S21SEC

Your Cybersecurity Company

Next Generation SOC:

Seguridad e Inteligencia en Medios de Pago

16 YEARS experience in the business of cibersecurity.

Prevención y respuesta ante incidentes

24x7x365

100%
CIBERSECURITY

S21sec

Perfil S21sec
Algunos datos

250
ESPECIALISTAS en seguridad certificados y reconocidos internacionalmente

20%
DE LAS COMPAÑÍAS DEL DOW JONES EUROSTOXX 50 SON CLIENTES DE S21SEC

Proyectos en
26
PAISES

RECONOCIDA por
ANALISTAS INTERNACIONALES
como una de las mejores empresas a nivel internacional

La
INNOVACIÓN
como motor de negocio

El Entorno


The world
is moving fast,
cybersecurity faster

Cybersecuridad es un asunto global y afecta a la agenda de todos los CxO

Global Study of Boardroom Issues and C-Suite Concerns

1. Regulatory changes and scrutiny may affect how our products/ services are produced or delivered
2. Economic conditions may significantly restrict growth opportunities
3. Our organisation may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/ or damage our brand
4. Our organisation´s succession challenges and ability to attract and retain top talent may limit our ability to achieve operational targets
5. Our organisation´s culture may not sufficiently encourage the timely identification and escalation of risk issues that have the potential to significantly affect our core operations and achievement of strategic objectives
6. Resistance to change may restrict our organisation from making necessary adjustments to the business
7. Ensuring privacy / identify management and information security / system protection may require significant resources
6. Our organisation may not be sufficiently prepared to manage an unexpected crisis significantly impacting our reputation

- Our organisation may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/ or damage our brand
- Our organisation´s culture may not sufficiently encourage the timely identification and escalation of risk issues that have the potential to significantly affect our core operations and achievement of strategic objectives
- Ensuring privacy / identify management and information security / system protection may require significant resources
- Our organisation may not be sufficiently prepared to manage an unexpected crisis significantly impacting our reputation

Protiviti, Executive Perspectives on Top Risks, 2015

Los ataques cibernéticos afectan a todas las industrias

Cyber Goes Well Beyond Banking

In May, eBay revealed that hackers had managed to steal personal records of 233 million users. The hack took place between February and March, with usernames, passwords, phone numbers and physical addresses compromised.

The State of Montana's health department revealed that a data breach may have affected more than 1 million people. The hack actually happened in July last year, but it wasn't discovered until May this year, with the identity of the intruders, and the extent of the damage done, still unclear.

Target announced in January that hackers had stolen data—including names, mailing addresses, phone numbers and email addresses—from over 70 million shoppers, and the credit card information of 40 million shoppers. 1-3 million of those credit cards were then sold on the black market.

Hacking group Rex Mundi held Domino's Pizza to ransom over 600,000 Belgian and French customer records: names, addresses, emails, phone numbers and even favourite pizza toppings.

In addition to all of its 11 channels, TV5Monde also lost control of its social media outlets and its websites. On a mobile site that was still active, the network said it was "hacked by an Islamist group.

As many as 300 oil and energy companies have been targeted by hackers in the largest ever coordinated cyber attack in Norway. Local reports suggest that 50 companies in the oil sector have already been breached while another 250 are at risk.

Various online news outlets, all stories relate to 2014/15

La evolución de los cyber criminals: de Amateur a crimen organizado

Romantic Era							Middle Ages					Age of Fraud				Age of eCrime		
1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006		2007	2008	2009	2010	2011	2012	2013

Attack Vectors

- Destructive viruses
- Localised
- Without propagation
- Lone warriors

- First phishing attacks
- (11S)

- Worms (Blaster et al)
- Botnets 1.0 (IRC)

- Cyber militias
- Multiple objectives

- Geopolitical attacks
- Botnets 2.0
- Bullet-proof ISP
- Infrastructure for sale

- Iframe business
- Pay per install
- Clickfraud
- Next Gen Botnets
- DDoS
- Infection kits
- C&C
- Cyberwarfare
- Industrial espionage

Motivators

- Personal challenge
- Technical knowledge
- Arrogance

- Fast cash
- Massive infections
- Press

- Cash at all cost
- Extortion

- Big money
- Total criminal concepts
- Control of the Internet
- Total domination

