Experiencia del AICM en Ciberseguridad

Aeropuerto Internacional de la Ciudad de México

Gerardo Oseguera Caballero
Jasiel Abreu López

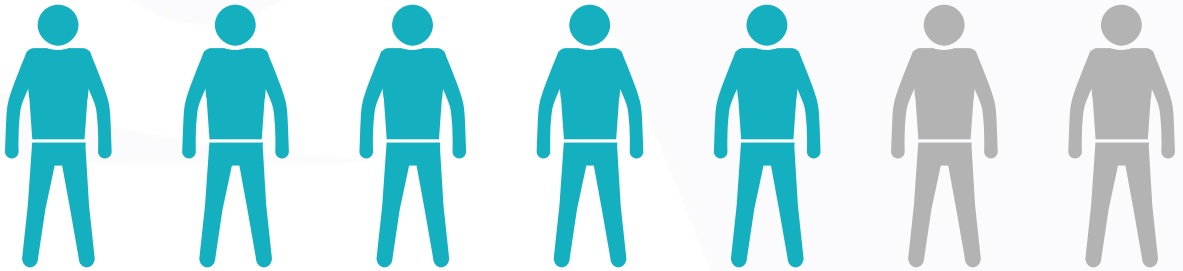
Diciembre 2018

¿Quiénes somos?

