Microsoft

WorkshopPLUS: DevOps Fundamentals

Module 4: Learn

Conditions and Terms of Use

Microsoft Confidential

This training package is proprietary and confidential and is intended only for uses described in the training materials. Content and software is provided to you under a Non-Disclosure Agreement and cannot be distributed. Copying or disclosing all or any portion of the content and/or software included in such packages is strictly prohibited.

The contents of this package are for informational and training purposes only and are provided "as is" without warranty of any kind, whether express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement.

Training package content, including URLs and other Internet website references, is subject to change without notice. Because Microsoft must respond to changing market conditions, the content should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

Copyright and Trademarks

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

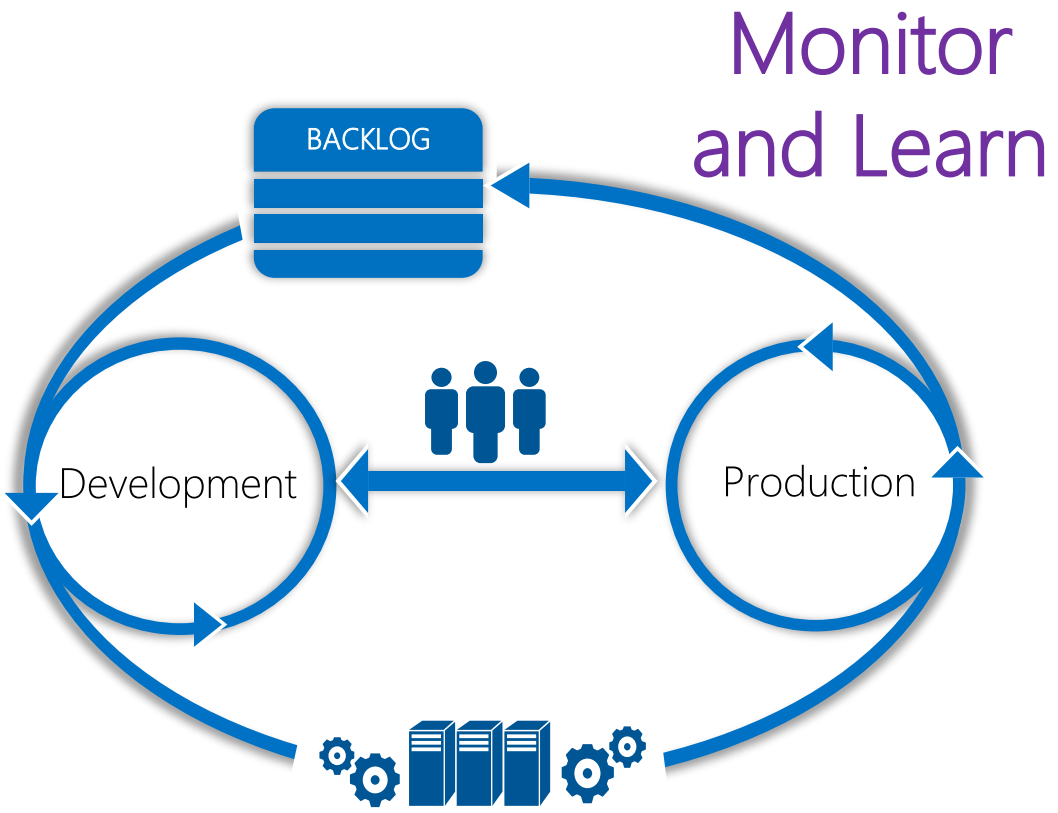
Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

For more information, see **Use of Microsoft Copyrighted Content** at
https://www.microsoft.com/en-us/legal/intellectualproperty/permissions/default.aspx

Microsoft®, Internet Explorer®, Outlook®, SkyDrive®, Windows Vista®, Zune®, Xbox 360®, DirectX®, Windows Server® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other Microsoft products mentioned herein may be either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are property of their respective owners.