Perpetrators

- Individuals
- Small groups

- Individuals
- Small groups

- Individuals
- Medium-sized groups

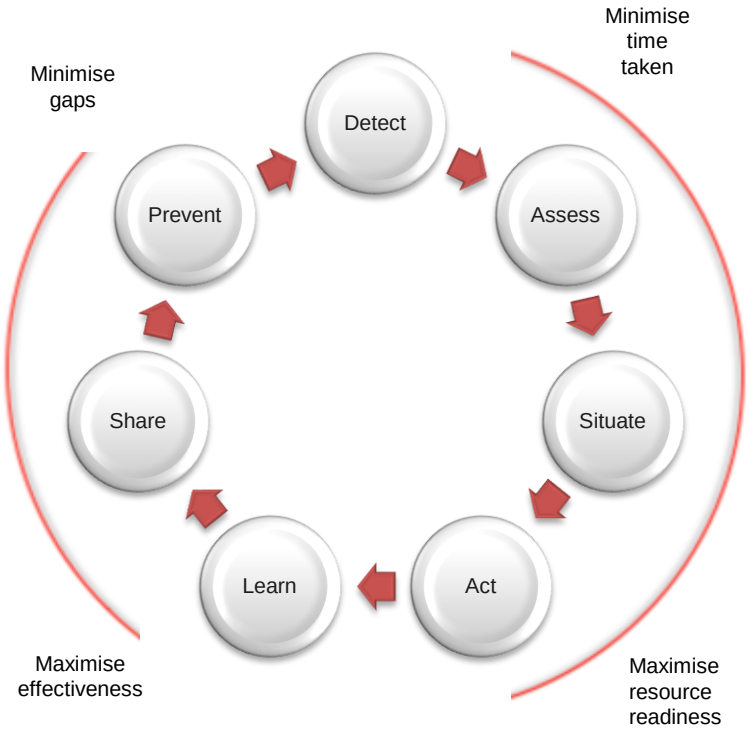
- Organised crime

El comportamiento hoy de las empresas: Servicios y Productos básicos

Basic Security Products	Basic Security Services
Vulnerability Management	Pentests and Vulnerability Scans
Perimeter Protection	Compliance Consulting
Malware / Anti-Virus Detection	Perimeter and Device Monitoring / Management
VPN / Remote Protected Access	Corporate Security Policies and Training
Application and Web Server Protection	

Las necesidades de las empresas para poder responder a las amenazas actuales

Cyber Threat Management Challenges



	Objective	Key Requirements
Detect	• Early warnings • Alerts	• Source of intelligence • Industry relationships
Assess	• Prioritise • Understand vectors	• Analytical framework • Analytics tools
Situate	• Inform affected areas • Coordinate	• Stakeholder involvement • Process
Act	• Incident response • Containment	• Tools • Process
Learn	• Continuous improvement • Cultural change	• Executive commitment • Resources
Share	• Engender 1+1=3 logic • Collaborate	• Ecosystem relationships • Credibility
Prevent	• Stop future attacks	• Tools • Infrastructure

Las empresas maduras en ciberseguridad solo buscan *partners* que les ayuden a su desarrollo en personas, procesos y tecnología de forma integral

Advanced Cyber Capabilities	Threat Intelligence	Behaviour Analytics	Context Correlation	Dynamic Response	Open Source Intelligence	Business Process Awareness
Business-orientated Professional Services						
Advanced End-Point Protection and Awareness						
Lateral Movement and Traffic Behaviour Analysis						
Encryption with Local and Cloud Info Protection						
Context-enriched Threat Intelligence						
Unified Security Analytics						

El día a día…!!!

- No existen las malas noticias, porque son sólo noticias.

Fraudes bancarios empleando comprobantes impresos

Fraude electrónico es inherente a todas las transacciones financieras de empresas

México, Brasil, Colombia y Venezuela lideran tasas de fraude financiero en A. Latina

Crece el fraude bancario online en México

Share/Bookmark

Según datos recogidos por la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) los fraudes bancarios en México reportaron

SUBANCO

Aumento de usuarios y de ataques alertan un a fraudes bancarios online

Fraude y Seguridad Bancaria

Una tendencia que irá en aumento en nuestra región durante el 2015, será la cantidad de **fraudes** qu en los bancos. Esto sigue una de las **tendencias mundiales de fraude digital**, que durante el 2014 a los bancos y empresas de *retail* más importantes del mundo. Los delincuentes ven en Latinoa **espacio de crecimiento en sus delitos debido** a la poca cultura de los usuarios en el manejo tra

Código malicioso: la nueva forma de realizar fraudes bancarios

Luego que el pharming y phishing perdieran terreno como métodos para sustraer fondos, esta nueva amenaza electrónica ha comenzando a ganar espacio y en silencio. Aunque la infección ocurre sin que el usuario se de cuenta, los bancos ya han tomado medidas.

Fraude, el mayor temor para los usuarios de banca móvil

El 31 por ciento de los latinoamericanos con cuenta bancaria aún no usa Internet para transacciones financieras, especialmente por temor a que los timen, según un estudio de Easy Solutions.

a un estudio de Moneta Technologies, justamente es el miedo al fraude y a la seguridad o de los escollos para la adopción de esta tecnología en ese país.

