CSIRTs, Construyendo confianza en la región

Universidad Nacional de La Plata

CERTUNLP

Javier Díaz
Nicolás Macia
Paula Venosa
Einar Lanfranco
Alejandro Sabolansky

CERTUNLP
Equipo de Respuesta a Incidentes de Seguridad

¿Quiénes somos?

- Formamos parte del equipo de Seguridad en el ámbito de la Universidad Nacional de La Plata que:
  - Realiza docencia, investigación y extensión en la Facultad de Informática.

SYPER
Cátedra de Grado y Postgrado

CÁTEDRAS DE GRADO
REDES Y SERVICIOS
Avanzadoso en Internet

DSA
Desarrollo Seguro de Aplicaciones

PKI UNLP
Grid

  - Trabaja en el centro de respuesta a incidentes de seguridad de la UNLP, el CERTUNLP.

CERTUNLP
Equipo de Respuesta a Incidentes de Seguridad

CeSPI
UNIVERSIDAD NACIONAL DE LA PLATA

UNIVERSIDAD NACIONAL DE LA PLATA

Sobre la red de la UNLP

- La red de la UNLP brinda servicios internos y de Internet a Facultades, Colegios y Laboratorios.
- 17 facultades, 5 colegios, más de 100 laboratorios todos con sus propias redes
- Dominio: *.unlp.edu.ar
- Bloques IP utilizados:
  - IPv4: 163.10.0.0/16
  - IPv6: 2800:340::/32
- Direcciones activas tomadas el Miércoles 17/8/2016 de 11:00 am a 11:59 am
  - IPv4: 19364
  - IPv6: 807

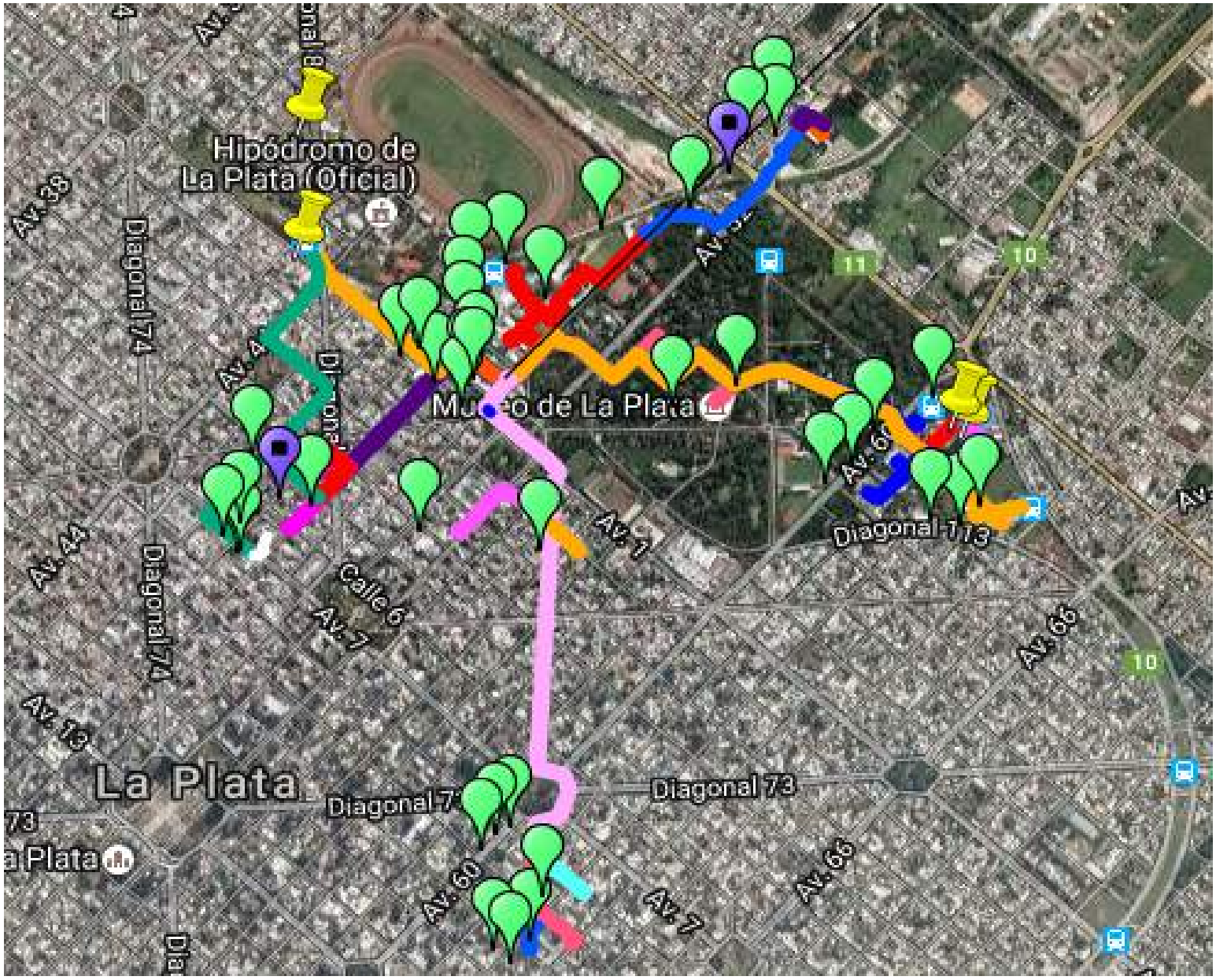
CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Sobre la red de la UNLP

- Actualmente conectada a:
  - Red de Interconexión Universitaria (RIU)
  - InnovaRed
  - Internet
  - Cámara Argentina de Internet (CABASE)

- La Universidad Nacional de La Plata (UNLP) es sede y miembro fundador del NAP CABASE La Plata.

Red de la UNLP



CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Motivación

- Hoy en día todas las organizaciones sin importar su naturaleza, están expuestas a ataques que tienen como origen o destino sus redes, sus servicios y sus aplicaciones. Ejemplos sobran:
- Hay ataques con objetivos específicos:
  - Uno de los primeros en atacar infraestructuras críticas: Stuxnet
    - Gusano informático descubierto en 2010 para espiar y reprogramar sistemas industriales.
    - Podía afectar infraestructuras críticas, como por ejemplo, una central nuclear.
  - Uno más actual contra el sistema financiero: Carbanak
    - Ataque persistente contra instituciones financieras (principalmente bancos de Rusia, USA, Alemania, China y Ucrania). Se estima un monto de **1000** millones de dólares.
    - El malware fue introducido mediante un email de phishing a un empleado administrativo.
    - Ver video

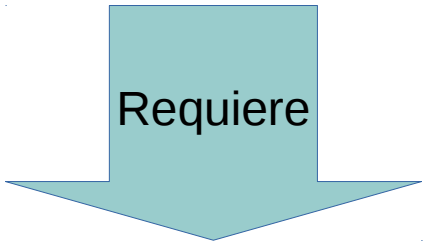
Motivación

- Hay ataques genéricos
  - Directamente en los equipos de los usuarios, como por ejemplo ransomware.
    - Ver video Locky
- Hay vulnerabilidades.....
  - En los sistemas que usamos, por ejemplo, errores en el Home Banking o malas campañas de concientización.
    - El video lo obviamos....

Este es COCO

Motivación

Continuo incremento de incidentes de seguridad de la información que afecta a las organizaciones



Definir políticas de seguridad y prácticas asociadas como parte de la estrategias de manejo de riesgo

También es preciso definir responsables para:

- la recepción y revisión de incidentes de seguridad
- el tratamiento y la respuesta a los mismos

CSIRTs

¿De qué se trata un CSIRT?

¿Qué son los CSIRTs?

