Rethinking Security Operations

Local, Agentic SOC in Your Pocket Architecture & Implementation Guide

Current SOC Challenges

Modern Security Operations Centers (SOCs) face structural friction across three critical vectors:

- **The Skills Gap:** Running an effective SOC requires highly skilled staff who must constantly address key operational demands:
  - Prioritizing an ever-increasing volume of events from disparate telemetry sources.
  - Determining which incidents require immediate attention and remediation.
  - Maintaining up-to-date knowledge across network security, OS internals, vulnerabilities, forensics, applications, and dozens of vendor tools.
  - Executing manual remediation on impacted systems.
  - Creating complex reports to satisfy mandatory compliance schemes.

  Meanwhile, adversaries are increasingly leveraging AI in their attacks—making cyberattacks faster, cheaper, and more effective.



Figure 1 The SOC Skills Gap

- **Cloud-Only :** Most security vendors are attempting to integrate AI into their offerings, but the most advanced features are typically available only in the public cloud. This presents a major hurdle for organizations that cannot use the public cloud for regulatory or security reasons.



Figure 2 Cloud-Only for advanced AI

- **Soaring SIEM Costs:** Commercial SIEM licensing models are typically based on data ingestion volume. By routing more and more telemetry to the SIEM, organizations hope to increase detection through correlation, turning the platform into a costly "wishing well". Add to that the complexity of legacy SIEMs—where teams must navigate complex, proprietary search languages (such as Splunk SPL)—and building SOAR workflows for remediation becomes difficult and expensive.



Figure 3 The SIEM Wishing Well

The Solution: Local, Agentic "SOC in Your Pocket"

Organizations can solve these challenges by adopting "SOC in Your Pocket"—an innovative approach leveraging agentic AI with Model Context Protocol (MCP) tools implemented natively within Kubernetes.

- **Bridge the Skills Gap via Natural Language:** Instead of constructing complex SIEM queries or toggling between dozens of security consoles, security teams interact using natural language.

> *"Do we have systems that may be compromised? Are these high-value assets? Are there privileged users logged on to these systems? Are there signs of lateral movement? Could you carry out remediation and forensic analysis on those systems and write a summary report?"*

- **Deploy Anywhere (On-Premises & Air-Gapped):** The cloud-only constraint is eliminated. Using a modular, microservices architecture based on Kubernetes, everything—including AI agents, LLMs, and MCP services—can run locally or inside a private cloud. This makes the solution ideal for air-gapped environments where public cloud connections are restricted or undesirable.
- **Eliminate Ingestion License Fees:** Soaring SIEM costs are avoided because the system does not rely on legacy SIEMs for event correlation. "SOC in Your Pocket" directly retrieves curated, high-quality events from existing security controls and correlates them using AI agents. This significantly reduces the volume of raw data sent to the SIEM.
- **Simplified Operations:** Correlation rules and SOAR playbooks use plain natural language (e.g., "start forensic analysis and isolate device") instead of vendor-specific query languages or complex SOAR workflow flowcharts.

Solution Architecture

The solution is implemented via microservices within a Kubernetes cluster deployed in public or private cloud environments. At the core of the design are AI agents. These agents receive instructions from the Web GUI frontend and leverage LLMs (hosted either inside or outside the Kubernetes cluster) to conduct intelligent analysis and recommend actions.

To gather relevant context from the customer environment, AI agents connect to MCP clients that query dedicated MCP servers for EDR, NDR, NAC, DNS Security, Identity, and Long-Term Logging.

