An IT Operations Approach to Observability

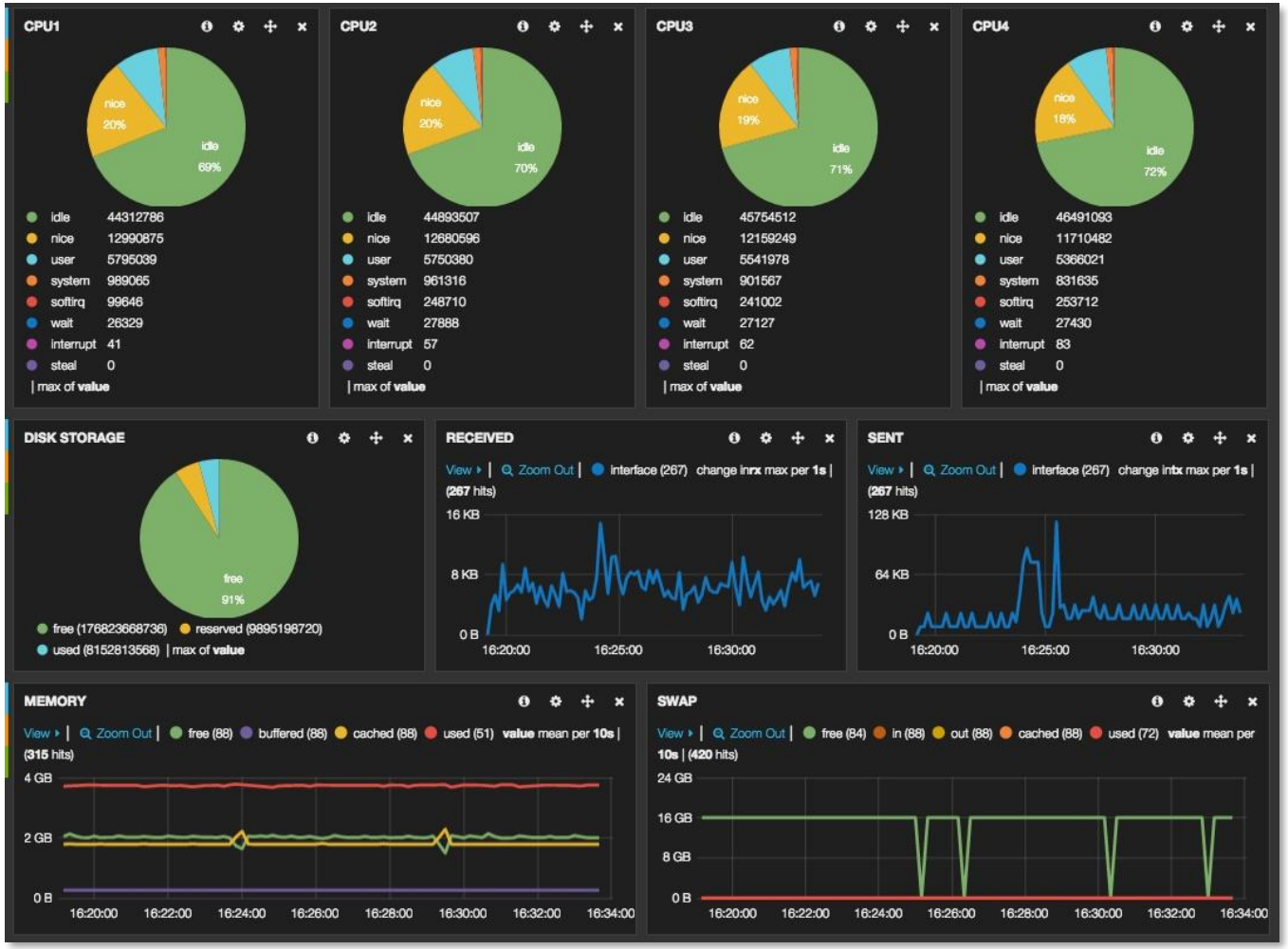
Linkedin.com/in/mikesoule/

An IT Operations Approach to Observability

- What is observability?
- How can I apply it?
- How do I measure?
- How can I act on it?

What is observability?

Single pane of glass



What is observability?

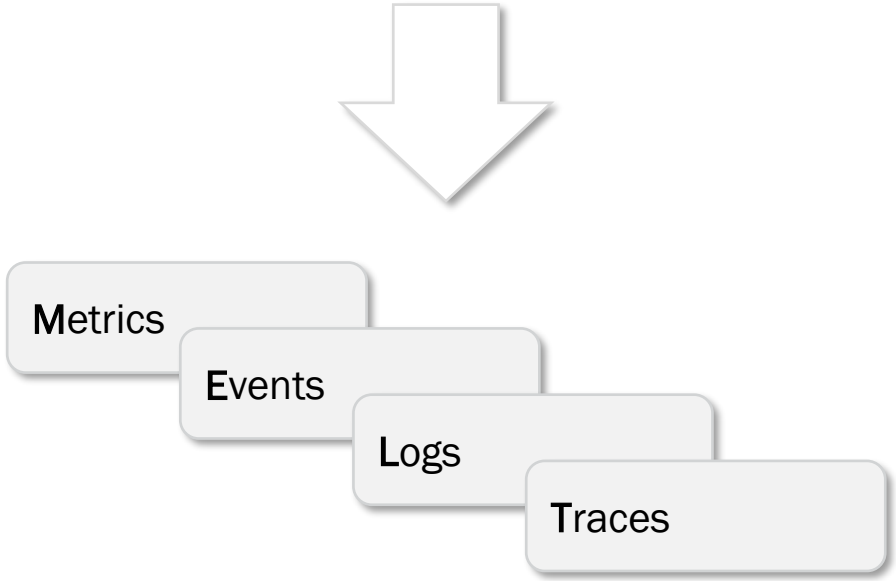
Single pane of glass

- Is the environment healthy or not?
- What is normal or anomalous?
- Is the environment efficient?
- What does any of this mean?

What is observability?

