EMMA:
Vigilancia sobre la red

Contexto:

La mejora continua implica complementar la implementación de medidas de seguridad con un incremento de la vigilancia. De este modo, es posible conseguir estándares de seguridad acreditables de acuerdo a las inspecciones STIC llevadas a cabo. **EMMA** es una solución del **CCN-CERT** para conseguir Vigilancia sobre la red.

¿Qué es Emma?

Emma es una solución que incrementa la seguridad de la red corporativa (tanto IT como OT) a través de **la visibilidad, control / respuesta y cumplimiento** de todos los activos que se conectan a la red (Wifi, Cableada y VPN), desde dispositivos de usuarios, IoT, OT a electrónica de red.

En la verificación del nivel de seguridad de los dispositivos de la electrónica de red (Cumplimiento), **EMMA** tiene integrado la lógica de **ROCÍO**. De este modo, se podrán hacer comprobaciones de manera centralizada y automatizada.

¿Por qué EMMA?

A través de la visibilidad, control / respuesta y cumplimiento que aporta **EMMA**, se puede disminuir el riesgo y el impacto de los ataques disruptivos y responder ante requisitos de regulaciones. Al tratarse de una solución centralizada, se reducen los esfuerzos de gestión y tiempos de respuesta.

Cada módulo está orientado a una función determinada que se adaptará a las necesidades específicas de las organizaciones.

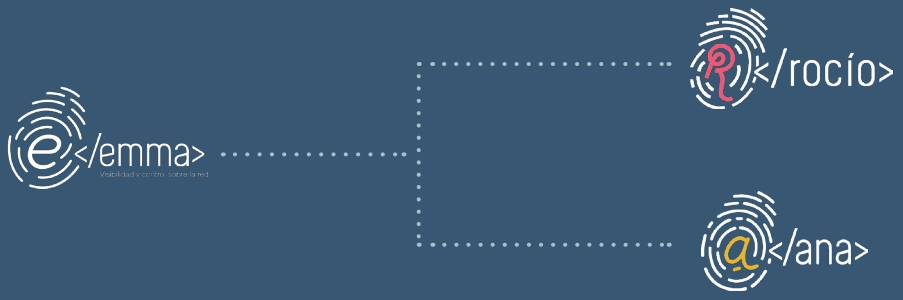
La modularidad de **EMMA** permite obtener mayor valor de la solución en menor tiempo, permite también centralizar esfuerzos y focalizar objetivos durante su implantación.

Las organizaciones pueden elegir aquellos módulos que sean de mayor interés para su situación actual. **EMMA** se puede adquirir e implementar por módulos funcionales, desplegando sólo las funcionalidades que se adapten a la necesidad de la organización, de esta manera se reducen riesgos e impactos operacionales durante el proceso de implementación y su despliegue ocurre de manera muy ágil.

EMMA tiene un diseño compuesto por 7 módulos: Visibilidad, Control y Respuesta, Segmentación, Cumplimiento, BYOD, Gestión de invitados y **EMMA**-VAR (Vigilancia en Accesos Remotos).

Soluciones del ecosistema

Además de los módulos mencionados, **EMMA** se integrará con soluciones del ecosistema CCN-CERT. Concretamente con las siguientes soluciones: Rocío y Ana.



Es una herramienta de auditoría de cumplimiento con el ENS/STIC en dispositivos de red.

Es un sistema de auditoría continúa desarrollado por el CCN-CERT que tiene por objetivo incrementar la capacidad de vigilancia y conocer la superficie de exposición.

Características

- **Adaptable** a la electrónica de red de distintos fabricantes y versiones (multi-fabricante y multi-versión)
- **Flexible:** Puede usar distintos mecanismos de visibilidad y control de dispositivos: 802.1x, SNMP Traps, Port Span, SFlow, Netflow, DHCP, Tablas MAC, con o sin agente, etc. EMMA puede integrarse con el Directorio Activo (AD), Protocolo Ligero de Acceso a Directorios (LDAP), Doble Factor de Autenticación y otras soluciones (NGFW, MDMs, SIEMs).
- **Centraliza las políticas:** Establece un punto central para la definición y ejecución de políticas de control de acceso / respuesta a la red para usuarios y dispositivos.
- **Analítica:** La CMDB de EMMA almacena una serie de datos de interés de todos los activos conectados en la red, sus características, eventos otráfico asociado, entre otros.. Por tanto, toda esa información puede ser mostrada de forma gráfica en tiempo real, agilizando las tareas de reporting permitiendo así obtener informes, así como integrarse con otras soluciones del CCN-CERT como ROCÍO.

