Threat Monitoring & Response

by Evolutio

Threat Monitoring & response **by Evolutio**

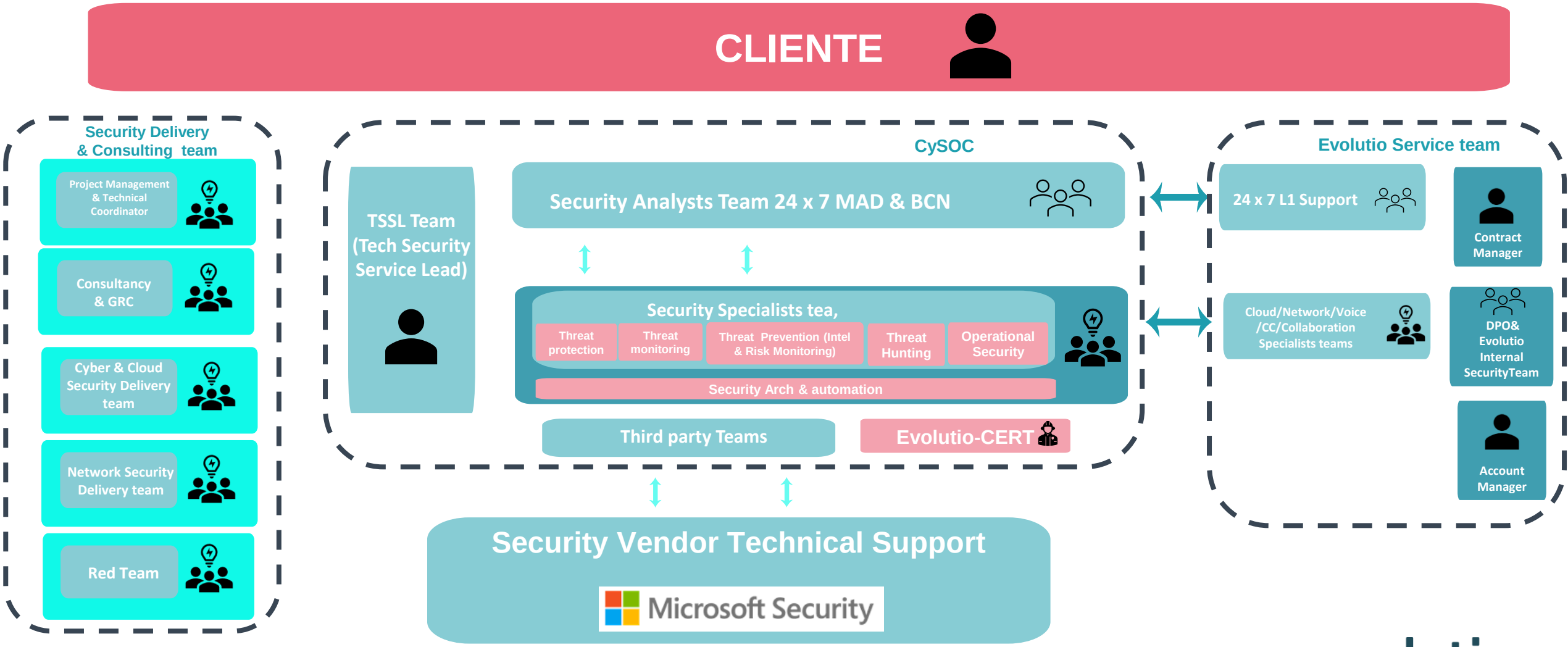
#Secure_route2cloud_

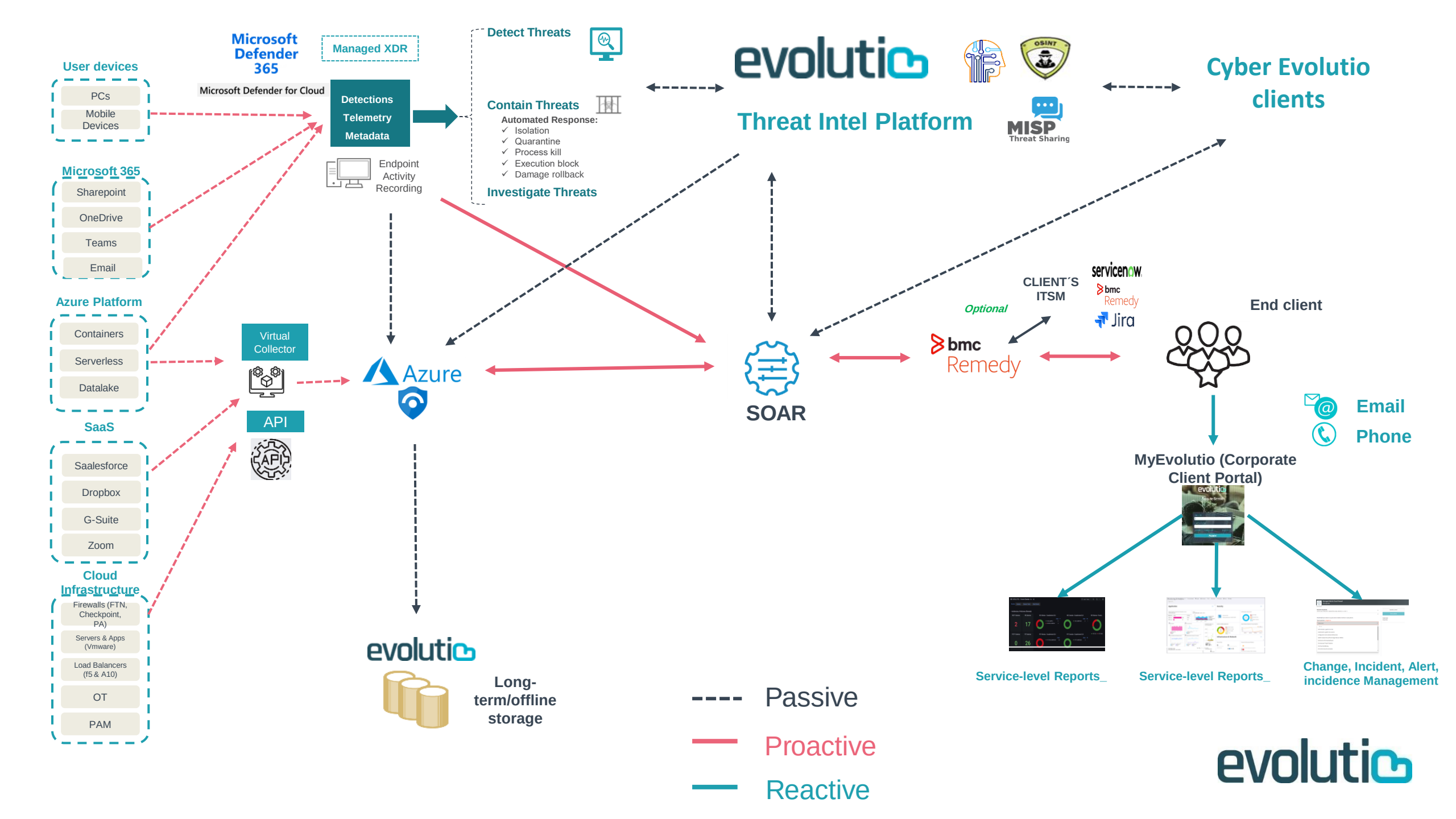
The Threat landscape to which any organisation is exposed requires the support of a strong, experienced & specialized Cyber team to react & respond accordingly

Based on our Cybersecurity capabilities & powered by a leading technology such as Microsoft Sentinel & Microsoft 365 defender, Evolutio offers a complete Threat Monitoring & Response service, fueled/enriched with Response, orchestration & Threat Hunting services under the name **Threat Monitoring & response by Evolutio**.

