Saving Time, Saving Money

The Business Case for Tuning Your SOCs detections and saving your analyst's time.

BLUF: Add in Case metrics and Log costs to your scheduled detection review

Agenda

- Speaker Introduction
- Our Mission today
- What is a SOC
- What is Wasted Time
    - SOC Stats
- Total Cost of Ownership for detections
    - Logging, Analyst Time, Frequency of Events, Compliance. Misc
- Record how we perform
    - Alert Classification
    - Median Time to Remediate
- Chesterton's fence
- Demo
- Take Aways
- Q&A
- Check out the Annex

Introduction – Chris Hamilton

- From Cincinnati Ohio, Living in the Northern Virginia Area.
- Currently at Oracle working in Cloud Security Operations
- Previous Security Operations & SOC work:
  - Microsoft – **Where we went from an outsourced T1, Small T2 model to a robust multi-team/multi-country SOC with ancillary supporting teams.**
  - KeyBank **– Where we built a Security Operations Center using MSSP and Internal Staffing from the ground up.**
  - US Army – **Where we built out Security Operations Planning and Staffing to support Incident Response, and Ancillary teams.**

* Fun Fact - Ohio is the greatest state in the United States

Our Mission Today (for the next 20 minutes)

Catch Bad People, doing bad things, as efficiently as possible, and were going to judge efficiency against ‘wasted’ time & money.

We are going to put ourselves into the mindset of a SOC analyst.