¿Cómo funciona EMMA?

La instalación de **EMMA** requiere dos máquinas virtuales (Core y Analytics) y opcionalmente una tercera (Sensor / Concentrador de VPNs, en el caso de **EMMA**-VAR). Salvo por el módulo **EMMA**-VAR, el Sensor es complementario y aporta una mayor visión del comportamiento de la red recogiendo metadatos sobre la comunicación generada por cada activo y dispositivo.

Core

- Motor de políticas
- CMDB
- Portal de administración

Analytics

- Motor de búsqueda
- Dashboards
- Informes

Sensor

- Decodificación de protocolos
- Comportamiento de red
- Port span / on-premise

Sensor + Concentrador VPN

- Decodificación de protocolos
- Comportamiento de red
- Port span / on-premise
- Concentrador de VPNs (módulo EMMA-VAR)

Módulo de EMMA Visibilidad: Descubrir y perfilar todos los activos del organismo.

- Inventariado continuo de dispositivos, infraestructura y usuarios en una **CMDB** centralizado
- Etiquetado de activos críticos por contexto de la organización y riesgos de seguridad
- La **CMDB** entendible permite incorporar otros atributos de la organización al nivel del activo y dispositivo (nivel de criticidad y riesgo)

Módulo de EMMA Control / respuesta: Control del acceso a la red, respuesta ante ataques.

- Punto único de definición y aplicación de políticas de acceso y de respuesta.
- Establecer controles de acceso a los dispositivos en función de su contexto y lógica de la organización.
- Autenticación de uno o dos factores (Directorio Activo (AD), Protocolo Ligero de Acceso a Directorios (LDAP), Doble Factor de Autenticación (2FA mediante OTP, Mobile Connect)
- Integración y adaptabilidad con otras soluciones de seguridad NGFW, SIEM, MDMs

Modulo Segmentación: Reducir la superficie de exposición.

- Aplicación de segmentación dinámicamente para reducir la superficie de exposición
- Aplicación de microsegmentación / ACLS a capa 3-4

Módulo Cumplimiento: Garantizar el cumplimiento de las políticas de seguridad del organismo y del CCN-CERT.

- Electrónica de red:
  - Centraliza y automatiza la comprobación de las configuraciones actuales de la electrónica de las organizaciones contra los estándares definidos en **Rocío**.

Módulo EMMA BYOD: Mitigar el riesgo de acceso de dispositivos BYOD.

- Controla el acceso en función del riesgo adicional y realiza un seguimiento de los accesos de equipos **BYOD.**
- Implementa el uso de una identidad corporativa única para **BYOD.**

Módulo EMMA Gestión de invitados: Facilita la gestión y mitiga el riesgo de los invitados.

- Punto único de definición y aplicación de políticas de acceso y de respuesta.
- Establecer controles de acceso a los dispositivos en función de su contexto y lógica de la organización.
- Autenticación de uno o dos factores (Directorio Activo (AD), Protocolo Ligero de Acceso a Directorios (LDAP), Doble Factor de Autenticación (2FA mediante OTP, Mobile Connect)
- Integración y adaptabilidad con otras soluciones de seguridad NGFW, SIEM, MDMs

Módulo EMMA Vigilancia en Accesos Remotos: Establece una conexión **segura** y **verificada** entre el usuario y los sistemas corporativos.

- Permite, deniega o limita el acceso en función de la postura de seguridad del endpoint y el rol del usuario del organismo
- Verificación doble de identidad (AD, LDAP + OTP)
- Establece una conexión **segura vía canal VPN**
- **Monitoriza** de manera continua el comportamiento de la conexión

emma@ccn-cert.cni.es
www.ccn-cert.cni.es