brokeCLAUDIA

Broken access control vulnerability in microCLAUDIA 3.2.0

ccn-cert
centro criptológico nacional

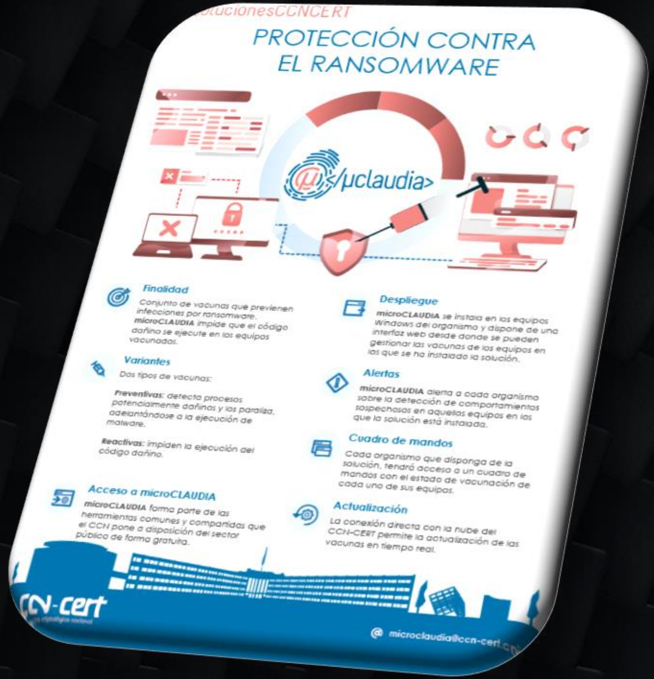
Broken Access Control

Moving up from the fifth position, 94% of applications were tested for some form of broken access control with the average incidence rate of 3.81%, and has the most occurrences in the contributed dataset with over 318k.

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=broken+access+control

microCLAUDIA

It is a CLAUDIA engine based capability that provides protection against harmful ransomware code to an organization's equipment. It does this by using a lightweight agent for Windows systems that handles vaccine deployment and execution.



olucionesCCNCERT

PROTECCIÓN CONTRA EL RANSOMWARE

Finalidad

Conjunto de vacunas que previenen infecciones por ransomware. **microCLAUDIA** impide que el código dañino se ejecute en los equipos vacunados.

Variantes

Dos tipos de vacunas:

Preventivas: detecta procesos potencialmente dañinos y los paraliza, adelantándose a la ejecución de malware.

Reactivas: impiden la ejecución del código dañino.

Acceso a microCLAUDIA

microCLAUDIA forma parte de las herramientas comunes y compartidas que el CCN pone a disposición del sector público de forma gratuita.

Despliegue

microCLAUDIA se instala en los equipos Windows del organismo y dispone de una interfaz web desde donde se pueden gestionar las vacunas de los equipos en los que se ha instalado la solución.

Alertas

microCLAUDIA alerta a cada organismo sobre la detección de comportamientos sospechosos en aquellos equipos en los que la solución está instalada.

Cuadro de mandos

Cada organismo que disponga de la solución, tendrá acceso a un cuadro de mandos con el estado de vacunación de cada uno de sus equipos.

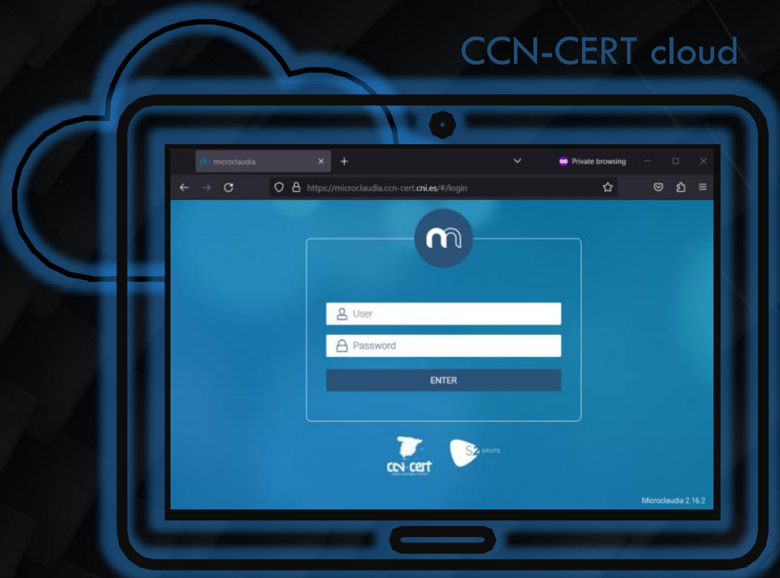
Actualización

La conexión directa con la nube del CCN-CERT permite la actualización de las vacunas en tiempo real.