Fraudes bancarios son el 80% de los ciberdelitos

En tres años, la Superintendencia de Bancos fraudulenta

LOS FRAUDES 'QUITAN EL SUEÑO' A LA BANCA

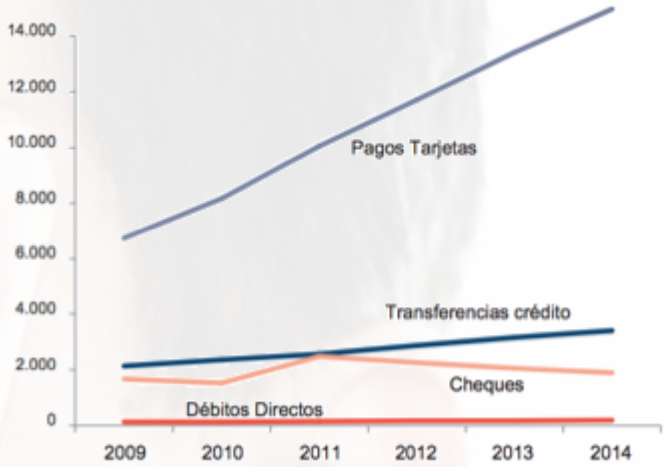
Las pérdidas de las financieras pueden ascender hasta al 30% de sus ingresos; Santander destacó que el delito obstaculiza la adopción de la banca electrónica.

Fraude millonario en Ecuador y Venezuela usó empresas fantasmas en Miami y Weston

Esas, si son malas noticias…

- Comités Ejecutivos
- Consejos de Administración
- Inversionistas
- Alta Dirección

- Cumplimiento
- Riesgos
- Seguridad de la Información
- Negocio



42% of frauds perpetrated by purely internal fraudsters

32% of frauds perpetrated by groups of internal and external fraudsters

25% of frauds perpetrated by external fraudsters

CISO (CHIEF INFORMATION SECURITY OFFICER)

- Seguridad de la información dentro de una organización e implementa las medidas de control necesarias en torno a ésta.
- Concientización de usuarios.
- Análisis de riesgos.
- Administración de seguridad.
- Definición de normas respecto al uso de la información.
- Seguridad física del equipo de cómputo.
- Capacitación y soporte.

EL NUEVO CISO, AHORA ES…!!!

CHIEF INFORMATION RISK OFFICER (*CIRO*)

- Conocimientos en seguridad tradicional (CISSP, CISM, etc.)
- Completo entendimiento y comprensión del negocio (MBA)
- Piensa como Abogado y como un Hacker.
- Líder (cómodo frente a la mesa directiva)
- Entendimiento del principio de la gestión de riesgos
- Habilidades bien conocidas y definidas del **CISO**

SOC

Definición

- Es una central de seguridad informática que previene, monitorea y controla la seguridad de la infraestructura de una organización.

Alcance

- Dotado de servidores, firewalls, sistemas de detección de intrusos, software antivirus y otros sistemas especializados, un SOC monitorea la actividad en las infraestructuras en tiempo real, las 24 horas del día, los 7 días de la semana los 365 días del año. Los datos y eventos obtenidos son analizados y rastreados por expertos certificados en estándares de seguridad.

Objetivo

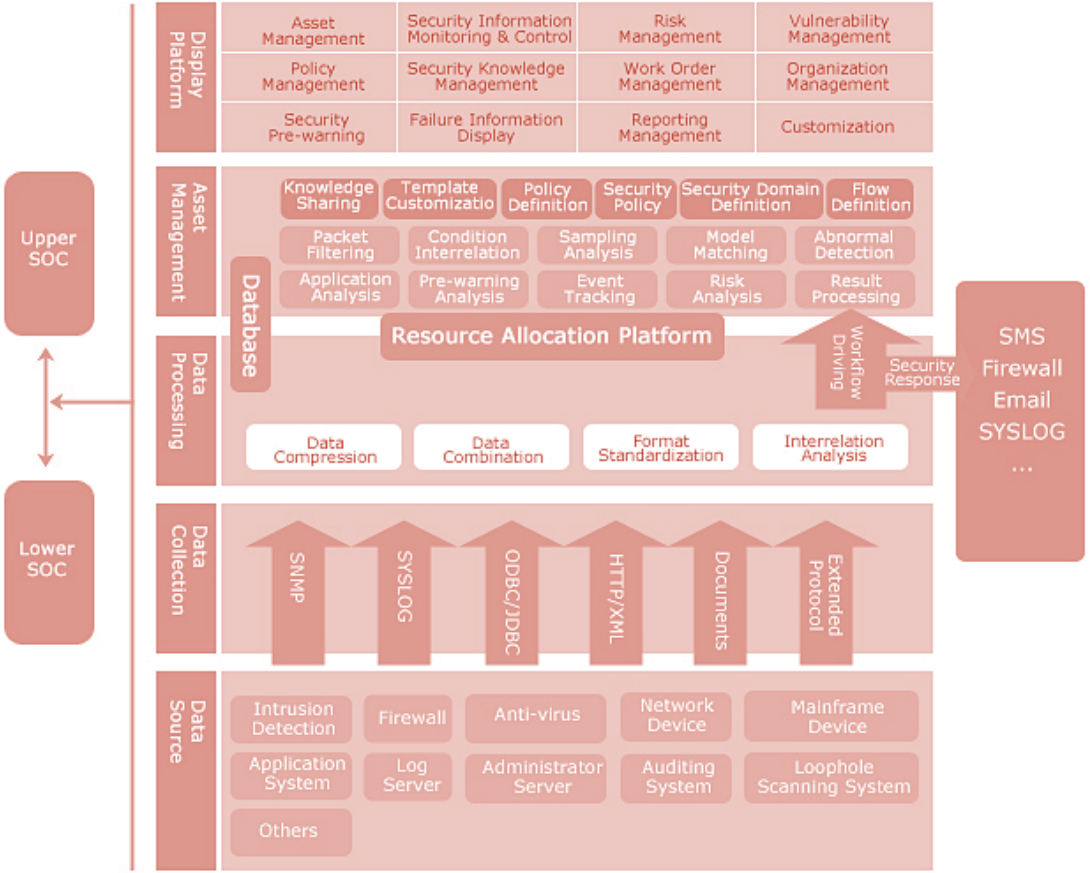
- Los servicios que presta van desde el diagnóstico de vulnerabilidades hasta la recuperación de desastres, pasando por la respuesta a incidentes, neutralización de ataques, programas de prevención, administración de riesgos y alertas de antivirus informáticos.

