Christopher Crowley - CCrowMontance

2019 SOC Survey Results Preview

Christopher Crowley

SANS Senior Instructor

- Background: Had root on most systems in employer at 15 years old (Not much #CYBER in the 80s)
- Sectors: Defense, Education, Energy, Government, Financial, Software Development, Telecom
- Regions: US, Europe, Middle East, Asia, Australia
- Currently: Consultant, author of (SANS deprecated) MGT517: Security Operations. Teaches: SecOps (soc-class.com), SANS: SEC511, SEC575, SEC504, …
- SOC build timeline project: https://www.montance.com/soc/timeline

Twitter: CCrowMontance

Introduction

SOC Survey Preview

- This talk is an excerpt of material from the 2019 SANS SOC Survey to be released in July
- Webcasts with additional details
  - July 10 : Results
  - July 11 : Discussion Forum
- See SANS website: www.SANS.org/webcasts

A Quick Aside About New Orleans

- Lived here ‘91 – ’05 (yes, left due to Katrina)
- Great city, stay safe, and remember *it’s not the heat, it’s the stupidity…*
- Some New Orleans recommendations (warning, I’m a snob)

  https://mgt517.com/nola

Excerpt From That Post

- Since we're in the CBD, my favorite nearby places Cochon (but I really like Butcher, it's less formal), Peche, Compere Lapin, August, Willa Jean, Juan's Flying Burrito (CBD location), Carmo, Luke on St. Charles, (great happy hour)...
- Nearby for coffee: Revelator Coffee
- Nearby for wine: Keife & Co, W.I.N.O
- Nearby bar for hangout: Lucy's Retired Surfer, Vic's Kangaroo

Survey Objectives

Survey Objectives

Our Intentions

- SANS intends to provide a community reference for helping to make decisions
- Collection of survey data and advice
- Historical review for trends over time
- Vendor sponsored, so attempt to stay impartial and objective

Challenges

Survey Challenges

Low Numbers – 517 Respondents

Answer Choices	Responses	
Yes	100.0%	517
No	0.0%	0

- 517 Respondents, but **no defined population**
- Based on a speculated population of SOCs worldwide, **around 300,000**
  - Dun and Bradstreet: 285 Million Companies
  - 1 in 1,000 has a SOC means about 300,000 SOCs
  - No better **global** population estimate that I'm aware of
  - Ernst & Young surveyed 1,200 (2017) said 50% don't have a SOC
  - See 2018 SOC Survey : https://mgt517.com/2018-survey

517 Respondents Upside

- I'm not *always* negative
- 517 Respondents – definitely the right people, with a good mix of technical and executives
- We also included in depth interviews to augment the data in the question portion

Technology – Use and Satisfaction

- We have a list of 49 technologies
- To try to organize this, we split the tech across the NIST Cyber Security Framework (CSF): Identify, Protect, Detect, Respond, Recover
- This was useful, but also confusing for respondents
- I have another talk in the Summit about technology taxonomy, stay tuned for that

Are You a Service Provider? Yes, Yes, or No?

- Managed service providers respond to the survey, which is great. But they are different in many ways that internal SOCs. This skews some numbers
- We ask the question if you're a service provider. If so, are you a company that only/primarily offers Security Services, or if you're a SOC that considers itself a service provider to internal constituents, and those constituents have a choice on who to buy the service from

Many Items Not Included Here

- I'm presenting data elements necessary for context, and some interesting things that didn't make it into the report
- The full "details" will be reserved for the findings webcast on July 10th
- Sign up at https://sans.org/webcasts

Questions are Mainly Frozen

- We have most of the questions that we will continue to ask
- This is going to allow us to see year over year trends
- I'm incredibly excited about this!
- Tell your co-workers, tell your friends to participate

The Unknown

- So, it is great that the questions are largely frozen
- The downside is: what if the Survey is asking the wrong questions?
- How would we know this?
  - Community feedback: vendor and participant
  - Competitors develop and publish new approach

Data Driven Review

Quick Demographics

No Surprises

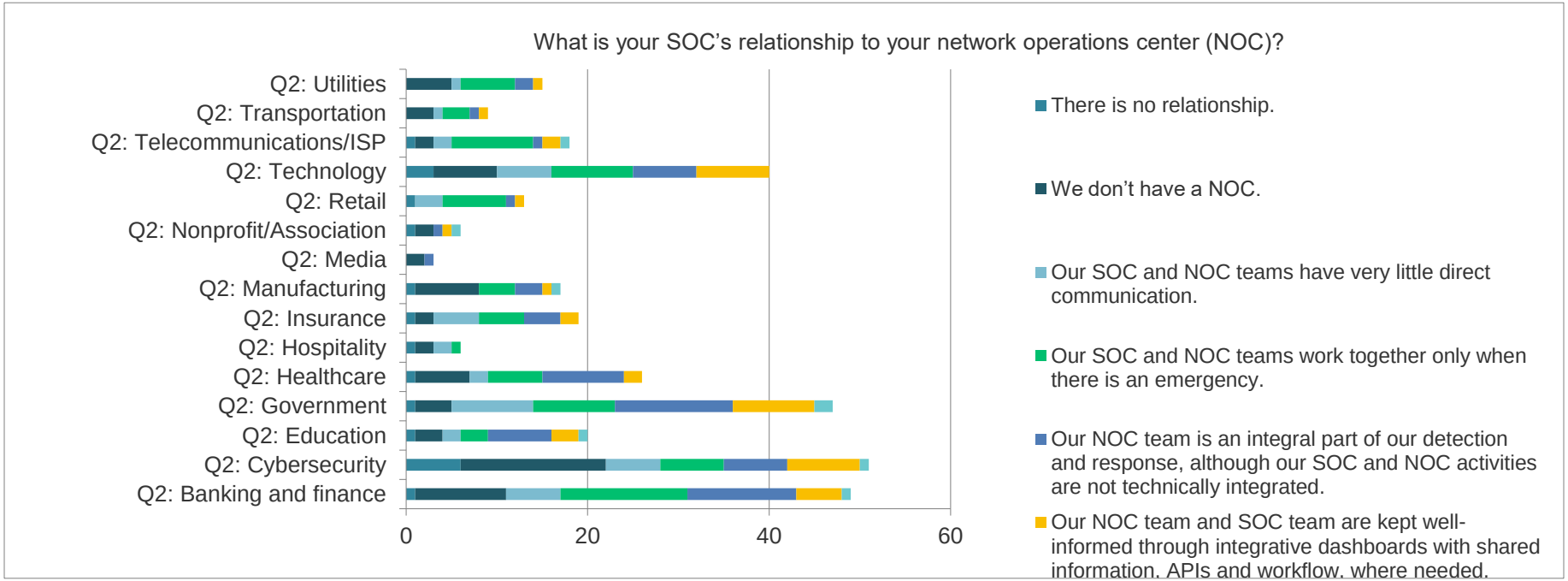
- HQ Locations: North America & Europe
  - Operate globally
- Sectors: Cyber, Government, Banking, Tech
- Size: no single characteristic
- Roles: technical staff, technical managers, or SOC managers

