Maximizing Security Operations

How to Enhance Your SOC's Capability and Maturity

Montance® LLC

CYBRARY | FOR TEAMS

Introductions

Amanda Davi

Director of Business Development

Cybrary

Chris Crowley

Consultant, Author of SOC-Class.com

Montance® LLC

Overview

- Purpose of a SOC and its importance to the greater picture of cybersecurity
- Impact on companies - How MSSPs help organizations
- Importance for the development of cybersecurity professionals and their career development
- Small - Internal, bigger internal, and MSSP

SOC Purpose

Industry References

- SOC-CMM
- NIST CSF
- MITRE: Top Ten Strategies of a World Class Cybersecurity Operations Center (Carson Zimmerman)
- Vendor Literature, for example McAfee:

  A Security Operation Center (SOC) is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

SOC Success Statement (SOCcess?)

Short:

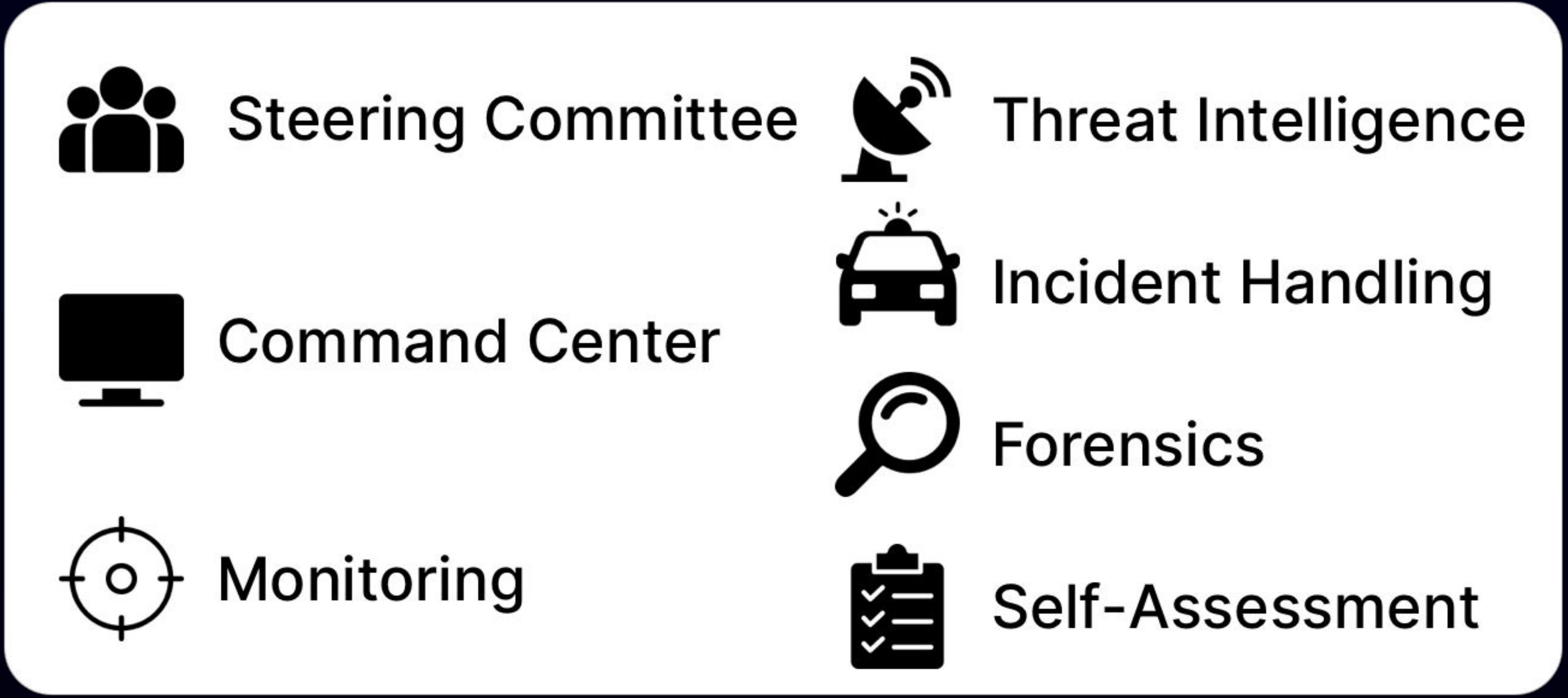
SOC is successful when it improves the organization’s security posture, detects then intervenes in unauthorized events to minimize the impact.

