MONTAR UN MINISTERIO?

SUJET ME THE CUBAT

“No battle plan ever survives contact with the enemy.”

Helmuth von Moltke the Elder
Prussian general
born October 26, 1800

MINISTERIO DE NUEVA CREACION

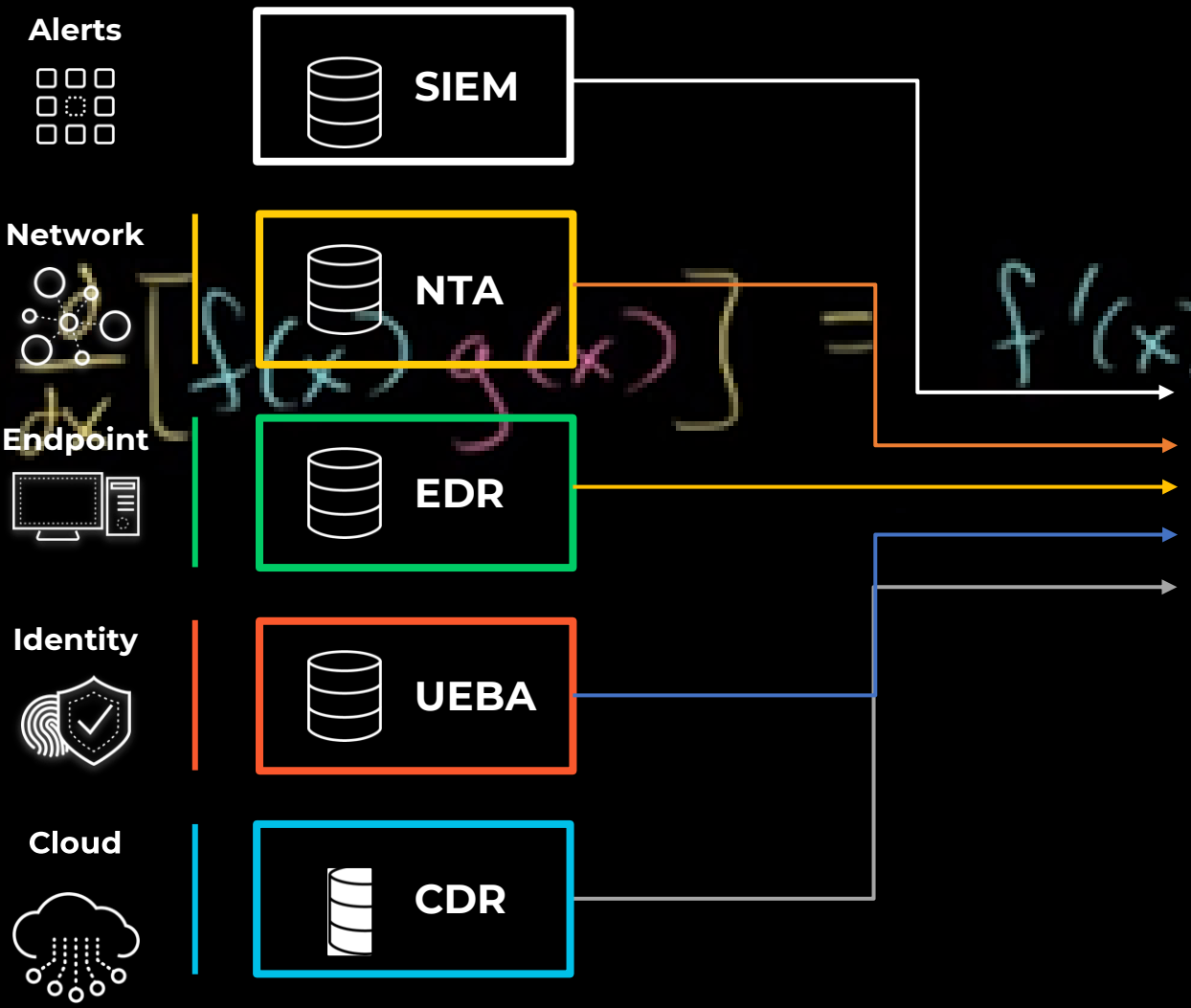
- INICIO SERVICIOS PRESTADOS 3º
- ATERRIZAJE EQUIPO NUEVO EN LA AGE
- PLAN ESTRATEGICO?? -> UN PLAN DE TRANSFORMACION DIGITAL…
- ALUCINAR… Y MANOS A LA OBRA