Sector (Q2) Driven Analysis

Larger

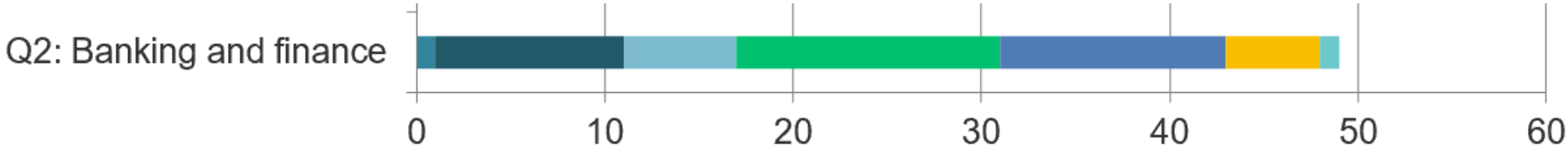
Question 10: SOC relationship to NOC

I know it is too small



Q2 v Q10: One drill down

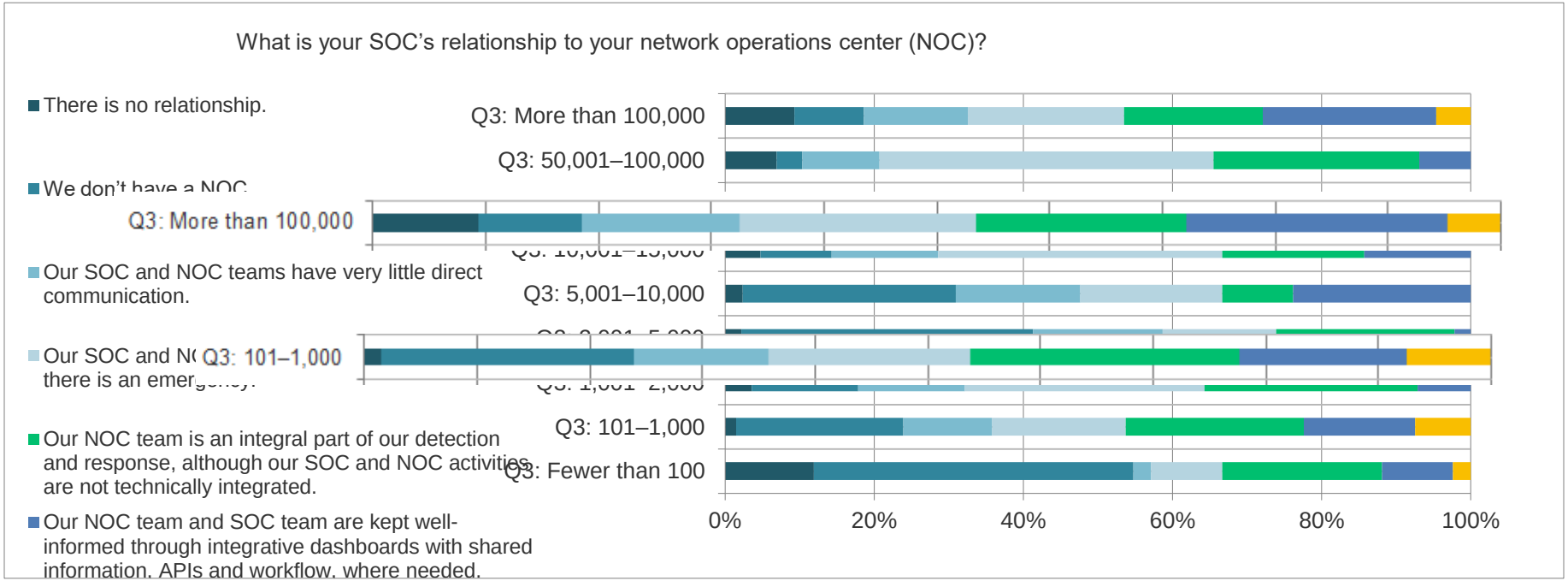
Banking and Finance



- No relationship: 1 (Final blue one: Other: 1)
- No NOC: 10
- Little direct communication: 6
- Work together only in emergency: 14
- NOC integral to response, not integrated teams: 12
- Integrated through dashboards, API, workflow, etc: 5

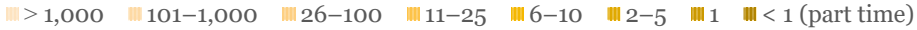
Q3 (Size) v Q10 (SOC-NOC)

Bigger and Smaller Tend to Be Better



Q3 (Size) v Q11 (Analysts/Maintainers)

Number of Maintainers (1 of 2)



	Fewer than 100	101–1,000	1,001–2,000	2,001–5,000	5,001–10,000	10,001–15,000	15,001–50,000	50,001–100,000	More than 100,000
> 1,000							1		2
101–1,000			1				1		4
26–100	1	2	1		6		5	6	13
11–25	1	7	2	3	5	6	14	9	10
6–10	9	13	5	8	10	9	10	4	2
2–5	17	25	13	26	18	5	9	5	5
1	6	5	4	1	2		2		
< 1 (part time)	1	5	2	5			1		1

2–5	17	25	13	26	18	5	9	5	5
1	6	5	4	1	2		2		
< 1 (part time)	1	5	2	5			1		1

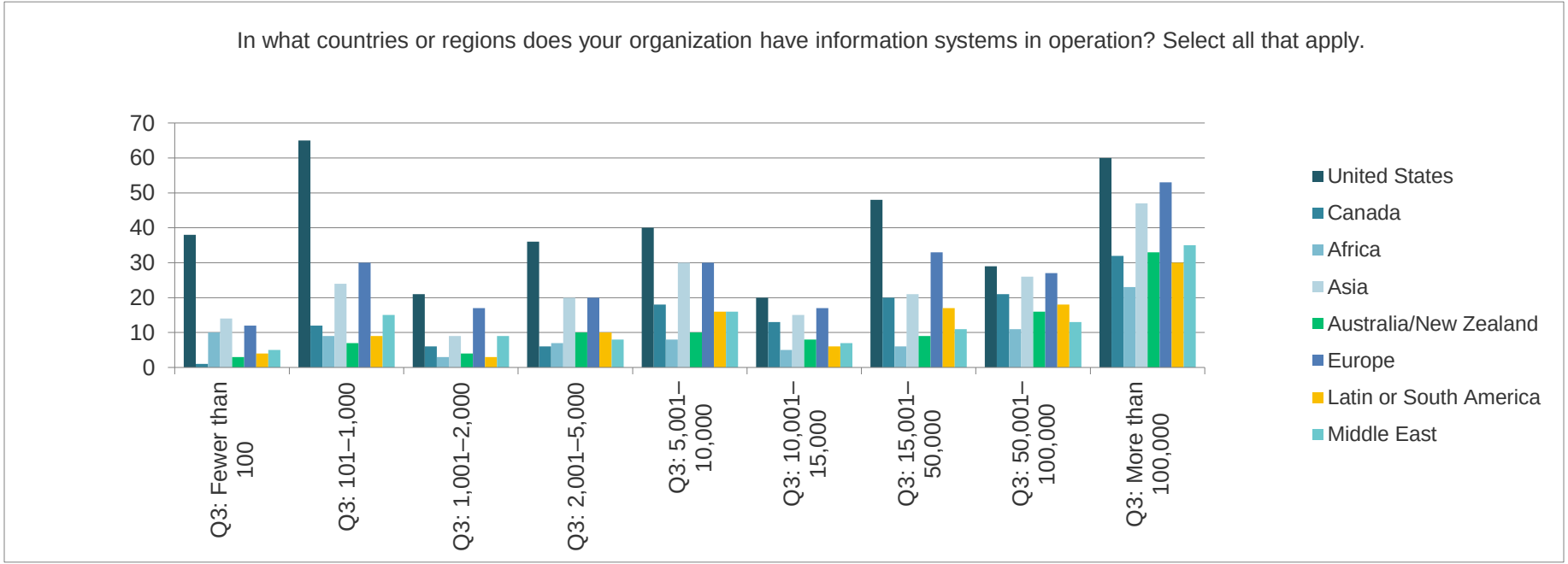
Q3 (Size) v Q11 (Analysts/Maintainers)

Number of Maintainers (2 of 2)

	FTEs Required to Maintain SOC Systems and Srvices (N=313)								
Organization Size	< 1 (part tir	1	2–5	6–10	11–25	26–100	101–1,000	> 1,000	Grand Tota
Fewer than 100	3	10	15	8	1				37
101–1,000	5	8	26	10	5				54
1,001–2,000	2	8	7	7	1	2			27
2,001–5,000	8	2	20	7	3	1			41
5,001–10,000	2	5	16	6	4	4	1		38
10,001–15,000	1	1	8	5	4				19
15,001–50,000	2	4	14	7	7	5		2	41
50,001–100,000			6	5	8	3			22
More than 100,000	1	1	7	6	5	7	4	3	34
Grand Total	24	39	119	61	38	22	5	5	313

Q3 (Size) v Q6 (Countries Operating)

Not Just Large Companies Operating Globally



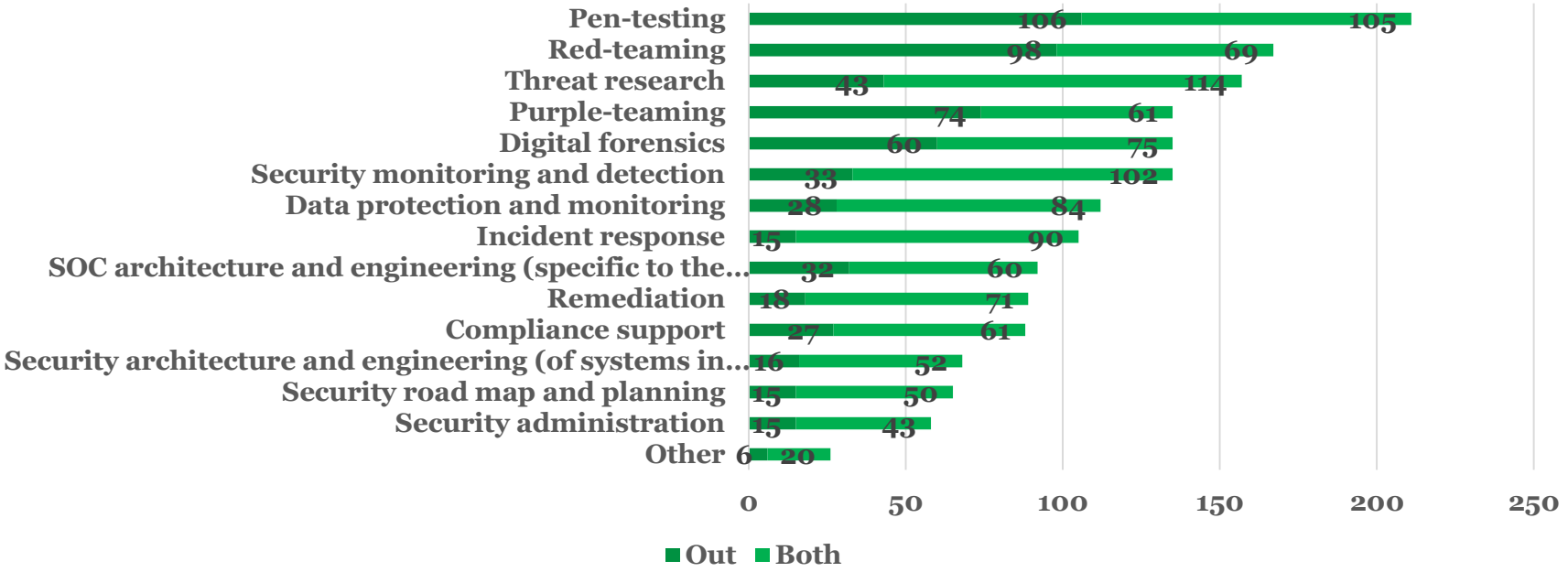
Q3 (Size) v Q12 (Activities-Outsource)

What Makes a SOC? What is Internal, Outsourced, and Both?

