Fundada 2003

Skína IT Solutions

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

Ing. Ricardo Naranjo Faccini, M.Sc.

2018-11-22

https://www.skinait.com/SOC-CSIRT-Escritos-54/

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.

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 organz/entidad/Nación
  - Externos: brindan servicios pagados de forma continua o según sea necesario.

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.

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 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.

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.**

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.

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

Roles del SOC o CSIRT

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.**

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:
    - ¿Quienes son? ¿Cómo me pueden ayudar? ¿cuándo acudir?
    - ¿Cómo puedo ayudarlos?

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

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.

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

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.
    - Distribuído.
- Auditorías periódicas.
  - Aconsejar / Capacitar personal.
    - moodle
  - Prevenir.

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.

Actividades del SOC

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

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.

Actividades reactivas

Desencadenadas por un incidente o requerimiento.

Actividades del SOC

- Triaje 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

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.

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

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

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.

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/

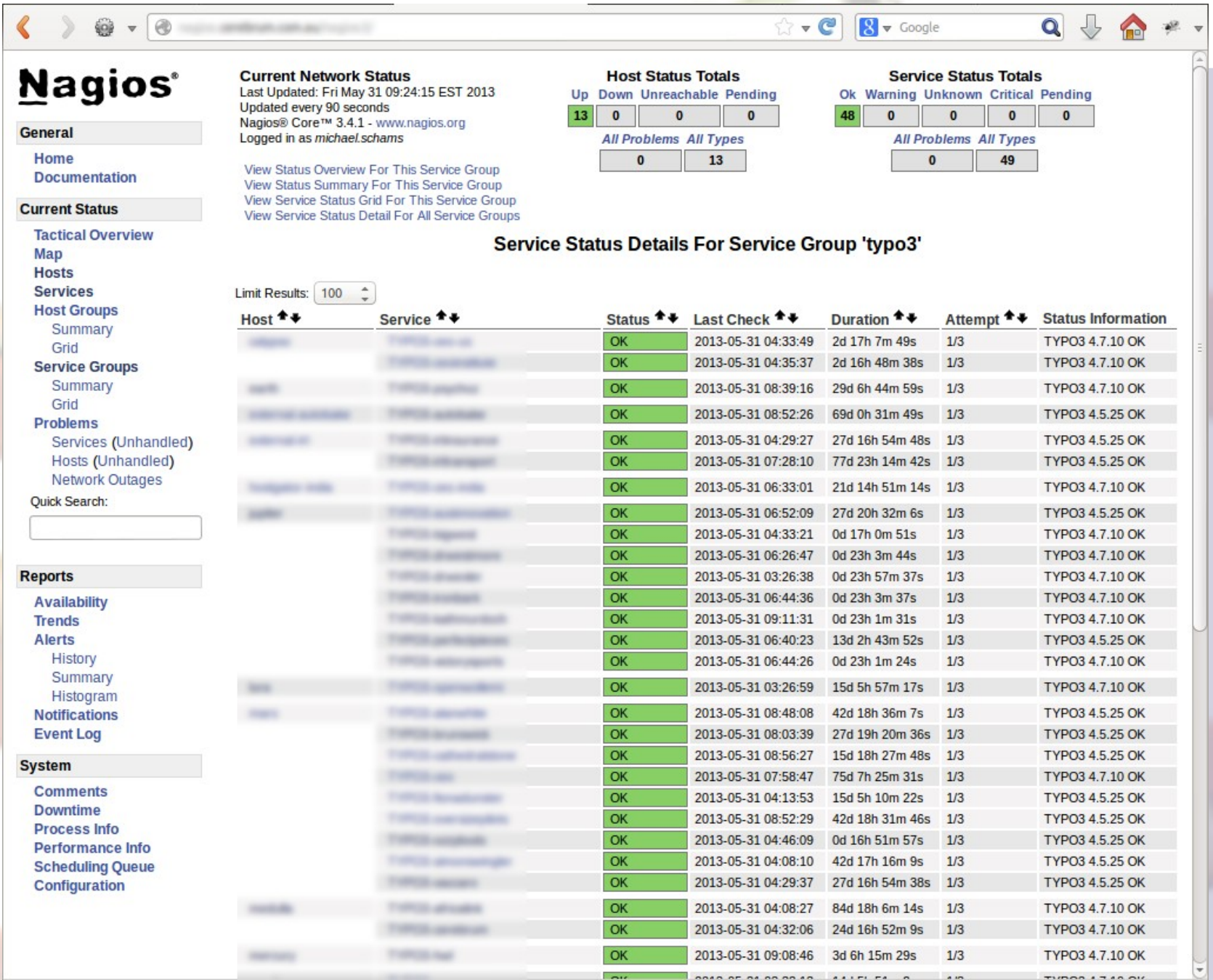
Herramientas de soporte al SOC

- Monitoreo centralizado y automatizado de bitácoras.
  - Nagios
  - Solarwinds

Nagios

Fundada 2003

SkínaIT Solutions



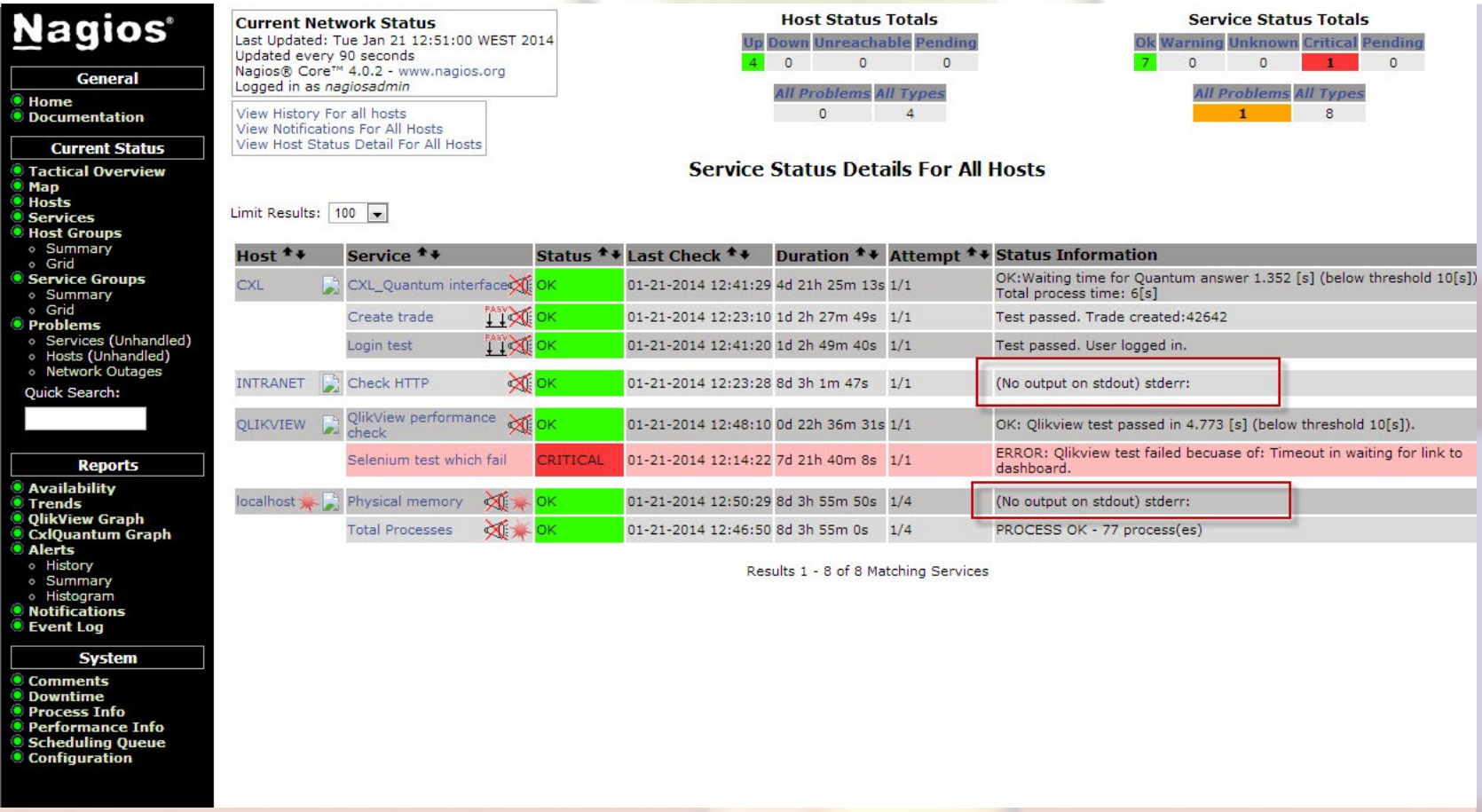
- Aspectos
- Roles
- Actividades
  - Preparatorias
  - Preventivas
  - Reactivas
- **Herramientas**
- Ejemplos
- Entidades

