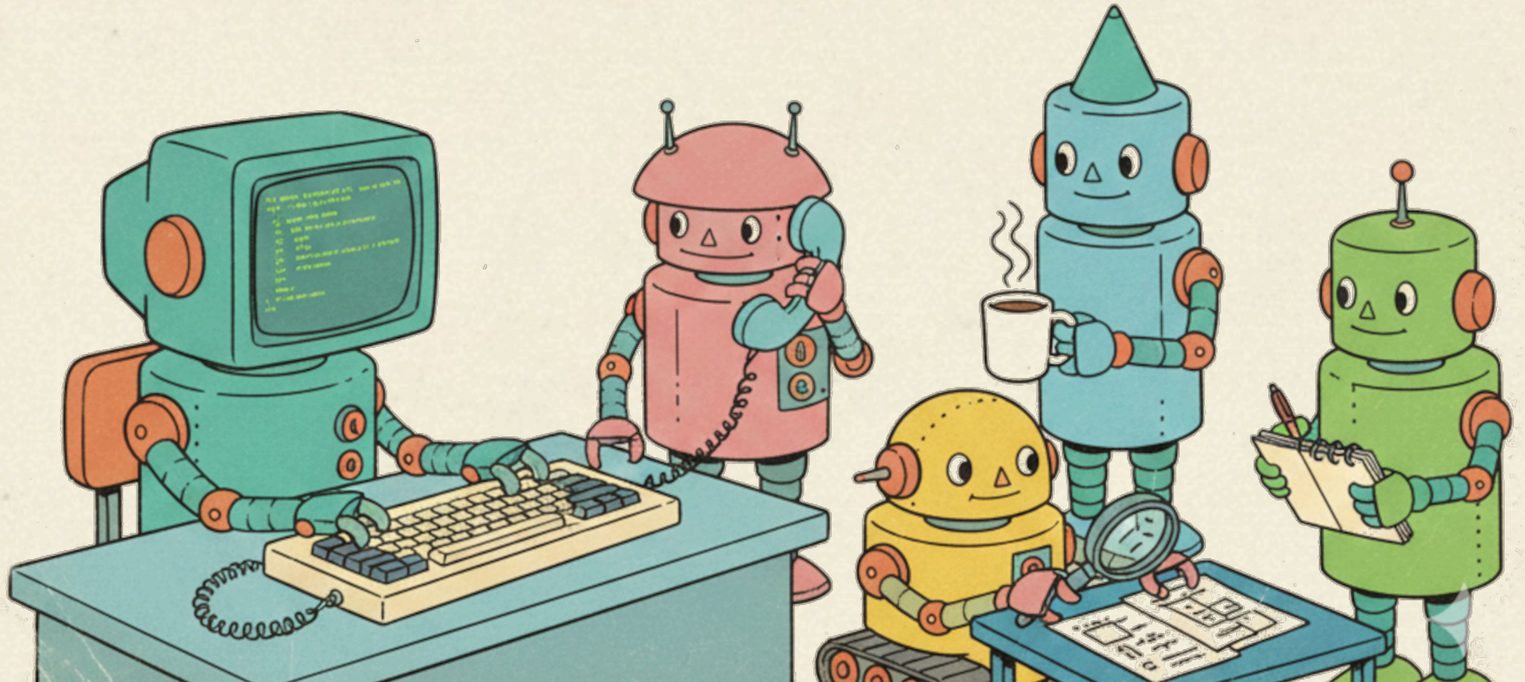
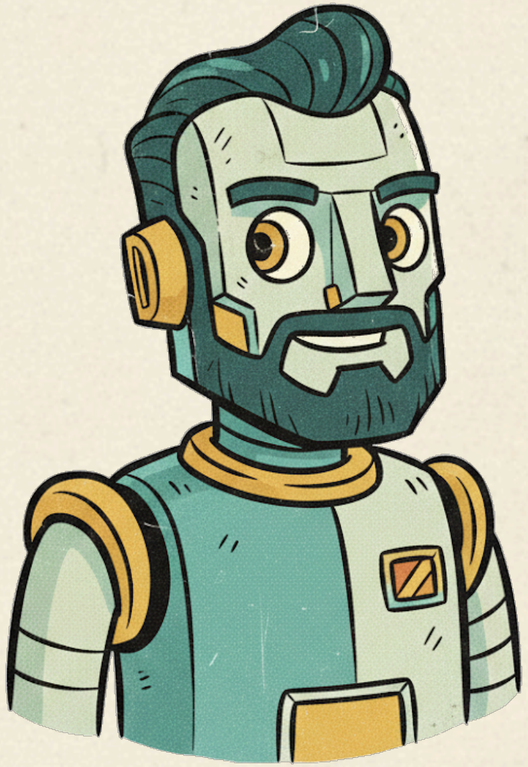
HOW TO WRITE SOC TICKETS THAT BUILD TRUST AND DRIVE ACTION



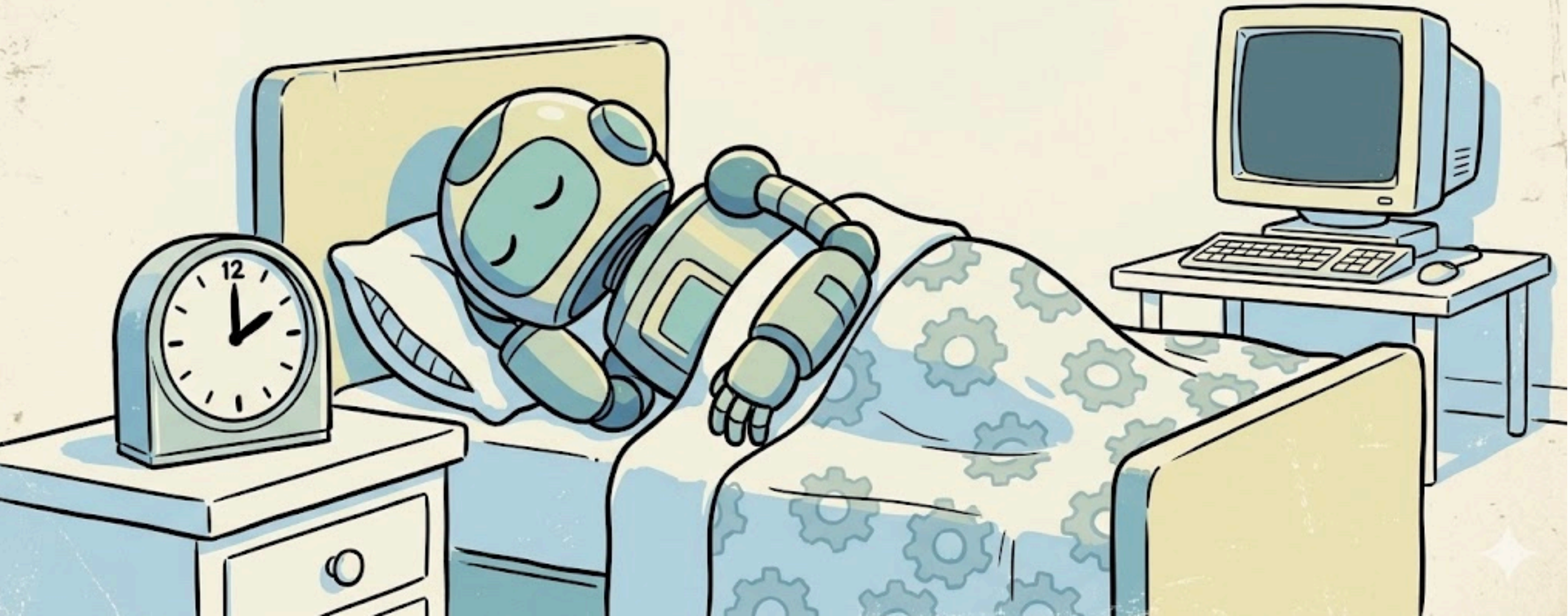
ABOUT ME

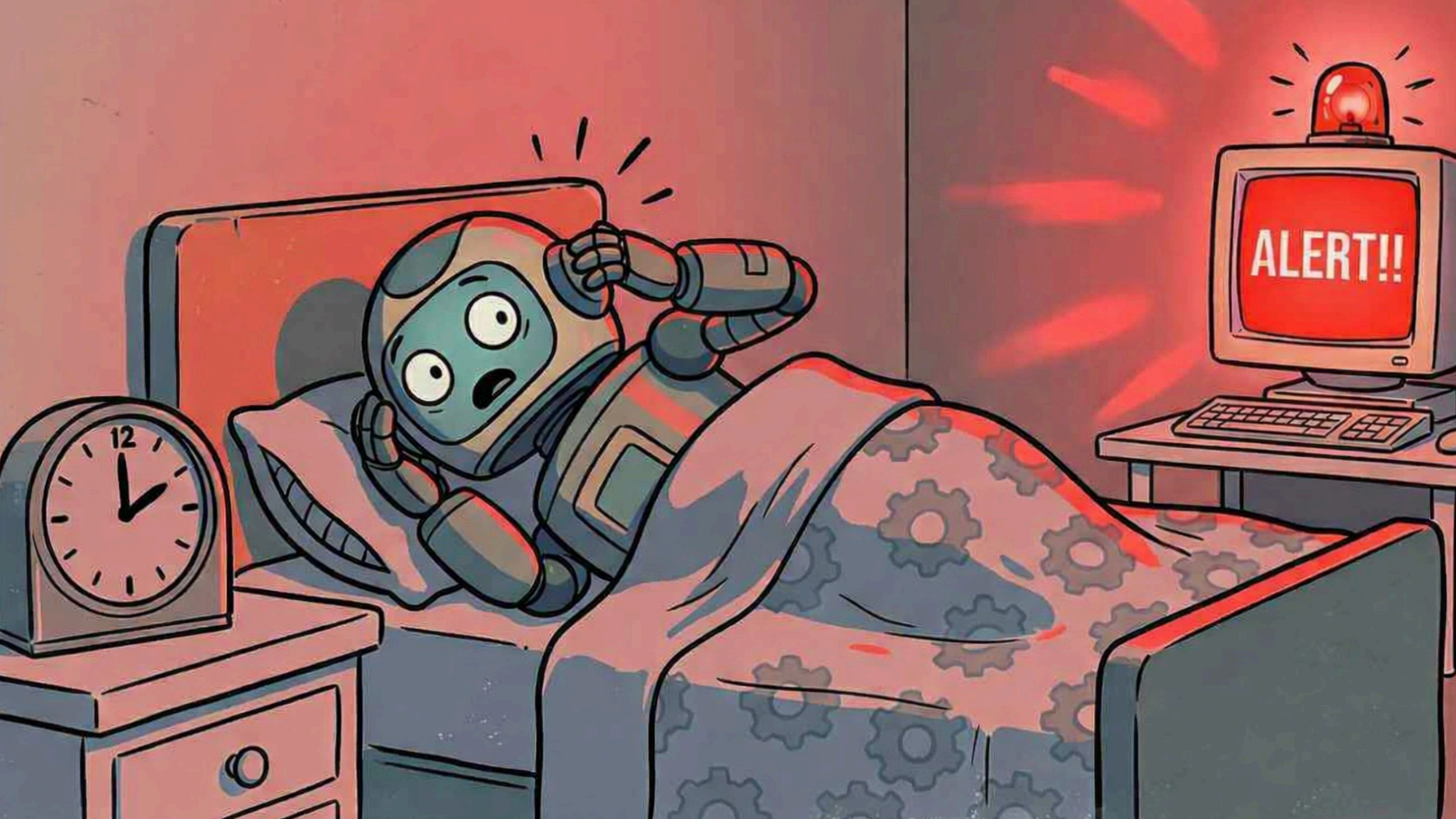
- SOC Analyst Tier II @ ProCircular
- 2500+ SOC ticket triaged
- Husband and Father
- Writer of Cyber Security Articles
- Creator of MEMEs

