SOC Modernization and the Role of XDR

Jon Oltsik, Senior Principal Analyst, ESG Fellow
Dave Gruber, Principal Analyst

PREPARED BY ESG FOR

Research Objectives

Examine the people, processes, and technology supporting the modernization of security operations.

Identify key value points, required metrics to back up those value points, and what's expected from both products and managed services for XDR and SOC modernization.

Determine current perception and role of XDR as a component of security operations modernization efforts.

Explore strategies used to automate triage, speed investigations, and help organizations find unknown threats.

Survey Details

QUANTITATIVE WEB-BASED SURVEY

- N=376 qualified completes
- North America (US and Canada)
- Field dates: 4/4/2022 – 4/15/2022

SURVEY RESPONDENTS

- IT and security professionals involved with cybersecurity technology and processes.
- Employed at organizations with 100 or more employees
  - Midmarket (500 to 999 employees, 16%)
  - Enterprise (1,000 or more employees, 84%)
- Multiple industry verticals including financial, manufacturing, business services, retail/wholesale, technology, among others
- Complete demographics included at end of presentation

A Few Housekeeping Items

Data Exclusivity Information

- All of the ESG clients that sponsored this research received the data on May 25, 2022 and will have exclusive access to the data for 90 days from this date. As such, the sponsor exclusivity period will end on August 26, 2022.
  - For the first 30 days, (May 25-June 24) the data will be under embargo while ESG schedules final results presentations with all sponsors. Sponsors can start using the data publicly on June 25, 2022.

- During this sponsor exclusivity period, **only** clients that sponsored this research can use/promote data points publicly. We do ask that you abide by ESG's research usage rights and citation policy, which can be found at the following link for your reference. If you do decide to use data points in content you create, we also request that no more than 5 data points be used per asset. After the exclusivity period is up, ESG will then start to write about and promote the findings through blog posts, reports/briefs, infographics, and other syndicated content.

Content and Deliverables

- ESG will deliver an eBook highlighting key findings by June 24
- ESG will create a library of instagraphics for sponsors to choose from and share by June 24

SOC MODERNIZATION: 5 KEY TRENDS

MORE DATA AND BETTER DETECTION RULES ARE STILL DESIRED.

Despite massive amount of security data in use, more is desired, as is better detection rules.

SECOPS PROCESS AUTOMATION INVESTMENTS ARE PROVING VALUABLE.

While implementation strategies vary, automation investments are paying off for most.

MITRE ATT&CK FRAMEWORK IS PROVING VALUABLE FOR MOST.

However, many are still figuring out how and where to apply it to gain value..

XDR MOMENTUM CONTINUES TO BUILD.

While much confusion exists about what XDR is, investment in support of advanced threat detection is significant.

THE USE OF MDR IS MAINSTREAM AND EXPANDING.

While use cases vary, MDR services are widely adopted across organizations of all sizes and maturity.

Double click the icon, then choose "*Change Graphic*" > "*From Icons*" in the drop-down menu located in the top left panel of ribbon.

More Than Half Think SecOps is More Difficult Today vs. Two Years Ago

5 Reasons Why

1. Growing attack surface
2. Threat landscape
3. More cloud usage
4. A growing number of security tools
5. Firefighting leaves no time to improve the program

The Expanding Attack Surface Creates More Challenges

1. More Vulnerabilities to Manage
2. Current Tools are Failing to Support Expanding Attack Surface
3. Modern Applications Development and Deployment has Increase Velocity Requiring New Skills