CO COLOMBIA

Nagios

Fundada 2003

Skína IT Solutions



Aspectos

Roles

Actividades

- Preparatorias
- Preventivas
- Reactivas

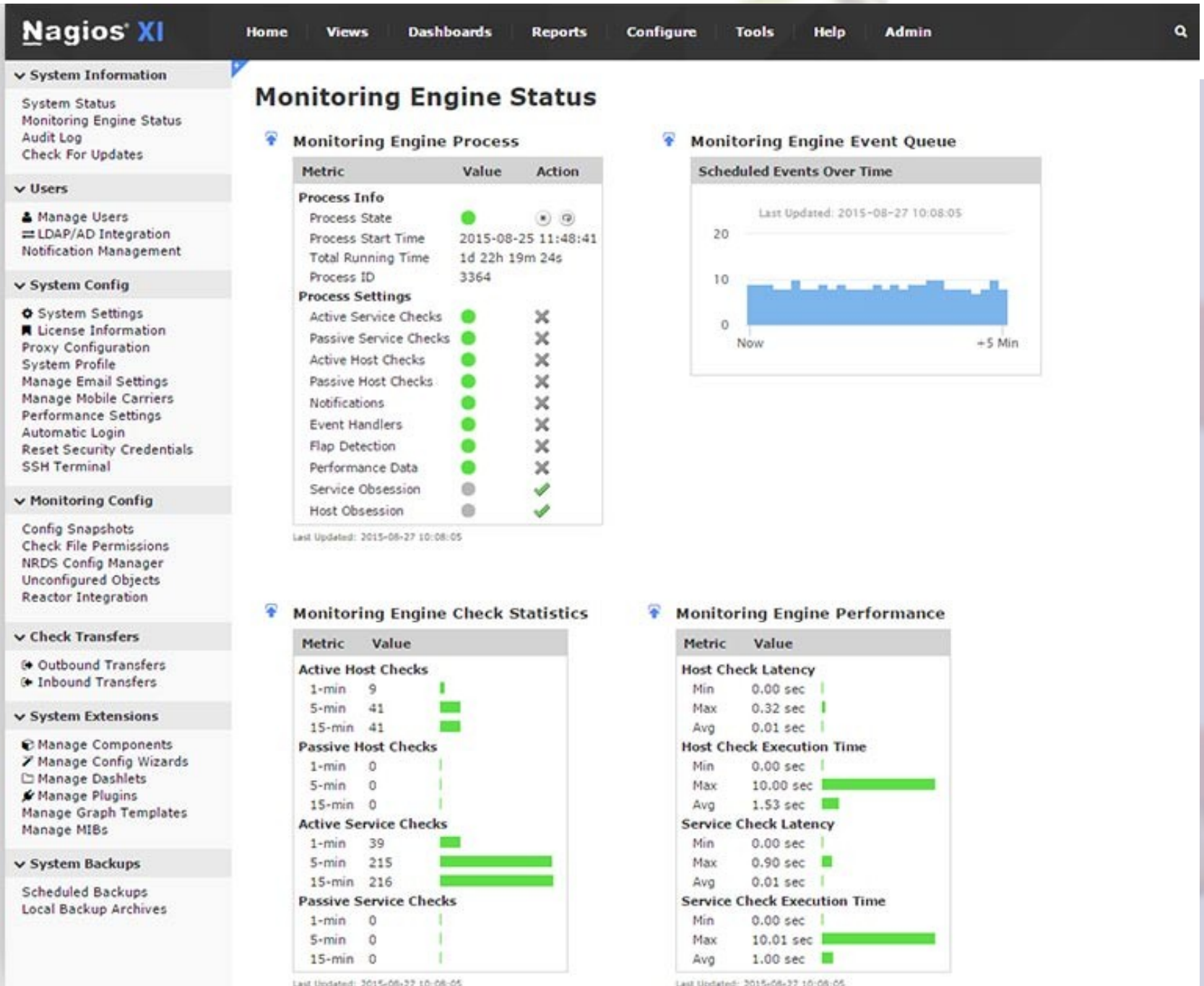
Herramientas

Ejemplos

Entidades

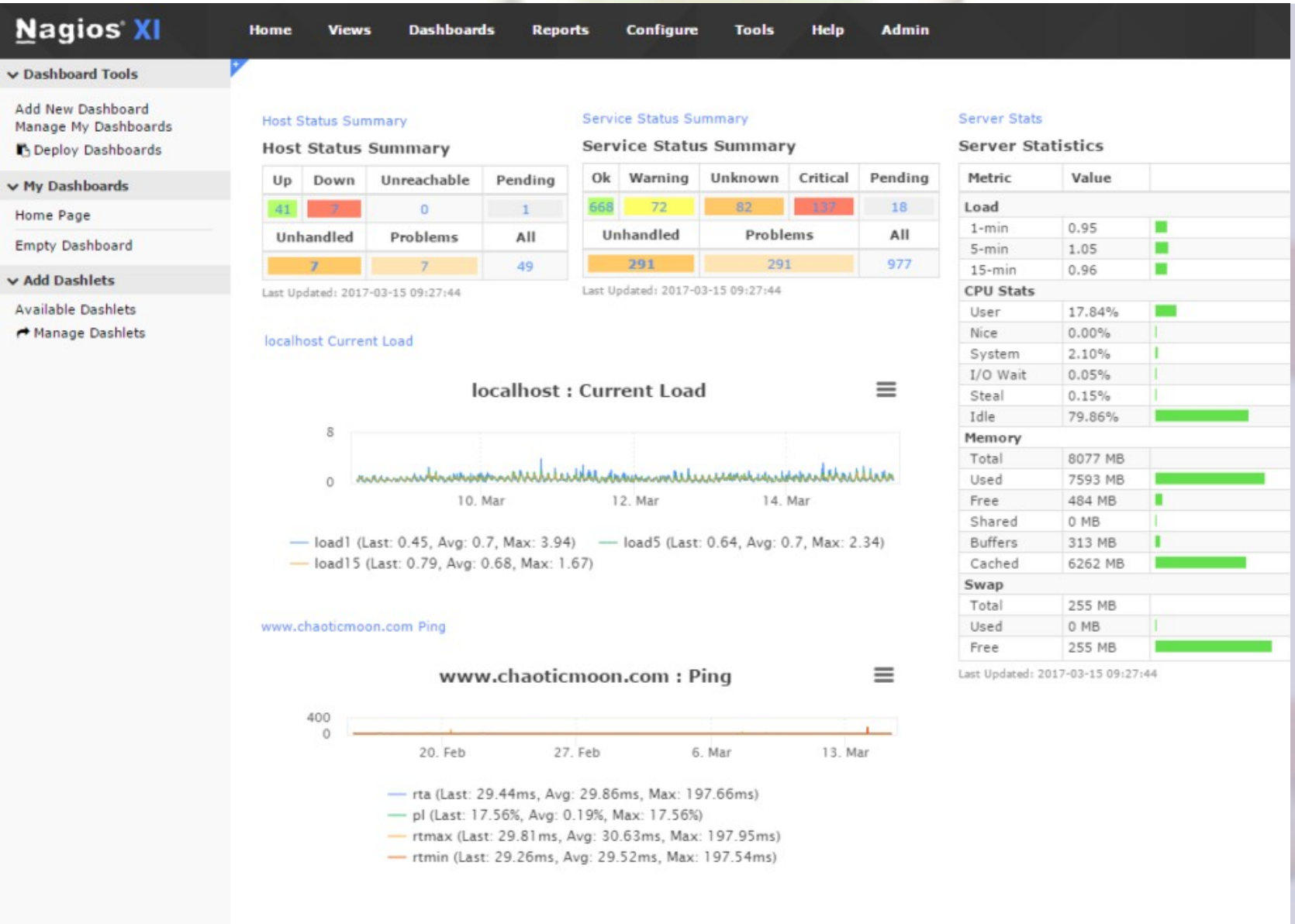
CO COLOMBIA

Nagios



Nagios

Fundada 2003
SkínaIT Solutions



CO COLOMBIA

Nagios

