Secure&IT by LKS Next

www.secureit.es

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad Categoría MEDIA RD 3/2010

CERT

Calidad Certificada ISO 9001:2015 Certificate Nº:57146

Seguridad Certificada ISO/IEC 27001:2013 Certificate Nº:48038

# Servicio de Vigilancia de la Ciberseguridad

**Francisco Valencia**
Director General
658 457 524 - francisco.valencia@secureit.es

Secure & IT by LKS Next

www.secureit.es

# ¿Falsa sensación de seguridad?

# Situación actual

- Movimientos sociales e inestabilidad política dan como resultado organizaciones de **hacktivismo**, **ciberdelincuencia**, **ciberterrorismo**, **ciberespionaje** y **ciberguerra**.
- Existen muchos intereses que tratan de desestabilizar el modelo económico occidental, con especial foco en las economías americana y europea
- El numero de ataques se ha incrementado en un **50% en 2020** con respecto a 2019, sumando más de **250.000 impactos graves en todo el Estado**
- España es ya el **tercer país mas ciberatacado** del mundo, aunque es el séptimo en protección.
- La situación causada por COVID-19 ha provocado un fuerte incremento en algunas de estas amenazas
- Ataques con mayor crecimiento:
  - **Ataques OT/IoT** -> Automoción, Medicina, Industria, Smart Cities, Infraestructuras, etc…
  - **Ransomware** -> El trío Emotet / Trickbot / Tyuk ha crecido enormemente, causando gravísimos impactos en empresas de todos los tamaños y sectores.
  - **Fraude al CEO** -> Ha perdido impactos pero sigue siendo una gran amenaza, con pagos ilícitos que alcanzan millones de euros
  - **Robo de credenciales y phishing** -> Especialmente a sistemas de correo cloud y redes sociales. Empleados para posteriores ataques
  - **Ataques a dispositivos móviles** -> Desde aplicaciones malintencionadas hasta puntos de acceso WIFI inseguros
  - **Robo de información con chantaje** -> Afecta a empresas, particulares, menores..

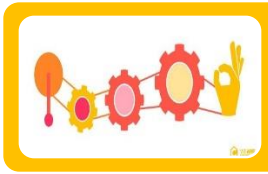
# Impacto y Responsabilidad

**ECONÓMICA**

- **Pérdidas económicas inmediatas o indirectas. De difícil cuantificación**

**REPUTACIONAL**

- **Prestigio y Confianza del entorno se ven gravemente afectados**



**OPERATIVA**

- **Producción, logística, y otros procesos pueden verse afectados**

**SOBRE LAS PERSONAS**

- **Exposición de datos, pérdida de trabajo, salud…**

**SOBRE EL CUMPLIMIENTO**

- **Responsabilidad civil o penal por incumplimiento del deber de aplicar medidas preventivas – Código de Derecho de la Ciberseguridad**

**SOBRE LA ESTRATEGIA**

- **Imposibilidad de cumplir objetivos estratégicos. Incluso riesgo de continuidad de negocio.**

**La empresa NO ES LA UNICA AFECTADA**

Es **irresponsable y poco ético** no aplicar medidas cuando se pueden ver afectados, además:

& Proveedores
& Clientes
& Socios
& Empleados
& Candidatos
& Ciudadanos
& Usuarios
& Etc..

Por eso existe regulación sectorial, industrial, jurídica y de buenas practicas. Para ayudar a la empresa a ser **RESPONSABLE**

# Acerca de Secure&IT

MONDRAGON HUMANITY AT WORK — Finance Industry Retail Knowledge

Empresa creada en 2009 por Abogados expertos en Derecho de las TIC, Ingenieros y Expertos en Seguridad de la Información.

Misión: Ayudar a las empresas a disminuir los riesgos a que se exponen a causa de la gestión de su información.

Líderes en auditoría e implantación de modelos avanzados de gestión de la ciberseguridad y el cumplimiento normativo

Trofeos de la Seguridad TIC — Mejor Empresa de Seguridad TIC

Equipo altamente cualificado, gran parte de la inversión destinada a formación.

Seguridad 360º para la información de su empresa:

Procesos Corporativos
Seguridad Informática
Cumplimiento Normativo
Ciberseguridad Industrial

Secure&View©. Dos centros de Seguridad SOC de control y supervisión 24x7x365 Madrid – Guipùzcoa

**ISO27001 / ISO9001 / CERT / ENS**

# Nuestros Servicios. Seguridad 360º


- & Protección de Datos - GDPR
- & Propiedad Intelectual
- & Comercio Electrónico
- & Telecomunicaciones
- & Firma Electrónica
- & Contratos TIC
- & Arbitraje y Mediación
- & Prevención del Delito
- & PCI-DSS
- & Esquema Nacional ENS
- & Peritajes Judiciales

- & Auditoría de Seguridad
- & Hacking Ético
- & Consultoría Seguridad
- & Diseño de redes seguras
- & Planes Directores
- & Análisis de Riesgos
- & Procesos corporativos
- & Planes de Continuidad
- & Formación. SecureAcademy
- & IEC 62443 / SGCI
- & ISO 27001 / SGSI
- & ISO 22301 / SGCN
- & ISO 20000 / SGSTI

- & SOC-CERT
- & 24 X 7 X 365
- & Monitorización
- & SIEM – Alertas
- & Respuesta rápida
- & Operación ISO 27001
- & Control de Políticas
- & Copias de Seguridad
- & Seguridad CLOUD
- & Sandboxing

- & Redes y Comunicaciones
- & Granjas de servidores
- & Firewalls UTM/NGFW
- & DNS Firewall
- & Anti DDOS
- & Web Firewall, WAF
- & Seguridad de Puesto/MDM
- & Seguridad Correo
- & Seguridad Bases de Datos
- & NAC
- & PKI, Identidad Digital
- & CASB
- & DLP/IRM
- & Sistemas industriales

# Servicio de vigilancia de la seguridad

- **EDR (Endpoint Detect and Response). Bitdefender EDR o Bitdefender ULTRA**
  - Tecnología que permite identificar amenazas avanzadas de seguridad, allí donde el EndPoint sólo no es capaz. Combina técnicas de IA y Sandboxing
  - Permite la respuesta rápida a eventos sospechosos, bloqueando dispositivos, eliminando procesos, etc. Idealmente el EDR debería estar integrado con el EPP, para automatizar acciones y evitar falsos positivos. Nuestra propuesta es Bitdefender Ultra

- **NTSA (Network Traffic Security Analitycs), BigPROBE**
  - Sonda instalada en la red. Captura todo el tráfico y lo cruza con 160 proveedores de threat intelligence, alertando a BigSIEM
  - Identifica ataques verticales y horizontales que no han sido identificados por las barreras perimetrales

- **Análisis de vulnerabilidades continuo**
  - Sistema que 24x7 busca vulnerabilidades en los sistemas expuestos, alertan cuando se identifica una nueva vulnerabilidad
  - Ideal para localizar vulnerabilidades zero-day que podrían se atacadas

- **BigSIEM**
  - Sistema de correlación de eventos de **Secure&IT**. Basado en BigDATA y una gran potencia de análisis
  - Capaz de ingestar datos de todo tipo de fuentes. Capacidad de orquestación de seguridad

