



TECH-CONSULTING

C I B E R S E G U R I D A D



PROTEGE TU
EMPRESA



GRUPO TECNOLÓGICO
MANTIS



La empresa comenzó su actividad en 2012 bajo la marca Tech-Consulting, posteriormente en 2015 se fundó Grupo Tecnológico Mantis S.L. como amparo de todos los servicios ofrecidos.

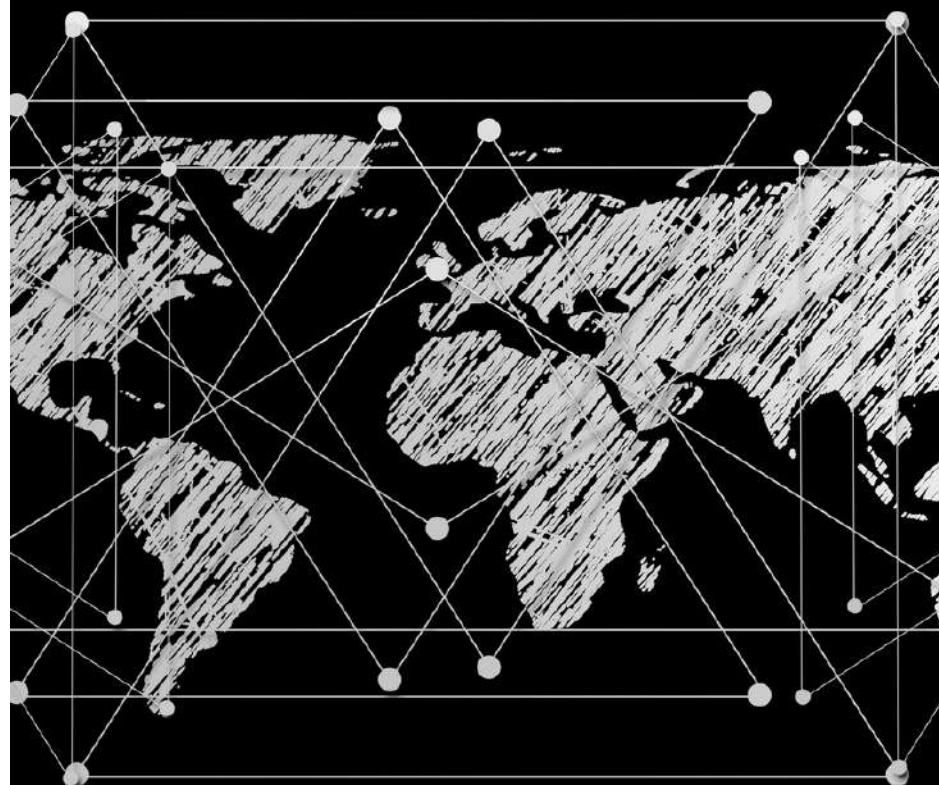
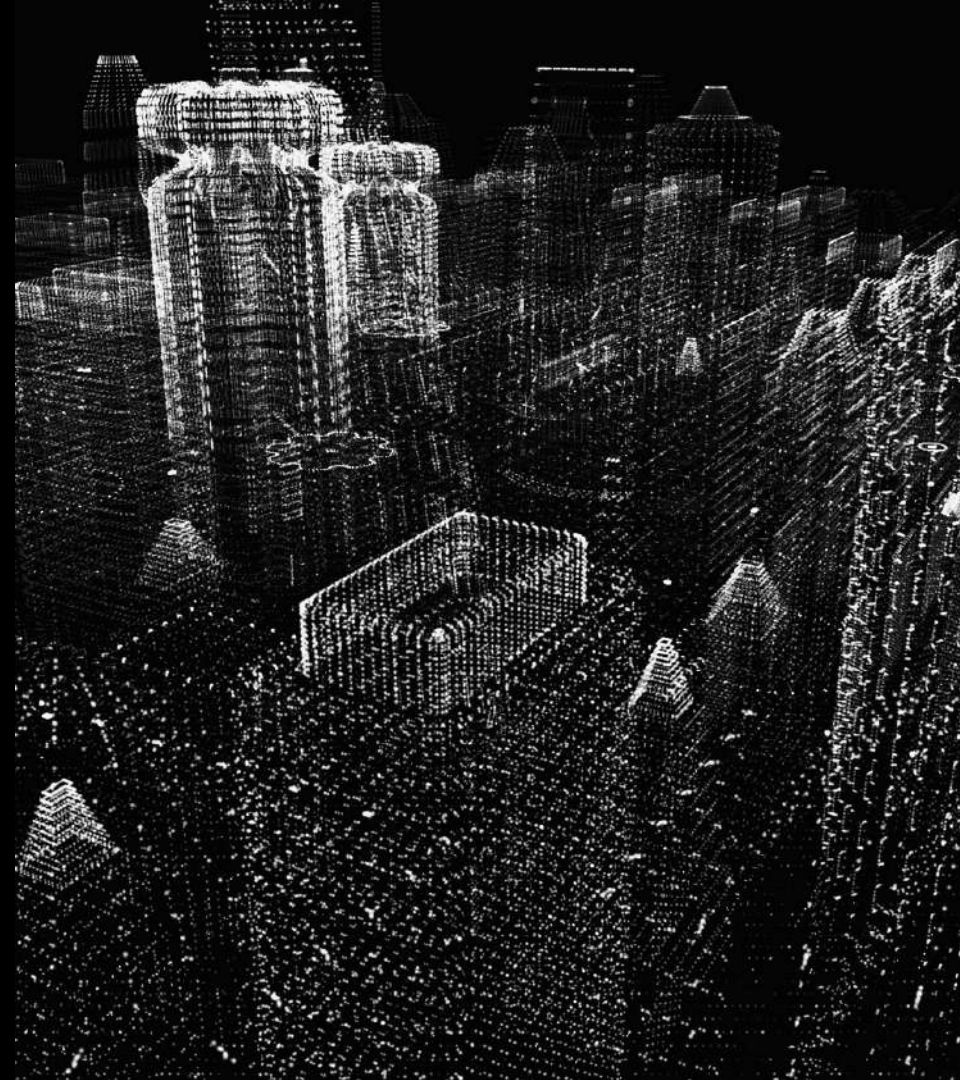
En 2018 se añadió Foortia a la familia y en 2020 Tandem estudio, que finalmente se ha terminado fusionando con Tech-Consulting.