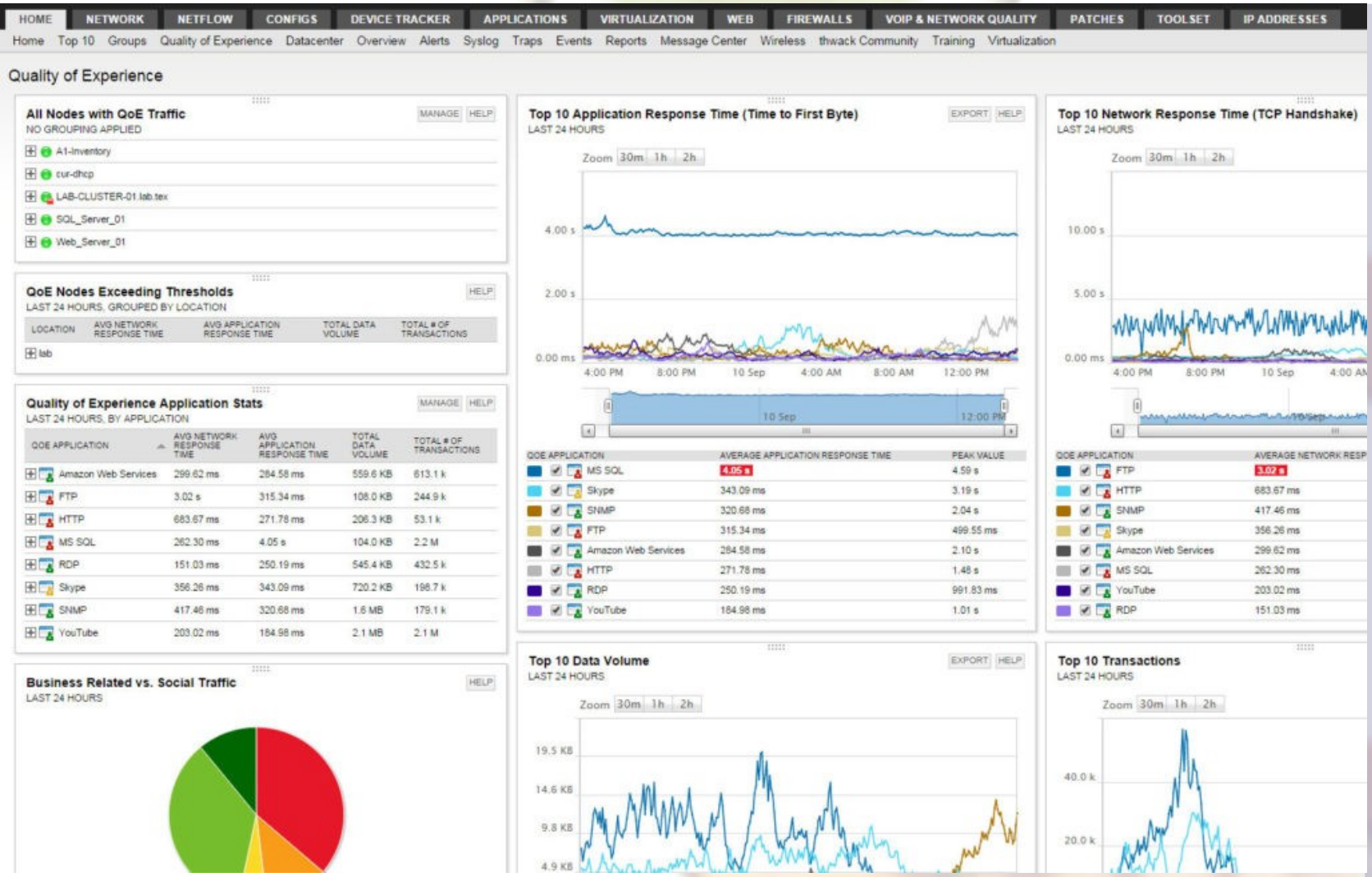
Fundada 2003

SkínaIT Solutions

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

CO COLOMBIA

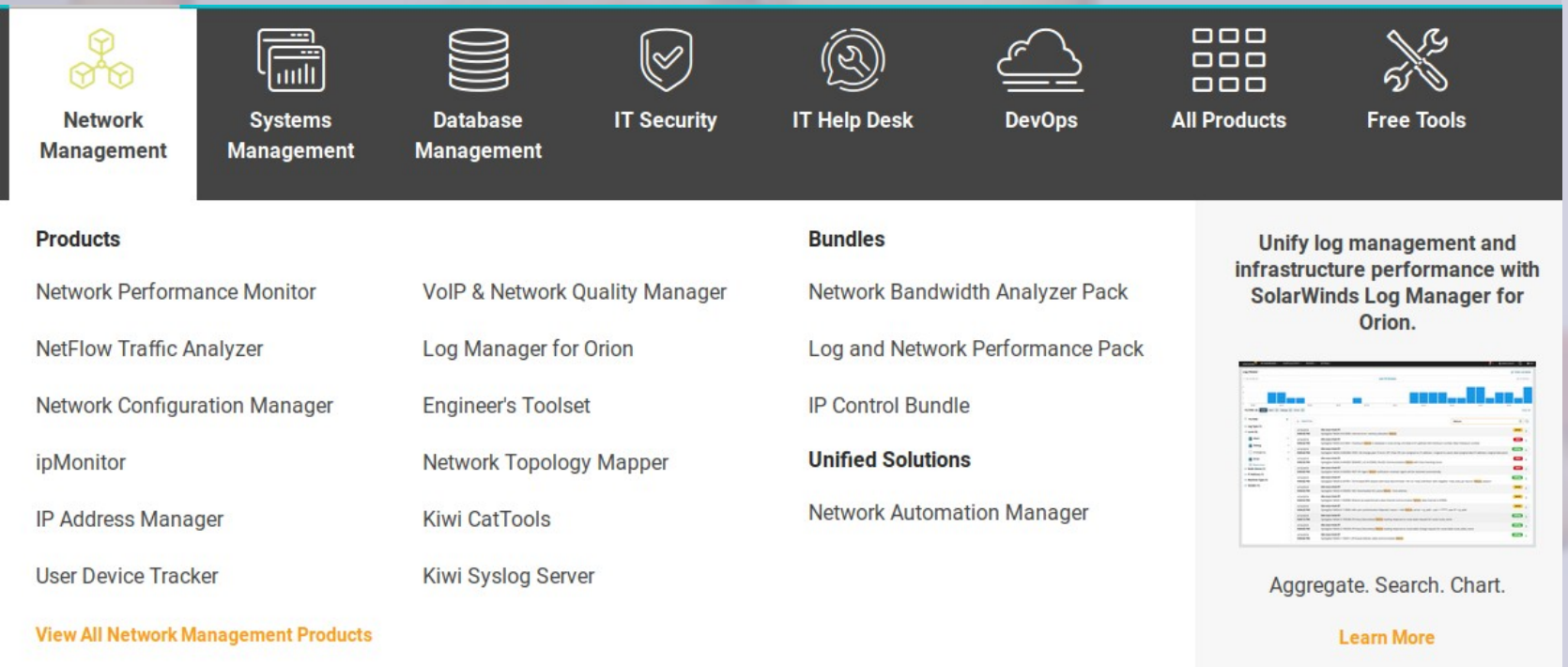
Solarwinds



Solarwinds

Solarwinds

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



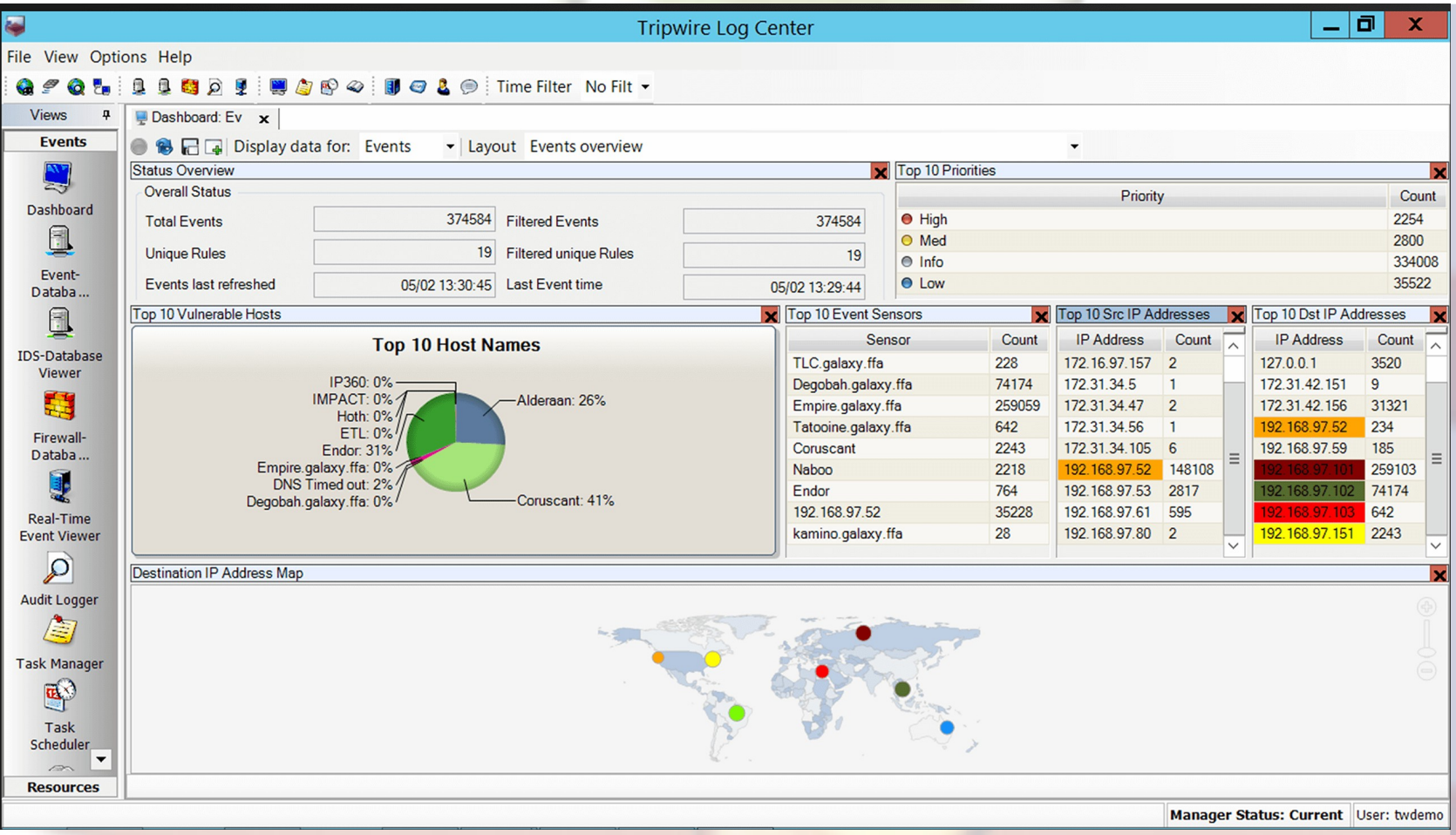
Herramientas de soporte al SOC

