



GAMAKER

ISO 27001

La norma internacional ISO 27000 especifica los requisitos para establecer, implantar, mantener y mejorar un adecuado Sistema de Gestión de la Seguridad de la Información (**SGSI**), y el cumplimiento de normativas y estándares de calidad para los niveles de servicio.



ISO 27001

Pautas para el diseño de un SGSI

Define 14 dominios, 35 objetivos de control y 114 controles.



Herramienta de gestión, permite diseñar, implantar y mantener metodologías y políticas.

Requisitos legales y normativos.

Riesgos físicos y lógicos, objetivos, métricas e indicadores.

Análisis personalizado de las necesidades de la organización

ISO 27001

Dominios de la ISO 27001:

- Políticas de seguridad
- Aspectos organizativos de la SI
- Seguridad ligada a los recursos humanos
- Gestión de activos
- Control de accesos
- Cifrado
- Seguridad física y ambiental



ISO 27001

Dominios de la ISO 27001:

- Seguridad de la operativa
- Seguridad de las comunicaciones
- Adquisición, desarrollo y mantenimiento de los SI
- Relaciones con los suministradores
- Gestión de incidentes en la seguridad de la información
- Aspectos de la seguridad de la información en la gestión de la continuidad de negocio
- Cumplimiento



SGSI

Herramienta de gestión.

Permite diseñar, implantar y mantener metodologías y políticas.

Requisitos legales y normativos.



Tener en cuenta: riesgos físicos y lógicos, objetivos, métricas e indicadores.

Se requiere de un análisis personalizado de las necesidades de la organización.



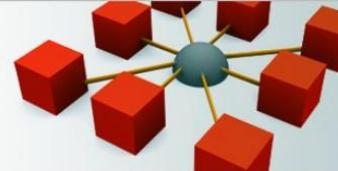
Español English

Inicio Aviso Legal Política de Privacidad Contacto Accesibilidad Agregar a favoritos



aei**ciberseguridad**

Agrupación Empresarial Innovadora
CIBERSEGURIDAD y Tecnologías Avanzadas



Presentación Noticias Miembros Colaboradores Actividades Formación Sello AEI Organigrama y Fines Biblioteca Contacto

Está usted en: Inicio

Introduzca su búsqueda

Buscar en toda la web

Buscar



Presentación de la Agrupación



La AGRUPACIÓN EMPRESARIAL INNOVADORA EN CIBERSEGURIDAD Y TECNOLOGÍAS AVANZADAS reúne a empresas, asociaciones, centros de I+D+i y entidades públicas o privadas interesadas en la promoción del sector de las Nuevas Tecnologías, sus industrias afines y auxiliares, así como otros sectores emparejados con el mismo, que deseen contribuir a los fines de la Agrupación, en el ámbito nacional de las Tecnologías de Seguridad.

El Instituto Nacional de Ciberseguridad (INCIBE) promovió la Agrupación, con el objetivo de dotar de una estructura propia al conjunto de empresas interesadas en la promoción y desarrollo de un Polo Empresarial y Tecnológico vinculado a sus fines, y reconoce, como sello de confianza, el Sello de Ciberseguridad para Organizaciones.

En 2016, la AEI Ciberseguridad entra a formar parte de los órganos de gobierno de la Organización Europea de Ciberseguridad (ECSO).

Sello de Ciberseguridad para Organizaciones

Cualquier entidad pública o privada que quieran demostrar que cumple con unos requisitos de ciberseguridad acorde con el esquema de la AEI de ciberseguridad.



Más información



Últimas noticias

La ciberseguridad, sinónimo de nuevas oportunidades de negocio



El pasado martes día 10 de julio se desarrolló el seminario web "La

Acceso a usuarios

Introduzca sus datos

Usuario

Introduzca su nombre de usuario

Contraseña

Entrar

Recuérdame en este PC

Olvidé la contraseña

Nube de tags

Sello de Ciberseguridad

Capítulo andaluz **INCIBE** socios

Cyberwatching.eu

BlockWall Junta Directiva H2020

Master de Seguridad **ENISE**

CITIC

AEI en Ciberseguridad

Formación Ciberseguridad

ECSO Ciberday ICE

Sello ciberseguridad

Webinar 11ENISE



Bienvenido

Su búsqueda



Abrir sesión



DEFENSA FRENTA A LAS CIBERAMENAZAS

[CCN-CERT](#) | [Gestión de incidentes](#) | [Formación](#) | [Guías](#) | [Informes](#) | [Soluciones](#) | [ENS](#) | [Seguridad al día](#) | [Comunicación](#) | [Empresas](#) | [Registro](#)

ÚLTIMA HORA 21/12/2018 12:06

Nuevas Guías CCN-STIC sobre Microsoft Windows Server 2016

[Inicio](#) > [Informes](#)

INFORMES

- [Públicos](#) >
- [Buenas Prácticas](#) >
- [Código Dañino](#)
- [Amenazas](#)
- [Actualidad](#)

Informes de Ciberseguridad CCN-CERT

Informes elaborados por el grupo de expertos del CCN-CERT con distinta periodicidad:

Categorías

- [Informes CCN-CERT Públicos](#)
- [Informes de Buenas Prácticas \(BP\)](#)

[Volver](#)

Mapa web



ccn-logo



TF-CSIRT
Trusted Introducer

EGC group

CSIRT.es

[AVISO LEGAL](#) | [POLÍTICA DE PRIVACIDAD](#) | [MAPA WEB](#) | [ACCESIBILIDAD](#) |

[POLÍTICA DE COOKIES](#) | [PRENSA](#) | [CONTACTO](#)

© 2019 Centro Criptológico Nacional, Argentona 30, 28023 MADRID



ENS (Esquema Nacional de Seguridad)

ENS para medios electrónicos de datos, informaciones y servicios.

- Acceso.
- Integridad.
- Disponibilidad.
- Autenticación.
- Trazabilidad.
- Conservación.



ENS (Esquema Nacional de Seguridad)

ENS, principios básicos.

- Seguridad integral.
- Gestión de riesgos.
- Prevención, Reacción y recuperación.
- Líneas de defensa.
- Reevaluación periódica.
- Función diferenciada.



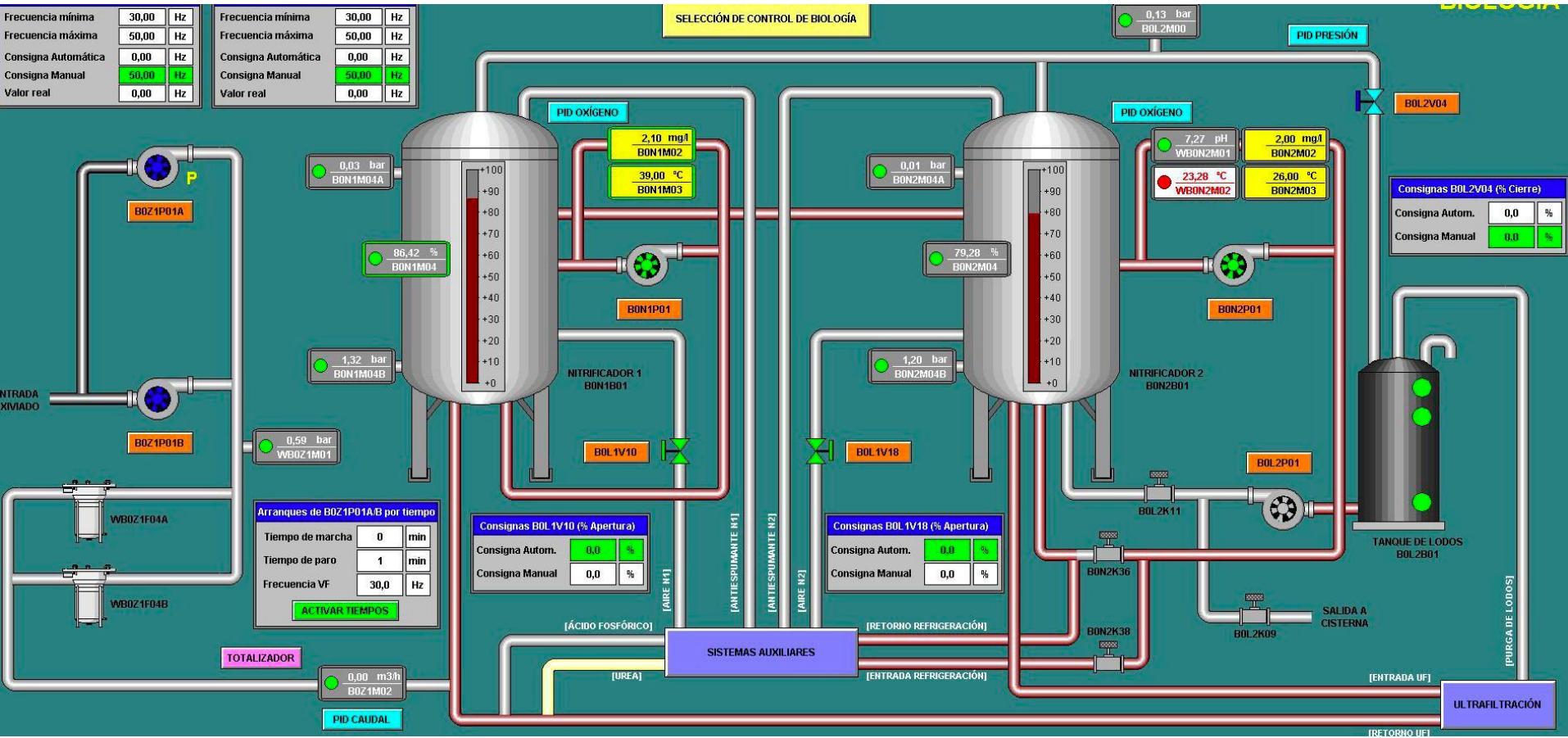
Magerit

Metodología de análisis y gestión de riesgos

- Concienciar de la existencia de riesgos y su gestión.
- Ofrece un método de análisis.
- Ayuda a descubrir y planificar el tratamiento de riesgos.
- Preparar procesos de evaluación, auditoría, certificación o acreditación.



Define una serie de elementos (tipos de activos, dimensiones de valoración, criterios de valoración, amenazas y salvaguardas.)



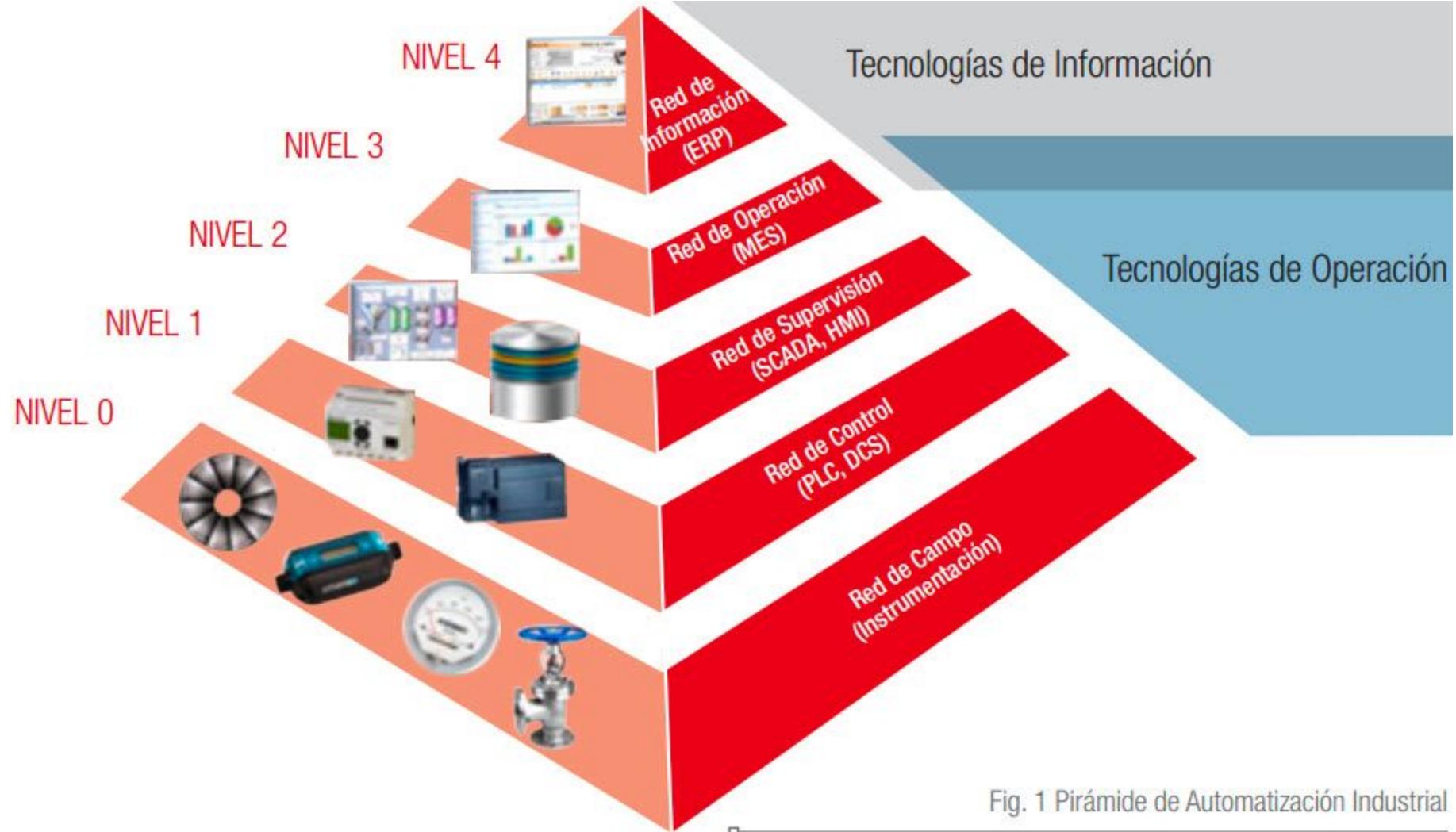


Fig. 1 Pirámide de Automatización Industrial





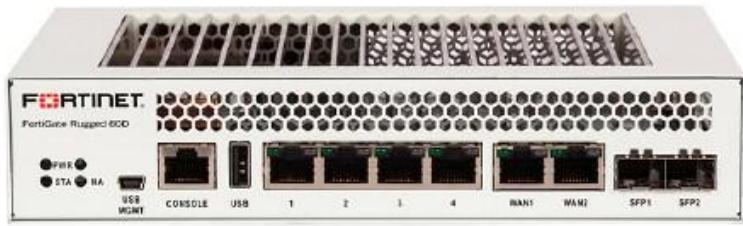


 **Modbus**  **PROFI
BUS®**

 **Modbus EtherNet**

 **PROFI
NET®** **EtherNet/IP**

 **BACnet**  **Modbus**









Principales vulnerabilidades que pueden existir*

0 1 2 3 4

| | | | | | |
|---|---|---|---|---|---|
| Falta de medidas de seguridad física | • | • | • | • | • |
| Arquitectura de red insegura | • | • | • | • | • |
| Posibilidad de Interceptar y alterar comportamiento de sensor | • | | | | |
| Debilidad en los protocolos de comunicación | • | • | • | • | • |
| Instalación configuración incorrecta o servicios innecesarios habilitados | • | • | • | • | |
| Falta de actualización de software | | • | • | • | • |
| Fallos 0-day | • | • | • | • | • |
| Almacenamiento sin protección | | • | • | • | • |
| Debilidad frente a Desbordamiento de buffer | • | • | • | • | • |
| Debilidad en identificación y autenticación (contraseñas) | • | • | • | | |

Principales vulnerabilidades que pueden existir*

0 1 2 3 4

| | | | | |
|---|---|---|---|---|
| Asignación incorrecta de privilegios | • | • | • | • |
| Debilidad frente a Fuzzing (técnicas para proporcionar datos invalidos e inesperados) | • | • | • | |
| Debilidad frente a ataques de Cross-Site Scripting | | • | • | • |
| Debilidad frente a ejecución de código remoto | | • | • | • |
| Personal de planta no capacitado en tecnologías de operación y/o información | • | • | • | • |
| Personal de TI no capacitado en tecnologías de operación | • | | • | • |
| Acuerdos de nivel de servicio insuficientes | • | • | • | • |
| Falta de control de cambios | • | • | • | • |
| Falta de planes de continuidad | • | • | • | • |
| Falta de procedimientos adecuados en el uso de las tecnologías de operación | • | • | • | |

Principales vulnerabilidades que pueden existir*

| | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| Personal contratado inadecuado o sin concienciación o formación en ciberseguridad | • | • | • | • | • |
| Falta de mecanismos de monitorización | • | • | • | • | • |
| Conexiones públicas desprotegidas | • | • | • | • | • |
| Uso de herramientas de red no permitidas | • | • | • | • | • |
| Existencia de servidores dual home | | • | • | • | • |
| Interfaz de acceso inadecuados | | | • | • | • |
| Documentación escasa | • | • | • | • | • |
| No realización de copias de seguridad (Perdida de datos, Ransomware,...) | • | • | • | • | • |
| Carencia de software anti-malware | • | • | • | • | • |
| Utilización de usuarios genéricos | • | • | • | • | • |

Desde FileMaker Desde HTML Desde el texto Nueva consulta de la base de datos Actualizar todo Conexiones Propiedades Editar vínculos A Z Z A Ordenar Filtro Avanzadas Texto en columnas Quitar duplicados Validación de datos Consolidar Análisis Y si Agrupar Desagrupar Subtotales Mostrar detalle

