Note on AIOps frameworks, with brief descriptions for each:

AIOps Frameworks – Intermediate-Level Overview

AIOps (Artificial Intelligence for IT Operations) refers to platforms and frameworks that use machine learning, big data analytics, and automation to enhance IT operations. These frameworks ingest vast volumes of operational data and help teams detect anomalies, predict issues, automate responses, and optimize performance.

Below is an intermediate-level overview of popular AIOps frameworks and what makes each unique.

1. Moogsoft AIOps

Description:
Moogsoft is one of the earliest AIOps platforms, focused heavily on **event correlation**, **noise reduction**, and **incident management**. It uses machine learning to combine related alerts into "situations," helping operations teams quickly identify root causes and reduce alert fatigue.

Strengths:

- Real-time anomaly detection
- Strong correlation engine
- Integrates with many monitoring tools

2. Splunk IT Service Intelligence (ITSI)

Description:
Splunk ITSI layers AIOps capabilities on top of Splunk's powerful data platform. It provides **service health monitoring**, **predictive analytics**, and **KPI-based dashboards**. It's commonly used in large enterprises due to Splunk's broad ecosystem.

Strengths:

- Deep observability via Splunk logs/metrics
- Customizable service health scores
- Predictive alerting

3. Dynatrace Davis AI

Description:
Dynatrace uses an embedded AI engine called **Davis** that automatically discovers environments, maps dependencies, and pinpoints the root cause of operational issues. It's known for its full-stack observability and autonomous operations.

Strengths:

- Automatic topology discovery
- Very accurate root-cause analysis
- Cloud-native focus

4. IBM Cloud Pak for AIOps

Description:
IBM's Cloud Pak is a modular AIOps solution that brings together logs, metrics, and application data to provide **incident prediction**, **probabilistic reasoning**, and **automated remediation**. It's popular in enterprises with hybrid-cloud environments.

Strengths:

- Enterprise-grade, modular architecture
- NLP for change and incident analysis
- Designed for hybrid/multi-cloud

5. BigPanda AIOps

Description:
BigPanda specializes in **event correlation**, **alert noise reduction**, and **root-cause analysis**. It ingests data from multiple monitoring tools and uses ML to unify events into actionable insights.

Strengths:

- Strong open-integration approach
- Scales well for large operations teams
- Clean, intuitive incident timelines

6. ServiceNow AIOps / Predictive AIOps

Description:
ServiceNow incorporates AIOps into its **IT Operations Management (ITOM)** suite. It leverages existing CMDB data to predict outages, correlate alerts, and automate remediation through workflows.

Strengths:

- Deep integration with ITSM and CMDB
- Predictive scoring for service health
- Strong workflow automation

7. Azure Monitor / Azure AIOps Capabilities

Description:
Microsoft Azure includes AIOps-enabled features within **Azure Monitor, Application Insights, and Log Analytics**. These tools provide intelligent alerting, anomaly detection, and end-to-end observability across Azure environments.

Strengths:

- Cloud-native automation and insights
- Excellent integration with DevOps pipelines
- Predictive analytics for Azure workloads

8. AWS DevOps Guru

Description:
AWS DevOps Guru provides AIOps functionality within the AWS ecosystem. It continuously analyzes operational data using ML to detect anomalies and recommend remediation steps.

Strengths:

- Native integration with AWS services
- Automated insight generation
- Minimal setup required

9. Google Cloud AIOps / Operations Suite

Description:
Google Cloud offers AIOps features integrated into **Cloud Monitoring, Logging, and Error Reporting**. It uses Google's ML capabilities for anomaly detection, predictive alerts, and automated trend analysis.

Strengths:

- Strong ML-driven insights
- Seamless GCP integration
- Scalable for cloud-native apps

Summary

AIOps frameworks vary in their strengths—some focus on event correlation, others on predictive intelligence, and some on full-stack observability. Selecting the right AIOps solution depends on the infrastructure complexity, existing toolchains, and desired automation level.