Gracias a nuestros partners contamos con un staff directo e indirecto de más de 400 técnicos especializados.

Trabajamos bajo el amparo de multinacionales integrados en sus equipos.

Descubre Tech-Consulting Design, nuestra rama especializada en diseño web y desarrollo, así como en la creación de identidad corporativa para tu empresa.

+492 CLIENTES
+400 PROFESIONALES
+19 SECTORES
+80 MARCAS Y SOCIOS



**TRABAJAMOS
A NIVEL
INTERNACIONAL**

Defiende, analiza, responde



+



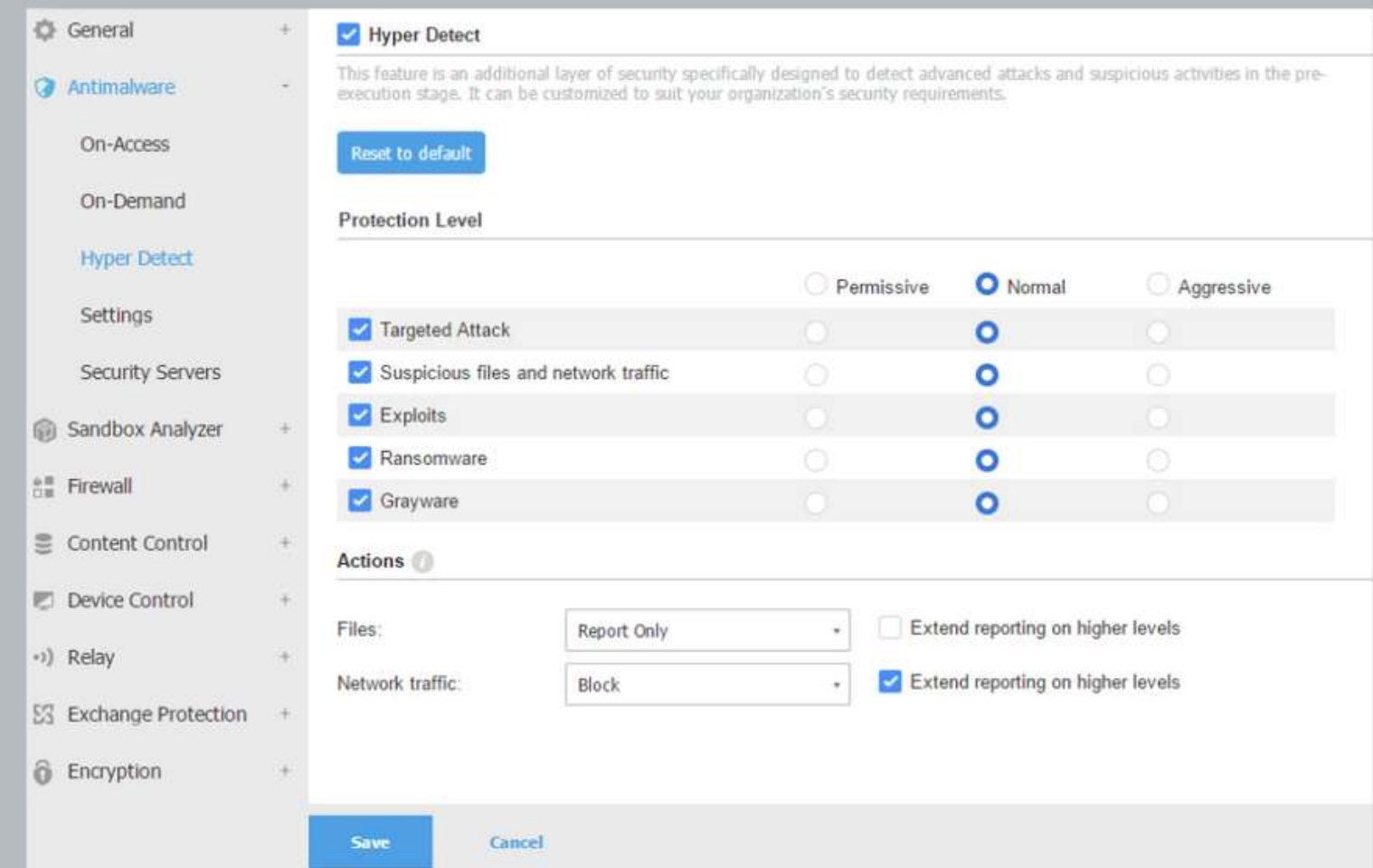
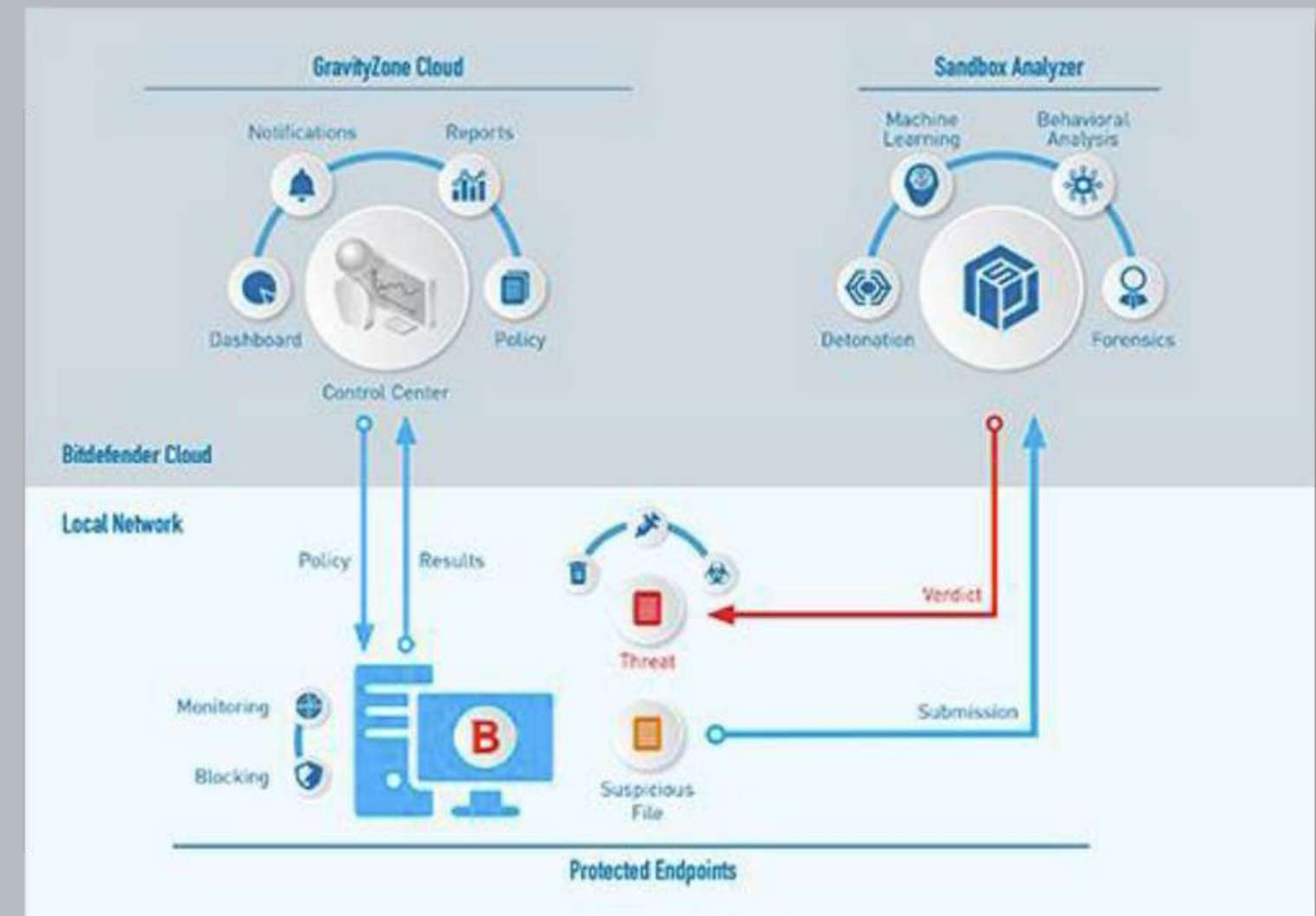
Dos soluciones complementarias e independientes para tu empresa





