proactivanet

High Performer Mid-Market SPRING 2024 · High Performer Latin America SPRING 2024 · High Performer SPRING 2024 · Gartner Peer Insights Customers' Choice 2024

HOJA DE PRODUCTO

Proactivanet CyberITAM

En un mundo totalmente digitalizado, donde las organizaciones dependen casi totalmente de los servicios e infraestructura TI, la **ciberseguridad se ha vuelto esencial** ya no solo **para proteger los datos**, sino también **para proteger la reputación y la continuidad del negocio.** Las ciber amenazas evolucionan constantemente, y los ataques suelen tener un impacto devastador, no solo financiero, sino también reputacional, lo cual mina la confianza de los clientes y la continuidad de la organización.

Por ello, implementar medidas de ciberseguridad proactivas y efectivas ya no es solo una opción, sino una necesidad para las empresas que buscan minimizar riesgos en un entorno cada vez más vulnerable.

En este sentido, la **integración de las prácticas de ciberseguridad y de gestión de activos de TI (ITAM) en una sola plataforma**, es clave para garantizar una **protección efectiva e integral de toda la infraestructura TI** corporativa. Al tener una **visibilidad completa y actualizada** de todos los activos de TI, desde cualquier dispositivo hardware hasta software, sin olvidar los servicios en la nube, el equipo de seguridad puede **identificar posibles vulnerabilidades y gestionar las amenazas de forma proactiva.** Esta visibilidad ayuda a identificar dispositivos sin parches, software de terceros desactualizado o configuraciones incorrectas, que de otra manera podrían pasar desapercibidas y convertirse en puntos de acceso para los atacantes.

Al contar con un **enfoque unificado**, las organizaciones pueden **responder de manera más rápida y eficiente ante incidentes**, reduciendo la complejidad y los costos asociados con la gestión de múltiples herramientas de seguridad y TI. Una plataforma integrada también permite a los equipos de seguridad y TI trabajar de forma colaborativa, alineando la administración de activos y las políticas de seguridad en función de las necesidades estratégicas de la organización, reduciendo significativamente el riesgo de brechas de seguridad. En definitiva, contar con una única fuente de verdad que consolide la información estratégica relacionada con la ciberseguridad y que tanto el CISO como el CIO puedan tomar decisiones informadas.

You are not doing cybersecurity if you are not doing ITAM

> El coste de los ciberataques para las empresas españolas **aumentó un 43% en 2022** frente al año anterior[...] las corporaciones con más de 1.000 empleados han visto un aumento del **coste medio** por esta problemática del 34%, hasta los **333.939 euros.**
>
> EuropaPress

INCLUYE:

- INTEGRACIÓN NATIVA CON ITAM Y CMDB
- INTEGRACIÓN NATIVA CON SERVICE DESK
- DETECCIÓN DE INTRUSOS EN TIEMPO REAL
- DETECCIÓN DE CAMBIOS RELEVANTES EN LAS COMUNICACIONES
- WINDOWS UPDATE Y ACTUALIZACIONES PENDIENTES DE SW
- DASHBOARDS ESPECÍFICOS DE CIBERSEGURIDAD EN TIEMPO REAL
- EVIDENCIAS PARA AUDITORÍAS DE CONTROL NORMATIVO (ENS, NIS2, DORA,...)
- BASE DE DATOS DE VULNERABILIDADES CENTRALIZADA (NVD, MITRE,...)
- DESPLIEGUE DE PARCHES Y ACTUALIZACIONES DE SW AUTOMÁTICA
- RELACIÓN INTELIGENTE ENTRE VULNERABILIDADES Y ACTIVOS
- GESTIÓN DE RIESGOS BASADO EN MAGERIT
- NOTIFICACIONES EN TIEMPO REAL MULTICANAL (WHATSAPP, MS TEAMS, TELEGRAM, SMS, EMAIL, ...).
- API REST Y WEBHOOKS PARA INTEGRACIÓN CON SIEMS, SOCS,...

ens Esquema Nacional de Seguridad · NIS2 · DORA · ISO 27000

Funcionalidades clave de este módulo

	STANDARD	ADVANCED	PREMIUM
Detección y notificación de intrusos en tiempo real			
Detección subredes	✓	✓	✓
Detección de intrusos en tiempo real	✓	✓	✓
Análisis patrones de comunicación	✗	✗	✓

Detección en tiempo real de las redes a las que se conectan los equipos corporativos, evidenciando el uso de redes corporativas, o redes "externas" sobre las que no se tiene detalle sobre su seguridad. Adicionalmente, para las redes corporativas se podrá activar la detección y notificación de intrusos en tiempo real o diferidas (WhatsApp, MS Teams, SMS, email) cuando se detecten equipos no inventariados.