Cantidad de pasajeros

+39 millones

*al mes de octubre de 2018



Cantidad de operaciones

+381 mil

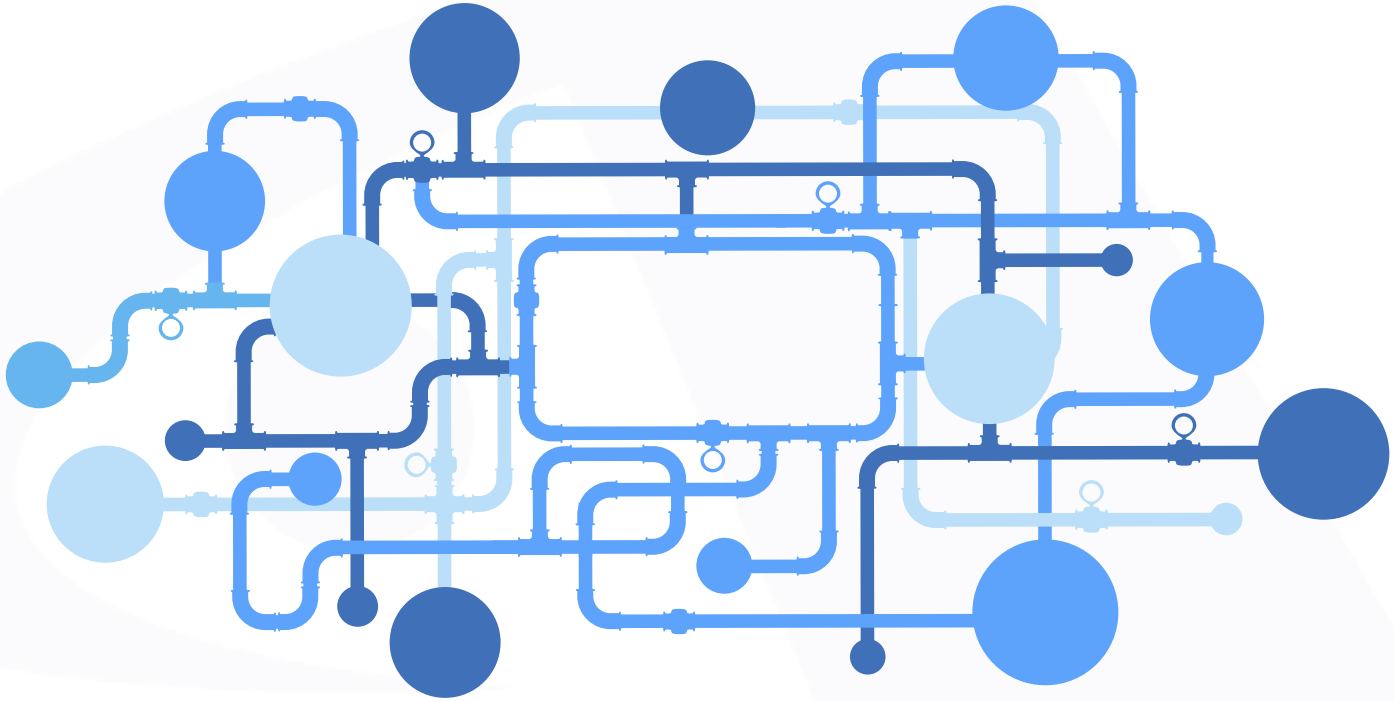
*al mes de octubre de 2018

Cantidad de carga

+480 mil toneladas

*al mes de octubre de 2018

Cantidad de nodos



+6 mil nodos de red

Sistemas Aeroportuarios

- Red Administrativa (LAN)
- Toma de Decisiones en Colaboración de Aeropuertos (CDM)
- Base de Datos Operacional Aeroportuaria (AOBD)
- Sistema de Gestión de Edificios (BMS)
- Red de Internet Público
- Cuarto de Control y Equipo de Monitoreo
- Sistema de Gestión de Credenciales de Seguridad
- Sistema de Antenas Distribuidas (DAS)
- Sistema de Visualización Dinámica (DDS)
- Sistema de Alarma de Incendios (FAS)

Sistemas Aeroportuarios *(continuación)*

- Sistema de Reloj Maestro
- Sistema de Distribución de Mensajes (MDS)
- Sistema de Distribución Multimedia (MMDS)
- Sistema de Ingresos de Estacionamiento
- Sistema de Gestión de Lugares de Estacionamiento
- Sistema Perimetral de Detección de Intrusos (PIDS)
- Sistema de Notificación Masiva y de Megafonía (PAMNS)
- Sistema de Visualización de Información de Rampa (RIDS)
- Sistema de Control de Acceso de Seguridad (SACS)
- Puestos de Inspección de Personas

Sistemas Aeroportuarios *(continuación)*

- Sistema de Detección de Explosivos para la inspección de equipajes. (EDS-CT)
- Sistema de Gestión de Información de Seguridad (SMIS)
