Maximizing Security Operations

How to Enhance Your SOC's Capability and Maturity

Part 2: SOC Architecture and Management

Montance® LLC

CYBRARY | FOR TEAMS

Introductions

Amanda Davi

Director of Business Development

Cybrary

Chris Crowley

Consultant, Author of SOC-Class.com

Montance® LLC

Overview

Part one covered: Functional Areas of a SOC; Purpose of a SOC and its importance to the greater picture of cybersecurity

- View Part 1: The Role of a SOC, on-demand

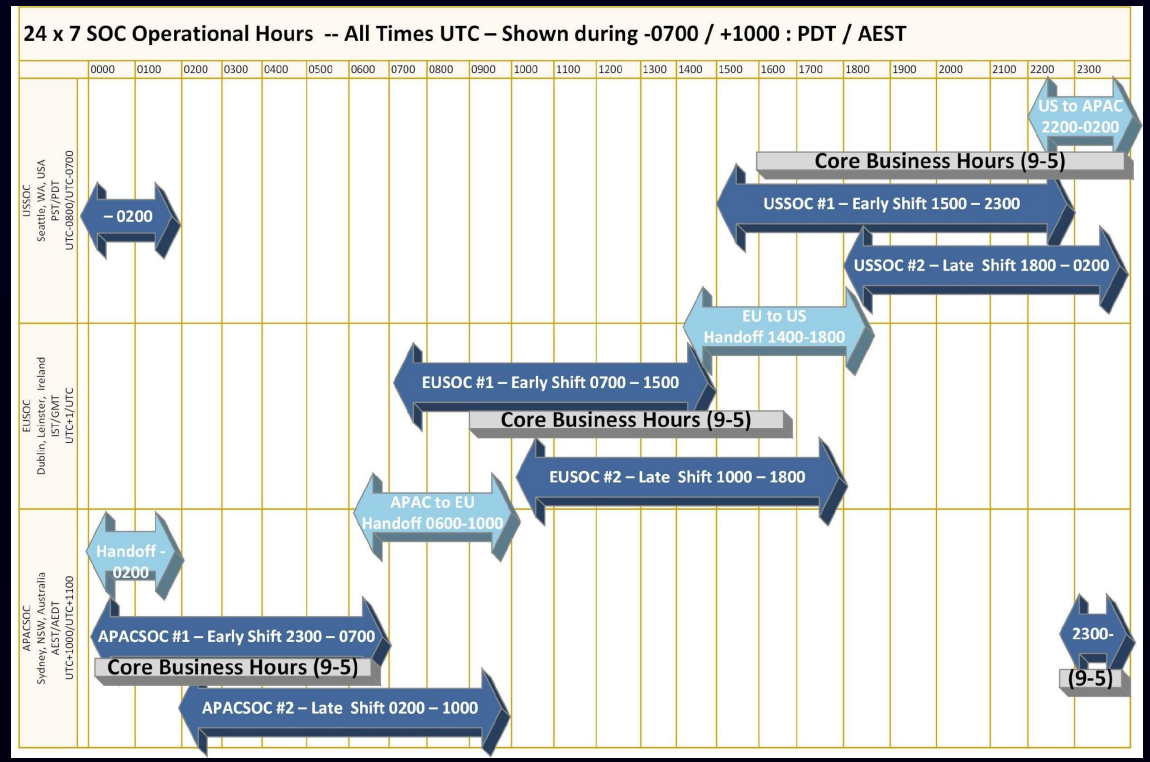
This talk covers:

- Architecture - How to address challenges - Technical elements of building a SOC, and how to manage technical professionals
- What do individuals need to know? (practitioners and management)
- Incident response: What happens when there's an active threat?

