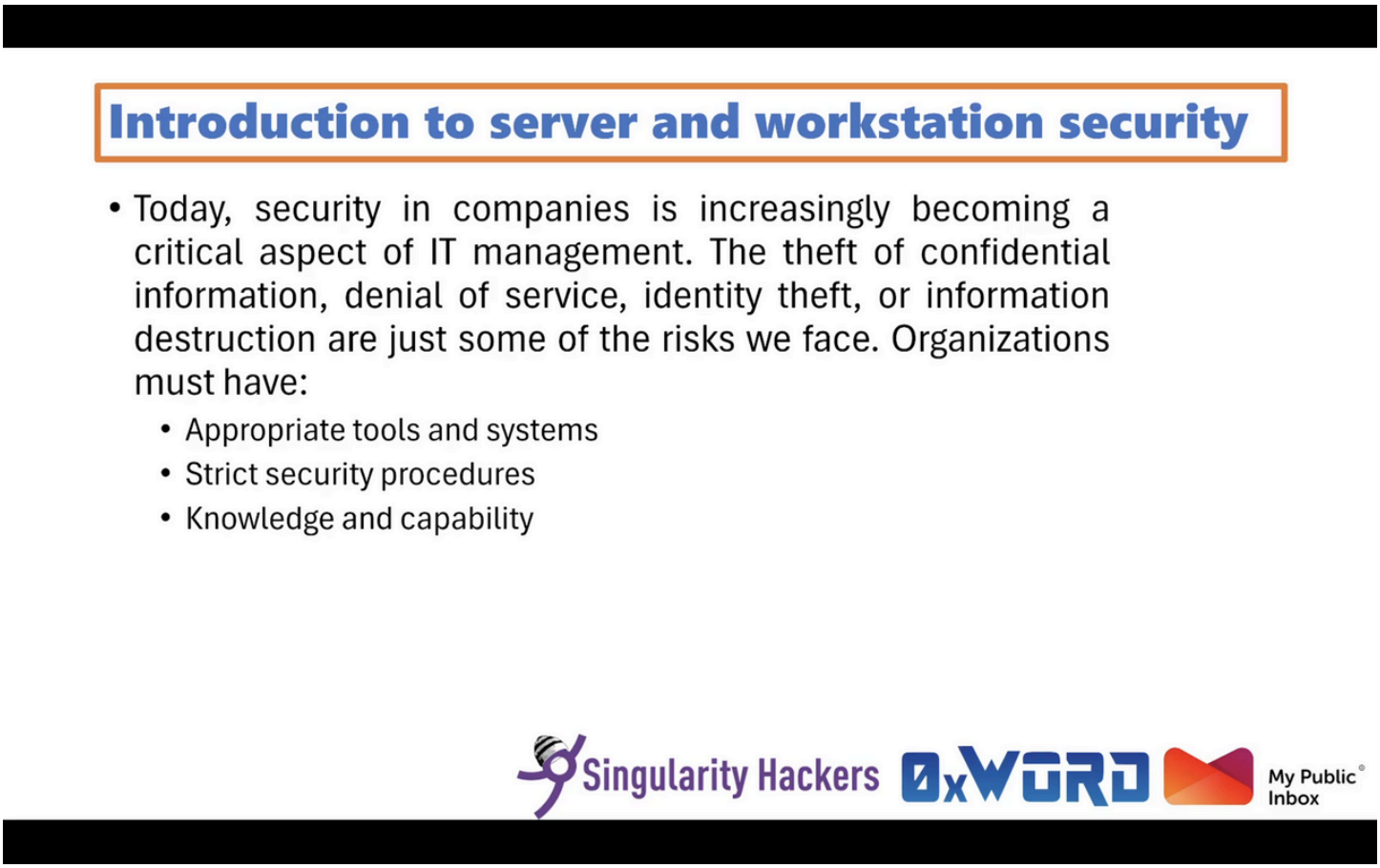
Introducción a la fortificación en sistemas GNU/Linux

Vamos a hablar de la introducción a la fortificación en sistemas Linux.

Hablaremos un poco del marco teórico y hablaremos de algunas cosas como pueden ser la introducción a la fortificación o la seguridad de servidores y estaciones de trabajo. Y volveremos a tocar el tema del modelo de defensa en profundidad (Defense in Depth) para entender que ya sean sistemas Windows, sistemas Linux, clientes Windows, clientes Linux, al final la fortificación la iremos realizando por capas.

Es cierto que en este módulo nos vamos a centrar en la parte de fortificación de sistemas Linux, por lo cual vamos a utilizar sobre todo las capas del nivel de hosting dentro del modelo de defensa en profundidad y a nivel de aplicación.



Empezamos hablando de que hoy en día sabemos que la seguridad en las empresas o en las organizaciones es cada vez un aspecto más crítico. Muchas noticias han ido saliendo, en esta misma formación, habéis visto algunos casos donde se refleja la importancia, la justificación en la inversión que tiene que hacer en en seguridad de información, en ciberseguridad y al final el robo de información confidencial, la servicio, la suplantación de identidad, el fraude, la destrucción de la propia información a través de diferentes operativas como puede ser el uso de

un malware o el uso incluso un atacante que quiere dañar a una organización, son riesgos a los que se enfrentan las organizaciones diariamente.

Por esto las organizaciones deben disponer, aparte de que tengamos un montón de soluciones técnicas, de firewalls, IDS, de IPS, anti malware, de políticas de equipo, etc. Necesitamos disponer de herramientas y sistemas adecuados, es decir, no por tener un IDS, no por tener un IPS, no por tener un firewall voy a estar más protegido o no, sino que debo tener el sistema adecuado, con una configuración adecuada y con un trato adecuado dentro de un sistema diseñado para defendernos de manera acorde.

Además debemos tener procedimientos de seguridad estrictos, es decir, debemos disponer primero diseñar ese plan de seguridad, esas políticas de seguridad y bajarlo desde arriba, desde la alta dirección hacia abajo. Esto es algo fundamental.

También necesitamos en las empresas o las organizaciones necesitan conocimiento y capacidad, esto es algo fundamental. Cada vez cobra más importancia al rol del Chief Knowledge Officer dentro de las organizaciones, es concentrar el conocimiento dentro de la organización, no externalizarlo y no depender de un tercero, sino que tener ese conocimiento y en el ámbito de ciberseguridad es algo fundamental tener ese conocimiento dentro de la organización y tener esas capacidades.

Capacidades cada uno a su nivel.

Es decir, no es lo mismo necesitar las capacidades que puede necesitar un contable de la organización o alguien de marketing, que por ejemplo alguien de IT.

Así que esto es algo importante también, ese conocimiento y capacidad en todas las organizaciones.

¿De qué nos vamos a proteger?

Nos preguntamos también un concepto que debemos entender para luego aplicar las fortificaciones.

¿De qué nos vamos a proteger? Todas esas amenazas que iremos viendo después, enumerándolas, pero lo primero es el software.

El software es algo fundamental, aparte del hardware, es algo fundamental dentro de las organizaciones y para la actividad de negocio.

Entonces nos podemos preguntar ¿Qué es el software seguro? ¿El software seguro qué es?

Bueno, pues el software seguro podemos decir que es el que se supone que hace lo que

debe hacer una aplicación que ha sido diseñada para realizar una tarea o X tareas y “nada más”. Esto de “nada más”, ¿Qué significa?

Si nos paramos a pensar en que es el software fiable, pues el software fiable podemos decir que es el software que hace lo que debe hacer.

Por ejemplo, si nosotros tenemos una aplicación que le damos una serie de números, hace una serie de operaciones y nos da el resultado, podemos decir que ése software es fiable porque está funcionando, pero puede ser que haya algún tipo de entrada, algún tipo de input a ese software, que de repente el software no haga todo para lo que está programado, sino que realmente haga otra cosa.

Eso es lo que corresponderíamos con ese “nada más”.

En el software seguro se supone que están “validadas” las entradas, de forma que no encontraremos un flujo de ejecución diferente para el cual fue diseñado el software.