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

Tripwire

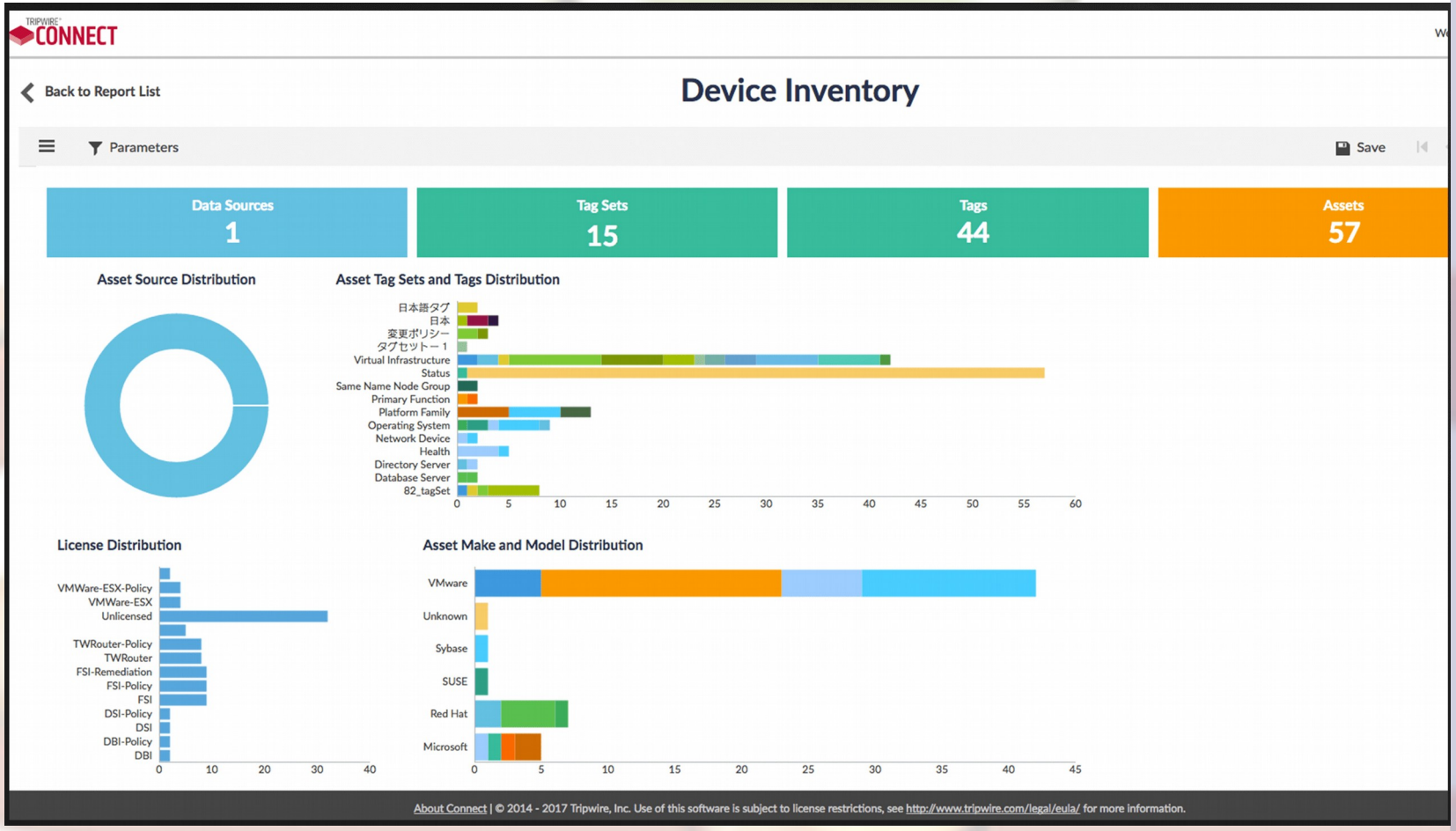
Fundada 2003

Skina IT Solutions



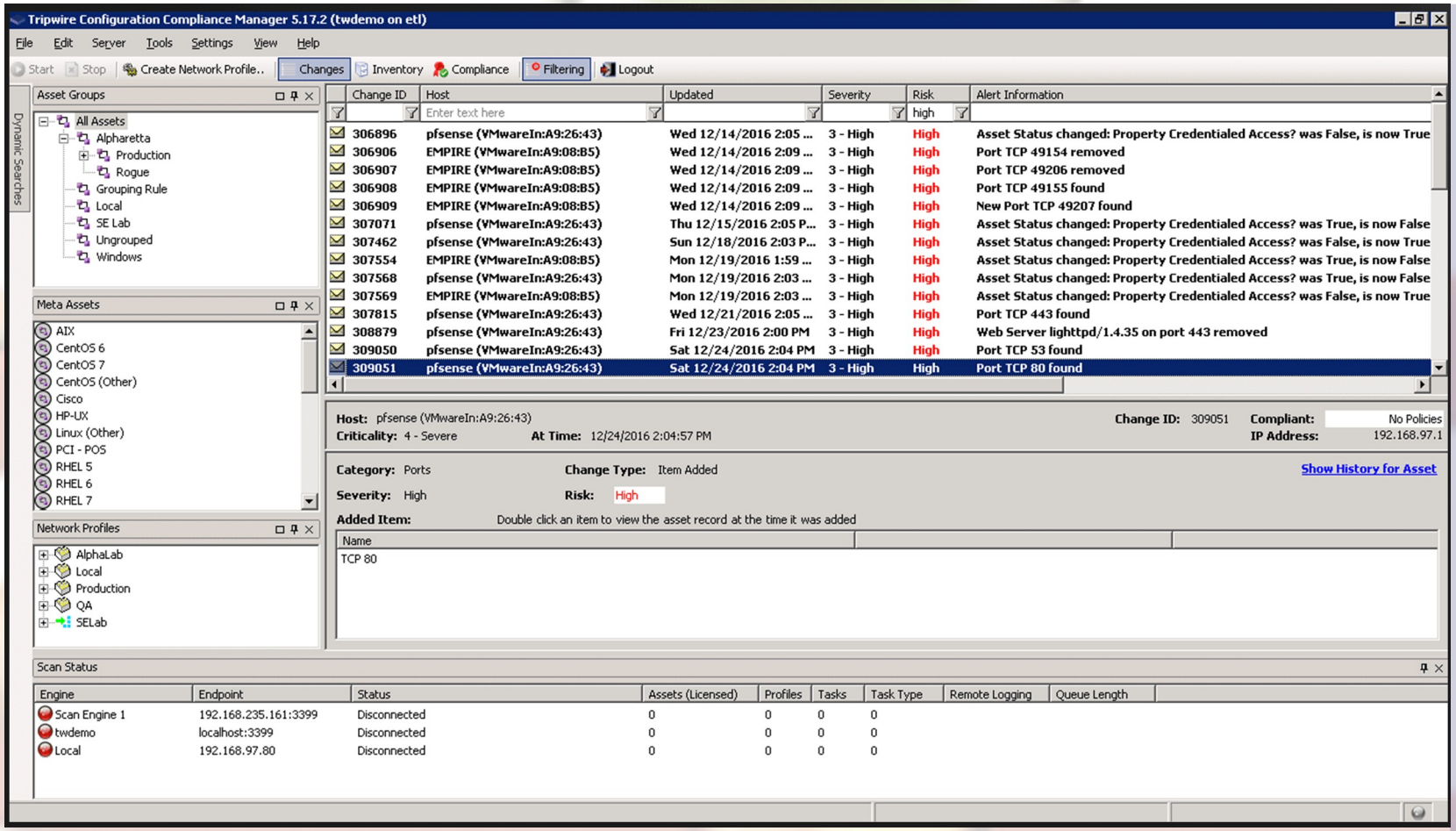
CO COLOMBIA

Tripwire



- Aspectos
- Roles
- Actividades
  - Preparatorias
  - Preventivas
  - Reactivas
- **Herramientas**
- Ejemplos
- Entidades

