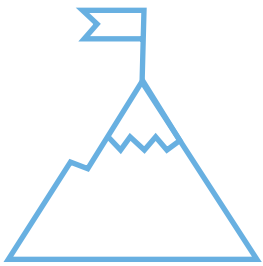




## Case study

# Cloud Security for a Leading European Sourcing and Service Provider

Our client is a leading European sourcing and services provider offering electrical, heating and plumbing, ventilation, and climate and energy solutions.



## Challenges

- ✓ Devise enterprise-level cloud security blueprint.
- ✓ Ensure real-time security monitoring and response of emerging threat and incidents.
- ✓ Ensure Cloud Defense SIEM deployment to protect environment from emerging cloud threat/attack and augment lack active threat hunting.
- ✓ Operationalize XDR solution to detect and protect endpoint, identity, application, O365, Azure AD, and Shadow IT applications from threat vectors.
- ✓ Automate security incident response with Next-Gen SOAR.
- ✓ Ensure enhanced cloud resilience with a cost optimized delivery model.

## LTIMindtree Solution

Defined a roadmap upgrade enterprise-level cloud security and implemented Active Cloud Defense solution.

Deployed MITRE ATT&CK Use cases, SOAR, Playbook, Workbook, and ITSM solution.

Deployed **and** configured Microsoft Defender Suite for Identity, O365, endpoint, application/MCAS for protecting the endpoint, ensuring identity and access control on applications, detecting threat and managing vulnerability, and security misconfiguration.

Helped achieve Steady state and ensured cyber resilience with continuous monitoring seamless (24\*7) support.



Deployed Microsoft SIEM solution, ingested necessary logs, third party technologies, Microsoft defender suite, Azure, O365, applications and Secure Data Lake solutions in cloud, and ensured threat detection & correlation.

Integrated User Entity Behavior Analytics (UEBA) and Threat Intelligence (TI) with SIEM solution for enrichment of security incident detection & correlation; augmented threat prevention with active Threat Hunting (TH) capability to ensure proactive IoA/IoC detection.

Deployed policies in Microsoft Cloud App Security (MCAS) to ensure Data Loss Prevention and Information protection.

# Defined Use cases and Playbooks



Phishing



Malware, threats



Identity protection



Suspicious User Activities



Security Misconfiguration



Threats & data loss protection on Application



Data Breach



Zero-day vulnerability



Real-time access policy verification



Credentials Compromise



Safe link, safe attachment

## Benefits



### Improved Cloud Defense Posture

by implementing Active Cloud Defense Resilience blueprint, LTIMindtree solution ensured timely detection of shadow IoAs and IoCs, prevention from critical threats with Active Threat hunting capability coupled secured Data Lake, protected client endpoint, identity, O365, application, Azure AD with Microsoft defender suite deployment.



### Enhanced Efficiency

Ensure real-time security monitoring (24\*7) and automated response to security incidents and attacks with advanced correlation techniques; augmented efficiency by reducing mean-time to detect response, and correlation of data breach and response by leveraging SOAR-led automation.



### **Optimized Operation**

Optimized the security operations and costs, by reducing efforts on noisy of false-positive alerts with help of EUBA & contextual Threat Intelligence and automating repetitive manual processes with effective Playbook, Workbook design ITSM integration.



### **Ensured Security & Compliance**

Assisted in meeting industry recommended compliance standard by deploying Cloud SIEM/SOC, Microsoft Defender suite.

**LTIMindtree** is a global technology consulting and digital solutions company that enables enterprises across industries to reimagine business models, accelerate innovation, and maximize growth by harnessing digital technologies. As a digital transformation partner to more than 700+ clients, LTIMindtree brings extensive domain and technology expertise to help drive superior competitive differentiation, customer experiences, and business outcomes in a converging world. Powered by nearly 90,000 talented and entrepreneurial professionals across more than 30 countries, LTIMindtree — a Larsen & Toubro Group company — combines the industry-acclaimed strengths of erstwhile Larsen and Toubro Infotech and Mindtree in solving the most complex business challenges and delivering transformation at scale. For more information, please visit [www.ltimindtree.com](http://www.ltimindtree.com).