L&T Technology Services

BECOME CYBER IMMUNE WITH LTTS SECURITY OPERATIONS CENTER

MANAGED SECURITY SERVICES

STATE OF THE MARKET

The world has undergone a seismic shift in the past few months. The needs of organizations and workforces have shifted drastically. While the organizations across the world are trying to adapt to the new normal with remote working & social distancing, this has exposed them to newer threats & attacks due to the lack of a secure infrastructure. The remote workforce has increased the attack surface for every organization due to which attacks like phishing, malware, identity thefts are on the rise. To protect critical assets, data, and reputation, organizations need trusted cybersecurity partners who can scale up at rapid space and enable rapid yet effective threat monitoring, threat intelligence, incident response, containment, and remediation.

PARTNER WITH LTTS FOR A CYBERIMMUNE INFRASTRUCTURE

LTTS managed security services have been designed to address gaps in traditional managed security services and deliver what organizations need most: to reduce the time it takes to detect threats. LTTS Security Operations Center (SOC) operates 24x7x365, remotely monitoring, and managing the security of your networks, critical assets ensuring security is not compromised as you transition to newer working models.

LTTS is your ideal partner to do a **Quick Security Vulnerability Assessment remotely** and setup remote security monitoring platform to help you monitor the security of your network and systems to ensure security is not compromised as we transition to newer working models

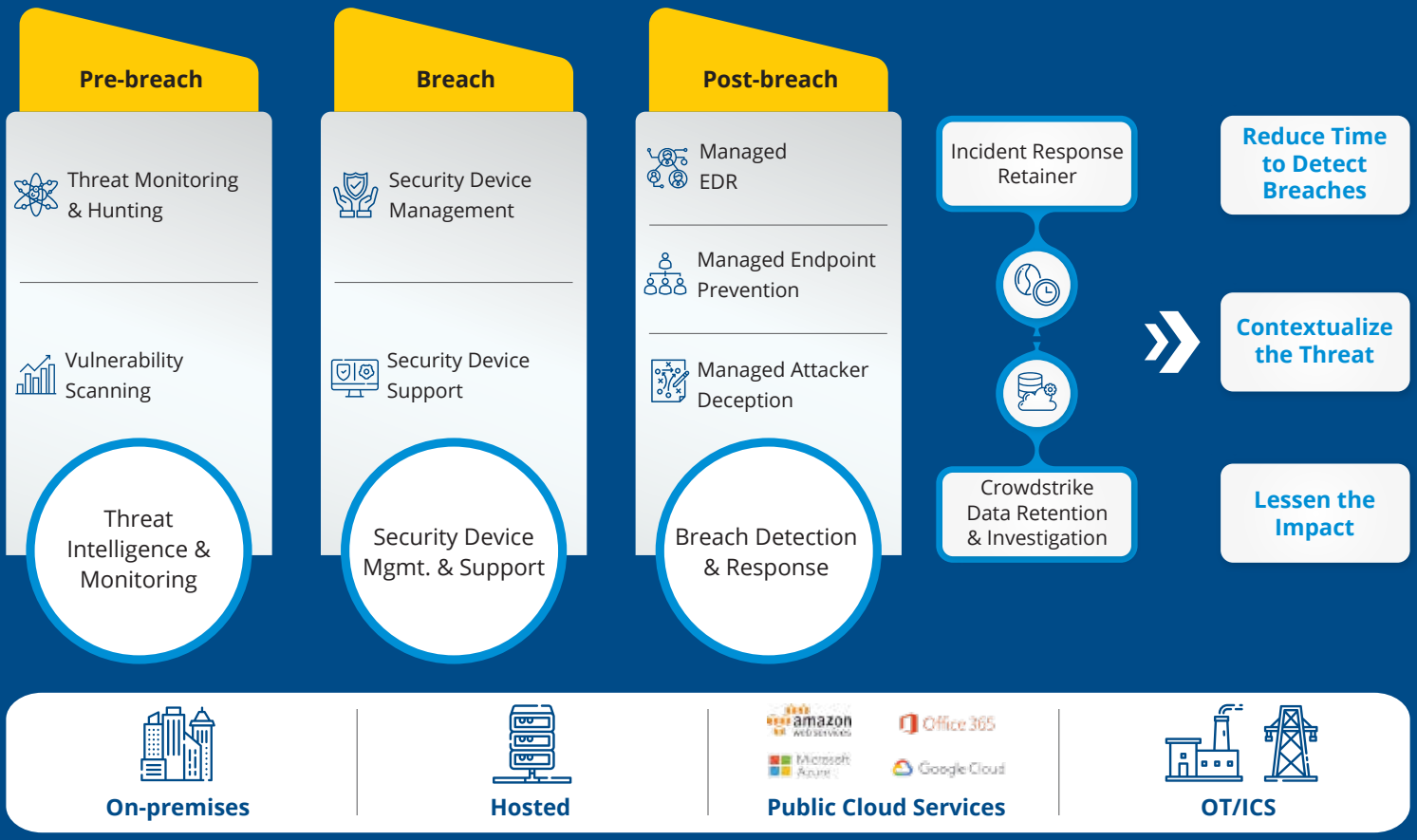
LTTS Managed Security Services have been designed to address gaps in traditional managed security services and deliver what organizations need most: to **reduce the time it takes to detect threats**