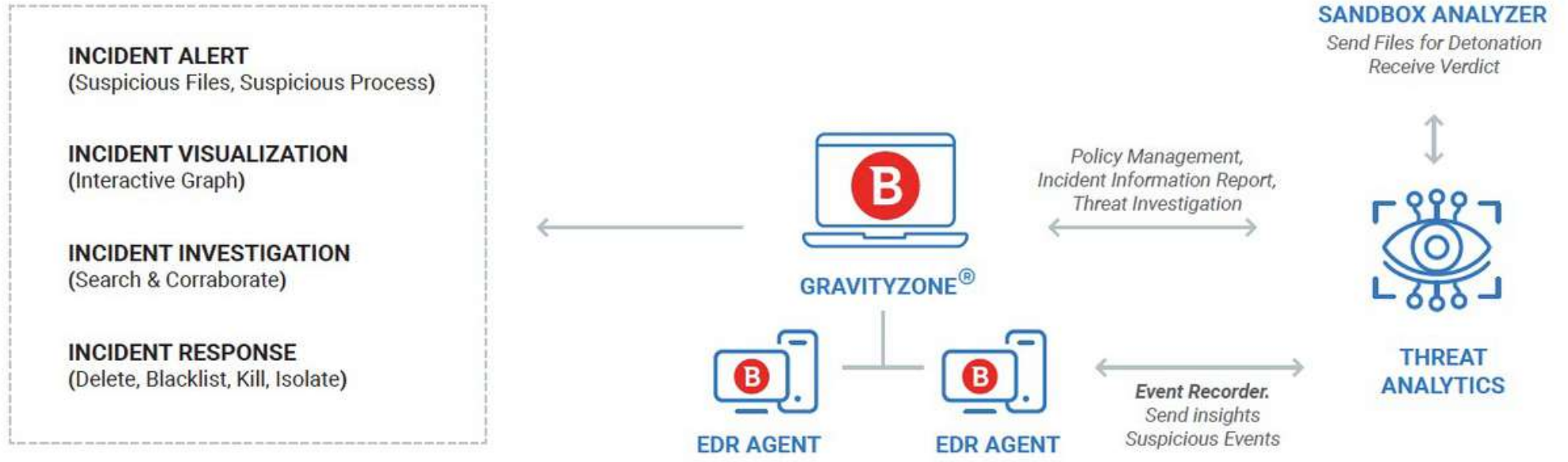
Bitdefender®
GravityZone

Módulos



Funcionamiento

Cómo funciona



Extended Incidents Endpoint Incidents Detected Threats

ID	Date	Status	Severity Score	Priority	Organization Impact	Last Kill Chain Phase
#26	Created at 11:47 on 11 Oct	Open	32	Unassigned	4 1 + 2 other	Exfiltration
#23	Created at 11:47 on 11 Oct	Open	32	Unassigned	4 1 + 2 other	Exfiltration
#21	Created at 11:47 on 11 Oct	Open	32	Unassigned	4 1 + 2 other	Exfiltration
#31	Created at 11:47 on 11 Oct	Open	32	Unassigned	4 1 + 2 other	Exfiltration
