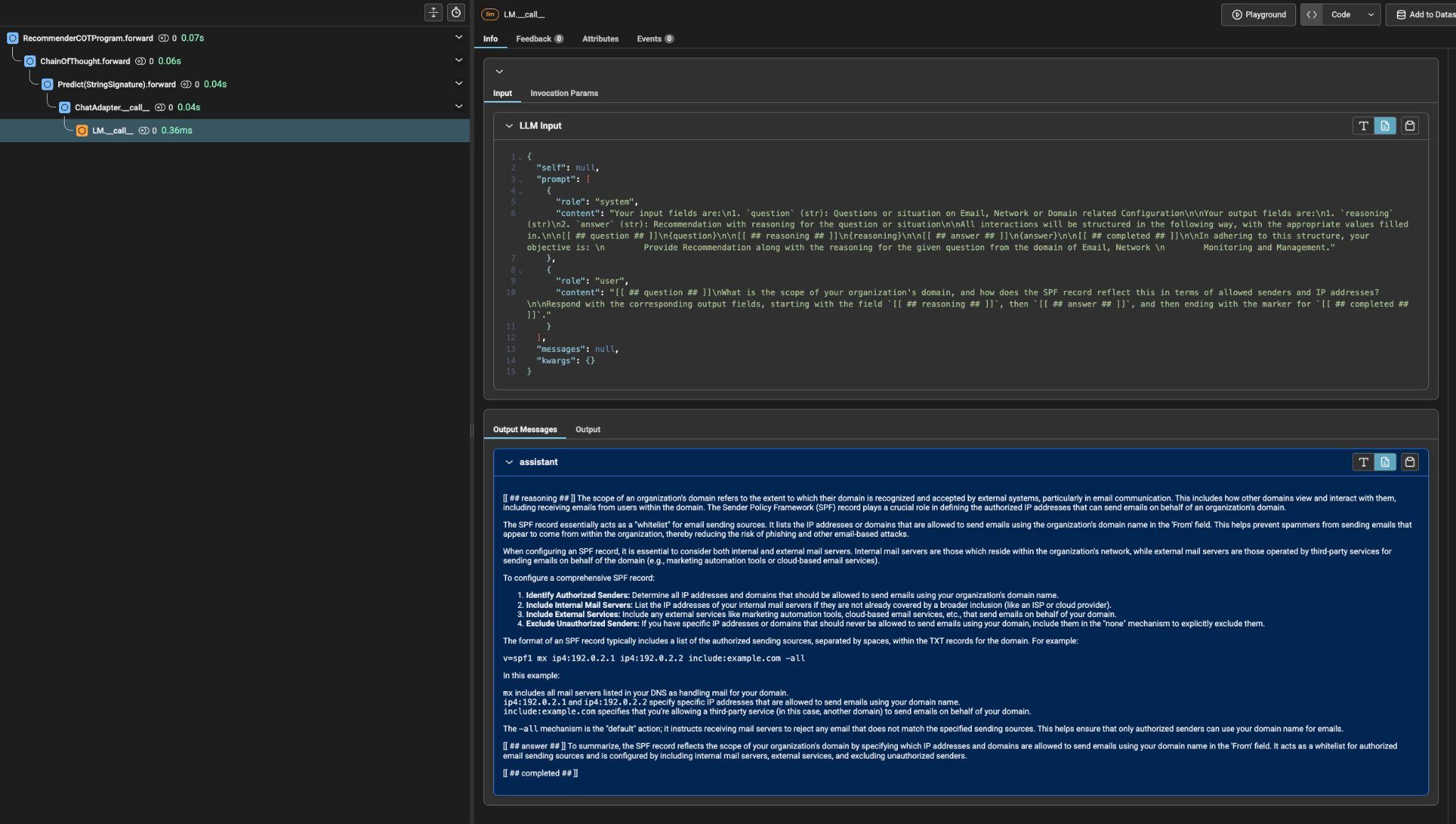
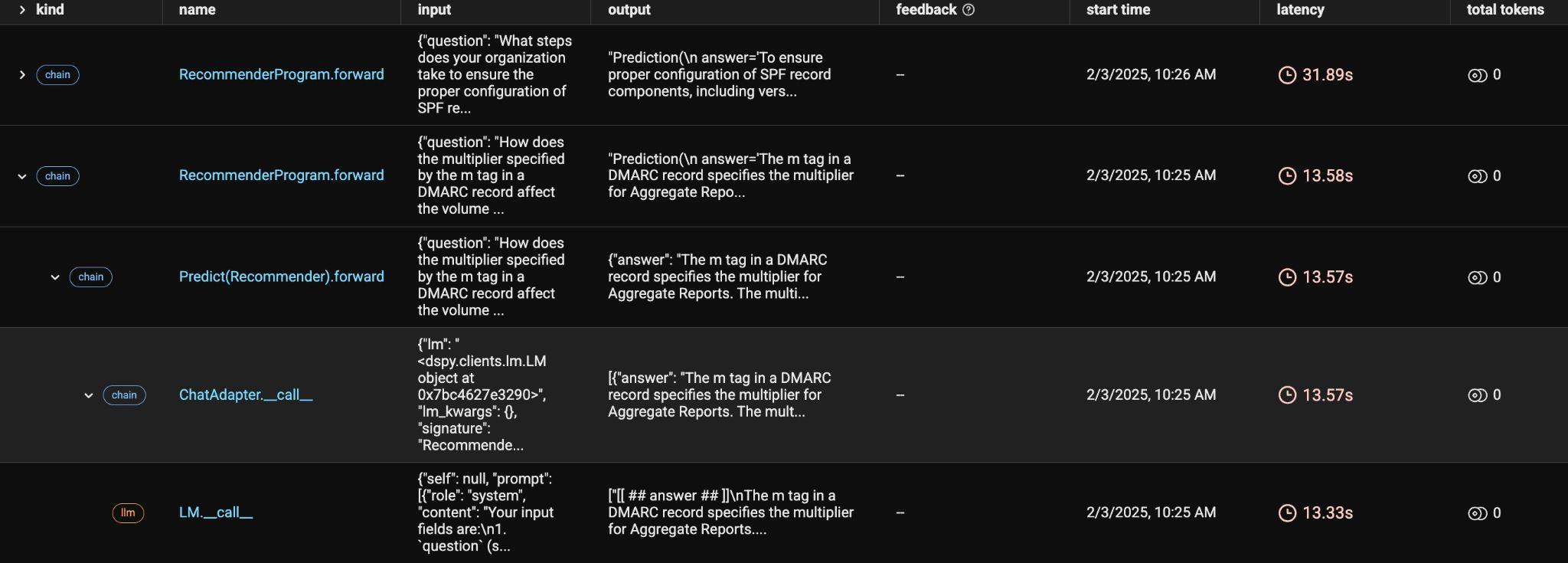
Below is a document which showcases some example traces from Pheonix tracing tool for the Llama3.2:8b model.