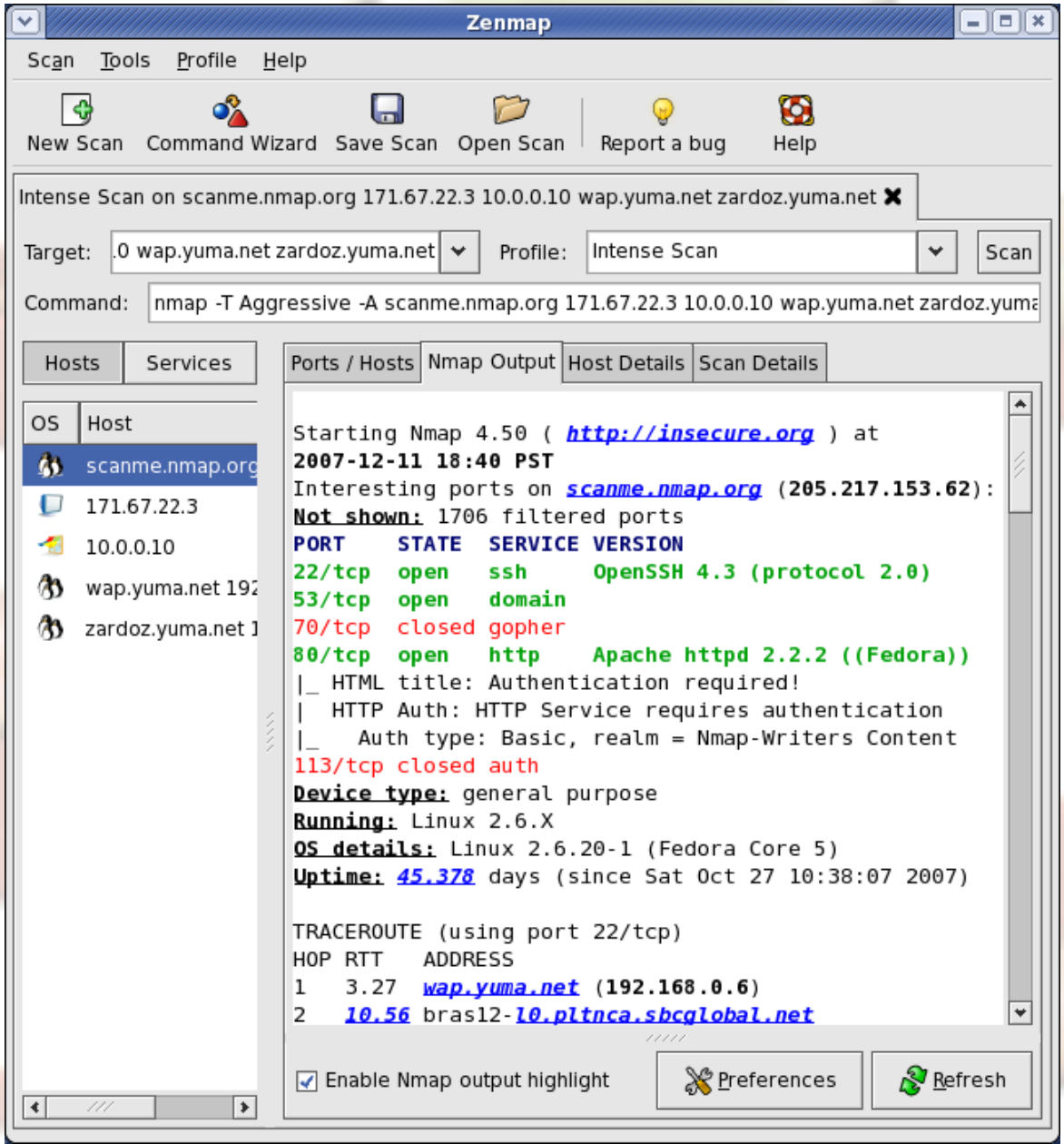
Tripwire



- Aspectos
- Roles
- Actividades
  - Preparatorias
  - Preventivas
  - Reactivas
- **Herramientas**
- Ejemplos
- Entidades

Herramientas de soporte al SOC

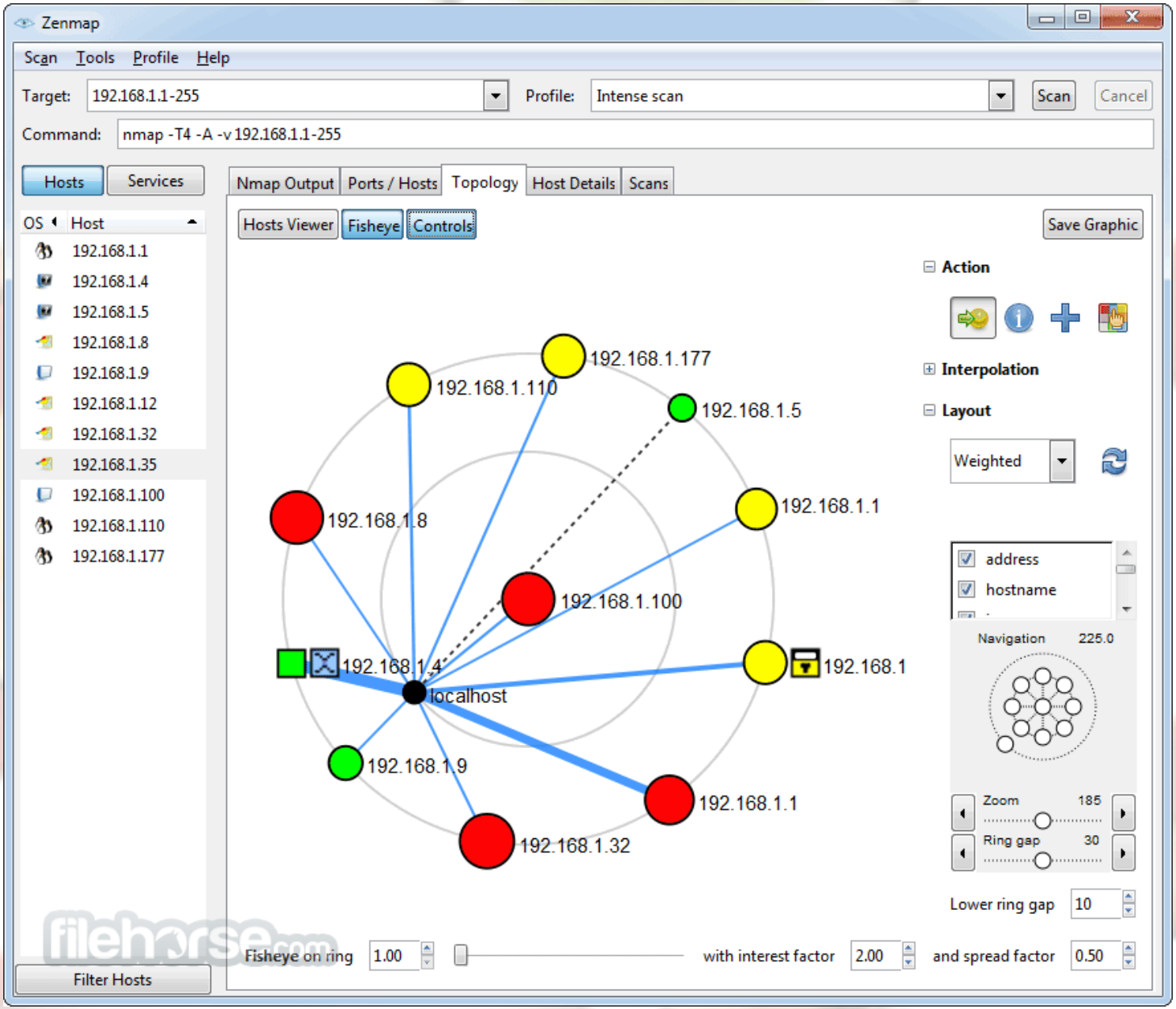
- Monitoreo centralizado y automatizado de bitácoras.
  - Nagios
  - Solarwinds
- Alerta ante cambios críticos:
  - Tripwire.
- Rastreo de puertos:
  - NMap