Module Objectives

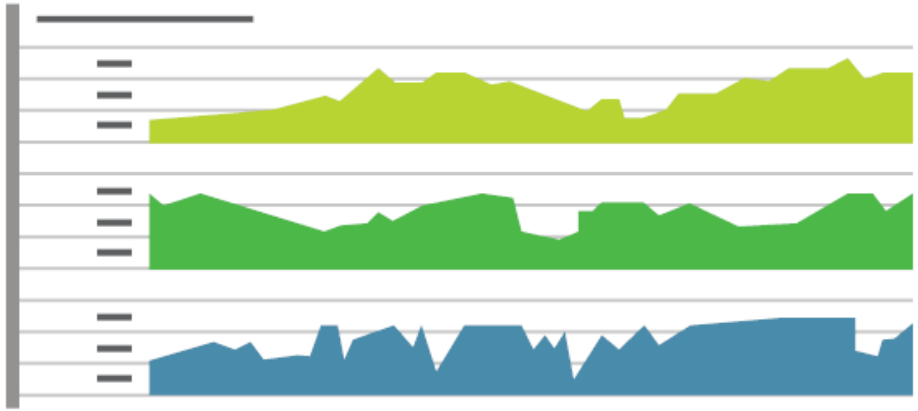
- Understand the importance of application monitoring
- Learn how to incorporate monitoring into your application
- See how to enable a validated learning process



Application Monitoring

What is Application Monitoring?

- Monitoring provides feedback from production and delivers information about an application's performance and usage patterns
- Usage patterns help project problematic times or trends, for example a regular pattern showing a surge in traffic from 8AM – 9AM
- Can also show longer patterns such as monthly report executions slowing down the system