**Zero-shot COT LLM call**

{"self": null, "prompt": [{"role": "system", "content": "Your input fields are:\n1. `question` (str): Questions or situation on Email, Network or Domain related Configuration\n\nYour output fields are:\n1. `reasoning` (str)\n2. `answer` (str): Recommendation with reasoning for the question or situation\n\nAll interactions will be structured in the following way, with the appropriate values filled in.\n\n[[ ## question ## ]]\n{question}\n\n[[ ## reasoning ## ]]\n{reasoning}\n\n[[ ## answer ## ]]\n{answer}\n\n[[ ## completed ## ]]\n\nIn adhering to this structure, your objective is: \n Provide Recommendation along with the reasoning for the given question from the domain of Email, Network \n Monitoring and Management."}, {"role": "user", "content": "[[ ## question ## ]]\nWhat is the scope of your organization's domain, and how does the SPF record reflect this in terms of allowed senders and IP addresses?\n\nRespond with the corresponding output fields, starting with the field `[[ ## reasoning ## ]]`, then `[[ ## answer ## ]]`, and then ending with the marker for `[[ ## completed ## ]]`."}], "messages": null, "kwargs": {}}



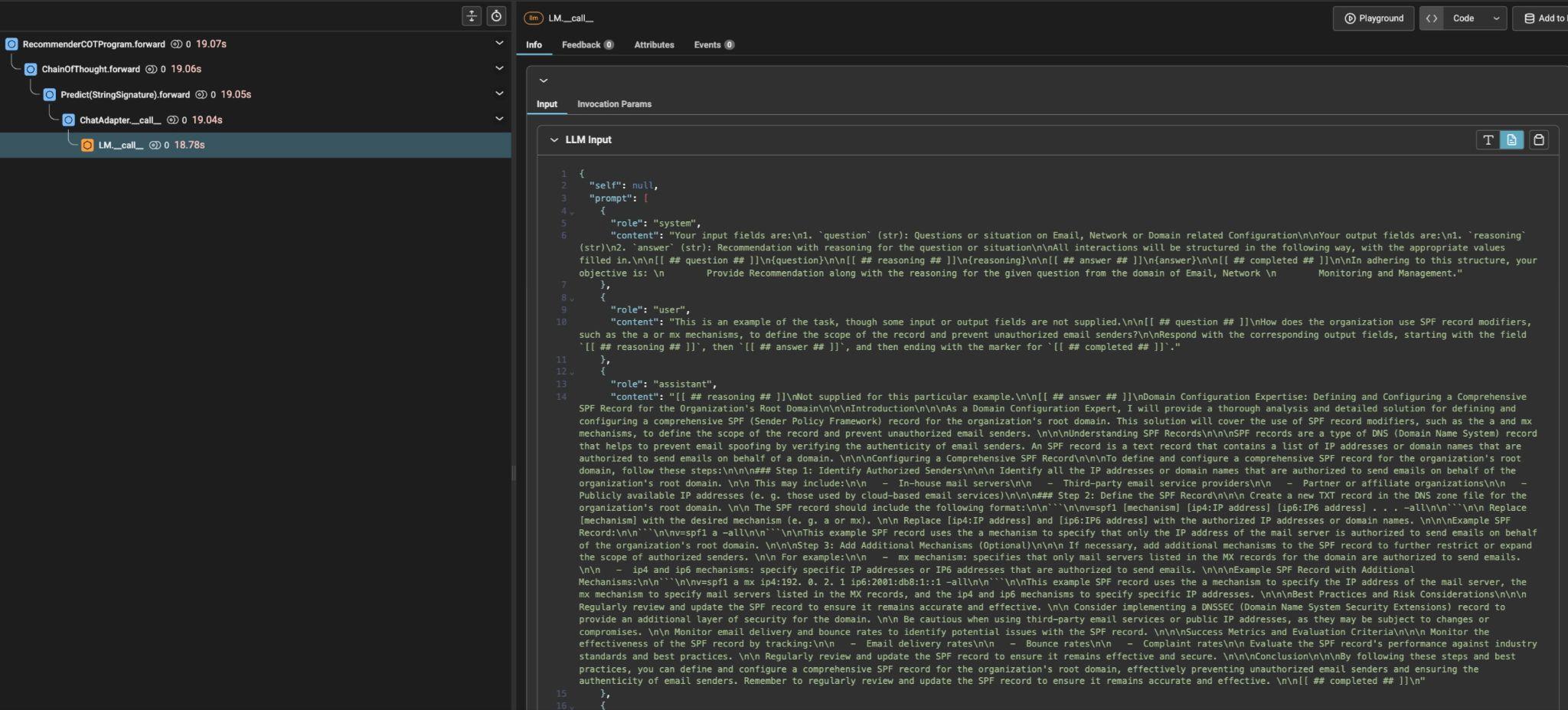
**LFS Predict Example ( Standard few shot )**



