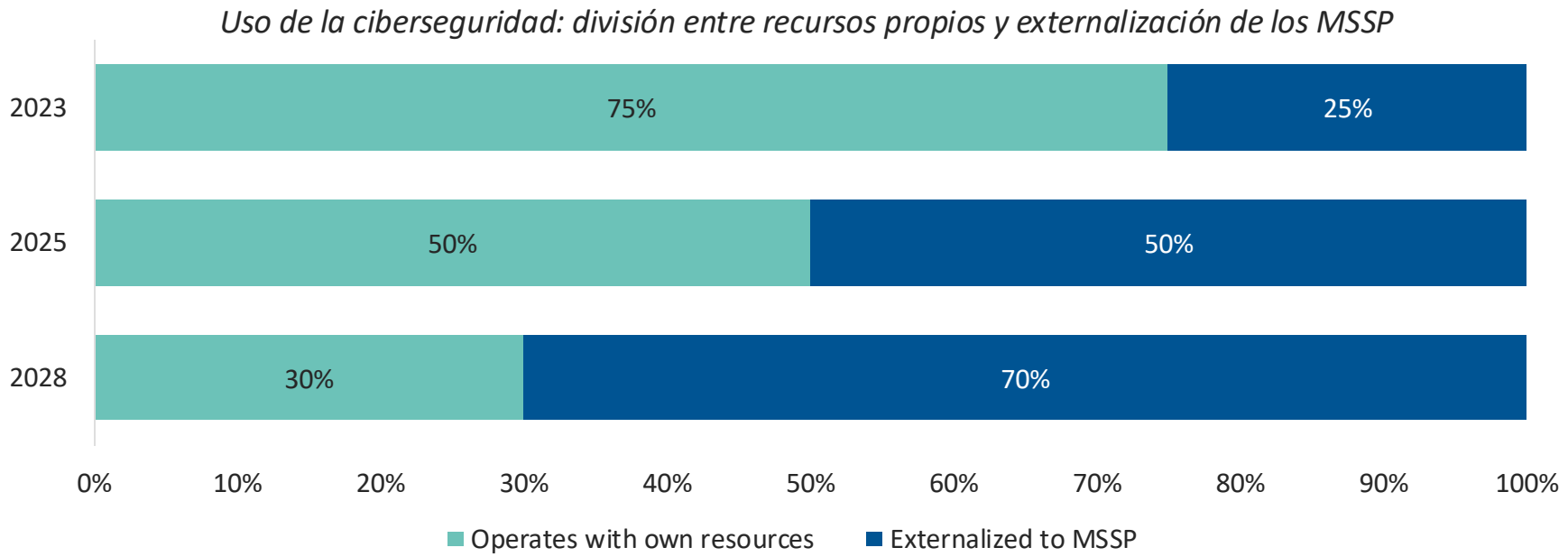
Invisible-bits

Ciberseguridad hacia la externalización de los MSSP



- Para 2025, el 50% de las empresas externalizarán operaciones de ciberseguridad a proveedores de servicios de seguridad gestionados (MSSP

Gartner

- **La ciberseguridad se está externalizando a proveedores de servicios de seguridad gestionados (MSSP) debido a:**
  - Gran complejidad operativa
  - Necesidad de contratar numerosos especialistas, costosos y difíciles de encontrar
  - Dificultad para justificar los costes operativos internos: gran impacto en la cuenta de resultados del negocio
  - Esto impide que el negocio de MSSP/MDR escale y tenga márgenes de beneficio muy bajos

Mercado altamente complejo:
El desastre de la ciberseguridad según Gartner

Customer 1

FIREWALLS | ENPOINTS | ACTIVE DIRECTORY | PUBLIC CLOUD | WORDLOAD

Infrastructure 1

splunk> SIEM & SOAR

Customer 2

FIREWALLS | ENPOINTS | AZURE AD | PUBLIC CLOUD | VIRTUALIZATION

Infrastructure 2

Microsoft Sentinel SIEM & SOAR

Customer (n)

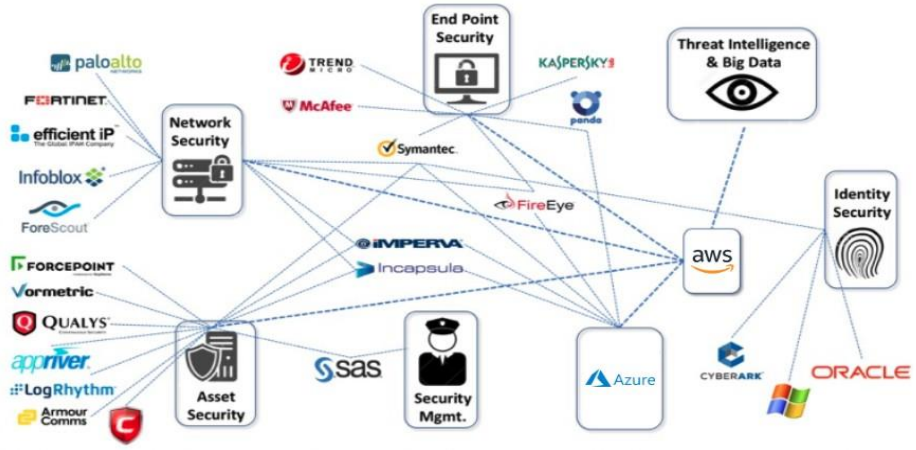
FIREWALLS | ENPOINTS | ACTIVE DIRECTORY | NETWORK | VIRTUALIZATION

Infrastructure (n)

