



SOC - Security Operations Center y CSIRT - Computer Security Information Response Team

Ing. Ricardo Naranjo Faccini, M.Sc.
2018-11-22



Al fin ¿cual es cual?

- **NOC**

- Network Operations Center
- Centro de operaciones de Red
- Ubicación de los servidores de una empresa y los equipos de red.
- Hoy en día: Interno/Externo/Mixto

- **SOC**

- Security operations center
- Centro de operaciones de Seguridad
 - Personas / Procesos / Tecnologías
 - brindan conocimiento situacional a través de
 - la detección / la contención / la reparación
 - Se encarga incidentes
 - Identificación, validación, priorización, análisis, notificación, investigación.

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



Al fin ¿cual es cual?

• CSIRT

- Computer Security Incident Response Team
- Equipo de respuesta ante incidentes informáticos
- Recibe informes de violaciones.
 - realiza análisis de los informes
 - responde a los remitentes.
- puede ser un grupo establecido o un conjunto ad hoc.
- Interno: parte de organiz/entidad/Nación
- Externos: brindan servicios pagados de forma continua o según sea necesario.

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



Al fin ¿cual es cual?

- **CERT**

- Computer Emergency Response Team
- Equipo de respuesta ante emergencias
- Aplican soluciones a problemas de ciberseguridad.
- Contratistas del gobierno
- Empleados de una corporación
- Deben considerar la seguridad
 - del punto final
 - de los datos en uso
 - de los datos en reposo.

- Pruebas y simulaciones para anticipar
- También necesitan controlar el daño rápidamente.

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



SOC <=> CSIRT

Equipos de respuesta a incidentes
Tienen diferentes roles y responsabilidades.
Defender redes y datos corporativos.
Prevenir, Detectar, Manejar, Responder.

SOC

- Enfocado en la identificación y atención de incidentes.
- Asume funciones de CSIRT si no existe.
- OPERATIVO.

CSIRT

- Entender el ataque.
- Minimizar y controlar consecuencias.
- Comunicarse con: implicados, directivos, clientes, entes de control, pares.
- Prevención - alertas tempranas.
- ESTRATÉGICO.

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



Aspectos fundamentales

SOC <=> CSIRT

- **Identificar ataques.**
 - Uso de tecnología.
- **Atender incidentes.**
- **Minimizar riesgos. (prevención)**
- **Mecanismos de autoprotección**
- **Permanente capacitación en amenazas y vulnerabilidades.**
- **Experiencia para analizar los datos recogidos.**
- **Comunicación con pares (CSIRT), comunidades y fabricantes.**

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades

Roles → SOC <=> CSIRT

- Information security manager
 - Dirige / Coordina / Reporta
- Inteligencia de ciber amenazas
 - Cyber Threat Intelligence Team
 - Convierte información en inteligencia
 - Base de conocimientos colaborativa
 - Diseña estrategias.
- Análisis de ciberamenazas
 - Cyber Threat Analysis Team
 - Analiza las amenazas/ataques
 - Reduce el ruido.

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



Roles → SOC <=> CSIRT

- **Gestión de vulnerabilidades**
 - Vulnerability Management Team
 - Contextualiza las amenazas contra los activos expuestos
- **Respuesta a incidentes**
 - Incident response team
 - Actúa en respuesta a los ataques
 - **Descifra la naturaleza del ataque**
 - **Caza al intruso**
- **Comunicaciones**
 - Interactúa oportunamente con funcionarios afectados.
 - Capacita/concientiza al personal.
 - **Reporta a autoridades y pares.**
 - **Mto. de base de datos de conocimiento.**

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades

Roles → SOC <=> CSIRT

- **Operadores 24/7**
 - Monitorean la infraestructura
 - Detectan los ataques
 - Están pendientes de vulnerabilidades
 - **Atentos a alertas de pares**
 - **Reportan a pares.**
- **Análisis forense**
- **Restituidores de la continuidad**
- **Asesoría legal / financiera**

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



Roles del SOC o CSIRT



Aspectos

Roles

Actividades

Preparatorias

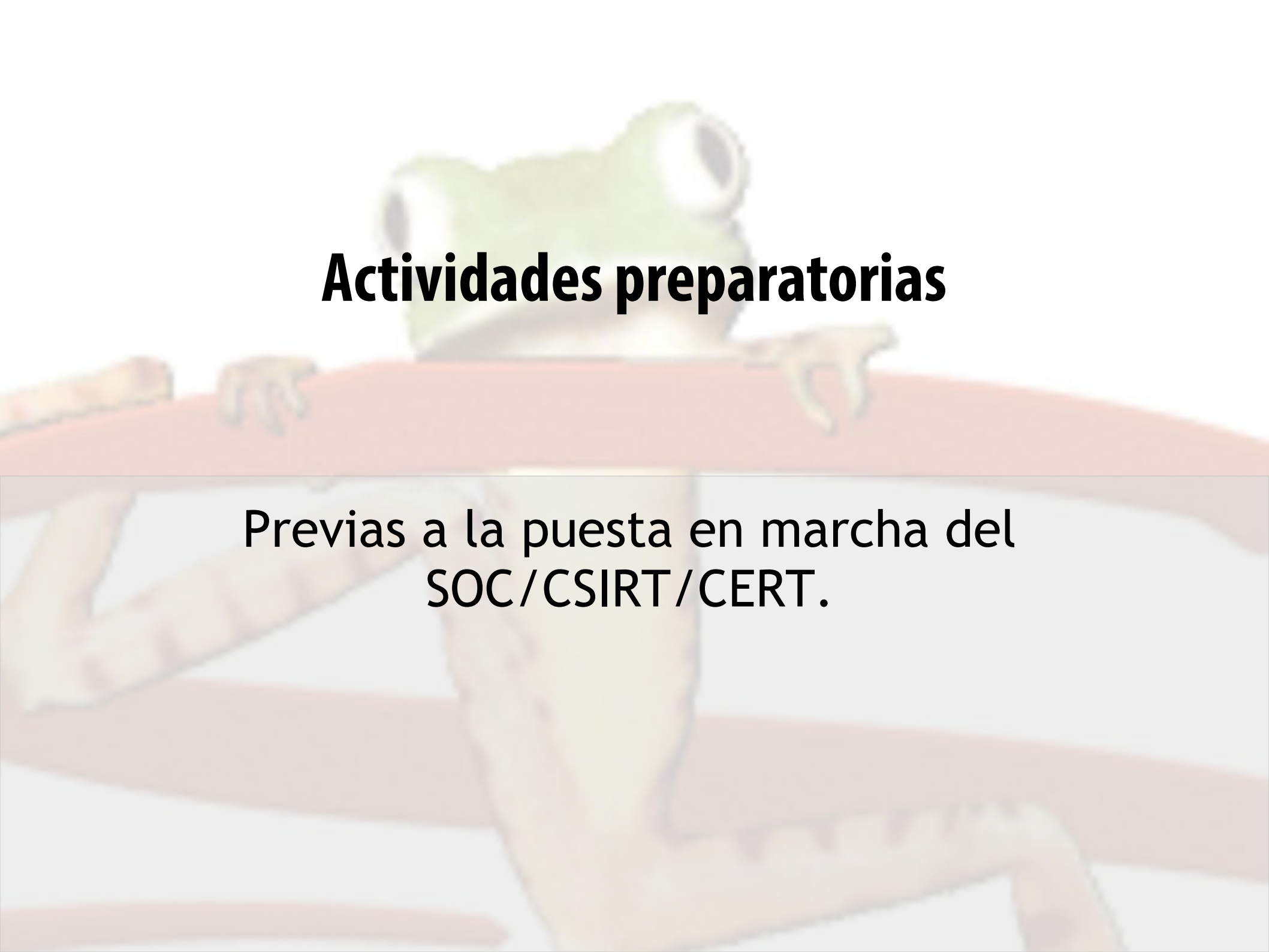
Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



Actividades preparatorias

Previas a la puesta en marcha del
SOC/CSIRT/CERT.

Conformar el equipo:

- **Competente:**
 - Habilidades, Disciplina, Disponibilidad.
 - Todos los roles una misma persona ← varios roles
 - Formación permanente.
 - En contacto con otros equipos.
- **Aseguramiento del propio equipo.**

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



Actividades del SOC

- **Establecer mecanismos de comunicación:**
 - **Intra-equipo:**
 - **Lenguaje estándar**
 - Sin jergas rebuscadas.
 - Conociendo nomenclatura del sector.
 - IOC = Indicadores de compromiso.
 - RIG = Kit de exploits común.
 - IPS = Sistema de prevención de intrusos.
 - **Identificadores únicos de:**
 - Recursos / Locaciones / Servicios.
 - **Software de comunicación.**
 - **Todo el equipo conectado**
 - **Establecer horarios de disponibilidad.**
 - **Con pares:**
 - ¿Quiénes son? ¿Cómo me pueden ayudar?
¿cuándo acudir?
 - ¿Cómo puedo ayudarlos?

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



Actividades → SOC <=> CSIRT

- **Inventario / Identificación / clasificación activos TIC:**

- **Información**
 - Metadatos / Bitácoras
- **Hardware**
 - Portátiles
 - Móviles
 - IoT
 - Ciberfísicos
- **Software**
 - Bases de datos
 - Web / Cloud
 - Apps
- **Servicios**
- **Redes**

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades

Actividades → SOC <=> CSIRT

- **Inventario/identificación de activos no TIC críticos.**
 - Fluído eléctrico.
 - Conectividad
 - Internet - servidores onLine/Cloud.
 - Infraestructura.
 - Buen nombre
 - Clima / plagas / polvo / sal marina...
 - Relaciones con:
 - Directivos, implicados, clientes, proveedores
 - Pares, entes de control.
 - Personal con condiciones especiales.
 - Secretos industriales.
 - Propiedad intelectual.

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



Actividades del SOC

- **Establecer línea base.**
 - Horas valle.
 - Horas pico.
 - Top ## de usuarios en consumo de:
 - Almacenamiento.
 - Tráfico.
 - Top ## de áreas en consumo.
 - Archivos de configuración.
 - Se determina según:
 - Organización.
 - Ubicación (local/remota).
 - Tecnología (OS).
 - md5, sha512, scripts, Tripwire

Aspectos

Roles

Actividades

Preparatorias

Preventivas

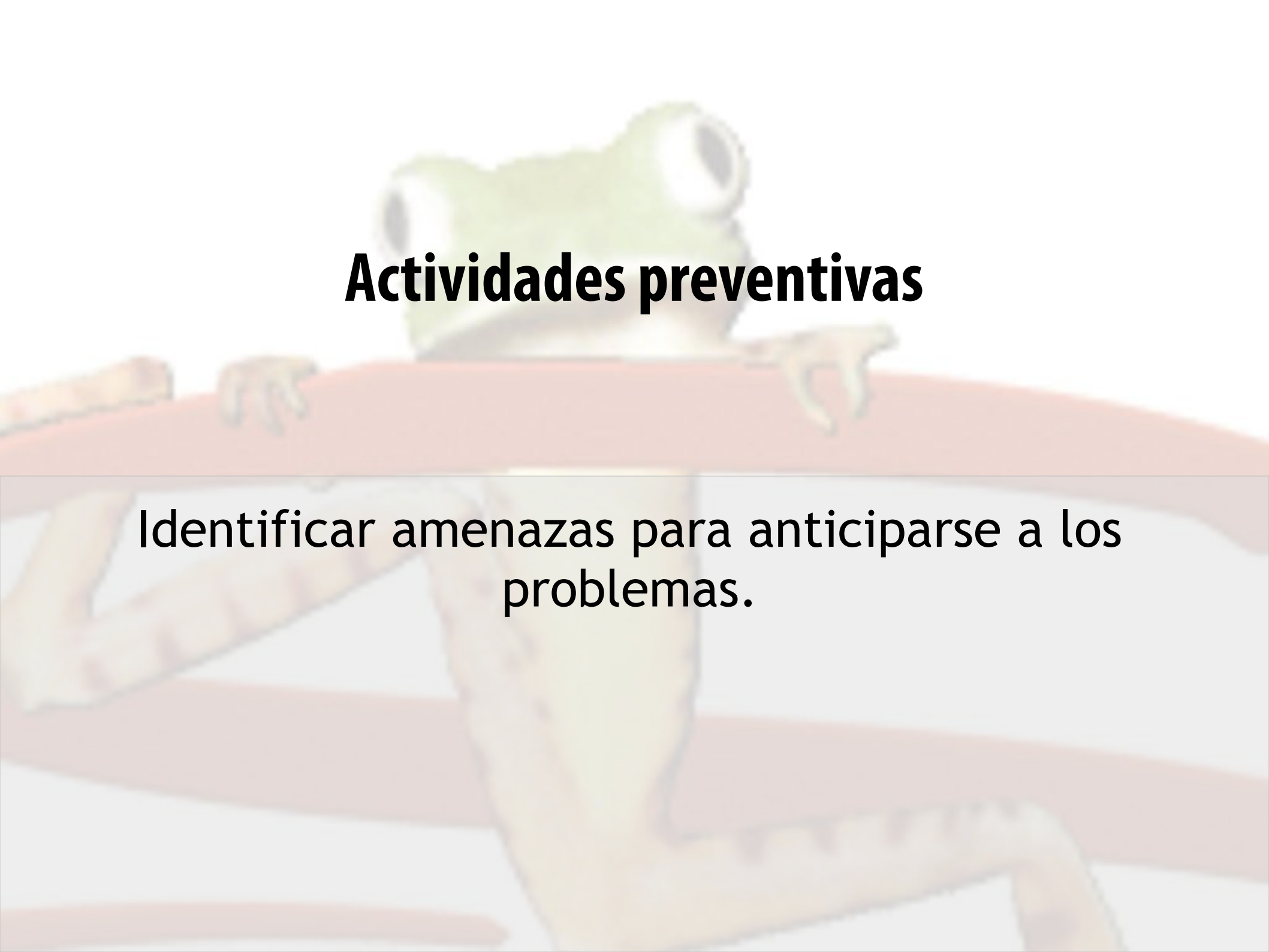
Reactivas

Herramientas

Ejemplos

Entidades



A green tree frog is perched on a thick, brown, curved branch. The frog is facing forward, with its large, white eyes and green skin clearly visible. The background is a soft, out-of-focus light green, suggesting a natural, forest-like environment. The frog's front legs are gripping the branch, and its body is slightly hunched over.