Un CSIRT o “Equipo de respuesta de incidentes de Seguridad Informática” es un equipo que ejecuta, coordina y apoya la respuesta a incidentes de seguridad que afectan a una comunidad objetivo

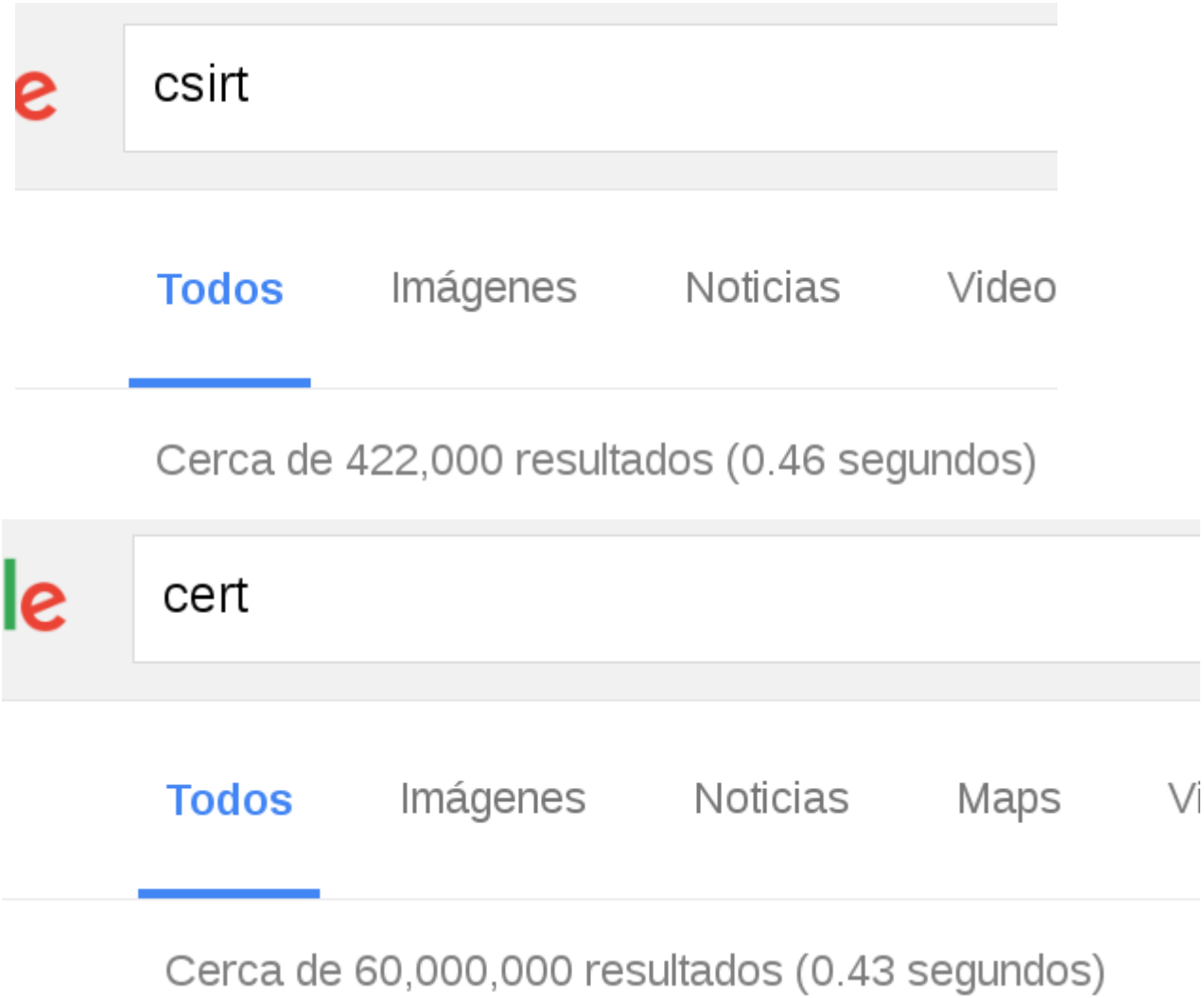
¿ CERT = CSIRT?

- CSIRT (Computer Security Incident Response Team) es el término genérico utilizado para equipos de tratamiento y respuesta a incidentes de seguridad.
- CERT (Computer Emergency Response Team) es el término originalmente utilizado.

  Se pueden usar ambos términos indistintamente. Aunque CERT es una marca registrada.

¿Qué son los CSIRTs?

¿ CERT = CSIRT?



CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Pasos en la formación de un CSIRT

Al crear un CSIRT es importante saber:

- ¿Cuál será su misión?
- ¿A quién dará servicio?
- ¿Qué servicios brindará?
- ¿Desde qué lugar en la organización?
- ¿En cooperación con quienes?

https://www.terena.org/activities/tf-csirt/starter-kit.html

Pasos en la formación de un CSIRT

Para eso hay que definir:

- Metas y objetivos
- Comunidad (Constituency)
- Servicios brindados
- Posición dentro de la organización (Organigrama)
- Relación con otros equipos

Tipos de CSIRTs

Algunas categorías generales de CSIRTs:

- **Centros de Coordinación:**

  Coordinan y facilitan el manejo de incidentes a través de diversos CSIRT. Un ejemplo de este tipo de CSIRT es el CERT Coordination Center (CERT/CC).

  También generan guías, boletines, mejores prácticas y alertas de ataques y vulnerabilidades.

- **CSIRTs Nacionales:**

  Proporcionan servicios de manejo de incidentes a un país. Algunos ejemplos son: Japan CERT Coordination Center (JPCERT/CC) o Singapur Computer Emergency Response Team (SingCERT) o ICIC CERT (Argentina).

Tipos de CSIRTs (cont)

- **CSIRTs Internos:**

  Proporcionan servicios de manejo de incidentes a su organización. Esto podría ser un CSIRT para un banco, una empresa de fabricación, una universidad o una agencia federal.

  Por ejemplo nuestro CSIRT: **CERTUNLP**.

- **Proveedores de Manejo de Incidentes:**

  Ofrecen servicios de manejo de incidentes a terceros.

- **Equipos de seguridad**

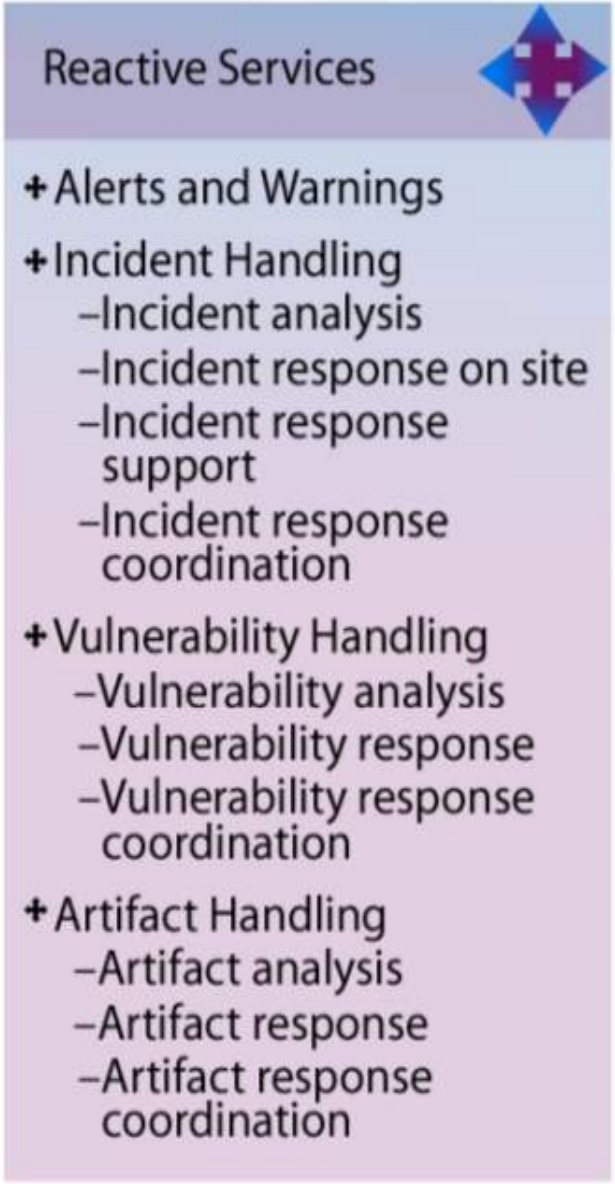
  No es un CSIRT propiamente dicho. Cumple informalmente sus funciones.

Servicios de un CSIRT

- Los servicios que presta un CSIRT pueden calificarse como:
  - **Servicios Reactivos**
  - **Servicios Proactivos**
  - **Servicios de Gestión de Calidad de Seguridad**

- Manuales de LACNIC: http://www.proyectoamparo.net/es/manuales

Servicios de un CSIRT



- **Servicios Reactivos**
  - Se activan como consecuencia de un evento o requerimiento.
  - Son el componente central en el trabajo de un CSIRT.

La **Gestión de Incidentes de Seguridad** es el único servicio **reactivo** que cualquier CSIRT debe brindar.

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Servicios de un CSIRT

- **Servicios Proactivos**
  - Proveen información que ayuda a proteger su comunidad y su infraestructura anticipándose a los ataques.
  - Su éxito reduce el número de incidentes futuros.

