Approaches to Network Threat Detection

Summary Results | January 2020

GATEPOINT RESEARCH PulseReport

Survey Summary

- Between September 2019 and January 2020, Gatepoint Research invited selected IT executives to participate in a survey themed *Approaches to Network Threat Detection.*
- Candidates were invited via email and 202 executives have participated to date.
- Management levels represented are predominantly senior decision makers: 10% hold the title CxO or VP, 62% are Directors, and 28% are Managers.
- Survey participants represent firms from a wide variety of industries including business services, construction, consumer services, financial services, healthcare, manufacturing (general, primary and high tech), mining, public administration, retail trade, telecom services, transportation, utilities, and wholesale trade.
- Responders work for firms with a wide range of revenue levels:
  - 59% work in Fortune 1000 companies with revenues over $1.5 billion;
  - 15% work in Large firms whose revenues are between $500 million and $1.5 billion;
  - 5% work in Mid-Market firms with $250 million to $500 million in revenues;
  - 21% work in Small companies with less than $250 million in revenues.
- 100% of responders participated voluntarily.

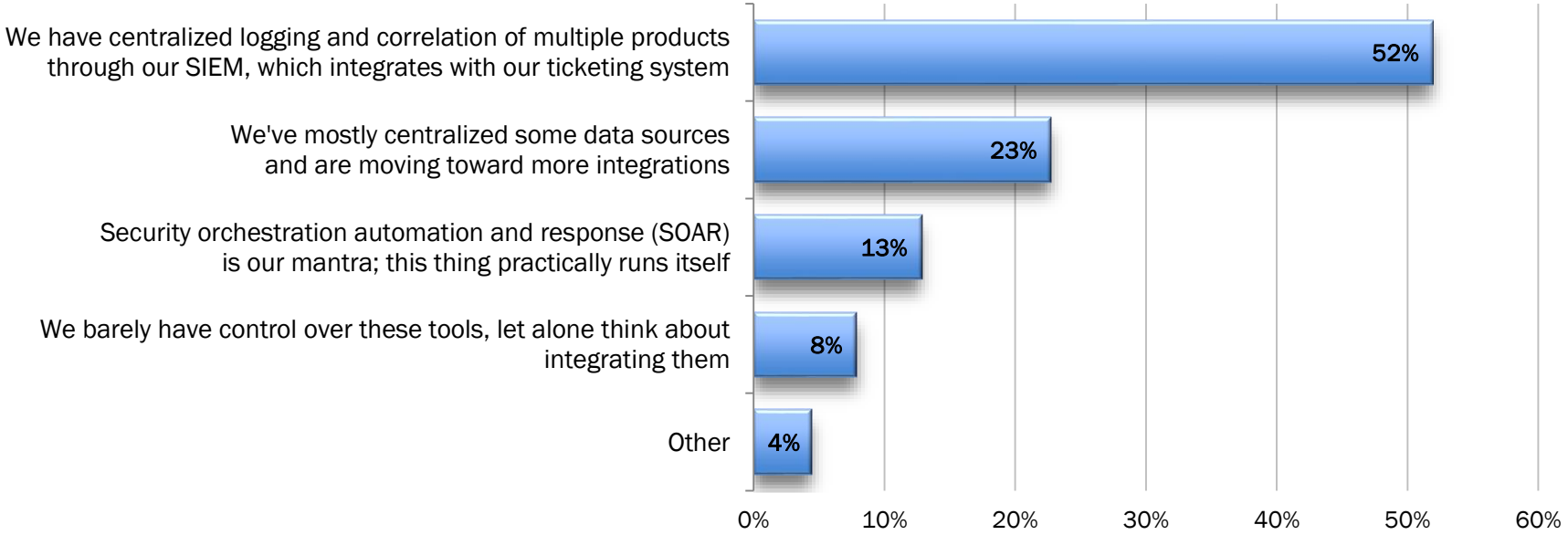
Executive Overview

It's obvious that effective network security depends on quick threat detection and response. But often, just getting good visibility into what is really happening on the network is hampered by inadequate tool integration or false positives, which in turn can generate slow or inappropriate incident responses. What are organizations doing to analyze incidents quickly and critically so they respond effectively?