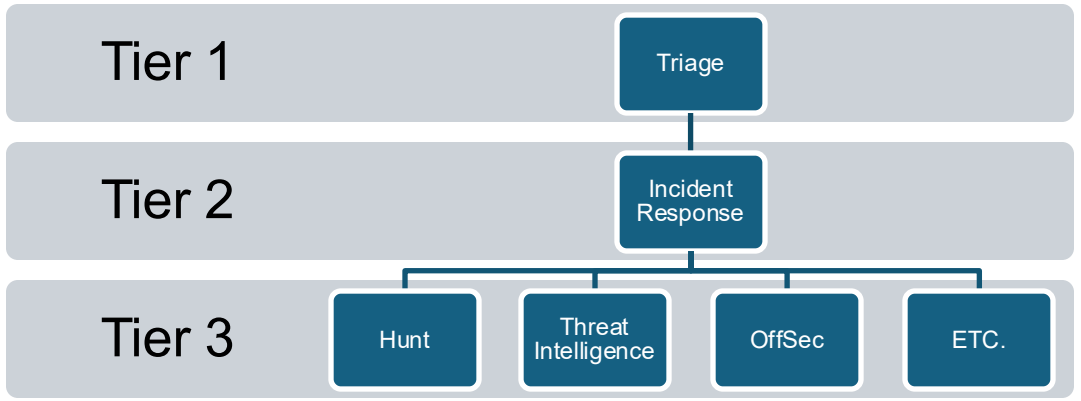
What is a SOC

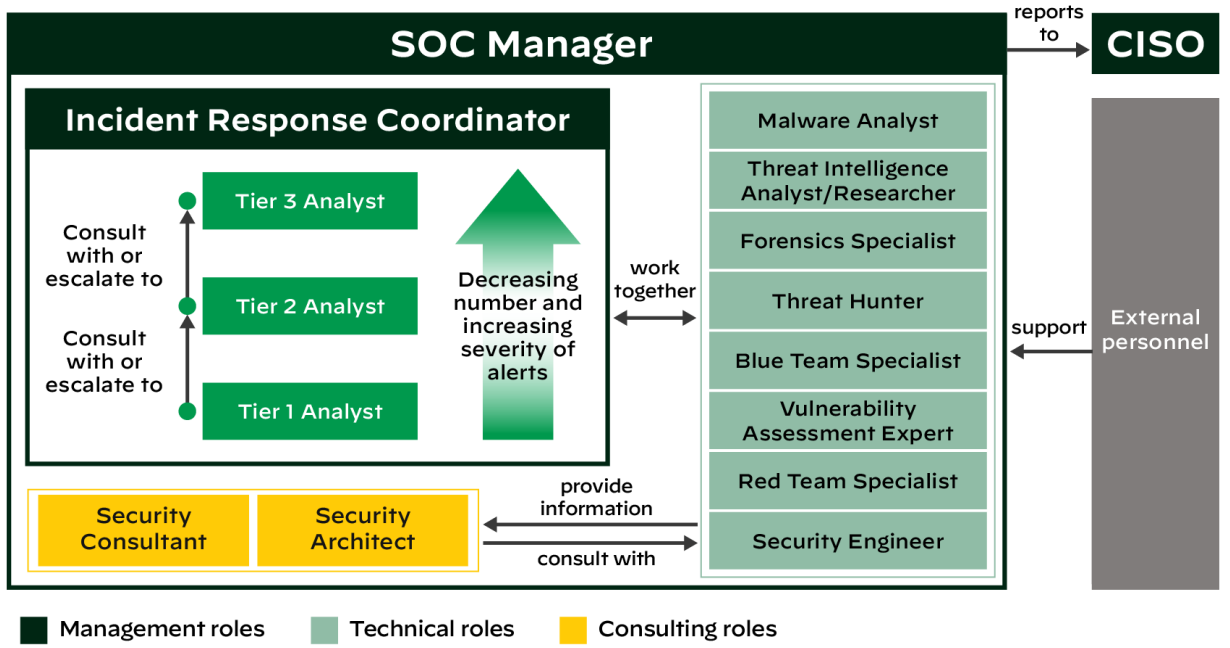
(It isn’t just incident handling, but we’re focusing on that today)

- A SOC deals with physical | cyber security issues, by monitoring and improving an organization's security posture; preventing, **detecting, analyzing,** and responding to incidents through a combination of technological solutions and processes.

What Does Your SOC look like today?

- Traditional Multi-Tier
  - Tier-1 Triage / Intrusion Detection
  - Tier-2 Escalation / Incident Response
  - Tier-3 Hunt / Problem Solving / Experts
- Subspeciality / Part Time Members
  - Digital Forensics
  - Reverse Engineering
  - Threat Intelligence
  - SDLC/Secure Code Review
  - OffSec / Cyber Threat Emulation