Actividades preventivas

Identificar amenazas para anticiparse a los problemas.

Actividades del SOC

- Definición de incidentes y prioridad
- Aseguramiento de plataformas
 - Servidores.
 - Apps / WebApps.
 - Estaciones de trabajo.
 - Conectores red / periféricos
 - Análisis de bitácoras.
 - Centralizado.
 - Distribuido.
- Auditorías periódicas.
 - aconsejar / Capacitar personal.
 - moodle
 - Prevenir.

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades

Actividades del SOC

- **Monitoreo de Infraestructura**
 - Comunicaciones / Almacenamiento.
 - Comparar con línea base
 - Periódicamente.
 - Homogénea a su establecimiento.
 - Identificar cambios:
 - Detectar posibles ataques.
 - Identificar falsos positivos.
 - Ajustar línea base.
 - Reaccionar oportuna y adecuadamente.
 - ¿desconectar equipo?
 - ¿interrumpir comunicaciones?
 - ¿establecer el tipo de ataque?
 - Monitorix.
 - Tripwire.

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



Actividades del SOC

- **Plan y operación de backups.**
 - Simulacros de recuperación.
 - Cuantificar/valorar el tiempo de:
 - Generación.
 - Recuperación.
- **Plan de mejora continua del SOC.**
 - Adquisición de nuevas herramientas.
 - Capacitación permanente.
 - Canales de comunicación para:
 - Identificar nuevas amenazas.
 - Adoptar buenas prácticas y procedimientos.
- **Actualizar los inventarios.**

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



Actividades del SOC

- **Detección de ataques**
 - Software especializado.
 - Antivirus.
 - NIDS - detección de intrusos.
 - Actualizado.
 - Honeypots.
- **Disposición final / Retención de la información.**
- **Plan de continuidad / recuperac.**
 - Simulacros.

Aspectos

Roles

Actividades

Preparatorias

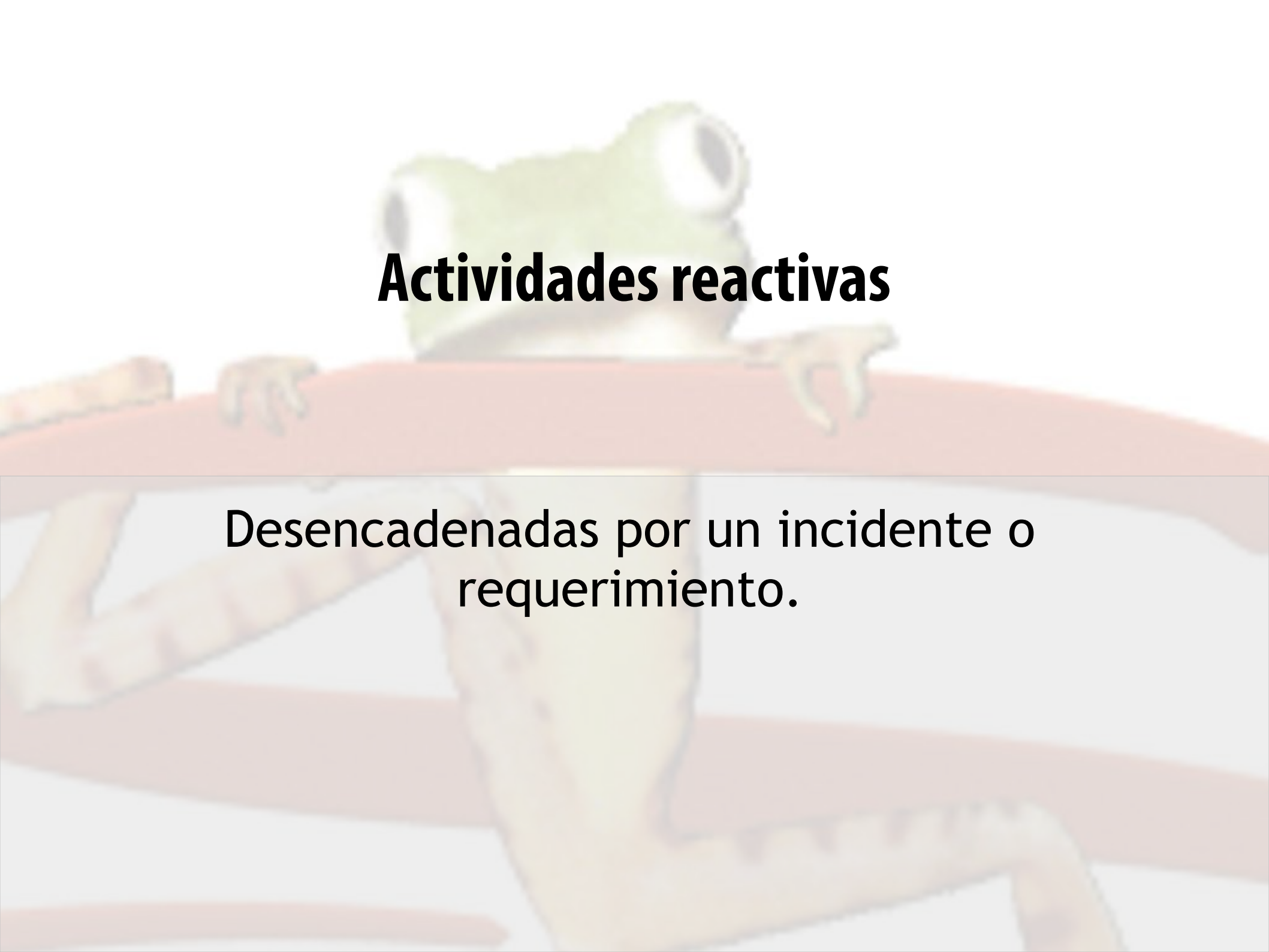
Preventivas

Reactivas

Herramientas

Ejemplos

Entidades

A green tree frog is perched on a thick, reddish-brown branch. The frog is facing forward, with its large, white eyes and dark pupils clearly visible. Its skin is a vibrant green with some darker spots. The background is a soft, out-of-focus light green, suggesting a natural, leafy environment. The frog's front legs are gripping the branch, and its hind legs are also visible, showing a lighter green color with some darker markings.

Actividades reactivas

Desencadenadas por un incidente o requerimiento.

Actividades del SOC

- **Triage de incidentes**

- **Verificación inicial.**
 - ¿Está sucediendo?
 - ¿que tan peligroso es?
 - Valor/identificación de los activos expuestos/afectados.
 - Nivel jerárquico del personal afectado.
- **Reducir falsos positivos.**
- **Priorización.**
- **Trabajo durante la operación de la infraestructura informática**

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades

Continuidad del servicio

- **Priorización**
 - Orden de los servicios a restablecer.
 - Identificar el mínimo nivel obligatorio.
- **Verificación**
 - De la afectación.
 - Sanidad de los backups
- **Recuperación.**
 - De los backups.
 - Reinstalación de aplicativos.
- **Estabilización.**
 - De la prestación del servicio.
 - Prevención de repeticiones.
 - Capacitación / Divulgación.

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades

Actividades del SOC

- **Comunicación con los implicados.**
 - Claros.
 - Depende de la formación del interlocutor
 - Sucintos.
 - Depende del nivel jerárquico del interlc.
 - Oportunos.
 - Depende de la prioridad del incidente.
 - Pertinentes.
 - Depende del valor del activo comprometido.
 - Homogéneos.
 - Detallando los activos. comprometidos:
 - Afectados.
 - Vulnerables.
 - Describiendo las acciones/recomendac.
 - Informando el riesgo residual.
 - Emisión de alertas / Denuncia de incidentes

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



Actividades del SOC

https://wiki.es.it-processmaps.com/index.php/KPIs_ITIL_-_Dise%C3%B1o_del_Servicio#Gesti.C3.B3n_de_la_Continuidad_del_Servicio_de_TI_.28ITSCM.29

● MEDIR

- Lo que no se mide, no se puede gestionar.
- KPI's ITIL
 - Gestión del Nivel de Servicio
 - Gestión de la Capacidad
 - Gestión de la Disponibilidad
 - Gestión de la Continuidad del Servicio de TI
 - Gestión de la Seguridad de TI
 - Q medidas preventivas
 - Ventana de exposición
 - Q incidentes graves
 - Tiempo de inactividad/interrupción
 - Q de pruebas de seguridad
 - # defectos identificados
 - Gestión de Suministradores

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades

Herramientas



Herramientas de soporte al SOC

- Sistema de gestión del ciclo de vida de los incidentes.
 - Visibilidad.
 - Trazabilidad.
 - Control.
 - Análisis.
 - Gobernabilidad.
 - Centralizada.
 - Ubiqua.
 - Punto único de reporte.
 - GROUPs - Skina IT Solutions.

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades

Herramientas de soporte al SOC

- **Inventario:**
 - **Activos**
 - TIC
 - No TIC - críticos
 - **Personal**
- **Base de datos de conocimientos.**
 - Alimentada desde diferentes fuentes.
 - Acceso abierto para todos.
 - Construcción colaborativa/moderada.
 - Interacción con pares.
- **GLPI** <https://glpi-project.org/>

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



Herramientas de soporte al SOC

- **Monitoreo centralizado y automatizado de bitácoras.**

- Nagios
- Solarwinds

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



Current Network Status
 Last Updated: Fri May 31 09:24:15 EST 2013
 Updated every 90 seconds
 Nagios® Core™ 3.4.1 - www.nagios.org
 Logged in as michael.schams

View Status Overview For This Service Group
 View Status Summary For This Service Group
 View Service Status Grid For This Service Group
 View Service Status Detail For All Service Groups

Host Status Totals

Up	Down	Unreachable	Pending
13	0	0	0

[All Problems](#) [All Types](#)

0	13
---	----

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
48	0	0	0	0

[All Problems](#) [All Types](#)

0	49
---	----

Service Status Details For Service Group 'typo3'

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
typo3	typo3	OK	2013-05-31 04:33:49	2d 17h 7m 49s	1/3	TYPO3 4.7.10 OK
typo3	typo3	OK	2013-05-31 04:35:37	2d 16h 48m 38s	1/3	TYPO3 4.7.10 OK
typo3	typo3	OK	2013-05-31 08:39:16	29d 6h 44m 59s	1/3	TYPO3 4.7.10 OK
typo3	typo3	OK	2013-05-31 08:52:26	69d 0h 31m 49s	1/3	TYPO3 4.5.25 OK
typo3	typo3	OK	2013-05-31 04:29:27	27d 16h 54m 48s	1/3	TYPO3 4.5.25 OK
typo3	typo3	OK	2013-05-31 07:28:10	77d 23h 14m 42s	1/3	TYPO3 4.5.25 OK
typo3	typo3	OK	2013-05-31 06:33:01	21d 14h 51m 14s	1/3	TYPO3 4.7.10 OK
typo3	typo3	OK	2013-05-31 06:52:09	27d 20h 32m 6s	1/3	TYPO3 4.5.25 OK
typo3	typo3	OK	2013-05-31 04:33:21	0d 17h 0m 51s	1/3	TYPO3 4.7.10 OK
typo3	typo3	OK	2013-05-31 06:26:47	0d 23h 3m 44s	1/3	TYPO3 4.7.10 OK
typo3	typo3	OK	2013-05-31 03:26:38	0d 23h 57m 37s	1/3	TYPO3 4.7.10 OK
typo3	typo3	OK	2013-05-31 06:44:36	0d 23h 3m 37s	1/3	TYPO3 4.7.10 OK
typo3	typo3	OK	2013-05-31 09:11:31	0d 23h 1m 31s	1/3	TYPO3 4.7.10 OK
typo3	typo3	OK	2013-05-31 06:40:23	13d 2h 43m 52s	1/3	TYPO3 4.5.25 OK
typo3	typo3	OK	2013-05-31 06:44:26	0d 23h 1m 24s	1/3	TYPO3 4.7.10 OK
typo3	typo3	OK	2013-05-31 03:26:59	15d 5h 57m 17s	1/3	TYPO3 4.7.10 OK
typo3	typo3	OK	2013-05-31 08:48:08	42d 18h 36m 7s	1/3	TYPO3 4.5.25 OK
typo3	typo3	OK	2013-05-31 08:03:39	27d 19h 20m 36s	1/3	TYPO3 4.5.25 OK
typo3	typo3	OK	2013-05-31 08:56:27	15d 18h 27m 48s	1/3	TYPO3 4.5.25 OK
typo3	typo3	OK	2013-05-31 07:58:47	75d 7h 25m 31s	1/3	TYPO3 4.7.10 OK
typo3	typo3	OK	2013-05-31 04:13:53	15d 5h 10m 22s	1/3	TYPO3 4.5.25 OK
typo3	typo3	OK	2013-05-31 08:52:29	42d 18h 31m 46s	1/3	TYPO3 4.5.25 OK
typo3	typo3	OK	2013-05-31 04:46:09	0d 16h 51m 57s	1/3	TYPO3 4.5.25 OK
typo3	typo3	OK	2013-05-31 04:08:10	42d 17h 16m 9s	1/3	TYPO3 4.5.25 OK
typo3	typo3	OK	2013-05-31 04:29:37	27d 16h 54m 38s	1/3	TYPO3 4.5.25 OK
typo3	typo3	OK	2013-05-31 04:08:27	84d 18h 6m 14s	1/3	TYPO3 4.7.10 OK
typo3	typo3	OK	2013-05-31 04:32:06	24d 16h 52m 9s	1/3	TYPO3 4.7.10 OK
typo3	typo3	OK	2013-05-31 09:08:46	3d 6h 15m 29s	1/3	TYPO3 4.7.10 OK