PLAN FINAL

- 3 GRUPOS O FASES PRINCIPALES, CADA UNO CON SU SEGURIDAD:
  - PUESTO DE TRABAJO : EDR, MICROCLAUDIA
  - INFRAESTRUCTURA:
    - PROPIA
    - NUBE PRIVADA
  - APLICACIONES
    - LOTE ESPECIFICO SEGURIDAD
- Y UN PILOTO HERRAMIENTAS CCN

ccn-cert
centro criptológico nacional

El problema: Demasiada información, aislada, falta de recursos -> INTEGRACION, VISION UNICA Y CENTRAL



~11K
Alertas por dia

4+
Días de investigación

< 30%
Cumplimiento KPI SOC

212
Dias resolución brechas

Fuentes:
[1]Forrester, The 2021 State of Security Operations
[2]The State of SOAR Report
[3]2022 Ponemon report

Por pedir que no sea….

01	**Idoneidad**	• Despliegue sencillo • Plataforma única, si es conocida, mejor • Fácil adopción • Enterprise
02	**Analíticas e Investigación**	• Detección automatizada • Modelos de AI avanzados • Amplia visibilidad • Reglas automáticas y propias
03	**Fuentes adicionales**	• Integraciones con terceros • Capacidad de quitar carga de logs del SIEM
04	**Automatización**	• Automatización de detección, investigación y RESPUESTA • Reducción de MTTD y MTTR • Automatizar automatizar automatizar…
05	**Estrategia**	• Visión “estratégica” y capacidad de crecimiento facil • Acompañando el ciclo de vida y madurez del SOC • Eliminación de silos, optimización de costes • Ecosistema soporte, formación, PARTNERS…

UN ANILLO PARA TODOS

- UNA SOLUCION TRANSVERSAL PARA DAR VISION UNICA AL SOC
- UNA VISION END TO END DE SERVICIOS Y SISTEMAS DISTINTOS
- ALINEADO CON COCS
- Y …MUSCULO… MUSCULO!

OBJETIVO

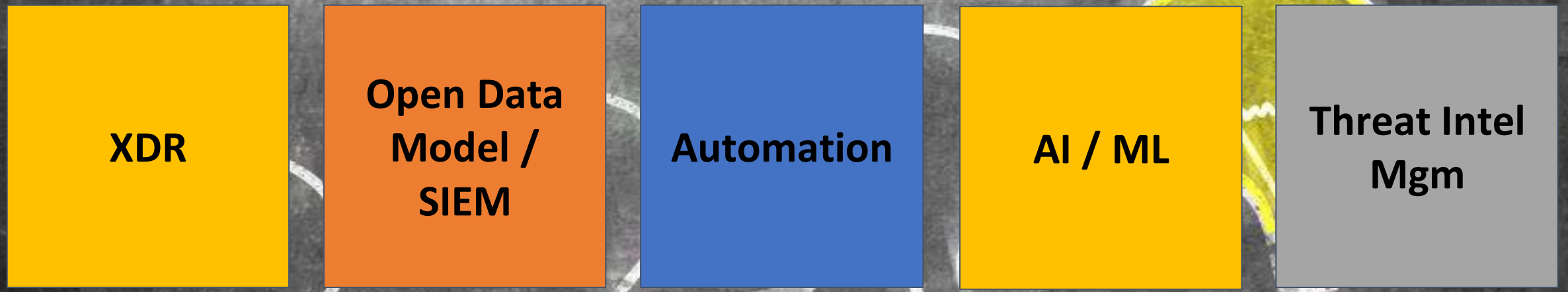
- VISION END TO END: CRUCE PUESTO DE TRABAJO Y DEL SERVIDOR DE APP, COMPORTAMIENTOS.
- ALINEACION TENANTS DISTINTOS SERVICIOS
- SOLUCION ‘GRANDE’ PARA SER TAN ‘PEQUEÑOS’
- ACALLAR LA ANSIEDAD Y LA OBSESION !!