Longer:

SOC is successful when it intervenes in adversary efforts to impact the availability, confidentiality, and integrity of the organization’s information assets. It does this by proactively making systems more resilient to impact and reactively detecting, containing, and eliminating adversary capability within our information assets.

My SOC “Reference Model”

Created for SOC-Class.com



- Steering Committee
- Command Center
- Monitoring
- Threat Intelligence
- Incident Handling
- Forensics
- Self-Assessment

Does My SOC Need to Do All of This?

- People ask me, “do you expect a team of only a few people to do threat intelligence and forensics?”
- Short answer is, “Yes.”
- I realize these will be done infrequently, inconsistently, and at low competence if the SOC is understaffed
- Which leads to the idea of what expectations there are for SOCs, and value propositions to optimize functional capability, usually in the form of outsourcing

Tell Us About Size/Functions/Outsourcing...

- The rest of this presentation is going to cover the findings in the 2020 SOC-Survey (https://soc-survey.com to download)
- Capability
  - Maturity
  - Size
  - Arrangements
  - Staff roles
- I’ll share anecdotes from what I have seen and some advice
- Still have questions after that? There will be time to ask.

SOC: Data on Deployments

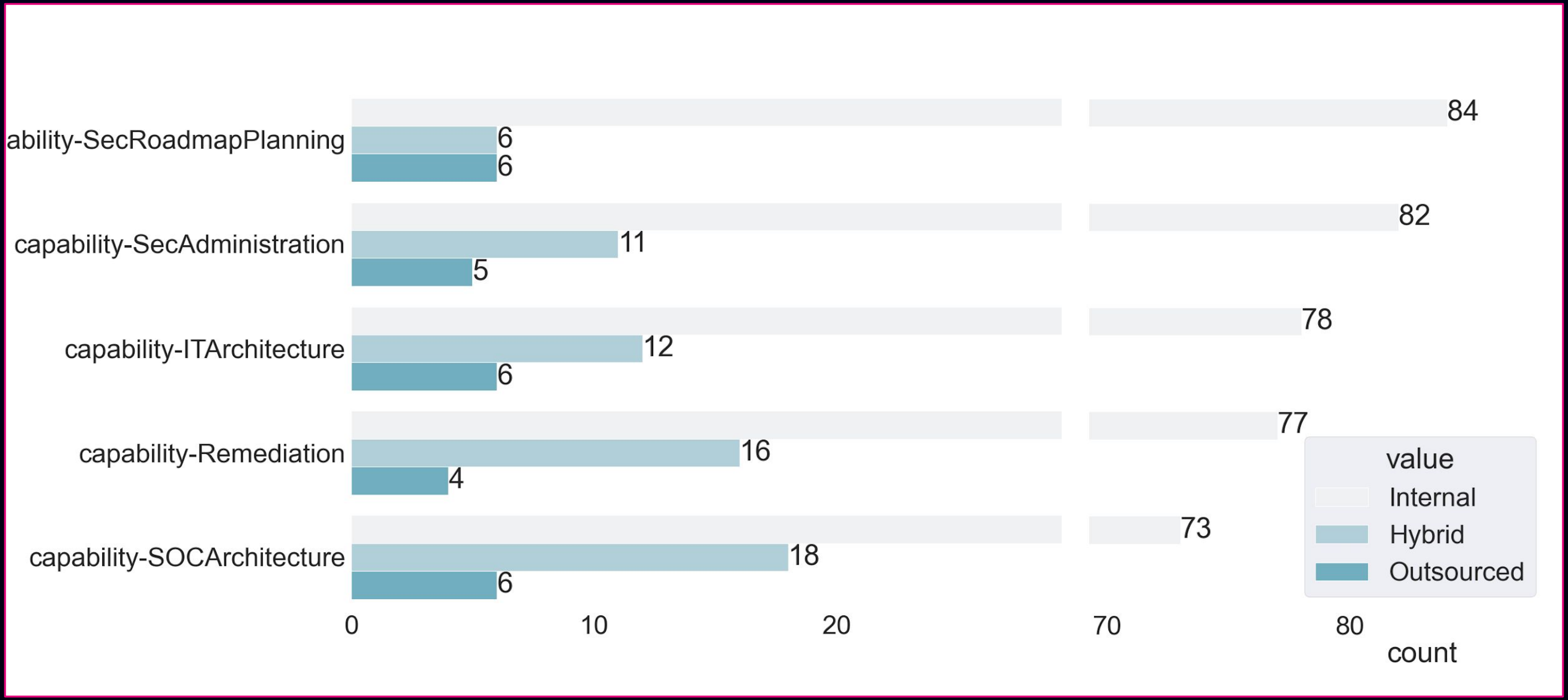
SOC Survey

- I’ve written a SOC Survey for the last four years: 2017-2020
- Download the full 2020 report: https://soc-survey.com
    - Please participate in future surveys
- A few items extracted here

2020 SOC Survey

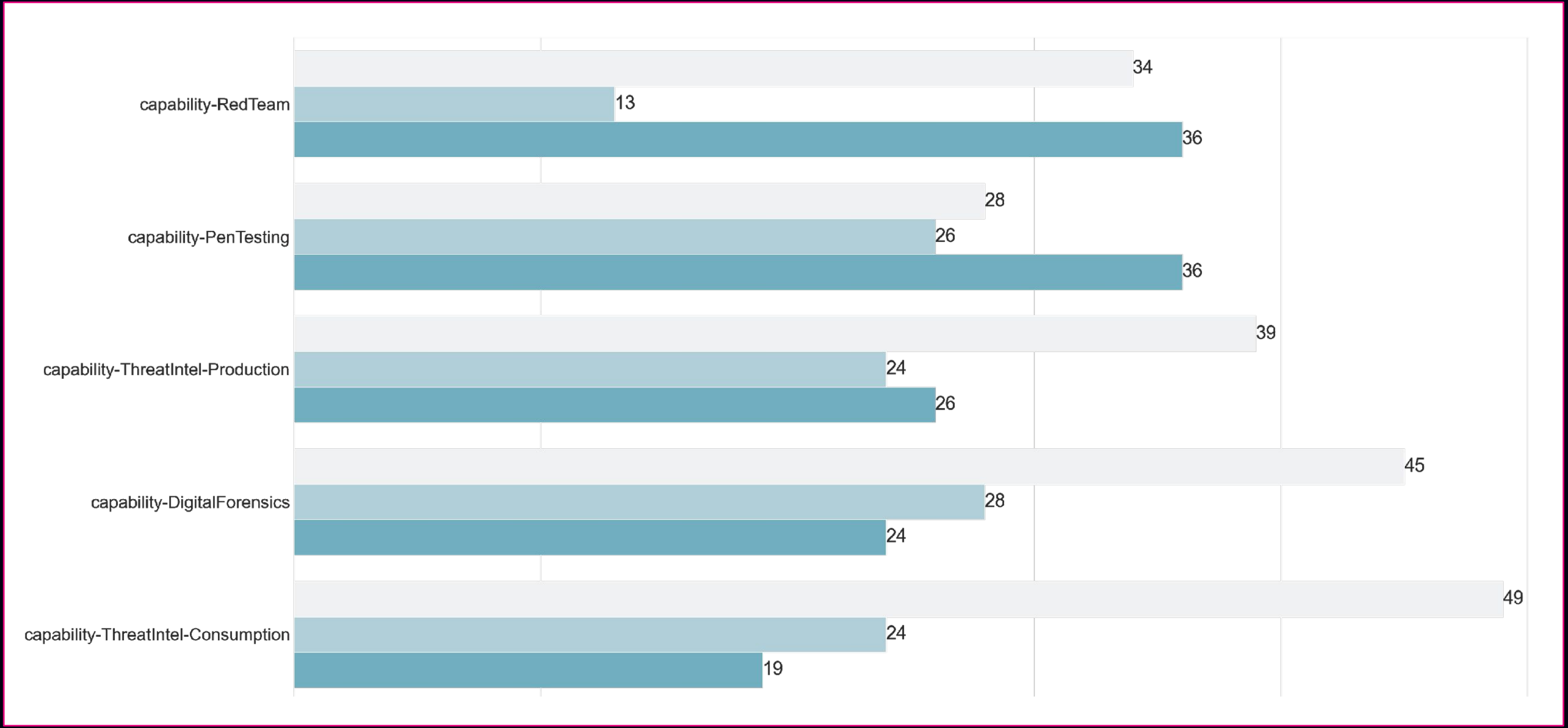
Based on the 2020 SOC-Survey.com we see a mix of internal/external capability