Architecture

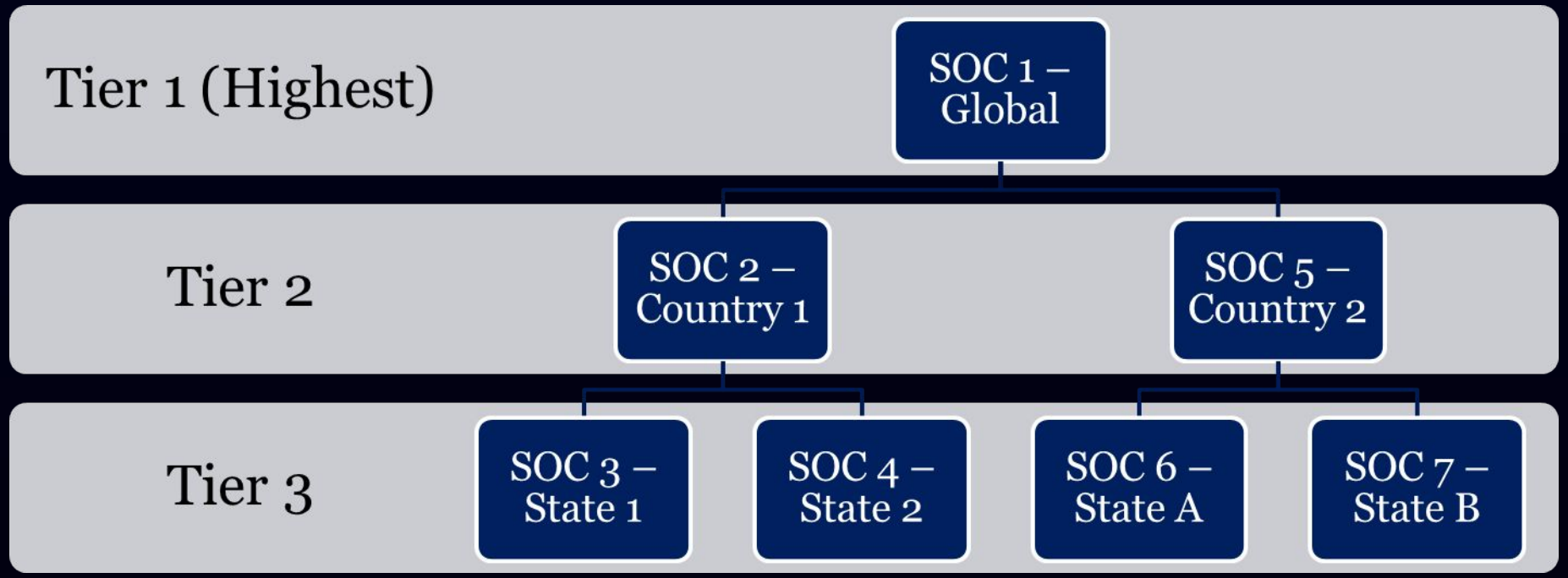
Follow the Sun

- 24×7 coverage, in multiple (usually three) locations
- Procedurally complex, hand-off management takes ongoing oversight
- Global/Big company strategy
- Often seen as a value proposition to add SOC headcount in lower cost location
- Spin on this strategy: “Follow the Stars” uses strengths of teams in different regions to work to their strengths