This survey asks respondents to report:

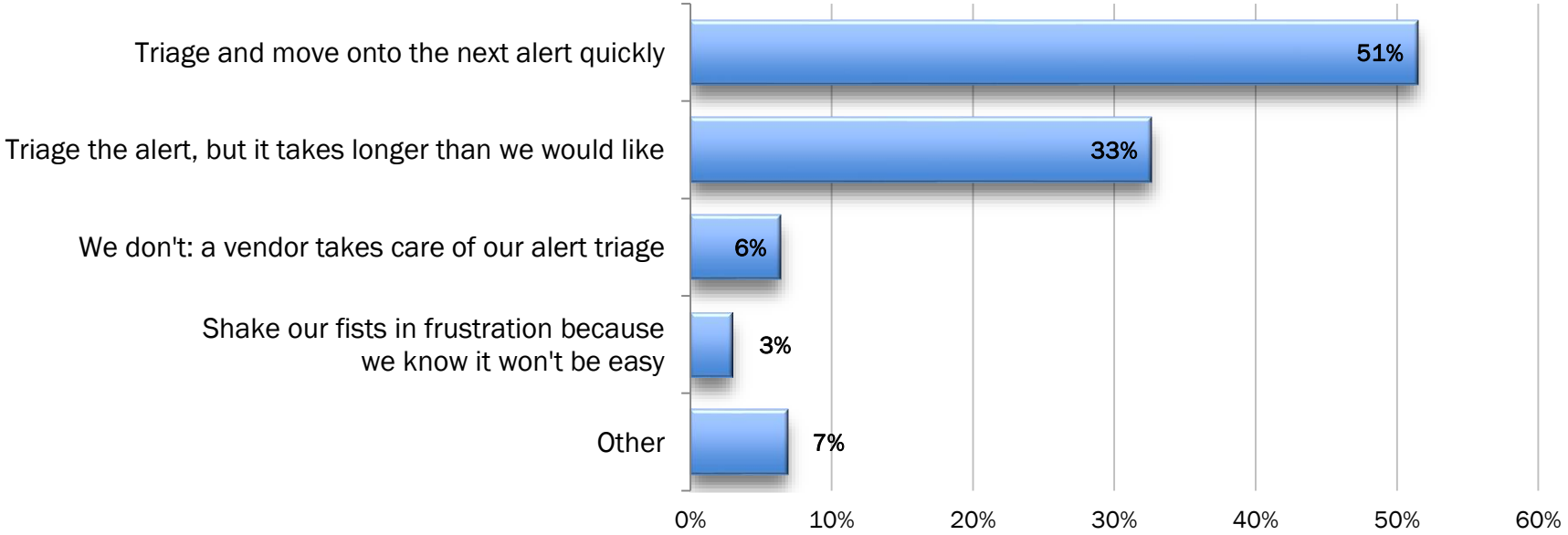
- How integrated are the tools in their security stack? Does their team react to alerts effectively?
- What about false positives – are they adequately detected and managed?
- What is their incident response process? Do they use network data for incident response?
- How would they rate their security team's incident response capabilities overall?
- How capable is their team in network forensics investigations?

What is the current level of integration between the tools deployed in your security stack?