- The graphs which follow are the cross-referenced results from capability and outsourcing to size
- There wasn't a strong correlation in most cases with size
- But, I'm going to share this because it might be a little insightful for attendees to compare their org size to what is outsourced and what is done

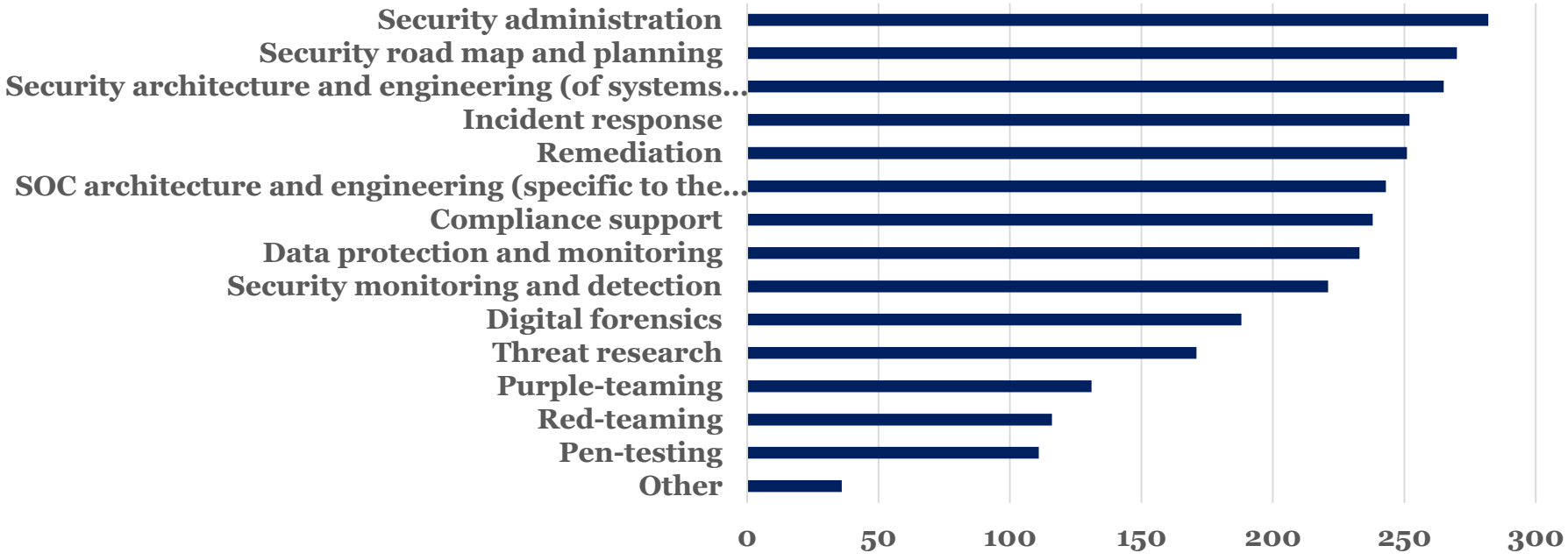
Q3 (Size) v Q12 (Activities-Outsource)

First, Q12 Overall – Outsourced and Both



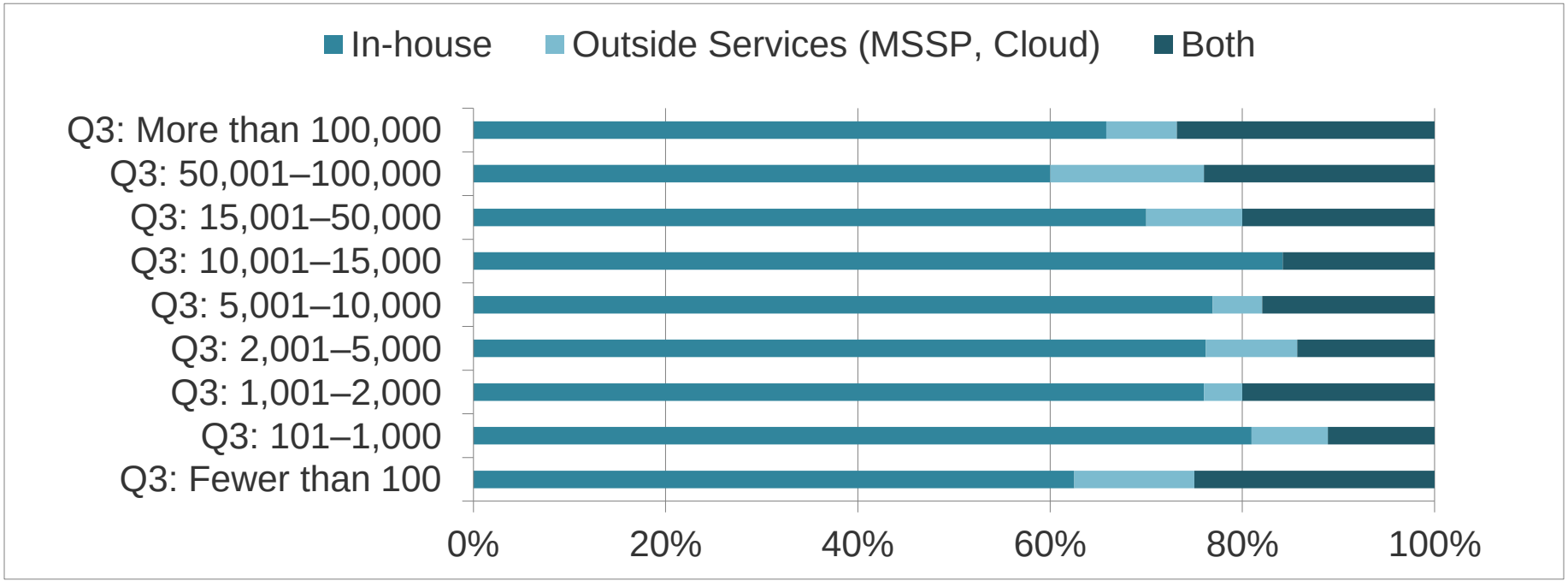
Q3 (Size) v Q12 (Activities-Outsource)

First, Q12 Overall – Internal Only



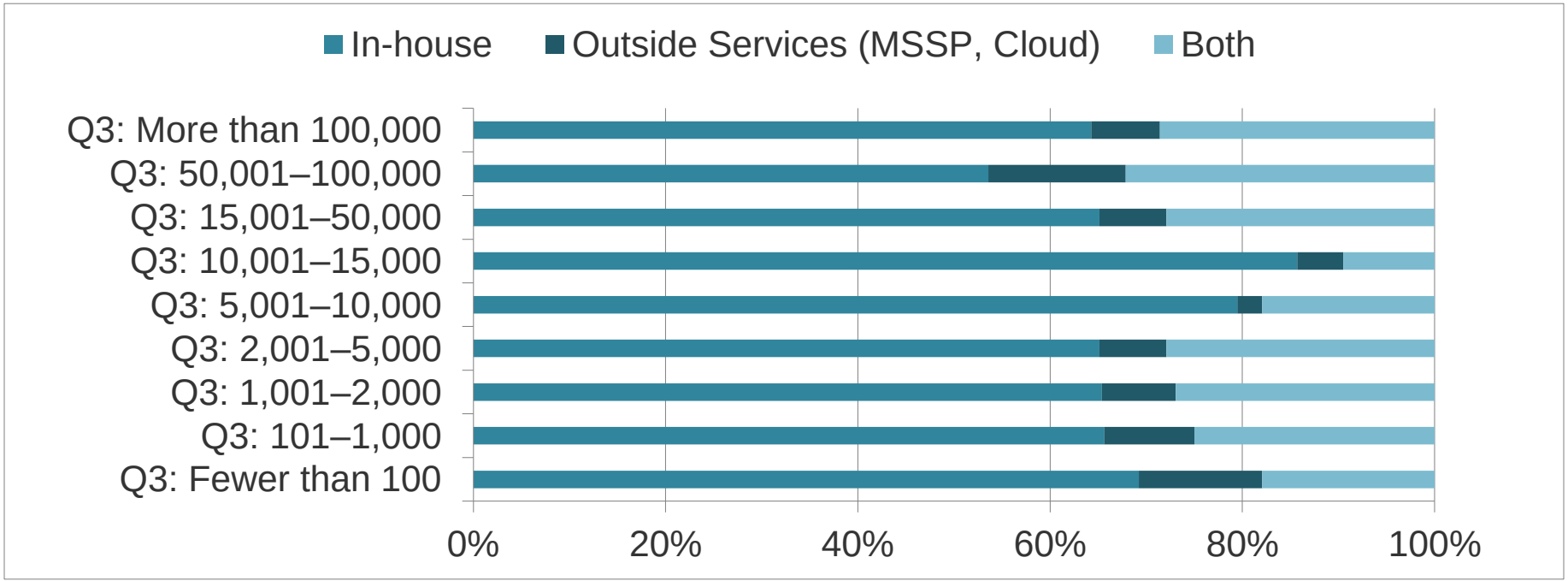
Q3 (Size) v Q12 (Activities-Outsource)