{"question": "How does the organization ensure that all mail servers and sending IP addresses are properly configured and included in the SPF record, and what measures are in place to prevent unauthorized IP addresses from being added?"}

"Prediction(\n answer=\"To ensure that all mail servers and sending IP addresses are properly configured and included in the SPF record, the organization should implement the following measures:\\n\\n1. \*\*Regular Audits and Scans\*\*: Conduct regular audits and scans of email infrastructure to identify any unauthorized or unconfigured mail servers or sending IP addresses.\\n\\n2. \*\*SPF Record Maintenance\*\*: Regularly review and update the SPF record to ensure it accurately reflects the organization's current email infrastructure, including all authorized mail servers and sending IP addresses.\\n\\n3. \*\*Automated Monitoring Tools\*\*: Utilize automated monitoring tools that can detect changes in email infrastructure and alert administrators of any potential issues or unauthorized additions to the SPF record.\\n\\n4. \*\*Change Management Process\*\*: Implement a formal change management process for updating the SPF record, which includes:\\n \* Reviewing proposed changes with relevant stakeholders\\n \* Documenting all changes made to the SPF record\\n \* Testing the updated SPF record before deployment\\n\\n5. \*\*Access Controls and Permissions\*\*: Establish strict access controls and permissions to ensure that only authorized personnel can update the SPF record or add new mail servers or sending IP addresses.\\n\\n6. \*\*Third-Party Service Integration\*\*: For third-party services, ensure they provide clear instructions on how to configure their email infrastructure to align with the organization's SPF record. Regularly review these configurations for accuracy and compliance.\\n\\n7. \*\*Employee Education and Awareness\*\*: Educate employees about the importance of accurate SPF configuration and the potential risks associated with unauthorized additions to the SPF record. This includes regular training sessions, workshops, or online courses on email security best practices.\\n\\n8. \*\*Incident Response Plan\*\*: Develop an incident response plan that outlines procedures for handling unauthorized changes to the SPF record or other email infrastructure issues. This plan should include steps for containment, eradication, recovery, and post-incident activities.\\n\\n9. \*\*Continuous Review and Improvement\*\*: Regularly review and update policies and procedures related to SPF configuration and management to ensure they remain effective in preventing unauthorized additions to the SPF record.\\n\\n10. \*\*Compliance with Industry Standards\*\*: Ensure that all measures taken align with industry standards for email security, such as those outlined by SANS Institute or recommended by relevant regulatory bodies.\\n\\nBy implementing these measures, organizations can significantly reduce the risk of unauthorized IP addresses being added to their SPF records and ensure a more secure email infrastructure.\"\n)"

**Few-shot COT**



"self": null,

"prompt": [

{

"role": "system",

"content": "Your input fields are:\n1. `question` (str): Questions or situation on Email, Network or Domain related Configuration\n\nYour output fields are:\n1. `reasoning` (str)\n2. `answer` (str): Recommendation with reasoning for the question or situation\n\nAll interactions will be structured in the following way, with the appropriate values filled in.\n\n[[ ## question ## ]]\n{question}\n\n[[ ## reasoning ## ]]\n{reasoning}\n\n[[ ## answer ## ]]\n{answer}\n\n[[ ## completed ## ]]\n\nIn adhering to this structure, your objective is: \n Provide Recommendation along with the reasoning for the given question from the domain of Email, Network \n Monitoring and Management."

