LTIMindtree MSOC – A Cloud-native Sentinel Platform – Workshop

Microsoft Sentinel is a cloud native scalable SIEM and SOAR solution. Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response. Azure Sentinel delivers a birds-eye view across the enterprise, alleviating the stress of increasingly sophisticated attacks and growing volumes of alerts, with long resolution timeframes.

1. Collect data at cloud-scale across all the users, devices, applications and infrastructure both at on-premise and cloud
2. Minimize false positives using AI/ML (analytics) and threat intelligence
3. Investigate threats using AI and hunt for adversaries hidden in the environment
4. Rapid incident response to threats using built-in orchestration, automation playbooks and workflows

During this eight-hour workshop, we will demonstrate the capabilities of Microsoft Sentinel, LTIMindtree's SOC process, frameworks, and accelerators to enhance threat detection and response.

Build and Integrate:

1. Rapid deployment of Microsoft Sentinel and its modules
2. Provision Sentinel workspaces across different geographies to meet local/region data regulatory requirements
3. Demonstrate log retention options and explain what works best in different scenarios
4. Onboarding of various log sources using different log source integration methods
5. Integration with collaboration tools such as Microsoft Teams, ServiceNow
6. Integration with Azure Lighthouse for single pane of glass monitoring

Manage and Operate:

1. SOC detection channels and corresponding sources
2. Incident detection, investigation and analysis using different use cases
3. Use case development and enhancements
4. Threat hunting framework and use cases

Enhance and Optimize:

1. Demonstration of the workflow automation using Logicapps
2. Incident prioritization
3. SOC analyst efficiency
4. Integration with OSINT threat intelligence

After this workshop, you will:

1. Understand the benefits of cloud native SIEM solutions
2. Be assured of meeting local/regional data regulatory compliance requirements
3. Understand rapid detection and response to evolving threats using Sentinel and LTIMindtree's SOC process
4. Know more about operational efficiency using LTIMindtree's SOC accelerators and framework
5. Gain visibility into threat and security posture