PRINCIPIOS DE CIBERSEGURIDAD

DOMINA LOS CONCEPTOS CLAVE

@PAOLAMEDRANO

LA TRIADA CID

Modelo que representa los principios fundacionales de la seguridad.

CONFIDENCIALIDAD

INTEGRIDAD **DISPONIBILIDAD**

Asegura que estás en el camino correcto para crear sistemas, datos y entornos seguros.

CONFIDENCIALIDAD

PALABRA CLAVE

PRIVACIDAD

CONCEPTO

Asegurar de que sólo las personas que tengan acceso a los sistemas y ver los datos puedan hacerlo.

EJEMPLO

Tener estrictas medidas de control de acceso como MFA

Cifrado de los datos en en reposo, en tránsito y en uso

INTEGRIDAD

PALABRA CLAVE

Veracidad y autenticidad de los datos

CONCEPTO

Asegurar que nuestros sistemas y datos están exactamente en el estado en que se supone que deben estar, y no han sido modificados de ninguna manera.

EJEMPLO

Hash de datos en tránsito y en reposo

Firmas digitales como certificados SSL/TTS

DISPONIBILIDAD

PALABRA CLAVE

GARANTÍA Y RESILENCIA

CONCEPTO

Asegurar que los sistemas funcionen como deben, cuando deben para que los datos estén disponibles cuando y donde se necesiten.

EJEMPLO

Servidores y bases de datos de respaldo

Rutas redundantes en toda la red

CONCEPTOS IMPORTANTES EN CIBERSEGURIDAD

@PAOLAMEDRANO

VULNERABILIDAD

CONCEPTO

Una **debilidad** en cualquier parte de una empresa que, si se explota, podría poner en peligro la CID de los sistemas y los datos.

EJEMPLOS

- Software sin parchear
- Uso de privilegios de superusuario o cuenta de administrador
- Puertos y protocolos abiertos que no son necesarios
- Errores de seguridad desconocidos en software o interfaces de programación
- Datos no cifrados en la red
- Vulnerabilidad de día cero

@PAOLAMEDRANO

EXPLOIT

CONCEPTO

Cualquier cosa que pueda **aprovecharse** de una **vulnerabilidad.**

EJEMPLOS

- Ataque de inyección SQL
- Secuencias de comandos en sitios cruzados (XSS)
- Desbordamiento del búfer
- Violación de la seguridad de la memoria
- Error de validación de entrada
- Ejecución remota de código
- Escalada de privilegios
- Explotación de día cero
- Falsificación de petición en sitios cruzados

@PAOLAMEDRANO

AMENAZA

CONCEPTO

Cualquier persona o cosa que pueda **explotar** vulnerabilidades en un entorno.

EJEMPLOS

- Malware y ransomware
- Virus, gusanos y programas espía
- Amenazas internas
- Amenazas externas
- Redes de bots

RIESGO

CONCEPTO

La **probabilidad** o posibilidad de que alguien o algo pueda **explotar** una v**ulnerabilidad** en un entorno

EJEMPLOS

- Evaluación cuantitativa del riesgo
- Evaluación cualitativa del riesgo

ENDURECIMIENTO

CONCEPTO

El acto de **corregir vulnerabilidades** en un entorno para **eliminar o reducir** el **riesgo** asociado a una amenaza que podría explotar una vulnerabilidad

EJEMPLOS

- Endurecimiento:
  - Sistema operativo (SO)
  - Servidores
  - Endpoint
  - Redes
  - Bases de datos
- Protección de aplicaciones
- Protección mediante contraseña
- Restricción del acceso físico y a la red
- Uso de antivirus, malware y spyware y spyware