Internal Top 5



2020 SOC Survey

External Top 5



Montance® LLC

CYBRARY | FOR TEAMS

Practical Outsourcing

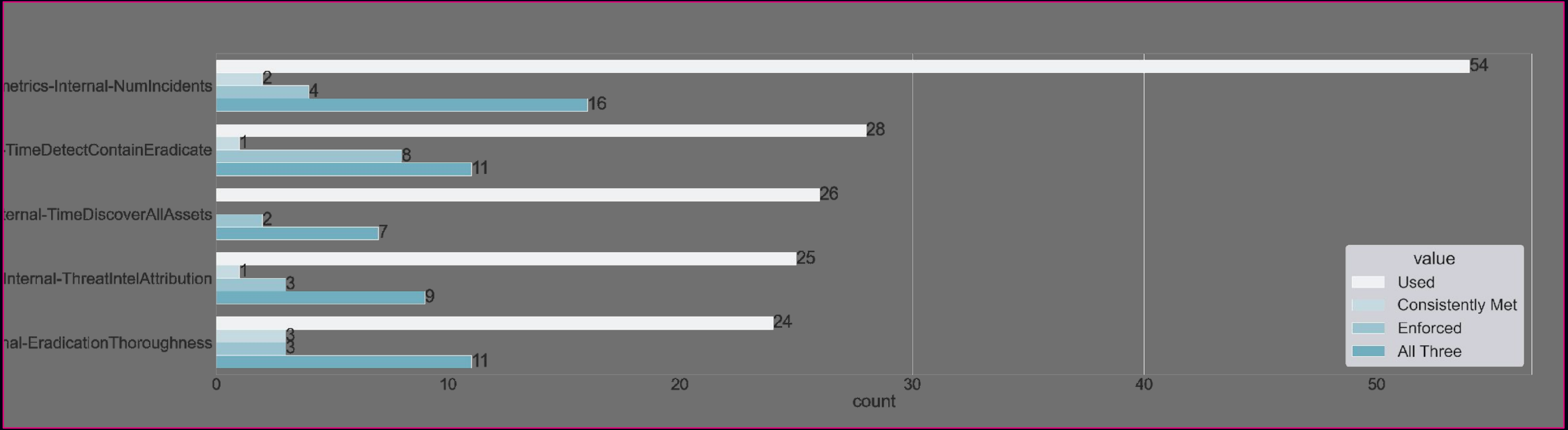
- Pentesting (and all variations of technical assessments)
    - Skill scarcity
    - Objective assessment
- Forensics
    - Skill scarcity
    - Objectivity
- Threat Intelligence
    - Access to data
    - Specialized skill set
- Companies outsource what is commonly called “Tier 1” monitoring
    - Can’t field a team 24×7 due to expense (need 6 FTEs to run one role 24×7), it’s a management headache

