TATA COMMUNICATIONS

STRENGTHENING CYBER RESILIENCE WITH THE TRIAD OF ANTICIPATE, DEFEND, RESPOND

Introduction

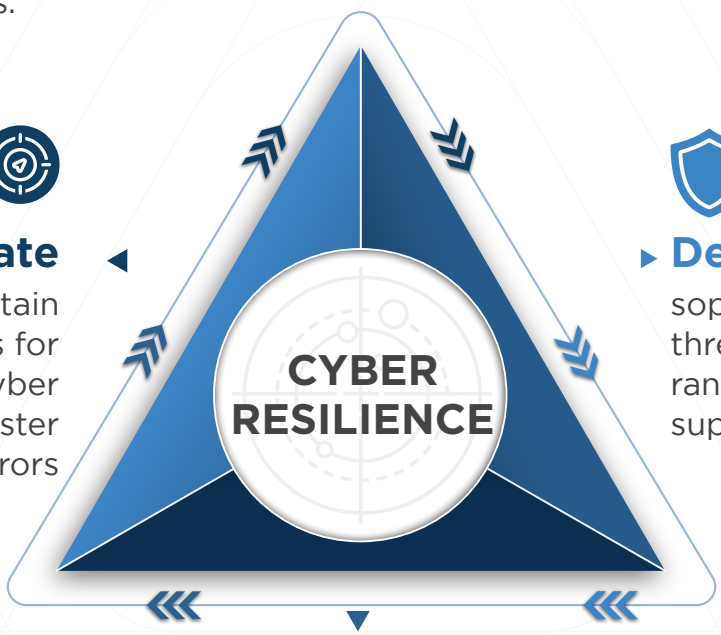
In today's digitally driven world, the threat landscape for businesses is more complex and dynamic than ever before. The rise of ransomware attacks disrupting businesses, geopolitical risks and cyber physical attacks all pose a significant threat to individual businesses and – at a broader level – national security. To counter these successfully, organisations must adopt a comprehensive approach to cybersecurity that focuses on anticipation, defence, and response. This methodology forms the foundation of an effective cyber resilience strategy.

Cyber resilience:

The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

Source: NIST SP 800-172

Tata Communications' Anticipate Defend Respond (ADR) methodology safeguards critical IT and OT infrastructure, including endpoints, workloads and VMs, across on-premises and hybrid environments. This, augmented by cyber recovery, helps boost an organisation's cyber resilience with predictive and scalable security by learning from past cyber incidents in real time and focusing on the shape of future attacks, offering better protection from threats.



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

Defend
sophisticated threats such as ransomware, APTs, supply chain attacks

Respond
to incidents rapidly and restore critical systems to minimise business disruption

Best practices for enhancing cyber resilience

Anticipate threats and maintain preparedness for adverse effects resulting from cyber threats, natural disasters or human error

Anticipation lies at the core of cyber resilience. It involves understanding potential threats and vulnerabilities before they materialise into full-fledged attacks. To anticipate threats effectively, organisations need to continuously monitor the threat landscape, analyse emerging trends, and stay informed about the tactics, techniques, and procedures (TTPs) used by threat actors.

Threat Intelligence

Leveraging threat intelligence feeds and platforms to gather information about potential threats targeting the organisation. This includes monitoring dark web forums, analysing malware samples, and tracking indicators of compromise (IOCs) and indicators of attack (IOAs).

Detection

Implementing continuous monitoring tools and techniques to detect security incidents in real time. This includes applying security controls like firewalls (FWs), intrusion detection systems (IDS), web application firewalls (WAFs), security information and event management (SIEM) systems, log analysis, and anomaly detection.

Risk Assessment

Conducting regular risk assessments to identify vulnerabilities within the organisation's infrastructure, applications, and processes. This involves evaluating the likelihood and potential impact of various cyber threats and prioritis ing mitigation efforts accordingly.

Security Awareness

Cultivating a culture of security awareness among employees through training programs, simulated phishing exercises, and regular communication about cybersecurity best practices. Educated and vigilant employees serve as an additional layer of defense against cyber threats.

TATA COMMUNICATIONS' VALUE ENHANCEMENT

8800 IOCs and IOAs shared through weekly and situational threat intelligence advisories, helping customers face cyber threats with confidence.

IOAs leverage code execution, C&C communications, and lateral movement to detect suspicious activities or threat methodologies in real time.

Netflow data augments threat scoring and provides high confidence IOCs while reducing false positives.