Servicios de un CSIRT

- **Servicios de Gestión de Calidad de Seguridad**
  - Mejoran servicios independientes del manejo de incidentes preexistentes (capacitaciones internas, auditoría, etc).
  - En general son servicios proactivos pero con una incidencia menor en la reducción de incidentes futuros.
  - Se valen de los conocimientos y la experiencia del personal del CSIRT.

Gestión de Incidentes

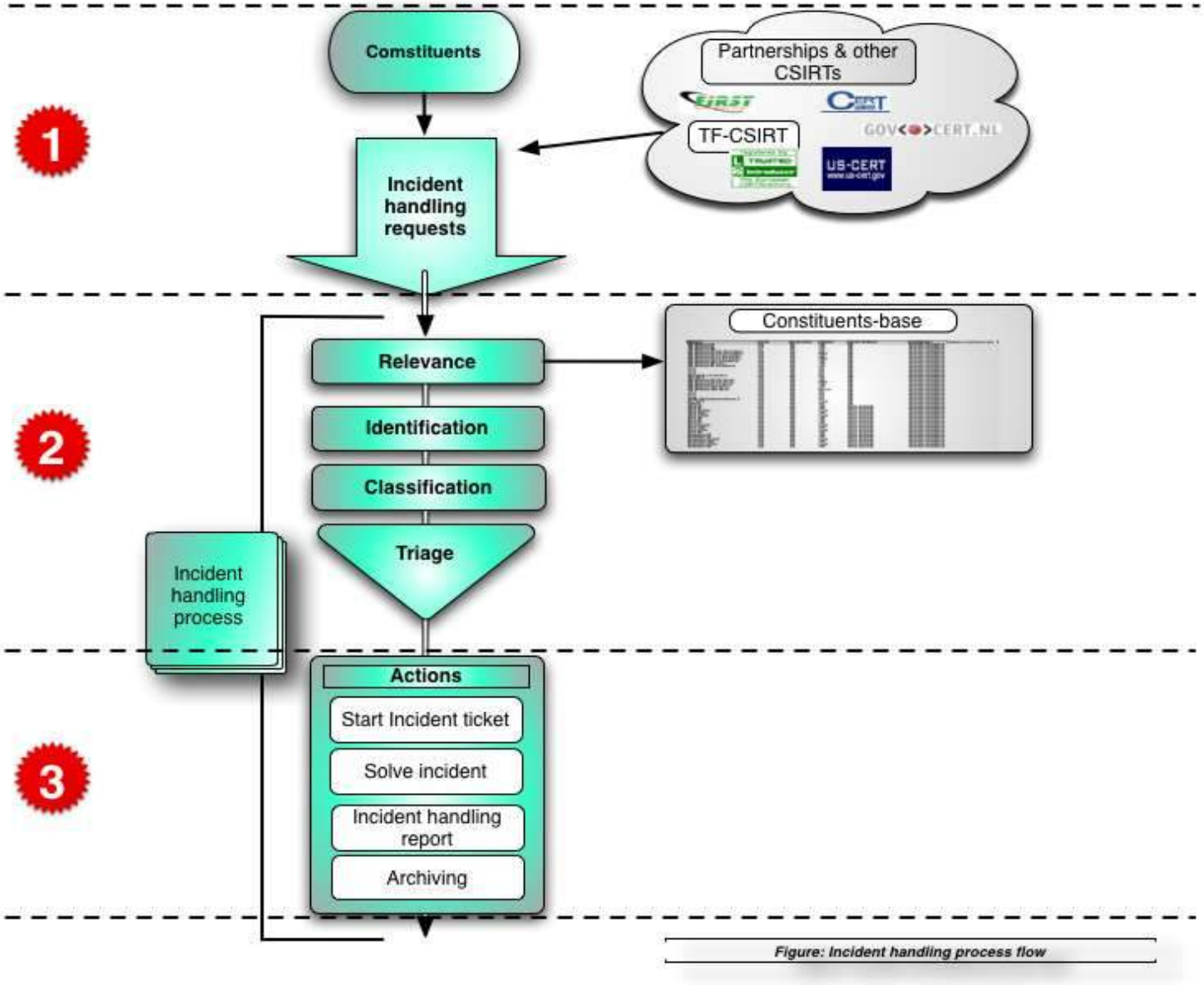


Figure: Incident handling process flow

Referencia: https://www.enisa.europa.eu/activities/cert/support/guide/workflows/incident-handling

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Aceptación del CSIRT en su comunidad

El éxito de un CSIRT está basado en:

- Que la comunidad conozca su CSIRT y los servicios que éste brinda.
- Que la comunidad entienda el compromiso del CSIRT en el manejo adecuado de la información de incidentes de seguridad.
- Que el equipo colabore e interactúe con otros CSIRTs en el manejo de incidentes.
- La capacitación continua de los integrantes del grupo.

Organismos de referencia

- **FIRST (Forum for Incident Response and Security Teams)**
  - Fomenta la cooperación y la coordinación en prevención de incidentes. Promueve el intercambio de información entre miembros y la comunidad en general. Desarrolla capacitaciones y talleres para la formación de nuevos CSIRTs
- **Iniciativas de LACNIC:**
  - **Proyecto AMPARO**
    - Su misión es el fortalecimiento de la capacidad de prevención y atención de incidentes de seguridad en América Latina y el Caribe, tanto en el ámbito privado como en organizaciones sociales.
    - Promover la difusión y capacitación de metodologías de trabajo de Centros de Respuesta a Incidentes de Seguridad Informática o CSIRTs (Computer Security Incident Response Teams).
  - **LACCSIRTs** – Espacio dentro de LACNIC para CSIRTs
  - **W.A.R.P. - Warning Advice and Reporting Point**

    Equipo Coordinador y Facilitador de manejo de incidentes de seguridad informática para la comunidad de miembros de LACNIC.
- **ENISA**, the European Union Agency for Network and Information Security

  Su objetivo es ser un punto de intercambio de información, mejores prácticas y conocimiento en el campo de la Seguridad Informática
- **ITU/UIT,** Union Internacional de Telecomunicaciones

  - Eventos de entrenammiento Cyberdrill

Sobre CERTUNLP

CERTUNLP

Equipo de Respuesta a Incidentes de Seguridad

CERTUNLP

Equipo de Respuesta a Incidentes de Seguridad

Sobre CERTUNLP

Misión de CERTUNLP:

- Gestionar incidentes de seguridad. Prevenir, detectar e investigar problemas de seguridad. Coordinar acciones para la protección de los usuarios y los servicios académicos de la UNLP.

Comunidad objetivo:

- Red de la UNLP:
  - Sistema Autónomo: 5692
  - Bloque IPv4: 163.10.0.0/16
  - Bloque IPv6: 2800:340::/32
- Dominio: *.unlp.edu.ar

Servicios:

- Gestión de Incidentes
- Auditorías de seguridad de redes y servicios
- Monitoreo de seguridad
- Desarrollo de herramientas
- Concientización / Educación

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Servicios Reactivos de CERTUNLP

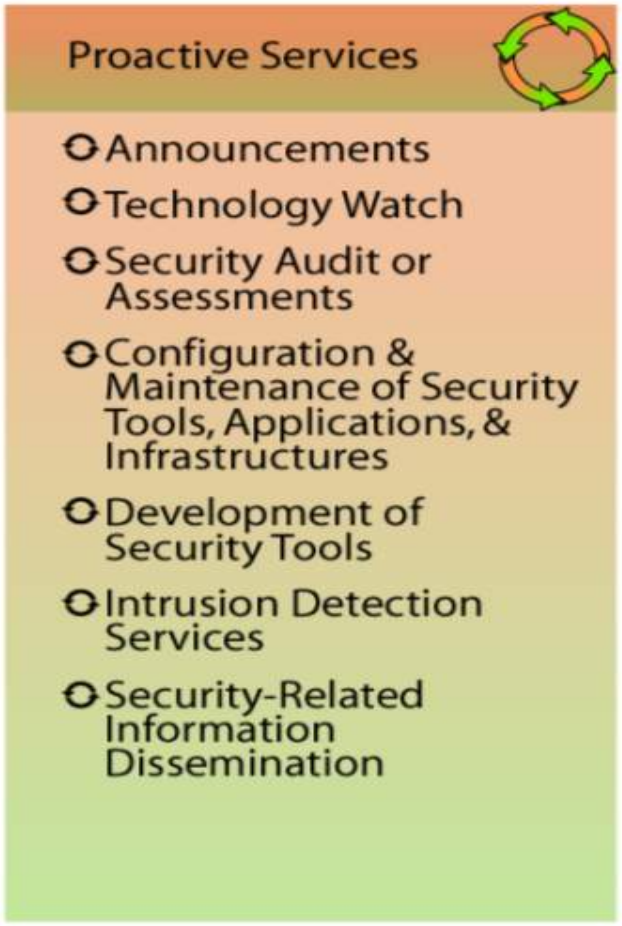
- Avisos y Alertas de seguridad
- Gestión de Incidentes:
  - Análisis de incidentes
    - Análisis Forense
  - Soporte en la solución
  - Coordinación

