ENDPoint TTP

Centro de Operaciones de Ciberseguridad

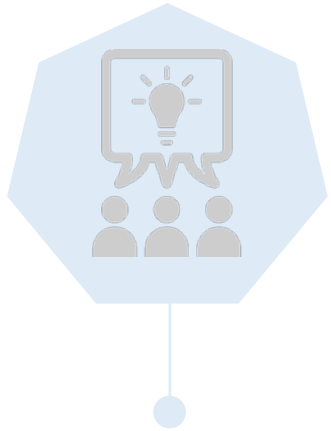
centro criptológico nacional

vSOC: respuesta a las necesidades prioritarias

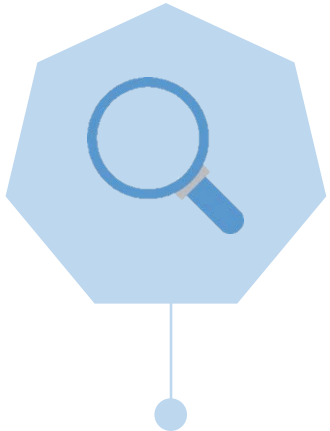
Objetivos vSOC

> **“Mejorar las capacidades de despliegue, actuación y protección de las entidades.”**

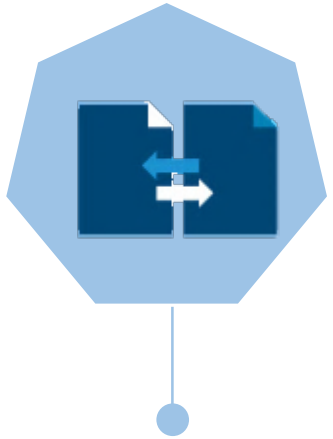
Dar seguridad a ayuntamientos y diputaciones



Más información de ataques



Mayor visibilidad sobre incidentes



Mayor capacidad de correlación de ataques

Mejor capacidad de respuesta

CCN
centro criptológico nacional

Evolución del malware

El efecto de una infección del virus *Barrotes*.

Monitorizar el equipo

- ✓Tiene un comportamiento anómalo
- ✓Las acciones del usuario son distintas
- ✓Controla la maquina antes de que se extienda la infección
- ✓Poder actuar sobre los equipos
- ✓OBTENER TTP (Tactics, Techniques and Procedures
- ✓)

PRE-ATT&CK

Enterprise

All Platforms

Linux

macOS

Windows

Mobile

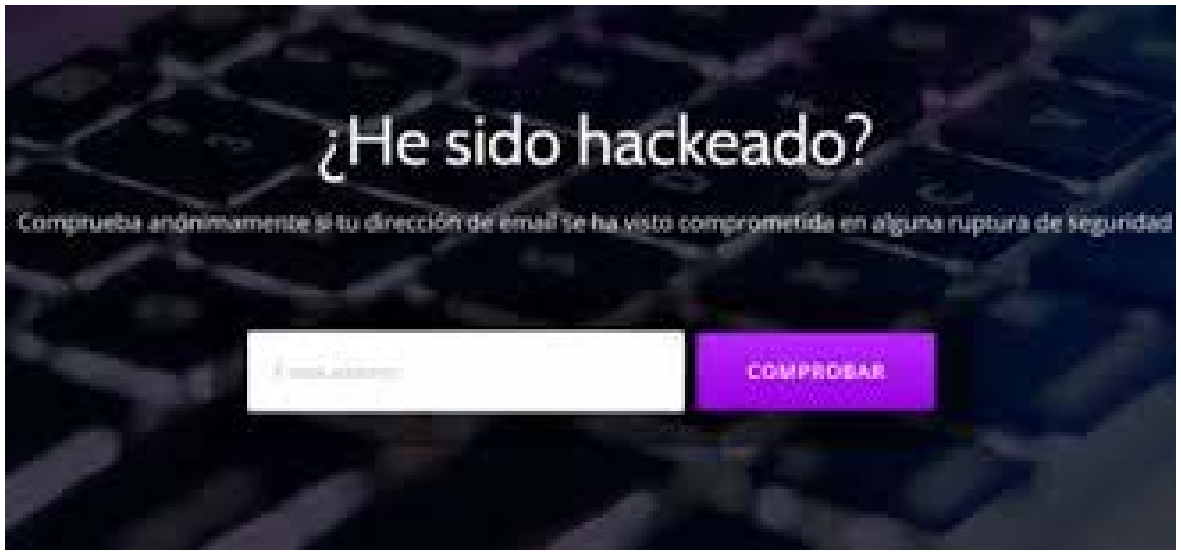
Enterprise Matrix

The full ATT&CK Matrix™ below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the knowledge base.