#28	Created at 11:47 on 11 Oct	Open	32	Unassigned	4 1 + 2 other	Exfiltration
#24	Created at 14:00 on 31 May	Open	80	Unassigned	1 1 + 13 other	Impact
#20	Created at 14:00 on 31 May	Open	80	Unassigned	1 1 + 13 other	Impact
#32	Created at 14:00 on 31 May	Investigating	80	Medium	1 1 + 13 other	Impact
#29	Created at 14:00 on 31 May	Open	80	Unassigned	1 1 + 13 other	Impact
#17	Created at 16:03 on 4 Oct	Open	58	Unassigned	1 3 + 7 other	Exfiltration

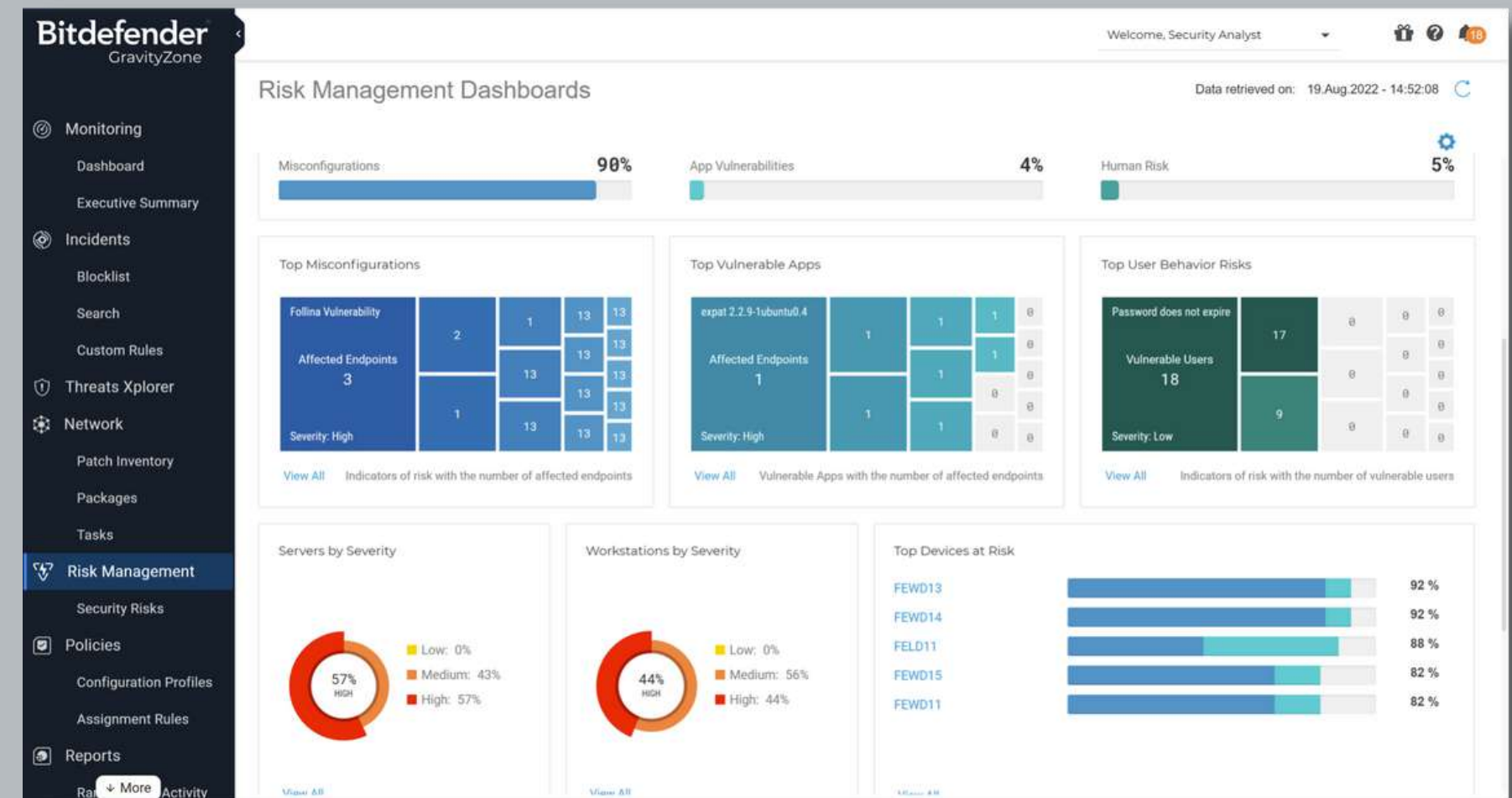
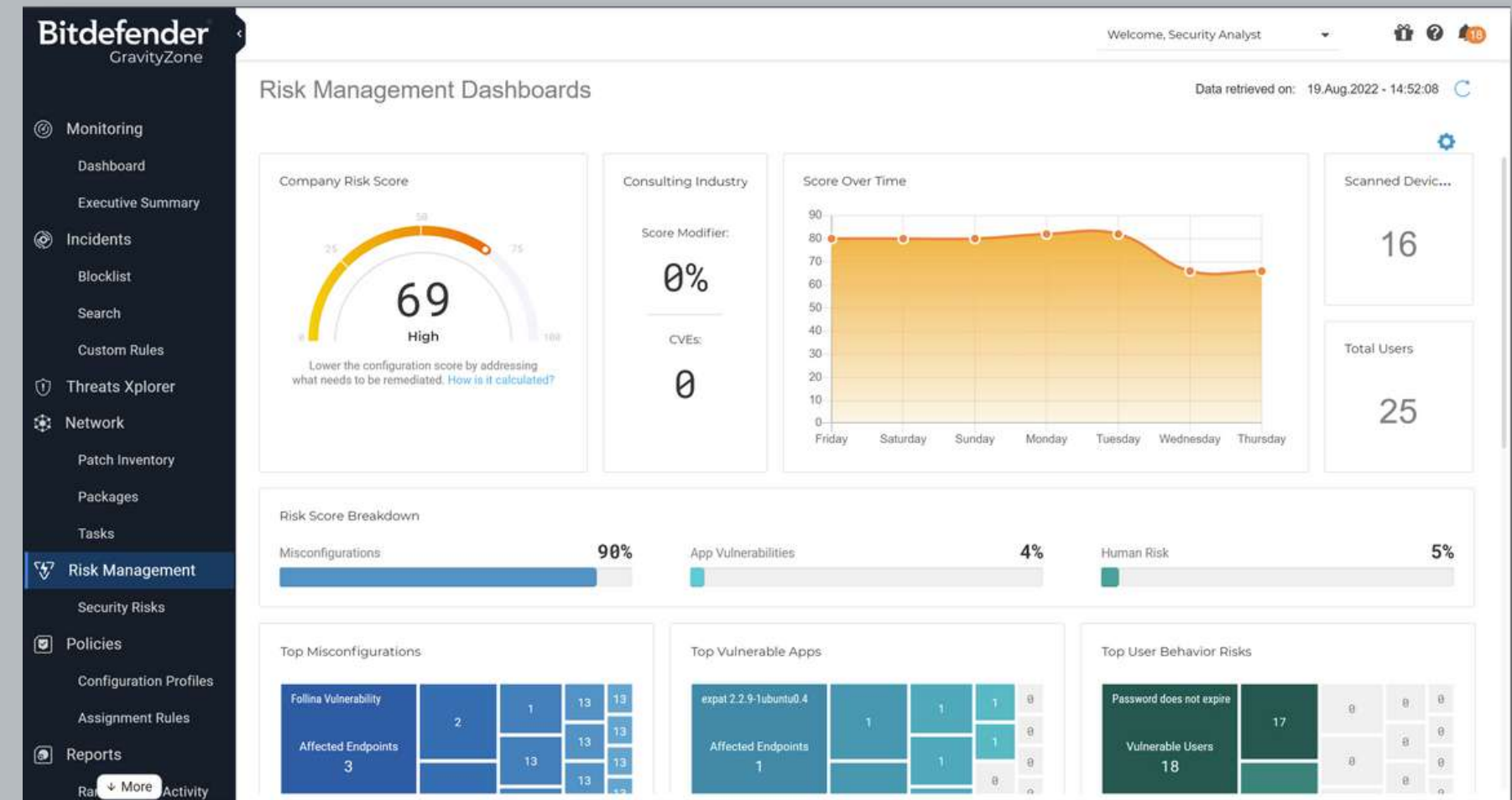
Incidentes