SOC: Maturity/Capability

SOC Size, Scale, Maturity

- First, Compliance/Security is a big split in my opinion
  - I label it a “security” SOC if they’re empowered to make change in to the organization, it’s IT systems, and it’s culture
  - I label it a “compliance” SOC if they’re no support to create security change
- Second, striving to be a learning SOC with long-term objectives and effective program for development of staff as well as ingestion of external information relevant to protected assets
- A few ways to measure maturity: MITRE ATT&CK (Defensive Gap Analysis + Threat Intel Informed prioritization) or SOC-CMM (download excel spreadsheet and assess)

Metrics


netrics-Internal-NumIncidents
-TimeDetectContainEradicate
ternal-TimeDiscoverAllAssets
Internal-ThreatIntelAttribution
nal-EradicationThoroughness
54
2
4
16
28
1
8
11
26
2
7
25
1
3
9
24
3
3
11
0
10
20
30
40
50
count
value
Used
Consistently Met
Enforced
All Three

Practical Metrics

- We offer possible loss prevention (SOC doesn’t guarantee protection)
- Quantity-based metrics: frequently little value in reporting without corresponding trending/moving average information
- Develop Service Level Objectives (SLOs) to meet performance objectives for things within the SOCs control
  - Service Level Objectives on adversary controlled actions don’t make sense
- Time-based metrics drive analysts to work fast
  - Have a corresponding quality metric
- Individual analyst tracking worthwhile but difficult, assess team contributions (e.g., queries built) rather than individual “tickets closed”

Advanced Metrics

- Incident Impact Quantification
  - Organizationally specific definition of the values for each system, and agreed upon guidance for characterizing low, moderate, high incidents
- Loss Prevention Calculation
  - Based on an agreed upon cost for incident handling and loss, what did the SOC help to prevent in terms of more involved clean up and damage control?
- Crowley's Incident Avoidability
  - Discrete scale: 1, 2, 3 (Avoidable, Risk Taken, Zero Day)
- More metrics: Zimmerman & Crowley: https://mgt517.com/first-metrics

Metrics to Users

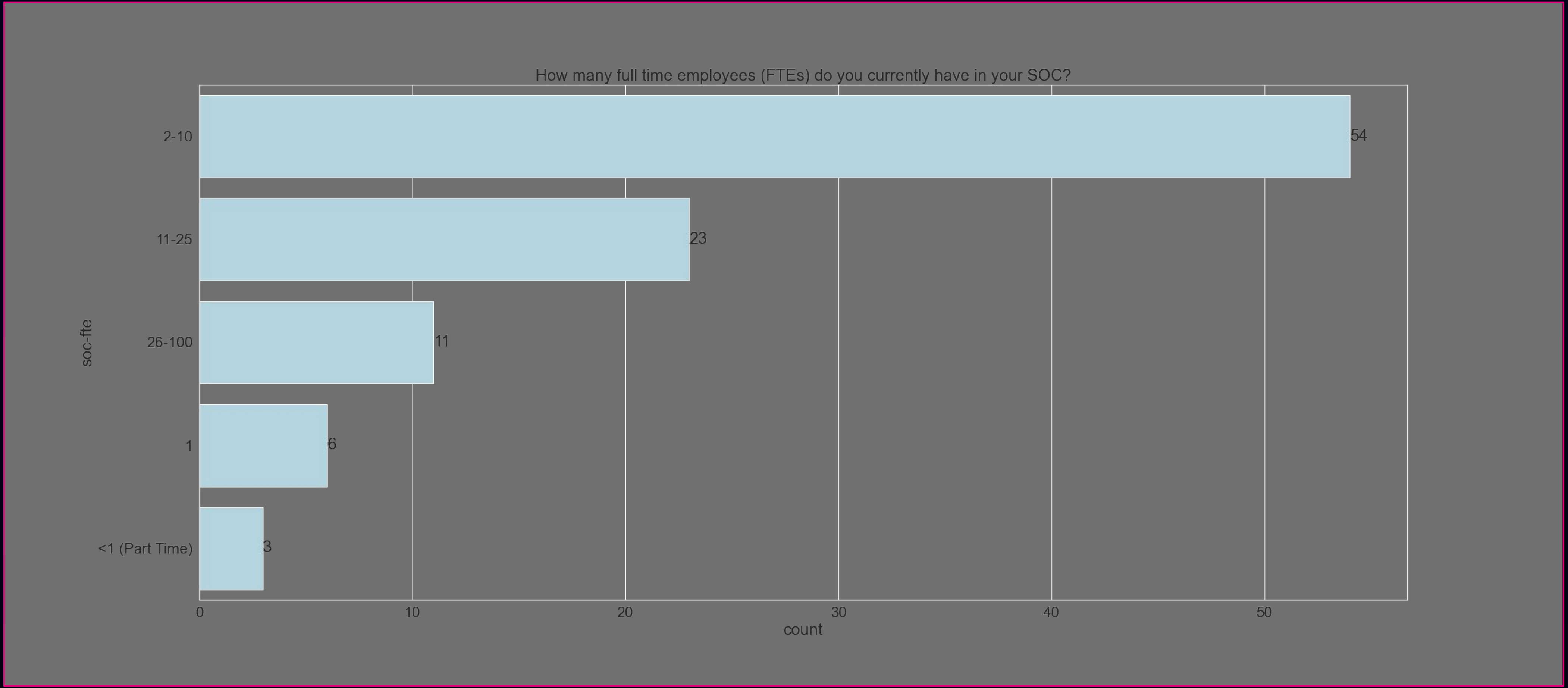
- Provide a “weather forecast” style set of information to users
  - What do they need to do/know right now?
  - Work with your awareness program for long-term behavioral changes
  - You may need to tailor messaging to different types of constituent: Executive team, and your company’s customers get different messaging
- Incident Avoidability bundled with Impact Quantification reported by business unit would make a phenomenal quarterly wrap up
  - It shows posture, realized impact, and adversary targeting in a single infographic

