2023 SOC Survey Highlights and Deep Dive

Montance® LLC

- Consultant: Montance®
- SOC-Class.com:
  Design, Build, Operate and Mature your SOC
- SOC-Survey.com: 2017-2024
- SANS Senior Instructor
- Sectors: Defense, Education, Energy, Government, Financial, Software Dev., Telecom…
- Open to connect on LinkedIn

Christopher Crowley

Surveys ‘R’ Lame

- If I say “data” in this presentation, please throw nerf balls at me! “Survey Responses” != data
- Population of SOCs in the world is not known
- 2024 SOC Survey question period open
  - https://soc-survey.com
    ^^^ please take it ^^^ release event info
- Coordinating and studying SOCs globally is hard: (understandable) data sharing concerns

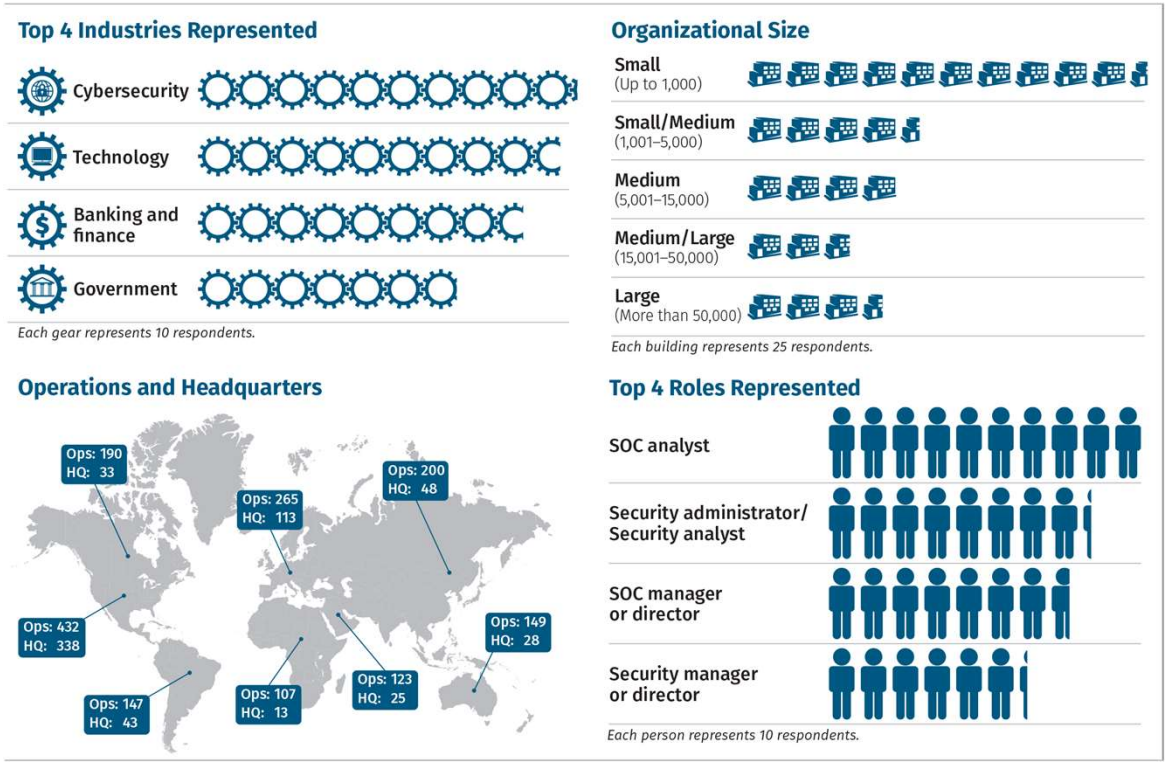
2023 SOC Survey

Analyst Program

- **641 respondents, mean time of 59 minutes**
- 7th year
- Proposed uses:
  - Strategic comparison to peers: capabilities, etc.
  - Technology comparison
- DEIDENT responses available on https://soc-survey.com
  - 2023 Jupyter notebook companion to released responses