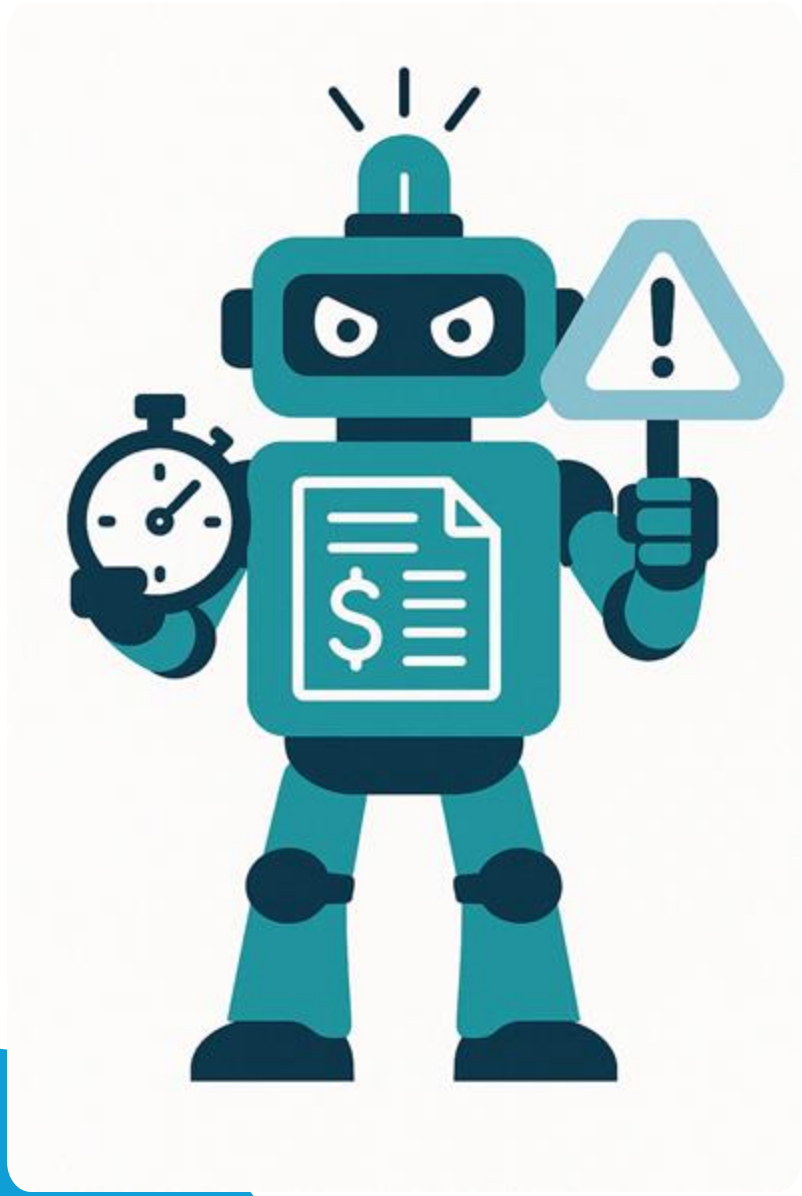
Source: Security Operations Center: A Systematic Study and Open Challenges

What is wasted time?

When it comes to ‘wasted’ time in the SOC it can mean a lot of things but for most it means false or benign positives.

SOC Stats

- On average SOC analysts work an extra **day every week -** *(Devo & Ponemon Institute)*
- In many SOCs, over **half the alerts** analysts chase turn out to be false alarms - *(Critical Start)*
- **Half of SOC teams** lose **1 out of every 4 analysts** each year. - *(Help Net Security)*
  - the average tenure in a high-noise SOC is often only 1–3 years – *(intrusion)*



What do we need to determine
The cost of a detection?

The cost of the log

Investigation time

Alert Classification

The cost of a log

Most products/services measure log cost in GB/$

Logs have a cost/value proposition

Value:

- Compliance
- Remediating Past Incidents
- Threat Hunting / Incident Response
- Following or setting Industry Trends

Cost:

- $$$
- Trade off - Not being able to ingest other logs due to Hardware or budget

We get more value out of a log by ingesting it fewer times.