Referencia: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305

CERTUNLP
Equipo de Respuesta a Incidentes de Seguridad

Servicios Proactivos de CERTUNLP

- Anuncios
- Auditorías de seguridad (Pentests)
- Monitoreo, detección y prevención de intrusiones
- Desarrollo de herramientas de Seguridad



Referencia: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305

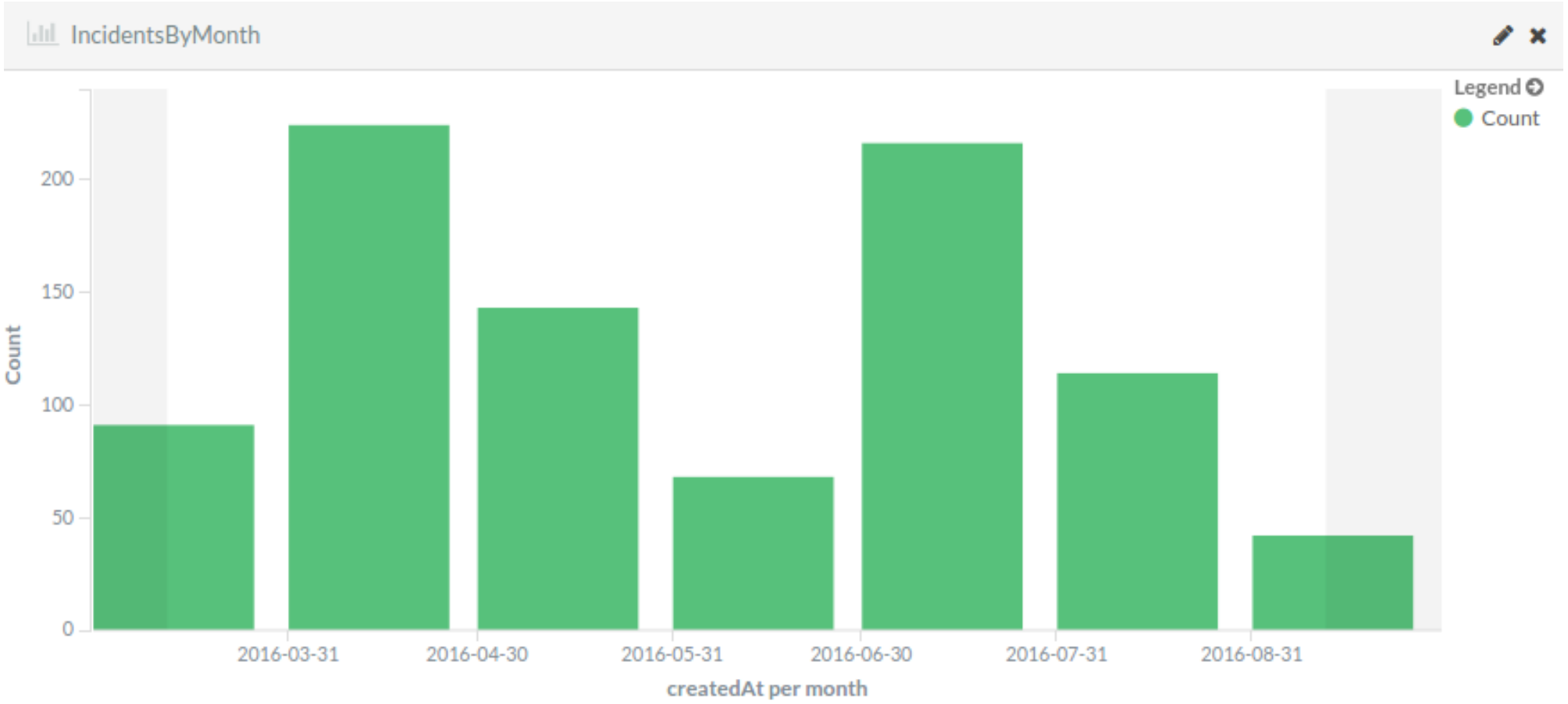
CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Servicios de Gestión de Calidad la Seguridad de CERTUNLP

- Consultoría
- Concientización
- Educación / Entrenamiento

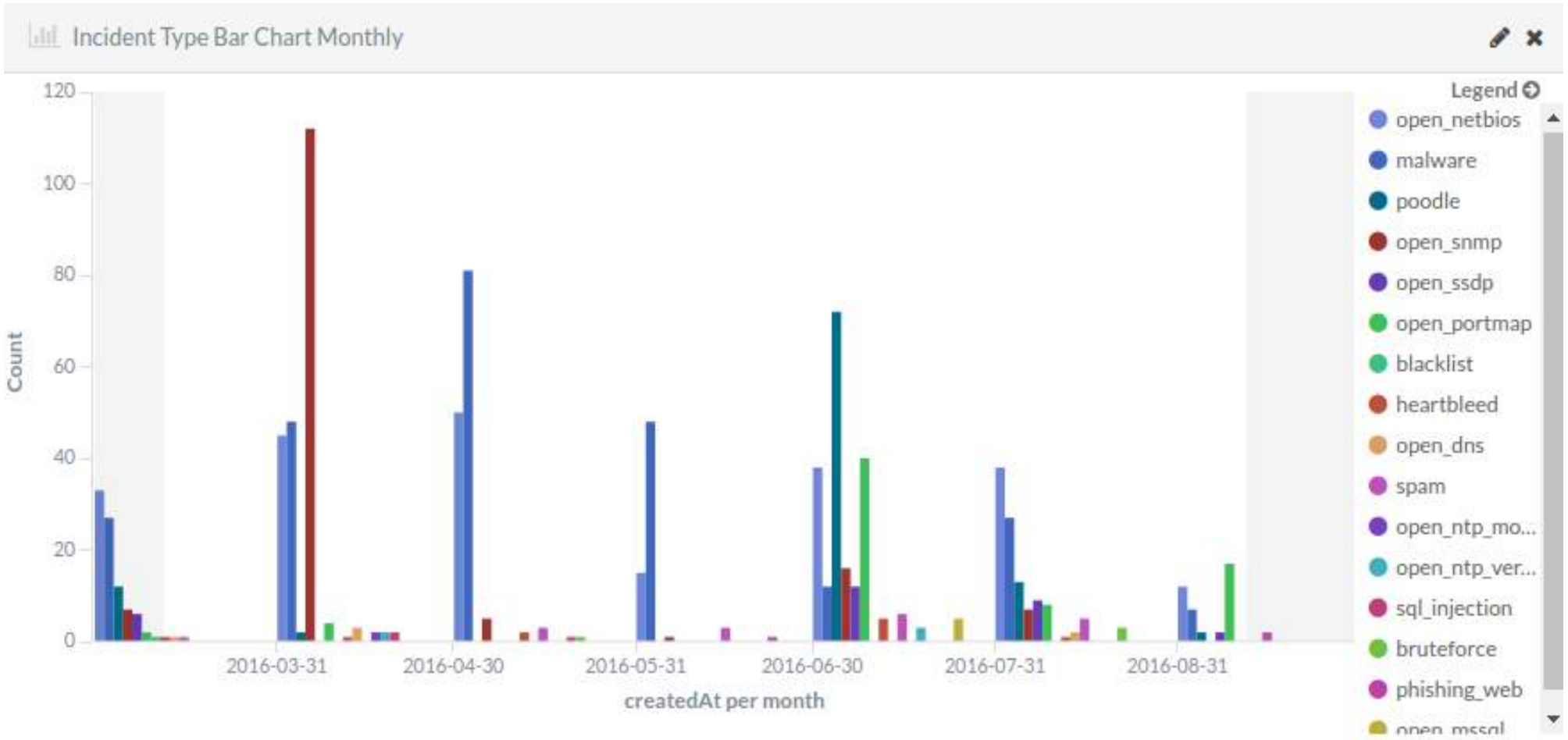
CERTUNLP
Equipo de Respuesta a Incidentes de Seguridad