A Look at Current SOC Maturity

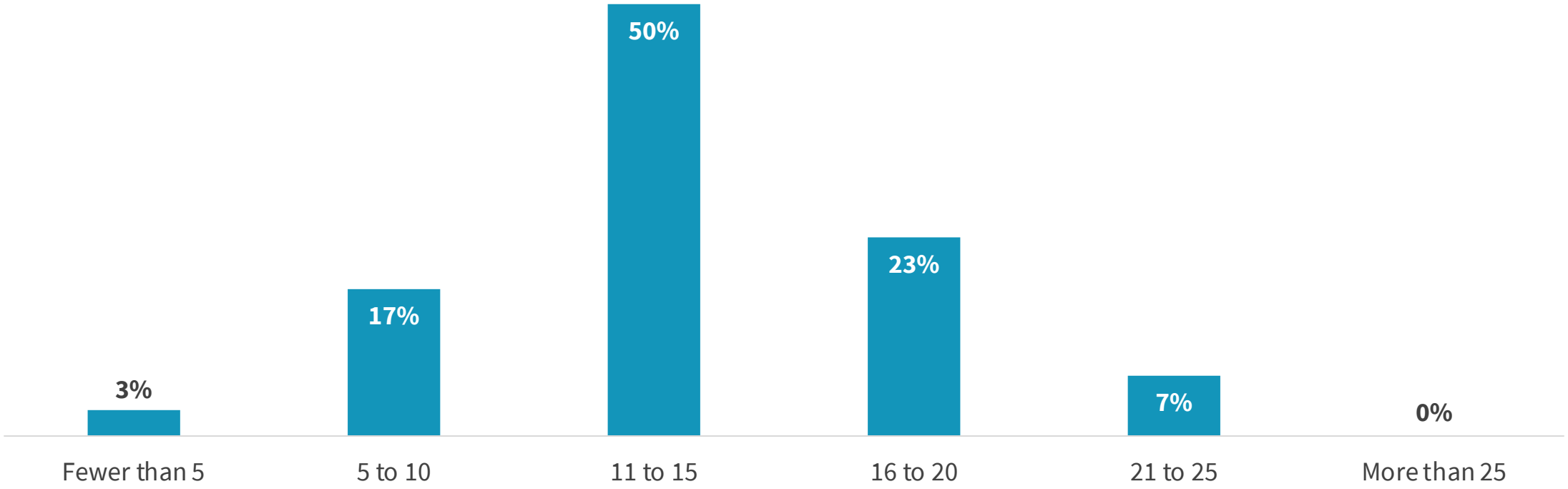
- Over 70% have 4+ years of SOC experience
- Most rely on traditional SOC metrics: MTTD/MTTR
- Operating models vary (tiered, aligned to threat vectors, common queue)
- Despite skills shortages, ¾ say they are happy with current staffing, yet many still report gaps "after hours"
- Many report acute skills issues in support of AppSec
- Expert skills are also in demand, and many are turning to MDR services to fill gaps