Compliance Support



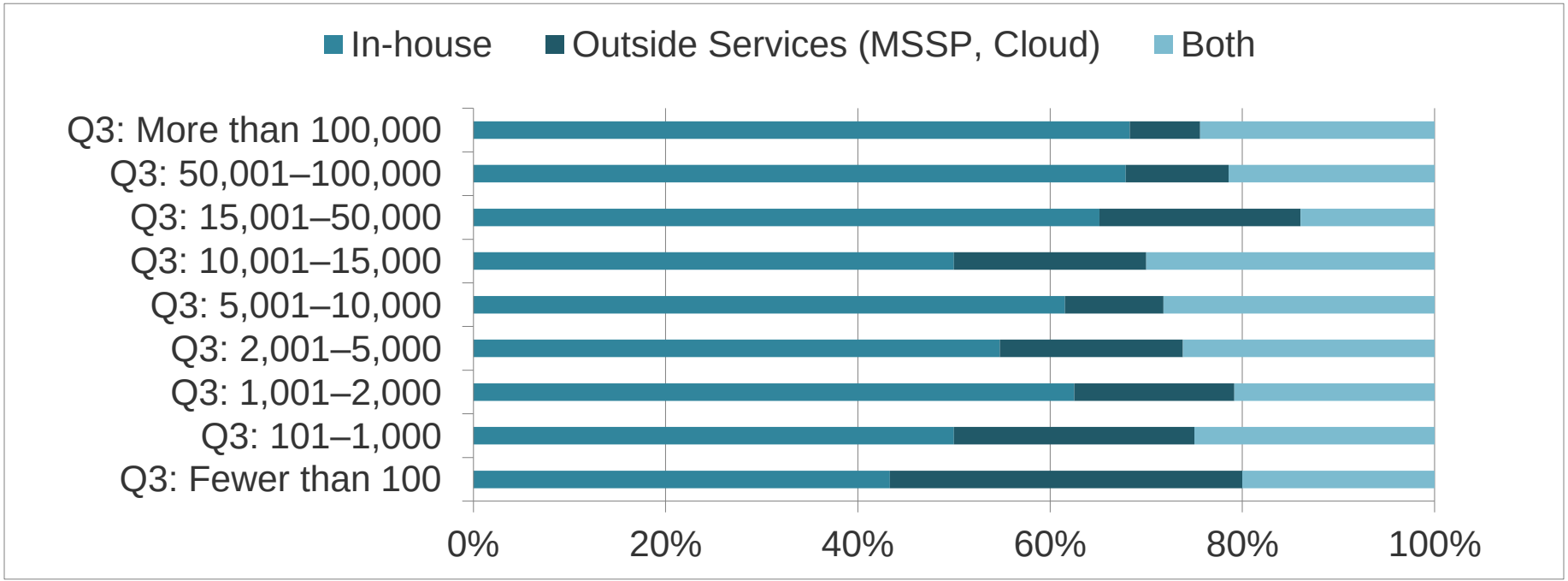
Q3 (Size) v Q12 (Activities-Outsource)

Data Protection and Monitoring



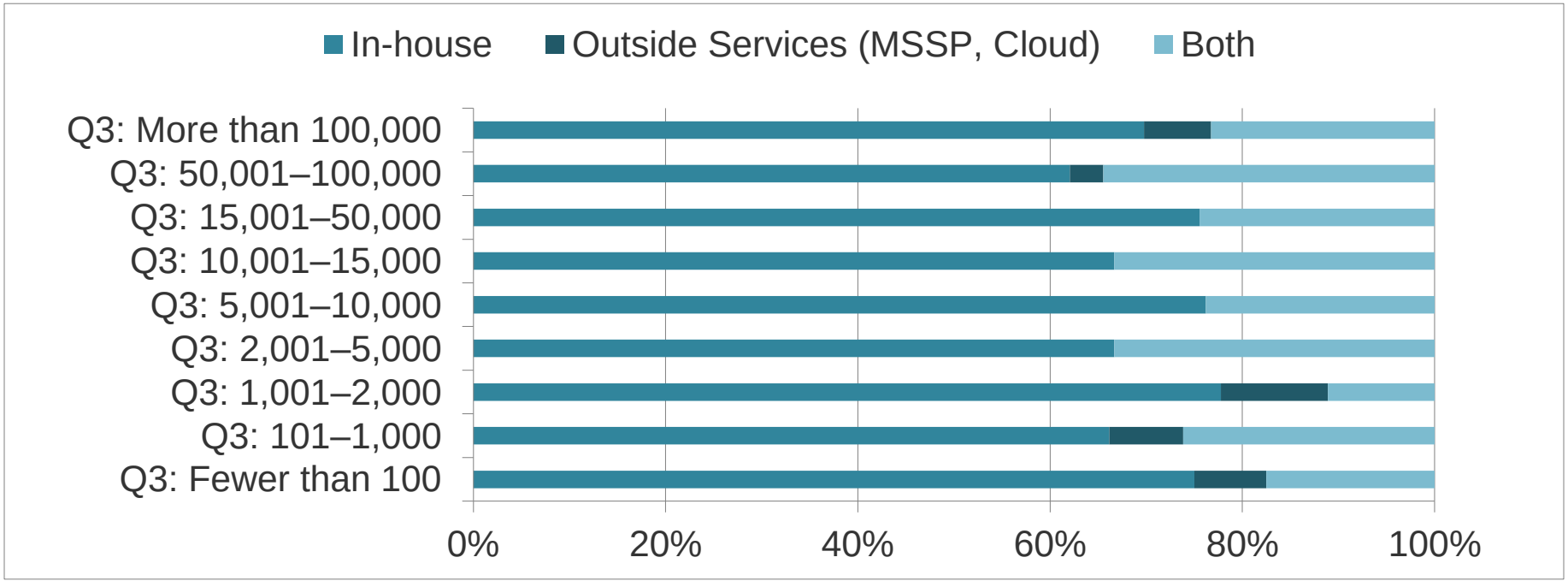
Q3 (Size) v Q12 (Activities-Outsource)

Digital Forensics



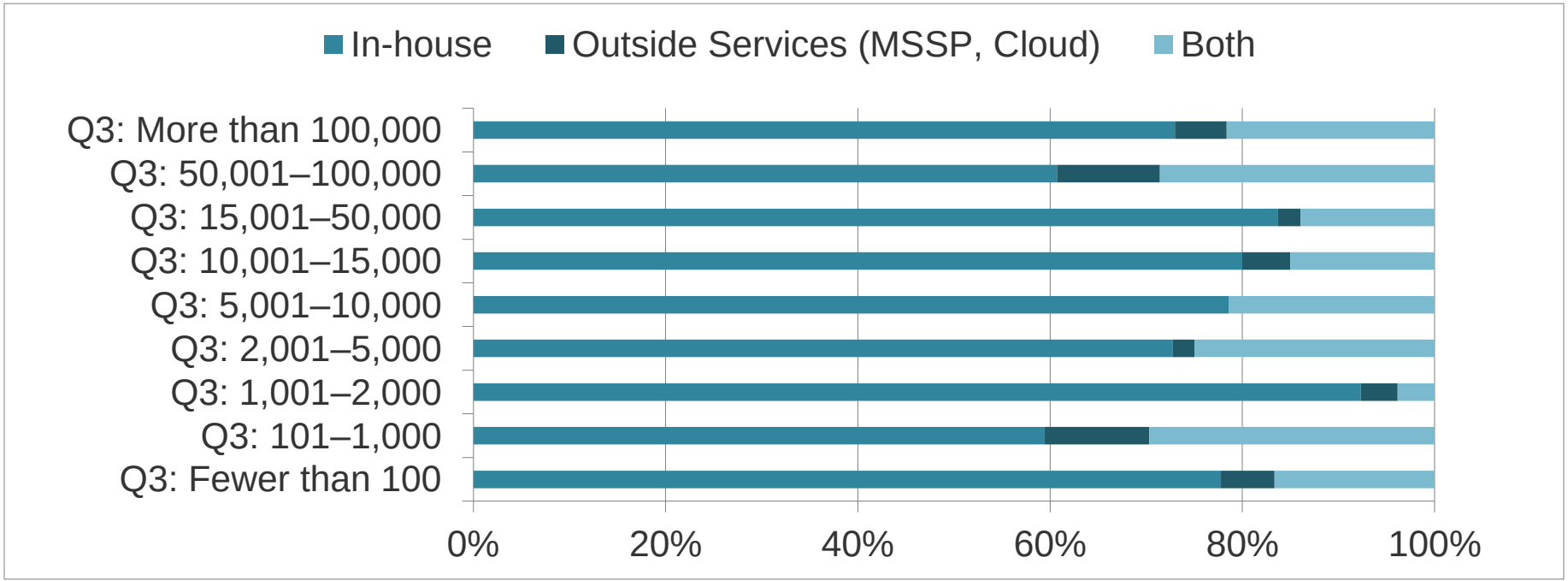
Q3 (Size) v Q12 (Activities-Outsource)