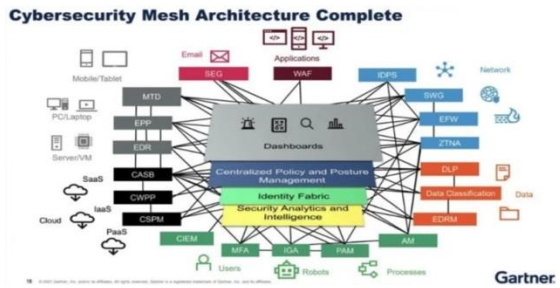
LogRhythm SIEM & SOAR

- Falta de visibilidad y operaciones multicliente
- Requiere operaciones manuales repetitivas de nivel 1 y 2 por cliente
- Requiere numerosos expertos en diferentes proveedores de ciberseguridad
- Los análisis e investigaciones deben ejecutarse en diferentes SIEM
- Las reglas de detección deben codificarse con diferentes formatos en diferentes SIEM
- Se deben crear manuales de mitigación para cada cliente

MSSP Security Operations Center



- Bajo beneficio debido a la baja eficiencia y operaciones no escalables en escenarios complejos de múltiples clientes



Históricamente, el mercado se ha caracterizado por una alta complejidad, lo que ha provocado que las empresas tengan baja escalabilidad y reduzcan sus beneficios. Esta tendencia del mercado es lo que Gartner denomina el "desastre de la ciberseguridad".

Los XDR dirigidos tanto a MSSPS como a usuarios finales

XDR players

XDR focus on MSSPs as final users

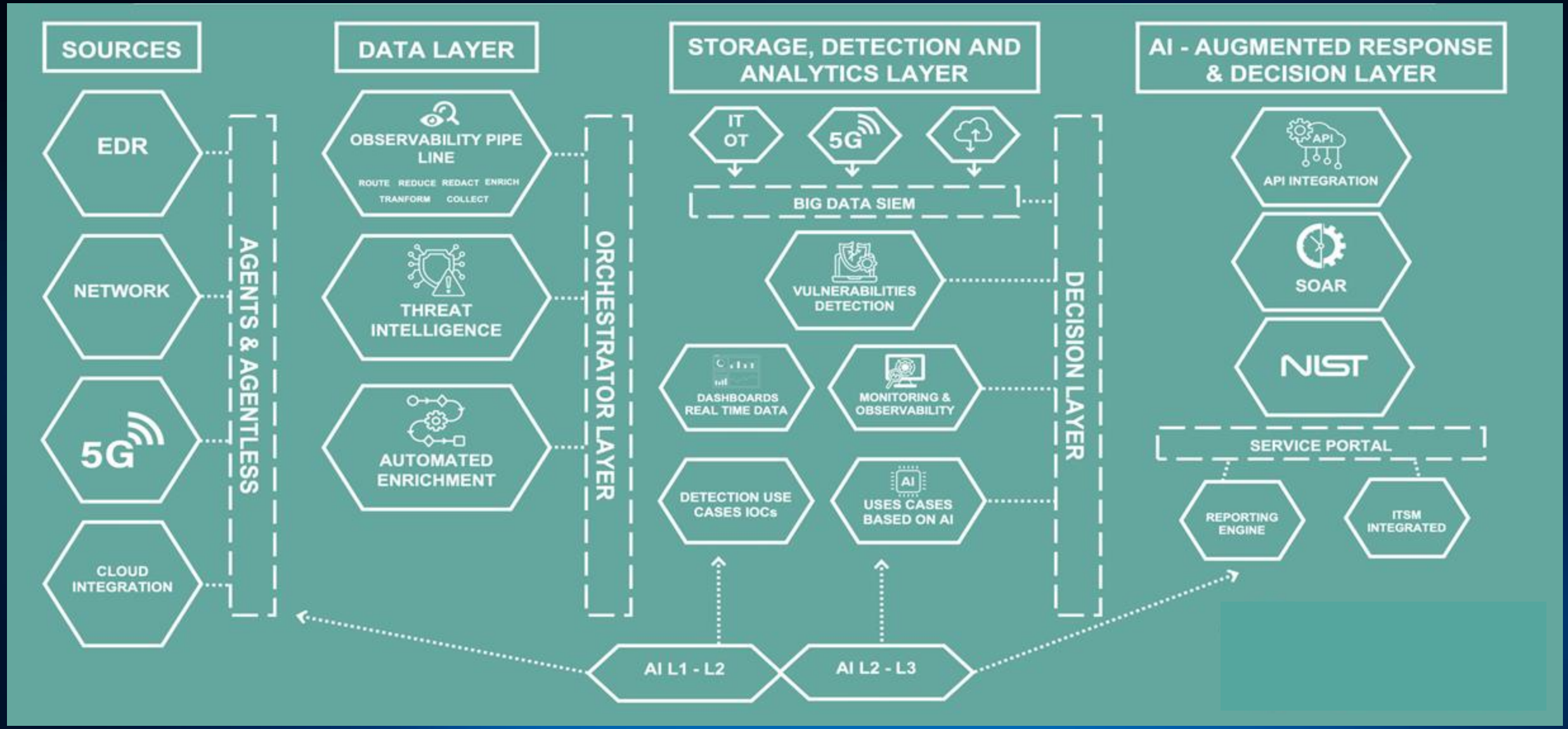
- Muchas soluciones XDR están diseñadas para ser escalables y aptas para su implementación por parte de los MSSP, con el fin de mejorar sus capacidades de prestación de servicios de seguridad gestionada a múltiples clientes.
- En este contexto, los proveedores de XDR pueden adaptar sus ofertas a las necesidades y requisitos específicos de los MSSP, lo que les permite gestionar y responder eficazmente a incidentes de seguridad en múltiples organizaciones. Este enfoque colaborativo ayuda a ampliar las capacidades avanzadas de detección y respuesta ante amenazas a una gama más amplia de clientes a través del modelo MSSP.