Modernizing Security Operations: *5 Key Trends*

Trend 1: More Data and Better Detection Rules Are Still Desired

Despite Multiple SecOps Sources, More Are Still Desired

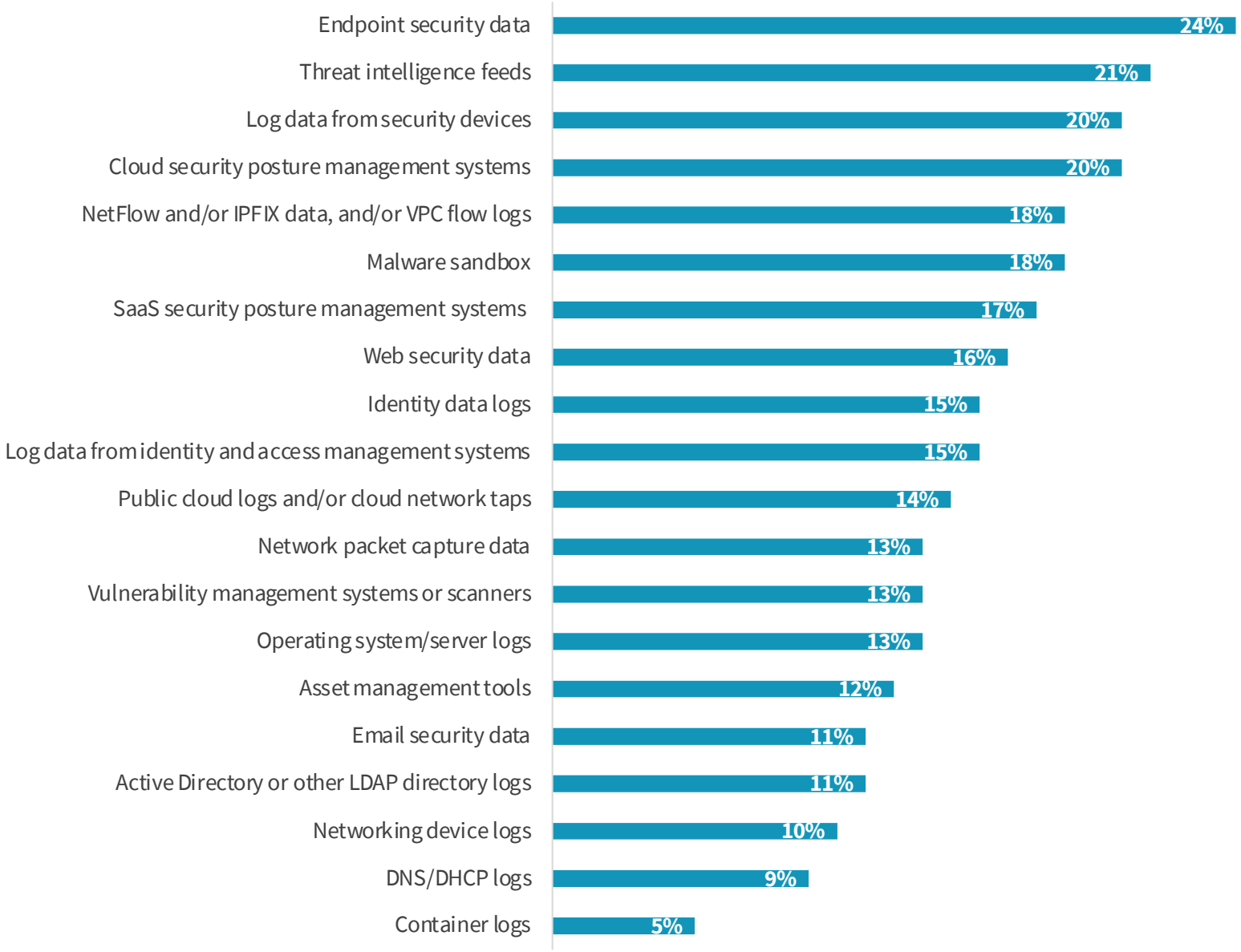
80% use more than 10 data sources



Question text: Approximately how many different data sources does your organization use for security operations (i.e., to monitor security across hybrid IT, for security analytics, etc.)? (Percent of respondents, N=376)

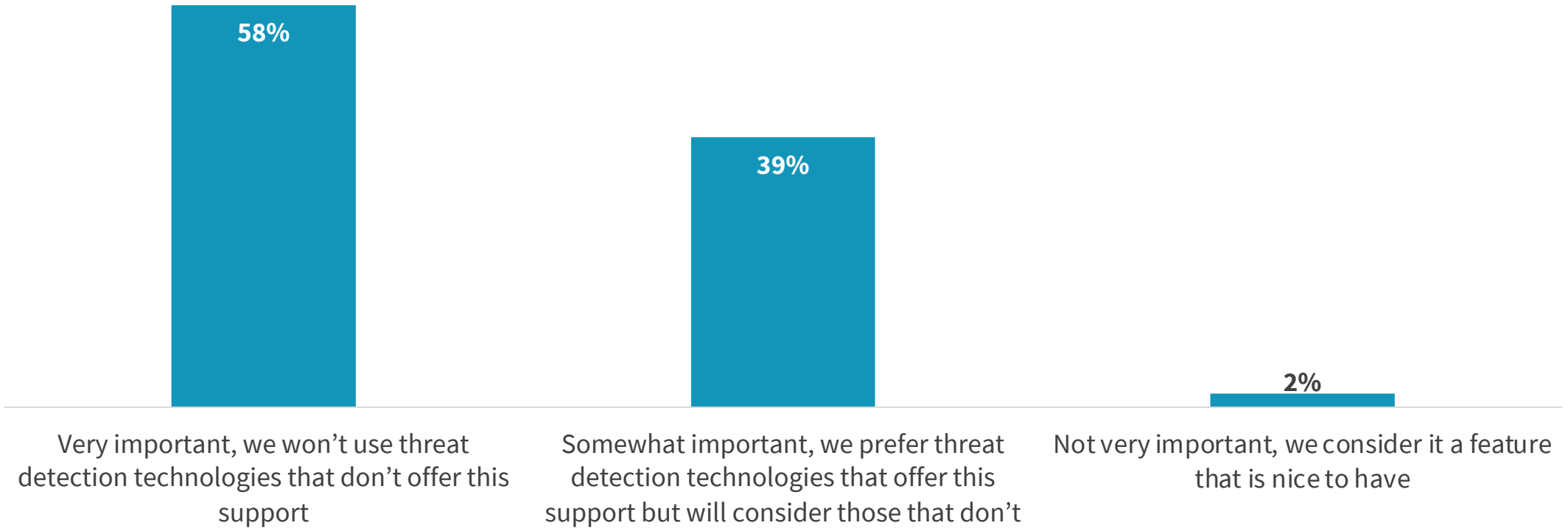
Despite the Move to XDR, Endpoint Data Is Still Most Valued

