LTIMindtree MSOC – A Cloud-native Sentinel Platform – Implementation Services

Today, organisations face the incredibly difficult task of protecting their expanding digital estate against growing cyber threats. The move to cloud and the mobile workforce has pushed beyond the borders of physical networks. Data, users and systems are everywhere. Meanwhile, the frequency and sophistication of threats are ever-growing. Security teams are under strain from the expanding breadth of defensive technologies, accelerating hybrid cloud adoption, and borderless, zero-trust networks. In addition, growing local/regional data privacy requirements and regulatory requirements have put organisations under pressure.

To meet the speed of cloud-scale, sophistication of threats and reduced time-to-detect and response, unleash the power of cloud-native solutions with built-in AI/ML, SOAR and threat-hunting capabilities to accelerate, modernize and develop intelligent security operations or managed detection and response.

LTIMindtree, a leading global managed security service provider, has extensive experience deploying Microsoft Sentinel across a wide-range customers across verticals with its distinct solutions that co-exist with existing and new groundup SIEM or while migrating to Microsoft Sentinel. Our accelerators and turn-key deliverables enable rapid provisioning to SOC operationalization.

Key Benefits and Differentiators:

1. Reduce cost through 30%-40% faster time to deploy
2. Assurance to meet the local and regional data regulatory compliance
3. Rapid provisioning and operationalization using LTIMindtree service accelerators
4. Reduce risk and threat landscape using LTIMindtree's 900+ proven advance threat detection and response use cases mapped to MITRE ATT&CK and compliances
5. 100+ certified Microsoft security professionals
6. Post-deployment hypercare support Microsoft Sentinel implementation service includes:

Week 1: Plan and Design

1. Understand the business, technical and operational security requirements
2. Gather native log source and integration options
3. Propose high-level design and validate the deployment pre-requisites
4. Identify and agree on out-of-the-box use cases on day one

Week 2: Deploy and Integrate

1. Automated the deployment of upto two Sentinel workspaces
2. Templates to integrate with Azure Lighthouse for seamless monitoring
3. Identify and integrate upto 10 customer selected native log sources
4. Test and validate the integration of above log sources
5. Design and implement operational and engineering-based RBAC as per customer requirements
6. Design documentation

Week 3: Configure and Tune

1. Configure the day one use cases – upto max of 10 use cases of customer selected
2. Enable out-of-the-box operational dashboards
3. Test and tune the use cases by reducing false alerts to a minimum of 10%
4. Prepare the operational and technical documentation

Week 4: Knowledge Transfer and Hypercare Support

1. Conduct basic awareness of the implementation to the operations team
2. Support issues reported by the operations team on the use cases deployed

LTIMindtree MSOC – A Cloud-native Sentinel Platform – Implementation Services

Key Service Deliverables:

1. Implementation plan
2. Design documents
3. Standard operating procedures and run books for managing deployed use cases
4. Hypercare support for one week

Next Steps:

- Manage the SOC services by the customer in-house team
- Engage with LTIMindtree to discuss on the managed detection and response services and onboard into the MSSP Platform