Federated / Hierarchical

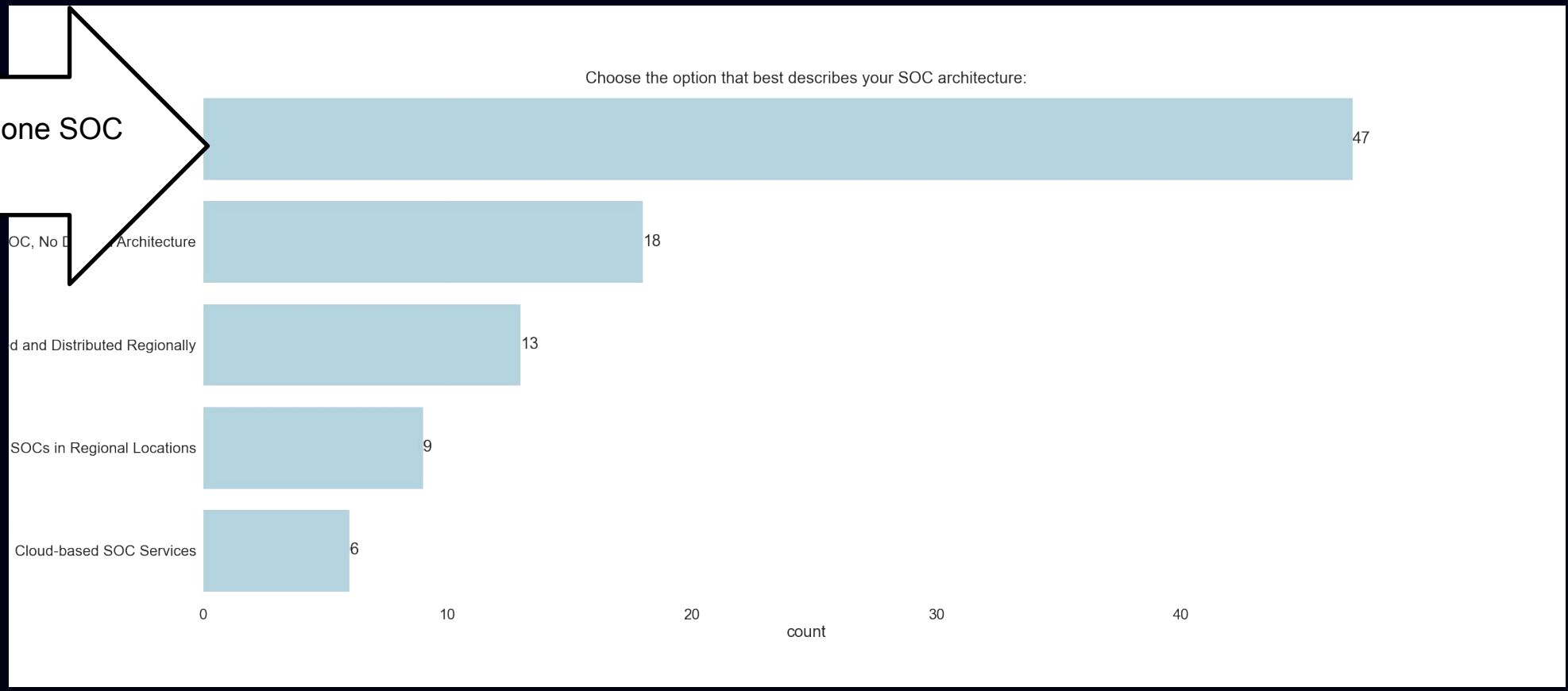
- When there are multiple SOCs in one organization, they're usually either federated or hierarchically organized
- Federated: independent, collaboration as appropriate basis decided on a case-wise approach. Decisions made in cooperative self-interest.
- Hierarchical: mandated information flow up, direction flows down



2020 SOC-Survey Architecture Results

- The 2020 SOC Survey discussed architecture and regional arrangement
- Results show:

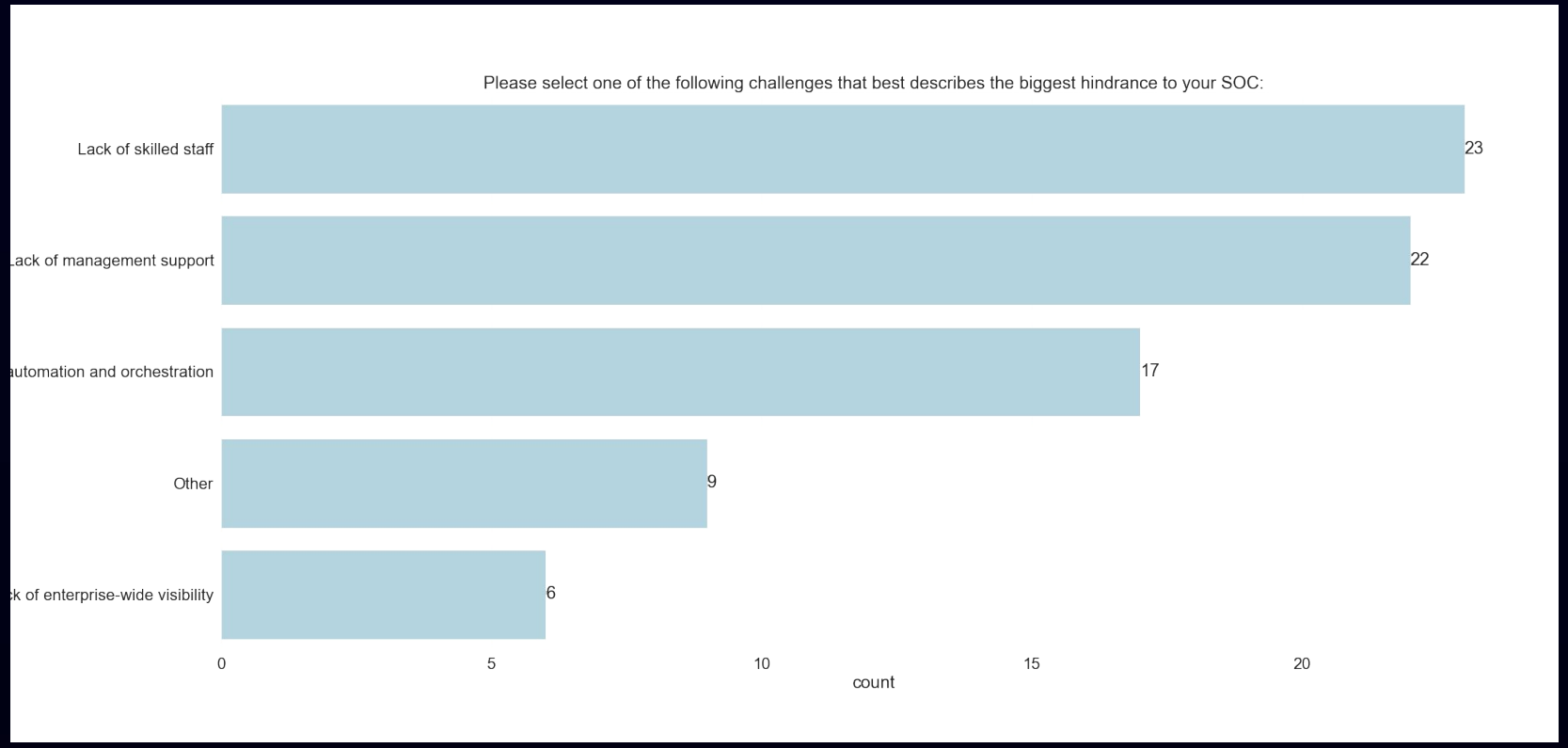
Centralized in one SOC (47)



SOC Challenges

Challenges

- Funding is an obvious one
- Skilled Staff
- Effective tool use
- 2020 SOC Survey asked about challenges
- The “Lack of management support” became an a/b test for the report in the 2020 SOC Survey



SOC Technology

Overview

- Technical elements of building a SOC
- Crowley RSA talk: Technology Taxonomy and previous related talks (SANS SOC Summit, ex.)
- Core principles: interoperability, staff to run, avoid becoming a “log collector” and focus on developing analytic capability
- Common mistake: buy tech to figure out what can be done with it
- Correct approach: Decide what you need to do, then buy the right tech to integrate into existing portfolio to add capability or increase efficiency