Single pane of glass

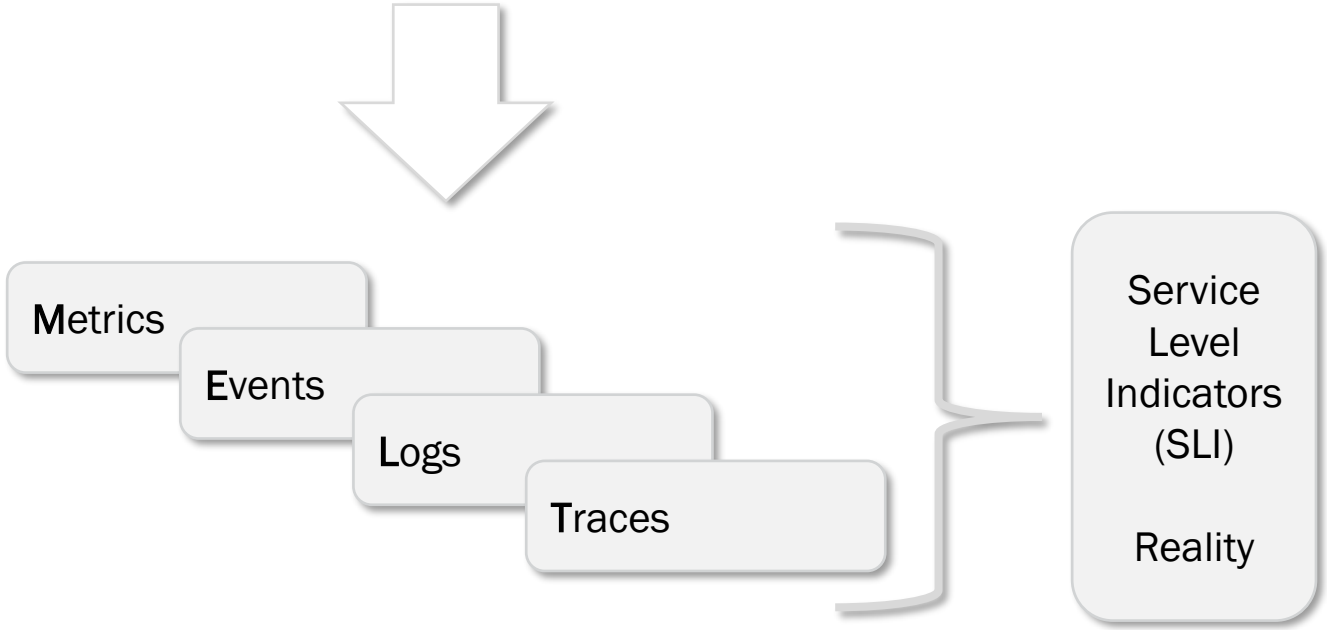
- Is the environment healthy or not?
- What is normal or anomalous?
- Is the environment efficient?
- What does any of this mean?



What is observability?

Single pane of glass

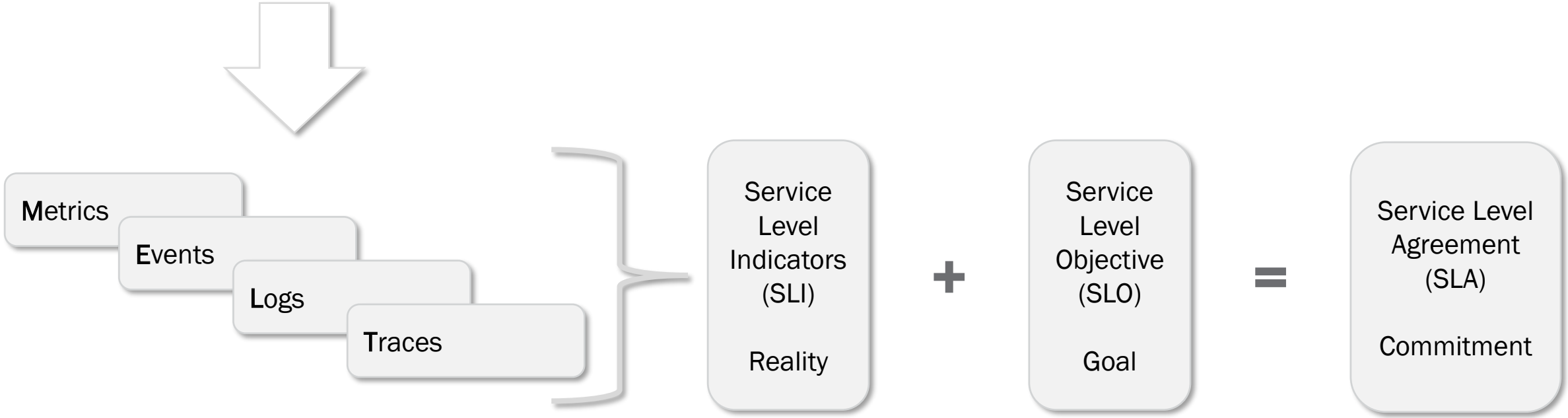
- Is the environment healthy or not?
- What is normal or anomalous?
- Is the environment efficient?
- What does any of this mean?



What is observability?

Single pane of glass

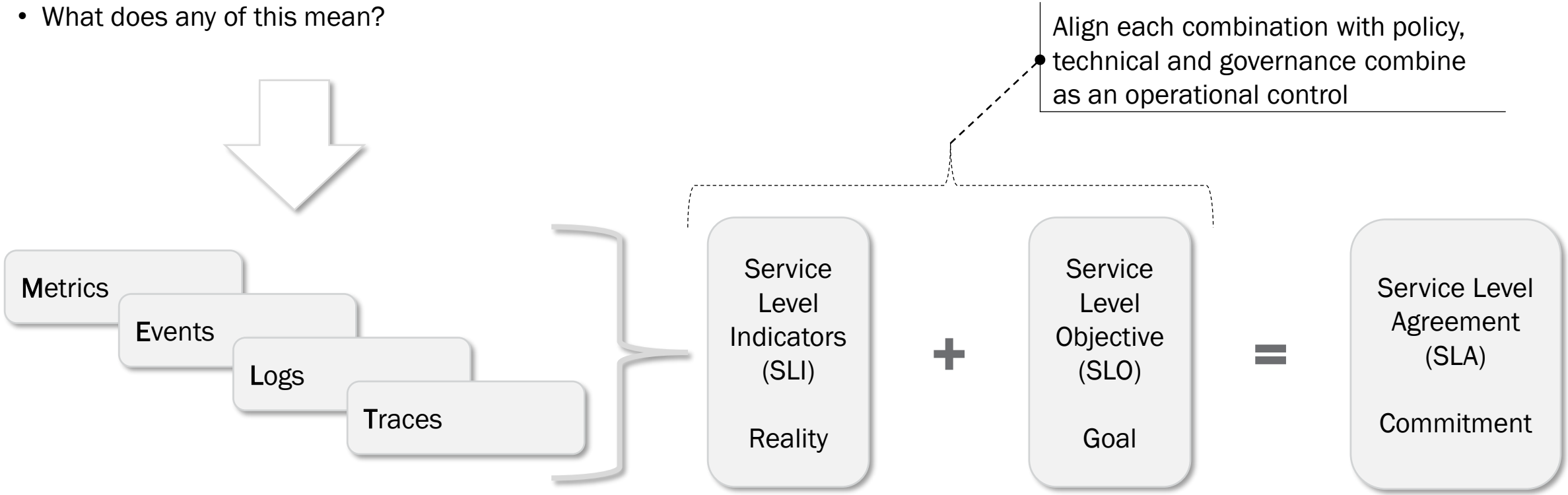
- Is the environment healthy or not?
- What is normal or anomalous?
- Is the environment efficient?
- What does any of this mean?



What is observability?

Single pane of glass

- Is the environment healthy or not?
- What is normal or anomalous?
- Is the environment efficient?
- What does any of this mean?

