TICAL 2024

Ciberseguridad en las Universidades Nacionales de Argentina

Estrategias de ARIU para la articulación

Lic. Alejandro Del Brocco

Presentación de ARIU

La Asociación Redes de Interconexión Universitaria ARIU es un emprendimiento conjunto de las Universidades Nacionales (UUNN) e Institutos Universitarios integrantes del CIN (Consejo de Rectores de las Universidades Nacionales) con el propósito de llevar adelante la gestión de redes para facilitar la comunicación informática a nivel nacional e internacional, de las universidades nacionales, promoviendo la investigación informática, tecnológica, educativa y el desarrollo cultural en el área de las TIC.

ARIU


DEL SUR
ESTADO DE SÃO PAULO
ESTADO DE RÍO DE JANEIRO
Paraguay
São Paulo
ESTADO DE PARANÁ
Chile
SANTA CATARINA
RÍO GRANDE DEL SUR
Santiago
Buenos Aires
Montevideo
Islas Georgias del Sur y Sandwich del Sur

ARIU Infraestructura

63

Universidades Nacionales

+65.000
Direcciones IPv4

+MM /32
Direcciones IPv6

+70GB/s
Ancho de Banda

DNS
3 servidores ZA
2 servidores Recursivos RPZ
22UNNN DNSECC
150 Servidores ANYCAST Mundial
I-K Root Servers

Peers
Google
CABASE
INNOVARED-RedClara
Telcom Argentina
Telefonica Argentina
Century Link

BFA
9 Nodos de Sellado
1 Nodo de Monitoreo
+10 Nodos de Aplicación

ARIU Servicios

63

Universidades Nacionales

+100
Salas de comunicación colaborativa

Capacitación
Para personal de las Areas de TI

+4000
Dominios
EDU.AR

Salas de VC
Fisicas y vituales para clases y defensas de Tesis

+300
Servidores Virtuales

Central PBX
Comunica todas las UUNN

Gestión
Diplomas Digitales
Actas Digitales

- Campus Virtuales
- Sistemas de Gestión Académica
- Almacenamiento de Información
- Sistema de Expediente Digital

Ciberseguridad

Teniendo en cuenta la infraestructura y los servicios que brinda ARIU y el constante crecimiento de los Ciber-ataques y amenazas, comenzamos a considerar soluciones enfocadas en la Ciberseguridad para la institución y las Universidades.

Primera Articulación

TICAL 2024

ARIU
Asociación Redes de Interconexión Universitaria

CiN Consejo Interuniversitario Nacional

SIU SISTEMA DE INFORMACIÓN UNIVERSITARIA

Acuerdos de Intercambio

TICAL 2024

Alcance de la red y eventos reportados

+65.000
Direcciones IPv4

+MM /32
Direcciones IPv6

+70GB/s
Ancho de Banda

+4000
Dominios
EDU.AR

+12.000
Mails con Reportes de incidentes

+80
Tipos de Reportes:
- Malware
- DDos
- Botnets
- Black Lists

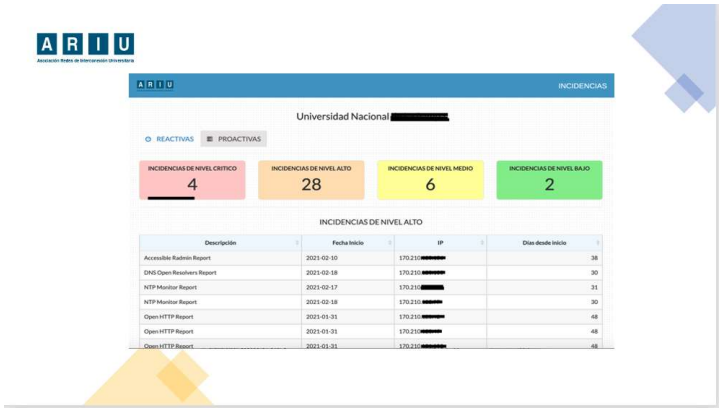
+500.000
Eventos de Seguridad procesados