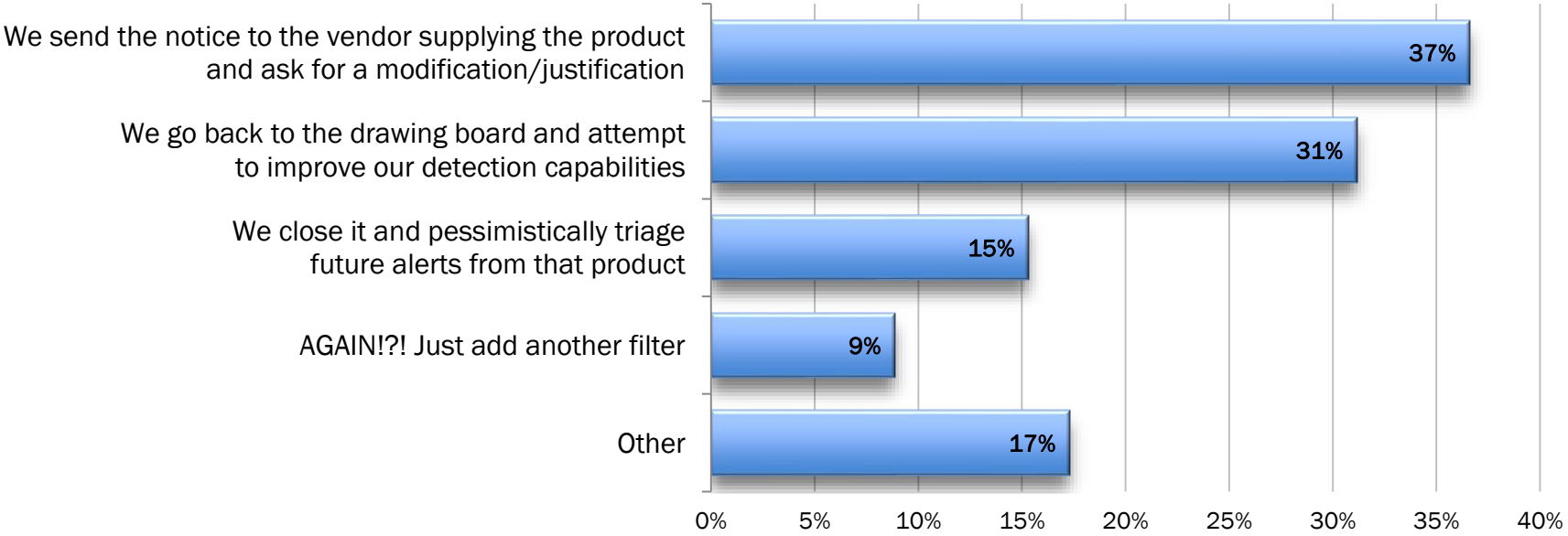
More than half of respondents (52%) report the tools in their security stack achieve integration via centralized logging and correlation through their SIEM. About a quarter have started integration by centralizing their data sources, and 13% extoll SOAR.

How does your team react to alerts from security tools?



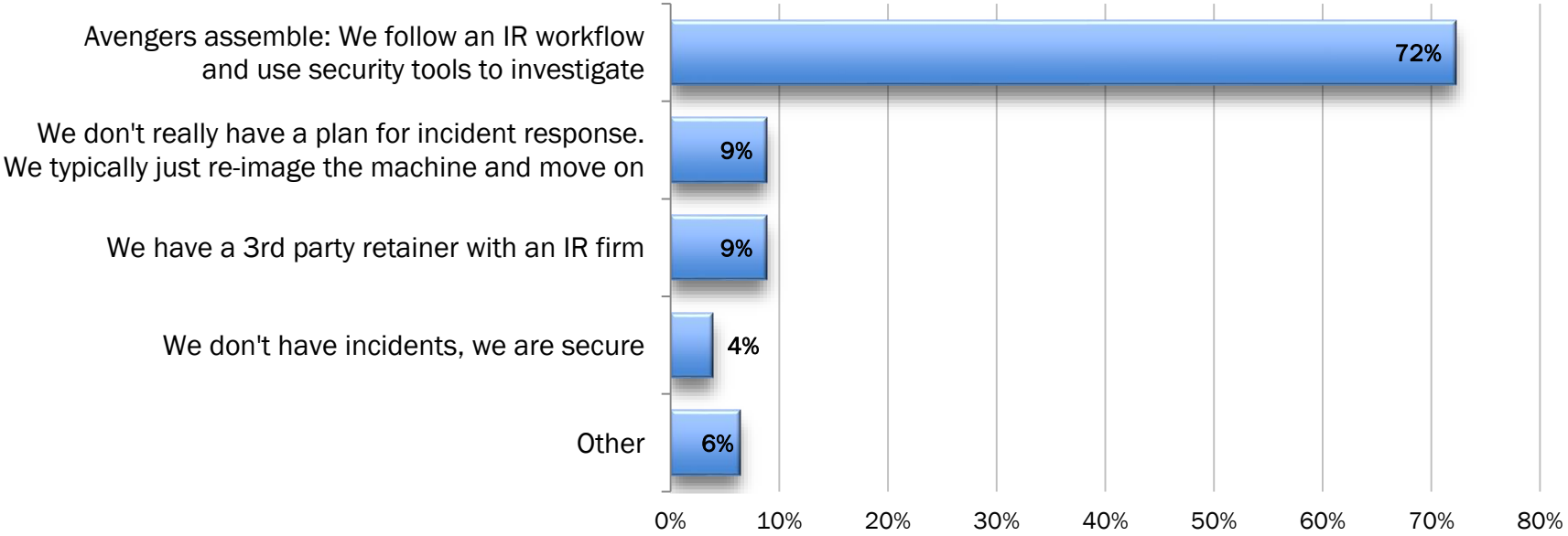
51% of respondents claim they can triage security alerts quickly; another 36% are not so pleased with the speed with which they can react.