CCN-cert

@ microclaudia@ccn-cert.c

CCN-cert
centro criptológico nacional

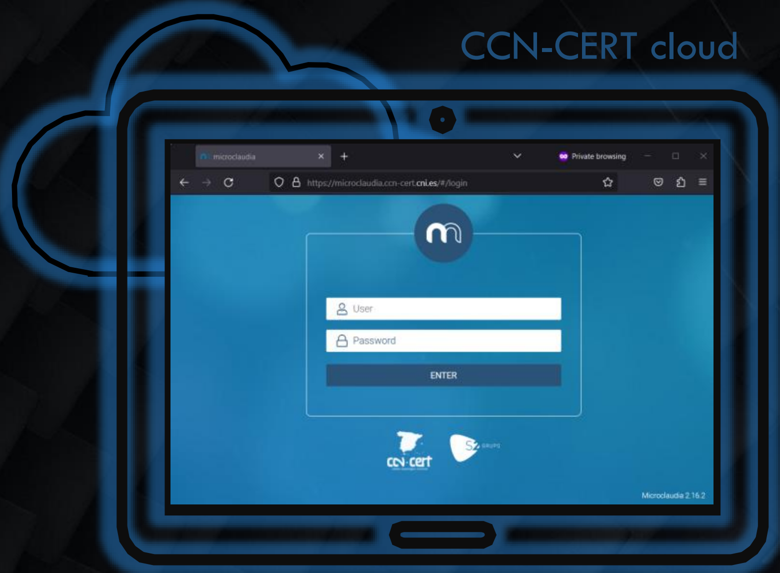


CCN-CERT cloud

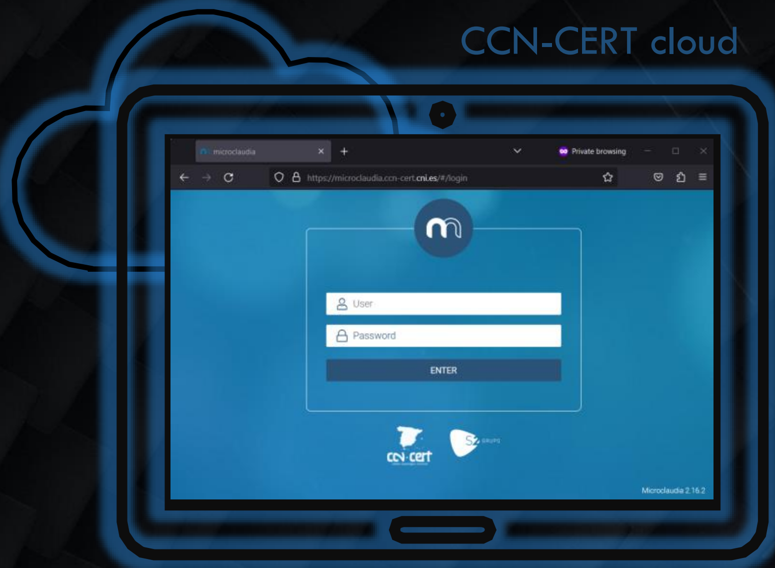
microCLAUDIA central service

ccn-cert
centro criptológico nacional

CCN-CERT cloud

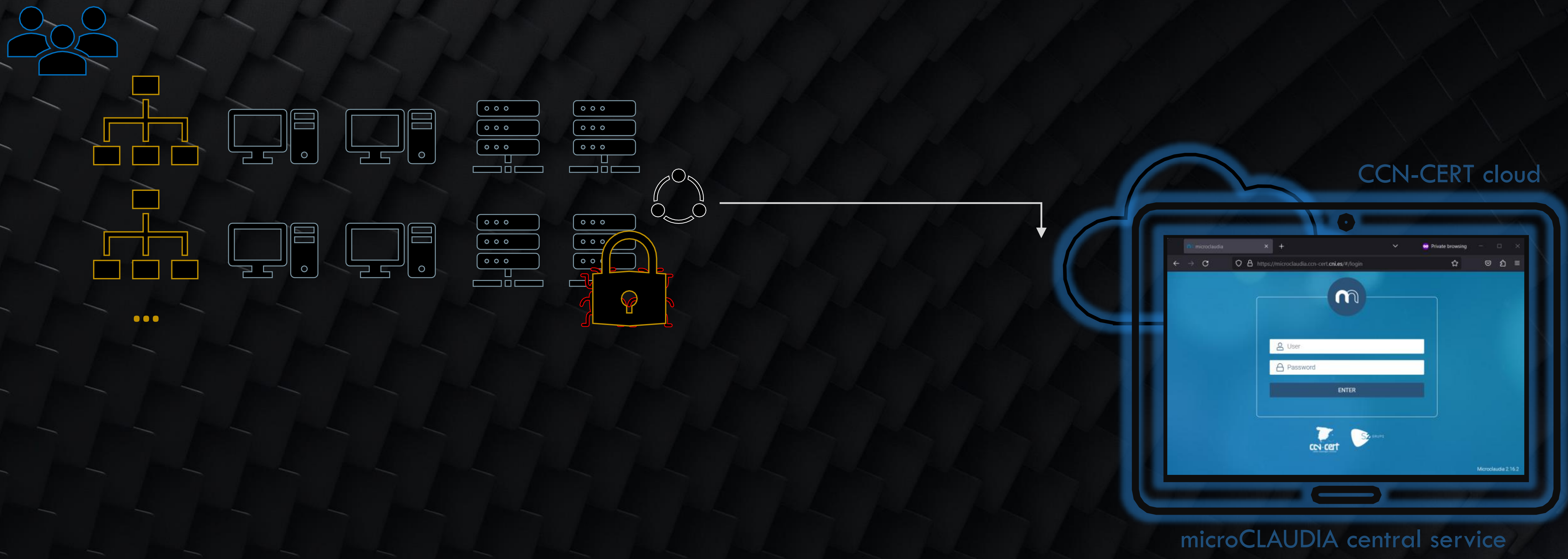


microCLAUDIA central service



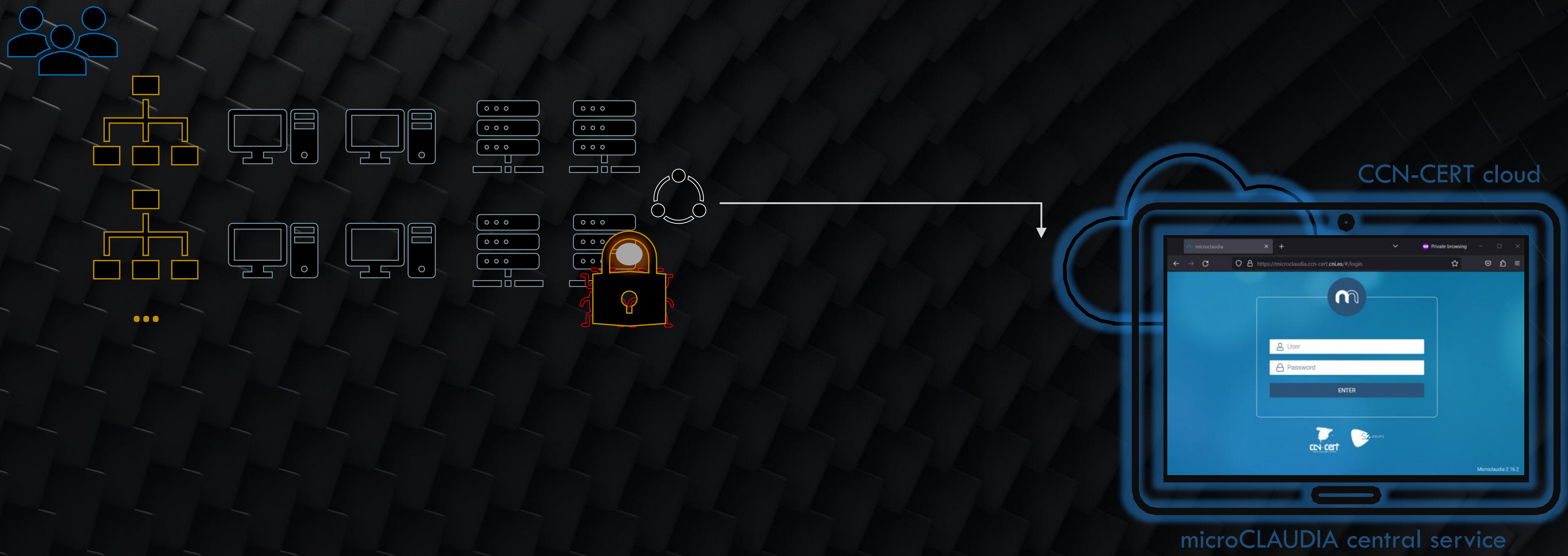
