Site Reliability Engineers (SREs)

- Chandan Gowda H S

SREs

- Site Reliability Engineers (SREs) sits at the intersection of software engineering and systems engineering. While there are potentially infinite permutations and combinations of how infrastructure and software components can be put together to achieve an objective,
- focusing on foundational skills allows SREs to work with complex systems and software,
- SREs bring in engineering practices to keep the site up.

Reliability

- Most important: does the product work?
- Reliability is the absence of errors.
- Unstable service likely indicates a variety of issues.
- Must attend to reliability all the time

SREs

- Define availability
- * SLO : Service level objective
- Determine level of availability
- * SLI : Service level indicator
- Details what happens when availibility fails
- * SLA : Service level agrement

SLO(Service level objective)

"Service level objectives(SLOs) specify a target level for the reliability of your service."

SLOs are tied to your SLIs

- Measured by SLI
- Can be a single target value or range of values
- Comman SLOs :99.5%,99.9%,99.99%.

- SLI(Service level indicator)

"A carefully defined quantitative measure of some aspect of level of service that is provided"

SLIs are metrics over time – specific to user journey such as request/response, data processing, or storage that show how well a service is doing.

Examples SLIs:

- Request Latency – How long it takes to return a response to a request.
- Failure Rate – A fraction of all rates recived. (unsucessfull / all request).
- Batch Throughput – Proportion of time = data processing rate > than a threshold

SLAs

"An Explicit or Implicit contract with your users that includes consequences of meeting (or missing) the SLOs they contains"

SLA Characteristics

- A Bussiness level agreement
- Can be explicit or implicit
- Explicit contract contain consequences
- * Refund for the service paid for
- * Service cost reduction on sliding scale
- May be offered on a per service basicss