- **SOC de Secure&IT**
  - Dos centros (Madrid-Arrasate), servicio 24x7x365, certificados ISO 27001, ENS, CERT, ISO9001..
  - Equipos de análisis, seguridad defensiva, seguridad ofensiva, ciberseguridad industrial y CSIRT

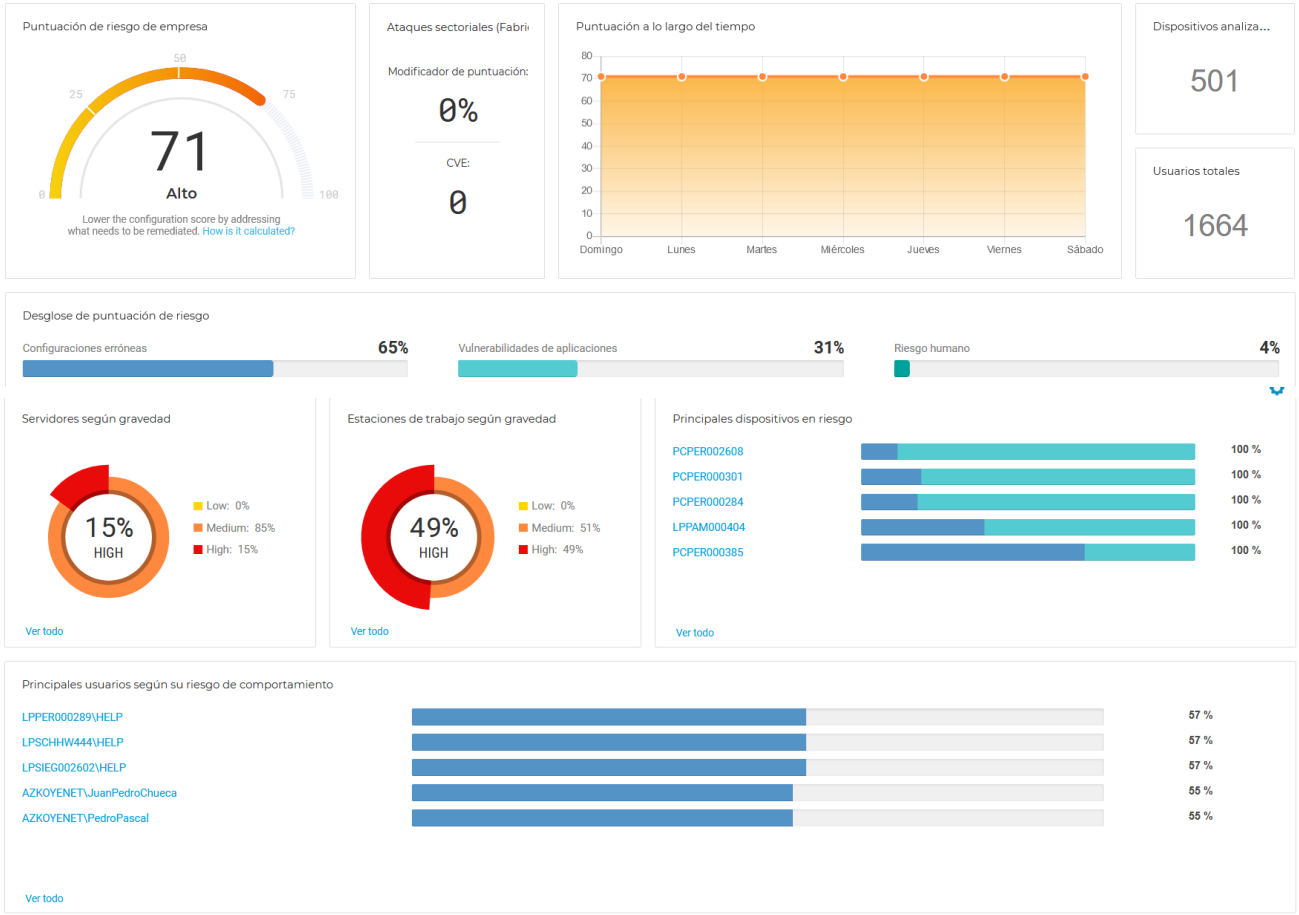
# EPP vs. EDR

**EPP = Endpoint Protection Platform**
**EDR = Endpoint Detection and Response**

| EPP | EDR |
|---|---|
| Mecanismo de defensa de primera línea que contiene amenazas | Supone que ya se ha producido una infracción y ayuda a investigarla y contenerla. |
| No requiere supervisión activa | Utilizado activamente por el personal de seguridad para responder ante incidentes |
| Detección pasiva de amenazas | Detección activa de amenazas |
| No proporciona visibilidad de la actividad en el punto final | Obtiene información de todos los endpoints protegidos y de la red |
| Capaz de prevenir amenazas conocidas y algunas amenazas desconocidas | Permite una protección frente a amenazas que un EPP no puede detectar |
| Centrado en proteger los endpoint de forma aislada | Proporciona datos y contexto para ataques que abarcan uno o múltiples endpoints |

**En resumen, EDR alertará cuando las barreras de seguridad han fallado**
**Necesita monitorización y actuación inmediata por parte de profesionales de seguridad, no actúa solo**
**Si no hay integración con el EPP, el análisis y la respuesta se ven limitadas**