How does your team manage false positive alerts from your security tools?



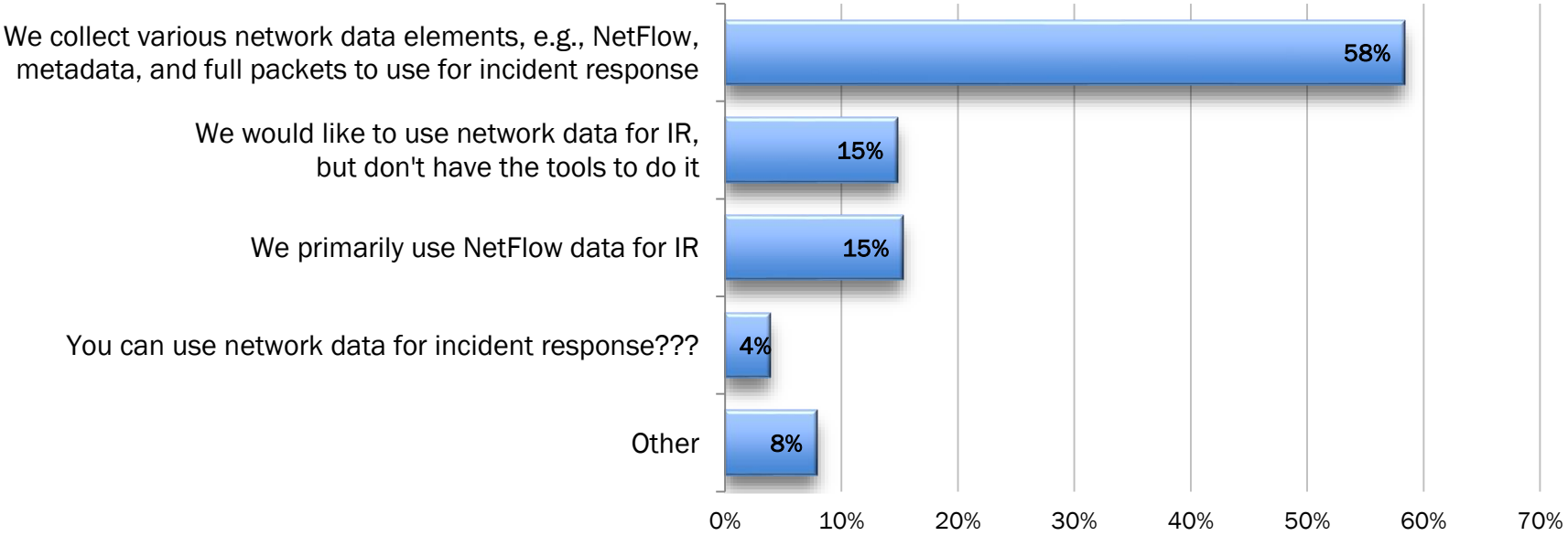
False positives generate a slew of close-the-barn-door-after-the-horse-has-bolted reactions: ask the product vendor to modify it or justify the alert (37%), use the incident to revise detection capabilities (31%), triage similar future alerts (15%), or shrug and add another filter (9%).