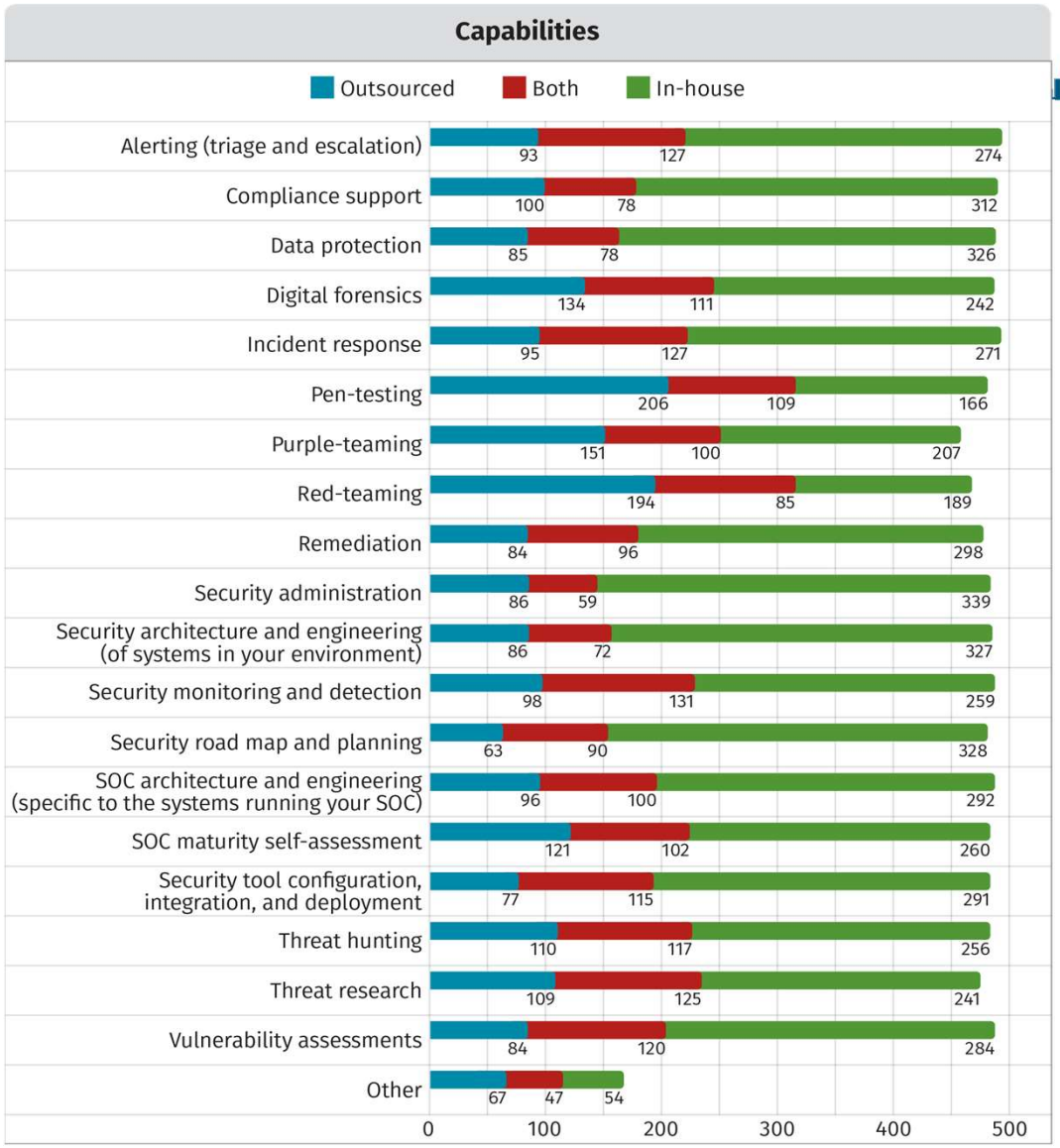
Demographics

- North America
- **Finance, Gov, and High tech**
- Only English this year



Top Capabilities

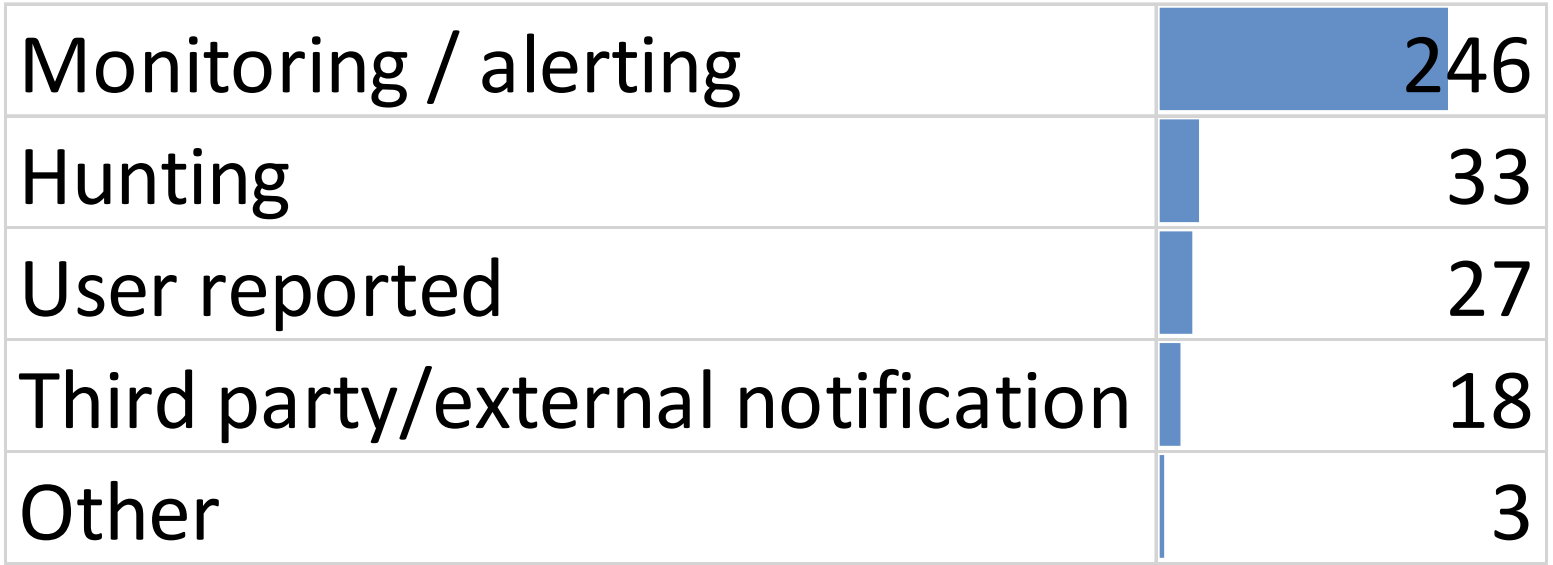
- Alerting & triage
- Incident response
- Compliance support
- Data protection
- Q3.13, n=545 (sorted by sum)



Key Finding: Incident Detection

Analyst Program

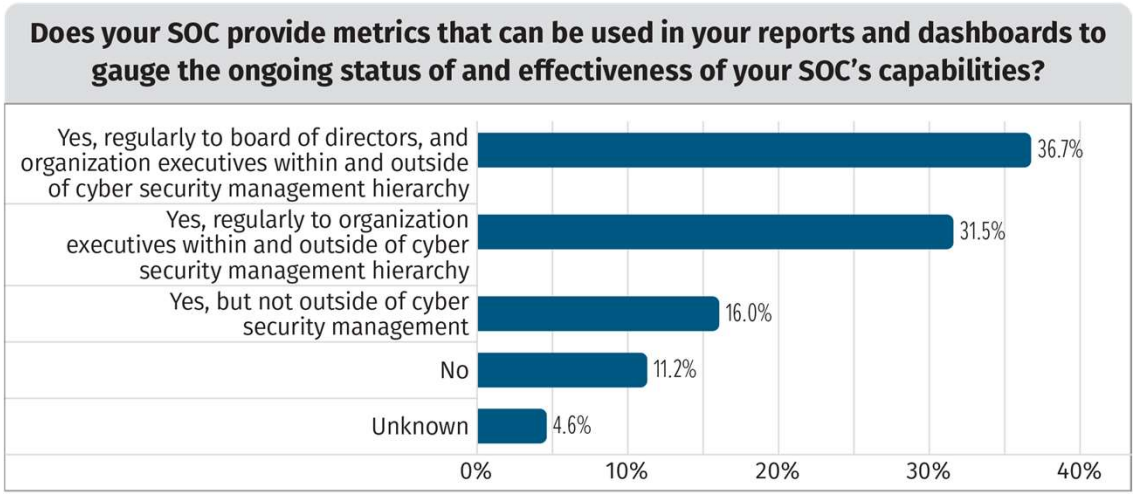
- More than 75% of respondents detected incidents before external notification; 9% via proactive threat hunting (Q3.31, n=360). Figure: **Top Detection method**



Key Finding: Metrics

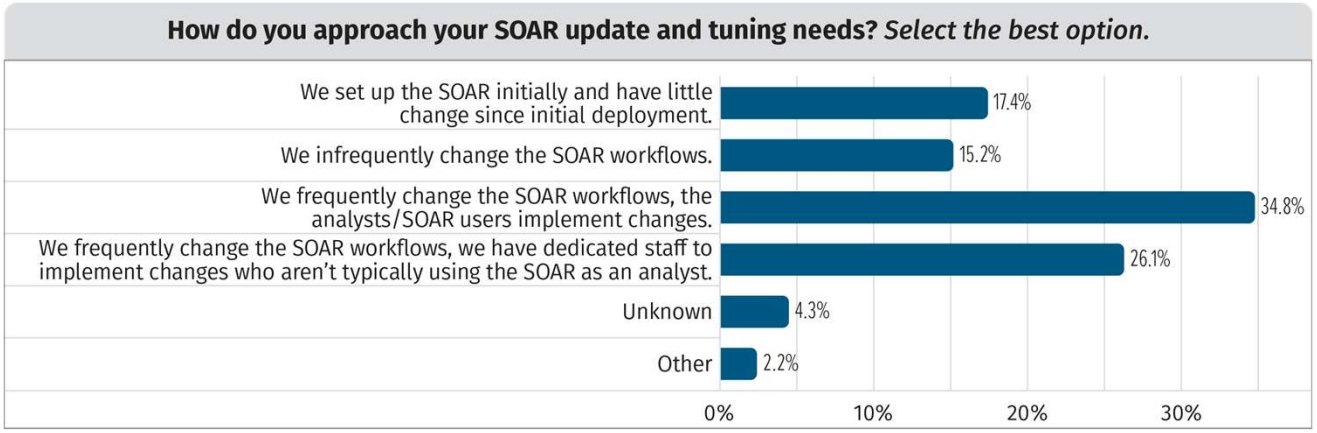
Analyst Program

- 84% of SOCs collect and expose metrics (Q3.47: 39/349, **11.2% - No**)
- Top three
  - Quantity of incidents
  - Time from detect to eradicate
  - Ratio of incidents from known/unknown vulnerabilities