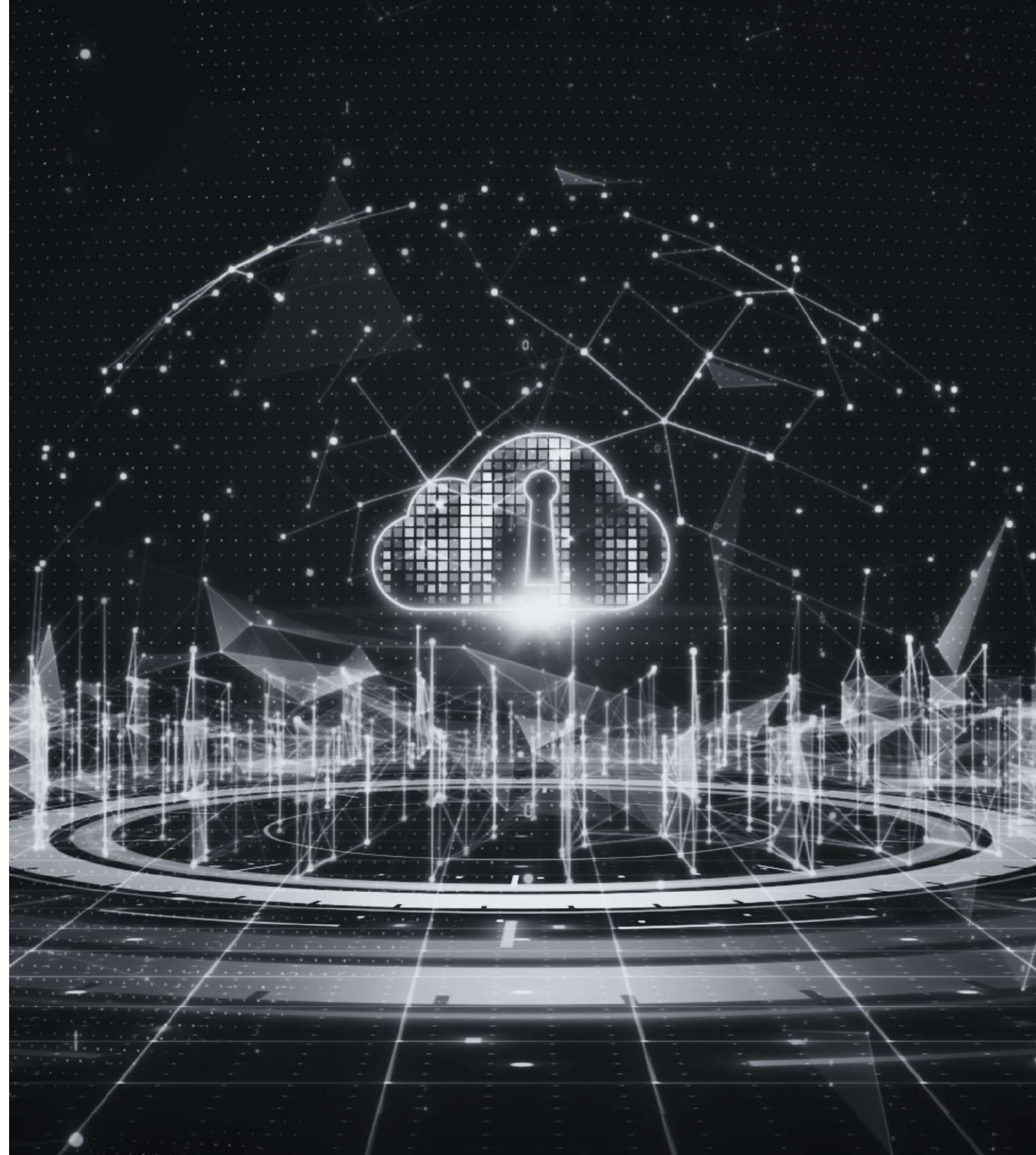
Análisis de riesgos

Análisis de riesgos por los usuarios y en los endpoints.

Analiza continuamente el riesgo de su organización utilizando cientos de factores para identificar, priorizar y brindar orientación sobre cómo mitigar los riesgos de usuarios, red y endpoints.



 **FORESCOUT**[®]



XDR



CENTRALIZACIÓN Y EVALUACIÓN DE INFORMACIÓN

GESTIÓN DE INCIDENTES

RESPUESTA INCIDENTES AUTOMATIZABLE

DETECCIÓN DE ALERTAS REALES



VS



The screenshot shows the ForeScout dashboard with the following sections:

- Entities with Active Detections and No Cases:** Critical (11, Violated SLA), High (8, Violated SLA), Med/Low (50).
- Unacknowledged Cases:** Change Requests (0), Technical Support (4, Violated SLA), Health Incidents (3).
- Offline Connectors:** 1.
- Log Ingestion Rates by Source (For the Last 24 Hours):**

LOG SOURCE	EVENTS	EPS TREND
Aws Cloudtrail	100.11k	4.3% ▼
Azure Active Directory v2.0	97	0%
Carbon Black Cloud	0	0%
Cisco Meraki	0	0%