Describe your incident response (IR) process from alert to incident escalation.



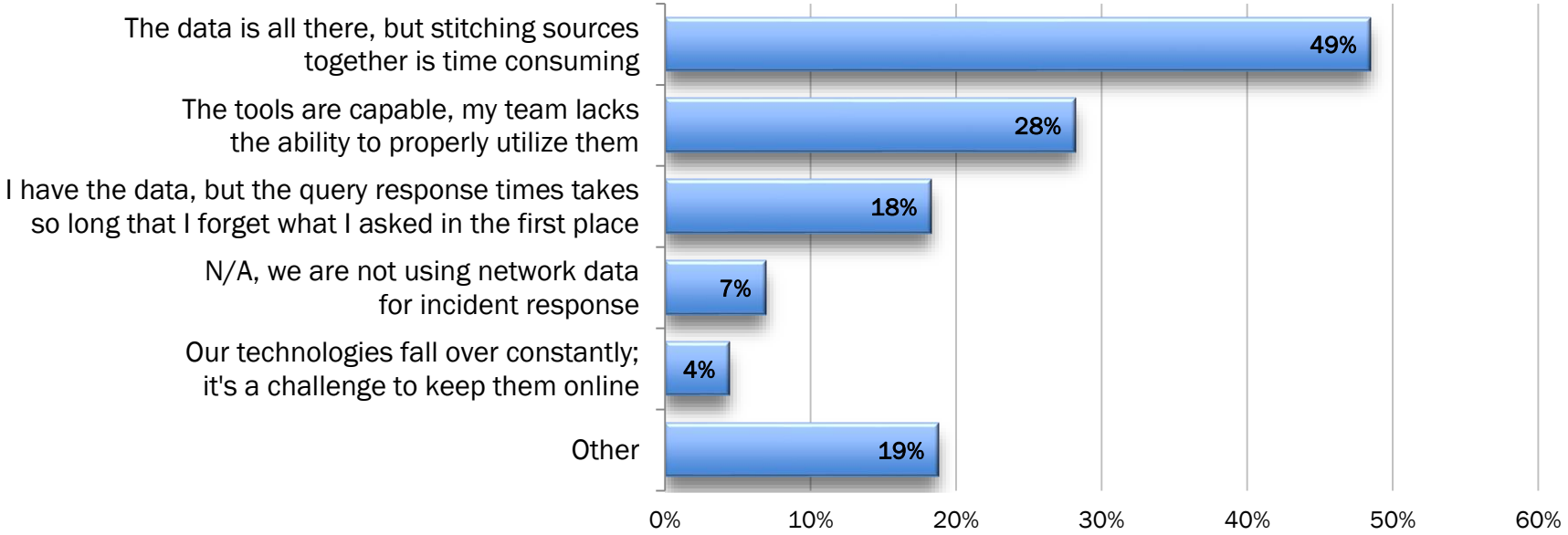
The vast majority of respondents (72%) follow an alert with an established IR workflow response, using security tools to investigate.

How does your team use network data for incident response (IR)?