Depending on the level of maturity, Evolutio offers different service bundles to fit Customers needs

Cybersecurity Service Model




User devices
PCs
Mobile Devices
Microsoft 365
Sharepoint
OneDrive
Teams
Email
Azure Platform
Containers
Serverless
Datalake
SaaS
Saalesforce
Dropbox
G-Suite
Zoom
Cloud Infrastructure
Firewalls (FTN, Checkpoint, PA)
Servers & Apps (Vmware)
Load Balancers (f5 & A10)
OT
PAM
Microsoft Defender 365
Managed XDR
Microsoft Defender for Cloud
Detections
Telemetry
Metadata
Endpoint Activity Recording
Detect Threats
Contain Threats
Automated Response:
✓ Isolation
✓ Quarantine
✓ Process kill
✓ Execution block
✓ Damage rollback
Investigate Threats
Virtual Collector
API
Azure
evolutio
Long-term/offline storage
evolutio
Threat Intel Platform
OSINT
MISP Threat Sharing
Cyber Evolutio clients
SOAR
Optional
CLIENT´S ITSM
servicenow
bmc Remedy
Jira
bmc Remedy
End client
Email
Phone
MyEvolutio (Corporate Client Portal)
Service-level Reports_
Service-level Reports_
Change, Incident, Alert, incidence Management
Passive
Proactive
Reactive
evolutio

Services Bundles: Managed Threat Monitoring (Microsoft Azure Sentinel)

Included | Excluded | Add-on Service

DESCRIPTION	SILVER	GOLD
Posture Risk Assessment	✗	✓
Source coverage map	✓	✓
Cyber use case (deployment & activation)	INCLUDED (A)	INCLUDED (Personalized Use cases) (B)
Non-native standard & intermmediate complex sources integration	OPTIONAL (C)	OPTIONAL (C)
Complex sources integration	OPTIONAL (D)	OPTIONAL (D)
Communication protocol adapted to Advanced Threat Monitoring	✓	✓
Event volumen & collection monitoring	✓	✓
Security alert, Threat & incident Monitoring, triage & análisis	✓ (24x7)	✓ (24x7)
Continual review of existing use cases	MONTHLY (E)	MONTHLY (E)
Service reports	MONTHLY (F)	MONTHLY (F)
Client actionable information based on alert analysis	✓	✓
Evolutio Threat Intel & SOAR capability	✓	✓
Technical Service Security lead nominated & recurrent follow-up Service meeting	MONTHLY	MONTHLY
General Service demands	INCLUDED (G)	INCLUDED (G)
Log retention & storage policy	3 m. online + 12 m. offline (For analysis purposes)	3 m. online + 12 m. offline (For analysis purposes)
Offline log Management & storage	OPCIONAL	OPCIONAL
Threat Intel Feed Export	✗	✓

Portfolio Protección de endpoint y otros vectores

Managed Endpoint Protection (EPP)

- ✓ 7x24 Monitorización y detección
- ✓ Optimización de reglas y políticas de seguridad
- ✓ Notificación de alertas críticas y detecciones/bloqueos realizados
- ✓ Gestión de consultas y cambios
- ✓ Gestión de incidencias de servicio
- ✓ Informes mensuales de nivel de servicio

Managed EDR-XDR + Threat Hunting

- ✓ Servicio Managed EDR
- ✓ Threat Hunting:
  - ✓ Servicio proactivo y dinámico
  - ✓ Basado en la telemetría del EDR y Threat Intel de Evolutio
  - ✓ Basado en hipótesis e indicios de inteligencia
  - ✓ Feedback y enriquecimiento del EDR
  - ✓ Informe mensual con hallazgos

Managed EDR

- ✓ Capacidades de monitorización, detección y respuesta a incidentes de seguridad
- ✓ 7x24 Monitorización, detección y contención
- ✓ Optimización de reglas y políticas de seguridad
- ✓ Notificación de alertas y detecciones/bloqueos realizados
- ✓ Gestión de consultas y catálogo de cambios del servicio
- ✓ Informes periódicos de servicio
- ✓ Informes sobre investigaciones de amenazas e informes post incidentes

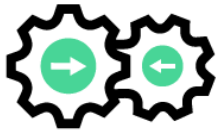
evolutio

Why is Evolutio a trusted & reliable partner to face up to these challenges?

#Secure_route2cloud_

Experience in continuous Threat Monitoring Use case Development

Orchestration & response capabilities



Holistic Threat Intel approach

Mature & specialized Security teams

Cloud & Security inherent approach

Mitre Attack Alignment

MITRE ATT&CK™