Proyectos del CCN. Necesidad apoyo

II
ENCUENTRO
DEL ENS

DIEZ AÑOS DE NUEVOS
RETOS Y SOLUCIONES

CCN
centro criptológico nacional

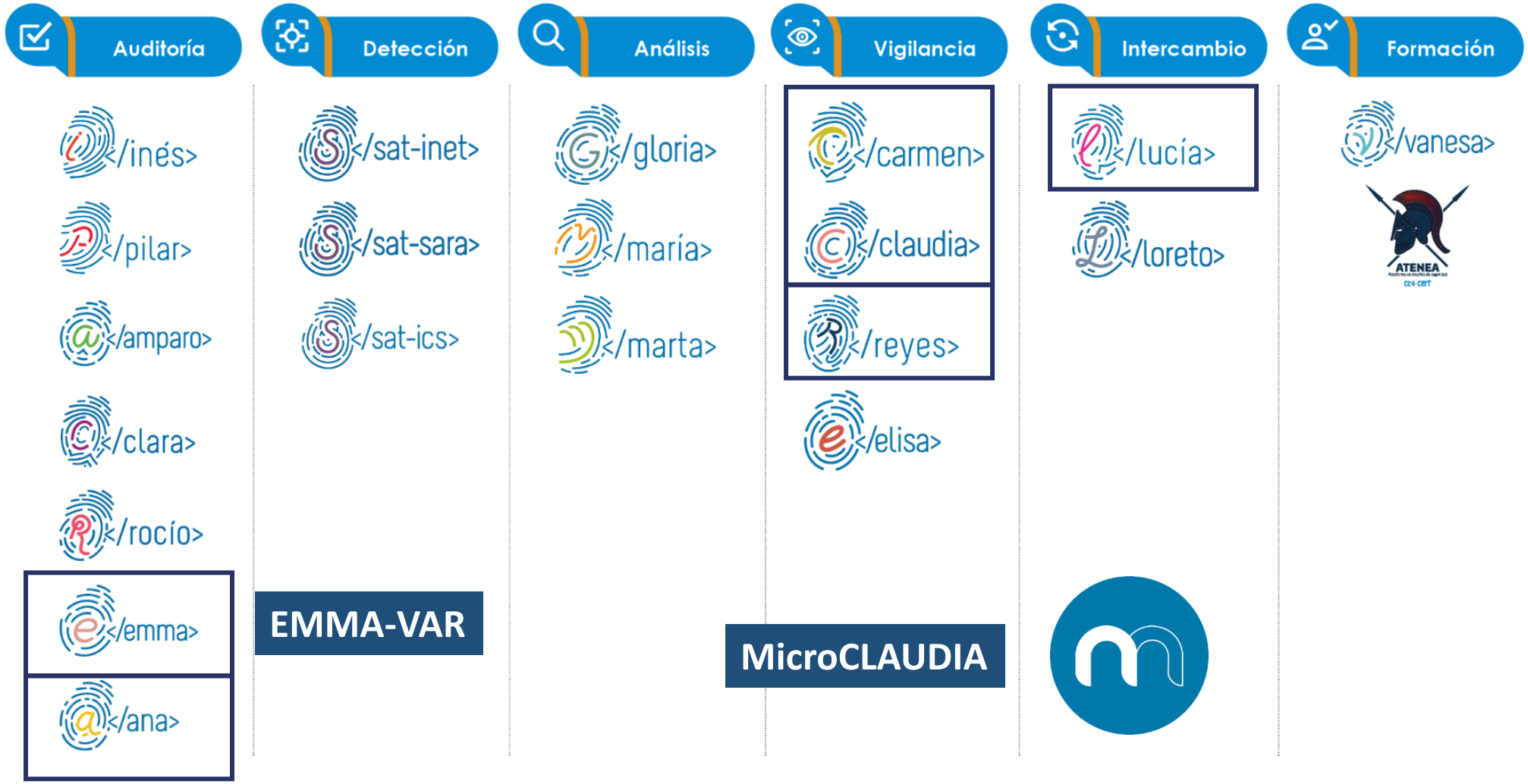
En colaboración con:

FEMP
FEDERACIÓN ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

Índice

1 Herramientas CCN-CERT



1 CARMEN. Esfuerzo de desarrollo

carmen Ciberinteligencia Avanzada
42
Implantaciones en organismos y empresas

carmen central
27
Integraciones con CARMEN Central

12
Despliegues en servidores y puestos usuarios

claudia

- Desarrollo propio
- Histogramas
- Gestión de listas (blancas y negras)