# EDR Bitdefender

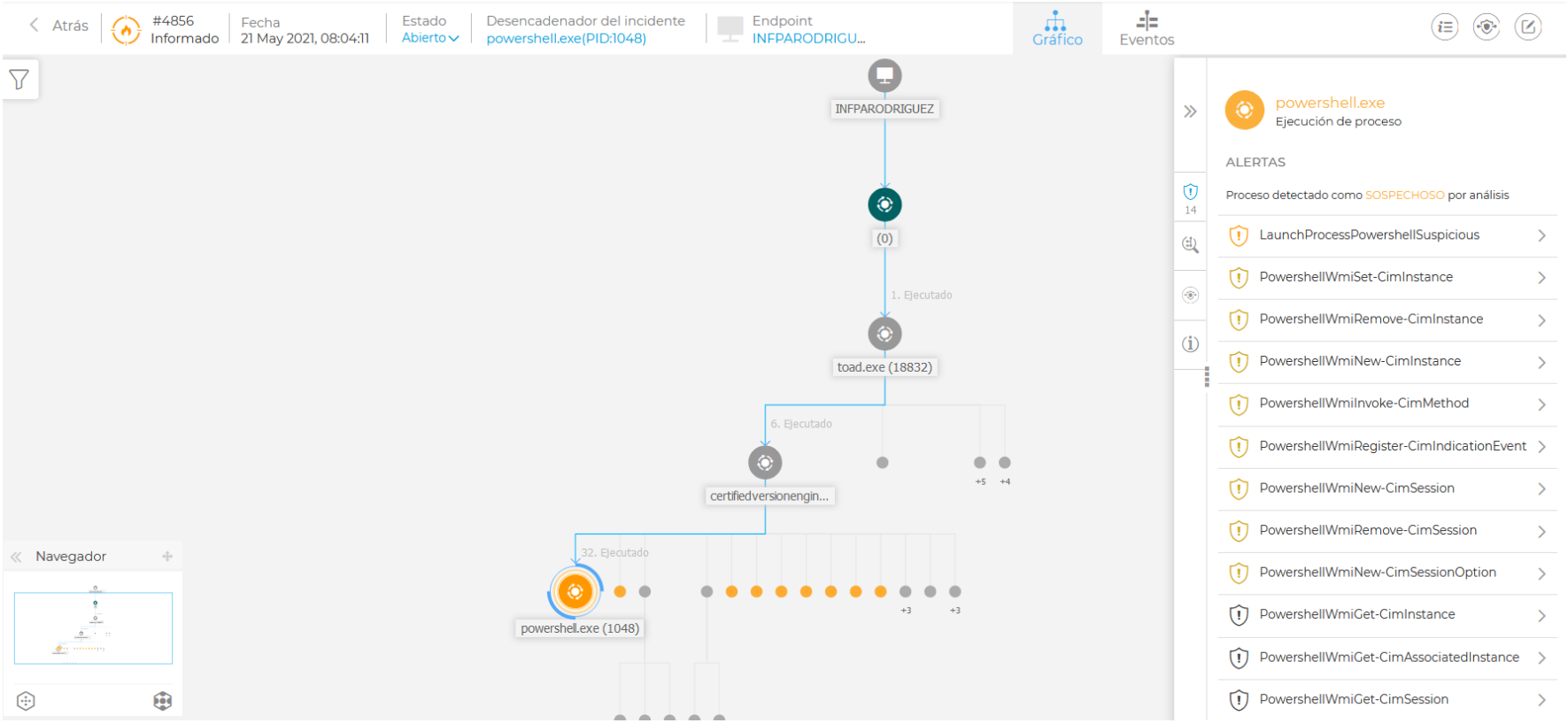



& Dashboards y reportes automáticos con el nivel de riesgo de la organización.

& Si se integra con el EPP, capacidad de mitigación de riesgos mediante gestión de parches y aplicación de configuraciones seguras.

& Al integrarse en el servicio **Secure&View**, los analistas de **Secure&IT** aportarán la mejor solución para la reducción efectiva del riesgo de la empresa

# EDR Bitdefender




& Potente, sencillo y eficaz panel de gestión de incidentes. Gráficamente se puede mover por equipo, proceso y daño causado.

& Desde la propia interface se pueden tomar las acciones correctivas (bloqueo de endpoint, bloqueo de proceso, cuarentena, etc.).

# EDR standalone o EDR+EPP

| CAPACIDADES GALARDONADAS COMO LAS MEJORES EN SU CATEGORÍA | BITDEFENDER EDR | EPP Y EDR GRAVITYZONE ULTRA |
|---|---|---|
| Antimalware | Solo informar | X |
| Prevención y mitigación de ransomware | Solo informar | X |
| Compatibilidad con Windows, Mac y Linux | Solo Windows | X |
| Compatibilidad con endpoints físicos y virtuales | X | X |
| Agente liviano | X | X |
| Consola de administración basada en la nube | X | X |
| Reparación automatizada | | X |
| Control de dispositivos y aplicaciones | | X |
| Control web y cortafuego basados en host | | X |
| Análisis de riesgos de aplicaciones y dispositivos | X | X |
| Análisis de la cadena de ataque | X | X |
| Cifrado de disco completo (complemento) | | X |
| Aplicación de parches contra vulnerabilidades (complemento) | | X |
| Análisis de riesgos por los usuarios | X | X |
| Detección y respuesta para endpoints (EDR) | X | X |

# BigPROBE, NTSA – Seguridad en la red

- **NTSA /Network Trafrfic Security Analytics)** es un concepto que permite registrar y analizar en tiempo real las amenazas de la red. **Secure&IT** ha desarrollado **BigPROBE**: elemento fundamental de cara a la protección de una infraestructura de red.

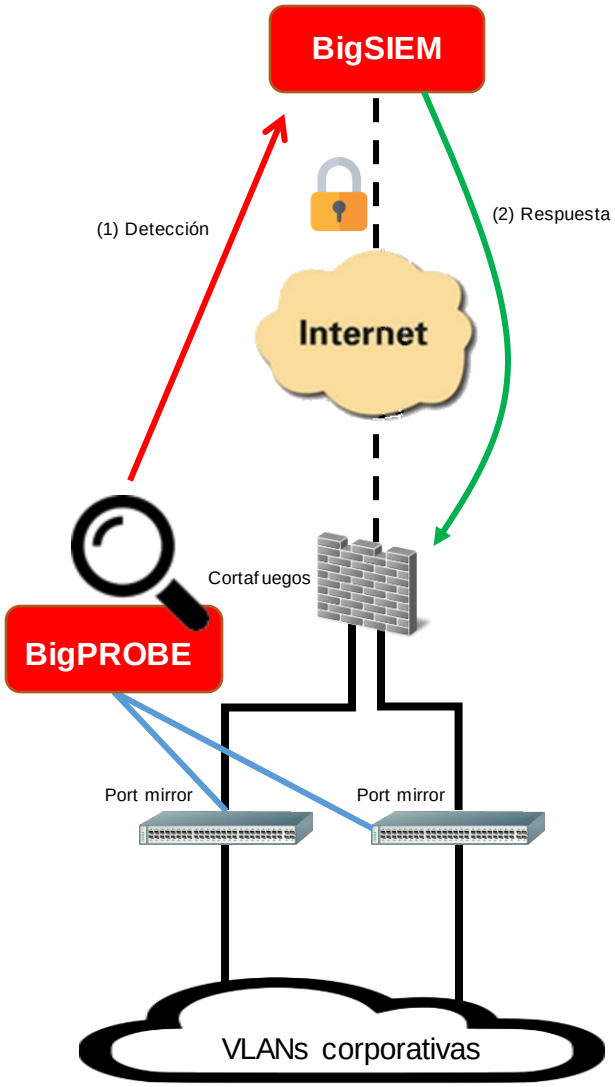
- **BigPROBE** se actualiza diariamente con más de 160 fuentes de inteligencia (theat intelligence) que le aportan información sobre las principales amenazas. **BigPROBE**, cuando identifica tráfico coincidente con una de estas fuentes, reporta a **BigSIEM** parta la toma de decisión y de acción. Además, BigPROBE realiza análisis estático y dinámico.

