RITM = (Request Item)

SCTASK = SC Task (Service Catalog Task)

What is Incident? ==>

“An unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet affected service is also an incident – for example, failure of one disk from a mirror set.”

What is Service Request? ==>

A Service Request is not a Request for Help (an incident) ➢ Service Request = Ordering Something (software, new desktop, access to a system, system privileges) ➢ Incident = Reporting an issue with technology, e.g., network outage, desktop computer doesn't turn on, password reset, etc.

What is Task Sequence in SCCM?

Task sequences in SCCM are used for applying images, configuring windows, installing drivers, installing applications, and installing application packages.

What is CM Trace?

CM Trace is one of the Configuration Manager tools. It allows you to view and monitor log files, including the following types: Log files in Configuration Manager or Client Component Manager (CCM) format. Plain ASCII or Unicode text files, such as Windows Installer logs.

| Priority Data lookup rules | | |
| --- | --- | --- |
| **Impact** | **Urgency** | **Priority** |
| 1 - High | 1 - High | 1 - Critical |
| 1 - High | 2 - Medium | 2 - High |
| 1 - High | 3 - Low | 3 - Moderate |
| 2 - Medium | 1 - High | 2 - High |
| 2 - Medium | 2 - Medium | 3 - Moderate |
| 2 - Medium | 3 - Low | 4 - Low |
| 3 - Low | 1 - High | 3 - Moderate |
| 3 - Low | 2 - Medium | 4 - Low |
| 3 - Low | 3 - Low | 5 - Planning |

| Incident states | |
| --- | --- |
| **State** | **Description** |
| New | Incident is logged but not yet investigated. |
| In Progress | Incident is assigned and is being investigated. |
| On Hold | The responsibility for the incident shifts temporarily to another entity to provide further information, evidence, or a resolution. When you select the On Hold option, the on hold reason list appears. If the On hold reason is Awaiting Caller, the Additional comments becomes mandatory.  Note: If the caller updates the incident, the On hold reason field is cleared and the state of the incident is changed to In Progress. An email notification is sent to the user whose name is mentioned in the Assigned to field as well as to the users in the Watch list. An incident can be placed in the On hold state one or more times prior to being closed. |
| Resolved | A satisfactory fix is provided for the incident to ensure that it does not occur again. |
| Closed | Incident is marked Closed after it is in the Resolved state for a specific duration and it is confirmed that the incident is satisfactorily resolved. |
| Canceled | Incident was triaged but found to be a duplicate incident, an unnecessary incident, or not an incident at all. |

What is UAT?

**User acceptance testing** (UAT) is the last phase of the software testing process. During UAT, actual software users test the software to make sure it can handle neccessary tasks in real-world scenarios, according to specifications

What is Windows ATP?

Windows Defender Advanced Threat Protection (ATP) is **a Microsoft security product that is designed to help enterprise-class organizations detect and respond to security threats**. ATP is a preventative and post-detection, investigative response feature to Windows Defender.

What is detection methods in SCCM?

In the Detection Rule dialog box, select a Setting type to detect the presence of the deployment type: File System: **Detect whether a specified file or folder exists on a device**. This detection indicates that the application is installed

What are logs in SCCM?

SCCM Logs are your best friend in Troubleshooting issues. SCCM logs are generated on the client and site server-side. The **client and server components record process information in individual log files.**

What is registry in server?

The registry or Windows registry is **a database of information, settings, options, and other values for software and hardware installed on all versions of Microsoft Windows operating systems**. When a program is installed, a new subkey is created in the registry.

Service Manager stores most registry values in the following locations: **HKEY\_CURRENT\_USER\Software\Microsoft\System Center<version>\Service Manager\Console**. **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\System Center<version>**

**Packages** are created the same way they are created in SCCM 2007, and the administrator only has about five screens to go through. Also, **management of the deployment of specific programs** is separated with packages. With applications, you are deploying all of the deployment types that you set up.

What does endpoint protection do?

Endpoint security is the practice of **securing endpoints or entry points of end-user devices such as desktops, laptops, and mobile devices from being exploited by malicious actors and campaigns**. Endpoint security systems protect these endpoints on a network or in the cloud from cybersecurity threats.

What is 3 strike rule in incident management?

There is 3 strike rule, which **sends users reminder each day for three days if state is awaiting user action and on no response, ticket should be auto closed**.