CrowdStrike EDR	0	0%
CrowdStrike Falcon Data Replicator	0	0%
Customer Defined Json	0	0%
Cybermdx Mdefend	0	0%
Cysiv Command	12.79k	0.3% ▼
Loggify Format Logs	0	0%
Cysiv Sensor	21.58k	71.9% ▲
ForeScout CyberMDX	0	0%
ForeScout eyeInspect Command Center	22	340% ▲
ForeScout Eyesight	24.87k	131.1% ▲
Generic Syslog	0	0%
- Top 5 Active Detections (For the Last 24 Hours):**
 - 1. CY-DR-0151: Forescout eyeInspect: Successful Blacklisted Credential Usage Detected (100% ▲)
 - 1. CY-DR-0154: Forescout eyeInspect: OT Security: Man In The Middle Attack Detected (100% ▲)
- Enriched Logs (For the Last 24 Hours):** Line graph showing log volume over time. Summary: Last 24 Hours, Events: 2.11m, Max EPS: 48.00, Avg EPS: 24.39.
- Indicators and Detections Triggered (For the Last 24 Hours):**

XDR



Soporte para más de 170 fuentes de datos.

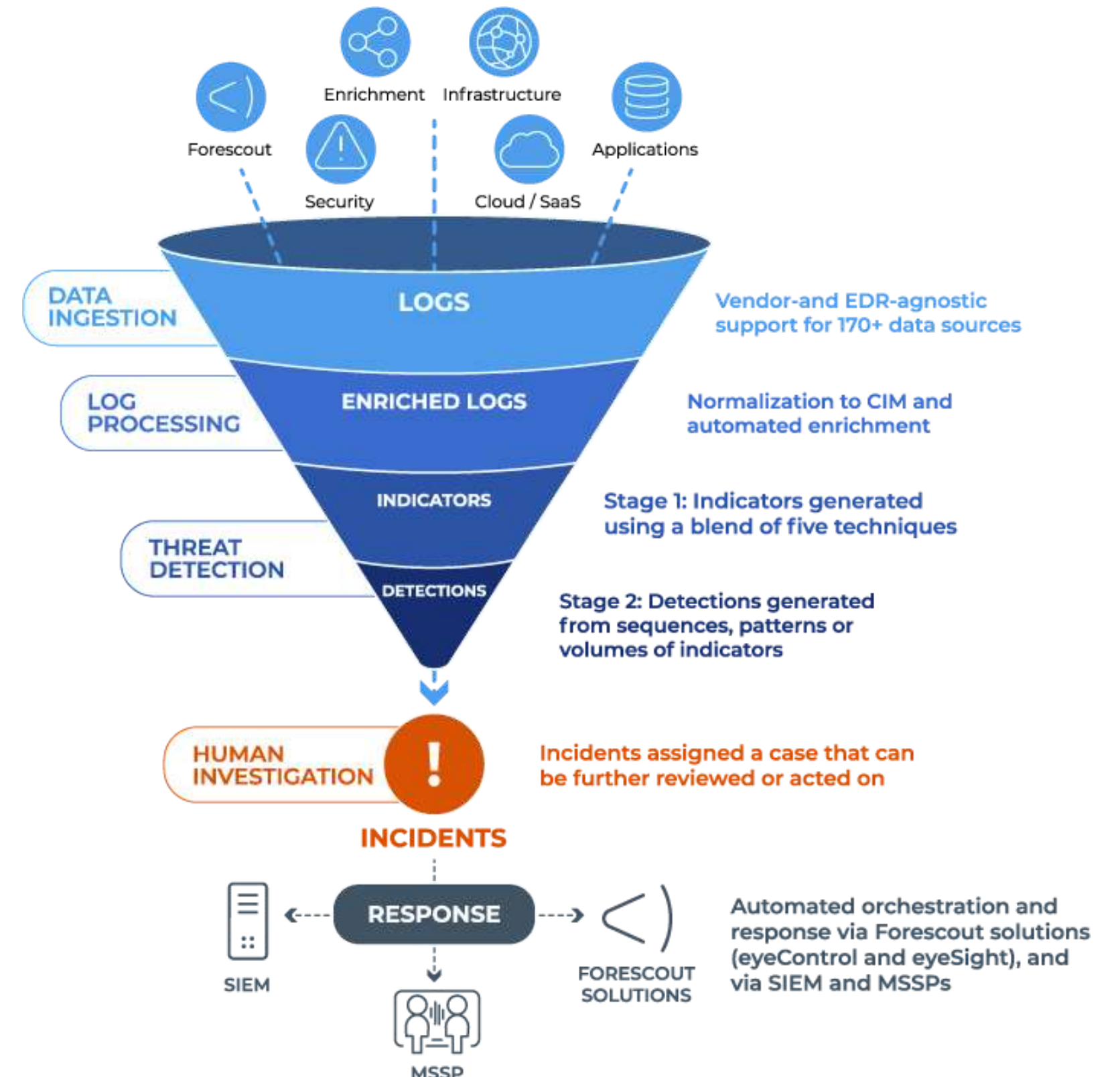
La estandarización (CIM), junto con datos enriquecidos, garantizan un análisis de datos y detección de amenazas más rápida, eficiente y estable.