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | |
|----|---|----------------------------|-----------------------------|-----------------------------|---|--------------|---|---|---|---|---|---|---|---|--|
| 1 | #SCADA StrangeLove Default/Hardcoded Passwords List | | | | | | | | | | | | | | |
| 2 | #Find more at http://www.scada.sl | | | | | | | | | | | | | | |
| 3 | #Please contact us at scadastrangelove@gmail.com and @scadasl | | | | | | | | | | | | | | |
| 4 | #release 1.1 by Oxana Andreeva (oxana.andreeva@inbox.ru) | | | | | | | | | | | | | | |
| 5 | | | | | | | | | | | | | | | |
| 6 | Vendor | Device | Default password | Port | Device type | Protocol | Source | | | | | | | | |
| 7 | ABB | AC 800M | service:ABB800xA | | Controller | | https://library.eabb.com/public/f355a67551218ae7c1257dc0003298c5/3BDS021515-600_en_AC_800M_6.0.pdf | | | | | | | | |
| 8 | ABB | SREA-01 | admin:admin | 80/tcp | Ethernet Adapter Module | http | https://www.inverterdrive.com/file/ABB-SREA-01-Manual | | | | | | | | |
| 9 | Adcon Telemetry | Telemetry Gateway A840-a | root:840sw | terminal program | Base Station | | http://www.adcon.com/index.php?option=com_docman&task=doc_download&gid=41&Itemid=239&lang=de | | | | | | | | |
| 10 | Adcon Telemetry | addVANTAGE Pro 6.1, 6.5 | root:root | 8080/tcp | HMI | HTTP | http://adcon.com/index.php?option=com_docman&task=doc_download&gid=31&Itemid=239&lang=en, http://adcon.com/index.php?option=com_docman&task=doc_download&gid=41&Itemid=239&lang=de | | | | | | | | |
| 11 | Advantech | SNMP-1000, MIC-3924 | advantech:admin | serial port | system management module, intelligent chassis management module | | http://support.elmark.com.pl/advantech/pdf/SNMP-1000man.pdf, https://ecauk.com/files/2011/08/Advantech-SNMP-1000-manual.pdf | | | | | | | | |
| 12 | Advantech | Advantech WebAccess bro | admin:blank | 80/tcp | browser-based HMI and SCADA soft | HTTP | http://advantech.vi.llwd.net/o35/www/webaccess/developer_manual/Advantech-WebAccess-Quick-Start-Guide.pdf | | | | | | | | |
| 13 | Advantech | EKI-7659C, EKI-7657C | admin:admin | 80/tcp | industrial switch | HTTP | http://www.rts.ua/catalog/advantech/pdf/EKI-7659C_2_201316.pdf | | | | | | | | |
| 14 | Advantech | ADAM-6200 Series | root:00000000 | 80/tcp | Intelligent Ethernet I/O Module | HTTP | http://www.bb-elec.com/Products/Manuals/ADAM-6200m-pdf.pdf | | | | | | | | |
| 15 | Advantech | ADAM-6050W | 0 | | I/O module | | http://datasheet.octopart.com/ADAM-6050W-AE-Advantech-datasheet-32780543.pdf | | | | | | | | |
| 16 | Advantech | ADAM-3600-A1F | Root:00000000, Admin:000000 | 80/tcp | Remote I/O Module | HTTP | https://www.proxis.ua/files/documents/UM-ADAM-3600-A1F-Ed1-EN.pdf | | | | | | | | |
| 17 | Alcatel-Lucent | OmniSwitch 6250 | admin:switch | 80/tcp, 23/tcp | switch | HTTP, Telnet | https://dariusfreemon.wordpress.com/tag/defaults/ | | | | | | | | |
| 18 | Allied Telesis | IE200 Series: AT-IE200-6G | manager:friend | terminal or terminal emulat | Industrial Ethernet Switches | | http://www.alliedtelesis.com/userfiles/file/IE200_InstallGuide_RevC.pdf | | | | | | | | |
| 19 | Alstom | KVG202/EN/M/E11, MICO AAAA | | | Relays | | https://www.gegridsolutions.com/alstomenergy/grid/Global/Grid/Resources/Documents/Automation/Technica | | | | | | | | |
| 20 | Argus | Argus Messenger | ArgusAdmin:masterkey | | Messenger | | https://dariusfreemon.wordpress.com/2015/07/11/argus-suite-multiple-default-credentials/ | | | | | | | | |
| 21 | Argus | Argus Address Manager | argus:argus | | Address Manager Software | | https://dariusfreemon.wordpress.com/2015/07/11/argus-suite-multiple-default-credentials/ | | | | | | | | |
| 22 | Astute Medical | ASTUTE140 Meter | 1234:1234 | | analyzer | | https://dariusfreemon.wordpress.com/2015/07/11/astute-medical-astute140-meter-default-user-credentials/ | | | | | | | | |
| 23 | B&B ELECTRONICS | CR10 v2 | root:root | 80/tcp | Industrial router | http | http://techniska.pl/downloadfile/1400014902-1208342584-pdf | | | | | | | | |
| 24 | B&B ELECTRONICS | Cone! 4.0.1 | root:root | 80/tcp | Industrial router | http | http://conel.ru/shared/files/201502/9_411.pdf | | | | | | | | |
| 25 | B&B ELECTRONICS | SPECTRE Router | root:root | 80/tcp | Router | http | b&b electronics SPECTRE Router.pdf | | | | | | | | |
| 26 | B&B ELECTRONICS | ER75/1 ER 75 DUO/ER 75 SI | root:root | 80/tcp | Industrial router | http | http://ec-mobile.ru/user_files/File/Cone!/ER75_1_Manual_RUS.pdf | | | | | | | | |
| 27 | B&B ELECTRONICS | LR77 v2 Libratum/LR77 v2 | root:root | 80/tcp | Industrial router | http | http://www.induowireless.com/wp-content/uploads/2014/12/lr77-v2-libratum-manual.pdf, http://data.komm | | | | | | | | |
| 28 | B&B ELECTRONICS | UR5i v2 | root:root | 80/tcp | Industrial router | http | http://www.cd.lucom.de/vpn-industrie-router/dokumentation/handbuch/ur5iv2-guide.pdf | | | | | | | | |
| 29 | B&B ELECTRONICS | UCR11-v2/UCR11 v2 SL | root:root | 80/tcp | Industrial router | http | http://www.induowireless.com/wp-content/uploads/2014/03/ucr11-3g-router-hspa-cdma.pdf | | | | | | | | |
| 30 | B&B ELECTRONICS | XR5i v2/XR5i v2/XR5i/XR5 | root:root | 80/tcp | Industrial router | http | http://www.cd.lucom.de/vpn-industrie-router/dokumentation/handbuch/xr5iv2e-guide.pdf | | | | | | | | |
| 31 | B&B ELECTRONICS | ES1A | root:dbps | 80/tcp | Converter | HTTP | http://www.bb-elec.com/Products/Manuals/pn-6909-rev03_ES1A-5012m.pdf | | | | | | | | |
| 32 | B&B ELECTRONICS | Vlinx VESR4x4 | <blank> | | SERIAL SERVER | | http://www.bb-elec.com/Products/Manuals/VESP211-5012m.pdf | | | | | | | | |
| 33 | B&B ELECTRONICS | Vlinx MESR9xx Modbus Gate | <blank> | | Modbus Gateway | | https://www.manualshelf.com/manual/b-b-electronics/vlinx-mesr9xx/modbus-gateway-brochure/page-31.htm | | | | | | | | |
| 34 | Barco | MediCal QAWeb Agent | Advanced:advanced | | client application | | https://dariusfreemon.wordpress.com/2015/07/10/barco-medical-qaweb-agent-default-password/ | | | | | | | | |
| 35 | Beckhoff Automation | CX5020 | webguest:1 | 23/tcp | PLC | Telnet | https://www.researchgate.net/publication/272420507_ICSSCADA_Security_Analysis_of_a_Beckhoff_CX5020_Pl | | | | | | | | |
| 36 | Beckhoff Automation | TwinCAT | Administrator:1 | | Software for the Windows control and automation technology | | https://infosys.beckhoff.com/english.php?content=/1033/sw_0s/html/cx1000_xs_xpe_geninfo.htm& | | | | | | | | |
| 37 | Beck IPC | IPC@CHIP | PPPSERVER: non:non | | PI C | nan:chan | https://www.beck-inc.com/files/ani/srvv/config.htm | | | | | | | | |



Control Systems

Home

Calendar

ICSJWG

Information Products

Training

Recommended Practices

Assessments

Standards & References

Related Sites

FAQ

Downloading and Installing CSET

Download CSET using the link at the bottom of this page or by [clicking here](#). After clicking the link, you will be asked to identify yourself and will then be given the opportunity to download the file *CSET_x.x.iso* (where *x.x* represents the download version).

The CSET download is in a file format known as "ISO." This file is an "image" of the equivalent installation files included on the CSET CD. Because of this format, it is necessary to process the download using one of the following methods:

1. Decompressing the File - Open the file using any one of the newer compression utility software programs.
2. Mounting the File - this method loads the ISO file using utility software to make the file appear like a virtual drive with the original CD loaded.
3. Burning the file to CD - this method uses CD-burn software and the ISO file to burn the files onto your own CD to create a physical disk identical to the CSET original.

These methods require separate software utilities. There are a variety of both free and purchased utility programs available through the Internet that will work with the ISO file format. As DHS does not recommend any specific application or vendor, it will be necessary for you to find a product that provides the necessary functionality. Step by step instructions for each method are provided below:

Decompressing the File

1. CLICK the "Download CSET" link at the bottom of this page and complete the requested information to download the ISO file.
2. SAVE the file to your hard drive of choice (i.e., your computer hard drive or USB drive) maintaining the file name and extension (.iso).
3. OPEN the ISO file with a compression utility program and SAVE the files to your hard drive of choice maintaining the original names and file extensions.
4. COMPLETE the *Installing the CSET Program* instructions below.

Mounting the File

1. CLICK the "Download CSET" link at the bottom of this page and complete the requested information to download the ISO file.
2. SAVE the file to your hard drive of choice (i.e., your computer hard drive or USB drive) maintaining the file name and extension (.iso).
3. RUN your ISO-specific utility program that is capable of mounting the file. COMPLETE the instructions within the utility software to create a virtual drive using the ISO file. If you do not have an ISO utility application you will need to find and install one before continuing with these instructions.
4. COMPLETE the *Installing the CSET Program* instructions below.

Burning the file to CD

1. CLICK the "Download CSET" link at the bottom of this page and complete the requested information to download the ISO file.
2. SAVE the file to the hard drive on your computer maintaining the filename and extension (.iso).
3. INSERT a blank, writable CD into the computer's CD drive.
4. RUN your CD-burn utility program. COMPLETE the instructions on your utility program to burn the ISO image to your DVD. (If you do not have an application that can do this, then you will need to find and install one before continuing with these instructions.)
5. COMPLETE the *Installing the CSET Program* instructions below.

Installing the CSET Program

1. FIND the CSET_Setup.exe file in the folder, virtual drive, or CD containing the CSET files.
2. DOUBLE-CLICK the CSET_Setup.exe file to execute. This will initiate the installer program.
3. COMPLETE the instructions in the installation wizard to install the CSET program.

 Preparation ▾ Assessment ▾ Results ▾ Diagram

CYBER SECURITY EVALUATION TOOL

Version 8.0



Prepare Your Assessment

CSET helps you determine the cybersecurity posture of your organization as you answer questions based on recognized industry standards about your systems and procedures.

Before you can answer questions, your question set needs to be identified. The 'Start Here' button begins the question identification and preparation process.

[Start Here >>](#)

Home Format



Files

General

Settings

Import/Export

Help

Stencils Symbols

| | |
|---------|-----------------------|
| ICS | Configuration Server |
| IT | DCS |
| Radio | EWS |
| Medical | FEP |
| General | Historian |
| Zone | HMI |
| Shapes | IED |
| | MTU |
| | PLC |
| | RTU |
| | SIS |
| | Terminal Server |
| | Unidirectional Device |

Save and Close



Document Tree

Search



Guidance

Reports

Templates

Standards

Access Control

Categorization

Chemical Industry

Contingency Planning

Cryptography & Encryption

Department of Defense

Electric Power Industry

General Control System Standards

Information Technology Specific Sta

InfoSec

Nuclear Reactors

Other Referenced Documents

Privacy

Processes & Procedures

Requirement Mode Only Standards

Resource Identification

Sector Specific Standards

Test & Evaluation

Publisher

Publication Year

Cyber Security Procurement Language

Catalog of Recommendations



Resource Library

This library of cyber security standards, reports, and templates are provided for your convenience. Additionally there are several cyber security guides and white papers to assist you in gaining a general background in cyber security, determining priorities, or specific helps. Specific helps include white papers and instructions on securing network components such as a firewall or web server.

Library documents may be browsed using the "Document Tree" tab on the left side of the screen. Documents are grouped by type and topic. If you are looking for a specific document a keyword or title search may also be performed using the "Search" tab in the left pane. Clicking on a document title link in the left-hand pane displays the document. To save a document to

Close

Sistemas de gestión de la CALIDAD y MEJORA CONTINUA:

Compromiso con buenas prácticas y la satisfacción total del cliente exigente.



International
Organization for
Standardization

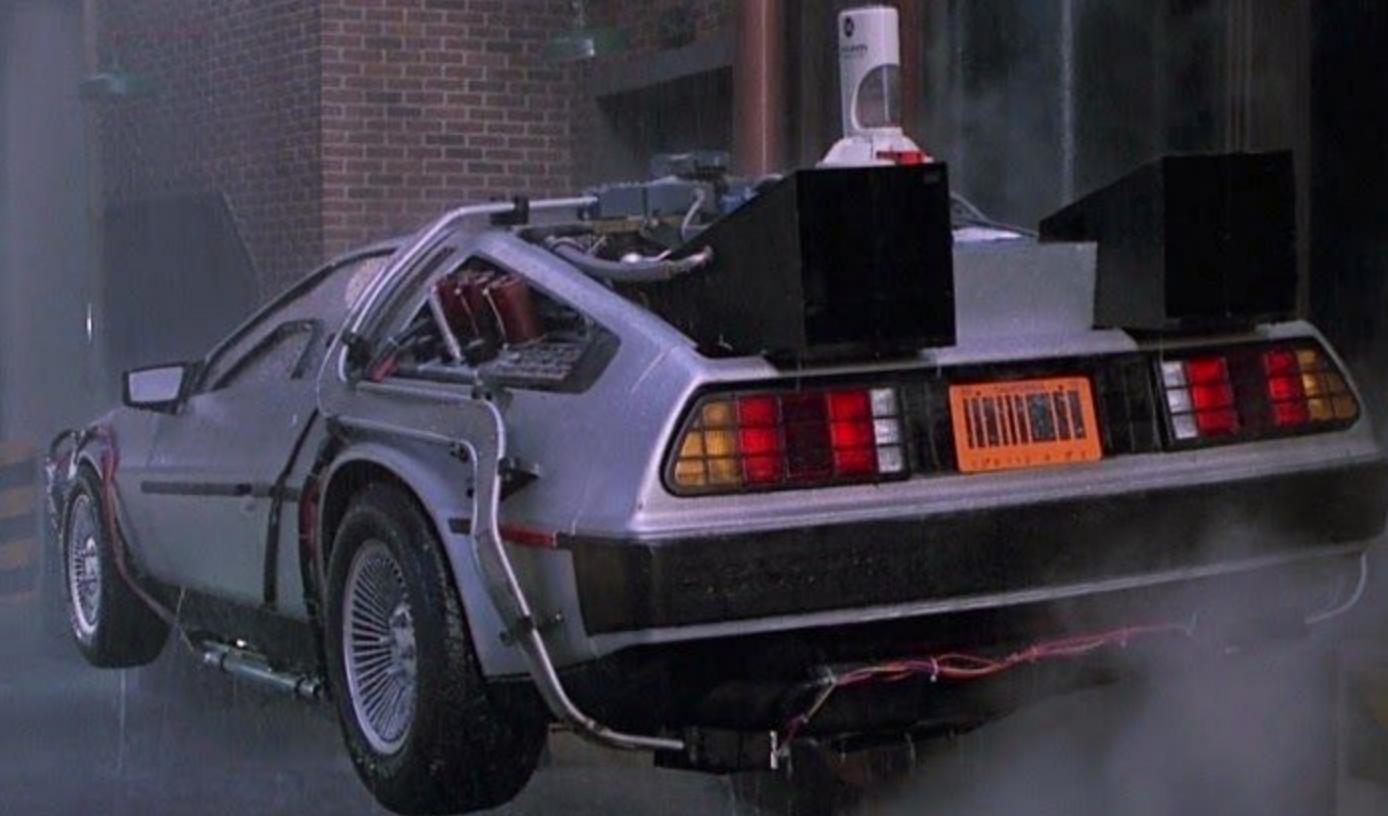


- La certificación **ISO 9001** es un conjunto de normas que determina los requisitos y el modelo de gestión para un sistema de Gestión de la Calidad.
- La certificación **ITIL** (Biblioteca de Infraestructura de Tecnologías de Información) es un conjunto de conceptos y buenas prácticas para la gestión de procesos en servicios, desarrollos y operaciones TIC.

Sistemas de gestión de la CALIDAD y MEJORA CONTINUA:

- **COBIT**, (Control Objectives for Information and related Technology) es una guía de mejores prácticas presentada como un marco de trabajo, dirigido al control y supervisión TIC.
- La certificación **ISO 27001** es el estándar internacional para la seguridad de la información publicado por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). Especifica los requisitos para establecer, implantar, mantener y mejorar un SGSI (Sistema de Gestión de Seguridad de la Información).
- El estándar (**PCI DSS**) de Seguridad de Datos de la Industria de Tarjetas de Pago es apropiado para el tratamiento, procesado y transmisión de datos sensibles e información crítica.
- **GDPR** (General Data Protection Regulation) o **RGPD** (Reglamento General de Protección de Datos)





RGPD (Reglamento General de Protección de Datos):

- Entró en vigor el 25 de mayo de 2016, pero comenzará a aplicarse el 25 de mayo de 2018.
 - ¿y la LOPD y el reglamento?: Siguen en vigor hasta que entre en funcionamiento el reglamento y se aprueben/modifiquen nueva normativa interna.
- Aplicación directa en toda la Unión Europea.
- E incluso la prestación de servicios u oferta de bienes de empresas fuera de la Unión pero que se ofrezca a interesados dentro UE.

RGPD (Reglamento General de Protección de Datos):

Novedades principales en el Reglamento Europeo de Protección de Datos:

- Consentimiento expresado.
- Desaparece la inscripción de ficheros en la AEPD.
- Derechos: **Derecho al olvido**, derecho a la portabilidad de los datos.
- Privacidad en el diseño y por defecto.
- Nuevas figuras: Evaluación de Impacto y el **Delegado de Protección de Datos**.
- Brechas e incidencias de seguridad.
- Infracciones y sanciones.



RGPD... Definiciones:

- **Tratamiento:** cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;
- **Fichero:** todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;
- **Responsable del tratamiento** la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

RGPD... Definiciones:

- **Encargado de tratamiento:** La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento. Ejemplo: Asesoría, empresa de limpieza, agencia de comunicación, auditoría, hosting, etc.
- **Consentimiento:** toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una **declaración o una clara acción afirmativa**, el tratamiento de datos personales que le conciernen. Solicitud de consentimiento para el tratamiento.
- **Categoría especiales** de datos: datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

RGPD... Principios del reglamento:



- Los datos serán tratados de manera lícita, leal y transparente.
- Recogidos con fines determinados, explícitos y legítimos (limitación de la finalidad).
- Adecuados, pertinentes y limitados (minimización de datos).
- Exactos y si fuera posible actualizados (exactitud).
- Mantenidos no más tiempo del necesario para los fines del tratamiento (limitación del plazo de conservación).
- Serán tratados de manera que se proteja su integridad y confidencialidad.
- Responsabilidad proactiva.

RGPD... Derechos de los ciudadanos en el RGPD:

- Derecho de Acceso.
- Derecho de Rectificación.
- Derecho de Cancelación.
- Derecho de Oposición.
- Derecho de supresión (**derecho al olvido**).
- Derecho a la limitación del tratamiento.
- Derecho a la portabilidad de datos.
- No ser objeto de decisiones individuales automatizadas.







[Inicio](#) | [Avisos](#) | [Incidentes](#) | [Reportar una vulnerabilidad](#) | [Alertas](#) | [Publicaciones](#) | [Intercambio de amenazas](#) | [Otras actividades](#) | [Sobre BCSC](#)

Respuesta a incidentes

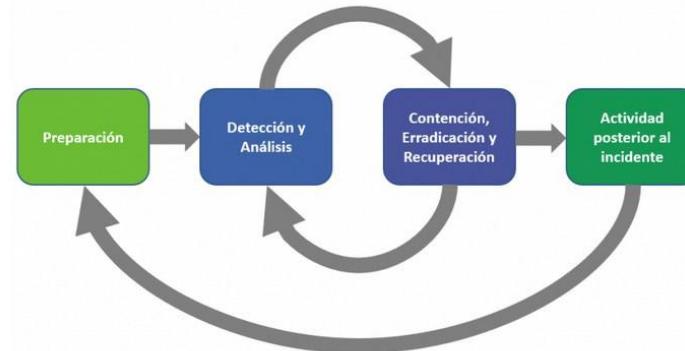
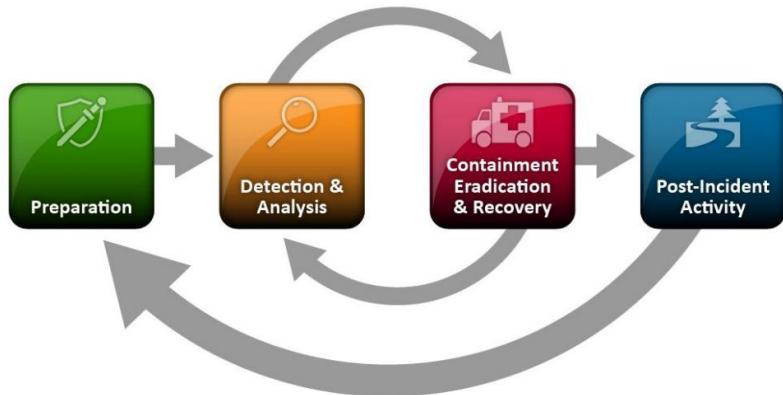


Diagrama basado en el ciclo de respuesta a incidentes propuesto por el NIST

Security Operation Center:



Un SOC basa sus servicios en:

- **Prevención;** minimizar las probabilidades de aparición de incidentes y disminuir la materialización de amenazas mediante una vigilancia permanente.
- **Detección;** monitorización constante de indicios de incidentes.
- **Análisis;** estudio y confirmación de alertas entre amenaza real y falso positivo.
- **Respuesta;** reacción ante incidentes.

