7AI

AI AGENTS FOR CYBERSECURITY:

OFFLOADING NON-HUMAN SECURITY WORK TO SHIFT PEOPLE UP FOR EXPONENTIALLY BETTER SECURITY OUTCOMES

REIMAGINING SECURITY WORK

Boredom is a thief. It sneaks into security teams, robbing them of focus, potential, and time. In a SOC (Security Operations Center) near you, analysts are drowning in alerts—most of them require basic investigation, yet each demands careful attention. This endless grind eats away at creativity and morale, leaving real opportunities for proactive defense overlooked.

This is the state of cybersecurity today: the most critical thinkers in your organization are stuck performing work better suited for machines. It doesn't have to be this way.

Imagine a future where AI agents take over the investigative work triggered by alerts from your existing systems, allowing your team to focus on strategic, creative tasks. Welcome to the era of AI agents for non-human security work.

This eBook will define what "non-human security work" is, demonstrate why AI is the perfect solution for automating investigations, and show how this leads to exponentially better security outcomes. It's time to shift your people up—and your organization forward.

1 WHAT IS NON-HUMAN SECURITY WORK (NHSW)?

DEFINING THE TERM

At its core, non-human security work refers to the investigative and operational tasks in cybersecurity that are essential yet repetitive. These tasks are triggered by alerts from detection systems—such as SIEM, EDR, or email gateways—and require thorough but predictable investigation and follow-up actions. While vital, they don't demand the intuition, creativity, or strategic thinking that humans excel at.

Technical Definition:

Non-Human Security Work is the execution of repetitive, scalable investigative tasks triggered by alerts from existing security systems, which can be automated using AI agents to enhance speed, accuracy, and scalability.

Emotional Definition:

It's the work that eats up time and energy—the tasks no one wants to do. By offloading it to AI agents, security teams can reclaim their focus and elevate their impact.

REAL-LIFE EXAMPLE

Meet Sarah, a SOC analyst. Every day, she sifts through alerts flagged by her company's EDR system. Each alert requires her to gather logs, cross-check IP addresses, verify file hashes, and look for indicators of compromise (IoCs). The steps are repetitive, yet critical.

When her team deploys AI agents to automate these investigations, Sarah is finally free to focus on developing response strategies for advanced threats.

2 THE SCOPE OF NON-HUMAN SECURITY WORK

EXAMPLES OF NON-HUMAN SECURITY WORK

Phishing Alert Investigations:

AI agents retrieve email headers, analyze links and attachments, and cross-reference against threat intelligence feeds, escalating only when additional action is required.

EDR Alert Investigation:

AI agents automatically collect and correlate endpoint activity logs, query file hashes against known databases, and enrich alerts with contextual insights for human review.

Threat Intelligence Correlation:

AI agents process threat feeds, match new vulnerabilities (e.g., CVEs) against internal systems, and prioritize relevant actions for remediation.

Comliance Investigations:

AI ensures that audit trails, log collection, and compliance tasks are managed seamlessly, reducing the burden on human teams.

THE NON-HUMAN WORK AI HANDLES BEST

- Correlating alerts with context from multiple systems (e.g., SIEM and EDR).
- Gathering and enriching data to support alert investigations.
- Automating routine responses, such as isolating endpoings or quarantining emails.
- Managing and organizing compliance-realted tasks.

3 HOW AI AGENTS TAKE ON NON-HUMAN SECURITY WORK

THE AI AGENT WORKFLOW

AI agents are designed to investigate and respond to alerts generated by your detection systems. Their workflow includes:

1. **Ingesting Alerts:** Receiving alerts from detection tools like EDR, SIEM, or email gateways.

2. **Gathering Context:** Automatically collecting related data, querying external threat feeds, and enriching alerts with additional data.

3. **Taking Action:** Executing investigation steps by deploying multiple mission-driven agents, operating tools, forming conclusions, and presenting results to other systems, creating tickets, or performing remediation actions.

Technical Deep Dive

Unlike traditional detection systems, AI agents work down-stream, focusing on alert investigations. They don't generate new alerts but instead ensure the alerts you already have are acted upon with precision and speed.

