NeoCISO: Pro Agentic AI for Your Existing Security Stack

Executive Summary

NeoCISO is a **Pro agentic AI Security Professional** that integrates with and overlays your existing security stack (SIEM, XDR, EDR, etc.)[11111111]. Its primary goal is to provide a **governed and explainable** security decision workflow end-to-end[22222]. By assembling context, making defensible determinations with a transparent **Why-Factor**, driving actions to verified closure, and capturing an audit-ready record [3333], NeoCISO helps security teams move past alert fatigue and audit preparation struggles[4]. It achieves this **without requiring rip-and-replace** of current tools, thereby lowering the total cost of ownership (TCO)[55555555555].

1. Synopsis of Key Capabilities

NeoCISO operates by owning the entire decision workflow from triage to audit record[666]. Its architecture ensures high signal quality and continuous compliance[77777].

A. Core Workflow & Features

- **Context Assembly:** Gathers live assets, owners, criticality, identity, exposure posture, and relevant history to enrich alerts[8888].
- **Professional Reasoning:** Decisions are grounded in industry standards like **MITRE ATT&CK** and **NIST/ISO controls**[9].
- **Why-Factor Narrative:** Generates a short, human-readable rationale that cites evidence and control mapping for every determination[10101010101010101010].
- **Governed Actions:** Proposes ranked steps with required **approval gates** and role-based controls before execution[1111111111111111111].
- **Verified Closure:** Executes actions via ITSM hand-off (e.g., ServiceNow/Jira) and tracks them to verified closure[121212121212121212].
- **Audit Vault:** Captures evidence, attestation, and immutable timelines, compressing audit prep from weeks to hours[131313131313131313131313131313].
- **Learning Loops:** Pro agentic AI feedback continuously reduces false positives and false negatives, improving signal quality[14141414].

B. Outcomes and Benefits

Audience	Key Outcome
Security Leaders	Defensible decision quality; board-ready narratives; KPI trends[15].
SOC Teams	Fewer hand-offs and context switches; explainable recommendations; promotion to exception-handlers[16].
Organization	Lower TCO; continuous compliance; clarity, not noise[171717171717171717].

2. Specific Security Case Examples

NeoCISO's value is demonstrated by how it processes specific security cases, providing comprehensive context, control mapping, and clear steps for closure.

Example 1: Dormant Privileged Account with Weak MFA Path

Workflow Step	Details	Artifact/Control Mapping
Case Summary	Dormant privileged account with weak MFA path detected on a Domain Admin[18].	
Why-Factor (Excerpt)	**Privilege anomaly** (no interactive login in 45 days) [19]and **Weak MFA path** (legacy service logins accepted password-only auth)[20].	Artifacts: AD query [21], IdP logs[22].
Determination	High severity - policy violation (privileged identity hygiene)[23].	
Controls Mapped	**NIST CSF (v1.1):** PR.AC-1, PR.AC-4, DE.AE-2[24]. **ISO 27001:** A.9.2.3, A.5.16 (Management of privileged access rights/Identity management)[25252525].	
Recommended Actions	1. Disable/reclassify account, rotate credentials, enforce strong MFA[26]. 2. Remove legacy auth path[27]. 3. Run lateral movement sweep[28].	

Workflow Step	Details	Artifact/Control Mapping
Verification	AD shows account disabled; IdP logs confirm MFA enforced; EDR shows no subsequent admin logons for 7 days[29].	

Example 2: Suspicious PowerShell via WMI Lateral Movement

Workflow Step	Details	Artifact/Control Mapping
Case Summary	Remote code execution via WMI spawns powershell.exe -EncodedCommand on a Tier-1 server[30].	
Why-Factor (Excerpt)	**Remote execution** (WMI spawning PS from admin workstation) [31]and **Tradecraft indicators** (Base64-encoded command, lateral connections)[32].	Artifacts: EDR process tree [33], ATT&CK T1047 (WMI)[34].
Determination	High severity - probable lateral movement using WMI + PowerShell[35].	
Controls Mapped	**NIST CSF (v1.1):** DE.CM-7, RS.MI-1 (Monitoring/Containment)[36]. **ISO 27001:** A.13.1.1 (Network controls), A.8.16 (Monitoring activities)[37].	
Recommended Actions	1. Contain affected endpoints, restrict remote WMI[38]. 2. Rotate credentials[39]. 3. Hunt for encoded PowerShell across fleet[40].	
Verification	No new WMI-spawned PowerShell events for 7 days; EDR shows zero lateral movement post-containment[41].	