S2GRUPO

microClaudia:
User Workstation Vaccination Center

microClaudia

microCLAUDIA is a user workstation vaccination system, where deploying an agent installed on devices, it distributes several “vaccines” which prevent ransomware type of infections and prevent the execution of this kind of malicious code being executed on computers where the solution is installed.

Key Features

→ **Quick and agile vaccine deployment:** easy and efficient deployment of new vaccines.

→ **Vaccine exceptions by organization:** Customisation of exceptions according to specific needs.

→ **Suspicious behaviour alerts:** Automatic alert with email notifications.

→ **Connection to the centralized vaccine system:** Continuous synchronisation with the central platform.

→ **Automatic agent notifications** and updates without manual intervention.

Examples of available Vaccines

BITPAYMERUP
CERBER
CLOP
CONTI
DHARMA
EGREGOR
EMILISUB
GRANDCRAB
DARKRACE
DARKSIDE
HACKBIT
MAKOP
MAZE
NEMTY
NJRAT
PHOBOS
RAGNAR LOCKER
RYUK
HIVE
GANDCRAB
SNAKE
SODINOKIBI
WANNACRY
NOKOYAWA
BLACKCAT
LOCKBIT
MEDUSALOCKER
BLACKBASTA
AZADI

Benefits + Value Proposition

→ **Advanced protección at all times:** Recognition and execution of certified vaccines in both connected and disconnected modes.

→ **Specialized vaccine development:** created by cybersecurity experts from Lab52 (S2GRUPO) and CCN, with real-time updates to quickly respond to new threats.

→ **User autonomy:** Enables organization administrators to manage the vaccination of their fleet of devices and servers, with the ability to apply vaccines by areas.

→ **Integration with GLORIA:** Complete traceability, event correlation, and automated notification alerts.

→ **On-demand telemetry control:** Detailed process monitoring when required.

Architecture and Technology

microCLAUDIA relies on a compatible agent with Windows™ and Linux systems, which uses advanced techniques to simulate execution controls employed by malware. This approach makes the ransomware believe it is already active, blocking its malicious behaviour from the beginning. The solution features a centralized web interface that allows organizations to download and execute the vaccines configured by them, as well as tomonitor the status of all devices. Additionally, the service includes automatic vaccine updates, ensuring continuous protection against new ransomware variants and execution methods.

The solution includes a centralised web interface which allows you to:

→ Download and execute customised vaccines configured by the organisation.

→ Monitor the protection status of all connected computers.

→ Ensure continuous protection through automatic updates against new ransomware variants.

Technical Specifications

→ Compatibility with Windows™ (**Windows XP** and above) and Windows Server (2023 and above systems).

→ **Support for Windows VDI** virtualized environments.

→ Generation of standard **Windows GOLDEN Image templates.**

→ Optional connection to the central service of **microCLAUDIA** in S2GRUPO cloud for vaccine downloads and automatic agent updates.

Installation Options

→ Manual.
→ Automated **(through GPO, SCCM, among others).**

Use cases

→ **Preventive Blocking:** Stops known malware used by ransomware groups by pretending the computer is already infected.

→ **Advanced Detection:** Identifies the execution of commands and techniques used in ransomware campaigns, including featured APT group threats.

→ **Personalized Protection:** Enables the application of vaccines designed specifically for the organisation, based on S2GRUPO´s cyberintelligence.

Success stories

→ **Customer testimonials:** available by the comercial sales team.

→ **Featured success story:** successul implementation case in the Government of Costa Rica, achieving a protected environment against critical threats.

Licensing models

Per-agent licensing, with scalable pricing according to organisation needs.

microClaudia: 5 KEY CONCEPTS

1. **Easy and fast** new vaccines deployment.
2. **Specialized Malware vaccines** development.
3. **Real Time Control:** On-demand Telemetry monitoring.
4. **Centralized Synchroni sation:** Continuous connection to the vaccine platform.
5. **Independent management:** Allows administrators to control and personalize the protection of the entire technology infrastructure.

Contact information

To learn more about how microClaudia can help protect your organization or to request a demo, contact us.
902 882 992 / hola@s2grupo.es /www.s2grupo.es