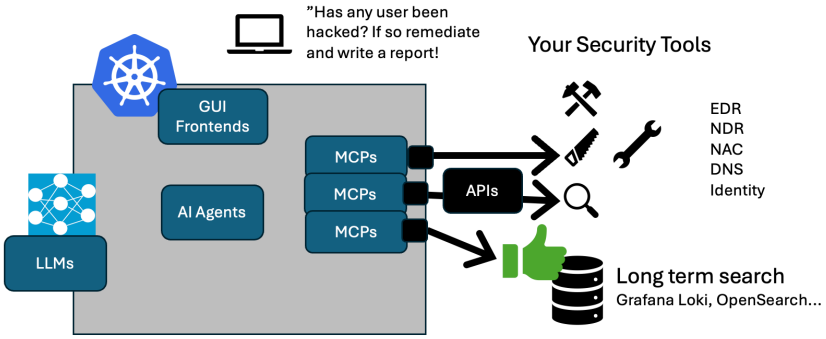


Figure 4 Solution Architecture

Technical Note on Context Optimization

Unoptimized MCP implementations can cause context windows to overflow, risking LLM output quality. To mitigate this risk, the solution leverages modular AI skills, significantly reducing context window overhead. Additionally, the solution uses custom-built MCP servers that leverage traditional APIs to interact with security platforms. This offers two key benefits:

- **Legacy Integration:** It enables integration with legacy systems that do not yet support MCP natively.
- **Precise Window Control:** It provides precise control over the context window by exposing only the MCP tools directly relevant to active SOC workflows.

SOC in Your Pocket in Action

Below is an example of an investigation workflow using SOC in Your Pocket:

1. Identify & Prioritize Compromised Systems: We query the system for endpoints showing high likelihood of compromise based on EDR and NDR telemetry, filtering for systems where active users hold privileged access. This correlation requires neither a SIEM nor vendor-specific integrations.

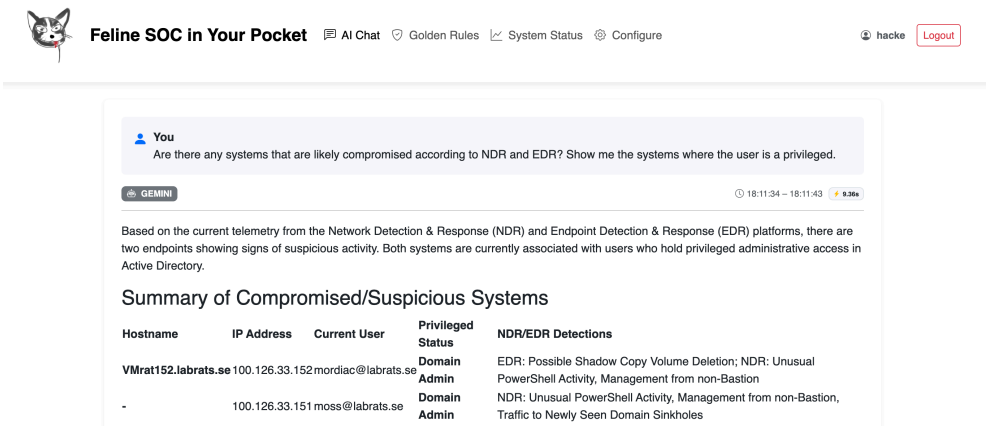


Figure 5 Identify Compromised Systems and Prioritize

2. Cross-Correlate DNS Telemetry: Next, we follow up by asking whether DNS Security has recorded related malicious findings for the identified endpoints.