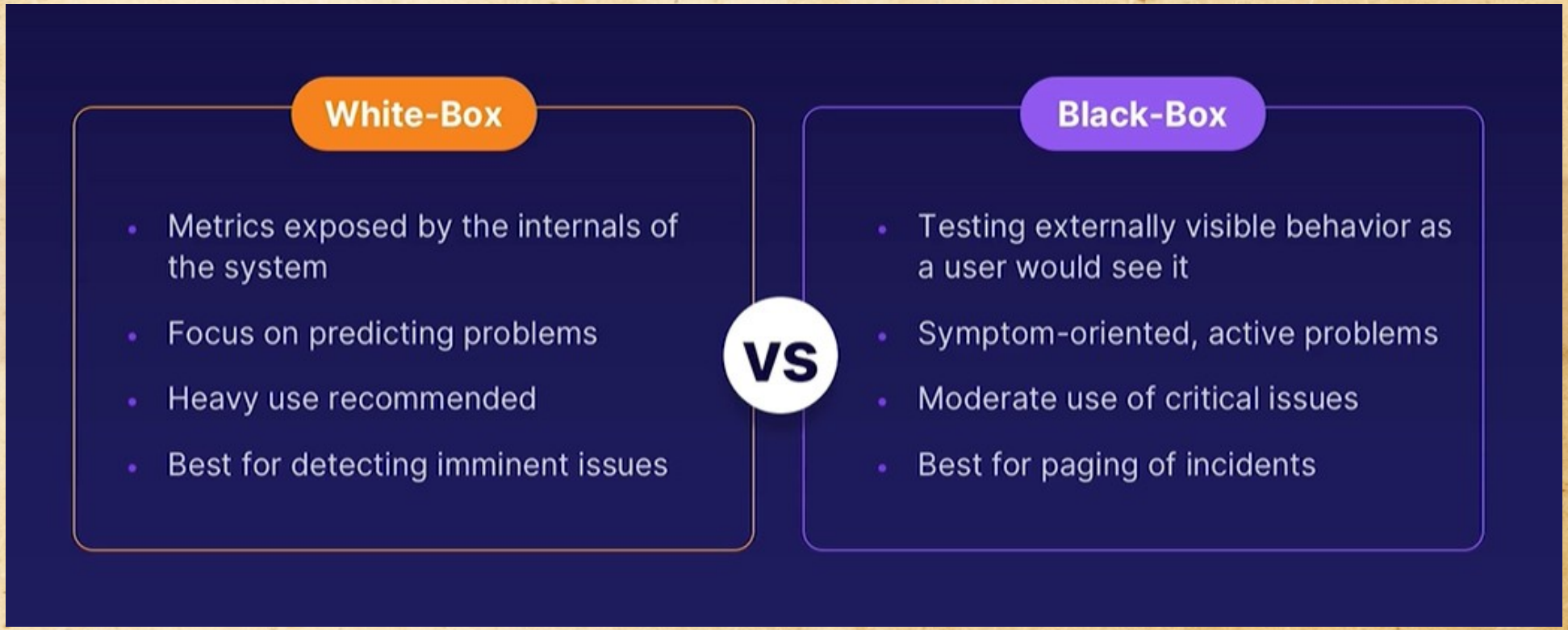
Monitoring

“Collecting, processing, aggregating, and displaying real-time quantitative data about system, such as query count and types, error count and types,processing times, and server lifetimes.”

Why Monitor?

- Analyzing the long-term trends
- Comparing over time groups
- Alerting
- Exposing in dashboard
- Debugging
- Security breach analysis

White box and black box monitoring



Alerts

“Alerts gives timely awarencess problems in your cloud application so you can resolve proble quickly”

How Alerts working

1) Set up monitoring

Conditions are continously monitoring.

Monitoring can track SLOs.

Can look for missing metrics.

Can watch for the thresholds.

2) Track metrics over time

- Track if condition persists for given amount of time
- Time windows less than 24 hours

- 3)Notify when condtion is passed
- Incedent created and displayed
- Alert can be sent via
- Email
- SMS text message

Some of sre investeble tool in dev

- Kubernites engine
- Container registry
- Cloud build
- Cloud source repository
- Spinnaker for google cloud
- Cloud monitoring
- Cloud Logging
- Cloud debugger
- Cloud trace
- Cloud profiler