- Sistema de Inspección Médica
- Quioscos de Información
- Sistema de Control de Supervisión y Adquisición de Datos (SCADA)
- Sistema de Vigilancia por Video (VSS)/Reconocimiento de Placas Vehiculares
- Sistema de Manejo de Equipaje (BHS)
- Comunicación por Voz (VoIP)

Sistemas Aeroportuarios *(continuación)*

- Sistema de Visualización de Información de Vuelos (FIDS)
- Sistema de Transporte Inteligente (APM)
- Sistema de Control para Iluminación
- Sistema de Radiocomunicación Interna
- Sistema de Separación de Flujos

Ataques exitosos

- JUN 06, 2010 – Ataque a la página oficial del AICM.
- MAR 21, 2015 – Ataque a la cuenta de Twitter

Inicio › Ciudad › Confirman "hackeo" a página web del AICM

Ciudad

Confirman "hackeo" a página web del AICM

Por - 6 junio, 2010

Tamaño de fuente: A A

Notimex

Autoridades aeroportuar
Internacional de la Ciud
que el servidor de la ter

Indicaron que luego de
restablecerá una vez qu

MEXICO DF

Reactivan pagina del
hackeo

Foto Ilustrativa

Luego de dos días de
de internet del Aeropu
fue reactivada a las 16

compartir

Me gusta A 2,4 mil personas les gusta e

Luego de dos días de estar fuera de línea tras ser "hackeada", l
de la Ciudad de México (AICM) fue reactivada a las 16:30 horas

Antes de ser subir la página, el área de sistemas de la terminal aérea tuvo un periodo de pruebas para verificar que el sistema no pudiera ser vulnerado nuevamente.