Aquí nos paramos a pensar y decimos, el software fiable es un software que nosotros utilizamos diariamente, porque al final el software que utilizamos diariamente sufre de vulnerabilidades.

El software seguro es el software que no tiene vulnerabilidades.

Pero claro, el software seguro no existe al 100%, es muy complejo poder verificar que un software es seguro 100%, es imposible.

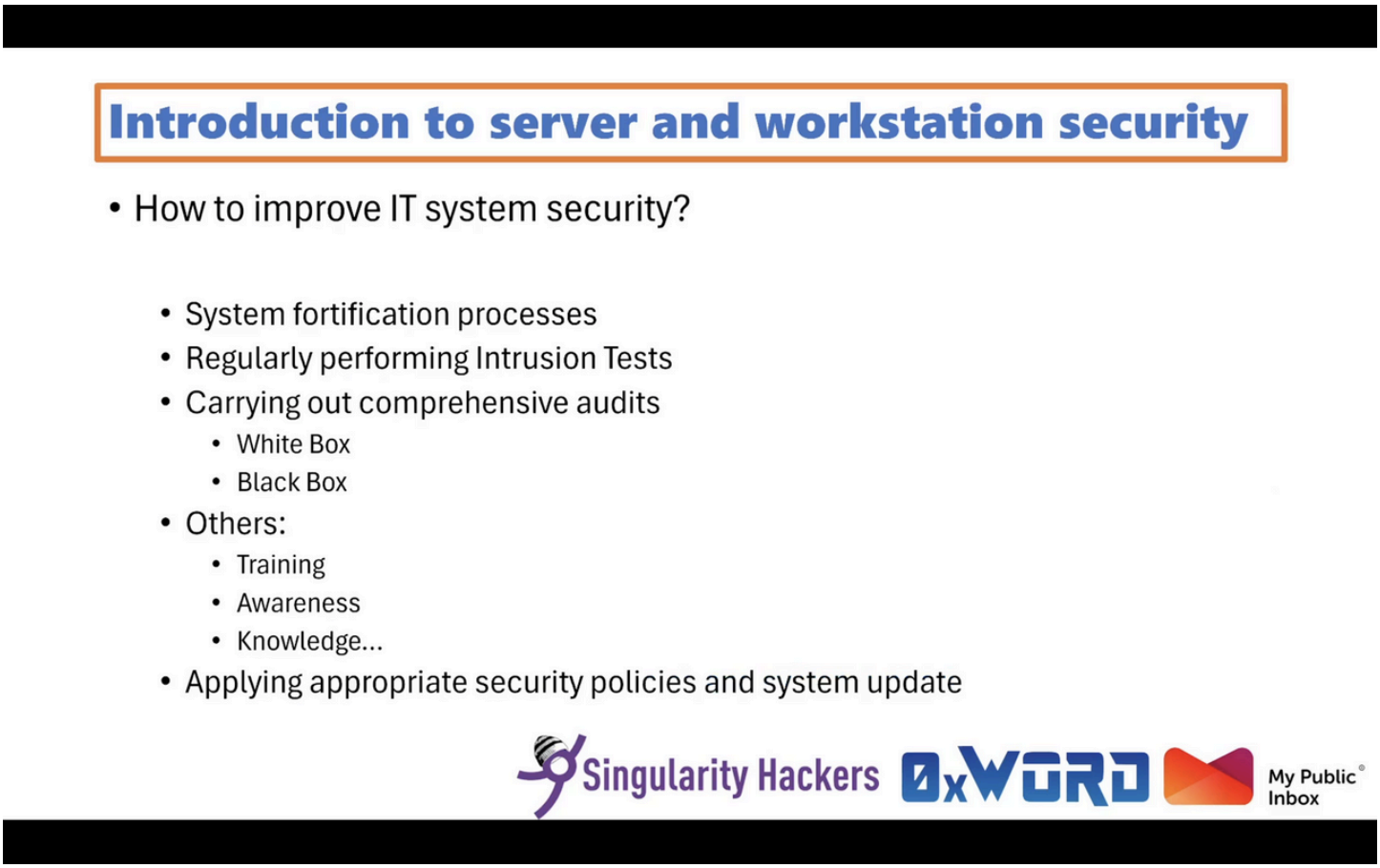
Entonces, ¿Qué ocurre?

Que hoy en día la complejidad del software está tan alta, los frameworks que utilizamos tán complejos, demasiada pila tecnológica por debajo como para poder verificarlo.

Bueno, podemos decir qué es el objetivo, el software seguro sería el objetivo al que yo debería intentar llegar.

Y bueno, quizá no vamos a llegar nunca, es un límite, nunca llegaremos a ese valor al cien por cien, pero cuanto más cerca estemos de ese cien por ciento más seguro será mi software.

¿Cómo mejoramos la seguridad de los sistemas?



Ahora nos vamos a preguntar también cómo mejoramos la seguridad de los sistemas.

Hay muchas cosas que tenemos que aplicar en el hardening, en este módulo vamos a verlo aplicado sobre sistemas Linux en diferentes capas dentro del propio sistema, pero por ejemplo la realización de procesos de fortificación a través de guías de hardening, guías de buenas prácticas que ya están validadas, hay guías muy oficiales, pues el NIST, INCIBE, hay diferentes entidades que tienen sus guías y podemos aplicar lógicamente estas guías de entidades o instituciones, ya sean público o no, pero esas instituciones que ya están validadas pues lógicamente son una buena fuente para poder fortificar, ya no solamente sean sistemas Linux, sistemas Windows, redes o cualquier entorno de hoy en día en una organización.

Por supuesto tenemos también la ejecución de los test de intrusión (Intrusion Tests).

Los test de intrusión al final nos permiten validar si encontramos algún tipo de camino que permita hacernos daño como organización.

Un ejercicio de Red Team también entraría aquí, auditorías, todo este tipo de cosas entrarían y las autoridades también entrarían en diferentes componentes, tanto en caja blanca, caja negra, incluso la caja gris también entraría.

Vemos que hay un apartado de Others que de nuevo hacemos hincapié en formación, concienciación y conocimiento.

Esto es importante, concienciación, capacitación, es muy importante porque al final es la base, es decir, nosotros tenemos que entender que por mucho que tengamos unas soluciones de

