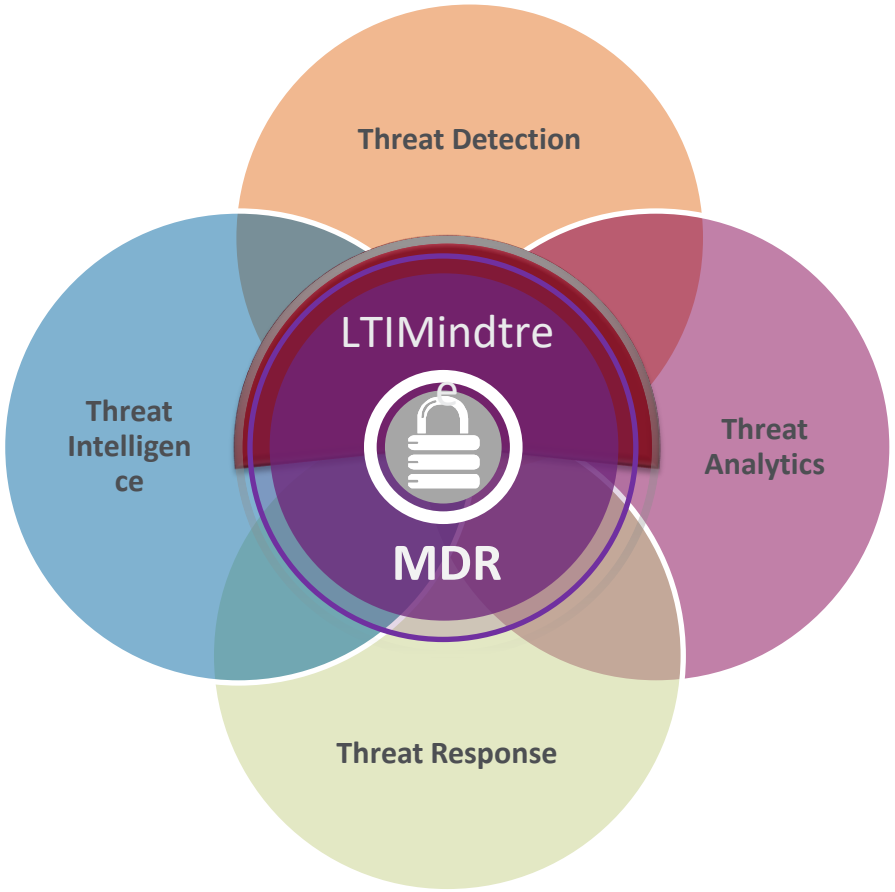

Benefits of Sentinel – Cloud Native SIEM

79% of SOC analyst efficiency over 3 years

79% cost reduction of SIEM

67% faster time to deploy and operate

Comply with local data regulatory requirements

24x7 Threat detection and response

Proven experience of Managed SOC

Experienced and certified security professionals

Threat advisory, Threat research and center of excellence

Experience in Customized integrations

Industry-specific threat intelligence

LTIMindtree's use case framework

Agenda

2.5 Hours	30 Minutes	2.5 Hours	30 Minutes	2 Hours

Built and Integrate
• Platform Provisioning
• Integration
  • Integration with Azure Lighthouse
  • Integration of log sources
  • Non-native log source
	Break	**Manage and Operate**
		• A day in the life of an SOC Analyst
		• Major Incident management workflow
		• Data Enrichment
		• Use case development and enhancement
			Break	**Enhance and Optimize**
				• Playbooks for Incident response
				• OSINT Integration

Hours mentioned are representative and will be customized as per customer needs