Windows Update			
Detección y listado de parches Windows pendientes de desplegar	✓	✓	✓
Actualización automática parches Windows Update	✗	✓	✓

Detección de los parches pendientes de aplicar en cada equipo Windows, con visión global (dado un parche, dónde falta aplicarlo) o individual (dado un equipo, qué parches tiene pendientes de aplicar), con opción a desplegarlos de manera automática y desatendida. Dashboard para visualizar el estado actual, parches con más actualizaciones pendientes, parches más críticos pendientes de desplegar, ...

Actualización SW de terceros Windows			
Detección de SW pendiente de actualizar	✗	✓	✓
Actualización automática SW Windows pendiente de actualizar	✗	✗	✓

Detección de las actualizaciones pendientes para aplicaciones de terceros ejecutándose en plataforma Windows (software de Adobe, Audodesk, compresores, herramientas ofimáticas, herramientas colaborativas, ...). La modalidad Premium podrá además lanzar las propias actualizaciones pendientes de manera automática y desatendida. Dashboard para el control automático del estado de parcheado del parque.

Controles para el seguimiento de la ciberseguridad			
Estado despliegue antivirus & antispyware	Solo Win Cliente	✓	✓
Estado despliegue firewall	Solo Win Cliente	✓	✓
Estado despliegue VPNs	✗	✓	✓
Estado encriptación HD (bitlocker)	✗	✓	✓
Estado despliegue herramientas control remoto	✗	✗	✓
Estado despliegue otro SW configurable	✗	✗	✓
Evolución histórica del estado de ciberseguridad	✗	✗	✓
Listados para el cumplimiento ENS, NIS2, DORA	✗	✗	✓

Detección de otros aspectos clave de ciberseguridad como el estado del antivirus, antispyware, firewall, encriptación de HDs, herramientas de control remoto, conectividad VPN, ... La versión Standard ofrecerá unas capacidades básicas sobre estos aspectos que serán más completas y multiplataforma en los niveles Premium y Advance. Los niveles superiores de CyberITAM aportan más información sobre el ciclo de vida del SO y su obsolescencia, explotación de datos gráfica sobre el estado y evolución en tiempo real, generación de evidencias para el cumplimiento de ENS, NIS2, DORA, ...

Funcionalidades clave de este módulo

	STANDARD	ADVANCED	PREMIUM
Integración con CMDB e ITSM			

Permite la integración de CyberITAM de manera nativa con el resto de los procesos de Service Desk y CMDB, permitiendo la creación automática de incidencias ante alertas de ciberseguridad y/o la visualización de dichas alertas directamente en los gráficos de la CMDB.

Creación de tickets automáticos ante alertas de ciberseguridad	✓	✓	✓
Alertas de ciberseguridad en CMDB	✗	✓	✓

Gestión de Vulnerabilidades			

Base de datos de vulnerabilidades centralizada y siempre actualizada (Incibe, MITRE, NVD, ...), relacionando automáticamente cada vulnerabilidad con los activos del inventario, eliminando falsos positivos gracias al uso de AISecOps de manera integrada.

BD vulnerabilidades	✗	✓	✓
Detección automática de remediaciones	✗	✗	✓

Gestión de Riesgos			

Facilita la implementación de un proceso de Gestión de Riesgos siguiendo la metodología Magerit, acorde a los requerimientos establecidos por el ENS, NIS2, DORA,... de manera totalmente integrada con el Inventario, CMDB y resto de procesos del Service Desk.

Gestión de riesgos según metodología Magerit para ENS, NIS2, DORA	✗	✗	✓

Alertas y notificaciones multicanal en tiempo real			

Sistema de notificaciones configurable, tanto en tiempo real como en diferido (por ejemplo, resúmenes diarios/semanales), utilizando distintos canales de comunicación en función de la criticidad de la notificación (SMS, WhatsApp, MS Teams, Email, Telegram, ...).