@PAOLAMEDRANO

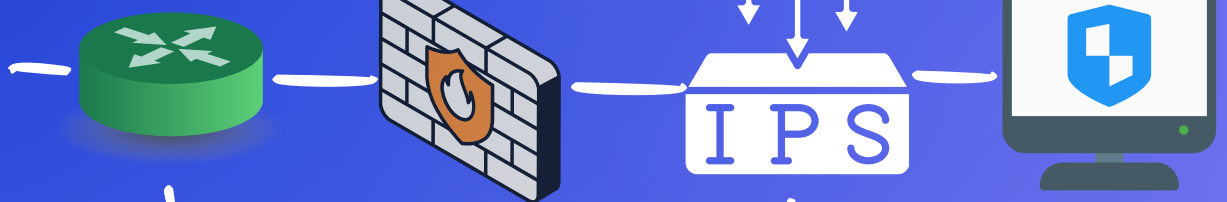
DEFENSA EN PROFUNDIDAD

CONCEPTO

Una **estrategia** que utiliza **multitud de medidas** para defenderse contra diversas amenazas.

Proporciona una inspección de paquetes/aplicaciones más profunda

Firewall, IPS, Antivirus y antimalware del host.



Router con una ACL que filtra el tráfico basándose en direcciones puertos y protocolos

Detectar anomalías

@PAOLAMEDRANO

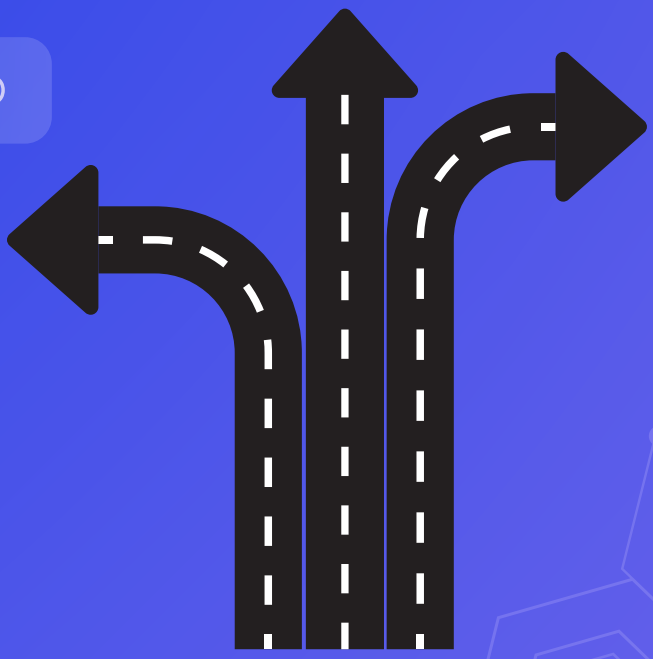
VECTOR DE ATAQUE

CONCEPTO

El **método o ruta** que un ciberdelincuente utiliza para un ataque para explotar vulnerabilidades.

EJEMPLOS

- Denegación de servicio distribuida (DDoS)
- Vulnerabilidad de día cero
- Phishing
- Ingeniería social
- Escaneo activo o pasivo



PEQUEÑO REPASO...

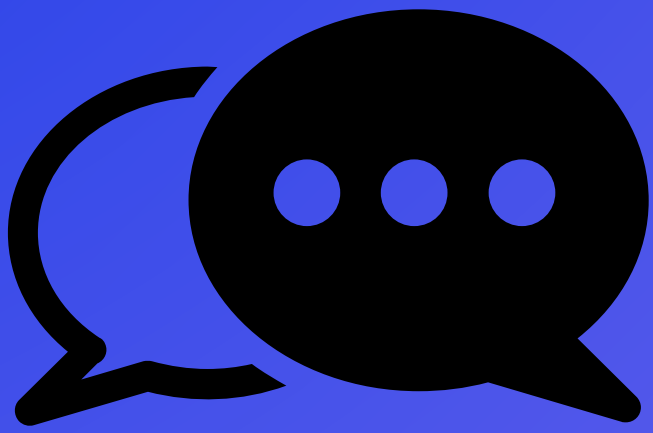
¿Cuál de las siguientes opciones identifica correctamente lo que sería un software sin parches?

a. Amenaza

b. Explotación

c. Vulnerabilidad

d. Endurecimiento



No olvides comentar la respuesta correcta :)

@PAOLAMEDRANO