# Why do most of the SOC projects fail?

**Catalin Patrascu**
Cyber Security Professional

# About me

- Currently working for Aera Technology - Security Operations and Engineering Manager
- Previously worked for Secureworks, CERT-RO and MoD
- Studied at Military Technical Academy (Bucharest) and Military High School (Alba Iulia)
- Passionate about cyber security and technology in general, Sci-Fi movies and football

**Feel free to ping me!**

- LinkedIn: **catalin.patrascu**
- Twitter: **@catalin_pat**
- Email: **cn.patrascu@gmail.com**

# The actual problem ...

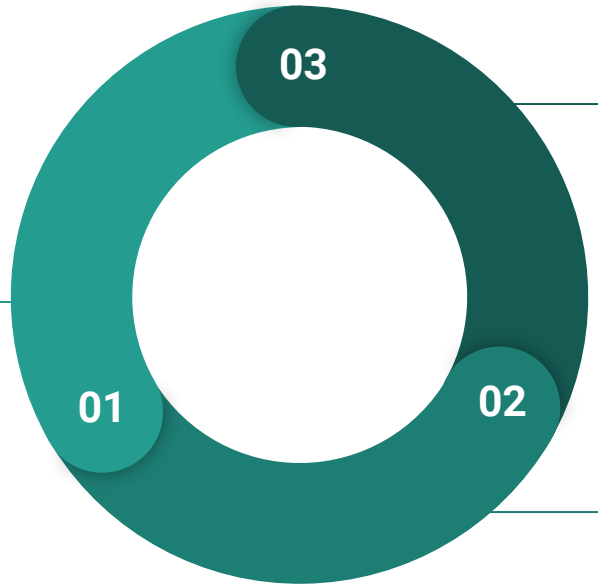
Only about 40% of the organizations  rate their SOC as highly effective

47% have confidence in the ability of their SOC to gather evidence and investigate to find the source of emerging threats

# SOC owners complaints

- The SOC operates as a separate entity
- The SOC throws things over the wall without regard to our capabilities
- In an emergency SOC analysts are pretty much on their own
- We don’t see any value beyond the monitoring
- We were sold amazing and they delivered far less than good
- We need someone who has the expertise and insight that we don’t have