},

{

"role": "user",

"content": "This is an example of the task, though some input or output fields are not supplied.\n\n[[ ## question ## ]]\nHow does the organization use SPF record modifiers, such as the a or mx mechanisms, to define the scope of the record and prevent unauthorized email senders?\n\nRespond with the corresponding output fields, starting with the field `[[ ## reasoning ## ]]`, then `[[ ## answer ## ]]`, and then ending with the marker for `[[ ## completed ## ]]`."

},

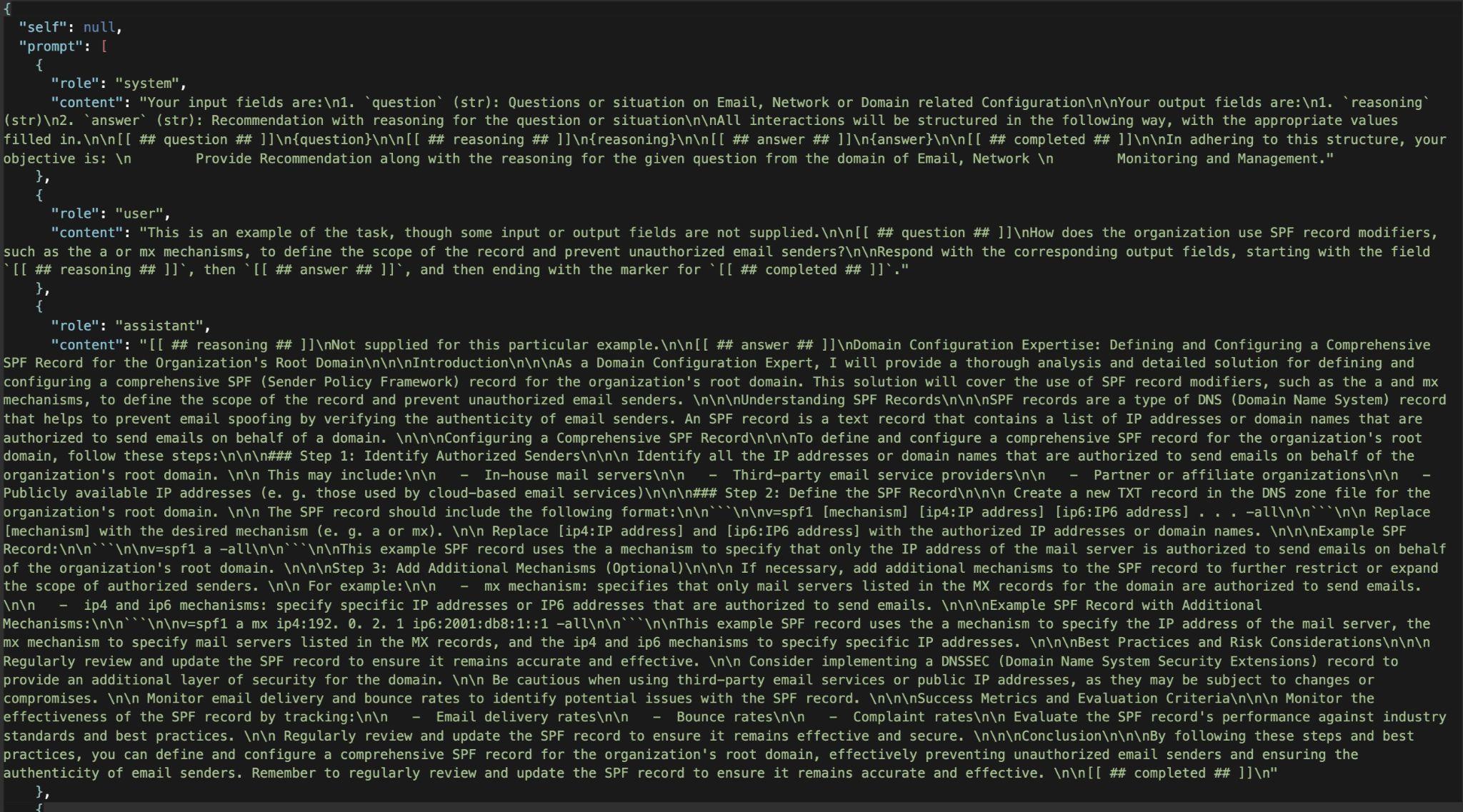
{

"role": "assistant",

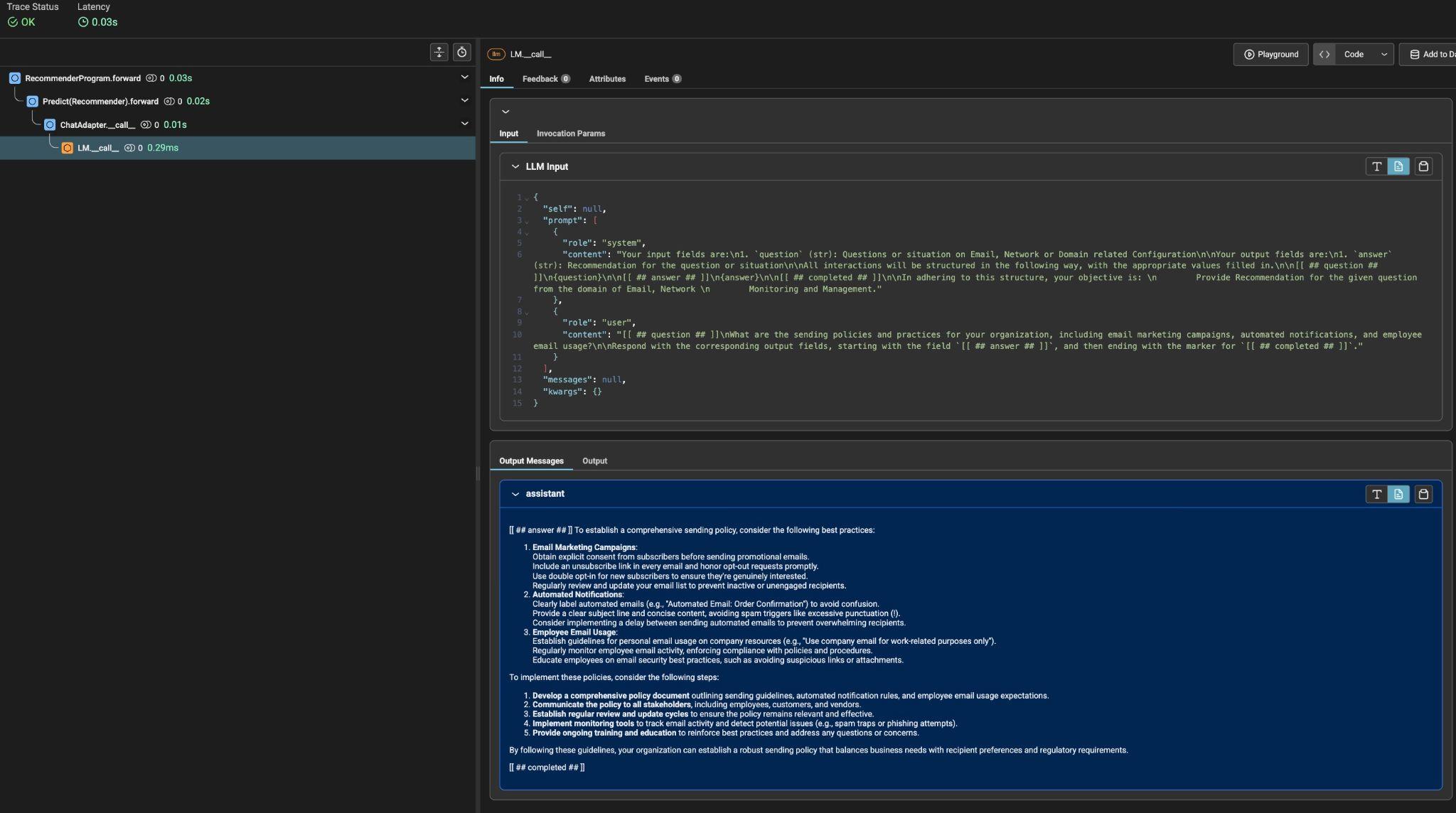
"content": "[[ ## reasoning ## ]]\nNot supplied for this particular example.\n\n[[ ## answer ## ]]\nDomain Configuration Expertise: Defining and Configuring a Comprehensive SPF Record for the Organization's Root Domain\n\n\nIntroduction\n\n\nAs a Domain Configuration Expert, I will provide a thorough analysis and detailed solution for defining and configuring a comprehensive SPF (Sender Policy Framework) record for the organization's root domain. This solution will cover the use of SPF record modifiers, such as the a and mx mechanisms, to define the scope of the record and prevent unauthorized email senders. \n\n\nUnderstanding SPF Records\n\n\nSPF records are a type of DNS (Domain Name System) record that helps to prevent email spoofing by verifying the authenticity of email senders. An SPF record is a text record that contains a list of IP addresses or domain names that are authorized to send emails on behalf of a domain. \n\n\nConfiguring a Comprehensive SPF Record\n\n\nTo define and configure a comprehensive SPF record for the organization's root domain, follow these steps:\n\n\n### Step 1: Identify Authorized Senders\n\n\n Identify all the IP addresses or domain names that are authorized to send emails on behalf of the organization's root domain. \n\n This may include:\n\n - In-house mail servers\n\n - Third-party email service providers\n\n - Partner or affiliate organizations\n\n - Publicly available IP addresses (e. g. those used by cloud-based email services)\n\n\n### Step 2: Define the SPF Record\n\n\n Create a new TXT record in the DNS zone file for the organization's root domain. \n\n The SPF record should include the following format:\n\n```\n\nv=spf1 [mechanism] [ip4:IP address] [ip6:IP6 address] . . . -all\n\n```\n\n Replace [mechanism] with the desired