TATA COMMUNICATIONS

TATA COMMUNICATIONS CYBER THREAT DETECTION AND RESPONSE

Rapid onboarding, faster detection, better threat response

The threat surface is ever-expanding, with multiple entry points available to threat actors. As a result, traditional threat management techniques are inadequate. According to the latest report, the average time to detect and contain a breach is 277 days[1]. Additionally, setting up an internal SOC can be time-consuming, taking months or even years to get the security expertise in-house, procure necessary tools and platforms, and implement it enterprise-wide with continuous maintenance. Lack of threat visibility due to siloed security tools and technologies across hybrid environments further leads to tool sprawl. According to a global study, large organisations must deal with an average of 75 to 100 security tools daily[2]. The increasing volume of log data and alert storms overwhelms the security teams, diverting attention and resources from strategic projects. The dearth of cybersecurity skills and their associated consequences still need to be addressed.

Key highlights:

- **Improved agility** with rapid onboarding in **2 weeks**
- **Elimination of blind spots** with Netflow integrated cyber threat intelligence and MITRE ATT&CK aligned threat hunting
- **Advanced threat detection** with **900+ SIEM use cases**
- **Operational efficiency** with over **99% reduction in MTTT** and MTTR through native SOAR
- **Comprehensive threat visibility** across hybrid environment with TC^X
- **Flexible** SOC services on-premises (captive), remote or hybrid

Tata Communications solution

Tata Communications' **Managed Detection and Response** (MDR) provides automated threat detection and response to identify and isolate cyber threats across the IT, OT and IoT infrastructure. Our market-leading platform leverages complex correlation rules and behaviour pattern analysis to analyse network, endpoint, user and other security logs. The ingested telemetry data, combined with context from the security infrastructure and enriched with commercial and proprietary threat intelligence and research, helps prevent zero-day threats and improves the mean time to detect and respond (the MTTD and MTTR).