# SOC Pillars

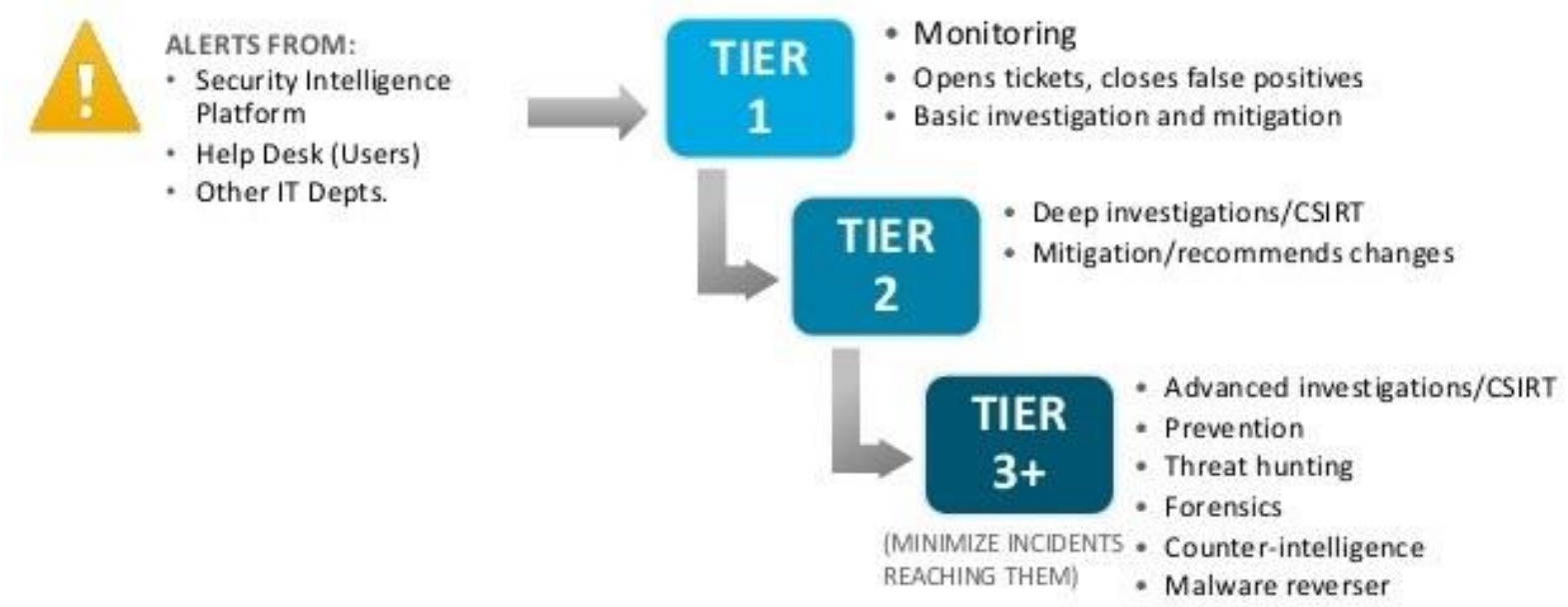



**Technology**

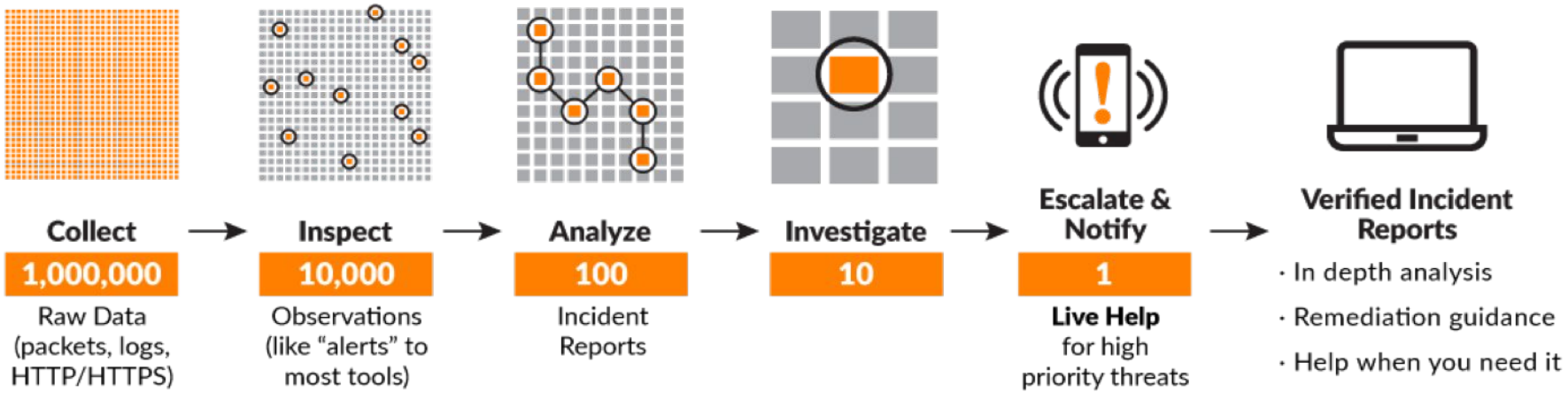
**People**

**Process**

# SOC Tiers


ALERTS FROM:
• Security Intelligence Platform
• Help Desk (Users)
• Other IT Depts.
TIER 1
• Monitoring
• Opens tickets, closes false positives
• Basic investigation and mitigation
TIER 2
• Deep investigations/CSIRT
• Mitigation/recommends changes
TIER 3+
• Advanced investigations/CSIRT
• Prevention
• Threat hunting
• Forensics
• Counter-intelligence
• Malware reverser
(MINIMIZE INCIDENTS REACHING THEM)

# But what is actually a SOC?



# What to look for when building a SOC

- Visibility
- Tools integration
- Data normalization and correlation
- Runbooks
- Control

# One picture that covers all ...

# Thank you!

**Questions? …**

**Now**

**Or later:**

- LinkedIn: **catalin.patrascu**
- Twitter: **@catalin_pat**
- Email: **cn.patrascu@gmail.com**