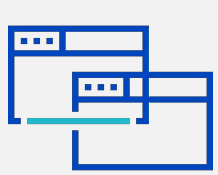
sumo logic

Going beyond the three pillars

Abelardo Gonzalez, Director of Product Marketing, Sumo Logic

Technology complexity is growing



Expanding tech stack

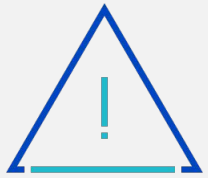
+

Exploding # of components

+

Rapid rate of change

=



Broadening attack surface

Data deluge

Legacy tools can’t keep up

“We think the definition of observability should be expanded in a couple of ways. Certainly, that’s the data you need—logs, metrics and traces. But all of this needs to be placed and correlated into a topology so that we see the relationships between everything, because that’s how you know if it can impact something else.”

- Charlie Rich, Gartner

A practical definition of Observability

An **observable system** is one that can both be:

1) **monitored** for known issues and performance standards (SLIs/KPIs), and
2) **debugged** (troubleshooting)

in order to **resolve issues quickly enough** to continue to meet availability and performance requirements

How is Observability different from monitoring

- **Monitoring** by itself only tells you that **something is broken**.
  - It is predicated on **knowing what to look for** beforehand

- **Observability** is about finding out **“why”**.
  - **Monolithic** applications often fail in **predictable** ways
  - **Modern** applications are **too complicated** to know all of the ways your application can fail
  - **Observability** allows you to ask the **right questions**

- So, **Monitoring** is a **subset** of **Observability**

Honest Status Page
@honest_update

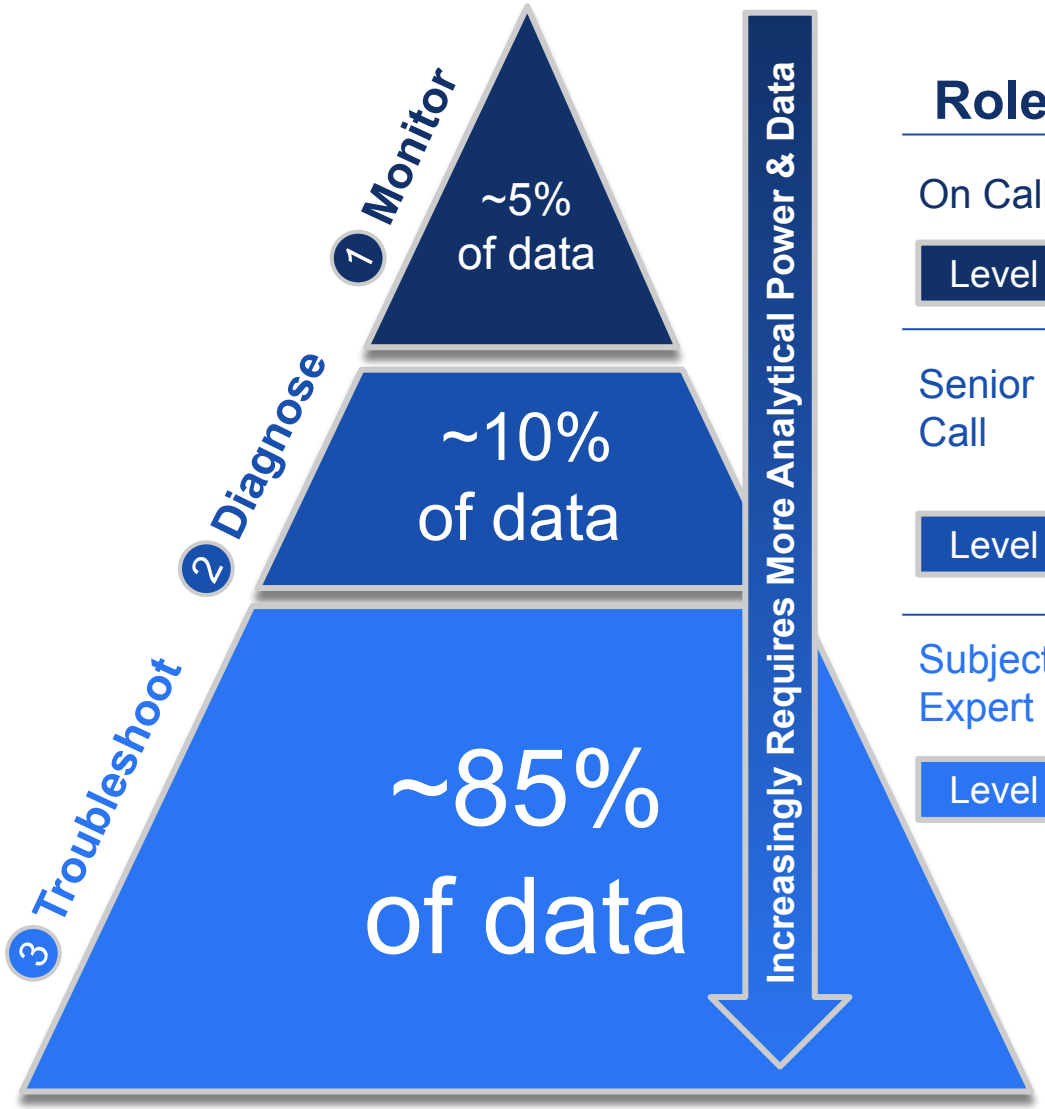
Follow

We replaced our monolith with micro services so that every outage could be more like a murder mystery.