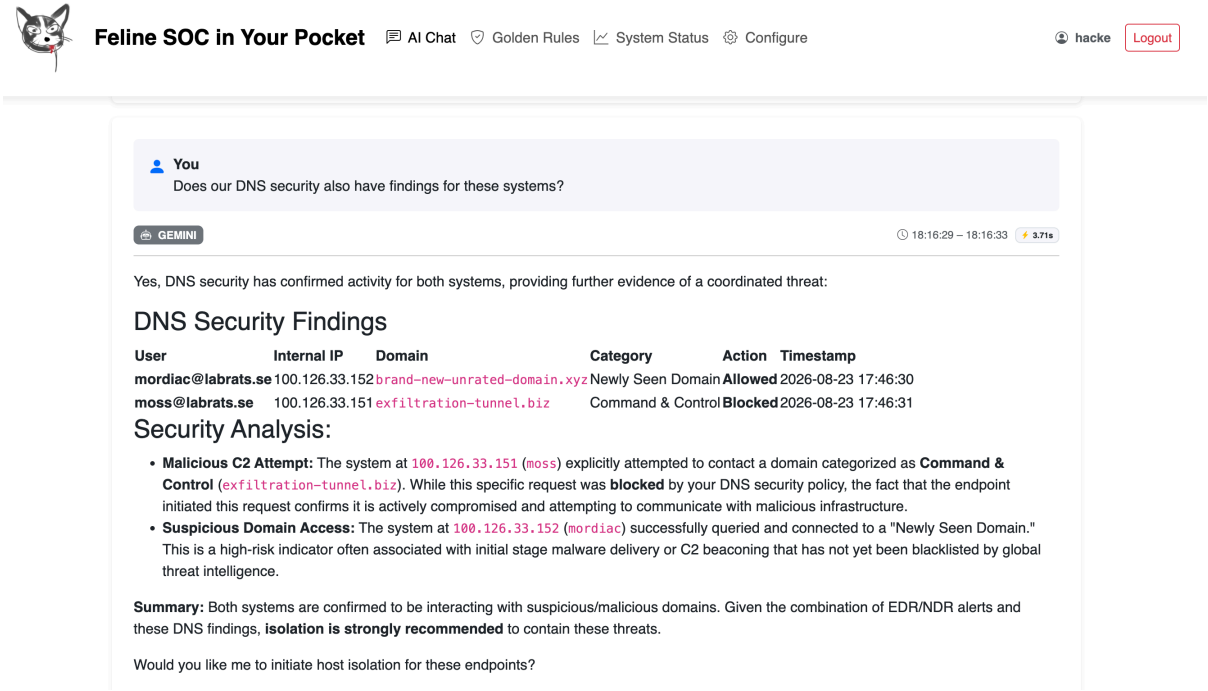
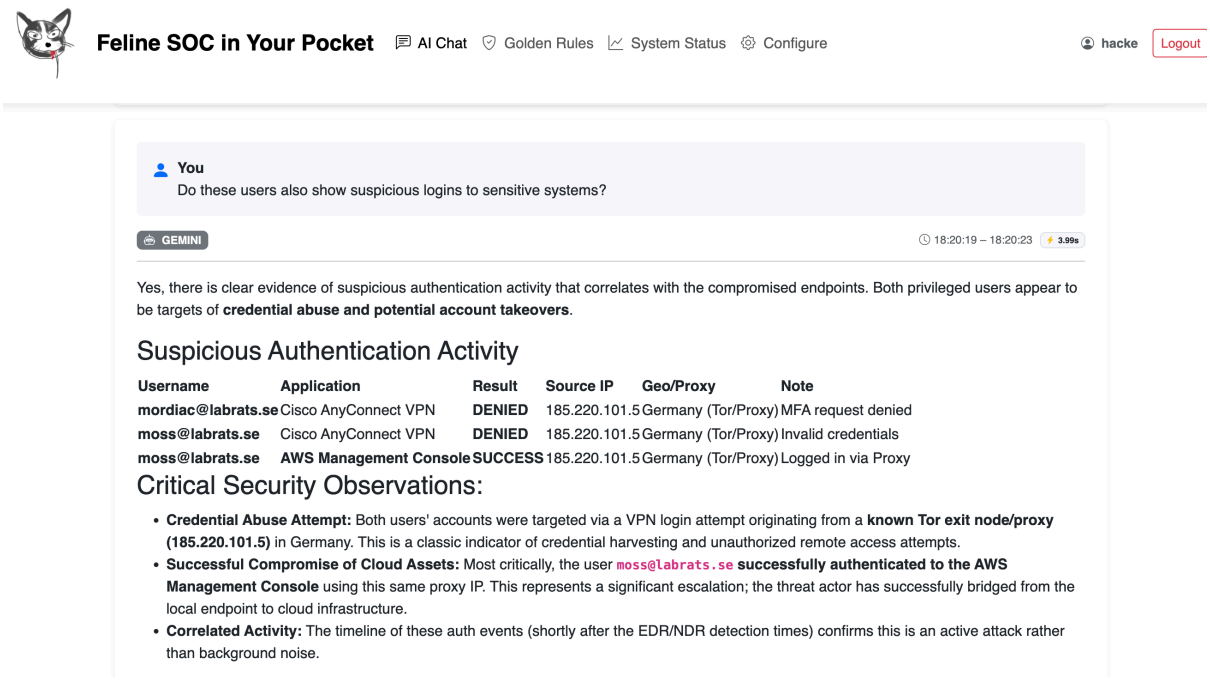
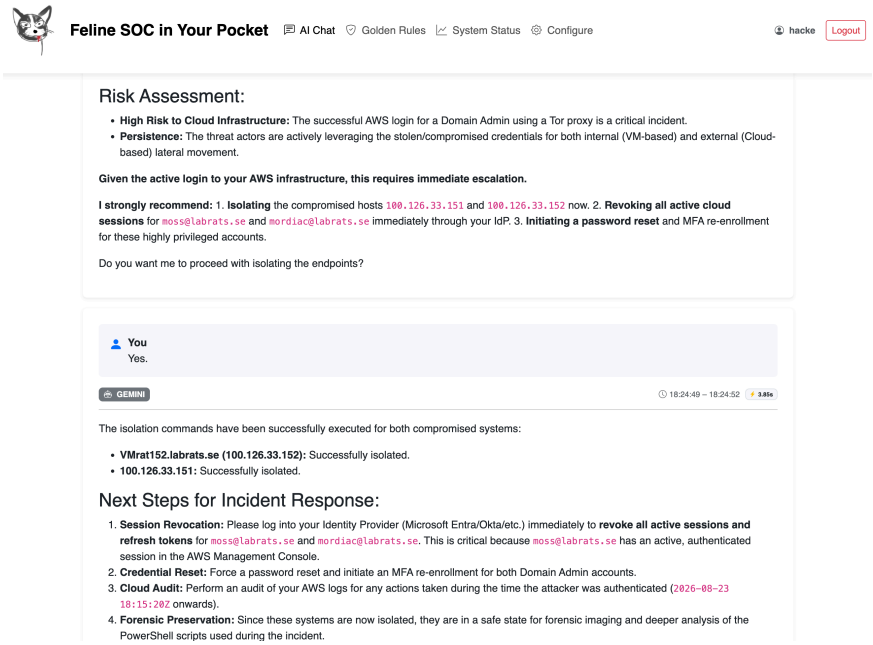