Estadísticas en la UNLP
Totales últimos 6 meses



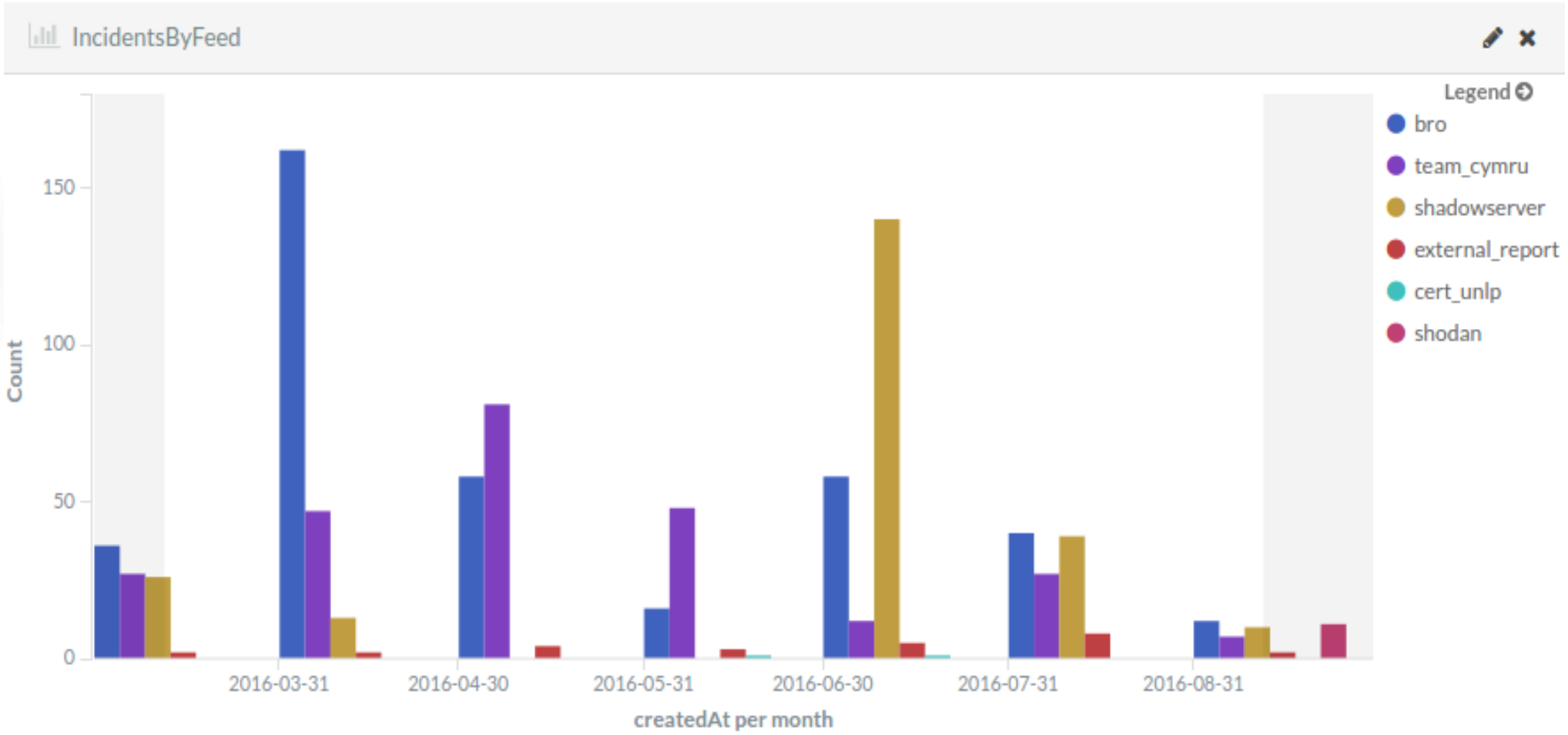
CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Tipos de incidentes de seguridad



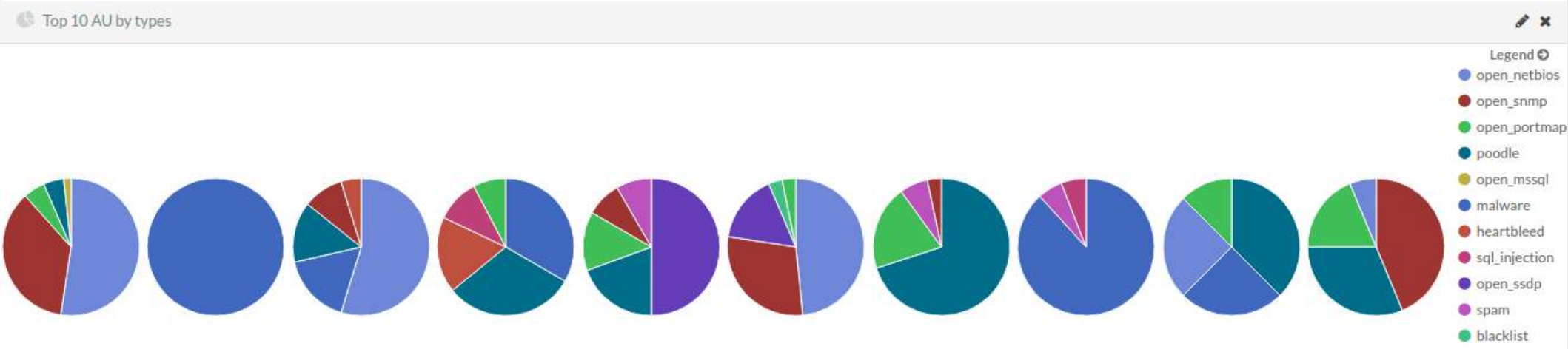
CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Origen de los incidentes de seguridad



CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Tipos de incidentes en el top 10 de Unidad Académica



CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Análisis de seguridad

Análisis de seguridad (Pentests) realizadas sobre distintos sistemas y aplicativos:

- UNLP
  - Sistemas Académicos
  - Sistemas internos
- SIU: Sistemas de Información Universitaria
  - Guaraní
  - Kolla
  - Toba
- CONICET
  - Sistema de voto electrónico

Auditorías de seguridad

Auditorías de seguridad realizadas sobre redes y servicios:

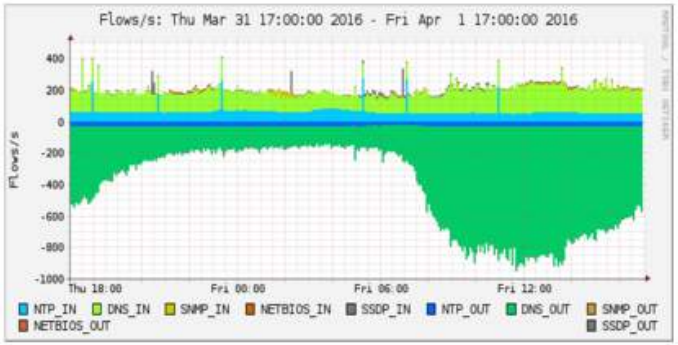
- Red de la UNLP
- Superintendencia de Delitos Complejos y Crimen Organizado
- Red del SIU
- Redes de miembros del NAP regional CABASE LPL
- Asociación de Universidades Grupo Montevideo (AUGM)

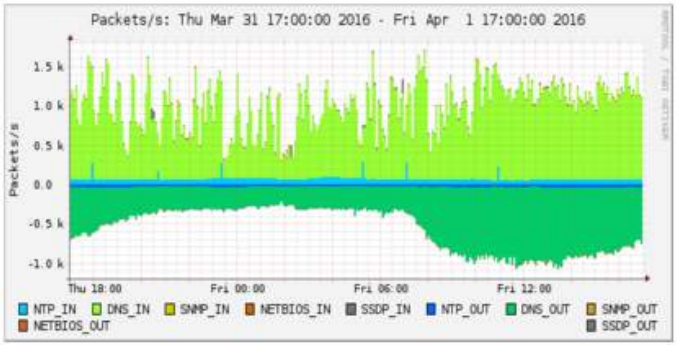
Chequeos periódicos de redes y servicios

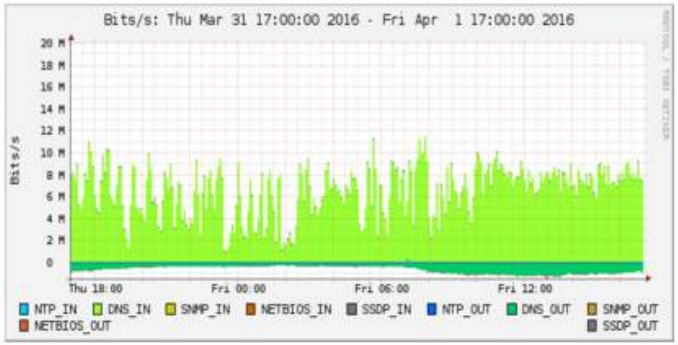
- Se realizan auditorías periódicas automatizadas sobre distintas redes de la UNLP y otros organismos bajo demanda.