4:10 PM - 7 Oct 2015

For those who don't remember the movie Clue

Why Observability is so hard



Role	Activities	Challenges	Implication
On Call Level 1	• **Alert** and notify • **Playbook** driven steps	• **Thresholds** only • **Incomplete** monitoring	• Increased **downtime** • **Reactive** monitoring • **Slower reaction** time
Senior On Call Level 2	• **Dashboard** focused • Triage based on **basic analytics**	• Forced to **sample** • Difficult to understand **dependencies**	• **Longer time** to identify issues • **Difficult to pinpoint** problem areas
Subject Matter Expert Level 3	• **Analytics-driven** investigation • **Expertise-driven** exploration	• Restricted to **pre-parsed** data • Can't identify **unknown-unknowns** • **Missing** data • Too much **manual**, **tedious** analysis	• **Problem resolution** takes too long • **Long lead-time** to establish cause & effect • Root causes remain hidden causing **repeated failures**

sumo logic

"Observability" requires **rich data** and **richer analytics** to get from **alert** to **resolution**.

1 **Monitor**
Using Unified Alerts for quick MTTI

2 **Diagnose**
With contextual information for better MTTD

3 **Troubleshoot**
Leveraging powerful analytics deliverting fast MTTR

~20% of data

~30% of data

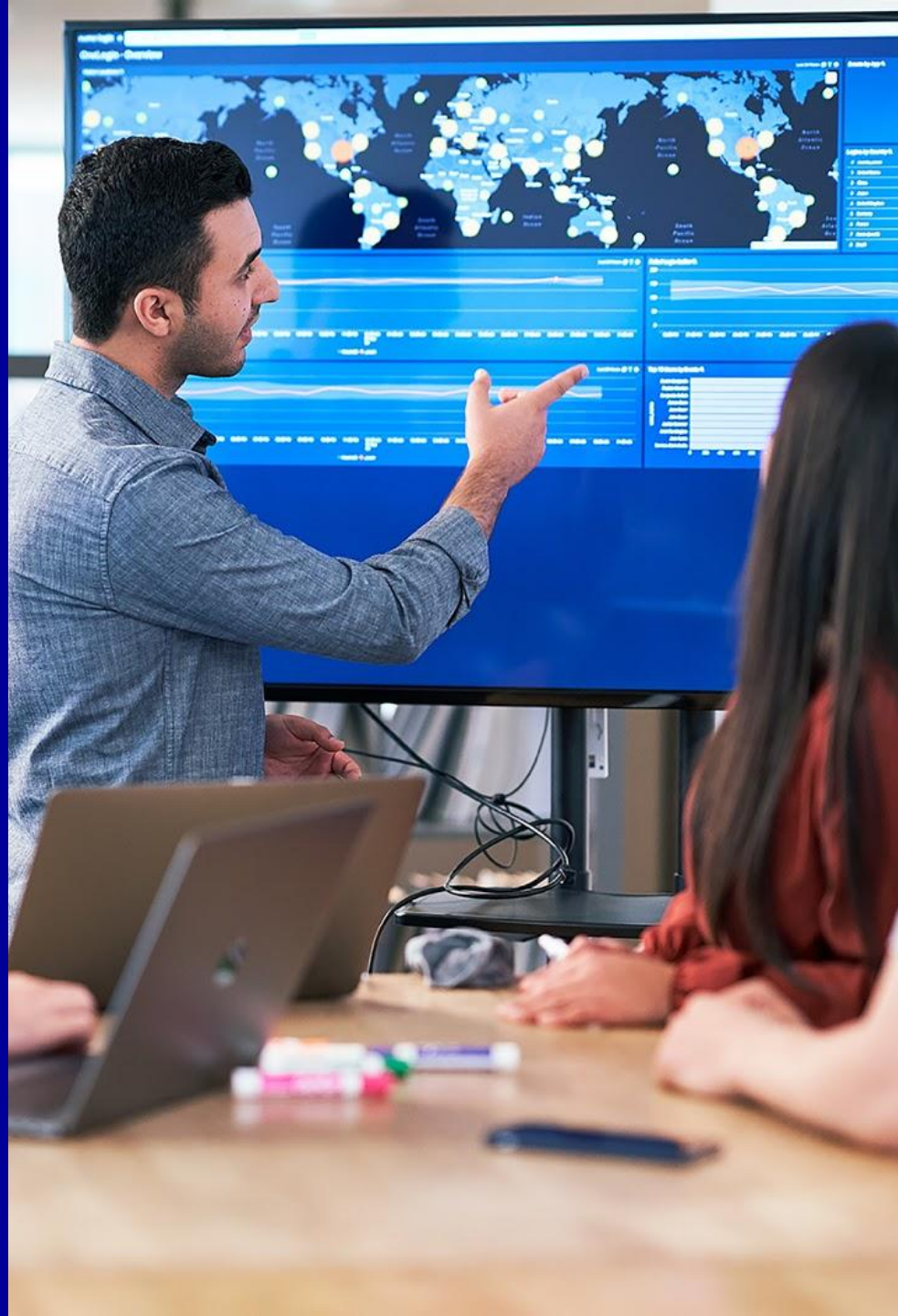