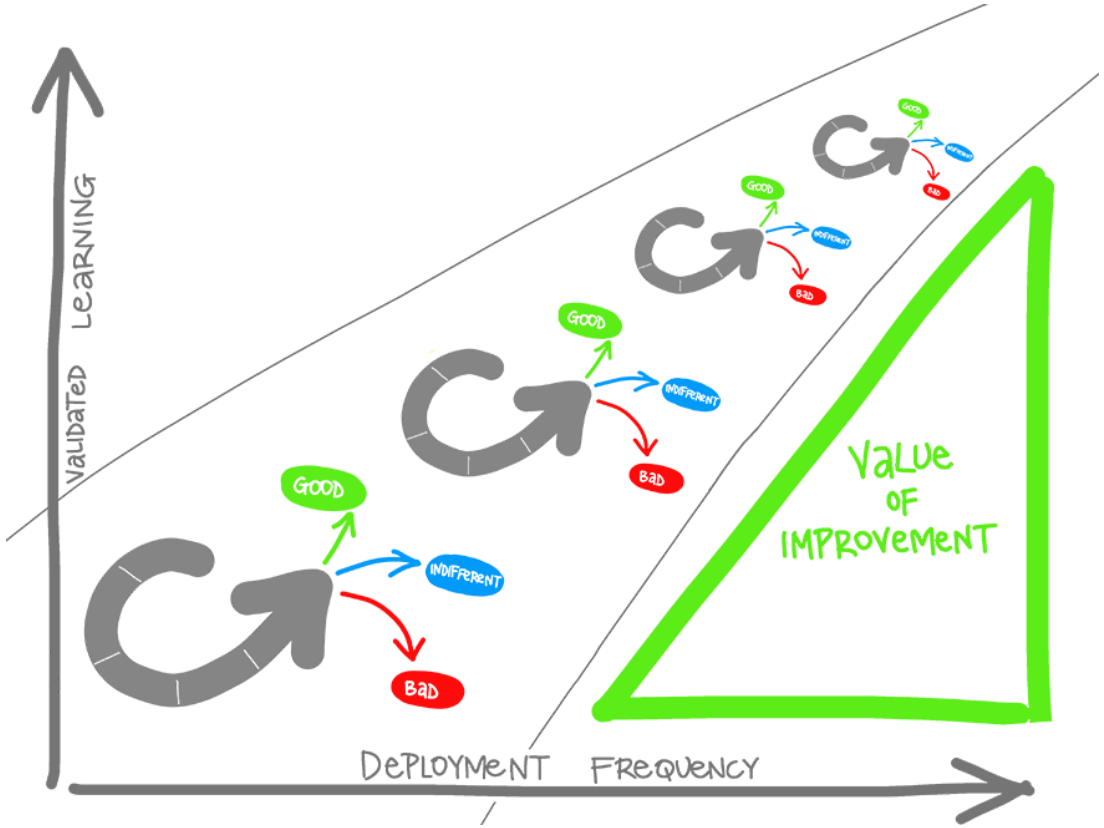


Application Monitoring Goals

- Achieve high availability by minimizing time to detect (TTD), and time to mitigate (TTM)
  - As soon as an issue is detected, rich diagnostic data about the issue is fed to the development team *through* application monitoring (**TTD**)
  - Teams act on the information to mitigate (resolve) the issue as quickly as possible so that customers are not affected (**TTM**)
- Enable "validated learning" by tracking usage. Every deployment is a chance to track experimental results that support or diminish the hypothesis that led to the deployment (cycle time)

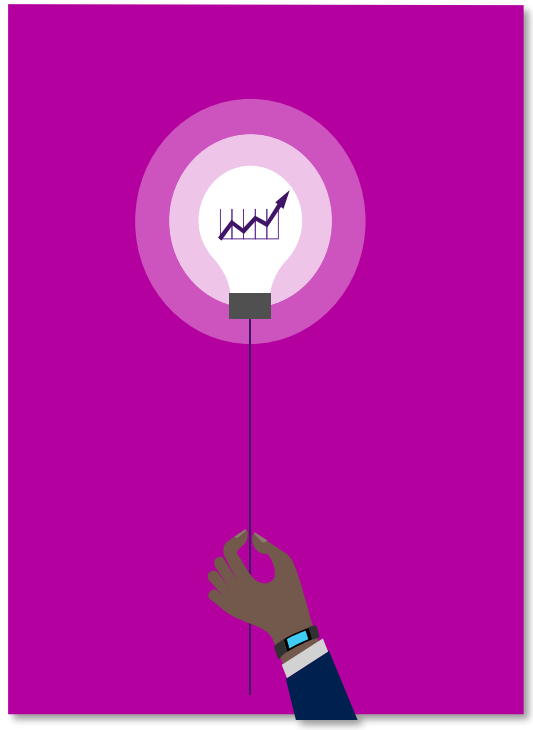
Validated Learning

- Each deployment is a chance to track experimental results
- Review these results and determine if the experiment was good, indifferent, or bad
- Track usage and differences between versions to measure the impact of change and drive business decisions
- Data-informed decisions lead to new work items and prioritization of the backlog



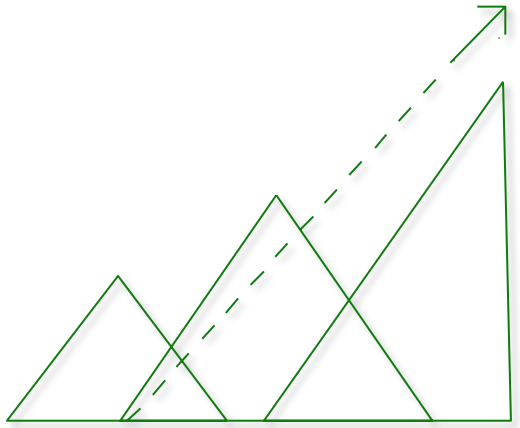
Telemetry

- Mechanism for collecting data from monitoring
- Agents can be used and installed in deployment environments to gather data from server logging, SDKs, or other sources