AGSAMA CYBERSECURITY

XDR focus on end-users

- Las empresas que desarrollan y ofrecen soluciones XDR también están dirigiendo su atención a organizaciones o negocios individuales que serán los consumidores finales de sus servicios de seguridad.
- En este contexto, las soluciones XDR están diseñadas para dotar a los usuarios finales de capacidades avanzadas de ciberseguridad.
- Estas soluciones buscan proporcionar un enfoque integral de la seguridad, permitiendo a las organizaciones defenderse mejor contra ciberamenazas sofisticadas.

cybereason · CROWDSTRIKE · RAPID7 · RELIAQUEST · SentinelOne · STELLAR CYBER · TEHTRIS FACE THE UNPREDICTABLE · Trellix


SOURCES
DATA LAYER
STORAGE, DETECTION AND ANALYTICS LAYER
AI - AUGMENTED RESPONSE & DECISION LAYER
EDR
NETWORK
5G
CLOUD INTEGRATION
AGENTS & AGENTLESS
OBSERVABILITY PIPE LINE
ROUTE REDUCE REDACT ENRICH
TRANFORM COLLECT
THREAT INTELLIGENCE
AUTOMATED ENRICHMENT
ORCHESTRATOR LAYER
IT
OT
5G
BIG DATA SIEM
VULNERABILITIES DETECTION
DASHBOARDS REAL TIME DATA
MONITORING & OBSERVABILITY
DETECTION USE CASES IOCs
AI
USES CASES BASED ON AI
DECISION LAYER
API
API INTEGRATION
SOAR
NIST
SERVICE PORTAL
REPORTING ENGINE
ITSM INTEGRATED
AI L1 - L2
AI L2 - L3

LA TECNOLOGIA
Multi-tenant MDR SOC Platform

5G Integration

Enrichment and classification

Service Portal

Threat Intelligence

Integration Framework

Compliance Controls enrichment

IT –Iot

API Integration Services

Data Lake SIEM

Reporting Engine

Observability

Archiving

Integration

Predictive AI

Dashboards generator

Detection rules engine

Hybrid environments abstraction

1st layer
Customers data sources

- Check Point Firewall
- FortiGate
- Blue Coat
- Google Cloud
- DeepSight
- Microsoft
- McAfee ePO
- Azure
- aws
- IMPERVA SecureSphere WAF
- zscaler
- paloalto networks AutoFocus

2nd layer
SIEMs

Option 1
Integration through currently SIEMs in place

- LogRhythm
- ArcSight
- splunk>
- McAfee Enterprise Security Manager
- QRadar

Option 2
Direct integration. No third party SIEM required

3rd layer
Sources abstraction

Activity Abstraction

- Ingestion & Processing
- Enrichment
- Detection Use Cases

SOC Unified management

Multi-tenant operations Interface

Data Lake
Integrations
Deployments
Investigation
Cases management
Dashboarding
Reporting
Alerting
Threat Intelligence
AI
SOAR

Invisible Bits MDR Platform