

Building an  
**Agentic Threat Intel System**



daemon.ajvanbeest.com

github.com/theaj42

- presentations

- sourdough.ai

ajvanbeest@protonmail.com

Threat intel is *hard*

25 Focused threat actors

8 APTs

11,275 discrete applications

Also, there's “news.”

Whaddya mean, *Agentic*?

The system is empowered:

It can make choices  
and take actions...

...without consulting a human.



So I built a *thing*

## Setup

Vuln scanner: Identify installed software packages

Find the vendor's security info page

Build durable data collector

## Daily Processing

Collect vendor security data

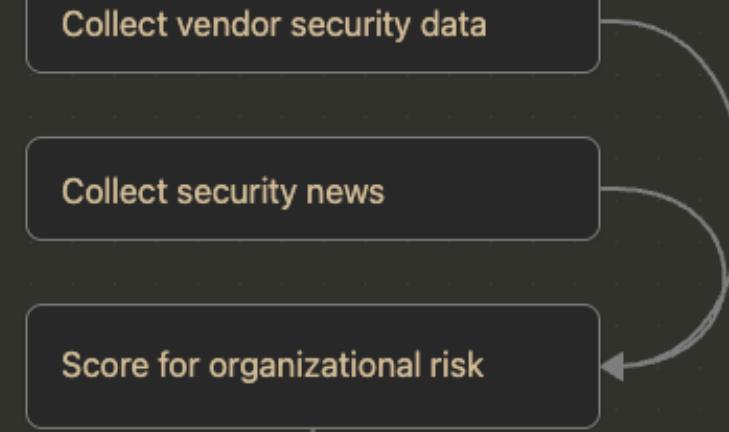
Collect security news

Score for organizational risk

Update dashboard

Update auditable CTI review log

Digest to Teams channel



# Threat Intelligence Monitor

## Vulnerability Intelligence & Trend Analysis

Critical Today

0

High Today

6

Total Threats

60

Avg Time to Ingest

5.1h

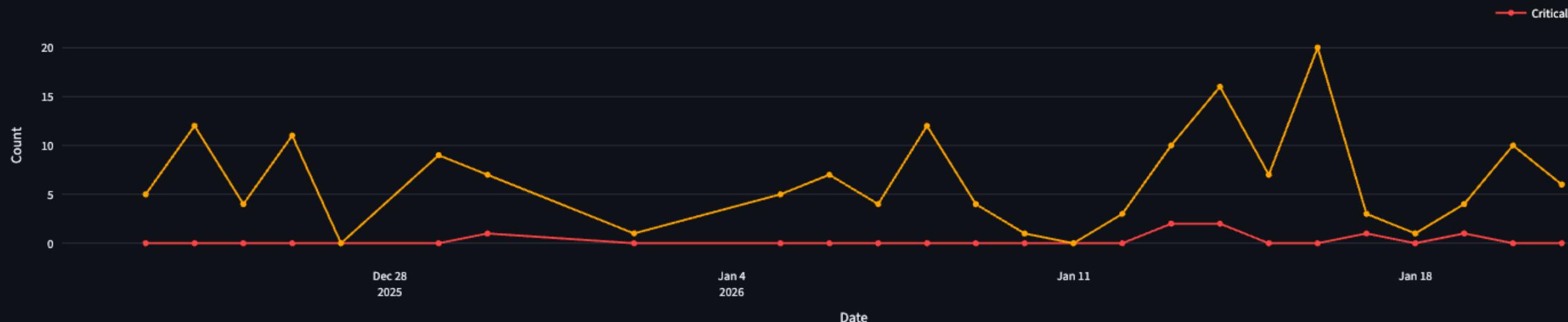
Last Updated

09:02 PST

### Vulnerability Trends

30 Days   6 Months   2 Years

#### Threat Volume - Last 30 Days



# Recent Threats

[Download Threats CSV](#)