- Ubicada detrás de los firewalls, en el perímetro interno de la red, y que de modo pasivo (utiliza un(os) puerto(s) mirror en la electrónica de red) es capaz de detectar todo tipo de ataques, tanto verticales como horizontales:

- **Conexiones con atacantes conocidos**
- **Tráfico SPAM**
- **Escaneos**
- **Spiders**
- **Intentos de distribución de malware**
- **Ransomware**
- **Conexiones con Red TOR**
- **Conexiones con proxies**

- **Conexiones a sitios de baja reputación**
- **Conexiones con dominios nuevos o de baja reputación**
- **Peticiones ilegales a DNS**
- **Exploraciones masivas**
- **Atacantes anónimos**
- **Ataques a servicios**
- **Malware**
- **Etc…**

# BigPROBE, NTSA – Seguridad en la red

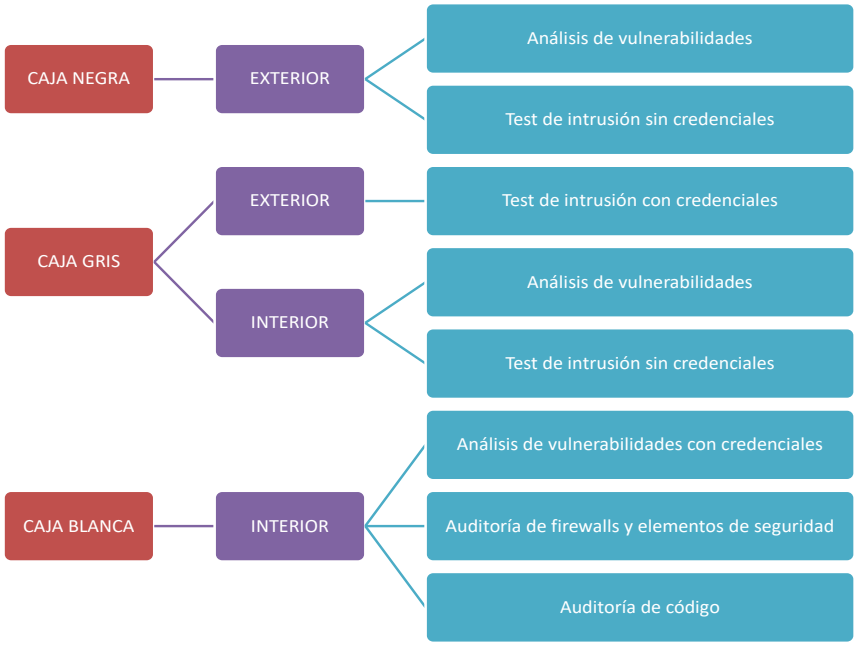


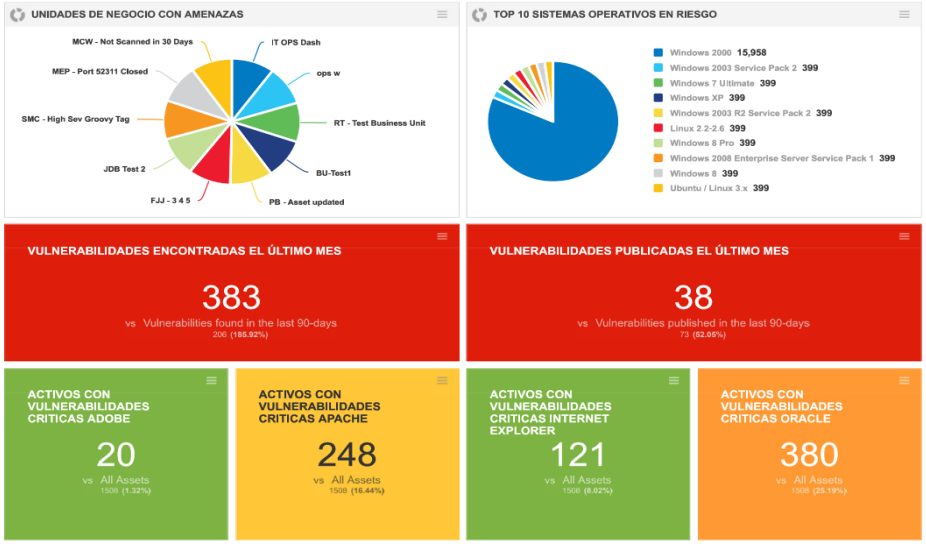

& **DESPLIEGUE: BigPROBE** sólo necesita visibilidad del tráfico, generalmente proporcionado mediante un puerto "mirror" en la electrónica de red (usuarios, servidores, o ambos). **BigPROBE** se instalará detrás de las defensas del existentes. Dispone de versiones hardware y virtuales

& **DETECCIÓN:** La sonda funciona mediante la comparación del tráfico analizado con más de cien fuentes de información (feeds de inteligencia) que **Secure&IT** gestiona y carga en la sonda diariamente (desde fuentes como badips, alienvault, virustotal, sorbs, spiderlabs, snort, suricata, etc..) hasta firmas específicas aportadas a Secure&IT por parte de INCIBE, CCN-CERT u otros CERTs).

& **RESPUESTA: BigSIEM** analiza la información, junto con otra facilitada por los firewalls, para determinar si realmente es un ataque o se trata de un falso positivo. En el caso de que se confirme el ataque, y si una regla en el cortafuegos puede neutralizarlo, **BigSIEM** lo llevará a cabo de forma automática. (Para esta función, el firewall debe estar integrado en **Secure&View**)

# Análisis continuo de vulnerabilidades




- La primera y más importante fase en un servicio de Red Team – Test de intrusión
- Se realiza de manera continua
- Cada nueva vulnerabilidad detectada aparece como una alerta en BigSIEM, incluyendo activo afectado y proceso de subsanación
- Para sistemas externos (Opcionalmente pueden ser internos)
- Permite reducir drásticamente la superficie de ataque de una organización.

Secure&IT by LKS Next

www.secureit.es

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad Categoría MEDIA RD 3/2010

CERT

Calidad Certificada ISO 9001:2015 Certificate Nº:57146

Seguridad Certificada ISO/IEC 27001:2013 Certificate Nº:48038

# ADVANCED-SOC SECURE&VIEW

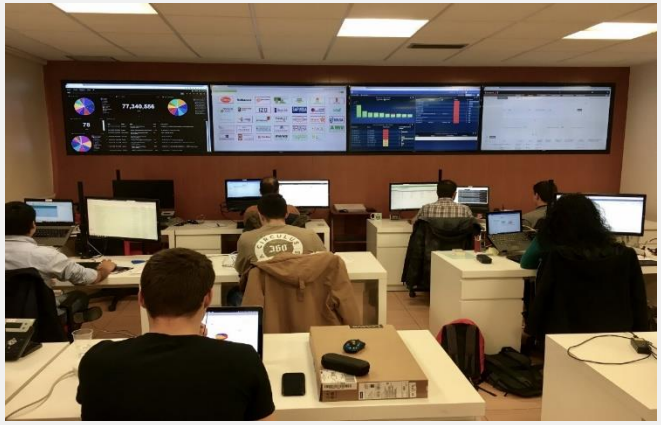
**Francisco Valencia**
Director General
658 457 524 - francisco.valencia@secureit.es

# Secure&View

- **Secure&View© es un servicio que permite que los dispositivos de seguridad sean monitorizados y/o gestionados por personal experto en ciberseguridad, ya estén en dependencias del cliente, en un proveedor o en la nube.**

- **De forma global Secure&View© ofrece tres importantes funcionalidades:**
  - Servicio de **Monitorización**. Vigilancia 24x7 de la seguridad de los dispositivos incluidos en el servicio, que permite reducir los riesgos de seguridad y acelerar la respuesta ante incidentes.
  - Servicio de **Seguridad Gestionada**. Permite externalizar la gestión de la seguridad de los elementos dentro del alcance del contrato. El servicio se presta por un equipo de personas expertos en Seguridad, Sistemas y Telecomunicaciones.
  - **Correlación de eventos de seguridad**: **Secure&View©** está basado en un potente SIEM (Security Information Event Management) que es capaz de identificar incidencias de seguridad, mediante la centralización, análisis y correlación de los logs de seguridad. Los dispositivos y sistemas incluidos dentro del alcance se configuran para que envíen los registros de forma segura **BigSIEM**.