Key components of Tata Communications MDR

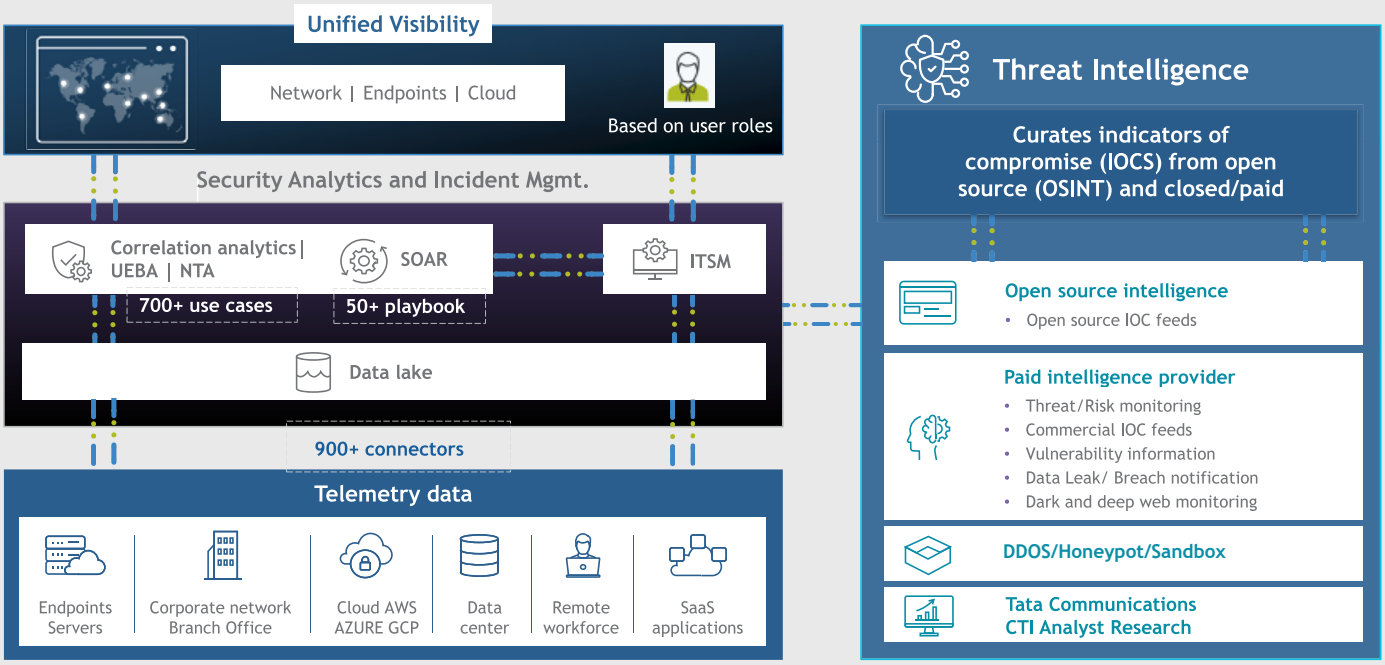


Figure 1

Components

Benefits

Components	Benefits
Security Analytics	Faster detection of threats with engineered SIEM use cases and risk profiling for assets supplemented with machine learning and analytics for detecting sophisticated attacks
User Behaviour Analytics	Enhanced visibility and efficiency in detecting malicious threats with In-built, rule-based User Behaviour Analysis to automatically identify and prioritise anomalous user behaviour
Threat Intelligence	Accurate threat detection and response with indigenous cyber threat intelligence system that contextualises feeds from 65+ sources, provides advisories and enriches log data
Security Automation and Orchestration	Automated threat response and remediation with 60+ engineered playbooks, reducing threat propagation and improving response time

TATA COMMUNICATIONS

TATA

Components

Benefits

Components	Benefits
Threat Visibility	A single pane of glass to visualise security posture, ticket status, and SLA tracking with native customer portal TCX dashboards
MITRE ATT&CK Support	Out-of-box support for MITRE ATT&CK to identify and address the threat actors' tactics, techniques, and procedures (TTP)
Data Retention	Meet compliance requirements and carry out historical log analysis for one year

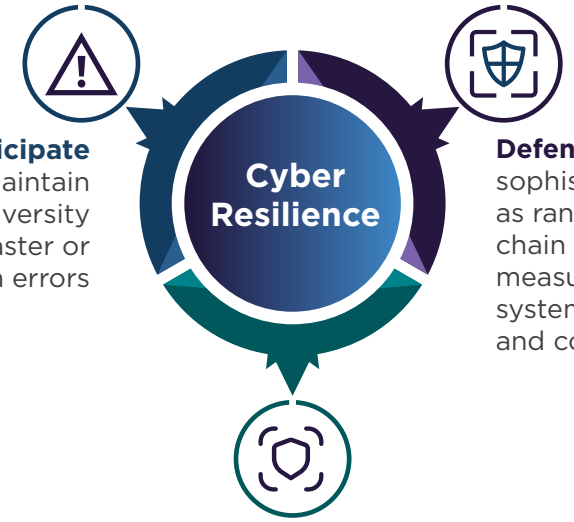
On-demand premium services further support the growing security needs of agile businesses.

- User Entity Behavioural Analytics (UEBA)
- Log-based threat hunting (manual and advanced)
- Brand protection including dark web monitoring and executive monitoring
- 'Red team' and 'Grey team' exercises
- Endpoint, network and identity threat detection and response

TATA COMMUNICATIONS

The Tata Communications Edge

Our MDR Solution is at the forefront of our cyber resilience initiatives for customers. Based on our IP, technology partnerships, and over a decade's experience in safeguarding global clients, Tata Communications Anticipate Defend Respond (ADR) methodology helps ensure proactive protection as well as business continuity in case of a cyber attack.