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



Nagios

Nagios®

General

- Home
- Documentation

Current Status

- Tactical Overview
- Map
- Hosts
- Services
- Host Groups
 - Summary
 - Grid
- Service Groups
 - Summary
 - Grid
- Problems
 - Services (Unhandled)
 - Hosts (Unhandled)
 - Network Outages

Quick Search:

Reports

- Availability
- Trends
- QlikView Graph
- CxlQuantum Graph
- Alerts
 - History
 - Summary
 - Histogram
- Notifications
- Event Log

System

- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue
- Configuration

Current Network Status

Last Updated: Tue Jan 21 12:51:00 WEST 2014
Updated every 90 seconds
Nagios® Core™ 4.0.2 - www.nagios.org
Logged in as nagiosadmin

View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
4	0	0	0

All Problems	All Types
0	4

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
7	0	0	1	0

All Problems	All Types
1	8

Service Status Details For All Hosts

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
CXL	CXL_Quantum interface	OK	01-21-2014 12:41:29	4d 21h 25m 13s	1/1	OK:Waiting time for Quantum answer 1.352 [s] (below threshold 10[s]) Total process time: 6[s]
	Create trade	OK	01-21-2014 12:23:10	1d 2h 27m 49s	1/1	Test passed. Trade created:42642
	Login test	OK	01-21-2014 12:41:20	1d 2h 49m 40s	1/1	Test passed. User logged in.
INTRANET	Check HTTP	OK	01-21-2014 12:23:28	8d 3h 1m 47s	1/1	(No output on stdout) stderr:
QLIKVIEW	QlikView performance check	OK	01-21-2014 12:48:10	0d 22h 36m 31s	1/1	OK: Qlikview test passed in 4.773 [s] (below threshold 10[s]).
	Selenium test which fail	CRITICAL	01-21-2014 12:14:22	7d 21h 40m 8s	1/1	ERROR: Qlikview test failed becuase of: Timeout in waiting for link to dashboard.
localhost	Physical memory	OK	01-21-2014 12:50:29	8d 3h 55m 50s	1/4	(No output on stdout) stderr:
	Total Processes	OK	01-21-2014 12:46:50	8d 3h 55m 0s	1/4	PROCESS OK - 77 process(es)

Results 1 - 8 of 8 Matching Services

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades

Nagios XI

[Home](#)
[Views](#)
[Dashboards](#)
[Reports](#)
[Configure](#)
[Tools](#)
[Help](#)
[Admin](#)

System Information

System Status
Monitoring Engine Status
Audit Log
Check For Updates

Users

Manage Users
LDAP/AD Integration
Notification Management

System Config

System Settings
License Information
Proxy Configuration
System Profile
Manage Email Settings
Manage Mobile Carriers
Performance Settings
Automatic Login
Reset Security Credentials
SSH Terminal

Monitoring Config

Config Snapshots
Check File Permissions
NRDS Config Manager
Unconfigured Objects
Reactor Integration

Check Transfers

Outbound Transfers
Inbound Transfers

System Extensions

Manage Components
Manage Config Wizards
Manage Dashlets
Manage Plugins
Manage Graph Templates
Manage MIBs

System Backups

Scheduled Backups
Local Backup Archives

Monitoring Engine Status

Monitoring Engine Process

Metric	Value	Action
Process Info		
Process State	●	⊕ ⊖
Process Start Time	2015-08-25 11:48:41	
Total Running Time	1d 22h 19m 24s	
Process ID	3364	
Process Settings		
Active Service Checks	●	✕
Passive Service Checks	●	✕
Active Host Checks	●	✕
Passive Host Checks	●	✕
Notifications	●	✕
Event Handlers	●	✕
Flap Detection	●	✕
Performance Data	●	✕
Service Obsession	●	✓
Host Obsession	●	✓

Last Updated: 2015-08-27 10:08:05

Monitoring Engine Event Queue

Scheduled Events Over Time

Last Updated: 2015-08-27 10:08:05



Monitoring Engine Check Statistics

Metric	Value
Active Host Checks	
1-min	9
5-min	41
15-min	41
Passive Host Checks	
1-min	0
5-min	0
15-min	0
Active Service Checks	
1-min	39
5-min	215
15-min	216
Passive Service Checks	
1-min	0
5-min	0
15-min	0

Last Updated: 2015-08-27 10:08:05

Monitoring Engine Performance

Metric	Value
Host Check Latency	
Min	0.00 sec
Max	0.32 sec
Avg	0.01 sec
Host Check Execution Time	
Min	0.00 sec
Max	10.00 sec
Avg	1.53 sec
Service Check Latency	
Min	0.00 sec
Max	0.90 sec
Avg	0.01 sec
Service Check Execution Time	
Min	0.00 sec
Max	10.01 sec
Avg	1.00 sec

Last Updated: 2015-08-27 10:08:05

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

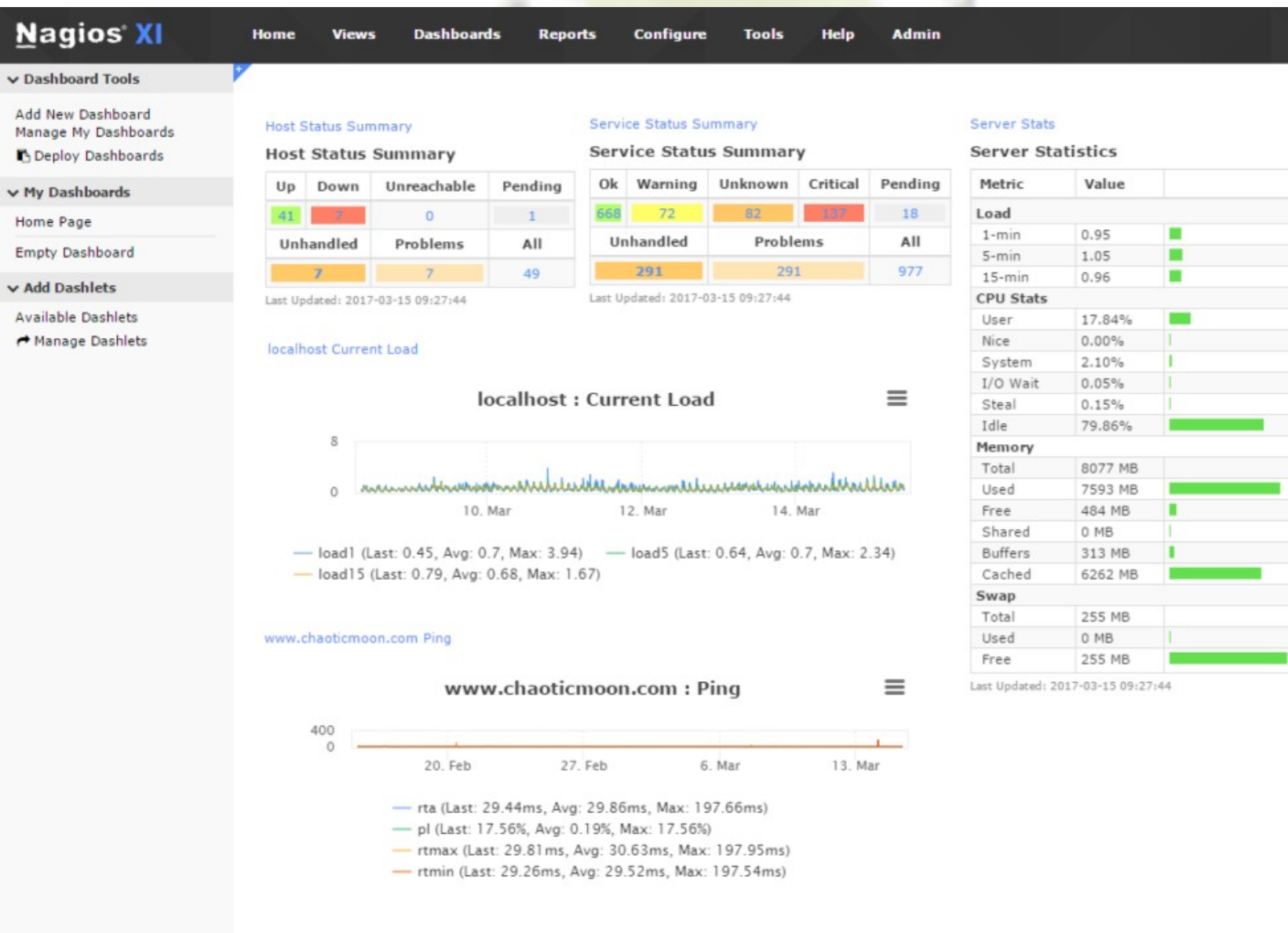
Herramientas

Ejemplos

Entidades



Nagios



Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades

Nagios

Nagios®

General

- Home
- Documentation

Monitoring

- Tactical Overview
- Service Detail
- Host Detail
- Status Overview
- Status Summary
- Status Grid
- Status Map
- 3-D Status Map
- Service Problems
- Host Problems
- Network Outages

- Comments
- Downtime

- Process Info
- Performance Info
- Scheduling Queue

Reporting

- Trends
- Availability
- Alert Histogram
- Alert History
- Alert Summary
- Notifications
- Event Log

Configuration

- View Config

	Monitor					
webprod03	Check Users	OK	01-26-2007 14:58:59	0d 4h 53m 23s	1/4	USERS OK - 1 users currently logged in
	Current Load	OK	01-26-2007 14:59:54	0d 4h 53m 23s	1/4	OK - load average: 0.21, 0.08, 0.05
	Memory Usage	OK	01-26-2007 14:55:29	0d 4h 53m 23s	1/4	OK: Memory Usage 56% - Total: 511 MB, Used: 287 MB, Free: 224 MB
	PING	OK	01-26-2007 14:56:14	0d 4h 50m 23s	1/4	PING OK - Packet loss = 0%, RTA = 0.16 ms
	Root Partition	OK	01-26-2007 14:57:09	0d 4h 50m 33s	1/4	DISK OK [243816 kB (5%) free on /dev/sda2]
	SWAP Usage	OK	01-26-2007 14:57:44	0d 4h 50m 33s	1/4	Swap ok - (null) 0% (0 out of 16386)
	Total Processes	OK	01-26-2007 14:58:29	0d 4h 50m 33s	1/4	OK - 95 processes running
	Xen Virtual Machine Monitor	CRITICAL	01-26-2007 14:59:04	0d 0h 44m 34s	4/4	Critical Xen VMs Usage - Total NB: 0 - detected VMs:
webprod04	Check Users	OK	01-26-2007 14:59:54	0d 0h 15m 33s	1/4	USERS OK - 2 users currently logged in
	Current Load	OK	01-26-2007 14:55:34	0d 0h 14m 53s	1/4	OK - load average: 0.30, 0.60, 0.44
	Memory Usage	OK	01-26-2007 14:56:19	0d 0h 14m 13s	1/4	OK: Memory Usage 37% - Total: 511 MB, Used: 190 MB, Free: 321 MB
	PING	OK	01-26-2007 14:57:10	0d 0h 13m 23s	1/4	PING OK - Packet loss = 0%, RTA = 0.27 ms
	Root Partition	OK	01-26-2007 14:57:49	0d 0h 12m 43s	1/4	DISK OK [3948940 kB (94%) free on /dev/sda2]
	SWAP Usage	OK	01-26-2007 14:58:34	0d 0h 11m 53s	1/4	Swap ok - (null) 0% (0 out of 16386)
	Total Processes	OK	01-26-2007 14:59:09	0d 0h 16m 22s	1/4	OK - 250 processes running
	Xen Virtual Machine Monitor	WARNING	01-26-2007 14:58:54	0d 0h 1m 33s	4/4	Warning Xen VMs Usage - Total NB: 1 - detected VMs: migrating-xen-vm4
webprod05	PING	OK	01-26-2007 14:55:39	0d 0h 24m 58s	1/4	PING OK - Packet loss = 0%, RTA = 0.25 ms
	Xen Virtual Machine Monitor	OK	01-26-2007 14:59:54	0d 0h 0m 33s	1/4	OK: Xen Hypervisor "webprod05" is running 4 Xen VMs: xen-vm1 xen-vm2 xen-vm3 xen-vm4
xen-vm1	Check Users	OK	01-26-2007 14:58:09	0d 0h 17m 23s	1/4	USERS OK - 1 users currently logged in
	Current Load	OK	01-26-2007 14:57:54	0d 3h 16m 21s	1/4	OK - load average: 1.54, 1.09, 0.48
	Memory Usage	OK	01-26-2007 14:58:39	0d 3h 15m 41s	1/4	OK: Memory Usage 8% - Total: 8195 MB, Used: 676 MB, Free: 7519 MB
	PING	OK	01-26-2007 14:59:15	0d 3h 15m 21s	1/4	PING OK - Packet loss = 0%, RTA = 0.49 ms
	Root Partition	OK	01-26-2007 14:59:59	0d 3h 14m 51s	1/4	DISK OK [4196280 kB (99%) free on udev]
	SWAP Usage	OK	01-26-2007 14:55:44	0d 3h 14m 1s	1/4	Swap ok - (null) 0% (0 out of 2055)
	Total Processes	OK	01-26-2007 14:57:29	0d 0h 18m 3s	1/4	OK - 88 processes running
xen-vm2	Check Users	OK	01-26-2007 14:57:15	0d 3h 7m 41s	1/4	USERS OK - 0 users currently logged in
	Current Load	OK	01-26-2007 14:57:59	0d 3h 7m 1s	1/4	OK - load average: 0.00, 0.00, 0.00
	Memory Usage	OK	01-26-2007 14:58:44	0d 3h 6m 21s	1/4	OK: Memory Usage 6% - Total: 1023 MB, Used: 64 MB, Free: 958 MB
	PING	OK	01-26-2007 14:59:19	0d 0h 48m 14s	1/4	PING OK - Packet loss = 0%, RTA = 0.43 ms
	Root Partition	OK	01-26-2007 15:00:05	0d 1h 15m 4s	1/4	DISK OK [524220 kB (99%) free on udev]
	SWAP Usage	OK	01-26-2007 14:55:49	0d 3h 9m 41s	1/4	Swap ok - (null) 0% (0 out of 2055)
	Total Processes	OK	01-26-2007 14:56:34	0d 3h 9m 1s	1/4	OK - 52 processes running