Primeros Servicios

TICAL 2024

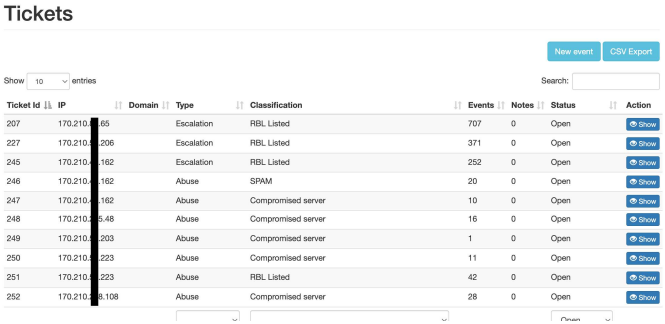
PECA

Plataforma de **E**ventos de **C**iberseguridad **A**RIU

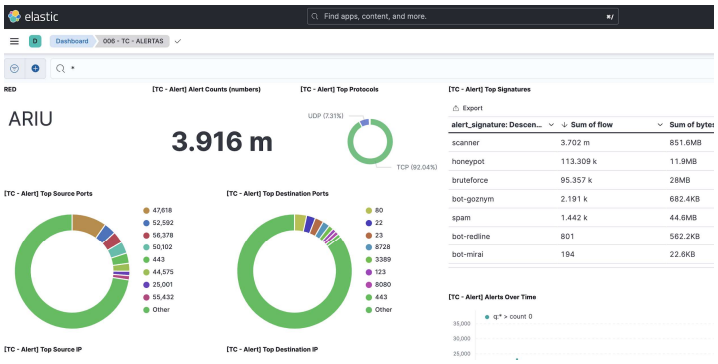


ABUSEIO

Open Source abuse management



Nimbus Threat Monitor



Camino crítico

RIUTEC 2022 – Primera presentación de MISP

Reuniones de Subcomisión de Ciberseguridad 2022-2023 dan lugar a las primeras pruebas de concepto

RIUTEC 2023 – Puesta en funcionamiento con 3 universidades

TICAL 2023 – Proyecto RedClara y CERN MISP

Segunda Articulación

TICAL 2024

CiN Consejo Interuniversitario Nacional

SIU SISTEMA DE INFORMACIÓN UNIVERSITARIA

ARIU Asociación Redes de Interconexión Universitaria

Red CLARA

CERN

Diseñando una solución

MISP - Malware Information Sharing Platform

Es una plataforma de código abierto diseñada para facilitar el intercambio de información sobre ciberamenazas. MISP permite almacenar, gestionar y compartir indicadores de compromiso (IoC), TTPs (tácticas, técnicas y procedimientos) y otros tipos de información relevante.

pDNSSOC

Es un sistema desarrollado por el CERN (Organización Europea para la Investigación Nuclear) para gestionar y proteger los servicios de DNS. Incorpora herramientas de inteligencia de amenazas y correlación de eventos para identificar patrones de ataques y vulnerabilidades en tiempo real.

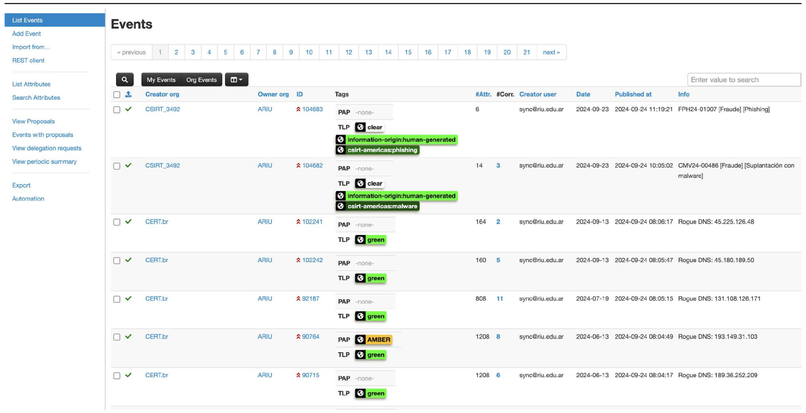
RPZ – Response Policy Zone

Es una técnica utilizada en sistemas DNS para implementar políticas de seguridad y control sobre las respuestas de los servidores DNS. Permite a los administradores redirigir, bloquear o modificar las respuestas de resolución de nombres.