SECURITY OPERATION CENTER

EL SOC CONVENCIONAL

Security Operation Center (SOC): Modelo

- Fuente de datos
- Colección de datos
- Monitoreo y procesamiento de datos
- Gestión de dispositivos
- Plataforma de monitoreo



NEXT GENERATION

SECURITY OPERATION CENTER

Definición

- Es una central de seguridad informática que previene, monitorea, **automatiza** y controla la seguridad de la infraestructura de una organización.

Alcance

- Dotado de servidores, firewalls, sistemas de detección de intrusos, software antivirus y correlacionadores (SIEM), emplea el mismo alcance del SOC convencional dotando de cierta automatización e inteligencia en el monitoreo y alertamiento.

Objetivo

- El objetivo es el mismo del SOC convencional, agregando la gestión del riesgo, manejo y respuesta a incidentes y automatización a nivel proceso y procedimientos.

NG-SOC/SOC 2.0. Modelo

- Gestión de eventos de seguridad de la información (SIEM)
- Automatización
- Gestión de riesgos
- Manejo y respuesta de incidentes

OSS/SIEM 2.0	PROACTIVE MONITORING	ALERT & NOTIFICATION	EVENT CORRELATION
	Automated Monitoring – SNMP Categorization of Monitored Objects Automated Monitored Object Reporting Integrated to Business Process Automated assignment of Risk Level	Automated Alert and Notification – SNMP Trap / IF-MAP event Alerts categorized based on Risk Level Notifications to Business Process Owner	Contextual correlation of events Situational awareness Mapped to Business Process
AUTOMATION	COMPLIANCE & AUDIT	CHANGE MANAGEMENT	CONFIGURATION MANAGEMENT
	Compliance templates created Compliance enforcement Compliance reporting Compliance violation reporting Auto-Archival Auto-Remediate Auto-Validate	Device change management process Automated approval process Linked to compliance template Change Control Validation Change Management History Log	Configuration Archival Configuration change mapped to change control Configuration Management Database Complete history of archived configuration Configuration Rollback
RISK MANAGEMENT 2.0	RISK RANKING	VULNERABILITY MANAGEMENT	REMEDIAL ACTION ASSIGNMENT
	Alerts/Events and Compliance Results are ranked based on risk level Automated Risk Based Detection Systems Risk based authentication Mapped to Risk Management Framework	Automated Vulnerability Assessment and Audit Vulnerability ID mapped to Risk Level Reference	Automated Owner Assignment Process based on business process / system owner Validate of remedial action completion
INCIDENT HANDLING	INCIDENT RESPONSE	BEHAVIOURAL ANALYSIS	REPORTING
	Network Forensics Investigation and Analysis Evidence Gathering Escalation Management	Network Behavioural Analysis Detection Anomaly Detection Predictive Analysis Business Process Profiling	Reporting based on incident Feedback and Review Process Prosecution / Disciplinary / Litigation

Definición

- Es la unidad dedicada a la generación de inteligencia con base en las fuentes de datos y que de cara al negocio genera información para la toma de decisiones.

Alcance

- Monitoriza las actividades relacionadas con el negocio y genera fuentes de información para dar seguimiento y cumplimiento a políticas como son: conoce a tu cliente, anti-fraude, temas relacionados con lavado de dinero y forense digital, para el manejo de incidentes.