Etapa 1: los indicadores de una amenaza se generan utilizando una combinación de técnicas (inteligencia cibernética, firmas y TTP, UEBA, estadísticas y valores atípicos, AI/ML sensible al contexto), y se asocian con un dispositivo o usuario.

Etapa 2: Las detecciones son amenazas probables que se generan a partir de secuencias, patrones o volúmenes de indicadores que se considera que ahora justifican la investigación humana.

Los incidentes son detecciones que han sido investigadas por un analista y marcadas como amenazas reales.

Analizados los incidentes, se pueden reenviar a un SIEM o MSSP. Además de tener una respuesta automática a través de soluciones ForeScout EyeControl y eyeSight.

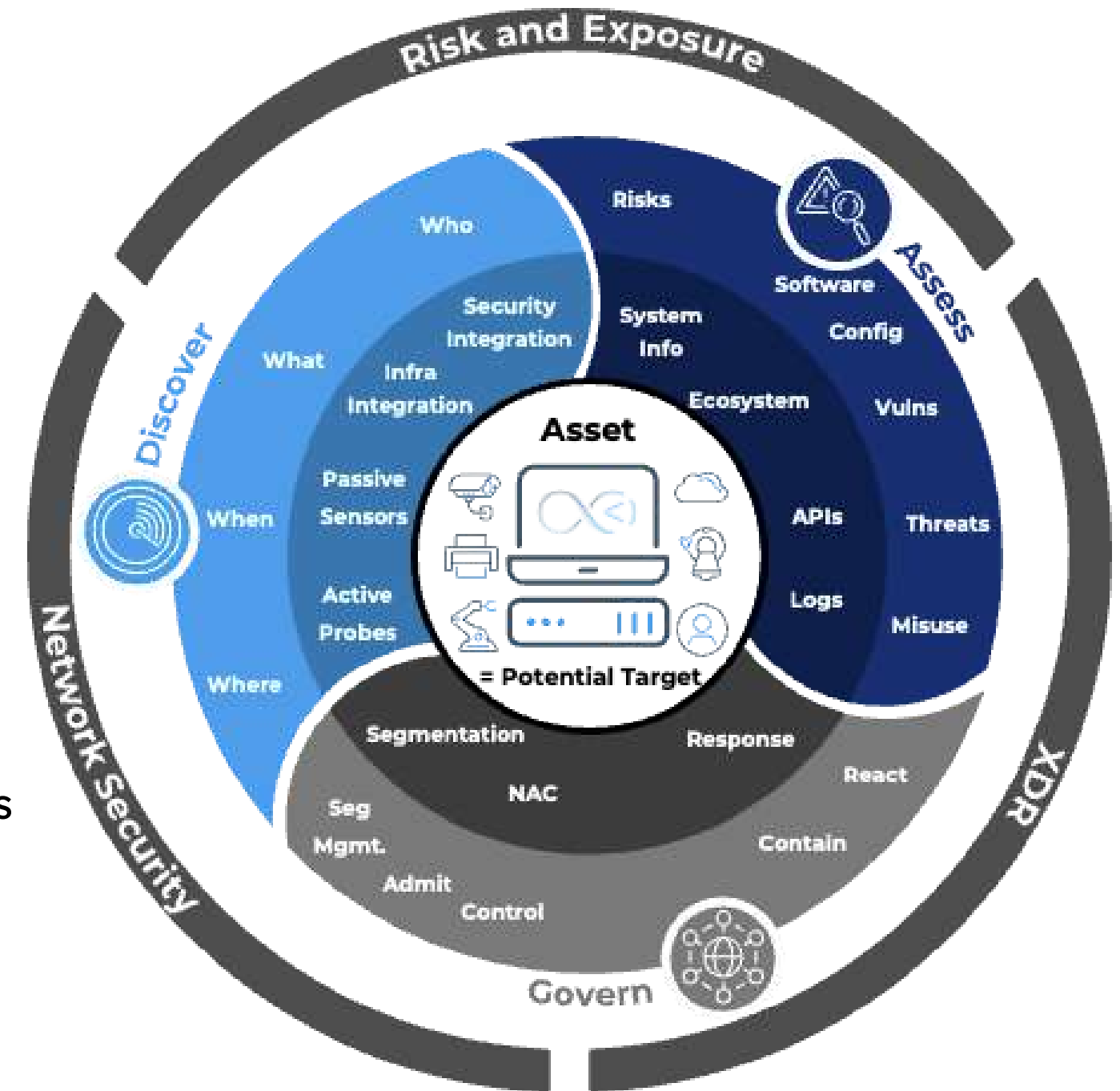


XDR



CIBERDEFENSA AVANZADA PARA EL ENTORNO INDUSTRIAL.

