacionals i internacionals per a poder complir amb totes les normatives, fins i tot les imposades de manera sectorial.

Quin és el problema?
Identifiquem els elements crítics que requereixen protecció immediata:

1. **Gestió dels permisos.**
   Abans, la majoria dels sistemes estaven aïllats. Ara **les xarxes IT y OT estan interconnectades**, amb la famosa "integració IT/OT".
   És necessari aplicar tècniques i implementacions de ciberseguretat en OT.
   >> Cal determinar els privilegis per a cada usuari autoritzat.
   >> Cal bloquejar els accessos als no autoritzats.

2. **Actualització de sistemes operatius: el maquinari (hardware) i el programari (software)**.
   Alguns sistemes hardware y software son anteriors al concepte de ciberseguretat.
   Cal garantir la compatibilitat amb les proteccions modernes.
   >>Software antivirus.
   >>Tecnologies d'escanejat d'amenaces.
   >>Plantejar bones polítiques d'*update* i apedaçament dels sistemes.

3. **Identificar els actius insegurs i els accessibles per IP des de l'exterior.**
   És el cas, per exemple, dels sensors i indicadors de pressió, plc's. hmi's, scada, etc.
   Les dades en aquests dispositius **poden ser manipulades**, la qual cosa impacta en la seguretat i fiabilitat de tot el sistema.
   Aquests sistemes són indexats per cercadors, que informaran

de les diferents vulnerabilitats dels sistemes i la seva disponibilitat.
Exemple: ***www.shodan.io***

4. **Bones pràctiques en la programació, desenvolupament i implementació.**
   Sovint s'usa i s'incorpora programari a mesura, però **programat amb escassa atenció a les tècniques de ciberseguretat**: el sistema OT queda exposat als atacs.
   Cal mantenir una bona praxi en totes les fases de desenvolupament i implementació dels sistemes.

5. **Polítiques de registre d'incidents.**
   Les empreses que estableixen un procés per a la notificació i comunicació d'esdeveniments del sistema poden usar aquestes dades per a detectar irregularitats i implementar mesures de seguretat.
   Cal monitoritzar l'activitat de l'empresa amb eines de supervisió, IDS, IPS, etc.

6. **Segmentació de la xarxa**.
   Una bona i ben definida segmentació de la xarxa, és la clau per a l'èxit en matèria de ciberseguretat.
   Moltes organitzacions no han separat encara les seves xarxes en diferents segments funcionals.
   Sense aquesta segmentació, les dades i les aplicacions infectades poden expandir-se d'un segment a un altre i els atacants que aconsegueixen traspassar les defenses perimetrals poden, fàcilment, moure's transversalment per la xarxa sense ser detectats.

7. **Pla de recuperació operacional i resposta davant incidents**.
   En el cas d'un atac, es necessita un procés documentat per a avaluar els danys, reparar sistemes i màquines i restablir les seves operacions.
   Els simulacres regulars de seguretat també ajuden els operadors a adoptar una recuperació ràpida i eficient.
   El pla ha d'establir prioritats, personal afectat, definició de cada rol dins la recuperació del desastre i retro-alimentació

d'aquest.

8. **Formació en matèria d'OT**.
   Moltes empreses tenen mancances de formació en matèria OT, la qual és imprescindible a l'hora d'establir polítiques de seguretat en aquests sistemes i complir amb les normatives existents.

Com ho fem?

Auditem aquests sistemes, que no solen estar tan ben protegits com deurien.

HMI's, scadas, sensors, etc. solen ser antics, i per això no compten amb una capa de protecció adequada en el seu disseny original.

Actuem en qualsevol sector i sigui quina sigui la grandària de l'empresa.

LLEGIU-NOS!

Tenim una sèrie d'articles tant en **el nostre blog** com a **Linkedin** per a reforçar la conscienciació que realitzem en quant a ciberseguretat industrial:

https://tecnoideas20.com/2020/02/06/exposicion-de-activos-ot/

https://tecnoideas20.com/2020/05/18/el-riesgo-cibernetico-por-sectores-salud-parte-i/

https://tecnoideas20.com/2020/05/07/el-riesgo-cibernetico-por-sectores-salud-parte-ii-farmaceuticas/

VEIEU-NOS!

I també podeu visitar el nostre **canal de Youtube**, on anem penjant presentacions, webinars, cursos, etc.

https://www.youtube.com/channel/UC7FRpS61xNxPUkIDCO8JuZw

FORMACIÓ

Per a completar la nostra oferta de ciberseguretat, oferim també diversos nivells de formació, ja que és un altre dels nostres punts forts.

És imprescindible una bona conscienciació per part de les empreses i dels seus treballadors dels riscos reals que existeixen en temes de ciberseguretat.

QUÈ OFERIM?

• **Petites xerrades de conscienciació** general o de temes més concrets i les seves solucions.

• **Xerrades a mida de les necessitats de la seva empresa.**

• **Formacions *in company***. Ens desplacem a la seva empresa per a oferir cursos o píndoles formatives a treballadors i directius, per a conscienciar i protegir els actius o formes segures de treballar.

• **Cursos per a professionals de tecnologies de la informació,** tant per als que estan actius com per als que es vulguin reciclar. Són formacions a diferents nivells dins de la ciberseguretat.

• **Tots els nostres cursos són bonificables** per a treballadors en actiu a través de la **Fundae** (Fundación Estatal para la Formación y el Empleo).

• Gairebé totes les nostres formacions **poden realitzar-se de manera presencial o en línia.**

Fundación Estatal
PARA LA FORMACIÓN EN EL EMPLEO

Aquesta és la nostra principal oferta formativa:

- **Ciberseguretat en el teletreball**
  Curs bàsic de 4 hores de durada.

- **Hacking ètic, bàsic i avançat**
  Cursos de 20 hores de durada.

- **Transformació digital de la indústria**
  Un curs de 12 hores de durada per a veure els avantatges de la tecnificació de la indústria i de la ciberseguretat en ella.

- **Auditories de sistemes de control industrial**
  Curs d'iniciació de 10 hores de durada.

- **Iniciació a forensia industrial**
  Curso d'iniciació de 20 hores.

- **Forense informàtic avançat**
  Curso de nivell mitjà de 20 hores.

- **Aplicant *machine learning* a la ciberseguretat**
  Curs de 25 hores.

- **I molts més cursos cada mes. A mesura també realitzem formacions segons les necessitats del seu personal.**
-

Més informació sobre els nostres cursos, AQUÍ.

Principals certificacions de TECNOideas2.0

La nostra professionalitat i bon fer queden patents en les següents certificacions obtingudes per la nostra empresa i els nostres professionals.

Formem part des del 2019 del Catàleg de l'Incibe, l'Instituto de Ciberseguridad de España.

Posseïm la màxima certificació professional (nivell Negre) del Centro de Ciberseguridad Industrial.

I a més posseïm aquestes **certificacions internacionals**:

EC-Council

CEH Certified Ethical Hacker
ETHICAL HACKER
PRACTICAL

CISSP®
Certified Information Systems Security Professional

Information Security Management System
ISO 27001 Certified
Lead Auditor

ISO 27001
INFORMATION SECURITY
MANAGEMENT SYSTEM