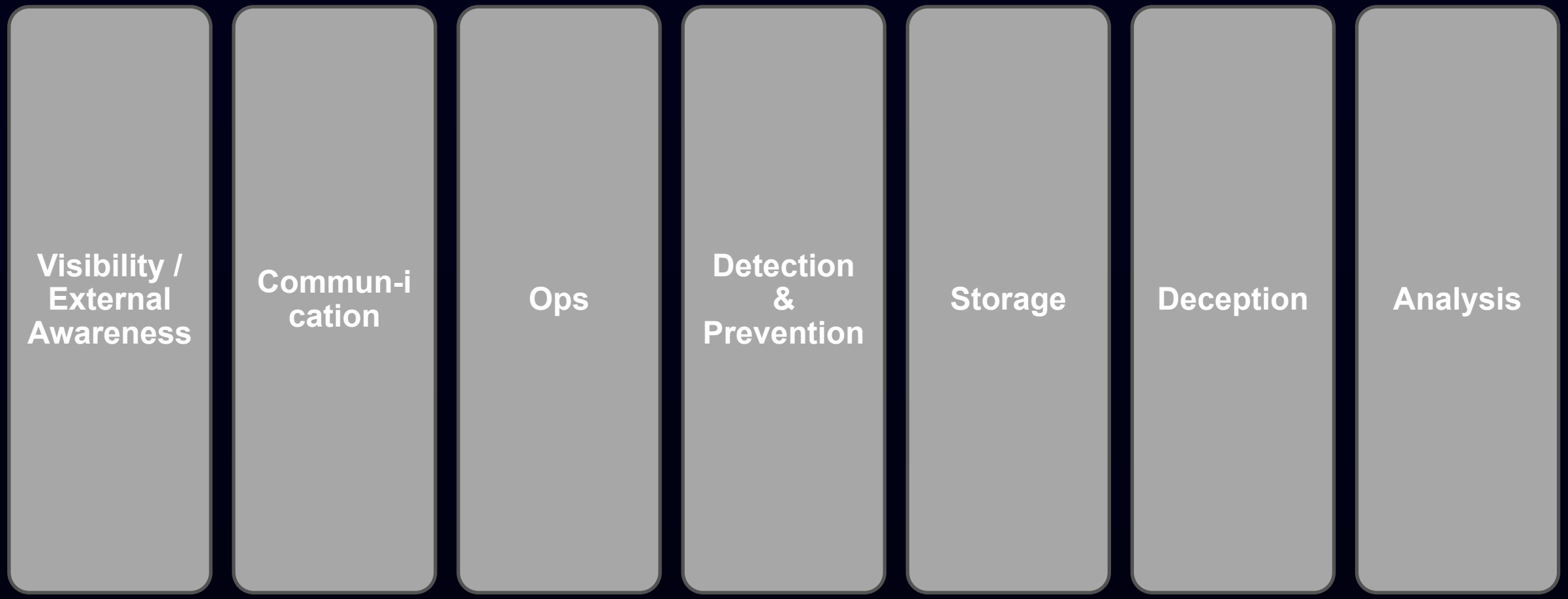
Technology “Shopping List”

- I’ve attempted to capture all technology needed
- Documented as the “technology taxonomy”
- Spreadsheet available of a per-functional area tech listing
- Tools like are like pets: each one requires a place to live, care and feeding, updates, maintenance. How many pets can you afford to keep?
- Federate tools and data!