Security Operation Center:

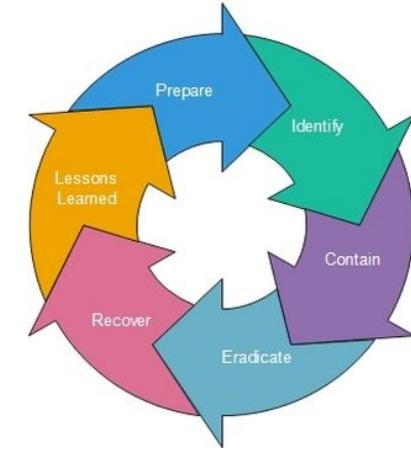
Objetivos de un SOC:

- Implantar, administrar y mejorar los servicios de un sistema de gestión y control para monitorización y trazabilidad permanente en tiempo real de los eventos de los sistemas, con objeto de detectar y prevenir incidentes.
- Implementar procedimientos para detectar, identificar, analizar, resolver y neutralizar la constante evolución de amenazas.
- Gestión de procesos de ciber-incidentes de seguridad.

Para cumplir eficazmente con estos objetivos, se definen previamente los siguientes procesos que los comprenden, con objeto de desarrollar e implementar una metodología y protocolos de reacción y respuesta constantes y de modo sistemático:

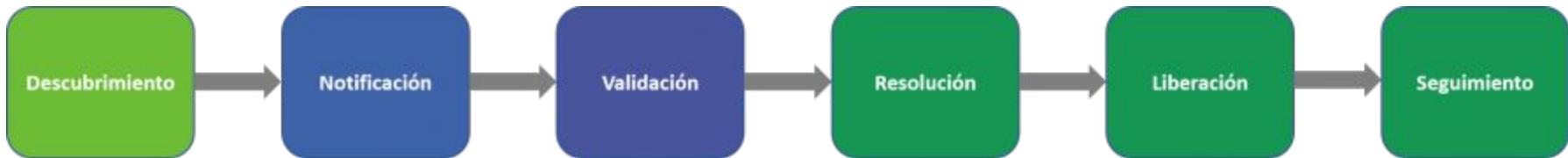


Security Operation Center:



GESTIÓN DE INCIDENTES DE SEGURIDAD:

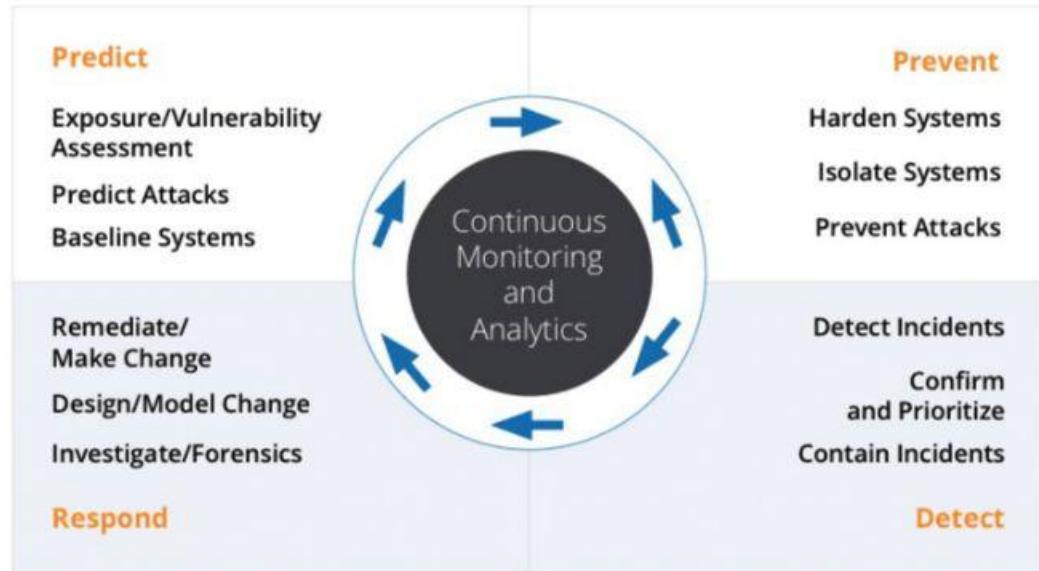
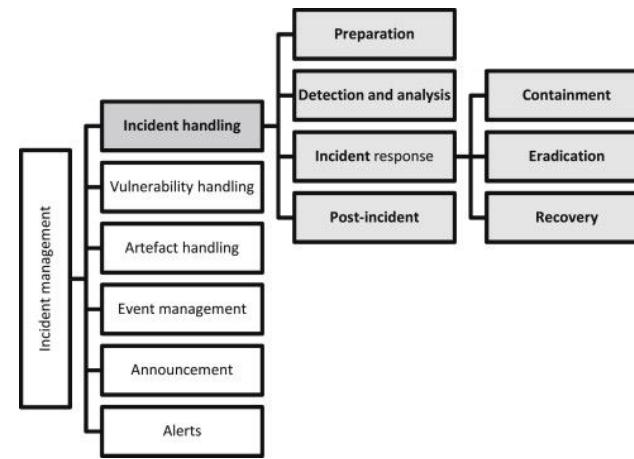
- Documentar el análisis del incidente identificado, verificado y evaluado.
- Notificación; Respuesta rápida, efectiva y ordenada a través de los canales establecidos.
- Informática Forense: Recolección, retención y presentación de evidencias.



Security Operation Center:

Ciclo de vida de un incidente:

- Preparación.
- Detección y Análisis.
- Mitigación; Contención, erradicación.
- Recuperación y actividad posterior al incidente.



Security Operation Center:



Detección de incidentes:

- De tipo **manual** (reportada por usuario) y automática (IDS y IPS).
- Provenientes de alertas con indicios de:
 - **precursores** (puede ocurrir)
 - **indicadores** (puede haber ocurrido o estar ocurriendo).

Security Operation Center:

Clasificación de incidentes.

Por niveles, según su peligrosidad, atendiendo a la repercusión de materialización de la amenaza:

- Persistencia.
- Código dañino.
- Disponibilidad.
- Obtención de información.
- Intrusión.
- Compromiso de la información.
- Fraude.
- Contenido abusivo.
- Políticas de seguridad.

| | | Impacto | Alto | Medio | Bajo |
|----------|-------|----------|------|-------|------|
| | | Urgencia | Alto | Medio | Bajo |
| Urgencia | Alto | 1 | 2 | 3 | |
| | Medio | 2 | 3 | 4 | |
| Bajo | | 3 | 4 | 5 | |



Security Operation Center:

Análisis de Impacto de ciber-incidentes; Criterios del impacto, respecto al:

- Impacto funcional de los sistemas
- Impacto en la información y servicios prestados
- Recuperación



Demasiado ruido blanco (alertas de poca consecuencia) o falsos positivos conducen a la fatiga de alertas por parte de los analistas.

Security Operation Center:

Estados de incidentes:

- Abierto: Notificado el cliente y a la espera de respuesta .
- Reportado: Notificado y con confirmación por parte del cliente.
- Gestionado: Solucionado con el soporte del equipo de forma conjunta con el cliente.
- Neutralizado: Solucionado desde nuestras instalaciones y notificado al cliente.



what are other words for countermeasures?

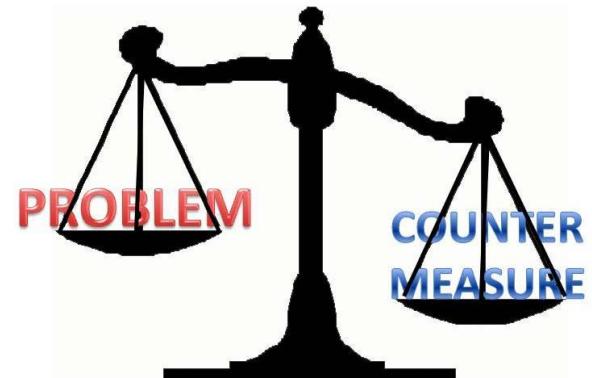
countermeasure, counterblast, cures, remedies, correctives, medications, antidotes, solutions, pills, reliefs



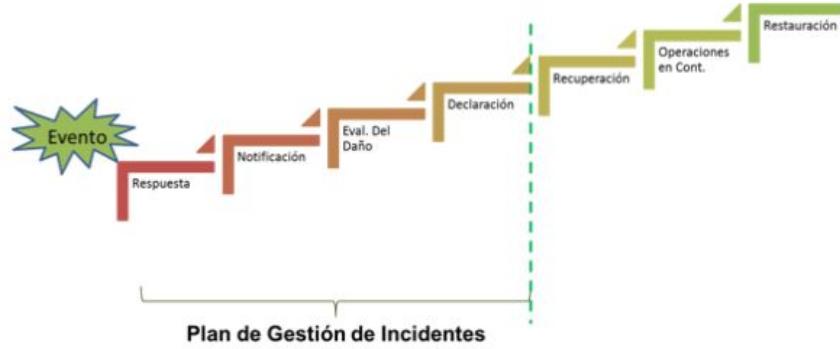
Security Operation Center:

Establecimiento de **Contramedidas** de defensa para el control de las diferentes **Fases de un ataque**:

- Selección del objetivo y Recopilado de información.
 - Reconocimiento OSINT, Enumeración y Análisis de vulnerabilidades.
- Vectores de ataque y Obtención de acceso.
- Escalada de privilegios.
- Mantenimiento del acceso.
- Borrado de huellas.



Security Operation Center:



Plan de respuesta a incidentes de seguridad:

- Constitución de Plan de respuesta a incidentes
- Definición de una guía de procedimientos
- Detección de un incidente de seguridad
- Contención, erradicación y recuperación
- Identificación del atacante y posibles actuaciones legales
- Documentar y reportar

Security Operation Center:

Uno de los modelos de proceso de **respuesta a incidentes** más frecuentemente utilizado es el modelo DOE / CIAC, que consta de seis etapas:

- Preparación,
- Identificación,
- Contención,
- Erradicación,
- Recuperación,
- y Lecciones aprendidas.



Security Operation Center:

Plan de recuperación ante desastres:

- Estrategia de recuperación
- Equipo de Respuesta a Incidentes de Seguridad (CSIRT)
- Equipo de Disponibilidad de Emergencia Informática (CERT)
- Análisis de Impacto de Negocios (**BIA**, Business Impact Analysis)
- **Plan de Contingencias**, donde se incluya el plan de recuperación de desastres:
 - Definición general del plan
 - Determinación de vulnerabilidades
 - Selección de los recursos alternativos
 - Preparación detallada del plan
 - Pruebas y mantenimiento

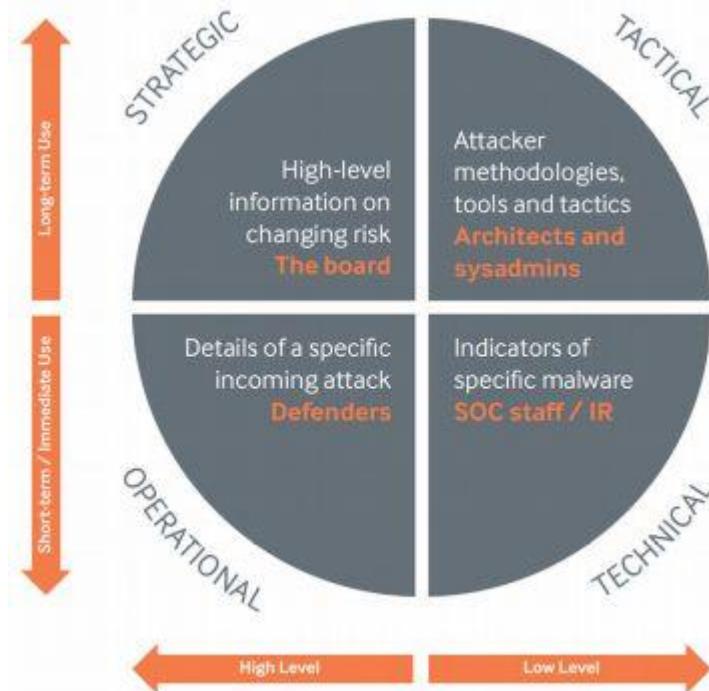


Security Operation Center:

INTELIGENCIA DE AMENAZAS:

Recolectar, Analizar y Evaluar:

- Evaluación de la vulnerabilidad
- Creación de la fuente interna documental de conocimiento
- Compartición e intercambio de información



Security Operation Center:

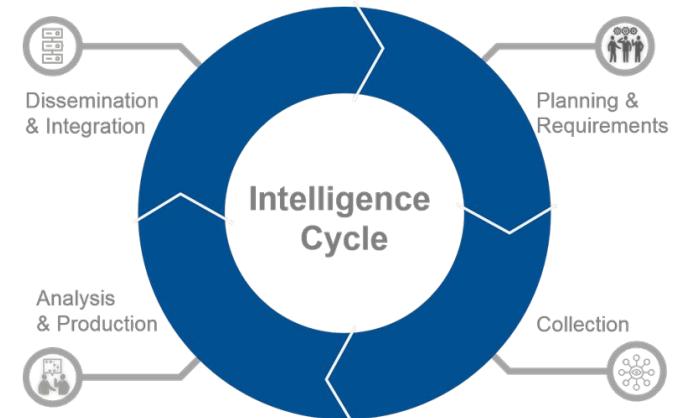
Valoración de amenazas:

- Degradación. Pérdida de rendimientos sobre la calidad de servicio (QoS)
- Probabilidad de ocurrencia
- Impacto



Cyber Threat Intelligence ayuda a las organizaciones a comprender y gestionar el riesgo empresarial.

- Inteligencia Estratégica sobre Amenazas
- Inteligencia Operacional de Amenazas
- Inteligencia Táctica de Amenazas
- Inteligencia Técnica de Amenazas



Security Operation Center:

ANÁLISIS Y GESTIÓN DE RIESGOS Y VULNERABILIDADES.

Monitorización continua de la seguridad de la información:

- Amenazas humanas
 - Amenazas de Ingeniería Social
- Amenazas de Hardware
- Amenazas de Red
- Amenazas Lógicas
 - Caballos de Troya
- Amenazas por Fenómenos Naturales



Security Operation Center:

Análisis de Riesgos:

- Recogida de información.
- Identificación y agrupación de activos.
- Identificación y evaluación de amenazas.
- Identificación y evaluación de vulnerabilidades.
- Identificación y valoración de impactos.
- Evaluación y análisis del riesgo y priorización.

Security Operation Center:

Gestión de Vulnerabilidades:

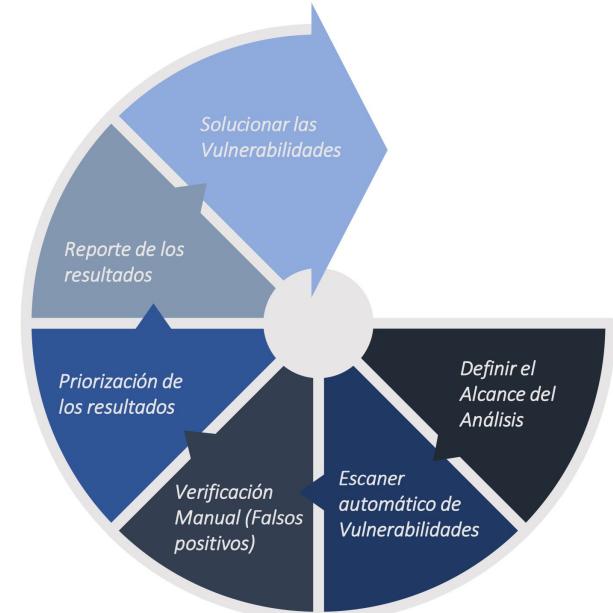
- Descubrimiento
- Notificación
- Validación
- Resolución
- Liberación y Seguimiento.



Security Operation Center:

Análisis de Vulnerabilidades (para minimizar la posibilidad de que una amenaza se materialice y llegue a convertirse en ataque):

- Físicas
- Naturales
- Hardware
- Software
- Red
- Factor humano





SOCaaS

SOC-as-a-Service

provides companies with the knowledge and skills necessary to combat cybersecurity threats.

El Centro de Operaciones de Ciberseguridad no sustituye ni reemplaza funciones o responsabilidades existentes en el cliente.

El objetivo final del SOC es apoyar, dar soporte y aumentar las capacidades existentes de vigilancia, defensa en profundidad y respuesta donde se detecten carencias.

- Monitorización, recolección, correlación y revisión de eventos. Análisis en tiempo real
- Detección temprana e identificación de incidentes fallidos y exitosos
- Gestión de informes periódicos de actividad y auditorías
- Evaluación, Análisis y solución de incidentes
- Prevención, mitigación, neutralización y contención de amenazas

SOCaaS



- Atendiendo la evolución tecnológica y anticipándose a las necesidades, se proporciona la prestación de un servicio adaptado y personalizado como una inversión estratégica que convierte a sus clientes de la PYME en proveedores ciberseguros, dotados de equipos, políticas y planes que protegen y aseguran la confidencialidad, integridad y disponibilidad de la información que gestionan sus sistemas.
- Situando la inversión en seguridad de las organizaciones clientes por debajo del coste de una potencial fuga o secuestro de información, acercando a la PYME servicios de ciberseguridad que hasta ahora solo podían acceder las grandes corporaciones; servicio ininterrumpido 24x7: Clúster de sistemas de **Alta Disponibilidad** y balanceo de carga, con redundancia y **tolerancia a fallos**.

SOCaaS



- Ofrece la prestación de unos servicios de SOC adaptados para apoyar el SGSI y el cumplimiento de los estándares internacionales recogidos en norma ISO 27001.
- Se personaliza un nivel de servicio requerido, adaptado a unas necesidades y respuesta establecidas.
- Un servicio externalizado facilita así a PYME afrontar con tranquilidad y garantías el cumplimiento, definiendo alcance y límites dentro de unos costes económicamente competitivos, asumibles y calculados en características y precio.
- De este modo, la inversión en seguridad se sitúa por debajo de los costes económicos de hacer frente a incidentes imprevistos.

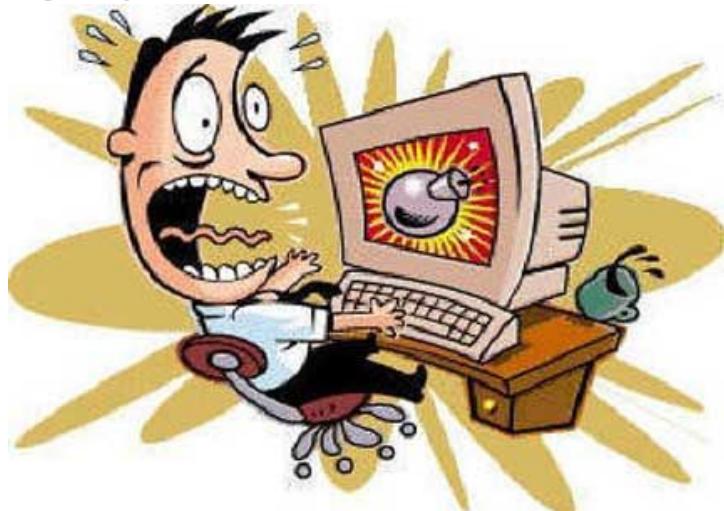
SOCaaS



“- un SOC debe estar integrado en la empresa, pero funcionar independiente a ella”.

Dentro de los servicios de un SOC estará también presente:

- la inversión en formación y concienciación.
- la investigación.