Last Modified: 2018-10-17T00:14:20.652Z

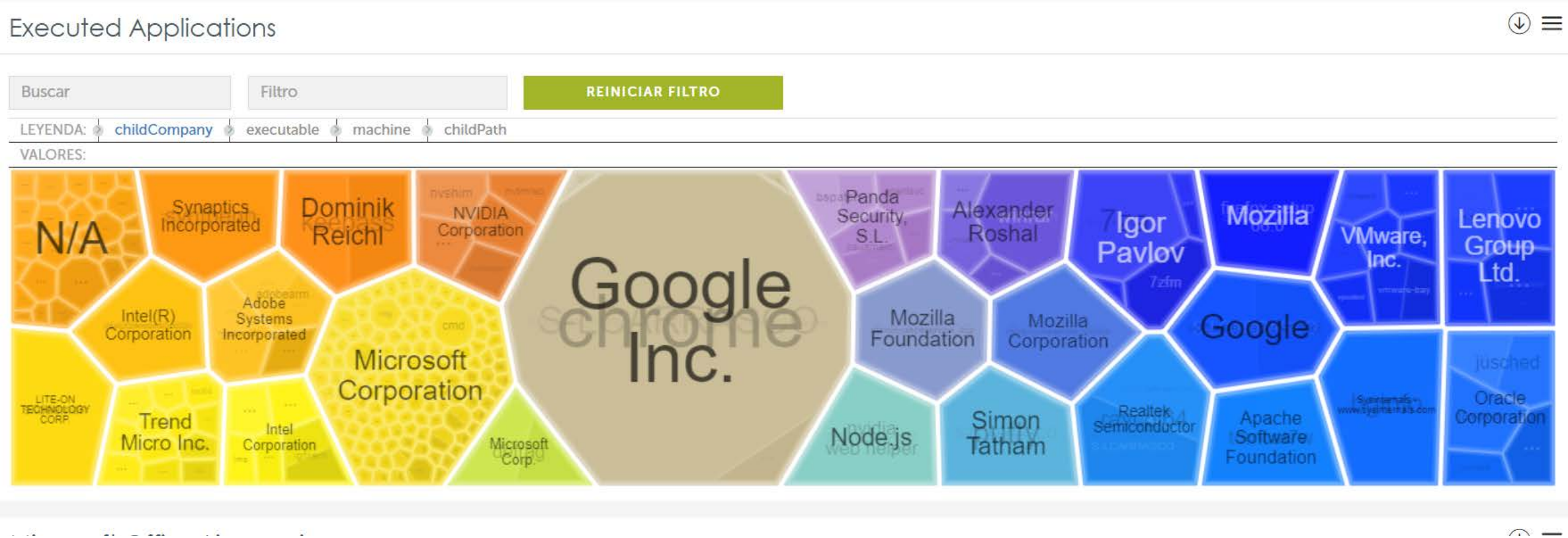
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels

Revisión de acciones pasadas

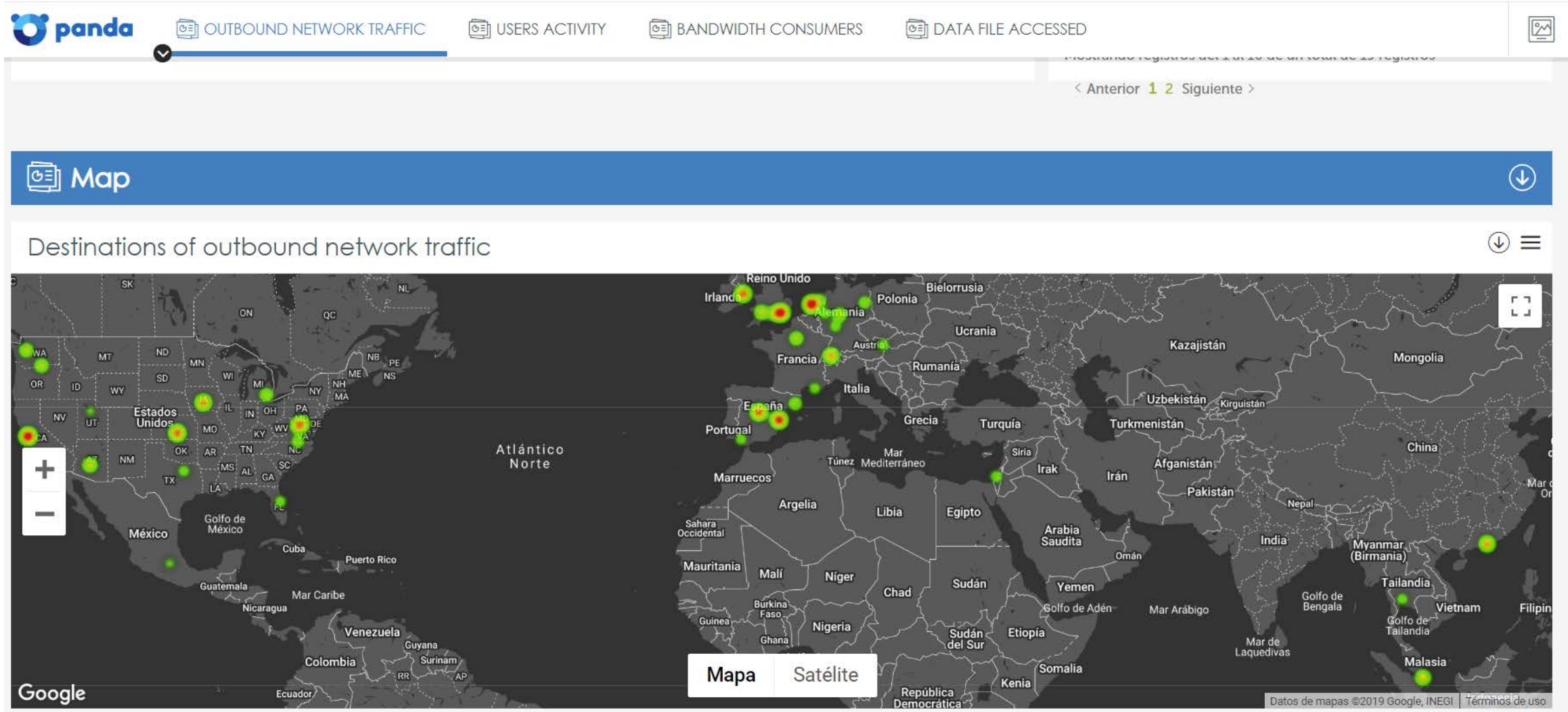


- ✓Los IOC actuales suelen relatar eventos acontecidos
- ✓Conocer si he sido atacado es clave
- ✓Ampliar mi revisión de estado
- ✓Mejorar mi seguridad perimetral

- **Tener un control de lo instalado en el pc**



Ubicar las conexiones por cada equipo



PANELES
Seguridad
Licencias
Informe ejecutivo

MIS LISTADOS Añadir
Estaciones y portátiles d...
Malware ejecutado
New list: Currently blocke...
New list: Exploit activity
nuevosequiposmios
PUPs ejecutados
Servidores desprotegidos
Advanced Visualization T...

Últimos 7 días

ESTADO DE PROTECCIÓN

Correctamente protegido (2) | Protección con error (1) | Error Instalando (1)

