DEEPWATCH™
Always Watching. Always Protecting.™

SOLUTION BRIEF

Deepwatch NEXA™ Ecosystem: Detection Advisor Agent

Proactive Threat Readiness. Intelligent Detection Validation. AI-Assisted Security Operations.

OVERVIEW

The NEXA Detection Advisor Agent is part of Deepwatch NEXA - a network of autonomous AI agents designed to perform security-focused tasks across the SOC lifecycle.

The Detection Advisor Agent helps security teams proactively assess threat readiness, validate detection coverage, identify telemetry gaps, and accelerate investigation workflows before incidents escalate into business-impacting events.

Rather than relying solely on manual searches, analyst intuition, or reactive investigations, the NEXA Detection Advisor Agent continuously evaluates organizational visibility, detection posture, and operational readiness across modern attack surfaces including Identity, SaaS, cloud and endpoint environments.

The result is faster decision-making, stronger detection coverage, reduced analyst burden, and more autonomous security operations.

WHY IT MATTERS

Modern attacks evolve faster than traditional SOC workflows.

Security teams are increasingly challenged by:

- Expanding attack surfaces across cloud, SaaS, identity, and developer ecosystems
- Detection gaps caused by incomplete telemetry or inconsistent configurations
- Manual, search-heavy investigations that slow response times
- Difficulty validating readiness against emerging threats before incidents occur
- Analyst fatigue and operational overload during active incidents

The NEXA Detection Advisor Agent helps organizations move from reactive investigations toward proactive, AI-assisted threat readiness and operational intelligence.

HOW IT WORKS

The NEXA Detection Advisor Agent continuously:

- ✓ Correlates telemetry and detections across security tools and environments
- ✓ Evaluates detection coverage against known attack techniques
- ✓ Identifies telemetry gaps and operational blind spots
- ✓ Maps threats to ATT&CK techniques and organizational exposure
- ✓ Generates AI-assisted recommendations and investigative guidance
- ✓ Prioritizes actions based on risk, visibility, and operational impact

The agent integrates into broader AI SOC and case management workflows, enabling security teams to move from manual investigation toward autonomous operational assistance.

AI-ASSISTED SECURITY OPERATIONS

The Detection Advisor Agent is designed to reduce dependency on manual querying and analyst-driven correlation by operationalizing AI directly into SOC workflows.

Capabilities include:

- ✓ Automated telemetry correlation
- ✓ AI-assisted investigations
- ✓ Contextual enrichment and prioritization
- ✓ Investigation graphing and relationship mapping
- ✓ AI-generated investigative narratives and summaries
- ✓ Recommended response actions and remediation guidance

This enables faster triage, reduced analyst fatigue, improved consistency, and greater operational scalability.

EXPLAINABILITY & TRANSPARENCY

NEXA emphasizes explainable AI and operational transparency.

Security teams can understand:

- ✓ Why detections triggered
- ✓ What telemetry and evidence contributed to prioritization
- ✓ How confidence scoring was derived
- ✓ Why recommendations were generated
- ✓ Which attack paths and behaviors influenced investigations

This provides technically mature teams with greater trust, auditability, and operational confidence in AI-assisted workflows.

DEEPWATCH™

KEY USE CASES

1. RECENT ATTACK & EMERGING THREAT READINESS

Assess your organizational readiness against newly disclosed attacks, active threat campaigns, or emerging adversary techniques.

Example Questions

- "Based on our current visibility and telemetry, how exposed are we to emerging ransomware families like BlackCat (ALPHV), LockBit, or Akira, and active zero-day threats such as MOVEit, Ivanti Connect Secure, or Citrix Bleed?"
- "Do we currently have the telemetry and detection coverage necessary to identify tactics associated with Scattered Spider?"
- "Which telemetry sources are critical for identifying <emerging threat name>, and where might we have visibility gaps?"

2. PROACTIVE THREAT COVERAGE VALIDATION

Validate whether your organization has the required telemetry, detections, and visibility to identify a specific malware campaign, threat actor, or attack technique before an incident occurs.

Example Questions

- "Do we have the telemetry, visibility, and detections required to identify early-stage ransomware activity related to BlackCat (ALPHV) before encryption or lateral movement occurs?"
- "If a ransomware attack successfully compromised systems, what detections would help us identify post-compromise behavior such as persistence, lateral movement, or data exfiltration?"
- "Do we have coverage for credential theft activity?"

3. TELEMETRY GAP IDENTIFICATION

Identify missing or inconsistent telemetry sources that could create blind spots across endpoints, cloud, identity, network, or distributed environments.

Example Questions

- "What telemetry is missing for this use case?"
- "If there are gaps in coverage, which systems, telemetry sources, or detections are missing and what should we prioritize first to reduce exposure?"
- "Which systems are not sending required logs?"

4. DETECTION READINESS ASSESSMENT

Evaluate whether critical detections are enabled, operational, tuned correctly, and consistently deployed across the environment.

Example Questions

- "What detections support a lateral movement threat scenario?"
- "Do we have the above detections enabled?"
- "Which ATT&CK techniques are currently missing in my detection coverage?"

5. INCIDENT & HISTORICAL EXPOSURE ANALYSIS

Review historical incidents, prior alerts, and detection activity tied to threats, malware, or attack patterns to understand exposure and operational effectiveness.

Example Questions

- "Have we seen activity related to this threat before?"
- "Show incident history from the past 7 days associated with this detection"
- "Which environments generated similar alerts historically connected to <detection ID>?"

6. GUIDED REMEDIATION & NEXT ACTIONS

Provide prioritized recommendations to improve visibility, reduce risk, and strengthen detection coverage.

Example Questions

- "What are the highest-priority detections that should be enabled first?"
- "What is the next most immediate step I can take to address gaps?"
- "What actions would most improve our security posture?"

THE DEEPWATCH ADVANTAGE

With the NEXA Detection Advisor Agent, Deepwatch enables organizations to:

- Validate threat readiness proactively
- Identify detection and telemetry gaps faster
- Reduce search-heavy analyst workflows
- Improve operational response speed
- Increase SOC efficiency and scalability
- Accelerate investigation and remediation workflows
- Operationalize AI across the security lifecycle

Move beyond reactive investigations.
Operate with proactive, AI-assisted security intelligence.

DEEPWATCH™
Always Watching. Always Protecting.

ABOUT DEEPWATCH

Deepwatch® is the leader in Precision MDR powered by AI and humans. We amplify human expertise with AI insights to reduce the risks that matter most to your business. Our protection is proactive, preemptive and responsive, tuned to your business, with no black boxes, and watched by experts 24/7/365.

CONTACT US

LEARN MORE

250 Cambridge Avenue
Palo Alto, CA 94306
www.deepwatch.com