2010 **2011** **2012** **2013**

- Desarrollo externalizado: **S2 Grupo**
- Dirección de proyecto: CCN-CERT
- Aumento de capacidades de detección
- Captura de tráfico
- Migración a PosgreSQL

2014 **2015** **2016** **2017**

- **Cambio de arquitectura SQL → NO-SQL (Elastic Search)**

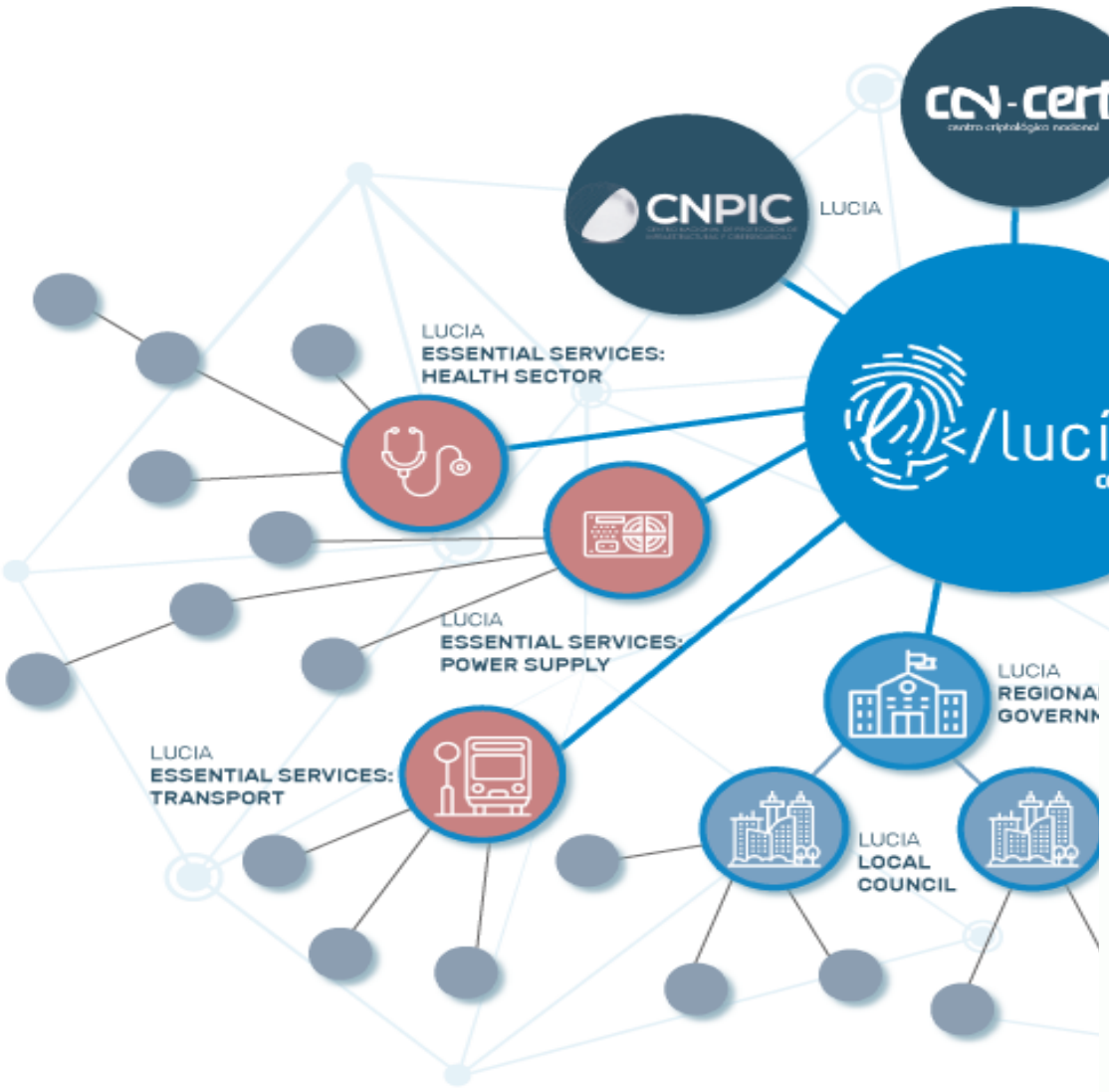
2018 **2019** **2020**

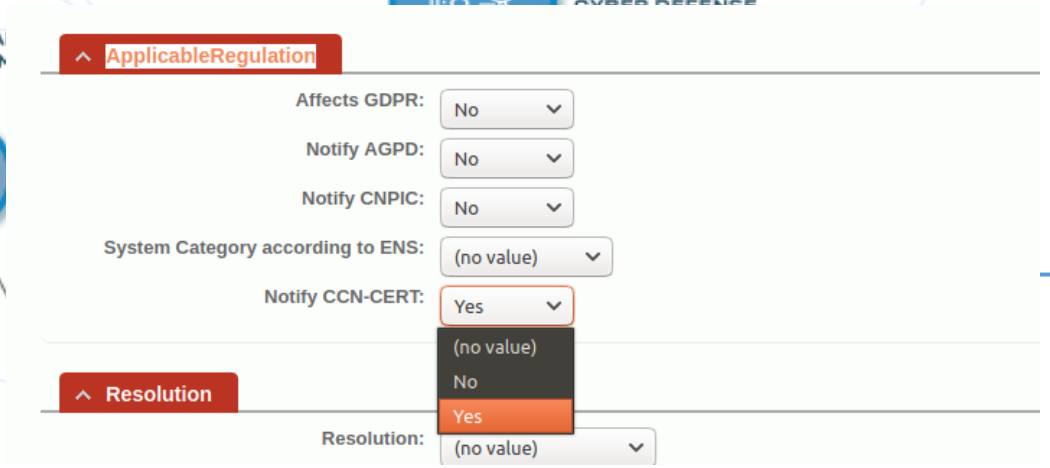
- Desarrollo de CARMEN Central