Key Finding: SOAR Tuning

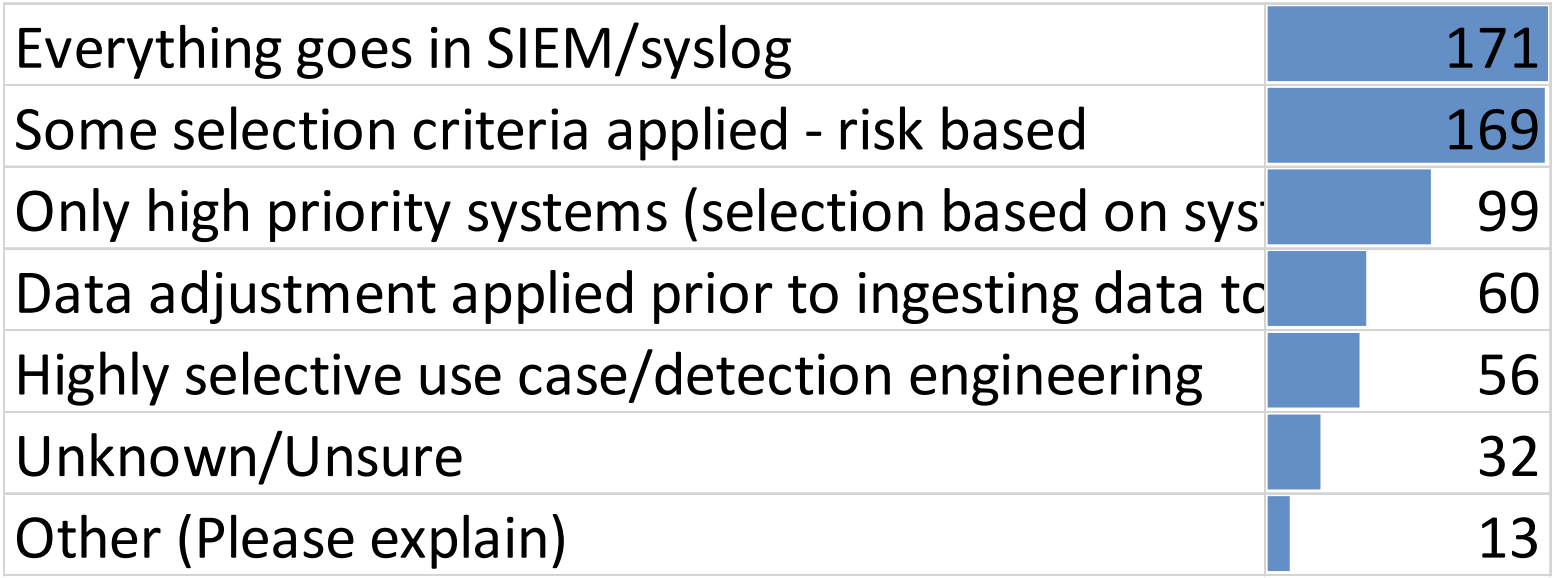
- Continual **tuning of SOAR by skilled analysts** is performed
  - SOAR as a work-style, not throwing a switch (Q3.33, n=46)
- SOAR work-style increases effectiveness more than reduces staffing needs



Key Finding: SIEM Data

Analyst Program

- What is the primary approach you use to decide what data to ingest into your SOC? (Q3.5, n=600)



Everything goes in SIEM/syslog	171
Some selection criteria applied - risk based	169
Only high priority systems (selection based on sys	99
Data adjustment applied prior to ingesting data to	60
Highly selective use case/detection engineering	56
Unknown/Unsure	32
Other (Please explain)	13

Key Finding: Budget

Analyst Program

Management *takes recommendations from SOC leads/managers, but ultimately* ***decides how to allocate funds, sometimes against SOC management's recommendations.*** (Q3.69, n=300)

How is funding allocated in your organization? Select the b	
Management takes recommendations from SO	126
Management and SOC leads/managers work to	73
Management takes recommendations from SO	56
Management pays little heed to the recommen	39
Other (Please comment)	6