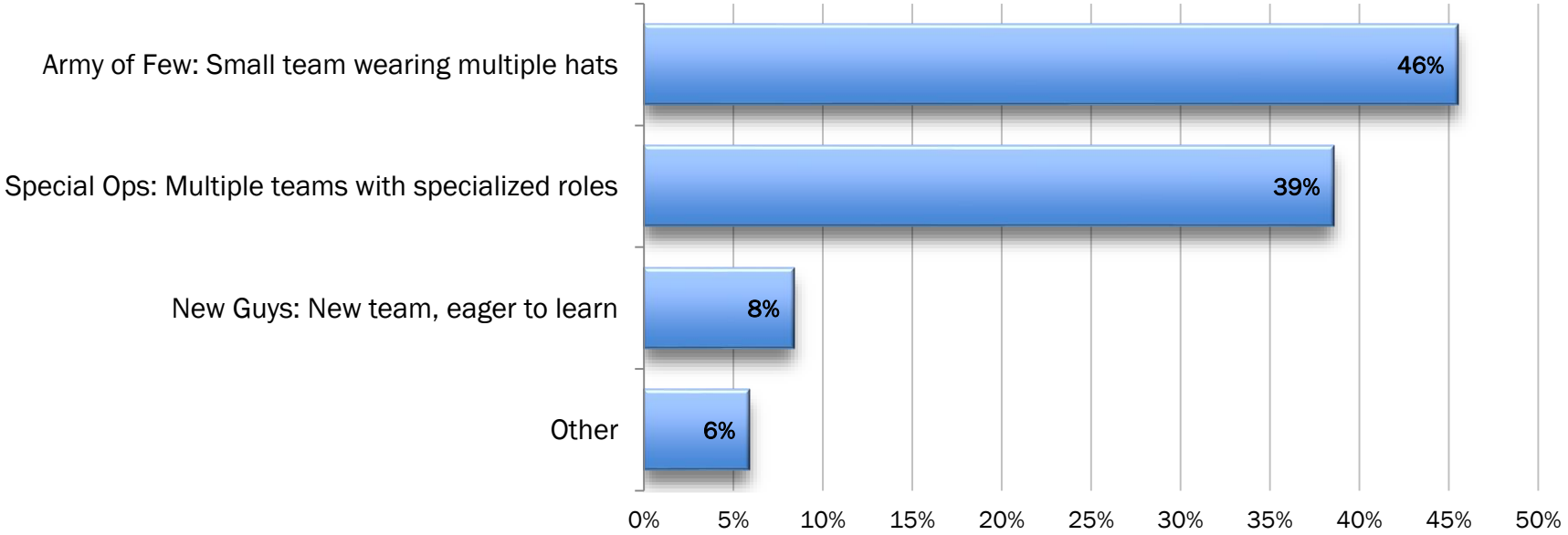
73% of those surveyed do have the capability to use network data in their incident response, either a variety of elements or just NetFlow data. The remainder either don't have the tools or don't know how to use this resource.

Do you find anything challenging about using network data for incident response?



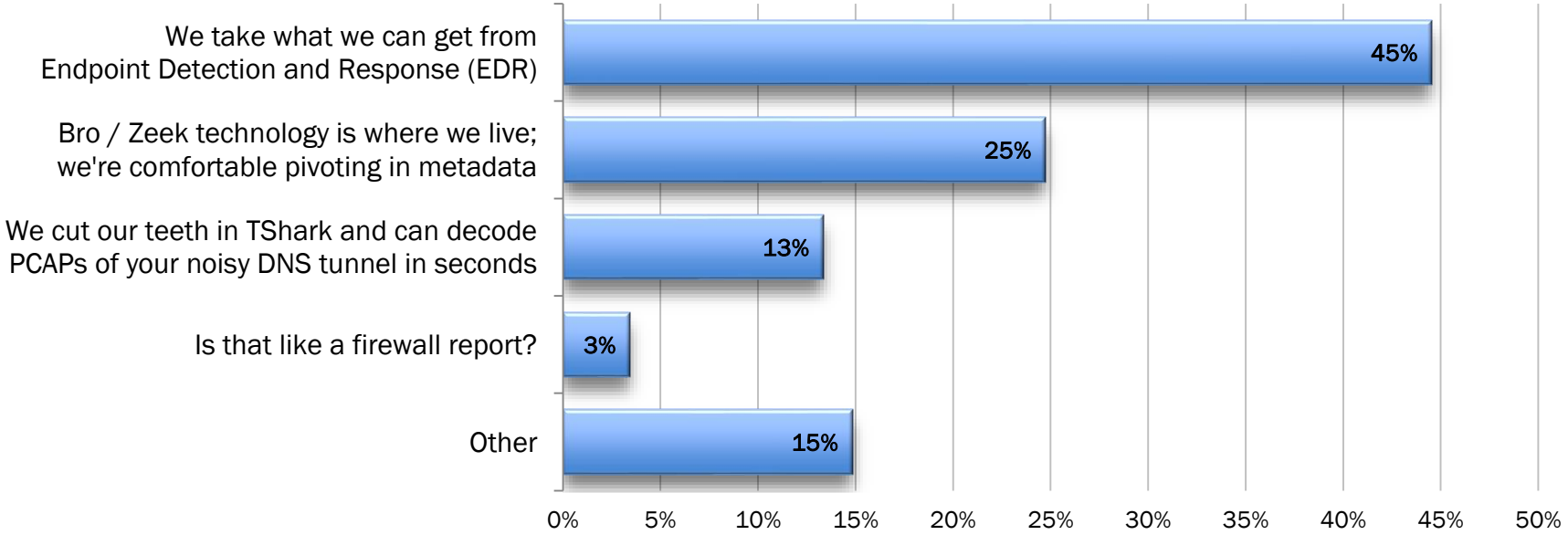
Using network data presents challenges: 49% of those surveyed admit that massaging network data into usable forms is too time consuming. Another 28% say their teams aren't trained to use the tools effectively. 18% fall asleep before their query returns a result.