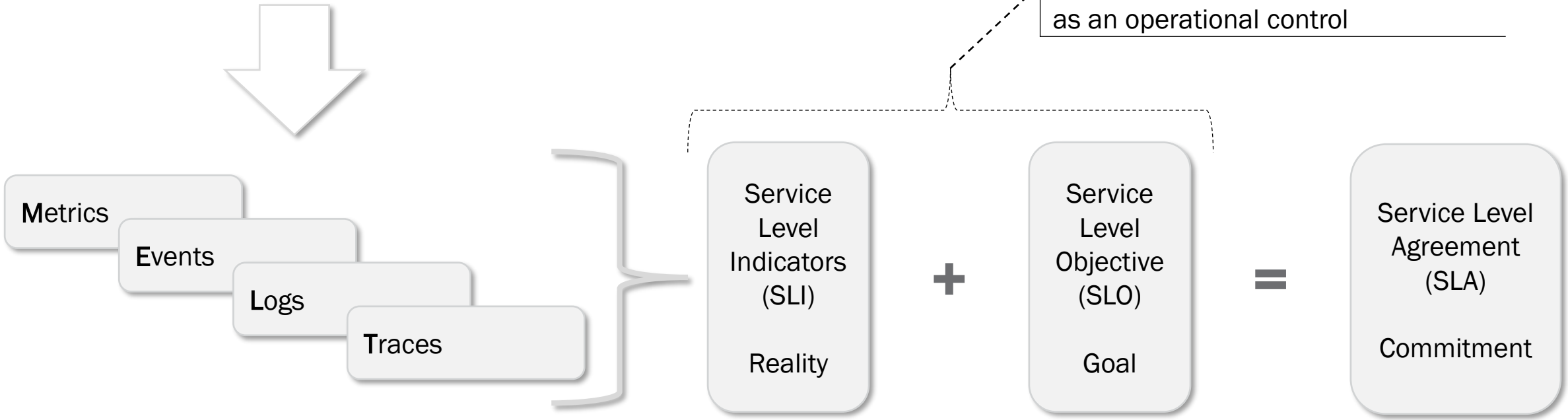


What is observability?

Single pane of glass

- Is the environment healthy or not?
- What is normal or anomalous?
- Is the environment efficient?
- What does any of this mean?

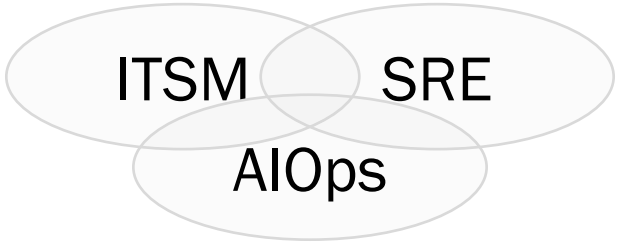
Align each combination with policy, technical and governance combine as an operational control



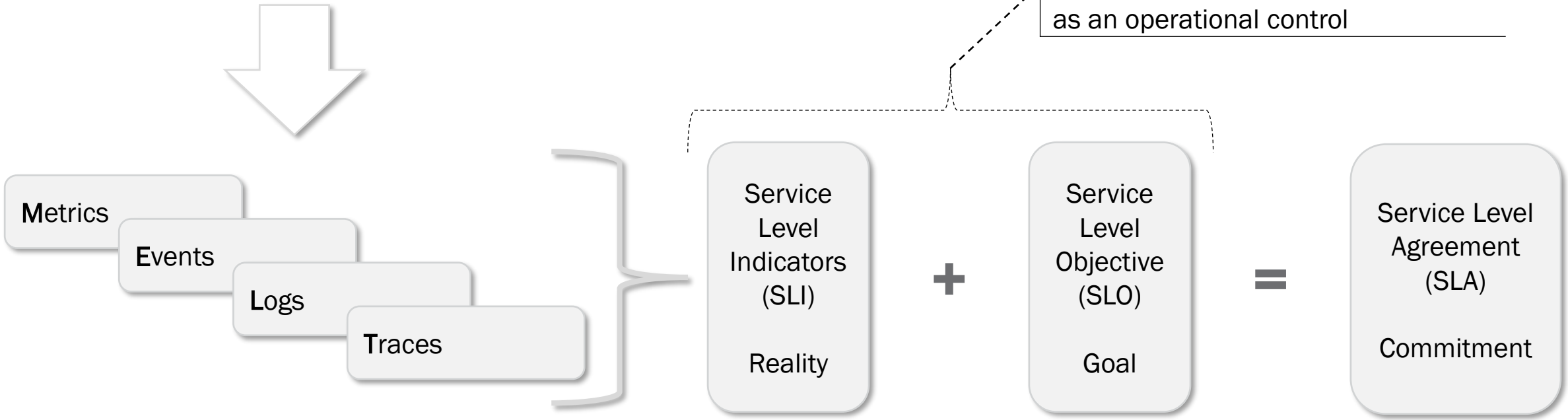
What is observability?

Single pane of glass

- Is the environment healthy or not?
- What is normal or anomalous?
- Is the environment efficient?
- What does any of this mean?



Align each combination with policy, technical and governance combine as an operational control

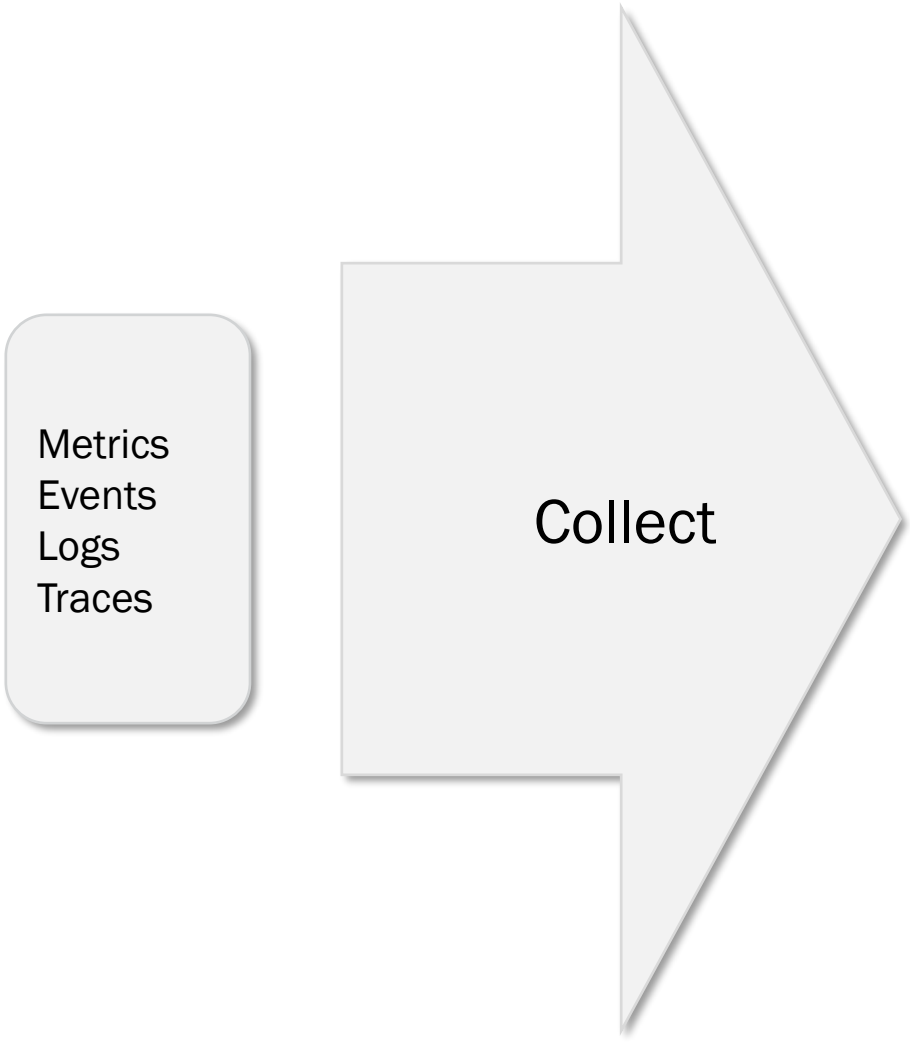


- What is observability?
- How can I apply it?
- How do I measure?
- How can I act on it?