[Inicio](#) | [Avisos](#) | [Incidentes](#) | [Reportar una vulnerabilidad](#) | [Alertas](#) | [Publicaciones](#) | [Intercambio de amenazas](#) | [Otras actividades](#) | [Sobre BCSC](#)

Publicaciones

Guías, Estudios e Informes



Publicaciones correspondientes al Observatorio Técnológico sobre tendencias, tecnologías, amenazas, etc. en ciberseguridad.

Boletines de Avisos Técnicos



Recopilación mensual de avisos técnicos publicados.

Boletines de Avisos SCI



Recopilación mensual de los avisos SCI publicados.

Infografías

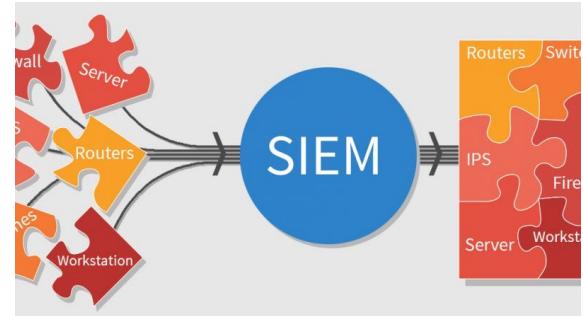


Consejos básicos para mejorar el nivel de ciberseguridad.

Security Information and Event Management.

SIEM:

- Gestión automática y centralizada de eventos.
- Recolección, análisis y presentación de información de red y eventos en los sistemas.
- Gestión de identidades y accesos.
- Gestión de vulnerabilidades.
- Auditoría de registro de sistema, servicios y cambios de configuración del sistema.



Security Information and Event Management.

LM (Log Management) Gestión de Logs:

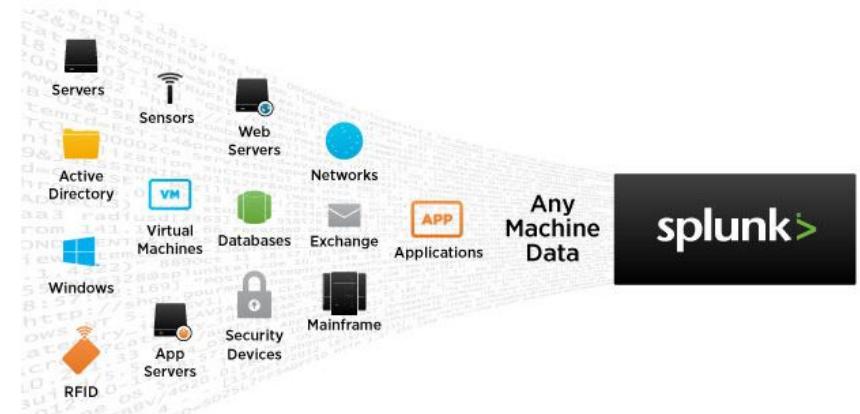
- Identificación de patrones de ataque.
- Acceso (y uso interno y externo) de datos confidenciales.
- Disponibilidad y rendimientos.
- Integración de datos.
- Supervisión y Gestión centralizada.
- Trazabilidad.



Security Information and Event Management.

Monitorización y Gestión de logs:

- Agregación, colección y normalización de datos.
- Correlación e indexación.
- Alerta.
- Informes.
- Dashboards.
- Cumplimiento.
- Retención.

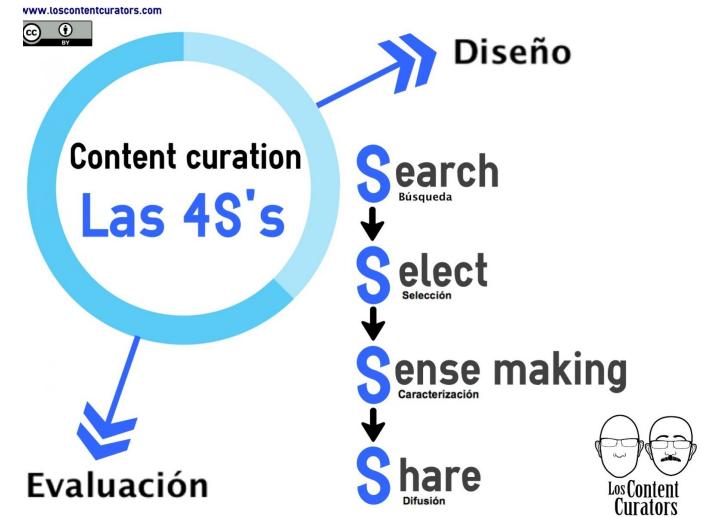
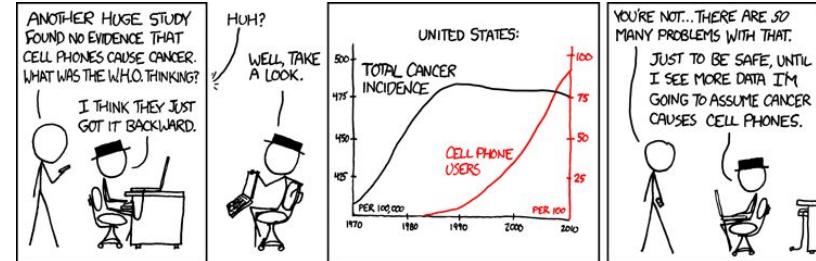


Security Information and Event Management.

Correlación:

Transformar datos en información, entender los sucesos para clasificación y análisis.

- Identificación de duplicados.
- Correspondencia con patrones de secuencia.
- Correspondencia de patrones de tiempo.
- Exposición de sistema y análisis de criticidad.
- Correspondencia de políticas de seguridad.



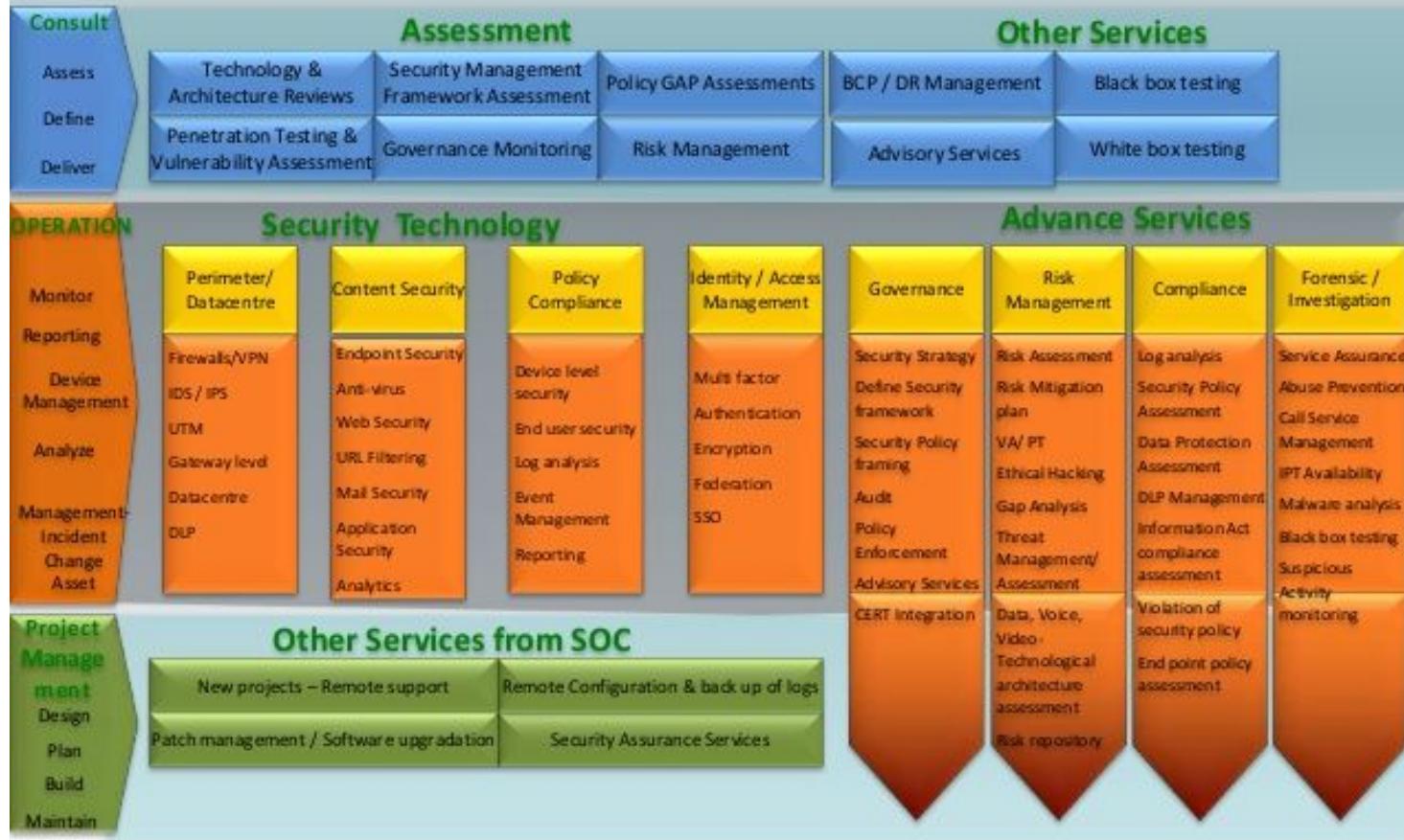
Security Information and Event Management.

El **objetivo** del **SIEM/SOC** se enfoca para la:

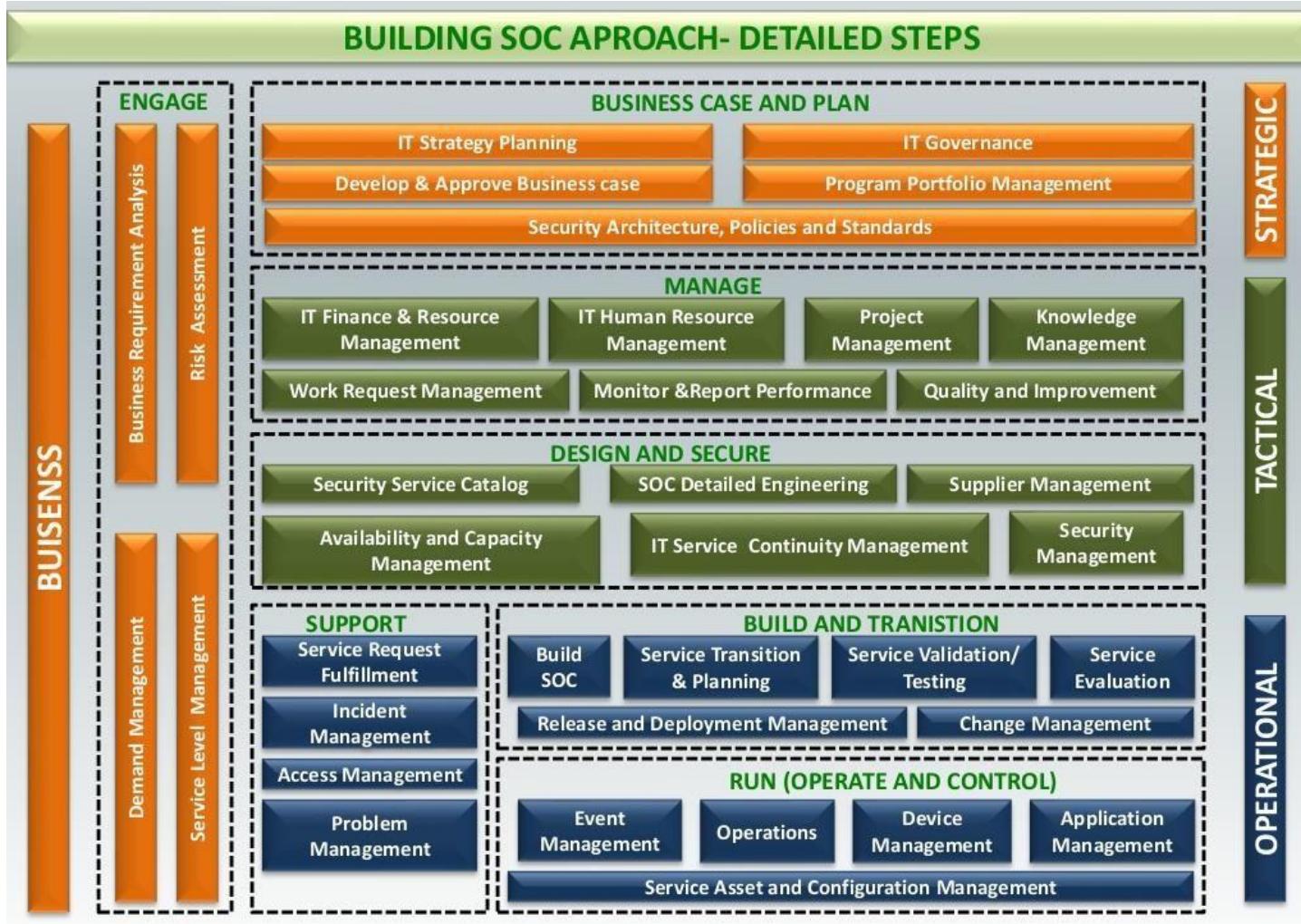
- Comprobación del cumplimiento de políticas, reglas y estándares.
- Detección de cambios en la configuración de los sistemas.
- Detección de vulnerabilidades del servicio.
- Detección de accesos y actividad no autorizados.
- Detección de identidad comprometida, robo y malos usos de información.
- Detección de fuga de información, divulgación y exfiltración de información sensible, protegida o confidencial.
- Detección de ciberataques.
- Detección de infecciones y malware, información corrupta, conexiones no legítimas, consumos de ancho de banda, instalación de software, puertas traseras, etc.



SOC Service Catalogue



BUILDING SOC APROACH- DETAILED STEPS





The Open Source Security Platform

Wazuh is a free, open source and enterprise-ready security monitoring solution for threat detection, integrity monitoring, incident response and compliance.

[Install Wazuh](#)[Free Hosted Trial](#)

Get started with Wazuh

Wazuh provides host-based security visibility using lightweight multi-platform agents.



Wazuh is open source

Flexible, scalable, no vendor lock-in and no license cost. Trusted by thousands of users.



How can we help you?

Wazuh provides professional support, training and consulting services.



Security Analytics



Intrusion Detection



Log Data Analysis



File Integrity Monitoring



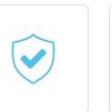
Vulnerability Detection



Configuration Assessment



Incident Response



Regulatory Compliance



Security Analytics

Wazuh is used to collect, aggregate, index and analyze security

Alert level evolution

HIDS... WAZUH - Open Source Host and Endpoint Security.



Wazuh es un sistema de detección de intrusos basado en host (HIDS), de código abierto y libre.

Realiza análisis de registros, comprobación de integridad, supervisión del registro de Windows, detección de rootkits, alertas basadas en el tiempo y respuestas activas.

HIDS... WAZUH - Open Source Host and Endpoint Security.

Proporciona detección de intrusiones para la mayoría de los sistemas operativos, incluidos Linux, OpenBSD, FreeBSD, OS X, Solaris y Windows. Wazuh tiene una arquitectura centralizada y multiplataforma que permite monitorizar y administrar múltiples sistemas.

- <https://github.com/wazuh/wazuh>
- <https://wazuh.com/>
- <https://documentation.wazuh.com/>
- <https://blog.wazuh.com/>

OSSEC, OpenSCAP y Elastic Stack... Descripción de los componentes de WAZUH

<https://documentation.wazuh.com/current/getting-started/index.html>

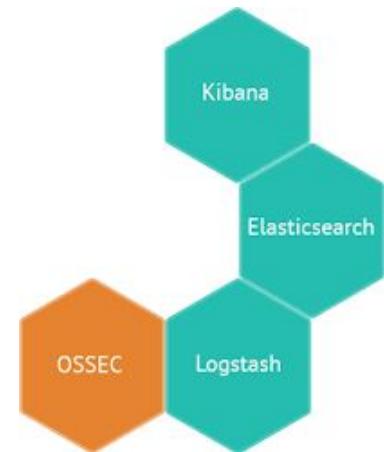
- **OSSEC HIDS** <http://ossec.github.io/> Wazuh es un fork de OSSEC que cumple con los requisitos Del Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS). Se trata de un sistema de detección de intrusos basado en host (HIDS) usado para la detección de seguridad, visibilidad y monitorización del cumplimiento.
- **OpenSCAP** <https://www.open-scap.org/> es OVAL (Open Vulnerability Assessment Language) <https://oval.mitre.org/> y XCCDF (Extensible Configuration Checklist Description Format) <https://scap.nist.gov/specifications/xccdf/> interprete usado para comprobar las configuraciones de sistema y detectar aplicaciones vulnerables.
- **Elastic Stack** <https://www.elastic.co/> es un paquete de software utilizado para recopilar, analizar, indexar, almacenar, buscar y presentar datos de registro.

Elastic Stack... Descripción de los componentes de WAZUH

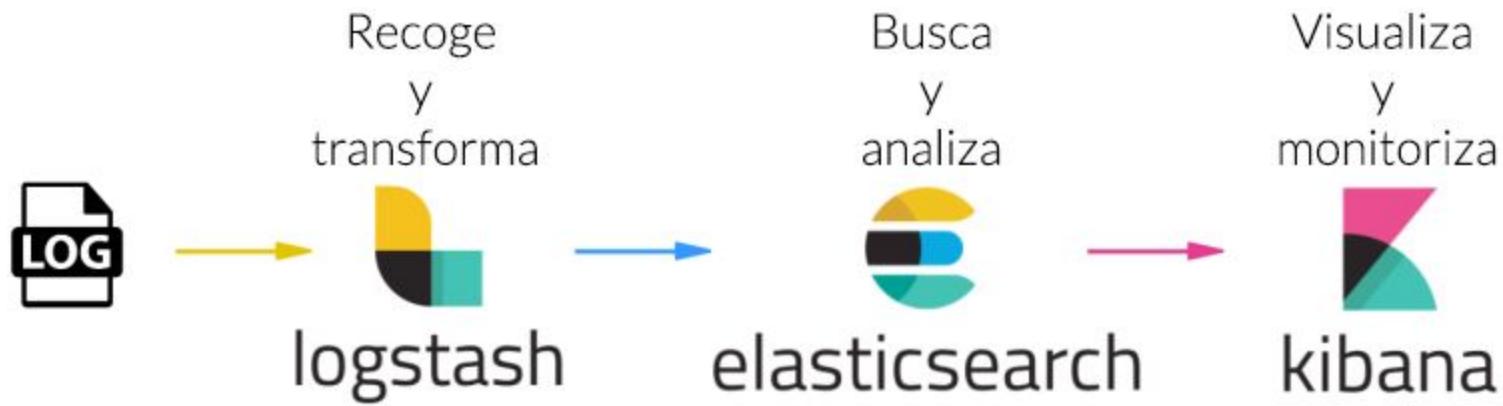


- **Filebeat** (para la extracción de datos de los registros de logs para su envío y centralización.)
 - <https://www.elastic.co/products/beats/filebeat>
 - <https://www.elastic.co/guide/en/beats/filebeat/current/index.html>
 - <https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-getting-started.html>
 - <https://github.com/elastic/beats/tree/master/filebeat>

Elastic Stack... Descripción de los componentes de WAZUH



- **ElasticSearch** <https://www.elastic.co/products/elasticsearch> motor de búsqueda y análisis de texto completo donde se almacenan datos ya optimizados por la indexación. Distribuido, escalable, tolerante a fallos y alta disponibilidad.
- **Logstash** <https://www.elastic.co/products/logstash> es una herramienta para recopilar registros de diferentes fuentes, analizarlos y almacenarlos para su uso posterior.
- **Kibana** <https://www.elastic.co/products/kibana> es un cuadro de mandos o tablero de visualización flexible e intuitivo para la monitorización.
<https://www.elastic.co/guide/en/kibana/current/index.html>