HACKEAN CUENTA DE AICM

Vistas: 2,107

Compartir en Twitter

M reporta supuesto "hackeo" a
uenta de Twitter

E 21 MARZO 2014 8:55

Internacional de la Ciudad de México
ó que su cuenta de Twitter @AICM3 fue
madrugada de hoy viernes.

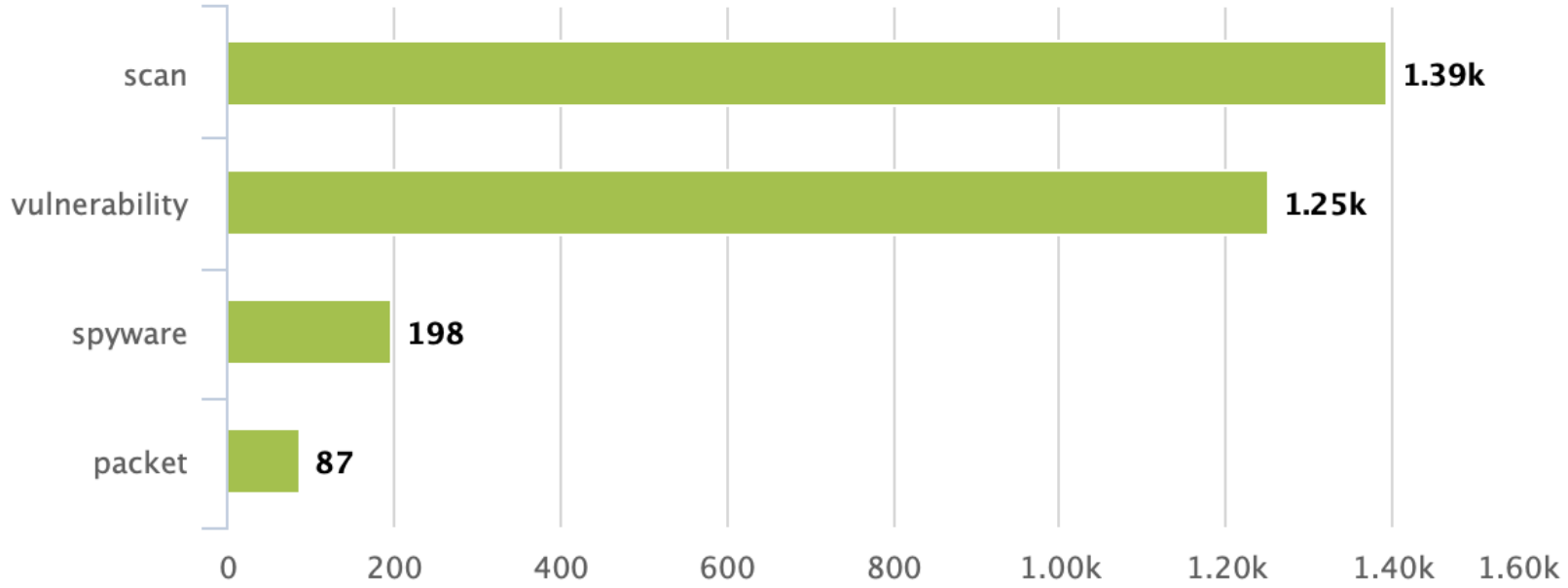
n mensaje publicado cerca de las 01:10
inal aérea detalló: "@AICM3, informa que
a' su cuenta. Entraron mensajes cuyo
ocemos".

¿Cómo nos protegemos?

- Firewalls. Que se mantienen actualizadas sus bases de datos, para detectar y bloquear toda amenaza

¿Cómo nos protegemos? (continuación)

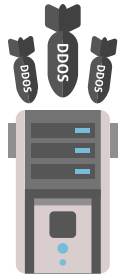
- Bloqueo de amenazas. Debido a la configuración del equipo se bloquean eventos con severidad Crítica, Alta o Media, adicional se bloquean eventos del tipo de inundación de paquetes TCP.