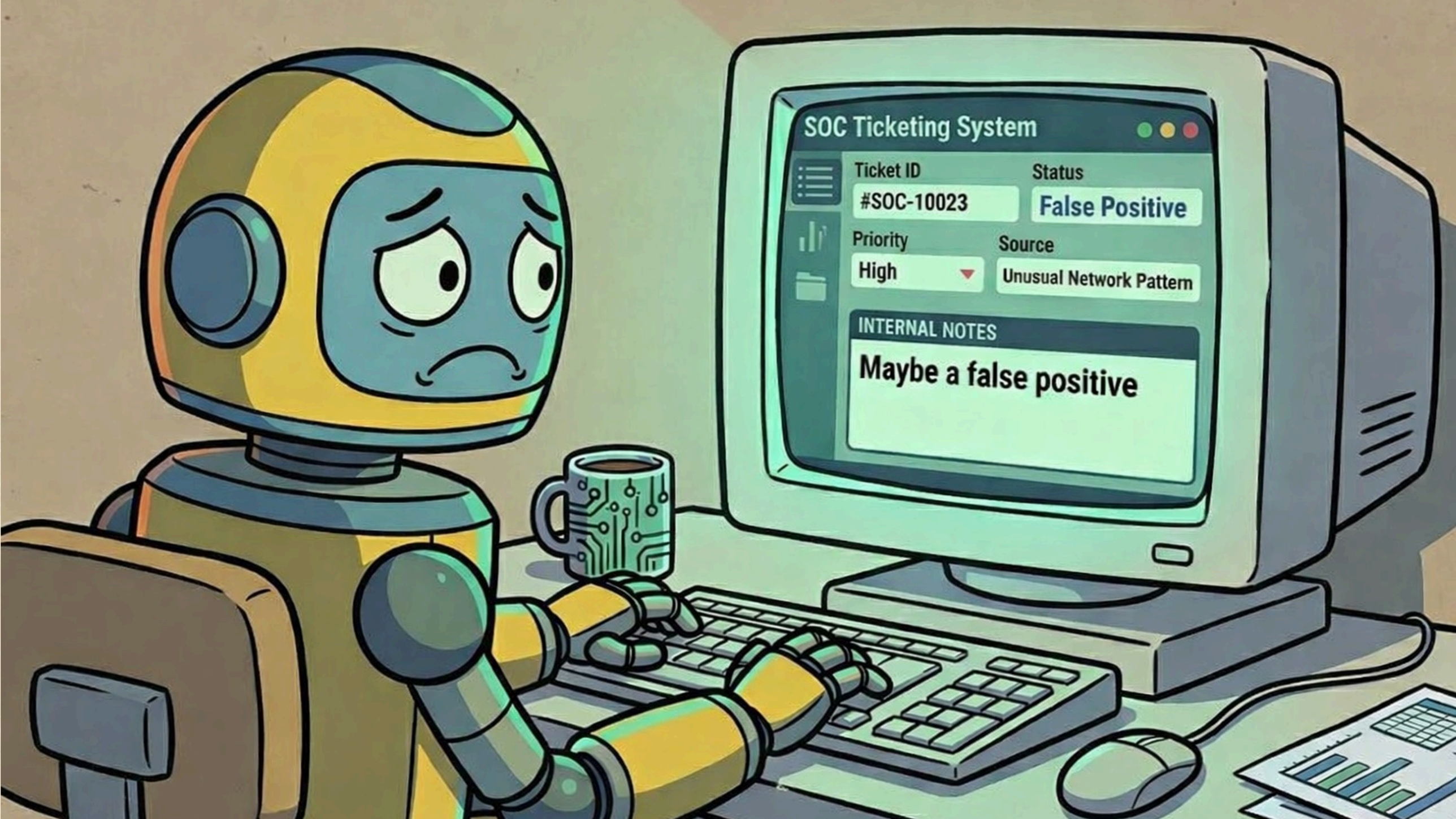
BHIS Survival Guide
SOC Edition
https://www.blackhillsinfosec.com/prompt-zine/prompt-issue-infosec-survival-guide-blue-book/



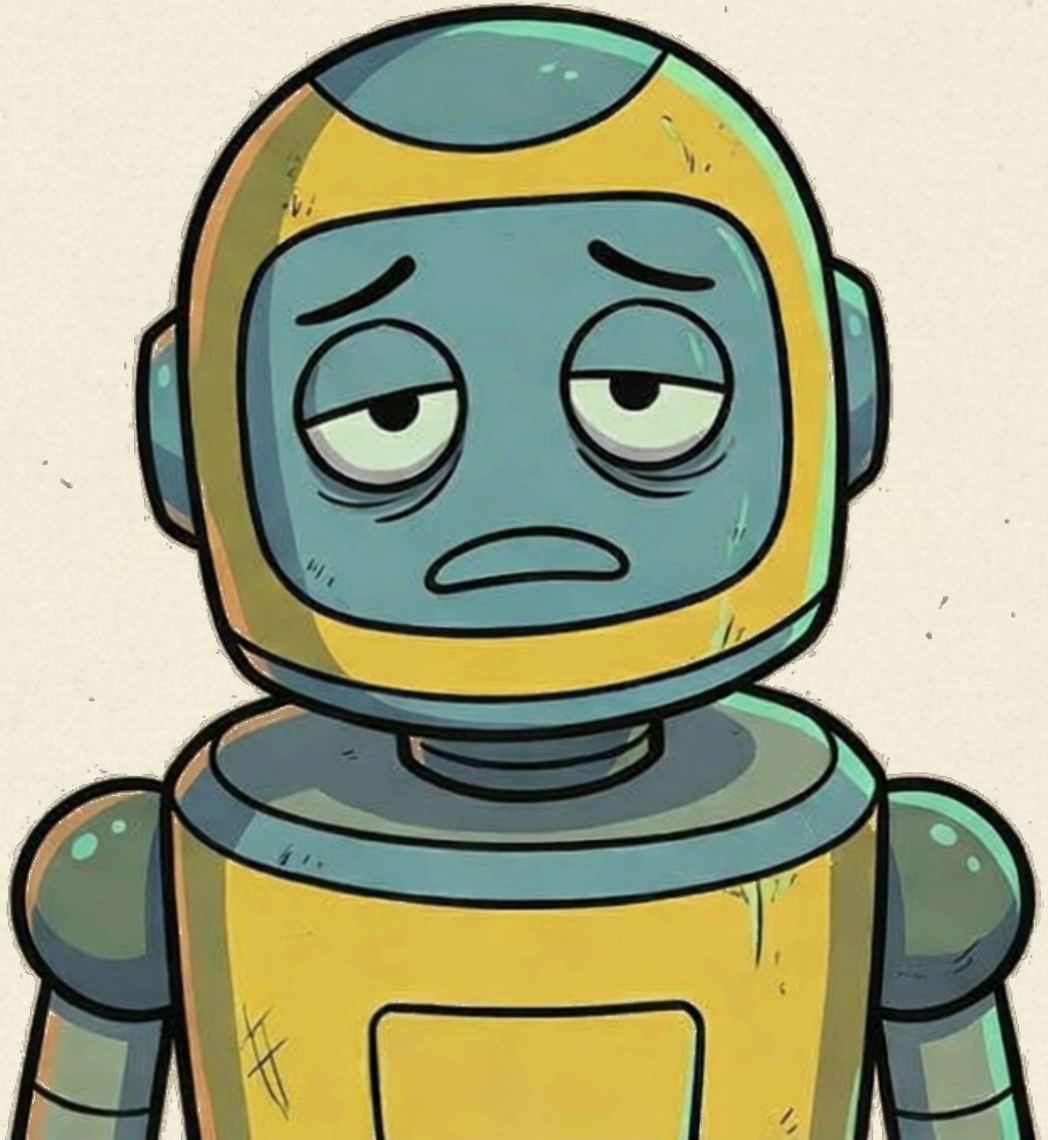
IT'S 2 AM..... AND YOUR ON-CALL



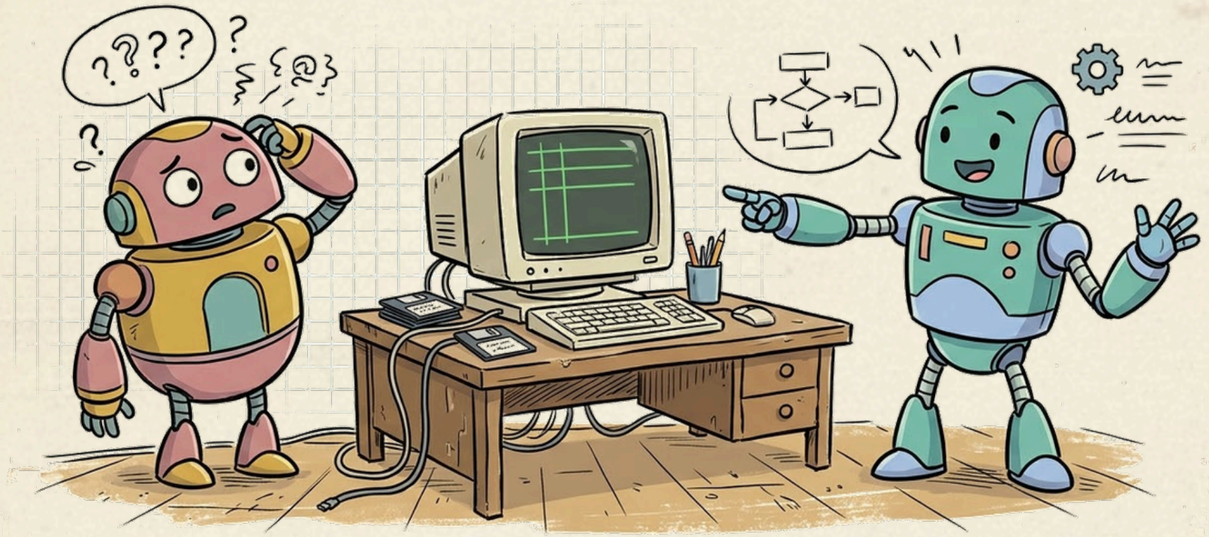

12
ALERT!!


SOC Ticketing System
Ticket ID
#SOC-10023
Status
False Positive
Priority
High
Source
Unusual Network Pattern
INTERNAL NOTES
Maybe a false positive

HAS THIS HAPPENED TO YOU?



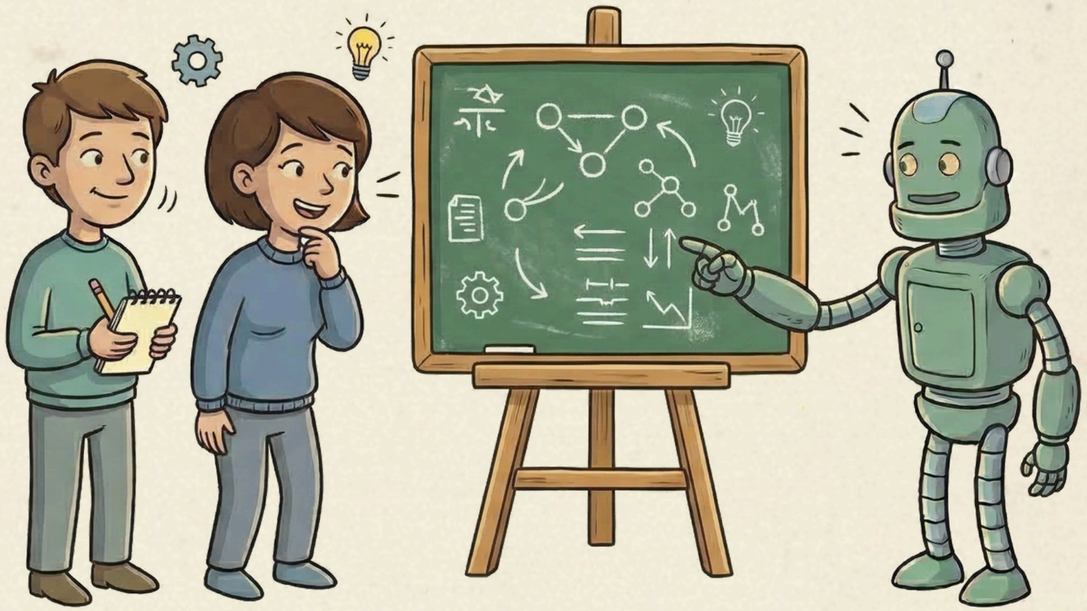
BEYOND THE TERMINAL



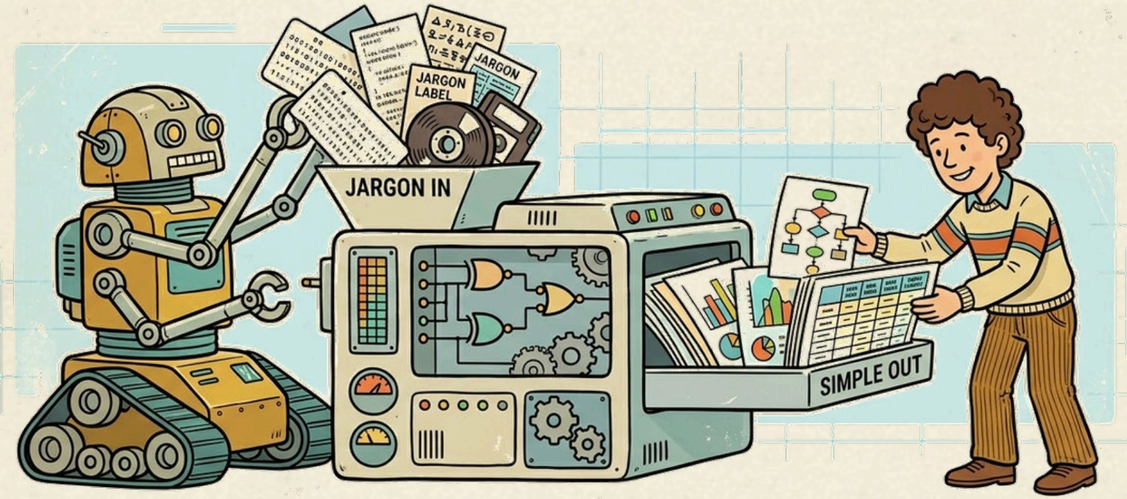
- Core Elements
- Technical Translator
- Ripple Effect
- Build Subroutines