Incident Response



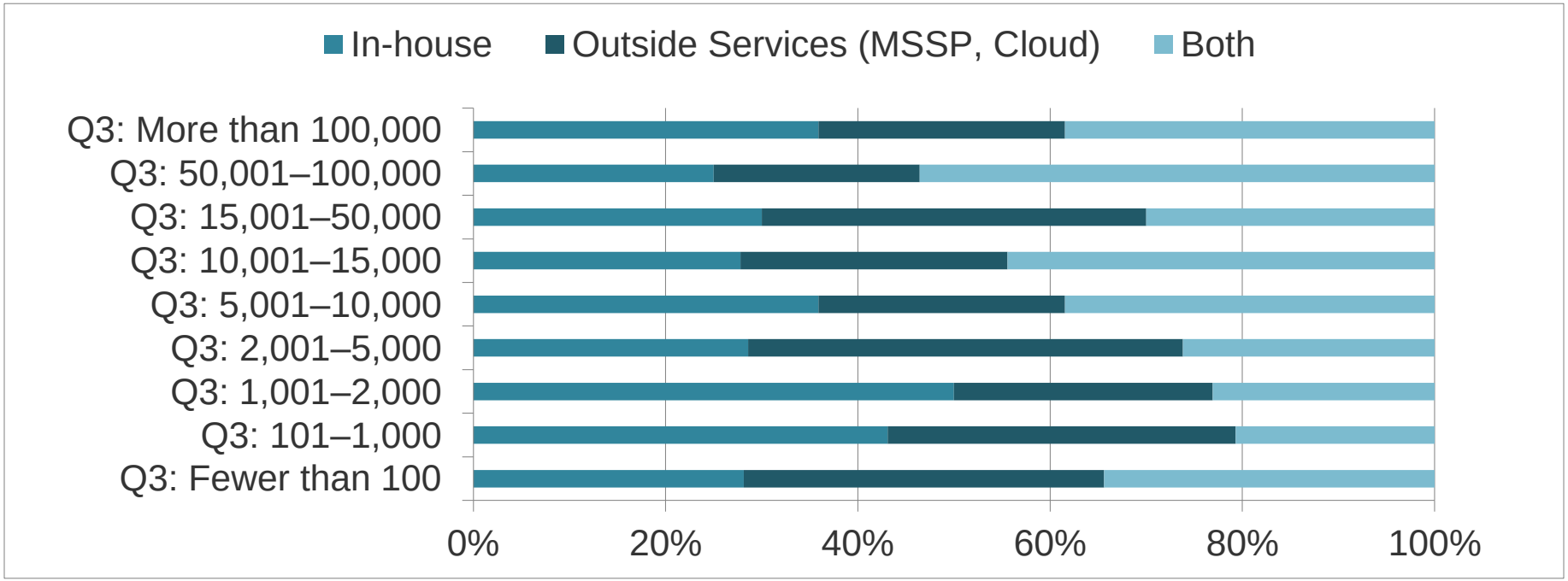
Q3 (Size) v Q12 (Activities-Outsource)

Remediation



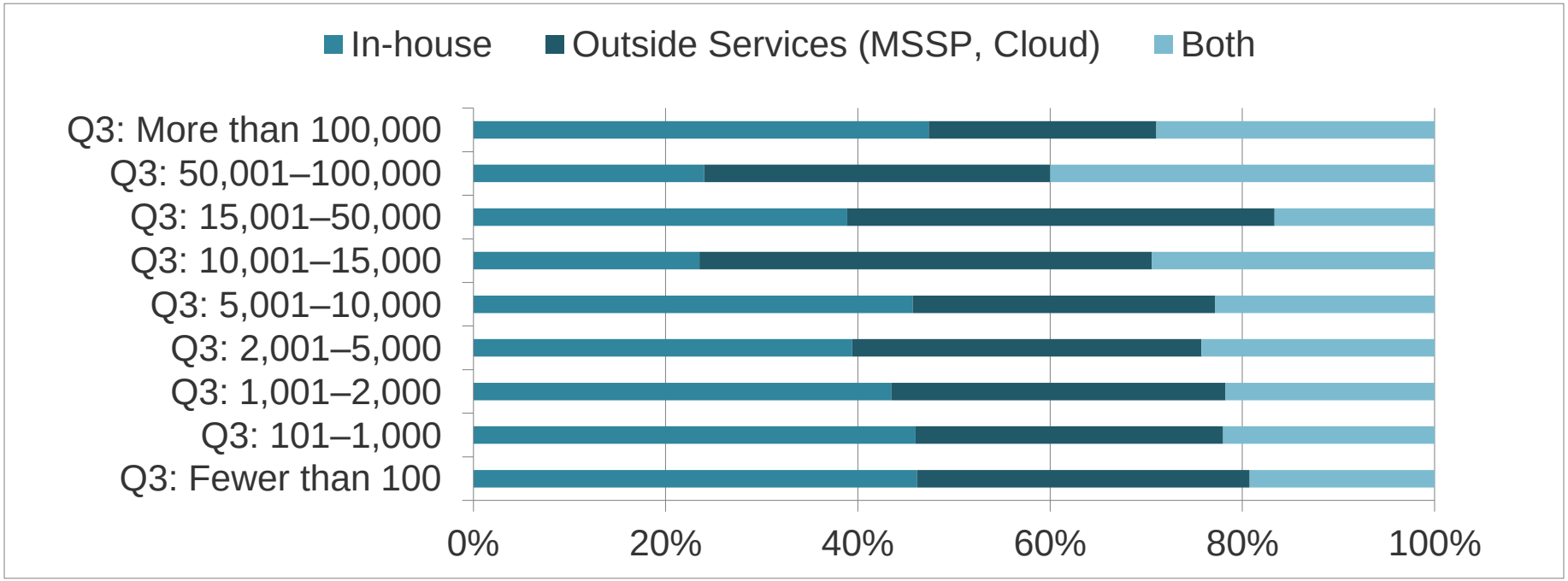
Q3 (Size) v Q12 (Activities-Outsource)

Pen Testing



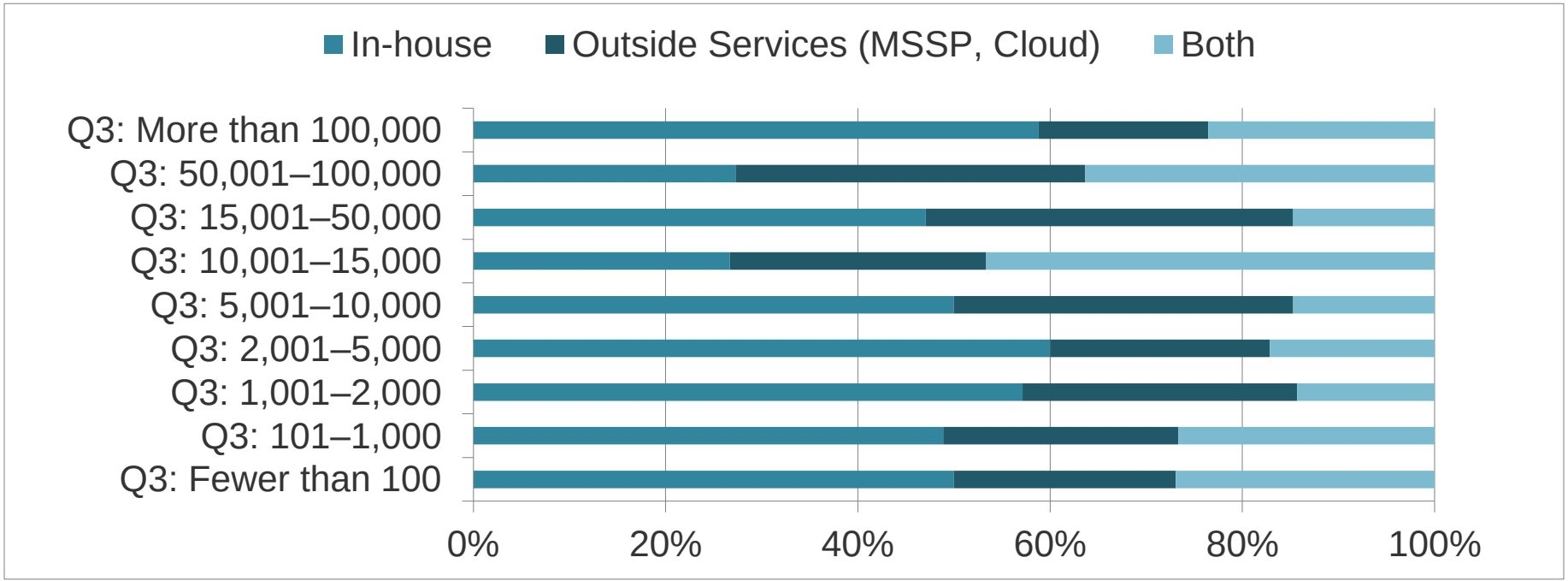
Q3 (Size) v Q12 (Activities-Outsource)