¿Cómo nos protegemos? (continuación)

Blocked Threats

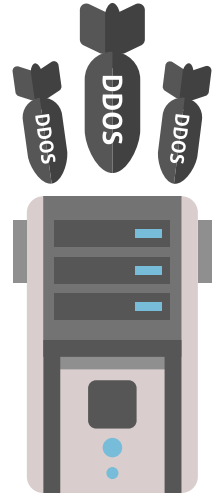
Threat Name	ID	Threat Type	Threat Categ...	Severity	Count
SCAN: Host Sweep	8002	scan	scan	medium	1.4k
ASUS/Netcore Router Default Credential Remote Code Execution Vulnerability	39438	vulnerability	code-execution	medium	727
SMB: User Password Brute Force Attempt	40004	vulnerability	brute-force	high	199
Sybase Database User Authentication Brute Force Attempt	40013	vulnerability	brute-force	high	194
TCP SYN with data	8723	packet	unknown	informational	87
ZeroAccess.Gen Command and Control Traffic	13235	spyware	botnet	critical	83
ChinaChopper.Gen Command and Control Traffic	12017	spyware	spyware	critical	73
Apache Struts Jakarta Multipart Parser Remote Code Execution Vulnerability	34221	vulnerability	code-execution	critical	40
Squid HTTP Header Parsing Assertion Failure Denial of Service Vulnerability	39682	vulnerability	dos	medium	29
generic:bigdata.adsunflower.com	210572640	spyware	dns-wildfire	medium	14
generic:zh.us.to	211052277	spyware	dns-wildfire	medium	13
TLS Network Security Protocol Information Disclosure Vulnerability - ROBOT	38407	vulnerability	info-leak	high	10
RPC Portmapper DUMP Request Detected	32796	vulnerability	info-leak	medium	9
Win32.Conficker.C p2p	12544	spyware	net-worm	critical	8
Netis/Netcore Router Default Credential Remote Code Execution Vulnerability	39587	vulnerability	code-execution	high	8
Microsoft Internet Explorer Cached Objects Zone Bypass Vulnerability	33813	vulnerability	code-execution	high	6
HTTP SQL Injection Attempt	36239	vulnerability	sql-injection	medium	4
Apache Struts Content-Type Remote Code Execution Vulnerability	33196	vulnerability	code-execution	critical	3
SCAN: TCP Port Scan	8001	scan	scan	medium	3
Suspicious DNS Query (Worm.gamarue:differentia.ru)	54920742	spyware	dns	medium	2
Apache Struts 2 Remote Code Execution Vulnerability	33948	vulnerability	code-execution	critical	2
HTTP SQL Injection Attempt	33338	vulnerability	sql-injection	medium	2
JBoss.Worm Command and Control Traffic	13121	spyware	net-worm	critical	2
Suspicious DNS Query (Worm.gamarue:differentia.ru)	54920742	spyware	dns-wildfire	medium	2
Dahua Security DVR Appliances Authentication Bypass Vulnerability	38926	vulnerability	code-execution	high	2
Avtech Devices Unauthenticated Information Disclosure Vulnerability	54525	vulnerability	info-leak	medium	2
Apache Struts2 OGNL Remote Code Execution Vulnerability	54691	vulnerability	code-execution	high	2
OpenSSL TLS Malformed Heartbeat Request Found - Heartbleed	36397	vulnerability	info-leak	medium	2
Squid Proxy Server Accept Language Denial of Service Vulnerability	36876	vulnerability	dos	high	2
HTTP SQL Injection Attempt	30514	vulnerability	sql-injection	medium	2
WordPress REST API Remote Code Execution Vulnerability	30571	vulnerability	code-execution	critical	1
ECShop Remote Code Execution Vulnerability	54648	vulnerability	code-execution	critical	1
generic:t2m.io	211387455	spyware	dns-wildfire	medium	1
WordPress CuckooTap Theme Arbitrary File Download Vulnerability	37363	vulnerability	info-leak	medium	1
LinkSys E-series Routers Remote Code Execution Vulnerability	36358	vulnerability	code-execution	high	1
DLink DSL Remote OS Command Injection Vulnerability	54505	vulnerability	code-execution	high	1
Wordpress MailPoet Newsletters Unauthenticated File Upload Vulnerability	37105	vulnerability	code-execution	medium	1
IBM Rational Quality Manager and Test Lab Manager Remote Code Execution Vulnerability	34181	vulnerability	code-execution	medium	1