TALKING TO HUMANS

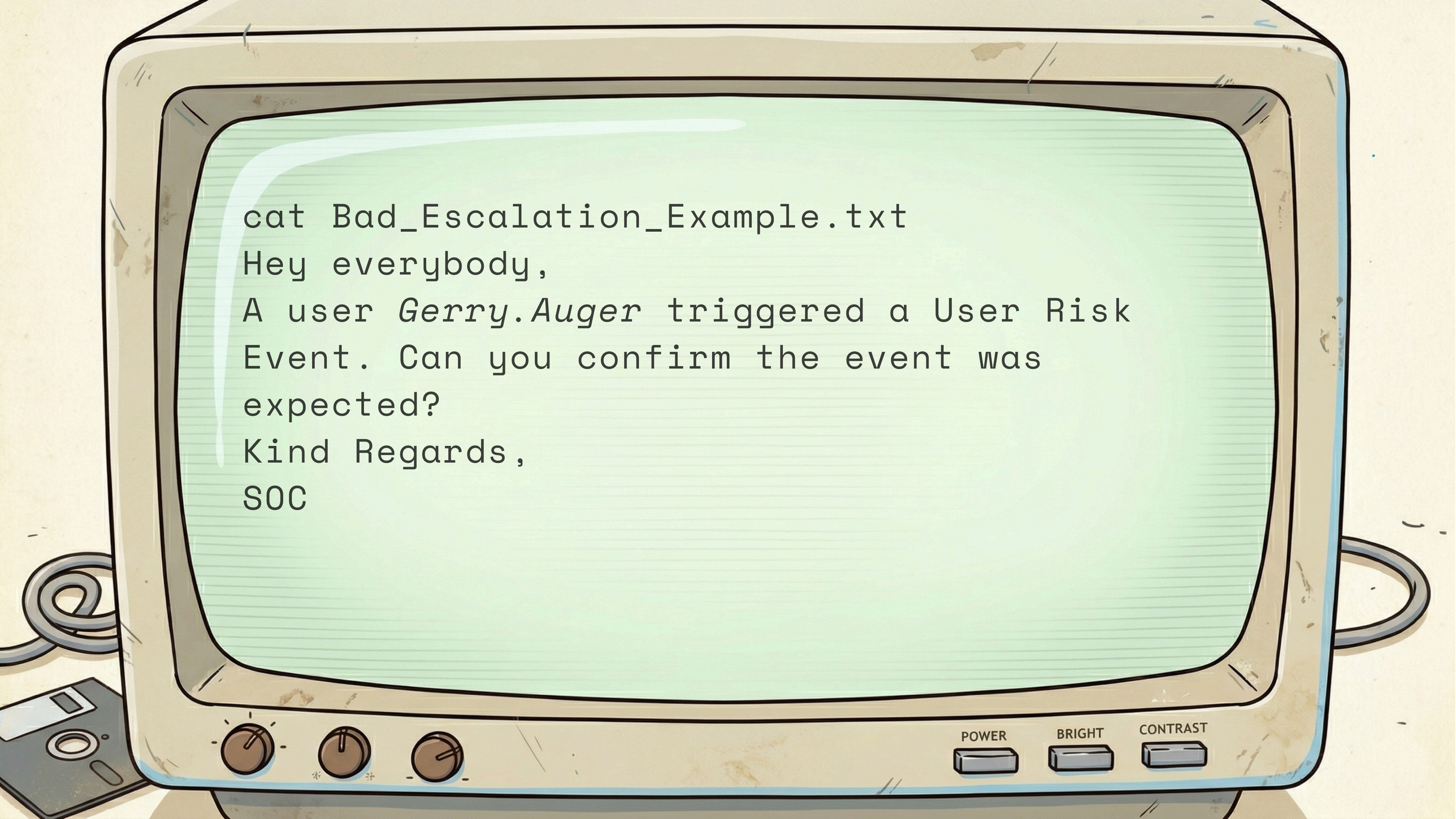
- Multi-Channel Analyst
  - Internal Team
  - External/Leadership
- MTTU

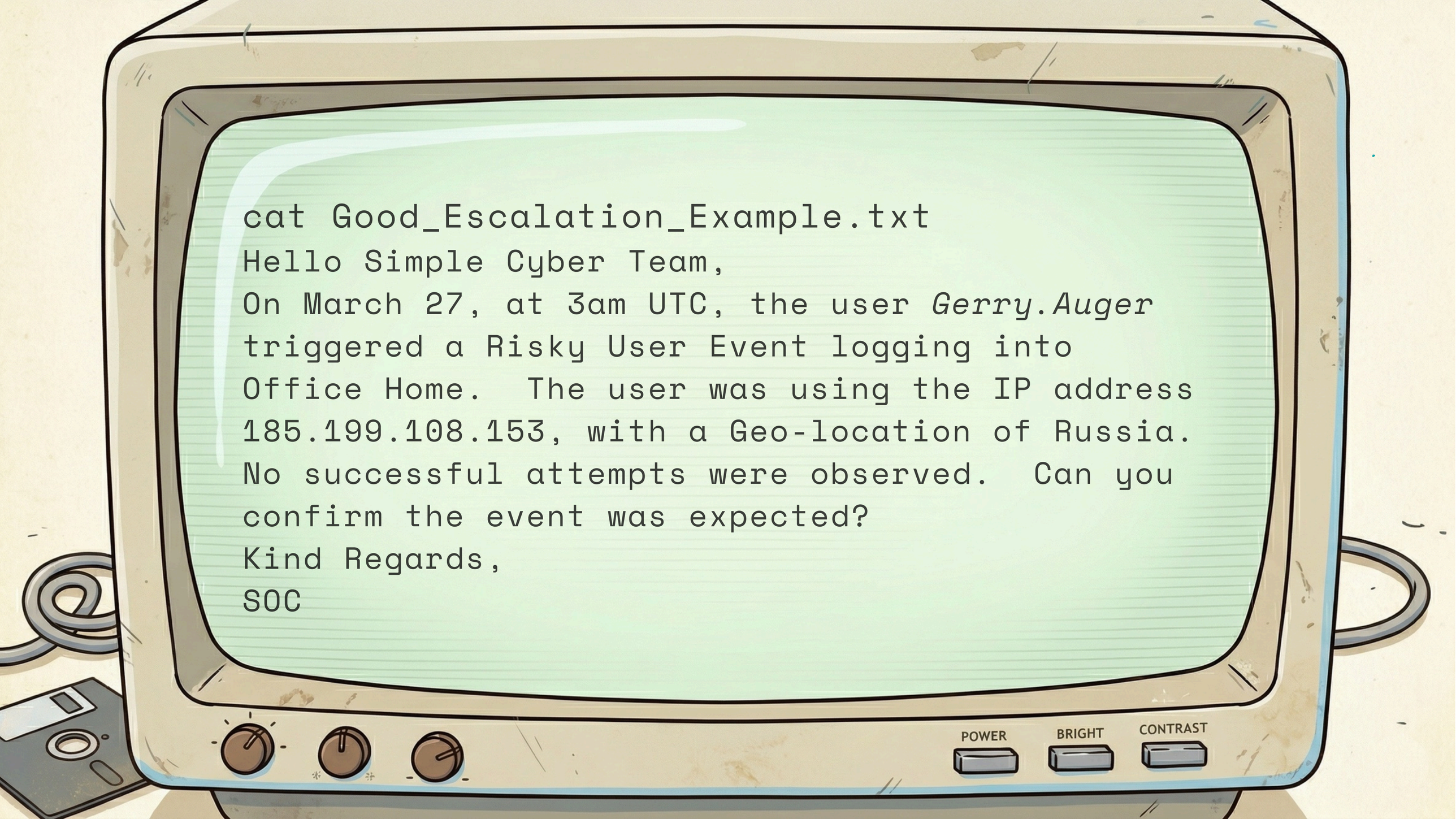


REBOOT YOUR VOCABULARY

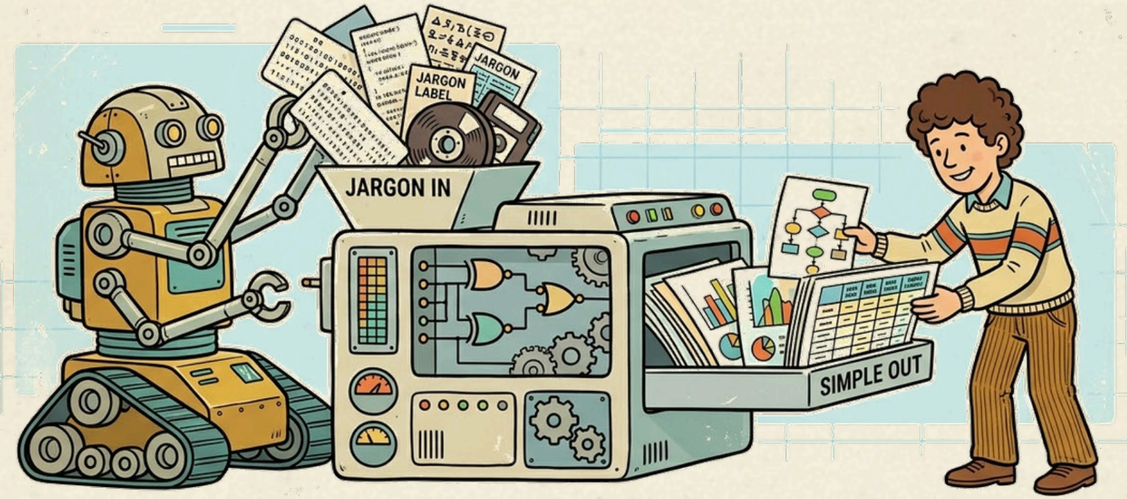


- Internal Power
- Know Your Audience
- Faucet Vs. Fire Hose


cat Bad_Escalation_Example.txt
Hey everybody,
A user *Gerry.Auger* triggered a User Risk Event. Can you confirm the event was expected?
Kind Regards,
SOC
POWER
BRIGHT
CONTRAST


cat Good_Escalation_Example.txt
Hello Simple Cyber Team,
On March 27, at 3am UTC, the user *Gerry.Auger* triggered a Risky User Event logging into Office Home. The user was using the IP address 185.199.108.153, with a Geo-location of Russia. No successful attempts were observed. Can you confirm the event was expected?
Kind Regards,
SOC
POWER
BRIGHT
CONTRAST