Objetivo

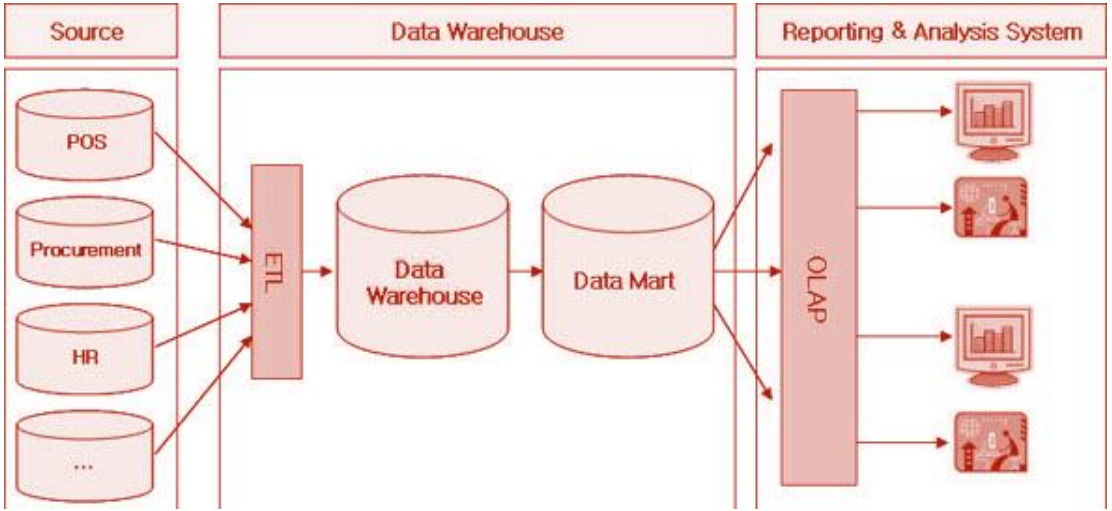
- Monitorear las actividades de las infraestructura y la transaccionalidad de las operaciones tanto tecnológicas como monetarias para la temprana detección de posibles fraudes o incidentes.

UNIDADES DE INTELIGENCIA

BUSINESS INTELLIGENCE

Unidad de Inteligencia. Modelo

- Fuentes de información, en sistemas centrales
- POS/ATM
- Fuentes de información, en sistemas satélites
- Recursos humanos



OSINT

- Inteligencia proveniente de recursos abiertos es decir de información disponible públicamente: medios de comunicación, leyes, presupuestos, declaraciones, dentro de este análisis de información abierta también podrían incluirse los análisis sociológicos, o el perfil psicológico de jefes de estado y de gobierno, análisis grafológicos, etc... este tipo de fuente representa hasta el 85% de la información bruta que recibe un servicio de inteligencia.

Security Intelligence

- Incluye el análisis y recopilación de fuentes de datos, asimismo incluye el monitoreo de actividad de red (NetFlow) el análisis se realiza mediante técnicas de Deep Packet Inspection.