Red Teaming



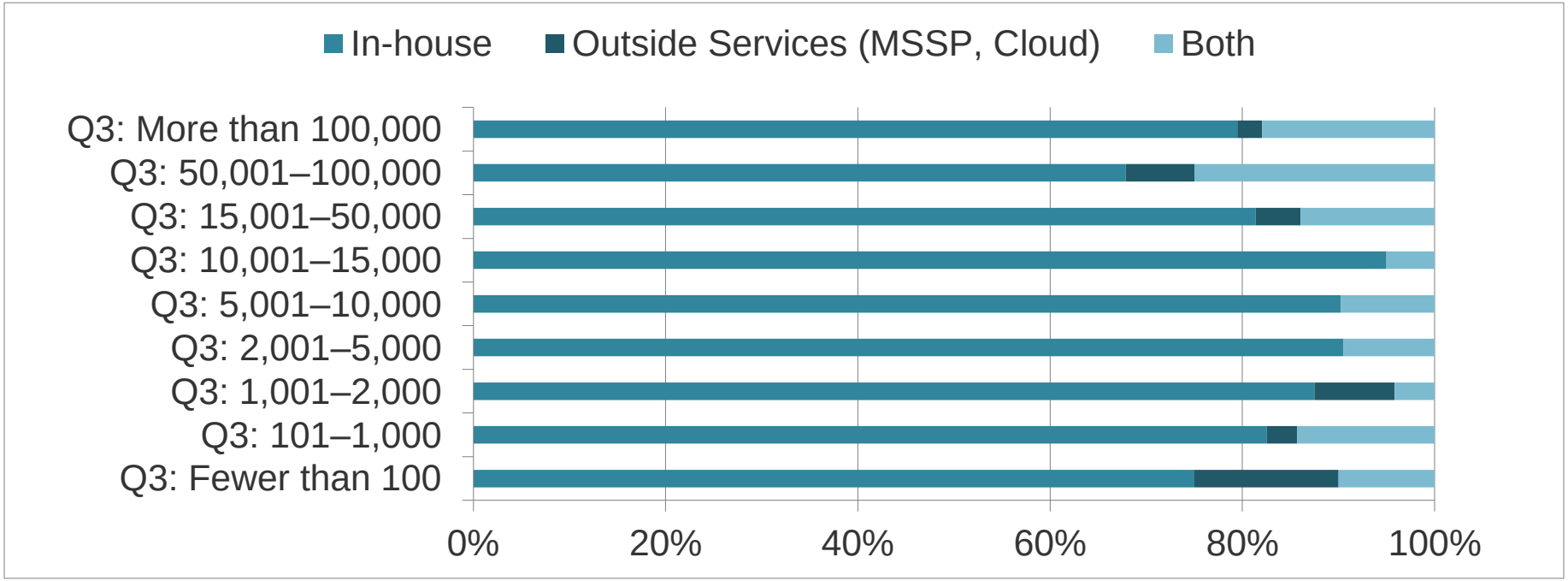
Q3 (Size) v Q12 (Activities-Outsource)

Purple Teaming



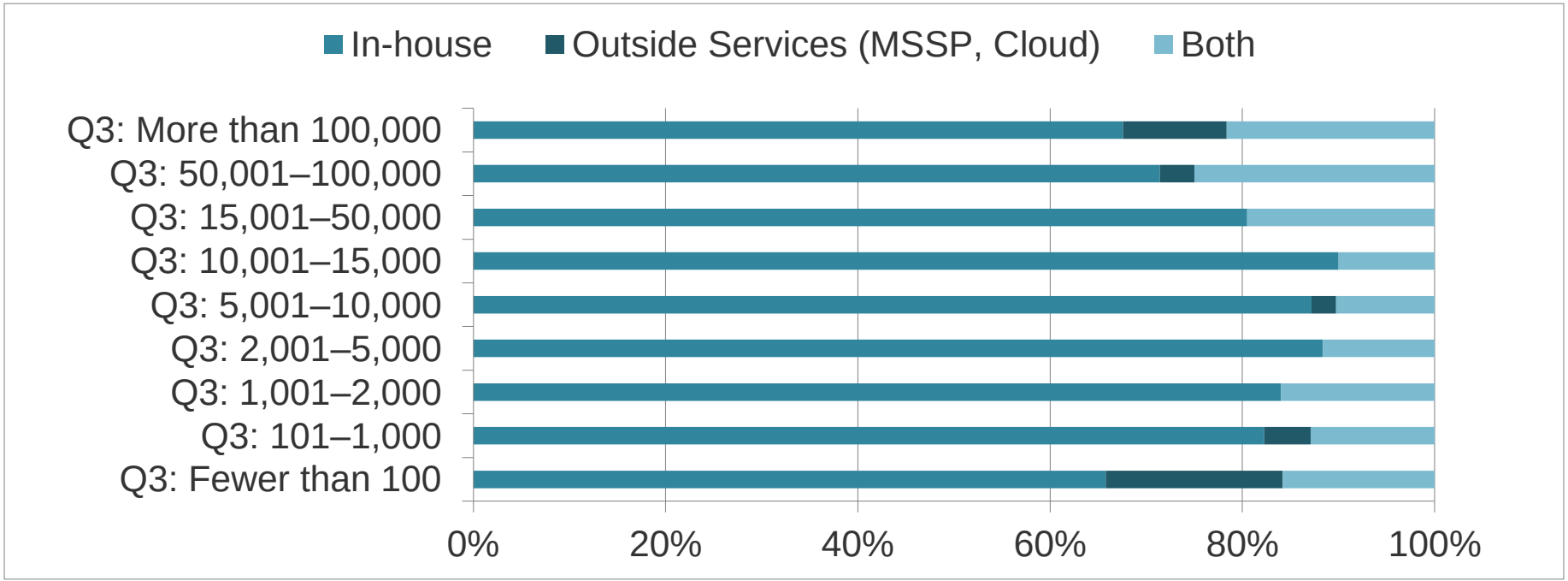
Q3 (Size) v Q12 (Activities-Outsource)

Security Administration



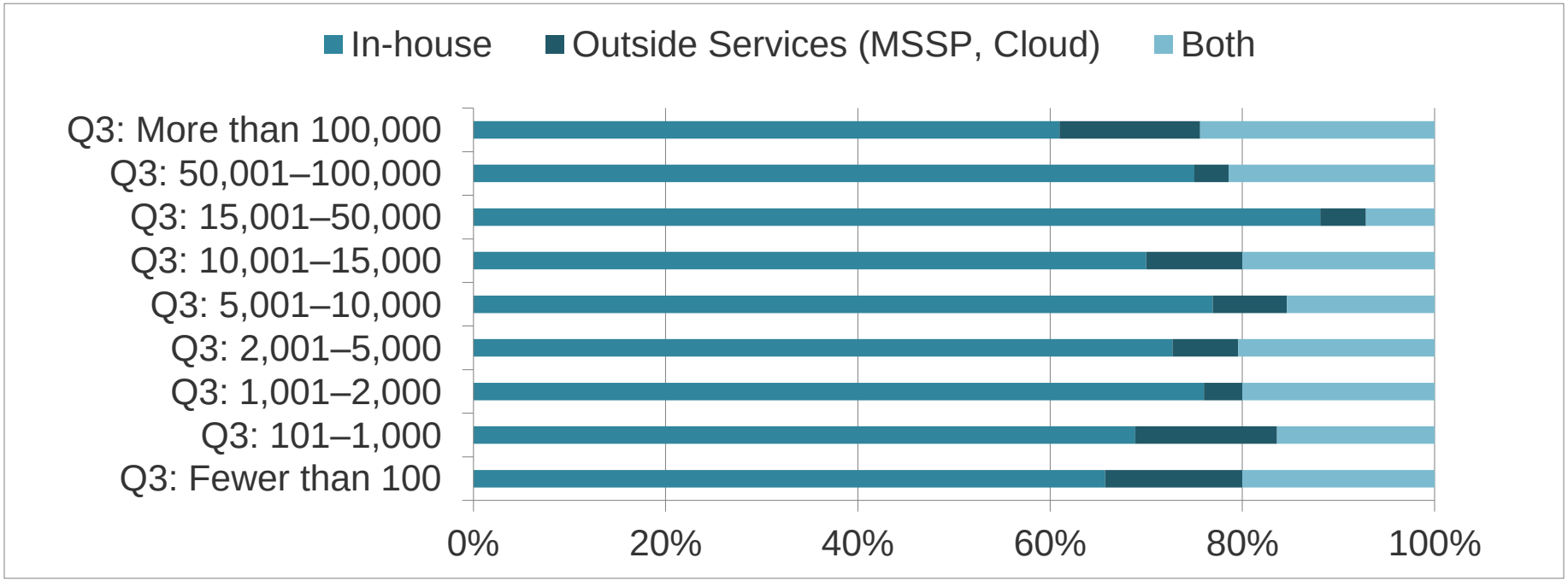
Q3 (Size) v Q12 (Activities-Outsource)