REBOOT YOUR VOCABULARY

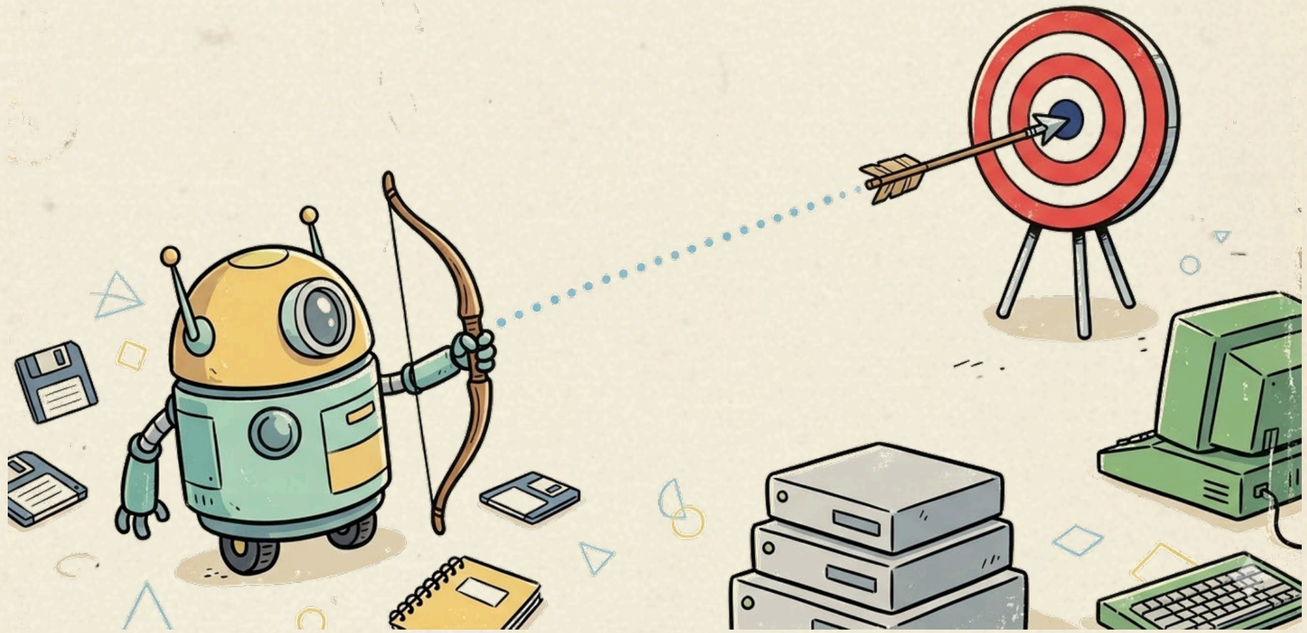


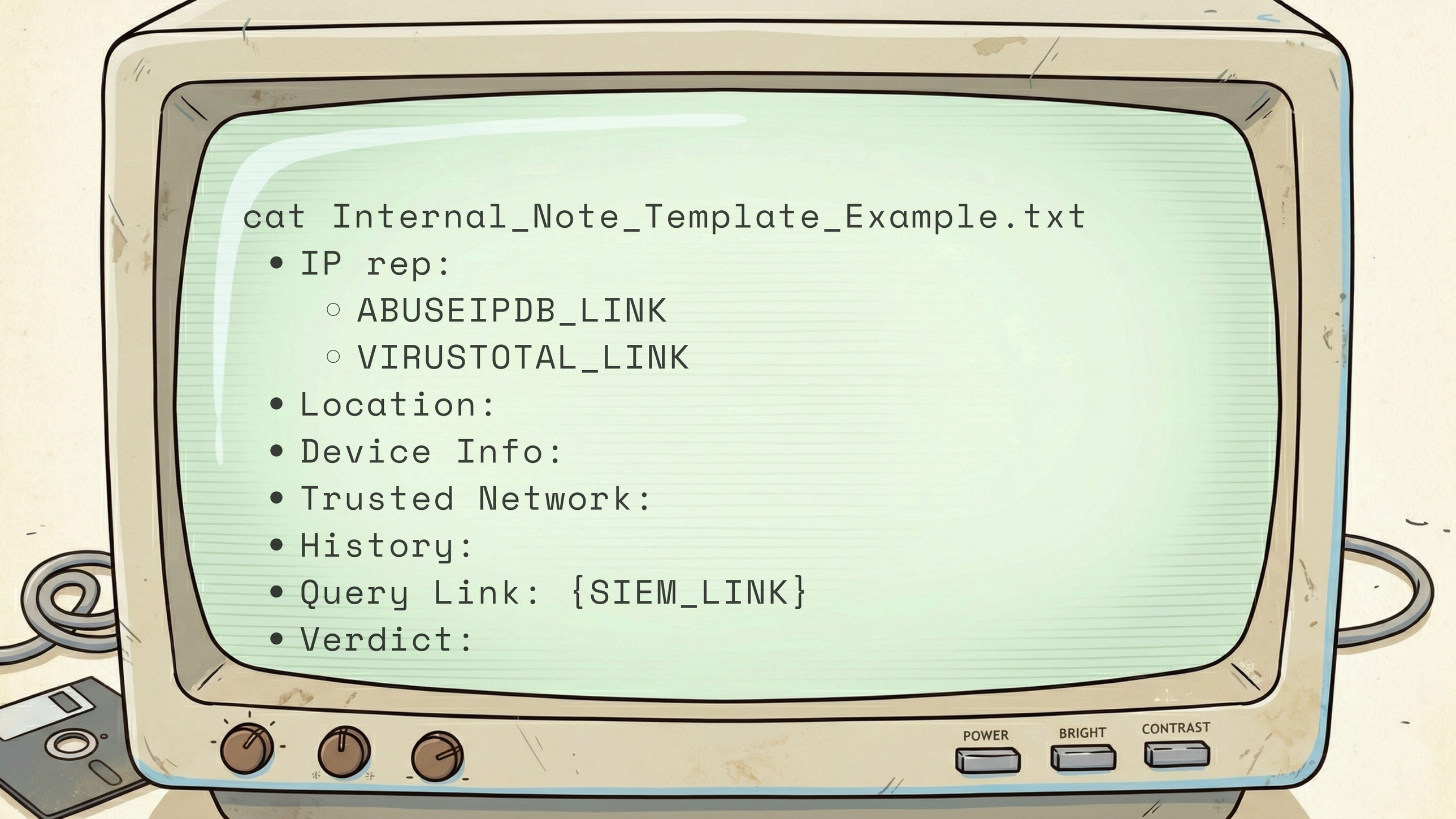
- Internal Power
- Know Your Audience
- Faucet Vs. Fire Hose


POWER
BRIGHT
CONTRAST

PLAIN TEXT PROTOCOL

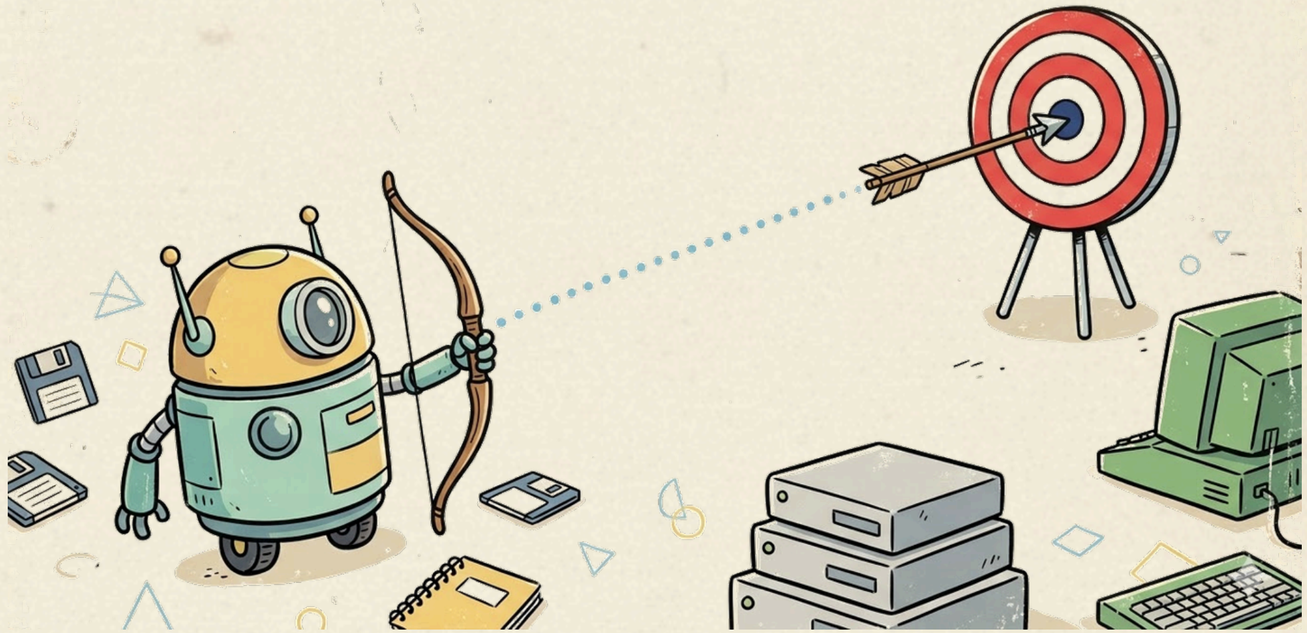
- Templates
- Structure
- Details




cat Internal_Note_Template_Example.txt
IP rep:
ABUSEIPDB_LINK
VIRUSTOTAL_LINK
Location:
Device Info:
Trusted Network:
History:
Query Link: {SIEM_LINK}
Verdict:
POWER
BRIGHT
CONTRAST