CCN-CERT cloud

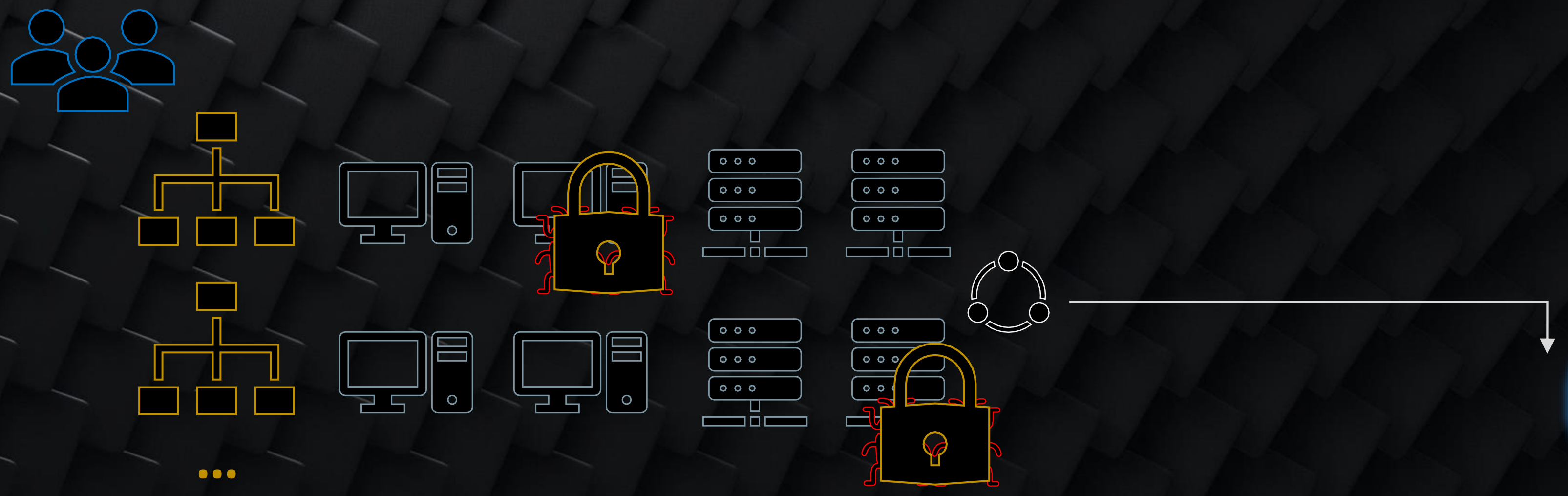
microCLAUDIA central service

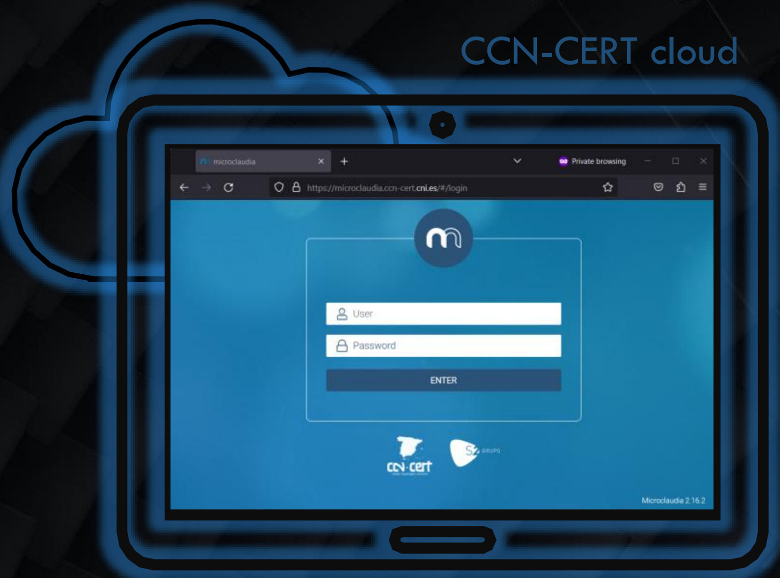


CCN-CERT cloud

microCLAUDIA central service


CCN-CERT cloud
microclaudia
Private browsing
https://microclaudia.ccn-cert.cni.es/#/login
User
Password
ENTER
ccn-cert
Microclaudia 2.16.2
microCLAUDIA central service