Círculos de CONFIANZA

¡COMO ESTA EL SERVICIO

- TRABAJO PREVIO: CONVENCER, COLABORAR
- Y TAMBIEN POSTERIOR: LAS 3 P’s

FASES



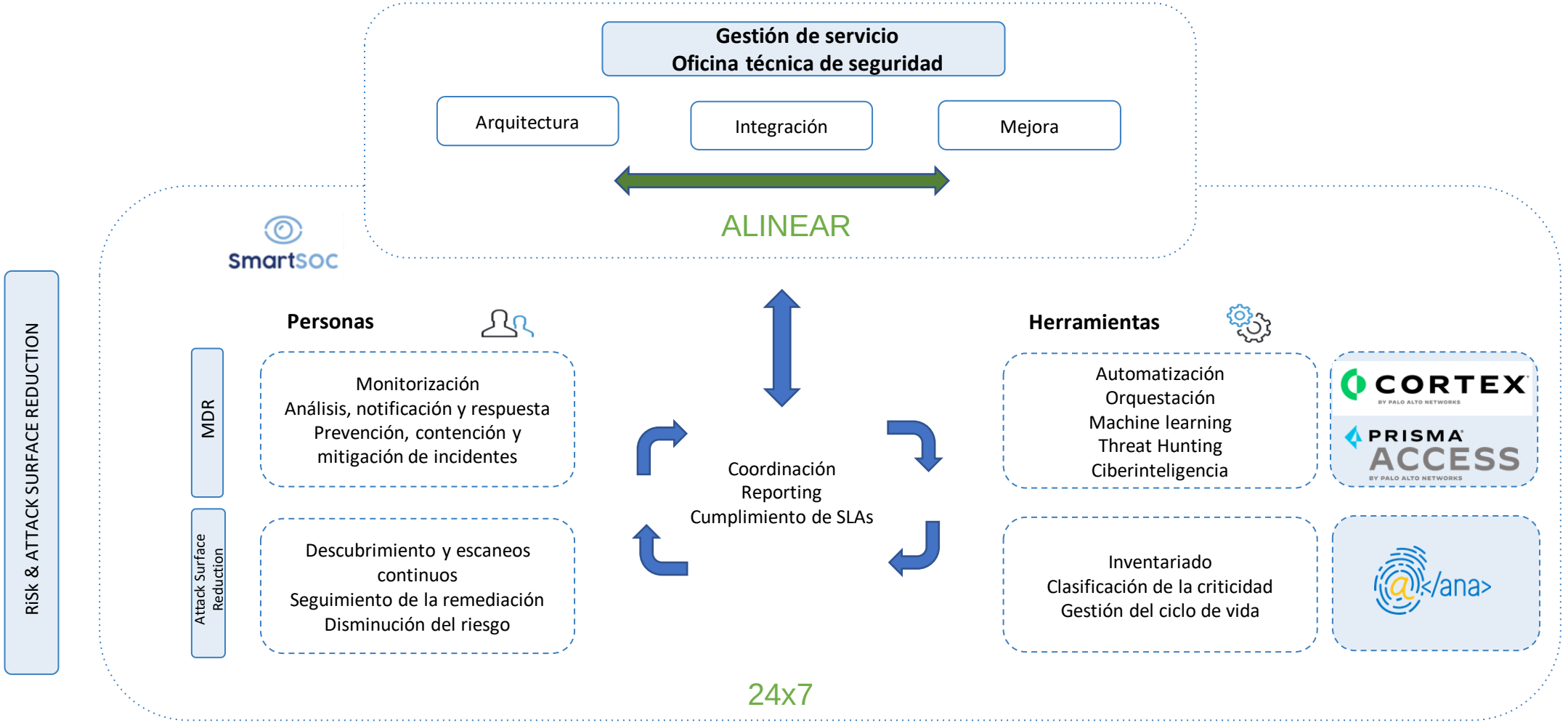
Fase 1: XDR, sensorIZAR

Fase 2: fuentes adicionales

Fase 3: orquestación y automatización

SmartSOC - Ministerio de Ciencia e Innvocación

Modelo del servicio



Objetivos:

- Reducir el riesgo, reducir superficie de ataque
- Responder ante incidentes de forma temprana

➢ **Función de la capa MDR:** Caza temprana de amenazas, prevención de incidentes, mitigación

➢ **Función de Attack Surface Reduction:** Descubrir nuevos puntos de exposición y gestionar la reducción de la exposición detectada

Competencias del servicio

MDR	Pentesting
Despliegue del agente de Cortex XDR	Descubrir agujeros de seguridad mediante escaneos
Creación y mantenimiento de reglas de prevención.	Retest para verificación
Integración de otras fuentes a monitorizar existentes en el ministerio (Firewall… etc)	Clasificación y priorización
Investigación forense de incidentes y Threat Hunting	Seguimiento del ciclio de vida y su remediación
Integración de listas dinámicas de bloqueo (EDL) para aplicaciones y portales	Disminución del riesgo
Reducir el tiempo de respuesta y de prevención mediante la automatización	
Generación de inteligencia de amenazas e indicadores de ataque	

Cortex XDR: El producto central para el SOC next-gen; integra y normaliza todos los datos y dirige la analítica con IA/ML

Protección completa del endpoint

Detección de amenazas

Investigación y respuesta rápidas y sencillas

Detección e Investigación de Amenazas con Analíticas e Indicios de múltiples fuentes