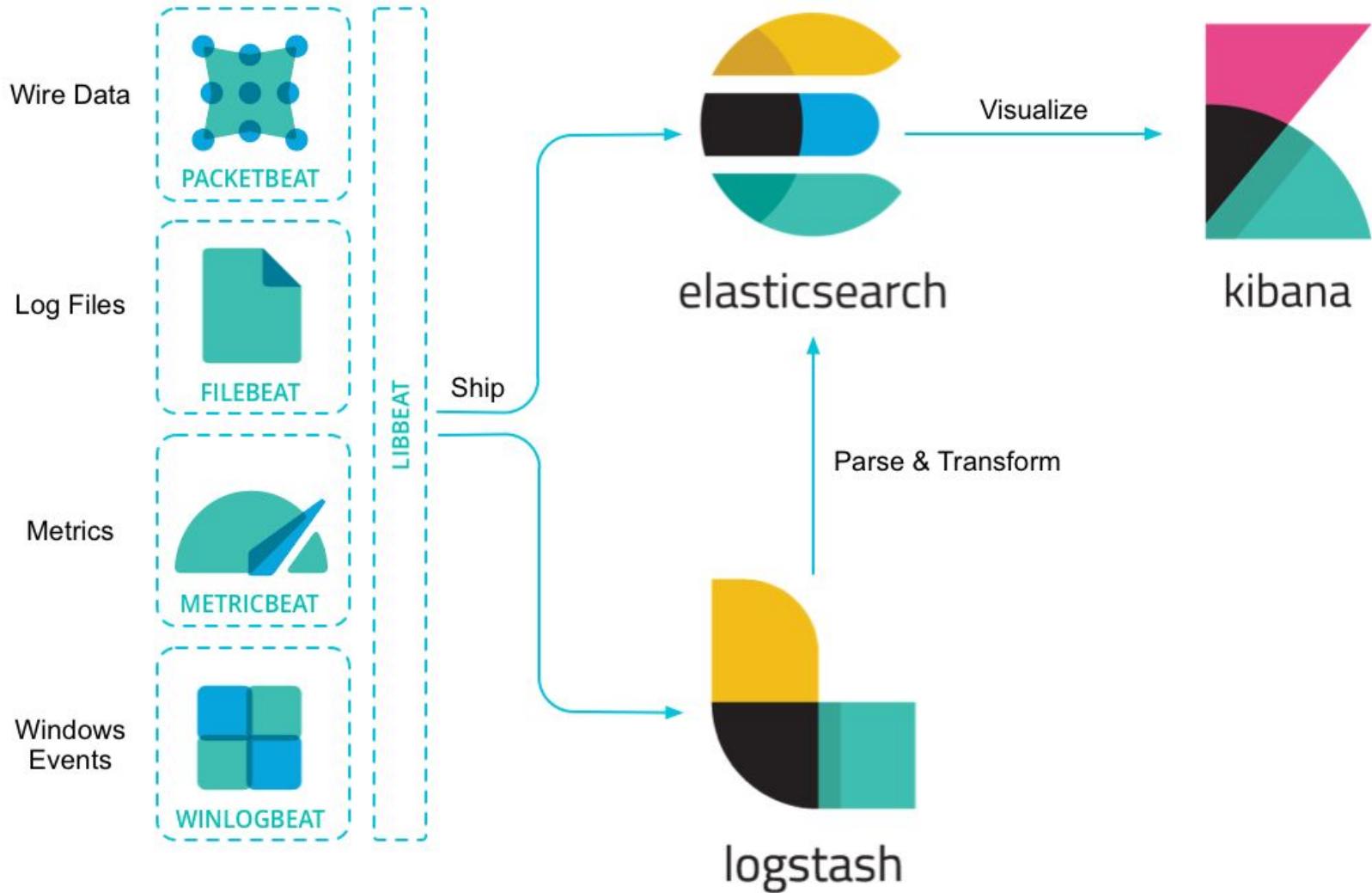
Elastic Stack... Descripción de los componentes de WAZUH

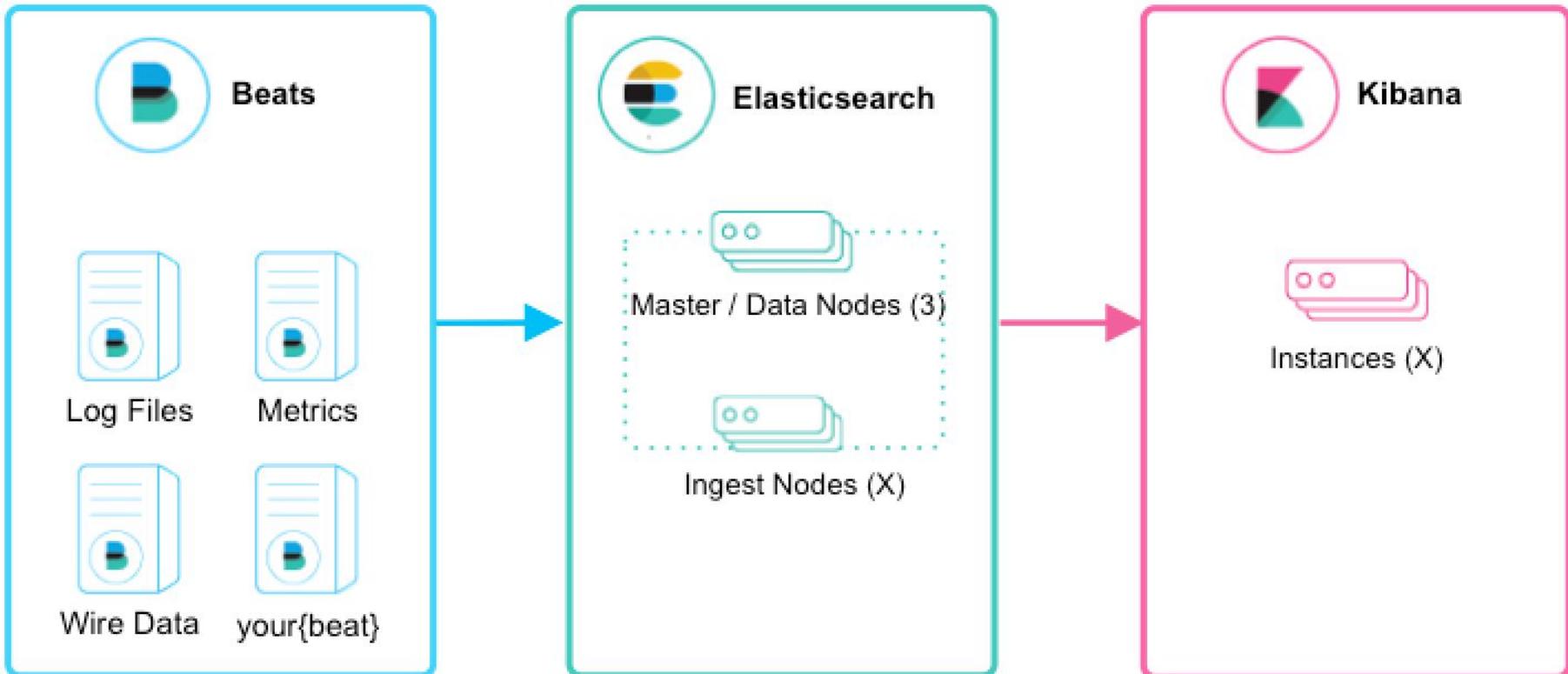
A estos tres pilares (ElasticSearch, Logstash, Kibana) también se le suman dos componentes adicionales:

- **Beats:** <https://www.elastic.co/fr/products/beats> Para la recopilación de datos entre plataformas y puede enviar estos datos a ElasticSearch directamente o a Logstash.
- **X-Pack:** <https://www.elastic.co/products/x-pack> El componente más reciente de la pila ELK ofrece algunos plugins como de seguridad, alertas, monitorización de todo el sistema, grafos y machine learning.

Con la suma de estos dos componentes a la pila ELK ahora el término sería sustituido por lo que conocemos como Elastic Stack.

<https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html>



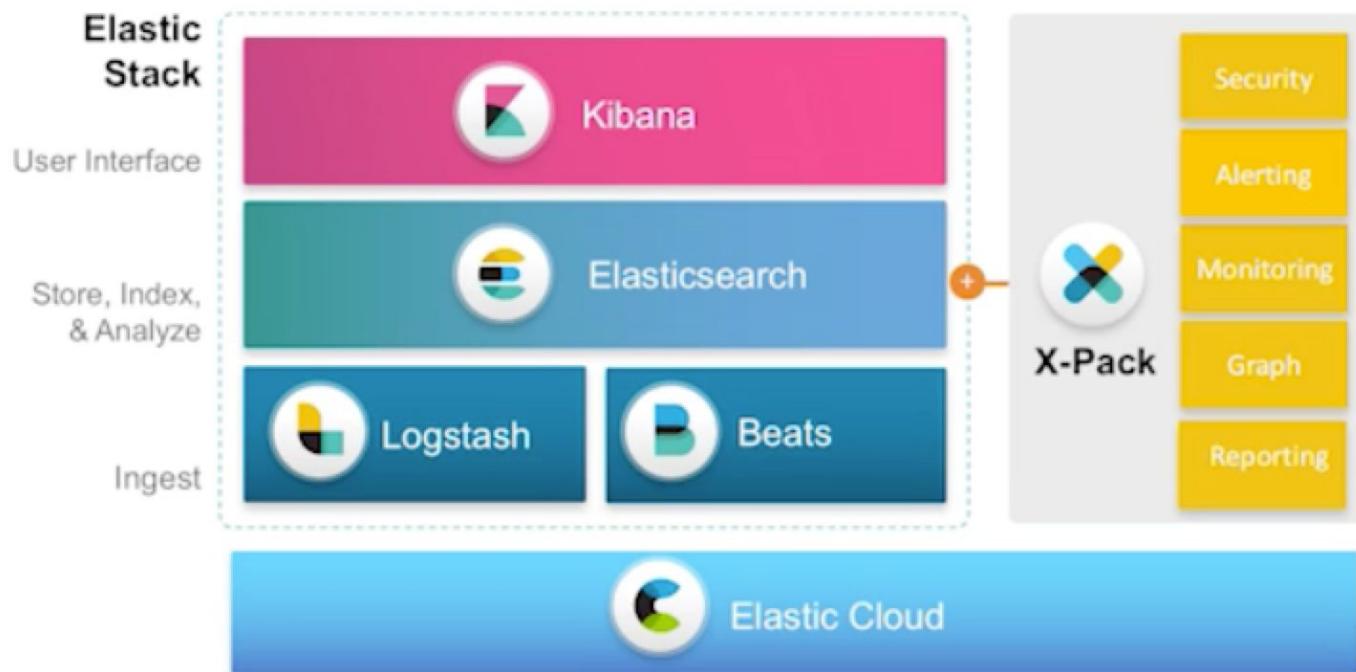


WAZUH... INSTALACIÓN.

<https://documentation.wazuh.com/current/installation-guide/index.html>

- **Servidor Wazuh** (análisis de datos recibidos por los agentes y generación de alarmas cuando un evento coincide con una regla).
- **Elastic Stack** (*Logstash* <https://www.elastic.co/guide/en/logstash/current/index.html>, *Elasticsearch* <https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html>, y *Kibana* <https://www.elastic.co/guide/en/kibana/current/index.html>) es un clúster donde se indexa, almacena y presenta gráficamente la información obtenida.
- **Agentes** de Wazuh ejecutándose en cada hosts. Se utilizan para recopilar diferentes tipos de datos de sistemas y aplicaciones, y detectar problemas de seguridad. El agente envía los datos recopilados al servidor Wazuh a través de un canal cifrado y autenticado. Para establecer este canal seguro, se utiliza un proceso de registro que implica claves precompartidas únicas.

Elastic Products



WAZUH... INSTALACIÓN.

<https://documentation.wazuh.com/current/user-manual/index.html>

- <http://ossec.github.io/docs/>
- <https://logz.io/learn/complete-guide-elk-stack/>





Watching

OSSEC watches it all, actively monitoring all aspects of system activity with file integrity monitoring, log monitoring, rootcheck, and process monitoring. With OSSEC you won't be in the dark about what is happening to your valuable computer system assets.

Alerting

When attacks happen OSSEC lets you know through alert logs and email alerts sent to you and your IT staff so you can take quick actions. OSSEC also exports alerts to any SIEM system via syslog so you can get real-time analytics and insights into your system security events.

Everywhere

Got a variety of operating systems to support and protect? OSSEC has you covered with comprehensive host based intrusion detection across multiple platforms including Linux, Solaris, AIX, HP-UX, BSD, Windows, Mac and VMware ESX.

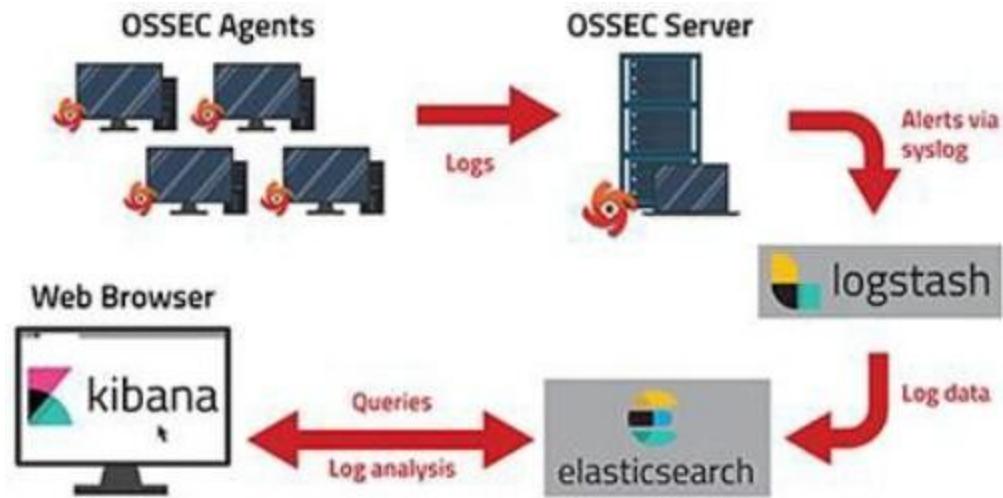
Host Intrusion Detection For Everyone

OSSEC... Open Source HIDS Security.

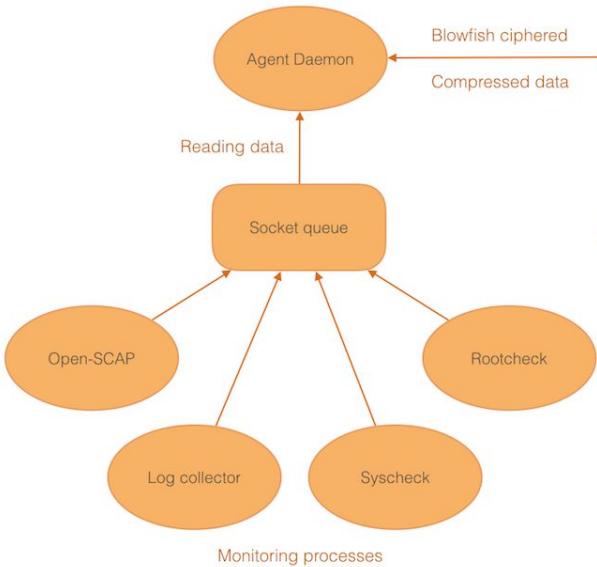
OSSEC <http://www.ossec.net/>, sistema Open Source de detección de intrusiones basado en host (HIDS) y ELK (Elasticsearch, Logstash, and Kibana) como un sistema unificado de información de seguridad y gestión de eventos (SIEM). Se emplea para detectar intrusiones, uso indebido de software, rootkits o configuraciones de seguridad débiles, entre otras cosas.

- <https://github.com/ossec/ossec-hids>
- <http://www.ossec.net/blog.html>
- <http://www.ossec.net/docs/>
- <http://www.ossec.net/downloads.html>
- <https://atomicorp.com/atomic-secured-ossec/>
- <http://github.com/wazuh/ossec-rules>

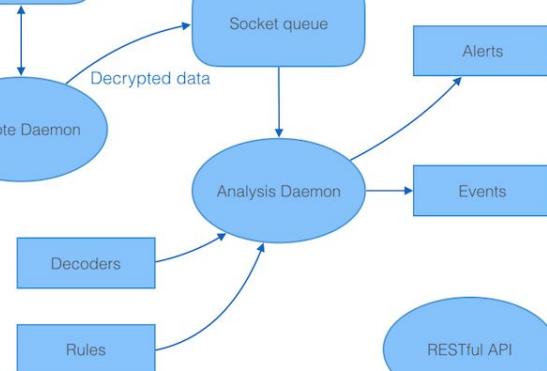




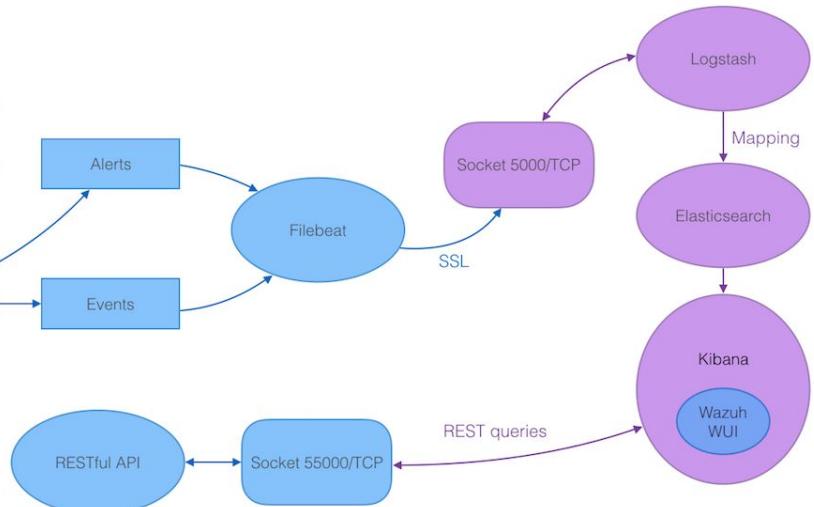
Agent processes

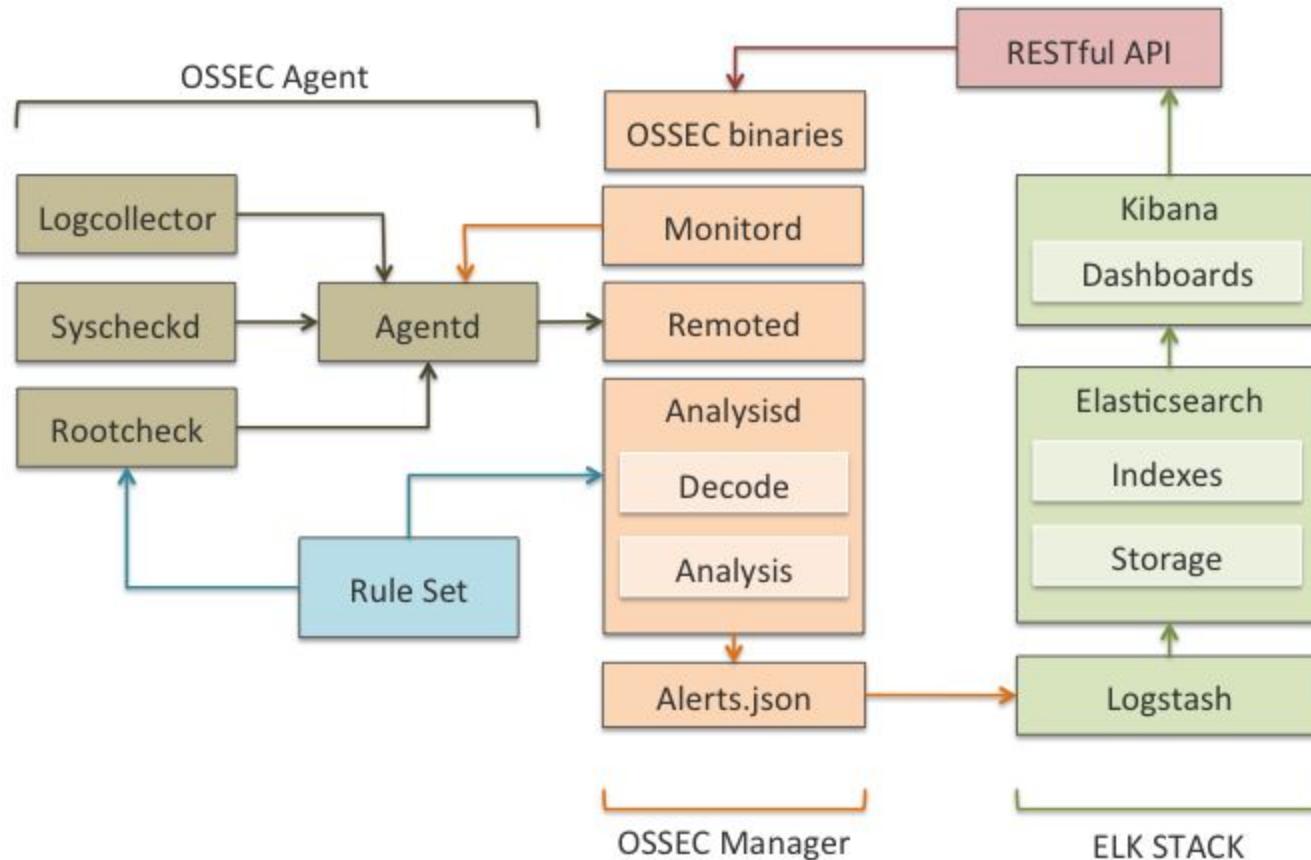


Manager processes



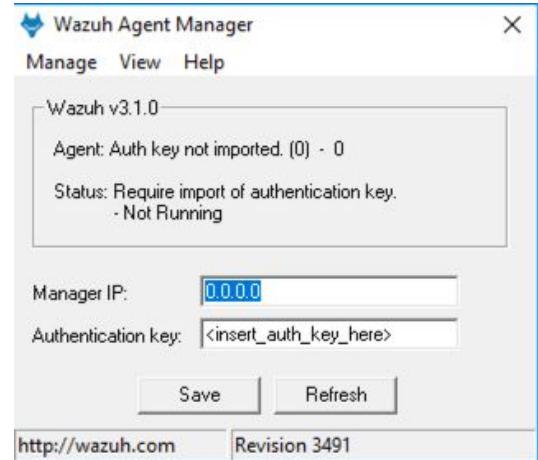
Elastic processes





WAZUH... Agents.