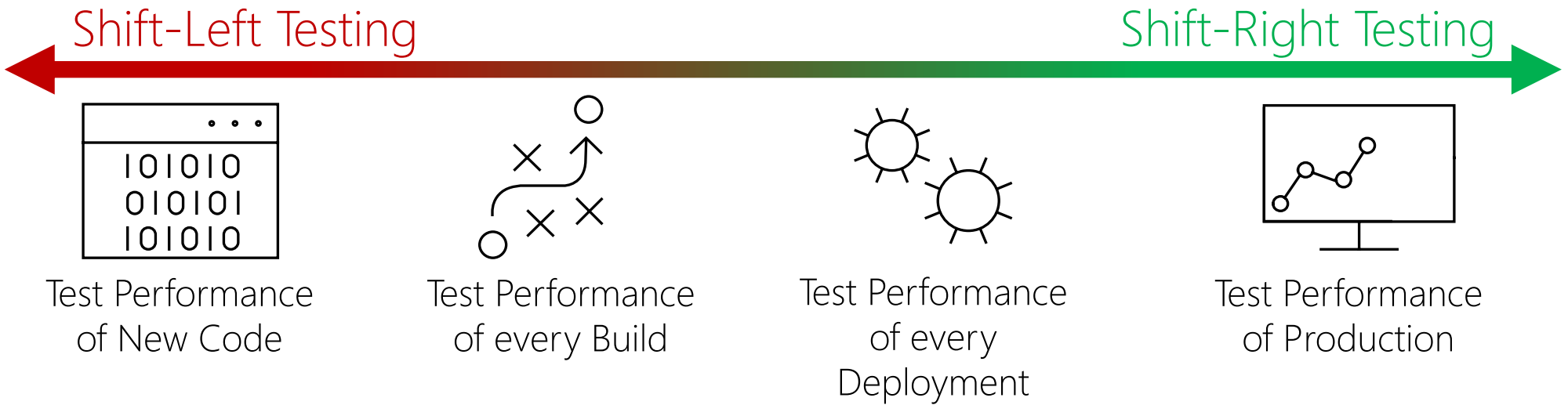
Synthetic Monitoring vs. Real-User Monitoring

- Synthetic Monitoring
  - uses a consistent set of transactions to assess performance and availability
  - predictable tests that have the advantage of allowing comparison from release to release
  - help with forming a baseline performance metric
- Real User Monitoring (RUM)
  - measures the experience from the user's browser, mobile device or desktop, and accounts for "last mile" conditions such as cellular networks, internet routing, and caching
  - Typically, does not provide repeatable measurement over time