How can we apply it?

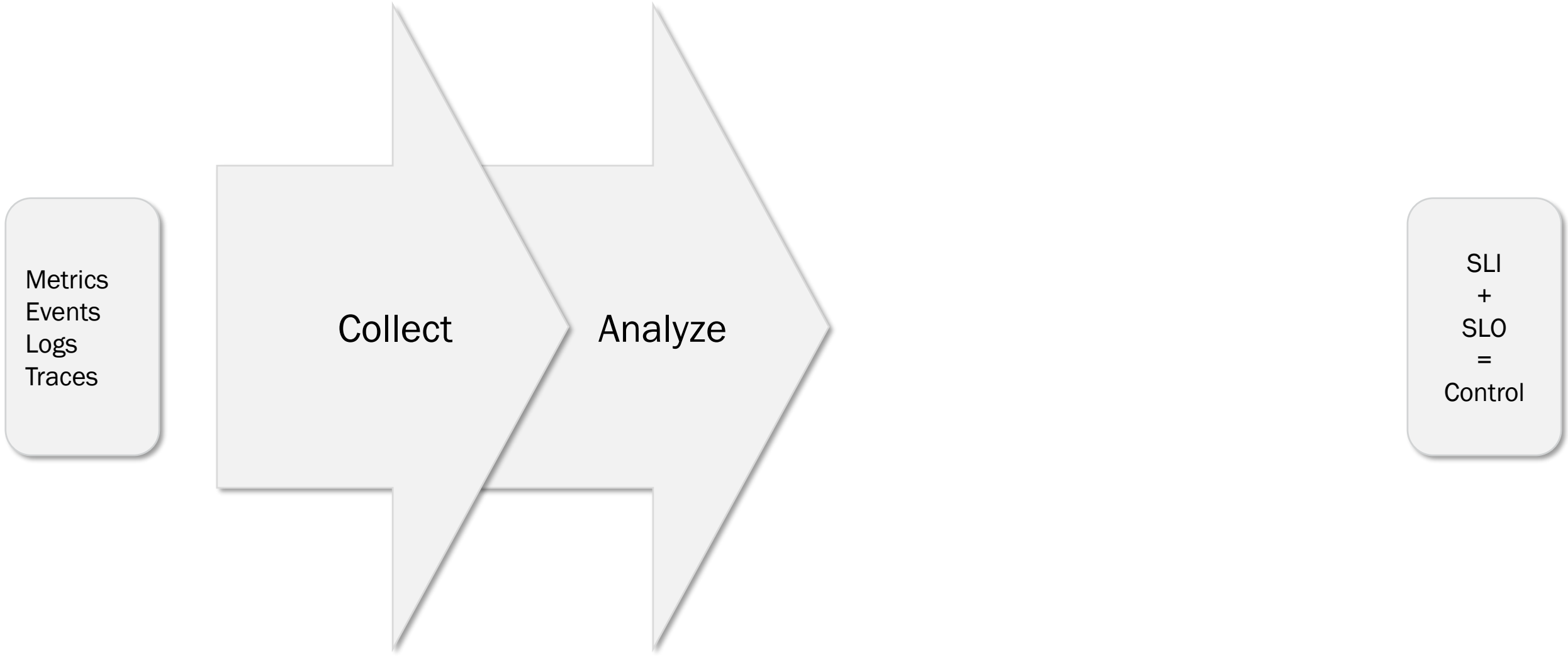
SLI
+
SLO
=
Control

How can we apply it?