Key Finding: Outsourcing

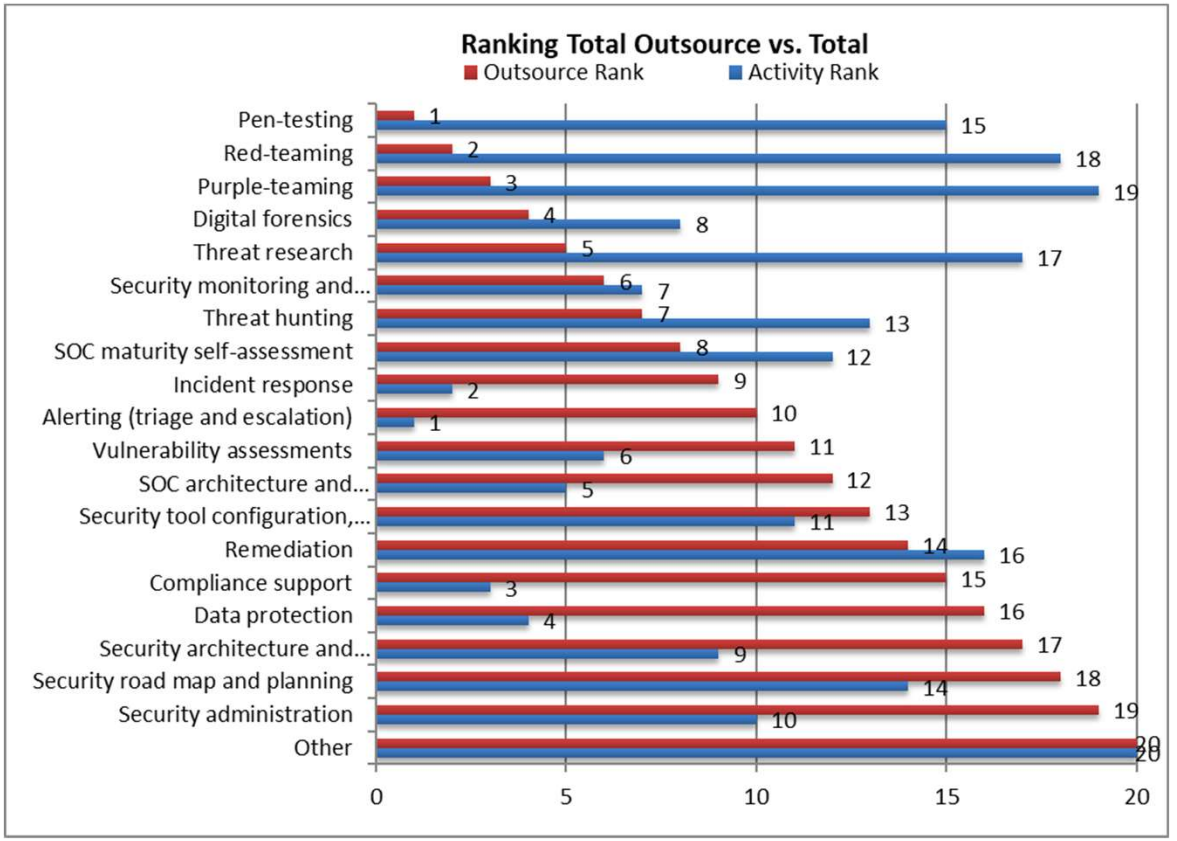
Analyst Program

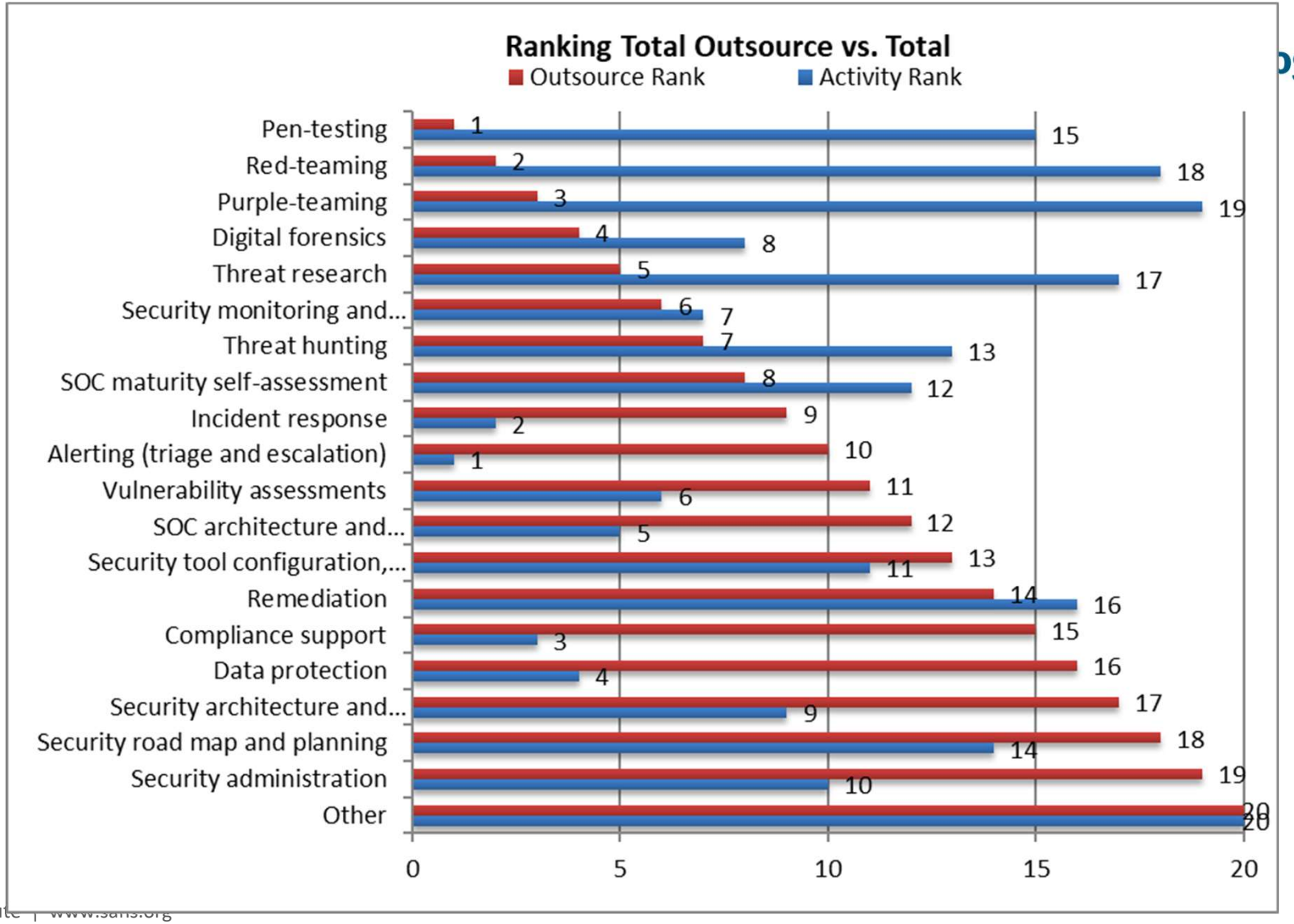
- Pen-testing (and variants) and forensics
- Whereas **in-house tends to be security system architecture, engineering, planning, and administration**

- Chart on next slide shows outsourced items tend to be less frequently done

Key Finding: Outsourcing (2)

- Red rank is highest to least outsourced
- Blue rank shows order capability is done
- **More likely outsourced are less likely done** (bigger next slide)

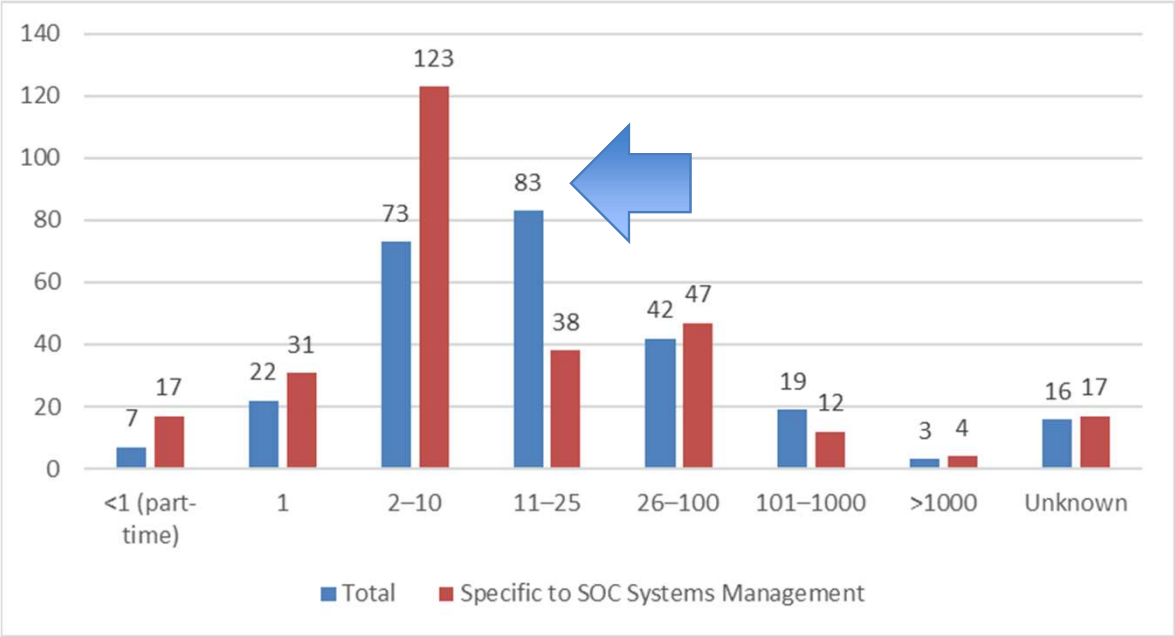



Ranking Total Outsource vs. Total
Outsource Rank
Activity Rank
Pen-testing
Red-teaming
Purple-teaming
Digital forensics
Threat research
Security monitoring and...
Threat hunting
SOC maturity self-assessment
Incident response
Alerting (triage and escalation)
Vulnerability assessments
SOC architecture and...
Security tool configuration,...
Remediation
Compliance support
Data protection
Security architecture and...
Security road map and planning
Security administration
Other
1
15
2
18
3
19
4
8
5
17
6
7
7
13
8
12
9
2
10
1
11
6
12
5
13
11
14
16
15
3
16
4
17
9
18
14
19
10
20
20
0
5
10
15
20

