

Cybersecurity Centre (CCMAD)

IndraMind Cyber and CCMAD collaborate in the
handling and response to cyber incidents in the
Spanish capital



Centro de
Ciberseguridad
Ayuntamiento
de Madrid

What do we know about the cyberattacks that hit Europe's airports?



TIMES OF CYBERCRIME AND CYBER SABOTAGE

In a context of accelerated digitalisation and major geopolitical tensions, **the public sector is one of the main targets of cybercrime**. This statement is backed up by data from the European Union Agency for Cybersecurity (ENISA) which, after analysing more than 2,500 cyberattacks between July 2022 and June 2023, found that **19% of these cyberattacks were directed against public administrations**, making it the most attacked sector.



SECURITY OPERATIONS CENTRE ROOM



CYBER VIRTUOUS CIRCLE

Engineering

define how we
defend ourselves

SOC

Monitor and
defend



Audit

the defences
before the *bad*
guys do

Management: CCMAD

Accountability: Cyber globally

Service: Coordination

Government, strategy and analytics
Dissemination of cyber culture
Institutional relations

Service: Operations

Perimeter security
Identity management
Electronic certification

Department: Compliance

Management and planning Risks
Third-party monitoring
Contracting
ENS, NIS, IICC Compliance
Personal Data compliance
Request management

Department: SOC

Digital surveillance
Detection mechanisms
Log management and correlation
Threat hunting
Incident response
Cyber crisis coordination

Department: Perimeter security

Secure communications
Remote access
Safe browsing

Department: Engineering

Architectures and Technologies
Technical security requirements
Bastion, secure configuration
Security in the life cycle

Department: Technical Audits

Attack surface analysis
Automated vulnerability analysis
Manual audits
RedTeam

- Digital surveillance
- Detection and response
- Continuous threat hunting
- Technology consulting
- Security in the development cycle
- Automated attack surface scanning
- Vulnerability audits
- ICT compliance consulting
- Cyber culture

LOT 1: Comprehensive cybersecurity services

Service 1 Cybersecurity operations

- 1.1 Digital surveillance
- 1.2 Monitoring and detection of security alerts
- 1.3 Response to security incidents
- 1.4 Proactive threat hunting
- 1.5 Forensic analysis
- 1.7 Cyber crisis response
- 1.8 Operation of cybersecurity tools

Service 2 Infrastructure security and development:

- 2.1 Technological consulting
- 2.2 Tests integrated into the development cycle

Service 3 Technical cybersecurity audits:

- 3.1 Automated vulnerability analysis
- 3.2 Manual asset audit

Service 4 Governance and compliance:

- 4.1 Strategic cybersecurity planning
- 4.2 Information on the state of security in Madrid
- 4.3 ICT compliance advice
- 4.4 Advice on GDPR compliance and relevant regulations
- 4.5 Regulatory production
- 4.6 Third-party risk management

Service 5 Cybersecurity culture:

- 5.1 Awareness
- 5.2 Dissemination
- 5.3 Organisation of events



SmartMDR AI-SOC Native

Technology Stack

Centro de Ciberseguridad (CCMAD)

IndraMind Cyber



SMARTCITY
EXPO WORLD CONGRESS



WHY THE TRADITIONAL SOC IS NOT ENOUGH?

Context

- Operational pressure on SOC demands a change in the way of working.
- The traditional model does not scale. Exponential event growth, alert fatigue, and a shortage of analysts.
- There is a need to evolve our SmartMDR platform into a more intelligent, efficient, and autonomous platform.

Motivation

- Respond to modern SOC new challenges: speed, adaptability, precision, and scalability.
- Leverage our proprietary technology to build a differentiated platform based on in-house AI.
- Improve the level of service without increasing operational costs.

Strategic Objective

- SmartMDR as an intelligent, orchestrated, modular, and scalable detection and response solution.
- Natively integrated AI to maximize the value of existing infrastructure and knowledge.
- Drastic reduction in the time required for attention, investigation, and response.

Current challenges

- Growth of unprioritized alerts → fatigue and loss of effectiveness.
- Lack of contextual correlation between sources (SIEM, EDR, NDR, etc.).
- Long investigation times for complex incidents.
- Dependence on static rules and expert knowledge for new TTPs.
- High operational cost compared to limited results.

What does SmartMDR solve?