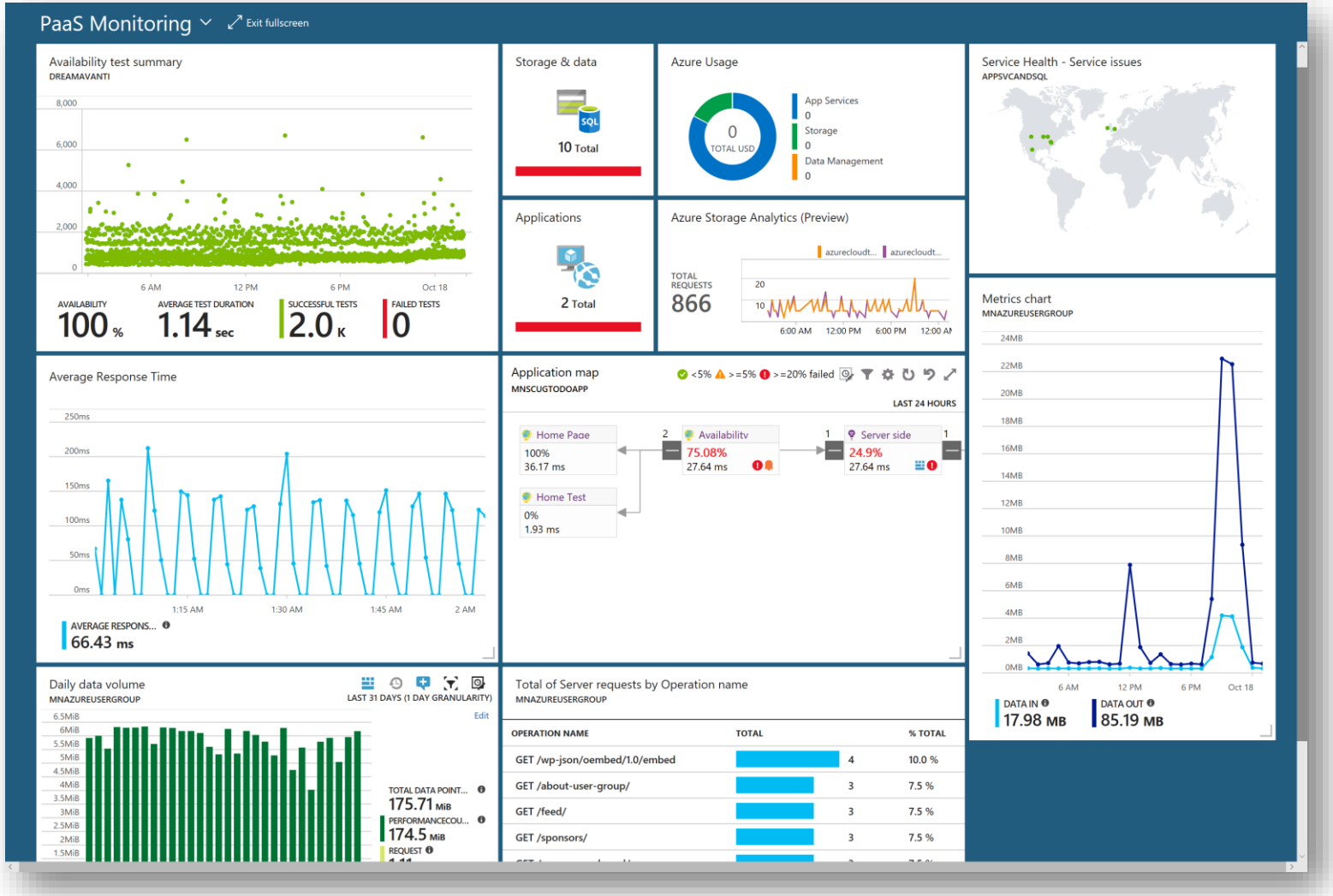


Shift-Right Testing

- A well-monitored deployment streams the data about its health and performance so that the team can spot production incidents immediately
- Monitoring will detect new anomalies and allow for prompt mitigation
- Adopt a pro-active approach and let telemetry and data point you in the right direction