Despliegue de agentes



- <https://documentation.wazuh.com/3.x/deploying-with-ansible/roles/wazuh-agent.html>
- https://documentation.wazuh.com/3.x/installation-guide/installing-wazuh-agent/wazuh_agent_windows.html
- <https://documentation.wazuh.com/3.x/user-manual/registering/index.html>
- <https://documentation.wazuh.com/3.x/deploying-with-ansible/reference.html#wazuh-ansible-reference-agent>
- <https://documentation.wazuh.com/3.x/installation-guide/packages-list/index.html>
- <https://documentation.wazuh.com/3.x/user-manual/capabilities/command-monitoring/command-configuration.htm>

WAZUH... Agents.

Instalación y configuración de los agentes para monitorizar sistemas Windows.

<https://documentation.wazuh.com/3.x/installation-guide/installing-wazuh-agent/index.html>

Los clientes para las diferentes plataformas pueden descargarse desde la url

<https://documentation.wazuh.com/3.x/installation-guide/packages-list/index.html>

<https://blog.wazuh.com/monitoring-usb-drives-in-windows-using-wazuh/>

1041 - vpc-agent-centos-public

ACTIVE

RESTART

vpc-agent-centos-public

X

OVERVIEW

FILE INTEGRITY

POLICY MONITORING

SCAP

AUDIT

PCI DSS

PANELS

DISCOVER

Last 1d

*

Q

vpc-agent-centos-public
Name10.0.0.125
IP AddressWazuh v2.0
VersionLinux vpc-agent-cent...
Operating system2017-05-22 13:22:08
Last keep alive

Top 5 alerts



- ssh: authentication failed
- unix_chkpwd: Password check failed
- PAM: User login failed
- syslog: User missed threshold
- Host-based anomaly detected

Top 5 groups



- syslog
- authentication_failed
- pam
- sshd
- access_control

Top 5 PCI DSS Requirements



- 10.2.4
- 10.2.5
- 10.6.1
- 2.2.4
- 11.4

Alert level evolution



Alerts



Kibana

WAZUH

Overview Management Agents Discover Dev tools ★manager - wazuh-alerts-3.x-* ⚙

Discover Visualize Dashboard Timelion Machine Learning APM Wazuh Graph Dev Tools Monitoring Management elastic Logout Collapse Formatted

Status

| | | | |
|--------------|---|-----------------|--------|
| Active | 6 | Never connected | 0 |
| Disconnected | 1 | Agents coverage | 85.71% |

Top

| | |
|-----------------------|-------------------|
| Last registered agent | manager (manager) |
| Higher activity | ag-windows |

Filter agents...

All states ▾

All OS platforms ▾

All versions ▾

| ID | Name | IP | Status | Group | OS platform | OS version | Agent version |
|-----|------------|------------|--------------|---------|-----------------------------------|-------------|---------------|
| 001 | ag-redhat | 10.0.0.166 | Active | redhat | Red Hat Enterprise Linux Server | 7.5 | Wazuh v3.3.0 |
| 005 | ag-debian | 10.0.0.128 | Active | default | Debian GNU/Linux | 8 | Wazuh v3.3.0 |
| 007 | ag-ubuntu | 10.0.0.152 | Active | default | Ubuntu | 16.04.3 LTS | Wazuh v3.3.0 |
| 008 | ag-centos | 10.0.0.86 | Active | default | CentOS Linux | 7 | Wazuh v3.4.0 |
| 013 | ag-amazon | 10.0.0.159 | Active | default | Amazon Linux AMI | 2017.09 | Wazuh v3.2.2 |
| 016 | ag-windows | 10.0.0.71 | Active | default | Microsoft Windows Server 2016 ... | 10.0.14393 | Wazuh v3.3.0 |
| 017 | ag-macosx | 10.0.0.250 | Disconnected | default | Mac OS X | 10.13.4 | Wazuh v3.2.2 |

WAZUH

- OVERVIEW
- MANAGER
- AGENTS
- DISCOVER
- DASHBOARDS

006 - vpc-agent-windows ACTIVE RESTART

vpc-agent-windows

OVERVIEW FILE INTEGRITY POLICY MONITORING SCAP AUDIT PCI DSS III PANELS DISCOVER Last 7 days

rule.groups:syscheck AND agent.name: vpc-agent-windows AND manager.name: vpc-ossec-manager

wazuh-alerts-* Selected Fields Available Fields

Count

May 20th 2017, 22:02:47.531 - May 27th 2017, 22:02:47.531 — by 3 hours

Time _source

- May 27th 2017, 21:50:19.000: {"syscheck": {"mtime_after": "2017-05-27T21:51:46", "uname_after": "Administrators", "md5_before": "9bd21b6878c0026f44722e4691b935ba", "gid_after": "0", "size_after": "84", "diff": "***** QUEUE\NDIFF\LOCAL\SANTIAGO\BANK_INFORMATION.TXT\state.1495026576\nCredit Card information\ncredit card number: 1111 1111 1111 2222\nBank: Wellsfargo\n*****\nQUEUE\NDIFF\LOCAL\SANTIAGO\BANK_INFORMATION.TXT\LAST-ENTRY\nCredit Card information\ncredit card number: 1111 1111 1111 3333\nBank: Wellsfargo\n*****\n", "mtime_after": "2017-05-17T06:09:36", "path": "C:\Santiago\banks\information.txt", "sha1_after": "1552ed313060bc04690db893b1a36784f0928", "gname_after": "", "uid_after": "0", "event": "modified", "perm_after": "100666", "md5_after": "e84437acf7dc876be62dd0131bab58c", "sha1_before": "82291804f0ab41bc68f3f80018c8768d15d82fa"}, "agent": {"ip": "10.0.0.124", "name": "vpc-agent-windows", "id": "006"}, "manager": {"name": "vpc-ossec-manager"}, "rule": {"firetimes": 1, "pci_dss": ["11.5"], "level": 7, "groups": ["ossec", "syscheck"]}, "description": "Integrity checksum changed.", "id": "559"}, "source": "/var/ossec/logs/alerts/alerts.json", "decoder": {"name": "

May 27th 2017, 21:50:19.000: {"syscheck": {"path": "C:\Santiago\password.txt", "event": "deleted"}, "agent": {"ip": "10.0.0.124", "name": "vpc-agent-windows", "id": "006"}, "manager": {"name": "vpc-ossec-manager"}, "rule": {"firetimes": 3, "pci_dss": ["11.5"], "level": 7, "groups": ["ossec", "syscheck"]}, "description": "File deleted. Unable to retrieve checksum.", "id": "553"}, "source": "/var/ossec/logs/alerts/alerts.json", "decoder": {"name": "syscheck_integrity_changed"}, "full_log": "File 'C:\Santiago\password.txt' was deleted. Unable to retrieve checksum.", "@timestamp": "2017-05-28T04:50:19.000Z", "host": "vpc-ossec-manager", "location": "syscheck", "GeoLocation": {}}

May 27th 2017, 21:49:47.000: {"syscheck": {"path": "C:\Santiago\Santiago.contact", "sha1_after": "8cbe907979919287bf8823831e168a9d919879f0", "uname_after": "Administrators", "gname_after": "", "mtime_after": "2017-05-27T21:51:29", "uid_after": "0", "gid_after": "871", "perm_after": "100666", "event": "added", "md5_after": "9d33d0bd9ff9aa214066c0277468d2e"}, "agent": {"ip": "10.0.0.124", "name": "vpc-agent-windows", "id": "006"}, "manager": {"name": "vpc-ossec-manager"}, "rule": {"firetimes": 3, "pci_dss": ["11.5"], "level": 5, "description": "File added to the system.", "groups": ["ossec", "syscheck"]}, "id": "554", "source": "/var/ossec/logs/alerts/alerts.json", "decoder": {"name": "syscheck_integrity_changed"}, "full_log": "New file 'C:\Santiago\Santiago.contact' added to the file system.", "@timestamp": "2017-05-28T04:49:47.000Z", "host": "vpc-ossec-manager", "location": "syscheck", "GeoLocation": {}}

May 27th 2017, 21:47:56.000: {"syscheck": {"path": "C:\Santiago/New Bitmap Image.bmp", "event": "deleted"}, "agent": {"ip": "10.0.0.124", "name": "vpc-agent-windows", "id": "006"}, "manager": {"name": "vpc-ossec-manager"}, "rule": {"firetimes": 2, "pci_dss": ["11.5"], "level": 7, "groups": ["ossec", "syscheck"]}, "description": "File deleted. Unable to retrieve checksum.", "id": "555"}, "source": "/var/ossec/logs/alerts/alerts.json", "decoder": {"name": "syscheck_integrity_changed"}, "full_log": "File 'C:\Santiago/New Bitmap Image.bmp' was deleted. Unable to retrieve checksum.", "@timestamp": "2017-05-28T04:47:56.000Z", "host": "vpc-ossec-manager", "location": "syscheck", "GeoLocation": {}}

May 27th 2017, 21:47:56.000: {"syscheck": {"path": "C:\Santiago/image.bmp", "sha1_after": "da39a3ee5e6b4b0d3255bfe95601890fd88709", "gname_after": "", "mtime_after": "2017-05-27T21:49:50", "uname_after": "Administrators", "size_after": "0", "uid_after": "0", "gid_after": "0", "event": "added", "perm_after": "100666", "md5_after": "d41d8cd98f00b204e988099secf8427e"}, "agent": {"ip": "10.0.0.124", "name": "vpc-agent-windows", "id": "006"}, "manager": {"name": "vpc-ossec-manager"}, "rule": {"firetimes": 2, "pci_dss": ["11.5"], "level": 5, "groups": ["ossec", "syscheck"]}, "description": "File added to the system.", "id": "554", "source": "/var/ossec/logs/alerts/alerts.json", "decoder": {"name": "syscheck_integrity_changed"}, "full_log": "New file 'C:\Santiago/image.bmp' added to the file system.", "@timestamp": "2017-05-28T04:47:56.000Z", "host": "vpc-ossec-manager", "location": "syscheck", "GeoLocation": {}}

May 27th 2017, 21:47:52.000: {"syscheck": {"path": "C:\Santiago/New Bitmap Image.bmp", "sha1_after": "da39a3ee5e6b4b0d3255bfe95601890fd88709", "mtime_after": "2017-05-27T21:49:50", "gname_after": "", "uid_after": "0", "event": "added", "perm_after": "100666", "md5_after": "d41d8cd98f00b204e988099secf8427e"}, "agent": {"ip": "10.0.0.124", "name": "vpc-agent-windows", "id": "006"}, "manager": {"name": "vpc-ossec-manager"}, "rule": {"firetimes": 2, "pci_dss": ["11.5"], "level": 7, "groups": ["ossec", "syscheck"]}, "description": "File deleted. Unable to retrieve checksum.", "id": "555"}, "source": "/var/ossec/logs/alerts/alerts.json", "decoder": {"name": "syscheck_integrity_changed"}, "full_log": "File 'C:\Santiago/New Bitmap Image.bmp' was deleted. Unable to retrieve checksum.", "@timestamp": "2017-05-28T04:47:52.000Z", "host": "vpc-ossec-manager", "location": "syscheck", "GeoLocation": {}}

WAZUH

OVERVIEW MANAGER AGENTS DISCOVER DASHBOARDS

002 - vpc-agent-centos-public ACTIVE RESUME

OVERVIEW FILE INTEGRITY POLICY MONITORING

vpc-agent-centos-public

PANELS DISCOVER DASHBOARDS

Last 24 hours

agent.name:vpc-agent-centos-public

wazuh-alerts*

Selected Fields

- agent.name
- agent.ip
- rule_id
- rule_level
- rule_description
- rule_group
- full_log

Available Fields

- @timestamp
- @version
- Geolocation.city_name
- Geolocation.country_code
- Geolocation.country_name
- Geolocation.ip
- Geolocation.latitude
- Geolocation.longitude
- Geolocation.region_code
- Geolocation.region_name
- Geolocation.timezone
- _id
- _index
- _score
- _type
- agentid
- decodername
- decoderparent
- offset
- raw
- host
- location
- log
- management
- other
- program_name
- rulefamilies
- rulefrequency
- ruleid
- source
- srcip
- target
- tag
- type

January 3rd 2017, 17:05:27.498 - January 4th 2017, 17:05:27.498 - (23 minutes)

| Time | agent.name | agent.ip | rule.level | rule.description | rule.group | rule.id | full_log |
|--------------------------------|-------------------------|------------|------------|---|---|----------------|---|
| January 4th 2017, 17:05:27.727 | vpc-agent-centos-public | 18.0.0.125 | 10 | Multiple authentication failures. | systlog, attacks, authentication, failures | 18.2.4, 18.2.5 | Jan 5 01:04:45 vpc-agent-centos-public unix_chpasswd[29815]: password check failed for user (root) |
| January 4th 2017, 17:05:38.726 | vpc-agent-centos-public | 18.0.0.125 | 10 | Multiple authentication failures. | systlog, attacks, authentication, failures | 18.2.4, 18.2.5 | Jan 5 01:04:45 vpc-agent-centos-public unix_sudo[29807]: Failed password for root from 58.238.284.132 port 56809 ssh2 |
| January 4th 2017, 17:05:38.726 | vpc-agent-centos-public | 18.0.0.125 | 5 | ssh: authentication failed. | systlog, sshd, authentication, failures | 18.2.4, 18.2.5 | Jan 5 01:04:45 vpc-agent-centos-public sshd[29995]: Failed password for root from 58.238.284.132 port 27179 ssh2 |
| January 4th 2017, 17:05:38.726 | vpc-agent-centos-public | 18.0.0.125 | 10 | systlog User missed the password more than one time | systlog, access_control, authentication, failures | 18.2.4, 18.2.5 | Jan 5 01:04:45 vpc-agent-centos-public sshd[29995]: PM 2 more authentication failures; logname=uid=0 ttyp0 shell=/bin/sh user=root |
| January 4th 2017, 17:05:38.726 | vpc-agent-centos-public | 18.0.0.125 | 5 | unix_chpass: Password check failed. | pm, systlog, authentication, failures | 18.2.4, 18.2.5 | Jan 5 01:04:45 vpc-agent-centos-public unix_chpasswd[29812]: password check failed for user (root) |
| January 4th 2017, 17:05:38.726 | vpc-agent-centos-public | 18.0.0.125 | 10 | Multiple authentication failures. | systlog, attacks, authentication, failures | 18.2.4, 18.2.5 | Jan 5 01:04:45 vpc-agent-centos-public unix_sudo[29807]: Failed password for root from 122.234.223.40 port 62427 ssh2 |
| January 4th 2017, 17:05:38.726 | vpc-agent-centos-public | 18.0.0.125 | 10 | Multiple authentication failures. | systlog, attacks, authentication, failures | 18.2.4, 18.2.5 | Jan 5 01:04:45 vpc-agent-centos-public unix_chpasswd[29812]: password check failed for user (root) |
| January 4th 2017, 17:05:38.726 | vpc-agent-centos-public | 18.0.0.125 | 5 | PM: User login failed. | pm, systlog, authentication, failures | 18.2.4, 18.2.5 | Jan 5 01:04:45 vpc-agent-centos-public sshd[29984]: pm_unix(sshd:auth): authentication failure; logname=uid=0 ttyp0 user=root rhost=122.234.229.48 userroot |
| January 4th 2017, 17:05:28.725 | vpc-agent-centos-public | 18.0.0.125 | 10 | Multiple authentication failures. | systlog, attacks, authentication, failures | 18.2.4, 18.2.5 | Jan 5 01:04:45 vpc-agent-centos-public unix_chpasswd[29810]: password check failed for user (root) |
| January 4th 2017, 17:05:28.725 | vpc-agent-centos-public | 18.0.0.125 | 5 | unix_chpass: Password check failed. | pm, systlog, authentication, failures | 18.2.4, 18.2.5 | Jan 5 01:04:45 vpc-agent-centos-public unix_chpasswd[29809]: password check failed for user (root) |
| January 4th 2017, 17:05:28.725 | vpc-agent-centos-public | 18.0.0.125 | 5 | PM: User login failed. | pm, systlog, authentication, failures | 18.2.4, 18.2.5 | Jan 5 01:04:45 vpc-agent-centos-public sshd[29807]: pm_unix(sshd:auth): authentication failure; logname=uid=0 ttyp0 user=root rhost=58.238.284.132 userroot |
| January 4th 2017, 17:05:28.725 | vpc-agent-centos-public | 18.0.0.125 | 10 | Multiple authentication failures. | systlog, attacks, authentication, failures | 18.2.4, 18.2.5 | Jan 5 01:04:45 vpc-agent-centos-public unix_sudo[29995]: Failed password for root from 58.238.284.132 port 27179 ssh2 |

SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

Existe una gran variedad de opciones para adoptar una solución SIEM, siendo pieza clave para el desarrollo de la actividad diaria en los diferentes modelos de SOC.

El soporte y mantenimiento de las limitaciones de una solución Open Source difiere frente soluciones propietarias basadas en licencias. En el mercado actual encontramos soluciones libres o basadas en un proveedor, disponiendo actualmente de las siguientes opciones mayoritarias:

SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

Security Onion

- <https://securityonion.net/>
- <https://github.com/Security-Onion-Solutions/security-onion/wiki>
- <https://blog.securityonion.net/>



SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

AlienVault Open Source SIEM (OSSIM)

<https://www.alienvault.com/products/ossim>



SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

EMC RSA Security Analytics - Centro de operaciones de seguridad avanzado.