PLAIN TEXT PROTOCOL

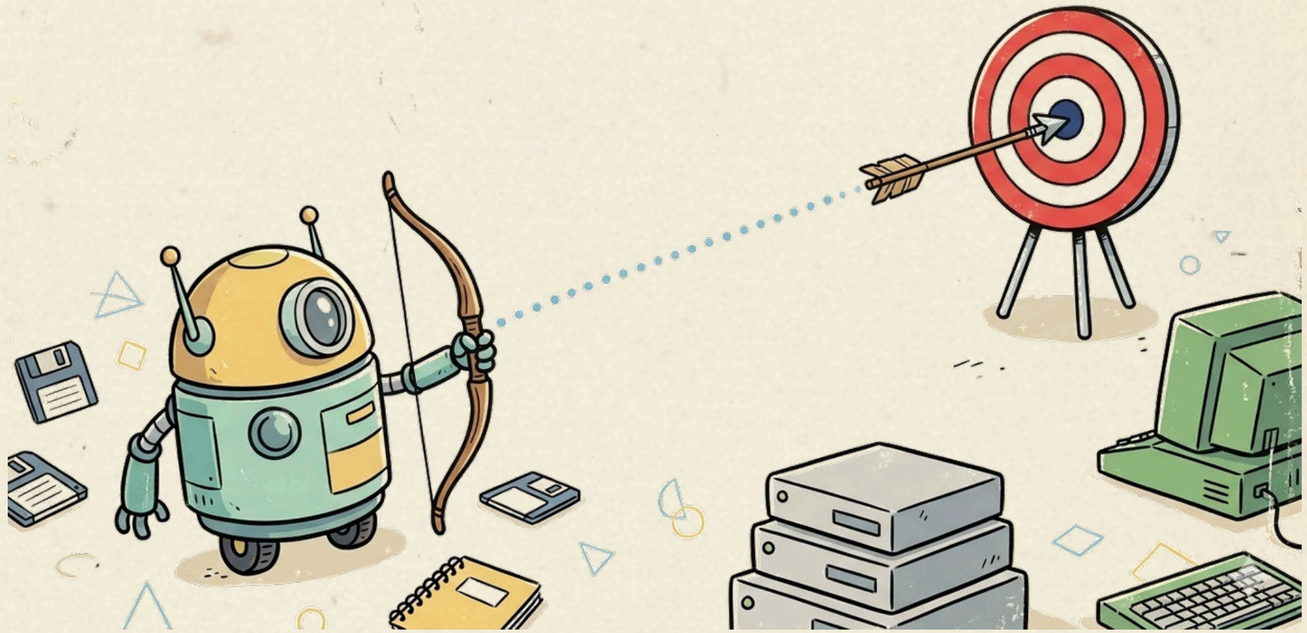
- Templates
- Structure
- Details

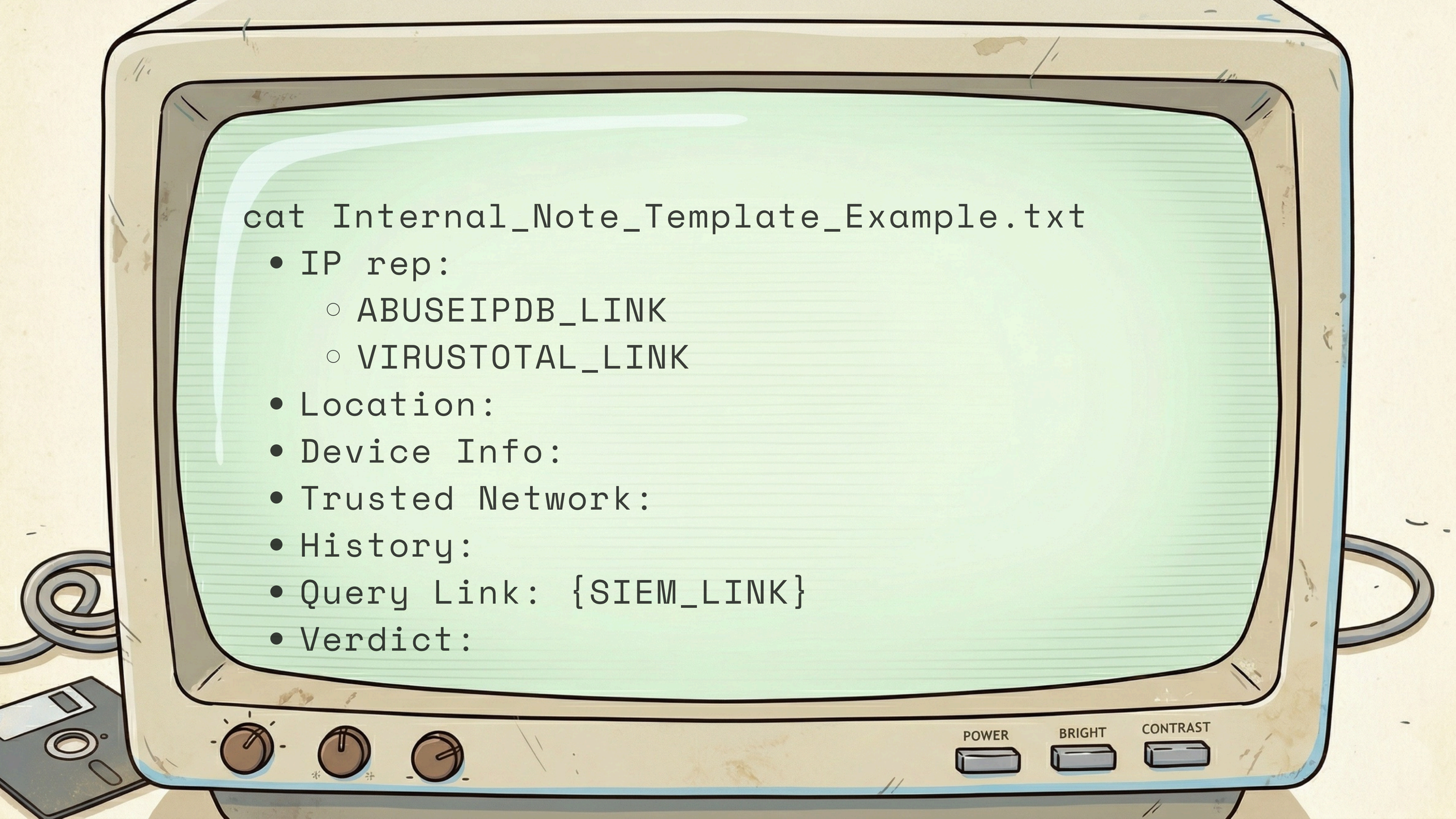



WAYNE'S WORLD
POWER
BRIGHT
CONTRAST

PLAIN TEXT PROTOCOL

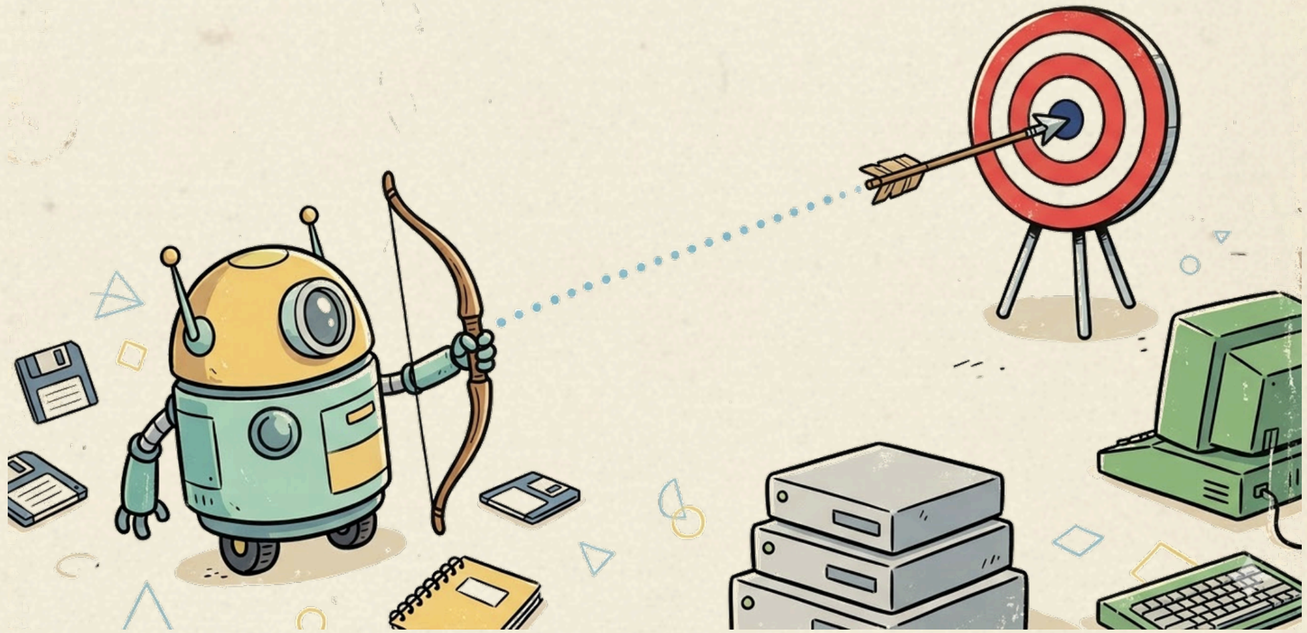
- Templates
- Structure
- Details



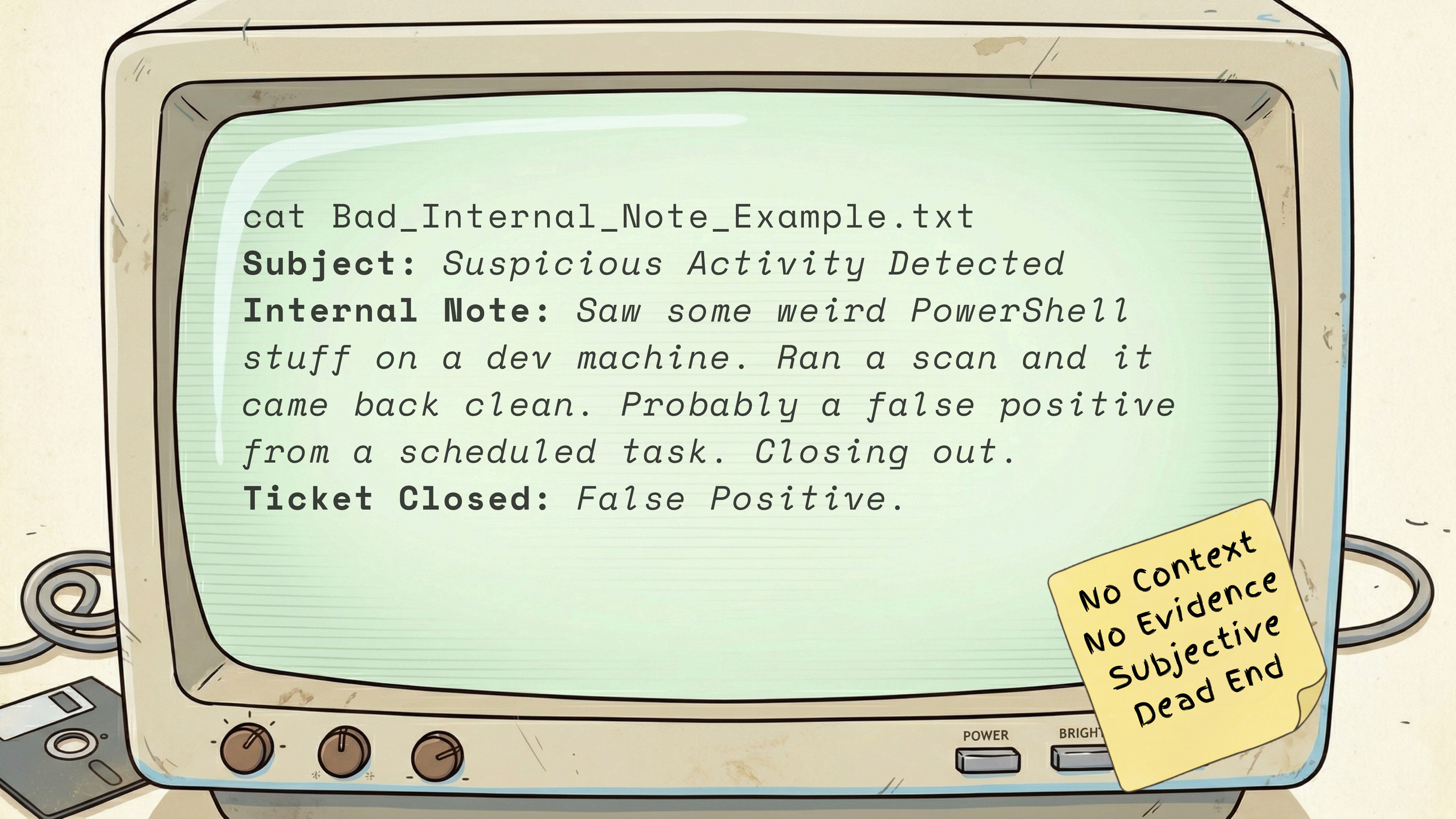

cat Internal_Note_Template_Example.txt
IP rep:
ABUSEIPDB_LINK
VIRUSTOTAL_LINK
Location:
Device Info:
Trusted Network:
History:
Query Link: {SIEM_LINK}
Verdict:
POWER
BRIGHT
CONTRAST