mechanism (e. g. a or mx). \n\n Replace [ip4:IP address] and [ip6:IP6 address] with the authorized IP addresses or domain names. \n\n\nExample SPF Record:\n\n```\n\nv=spf1 a -all\n\n```\n\nThis example SPF record uses the a mechanism to specify that only the IP address of the mail server is authorized to send emails on behalf of the organization's root domain. \n\n\nStep 3: Add Additional Mechanisms (Optional)\n\n\n If necessary, add additional mechanisms to the SPF record to further restrict or expand the scope of authorized senders. \n\n For example:\n\n - mx mechanism: specifies that only mail servers listed in the MX records for the domain are authorized to send emails. \n\n - ip4 and ip6 mechanisms: specify specific IP addresses or IP6 addresses that are authorized to send emails. \n\n\nExample SPF Record with Additional Mechanisms:\n\n```\n\nv=spf1 a mx ip4:192. 0. 2. 1 ip6:2001:db8:1::1 -all\n\n```\n\nThis example SPF record uses the a mechanism to specify the IP address of the mail server, the mx mechanism to specify mail servers listed in the MX records, and the ip4 and ip6 mechanisms to specify specific IP addresses. \n\n\nBest Practices and Risk Considerations\n\n\n Regularly review and update the SPF record to ensure it remains accurate and effective. \n\n Consider implementing a DNSSEC (Domain Name System Security Extensions) record to provide an additional layer of security for the domain. \n\n Be cautious when using third-party email services or public IP addresses, as they may be subject to changes or compromises. \n\n Monitor email delivery and bounce rates to identify potential issues with the SPF record. \n\n\nSuccess Metrics and Evaluation Criteria\n\n\n Monitor the effectiveness of the SPF record by tracking:\n\n - Email delivery rates\n\n - Bounce rates\n\n - Complaint rates\n\n Evaluate the SPF record's performance against industry standards and best practices. \n\n Regularly review and update the SPF record to ensure it remains effective and secure. \n\n\nConclusion\n\n\nBy following these steps and best practices, you can define and configure a comprehensive SPF record for the organization's root domain, effectively preventing unauthorized email senders and ensuring the authenticity of email senders. Remember to regularly review and update the SPF record to ensure it remains accurate and effective. \n\n[[ ## completed ## ]]\n"