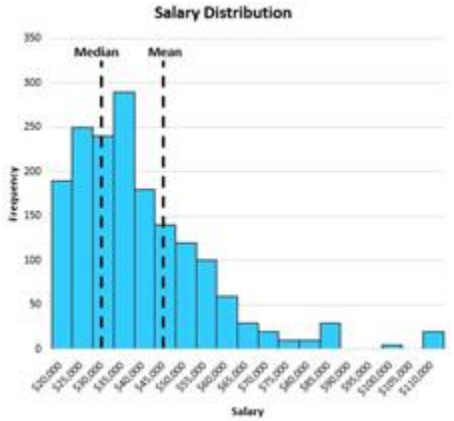
Record how we perform

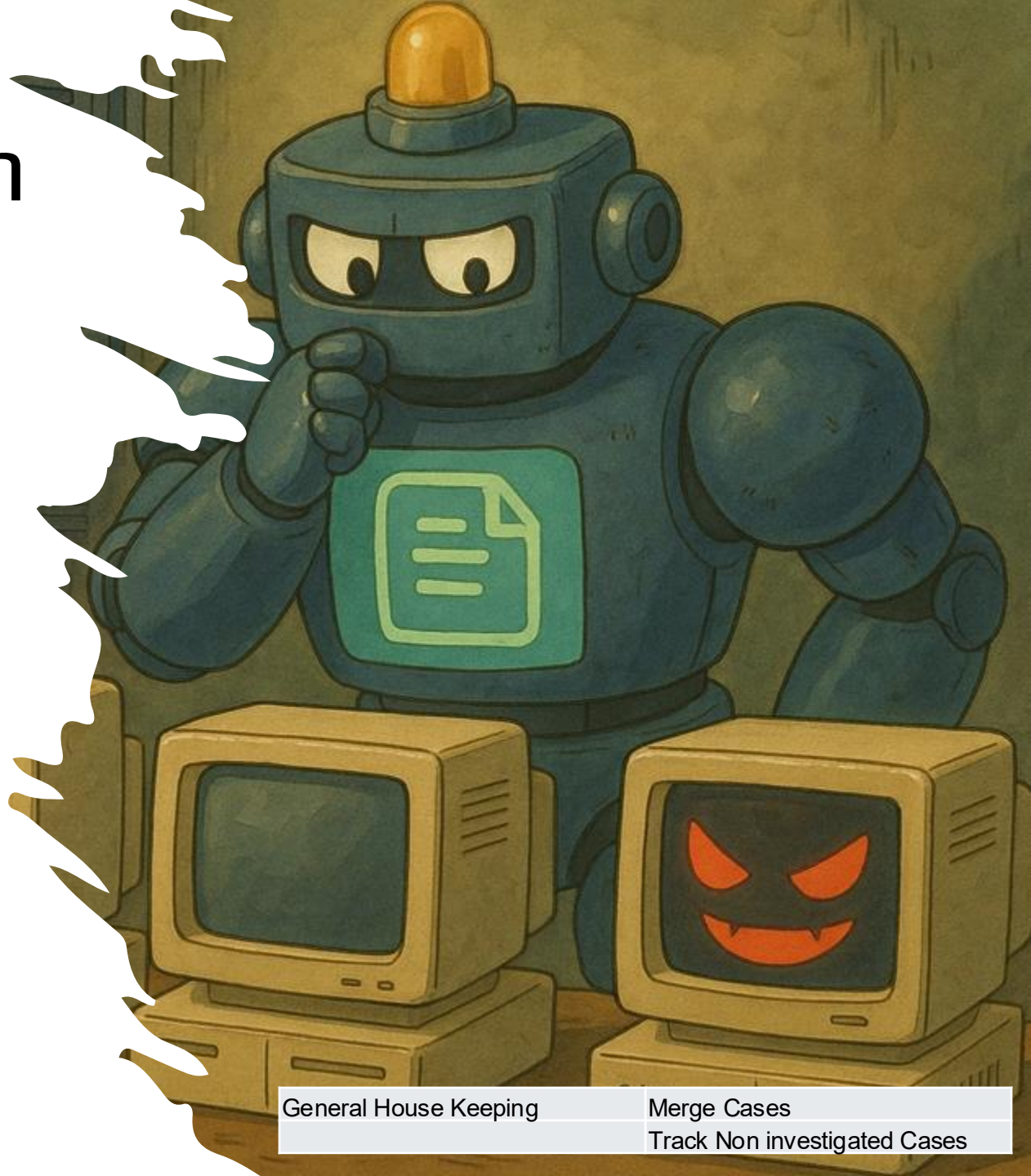
A key part of measuring detection efficiency is gathering investigation metrics.