Monitoring is Crucial in DevOps



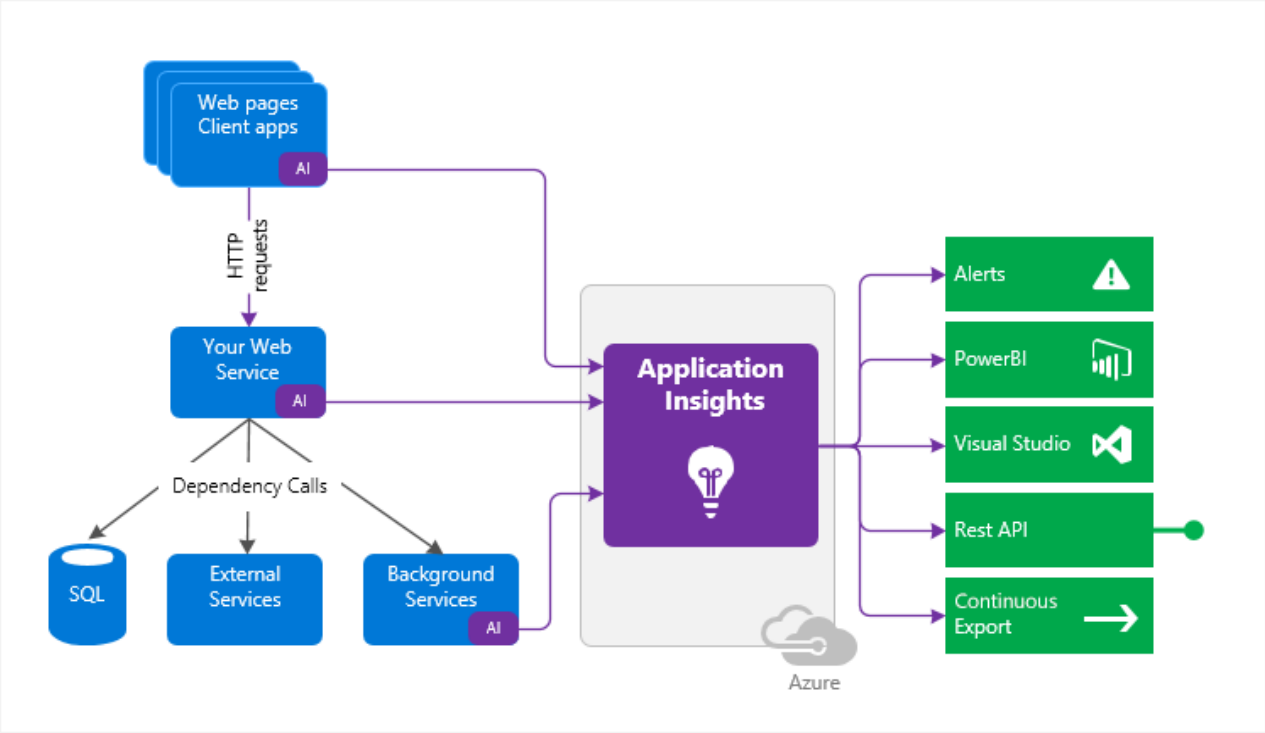
- Effective monitoring is essential to allow DevOps teams to deliver at speed, get feedback from production, and increase customers satisfaction, acquisition and retention

Introducing Application Insights

Application Insights, a feature of Azure Monitor, is an extensible Application Performance Management (APM) service for developers and DevOps professionals. Use it to monitor your live applications. It will automatically detect performance anomalies and includes powerful analytics tools to help you diagnose issues and to understand what users do with your application.

How does Application Insights Work?

- Install instrumentation package into your application
- Instrumentation monitors your application and directs telemetry data to Azure Application Insights using a GUID called an Instrumentation Key



Overhead

- Impact on your application is minimal
- Tracking calls are non-blocking
- Data is batched and sent on a separate thread