~50% of data

More Data Requiring More Sophisticated Analytics

Source: Based on Sumo Logic Internal Analysis

sumo logic

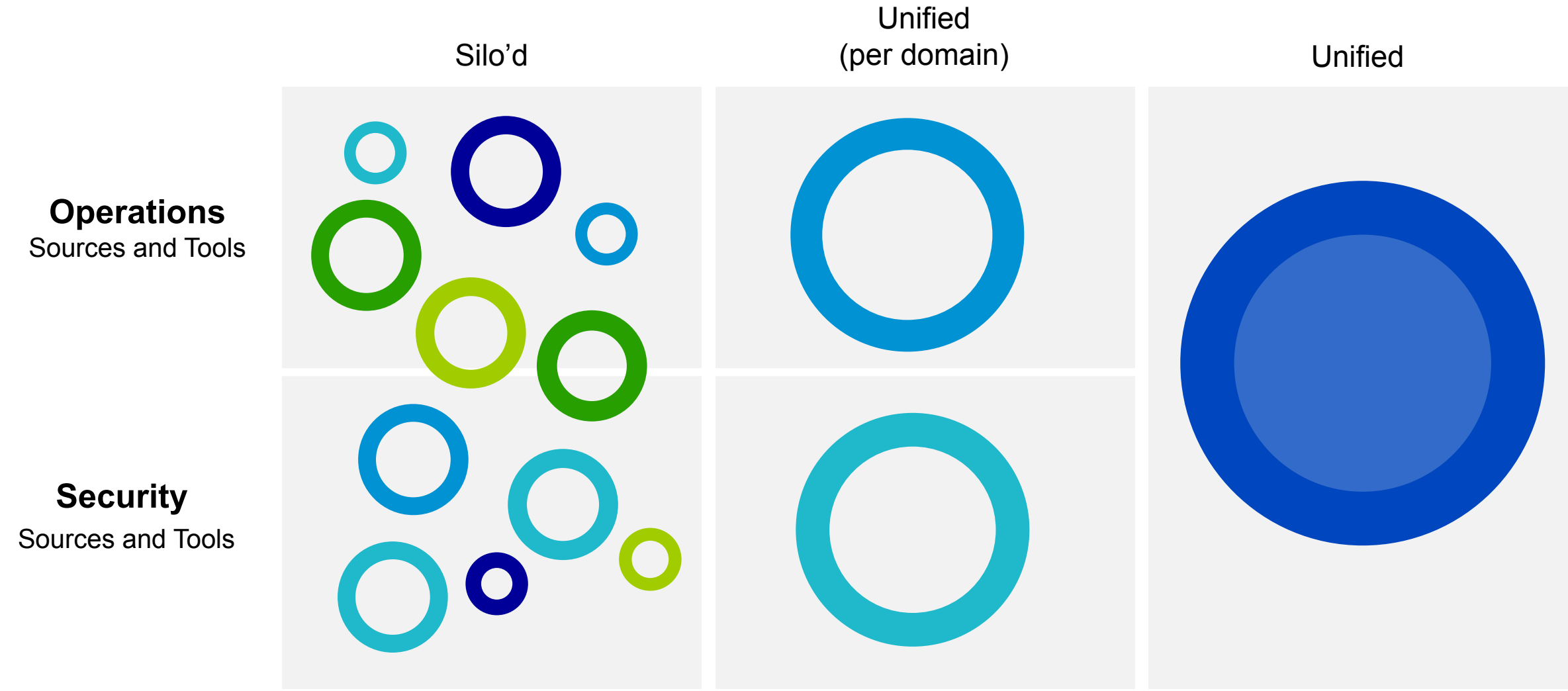
How do we go about achieving this?



sumo logic

How are you managing that complexity?

On-premises or cloud-based solutions?



Simple Steps to Achieving Observability

1. Determine your Objectives
2. Evaluate existing telemetry
3. Add new telemetry
4. Deploy
5. Repeat

Objectives-Driven Observability

- **Step 1**: What are your goals/objectives?
  - Service Level Objectives (SLOs) or Key Performance Objectives (KPOs)
- **Step 2**: How do you measure those goals?
  - Service Level Indicators (SLIs) or Key Performance Indicators (KPIs)
- **Step 3**: Can you measure your SLIs with your current data?
- **Step 4**: (If No) Add more data - Logs, Metrics, Traces/APM

Three key takeaways

Observability is meant to address the new realities of keeping modern applications reliable

1. Monitoring is a subset of Observability
2. Domain agnostic analytics is essential to Troubleshooting
3. Start with your objectives and work from there

Thank you

Abelardo Gonzalez

Director of Product Marketing, Sumo Logic

Email: agonzalez@sumologic.com

sumo logic

s u

Empowering the people who power modern business

m o