<http://spain.emc.com/security/security-analytics/security-analytics.htm>



The Security Division of EMC

SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

HP ArcSight Enterprise Security Manager (ESM)

<http://www8.hp.com/es/es/software-solutions/arcsight-esm-enterprise-security-management/>



SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

IBM Security QRadar SIEM

<https://www.ibm.com/es-es/marketplace/ibm-qradar-siem>



SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

LogRhythm Security Intelligence Platform

<https://es.logrhythm.com/products/threat-lifecycle-management-platform/>

<https://es.logrhythm.com/>



SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

McAfee Enterprise Security Manager

<https://www.mcafee.com/es/products/enterprise-security-manager.aspx>



SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

SolarWinds Log & Event Manager

<https://www.solarwinds.com/es/siem-security-information-event-management-software>

<https://www.solarwinds.com/es/log-event-manager-software>



SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

Splunk Enterprise

https://www.splunk.com/en_us/software/enterprise-security.html

https://www.splunk.com/es_es/products/splunk-enterprise.html



SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

Lookwise Enterprise Manager

<https://www.s21sec.com/es/lookwise-enterprise-manager/>



SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

Graylog 2

<https://www.graylog.org/>



SIEM... Soluciones Open Source para la Gestión de Eventos e Información de Seguridad.

LOGanalyzer

<http://log analyzer.adiscon.com/>



Top SIEM Vendors

| SIEM VENDOR | THREATS BLOCKED | SOURCES INGESTED | PERFORMANCE | VALUE | IMPLEMENTATION | MANAGEMENT | SUPPORT | SCALABILITY |
|----------------------------------|-----------------|------------------|-------------|-------|----------------|------------|---------|-------------|
| splunk > ES | •••• | ••• | ••• | ••• | •• | ••• | •• | ••• |
| LogRhythm™ ENTERPRISE | ••• | ••••• | ••• | •• | ••• | ••• | ••• | ••• |
| AlienVault USM | ••• | ••• | ••• | ••••• | ••• | •• | •• | ••• |
| MICRO FOCUS ArcSight | •• | ••• | ••• | •• | ••• | ••••• | •• | ••• |
| MICRO FOCUS Sentinel | •• | •• | •• | ••• | ••• | ••• | •• | ••• |
| McAfee ESM | ••• | ••• | ••• | ••• | •• | •• | ••• | ••• |
| Trustwave SIEM | ••• | ••• | ••• | ••• | •• | ••• | •• | ••••• |
| IBM QRadar | ••• | ••• | ••••• | ••• | •• | ••• | ••• | ••• |
| RSA NetWitness | •• | •• | ••• | •• | •• | •• | ••• | ••• |
| solarwinds LEM | •• | ••• | •• | •• | ••••• | •• | ••• | ••• |

SOURCE: eSecurityPlanet.com

Figure 1. Magic Quadrant for Security Information and Event Management



Source: Gartner (August 2016)

Figure 1. Magic Quadrant for Security Information and Event Management



Source: Gartner (December 2017)

© Gartner, Inc

SIEM... Otras opciones **alternativas** para componentes compatibles:

Plataforma de despliegue y gestión de sistemas de contenedores Docker y Kubernetes.

<https://rancher.com/>

<https://github.com/rancher/rancher>



SIEM... Otras opciones **alternativas** para componentes compatibles:

Middleware de mensajería para la negociación de mensajes de código abierto.

- <https://www.rabbitmq.com/>
- <https://www.rabbitmq.com/getstarted.html>
- <https://www.rabbitmq.com/documentation.html>
- <https://www.rabbitmq.com/download.html>
- <https://github.com/rabbitmq/rabbitmq-tutorials>



SIEM... Otras opciones **alternativas** para componentes compatibles:

Sistema para almacenar y compartir información relacionada con los resultados de las pruebas de penetración.

<https://dradisframework.com/ce/>

<https://dradisframework.com/ce/documentation/>

<https://github.com/dradis/dradis-ce>



SIEM... Otras opciones **alternativas** para componentes compatibles:

Aplicación para el inventariado, auditoría, documentación y gestión de redes.

<https://www.open-audit.org/>

<https://github.com/Opmantek/open-audit>

<https://community.opmantek.com/display/OA/Home>



SIEM... Otras opciones **alternativas** para componentes compatibles:

Soluciones automáticas de informes, logs y alertas.

<https://www.skedler.com/>

<https://www.skedler.com/documentation/>



SIEM... Otras opciones **alternativas** para componentes compatibles:

Gestión y compartición inteligencia de amenazas.

<https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/minemeld>

<https://github.com/PaloAltoNetworks/minemeld>

<https://github.com/PaloAltoNetworks/minemeld/wiki>



SIEM... Otras opciones **alternativas** para componentes compatibles:

Análisis y visualización de métricas en tiempo real.

<https://grafana.com/>

<https://github.com/grafana/grafana>



SIEMonster <https://siemonster.com/>



<https://kb.siemonster.com/help/get-started-with-knowledgeowl>

SIEMonster V3 Virtual Machine Build Guide

<https://kb.siemonster.com/help/siemonster-v3-virtual-machine-build-guide>

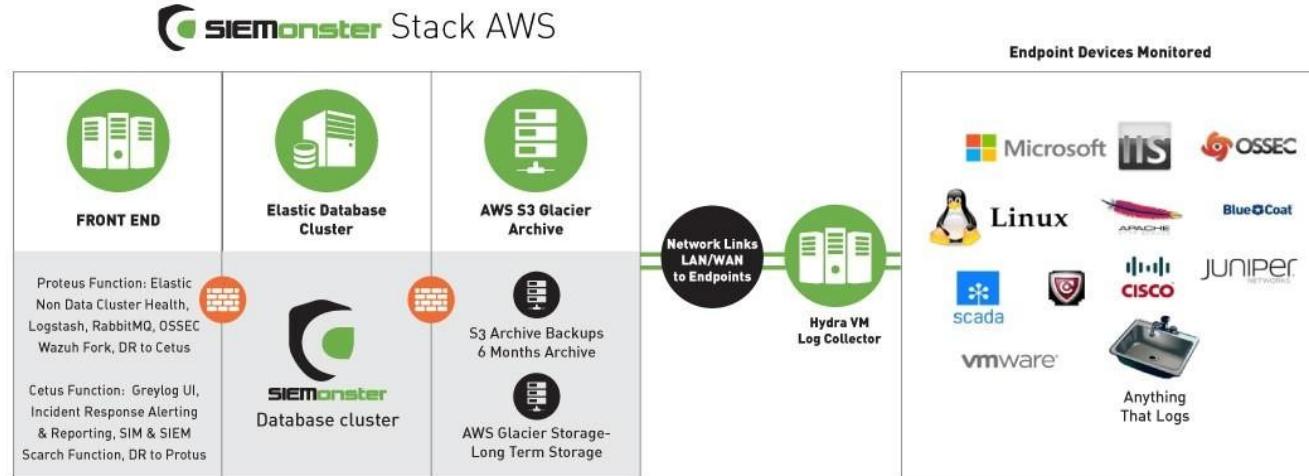
<https://dyzz9obi78pm5.cloudfront.net/app/image/id/5a6d75cd8e121c965f7a7a8c/n/siemonster-v3-vm-build-guide-v18.pdf>

SIEMonster

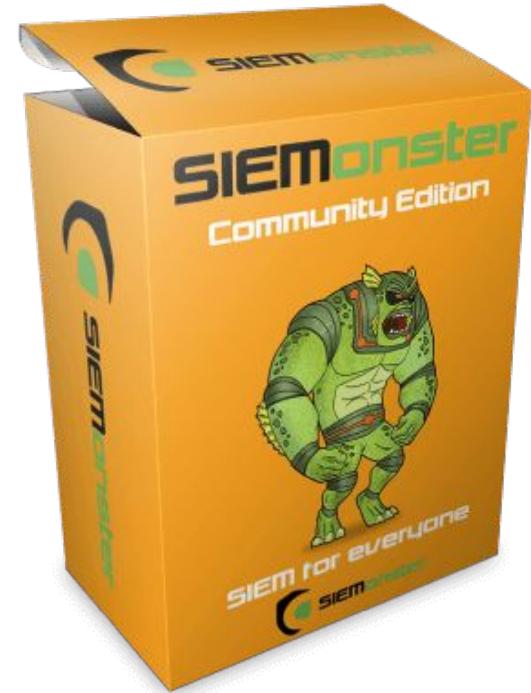
SIEMonster <https://siemonster.com/>

SIEMonster Operations Guide <https://kb.siemonster.com/help/siemonster-operations-guide>

<https://dyzz9obi78pm5.cloudfront.net/app/image/id/5a5c82378e121c3358a273cf/n/siemonster-v3-operations-guide-v11.pdf>



SIEMonster <https://siemonster.com/>



SIEMonster High Level Design

<https://kb.siemonster.com/help/siemonster-high-level-design>

<https://dyzz9obi78pm5.cloudfront.net/app/image/id/5a5bfa2d6e121cc31ab45a9d/n/siemonster-v3-high-level-design-v14.pdf>

SIEMonster is an Affordable Security Monitoring Software Solution

With the Scalability & the Features
of More Expensive Solutions

[LEARN MORE](#)

See what **SIEMonster** can do [Watch Demo](#)



SIEMonster Features



Human Based Behavior
SIEMonster now provides Human Based behavior correlation options to enrich your alerts and minimize false positives.



Threat Intelligence
SIEMonster provides real time Threat intelligence with commercial or opensource feeds to stop real time attacks.



Deep Learning
Using Machine Learning, Human Based Behavior analytics watch SIEMonster Deep Learning kill the attacks automatically.



SMB & Enterprise
Whether you're a SMB, Enterprise or Managed Security Service Provider, SIEMonster has the scalable solution for you.



Cloud or Onsite
SIEMonster allows you to run, onsite in a VM, Bare metal or any of the Cloud providers such as Amazon, GCP or Azure.

[Learn more ➔](#)[Learn more ➔](#)[Learn more ➔](#)[Learn more ➔](#)[Learn more ➔](#)

SIEMonster V3.0 out now [Download Now](#)



PRODUCTS

DOWNLOADS

SUPPORT

CONTACT SALES

NEWS

PARTNERS

ABOUT US



What is SIEMonster.
Introduction video on
what
is SIEMonster.



SIEMonster OSINT.
SIEMonster's Open
Source integrated
Threat Intelligence.



SIEMonster Demo.
Video on how the
dashboard and other
elements work.



**SMB-Enterprise
Demo.**
A detailed
walkthrough video
about SIEMonster V4.

[PRODUCTS](#) ▾[DOWNLOADS](#)[SUPPORT](#) ▾[CONTACT SALES](#)[NEWS](#)[PARTNERS](#)[ABOUT US](#)

You can have your very
own SIEMonster

Send me a Monster!

[Purchase Now](#)





Welcome to the SIEMonster Knowledge Base

Search for articles...



Documents

Videos

Wishlist

Popular Articles

- [SIEMonster V3 Virtual Machine Build Guide](#)
- [SIEMonster High Level Design](#)
- [SIEMonster Operations Guide](#)
- [SIEMonster V3 Bare Metal Build Guide](#)
- [SIEMonster Version 3 DIY VM Install Video Step by Step](#)
- [See more...](#)

New Articles

- [SIEMonster Version 3 DIY VM Install Video Step by Step](#)
- [SIEMonster V3 Amazon AWS Build Guide](#)
- [SIEMonster V3 VM Image Builder](#)
- [SIEMonster V3 Bare Metal Build Guide](#)
- [Wishlist via Trello](#)
- [See more...](#)

Updated Articles

- [SIEMonster Version 3 DIY VM Install Video Step by Step](#)
- [SIEMonster V3 Virtual Machine Build Guide](#)
- [SIEMonster V3 Bare Metal Build Guide](#)
- [SIEMonster V3 Amazon AWS Build Guide](#)
- [SIEMonster High Level Design](#)
- [See more...](#)

SIEMonster <https://siemonster.com/>

Presentando a los Monstruos:

- *Makara*: Rancher, Servidor de Orquestación, Ingestion Server.
- *Proteus* (Proteo): Servidor de Aplicación, Ingestion Server. (Logstash, SyslogNG, RabbitMQ, OSSEC, Wazuh.)
- *Capricorn*: Servidor de Aplicación. (411 Alerts, Kibana, Reporting, OSINT, Health Monitor, Event Monitor, Incidence Response FIR (Ticketing).)
- *Kraken*: Elasticsearch.
- *Tiamat*: Elasticsearch.
- *Ikuturso* (Iku Turso)
- *Hydra* (Hydra of Lerna)

SIEMonster <https://siemonster.com/> Funciones de los monstruos:

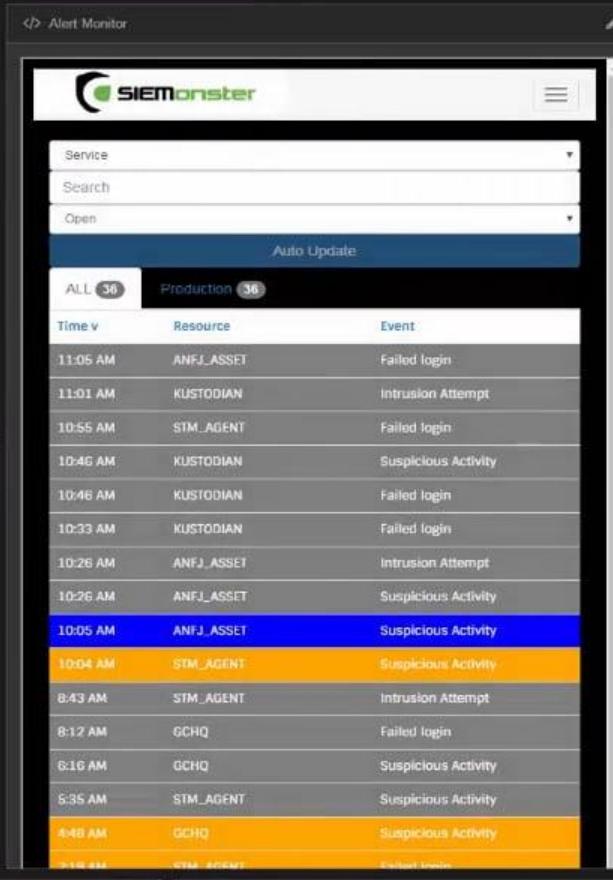
- **Makara:** Planificación y coordinación del Rancher (Plataforma de software de código abierto que permite ejecutar contenedores en producción a las organizaciones), aplicación front-end web, servidor NFS y análisis y procesamiento de registro de eventos desde la cola de mensajes RabbitMQ antes de pasar al nodo ES Client 1 Elastic.
- **Proteus (Proteo):** Ingerir y procesar datos de endpoint entrantes y reenviar al intermediario de mensajes RabbitMQ y proporcionar alojamiento para cualquiera de las aplicaciones agrupadas. Recibe los registros de los Windows, Linux, aplicaciones y hardware que proporciona el syslog. Los agentes proporcionan encriptación TLS / SSL usando diferentes certificados.
- **Capricorn:** Elastic Client Node 2 y proporciona alojamiento para cualquiera de las aplicaciones agrupadas.
- **Kraken:** Cluster Node 1 Elastic que almacena todos sus datos SIEM a largo plazo en la base de datos proporcionando redundancia para Tiamat Cluster Node 2.
- **Tiamat:** Cluster Node 2 Elastic que almacena todos sus datos SIEM a largo plazo en la base de datos proporcionando redundancia para Kraken Cluster Node 1.
- **Ikuturso (Iku Turso):** Es un sensor de red alejado de SIEM que se encuentra en una DMZ o borde de red, ejecutando BRO, LOGSTASH, RabbitMQ, Suricata con la capacidad de bloquear el tráfico conocido utilizando Threat Intelligence. También proporciona capacidades forenses de ataques conocidos con aplicaciones e inspección de paquetes de red.
- **Hydra (Hydra of Lerna):** Servidor de recopilación de registros en el sitio del cliente que envía de forma segura los datos recopilados a SIEMonster MSSP para su procesamiento y almacenamiento.

SIEMONSTER

Discover Visualize Dashboard Settings

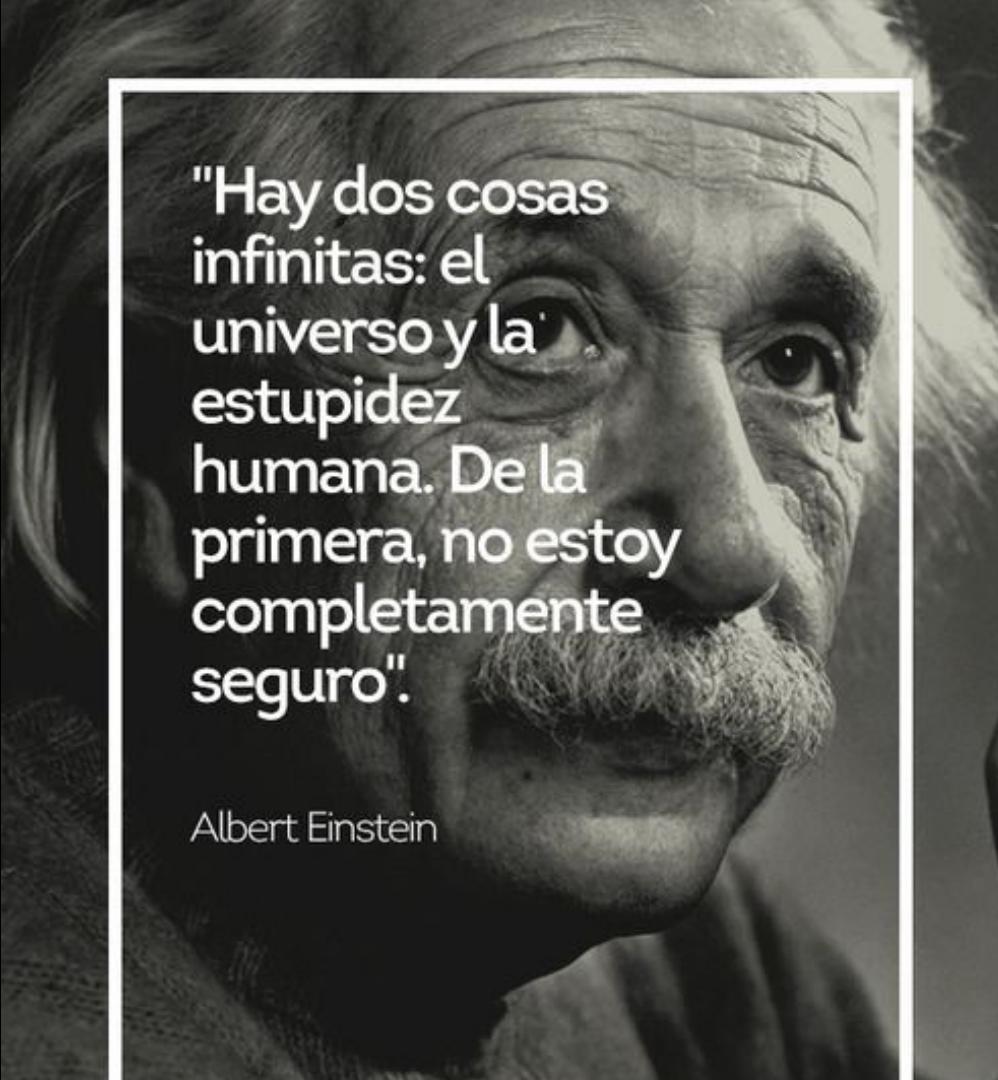
© 1-241

Review-Demo



Recomendaciones clave

A photograph of a person's hand reaching upwards from the bottom center of the frame. The hand is positioned as if it is about to grasp a single key from a group of many keys hanging by strings from the top edge of the frame. The background is a dark, solid color. The lighting is dramatic, coming from the side to highlight the hand and the metallic keys.

A black and white close-up photograph of Albert Einstein's face. He has his signature wild, wavy hair and a full, bushy white beard. His gaze is directed towards the right of the frame, and he has a thoughtful, slightly weary expression. The lighting is dramatic, highlighting the texture of his skin and the contours of his face.