Staff

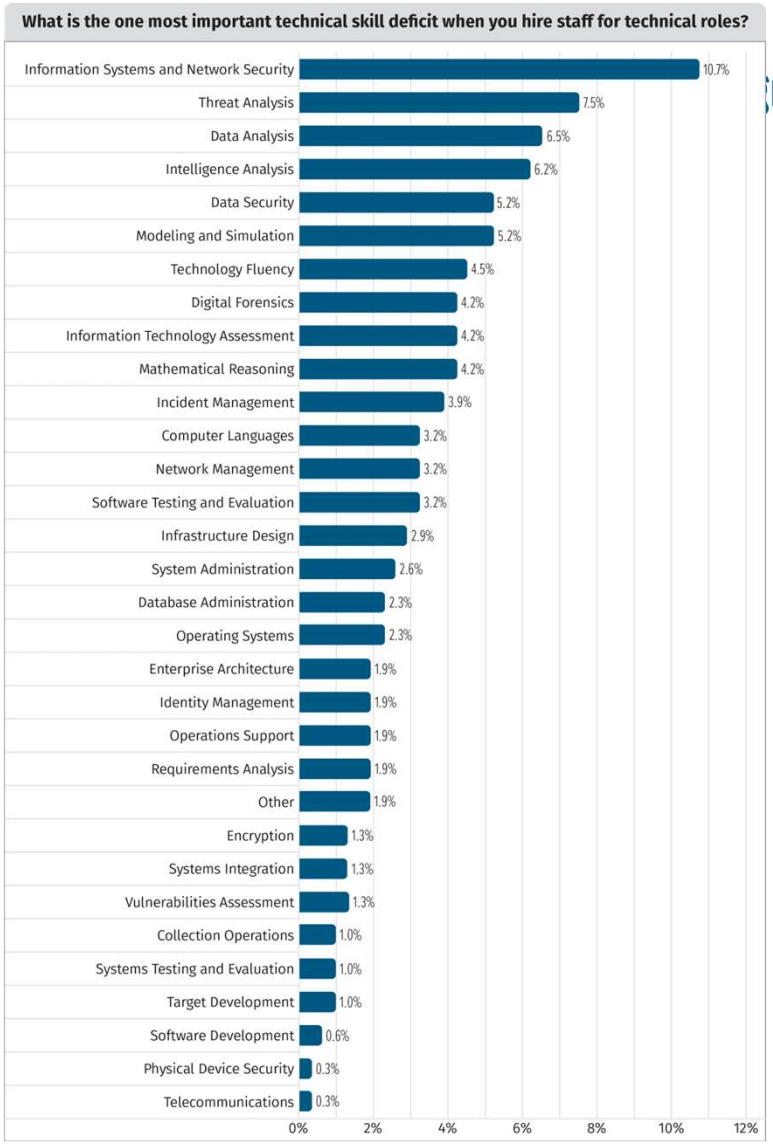
Analyst Program

- Most common size: **11-25** (Q3.58, n=335)
- Blue is total size. Red is SOC systems management staff.



Staff: Hiring - Skills

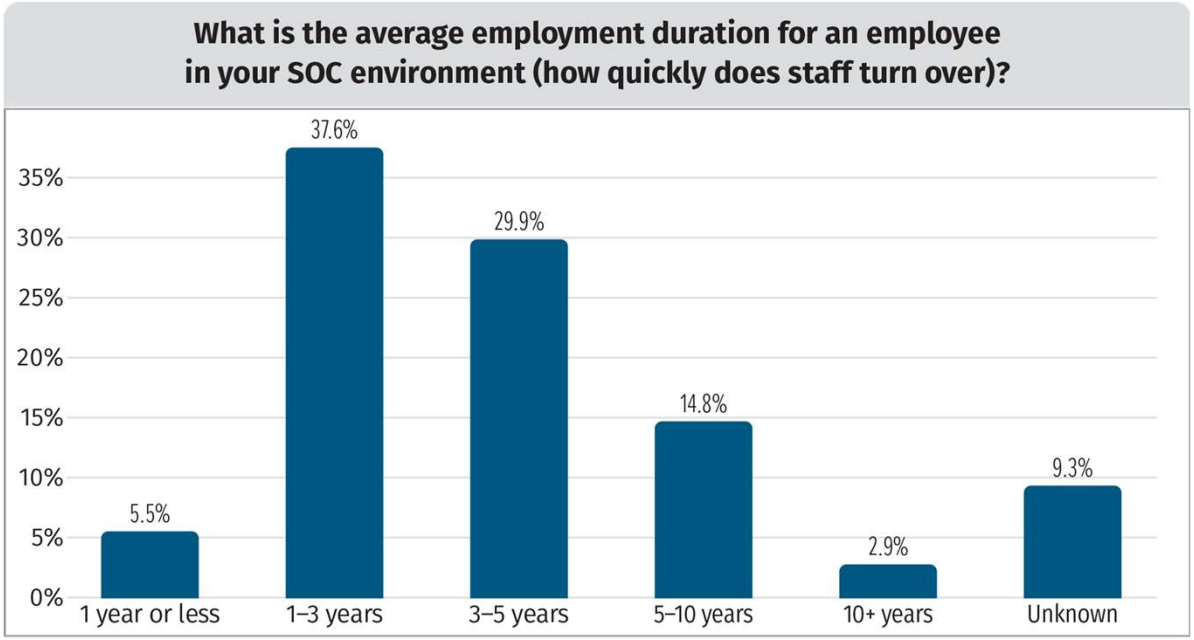
- Skill deficits hiring to address
  - **InfoSec ☺**
  - **Threat analysis**
  - **Data analysis**
  - **Intelligence analysis**
- Q3.64, n=308