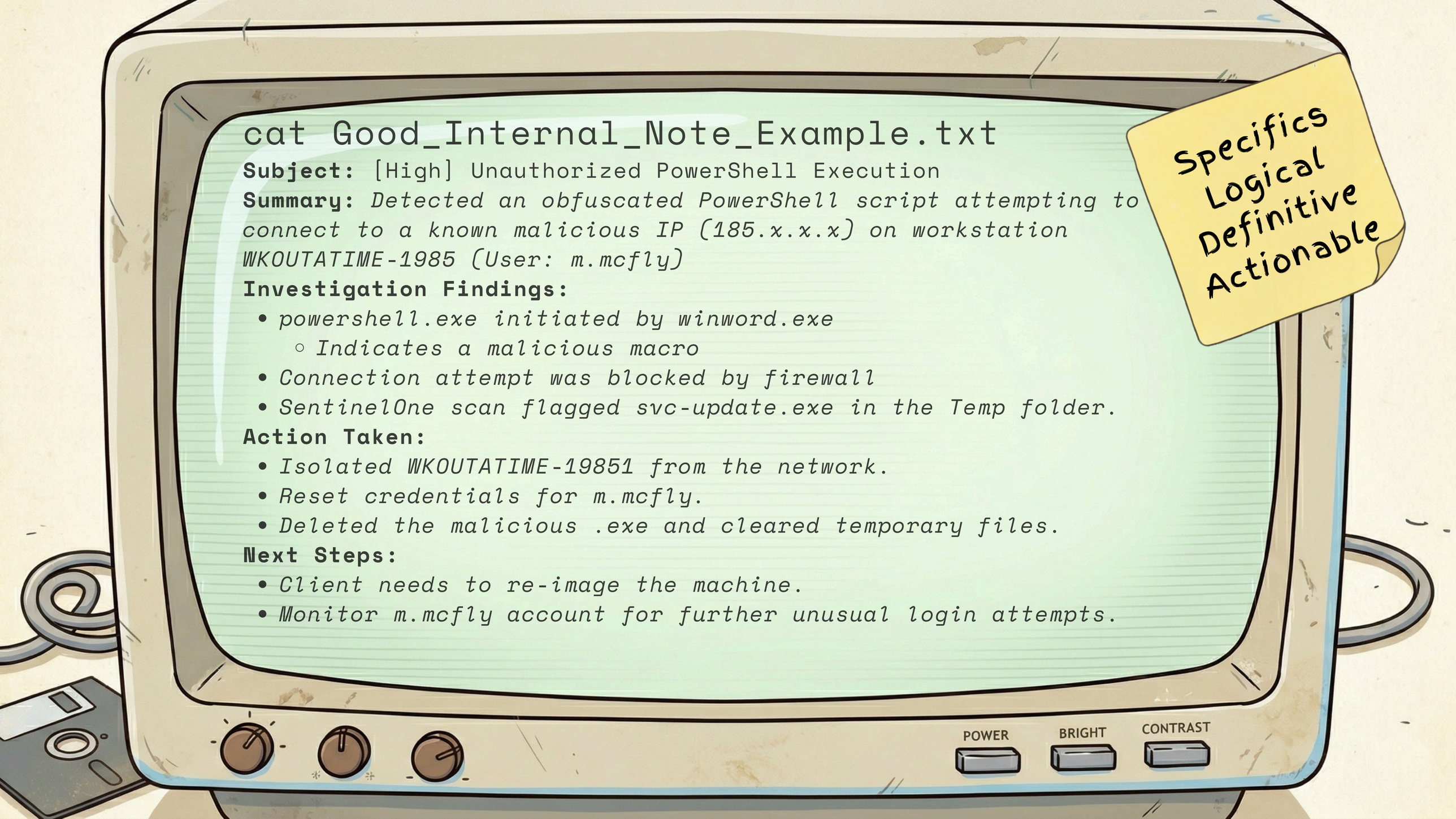
PLAIN TEXT PROTOCOL

- Templates
- Structure
- Details



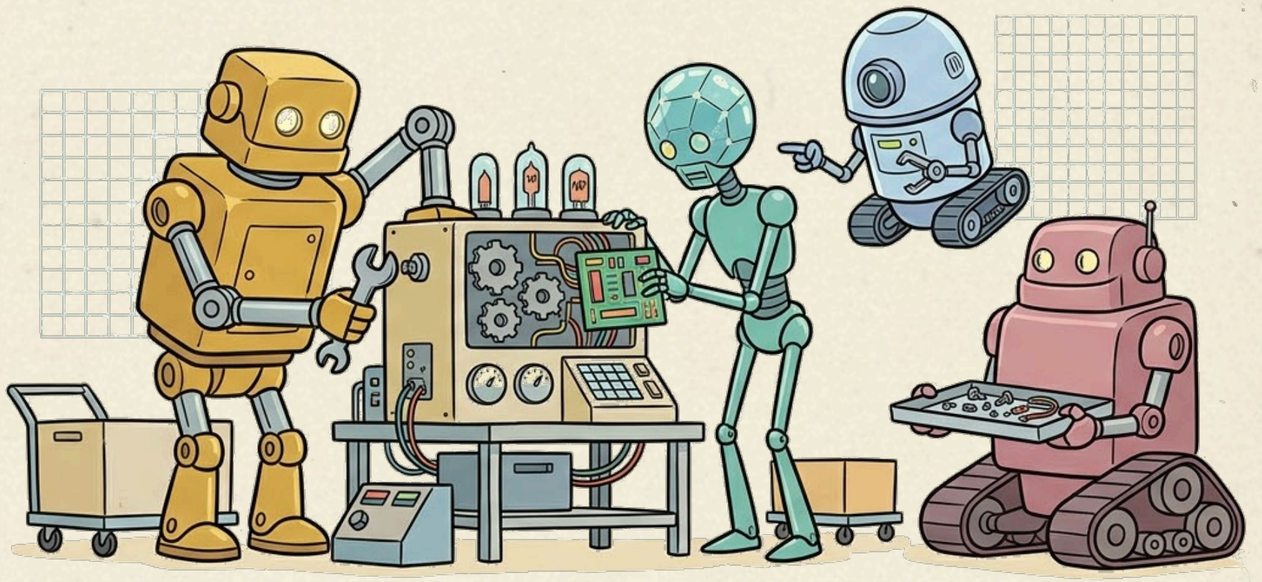

WHAT
POWER
BRIGHT
CONTRAST

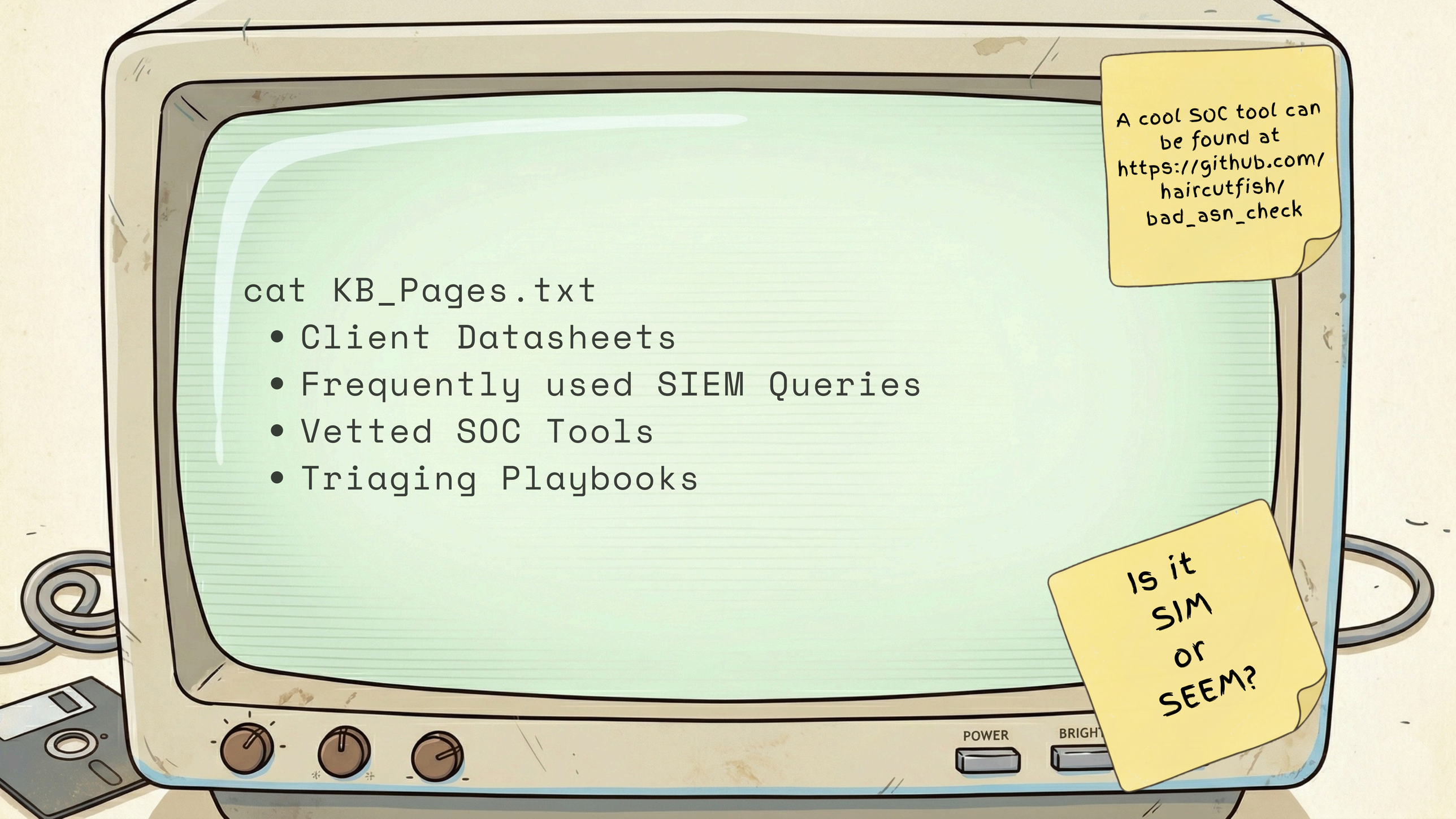

cat Bad_Internal_Note_Example.txt
Subject: *Suspicious Activity Detected*
Internal Note: *Saw some weird PowerShell stuff on a dev machine. Ran a scan and it came back clean. Probably a false positive from a scheduled task. Closing out.*
Ticket Closed: *False Positive.*
POWER
No Context
No Evidence
Subjective
Dead End


cat Good_Internal_Note_Example.txt
Subject: [High] Unauthorized PowerShell Execution
Summary: Detected an obfuscated PowerShell script attempting to connect to a known malicious IP (185.x.x.x) on workstation WKOUTATIME-1985 (User: m.mcfly)
Investigation Findings:
powershell.exe initiated by winword.exe
Indicates a malicious macro
Connection attempt was blocked by firewall
SentinelOne scan flagged svc-update.exe in the Temp folder.
Action Taken:
Isolated WKOUTATIME-19851 from the network.
Reset credentials for m.mcfly.
Deleted the malicious .exe and cleared temporary files.
Next Steps:
Client needs to re-image the machine.
Monitor m.mcfly account for further unusual login attempts.
Specifics
Logical
Definitive
Actionable
POWER
BRIGHT
CONTRAST

PEER TO PEER

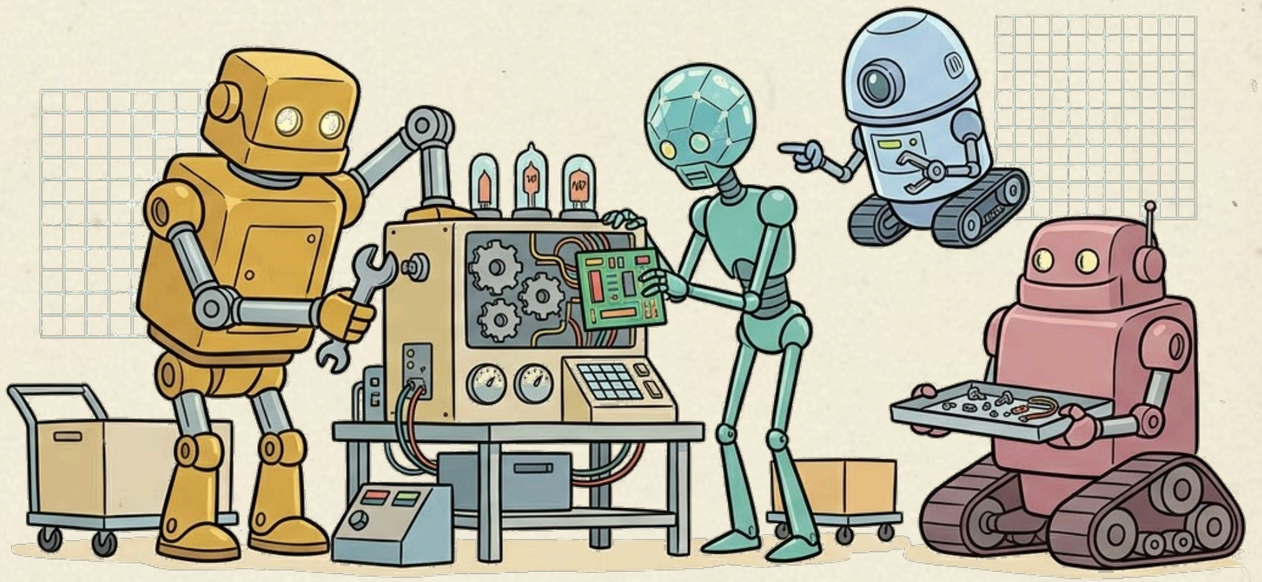
- No Silos
- Knowledge Base
- Team To Team



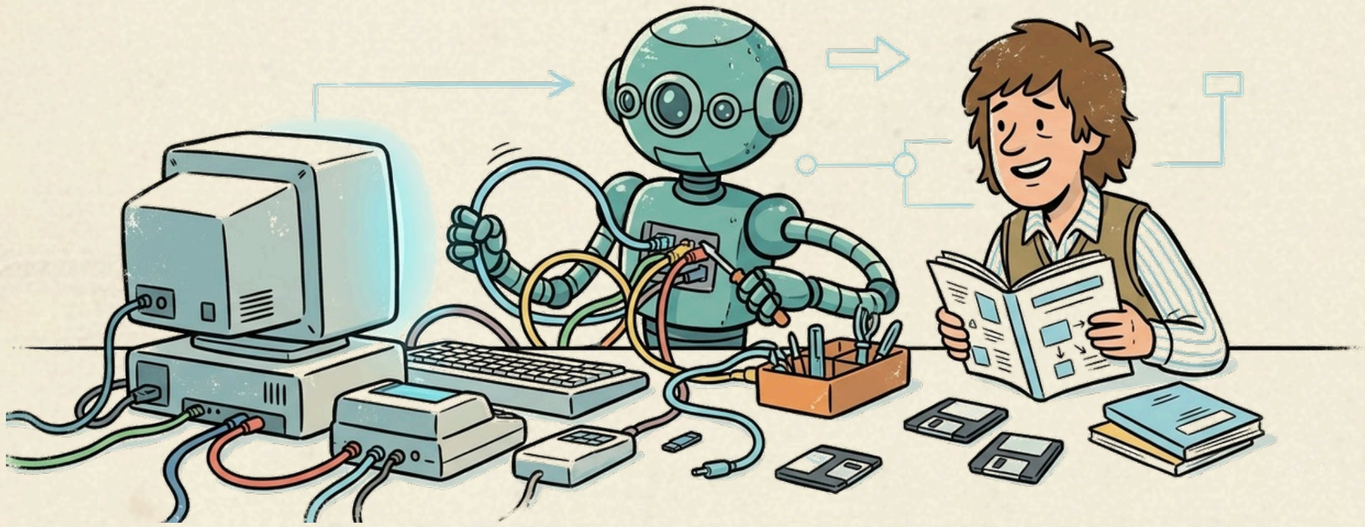

cat KB_Pages.txt
• Client Datasheets
• Frequently used SIEM Queries
• Vetted SOC Tools
• Triaging Playbooks
A cool SOC tool can be found at https://github.com/haircutfish/bad_asn_check
Is it SIM or SEEM?
POWER

PEER TO PEER

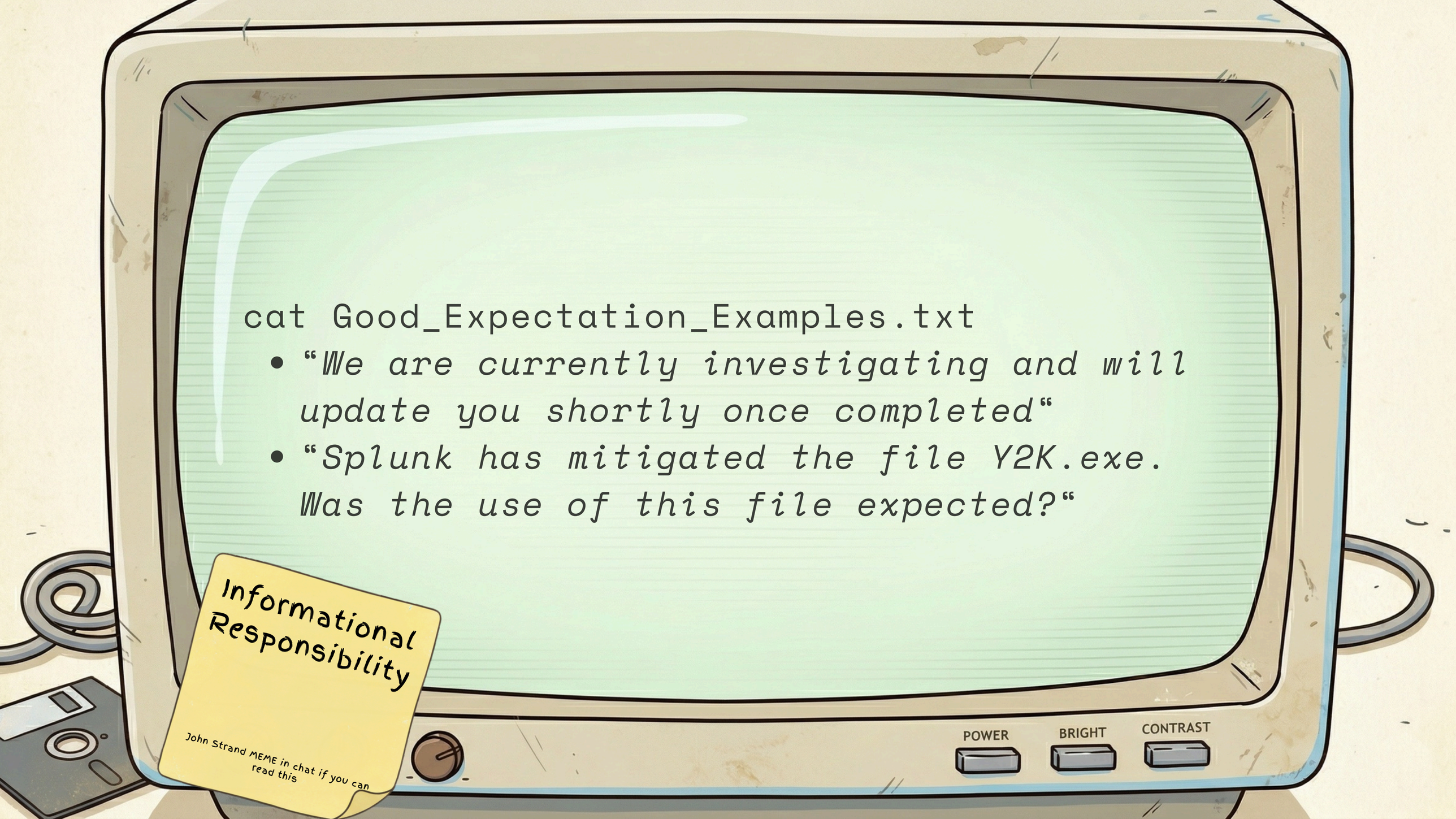
- No Silos
- Knowledge Base
- Team To Team