- **Secure&View© se presta mediante el trabajo en equipo de varios tipos de analistas especializados (Seguridad Defensiva, Seguridad Ofensiva, Analistas de Seguridad y Respuesta ante Incidentes), que gestionan la seguridad de los sistemas y monitorizan de forma constante las alertas y las amenazas que se reciben desde los elementos de seguridad cubiertos por el servicio, por ejemplo:**
  - Firewalls (NGFW y UTM)
  - WAF (Web Application Firewall)
  - IDS / IPS
  - Balanceadores
  - Equipos de red
  - Servidores
  - Seguridad en el puesto y EDR
  - Protección de correo electrónico
  - Entornos cloud
  - Etc.



# Necesidad de monitorización avanzada

**CUMPLIMIENTO**

**Satisfacer la demanda que le es exigida a la organización.**

& Exigencias **Legales** (Privacidad…)
& Normas **Sectoriales** (PCI-DSS, ENS, TISAX…)
& **Estándares** (ISO 27001, IEC62443….)
& Medidas dispuestas por **Clientes**

**PROCESOS**

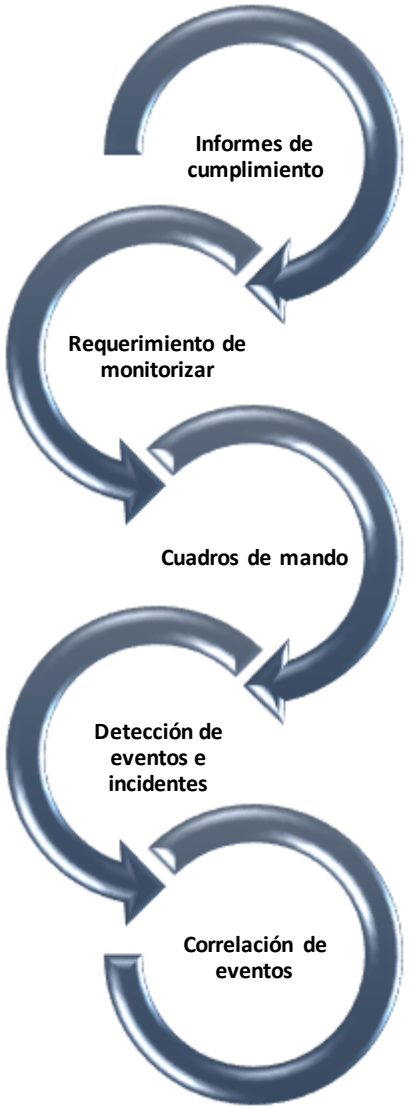
**Permiten dotar al CEO de un "cuadro de mando" de la gestión de su seguridad.**

& Identificación y valoración de **Activos**
& Análisis de **Riesgos**
& Roles y **Responsabilidades**
& **Medidas** aplicadas y sus **Resultados**

**SEGURIDAD TI**

**Protegen las vulnerabilidades propias de los sistemas informáticos:**

& Sistemas anti **malware**
& Protección contra **hackers**
& **Copias** de seguridad
& **Criptografía**



# Requerimientos de cumplimiento

## EXIGENCIA DE REGISTRO

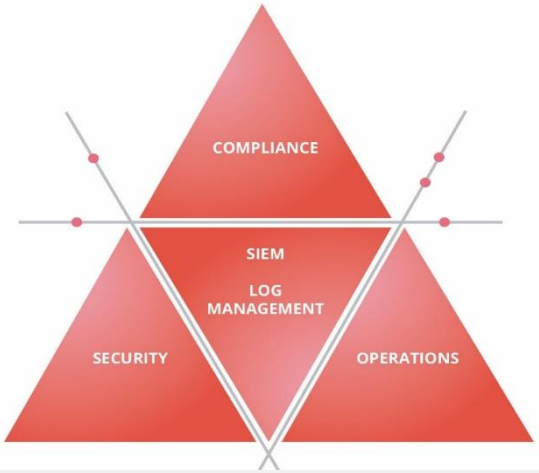
- & LEY 34/02 SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y EL COMERCIO ELECTRONICO (ART. 27)
- & 59/03 FIRMA ELECTRÓNICA (ART. 17)
- & RD 1720/07 PROTECCIÓN DE DATOS (ART. 102)
- & RD 03/10 ESQUEMA NACIONAL DE SEGURIDAD (ART. 24)
- & LEY 10/10 BLANQUEO DE CAPITALES (ART. 25)
- & RD 304/14 BLANQUEO DE CAPITALES (ART. 18)
- & LEY 25/07 CONSERVACIÓN DE DATOS RELATIVOS A COMUNICACIONES ELECTRÓNICAS (ART. 3, ART. 5)
- & PCI-DSS V3.2 (REQ 3.1, REQ 3.6, REQ 8)
- & LEY 26/06 MEDIACIÓN DE SEGUROS (ART. 8)
- & RD 764/10 MEDIACION DE SEGUROS (CAP I, ART. 1)
- & LEY 41/02 AUTONOMIA DEL PACIENTE (ART. 2)
- & FOOD AND DRUGS ADMINISTRATION (ART. 4)

## ADEMAS: MONITORIZACIÓN Y DETECCIÓN DE INCIDENTES

- & GENERAL DATA PROTECTION REGULATION - GDPR (ART 32, ART.33)
- & RD 03/10 ESQUEMA NACIONAL DE SEGURIDAD (ART. 23)
- & LEY ORGÁNICA 10/95 CÓDIGO PENAL (ART. 31BIS)
- & PCI-DSS V3.2 (REQ 5.1, REQ 10.5, REQ 11.1)
- & ISO 27001 (REQ A.12.4)
- & ISO 22301 (REQ 8.4)
- & ISO 20000-1 (REQ 6.6)
- & HIPAA (AP. 164.308)
- & SOX (SECC 404)