Severity	Title	Source	Published	Ingested	Score
⚠ HIGH	Fake Lastpass emails pose as password vault backup alerts	BleepingComputer	2026-01-21 03:58	2026-01-21 09:02	100
⚠ HIGH	Microsoft shares workaround for Outlook freezes after Windows update	BleepingComputer	2026-01-21 02:12	2026-01-21 08:02	95
⚠ HIGH	Cisco Unified Communications Products Remote Code Execution Vulnerability	Cisco	2026-01-21 08:00	2026-01-21 08:02	90
⚠ HIGH	Hackers exploit security testing apps to breach Fortune 500 firms	BleepingComputer	2026-01-21 01:00	2026-01-21 07:02	85
⚠ HIGH	You Got Phished? Of Course! You're Human...	BleepingComputer	2026-01-21 01:30	2026-01-21 07:02	80
⚠ HIGH	The hidden cost of PKI: Why certificate failures aren't just an IT problem	CyberArk	2026-01-21 05:17	2026-01-21 06:01	75
⚠ HIGH	CVE-2026-20848 Windows SMB Server Elevation of Privilege Vulnerability	Microsoft MSRC	2026-01-20 00:00	2026-01-20 16:01	70
⚠ HIGH	CVE-2026-20830 Capability Access Management Service (camsvc) Elevation of Privilege Vulnerability	Microsoft MSRC	2026-01-20 00:00	2026-01-20 16:01	65
⚠ HIGH	Supreme Court to consider whether geofence warrants are constitutional	The Record	2026-01-20 11:05	2026-01-20 12:02	60
⚠ HIGH	VoidLink cloud malware shows clear signs of being AI-generated	BleepingComputer	2026-01-20 06:35	2026-01-20 12:02	55

# Threat Details

Select a threat to view details:

Microsoft shares workaround for Outlook freezes after Windows update

Microsoft shares workaround for Outlook freezes after Windows update

Score Breakdown:

🔗 Source: [BleepingComputer](#)

- Total Score: 3/5

Synopsis:

- Relevance: 5

Microsoft shared a temporary workaround for customers experiencing Outlook freezes after installing this month's Windows security updates. [...]

- Exploitation: 1

- Severity: 3

- Targeting: 1

Timeline:

- Published: 2026-01-21 02:12 PST

- Ingested: 2026-01-21 08:02 PST

# Exposure Analysis

Query Qualys VMDR to check if any Dexcom assets are affected by a specific CVE.

**Found 15 CVEs in critical/high threats**

Select CVE to check exposure:

CVE-2026-0901

 Check Qualys Exposure



## Threat Intel Digest - 2026-01-21 ...



0 Critical



0 High



9 Medium



### Medium Priority

- [Make Identity Threat Detection your security strategy for 2026](#)
- [Hackers target Afghan government workers with fake correspondence from senior officials](#)
- [How the future of privilege is reshaping compliance](#)
- [Gemini AI assistant tricked into leaking Google Calendar data](#)
- [EU plans cybersecurity overhaul to block foreign high-risk suppliers](#)

...and 4 more.

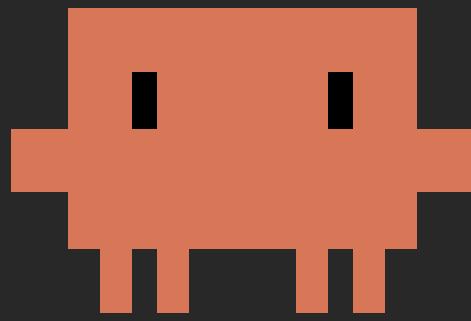
---

AJ Van Beest used a Workflow template to send this card.  
[Get template](#)

The *patterns*

Use good tools

```
❯ claude --dangerously-skip-permissions
```



Claude Code v2.1.14  
Opus 4.5 · Claude Max  
/Users/███████

Use spec-driven development:

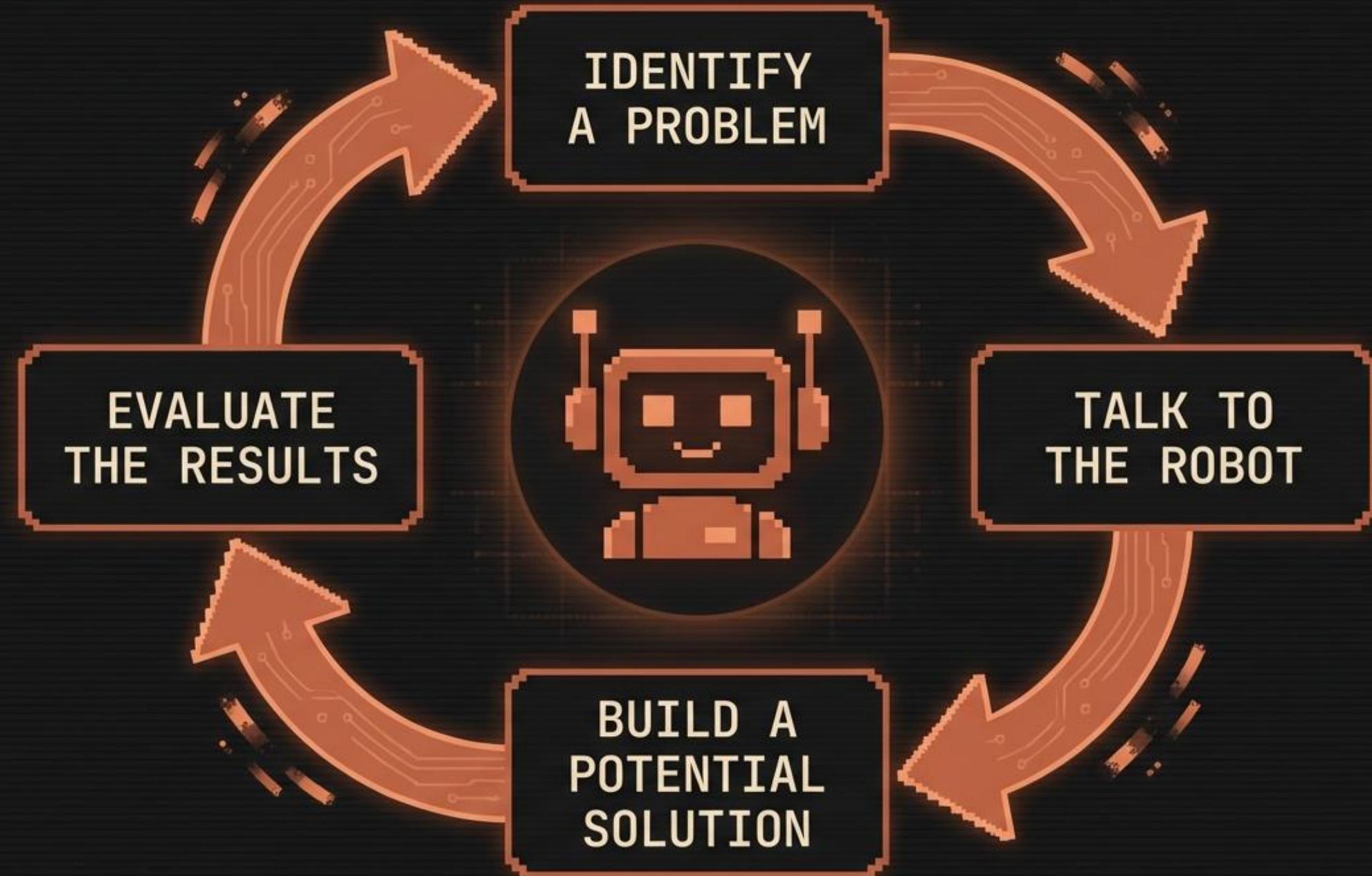
*What* vs. How

# Use real data

What is “Good?”

Let the robot cook

Your turn: *A cookbook*



Tip: \*Talk\* to the robot

Tip: \*Ask\* the robot

**CRITICAL NOTE...**

You own the outcome

# Kthxbye

[daemon.ajvanbeest.com](http://daemon.ajvanbeest.com)

[github.com/theaj42](https://github.com/theaj42)

[ajvanbeest@protonmail.com](mailto:ajvanbeest@protonmail.com)