How would you describe your security team's overall incident response capabilities?



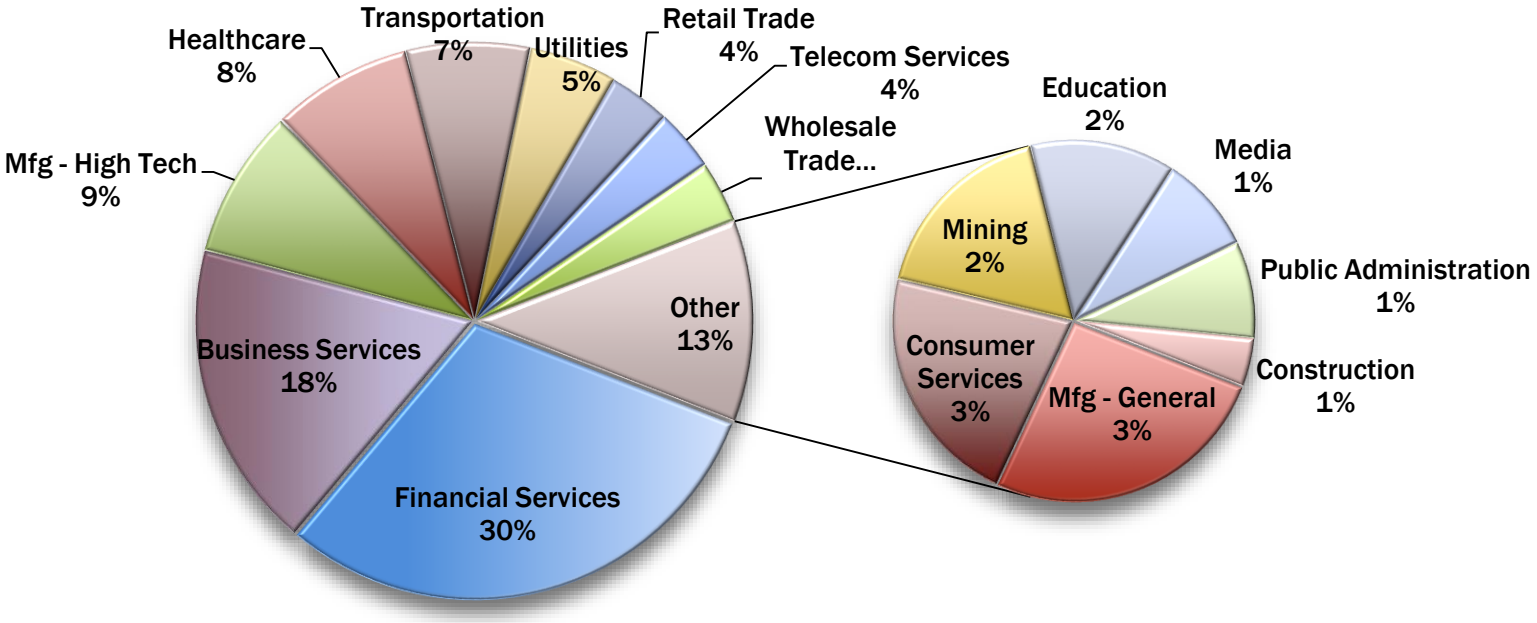
Nearly half of organizations surveyed characterize their incident response unit as a small team who are multitalented (or perhaps thinly stretched). 39% apply multiple teams to different roles and 8% are the few, the proud, the new.

