Artificial Intelligence and Machine Learning: What does it mean for Observability?

splunk>
a **CISCO** company
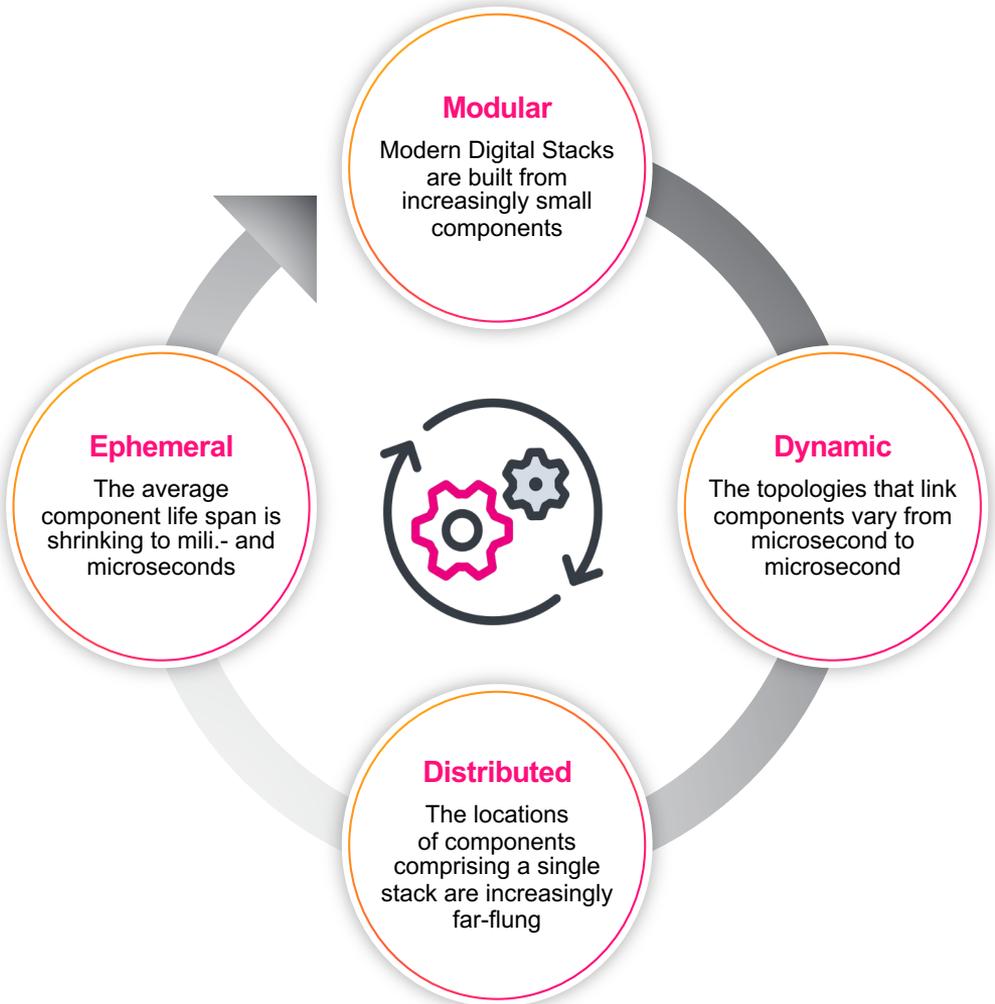
Making Observability Intelligent

William Cappelli

Observability Strategist

splunk>

"

Until now, AIOps has spoken in the language of events and alerts; it must learn the language of telemetry.

System Complexity

Modular
Modern Digital Stacks are built from increasingly small components

Dynamic
The topologies that link components vary from microsecond to microsecond

Distributed
The locations of components comprising a single stack are increasingly far-flung

Ephemeral
The average component life span is shrinking to mili.- and microseconds

Data Complexity

Volume
The amount of self-descriptive data is increasing by an order of magnitude every 5 years

Velocity
Rate of self descriptive data generation is increasing by 20% a year

Variety
The number of data types monitored has doubled over the past ten years

Vectoriality
Avg data dimensions have increased by two orders of magnitude over the last five years

0010
01010
0101

The Monitoring Design Plan

1975 - 2025

Samples
Assuming low entropy, monitoring data is sampled - less than 5% is norm.