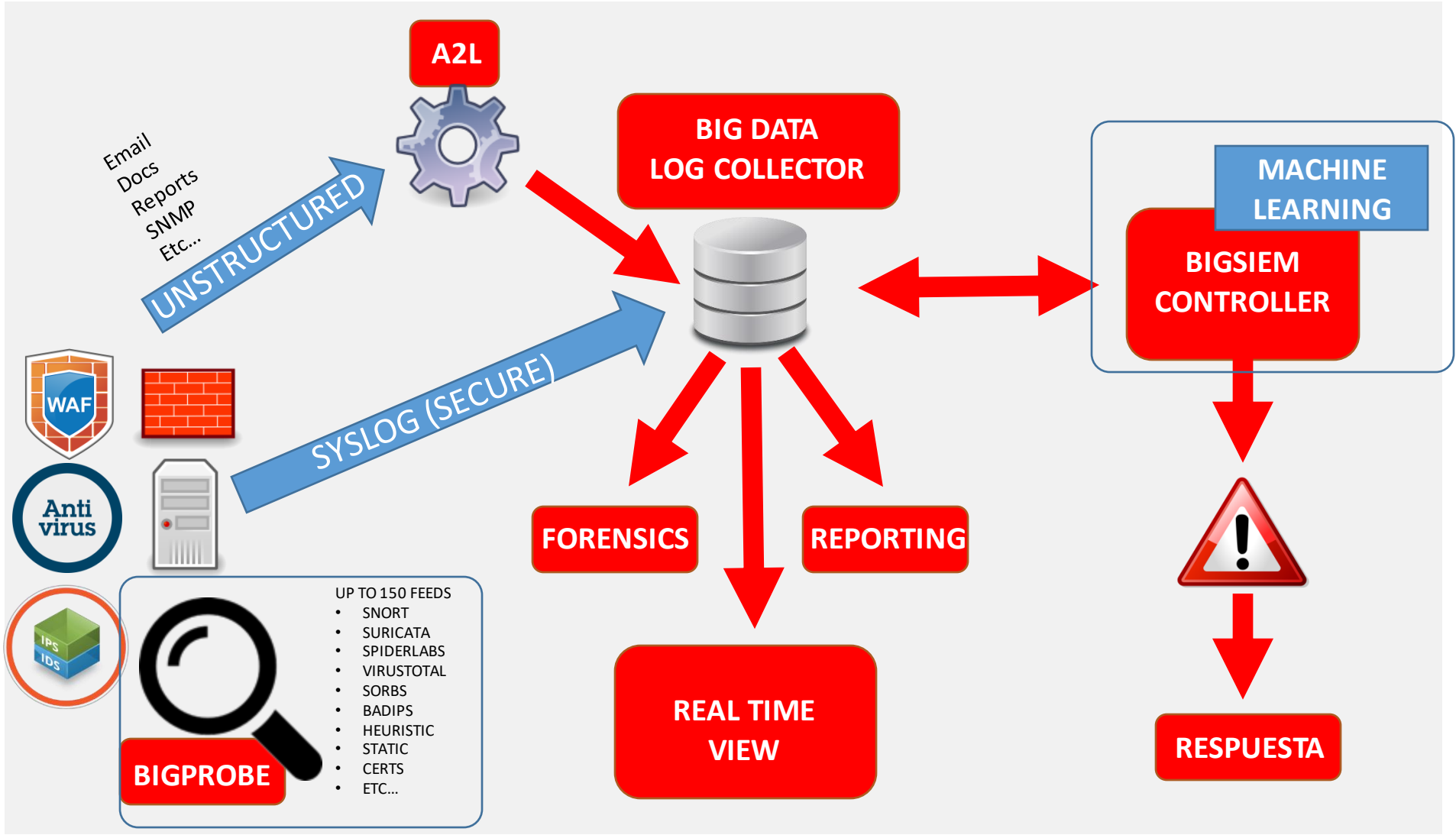
# BigSIEM
# (Security Information Event Management)

- **BigDATA**: clúster de crecimiento dinámico, tanto horizontal como vertical, para el almacenamiento, recolección y análisis de logs y eventos de monitorización.
- **Threat Analyzer**: análisis heurístico y en base a firmas propias y de terceros entre los que se encuentran más de un centenar de proveedores y los más grandes del mercado, alienvault, snort, suricata…
- **Dynamic Malware Analyzer**: SandBox propia e integración con más de 50 proveedores para el análisis de malware, tanto en demanda como de forma automatizada en base a la monitorización definida, con capacidad de analizar la mayoría de las descargas detectadas, siendo un extra sobre las medidas de seguridad del antivirus.
- **Intelligence Engine**: nuestro motor de inteligencia es un desarrollo ad-hoc diseñado por nuestros ingenieros y analistas en inteligencia y seguridad, capaz de realizar correlación de eventos, detección heurística avanzada, monitorización y alerta, aprendiendo del comportamiento de los sistemas de nuestros clientes.

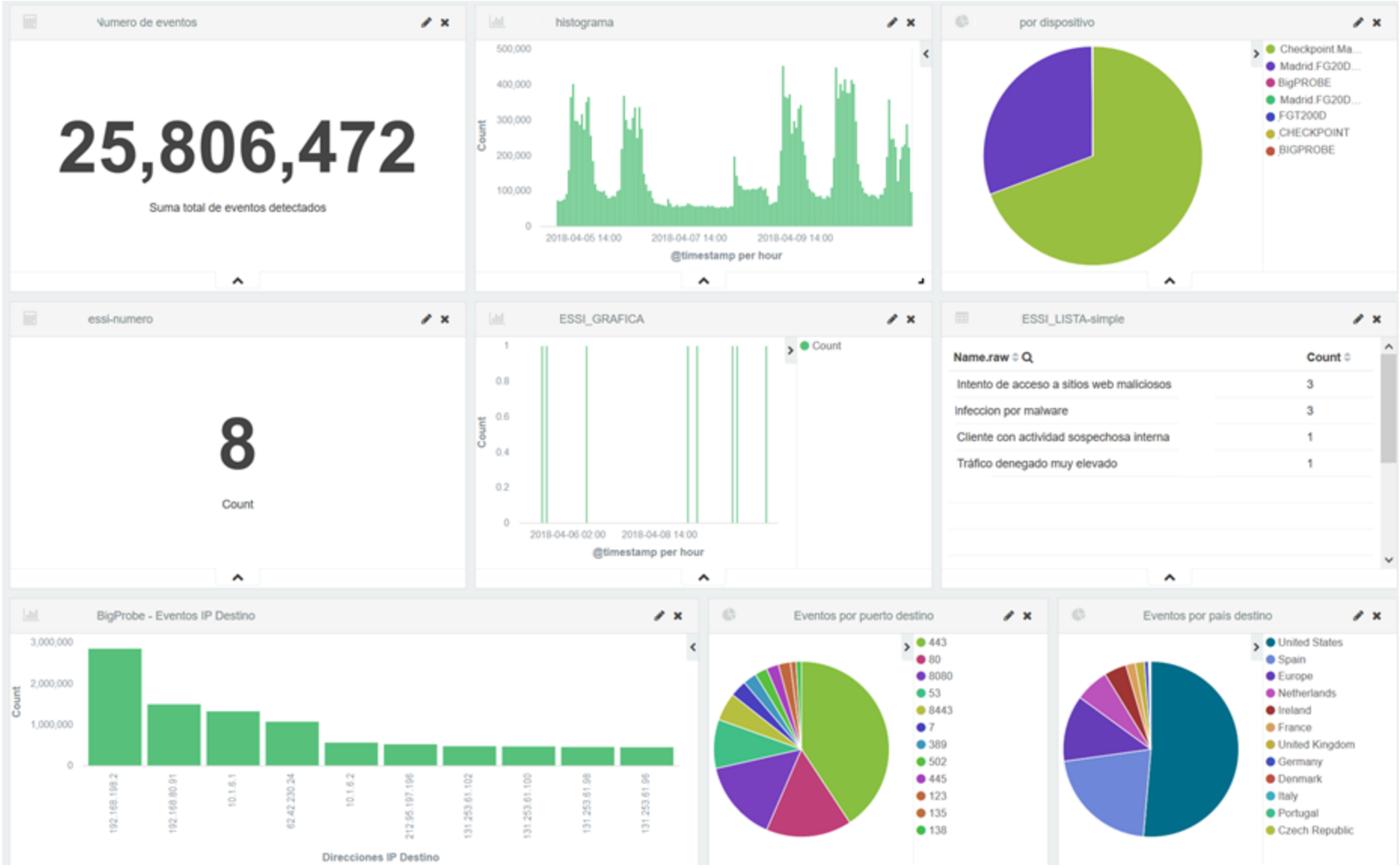



- Análisis en tiempo real
- Almacenamiento y registro de los datos
- Categorización y de los registros
- Inteligencia de negocio
- Alertas y notificaciones
- Herramientas de visualización y control
- Priorización de eventos
- Reporting
- Cumplimiento