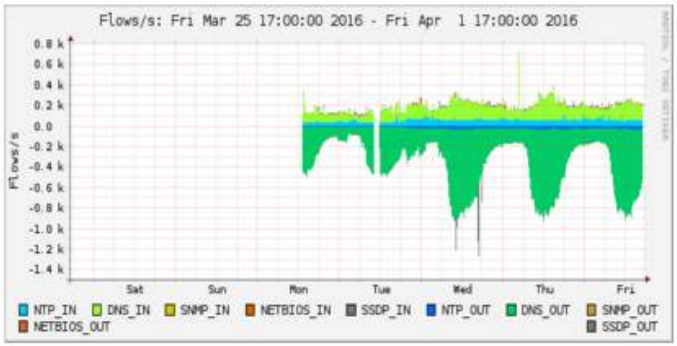
Monitoreo de seguridad de red

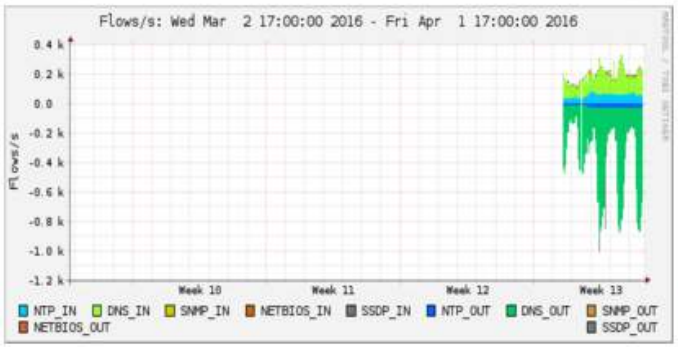
El monitoreo de red permite analizar el uso de los recursos de red para detectar anomalías

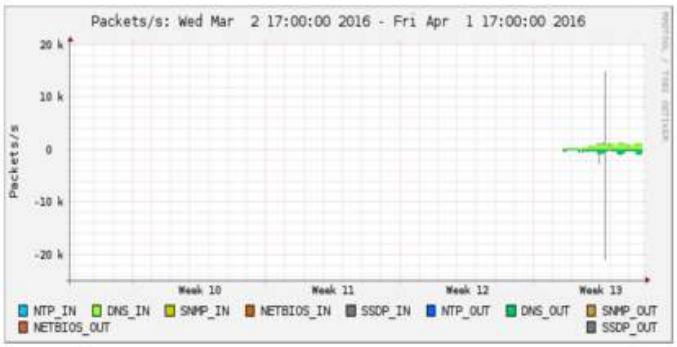


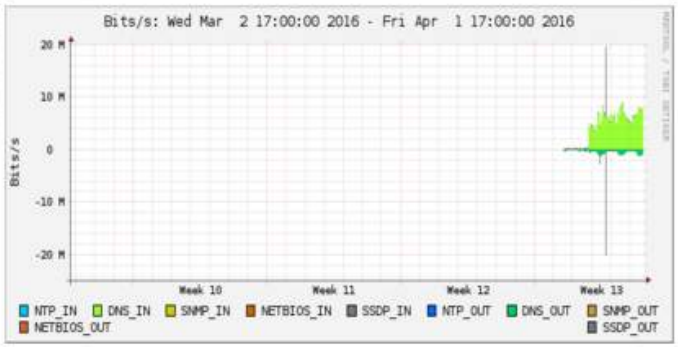












Monitoreo de seguridad

CERTUNLP detecta amenazas e incidentes de seguridad en función de las siguientes actividades de monitoreo:

- Recolección y procesamiento de NetFlow / sFlow
- Detección de distintos problemas a través del uso de BRO-IDS
  - Scans de puertos / Ataques de fuerza bruta
  - Heartbleed, Poodle / SQL Injections
  - Protocolos amplificables: OpenDNS, OpenNetBios, OpenSNMP
- Honeypots: SpamPot / Darknet
- Búsqueda continua en buscadores: Shodan, Open Resolver Project

Herramientas utilizadas

En la operatoria de un CSIRT se utilizan distintas herramientas para la realización de los diferentes servicios brindados.

En el caso de CERTUNLP se desarrollaron herramientas propias que se usan y se dan a la comunidad como software libre:

- **Ngen:** CSIRT Incident Report System: Sistema web de gestión de incidentes de seguridad.
- **Kintun**: Servicio de scanner de vulnerabilidades via API REST para la detección de:
  - Servicios vulnerables que se prestan a posibles ataques de amplificación en DDOS (NTP info, NTP monlist, Open DNS, Open Netbios)
  - Servicios con distintas vulnerabilidades (heartbleed, poodle, open smtp relays)
  - Servicios proxies HTTP y SOCKs abiertos
- **Saga**: herramienta de centralización de consultas de información vía web para investigaciones judiciales. (en fase de desarrollo)

Herramientas publicadas

- NGEN y Kitun pueden obtenerse de GitHub

https://github.com/CERTUNLP

Actividades en la comunidad

- Gestión de la Infraestructura de Clave Pública (PKI UNLP Grid)
  - Emisión de certificados digitales para e-ciencia de Argentina.
- Participación en **LACCSIRTs** – Espacio interno de LACNIC para CSIRTs
  - Coordinación de las reuniones virtuales (host).
- Participación en eventos internacionales de entrenamiento como Cyberdrill organizado por la UIT / ITU
- Actividades de concientización:
  - Personal no técnico BCRA.
  - Proyectos de extensión.

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Actividades en la comunidad

- Participación en competencias de seguridad: CTF (Capture The Flag)
  - Un CTF es una competencia de seguridad de ataque defensa donde compiten distintos equipos entre sí.
  - Hay distintas alternativas de implementación, pero en general se cuenta con una infraestructura a proteger al mismo tiempo que se intenta vulnerar a los demás equipos para obtener los FLAGS.
  - Con los FLAGS es que se obtienen los puntos.
  - Suelen involucrar todo tipo de conceptos, entre ellos: ingeniería social, forensia, seguridad de aplicaciones web, criptografía, reversing de binarios, desarrollo de exploits, redacción de reportes, etc.
- Algunos resultados:
  - 2dos en INTERNACIONAL CYBEREX 2016 - Organizado por: OEA e INCIBE
  - 1ros en INTERNACIONAL CYBEREX 2015 - Organizado por: OEA e INCIBE.
  - 4tos en iCTF 2012 - Organizado por: University of California (UCSB).
  - 2dos en Da.Op3n 2005. Organizado por Darmstadt University of Technology – Alemania

Actividades en la comunidad

Ciberseguridad: los mejores del continente, en 50 y 120

Los encargados de la seguridad informática de la UNLP ganaron una competencia en la OEA

30 de Septiembre de 2015 | 03:16

1 / 2 Los integrantes del equipo responsable de la seguridad del sistema informáti

Informáticos de la UNLP, premiados en competencia internacional de ciberseguridad

Por segundo año consecutivo, el Equipo de Respuesta a Incidentes Informáticos de la Universidad Nacional de La Plata, CertUnlp, se posicionó entre los primeros puestos de la distinguida competencia de ciberseguridad "International CyberEx", en la cual obtuvo el segundo puesto detrás del equipo de Colombia.

El equipo platense está conformado por Nicolás Macia (capitán), Einar Lanfranco, Mateo Durante, Damián Rubio, Matías Ferrigno, Carlos Damián Piazza, Alejandro Sabolansky y Agustín Aguirre.

La modalidad de la competencia fue la siguiente: durante ocho horas los participantes intentaron resolver los 68 desafíos propuestos por la organización, compitiendo como equipo contra las dificultades de los eventos y el tiempo de resolución de los mismos, todo de manera virtual y remota.

El objetivo de este tipo de certámenes consiste en fortalecer las capacidades de respuesta ante incidentes cibernéticos y mejorar la colaboración y cooperación frente a los mismos.