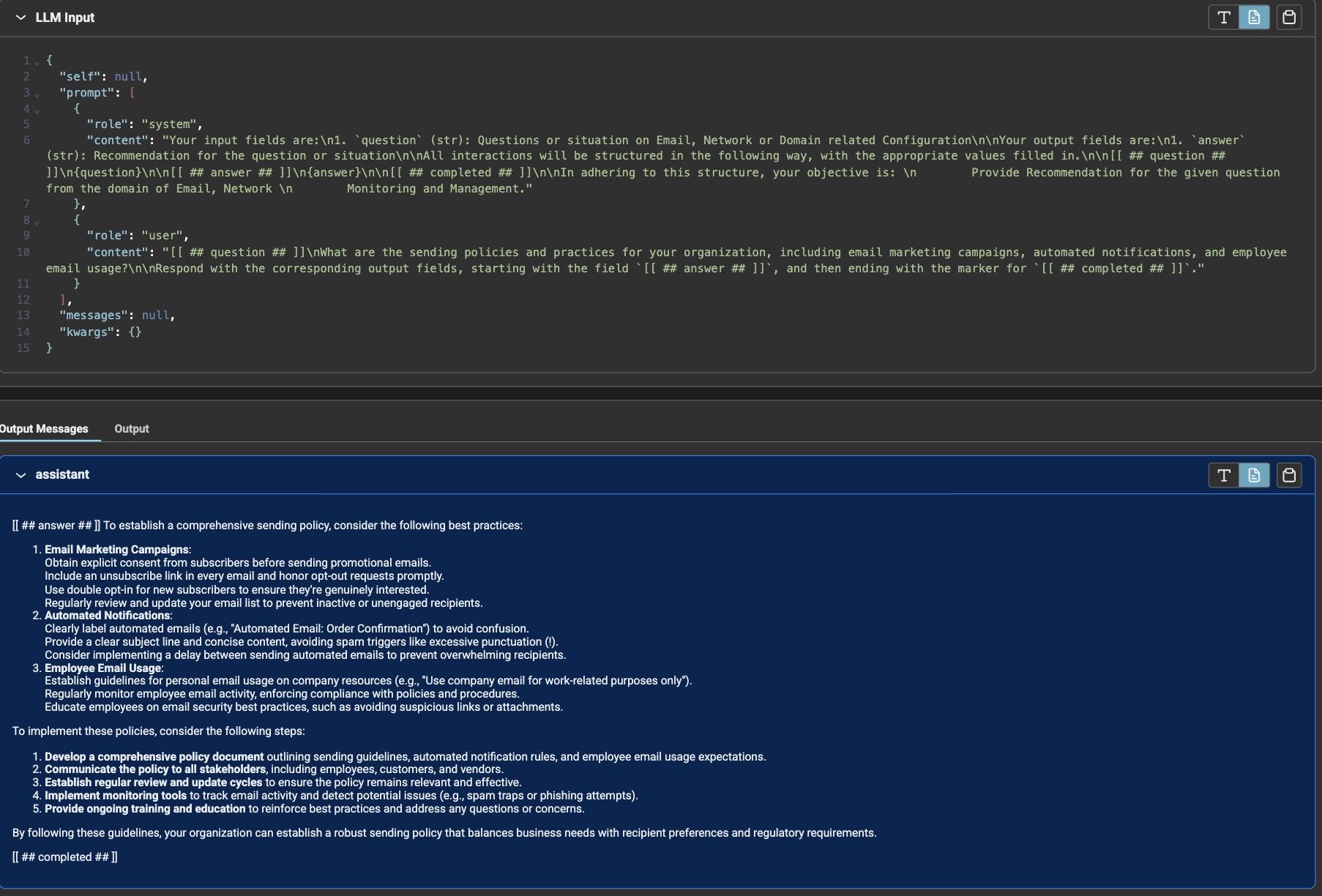
},

{



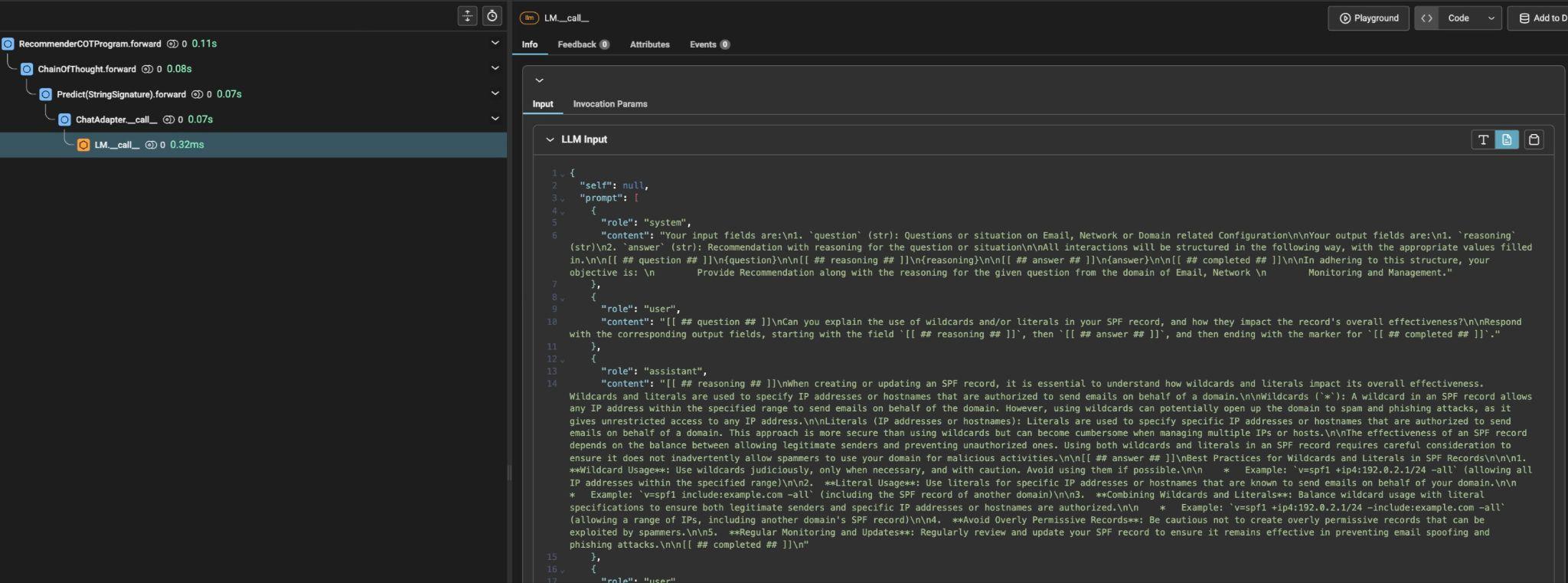
**Zero Shot Predict ( Standard )**





{"self": null, "prompt": [{"role": "system", "content": "Your input fields are:\n1. `question` (str): Questions or situation on Email, Network or Domain related Configuration\n\nYour output fields are:\n1. `answer` (str): Recommendation for the question or situation\n\nAll interactions will be structured in the following way, with the appropriate values filled in.\n\n[[ ## question ## ]]\n{question}\n\n[[ ## answer ## ]]\n{answer}\n\n[[ ## completed ## ]]\n\nIn adhering to this structure, your objective is: \n Provide Recommendation for the given question from the domain of Email, Network \n Monitoring and Management."}, {"role": "user", "content": "[[ ## question ## ]]\nWhat are the sending policies and practices for your organization, including email marketing campaigns, automated notifications, and employee email usage?\n\nRespond with the corresponding output fields, starting with the field `[[ ## answer ## ]]`, and then ending with the marker for `[[ ## completed ## ]]`."}], "messages": null, "kwargs": {}}

**Bootstrap Few-shot COT**



{

"self": null,

"prompt": [

{

"role": "system",

"content": "Your input fields are:\n1. `question` (str): Questions or situation on Email, Network or Domain related Configuration\n\nYour output fields are:\n1. `reasoning` (str)\n2. `answer` (str): Recommendation with reasoning for the question or situation\n\nAll interactions will be structured in the following way, with the appropriate values filled in.\n\n[[ ## question ## ]]\n{question}\n\n[[ ## reasoning ## ]]\n{reasoning}\n\n[[ ## answer ## ]]\n{answer}\n\n[[ ## completed ## ]]\n\nIn adhering to this structure, your objective is: \n Provide Recommendation along with the reasoning for the given question from the domain of Email, Network \n Monitoring and Management."

