

# XSIAM a AgentiX

## nová éra inteligentného SecOps

**Luboš Klokner** | Solutions Consultant

---

November 2025

# Need for SOC

## Invisibility of Threats

- Attackers today masquerade as legitimate traffic
- Without a centralized surveillance (SOC), you only see fragments, not the full picture of the attack

## Speed and Volume

- We are faced with thousands of alerts every day
- Human capacity is no longer sufficient to manually sort out what is a false alarm and what is a critical incident

## Regulations and Trust

- With the advent of directives like NIS2, security is no longer just an 'IT issue'
- IT and Cyber Security is a legal obligation and a question of brand survival.



- Home
- Dashboard
- Alerts
- Incidents
- Investigation
- Reporting
- Settings
- Help

Data Inventory

Good Afternoon, Lubos

4,553

ENDPOINTS

Microsoft

Google

Amazon

Facebook

Twitter

LinkedIn

Instagram

YouTube

WhatsApp

+7

DATA SOURCES

2,662  
ISSUES

280  
ISSUES

286K

PREVENTED  
EVENTS

12  
CASES

122  
CASES

Events Ingestion

5 B/24H

EventsData Ingestion

43 B/7 TB/24H

DataTotal-Open Cases

65 23/24H

C 3 H 3 M 4 L 1

2 30.5K

COLLECTION ERRORS  
PREVENTED EVENTS



- Settings
- Grid
- Alerts
- Help

LK



anthropic.com

AI

ResearchEconomic FuturesCommitmentsLearnNews

Try Claude

Policy

# Disrupting the first reported AI-orchestrated cyber espionage campaign

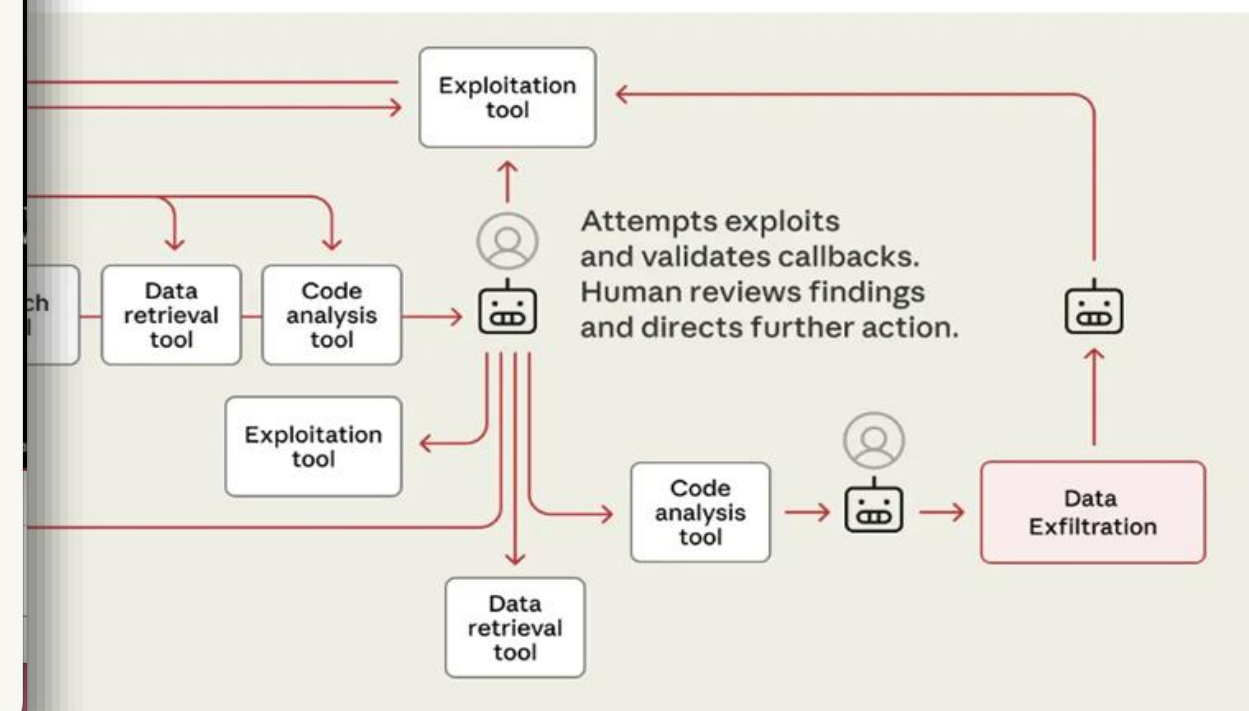
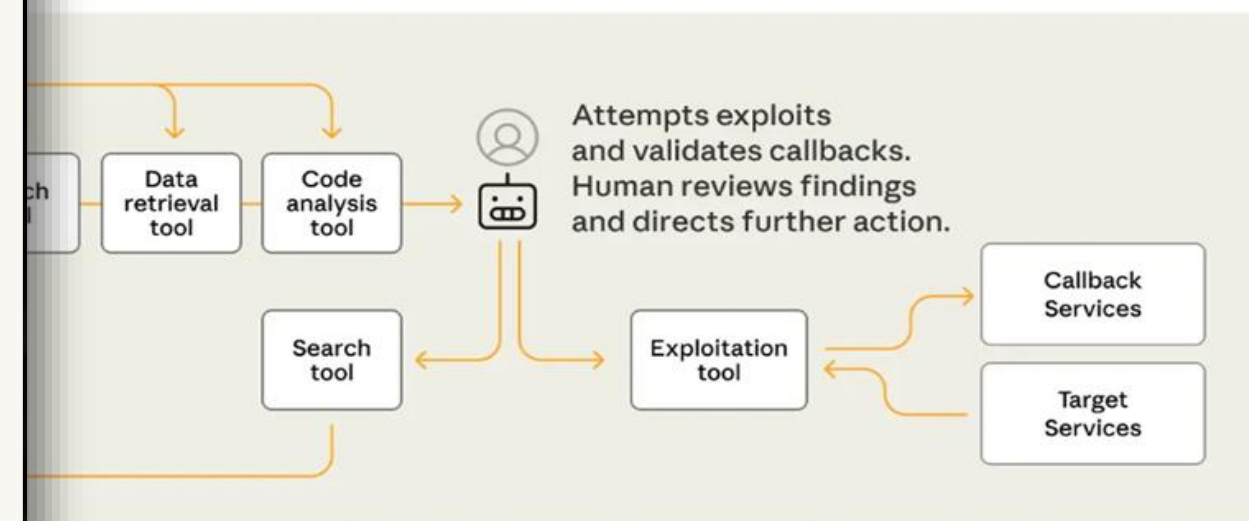
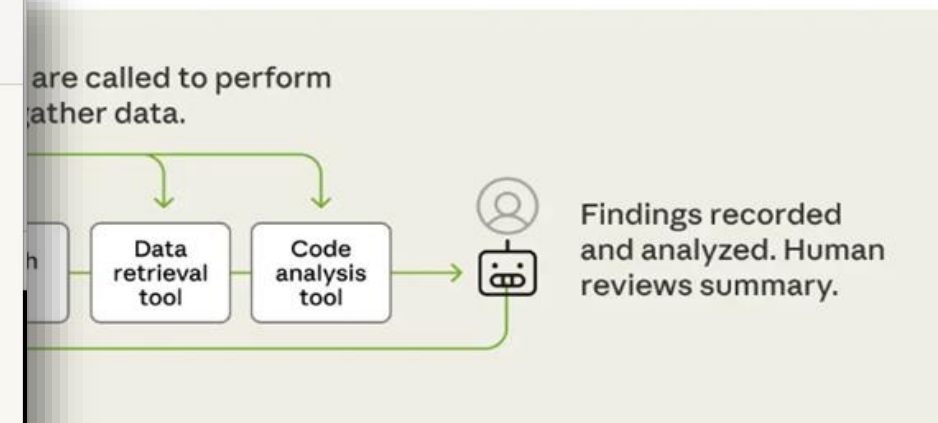
13 Nov 2025 • 7 min read