4 THE HUMAN SHIFT: WHAT ANALYSTS CAN DO NOW

THE NEW ROLE OF SECURITY TEAMS

When AI agents handle non-human security work, analysts can focus on tasks that require intuition, strategy, and creativity, such as:

- **Strategic Threat Hunting:** Proactively seeking patterns and behaviors indicative of advanced threats by analyzing broader trends.
- **Incident Response Leadership:** Coordinating responses to escalated incidents with clear and enriched data provided by AI agents.
- **Continuous Improvement:** Developing more effective playbooks and refining investigation workflows to make the entire system more resilient.
- **Proactive Defense:** Testing defenses against emerging threats and simulating potential attack scenarios.

THE SECURITY ANALYST'S DAY BEFORE AND AFTER AI AGENTS

Before AI Agents

- 8 hours spent investigating alerts, gathering data, and performing routine follow-ups.
- 1 hour left for strategic analysis or proactive threat hunting.

After AI Agents

- 1 hour spent reviewing escalations and refining playbooks.
- 7 hours free for advanced threat hunting and strategic initiatives.

5 WHY AI-DRIVEN SECURITY RESULTS IN EXPONENTIALLY BETTER SECURITY OUTCOMES

KEY BENEFITS

1. **Operational Efficiency:** Faster investigation and resolution of alerts, reducing time to response (MTTR).

2. **Analyst Potential Unlocked:** Analysts focus on high-value, engaging work rather than repetitive investigations.

3. **Scalability:** AI agents handle an ever-increasing volume of alerts without adding headcount.

4. **Consistency:** Automated AI flows ensure consistent investigation, reducing errors.

SUCCESS METRICS: AI AGENTS IN ACTION

- 90% reduction in time spent on alert investigations.
- 70% faster resolution of low-priority incidents.
- Significant improvements in employee satisfaction and retention among SOC analysts.

6 BUILDING THE AI-NATIVE SECURITY TEAM

ADOPTING AI AGENTS

Organizations must approach AI adoption thoughtfully:

- Start with high-volume, low-complexity alert investigations (e.g., phishing or EDR alerts).
- Gradually expand to more complex workflows, such as orchestrating multi-step responses.

Cultural Shifts

Help your team see AI agents as partners, not replacements. Highlight how these tools augment their abilities and allow them to focus on meaningful work.

CASE STUDIES

STREAMLINING USER-REPORTED PHISHING INVESTIGATIONS

Customer Profile:

A mid-sized financial institution struggled to manage phishing emails reported by employees. Their SOC team received hundreds of user-reported phishing alerts daily, most of which required manual investigation to verify legitimacy. This repetitive process consumed over 50 hours per week, leaving little time for proactive threat hunting or response planning.

Solution:

The institution implemented 7AI agents to handle the investigation of user-reported phishing emails. Whenever an employee flagged an email, the AI agent automatically retrieved email headers, analyzed attachments in a sandbox, and cross-referenced links against external threat intelligence feeds. The agent categorized emails as safe, suspicious, or confirmed phishing attempts, escalating only the latter two to analysts.

Outcome:

Within the first month, the organization reduced its manual phishing investigation workload by 85%. Analysts were able to focus on actionable escalations while response times for genuine phishing attempts dropped from hours to just minutes. Employee trust in the security team improved as a result of faster feedback on their reports.

Customer Quote:

"*Our employees rely on us to validate suspicious emails, but the volume of reports was overwhelming. The AI agents FROM 7AI transformed how we handle phishing investigations, ensuring faster responses and more time for our team to focus on critical threats.*"

– Director of Cybersecurity Operations

ACCELERATING EDR ALERT TRIAGE AND CONTEXT

Customer Profile:

A global manufacturing company struggled to manage the high volume of alerts generated by their EDR platform. Analysts spent countless hours gathering logs, correlating alerts, and investigating file hashes—tasks that were essential but repetitive.

Solution:

7AI agents were deployed to ingest EDR alerts, automatically collect contextual data (e.g., endpoint activity logs, related IP addresses), and enrich findings with threat intelligence. For high-confidence alerts, the agents suggested containment actions such as isolating endpoints or blocking processes.

Outcome:

The company saw a 70% reduction in the time required to triage EDR alerts. Analysts reported greater job satisfaction as they shifted their focus to proactive threat hunting and incident response.