Aspectos

Roles

Actividades

Preparatorias

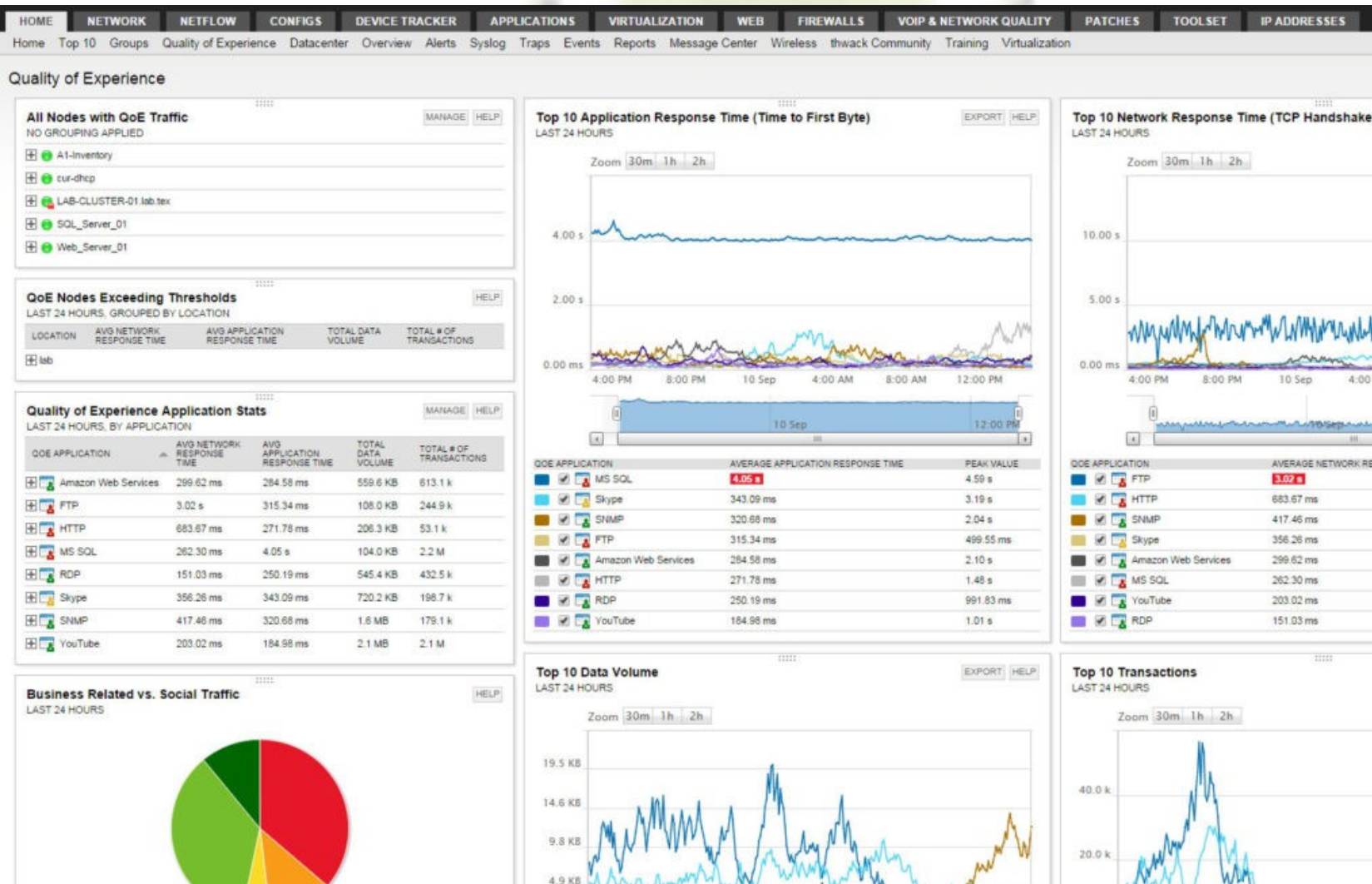
Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades

Solarwinds



Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades

- Emulación de redes
 - GNS3
 - Protegido con GPLv3
 - <https://youtu.be/iLmEJv9yo0M>

Aspectos

Roles

Actividades

Preparatorias

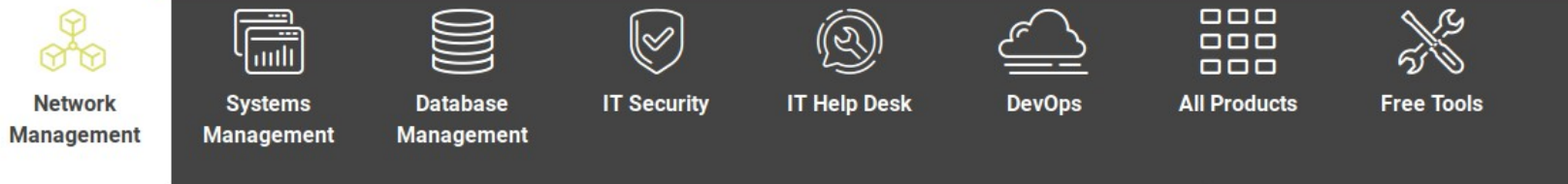
Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



Products

Network Performance Monitor

NetFlow Traffic Analyzer

Network Configuration Manager

ipMonitor

IP Address Manager

User Device Tracker

[View All Network Management Products](#)

VoIP & Network Quality Manager

Log Manager for Orion

Engineer's Toolset

Network Topology Mapper

Kiwi CatTools

Kiwi Syslog Server

Bundles

Network Bandwidth Analyzer Pack

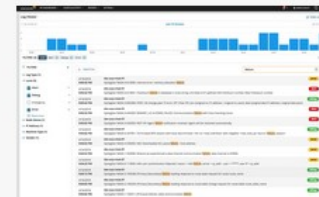
Log and Network Performance Pack

IP Control Bundle

Unified Solutions

Network Automation Manager

Unify log management and infrastructure performance with SolarWinds Log Manager for Orion.



Aggregate. Search. Chart.

[Learn More](#)

Herramientas de soporte al SOC

- **Monitoreo centralizado y automatizado de bitácoras.**
 - Nagios
 - Solarwinds
- **Alerta ante cambios críticos:**
 - Tripwire.

Aspectos

Roles

Actividades

Preparatorias

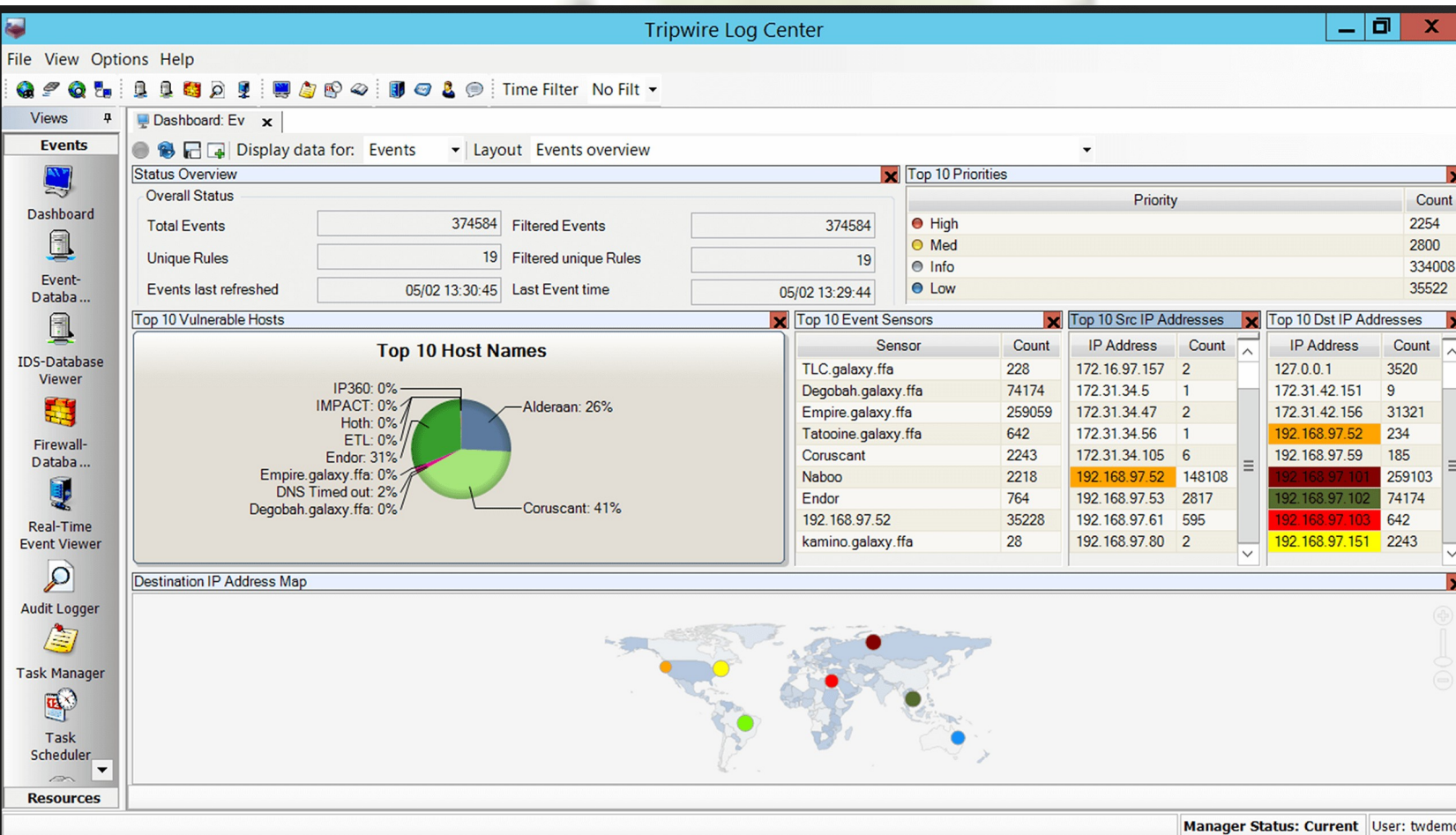
Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades

Aspectos

Roles

Actividades

Preparatorias

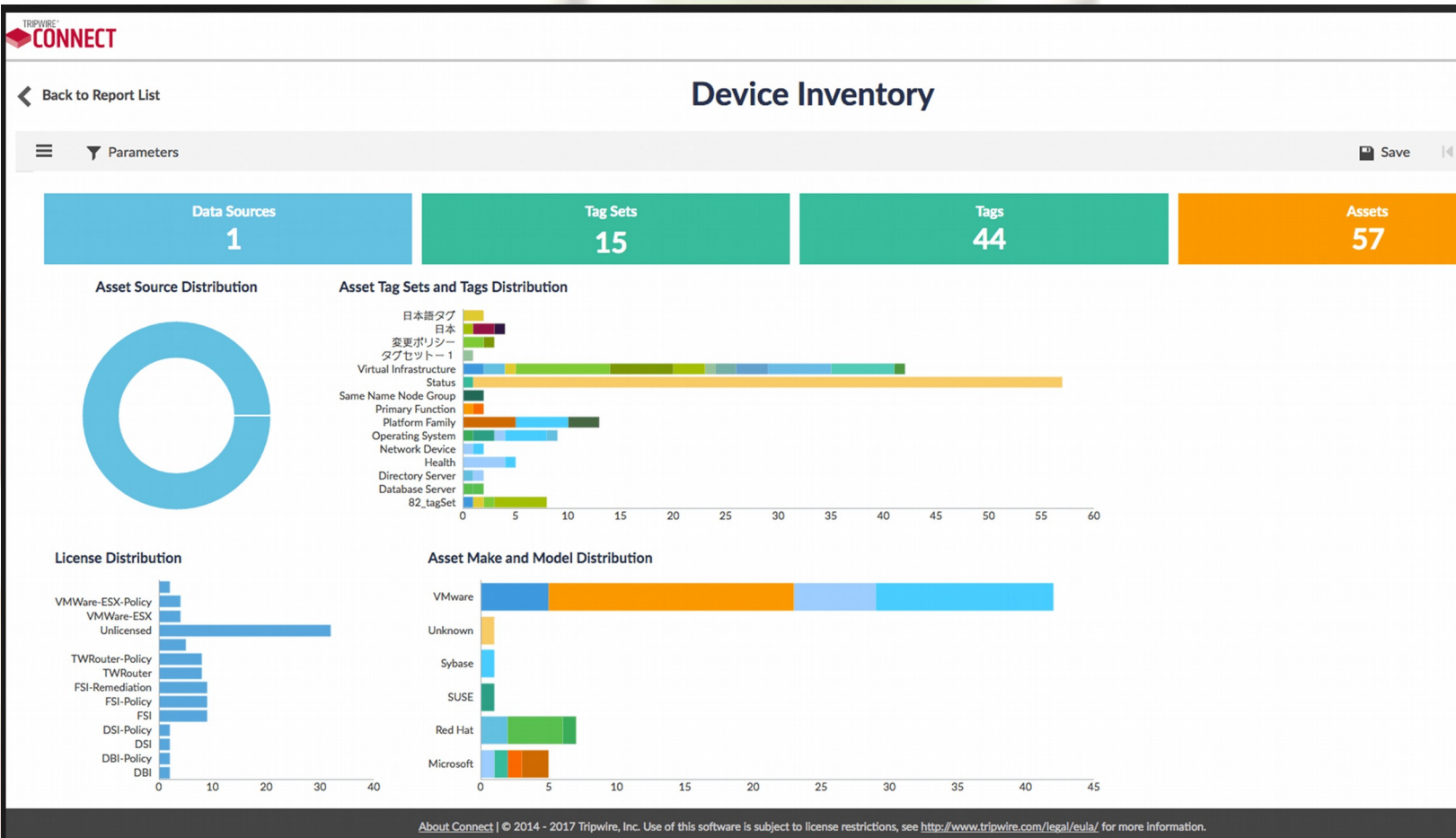
Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



Tripwire

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades

Tripwire Configuration Compliance Manager 5.17.2 (twdemo on etl)

File Edit Server Tools Settings View Help

Start Stop Create Network Profile... Changes Inventory Compliance Filtering Logout

Asset Groups

- All Assets
 - Alpharetta
 - Production
 - Rogue
 - Grouping Rule
 - Local
 - SE Lab
 - Ungrouped
 - Windows

Meta Assets

- AIX
- CentOS 6
- CentOS 7
- CentOS (Other)
- Cisco
- HP-UX
- Linux (Other)
- PCI - POS
- RHEL 5
- RHEL 6
- RHEL 7

Network Profiles

- AlphaLab
- Local
- Production
- QA
- SELab

Change ID	Host	Updated	Severity	Risk	Alert Information
306896	pfense (VMwareIn:A9:26:43)	Wed 12/14/2016 2:05 ...	3 - High	High	Asset Status changed: Property Credentialed Access? was False, is now True
306906	EMPIRE (VMwareIn:A9:08:B5)	Wed 12/14/2016 2:09 ...	3 - High	High	Port TCP 49154 removed
306907	EMPIRE (VMwareIn:A9:08:B5)	Wed 12/14/2016 2:09 ...	3 - High	High	Port TCP 49206 removed
306908	EMPIRE (VMwareIn:A9:08:B5)	Wed 12/14/2016 2:09 ...	3 - High	High	Port TCP 49155 found
306909	EMPIRE (VMwareIn:A9:08:B5)	Wed 12/14/2016 2:09 ...	3 - High	High	New Port TCP 49207 found
307071	pfense (VMwareIn:A9:26:43)	Thu 12/15/2016 2:05 P...	3 - High	High	Asset Status changed: Property Credentialed Access? was True, is now False
307462	pfense (VMwareIn:A9:26:43)	Sun 12/18/2016 2:03 P...	3 - High	High	Asset Status changed: Property Credentialed Access? was False, is now True
307554	EMPIRE (VMwareIn:A9:08:B5)	Mon 12/19/2016 1:59 ...	3 - High	High	Asset Status changed: Property Credentialed Access? was True, is now False
307568	pfense (VMwareIn:A9:26:43)	Mon 12/19/2016 2:03 ...	3 - High	High	Asset Status changed: Property Credentialed Access? was True, is now False
307569	EMPIRE (VMwareIn:A9:08:B5)	Mon 12/19/2016 2:03 ...	3 - High	High	Asset Status changed: Property Credentialed Access? was False, is now True
307815	pfense (VMwareIn:A9:26:43)	Wed 12/21/2016 2:05 ...	3 - High	High	Port TCP 443 found
308879	pfense (VMwareIn:A9:26:43)	Fri 12/23/2016 2:00 PM	3 - High	High	Web Server lighttpd/1.4.35 on port 443 removed
309050	pfense (VMwareIn:A9:26:43)	Sat 12/24/2016 2:04 PM	3 - High	High	Port TCP 53 found
309051	pfense (VMwareIn:A9:26:43)	Sat 12/24/2016 2:04 PM	3 - High	High	Port TCP 80 found

Host: pfense (VMwareIn:A9:26:43) **Change ID:** 309051 **Compliant:** No Policies **IP Address:** 192.168.97.1

Criticality: 4 - Severe **At Time:** 12/24/2016 2:04:57 PM

Category: Ports **Change Type:** Item Added [Show History for Asset](#)

Severity: High **Risk:** High

Added Item: Double click an item to view the asset record at the time it was added

Name	
TCP 80	

Scan Status

Engine	Endpoint	Status	Assets (Licensed)	Profiles	Tasks	Task Type	Remote Logging	Queue Length
Scan Engine 1	192.168.235.161:3399	Disconnected	0	0	0	0		
twdemo	localhost:3399	Disconnected	0	0	0	0		
Local	192.168.97.80	Disconnected	0	0	0	0		

Herramientas de soporte al SOC

- **Monitoreo centralizado y automatizado de bitácoras.**
 - Nagios
 - Solarwinds
- **Alerta ante cambios críticos:**
 - Tripwire.
- **Rastreo de puertos:**
 - NMap

Aspectos

Roles

Actividades

Preparatorias

Preventivas

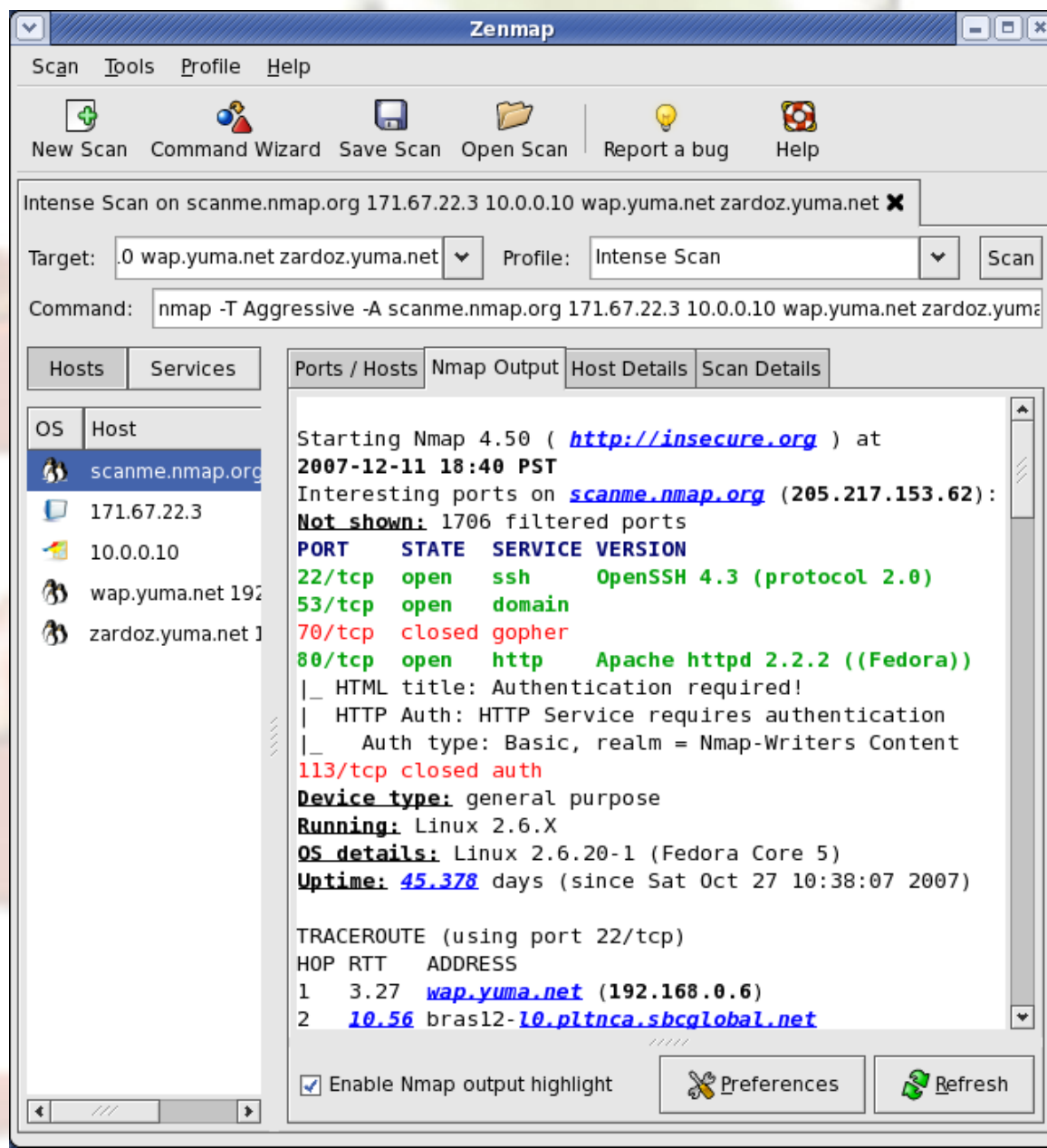
Reactivas

Herramientas

Ejemplos

Entidades





Aspectos

Roles

Actividades

Preparatorias

Preventivas

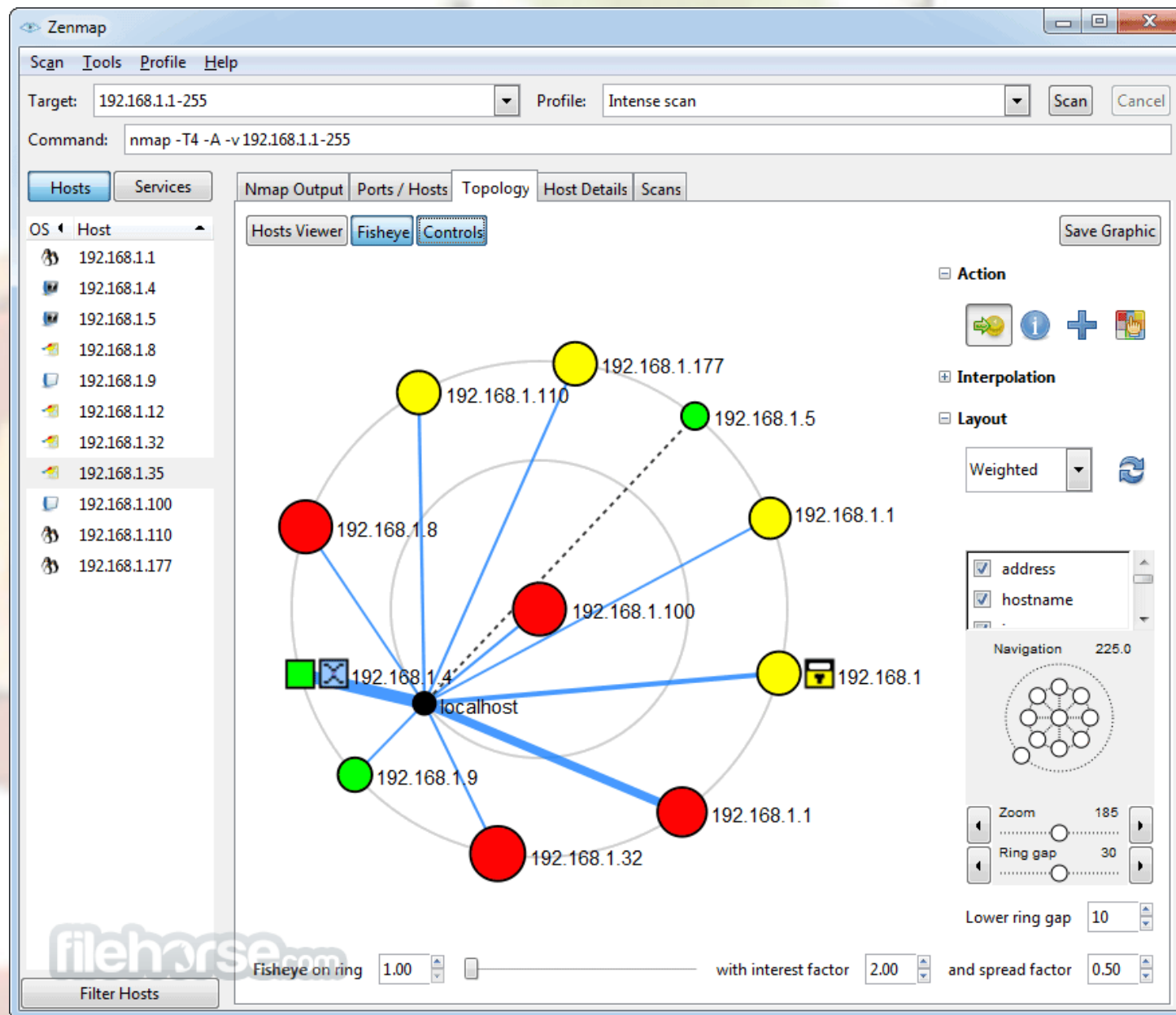
Reactivas

Herramientas

Ejemplos

Entidades





Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades

Herramientas de soporte al SOC

- **Monitoreo centralizado y automatizado de bitácoras.**
 - Nagios
 - Solarwinds
- **Alerta ante cambios críticos:**
 - Tripwire.
- **Rastreo de puertos:**
 - NMap
- **Análisis de tramas de red:**
 - Wireshark