- Drastic reduction of false positives based on AI and automatic enrichment.
- Dynamic and self-evolving use cases, driven by integrated intelligence.
- Automation of the detection-investigation-response cycle, reducing the average response time.
- Efficient and sustainable model, designed to scale without increasing technical resources.

SmartMDR AI-SOC NATIVE

Sovereign Agentic AI

Substantially improves security incident investigation and resolution, reducing analyst workload and response times (80% efficiencies) and increasing quality with success rates higher than those of human analysts, based on IndraMind's supercomputing capabilities.

Cognitive triage and unified management

Together with the AI analyst, Triage classifies, scores, escalates, and tracks alerts based on criticality, origin, history, and context.

With Detect One, we offer an aggregated and unified view that facilitates the governance of MDR services.

Modular and open architecture

Integration with multiple customer sources and systems (SIEM/xDR technology agnostic), with modular or integrated deployment, whether in sovereign cloud, on-premises, or hybrid.

<10'

SLA critical incident detection

<2%

False positives

+80%

Reduction of low-value alerts

0

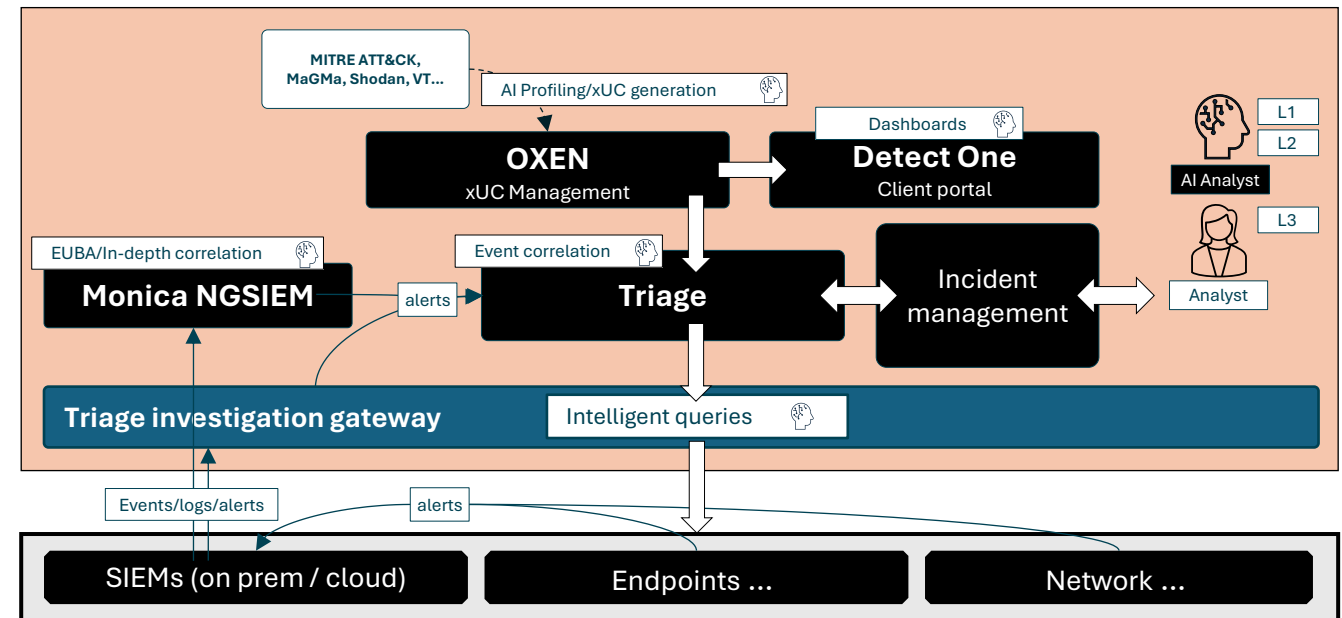
High-impact incidents

Up to 5-times

Improvement in cyber incident investigation and resolution

To address the exponential increase in events, alert fatigue, and analyst shortages...

- A smarter, more autonomous platform.
- Powered by AI and automation.
- Maximum operational effectiveness and efficiency, exploiting its full potential in correlation, detection, and response.



SO... IT WORKS?