El grupo es parte del Equipo de Respuesta a Incidentes Informáticos

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Últimas presentaciones

- LACNIC XXIII
  - CERTUNLP: hacia un sistema de gestión de incidentes integrable"
  - LACCSIRTs e-Forum: un año después
- ITU - Foro de Ciberseguridad y Tercer Taller Ejercicio Práctico de Aprendizaje Aplicado para Equipos de Respuesta Ante Emergencias Cibernéticas para la Región de América
  - Retos del desarrollo de competencias profesionales para la ciberseguridad: Un enfoque académico
- LACNIC XXIV
  - Ngen - CSIRT Incident Report System
  - Formación de recursos en ciberseguridad en la UNLP: Un enfoque práctico
- CABASE – ARNOG
  - Ataques de amplificación y protección de servicios esenciales

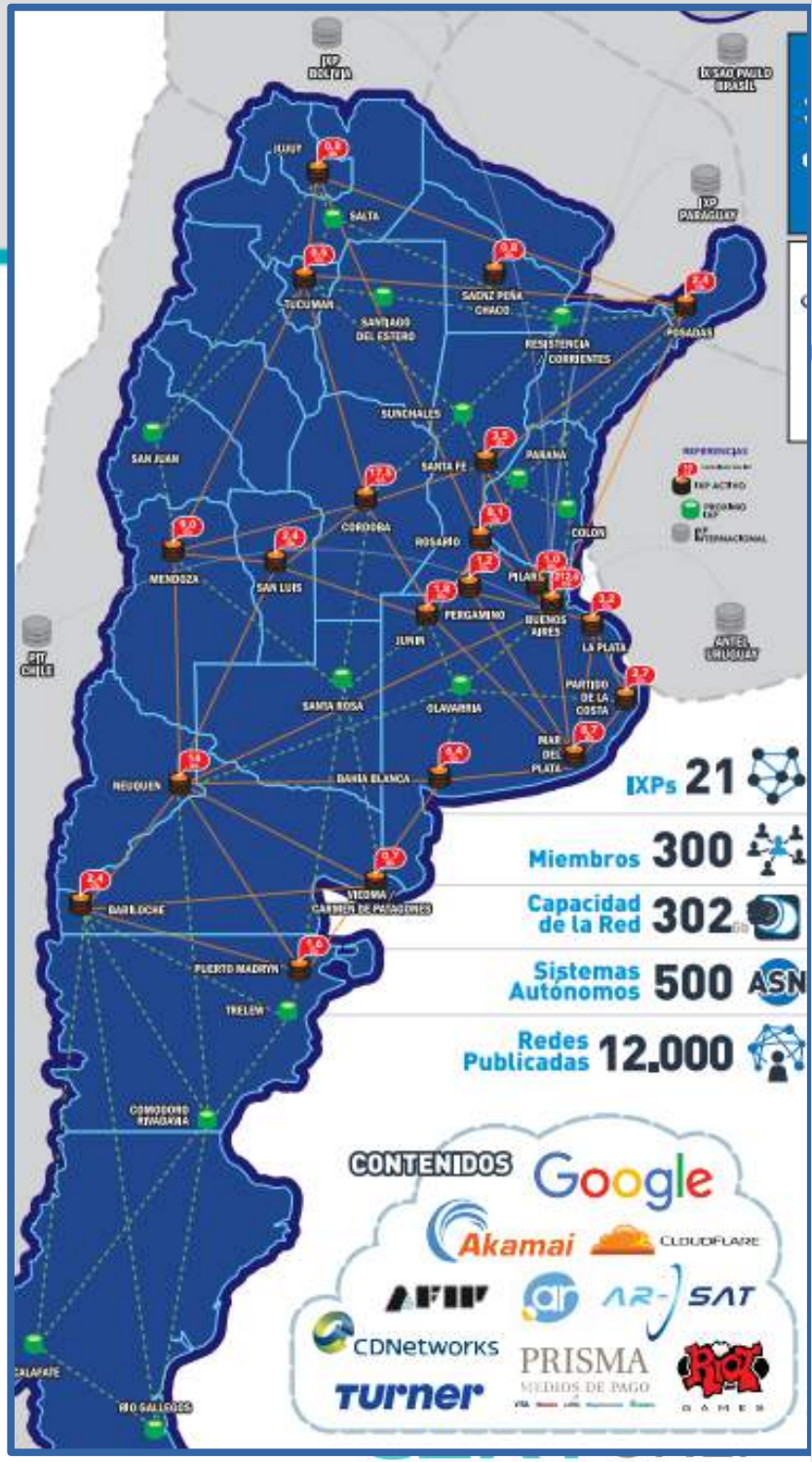
Últimas presentaciones

- ADACSI – CIBER 2015
  - Formación en Ciberseguridad en la UNLP: un enfoque práctico"
  - Panel sobre Computer Security Incident Response Team (CSIRT)
- CABASE – ARNOG
  - Charla: DDoS. Alternativas en la detección y mitigación
- LACNIC XXV
  - Apertura conjunta con LACNIC de la reunión de CSIRTs
- ITU - Semana de Ciberseguridad desde la Mitad del Mundo
  - Academic CIRT, functions, benefits, services
  - The role of Academia on Cybersecurity
  - Proyecto Academia UIT

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

UNLP y CABASE

- UNLP es miembro de CABASE
- El punto de interconexión es el NAP regional LPL (La Plata)
  - La infraestructura está alojada en las instalaciones de la UNLP
  - Actualmente 15 miembros conectados



Fuente:
http://www.cabase.org.ar/wp-content/uploads/2016/05/Poster-Cabase-2016-FRENTE-v6.pdf

Análisis de seguridad en NAP LPL

En Diciembre de 2014 se realizó un análisis de vulnerabilidades en las redes de los miembros del NAP LPL

- Por entonces había 9 miembros
- Se analizaron 13.056 direcciones IPs
- Se buscaron problemas de:
  - Heartbleed: en distintos puertos seguros
  - DNS: Open resolvers
  - SMTP: Open relays
  - NTP: monlist

```
Resultados
----------------------
 3 Heartbleed
19 DNS: Open Resolver
 0 SMTP: Open relays
 7 NTP: Monlist
```

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

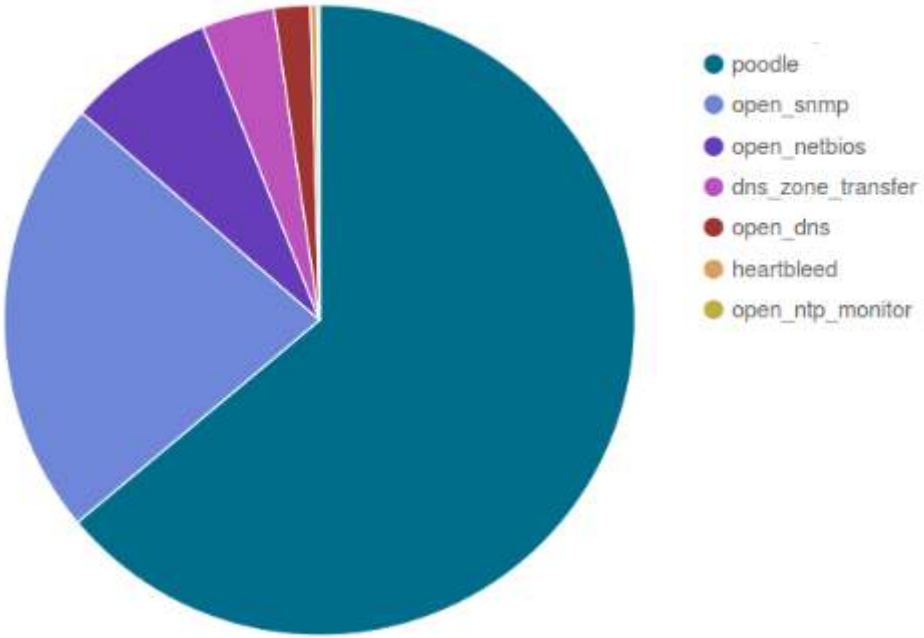
Análisis de seguridad en NAP LPL

- En Mayo de 2016 se presentó un nuevo informe de vulnerabilidades en redes de miembros del NAP LPL
- Se analizó las redes de los 10 miembros conectados
  - Se analizó solamente el espacio IPv4
  - Se analizaron 78.848 direcciones IPv4
  - Se hizo foco en la búsqueda de problemas relacionados con ataques de amplificación y DDoS

Análisis de seguridad en NAP LPL

Distribución de vulnerabilidades:

- De un total de 78.848 IPv4



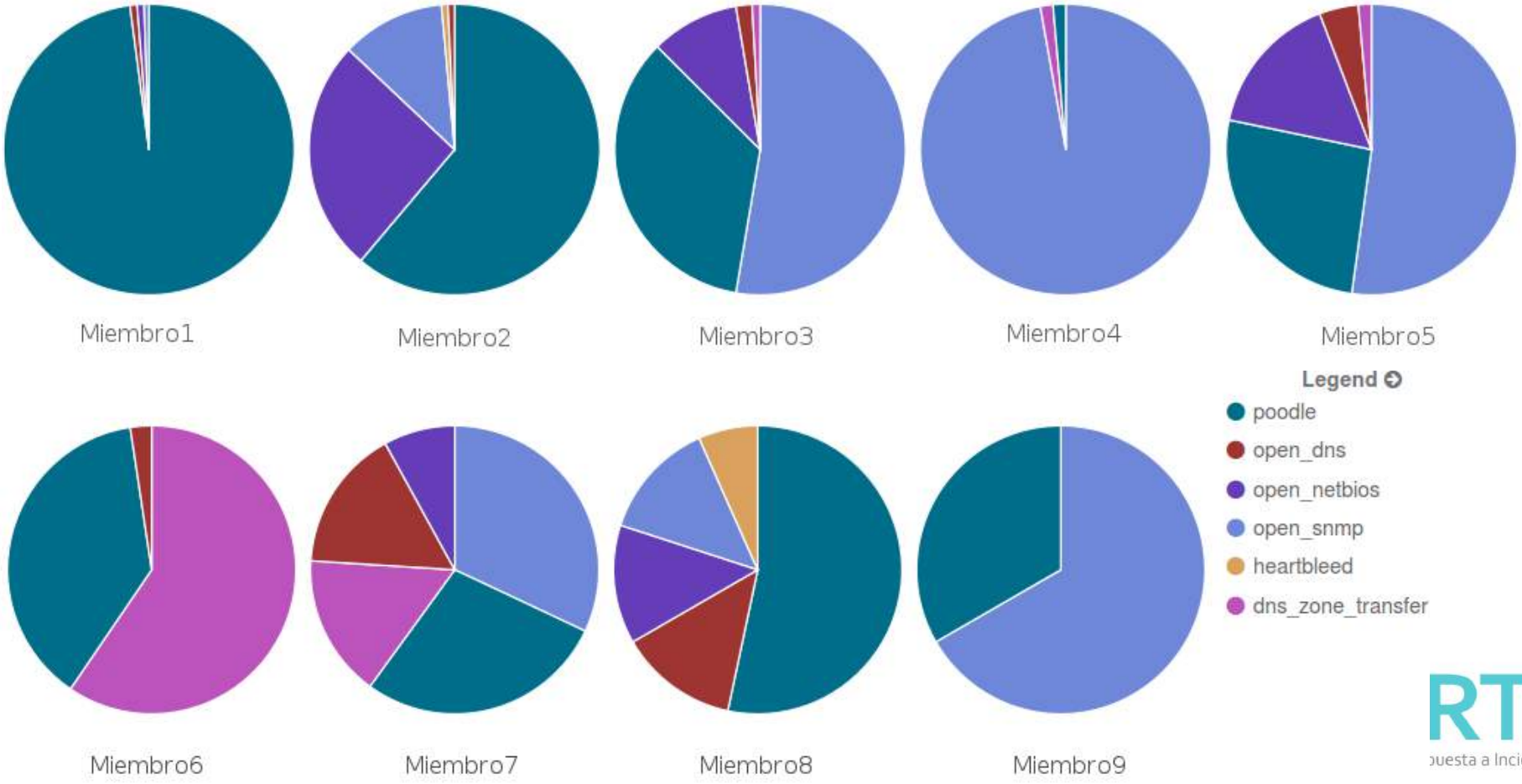
Vulnerabilidad	Encontrados	Porcentaje
Poodle	551	63,92%
Heartbleed	3	0,35%
Open NTP Monitor	1	0,12%
Open NTP Version	0	0%
Open Netbios	65	7,54%
DNS Zone Tansfer	32	3,71%
Open DNS	16	1,86%
Open SNMP	194	22,51%
Open SMTP Relay	0	0%
Total	862	100%

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Análisis de seguridad en NAP LPL

Distribución de vulnerabilidades por miembro

- Uno de los miembros no tenia vulnerabilidades



RT UNLP
puesta a Incidentes de Seguridad

Charlas a operadores de red

Encuentro Nacional de Técnicos de CABASE

Noviembre de 2015 – Río Tercero. Córdoba

- Charla: Ataques de amplificación y protección de servicios esenciales
  - Problemas de amplificación
  - Servicios vulnerables y configuraciones adecuadas
  - BCP 38: Buenas prácticas de filtros en un ISP
  - BCP 134: La experiencia de Brasil contra el SPAM

Charlas a operadores de red

5ta Jornada Técnica ARNOG + IETF 95

Abril de 2016 – CABA

- Charla: DDoS. Alternativas en la detección y mitigación
  - Problemas de reflexión y amplificación
  - Servicios vulnerables
  - Prevención:
    - Buenas prácticas de configuración en servicios vulnerables
    - Filtros antispoofing
    - Mecanismos de detección de vulnerabilidades (filtros & servicios)
  - Mecanismos de detección de ataques de DDoS
  - Técnicas de mitigación de DDoS

Un pequeño error...
Un gran problema...

- DNS es un servicio esencial
  - Mal configurado se presta a ataques de amplificación.
  - Para concientizar a los operadores sobre la importancia de proteger sus redes se realizó una demostración con:
    - 1 servidor DNS vulnerable
    - Ataque en el que el usuario envía 1.2MB
    - Y la víctima recibe 250MB

- Video charla ArNOG

PLAN DE ACCIÓN

Próximos pasos....

Plan de acción con Innovared y sus miembros

Entre las actividades en las que podemos intervenir podemos mencionar:

- la colaboración en la formación de recursos humanos
- y el acompañamiento en la puesta marcha de nuevos CSIRT dentro de la comunidad

La necesidad de que cada miembro tenga un CSIRT propio radica en que es el único que tiene la potestad para gestionar los incidentes de seguridad en sus redes.

Plan de acción

Definidos los equipos dedicados a la seguridad, es preciso:

- Conformar un directorio que incluya a los responsables de seguridad de InnovaRed y sus distintos miembros.
- Promover el uso de PGP para garantizar la confidencialidad de las comunicaciones con información sensible. Por ejemplo, las relacionadas a incidentes de seguridad o informes de auditoría.
- Armar una lista de correo cerrada en la que estén en primera instancia los responsables de seguridad de los distintos miembros de InnovaRed.

Plan de acción a futuro

- Trabajar junto a los nuevos CSIRTs para:
  - Desarrollar un protocolo de prevención de incidentes.
  - Investigar incidentes de seguridad detectados en la red o los servicios de InnovaRed.
  - Realizar evaluaciones preventivas de seguridad sobre redes y servicios (testeos de seguridad de red, servicios y aplicaciones).
  - Participar en forma conjunta en eventos o paneles relacionados con ciberseguridad.

Semana de la seguridad Informática

- Todos los 30 de noviembre a nivel mundial se llevan a cabo eventos por el día Internacional de la Seguridad Informática.
- Aprovechando esa fecha organizaremos en esa semana un evento junto a InnovaRed donde estarán invitados a participar a todos los miembros.

CERT UNLP
Equipo de Respuesta a Incidentes de Seguridad

Semana de la seguridad Informática

- Para esa jornada planteamos los siguientes objetivos:
  - Conformación de lista de responsables de seguridad de la información de InnovaRed y sus miembros
  - Taller Hands On:
    - Generación de identidad PGP
    - Ejercicio de simulación estilo Cyberdrill

Hands On PGP

- Pretty good Privacy
  - Conceptos y cuidados sobre PGP
  - Generación de claves PGP
  - Publicación y uso
  - Intercambio de claves públicas entre los asistentes al taller
  - Resultados esperados:
    - Todos los asistentes con claves PGP generadas
    - Generación de anillo de confianza

Ejercicio de simulación estilo Cyberdrill

- Ejercicio por equipos formados entre los asistentes
- Presentación de escenarios reales que involucren algún incidente de seguridad a definir
- Objetivo: Atención del incidente, incluyendo:
  - Recepción del reclamo
  - Análisis del evento
  - Reporte final

Gracias!!

Contactos:

Javier Díaz: jdiaz@unlp.edu.ar

Nicolás Macia: nmacia@cert.unlp.edu.ar

Paula Venosa: pvenosa@cert.unlp.edu.ar

Einar Lanfranco: elanfranco@cert.unlp.edu.ar

CeSPI
UNIVERSIDAD NACIONAL DE LA PLATA

UNIVERSIDAD NACIONAL DE LA PLATA

CERTUNLP
Equipo de Respuesta a Incidentes de Seguridad