Staff: Employment Duration

Analyst Program

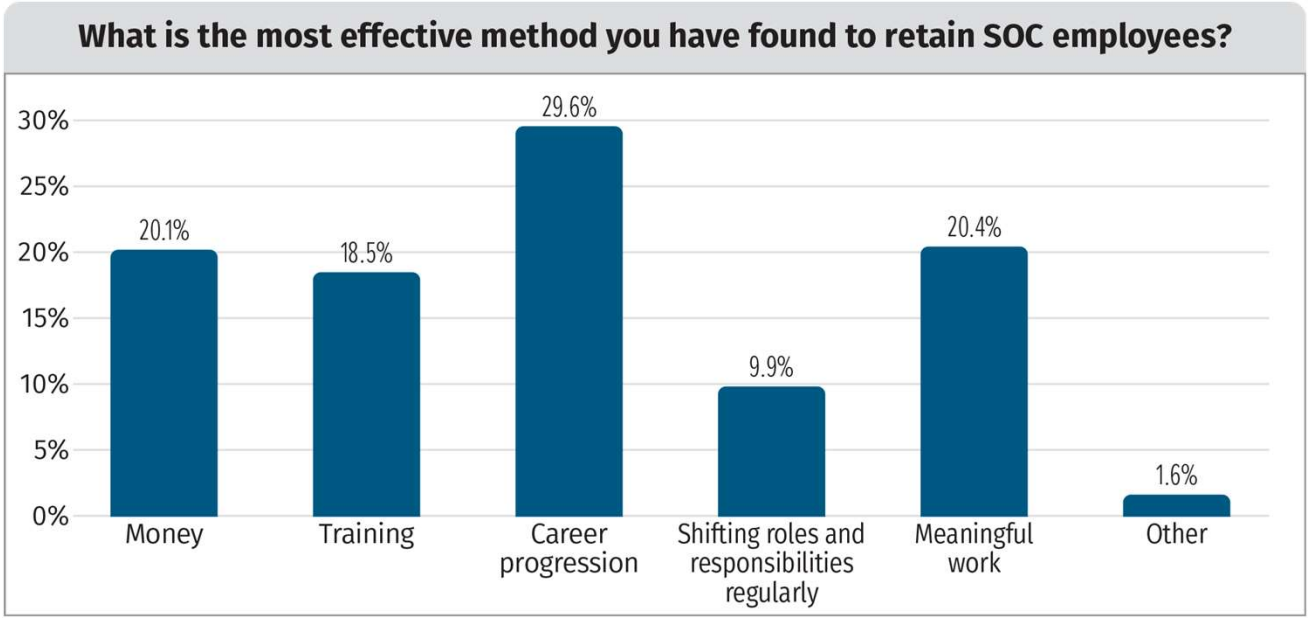
- Aligned w/ industry average 1-3 years (Q3.60, n=311)



Staff: Retention

Analyst Program

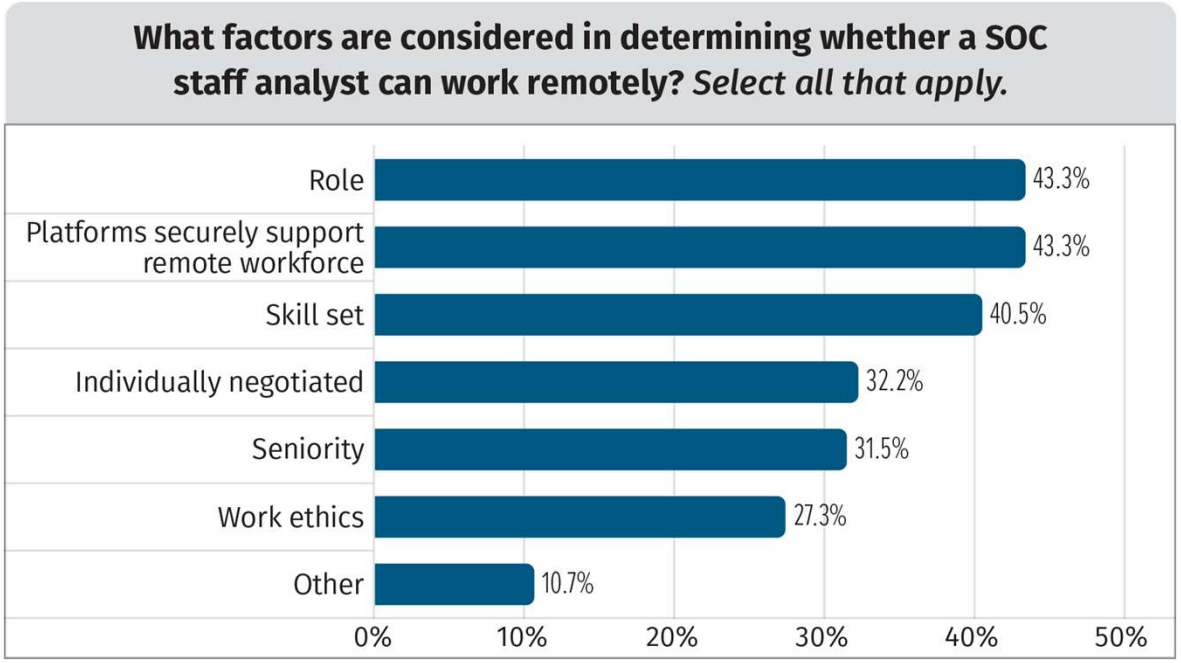
- **Career progression** substantially exceeds **meaningful work or money** for staff retention (Q3.66, n=314)



Staff: Remote Work

Analyst Program

- Remote work continues to be available
- Platforms appropriate, staff role, and skillset matter most (Q3.25, n=289)