SOC
Modelo S21SEC

CYBER THREAT INTELLIGENCE CENTER

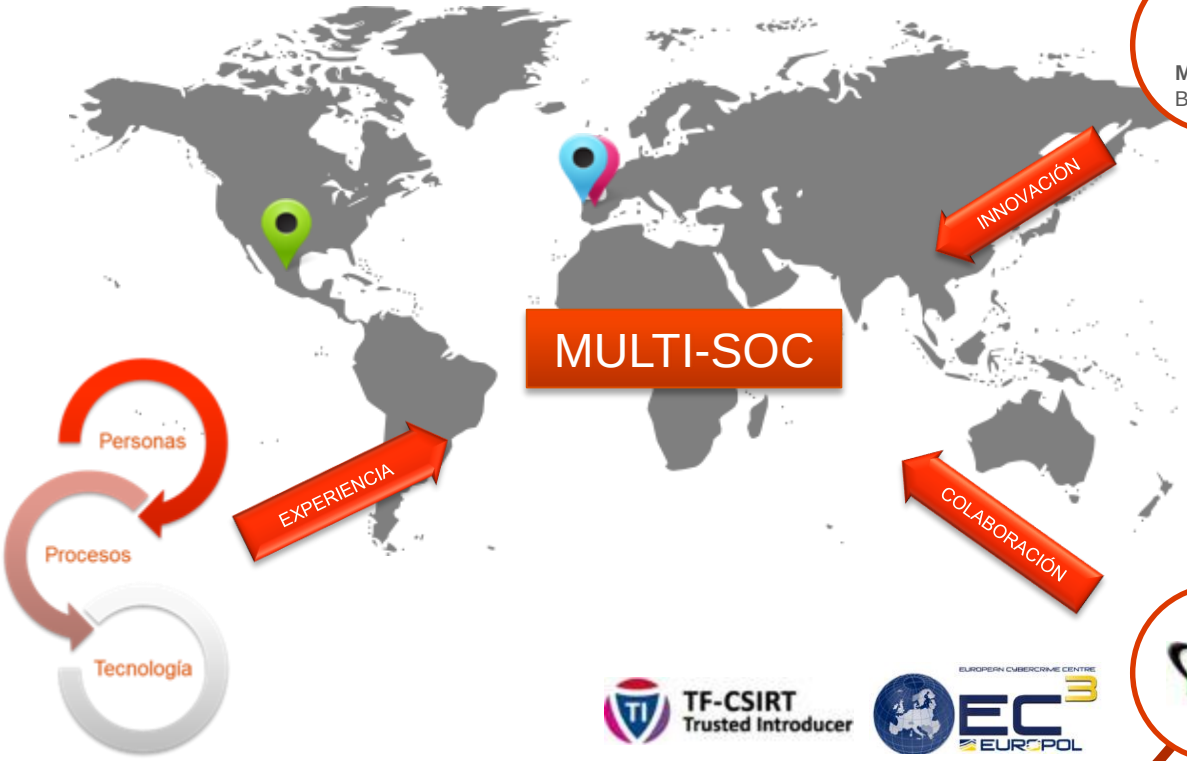
PURE PLAY CYBERSECURITY COMPANY

lookwise™ ENTERPRISE MANAGER EM

lookwise™ DEVICE MANAGER DM

Centro de Operaciones de Seguridad

9 años de experiencia en SOC, más de 5 años como CERT



MINERO
Blackbox

Optimización de Procesos

- Sensor – Algoritmo Propio
- Agilidad en el Triaje

METABoX
Powered by **TIMON**
Threat Intelligence MONitorization

Gestión del Conocimiento

- Experiencia
- Herramientas e Innovación

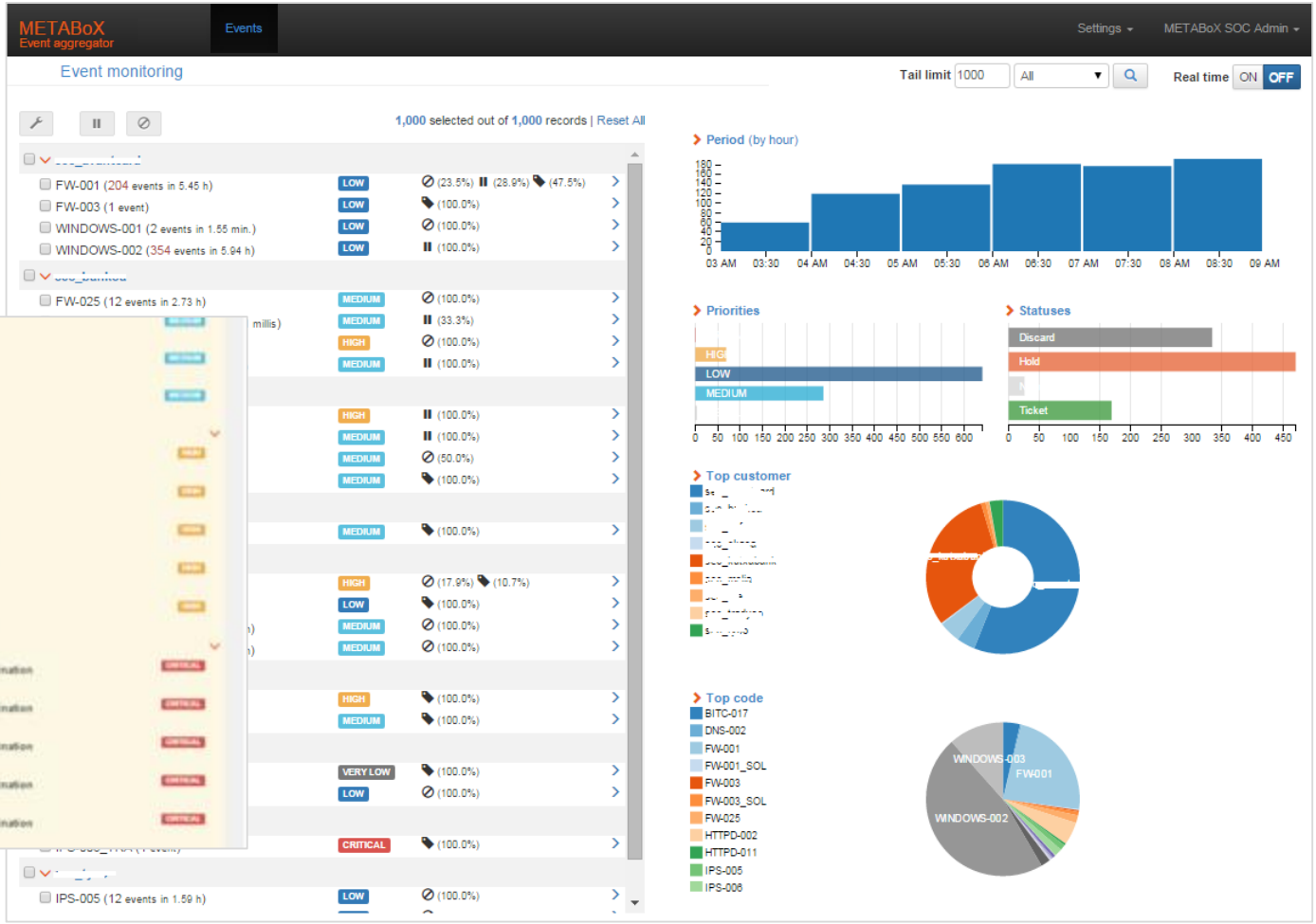
Gestión del Talento

- Atracción del talento
- Desarrollo profesional

Lugar en el Entorno

- CERT
- Colaboración

METABoX
Agregación en tiempo real



S21sec

Referencias en la implementación de SOC

- S21sec tiene la capacidad necesaria para ayudar en los pasos requeridos, que para nosotros son los siguientes:
  1. Consultoría inicial para entender el status quo, establecer objetivos estratégicos, requerimientos técnicos, partes interesadas y definir el plan global.
  2. Plan detallado de diseño e implementación
  3. Seguimiento, control, formación y certificación

- Hemos ayudado a nuestros clientes a implementar su propio SOC
  - Totalmente autosuficientes
  - Compartiendo servicios