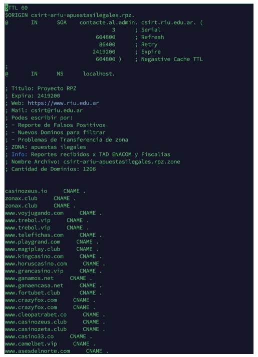
Integración de la solución

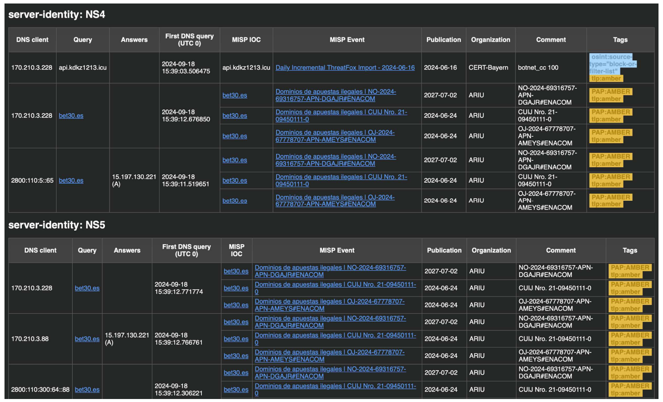
TICAL 2024

MISP Threat Sharing



RPZ





Tercer Articulación

TICAL 2024

SIU SISTEMA DE INFORMACIÓN UNIVERSITARIA

CERN

CiN Consejo Interuniversitario Nacional

Red CLARA

ARIU
Asociación Redes de Interconexión Universitaria

ENACOM
Ente Nacional de Comunicaciones

Universidad Nacional de Quilmes

UNL UNIVERSIDAD NACIONAL DEL LITORAL

Universidad Nacional del Comahue 1972

Universidad Nacional del Sur UNS Bahía Blanca

UNPAZ

CONICET

Universidad Nacional de General Sarmiento

UNIVERSIDAD NACIONAL DE LA PLATA

UNLPam
Universidad Nacional de La Pampa

UNC Universidad Nacional de Córdoba

CÁMARA ARGENTINA DE Internet

CERT.ar

Métricas Actuales

TICAL 2024

MISP Threat Sharing

- 14 Organizaciones conectadas
- 1217 IOC procesadas
- 6 Universidades en proceso de adhesión

RPZ

- Apuestas Ilegales
- Cloinblocker
- Porn
- Torbloker

- Reportes Match cada 1 hora
- 4 Servidores recursivos ARIU
- 8 Universidades en uso
- 10 en proceso

Trabajando Actualmente

Nuevas articulaciones

- Actores Gubernamentales: CERT de la Provincia de Buenos Aires y ReNaPer
- Universidades Privadas: CRUP
- Instituciones Privadas: Cámaras y Empresas

Servicio de Recuperación ante ataques

- Servicio centralizado para que cada institución tenga su primera, segunda o tercera instancia de copias de respaldo con protección de los datos.

Propuesta de SOC

- Diseñamos un SOC con software Open Source
- Construimos una solución basada en contenedores para el despliegue rápido
- Articulamos para sumar reportes al MISP