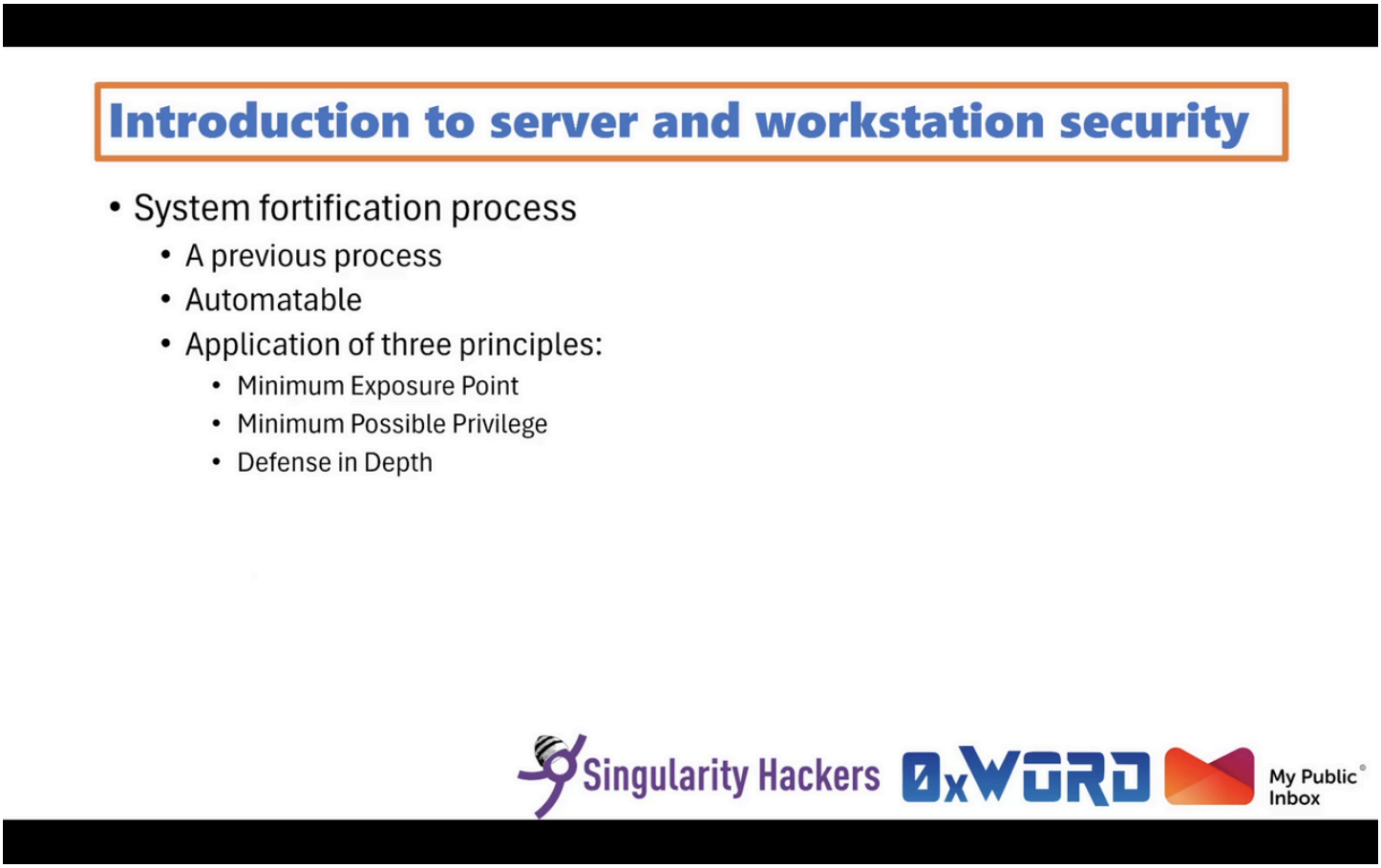
seguridad potentes, muy buenas, si la base de todo esto que son las personas, no tienen ese conocimiento, no tienen esa concienciación, no tienen esa formación a distintos niveles como hemos dicho antes, tendremos un problema porque nuestra base será frágil.

Entonces de nada valdrá tener una buena fortificación de sistemas si la base de todo esto que son las personas, que son entorno físico, es frágil.

Además también hablamos de aplicar políticas adecuadas de seguridad y actualizaciones sistemas. Las actualizaciones es algo fundamental hoy en día, quizá haya mucho más interiorizado que hace 10 o 15 años, pero hoy en día es mucho más sencillo encontrar que los sistemas están actualizados.

Aunque también fijémonos que seguramente en la formación lo estáis viendo en algún punto, OWASP nos dice que sigue siendo una de las vulnerabilidades que más se encuentra en ése top 10 de OWASP en el mundo web. Componentes sin actualizar, aplicaciones desactualizadas que provocan la intrusión de un atacante en un sistema.

Proceso de fortificación de sistemas



En este proceso de fortificación debemos entender que hay una parte del proceso que es a priori. Tenemos que diseñar, tenemos que evaluar cómo vamos a aplicar o qué queremos realmente proteger dentro de los servidores, dentro de los clientes.

Lógicamente un servidor no es lo mismo que un equipo cliente o una estación de trabajo (Workstation). Un servidor tiene generalmente más usuarios conectados, comparte más

información, tiene mayor criticidad que un equipo cliente, donde al final el ámbito (scope), la dinámica del sistema es mucho menor, porque al final tenemos a un usuario que poco más que ese usuario va a utilizar ese equipo cliente.

Sin embargo, en un servidor al final tenemos diferentes administradores, diferentes usuarios que están consultando, consumiendo información, que están instalando, que están realizando cambios de permisos. Hay muchísimo dinamismo y eso puede lógicamente provocar pequeñas debilidades, incluso vulnerabilidades en esos servidores.

Es necesario hacer esa evaluación, ese proceso a priori, donde tengamos la posibilidad de diseñar cuál es la estrategia de la fortificación, aplicar las guías adecuadas y entender también cuál es el entorno de naturaleza de nuestros sistemas.

Lógicamente todas las empresas no son iguales, ¿No?

No todas las empresas tienen los mismos servidores, ni los mismos servicios, ni ofrecen los equipos clientes, tienen las mismas aplicaciones, ni tienen nada igual. Entonces tenemos que aplicar y diseñar esa fortificación a priori antes de ponernos a implantarla.

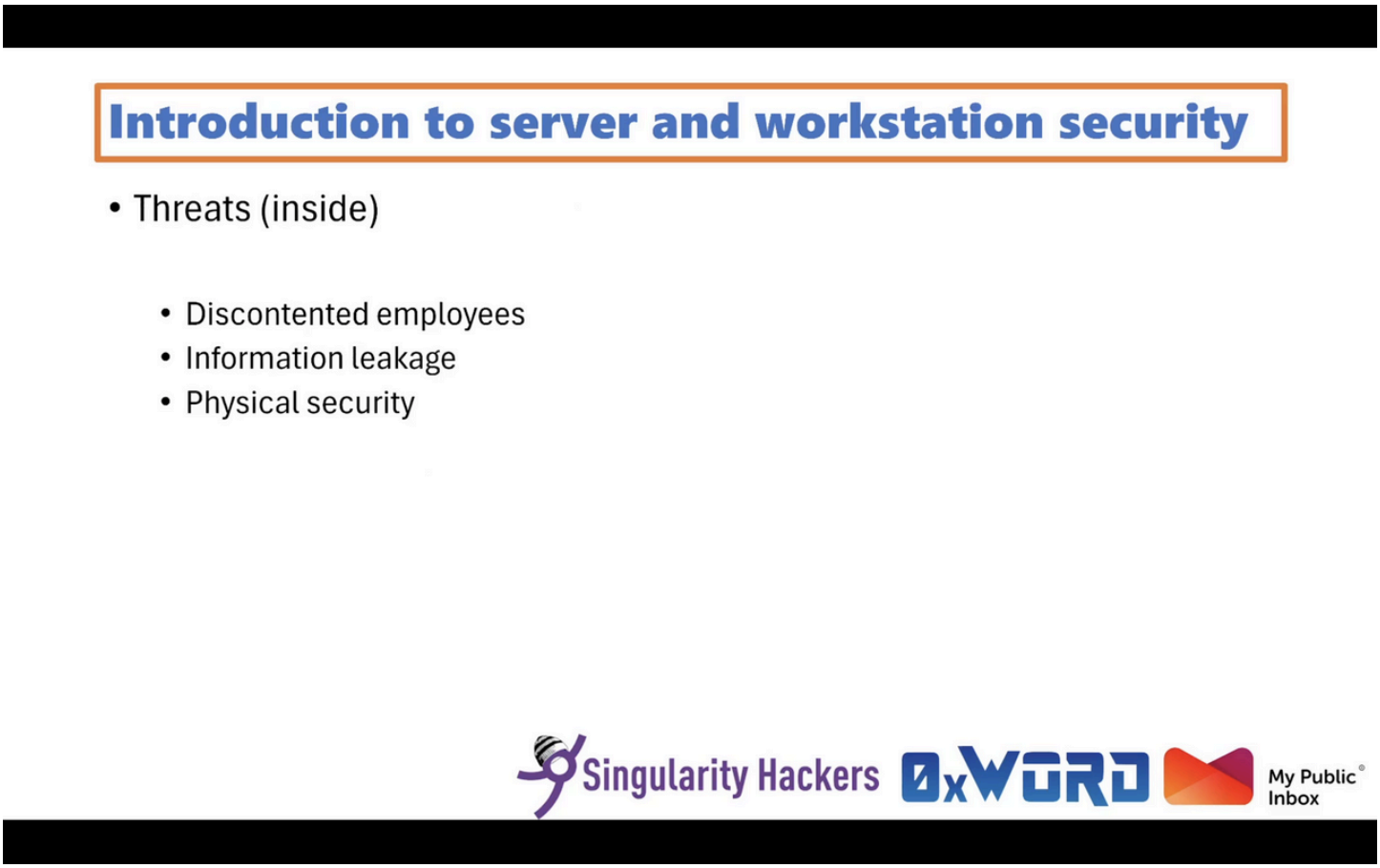
Luego existe también, por ejemplo, el tema de plataformado, que es una buena práctica, es decir, oye, pues yo me creo una serie de plantillas y yo voy plataformando con esas plantillas los equipos de los clientes, incluso los servidores, en función de las necesidades que tengan los usuarios. No es lo mismo un usuario de IT que un usuario de contabilidad o que un usuario de marketing. Eso también es algo a tener en cuenta.