SOC: Size

SOC Size

- The majority of SOCs are small
  - Usually internal SOCs
- Some MSSPs are small in staff size, and basically only offer the “monitoring” function
- Some SOCs get large, 100+ full-time staff, almost always MSSPs that grow this large
  - The SOC-Survey.com has the response set, and Python code showing how to select for attributes of responses if you’re interested in exploring further

2020 SOC Survey: SOC Size

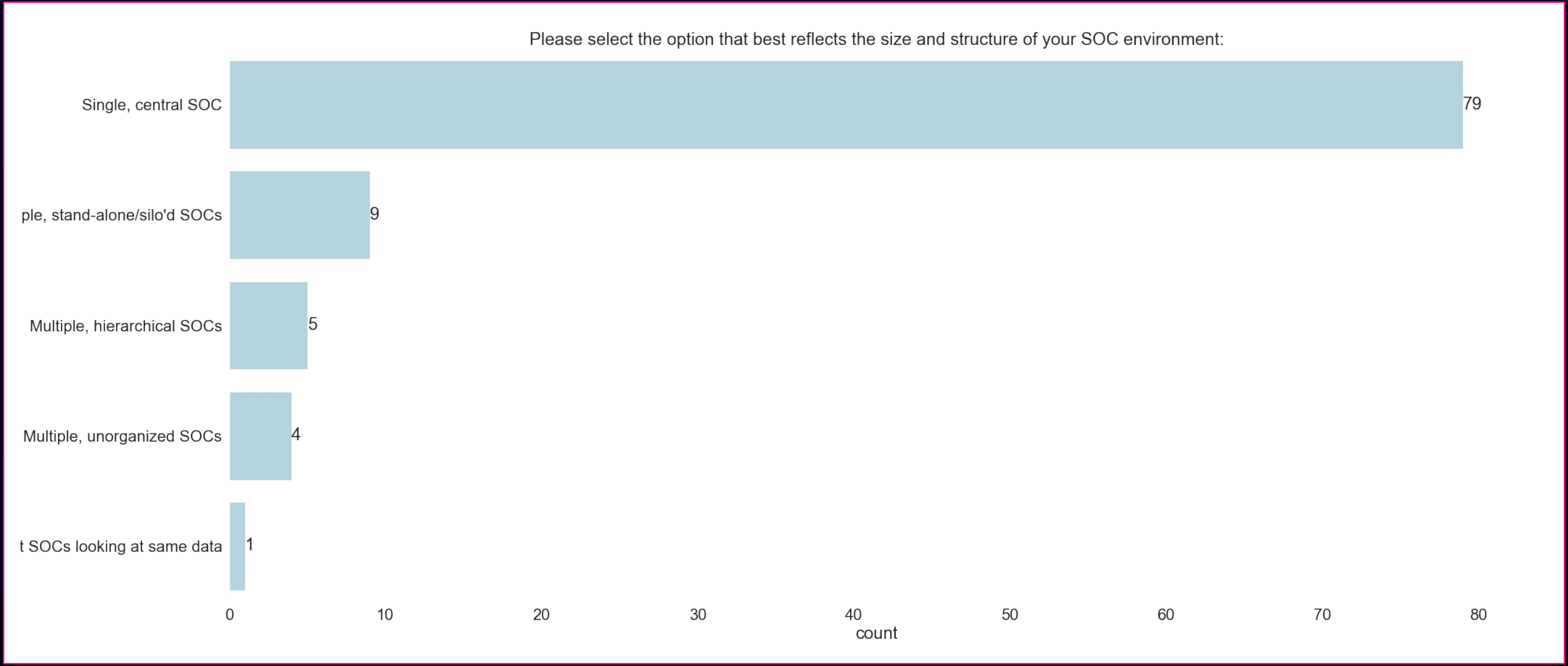


Montance® LLC

SOC Arrangements

- Follow-the-sun
- Regional deployments
- Business-line Fiefdoms
- Multi-SOC coordination: Federated, hierarchical,…

2020 SOC Survey: SOC Deployments



Montance® LLC

CYBRARY | FOR TEAMS

SOC: Staff

Staff Roles

- Most SOCs (size 2-10 groupings) are going to expect staff to be fluid between the functions I mentioned (command center, monitoring, incident response, forensics, threat intel, self-assessment)
  - Generalist: flexibility and adaptability expectations are high; frequently expected to handle all aspects of the larger process
- Larger SOCs are going to hire for specializations (probably along these functional lines, but not always) to fill roles, and maintain the “24×7” L1 / L2 / L3 strategy
  - Specialist: rigor and procedure are expected along with specialization; frequently low visibility on the larger process

Career Path

- Many start a Cyber Career as a “SOC Analyst” and hate it ☺️