SRE Team

Application Support

Environment Support

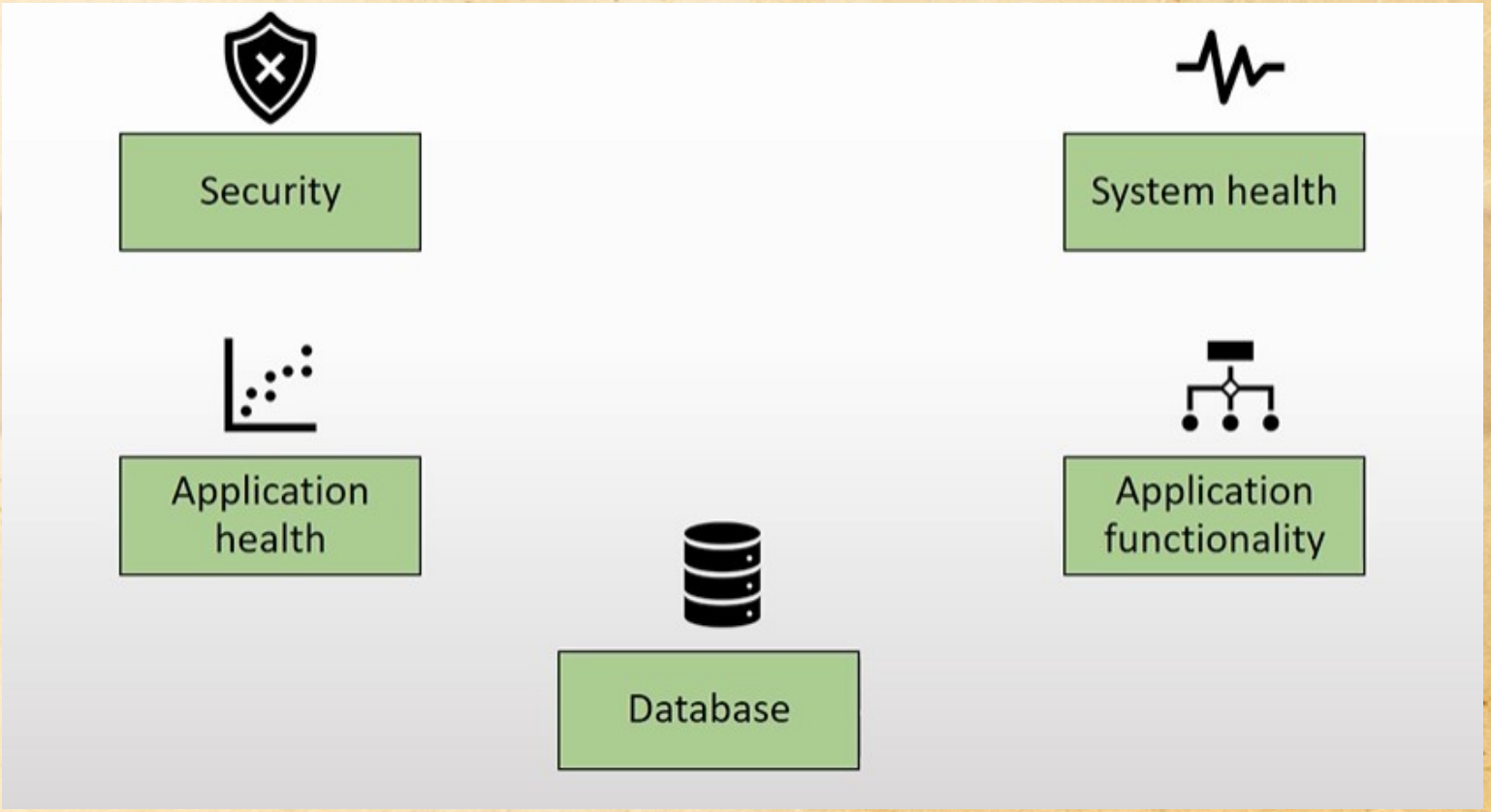
Change Management

Incident Management

SRE - Responsibility

- Application health monitoring
- Capacity Planning
- Change management and communication
- Retrospective
- Incident management and communication
- SLA
- SOP

Vertical Monitoring



Verticals of monitoring – Security

KPIs of security monitoring

- Accounts & credentials
- Infrastructure access
- Phishing attack pattern
- Access from unusual location
- Unauthorized deployment
- Pattern of APIs access incidents
- Intrusion attempts

How to monitor

- SPI(Sensitive Personal Information) data encryption
- Failed login attempts threshold monitoring
- Geolocation mapping from IP
- Error codes
- Vulnerability scanning

Tools




Verticals of monitoring – System health

Structural system health monitoring


CPU utilization


Server ping test


Server load average


File system usage


Memory utilization


Network


Firewall

How to monitor

Server performance

- Percentage of CPU utilization
- Load average
- Percentage of memory utilization

Server response

- Ping test – data packet loss
- Percentage of file system used
- Network – data loss between source and destination
- Firewall access log

Tools

Nagios

Azure Monitor

Grafana

Amazon Cloudwatch

AppDynami

SF

Verticals of monitoring – Application functionality

Metrics of functional monitoring

Application flow

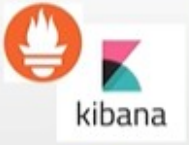
API response

How to monitor

Application flow
- Business logic
- Error code

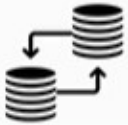
API response
- Response time
- Failure rate
- Anomaly detection

Tools



Verticals of monitoring – Database

Critical database monitoring elements



Replication lag

Open connection

IOPS

Expensive query

Throughput

Space usage

Error

How to monitor

Performance

- Data replication lag
- Number of open connections
- IOPS
- Long running DB queries
- DB throughput
- DB storage usage percentage