Luego también decimos que es automatizable (Automatable). Debemos hacerlo lo más automatizable posible y ahí están los entornos de plataformado para poder automatizarlo utilizando plantillas. Hoy en día con la virtualización también es bastante interesante el proceso.

Aquí al lado saben de que hay aplicaciones de tres principios, que es el mínimo punto de exposición (Minimum Exposure Point), mínimo privilegio posible (Minimum Possible Privilege) y la defensa profundidad (Defense in Depth).

Sobre todo nos quedamos con la defensa a profundidad por el modelo que propone. Vamos a poner un zoom, vamos a hacer un foco y vamos a hablar del modelo aplicado en este caso, equipos y aplicaciones de los sistemas Linux.

Threats, inside and outside



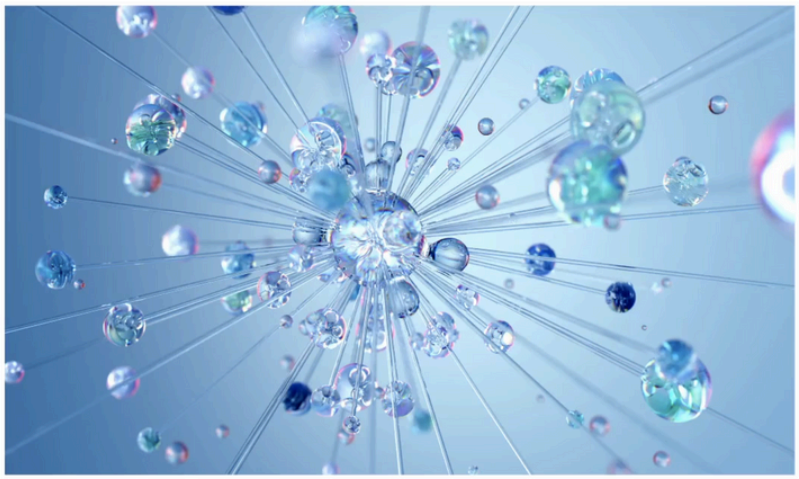
Si hablamos de amenazas, amenazas internas, pues aquí nos aparecen los empleados descontentos, los insiders que también se han tratado en esta formación, la fuga de información cuando se exfiltra, el proceso de exfiltración (Leakage), que también se puede hacer en un proyecto de Hacking Ético, se puede hablar de esas pruebas de exfiltración de datos para ver si mis protecciones son adecuadas y consigo evitar esa fuga de información. Mejor hacer esa prueba en un proyecto Hacking Ético a que realmente ocurra en una empresa y tenga un incidente de seguridad.

Y luego también aquí hablamos de la seguridad física, es decir, claro, las personas que tienen acceso a la organización, que tienen acceso a un contacto físico con la organización, pues necesitamos tener esa seguridad.

Si recordamos el modelo de defensa en profundidad, nos hablaba de la primera capa son las personas, pero la segunda capa es la seguridad física. Tampoco nos vale de nada tener los mejores firewall, los mejores ids, los mejores antivirus, si luego realmente cualquiera puede entrar en mi organización y cualquiera puede acceder a un CPD o a un cuarto donde tengan información sensible.

Introduction to server and workstation security

- Threats (outside)
  - Attacks against the perimeter
  - Client-side attacks
  - Targeted attacks
  - Different types of malware
  - Vulnerabilities



Picture source: Google DeepMind. Free use. https://www.pexels.com/es-es/foto/abstracto-tecnologia-investigacion-digital-17485657/

Singularity Hackers 0xWORD My Public Inbox

Luego tenemos las amenazas externas.

Empezamos con los ataques contra el perímetro (attacks against the perimeter). Las empresas al final sufren de ataques en Internet. Cualquier servicio expuesto que tengamos va a sufrir intentos de ataque en algún momento de su vida seguramente. Hoy en día hablamos de perímetro, pero también hablamos de cloud, es decir, las empresas también tienen los servicios en el cloud y por supuesto el cloud nos da una capa extra, pero también hay que fortificarlo. Lógicamente el cloud nos da hasta donde nos da y nosotros tenemos que poner nuestras medidas y nuestras protecciones.

Tenemos ataques en el lugar de cliente (Client-side attacks). Estos son ataques que al final nos llegan principalmente por el correo electrónico, el típico documento donde abrimos y tenemos una macro maliciosa, o el típico documento PDF que cuando abrimos explota la vulnerabilidad de mi lector del PDF o cualquier ataque por una URL que nos envía, pincho en la URL, entonces me conecto a una página que me envía un exploit contra mi navegador. Este tipo de cosas son ataques client-side, porque realmente ocurren con la interacción del usuario.

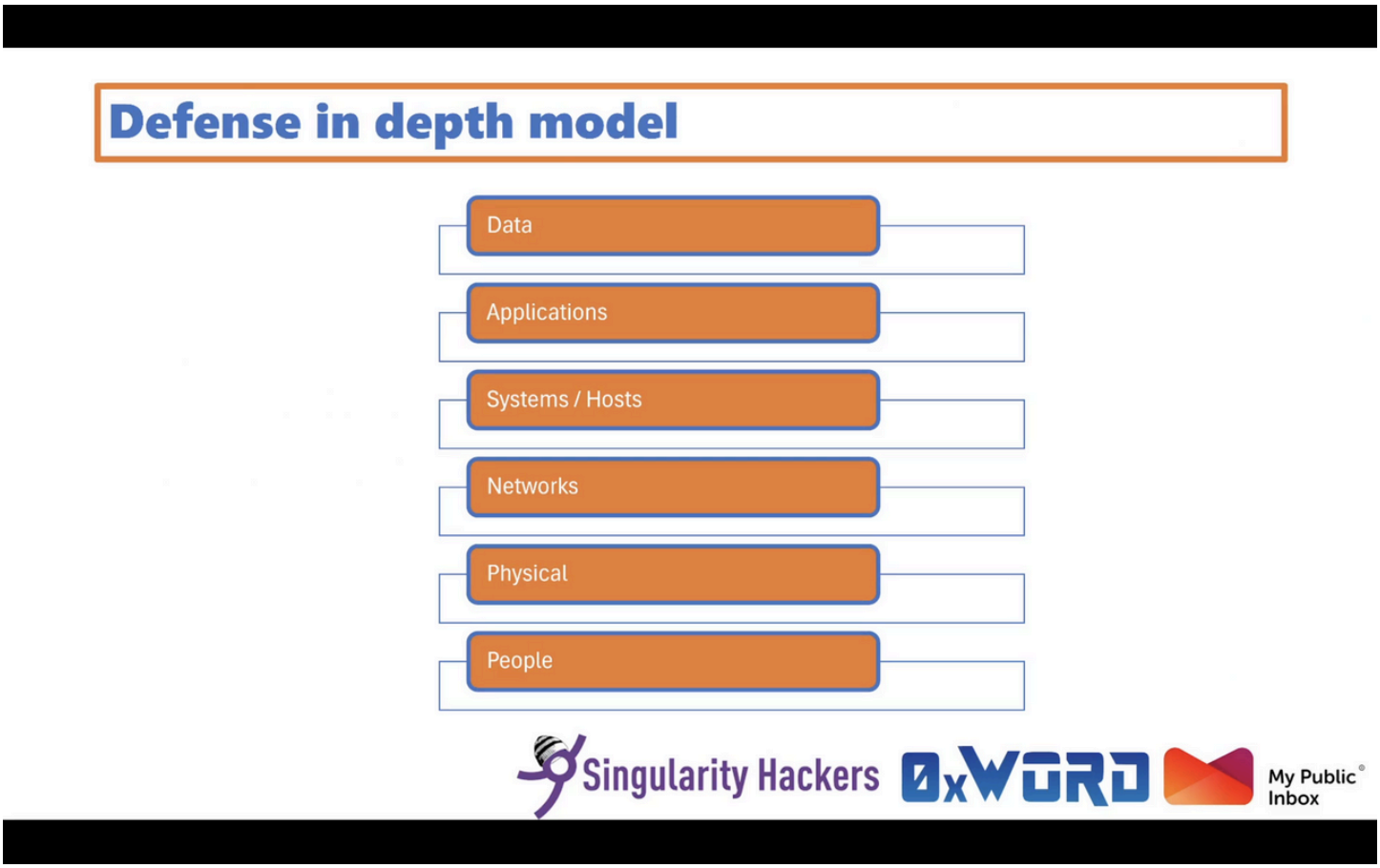
Luego tenemos los ataques dirigidos (targeted attacks). Son ataques dirigidos a personas VIP, principalmente de la empresa o personas que tienen contacto con esos VIP. Entonces son ataques que por ejemplo, por ejemplificarlo, tenemos la estafa del CEO, que es uno de los ataques más utilizados hoy en día por ciberdelincuentes para estafar a las organizaciones.