Rate your team's capability in network forensics.



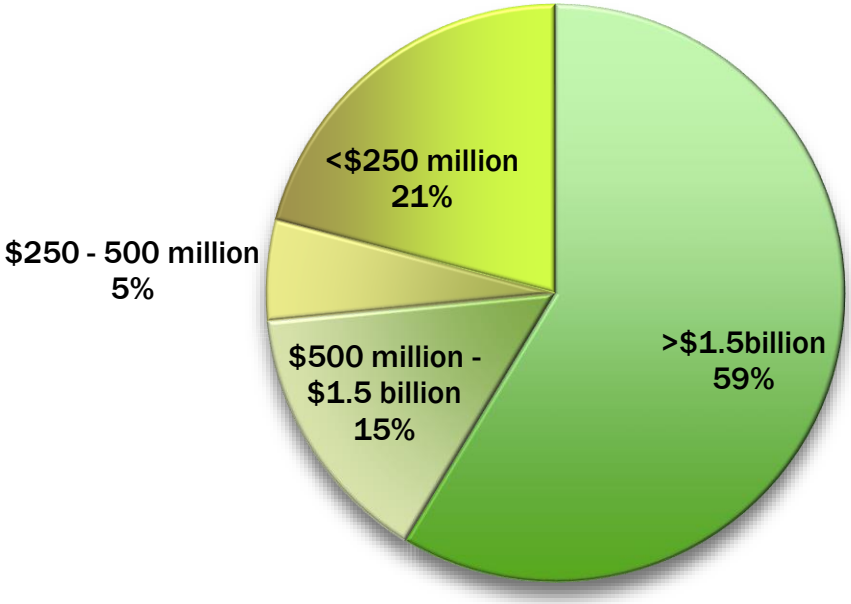
Regarding network forensics, 45% of respondents only analyze EDR results; 25% speak Bro/Zeek and 13% boast they are network protocol analyzing gurus.

Profile of Responders: Industry Sectors



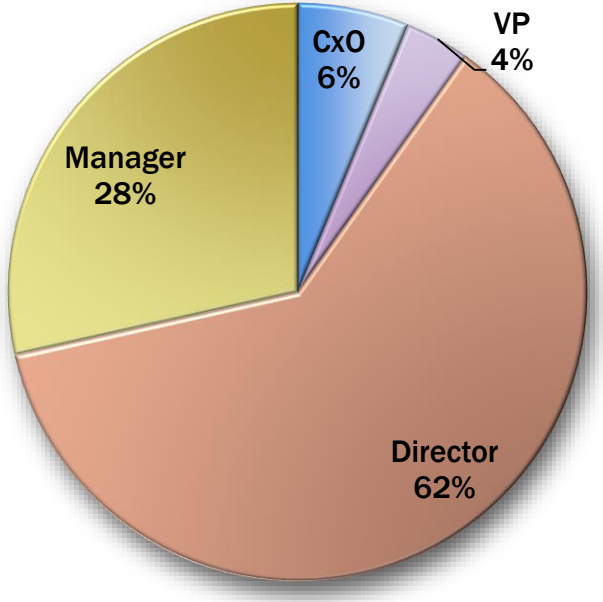
Responders represent a wide variety of industries.

Profile of Responders: Revenue



59% of those surveyed work in Fortune 1000 companies with revenues over $1.5 billion.

Profile of Responders: Job Level



72% of those surveyed hold Director or executive level positions in their organizations.

Gigamon Insight is a cloud-based network threat detection and response solution that helps you identify blind spots and detect, hunt and investigate threats across your entire network.

Learn more at Gigamon.com