Customer Quote:

"*7AI agents took over the grunt work of triaging EDR alerts, allowing us to focus on higher-value tasks. Our team feels more empowered, and our incident response times have never been faster.*"

– SOC Manager

ENHANCING THREAT INTELLIGENCE CORRELATION

Customer Profile:

A healthcare organization was overwhelmed by the constant influx of threat intelligence feeds. Matching these feeds against internal telemetry required manual effort, and critical vulnerabilities were often delayed in being addressed.

Solution:

AI agents were deployed to ingest and correlate external threat intelligence feeds with the organization's internal logs and vulnerability data. The agents prioritized CVEs and flagged systems requiring immediate remediation.

Outcome:

The organization improved its remediation timeline by 50% and reduced the number of overlooked vulnerabilities. Security teams were able to focus on creating stronger proactive defense strategies.

Customer Quote:

"*7AI agents gave us a way to stay ahead of the flood of threat intelligence. They connected the dots we never had time to, and we now address critical vulnerabilities much faster.*"

– Chief Information Security Officer

INVESTIGATING IDENTITY ALERTS WITH CONTEXTUAL AI AUTOMATION

Customer Profile:

A technology company with a hybrid workforce faced a high volume of identity-related alerts from their identity and access management (IAM) system. Alerts such as unusual login patterns, impossible travel events, and failed multi-factor authentication (MFA) attempts required manual follow-up by analysts to confirm whether they were legitimate or indicative of account compromise.

Solution:

AI agents were deployed to investigate identity alerts automatically. When an alert was triggered, the AI agent gathered contextual data, such as login timestamps, IP geolocation, and recent activity on the account. The agent correlated this data with known patterns, verified authentication logs, and flagged only cases that required human review or immediate remediation.

Outcome:

The SOC team reduced time spent investigating identity alerts by 75%, freeing analysts to focus on improving IAM policies and responding to confirmed incidents. The reduced investigation time also significantly lowered the mean time to respond (MTTR) to potential account compromises.

Customer Quote:

"*Before 7AI, every identity alert meant hours of log analysis to determine risk. Now, the agents handle the investigations, giving us clear, actionable insights without the noise. Our team can now focus on building a stronger identity defense strategy.*"

– SOC Manager

AUTOMATING CLOUD SECURITY ALERT INVESTIGATIONS

Customer Profile:

A fast-growing e-commerce company using a multi-cloud infrastructure faced constant alerts from their cloud security monitoring tools. Alerts included anomalous API calls, unexpected resource configurations, and suspected policy violations. The sheer volume and complexity of alerts made manual investigations slow and error-prone.

Solution:

AI agents were integrated with the cloud monitoring tools to investigate alerts autonomously. For each alert, the AI agent pulled relevant logs, queried configurations, cross-referenced known vulnerabilities, and identified whether the activity aligned with legitimate business operations. In cases of clear violations, the agent automatically reverted misconfigurations or escalated for further review.

Outcome:

The company achieved a 60% reduction in manual cloud alert investigations, improving the security team's ability to respond to critical misconfigurations and potential breaches. Automated remediation of low-risk misconfigurations also ensured continuous compliance without disrupting operations.

Customer Quote:

"*Our cloud environment is constantly evolving, and the volume of alerts made it hard to keep up. AI agents gave us the tools to quickly investigate and remediate issues, ensuring our cloud stays secure while we scale.*"

– Cloud Security Architect

A FUTURE WITHOUT LIMITS

Cybersecurity doesn’t have to be a battle against monotony. By offloading non-human security work—automating investigations and repetitive tasks triggered by alerts—AI agents unlock a future where human creativity and machine precision combine to deliver unparalleled security outcomes.

It’s time to embrace this shift—because the threats won’t wait, and neither should your team.

ABOUT 7AI

7AI is the leader in **agentic security**, bringing a **swarming ecosystem of AI agents** to the fight against cyber threats. With the first-ever ecosystem of AI security agents, 7AI delivers bespoke precision at machine speed—tailored to your environment, workflows, and needs. This is security that works like you do: fast, adaptive, and focused on outcomes that matter.

LEARN MORE AT 7AI.COM