Datos de Red

Datos de Endpoint

Datos de Nube

Datos de Identidad

Coser datos en una historia unificada

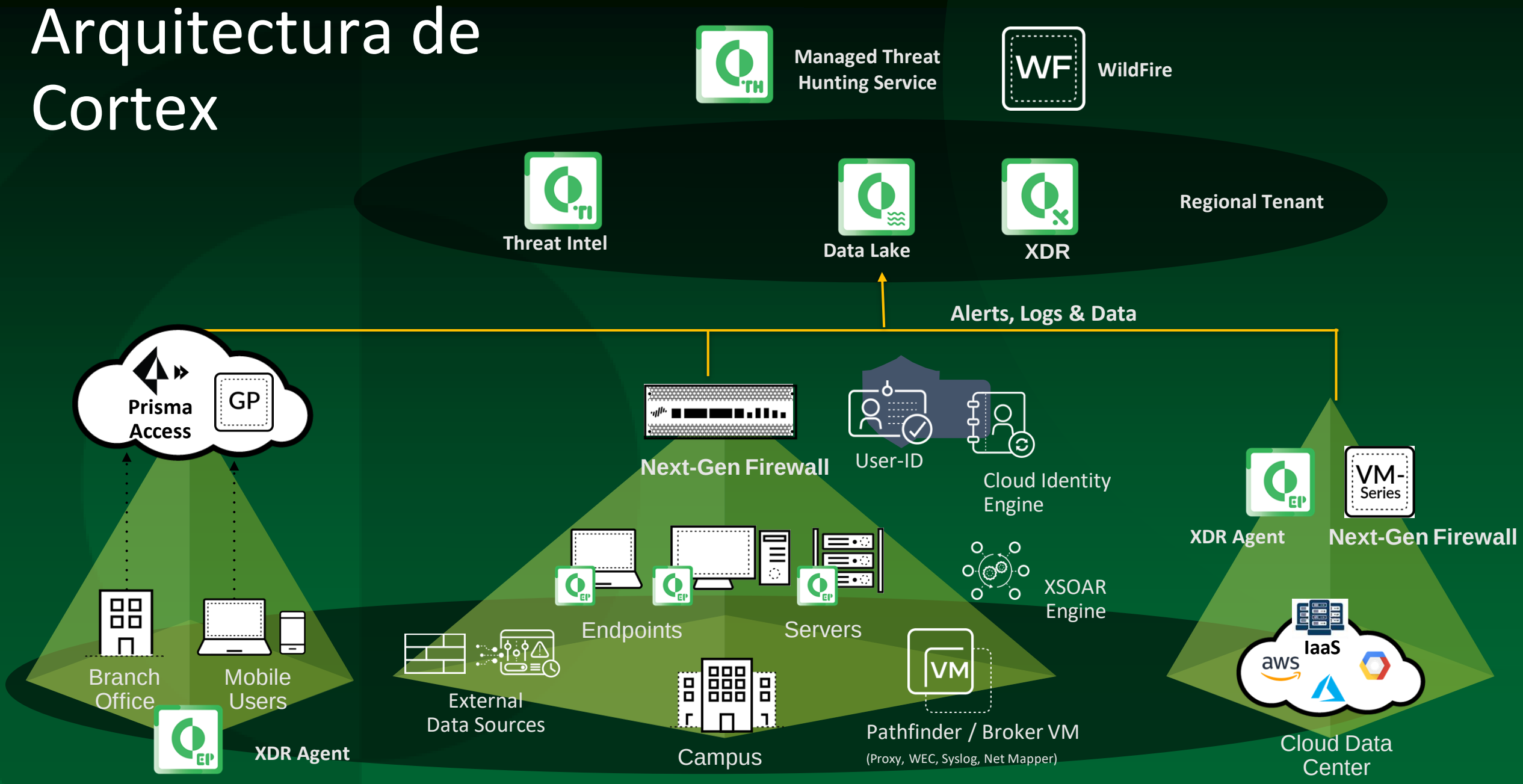
Analizar historias con ML y Analíticas de Comportamiento

- Perfiles de comportamiento de hosts, user y procesos
- Clasificar Usuarios y Hosts
- Detectar actividad anómala

Investigaciones ágiles con indicios multi-fuente y agrupado de alertas mediante IA.