Health

- DB connection error
- DB VM monitoring

Tools

Amazon Cloudwatch

ORACLE ENTERPRISE MANAGER

splunk>

Nagios

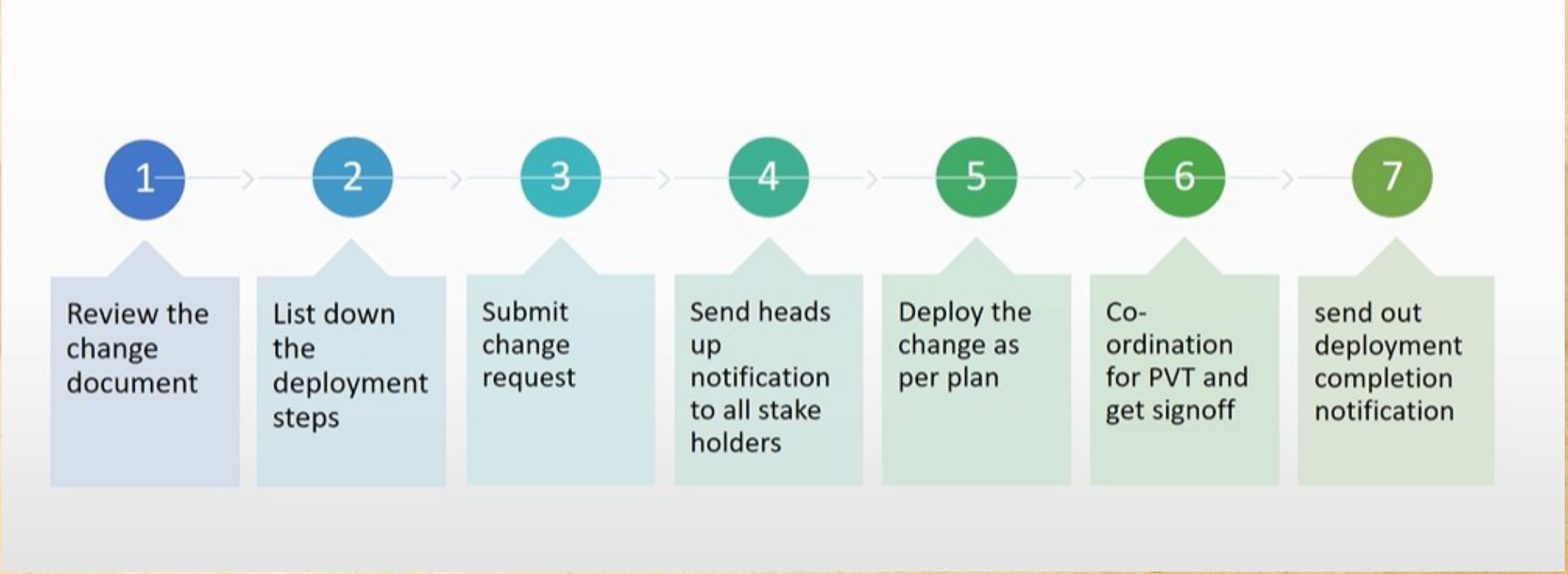
Incident management

The purpose of incident management process is to restore normal service Operation as quickly as possible and minimize the adverse impact on bussiness operations, ensuring that agreed levels of service quality are Maintained.