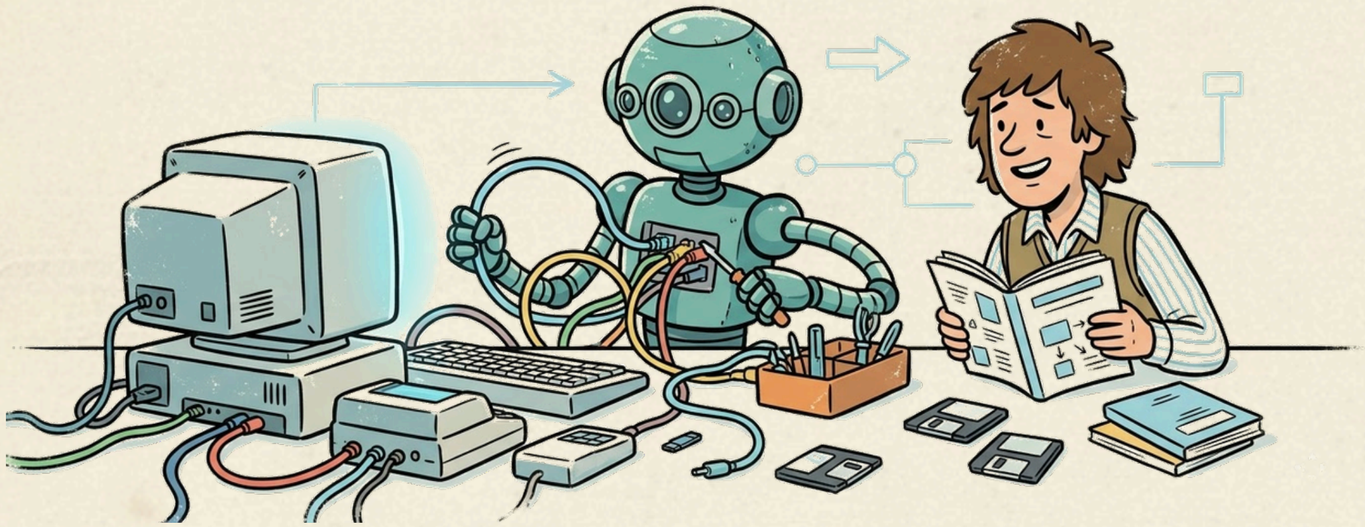
THE CLIENT SESSION



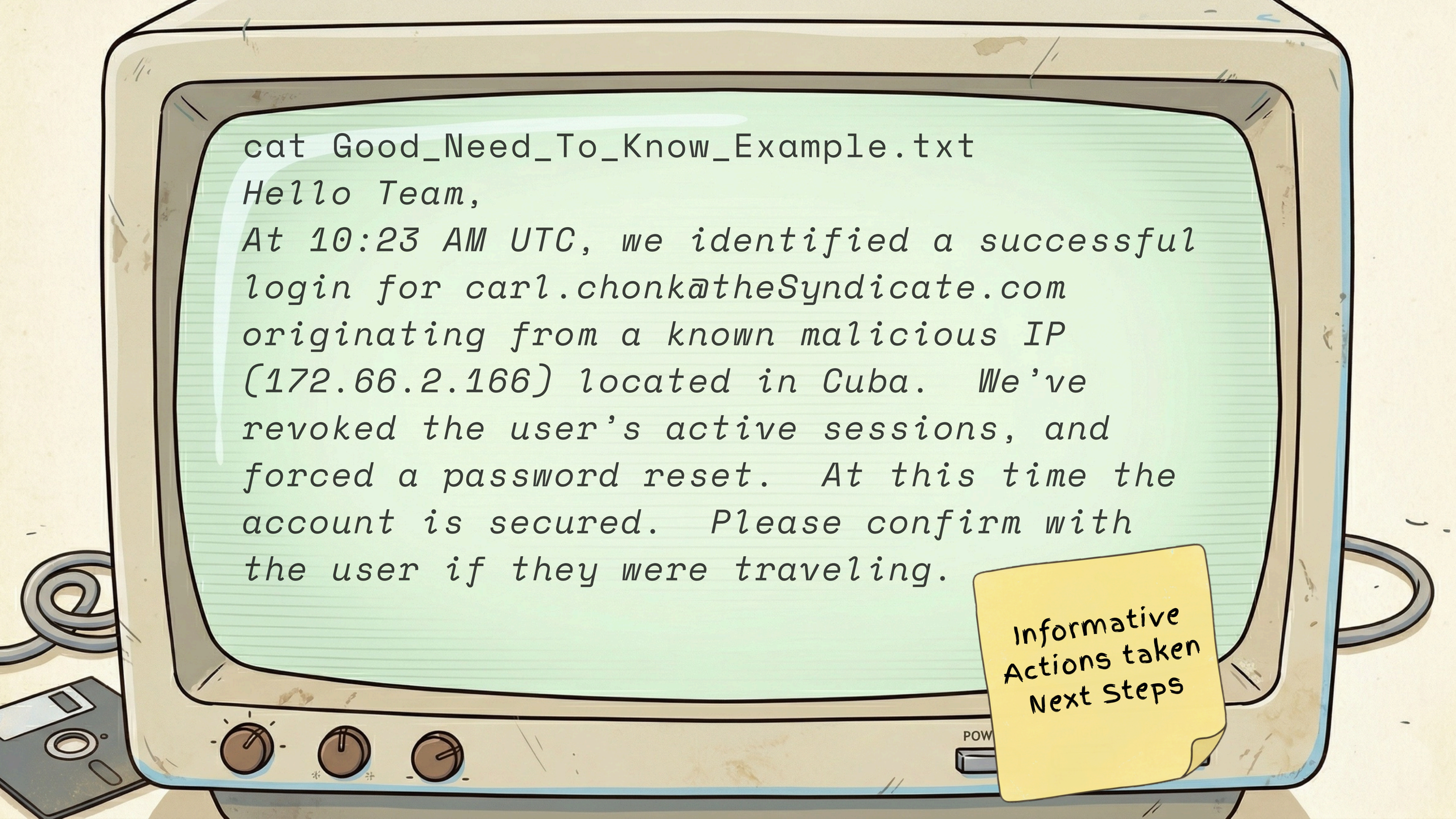
- Expectations
- Need To Know
- Built-in Trust


cat Good_Expectation_Examples.txt
• “We are currently investigating and will update you shortly once completed“
• “Splunk has mitigated the file Y2K.exe. Was the use of this file expected?“
Informational Responsibility
John Strand MEME in chat if you can read this
POWER
BRIGHT
CONTRAST

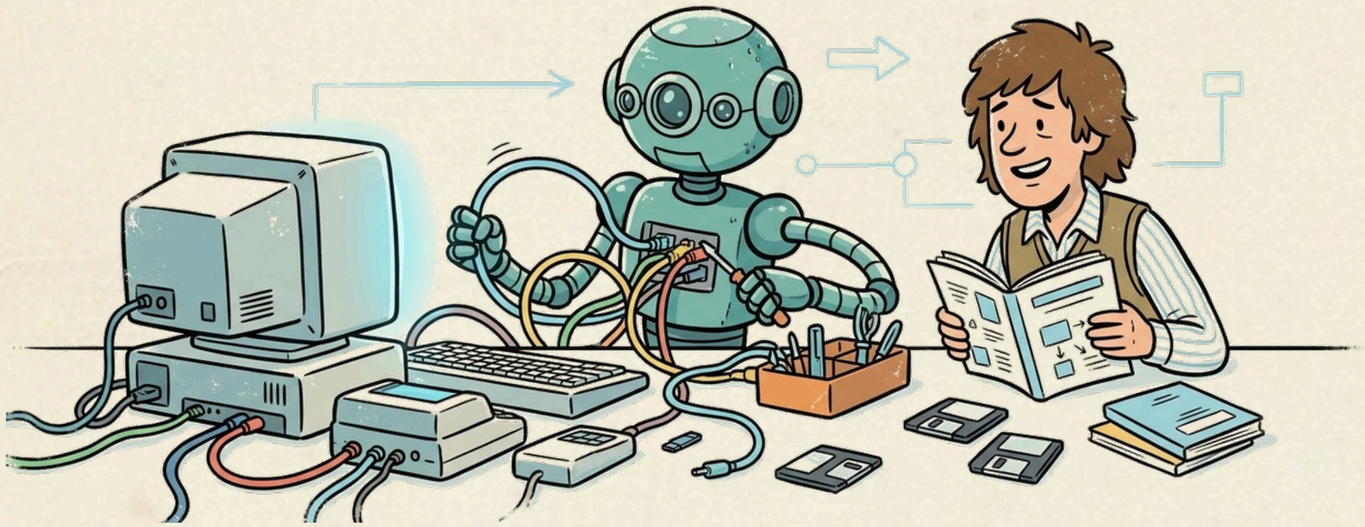
THE CLIENT SESSION



- Expectations
- Need To Know
- Built-in Trust

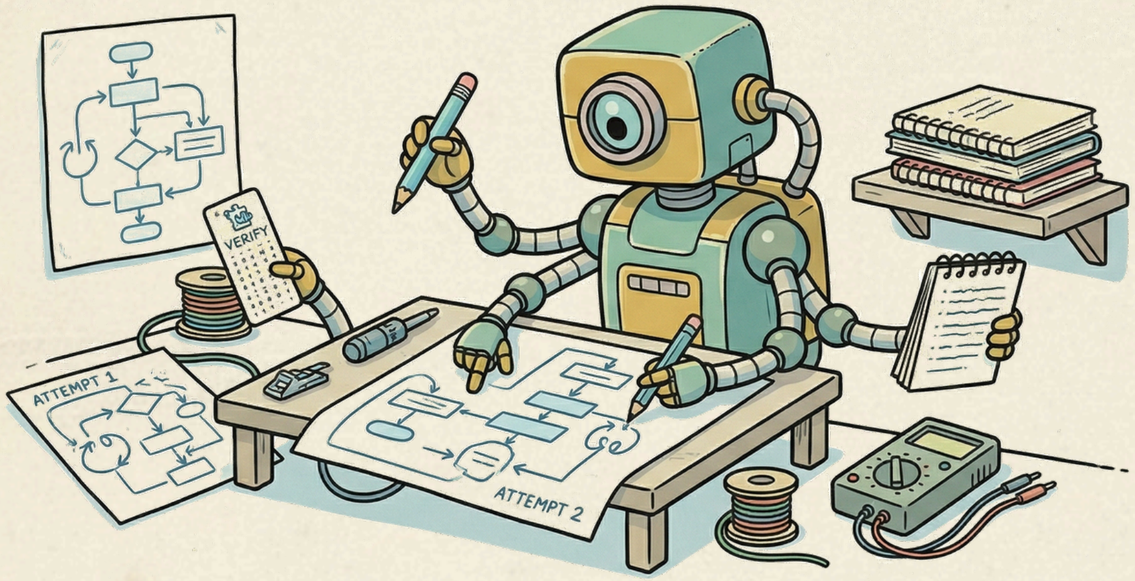

cat Good_Need_To_Know_Example.txt
Hello Team,
At 10:23 AM UTC, we identified a successful login for carl.chonk@theSyndicate.com originating from a known malicious IP (172.66.2.166) located in Cuba. We've revoked the user's active sessions, and forced a password reset. At this time the account is secured. Please confirm with the user if they were traveling.
Informative
Actions taken
Next Steps