Anticipate
threats and maintain preparedness for adversity from natural disaster or human errors

Defend
sophisticated threats such as ransomware, APTs, supply chain attacks with robust measures and prevent system penetration and compromise

Respond
and restore critical systems rapidly to minimise business disruption

Platform

Integrated platform built on the NIST and SAFe Framework including SIEM, cyber threat intelligence, SOAR, and network analytics platform

Scalability

Enterprise grade MDR with 14 Billion events screened for threats daily

Interoperability

950+ Out of the box integration connectors

Business assurance

99.99% service availability with 24*7 Global SOC and Redundant Delivery Centers

Compliance

Adherence to industry mandates like NIST, PCI-DSS, CSA, HIPAA, SOC1 Type II, SOC2 Type II, SOC3 Type II, etc

Security expertise

Industry certified cyber security professionals

TATA COMMUNICATIONS

TATA

Solution tailored to meet your security requirements

Type	MDR service elements	Essentials	Premium	Elite
Core/MDR	Log collection, processing	Yes	Yes	Yes
	Retention (3m Online / 9m Offline)	Yes	Yes	Yes
	SOC Services (24 x 7)	Yes	Yes	Yes
	SLA Platform	99.9%	99.9%	99.9%
	Standard use cases	Yes	Yes	Yes
	CTI Standard (customised advisories)	Yes	Yes	Yes
	OOTB 3 custom parser (Non-API)	Yes	Yes	Yes
	3 SOAR Workflows	Yes	Yes	Yes
	Threat hunting (IOC based retro hunting with quarterly report)	Yes	Yes	Yes
MDR	HA – Data collectors (except public cloud)	+	Yes (1x HA license)	Yes (1x HA license)
Service add-on	Integrated EDR/XDR	+	+	+
Service add-on	ASM with risk scoring	+	+	+
Service add-on	Breach attack simulation	+	+	+
Service add-on	DFIR(Per year)	+	50hrs	100hrs
Service add-on	CTI Advanced (dark web, brand monitoring, take down)	+	+	+
Service add-on	Custom – threat intel, vulnerability tool / Report integration	+	Yes	Yes
Service add-on	ITSM e-Bonding	+	+	Yes
Threat hunting	Advanced threat hunting (hypothesis, Situational)	+	+	Yes
Service add-on	Custom parsers (API)	+	+	+
Service add-on	NDR	+	+	+

TATA COMMUNICATIONS

TATA

Experience Advanced Threat Protection

Demo

Stay up to date on latest threats with our threat advisory

Customer testimonial

Cyber security has become an important concern for all as the business grows. System downtime means revenue loss for the business and affects credibility. Our partnership with Tata Communications ensures security across multiple security domains. With one of the broadest portfolios of managed security services, including DDoS mitigation, network/web application firewall, SIEM, and Vulnerability Assessment, Tata Communications delivers security strategies that help us understand risks, identify and respond to threats quickly, gauge our current security state and prepare ourselves to protect against today's most sophisticated attacks. To bolster our security posture and to keep up with the ever-evolving information security landscape, we partnered for our security operations with them around five years back. Their advanced Security Operations Center (SOC) comprises a team of highly skilled people operating round-the-clock to monitor, prevent, detect, analyse and respond to cyber security incidents. As our managed security services provider, Tata Communications supports us with a comprehensive approach to managing the cost and complexity of security technologies. We are confident that with them, we can conduct our business processes effectively without being unduly concerned about security operations.

- Col Rajmohan Rajgopala (Retd), Head IT Infrastructure and Infosec, Titan

Awards and recognition

IDC Analyze the Future — 'Major Player' in IDC MarketScape APAC Managed Security Services 2024

KuppingerCole ANALYSTS — 'Product Leader' in KuppingerCole 2023 Leadership Compass for MDR

NelsonHall NEAT Leader 2022 — 'Leader' in NelsonHall NEAT 2022 for Managed Cyber Security Services, Incident Response and Backup Services

FROST & SULLIVAN — India Managed Security Services Industry Excellence in Best Practices - Company of the year 2022

Everest Group RESEARCH — 'Major Contender' in Everest Research: IT Security Services PEAK Matrix® Assessment 2022 - Europe

Sources:

1 IBM Cost of Data Breach report 2023
2 Panaseer 2023 Security Leaders Peer report

For more information, visit us at www.tatacommunicatons.com

Schedule a consultation