NMAP

Fundada 2003

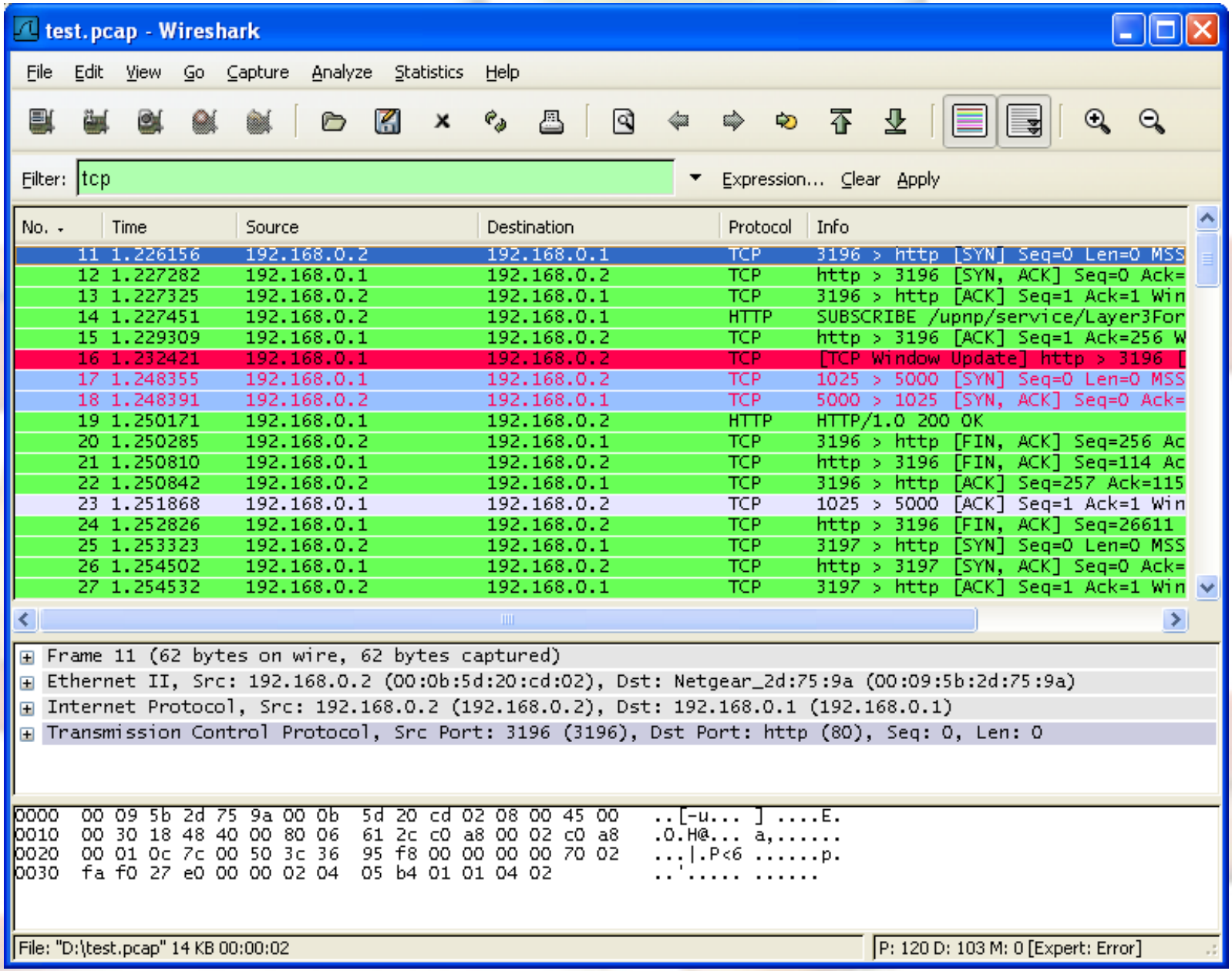
SkínaIT Solutions

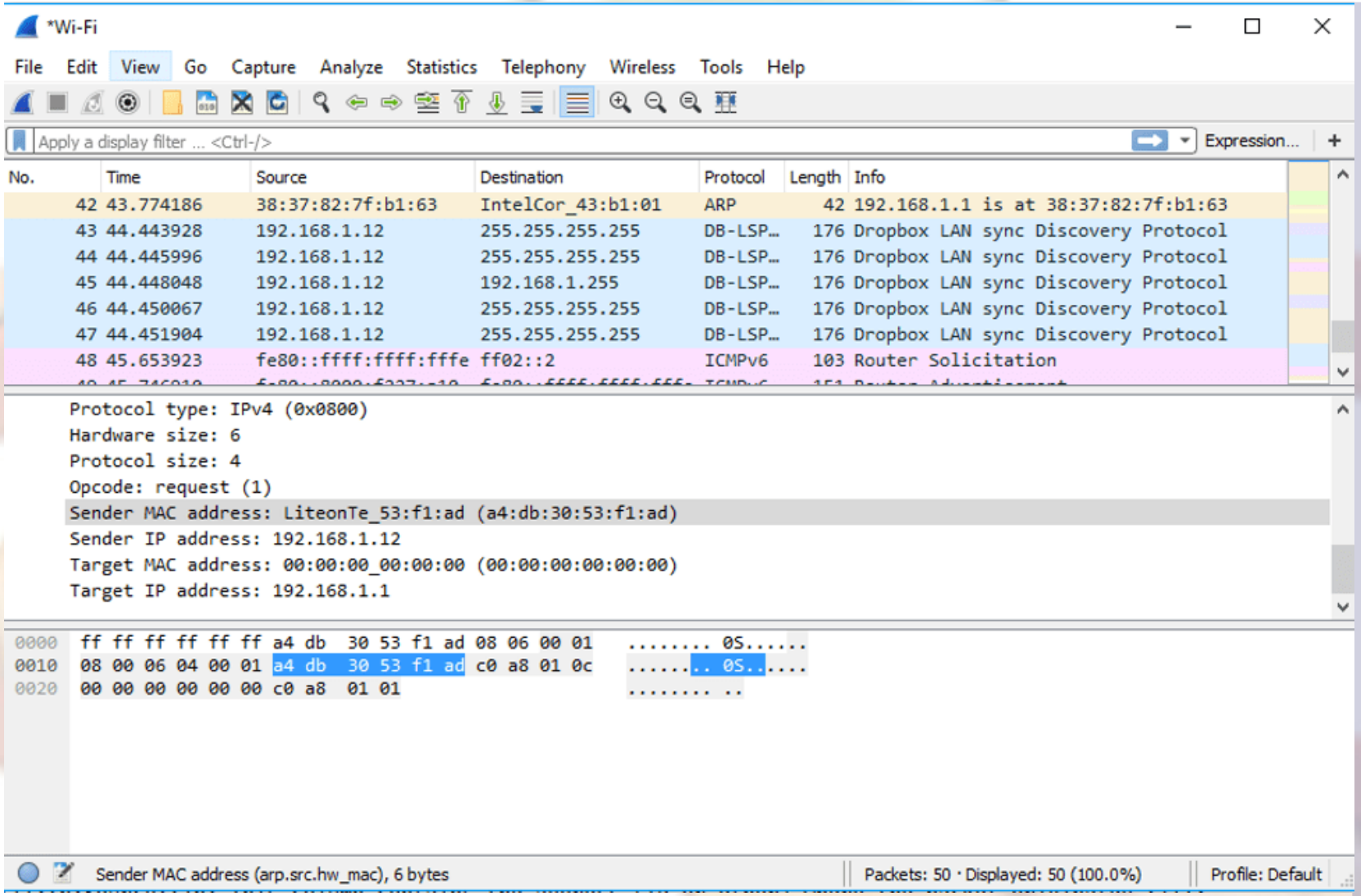


CO COLOMBIA

Herramientas de soporte al SOC

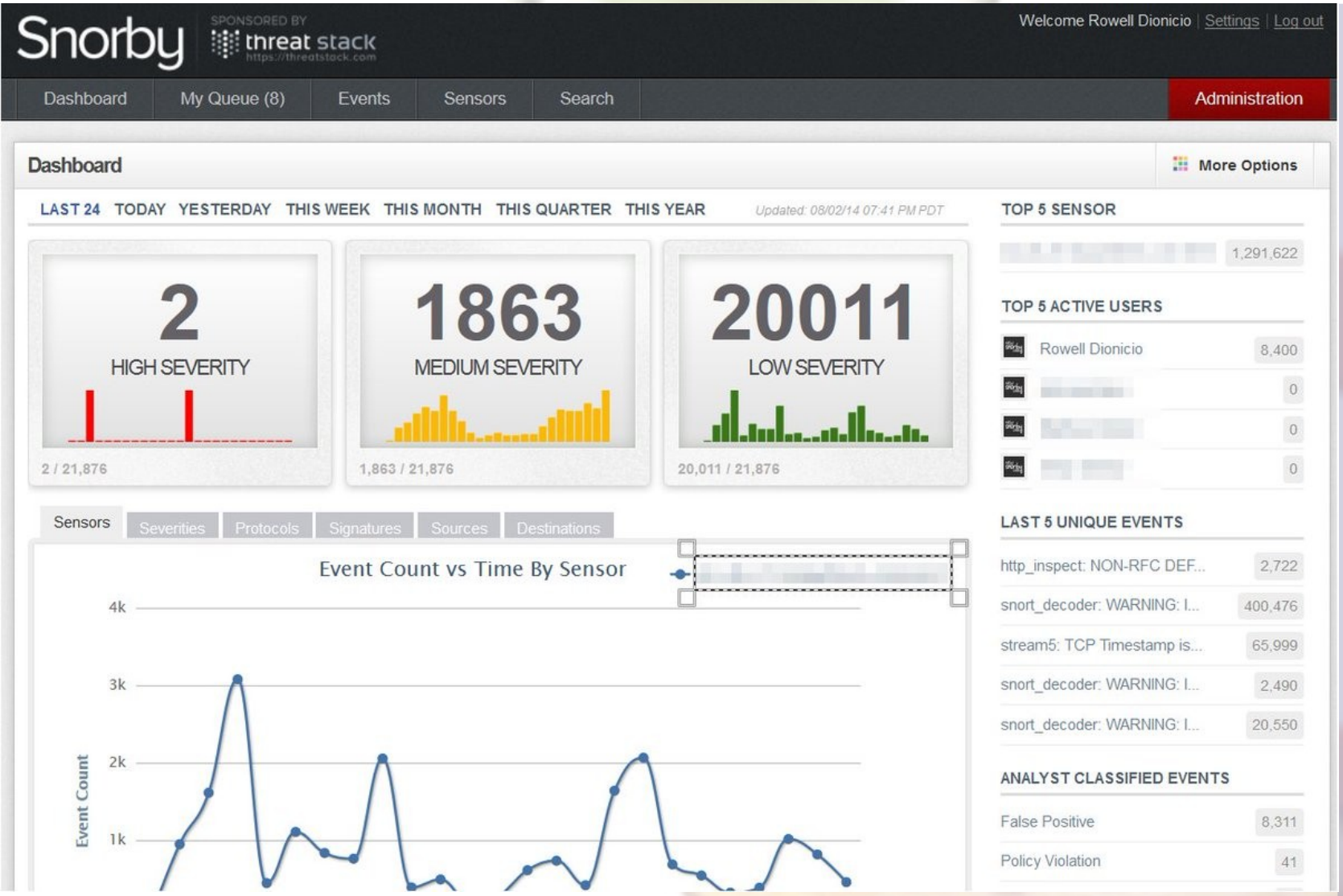
- Monitoreo centralizado y automatizado de bitácoras.
  - Nagios
  - Solarwinds
- Alerta ante cambios críticos:
  - Tripwire.
- Rastreo de puertos:
  - NMap
- Analisis de tramas de red:
  - Wireshark


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 .0.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]