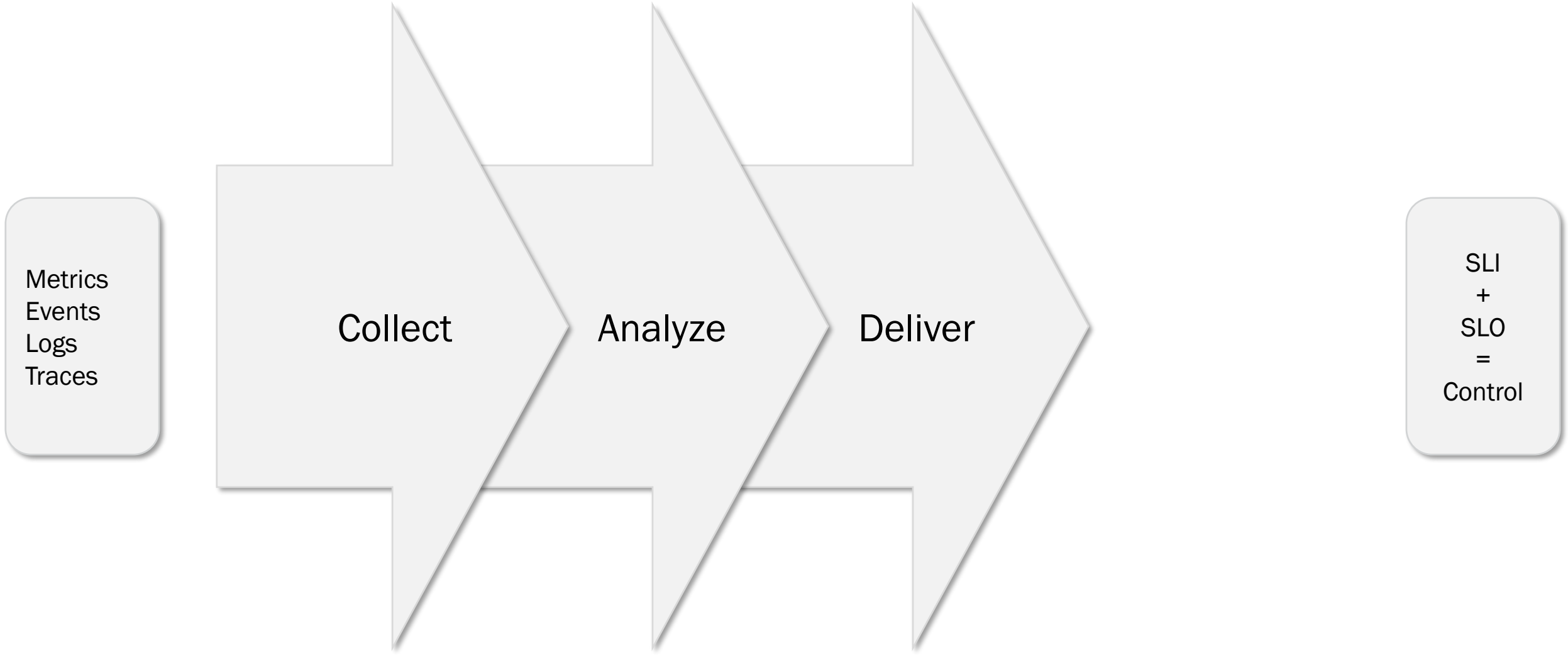


SLI
+
SLO
=
Control

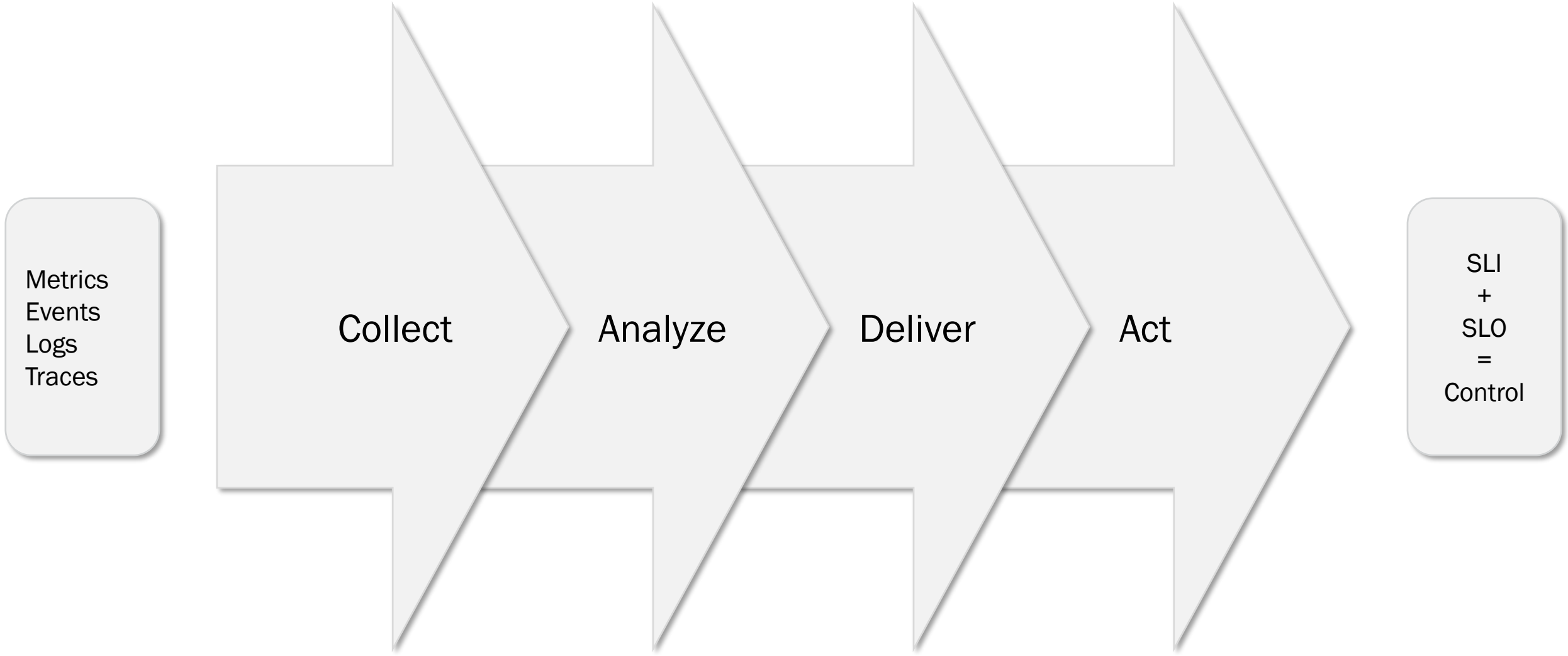
How can we apply it?



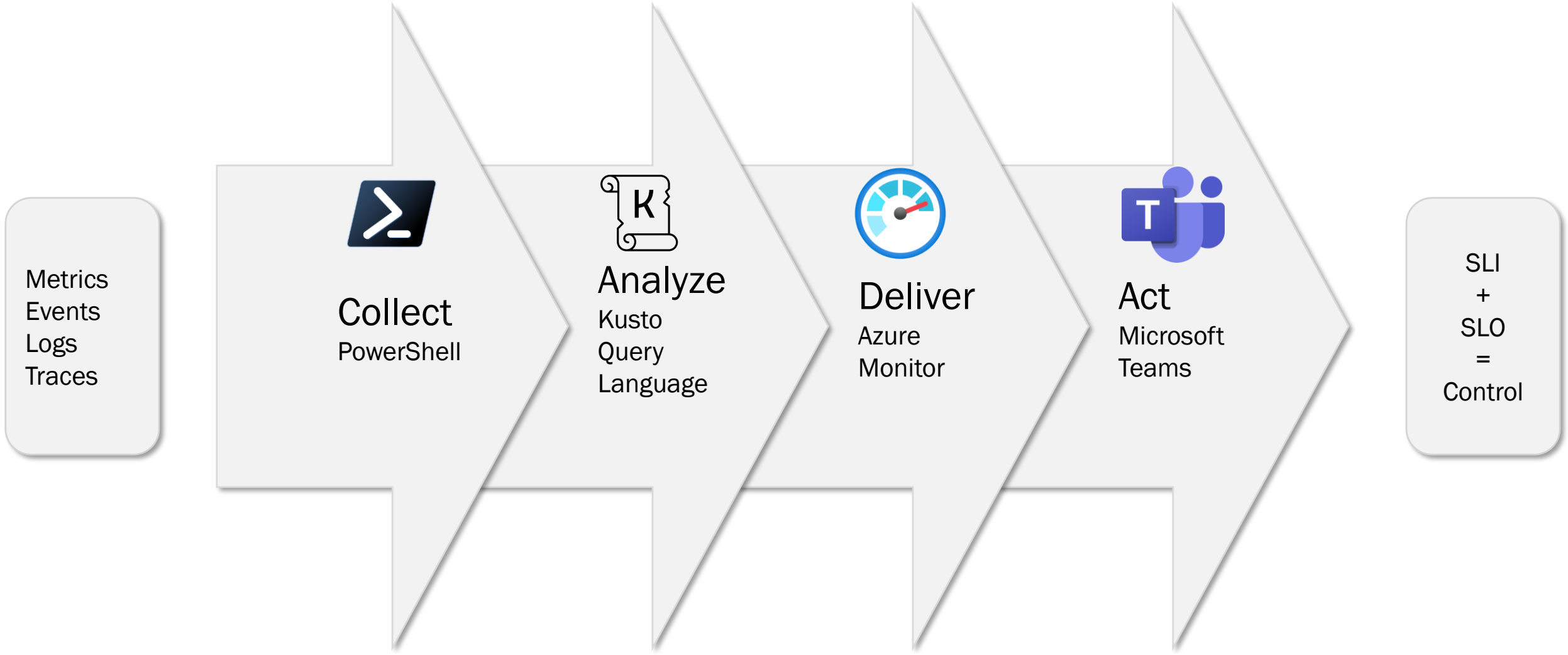
How can we apply it?



How can we apply it?