THE CLIENT SESSION

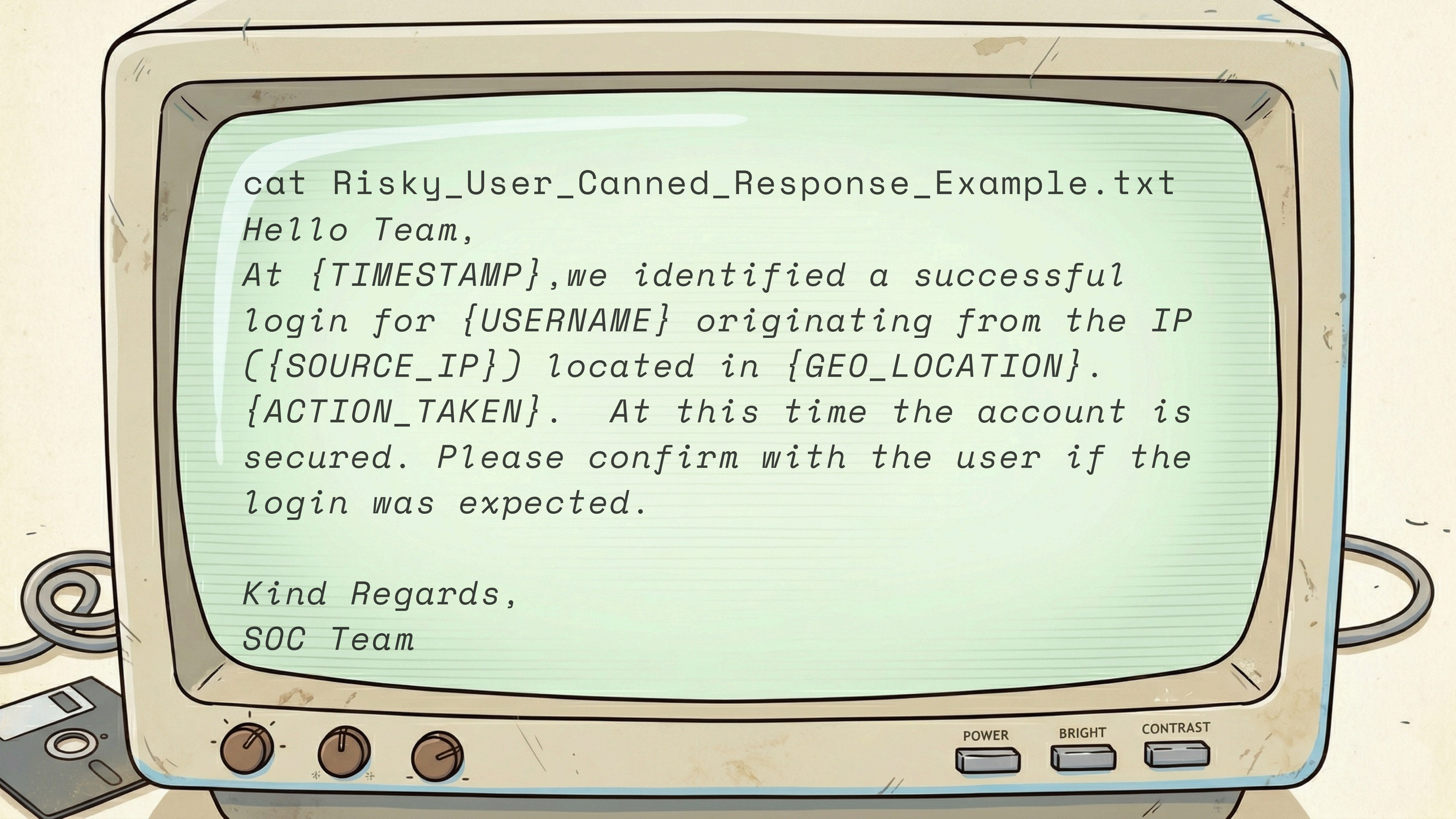


- Expectations
- Need To Know
- Built-in Trust

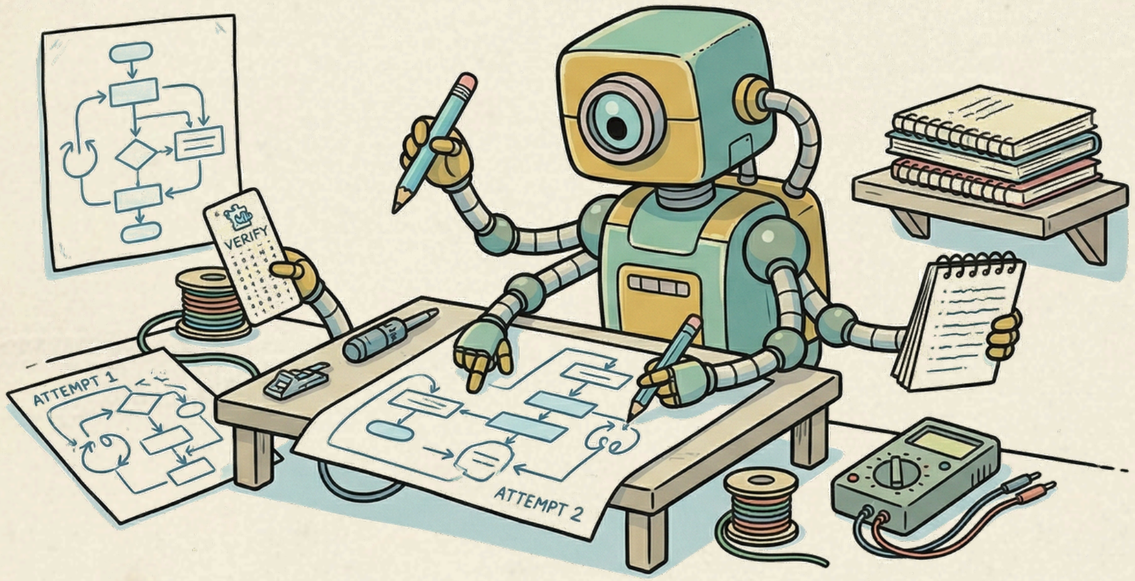
HOTFIX TODAY



- Self Audit
- Canned Responses
- Seek Feedback


cat Risky_User_Canned_Response_Example.txt
Hello Team,
At {TIMESTAMP},we identified a successful login for {USERNAME} originating from the IP ({SOURCE_IP}) located in {GEO_LOCATION}. {ACTION_TAKEN}. At this time the account is secured. Please confirm with the user if the login was expected.
Kind Regards,
SOC Team
POWER
BRIGHT
CONTRAST

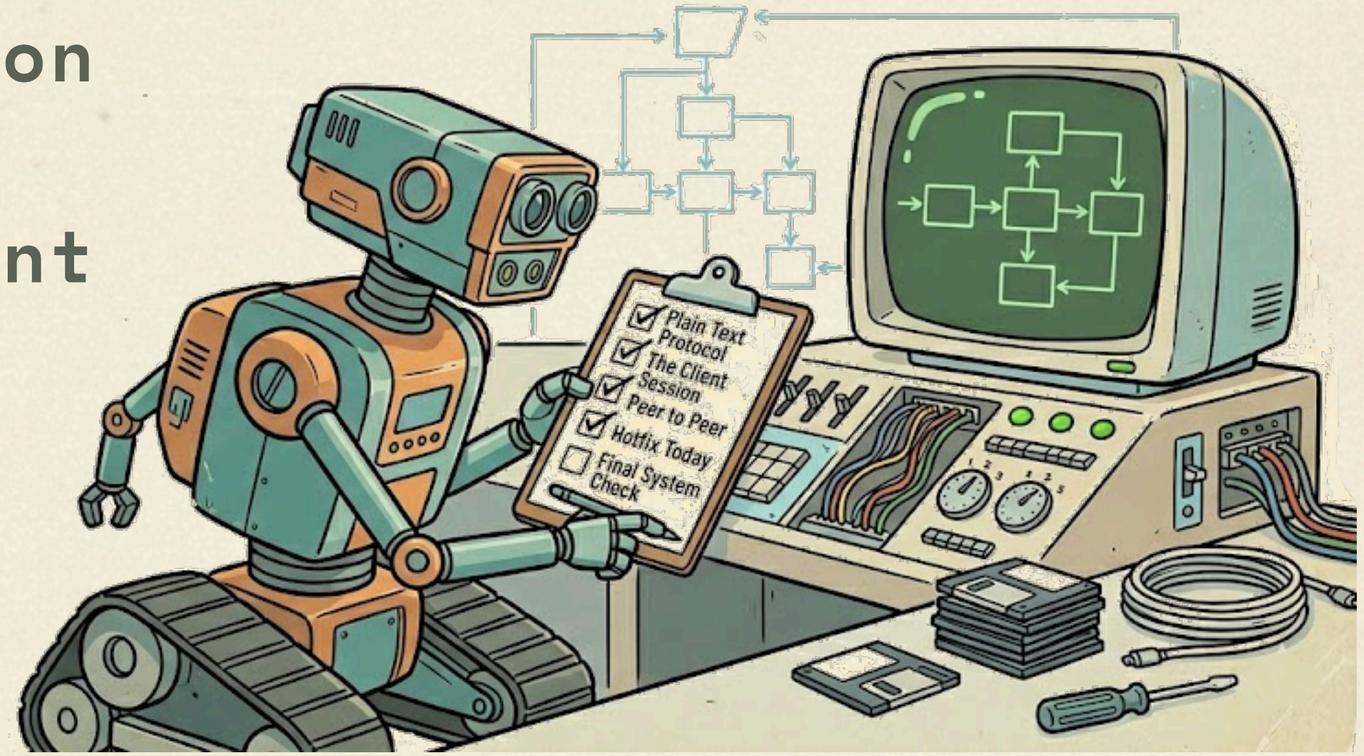
HOTFIX TODAY



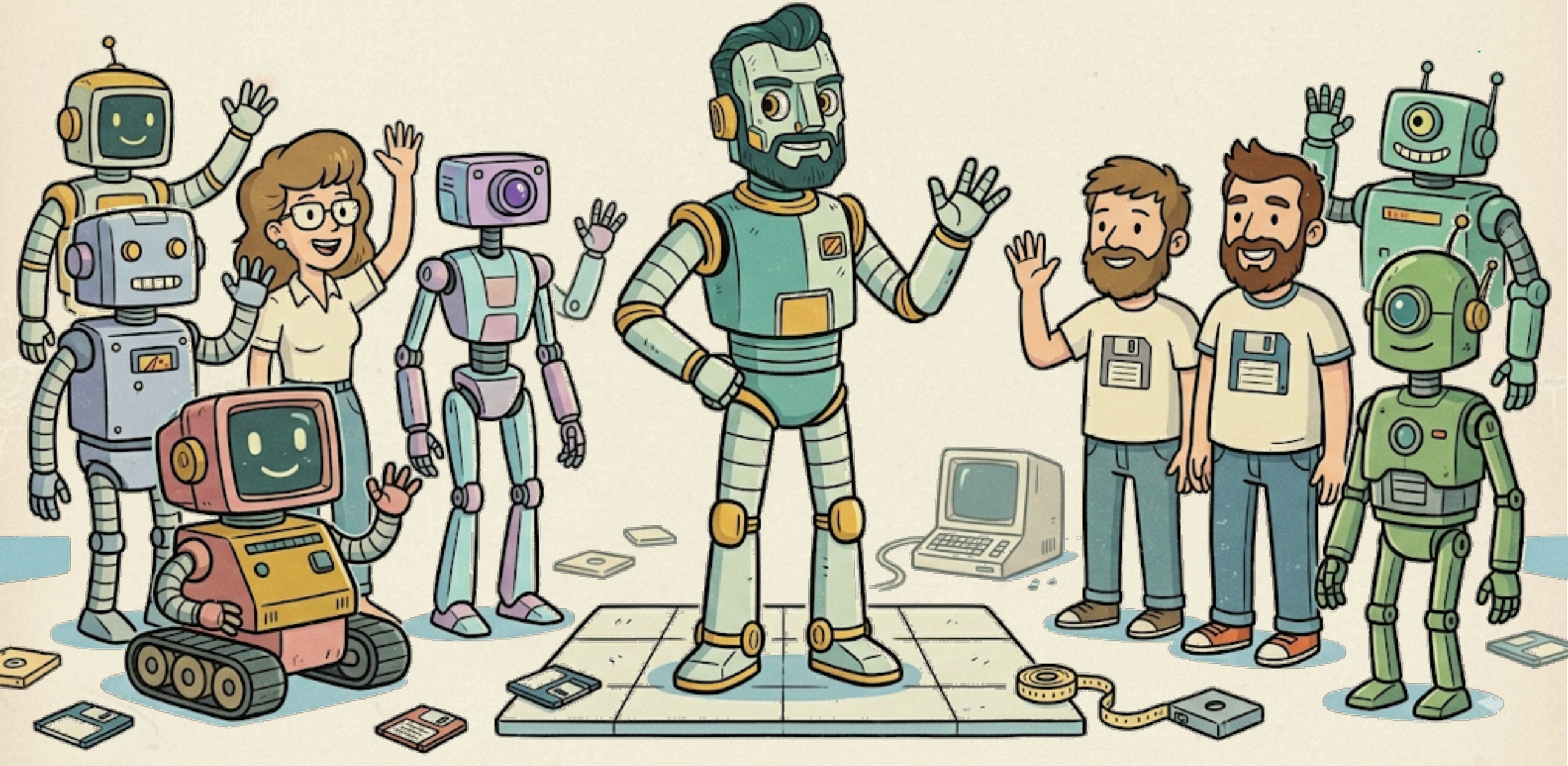
- Self Audit
- Canned Responses
- Seek Feedback

FINAL SYSTEM CHECK

- Clear Communication
- In SOC we Trust
- Ongoing Improvement



THANK YOU FOR ATTENDING



cat Social.txt


LinkedIn: https://www.linkedin.com/in/danrearden/


Discord:Haircutfish


Medium:https://medium.com/@haircutfish


Website: haircutfish.com

BHIS Survival Guide SOC Edition

https://www.blackhillsinfosec.com/prompt-zine/prompt-issue-infosec-survival-guide-blue-book/