Tenemos también los diferentes tipos de malware, hemos hablado ya en otros casos que si ransomware, troyanos, spyware, diferentes tipos de malware, cada uno con su funcionalidad y cada uno con su impacto sobre la organización. Son amenazas a las cuales las empresas se

enfrentan día a día. Una infección interna en la red de una organización puede causar el caos y puede causar que tengamos un impacto en la actividad de negocio y que tengamos que parar incluso y aislar equipos hasta poder eliminar o erradicar la amenaza.

Y luego también las vulnerabilidades. Las vulnerabilidades al final van ligado un poco ataques contra perímetro, ataques client-side. Las vulnerabilidades es algo que nos afecta en todos los ámbitos, es decir, las vulnerabilidades es algo que tenemos que tener muy en cuenta, tenemos que intentar detectarlas lo antes posible, erradicarlas, porque al final si no las tenemos en cuenta, lógicamente los atacantes lo van a tener en cuenta, con lo cual es algo que tenemos que tener en nuestro ciclo de vida de seguridad.

Modelo de Defense in Depth

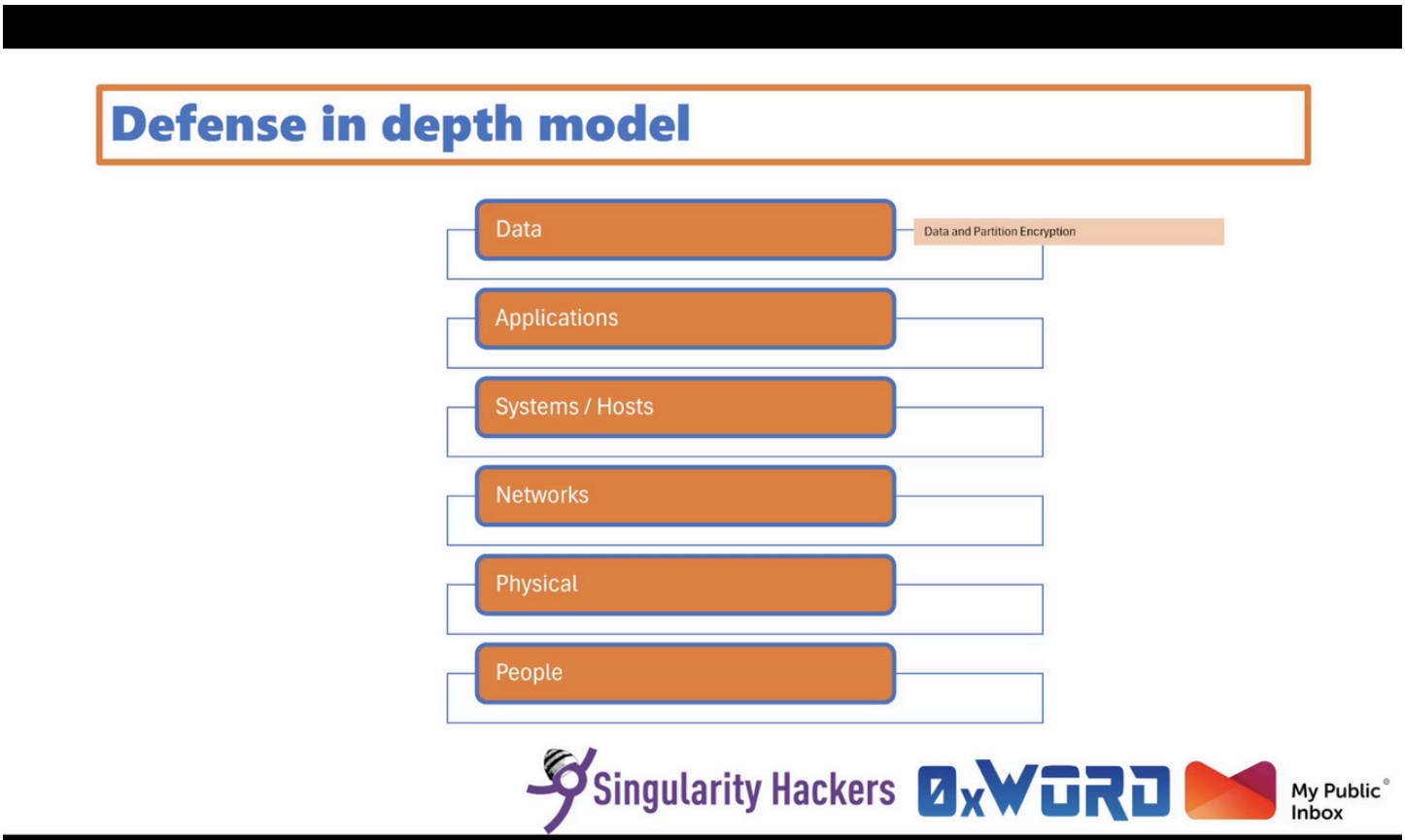


Tenemos aquí para recordar el modelo de defensa en profundidad, recordad que es un modelo que viene del entorno militar, que proporciona diferentes líneas de defensa.