Figure 6 Adding DNS Security Findings

3. Check Identity Access: We analyze whether the affected user accounts show suspicious authentication attempts against sensitive internal systems or cloud management consoles.



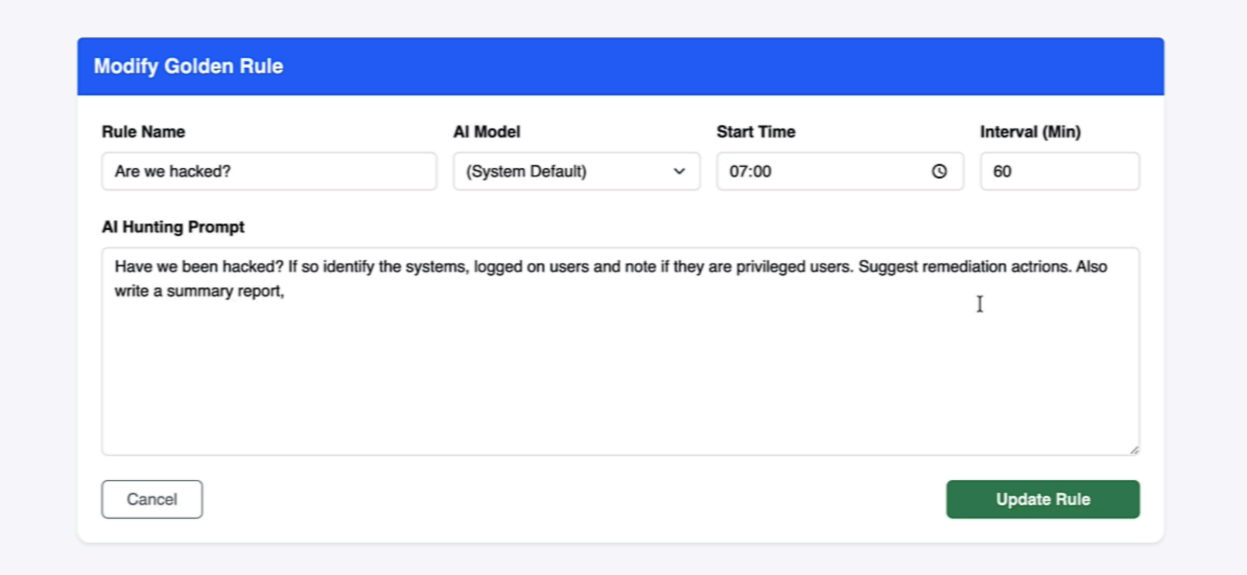
4. Automate Remediation: The user approves the recommended isolation and session revocation actions, and the system executes containment commands across the targeted hosts.