Structured Event Records
Data is packed into event record formats intended to represent states.

Database
Records stored in database.

Predefined Model
Records from database are compared to model - alert if mismatch.
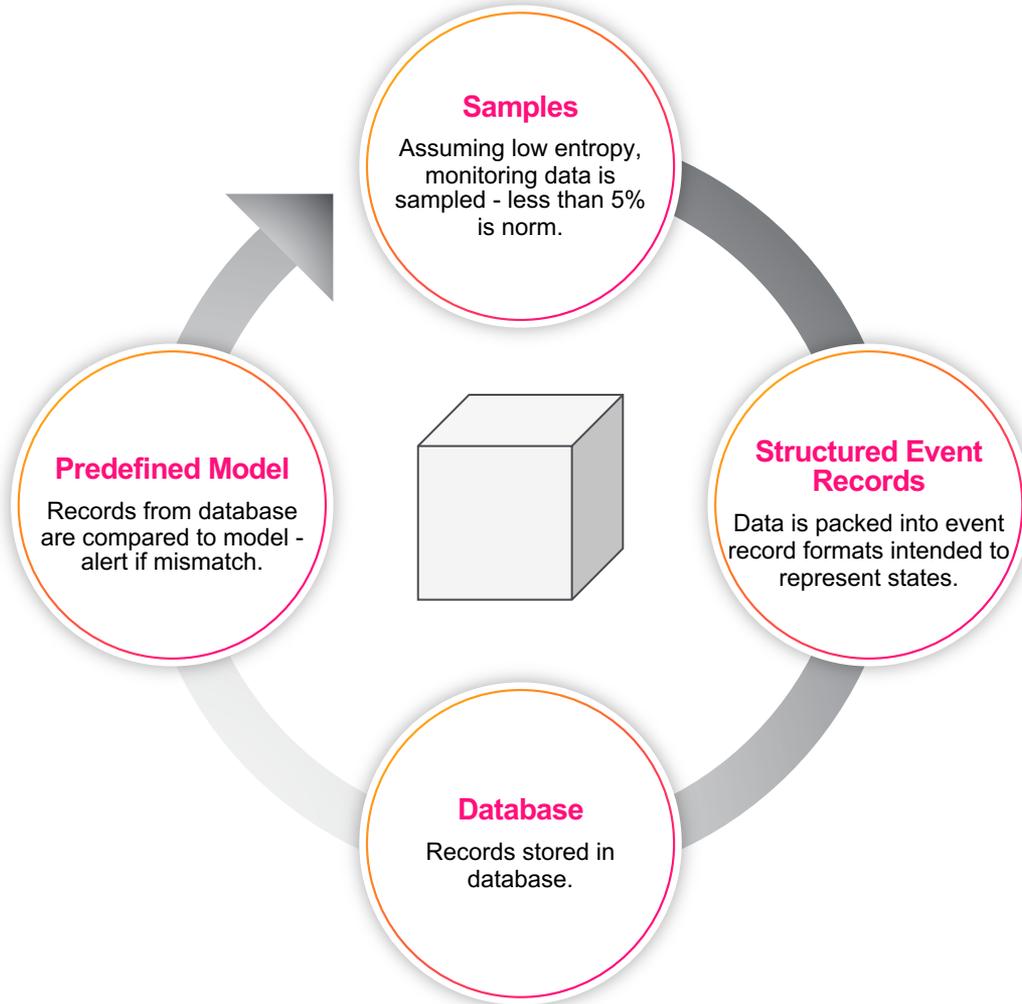
But… it does not work anymore!