- Usually the fault of the business, using inexperienced staff in analyst roles without adequate context, skills, and guidance because no one else is willing to work 10-12 hour overnight/swing shifts
  - A lot has been written/presented on this in the last five years
  - My favorite quote from the SOC lead for a massive well-known MSSP, “Do you really want a sleep deprived, inexperienced staff member making the most important decision in the SOC?” That most important decision being the selection of which alerts should be investigated further.
- Seek training, and embody the spirit of constant training for improvement, see my YouTube for SOC training program video: https://mgt517.com/youtube

SOC: Conclusion

Conclusion

- SOC is responsible for security monitoring and response
- SOC mission is loss prevention
- Globally, SOC size and shape vary dramatically in organizations
- Staff roles within the SOC vary widely from generalist to detailed specialist, depending on the maturity, size, and shape of the SOC
    - Perceived opinion of SOC analyst value varies dramatically, too
- In the next installment of this webcast series, we'll discuss more details

Let's Connect

Amanda Davi

adavi@cybrary.it

linkedin.com/in/amanda-davi

www.cybrary.it/business

Chris Crowley

chris@montance.com

mgt517.com/linkedin

www.soc-class.com

Resources

- SOC Career Pathways- Level 1, Level 2, Level 3
- Free E-Book by MITRE- Ten Strategies of a World-Class Cybersecurity Operations Center
- SOC Survey Key Findings and Results Video Series

Thanks For Joining Us!