AIRBUS

BBVA

renfe

produban

REPSOL

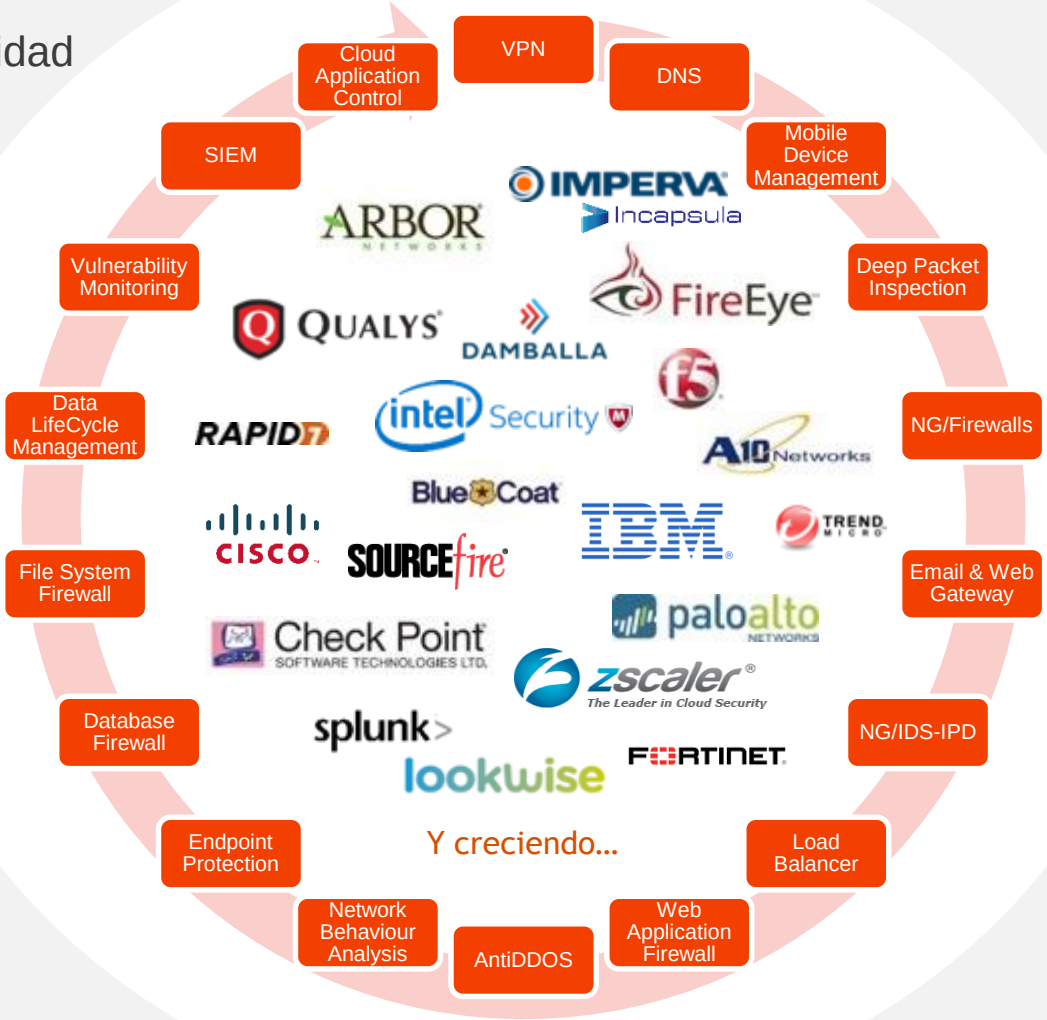
INTECO

CaixaBank

INFOTEC

Centro de Operaciones de Seguridad

Gestión de Dispositivos



- **Amenazas** continúan, cada vez son mas difíciles de controlar, debido a las infraestructuras **complejas** y a los controles débiles que implementados.
- **Tendencia** de las instituciones financieras, están mas enfocadas a servicios tecnológicos.
- Normatividad, Regulaciones y Negocio, el reto: encontrar el **equilibrio** perfecto para dar **cumplimiento**, disminuir los **riesgos** y mantener segura la información.
- BIG Data, a grandes fuentes de información, emplear metodologías que generen **inteligencia** necesaria para hacer frente a los nuevos retos de la seguridad.
- CISO & CIRO, deben contar con el **apoyo** de la **alta dirección** y contar con socios estratégicos en **Ciberseguridad** quien los apoye.
- **CTIC**, primer modelo **MultiSOC** que genera Inteligencia para la **detección, prevención**, reacción y contención de amenazas y riesgo tecnológicos y operativos.

EN CONCLUSION

Medios de Pago y NG-SOC

S21 SEC

Your Cybersecurity Company

Σ21 Advanced Cybersecurity Services

- Web Fraud Protection
- Data Leak Detection
- Advanced Security Feeds
- Malware Analysis
- Cyber Threat Alerts

Σ21 SOC/CERT Services