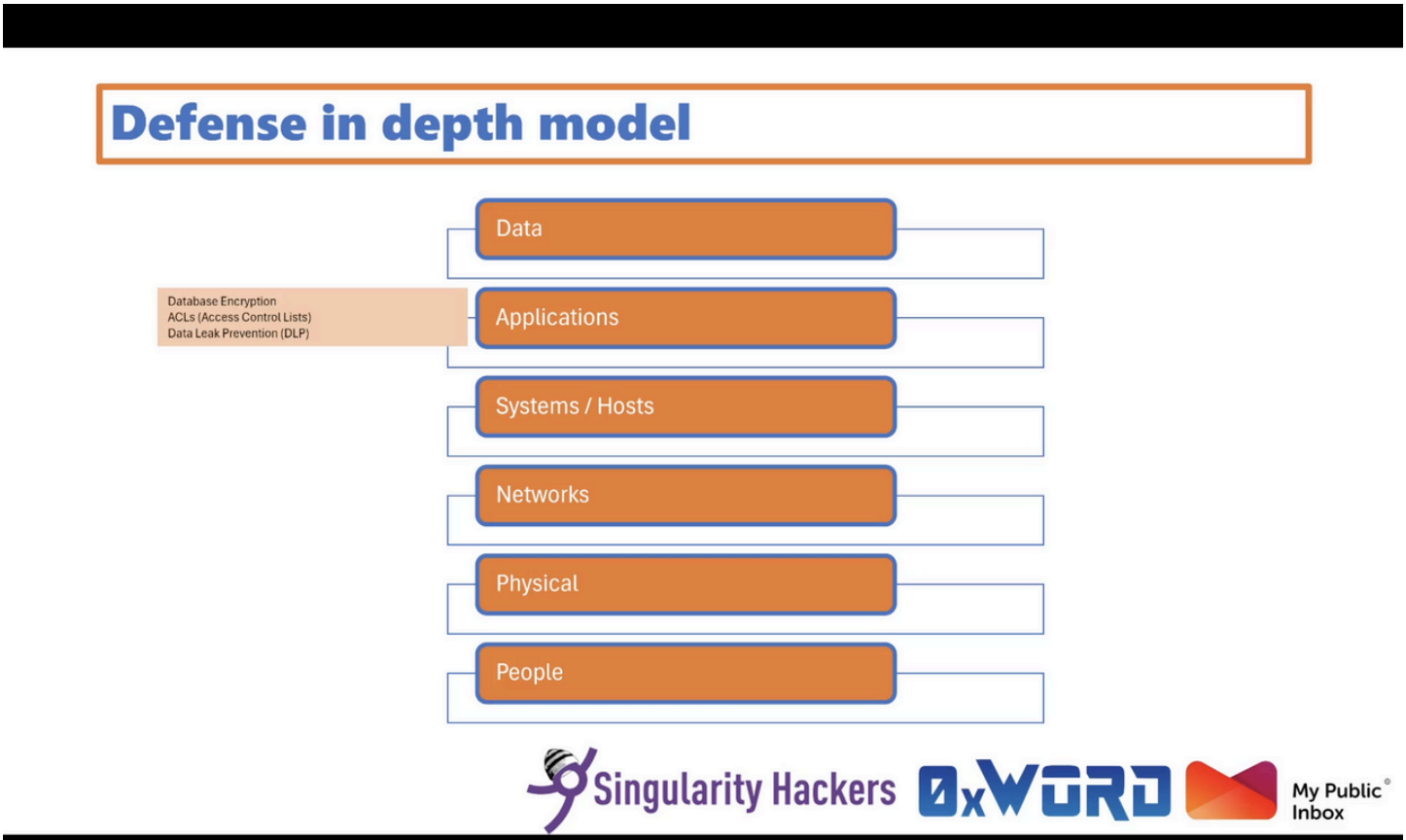
Hablamos de las personas como primera base, hablamos de la seguridad física como segunda y luego empezamos a hablar ya del perímetro, de las redes internas, de fortificar los equipos, de fortificar las aplicaciones, hasta llegar a la fortificación del dato, que es lo que realmente estamos queriendo proteger.

Al final podemos decir que se crean capas de defensa. Cuantas más capas de defensa, cuantas más cueste llegar hacia la información, que es lo que el atacante va a buscar, pues realmente menor probabilidad tendremos de sufrir ataques, pero no significa nunca estaremos seguros al 100%. Esto al final consiste en ir reduciendo la probabilidad de que me ataquen.

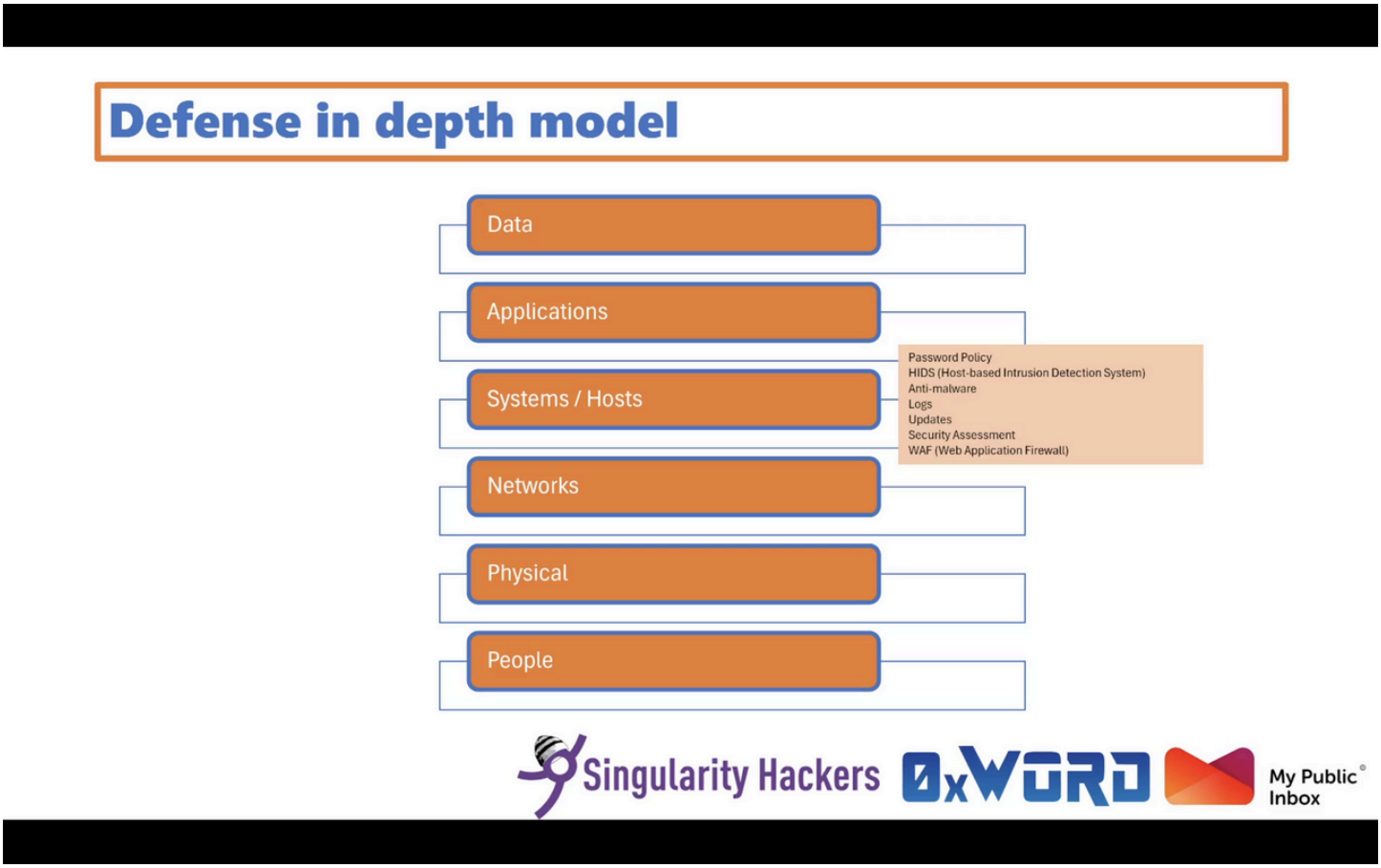
Si vamos a la parte de Data, tenemos por ejemplo particionamiento, bueno el cifrado de particiones, cifrado del dato como tal, de la carpeta del archivo hasta ese nivel.