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



test.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: tcp Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
11	1.226156	192.168.0.2	192.168.0.1	TCP	3196 > http [SYN] Seq=0 Len=0 MSS
12	1.227282	192.168.0.1	192.168.0.2	TCP	http > 3196 [SYN, ACK] Seq=0 Ack=
13	1.227325	192.168.0.2	192.168.0.1	TCP	3196 > http [ACK] Seq=1 Ack=1 Win
14	1.227451	192.168.0.2	192.168.0.1	HTTP	SUBSCRIBE /upnp/service/Layer3For
15	1.229309	192.168.0.1	192.168.0.2	TCP	http > 3196 [ACK] Seq=1 Ack=256 W
16	1.232421	192.168.0.1	192.168.0.2	TCP	[TCP Window Update] http > 3196
17	1.248355	192.168.0.1	192.168.0.2	TCP	1025 > 5000 [SYN] Seq=0 Len=0 MSS
18	1.248391	192.168.0.2	192.168.0.1	TCP	5000 > 1025 [SYN, ACK] Seq=0 Ack=
19	1.250171	192.168.0.1	192.168.0.2	HTTP	HTTP/1.0 200 OK
20	1.250285	192.168.0.2	192.168.0.1	TCP	3196 > http [FIN, ACK] Seq=256 Ac
21	1.250810	192.168.0.1	192.168.0.2	TCP	http > 3196 [FIN, ACK] Seq=114 Ac
22	1.250842	192.168.0.2	192.168.0.1	TCP	3196 > http [ACK] Seq=257 Ack=115
23	1.251868	192.168.0.1	192.168.0.2	TCP	1025 > 5000 [ACK] Seq=1 Ack=1 Win
24	1.252826	192.168.0.1	192.168.0.2	TCP	http > 3196 [FIN, ACK] Seq=26611
25	1.253323	192.168.0.2	192.168.0.1	TCP	3197 > http [SYN] Seq=0 Len=0 MSS
26	1.254502	192.168.0.1	192.168.0.2	TCP	http > 3197 [SYN, ACK] Seq=0 Ack=
27	1.254532	192.168.0.2	192.168.0.1	TCP	3197 > http [ACK] Seq=1 Ack=1 Win

Frame 11 (62 bytes on wire, 62 bytes captured)

Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)

Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)

Transmission Control Protocol, Src Port: 3196 (3196), Dst Port: http (80), Seq: 0, Len: 0

```

0000  00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00  ..[-u... ] ....E.
0010  00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8  .O.H@... a,.....
0020  00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02  ...|.P<6 .....p.
0030  fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02      ...'.....
  
```

File: "D:\test.pcap" 14 KB 00:00:02 P: 120 D: 103 M: 0 [Expert: Error]

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades





Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
42	43.774186	38:37:82:7f:b1:63	IntelCor_43:b1:01	ARP	42	192.168.1.1 is at 38:37:82:7f:b1:63
43	44.443928	192.168.1.12	255.255.255.255	DB-LSP...	176	Dropbox LAN sync Discovery Protocol
44	44.445996	192.168.1.12	255.255.255.255	DB-LSP...	176	Dropbox LAN sync Discovery Protocol
45	44.448048	192.168.1.12	192.168.1.255	DB-LSP...	176	Dropbox LAN sync Discovery Protocol
46	44.450067	192.168.1.12	255.255.255.255	DB-LSP...	176	Dropbox LAN sync Discovery Protocol
47	44.451904	192.168.1.12	255.255.255.255	DB-LSP...	176	Dropbox LAN sync Discovery Protocol
48	45.653923	fe80::ffff:ffff:ffff:fffe	ff02::2	ICMPv6	103	Router Solicitation
49	45.746010	fe80::8000:5337::10	fe80::ffff:ffff:ffff:ffff	ICMPv6	151	Router Advertisement

Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: LiteonTe_53:f1:ad (a4:db:30:53:f1:ad)
Sender IP address: 192.168.1.12
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.1.1

0000 ff ff ff ff ff ff a4 db 30 53 f1 ad 08 06 00 01 05.....
0010 08 00 06 04 00 01 a4 db 30 53 f1 ad c0 a8 01 0c 05.....
0020 00 00 00 00 00 00 c0 a8 01 01

Sender MAC address (arp.src.hw_mac), 6 bytes | Packets: 50 · Displayed: 50 (100.0%) | Profile: Default

Herramientas de soporte al SOC

- **Monitoreo centralizado y automatizado de bitácoras.**
 - Nagios
 - Solarwinds
- **Alerta ante cambios críticos:**
 - Tripwire.
- **Rastreo de puertos:**
 - NMap
- **Análisis de tramas de red:**
 - Wireshark
- **Detección de intrusos.**
 - Snort

Aspectos

Roles

Actividades

Preparatorias

Preventivas

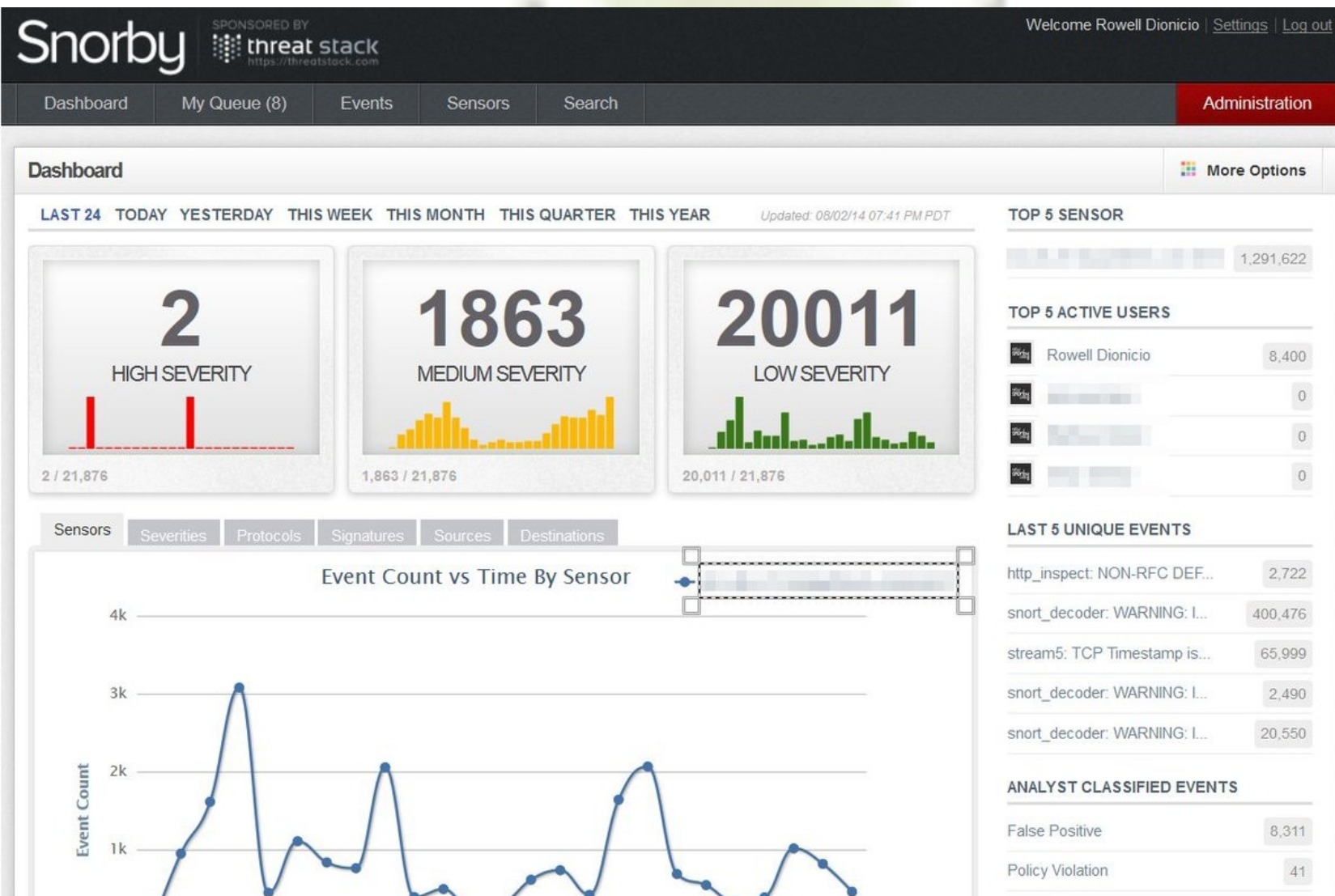
Reactivas

Herramientas

Ejemplos

Entidades





Aspectos

Roles

Actividades

Preparatorias

Preventivas

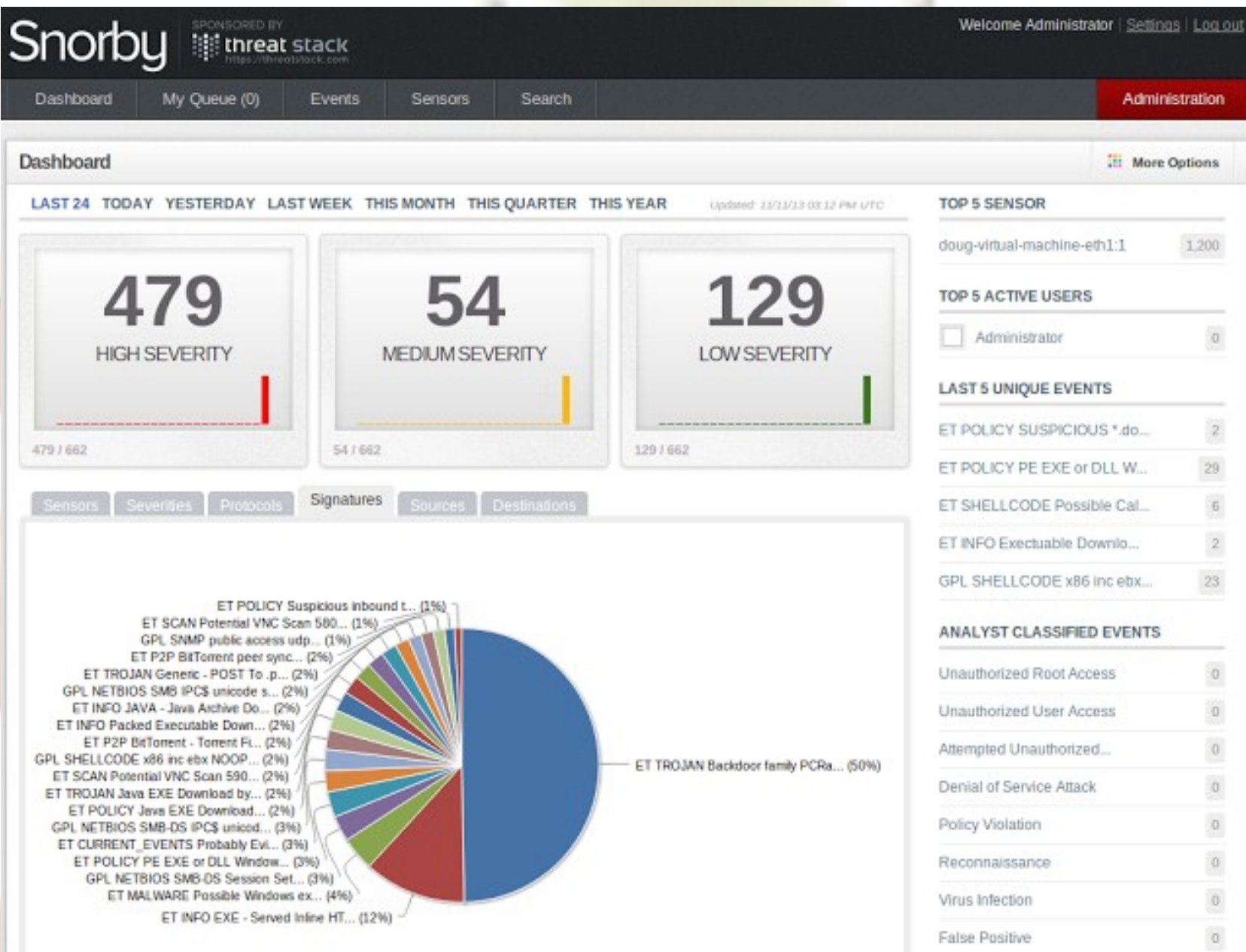
Reactivas

Herramientas

Ejemplos

Entidades





Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades





Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Snort Vulnerability Research Team (VRT) Rules

Enable Snort VRT ☒ Click to enable download of Snort VRT free Registered User or paid Subscriber rules

[Sign Up for a free Registered User Rule Account](#)
[Sign Up for paid Sourcefire VRT Certified Subscriber Rules](#)

Snort Oinkmaster Code

Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)

Snort GPLv2 Community Rules

Enable Snort GPLv2 ☐ Click to enable download of Snort GPLv2 Community rules

The Snort Community Ruleset is a GPLv2 VRT certified ruleset that is distributed free of charge without any VRT License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.