At a minimum we'll need:

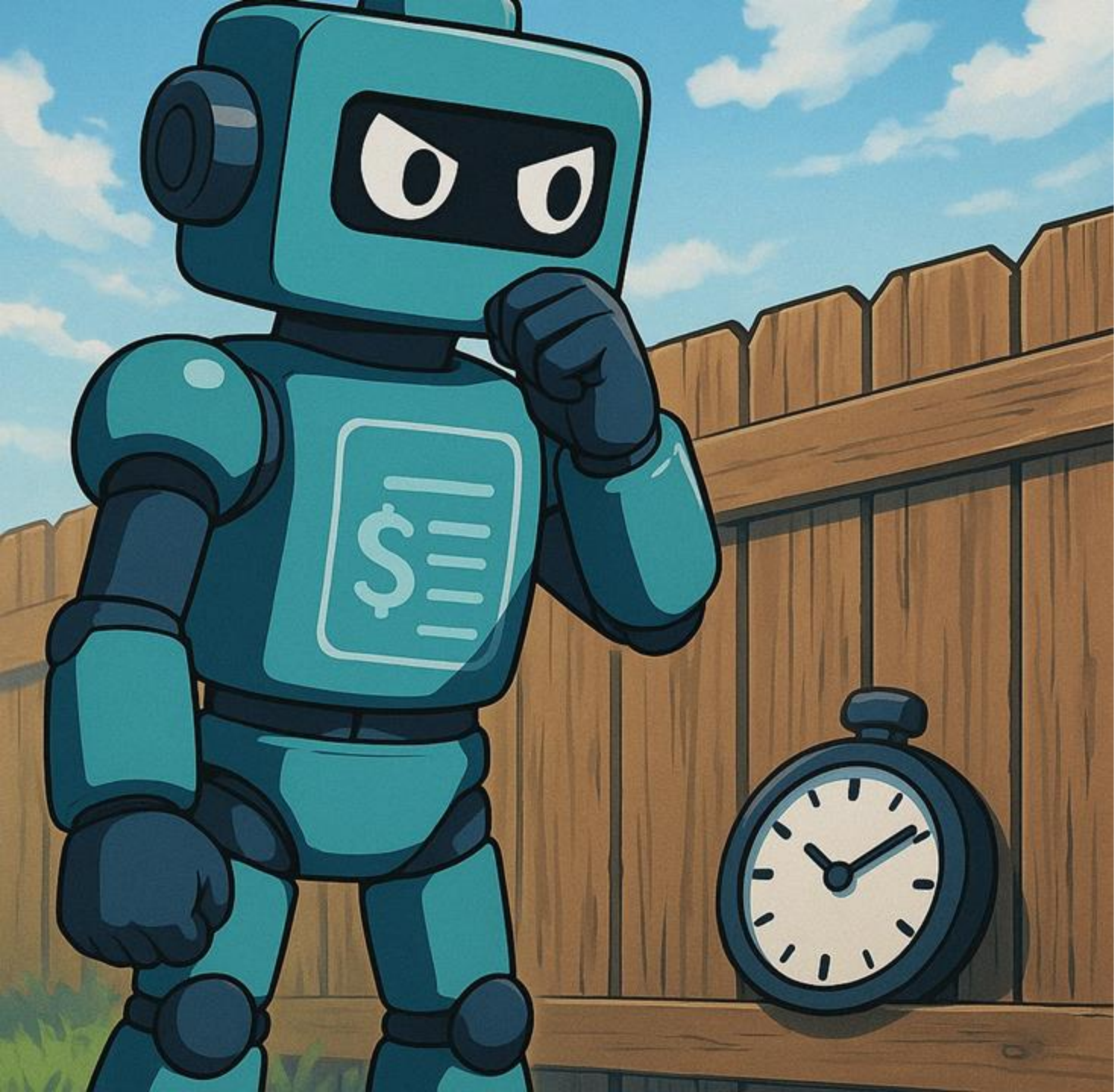
- The Alert Classification
  - True Positive – A detected malicious action
  - Benign Positive - An action detected that is real, but not malicious, such as a penetration test.
  - False Positive - A false alarm, meaning the activity didn't happen.
- Median Time to Remediate/Closure
  - Analyst Assignment time – Closure/Remediation time

Median! Not Mean!





General House Keeping	Merge Cases
	Track Non investigated Cases



Before we dig in let’s look at the fence

Every alert rule, no matter how noisy, was created for a reason.