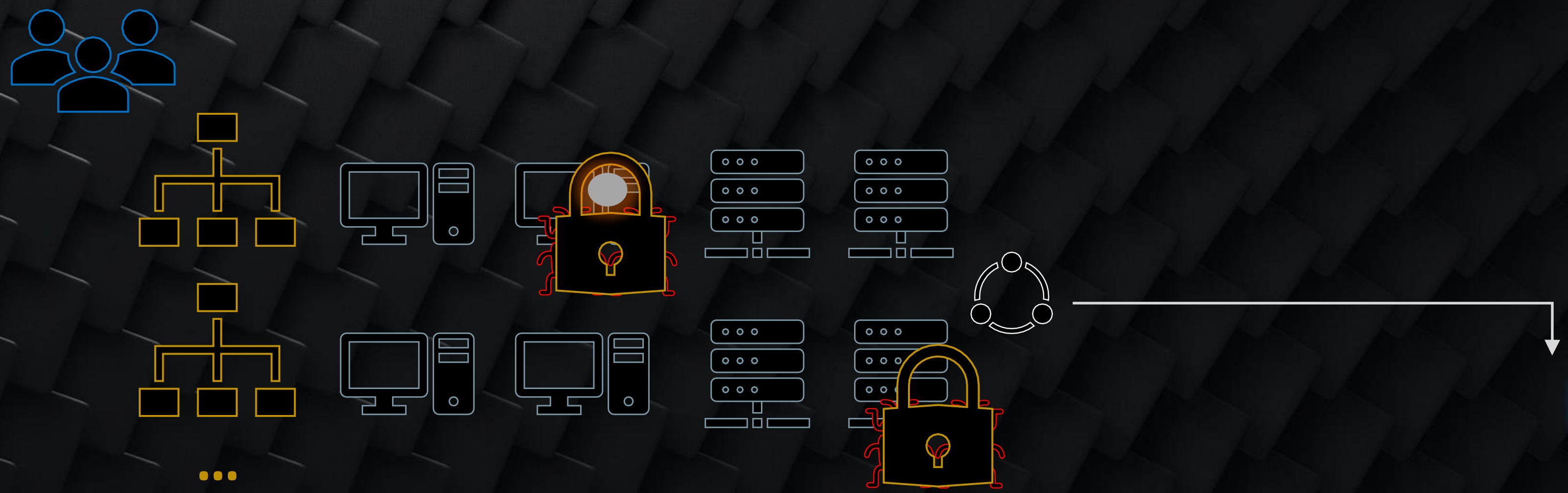




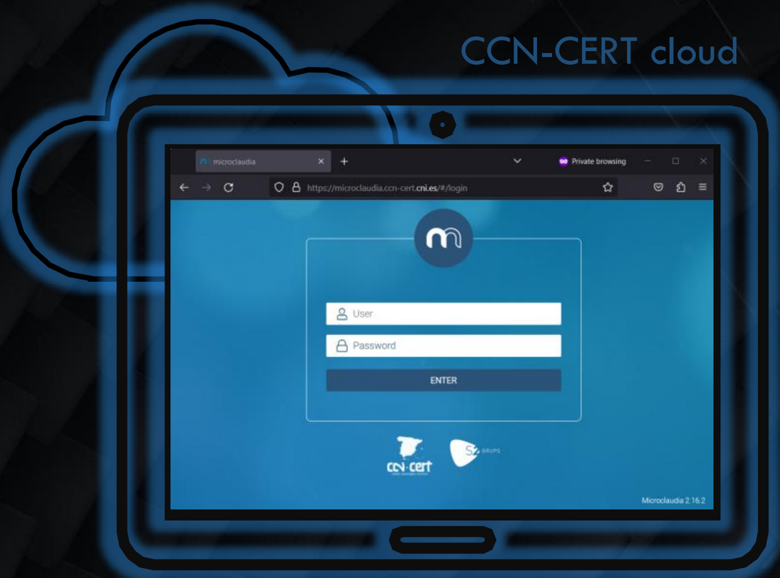
CCN-CERT cloud

microCLAUDIA central service

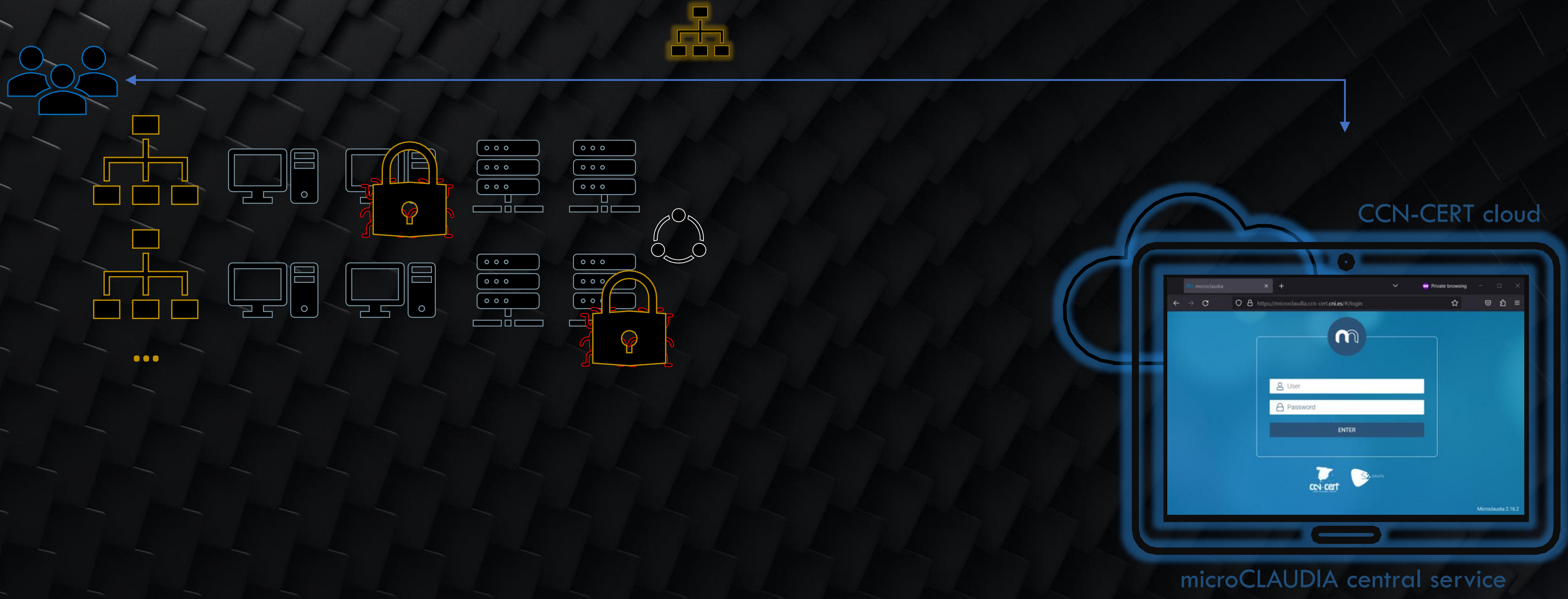
ccn-cert centro criptológico nacional



CCN-CERT cloud

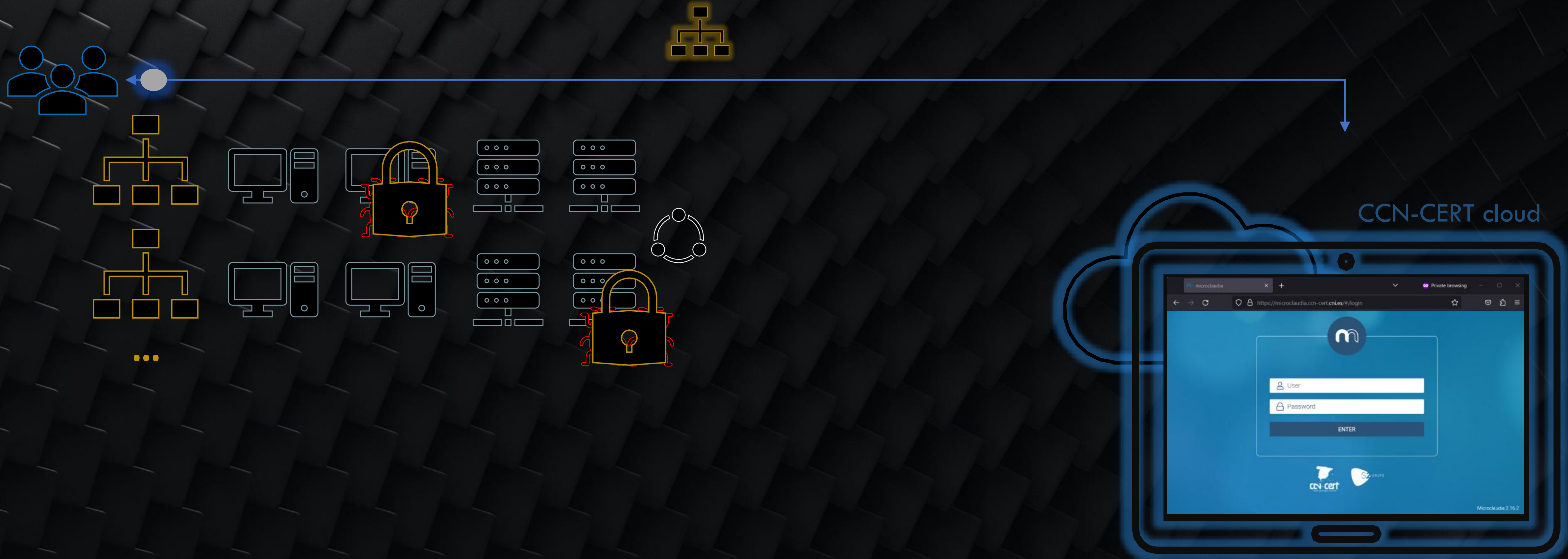


microCLAUDIA central service



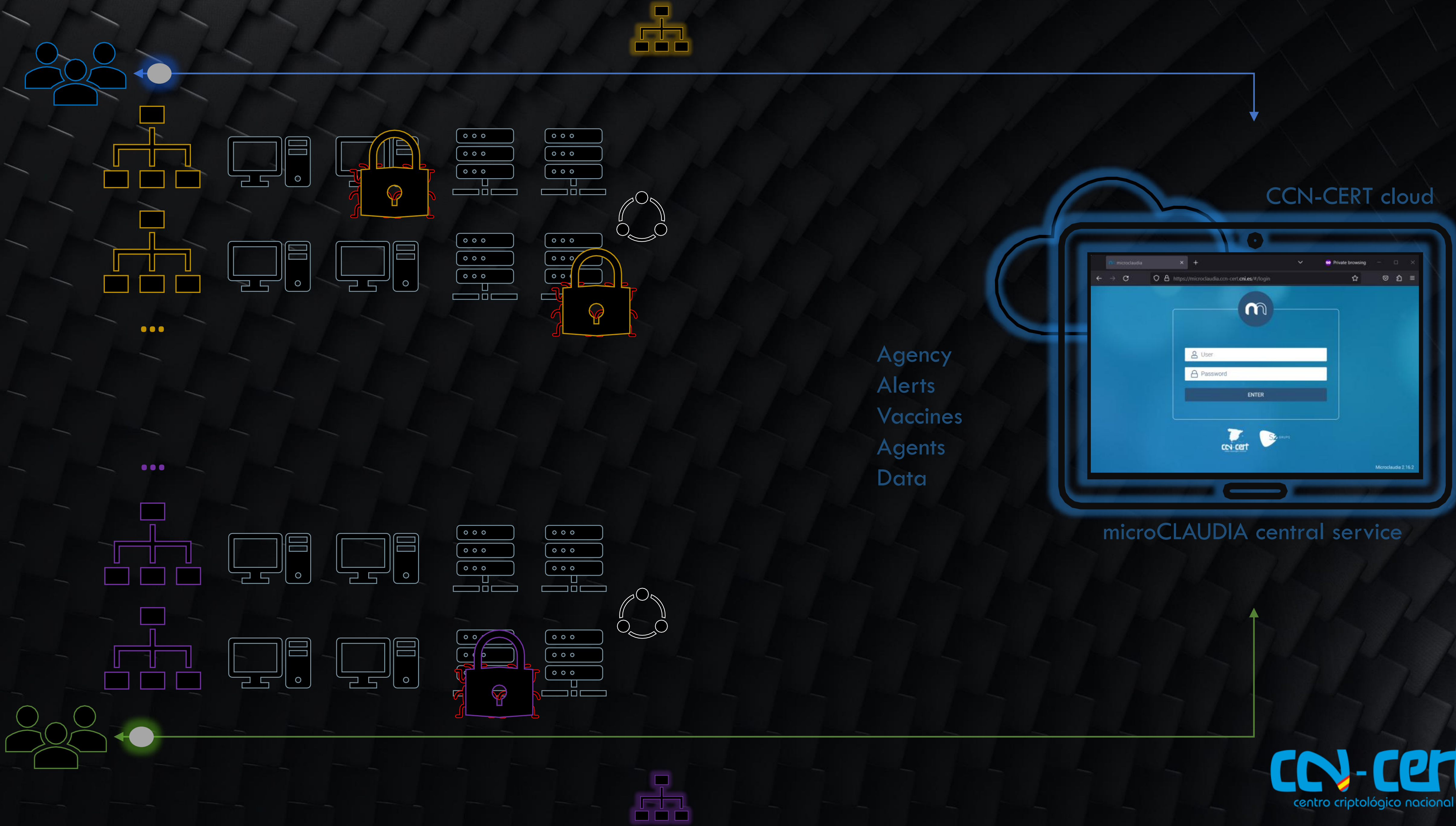
CCN-CERT cloud

microCLAUDIA central service



CCN-CERT cloud

microCLAUDIA central service



ccn-cert
centro criptológico nacional

brokeCLAUDIA

- Broken access control vulnerabilities exist when a user can access resources or perform actions that they are not supposed to be able to.
- In version 3.2.0 and earlier versions of microCLAUDIA, there is a broken access control vulnerability (brokeCLAUDIA) that allows an attacker who has previously gained access to an account to access or modify data from other organizations not associated with the user.
- In other words, the attacker could manipulate information from organizations that are not directly related to the compromised account.