Emerging Threats (ET) Rules

Enable ET Open ☒ Click to enable download of Emerging Threats Open rules

ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.

Enable ET Pro ☐ Click to enable download of Emerging Threats Pro rules

[Sign Up for an ETPro Account](#)
ETPro for Snort offers daily updates and extensive coverage of current malware threats.

Sourcefire OpenAppID Detectors

Enable OpenAppID ☐ Click to enable download of Sourcefire OpenAppID Detectors

The OpenAppID package contains the application signatures required by the AppID preprocessor.

OpenAppID Version

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades





Snort - Network Intrusion ... NST Screen Shots (NST v1...

https://172.16.1.69/nstwui/cgi-bin/networking/snort.cgi

Network Interface Sensor	eth0 eth1 eth2 eth3 eth4 Note: Click on a NIC Adapter Icon for detailed Network Interface information.
Base Configuration Snort Rule Set Archives	☒ Local Disk: "/usr/share/snortrules/rules" ☐ Custom Snort Base Rules <input <="" <input="" p="" type="text" value="Password:"/> http://172.16.1.72/nst/snort-rules.tar.gz ☐ Current Registered Snort Rules <a href="http://www.snort.org/pub-bin/oinkmaster.cgi/<oinkcode>/snortrules-snapshot-CURRENT.tar.gz">http://www.snort.org/pub-bin/oinkmaster.cgi/<oinkcode>/snortrules-snapshot-CURRENT.tar.gz Notes: - Use: "Custom Snort Base Rules" to retrieve base configuration Snort rules from a specific archive site. - Use: "Current Registered Snort Rules" if one has obtained a registered "Oink Code" from "snort.org". Replace the "<oinkcode>" place holder with your own registered Oinkmaster "Oink Code". - An archive <u>must</u> contain at least a valid "snort.conf" file. - Use the "User Id" and "Password" fields for base rule site authentication if required.
Additional Snort Rule Set Archives	☐ Current Emerging Threats Rules http://emergingthreats.net/rules/emerging.rules.tar.gz ☐ Additional Rule Sets: 1 http://172.16.1.72/nst/snort-rules1.tar.gz ☐ Additional Rule Sets: 2 <input <="" <input="" p="" type="text" value="Password:"/> http://172.16.1.72/nst/snort-rules2.tar.gz Note: Use the "User ID" and "Password" fields for additional rule site authentication if required.
Setup/Start Snort	☐ Startup this instance of Snort immediately after setup.
Home Net	any Note: You may want to consider using: "172.16.1.0/24", "24.0.0.0/8" and/or "24.97.150.194/32". Examples: "any", "Seth0_ADDRESS", "10.1.1.0/24", "[10.1.1.0/24,192.168.1.0/24]".
External Net	any Note: Examples: "any", "Seth1_ADDRESS", "!\$HOME_NET".
Sensor Alias Name	172.16.1.69 Network 1
Additional Setup Snort Script Options	<code>-v -rdir /var/nst</code> Action: [Clear] [-v] [-rdir /var/nst] [Change Snort MySQL Database Access Password] Note: - Do not use the Interface: "-i", Base Rule Source: "-r", Additional Rule Sources: "-ars", "--External_NET", "--HOME_NET" or the "--sensor-name" options. These are already included above. See: "Setup Snort Script Options" below. - Use the "Change Snort MySQL Database Access Password" action to <i>change</i> the "password" for Snort to store IDS alerts to the local MySQL database.
Remote Snort IDS Collector Options	☐ Use a remote Snort IDS Collector. <input <="" <input="" p="" text"="" type="text" value="Password:"/>
Additional Snort Command Options	Docs: [Snort Man Page] [Snort Reference Manual] [Snort FAQ] Note: Do not use the Daemon Mode: "-D", Listen On Interface: "-i" or the Use Rules File: "-c" option. These are already included above. See the "snort" man page for available options.

Setup/Start Snort

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



Herramientas

- **Identificación de vulnerabilidades**

- **OpenSource / Free**



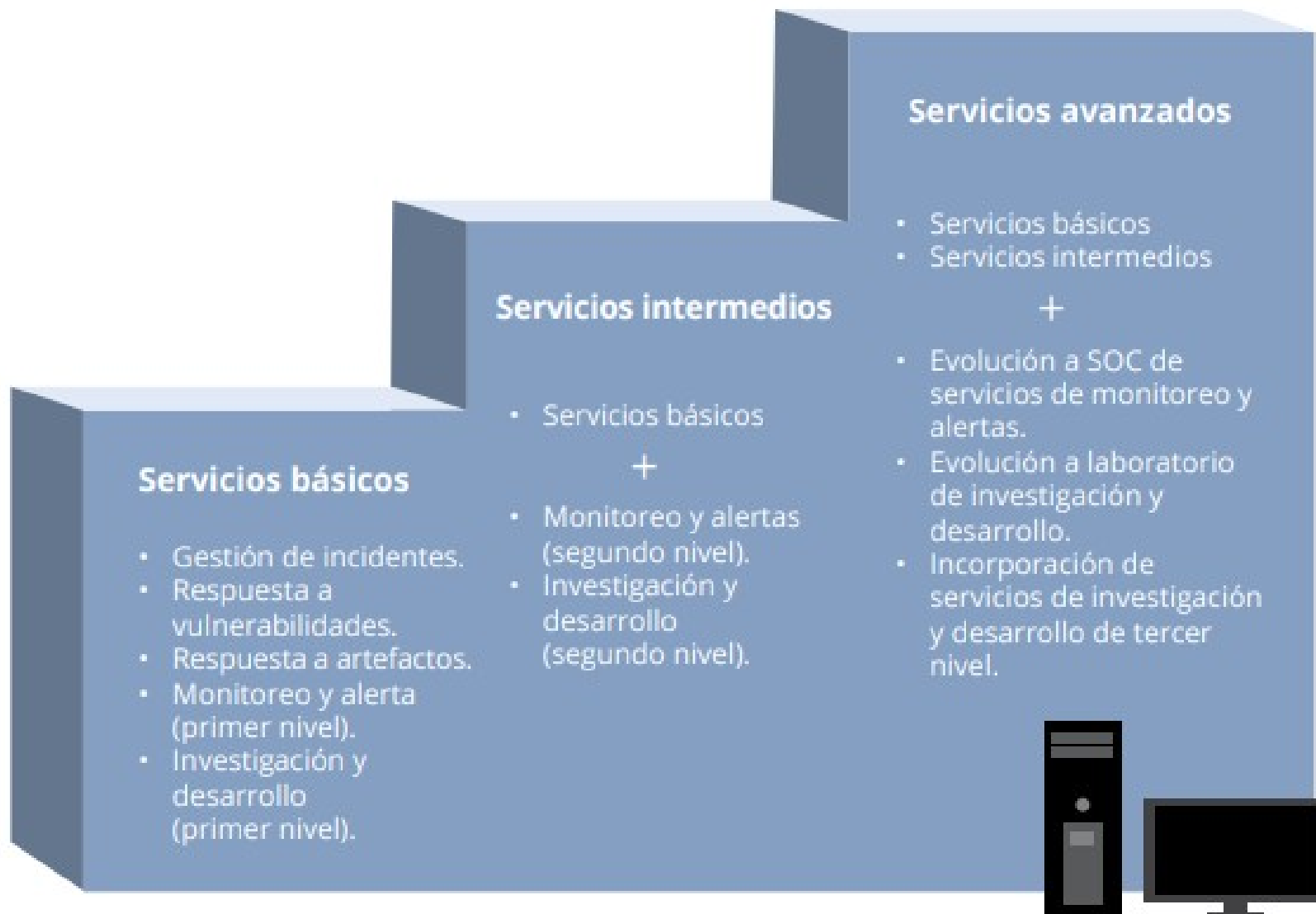
- **Privado**



Ejemplos



Madurez CIRT según la OEA



Aspectos

Roles

Actividades

Preparatorias

Preventivas

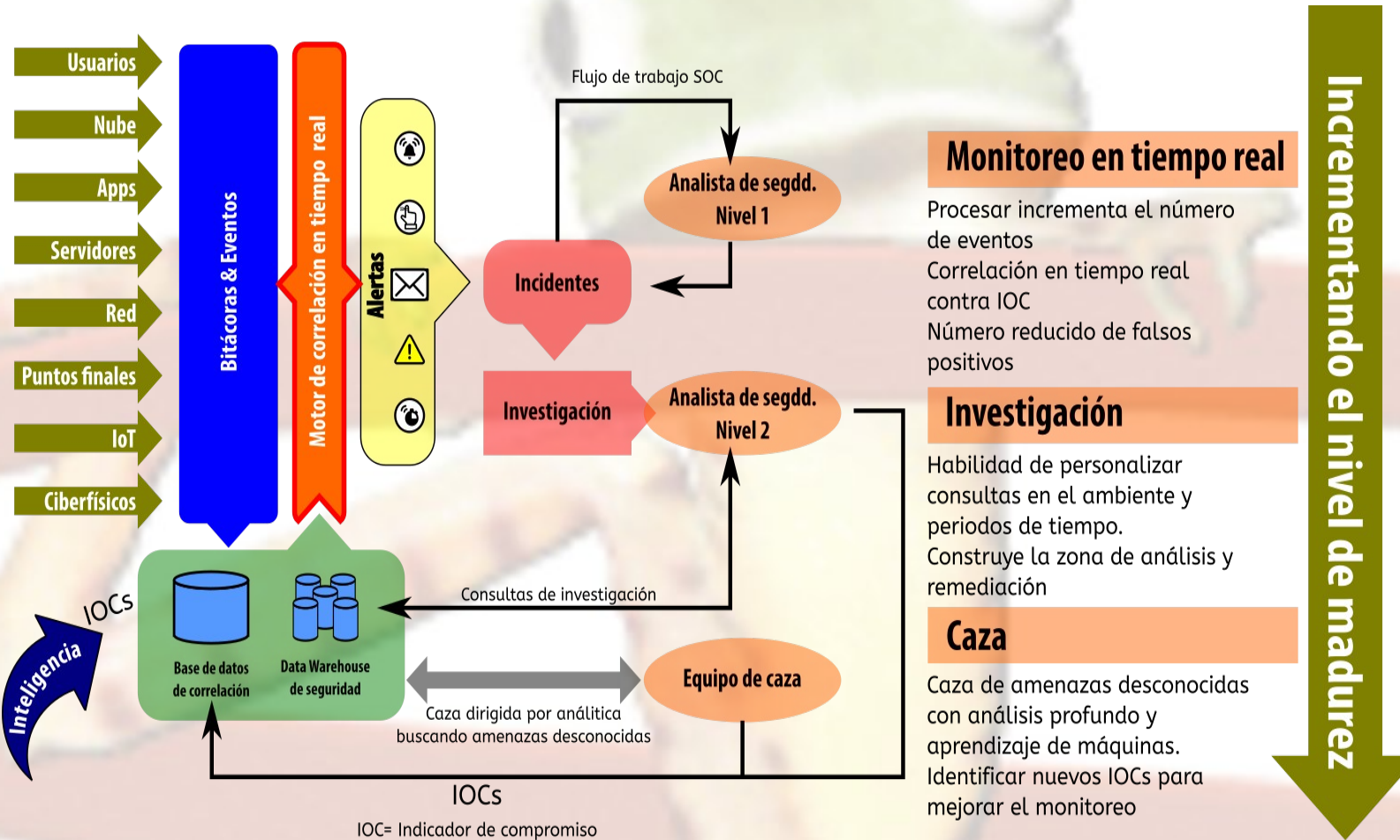
Reactivas

Herramientas

Ejemplos

Entidades

Modelo HP



Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades

Fuente: Paul Brettle, Hewlett Packard

<https://www.youtube.com/watch?v=ih0SC-dN6MU>

HP's: Security Intelligence Capability

• <https://youtu.be/ih0SC-dN6MU>

Security intelligence

Análisis en profundidad
Fusión de información
Análisis predictivo por naturaleza
Descubrimiento de nuevas amenazas
Casos de uso avanzados

Real time analysis & incident response

Monitoreo de eventos en tiempo real
CIRT - Flujo de trabajo integrado
Minimizar los tiempos de respuesta
Afinamiento continuo

Near time alerting

Retroalimentación de los eventos
Correlación de alta fidelidad
Reportes personalizados

Data Analysis

Tecnologías de correlación
Análisis de evidencia forense
Construcción de reportes automáticos