Security Architecture and Engineering – IT Systems



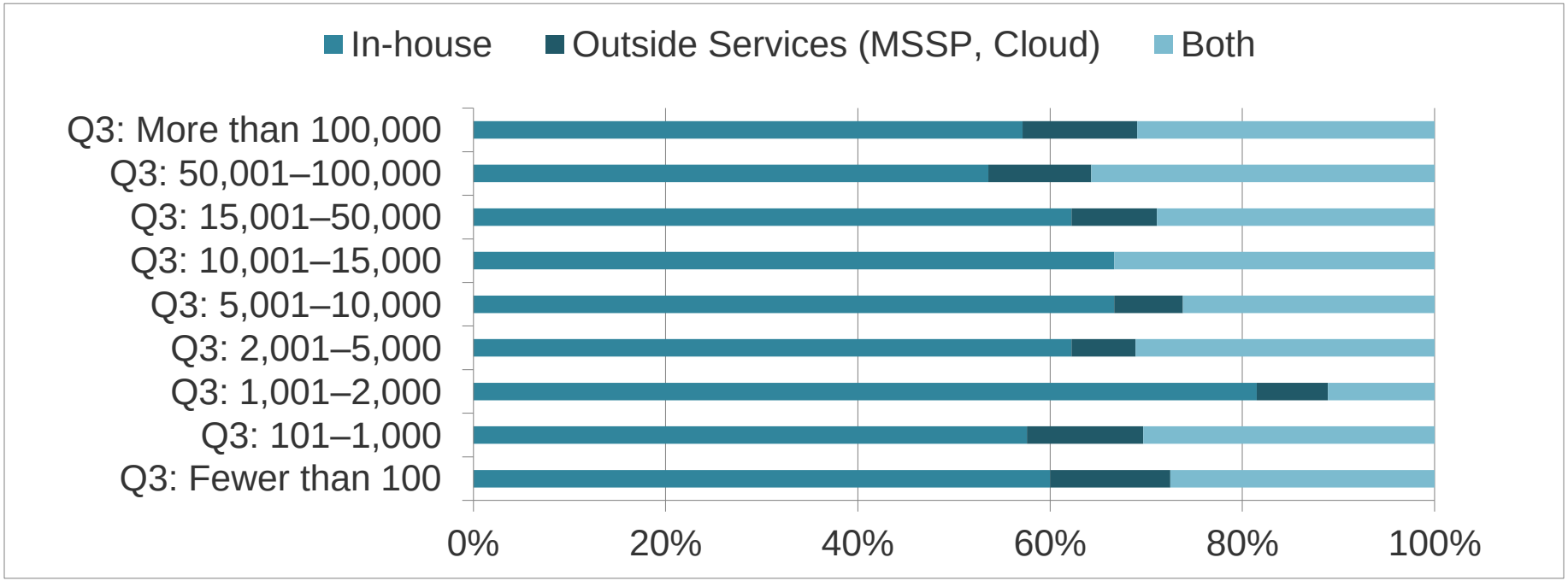
Q3 (Size) v Q12 (Activities-Outsource)

SOC System Architecture and Engineering



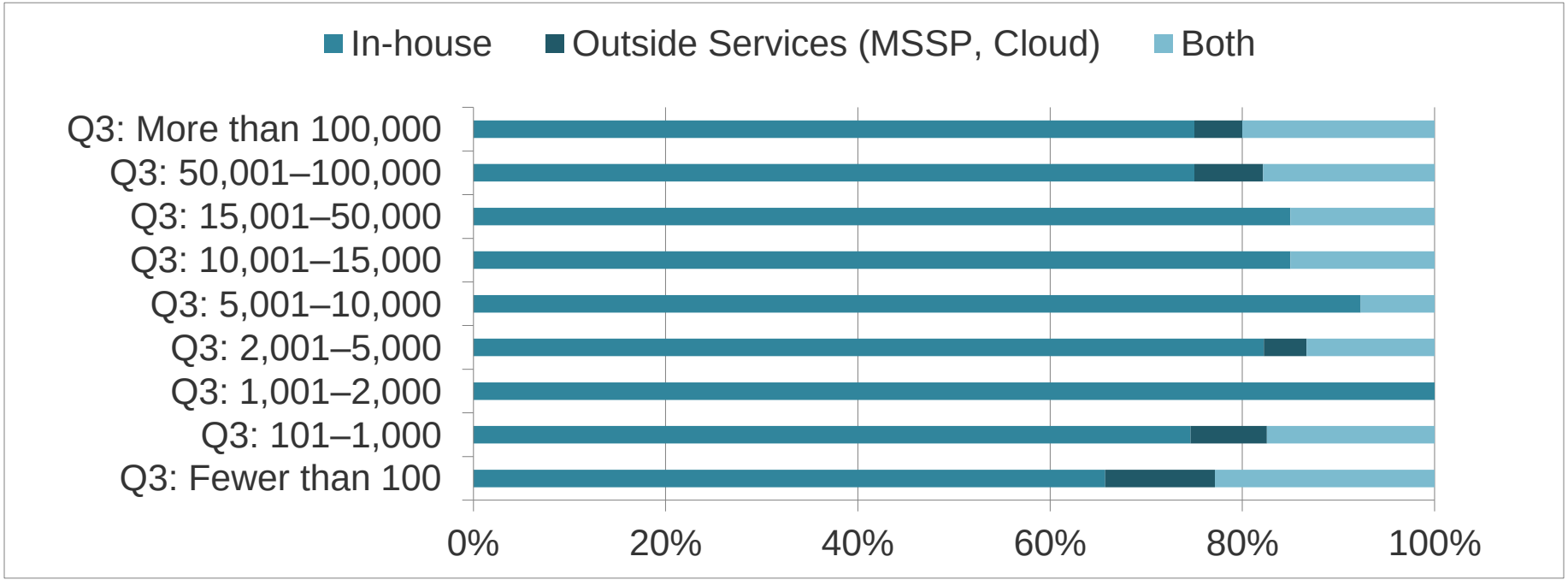
Q3 (Size) v Q12 (Activities-Outsource)

Security Monitoring and Detection



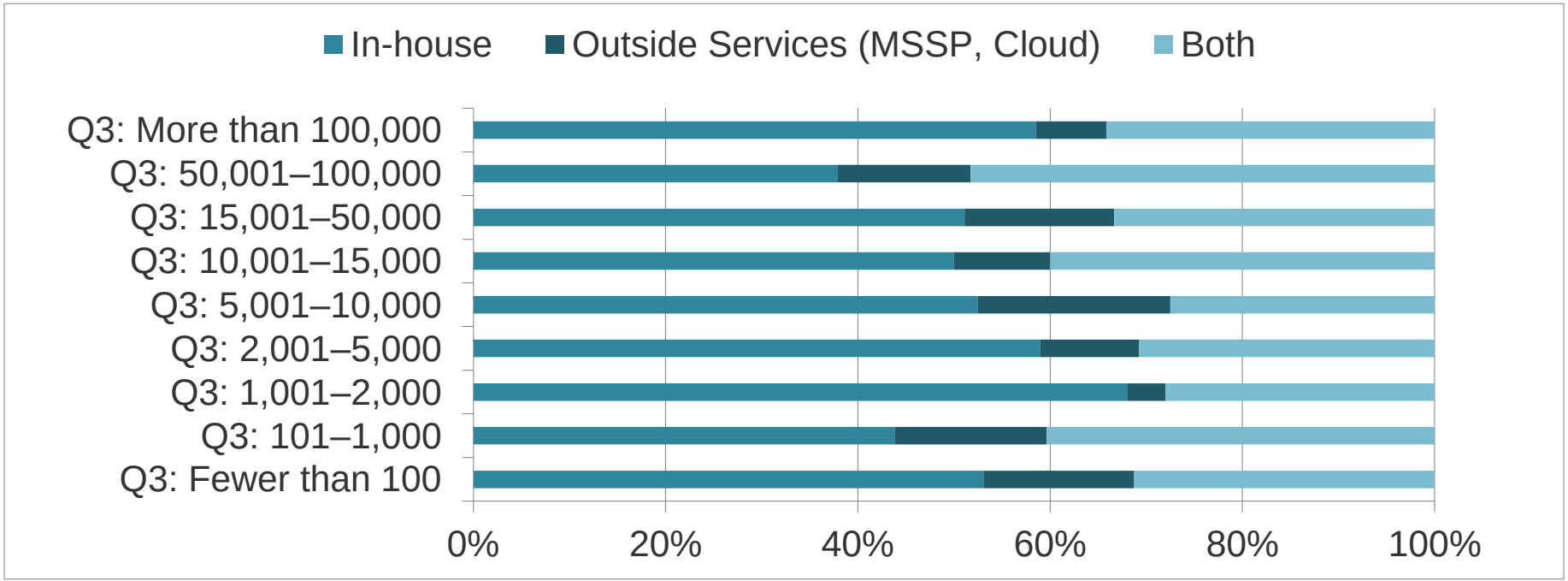
Q3 (Size) v Q12 (Activities-Outsource)