Periodic DR drills ensure effective strategy while simplifying failover and failback processes that are assured by guaranteed SLAs.

Defend sophisticated threats such as ransomware, APTs, and supply chain threats, and protect mission-critical IT infrastructure.

Once potential threats are identified, organisations must implement robust mechanisms to safeguard their assets and data. Defending against cyber threats requires a multi-layered approach that combines technology, processes, and personnel.

Endpoint Protection

Deploying endpoint security solutions such as antivirus, endpoint detection and response (EDR) tools, and next-generation firewalls to protect devices and endpoints from malware, ransomware, and other malicious activities.

Network Security

Implementing network security measures such as intrusion detection and prevention systems (IDPS), secure web gateways (SWG), and network segmentation to detect and block unauthorised access attempts and malicious traffic.

Cloud Security

Deploying security controls to protect cloud workloads, controlling access to critical cloud apps and resources and addressing cloud misconfigurations by conducting thorough assessments of cloud infrastructure settings, implementing automated tools for configuration management, and establishing clear policies and procedures for configuration changes.

Identity and Access Management (IAM)

Enforcing strong authentication mechanisms, least-privilege principles, and access controls to ensure that only authorised users have access to sensitive data and resources. This includes implementing multi-factor authentication (MFA) and regular access reviews.

TATA COMMUNICATIONS' VALUE ENHANCEMENT

Vast partner ecosystem of 55+ security OEMs and intellectual properties that protect networks, cloud, endpoints and other critical IT and OT estate.

Protect critical assets from endpoint to cloud with DLP, application level micro-segmentation, native DDoS protection, VAPT, SAST, DAST, and CNAPP to fortify crown jewels.

Halt lateral movement of advanced threats with an open integrated MDR solution that is built on 900+ use cases, and 100+ MITRE ATT&CK aligned threat hunting queries.

Offer unified threat visibility with granularity across network, cloud and endpoints through indigenous TCx portal.

Click to read more

Respond to cyber threats and restore critical systems to reduce business disruption

Despite best efforts to anticipate and defend against cyber threats, incidents can still occur. Therefore, organisations must have robust incident response plans in place to detect, contain, and mitigate the impact of security breaches promptly. Leveraging a SOAR-enabled incident response helps organisations investigate, respond to, and recover from cyber-attacks, while iteratively refining defence strategies through a feedback loop. This continuous improvement approach ensures that each such incident response enhances the organisation's resilience against evolving threats, bolstering its overall security posture.

Incident Response Team

Establishing a dedicated incident response team comprising cybersecurity professionals with the skills and expertise to investigate security incidents, coordinate response efforts, and communicate with relevant stakeholders.

Containment and Mitigation

Taking immediate actions to contain the scope of the incident and mitigate its impact on the organisation. This may involve isolating affected systems, restoring from backups, and implementing temporary workarounds to restore normal operations.

Post-Incident Analysis

Conducting a thorough post-incident analysis to identify the root cause of the security incident, assess the effectiveness of the response efforts, and identify lessons learned for future improvements.

TATA COMMUNICATIONS' VALUE ENHANCEMENT

Respond automatically and halt over one third of lateral threats with native SOAR

- Indigenously built SOAR platform responds to 94% of the L1 tickets automatically with 65+ playbooks that are customisable
- Air gapped recovery environment with industry leading Recovery Time Objective (RTO), Recovery Point Objective (RPO) can be customised based on criticality of the applications
- 100% DR success guarantees tied to SLAs with low latency from our geo-diverse DCs to restore operations post natural disasters, infrastructure failures, cyber breaches or human errors
- Multiple DR deployment options, dedicated DR SPOC with a proven SLAs offering 99.9% infrastructure availability
- Secured backup data with encryption, MFA, RBAC, periodic scans to ensure the data is not corrupted, with proven SLAs offering 99.9% infrastructure availability

Click to read more

Achieving cyber resilience through proven best practices and methodology is crucial. By proactively anticipating potential threats, implementing robust defence mechanisms, and efficiently responding to incidents, businesses can strengthen their security posture and mitigate the impact of cyber-attacks. Embracing a culture of continuous improvement and adaptation is key, as it allows organisations to stay one step ahead of evolving threats and safeguard their critical assets effectively. Ultimately, by integrating these principles into their cybersecurity strategy, organisations can enhance their resilience and ensure operational continuity in the face of ever-present and ever-evolving cyber risks.

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

CONTACT US