How can we apply it?

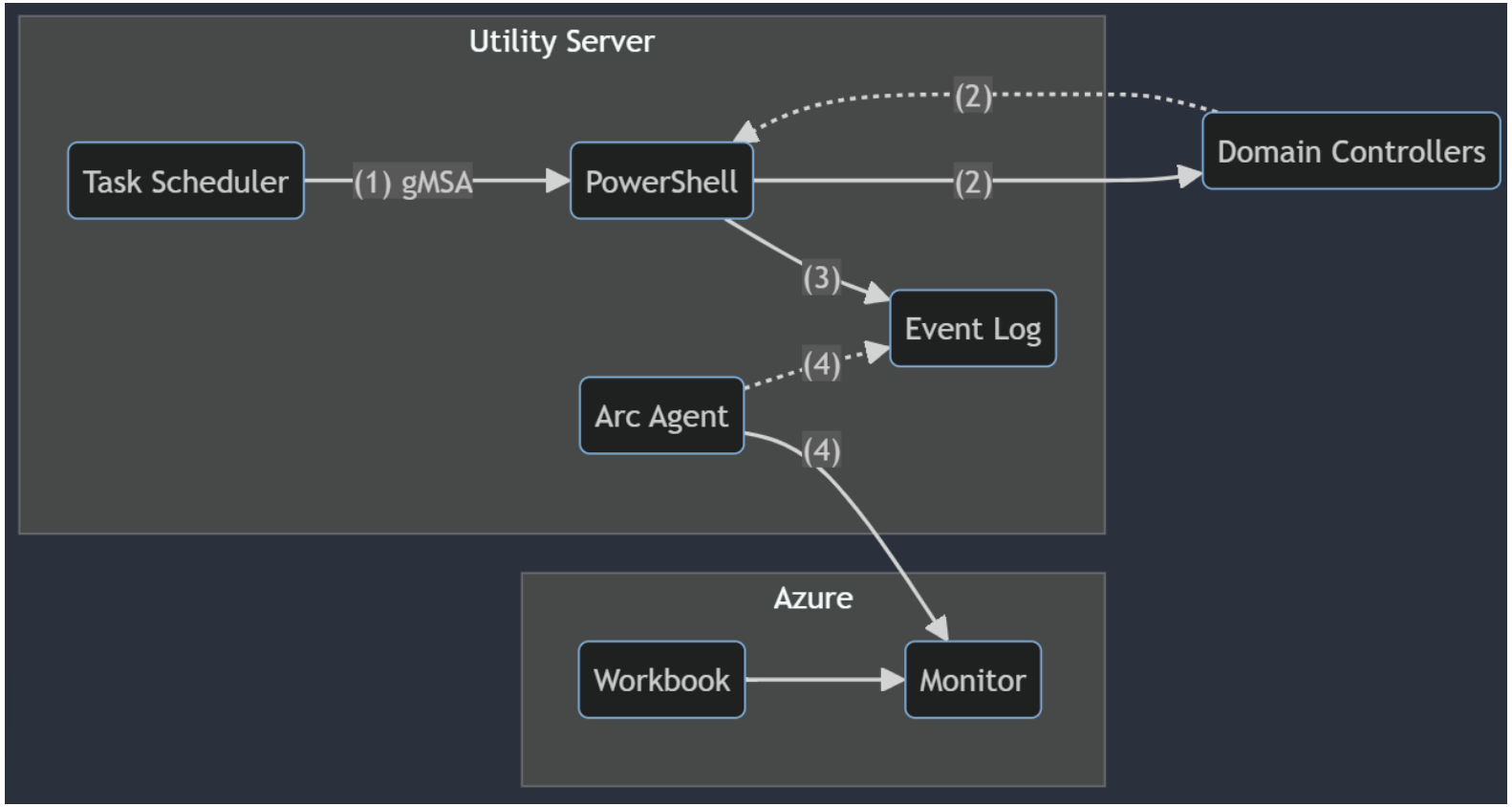


- What is observability?
- How can I apply it?
- How do I measure?
- How can I act on it?

How do I measure?

MELT

Collect



Controls (SLI + SLO)

How do I measure?

MELT

Collect

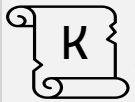
```
[…]`$(Get-ObsAdds400)}`""

$principal = New-ScheduledTaskPrincipal -UserId
"DEMO\Observability$" -RunLevel Highest -LogonType
Password

Register-ScheduledTask "Get-ObsAdds400" -TaskPath
"\Observability" -InputObject $task
```

Controls (SLI + SLO)

How do I measure?

MELT


Collect


Analyze

- Filter Event ID in Event Log for Domain
- Filter Group Policy Objects (GPO) with disabled status

```
Event
| where EventLog == "ObservabilityWithPowerShell"
| where EventID == 400
| project RenderedDescription
| extend detail=todynamic(RenderedDescription)
| where detail.Domain == '{Domain}'
| where detail.GpoStatus == 0
```

Controls (SLI + SLO)

How do I measure?

MELT

Collect

Analyze

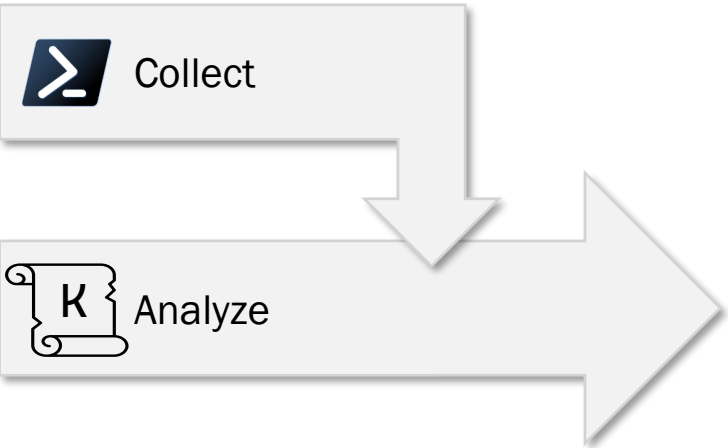
Controls (SLI + SLO)

- Filter Most Recent Event ID in Event Log for Domain
- Filter Group Policy Objects (GPO) with disabled status
- Filter disabled GPOs that haven't been recently modified

```
[…]
| extend modifed=unixtime_seconds_todatetime(tolong(repl
ace(@"\D", "", tostring(detail.ModificationTime)))/1000)
| extend days=datetime_diff('day',now(),modifed)
| extend detail.DisplayName, detail.Owner
| distinct tostring(detail_Owner),
tostring(detail_DisplayName), days
| where days >= 3
```

How do I measure?

MELT



Controls (SLI + SLO)

- Filter Most Recent Event ID in Event Log for Domain
- Filter Group Policy Objects (GPO) with disabled status
- Filter disabled GPOs that haven't been recently modified
- Count number of GPOs by owner

```
[…]
| summarize count(detail_DisplayName) by
tostring(detail_Owner)
| extend title="Number of stale & disabled policies"
```

How do I measure?

MELT

Collect

Analyze

Deliver

Controls (SLI + SLO)

User & Computer Configuration

Number of stale & disabled policies

1

DEMO\Domain Admins

get-gpo.json.01

Description: The number of Group Policy Objects by Owner that are disabled without modification in the past 3 days.