CCN-CERT cloud

https://microclaudia.ccn-cert.cni.es/#/login

User

Password

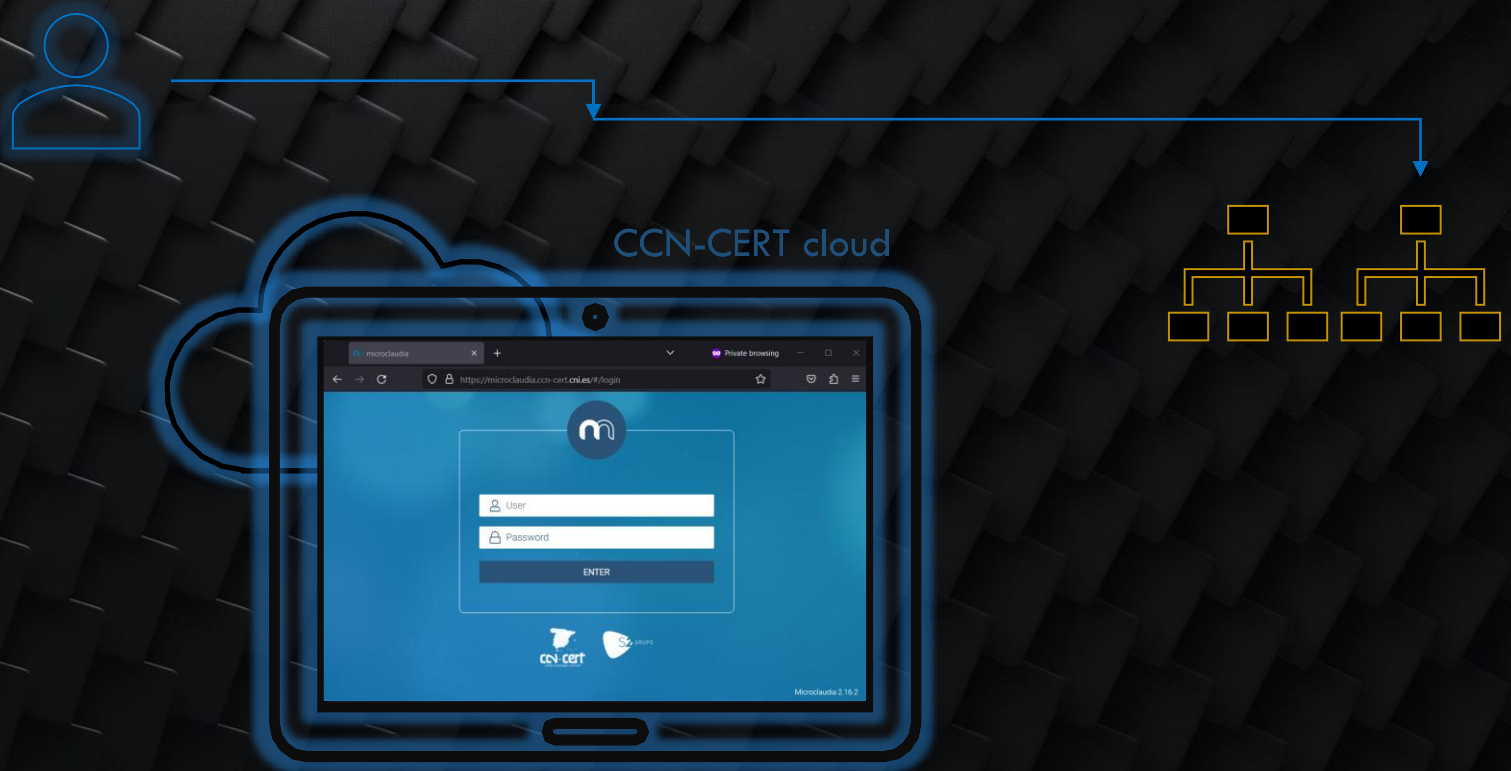
Microclaudia 2.16.2

microCLAUDIA central service

microclaudia
Private browsing
https://microclaudia.ccn-cert.cni.es/#/login
User
Password
ENTER
ccn-cert
Microclaudia 2.16.2