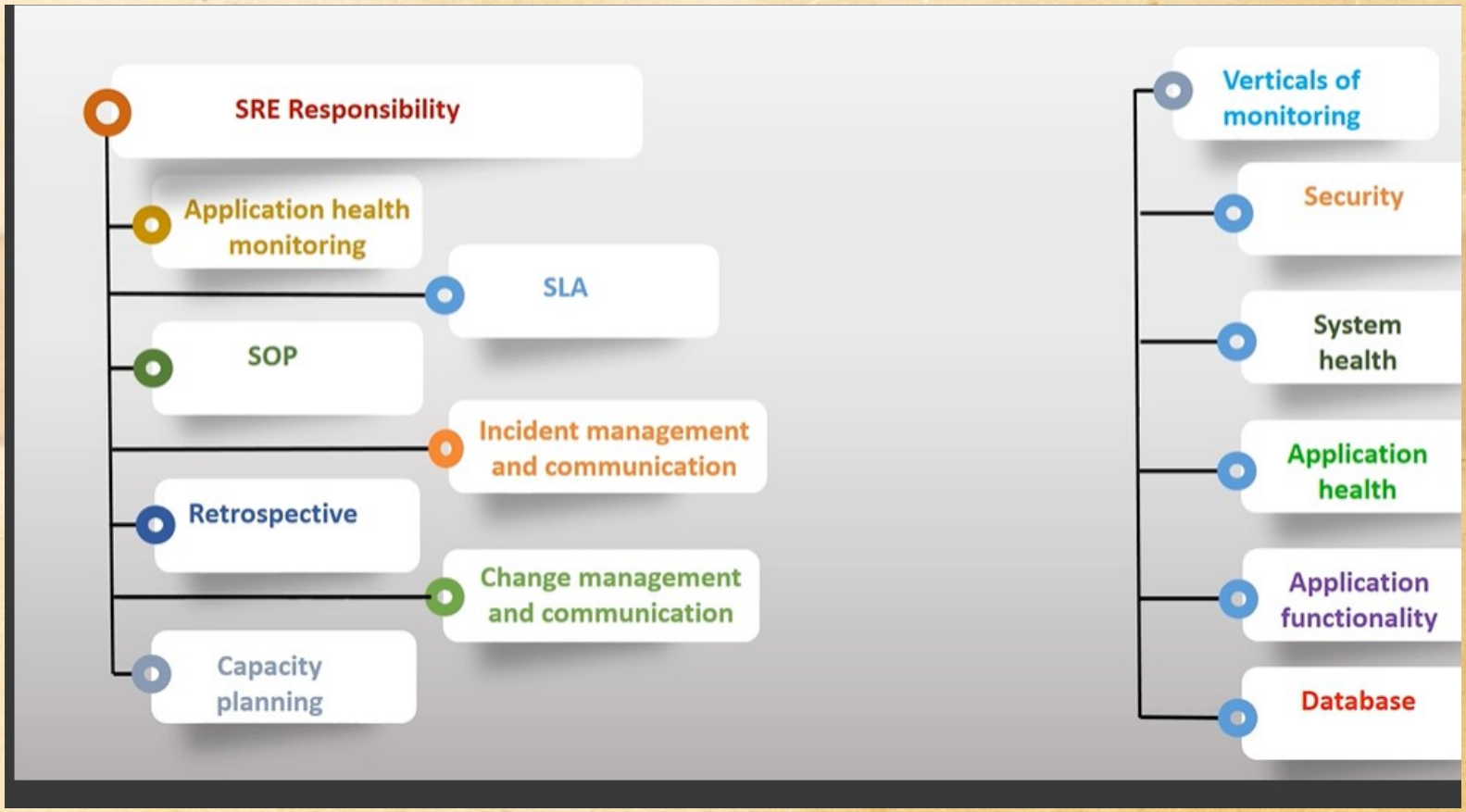
How to achive:

- Alert acknowledge
- Identify severity
- Follow SOP
- Bussiness impact assessment
- Notification of issue to stake holders

Change management



Summary


SRE Responsibility
Application health monitoring
SLA
SOP
Incident management and communication
Retrospective
Change management and communication
Capacity planning
Verticals of monitoring
Security
System health
Application health
Application functionality
Database

Monitor tools

Purpose

- Capture metrics from application
- Compare it with alerting condition
- Trigger email/ticket if condtion is meet
- Build dashboard on these tools for graphical represention of data
- **Log monitor tool**
- Splunk (licensed)
- Kiban (open source)

Security monitoring tool

- Solorwinds
- Intruder
- **System health and monitoring tools**
- Grafana and prometheus
- Nagios
- **Database monitoring tool**
- Oracle enterprise manager
- Solarwinds