},

{

"role": "user",

"content": "[[ ## question ## ]]\nCan you explain the use of wildcards and/or literals in your SPF record, and how they impact the record's overall effectiveness?\n\nRespond with the corresponding output fields, starting with the field `[[ ## reasoning ## ]]`, then `[[ ## answer ## ]]`, and then ending with the marker for `[[ ## completed ## ]]`."

},

{

"role": "assistant",

"content": "[[ ## reasoning ## ]]\nWhen creating or updating an SPF record, it is essential to understand how wildcards and literals impact its overall effectiveness. Wildcards and literals are used to specify IP addresses or hostnames that are authorized to send emails on behalf of a domain.\n\nWildcards (`\*`): A wildcard in an SPF record allows any IP address within the specified range to send emails on behalf of the domain. However, using wildcards can potentially open up the domain to spam and phishing attacks, as it gives unrestricted access to any IP address.\n\nLiterals (IP addresses or hostnames): Literals are used to specify specific IP addresses or hostnames that are authorized to send emails on behalf of a domain. This approach is more secure than using wildcards but can become cumbersome when managing multiple IPs or hosts.\n\nThe effectiveness of an SPF record depends on the balance between allowing legitimate senders and preventing unauthorized ones. Using both wildcards and literals in an SPF record requires careful consideration to ensure it does not inadvertently allow spammers to use your domain for malicious activities.\n\n[[ ## answer ## ]]\nBest Practices for Wildcards and Literals in SPF Records\n\n\n1. \*\*Wildcard Usage\*\*: Use wildcards judiciously, only when necessary, and with caution. Avoid using them if possible.\n\n \* Example: `v=spf1 +ip4:192.0.2.1/24 -all` (allowing all IP addresses within the specified range)\n\n2. \*\*Literal Usage\*\*: Use literals for specific IP addresses or hostnames that are known to send emails on behalf of your domain.\n\n \* Example: `v=spf1 include:example.com -all` (including the SPF record of another domain)\n\n3. \*\*Combining Wildcards and Literals\*\*: Balance wildcard usage with literal specifications to ensure both legitimate senders and specific IP addresses or hostnames are authorized.\n\n \* Example: `v=spf1 +ip4:192.0.2.1/24 -include:example.com -all` (allowing a range of IPs, including another domain's SPF record)\n\n4. \*\*Avoid Overly Permissive Records\*\*: Be cautious not to create overly permissive records that can be exploited by spammers.\n\n5. \*\*Regular Monitoring and Updates\*\*: Regularly review and update your SPF record to ensure it remains effective in preventing email spoofing and phishing attacks.\n\n[[ ## completed ## ]]\n"

},

LLM output

[[ ## reasoning ## ]]

Preventing unauthorized changes to the SPF record is crucial to maintaining email security and preventing potential issues. To ensure that only authorized personnel can make changes, our organization implements a multi-layered approach involving technical controls, access management, and change management procedures.

[[ ## answer ## ]]

Measures in Place for Unauthorized Changes to SPF Record

To prevent unauthorized changes to the SPF record:

1. \*\*Access Control\*\*: Restrict access to modify SPF records to authorized personnel through role-based access control (RBAC) or identity and access management (IAM) systems. Ensure that only designated individuals have the necessary permissions.

2. \*\*Change Management Procedures\*\*: Establish formal change management procedures for modifying SPF records, which include:

\* Change requests: Document all changes and submit them to a centralized request system.

\* Approval process: Obtain approval from authorized personnel before making any modifications.

\* Review and testing: Conduct thorough reviews and tests of the modified record before deployment.

3. \*\*Versioning and Auditing\*\*: Implement version control for SPF records, which includes:

\* Version tracking: Maintain a record of all changes made to the SPF record, including date, time, and description of modifications.

\* Audit logging: Log all SPF record updates and changes in a centralized audit log.

4. \*\*Automated Validation\*\*: Utilize automated tools for SPF record validation and verification before deployment, such as `spfquery` or `spfcheck`. These tools can help identify potential issues with the modified record.

5. \*\*DNSSEC\*\*: Implement Domain Name System Security Extensions (DNSSEC) to provide an additional layer of security for DNS transactions. This includes signing the SPF record using a private key and verifying it on receipt.

6. \*\*Regular Reviews and Updates\*\*: Schedule regular reviews of SPF records to ensure they remain accurate and effective. Update records as needed based on changes in your email infrastructure or senders.

7. \*\*Documentation and Training\*\*: Maintain up-to-date documentation for SPF record configuration, including instructions for authorized personnel. Provide training to those with access rights to modify the record on best practices for SPF record management.

8. \*\*Third-Party Services\*\*: If using third-party services (e.g., email service providers) that manage SPF records on your behalf, ensure they have robust security measures in place and follow their change management procedures.

By implementing these measures, you can effectively prevent unauthorized changes to the SPF record and maintain a secure email infrastructure.

[[ ## completed ## ]]