


Cheat Sheet: ChatGPT Prompts for Security Audits

1. R.O.L.E. Framework for Prompt Engineering

Element	Purpose	Example
Role	Assign a specific professional role to ChatGPT	"Act as a SOC Analyst"
Objective	Clearly define what you want it to do	"Extract all Indicators of Compromise (IOCs) from the report"
Limitations	Specify output format, scope, word limits	"Output as a markdown table. No commentary."
Example	Provide a mini-sample or output structure to guide ChatGPT	Feed ChatGPT with necessary output as applicable

2. Top Prompt Structures You'll Reuse

Task	Sample Prompt Snippet
IOC Extraction	"Act as a SOC analyst. Extract all IOCs and output as a table"
MITRE ATT&CK Mapping	"Act as a threat hunter. Map behaviors to MITRE Tactics and Techniques"
Risk Scoring (RAG Analysis)	"Classify findings using Red-Amber-Green ratings with short explanations"
Framework Control Matching	"Map findings to CIS Benchmarks and PCI DSS controls with IDs"
Executive Threat Summary	"Summarize this incident in 150 words, listing risks and mitigations"

 Adapt these templates across audits, assessments, and threat reports

3. Advanced AI Prompt Template (Enterprise-Grade Reporting)

```
{  
  "prompt": "Scenario:  
A financial services company detects suspicious outbound traffic and abnormal process  
execution on a Windows Server 2022 instance. The SOC confirms that the activity began after a  
user opened a phishing document linked to a zero-day vulnerability (CVE-2023-36884). The  
goal is to investigate the incident using ChatGPT and generate a compliance audit report  
covering access control and encryption configurations, mapped to the CIS Microsoft Windows  
Server 2022 Benchmark and PCI DSS v4.0
```

Sample CVE Text:

CVE-2023-36884 – A remote code execution vulnerability in Microsoft Office and Windows triggered via malicious Word documents. Attackers gain user-level privileges after HTML rendering

Affected Systems: Windows 10/11, Office 2016–365

Severity: CVSS 8.8

Attack Vector: Remote (phishing delivery)

Mitigation: Disable Preview Pane, Enable Defender ASR rules

Act as a threat intelligence analyst. Summarize the following CVE. Include affected systems, method of attack, severity, and recommended mitigations. Use bullet points. Limit to 150 words. Ask clarifying questions before responding.

Sample Incident Narrative:

The malicious document came from alerts@secure-docs[.]com. After execution, the system connected to 193.29.13.47. Two domains were resolved: remote-update-win32[.]live and sync-sharepoint365[.]info.

File hash of the dropped DLL:

SHA256: 87c4db79a72e743cafb86c95de0c1c23e94389dff1db2a844b6ef24549aa421

Filename: updcenter.dll

Act as a SOC analyst. Extract IOCs from the incident report. Group the results into IPs, domains, file hashes, and filenames. Output in a structured table format. No commentary. Ask clarifying questions before proceeding.

Act as a threat hunter. Map the activity in the incident report to MITRE ATT&CK tactics and techniques. Use a table with columns: Tactic, Technique, Technique ID, and Description. Ask clarifying questions if mapping is uncertain.

Before we move to reporting, let's reiterate our regulatory audit goal
You are auditing for compliance with:

CIS Microsoft Windows Server 2022 Benchmark (focus: encryption, access control)
PCI DSS v4.0 controls (focus: 8.x access requirements and 10.x logging requirements)

The goal is to ensure that mitigations and control weaknesses discovered align with these frameworks",

"role": "Threat Intelligence Analyst",

"department": "Security Operations Center (SOC)",

"task": "Summarize a CVE, extract IOCs, and map activity to MITRE ATT&CK. Then create a detailed security audit report with the following sections: Cover Page, Executive Summary, Methodology, Detailed Findings, Compliance Mapping with RAG status, Remediation Plan",