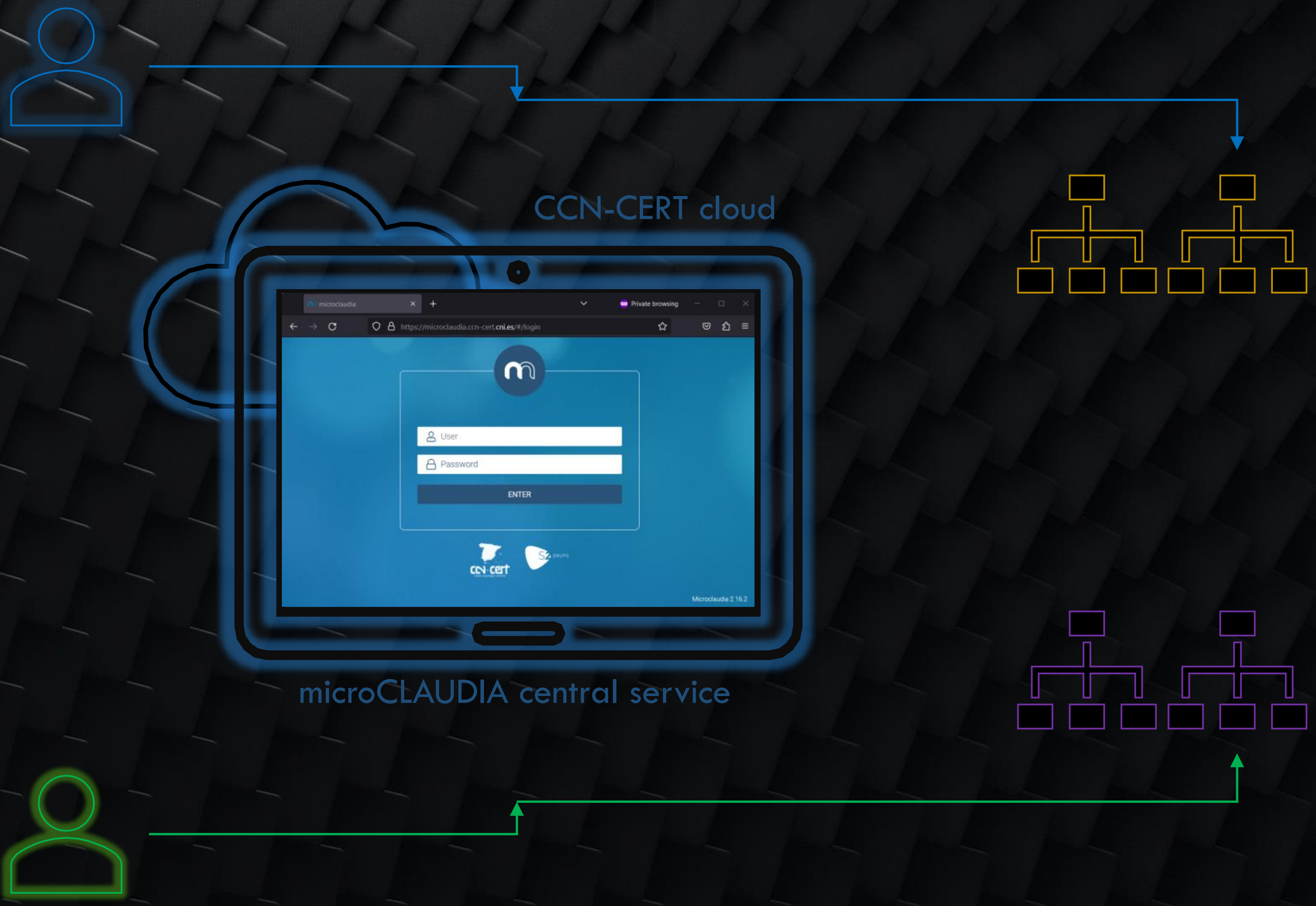
CCN-CERT cloud

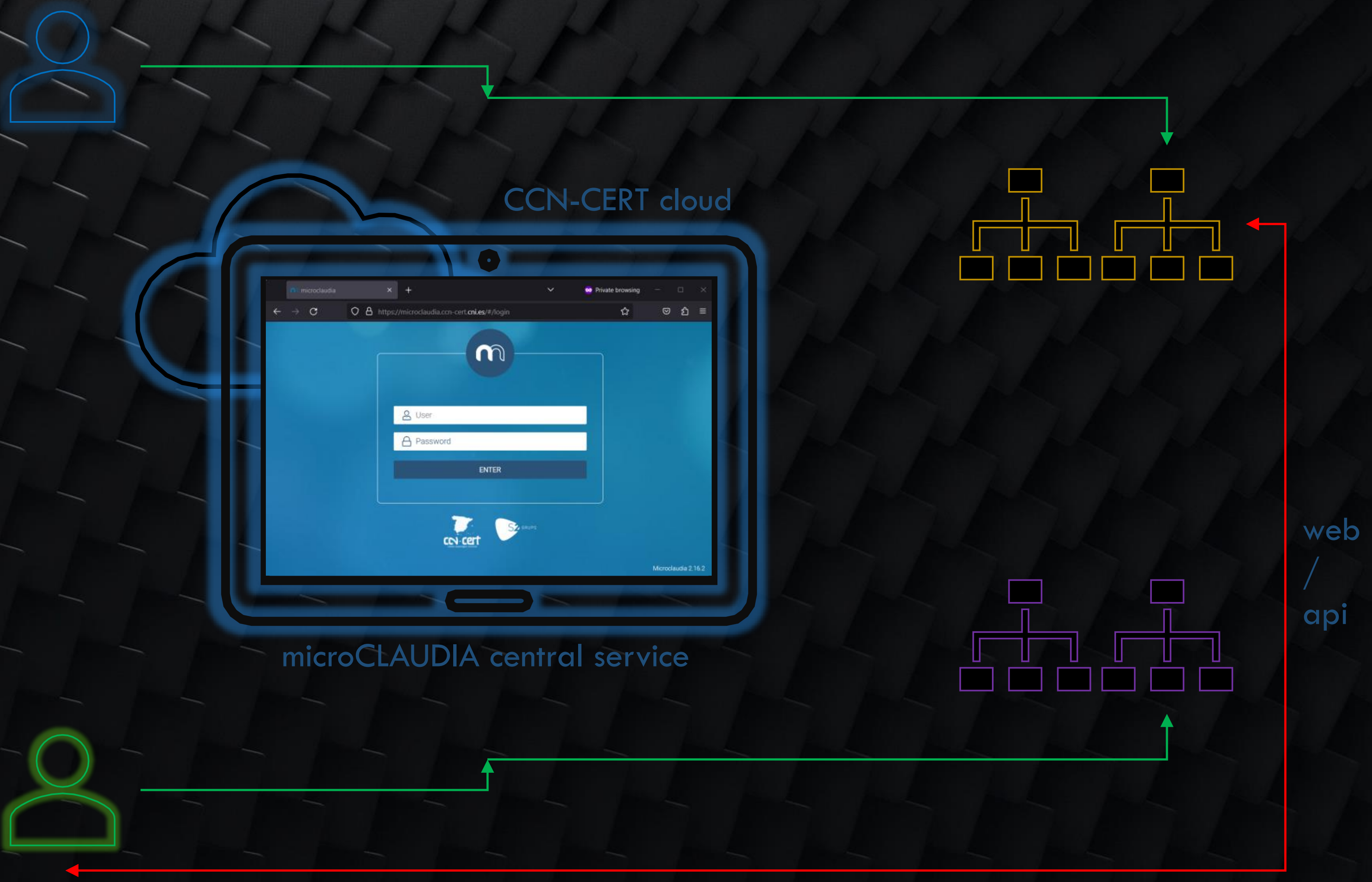
microCLAUDIA central service



CCN-CERT cloud

microCLAUDIA central service

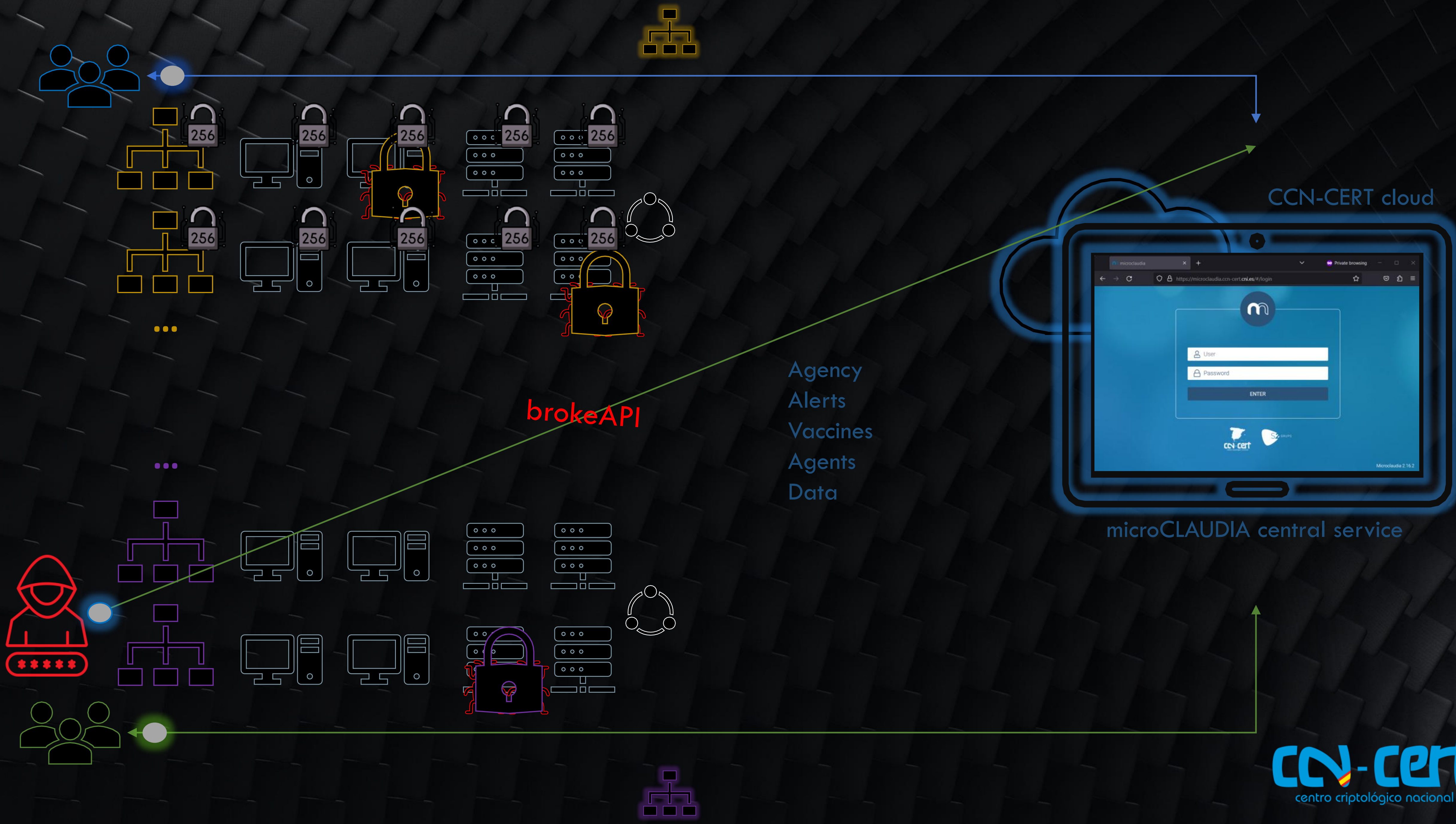

CCN-CERT cloud
microclaudia
Private browsing
https://microclaudia.ccn-cert.cni.es/#/login
User
Password
ENTER
ccn-cert
S2 GRUPO
Microclaudia 2.16.2
microCLAUDIA central service



CCN-CERT cloud

microCLAUDIA central service

web
/
api



CCN-CERT cloud

Agency

Alerts

Vaccines

Agents

Data

microCLAUDIA central service

ccn-cert
centro criptológico nacional

brokeCLAUDIA

To successfully exploit this vulnerability, it's crucial to grasp the following key aspects:

1. The attacker needs to obtain the identifiers associated with those organizations to perform the unauthorized actions.

2. The vulnerability exists only when making requests through the API, not through the web interface.

3. The identifiers used in web requests are transmitted in the URL, which poses a risk if an attacker gains access to the identifiers by dumping the history of a compromised machine.

4. The manager role grants the ability to modify (activate/deactivate vaccines, install/uninstall agents, etc.) data.

CCN-CERT
centro criptológico nacional

Remediation

Remediation

In order to remediate the broken access control vulnerability identified in microCLAUDIA, it is essential to implement several key measures.

First and foremost, it is imperative to enhance API controls to prevent unauthorized access to information. Implement checks to ensure that direct access to data is restricted, and enforce verification processes to confirm the association of the user with the organization before granting access.

Moreover, it is crucial to address the specific security concern related to the transmission of identifiers in GET requests. This entails ensuring that identifiers vital for the main functionality are not transmitted in a manner that exposes them. Adopting secure methods of transmission is highly recommended to fortify this aspect of microCLAUDIA's security architecture.

By diligently implementing these measures, the identified broken access control vulnerability in microCLAUDIA can be effectively mitigated. The combination of enhanced API controls and secure data transmission practices forms a robust defense, significantly reducing the risk of unauthorized access and manipulation of sensitive information.

Thank you

https://github.com/TheMalwareGuardian/brokeCLAUDIA

ccn-cert
centro criptológico nacional

Questions?