Governance: Disabled resources *must* be deleted within 3 days if unused.

Technical: Configure scheduled task to delete objects.

- What is observability?
- How can I apply it?
- How do I measure?
- How can I act on it?

How can I act on it?

MELT

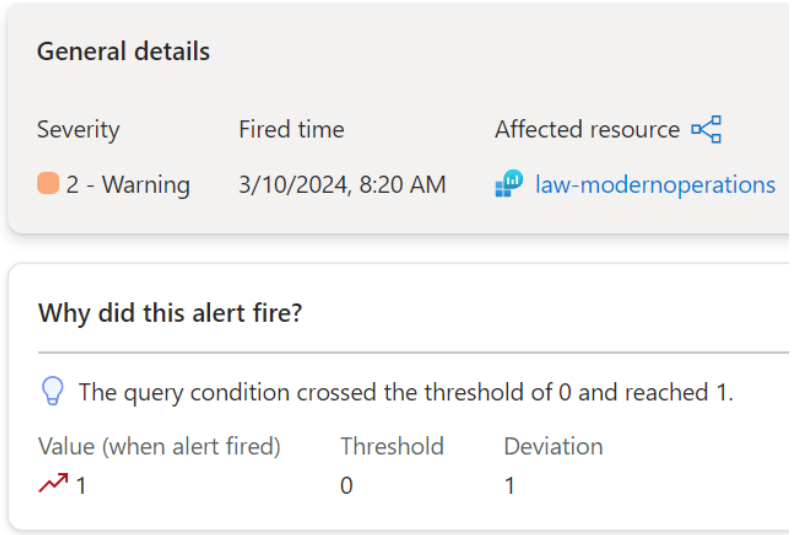
Collect

Analyze

Deliver

Act

Controls (SLI + SLO)



How can I act on it?

MELT

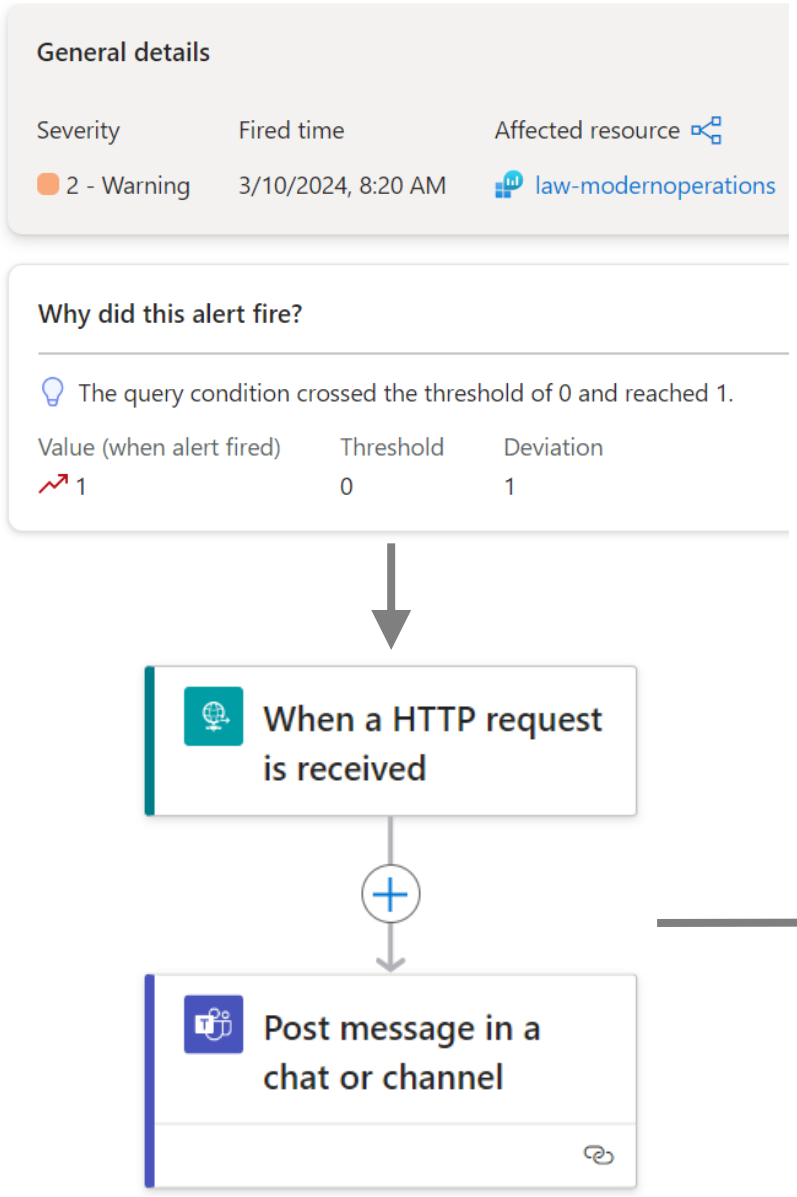
Collect

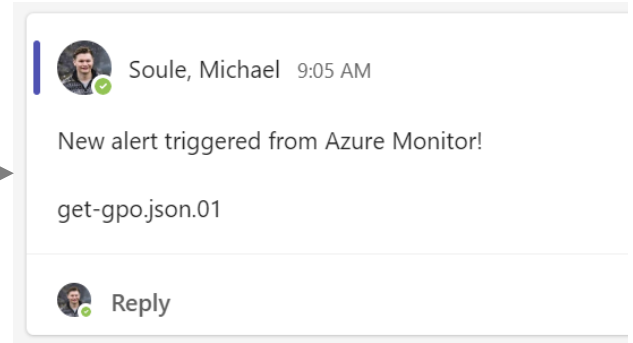
Analyze

Deliver

Act

Controls (SLI + SLO)





Linkedin.com/in/mikesoule/

How can I act on it?