EQUIPOS SIN CONEXIÓN

> 72 horas	> 7 días	> 30 días
2	2	2

PROTECCIÓN DESACTUALIZADA

1	Protección
1	Conocimiento
0	Pendiente de reinicio

PROGRAMAS PERMITIDOS POR EL ADMINISTRADOR

0

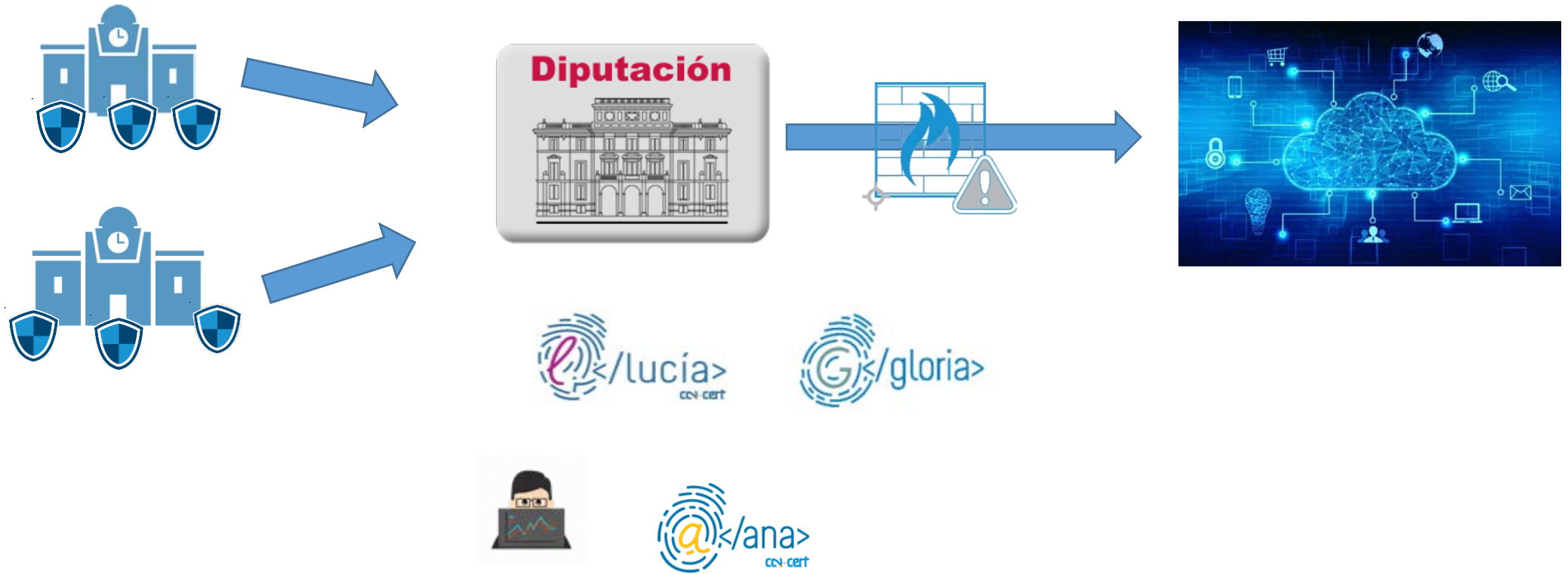
CLASIFICACIÓN DE TODOS LOS PROGRAMAS EJECUTADOS Y ANALIZADOS

CONFIABLES	290	(100,00%)
MALWARE	0	(0,00%)
EXPLOITS	0	(0,00%)
PUPS	0	(0,00%)

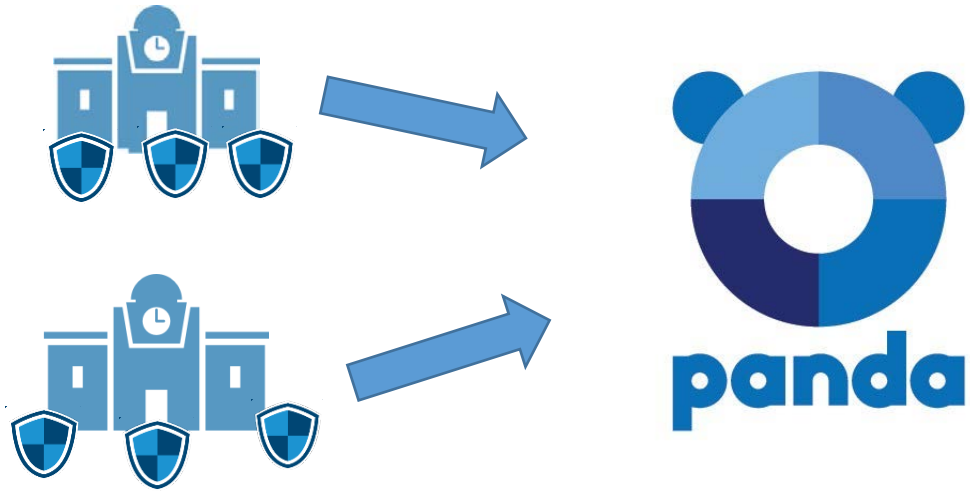
ACTIVIDAD DE MALWARE

PROGRAMAS ACTUALMENTE BLOQUEADOS EN CLASIFICACIÓN

Remediación del equipo de forma remota



PANDA NUBE ADMINSITRACION



Ayuda

Comunidad CCN-CERT

Muchas Gracias

E-mails

info@ccn-cert.cni.es

ccn@cni.es

sondas@ccn-cert.cni.es

redsara@ccn-cert.cni.es

organismo.certificacion@cni.es

Páginas web:

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es