- Integración con REYES
- Análisis automático de adjuntos de correo
- Carga de ficheros pcap

- Desarrollo de CLAUDIA
- Integración con MARTA
- Integración con LUCIA
- Integración con Panda Adaptive Defense

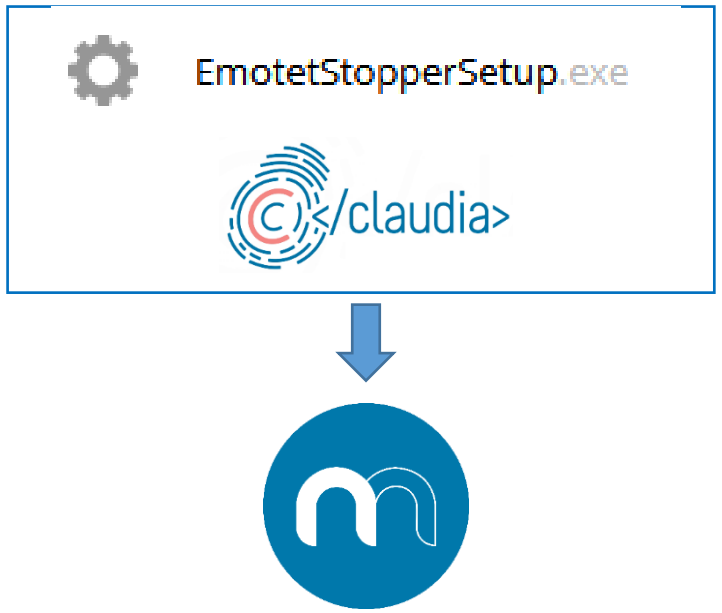
MicroCLAUDIA

1 LUCIA. Esfuerzo en intercambio





1 Herramientas CCN-CERT. MICROCLAUDIA

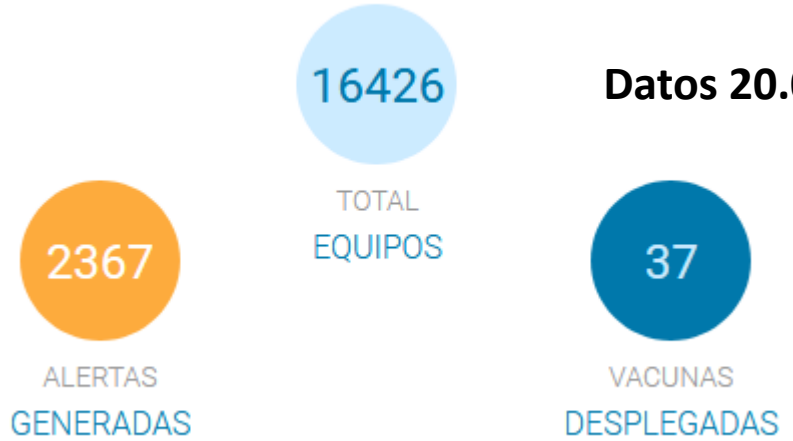


RESULTADOS:

- Nuevos incidentes relacionados con nuevass muestras de ransomware: Snake (Fresenius) / Hydra / Robinhood / Xorsit / MorrsbatchCrypto / Cryptolocker….
  - **Informe Código Dañino + Vacuna**
- **Ataque parados desde el 27 de abril con microCLAUDA-->+200.**
- **Alertas +2000**

OBJETIVOS:

- Mayor esfuerzo en vacunas
- Vacunas genéricas que paran TTP,s de grupos de ataques
- Mejor visibilidad de alertas
- Facilidad de escalado a CLAUDIA
- Integración con SIEM GLORIA / Hasta ahora conexión con CARMEN
- Uso en organismo



Datos 20.06.2020

2 ENS. Lecciones aprendidas

- Incidentes por sistemas fuera de soporte y falta de actualización.
- Incidentes por falta de capacidad de detección
- Incidentes por falta de medidas antiDDoS.
- Incidentes por falta de adecuadas configuraciones de seguridad
- Incidentes por falta de políticas de seguridad y concienciación de usuarios
- Escasa preparación ante incidentes complejos. Sin estructura ni herramientas.

- MUY REACTIVOS
- SUPERFICIE DE EXPOSICIÓN ELEVADA
- AUSENCIA DE VIGILANCIA
- NO SE NOTIFICAN LOS INCIDENTES

Actualización + Config. Seguridad + Vigilancia + Serv. Externalizados + Auditorias + Servicios ciberseguridad compartidos

3 Centros de Operaciones de Ciberseguridad

SOC

5

objetivos de los Centros de Operaciones de Ciberseguridad.

- Potenciar las capacidades de seguridad
- Más información de ataques
- Conocer la exposición ante ataques
- Mayor capacidad de correlación de ataques
- Mejor capacidad de respuesta

Plan de acción

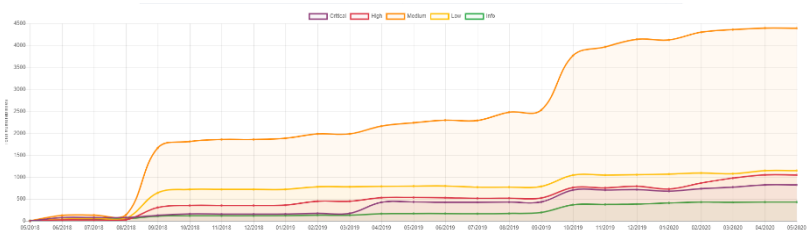
88

medidas para garantizar la continuidad del trabajo en remoto.

Medidas del Plan de acción

- ✓ Concienciación de usuarios
- ✓ Protección del acceso remoto
- ✓ Protección del correo electrónico
- ✓ Protección de la videoconferencia
- ✓ Incremento de la detección y vigilancia

- **Uso de herramientas comunes**



4 Necesidad de soporte

- Necesidad que en el sector público se ponga en valor las herramientas / **servicios de ciberseguridad comunes y compartidos**
- Se necesitan mejoras anuales, muchas peticiones de organismos pero SIN PRESUPUESTOS PARA ESTAS HERAMIENTAS.
- Difícil continuar el soporte por parte de un solo organismo
- Necesidad de convenios u otros instrumentos para su desarrollo y evolución.

Organismos ven la herramienta como una solución para su sistema de seguridad y no se ve su aportación a la mejora general de la solución.

5 Plataforma común de intercambio

Capacidad de **intercambio** de información sobre **ciberamenazas**

Capacidad de **registro y notificación** de vulnerabilidades

Capacidad de **intercambio masivo de datos**

Capacidad de gestión de ciberincidentes

Con incorporación de taxonomía, criticidad, inclusión de autoridades subordinadas, notificaciones a terceros y métricas de eficiencia en su resolución.

Capacidad de **análisis de muestras**

Capacidad de **comunicaciones seguras** entre los actores involucrados en diferentes formatos y plataformas

Generación de **estadísticas e informes** agregados

6 CONCLUSIONES

Prevención

Desarrollar

Capacidades Técnicas y Humanas

- Herramientas CCN-CERT
- Programa formación personal

Detección

Defender

Medidas activas

- Integración capacidades
- Soluciones comunes
  - DNS AAPP
  - ANA
  - INES

Respuesta

Disuadir

SOC integrados

- Colaboración público-privada
- Respuesta conjunta

II ENCUENTRO DEL ENS

DIEZ AÑOS DE NUEVOS RETOS Y SOLUCIONES

centro criptológico nacional

En colaboración con:

FEDERACIÓN ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

GOBIERNO DE ESPAÑA · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

Muchas gracias.

Estratégicos

Estándar