# BigSIEM: SIEM SaaS & Emergency Response



# BigSIEM: Capacidad de Análisis



# BigSIEM: Capacidad de Análisis

## & BigSIEM: Más de 1000 variables analizadas

- & Tráfico aceptado y denegado
- & Sesiones
- & Tamaño paquetes
- & Inicios de sesión
- & Login aceptados o bloqueados
- & Malware detectado
- & Correos electrónicos
- & Acceso WEB
- & Ficheros abiertos, copiados, movidos…
- & Etc…

## & Correlación de eventos entre distintos sistemas

- & Firewall
- & DNS firewall
- & Antivirus de perímetro y puesto
- & Sistemas de cifrado
- & Sistemas de copia de seguridad
- & Servidores
- & Control de contenidos, proxys
- & IPS / IDS
- & Correo electrónico
- & Sandbox
- & Etc…

## & Sonda BigPROBE

- & Detección automática de anomalías de tráfico
- & Cruce automático con más de 150 fuentes de inteligencia
- & Redes TOR
- & Malware
- & Reputación IP
- & Reputación dominios
- & Spam
- & Detección automática comportamiento ransomware
- & Análisis horizontal y vertical de tráfico

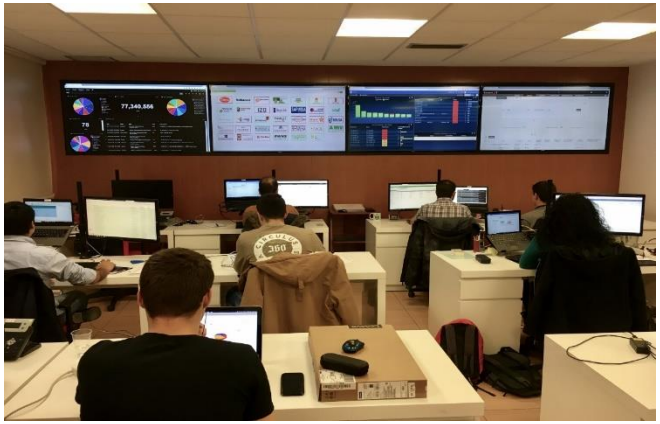
## & Análisis (correlación) cruzada

- & Carga manual de información de ataque
- & Análisis heurístico
- & Seguridad WIFI (AP Rogues, etc.)
- & Correlación entre clientes del CERT
- & Carga de avisos y alertas de CERTS gubernamentales, como CCN-CERT
- & Carga de vulnerabilidades de fabricantes (Microsoft, Cisco, Adobe, etc.)
- & Detección de vulnerabilidades mediante escaneo continuo

# Secure&View©. Capacidad de Respuesta

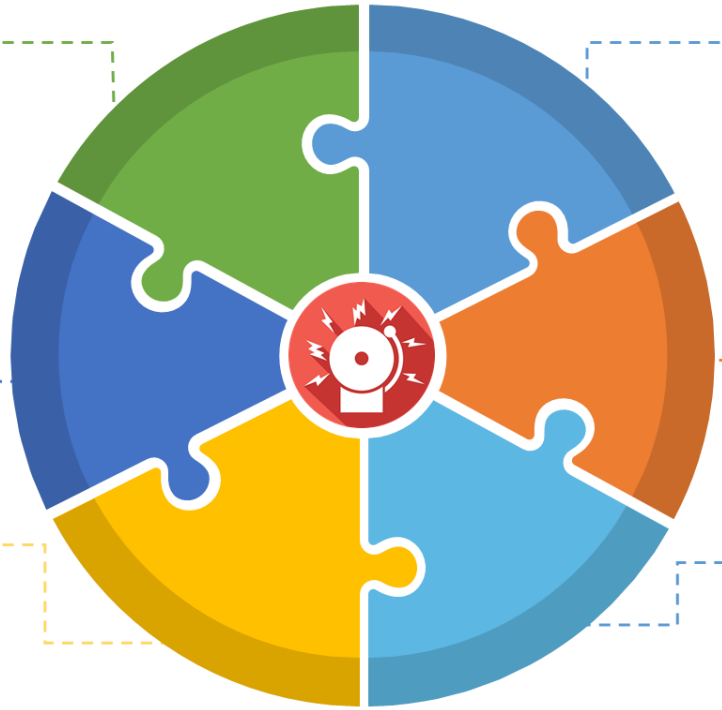
## SERVICIOS

- Alertas de seguridad
- Avisos de vulnerabilidades
- Monitorización
- Gestión de incidencias
- Gestión de vulnerabilidades
- Auditorías
- Test de Intrusión
- Inteligencia y análisis
- Gestión de dispositivos
  - Firewalls
  - WAF
  - Antimalware
  - MDM/MDS
  - DNS Firewall
- Análisis de Riesgos
- Continuidad de Negocio
- Formación
- Consultoría
- Evaluación de productos
- Cumplimiento




- Dos Centros en España con servicio **24x7x365**
- **ISO27001:2013**
- **ISO9001:2015**
- **Esquema Nacional de Seguridad - ENS**
- Acreditado **CERT** (Community Emergency Response Team)
- Equipos de respuesta **CSIRT** a incidentes de seguridad

# Alertas y respuestas BigSIEM



## INFO

Se trata de meros eventos informativos. No revisten impacto sobre la seguridad, pero puede ser interesante conocerlos en ciertas actividades

## AVISO

Evento de seguridad de riesgo medio gestionado por el cliente, que recibirá soporte del SOC si fuera necesario

## CUARENTENA

Evento de seguridad detectado por **BigSIEM** y que se puede detener a través de un bloqueo de tráfico automático

## BAJO

Evento catalogado de riesgo de seguridad bajo, que debido a sus características no require de una respuesta, aunque puede abrirse un ticket para más info o soporte