Before disabling or tuning a detection, ask:

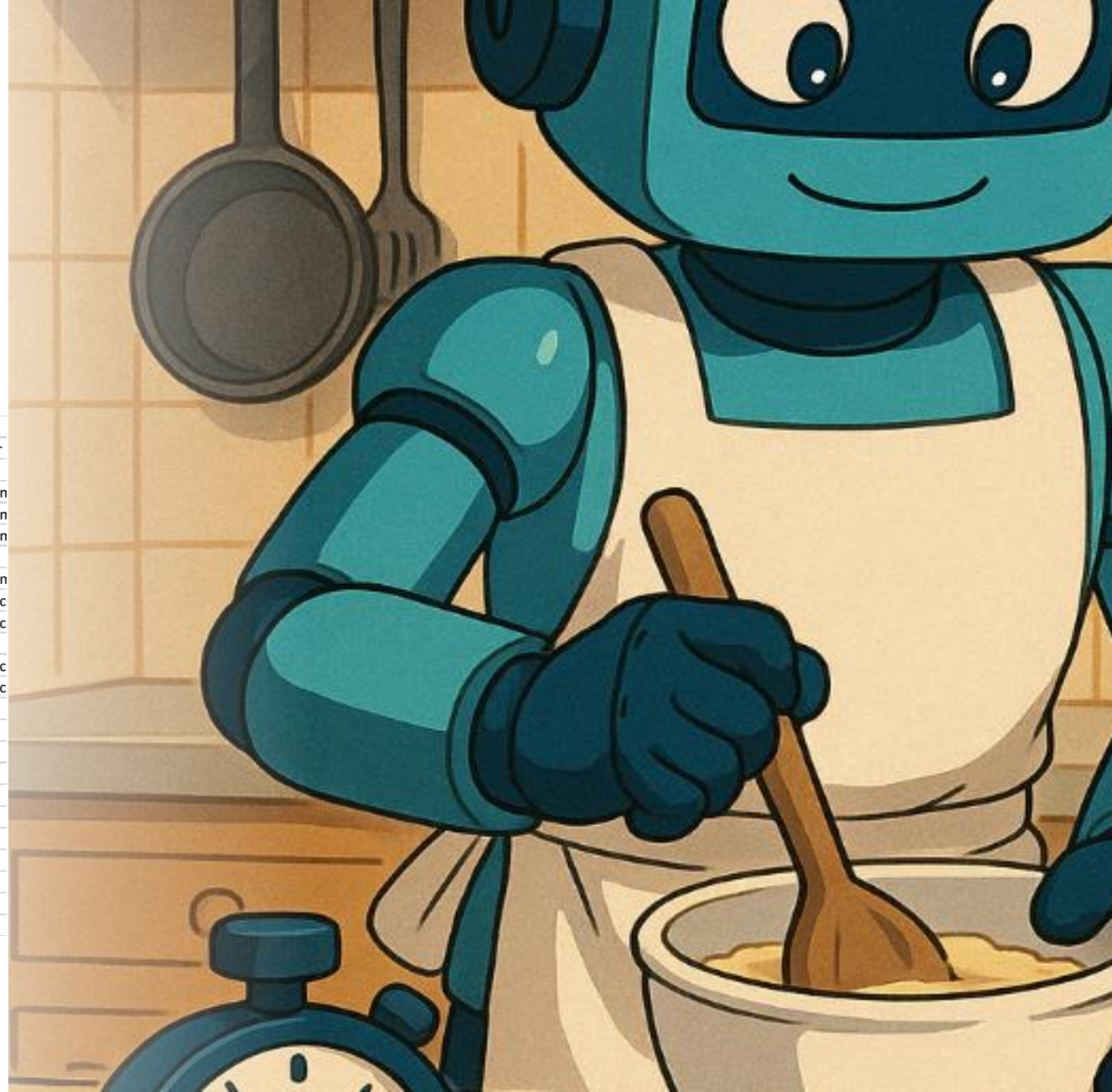
What threat was this meant to catch?