Monolithic Apps (2007 - 2011)

DEV   OPS
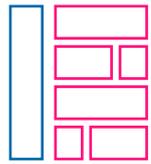
Events, Rules, Alerts

DC   VM VM VM VM VM VM

Multi-Tier Apps (2011 - 2015)

DEV ↔ OPS

Numbers, Models, Reports

DC   VM VM VM VM VM VM
Private   Public
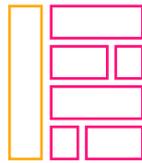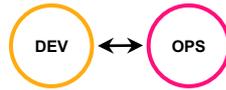
Modular Apps (2015 -2020)

→ DEV   OPS ←

Logs, Metrics, Search

VM VM VM
Private   Public
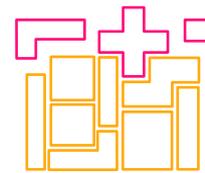
Ephemeral Apps (2020 - ?)

→ DEV OPS ←
?
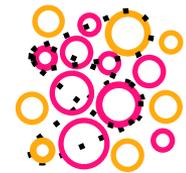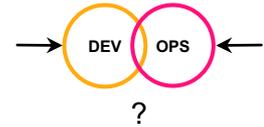
Full Telemetry, AI, Automation

Private   Public

Full-Stack Visibility
and **Context-Rich Insights**

splunk>

Observability **Is a Data Problem**

The more observable a system, the quicker we can understand why it's acting up and fix it

Metrics

Do I have a problem?

Traces

Where is the problem?

Logs

Why is the problem happening?