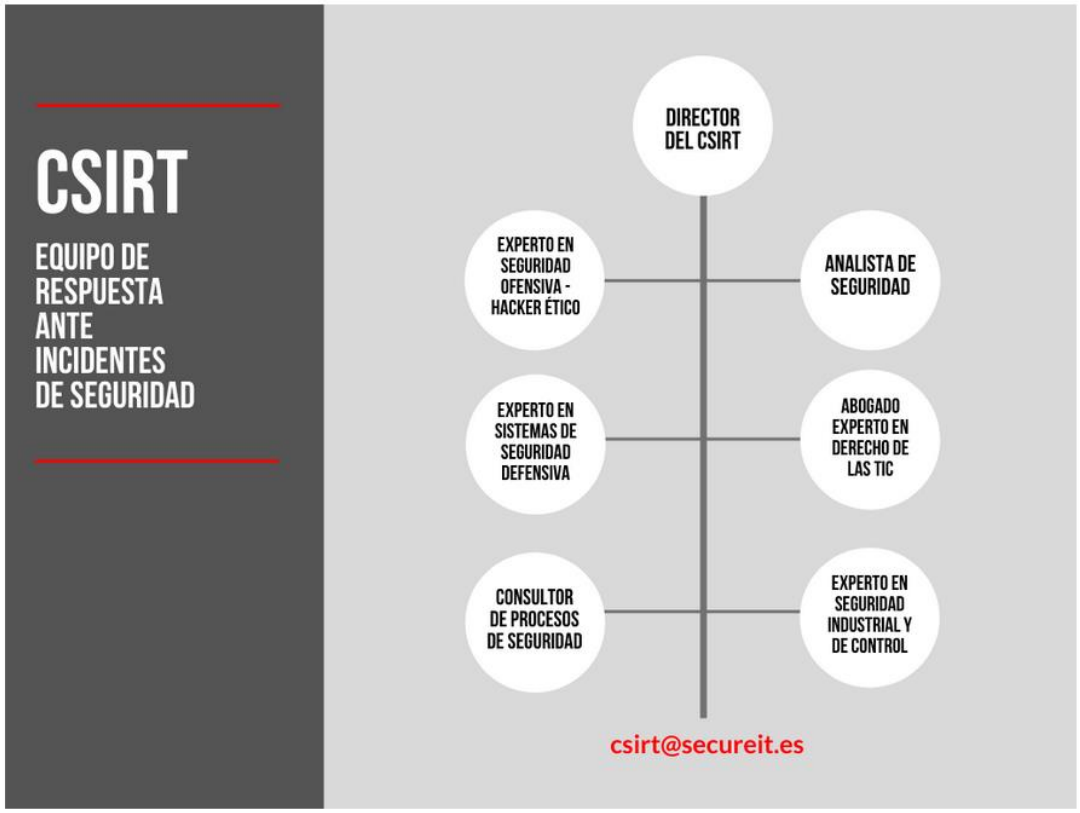
## MEDIO

**BigSIEM** ha detectado una situación de potencial riesgo, pero no tiene toda la información para identificarlo como tal, así que el evento necesita ser analizado por los analistas del SOC. Se abre un ticket en cada caso

## ALTO

Se ha identificado un evento de riesgo alto que require la intervención de los técnicos del SOC. En función de la naturaleza del evento, podría implicarse al equipo del CSIRT

# Respuesta ante eventos de seguridad

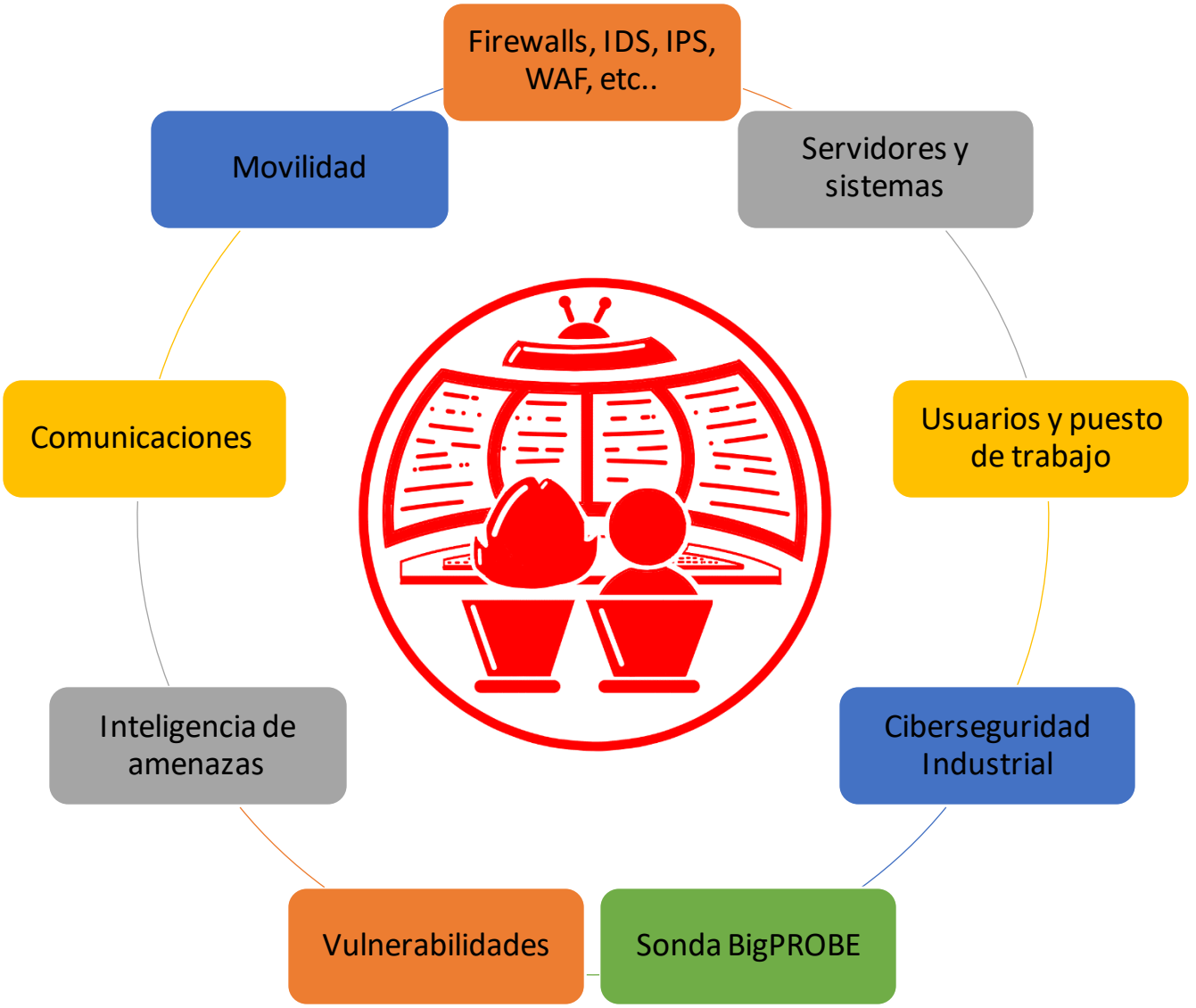




**CSIRT**

- & Respuesta técnica urgente
- & Coordinación para frenar el impacto
- & Coordinación de actividades jurídicas
- & Oficina de atención al afectado
- & Investigación forense
- & Plan de reducción de riesgo futuro
- & Relación con CFSE
- & Notificación de brechas
- & Gestión de seguros
- & Etc.

# Elemento central en la gestión de la ciberseguridad



Secure&IT by LKS Next

www.secureit.es

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad Categoría MEDIA RD 3/2010

CERT

Calidad Certificada ISO 9001:2015 Certificate Nº:57146

Seguridad Certificada ISO/IEC 27001:2013 Certificate Nº:48038

# MUCHAS GRACIAS

Francisco Valencia
Director General
Secure&IT
francisco.valencia@secureit.es
911 196 995