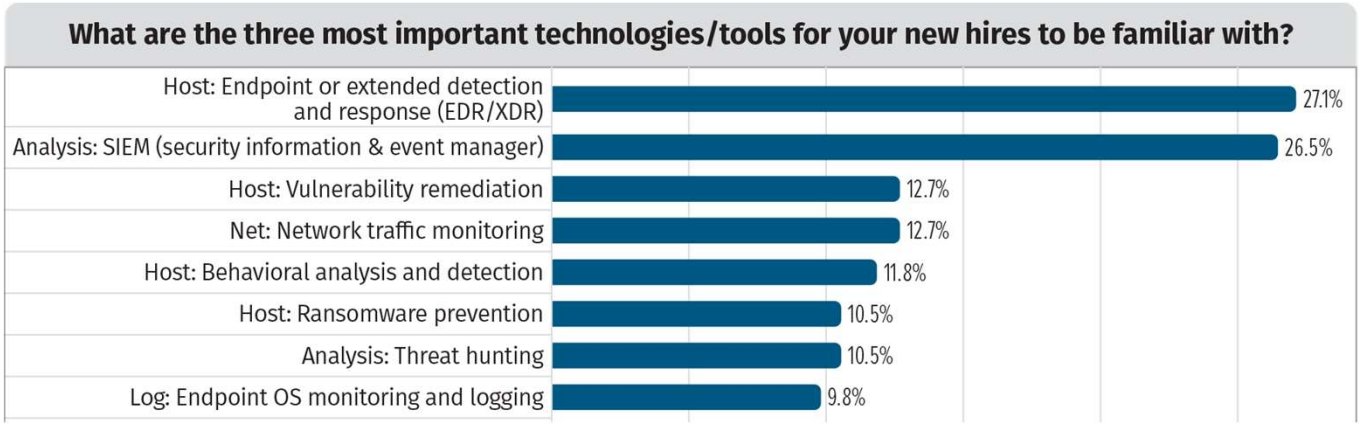


Staff + Technology

Analyst Program

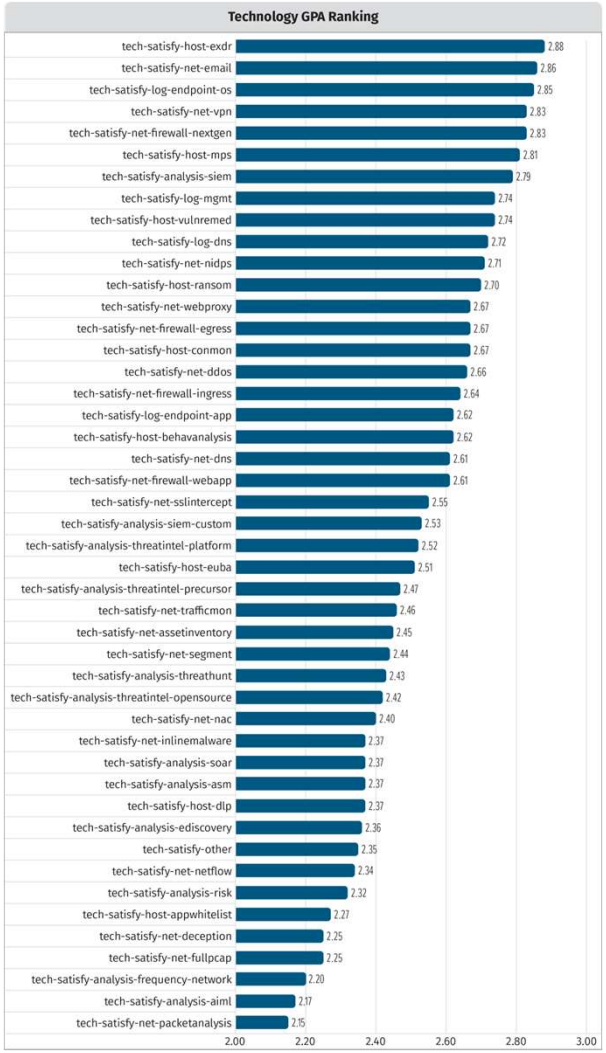
- Most important technology for new hires
  - **EDR**
  - **SIEM**
  - Network monitoring
  - Vuln mgmt.

Q3.65, n=306



Technology

- Discussion on next few slides



Analyst Program

Technology: Who Got As?

Analyst Program

- Answer? **Nobody got an A**. (Q3.39, n=194)
- Highest overall GPA was **2.89 : EXDR**
- Top 5 technologies:
  - **EXDR (2.89)**
  - Email filter (2.87)
  - Endpoint OS logging (2.86)
  - Nextgen firewall (2.85)
  - VPN (2.85)

Technology: Bottom Rankings

Analyst Program

- Bottom five (Q3.39, n=194)
  - Full PCAP (2.28)
  - Deception (2.26)
  - Network frequency analysis (2.21)
  - Network packet analysis (2.18)
  - **Artificial Intelligence / Machine Learning (2.18)**

Technology: Deployment State

- Technology with **higher satisfaction tends to accomplish production deployment**

	Production Sum	Production	Production	Implemen	Purchased	Planned	Total
Host: Vulnerability remediation	122	76	46	30	5	12	169
Net: Network intrusion detection system (IDS)/intrusion	119	72	47	30	10	8	167
Net: Next-generation firewall (NGF)	119	76	43	25	8	14	166
Host: Malware protection system (MPS)	118	70	48	34	3	9	164
Net: VPN (access protection and control)	118	85	33	36	10	4	168
Net: Email security (SWG and SEG)	117	80	37	29	12	11	169
Analysis: SIEM (security information and event manage	114	68	46	36	10	8	168
Host: Endpoint or extended detection and response (ED	113	65	48	33	12	11	169
Log: Endpoint OS monitoring and logging	109	65	44	47	9	3	168
Log: Log management	107	58	49	40	8	11	166
Net: Ingress filtering	106	65	41	33	10	13	162
Host: Ransomware prevention	105	64	41	48	6	11	170
Net :Network segmentation	105	53	52	40	12	13	170
Net: Web application firewall (WAF)	105	60	45	39	8	15	167
Net: Web proxy	105	71	34	30	12	16	163
Net: DNS security/DNS firewall	104	65	39	35	10	16	165
Net: Network traffic monitoring	102	54	48	36	12	13	163
Log: DNS log monitoring	101	56	45	46	8	15	170
Net: DoS and DDoS protection	101	50	51	34	12	20	167
Analysis: Customized or tailored SIEM use-case monitor	100	55	45	34	12	16	162
Log: Endpoint application log monitoring	100	48	52	39	11	19	169
Host: Continuous monitoring and assessment	99	61	38	40	13	11	163
Net: Asset discovery and inventory	99	48	51	42	12	14	167
Net: Egress filtering	97	57	40	38	11	21	167
Net: SSL/TLS traffic inspection	97	51	46	35	14	19	165
Analysis: Threat intelligence (open source, vendor provi	95	50	45	34	12	20	161
Net: NetFlow analysis	95	36	59	32	11	25	163
Host: User behavior and entity monitoring	91	45	46	37	16	23	167
Net: Network Access Control (NAC)	91	47	44	36	15	21	163
Analysis: Attack surface management	90	41	49	44	7	22	163
Host: Behavioral analysis and detection	90	50	40	45	12	20	167
Host: Data loss prevention	89	43	46	39	14	23	165
Analysis: Threat hunting	87	45	42	44	10	24	165
Analysis: Threat intelligence platform (TIP)	87	52	35	37	18	23	165
Analysis: E-discovery (support legal requests for specifi	84	48	36	34	12	32	162
Net: Malware detonation device (inline malware destru	84	48	36	34	13	31	162
Analysis: External threat intelligence (for online precurs	83	41	42	39	11	28	161
Host: Application whitelisting	80	41	39	45	15	25	165
Net: Full packet capture	80	38	42	30	16	38	164
Net: Packet analysis (other than full PCAP)	77	32	45	35	13	36	161
Analysis: digital asset risk analysis and assessment	76	37	39	41	15	27	159
Analysis: SOAR (Security Orchestration, Automation, Re	75	37	38	41	16	31	163
Analysis: AI or machine learning	70	31	39	44	14	33	161
Analysis: Frequency analysis for network connections	70	34	36	37	12	43	162
Net: Deception technologies such as honey potting	64	33	31	42	20	39	165
Other (Please specify)	29	15	14	23	8	14	74