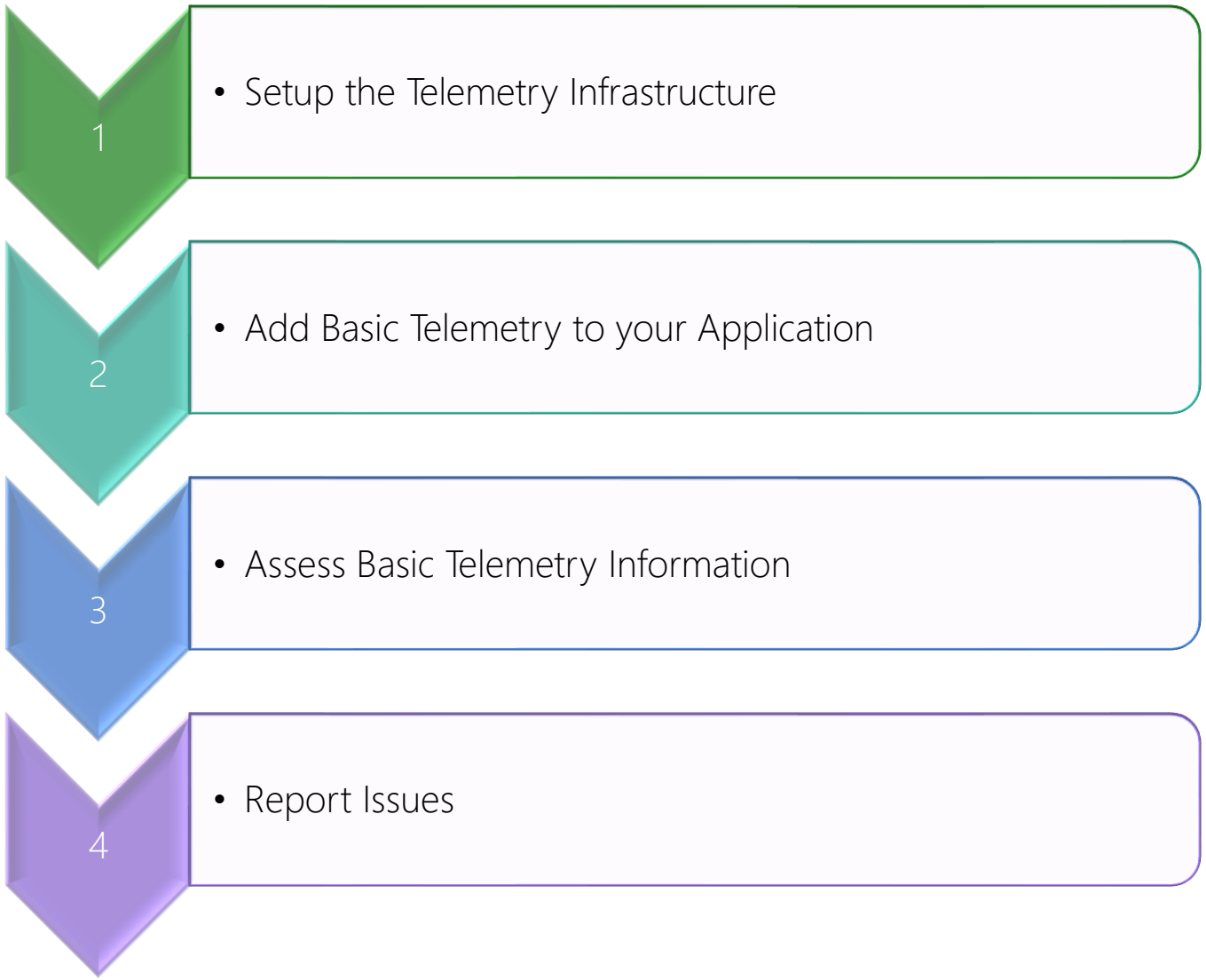
Monitors

- Request Rates, Response Times, and Failure Rates
- Dependency Rates, Response Times and Failure Rates
- Exceptions
- Page Views
- Performance Counters
- Users and Session Counts
- Host Diagnostics from Azure or Docker
- Custom events and more

Demonstration: Application Monitoring

We will use Application Insights to monitor the health and usage of your application.

Demonstration Review



Module 4: Learn

Lab 7: Application Monitoring

Exercise 1: Setup Telemetry Infrastructure
Exercise 2: Add Telemetry to the Application
Exercise 3: Assess Basic Telemetry Information
Exercise 4: Report Issues

Lab Time: 60 minutes (about 1 hour)

Knowledge Check

Question #1: What is Validated Learning?

Quantifiable; based on data such as revenue, user engagement, and feedback. The result is learning that is evidence-based and actionable, leading to genuine product improvements in each iteration or sprint.

Question #2: What is Time to Detect (TTD)?

Or Mean Time to Detect (MTTD), is a key performance indicator (KPI) metric for IT Incident Management and refers to the average amount of time it takes to discover an issue.

Question #3: What is Time to Remediate (TTR)?

Or Mean Time to Remediate, refers to the time it takes to fix a failed system.