Herramientas de soporte al SOC

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



Aspectos

Roles

Actividades

Preparatorias

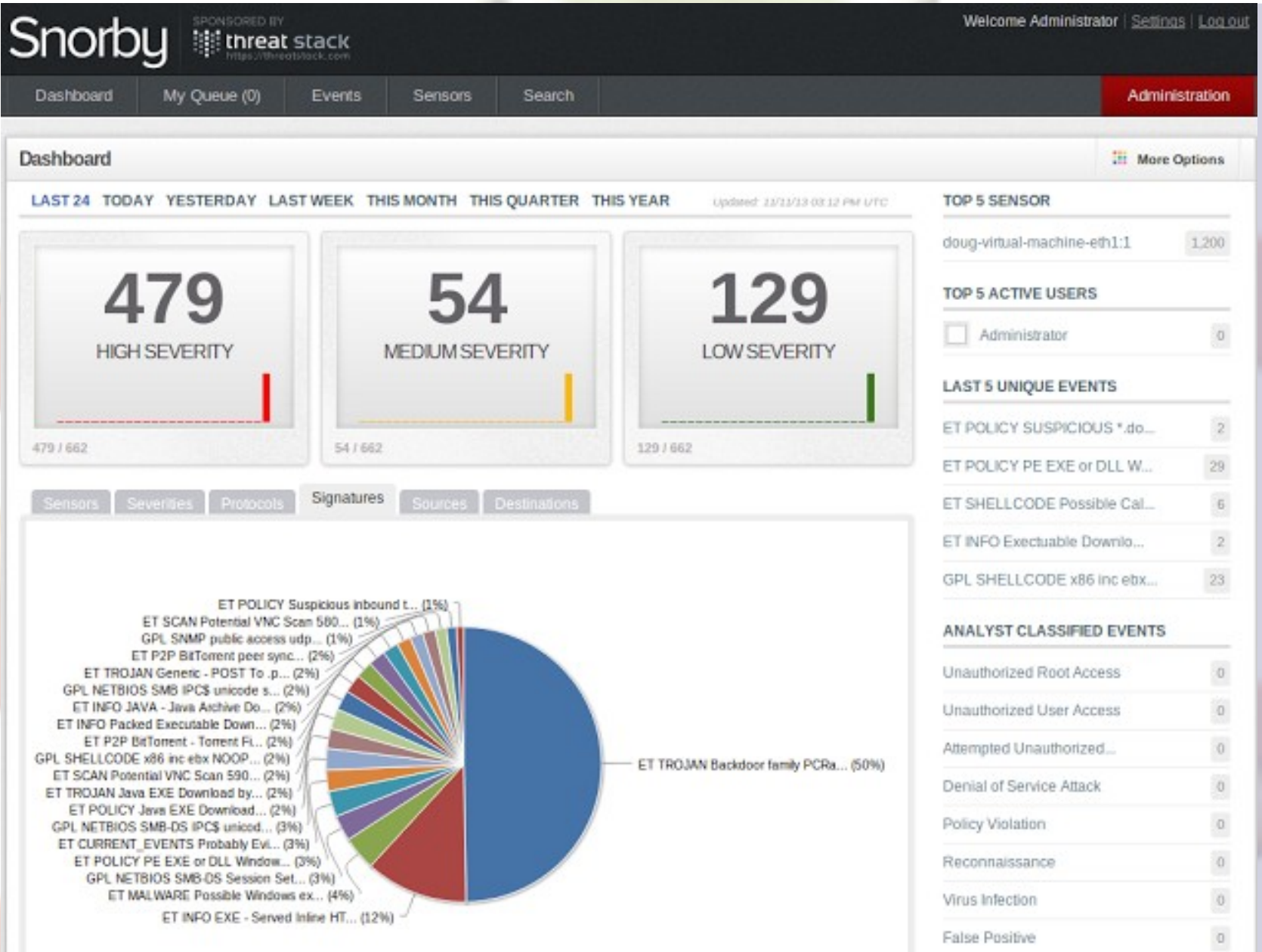
Preventivas

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

Snort GPLv2 Community Rules

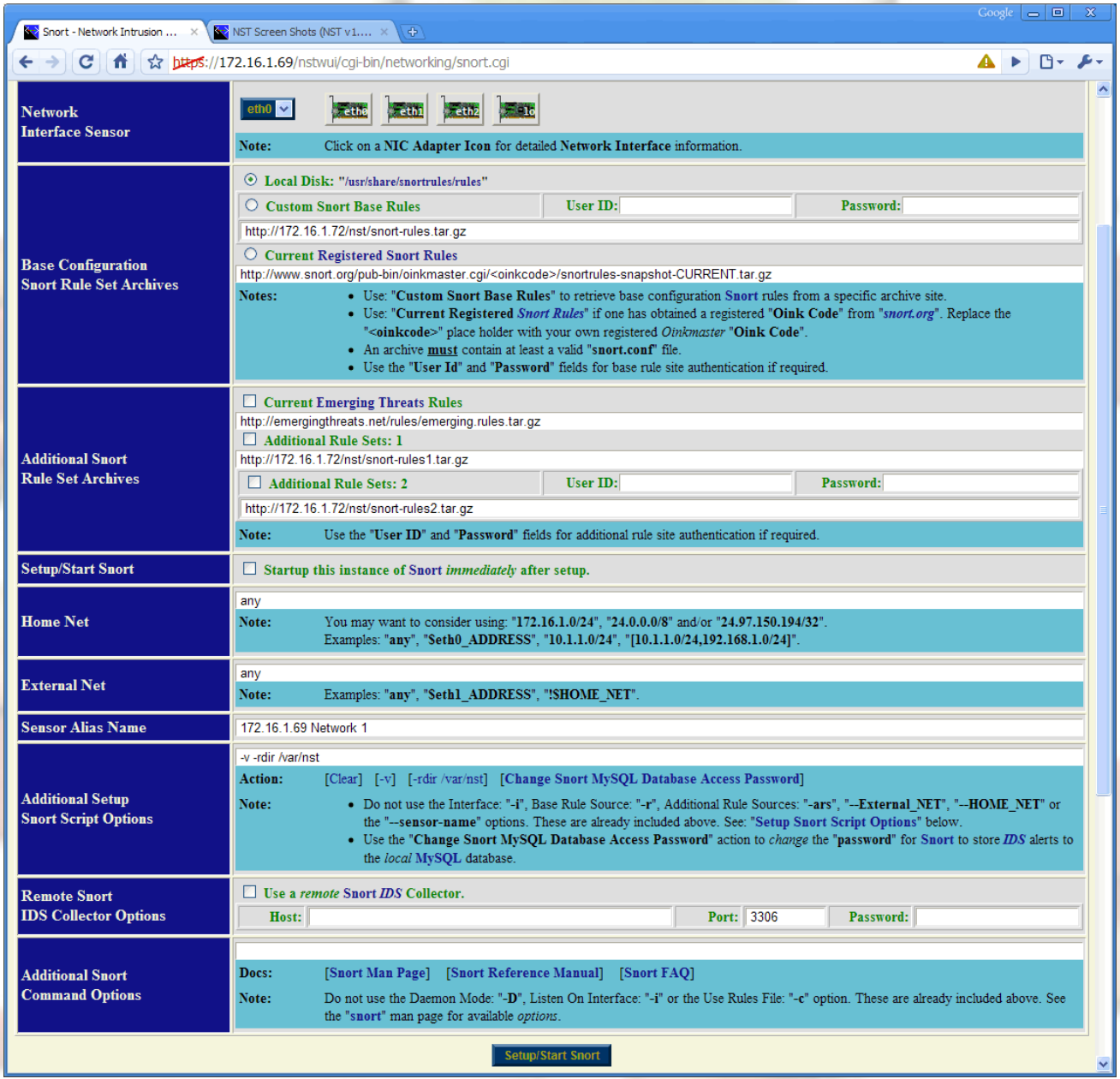
Enable Snort GPLv2	☐ Click to enable download of Snort GPLv2 Community rules
	The Snort Community Ruleset is a GPLv2 VRT certified ruleset that is distributed free of charge without any VRT License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.