Log Management

Bitácoras centralizadas
Datos retenidos
Cumplimiento de normatividad

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades

Fujitsu - Outsourcing

- <https://youtu.be/6LwyTWPKDnQ>

Aspectos

Roles

Actividades

Preparatorias

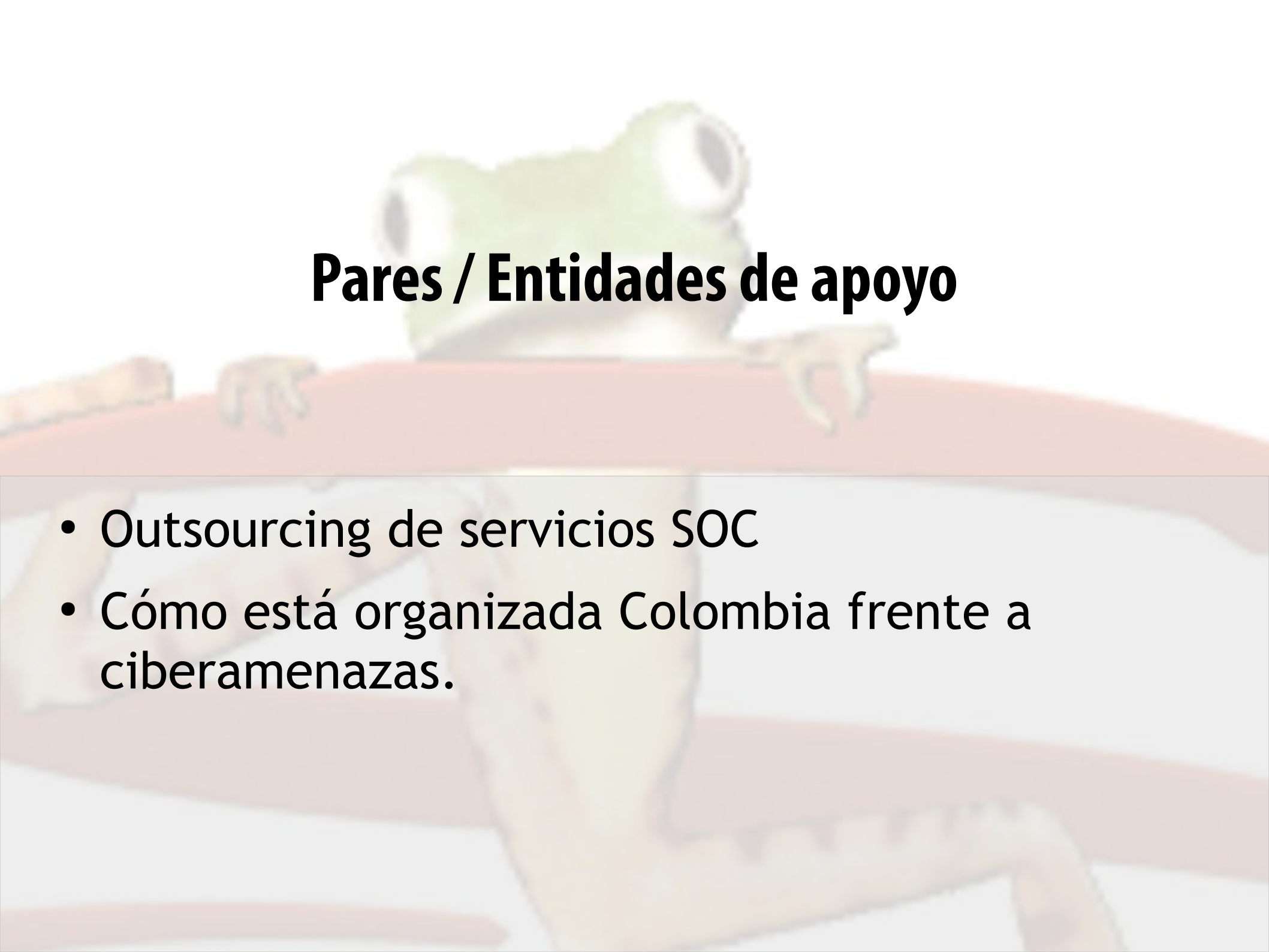
Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



Pares / Entidades de apoyo

- Outsourcing de servicios SOC
- Cómo está organizada Colombia frente a ciberamenazas.

CONPES 3701 de 2011

<https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf>

- Lineamientos de política para ciberseguridad y ciberdefensa.



Gráfica No. 5 Modelo de Coordinación
Fuente: Ministerio de Defensa Nacional

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



Instituciones de Ciberdefensa Nacional



Comando Conjunto Cibernético



Unidad Cibernética Ejército Nacional



Unidad Cibernética Armada Nacional



Unidad Cibernética Fuerza Aérea

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades

CONPES 3854 de 2016

• Política Nal. de seguridad digital

Institucionalidad en materia de Seguridad Digital

**COORDINADOR NACIONAL:
PRESIDENCIA DE LA REPÚBLICA**



INVESTIGACIÓN Y
RESPUESTA ANTE
DELITOS
CIBERNÉTICOS



SALVAGUARDAR LOS
INTERESES
NACIONALES EN EL
CIBERESPACIO



COORDINAR A NIVEL
NACIONAL EN
ASPECTOS DE
CIBERSEGURIDAD Y
CIBERDEFENSA



MINTIC

CONCIENCIA
CIUDADANA
LÍDER DE LA POLÍTICA
DE SEGURIDAD
DIGITAL PARA
GOBIERNO



JUDICIALIZACIÓN



PRIMER CSIRT
SECTORIAL, CSIRT DE
GOBIERNO

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



CONPES 3854 de 2016 “Política Nacional De Seguridad Digital”

<https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>

- Concepto de “seguridad digital”
- Identifica ejes de acción.
 - Fortalecer.
 - Consolidar.
 - “elaborar el plan de fortalecimiento de las capacidades operativas, administrativas, humanas, científicas, de infraestructura física y tecnológica del Grupo colCERT, como punto focal nacional para la gestión de incidentes digitales en Colombia”

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



- **FIRST** (<https://www.first.org/>)
- **Global Forum of Incident Response and Security Teams**

Team	Official Team Name	Country
CSIRT OLIMPIA	COMPUTER SECURITY INCIDENT RESPONSE TEAM OF OLIMPIA DIGITAL	 CO
CSIRT-CCIT	Computer Security Incident Response Team of the Colombian Informatics and Telecommunications Chamber	 CO
CSIRT-ETB	Computer Security Incident Response Team - Empresa de Telecomunicaciones de Bogotá S.A. ESP	 CO
CSIRTPONAL	Response Team Computer Security Incident of the Colombian National Police	 CO
DigiCSIRT	DigiSOC Computer Security Incident Response Team	 CO
ETEK-CSIRT	Computer Security Incident response team of ETEK International	 CO
ShieldNow	ShieldNow	 CO
SOC Team Claro Colombia	Security Operations Center Team Claro Colombia	 CO
SOC-CCOC	Security Operations Center - Cyber Operations Command Joint	 CO

FIRST follows the International Olympic Committee (IOC) country name listings.

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



¿De quién depende el ColCERT?



Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades

CSIRT sectoriales en Colombia

- **CSIRT Defensa - 2012**
- **CSIRT Gobierno - 2017**
- **CSIRT Financiero -2017**
- **CSIRT Eléctrico (En construcción)**

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

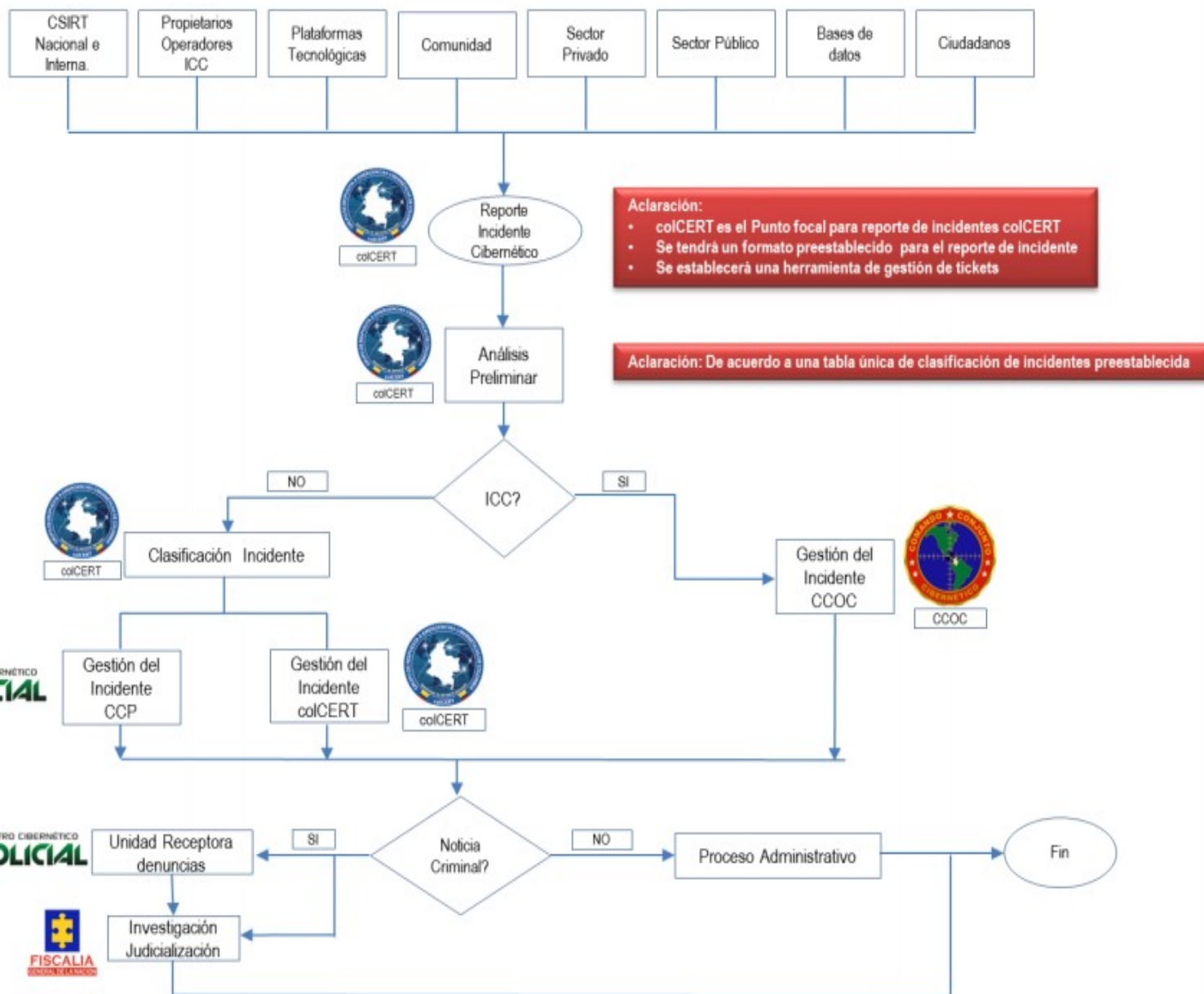
Herramientas

Ejemplos

Entidades



Reporte de incidentes



Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades

Denuncias de Cibercrimen en la PONAL

The screenshot displays the PONAL website interface. At the top, there's a header with the logos of the Policía Nacional de Colombia and the República de Colombia, along with the date and time: Domingo 19 de Mayo de 2019 18:11:59. Below the header is a navigation bar with icons for Inicio, Servicios, Ciberseguridad, APPS, Mural Cibercrimen, Observatorio Cibercrimen, Multimedia, Ciberincidentes, and Contáctenos. The main content area features a large banner for the 'CENTRO CIBERNÉTICO POLICIAL' with the text '¡ADENUNCIAR! Sistema Nacional de Denuncia Virtual'. A hand is shown using a stylus to interact with a tablet displaying the system. On the left side of the banner, there's a list of cybercrimes: Mediosidad, Violencia, Estafa por compra y/o venta, Mensajes de texto, Malware, Ingeniería y/o Colaboración a través, and Swatting. On the right side, there's a list of user types: Ciudadano, Ciudadano, Ciudadano, Ciudadano, Ciudadano, Ciudadano, and Ciudadano. At the bottom left, there's a button labeled 'Reportar Incidente Informático' and a status bar showing 'Esperando zopim.com...'. At the bottom right, there's a logo for 'CAI VIRTUAL'.

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades



Denuncias de Cibercrimen en la PONAL



 Análisis de Malware A través de esta opción, usted podrá cargar su muestra de Malware para ser analizada.  Ingresar	 Reporte Reporte los delitos informáticos - Ley 1273 de 2009.  Ingresar
 CAI Virtual Primera iniciativa en Iberoamérica en atención en línea policial.  Ingresar	 Ciberseguridad Encuentre las recomendaciones, boletines, guías, informes e infografías de ciberseguridad.  Ingresar
 APPS Aplicaciones móviles para el fortalecimiento de la ciberseguridad.  Ingresar	 Mural Cibercrimen Publicación de las diferentes modalidades delictivas presentadas por los ciberdelincuentes.  Ingresar

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades

Referencias

- <https://www.dflabs.com/blog/understanding-the-difference-between-socs-and-csirts/>
- <https://www.blogdelciso.com/2018/08/15/noc-soc-csirtcert-no-es-lo-mismo/>
- <https://www.techopedia.com/definition/31003/computer-emergency-response-team-cert>
- <https://www.csirt.org/>

Aspectos

Roles

Actividades

Preparatorias

Preventivas

Reactivas

Herramientas

Ejemplos

Entidades

A green tree frog is perched on a thick, reddish-brown branch. The frog is facing forward, with its large, white eyes and green skin clearly visible. The background is a soft, out-of-focus light green.

Muchas Gracias

¿Preguntas?

ventas@skinait.com

<http://www.skinait.com>

Security Operations Center por Ricardo Naranjo Faccini se distribuye bajo una Licencia Creative Commons Atribución 4.0 Internacional.

Basada en una obra en <https://www.skinait.com/SOC-CSIRT-Escritos-54/>.