MELT

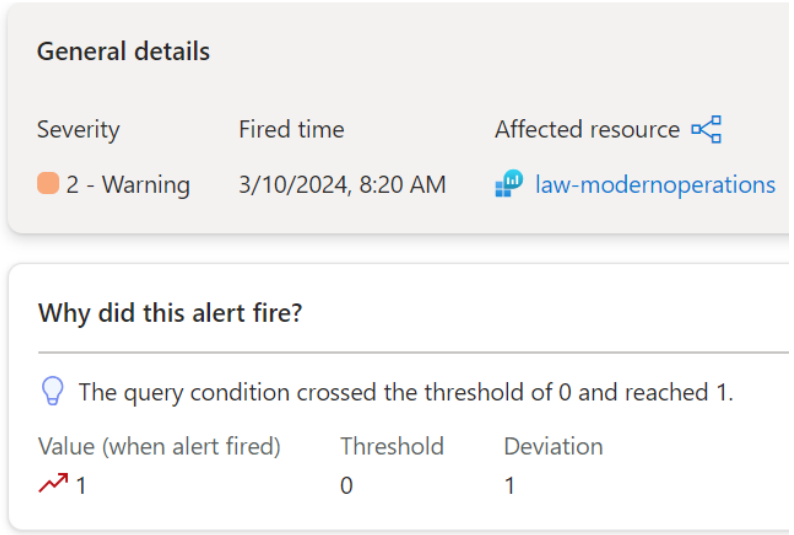
Collect

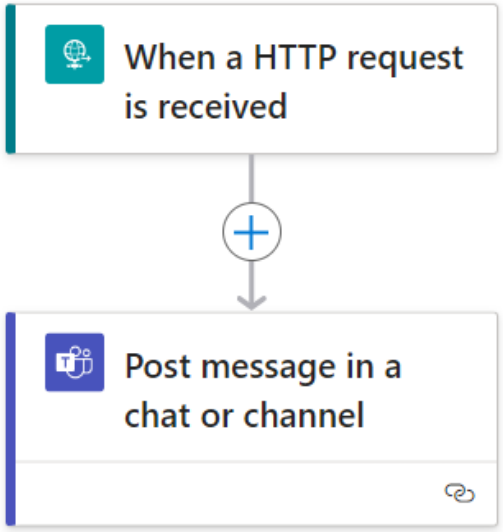
Analyze

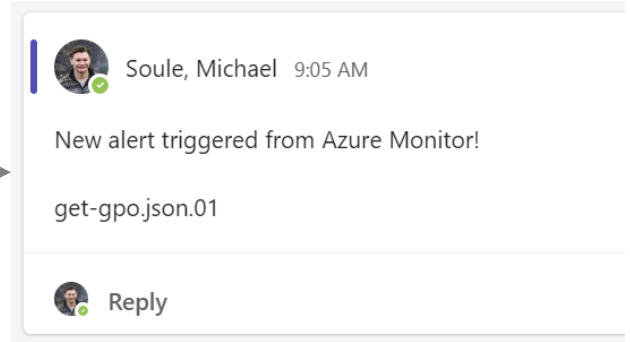
Deliver

Act

Controls (SLI + SLO)



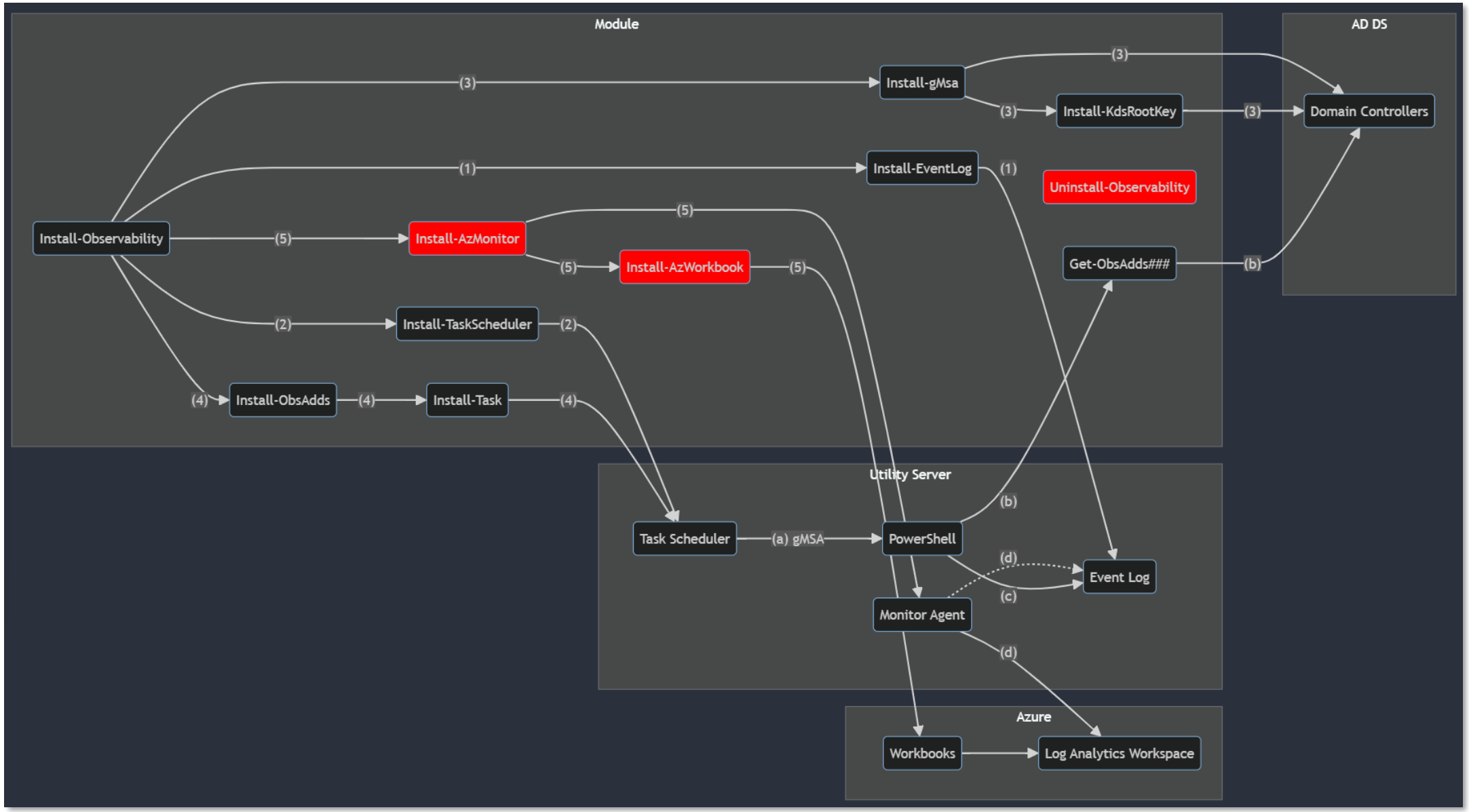




- Create a case automatically in your ITSM
- Integrate Azure Open AI to suggest KBs or similar past cases
- Trigger self-healing

- What service are you managing?
- What is optimal management?

Linkedin.com/in/mikesoule/


Module
AD DS
Install-gMsa
Install-KdsRootKey
Domain Controllers
Install-EventLog
Uninstall-Observability
Install-Observability
Install-AzMonitor
Install-AzWorkbook
Get-ObsAdds###
Install-TaskScheduler
Install-ObsAdds
Install-Task
Utility Server
Task Scheduler
(a) gMSA
PowerShell
Event Log
Monitor Agent
Azure
Workbooks
Log Analytics Workspace

Who is Michael Soule?

Michael Soule
National Director
Sentinel Technologies
misoule@sentinel.com

SENTINEL®

FORTIS By Sentinel
Advancing Your Protection

- Migration & Modernization
- Identity & Security
- Hybrid Cloud
- Licensing & Cost Optimization

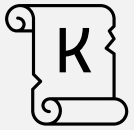
Linkedin.com/in/mikesoule/


PURESTORAGE®
ScriptRunner®
The #1 for PowerShell Management
PDQ DataON
PATCH MY PC
MANNING
Chocolatey
SNIA
DMTF

How can we apply it?

Metrics
Events
Logs
Traces

Collect
PowerShell



Analyze
Kusto
Query
Language

Deliver
Azure
Monitor

Act
Microsoft
Teams

SLI
+
SLO
=
Control