- Has the risk gone away, or is it just poorly implemented?

Let’s look at some some Data

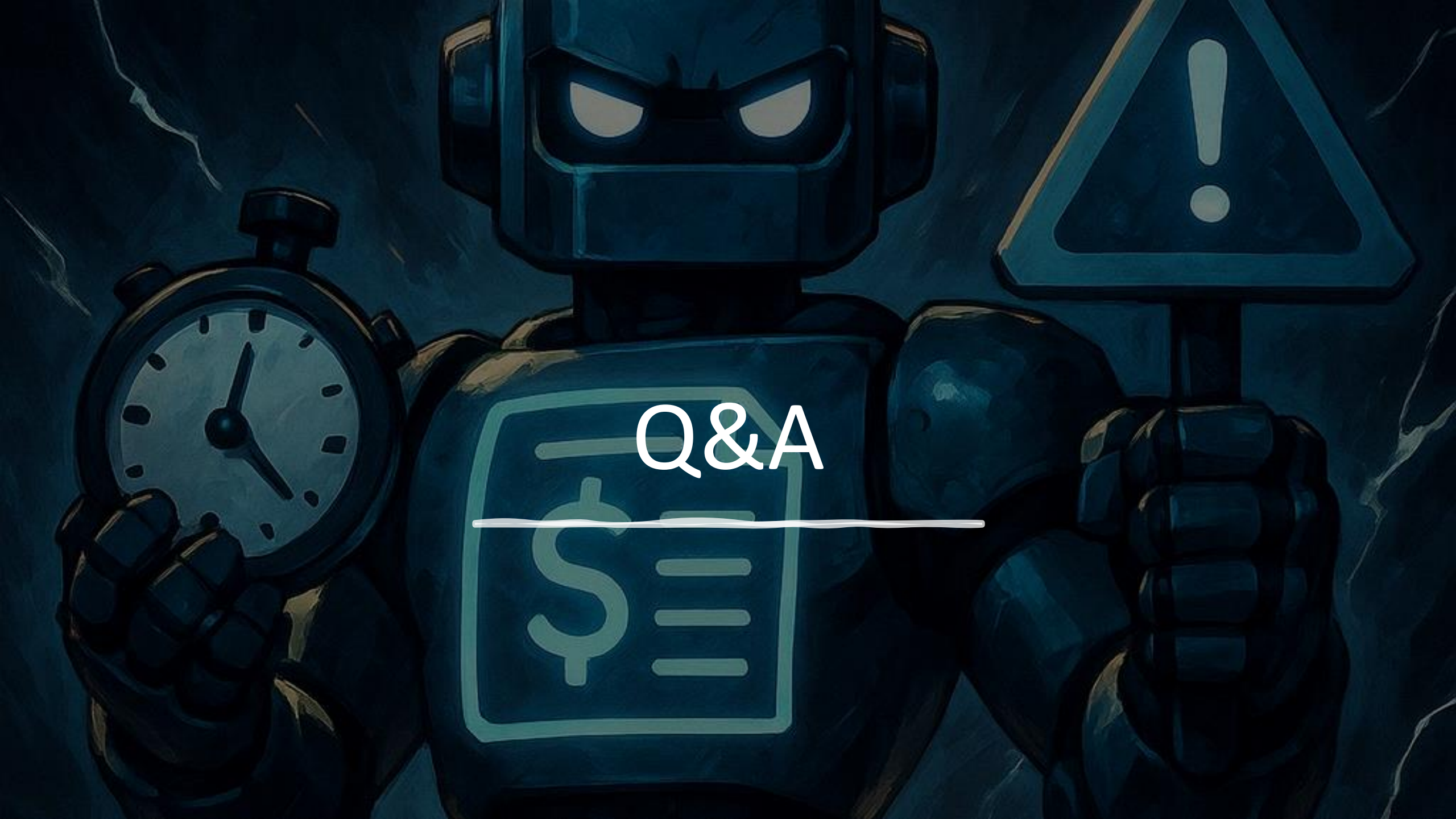
- We have Our Log Cost, Our Alert Classification, our Median time to Remediate, lets crunch some numbers.