Alertas por email	✓	✓	✓
Alertas avanzadas (SMS, WhatsApp, MS Teams, ...)	✗	✓	✓

API e integraciones			

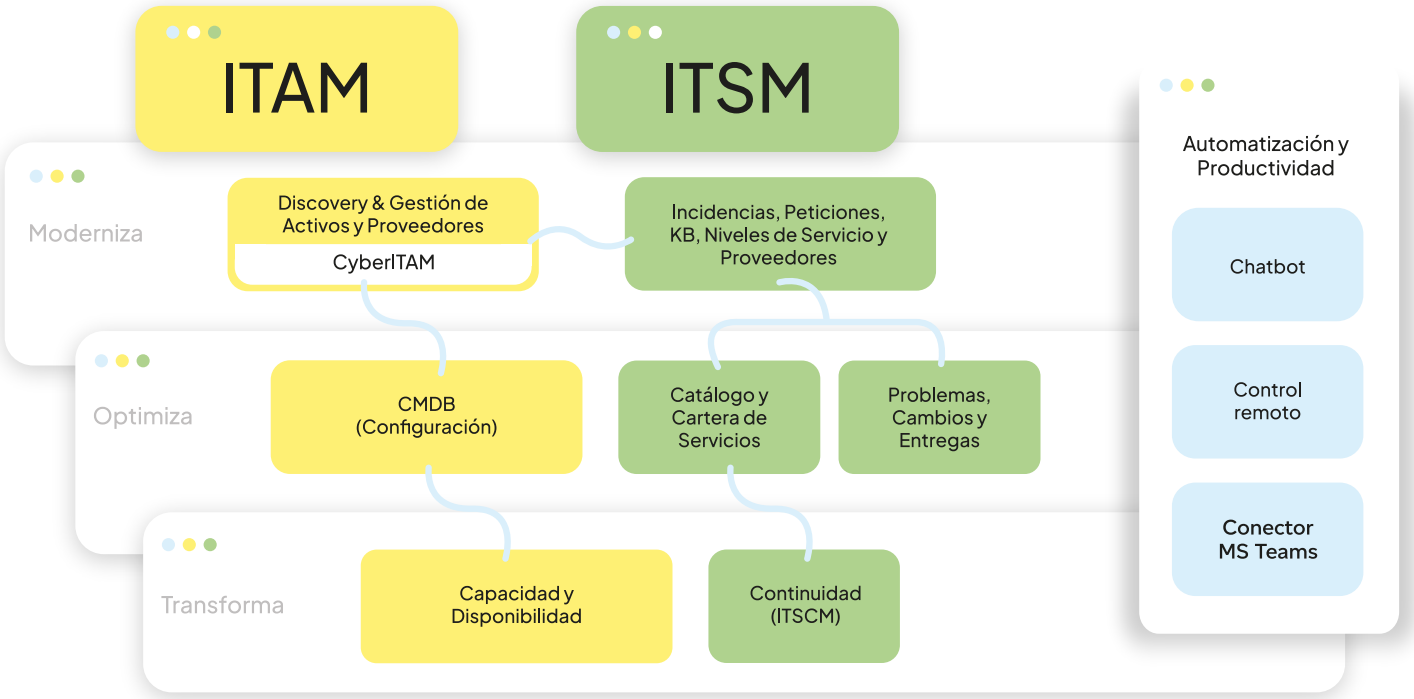
Integraciones bidireccionales con sistemas de 3os vía API REST, así como notificación de eventos en tiempo real a SOCs / SIEMs (avisar al SOC de inmediato cuando se detecte un equipo desconocido en determinada subred, o avisar al SIEM cuando se pare un firewall en un equipo, ...).

Integración escáneres de vulnerabilidades externas	✗	✗	✓
API REST	✓	✓	✓
Webhooks seguridad en tiempo real	✗	✓	✓

proactivanet — Proactivanet CyberITAM

Mapa de Soluciones & Ficha Técnica

NOV 2024



FICHA TÉCNICA	
NOMBRE DEL MÓDULO	**CyberITAM**
DEPENDENCIAS CON OTROS MÓDULOS	Discovery & Gestión de Activos.
MODALIDADES DE CONTRATACIÓN	• **Licencia Perpetua OnPremise.** • **Alquiler Anual OnPremise** (incluye soporte y suscripción de versiones). • **Servicio Saas** (incluye soporte y suscripción de versiones).
FORMA DE LICENCIAMIENTO	El módulo se licencia en función del número de activos con Sistema Operativo que se vayan a inventariar de manera automática **(PCs, Servidores.** Otros dispositivos con IP tales como routers, impresoras, etc., así como los activos dados de alta de manera automática, no consumen licencia.
NIVELES DE LICENCIAMIENTO	• **Standard** • **Advanced** • **Premium**

PinkVERIFY® Certified 16 PROCESSES

PinkVERIFY es una marca registrada por Pink Elephant.

PeopleCert ITIL®4 ACCREDITED TOOL VENDOR BRONZE Proactivanet v10