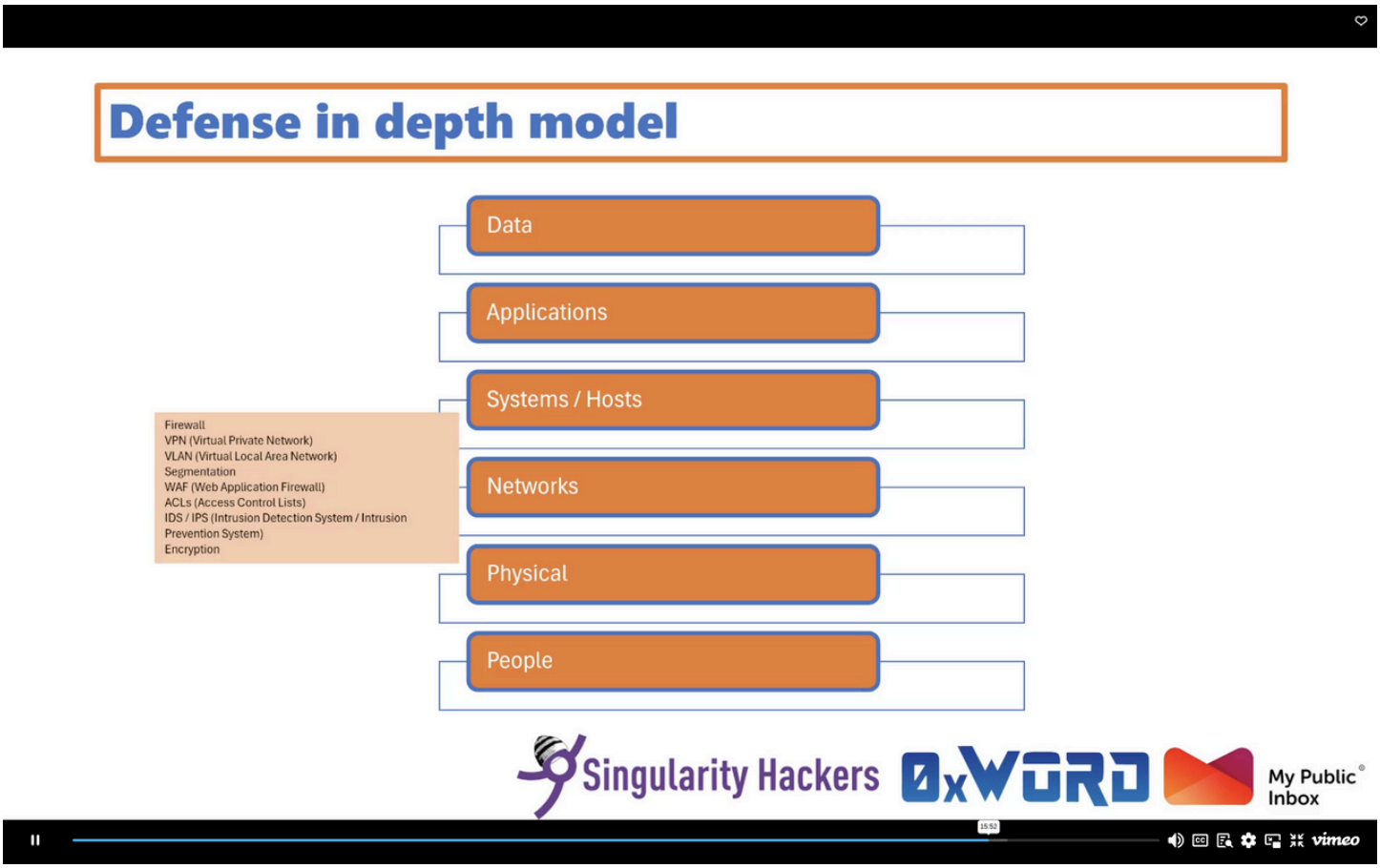
En las aplicaciones, por refrescar un poco el cifrado de bases de datos, lista de control de acceso, DLPS para intentar de evitar la fuga de información.



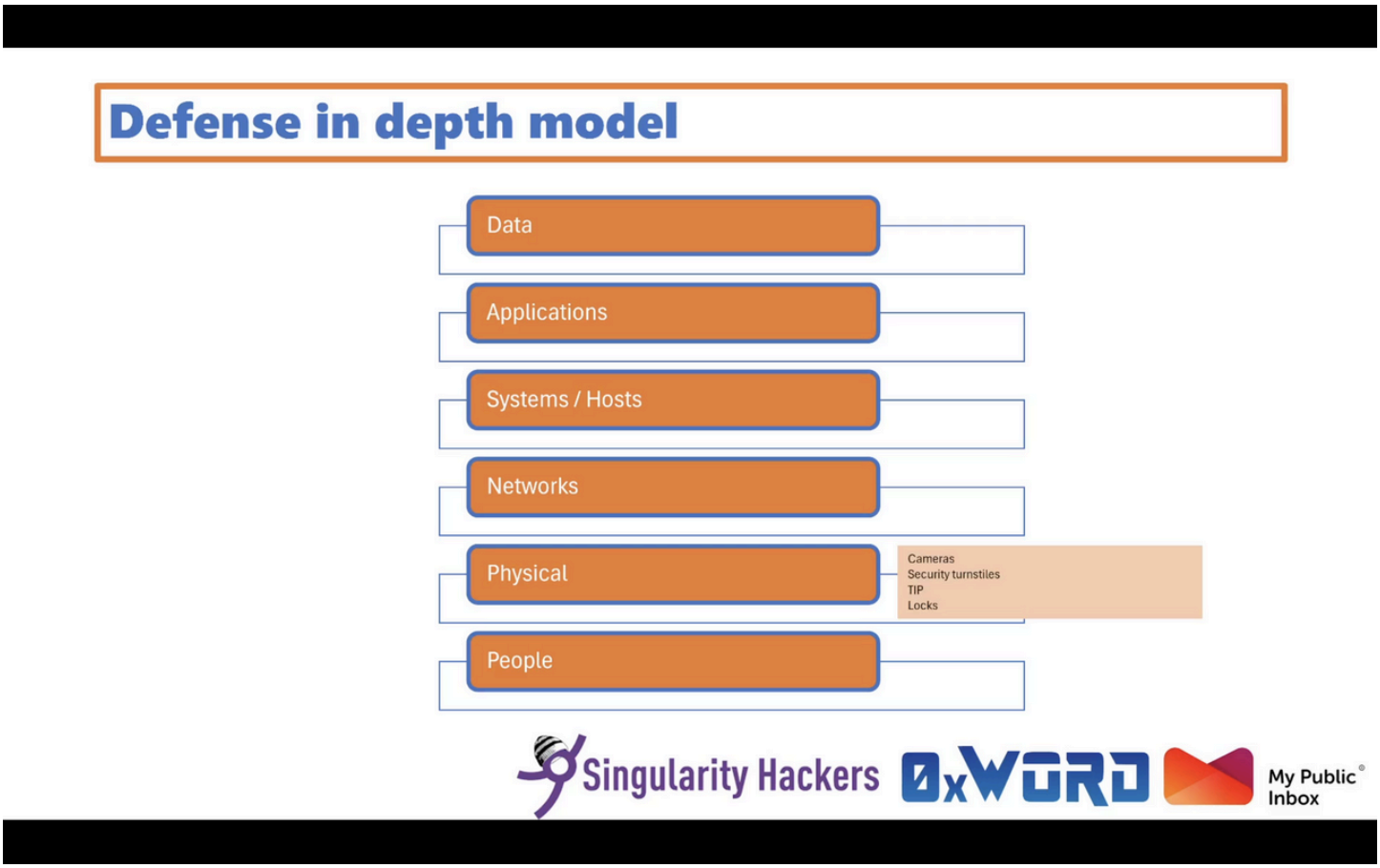
En sistemas hablamos de protecciones de política de contraseñas, HIDS, antimalware, gestión de logs, centralización de logs a través de SIEMS. También por ejemplo actualizaciones, políticas de actualización, wav, evaluaciones deseguridad, pentest, auditoría. Al final es donde pondremos el foco, tanto en aplicaciones como en sistema, en la parte de Linux, en este módulo.



Redes, ya lo hemos visto, pero bueno, redes, Firewall, VPN, vlans, WAF, ACL, IDS, IPS. Al final toda esta parte. Entonces, fijaros si hay elementos, y hay más, pero esto es un subconjunto de ejemplos, elementos en cada capa que se puede aplicar. Lógicamente, cada empresa tendrá que ceñirse a unos presupuestos, inversiones en seguridad, y con eso tendrá que configurar su política de seguridad.