Technology	Specific Product Selected	Owned / Managed by Function?	Using Another Function's Technology? (If Yes, Cite Function)	Outsourced?	Oursource Partner?	Estimated Purchase Price	Estimated Annual Support and Maintenance Percentage	Estimated Annual Support / Maintenance Annual Increase	Year 1 Annual Maintenance Cost	Year 2 Annual Maintenance Cost	Year 3 Annual Maintenance Cost
Performance Monitoring	What's Up					$5,000.00	25%		$1,250.00	$1,250.00	$1,250.00
External Threat Feeds		No	Threat Intel						$0.00	$0.00	$0.00
Network Security Monitoring											
SIEM	Splunk	Yes				$200,000.00	30%	5%	$60,000.00	$70,000.00	$80,000.00
NIDS	Security Onion	Yes				$15,000.00	20%	5%	$3,000.00	$3,750.00	$4,500.00
NIPS	n/a	Yes						5%	$0.00	$0.00	$0.00
HIDS	Widows Event Logs	Yes							$0.00	$0.00	$0.00
EPS		Yes							$0.00	$0.00	$0.00
HIPS	CarbonBlack	Yes				$35,000.00	20%	5%	$7,000.00	$8,750.00	$10,500.00
Host Event Logs	Windows Event Logs	Yes						25%	$0.00	$0.00	$0.00
Network Infrastructure Logs	Splunk (existing)	No						5%	$0.00	$0.00	$0.00
Application	Splunk										

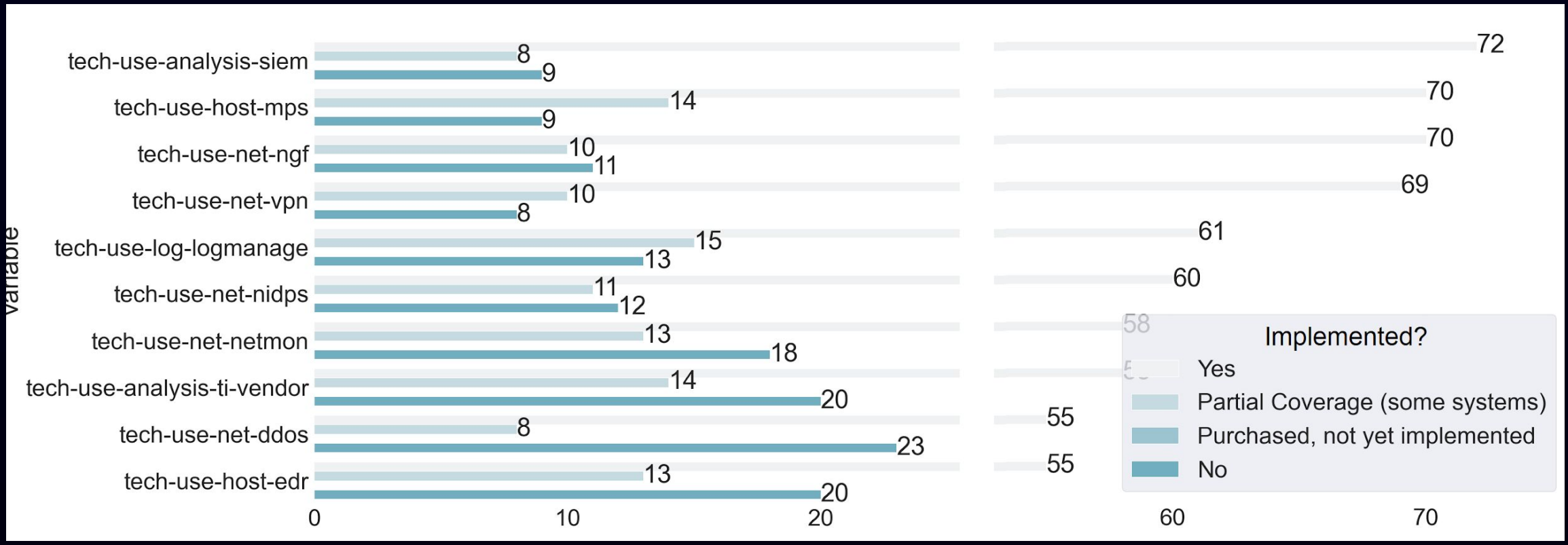
Montance® Technology Taxonomy

- High level categories (extensive sub-categories and individual tech)



2020 SOC Survey Technology

- Technology satisfaction graded
- Technology in terms of deployment state (yes, partial, owned not implemented)



SOC Staff:
Managing Analysts

Overview

- How to manage technical professionals
- I've also given a talk with a lot of details about this program of training, youtube "vIntro to vHard" (short and long versions)
- Was originally given at Educause 2020

Training Objectives

- Most SOC staff are not fully developed to be SOC Staff, ongoing training is necessary. Even the best people are tasked with a multitude of things and are out of practice
    - What are you trying to develop in SOC staff?
    - Memory?
    - Analysis?
    - Organizational Awareness?
    - Threat modeling / prediction?