LTTS **24x7x365 Managed Security Services** are aligned to the different stages of an attack, which can be broadly divided into pre-breach, breach, and post-breach

LTTS can quickly setup **Security Operations Center (SOC)** for you to ensure continuous monitoring and maintain your desired security posture

LTTS offers **flexible business models** customizable for your need

As part of Managed Security Services we continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cyber security incidents



KEY DIFFERENTIATORS

- Advanced SOC solution combining expert analysts, threat monitoring, intelligence sharing & innovative technologies
- Integrated EDR & SIEM service
- Artificial Intelligence aided threat hunting and investigations
- Support for Industrial IoT, ICS, and OT Security
- Platform-based approach for Automation of Incident Remediation tasks

- Agility - Large resource pool with the ability to quickly ramp-up and ramp-down
- Domain expertise - LTTS team of security professionals have extensive experience in executing complex assignments
- Service quality and responsive delivery. Performance is driven by metrics and service level agreements (SLAs) to ensure tangible outcomes
- Flexible pricing options – Customers can choose a service plan that matches the enterprise's requirements
- LTTS Security CoE coupled with Strategic Partnership with KUDELSKI SECURITY

BENEFITS

- Early detection of violations and anomalies
- A quick and effective response to threats, emergency, or disaster situation
- Continuous improvement of security posture
- Visibility and protection from events that threaten the safety, quality, and productivity of the mission-critical systems
- Reduce Operational Downtime and Lower Cyber Risk
- Proactive Protection against all kinds of cyber threat
- Cost efficiency by leveraging our hosted technologies platform

CASE STUDY - 1

Providing emergency support in detecting, containing, and mitigating a cyber-attack and facilitating a rapid return to business as usual for the client.

The Challenge:

- An extortion attempt by a hacker that quickly escalated.
- Required an immediate action by cyber intrusion experts to investigate the attack logical flow, identify the components affected, provide a containment strategy, and mitigation advice to prevent follow-on attacks.

Solution:

- Started a remote investigation within the next business day, analyzing the attack vector, the attack flow timeline, and performing cyber threat hunting.
- As there was no endpoint protection in place, we deployed endpoint detection & response agents to 98% of the enterprise machines.
- Attack containment – Provided guidance and support on blocking identified attackers and limiting the exploited attack vectors.
- Attack mitigation –Provided guidance on implementing attack mitigation strategies to prevent follow-on attacks

The Outcome:

- Our Incident Response Team Identified, contained and eradicated the attack within 2 weeks, and effectively reduced business impact to customer's brand & reputation.
- Return to 'business as usual' within 3 weeks with full remediation, having mitigated the attack vector.
- Provided strategic recommendations prioritized to build resilience against cyber threats & threat actors.

CASE STUDY - 2

Managing a crisis following a cyber-attack and delivering an exceptionally quick containment for the client.

The Challenge:

- The client detected a compromise of their cloud computing environment, with over 300 Frontend and Backend systems, and had no indication of the attack vector utilized by the threat actor. This limited their containment options.
- Required an immediate action by cyber intrusion experts to investigate the attack profile, incident timeline, potential backdoors, threat vectors, identify the affected systems, provide a containment strategy, validate containment, and provide long term remediation recommendations.

Solution:

- Started a remote investigation within 4 hours of the initial emergency call, cyber intrusion experts worked simultaneously to provide 10-days of focused action including crisis management, forensic analysis, threat hunting, and attack monitoring.
- As there was no endpoint protection in place, We deployed Endpoint Detection & Response agents onto all systems within the cloud environment.
- Attack containment and remediation - We analyzed the attack profile, attack vectors, and incident timeline, identified the affected systems, provided a containment strategy, validated containment, and provided long term remediation recommendations.
- Our crisis manager bridged the gap between the client's leadership, client technical teams, and our task force, and provided guidance and support throughout the engagement. Attacks

The Outcome:

- Immediate containment, limited impact of the attack, limited financial implications.
- The infected application returned to business as normal status within 10 days.
- Provided remediation and hardening recommendations building resilience in the cloud against cyber threats & threat actors.

L&T Technology Services

ENGINEERING **THE CHANGE**