Security Road Map and Planning



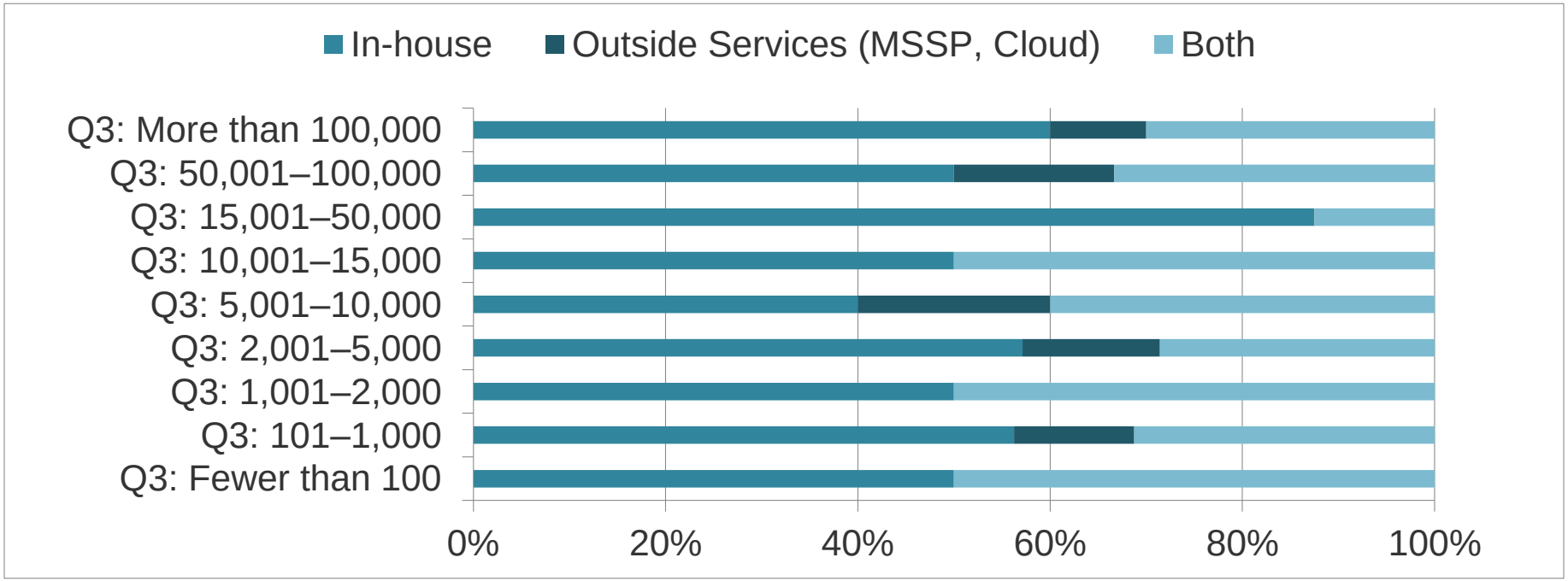
Q3 (Size) v Q12 (Activities-Outsource)

Threat Research



Q3 (Size) v Q12 (Activities-Outsource)

Other



Q3 (Size) v Q12 (Activities-Outsource)

Other List

- Seeking Outside Help From Security Partners
- Vulnerability Assessment
- Aws redlock workday office 365
- NERC-CIP monitoring requirements provider
- Security Service Desk
- Certification related activities (PCI-DSS, etc)

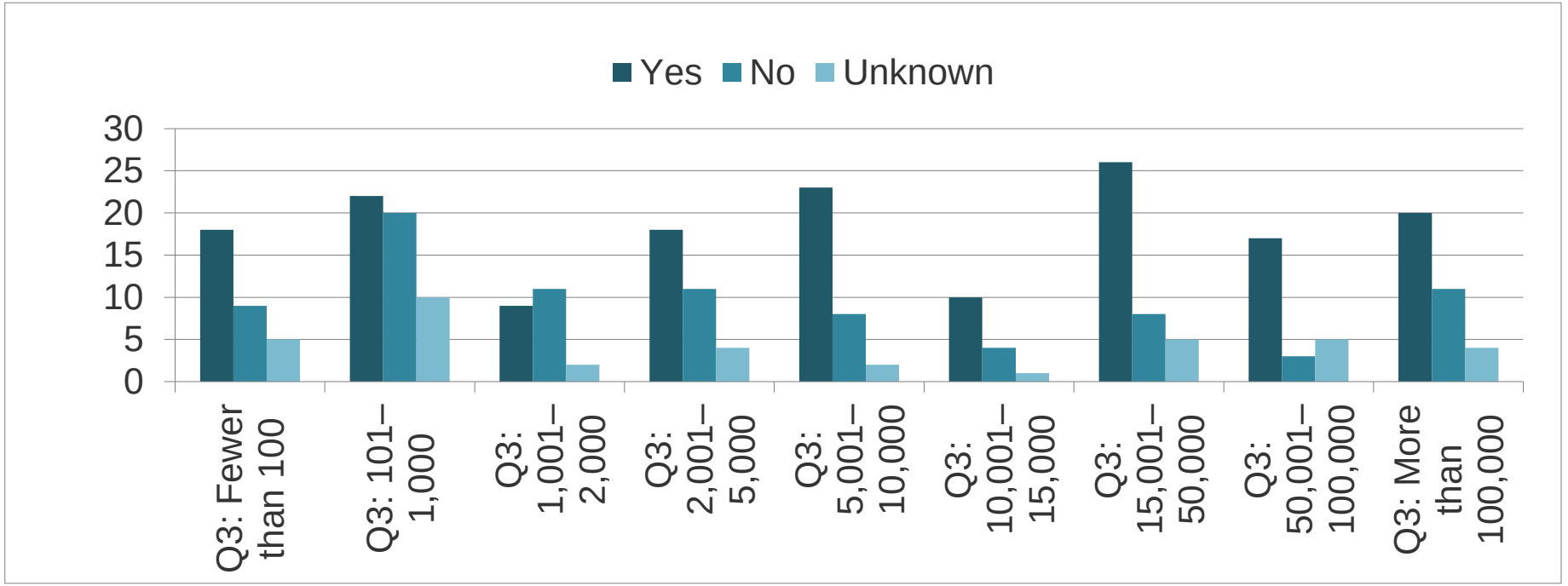
Metrics

Metrics Are One of My Current Focuses

- Co-Authored metrics talk at FIRST that Carson Zimmerman just presented in Edinburgh, UK: https://mgt517.com/first-metrics
- Trying to establish some baseline suite of metrics for SOCs to collect and (dare I suggest) compare
- ATT&CK coverage might be a cool place to start for SOC-SOC comparisons with your peers / competimates

Q3 (Size) v Q27 (Metrics)

Does Your SOC Provide Metrics?



Data Question

Are There Data Scientists Who Are Interested?

- Possible collaborations in further analysis?
- Had one request for a specific element of 2018 data
- Likely would be constrained in some way
- Possible full open source release of data
- I'm interested in opinions on how this might be conducted. Twitter your thoughts: @CCrowMontance #SOCSurvey

Opinions (reflecting on Survey Data)

Defined Handoffs with NOC

At Least Have Clear Workflows

- I spoke about Q2 v Q10: Sector based depiction of banking and finance coordination
- Overall, about 30% are in the two “best” categories, that’s a broad area for overall improvement
- It will take (my estimate) 3-6 months to get traction (just getting management approvals and meetings set up, definition of tasks etc.) in this space if you have no integration currently

Defined Handoffs with NOC

Why Are Large and Small Better at SOC-NOC

- I think large organizations have an expectation of rigor in information technology, and can afford the expense required to develop rigor
- Small organizations, on the other hand, don't need the rigor and can rely on direct relationships between the staff in the SOC and NOC, and are so deprived of resources, have no option but to make do with the most efficient operations, reusing one another's tools

Number of Maintainers

Q3 (Org Size) v Q11 (Maintainers)

- I don’t have a formula for the maintainers required
- You need someone, probably multiple people doing the care and feeding of the systems so they operate with high uptime and reliable performance
- I think you need a Dev, QA, and Stage environment for your SOC systems
  - This may not be “easy” but it is definitely achievable

Global IT Systems

Multiple Region Operations

- 24x7x365 x Global distribution of systems with varying legal requirements is expected in a large enterprise
- Maybe surprising (it is a bit to me) that smaller companies are reporting they're facing IT operations around the globe
- Anecdotally, I've had discussions with people who have this challenge One example has 5 FTEs to do both IT and Security work with Global scope: An organization 90%+ people in this room have heard of, but don't realize is only about 3-5,000 employees and contractors

Speculation (on the Future)

My Projections

2020 – Nothing Dramatic Herein

- SOAR will be implemented well by a small percentage of SOCs (should see an uptick in the technology satisfaction of this)
- No change in “Qualified Staff” (will be the highest ranked “problem” again next year)
- SOCs will continue to grow, but this growth trend has only a couple of years left (Org size v. SOC Analyst count will not increase past 2022)
- Outsourcing will increase (Outsourcing percentages increase)

Conclusion

Action Items

Recap

- SOC Survey: Useful, challenges, improving
- Issue: Are we asking the right questions?
- Data is “muddy” – interesting, but uncertain
- Possible data release / access
- Push for good SOC-NOC integration (and Metrics)

Thank You

- CCrowMontance (twitter)
- https://www.mgt517.com/soc for this slide deck & other public decks, plus additional references
  - Redistribution authorized, but please provide citation
- https://www.montance.com/soc/timeline : current project for building a SOC