Training Objectives

USAF Cadet Study: Motivation of the least fit person on the team has most benefit

Thus, our results suggest that there is an efficiency motivation for improving the health habits of the least physically fit individuals, as doing so may ultimately affect the health of many more individuals by harnessing the effect of the social multiplier.

SOC Staff:
Fundamental Knowledge

Training by Levels or Roles?

- NICE from NIST has an amazing spreadsheet you should look at
- I use a simplified version based on Junior / Mid / Senior
- Senior, is someone who is capable of making decisions after weighing all of the organizational and environmental factors and constraints to arrive at an optimal approach

NICE Specialty Area	NICE Specialty Area Definition	Work Role	Work Role Definition	Work Role ID	KSAs	Tasks
PROTECT and DEFEND (PR) - *Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.*						
Cybersecurity Defense Analysis (CDA)	Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network to protect information, information systems, and networks from threats.	Cyber Defense Analyst	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.	PR-CDA-001	Click to view KSAs	Click to view Tasks
Cybersecurity Defense Infrastructure Support (INF)	Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.	Cyber Defense Infrastructure Support Specialist	Tests, implements, deploys, maintains, and administers the infrastructure hardware and software.	PR-INF-001	Click to view KSAs	Click to view Tasks
Incident Response (CIR)	Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.	Cyber Defense Incident Responder	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.	PR-CIR-001	Click to view KSAs	Click to view Tasks
Vulnerability Assessment and Management (VAM)	Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations.	Vulnerability Assessment Analyst	Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.	PR-VAM-001	Click to view KSAs	Click to view Tasks
ANALYZE (AN) - *Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.*						

Junior

- How computers talk to one another: DNS, IP, TCP/UDP, HTTP(s), TLS
- Common successful adversary techniques and tactics (MITRE ATT&CK is a good list) for C2, attacks (service side, client side, phishing, web app attacks, etc.)
- Basic host based acquisition, pre-forensic collection, baseline development, and hunting in this data
- Report writing fundamentals

Mid-Level

- All junior, plus:
  - Host memory collection and basic analysis
  - Basic reverse engineering
  - Architecture and security specifications
  - Organization OSINT research
  - Report writing fundamentals, review of all reports written by other analysts

Senior

- All junior and Mid-Level plus:
  - Advanced assessment creation (eg. novel C2 development)
  - Advanced memory, advanced host and forensic analysis
  - Insider threat hunting scenario development
  - Use case development lead modeling business need
  - Hunt team program lead (create new hunts based on current threat intelligence)
  - Report writing fundamentals, info graphical depiction of complicated information and all metrics review

SOC: Conclusion

Conclusion

- SOCs take a lot of different forms: follow the sun, federated, hierarchical
- Technology is necessary, but usually takes too much of the focus. Many SOCs end up just being another instance of IT that requires care and feeding instead of accomplishing cybersecurity objectives
- Staff training takes many forms, and requires thoughtful planning
- The relationship between incident handling and the SOC is critical and varied in implementation: SOC might be MSSP initial and you do IR, IR is embedded, or adjacent, or third-party (MSSP)

- In the next installment of this webcast series, we'll discuss more details about hiring and retaining staff!

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
- Montance® SOC Build Timeline: https://montance.com/timeline/
- SOC Survey Key Findings and Results Video Series

Thanks For Joining Us!