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

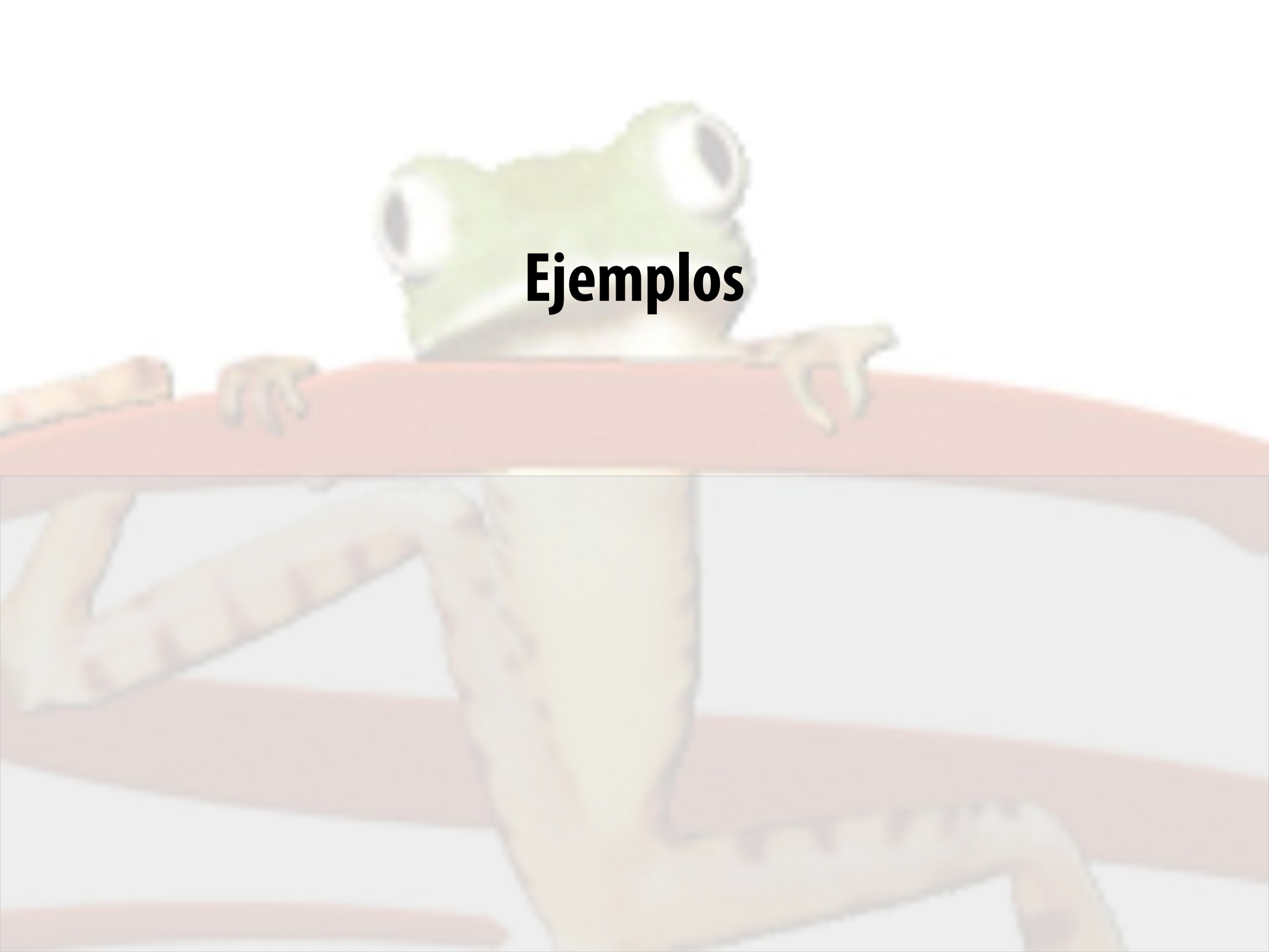
Ejemplos

Entidades

Herramientas

- Identificación de vulnerabilidades
  - OpenSource / Free

  - Privado

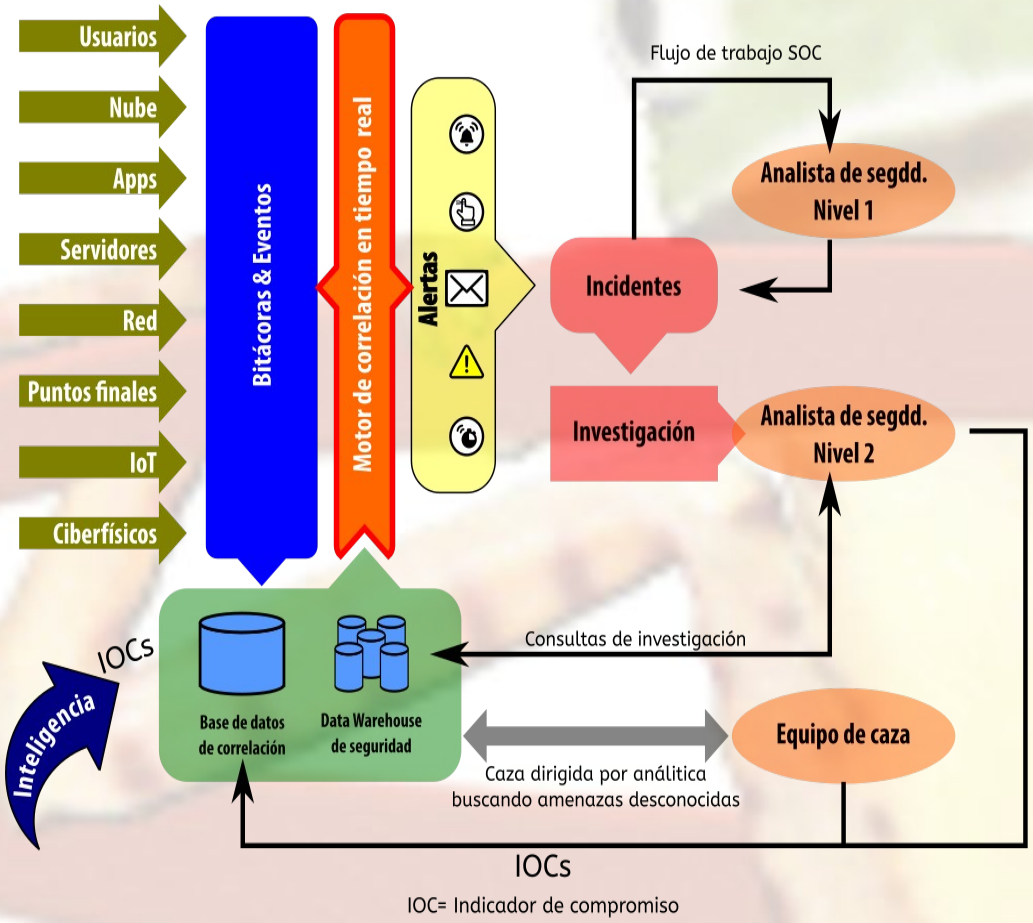


Ejemplos

Madurez CIRT según la OEA

OEA - Documento “Buenas Prácticas para establecer un CSIRT nacional”

Modelo HP



Monitoreo en tiempo real

Procesar incrementa el número de eventos
Correlación en tiempo real contra IOC
Número reducido de falsos positivos

Investigación

Habilidad de personalizar consultas en el ambiente y periodos de tiempo.
Construye la zona de análisis y remediación

Caza

Caza de amenazas desconocidas con análisis profundo y aprendizaje de máquinas.
Identificar nuevos IOCs para mejorar el monitoreo

Incrementando el nivel de madurez

Fuente: Paul Brettle, Hewlett Packard

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

HP's: Security Intelligence Capability

- https://youtu.be/ih0SC-dN6MU

Log Management

Bitácoras centralizadas
Datos retenidos
Cumplimiento de normatividad

Data Analysis

Tecnologías de correlación
Análisis de evidencia forence
Construcción de reportes automáticos

Near time alerting

Retroalimentación de los eventos
Correlación de alta fidelidad
Reportes personalizados

Real time analysis & incident response

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

Security intelligence

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

Fujitsu - Outsourcing

- https://youtu.be/6LwyTWPKDnQ

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

Instituciones de Ciberdefensa Nacional

Fundada 2003
Skína IT Solutions

Comando Conjunto Cibernético

Unidad Cibernética Ejército Nacional

Unidad Cibernética Armada Nacional

Unidad Cibernética Fuerza Aérea

CO COLOMBIA

CONPES 3854 de 2016

- Política Nal. de seguridad digital

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"

FIRST

- **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.

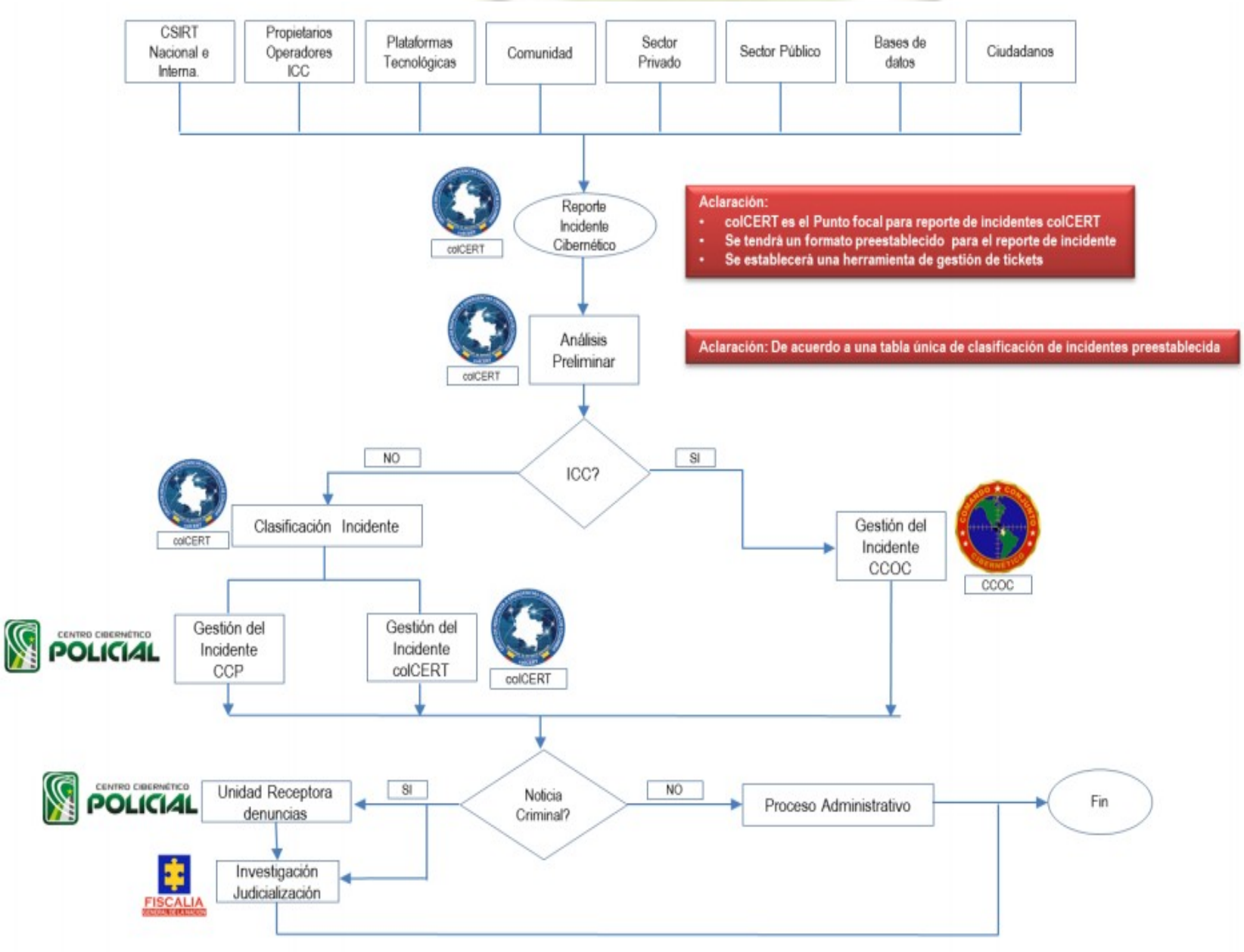
¿De quién depende el ColCERT?

Fuente: colCERT

CSIRT sectoriales en Colombia

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

Reporte de incidentes



Denuncias de Cibercrimen en la PONAL

Denuncias de Cibercrimen en la PONAL

- 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/
- hxxps://www.techopedia.com/definition/31003/computer-emergency-response-team-cert
- hxxp://www.csirt.org/

Muchas Gracias

¿Preguntas?

ventas@skinait.com

http://www.skinait.com