Read the report

We recently argued that an inflection point had been reached in cybersecurity: a point at which AI models had become genuinely useful for cybersecurity operations, both for good and for ill. This was based on systematic evaluations showing cyber capabilities doubling in six months; we'd also been tracking real-world cyberattacks, observing how malicious actors were using AI capabilities. While we predicted these capabilities would continue to evolve, what has stood out to us is how quickly they have done so at scale.

In mid-September 2025, we detected suspicious activity that later investigation determined to be a highly sophisticated espionage campaign. The attackers used AI's "agentic" capabilities to an unprecedented degree—using AI not just as an advisor, but to execute the cyberattacks themselves.

The threat actor—whom we assess with high confidence was a Chinese state-sponsored group—manipulated our Claude Code tool into attempting infiltration into roughly thirty global targets and succeeded in a small number of cases. The operation targeted large tech companies, financial





Dashboard

Alerts

Visualize

Settings

Help

EM

2,234  
PRE-CONFIGURED  
TRIGGERS

Automations  
2,234 Plans

598  
USER PROMPTS



Email Investigation Agent  
158 Plans



Endpoint Investigation Agent  
154 Plans



Network Security Agent  
91 Plans



Threat Intel Agent  
113 Plans



IT Agent  
60 Plans



+ 8 Other Agents

94%  
2,656  
FULLY EXECUTED  
PLANS

176  
PLANS TO  
REVIEW

Total Open Cases  
57  
Start Investigation

Cases Resolved with Agentix  
81%

MTTR  
42Min

External Interactions  
3,523





# Agentix Hub

Agents


Actions


Search in Enabled Agents 




+ Build a New Agent

Enabled Agents (8 of 19)


Sort by Creation time 

- 


**Threat Intel**  
By Cortex




Gathers fresh threat data, enriches indicators and vulnerabilities, links them to past or current incidents, and publishes clear briefings so the whole SOC acts on the latest...

15 Actions
- 


**Network Security**  
By Cortex




Manages Palo Alto Networks Panorama and Firewalls, as well as third-party network security products. Streamlines work for network security engineers by performing...

20 Actions
- 


**IT**  
By Cortex




Automates identity lifecycle enforcement, real-time containment on endpoints and networks, vulnerability and patch governance, asset intelligence upkeep, and end-to-...

16 Actions
- 


**Endpoint Investigation**  
By Cortex




Unifies host-level containment, forensic collection, and remediation across all major EDR/XDR platforms while feeding evidence and status into the SOC's ticketing and...

24 Actions
- 


**Email Investigation**  
By Cortex



Automates the full lifecycle of email-borne threat response, spanning mailbox search, forensic collection, analysis, containment, and incident closure across all major mail...

15 Actions
- 

**Triage and Escalation Agent**  
By twaizman@paloaltonetworks.com



This agent enriches incidents and sets severity and assignment according to initial triage

Action Center +2 25 Actions

94 %

2,656

FULLY EXECUTED PLANS

176

PLANS TO REVIEW

Actions

Gmail





Good afternoon Emran,  
How can I help you today?



From this Unit 42 post - <https://unit42.paloaltonetworks.com/medusa-ransomware-escalation-new-leak-site/> - extract the file IOCs, enrich them, check for sightings in our tenant and related alerts/issues, then give me clear lists plus a brief summary, and email it to me.

94%

2,656

## FULLY EXECUTED PLANS

176

## PLANS TO REVIEW

# Thank You

---

[paloaltonetworks.com](https://paloaltonetworks.com)