- Application Abuse
- Brute-force Attacks
- Buffer Overflow attacks
- Cloud Resources Scanning
- Cloud Service Misconfigurations
- Cloud: Unauthorized Access
- Cloud: Unsecure Storage Detection
- Command & Control Connection
- Compliance Violations
- Cross Site Scripting
- Crypto-Jacking
- Data Exfiltration
- File Access Failures
- Illegal Resource Access
- Insider Threats
- Lateral Movement
- Malware / Outbreaks
- Network Scanning
- Password Cracking
- Phishing Attacks
- Port and Vulnerability Scans
- Ransomware
- SQL Injection
- Suspicious Behavior
- Unauthorized Access to Systems
- Unauthorized Changes To Firewall Rules
- Unauthorized Service Restarts
- Unauthorized Service/Process Creation
- Vulnerability Exploitation
- Web Application Misconfiguration
- Web-Application Attacks (All Layer-7 web attacks)
- Worm / Virus Outbreak



ESQUEMA

Defiende, analiza, responde



+



Dos soluciones complementarias e independientes para tu empresa



¡GRACIAS!




GRUPO TECNOLÓGICO
MANTIS

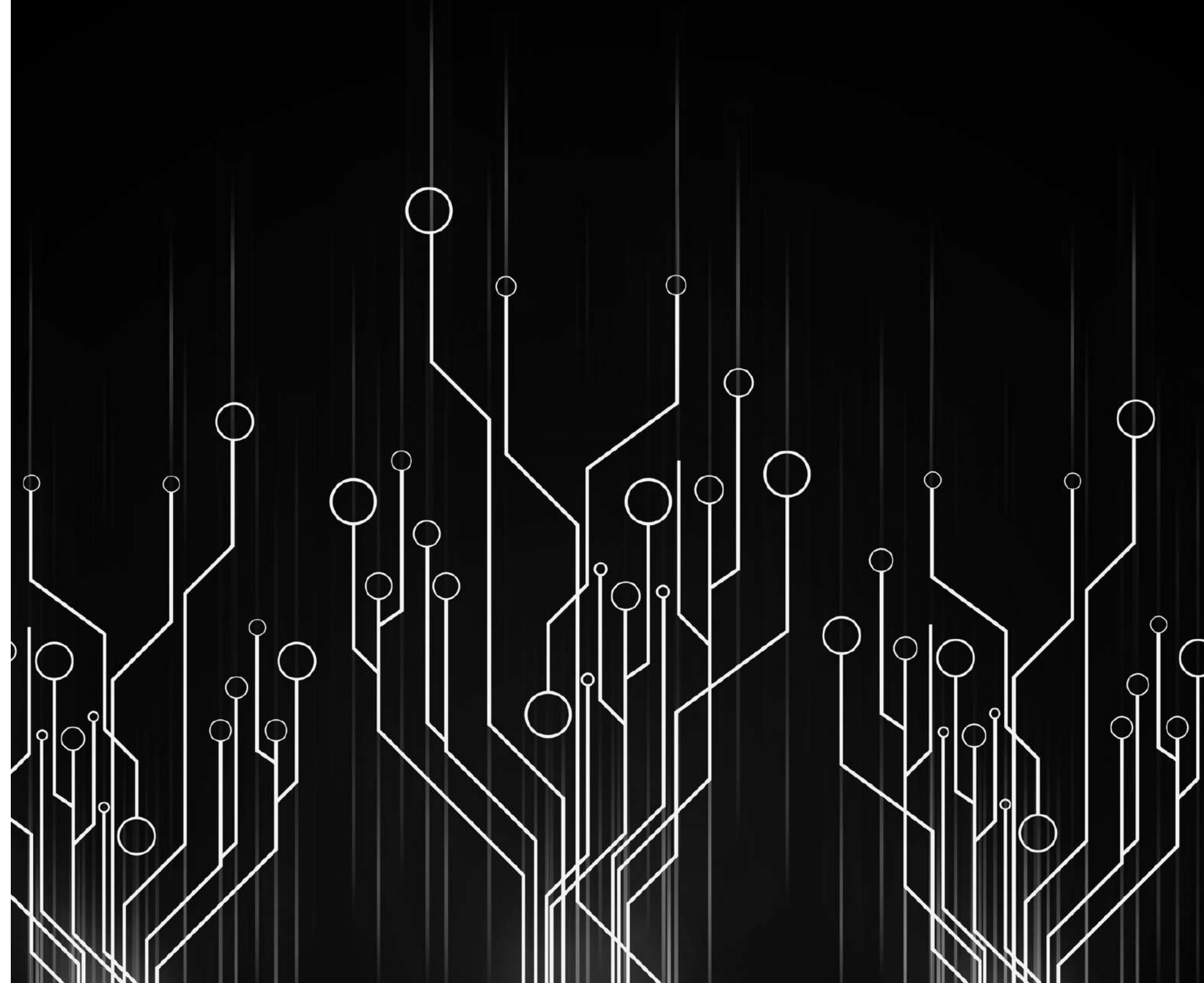


 +34 968 95 83 98

 info@techconsulting.es
r.ortin@techconsulting.es

 Calle Zaplana, 11 - Entlo. Yecla (Murcia)

W W W . G R U P O T E C N O L O G I C O M A N T I S . E S





TECH-CONSULTING

W W W . T E C H C O N S U L T I N G . E S