Human

Se identifica actividad reportada anteriormente en el incidente [SIA-2729: SIA-CC-SNC-001 \[PFW\] Communications over suspicious ports to internet](#) **CLOSED** donde se verifica que la IP [redacted] es una maquina interna. Se procede a su cierre como Falso Positivo sin impacto.

actualizado: Comentario sobre solución 27 de mayo de 2025, 16:08

Nada → Las IPs [redacted] son máquinas internas nuestras. Falso positivo

Un saludo.

AI

El 14 de octubre de 2025 a las 10:38:19 UTC, se detectó una alerta de **alta severidad** (puntuación de riesgo: 73) en el entorno **CyberArk** de la organización **SIA**, vinculada al uso del usuario crítico [redacted] (IP origen: [redacted]) para recuperar la contraseña del usuario administrativo **SafeOwner** (IP destino: [redacted] máquina **ALC-VAULT**). La acción, clasificada como **'retrieve password'** con motivo **'Show Password'**, se ejecutó con éxito y está asociada al safe **[redacted]** y la política **[redacted]**. Aunque no se detectaron intentos fallidos previos ni actividad sospechosa reciente del usuario [redacted], la alerta coincide con patrones observados en tickets anteriores ([SIA-2997](#), [SIA-3229](#)) donde usuarios administrativos (**[redacted]**) realizaron acciones similares sin validación explícita de legitimidad. La **IP gateway** [redacted] (pública) aparece recurrentemente en eventos legítimos, pero su análisis de reputación no fue solicitado. Dada la **técnica MITRE T1078 (Valid Accounts)** y la falta de confirmación previa para [redacted] se recomienda **notificar al cliente** para validar la legitimidad de la acción y descartar un posible abuso de credenciales privilegiadas.

AI

La alerta analizada corresponde a **12 eventos de tráfico SSH aceptado** desde la IP interna [redacted] (asociada al usuario [redacted] en 10 eventos) hacia la IP [redacted] (geolocalizada en Nagoya, Japón, pero **confirmada como infraestructura interna de SIA** en tickets anteriores). La investigación revela que:

- Todas las conexiones fueron aceptadas por el firewall (reglas **414** y **217**, categoría **unscanned**).
- No hay evidencia de bloqueos ni actividad maliciosa en los últimos 3 días hacia esta IP.
- La IP de destino ([redacted]) tiene reputación **legítima** (VirusTotal: 0/95 malicioso; AbuseIPDB: 0 reportes) y está validada en **5 tickets cerrados como "False positive"** ([SIA-3057](#), [SIA-3021](#), etc.), donde se confirma su pertenencia a servidores internos de SIA.
- El usuario [redacted] pertenece al grupo **SSLVpnRedInterna Radius**, lo que sugiere acceso autorizado.
- Patrón recurrente:** El tráfico SSH hacia este rango de IPs [redacted] es habitual y ha sido previamente validado como legítimo.

Conclusión: La alerta es un **falso positivo** asociado a actividad interna autorizada. Se recomienda **no notificar al cliente** y cerrar el ticket como **Legitimate activity**.

Human

Fecha y hora del primer evento de la alerta(UTC): Oct 14, 2025 @ 12:38:19.000

Usuario que realiza las acciones: [redacted]

Usuario empleado (Cyberark): SafeOwner

Máquina/ruta relacionada: [redacted]

Cyberark Safe: cyberarkpas.audit.safe

Acción/es realizadas: retrieve password

Reason: (Action: Show Password)

Número de eventos: 1

Análisis detallado: Se ha detectado una alerta relacionada con el uso del usuario SafeOwner por parte del usuario ialin en la plataforma de Cyberark con la maquina [redacted]. Se realiza una búsqueda de actividad adicional realizada por el usuario "*" en los últimos 7 días observando únicamente 1 evento adicional donde el usuario empleado es SafeOwner (Maquina: [redacted] Acción: retrieve password). No se detectan eventos adicionales sobre los usuarios empleados en el mismo intervalo de tiempo.

No se detecta alertas recientes (últimos 30 días) del usuario [redacted]

Recomendaciones:

Verificar si se trata de actividad legítima. En caso contrario, se recomienda resetear las credenciales de la cuenta [redacted] y ejecutar un un escaneo con la herramienta EDR/AV en las máquinas involucradas.

YES... IT WORKS!!!



Capital
Digital



MADRID

THANKS!

Centro de Ciberseguridad (CCMAD)

IndraMind Cyber



SMARTCITY
EXPO WORLD CONGRESS