Servicio de Recuperación ante ataques

TICAL 2024

Infraestructura ARIU

Virtualización de Servicios de Backup de 1ra, 2da o 3ra instancia

Storage Centralizado

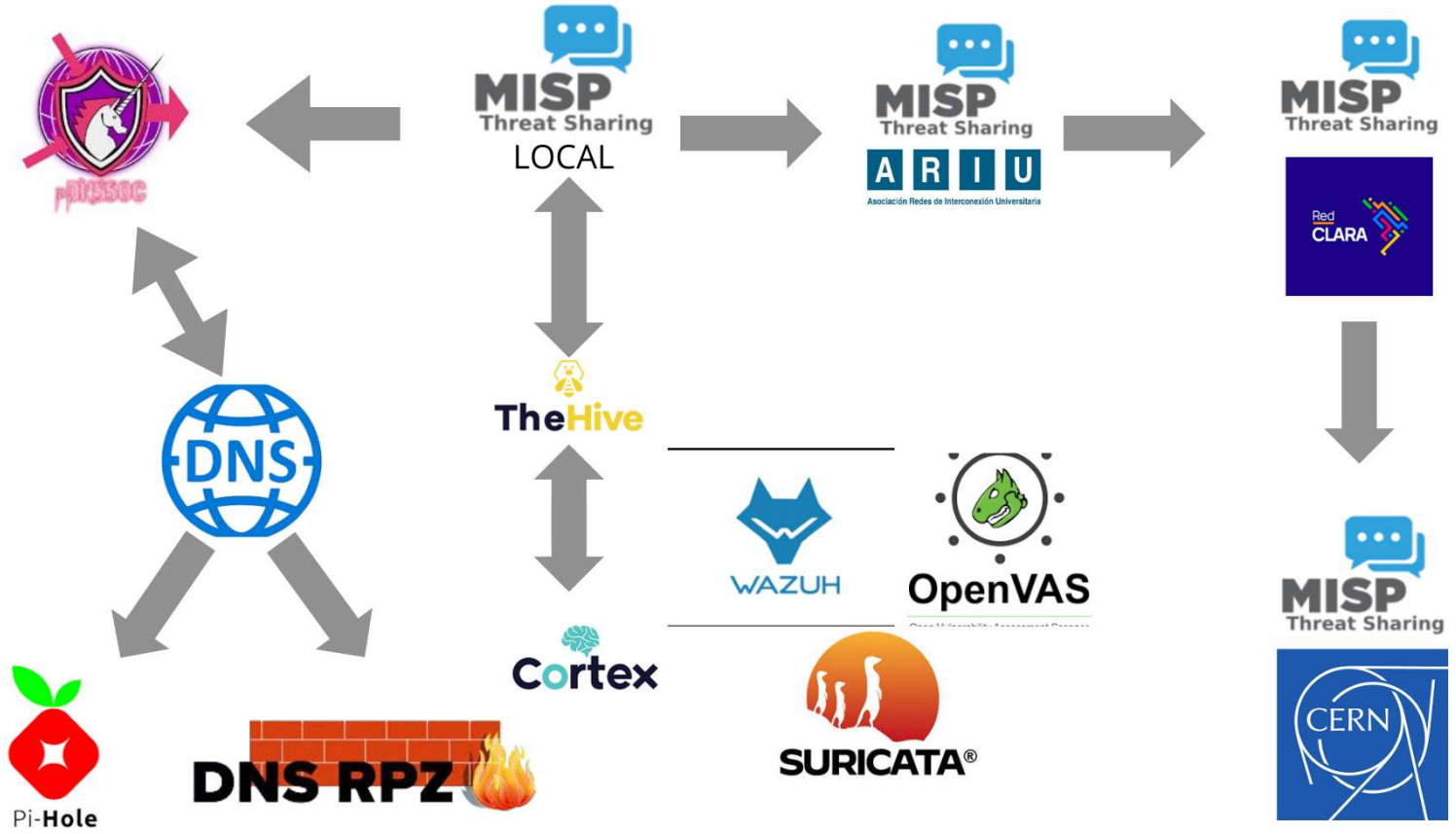
Solución de almacenamiento 5 TB ampliable a 10TB para cada Universidad Conectada

Seguridad

Encriptación de datos
Espejado de Volúmenes
Clonado
WORM Escritura única
Instantáneas

Propuesta de SOC

TICAL 2024



Creditos
Fabian Ampalio
UNQ

Agradecimientos

- Equipo Técnico de ARIU
- Subcomisión de Ciberseguridad del CIN
- Equipo Técnico de las UUNN
- Equipo Técnico de RedClara
- Pau Cutrina y equipo del CERN

Analia Barberio
Coordinadora Subcomsión de
Ciberseguridad del CIN

Luciano Minuchin
Coordinador Ciberseguridad
ARIU

Fabian Ampalio
Responsable Ciberseguridad
UNQ

¡GRACIAS!

OBRIGADO!

THANKS!

¿Alguna pregunta? Alguma pergunta? Any questions?

Contacto

alejandro@riu.edu.ar

lminuchin@riu.edu.ar