Golden Rules: “Automating the AI”

We have shown how we can use AI to help our SOC, correlating events, prioritizing incidents and suggest and carry out remediations.

But we can also automate all this! Golden rules allow you to define rules in natural language. These rules are executed at specified intervals and the result is sent to your preferred output (Teams, Slack, Google Chat, … any webhook).



Next Steps & Implementation Roadmap

Is SOC in Your Pocket right for your organization? If so, we recommend the following phased deployment process:

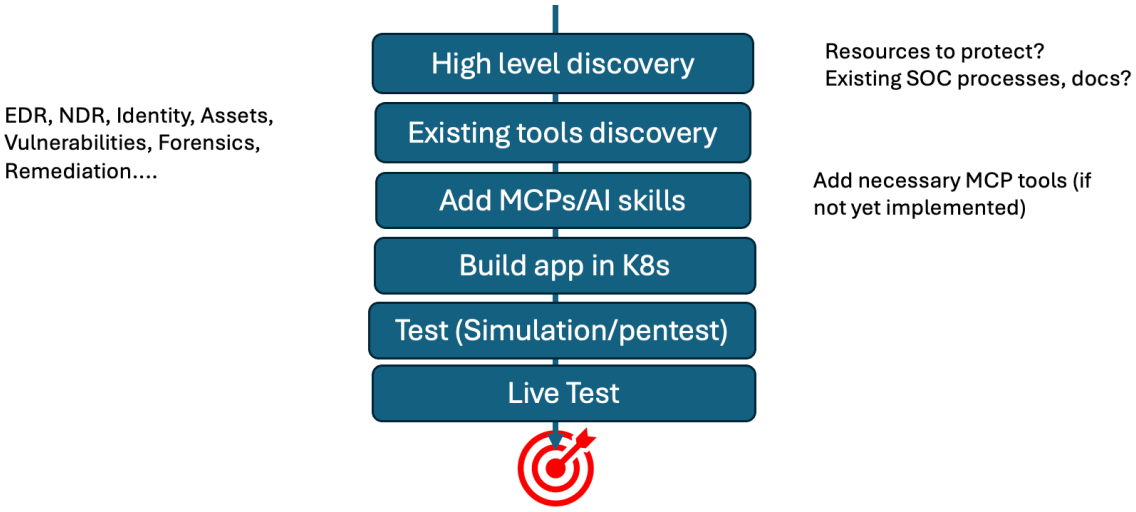


Figure 7 Implementing Soc In Your Pocket

1. High-Level Discovery: Identify critical assets to protect (e.g., patient records, OT equipment, financial databases) and evaluate existing SOC workflows, documentation, and reporting requirements.

2. Existing Tools Discovery: Audit active security tools (EDR, NDR, DNS, Identity). If a specific vendor is not currently supported, custom MCP integrations can be added quickly.

3. Build & Configure in Kubernetes: Deploy the application microservices into your environment (including private cloud options). Configure necessary API keys; read-only permissions are sufficient for initial deployment, reserving write access for endpoint quarantine or automated remediation functions.

4. Validation & Testing: Execute simulation and penetration tests to confirm the solution performs as expected and aligns with established SOC incident handling procedures.

5. Live Deployment: Transition to live operational mode. Implementation carries zero operational risk to network traffic, as SOC in Your Pocket operates out-of-band and does not sit in-line.

Are you ready to transform your SOC?