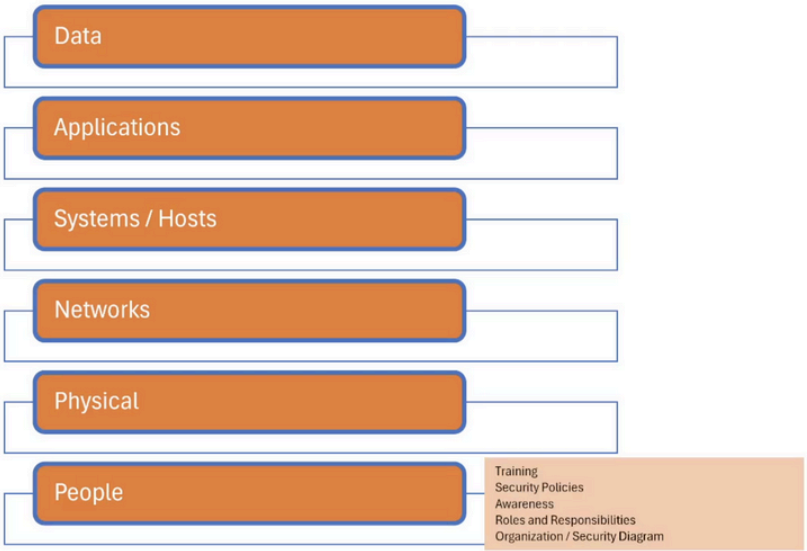


Seguridad física, hablamos ya de elementos físicos, cámaras, tarjetas de identificación, cerraduras, entornos.



Y luego las personas. Entrenamiento, concienciación, formación.

Defense in depth model



Singularity Hackers 0xWORD My Public Inbox

Bien, lo que hay que conocer, Lo que hay que conocer. Bueno, ¿Qué tenemos que conocer?

Defense in depth model

- Know what you have:
  - Don't have technology just for the sake of having it
  - Better well-configured than good by default
  - Software updates always
  - Pre-production environments
  - Virtualization
  - Low cost

Singularity Hackers 0xWORD My Public Inbox

Hay que conocer de qué se dispone, ¿De qué se dispone? No disponer de tecnología por disponer es muy importante.

Es decir, yo tengo un inventario, un inventariado de lo que yo tengo, tengo todos estos sistemas, tengo todo esto expuesto, tengo esto no expuesto, tengo todo ese diagrama organizativo y tengo toda esa información. Y lo que tengo que tener claro es, no se me pueden olvidar máquinas, lo que ocurre en algunas empresas es de repente una máquina, esta máquina, no sabemos, está ahí, es nuestra, pero no sabemos ni qué hace ni quién es, y tiene Windows 2000.

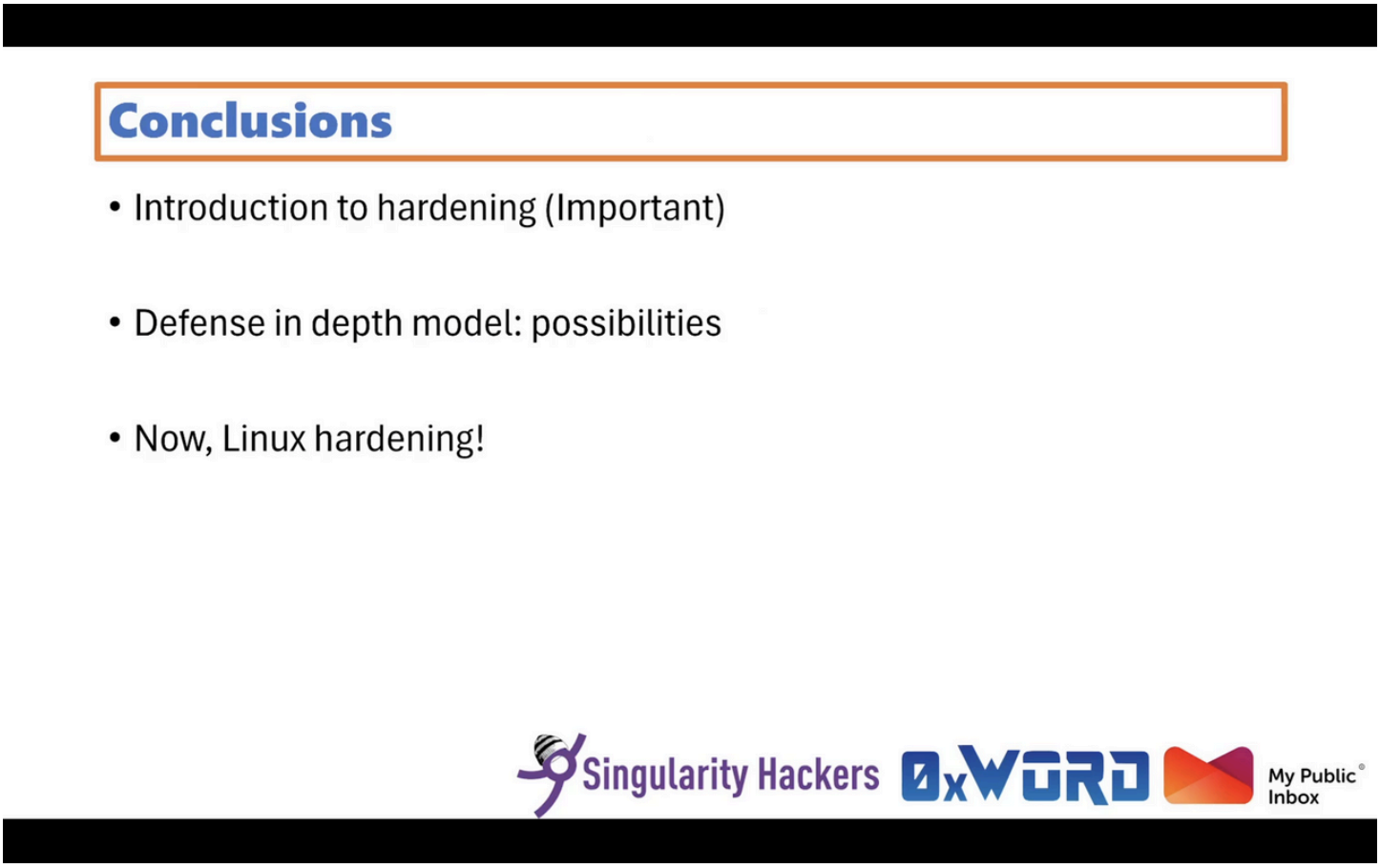
Bueno, esto es un riesgo de seguridad, porque puede dar acceso a la red, porque pueden pivotar a través de ella, porque pueden hacer muchas cosas.

Entonces, debemos conocer lo que tenemos y no disponer de tecnología por disponer, es decir, lo que tengamos, lo tengamos bien configurado y nunca por defecto. Es decir, más vale lo bien configurado que lo bueno por defecto.

Hay cosas que por defecto tienen una seguridad mínima, pero normalmente, generalmente, uno puede aplicar mejor las medidas de seguridad cuando uno configura y tiene conocimiento para configurar los diferentes productos o servicios en los que haya invertido.

Actualizaciones de software, siempre hay que hacerlo.

Los entornos de producción, por supuesto, son muy, muy importantes en los entornos organizativos.



Bien, como conclusión, hemos tratado esta introducción a la fortificación, empezamos a poner el foco ya en el sistema Linux, hemos visto dónde estamos, las necesidades de la fortificación, hemos ligado ya con las amenazas y con todo esto que hemos ido viendo en otros módulos.

Y ahora hemos estado viendo también las posibilidades que tenemos con el modelo de defensa en profundidad.

Hemos puesto el zoom en la parte de equipos y de aplicaciones y a partir de ahora iremos comentando ya a diferentes niveles dentro de la parte de fortificación del sistema Linux.