	A	B	C	D	F	GPA	Total
Host: Vulnerability remediation	38	61	41	11	6	2.7	157
Net: Network intrusion detection system (IDS)/intrusion prevention system (I	40	54	42	15	4	2.7	155
Net: Next-generation firewall (NGF)	50	54	34	9	7	2.9	154
Host: Malware protection system (MPS)	44	56	40	10	5	2.8	155
Net: VPN (access protection and control)	53	51	34	14	5	2.8	157
Net: Email security (SWG and SEG)	54	49	36	10	6	2.9	155
Analysis: SIEM (security information and event manager)	47	49	41	15	3	2.8	155
Host: Endpoint or extended detection and response (EDR/XDR)	57	50	31	16	4	2.9	158
Log: Endpoint OS monitoring and logging	45	62	37	12	2	2.9	158
Log: Log management	43	58	36	13	6	2.8	156
Net: Ingress filtering	36	54	34	11	11	2.6	146
Host: Ransomware prevention	45	47	47	14	5	2.7	158
Net :Network segmentation	39	44	41	20	16	2.4	160
Net: Web application firewall (WAF)	38	57	34	16	11	2.6	156
Net: Web proxy	40	54	33	19	5	2.7	151
Net: DNS security/DNS firewall	34	57	39	12	9	2.6	151
Net: Network traffic monitoring	33	45	38	23	9	2.5	148
Log: DNS log monitoring	48	50	36	14	8	2.7	156
Net: DoS and DDoS protection	45	51	32	21	7	2.7	156
Analysis: Customized or tailored SIEM use-case monitoring	39	40	46	16	10	2.5	151
Log: Endpoint application log monitoring	44	51	33	19	11	2.6	158
Host: Continuous monitoring and assessment	41	52	33	18	6	2.7	150
Net: Asset discovery and inventory	35	43	46	13	14	2.5	151
Net: Egress filtering	35	59	37	13	6	2.7	150
Net: SSL/TLS traffic inspection	37	52	36	13	14	2.6	152
Analysis: Threat intelligence (open source, vendor provided)	29	43	46	19	10	2.4	147
Net: NetFlow analysis	29	43	38	22	14	2.3	146
Host: User behavior and entity monitoring	34	52	43	9	16	2.5	154
Net: Network Access Control (NAC)	31	41	50	13	14	2.4	149
Analysis: Attack surface management	27	48	42	16	14	2.4	147
Host: Behavioral analysis and detection	44	47	40	10	14	2.6	155
Host: Data loss prevention	27	45	53	11	17	2.4	153
Analysis: Threat hunting	32	48	41	16	14	2.5	151
Analysis: Threat intelligence platform (TIP)	34	47	38	17	10	2.5	146
Analysis: E-discovery (support legal requests for specific information collectio	32	41	39	20	15	2.4	147
Net: Malware detonation device (inline malware destruction)	32	45	40	11	20	2.4	148
Analysis: External threat intelligence (for online precursors)	29	47	39	23	6	2.5	144
Host: Application whitelisting	23	49	50	14	18	2.3	154
Net: Full packet capture	34	39	36	21	22	2.3	152
Net: Packet analysis (other than full PCAP)	23	47	36	16	25	2.2	147
Analysis: digital asset risk analysis and assessment	26	44	40	18	16	2.3	144
Analysis: SOAR (Security Orchestration, Automation, Response)	34	35	47	13	17	2.4	146
Analysis: AI or machine learning	25	38	43	23	19	2.2	148
Analysis: Frequency analysis for network connections	28	37	38	21	21	2.2	145
Net: Deception technologies such as honey potting	25	44	45	13	21	2.3	148
Other (Please specify)	15	13	14	5	10	2.3	57

Technology: Deployment State

- Sorted by highest count of production deployment
- GPAs at the top of the scale

		GPA
Host: Vulnerability remediation	122	2.7
Net: Network intrusion detection system (IDS)/intrusior	119	2.7
Net: Next-generation firewall (NGF)	119	2.9
Host: Malware protection system (MPS)	118	2.8
Net: VPN (access protection and control)	118	2.8

Jupyter Notebook Installation Information (Not Required)

Montance® LLC

Python

- Python 3 Install
- Download and install: https://www.python.org/downloads/
- I'll use this to manipulate the data
- Many applications and uses for python
- If you don't know how to script already, python or powershell are (in my opinion) the most generally applicable languages now

Pandas

- Install pandas
- https://numfocus.org/ - organization supporting a multitude of opensource projects

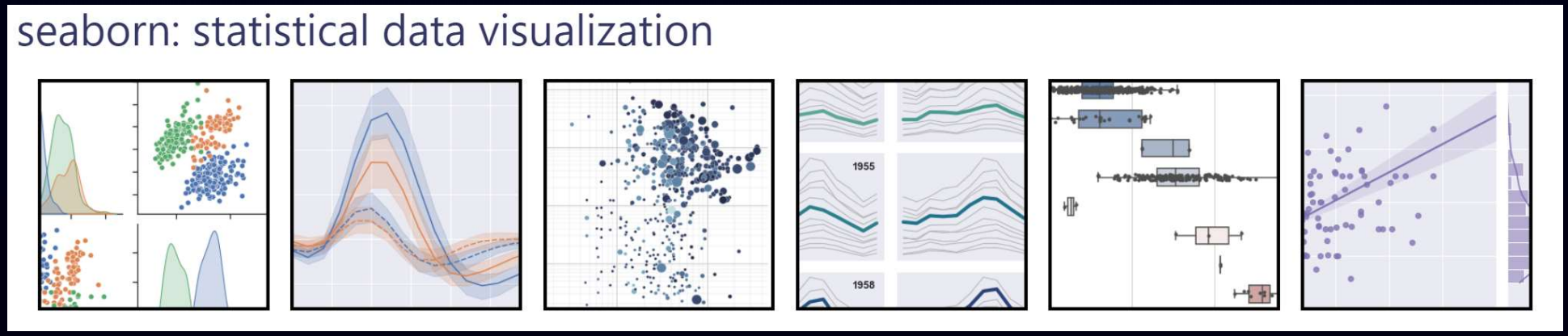
- pip install pandas
  - Pandas provides data frame support (spreadsheet in memory)
  - For reference: https://pandas.pydata.org/docs/getting_started/install.html

Seaborn

- Seaborn Install

- pip install matplotlib # if you don't have it already
- pip install seaborn

- https://seaborn.pydata.org/installing.html



Jupyterlab

- Install Jupyterlab from : https://jupyter.org/install
  or easier to use pip

- pip install jupyterlab

- jupyter notebook (or jupyter lab)

Others

- pip install openpyxl
  # excel support
- pip install wordcloud
  # make cool pictures from words

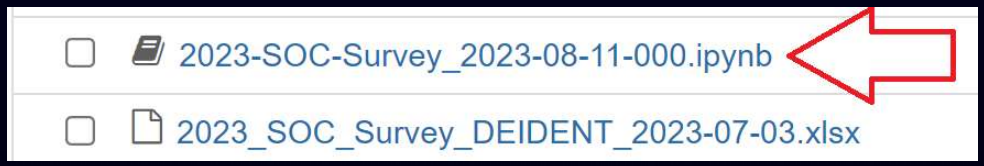
Montance® LLC

Start

1. jupyter notebook

```
n\jupyter_working_dir> jupyter notebook
```

2. Launch notebook from webpage



3. Write python

```
In [ ]: import matplotlib
        import matplotlib.pyplot as plt
        from matplotlib import font_manager
        import seaborn as sns
        import os

        %matplotlib inline
        import pandas as pd
        df = pd.read_excel('.\\2023_SOC_Survey_DEIDENT_2023-07-03.xlsx', engine='openpyxl')
        df_orig = df.copy()   ### need to .copy here to address key errors later?
        df = df_orig.copy().iloc[2:,:]  ### need to .copy here to address key errors later?
        df.shape
```

Typo time!
Watch me fumble
through a Jupyter Notebook

Thank you!
@CCrowMontance
mgt517.com/linkedin
https://montance.com/pres

Christopher Crowley