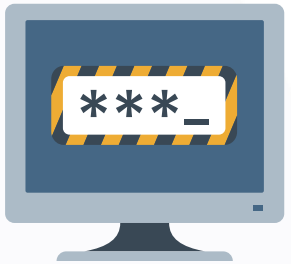


Principales Amenazas Detectadas

¿Cómo nos protegemos? (continuación)

- Procedimientos
- NOC/SOC
- Sistema de Detección de Intrusos
- Capacitación
- Filtrado DDoS
- Encriptación de Bases de Datos y VoIP
- VPN
- Pentesting
- Antivirus



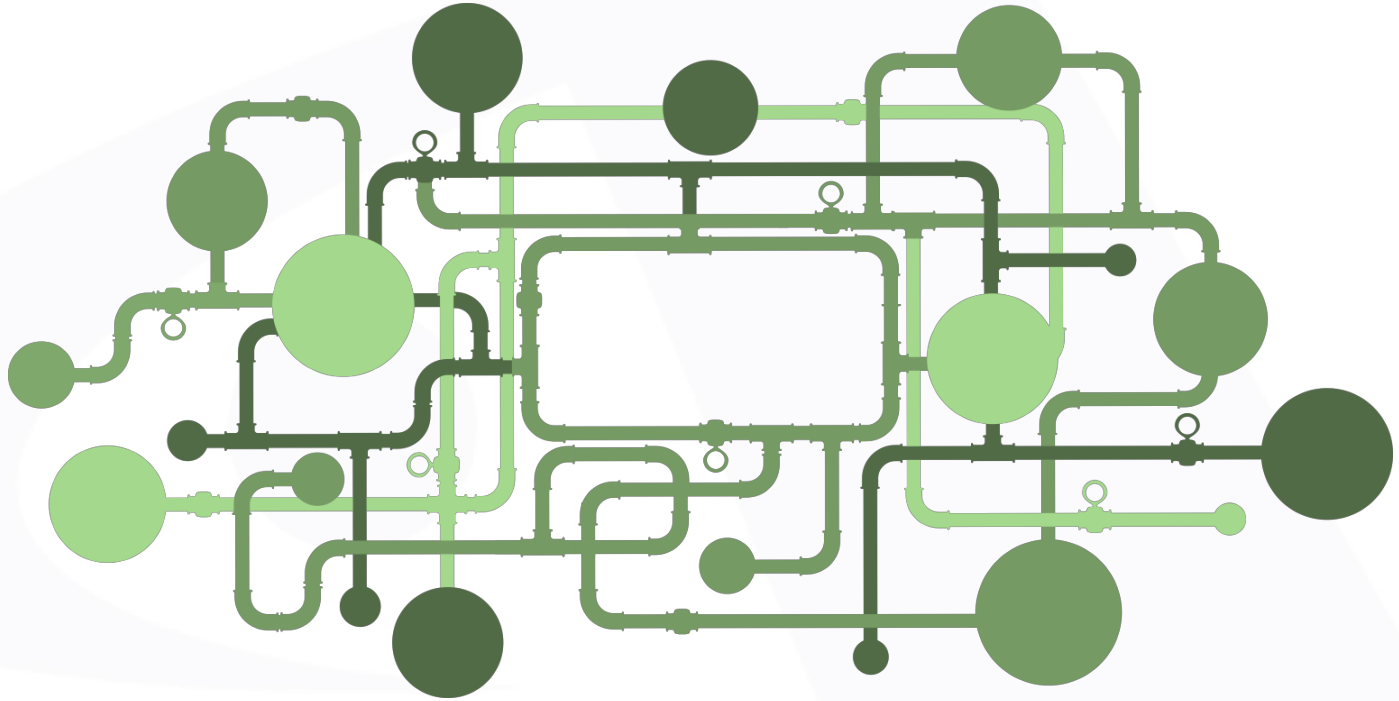


¿Cómo nos protegemos? (continuación)

- Separación de Redes
- Certificación de Aplicaciones
- Directorio Activo
- Definición de Políticas y Privilegios
- Purga de Código
- Bloqueo de Páginas
- Uso de Máquinas Virtuales
- Entre otras…

Ciberseguridad AVSEC

Nodos de equipos de seguridad



+2.5 mil nodos de red

Entre cámaras, servidores, servidores de almacenamiento, estaciones de trabajo, etc.

Análisis de riesgos

Mediante el cual se detectó la infraestructura crítica que debemos proteger en materia AVSEC:

- Sistema de Gestión de Información de Seguridad (SMIS)
- Cuarto de Control y Equipo de Monitoreo
- Sistema de Gestión de Credenciales de Seguridad
- Sistema Perimetral de Detección de Intrusos (PIDS)

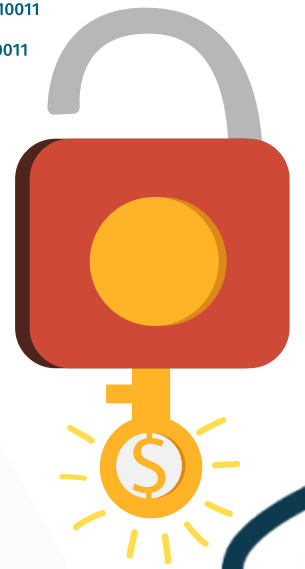
Análisis de riesgos (continuación)

- Sistema de Control de Acceso de Seguridad (SACS)
- Sistema Perimetral de Detección de Intrusos (PIDS)
- Sistema de Detección de Explosivos para la inspección de equipajes. (EDS-CT)
- Sistema de Vigilancia por Video (VSS)/Reconocimiento de Placas Vehiculares
- Sistema de Separación de Flujos

¿Qué debíamos hacer?

Medidas que se adoptaron

- Instalación de Firewall que nos permite separarnos de la Red Administrativa
- Cambio de Contraseñas
- Cierre de puertos en Switchs
- Implementación de NOC de seguridad