* Cloud data includes Prisma Access, VM Series, and cloud flow logs

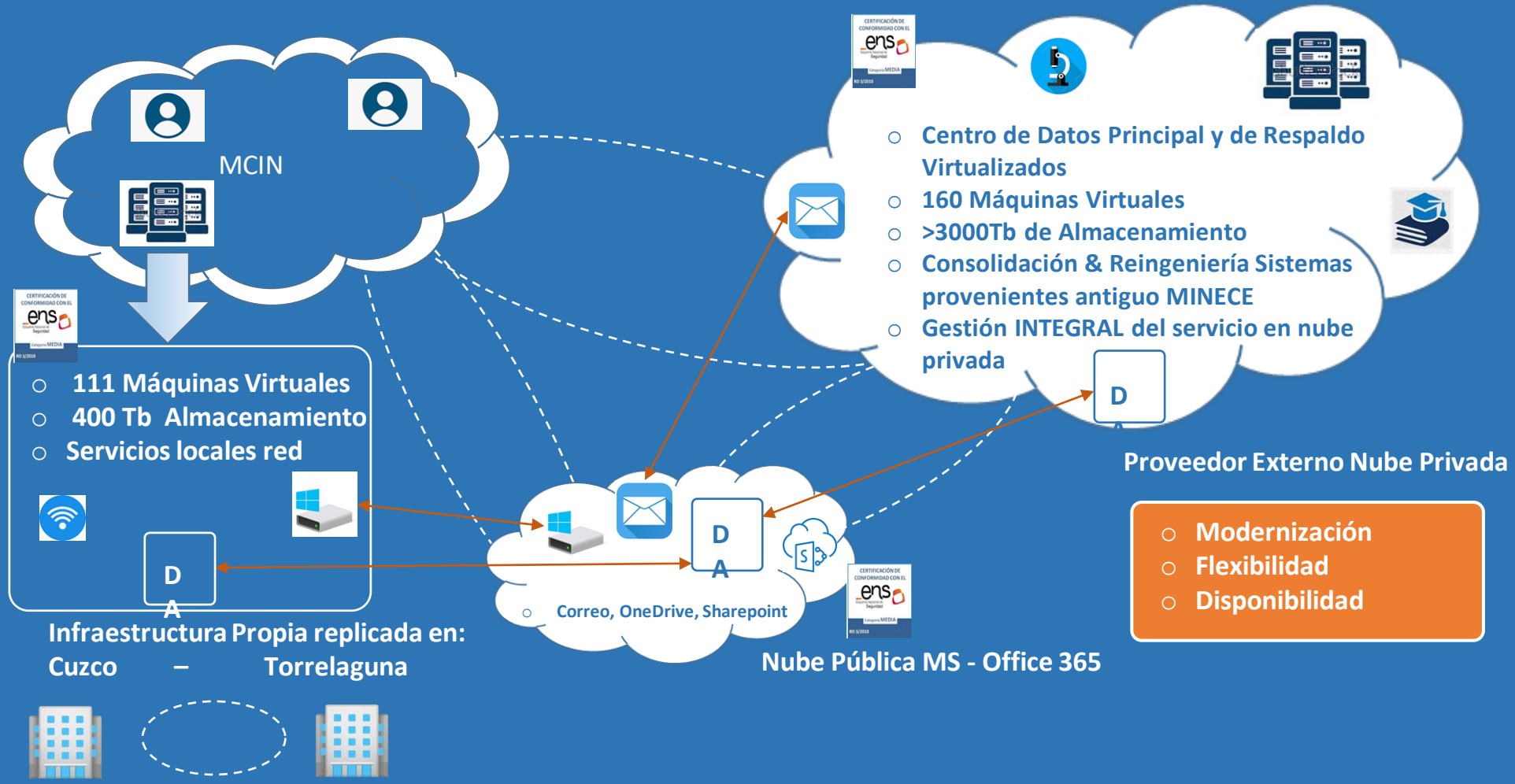
Arquitectura de Cortex



CUÑAS PUBLICITARIAS

Algo tendré que vender yo….

Nube MCIN


MCIN
111 Máquinas Virtuales
400 Tb Almacenamiento
Servicios locales red
D
A
Infraestructura Propia replicada en:
Cuzco – Torrelaguna
D
A
Correo, OneDrive, Sharepoint
Nube Pública MS - Office 365
Centro de Datos Principal y de Respaldo Virtualizados
160 Máquinas Virtuales
>3000Tb de Almacenamiento
Consolidación & Reingeniería Sistemas provenientes antiguo MINECE
Gestión INTEGRAL del servicio en nube privada
D
Proveedor Externo Nube Privada
Modernización
Flexibilidad
Disponibilidad

En breves cifras……..

- 280 MAQUINAS VIRTUALES
- 3650 TB ALMACENAMIENTO
- 1200 USUARIOS INTERNOS
- 230 APLICACIONES
- ~ 50 SERVICIOS TIC
- 9,5 M € DE PTO ANUAL

FUNCIONARIOS RPT: 18

- 121.983 CIUDADANOS USUARIOS
- +26 CONVOCATORIAS ANUALES
- 31.666 SOLICITUDES TRAMITADAS 2021
- 1.088 M € GESTIONADOS 2021
- 10.609 INCIDENCIAS Y PETICIONES DE CIUDADANOS

Pinceles o pintores ….