- Continuous Vulnerability Tracking
- Incident Response Centre
- Security and Event Management
- Security Device Management

Σ21 Advisory

- Auditing & Code Analysis
- Specialized Hacking
- Consulting and Compliance
- Telecom Security
- Industrial Cybersecurity
- Solutions Integration
- Academy

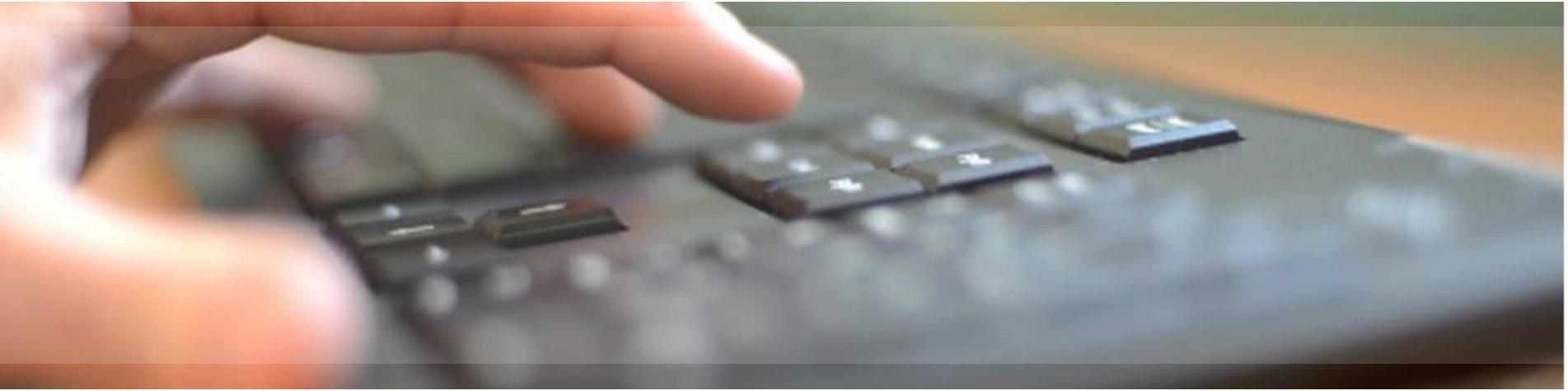
PORTFOLIO ΣSIGMA21

THE AUTHOR

Sabas Casas del Río

VP LATAM

scasas@s21sec.com



linkedin.com/company/s21sec

facebook.com/pages/S21sec

twitter.com/@S21sec

SOCIAL MEDIA

S21 SEC

Your Cybersecurity Company

SPAIN

MADRID
Valgrande, 6
CP 28108
Alcobendas

T: +34 902222521
F: +34 916616679

BARCELONA
C/ Tarragona,141-157
Piso 14
CP 08007

T: +34 902222521
F: +34 936746144

SAN SEBASTIÁN
P.E Zuatzu
Ed. Urgull. 2º
CP 20018

T: +34 902222521
F: +34 916616679

PAMPLONA
P.E La Muga, 11-1
CP 31160
Orcoyen

T: +34 902222521
F: +34 916616679

PORTUGAL

LISBOA
Rua do Virato, 13B, 4º Andar
1050-233
Portugal

T: +351 220107120
F: +351 220107121

PORTO
Lugar do Espido, via norte
4470-177
Maia

T: +351 220107120
F: +351 220107121

MEXICO

MEXICO DF
Zamora 33, 6, Condesa
06140
Condesa. Ciudad de Mexico

T: +52 5533005200

UK

READING
Davison House,
Forbury Square
RG1 3EU

Reading.
UK

OFFICES

S21 SEC
Your Cybersecurity Company

S21SEC

Your Cybersecurity Company

s21sec.com