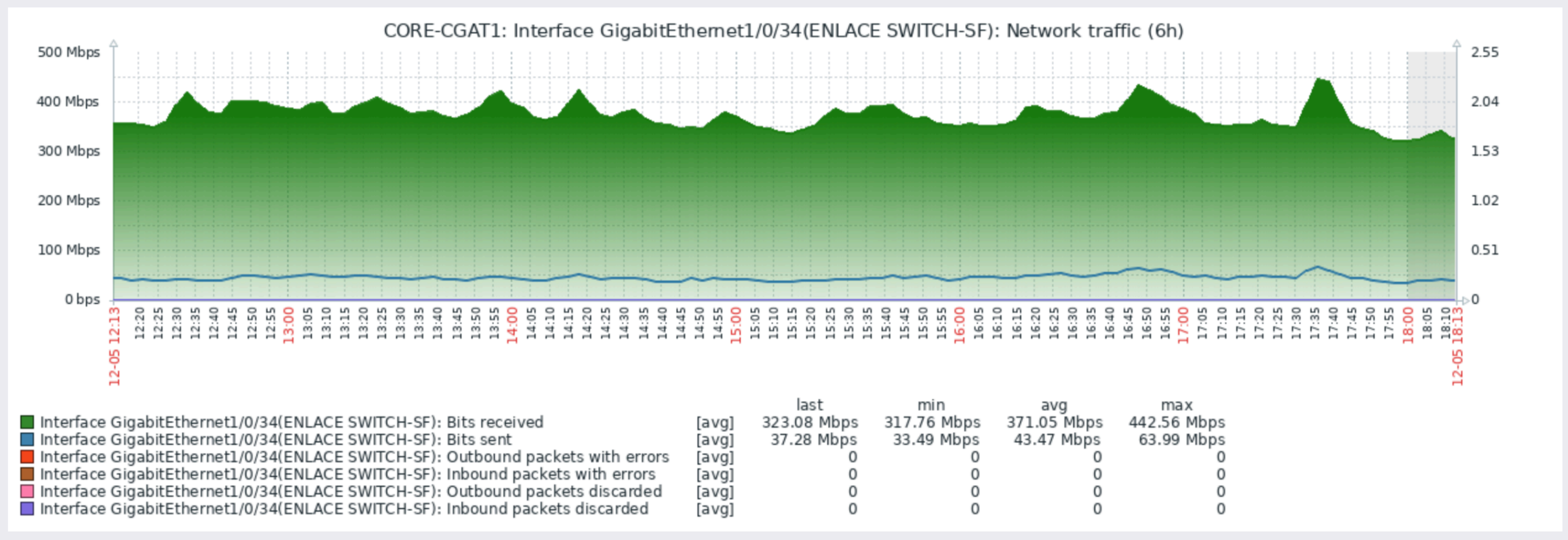
NOC (Network Operations Center)

Problems

Time ▼	Recovery time	Status	Info	Host	Problem • Severity	Duration	Ack	Actions
18:02:30	18:02:33			SWS-CGAT1-02	Zabbix agent en SWS-CGAT1-02 perdió la comunicación por mas de 1 minuto	3s	No	Done 6
18:00								
17:45:42				AX-CAL-101-57	Interface eth0: High bandwidth usage >95%	20m 36s	No	Done 2
17:34:20		PROBLEM		AX-EV3-022-100	Interface eth0: High bandwidth usage >95%	31m 58s	No	Done 2
17:09:41	17:39:41			AX-CAL-101-57	Interface eth0: High bandwidth usage >95%	30m	No	Done 4
17:00								
14:11:52		PROBLEM		CF-DC-19-2111	Unavailable by ICMP ping	3h 54m 26s	No	Done 1

NOC (Network Operations Center)

NOC (Network Operations Center)



Evolución a un NOC/SOC

Resolución en ENTRADA OSCAR 03 - AXIS con el nivel Warning

zabbixaicm@gmail.com
Mar 04/12/2018, 15:41
Usted

Problem has been resolved at 17:41:50 on 2018.12.04
Problem name: AX-EV3-022-100 has been restarted
Host: AX-EV3-022-100
Severity: Warning

Original problem ID: 26973847

Problema en SWITCH-SF con el nivel Average

zabbixaicm@gmail.com
Mié 05/12/2018, 18:08
Usted

Problem started at 20:08:03 on 2018.12.05
Problem name: Interface Unit: 1 1000BASE-T RJ45 Gigabit Ethernet Frontpanel Port 5: Link down
Host: SWITCH-SF
Severity: Average

Original problem ID: 27326789

¿Qué sigue?

¿Qué sigue?

- Completar la implementación de Ciberseguridad
- Separación total de redes
- Obtener por lo menos, la certificación ISO 27001
- Aplicar lo aprendido en el taller

¿Preguntas?

¡Muchas Gracias!

“Sed quis custodiet ipsos custodes? (¿Quién vigila a los vigilantes?)”

-Anónimo.