	Derived Field	Description	Source
Detection	N	Detection Identifier	SIEM/Vendor
Total Fires	Y	Total Number of detetion triggers	
TP	N	True Positive Alarms	Case Managen
BP	N	Benign Positive Alarms	Case Managen
FP	N	False Positive Alarms	Case Managen
TP Rate	Y	TP rate vs total number of fires	
MTTR Minutes	N	Median Time to Remediate	Case Managen
Detection Description	N	Detection Description	Detection Dic
Log Source	N	Log Source	Detection Dic
Log Cost per Day	Y	Costs per day	Log Source
Detection Genesis	N	What caused the detection to be generated	Detection Dic
True Negative Cost	N	Assumed cost of True Negative	Detection Dic
Potential Negative cost	Y	TP * True Negative Cost	
Log Source Ingestion Start Date	N	Log Source Ingestion Start Date	Log Source
Days Since Ingestion Start	Y	Days since Log Investion date	
Total Log Cost	N	Total Log cost to date	Log Source
Total Log Cost (Last 365)	N	Total Log cost last 365	Log Source
True Positive HR (Last365)	Y	True Postives in Hours worked	
False Positive Hr (Last365)	Y	False Postives in Hours worked	
alse Positive Analyst Cost(Last 365)	Y	False Positive Analyst Cost Last 365	
False Positive Log Cost(Last 365)	Y	False Positive Log Costs Last 365	
False Positive Cost(Last 365)	Y	Total False Positive Cost Last 365	
False Postive V True Positive	Y	Did the Potential True Negative Cost outway to the total cost	



Key Take Aways

- Review detection logic alongside case metrics on a regular cadence
  - Use this data to justify Tooling & Detection efficiency improvements
- Reducing false positives improves SOC **accuracy**.
  - When alerts are more actionable, analysts gain confidence in the systems and are less likely to ignore alerts.


Q&A

Thanks for coming!

Sources and Citations

- Alahmadi, Ammar, et al. “99% False Positives: A Qualitative Study of Security Alert Investigations.” *USENIX Security Symposium*, 2022. https://www.usenix.org/conference/usenixsecurity22/presentation/alahmadi
- Critical Start. *Impact of Security Alert Overload.* 2019. https://www.criticalstart.com/news/impact-of-security-alert-overload
- Devo & Ponemon Institute. *2022 SOC Performance Report.* Devo Technology, 2022. https://www.devo.com/resources/report/2022-soc-performance-report
- IBM. *Cost of a Data Breach Report 2023.* IBM Security, 2023. https://www.ibm.com/reports/data-breach
- Ponemon Institute. *The Cost of Malware Containment and Investigation.* Ponemon Research, 2019. https://www.ponemon.org/library/the-cost-of-malware-containment-and-investigation
- SANS Institute. *SANS 2022 SOC Survey Report.* SANS, 2022. https://www.sans.org/white-papers/soc-survey-2022
- Tines. *The Voice of the SOC Analyst: 2022 Report.* Tines, 2022. https://www.tines.com/reports/voice-of-the-soc-analyst
- Trend Micro. “Cybersecurity Tool Sprawl Drives Enterprises to Outsource Detection and Response.” *Multivu*, 2022. https://www.multivu.com/players/English/8967351-trend-micro-cybersecurity-tool-sprawl-drives-plans-outsource-detection-response
- Help Net Security. “SOC Alert Overload Contributing to Analyst Turnover.” *Help Net Security*, 29 Aug. 2019. https://www.helpnetsecurity.com/2019/08/29/soc-alert-overload