"task_description": "As a threat intelligence analyst, analyze CVE-2023-36884 in the context of a phishing-based intrusion affecting a Windows Server 2022 instance. Include a summary of the CVE, extract all indicators of compromise (IOCs), and map incident activity to MITRE ATT&CK techniques. Output should support future compliance audits aligned with CIS Microsoft Windows Server 2022 Benchmark and PCI DSS v4.0. Use tables for structured presentation.",

"rules": {

"rule_1": "Ask the user 3-5 clarifying questions before generating the report.",

"rule_2": "Format all risk analysis using a table with Red-Amber-Green (RAG) ratings.",

"rule_3": "Evaluate the report using a predefined rubric and present results in table format.",

"rule_4": "DO NOT fabricate legal citations. Use only verified compliance sources.",

"rule_5": "Provide up to 3 refinement options: (1) Improve Report, (2) Re-Evaluate with Different Standard, (3) Adjust Format or Scope.",

"rule_6": "Incorporate insights from the key references to enhance the report's depth and accuracy."

},

"key_references": {

"key_reference_1": {

"title": "CIS Microsoft Windows Server 2022 Benchmark",

"organization": "Center for Internet Security",

"version": "v1.0.0",

"release_date": "March 29, 2023",

"key_insights": [

"Recommends configuration settings to harden Windows Server 2022 environments.",

"Focus areas include account policies, audit settings, user rights assignments, and encryption protocols.",

"Emphasizes secure configuration for services such as SMB, RDP, and Windows Defender.",

"Supports reducing attack surface and aligning with broader security frameworks.",

```

    "Includes mappings to compliance standards such as PCI DSS and NIST 800-53."
  ]
},
"key_reference_2": {
  "title": "PCI DSS v4.0",
  "organization": "PCI Security Standards Council",
  "release_date": "March 2022",
  "key_insights": [
    "Details security requirements for protecting cardholder data in digital environments.",
    "Section 8 emphasizes strong access control measures (e.g., MFA, unique IDs, least privilege).",
    "Section 10 covers audit logging, retention, and monitoring of security events.",
    "Encourages continuous risk assessments and threat monitoring practices.",
    "Applies to any entity that stores, processes, or transmits payment card data."
  ]
}
},

"evaluationRubric": {
  "1": "Poor - Major gaps in compliance assessment.",
  "5": "Average - Some compliance coverage, but lacks depth.",
  "8": "Proficient - Well-structured, thorough compliance report.",
  "10": "Outstanding - Fully optimized, industry-best compliance report."
}
}

```

✓ Use this full structure when generating compliance reports, audit findings, and risk summaries

4. Pro Tips for High-Quality, Secure Prompting

- Always define the Role clearly ("Act as a cybersecurity auditor...")
- Never paste live production logs — always sanitize inputs
- Use Limitations to control verbosity (e.g., word counts, tables)
- Request clarifying questions first before AI responds
- Validate outputs manually against CIS, PCI DSS, ISO, and NIST documents
- Document prompt history for traceability and compliance

✓ Treat AI outputs like junior analyst work—review, validate, and correct where needed



Quick Visual: Example Audit Workflow Using Prompts

1. Analyze Threat (summarize CVE) -->
2. Extract IOCs -->
3. Map to MITRE -->
4. Score risks using RAG -->
5. Align to Framework Controls -->
6. Generate Executive Report

✓ Each step is supported by structured prompts built on R.O.L.E. and Advanced Template principles



Core References for Validation

1. CIS Microsoft Windows Server 2025 Benchmark v1.0.0
https://www.cisecurity.org/benchmark/microsoft_windows_server
2. PCI DSS v4.0 Official Documentation
https://www.pcisecuritystandards.org/document_library
3. NIST Special Publication 800-53 Revision 5 (Security and Privacy Controls for Information Systems)
<https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>
4. MITRE ATT&CK Framework
<https://attack.mitre.org/>