Detect

Troubleshoot

Root Cause

The Five Dimensions of AIOps

Metrics, Traces, Logs

Correlated Events

Incidents, Causal Chains of Events

Teams, Plans, Learning

Automated Processes

Signals → Response

Select

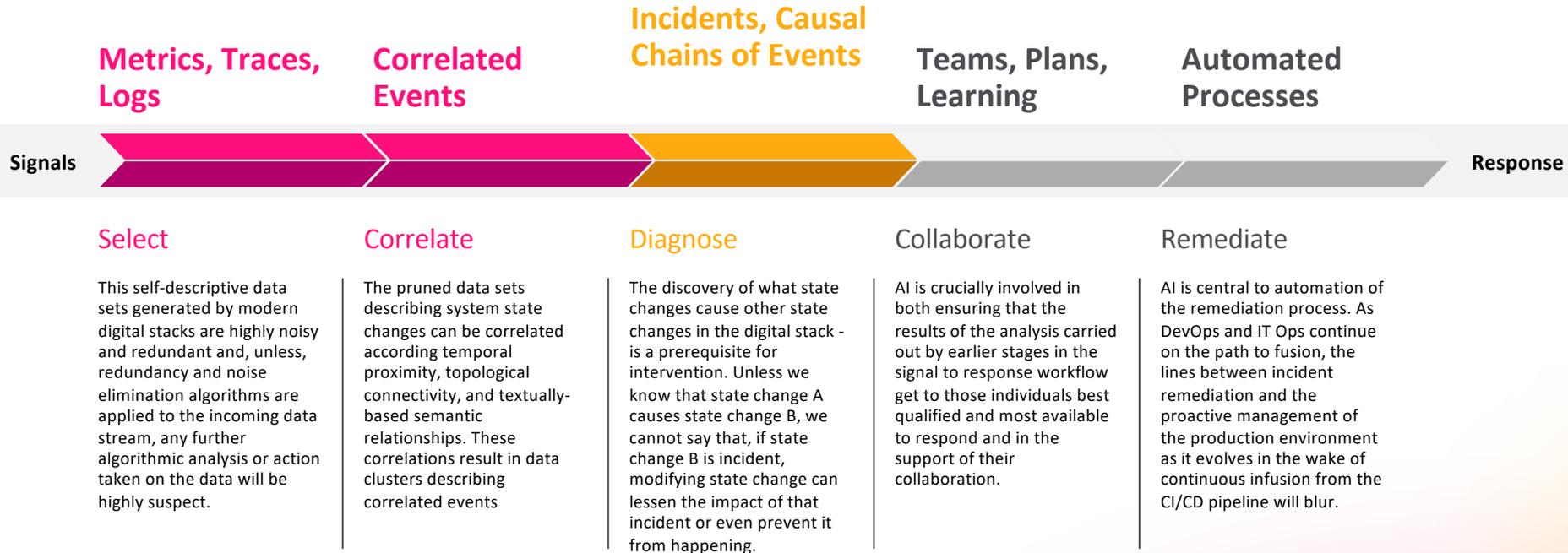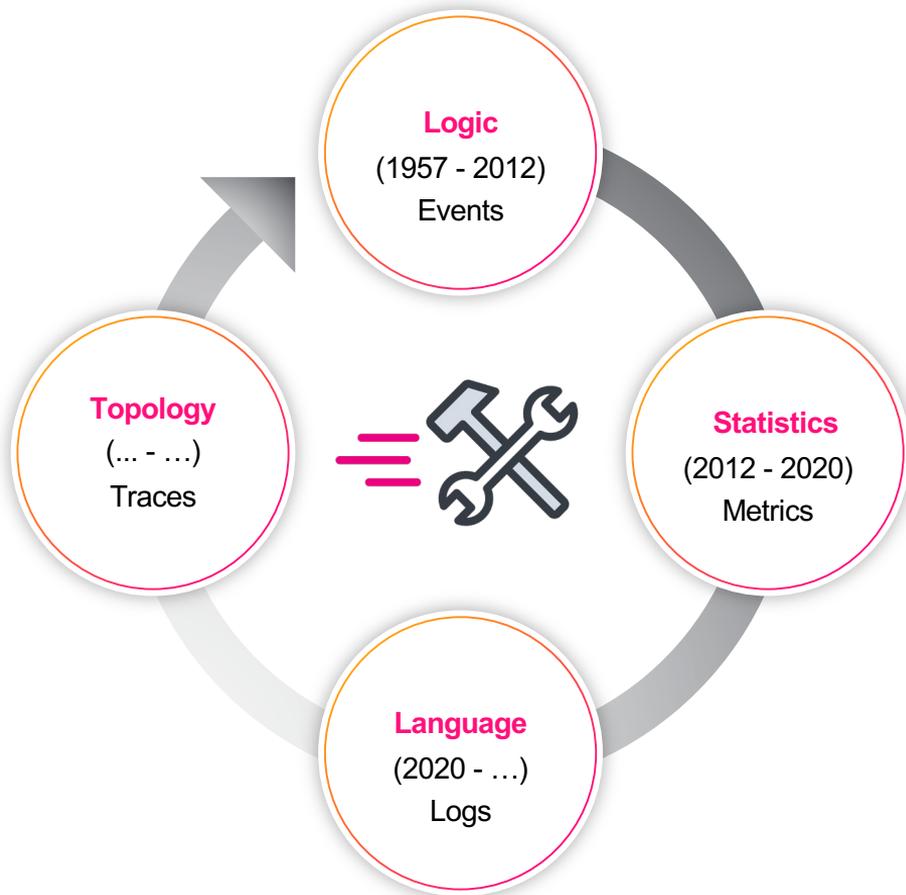This self-descriptive data sets generated by modern digital stacks are highly noisy and redundant and, unless, redundancy and noise elimination algorithms are applied to the incoming data stream, any further algorithmic analysis or action taken on the data will be highly suspect.

Correlate

The pruned data sets describing system state changes can be correlated according temporal proximity, topological connectivity, and textually-based semantic relationships. These correlations result in data clusters describing correlated events

Diagnose

The discovery of what state changes cause other state changes in the digital stack - is a prerequisite for intervention. Unless we know that state change A causes state change B, we cannot say that, if state change B is incident, modifying state change can lessen the impact of that incident or even prevent it from happening.

Collaborate

AI is crucially involved in both ensuring that the results of the analysis carried out by earlier stages in the signal to response workflow get to those individuals best qualified and most available to respond and in the support of their collaboration.

Remediate

AI is central to automation of the remediation process. As DevOps and IT Ops continue on the path to fusion, the lines between incident remediation and the proactive management of the production environment as it evolves in the wake of continuous infusion from the CI/CD pipeline will blur.

Where is AI going?

"

Telemetry without AI is blind; AI without telemetry is empty.

Thank You

splunk>
a **CISCO** company

cisco Connect

Let's go