1. Main Security Risks

Area	Risk	Example
IoT Devices	Device compromise	Attacker injects fake telemetry data to hide a fault or trigger false alerts
Data Transmission	Data interception / tampering	If telemetry is sent over insecure channels, attackers can modify it in transit
Data Storage	Sensitive data exposure	Stored device logs or alerts may contain operational or location data
AI/ML Models	Model poisoning	Malicious data could bias the model's anomaly detection
APIs & Dashboards	Unauthorized access	If alerts/explanations are exposed via APIs or dashboards without proper access control
Alerting System	Alert spoofing	Attackers send fake high-severity alerts to cause confusion or downtime
Cloud/Edge	Misconfiguration	Publicly exposed endpoints, weak authentication, unpatched vulnerabilities