"Hay dos cosas
infinitas: el
universo y la
estupidez
humana. De la
primera, no estoy
completamente
seguro".

Albert Einstein

“El 90%
del éxito
se basa
simplemente
en
insistir”



Woody Allen

Principios básicos de Ciberseguridad...

- **Actualización constante.** Parcheo de vulnerabilidades para mitigar el riesgo permanente. Sistemas antimalware.
- **Bastionado o fortificación.** Control y filtrado de accesos. Hardening. Configuraciones adecuadas que permitan un funcionamiento seguro del sistema. Medidas de Resiliencia avanzadas que nos permitan seguir proporcionando los servicios críticos de nuestra organización en un entorno altamente degradado.
- **Concienciación y Ciberinteligencia.** Convirtiendo una amenaza desconocida en una conocida. Capacidad interna de análisis para la obtención de unos indicadores de compromiso (IOC) e indicadores de ataque (IOA), que nos permitan detectar con tiempo y en la forma adecuada, un posible compromiso de seguridad de nuestros sistemas, logrando así adelantarnos al atacante. Sistemas IDS/IPS. Mecanismos de detección de acciones anómalas, o maliciosas. Adaptación a una amenaza cambiante.
- **Defensa Activa.** Evolución de las amenazas y sobre la percepción de dichas amenazas. Proactivo, cambiando de estrategia sobre la marcha y adaptación dinámica a la amenaza desconocida compleja, numerosa y cambiante. Estrategias de monitorización, detección, protección, mitigación y remediación, más efectivas y adaptadas a la amenaza en cada momento.


[Inicio](#) | [Avisos](#) | [Incidentes](#) | [Reportar una vulnerabilidad](#) | [Alertas](#) | [Publicaciones](#) | [Intercambio de amenazas](#) | [Otras actividades](#) | [Sobre BCSC](#)

Libro blanco de la ciberseguridad en Euskadi


 26/12/2018 | [in](#) [Twitter](#) [f](#) | [PDF](#) [DOCX](#) | [RSS](#)
Se han catalogado 109 organizaciones en el ámbito de la ciberseguridad en Euskadi.

Aunar en un mismo territorio, una fuerte demanda de servicios de ciberseguridad y una completa oferta de soluciones está permitiendo posicionar a Euskadi como un ecosistema muy interesante para la inversión y el emprendimiento a nivel internacional.

Hoy en día, la adopción tecnológica por parte de la sociedad ha supuesto un desafío para los sectores público y privado que han tenido que involucrarse en los avances actuales para poder satisfacer los nuevos requerimientos de la sociedad y el mercado, debido a que las nuevas tecnologías se integran en su desarrollo con una celeridad cada vez mayor.

La adopción de las nuevas tecnologías ha traído consigo la transformación digital de la sociedad, organizaciones públicas y empresas, y junto a dicha transformación, la aparición de nuevas amenazas y riesgos.

La propia Comisión Europea, con el objetivo de minimizar los impactos de las nuevas amenazas y riesgos en la Unión Europea (UE), marca una estrategia de ciberseguridad que tiene como objetivos impulsar los valores europeos de libertad y democracia y velar por un crecimiento seguro de la economía digital. Para ello, recientemente ha aprobado diversas regulaciones y directivas entre las que destaca la Directiva NIS, cuyo objetivo es reforzar la ciberresiliencia de los sistemas informáticos, reduciendo los impactos de la delincuencia en la red y fortaleciendo la política de ciberseguridad y ciberdefensa internacional de la UE.

Por otro lado, el nuevo Reglamento General de Protección de Datos (UE) 2016/679, (en adelante GDPR), aprobado el pasado 27 de abril por el Parlamento Europeo, ha supuesto un nuevo marco jurídico en materia de protección de datos para toda la Unión Europea. Dicho reglamento refuerza los principios de privacidad y regula nuevos derechos para los afectados y nuevas obligaciones; todo ello, sobre la base del nuevo principio de responsabilidad proactiva y de rendición de cuentas, que impone a las entidades cuyas operaciones impliquen el tratamiento de datos personales un deber de diligencia.

Dentro de este contexto, **Euskadi**, como ejemplo de sociedad moderna y avanzada, se encamina hacia un modelo de mayor cohesión social, **seguridad y resiliencia**. Por ello, gracias al impulso del Gobierno Vasco, se implantó el **Basque CyberSecurity Centre**, (en adelante, BCSC o el Centro), que se enmarca organizativamente en la Agencia Vasca de Desarrollo Empresarial (en adelante SPR), dentro de la Sociedad Para La Transformación Competitiva - Eráldakera Lehiakorrerako Sozietatea S.A. (en adelante Grupo SPR), sociedad dependiente del Departamento de desarrollo Económico e Infraestructuras del Gobierno.

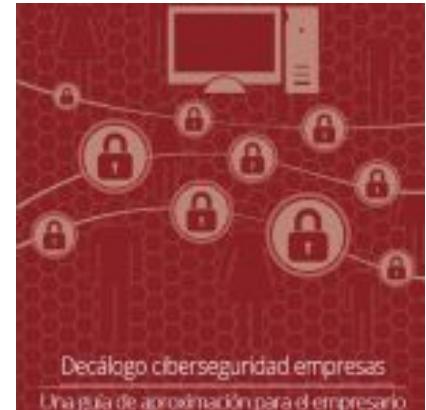
Para tener una primera imagen de la situación general del ecosistema vasco de ciberseguridad, se ha elaborado el presente **estudio** que muestra un análisis del sector de la ciberseguridad incluyendo aspectos clave como perspectivas y oportunidades del sector y el detalle de la situación actual de las **organizaciones dedicadas a la ciberseguridad existentes en Euskadi**.

El documento está disponible en el siguiente enlace. La infografía puede ser consultada aquí.

Referencias:

Decalogue of cybersecurity for Business.

Decálogo de la ciberseguridad empresarial.



Diez pasos imprescindibles que has de tomar para ser una pyme cibersegura y de ese modo promover la confianza en tu negocio.

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf

Referencias:

Glossary of technical terms used in cybersecurity.

Glosario de términos técnicos utilizados en ciberseguridad.



Siglas y acrónimos, extranjerismos, calcos y préstamos lingüísticos.

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

Referencias:

- Cloud computing https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-cloud-computing_0.pdf
- BYOD (Bring Your Own Device). https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_dispositivos_moviles_metad.pdf
- RANSOMWARE. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware_metad.pdf
- Secure deletion of confidential information.
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_borrado_seguro_metad_0.pdf
- Biometric technologies applied to cybersecurity.
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf
- Secure storage (and retrieval) of information.
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_almacenamiento_seguro_metad_0.pdf
- Corporate digital identity cybersecurity and online reputation.
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_identidad_online_metad_0.pdf
- How to handle the leak of sensitive and confidential information.
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_fuga_informacion_0.pdf
- Cybersecurity and Risk Management.
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_0.pdf
- CyberSecurity for e-business.
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_comercio_electronico_metad_0.pdf

Referencias:

- Código de Derecho de la Ciberseguridad.
https://www.boe.es/legislacion/codigos/abrir_pdf.php?fich=173_Codigo_de_Derecho_de_la_Ciberseguridad.pdf
- Oficina de seguridad del internauta <https://www.osi.es>
- Incibe, instituto de ciberseguridad <https://www.incibe.es/>
<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2856-ccn-cert-ia-09-18-ciberamenazas-y-tendencias-2018-resumen-ejecutivo-2018/file.html>
- Centro Vasco de Ciberseguridad <https://www.basquecybersecurity.eus/es/>
- Red de Excelencia de Investigación en Ciberseguridad <https://www.renic.es/es>
- Centro criptológico <https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html>
- Centro de protección de infraestructuras críticas <http://www.cnpic.es/>
- Dpto. de Seguridad <http://www.dsn.gob.es/>
- Privacidad y Protección de datos <https://www.aepd.es/guias/index.html>


[Inicio](#) | [Avisos](#) | [Incidentes](#) | [Reportar una vulnerabilidad](#) | [Alertas](#) | [Publicaciones](#) | [Intercambio de amenazas](#) | [Otras actividades](#) | [Sobre BCSC](#)

Ciberseguridad Industrial en Euskadi

ACTUALIDAD BCSC



102 empresas vascas reciben las primeras ayudas del Gobierno Vasco para impulsar la ciberseguridad industrial

102 empresas, 56 guipuzcoanas, 25 vizcainas y 21 alavesas, se beneficiarán este año del programa de ayudas del Gobierno Vasco para impulsar la ciberseguridad industrial pionero en nuestro entorno y que, impulsadas por el Grupo SPII, tenía una partida inicial de 600.000 euros y se ha ampliado hasta el millón de euros ante la fuerte demanda por parte de las empresas. Esta inversión pública va a servir para promover una inversión privada en ciberseguridad que alcanza los 2,34 millones euros.



Libro blanco de la ciberseguridad en Euskadi

Hoy en día, la adopción tecnológica por parte de la sociedad ha supuesto un desafío para los sectores público y privado que han tenido que involucrarse en los avances actuales para poder satisfacer los nuevos requerimientos de la sociedad y el mercado, debido a que las nuevas tecnologías se integran en su desarrollo con una celeridad cada vez mayor.



BCSC colabora con la Diputación Foral de Álava y la Cámara de Comercio de Álava en la concienciación en ciberseguridad en empresas

Uno de los principales objetivos del Centro Vasco de Ciberseguridad (CVCS) es elevar el nivel de medidas en ciberseguridad de la sociedad vasca en todos sus estratos, incluidas las empresas. Perseguindo dicho objetivo, BCSC ha colaborado en la organización de la jornada 'La Ciberseguridad en las empresas alavesas', en colaboración con la Diputación Foral de Álava y la Cámara de Comercio de Álava. Con esta, son ya 17 las jornadas de concienciación impulsadas por el Centro en lo que va de año, con la asistencia de más de 500 profesionales.

[Ver todas las noticias...](#)

Copias de seguridad: una guía de aproximación para el empresario

Esta guía pretende dar a conocer los aspectos más relevantes de las copias de seguridad para ayudarte a comprender tanto su importancia, como las distintas soluciones aplicables dependiendo de nuestro modelo de negocio.

[Descarga la guía](#)

Protege tu empresa ▾ Eventos ▾ Otras actividades ▾ Qué es INCIBE ▾



protege
tuempresa

NO CONVIERTAS
LA TECNOLOGÍA
EN UN MAL SUEÑO



Cifrado seguro de correo electrónico con PGP

Explicación sobre cómo mantener la confidencialidad, integridad y autenticidad en las comunicaciones mediante la implantación del estándar PGP. Se presenta de una manera simple la utilización de este estándar, a través de los clientes de correo electrónico Microsoft Outlook y Thunderbird.

[Más información](#)[Alerta](#) [Incidentes](#) [Servicios](#) [Publicaciones](#) [Sobre INCIBE-CERT](#)

Reporte de incidentes



Avisos

- ◆ Fuga de credenciales Wi-Fi en routers Livebox de Orange
28/12/2018
- ◆ Múltiples vulnerabilidades en productos de WIBU-SYSTEMS
21/12/2018
- ◆ Vulnerabilidad de inserción de archivos en Kibana
21/12/2018

[Ver más](#)

Avisos SCI

- ◆ Corrupción de memoria en Zelio Soft de Schneider Electric
28/12/2018
- ◆ Múltiples vulnerabilidades en productos de Schneider Electric
26/12/2018
- ◆ Denegación de servicio en el controlador Vnet/IP Open Communication de Yokogawa
21/12/2018

[Ver más](#)



Oficina
de Seguridad
del Internauta

[¿Quiénes somos?](#) [Encuesta de valoración](#) [Contacto](#) [Boletines](#)

[Ponte al día](#) [Campañas](#) [Protégete](#) [Recursos](#) [Soporte técnico](#) [Juegos educativos](#) [IS4K](#)

Buscar



GUÍA DE PRIVACIDAD Y SEGURIDAD EN INTERNET

[Descargar la guía](#)



incibe_
INSTITUTO NACIONAL DE
LA CONFIANZA Y LA
SEGURIDAD

OSI
Oficina
de Seguridad
del Internauta

Historias reales

“

No hagas clic en todo lo que lees

”



Referencias:

- CSIRT: Computer Security Incident Response Team. <https://www.csirt.es/> Asociación independiente y sin ánimo de lucro compuesto por los equipos de respuesta a incidentes de seguridad CSIRT/CERT, sean públicos o privados.
<https://www.csirt.es/index.php/es/miembros>
- CSIRT-kit <http://www.csirt-kit.org/> es una imagen ova de máquina virtual para equipos de respuesta a incidentes.
- TF-CSIRT <https://www.trusted-introducer.org/>
- ENISA <https://www.enisa.europa.eu/> Agencia de Seguridad de las Redes y de la Información
- CERT (Computer Emergency Response Team) <https://www.cert.org/>
- CERT de Seguridad e Industria <https://www.incibe-cert.es/guias-y-estudios>
- Industrial Control Systems Cyber Emergency Response Team <https://ics-cert.us-cert.gov/>

Referencias:

- CERT-EU <https://cert.europa.eu/>
- European Government CERTs group <http://www.egc-group.org/>
- FIRST <https://www.first.org/> foro global de respuesta a incidentes.
- Unifying the global response to cyber crime <https://apwg.org/>
- NIST <https://www.nist.gov/> Instituto de Estándares y Tecnología.
- SANS Institute <https://www.sans.org/security-resources/>

Referencias: Sistemas de Control Industrial

<https://www.cci-es.org/>

<https://www.incibe-cert.es/>

<https://ics-cert.us-cert.gov/>

<https://www.incibe.es/>

<https://www.basquecybersecurity.eus/>



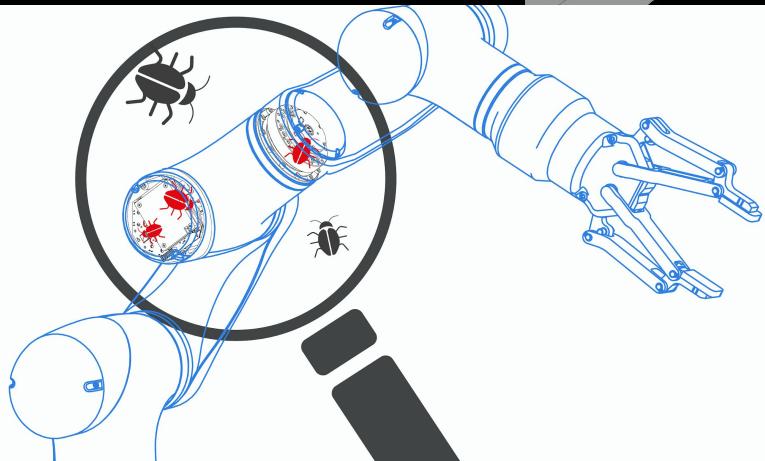
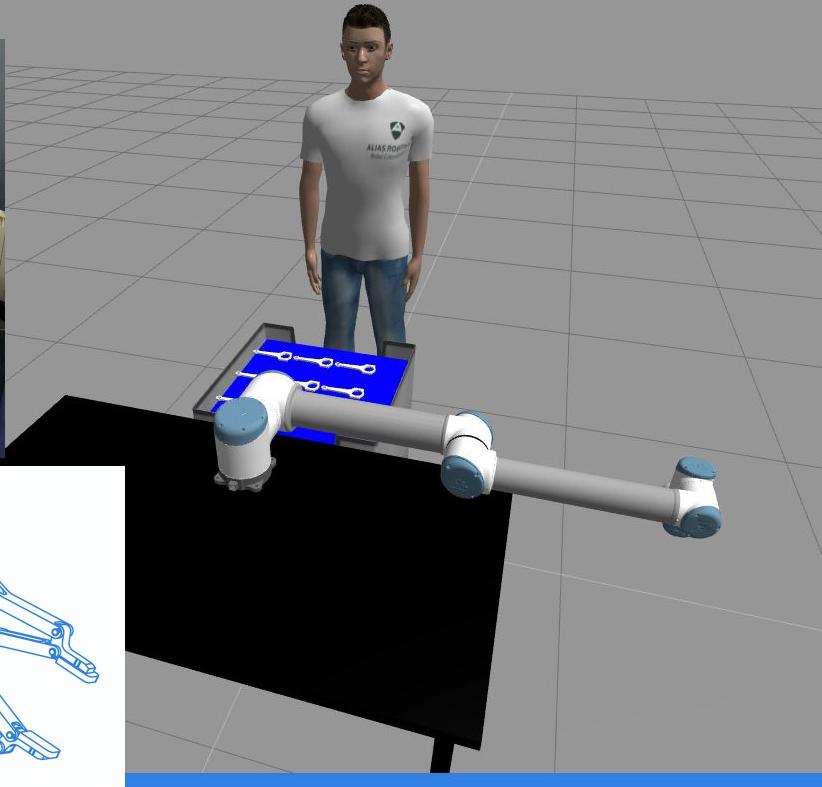


STOP SCENARIO



Scenario4:
Even if collaborative robots are fun to play with,
if they are out of control, they can be dangerous too!
Try to hit the worker with the robot in order to get the flag.

```
*****  
* Wait until the scenario becomes ready *  
*****  
root@39e98683c99d:~# rostopic list  
/ariac/logical_camera  
/arm_controller/command  
/arm_controller/follow_joint_trajectory/cancel  
/arm_controller/follow_joint_trajectory/feedback  
/arm_controller/follow_joint_trajectory/goal  
/arm_controller/follow_joint_trajectory/result  
/arm_controller/follow_joint_trajectory/status  
/arm_controller/state  
/attached_collision_object  
/calibrated  
/calibrated_point  
/clock  
/collision_object  
/execute_trajectory/cancel  
/execute_trajectory/feedback  
/execute_trajectory/goal  
/execute_trajectory/result  
/execute_trajectory/status  
/file  
/gazebo/link_states  
/gazebo/model_states  
/gazebo/parameter_descriptions  
/gazebo/parameter_updates  
/gazebo/set_link_state  
/gazebo/set_model_state  
/initialpose  
/joint_states  
/move_base_simple/goal  
/move_group/cancel  
/move_group/display_contacts  
/move_group/display_planned_path  
/move_group/feedback  
/move_group/goal  
/move_group/monitored_planning_scene  
/move_group/parameter_descriptions  
/move_group/ompl/parameter_updates  
/move_group/plan_execution/parameter_descriptions  
/move_group/planning_scene_monitor/parameter_descriptions  
/move_group/planning_scene_monitor/parameter_updates  
/move_group/restart  
/move_group/sense_for_plan/parameter_descriptions  
/move_group/sense_for_plan/parameter_updates  
/move_group/status
```



no olviden vitaminarse y supermineralizarse!





MAY
**THE FORCE
BE WITH YOU**

We Can Do It!



MERSI

Баярлалаа

спасибо

kiitos
dankie
dhanyavad

bedankt
bayaralaa
gracie
hyva

dziekuje

sobodi
dekuji

obrigado

mesi
didil madhaba
najis tuke
kam sah hamnida

THANK YOU

дякую

vinaka

blagodarann

nam

nantu

dhanyavat

nam

ESKERRIK ASKO

sukriya
terima kasih

감사합니다

go raibh maith agat

merci

danke

vinaka

blagodarann

nam

ngiyabonga

welalin lack

dank je

misaotra

matondo

paldies grazzi

mahao

gracias

tapadh leat

хвала

asante manana

obrigada

lenki

gracias

djiere dieut

lau

mochchakkeram

мамнун

chokrane murakoze

lenki

gracias

arigato

diolch

dhanyavadagalu

shukriya

мерси

Schukria

Spas

teşekkür ederim

mahaao

gracias

tapadh leat

хвала

asante manana

obrigada

lenki

gracias

djiere dieut

lau

mochchakkeram

мамнун

chokrane murakoze

lenki

gracias

arigato

diolch

dhanyavadagalu

shukriya

мерси

Schukria

شکریا

Schukria