As always, threat intel is also a top priority. Why are container logs so low? Ephemeral?



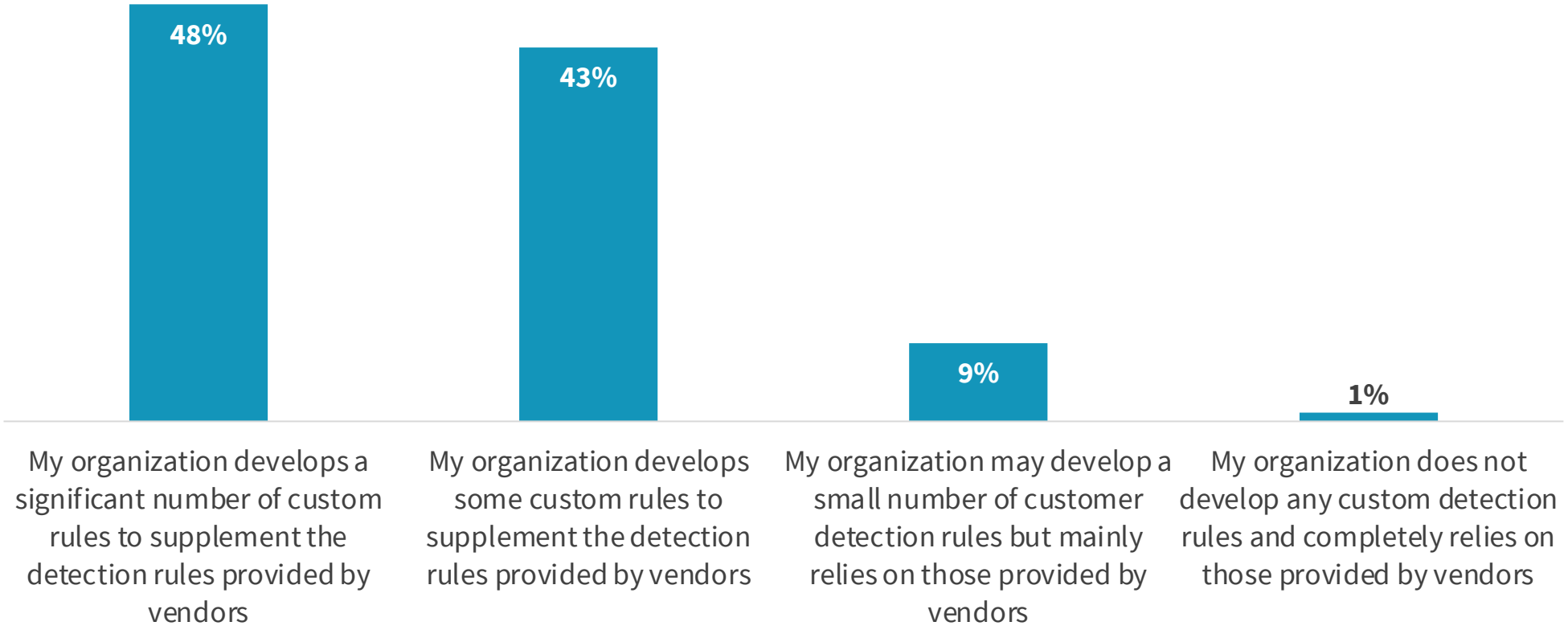
Question text:
Of all the data sources your organization uses for security analytics/operations, which would you say are the most important for security operations (i.e., monitoring, analytics, etc.)? (Percent of respondents, N=376, three responses accepted)

Custom Detection Rules Are Important for Most



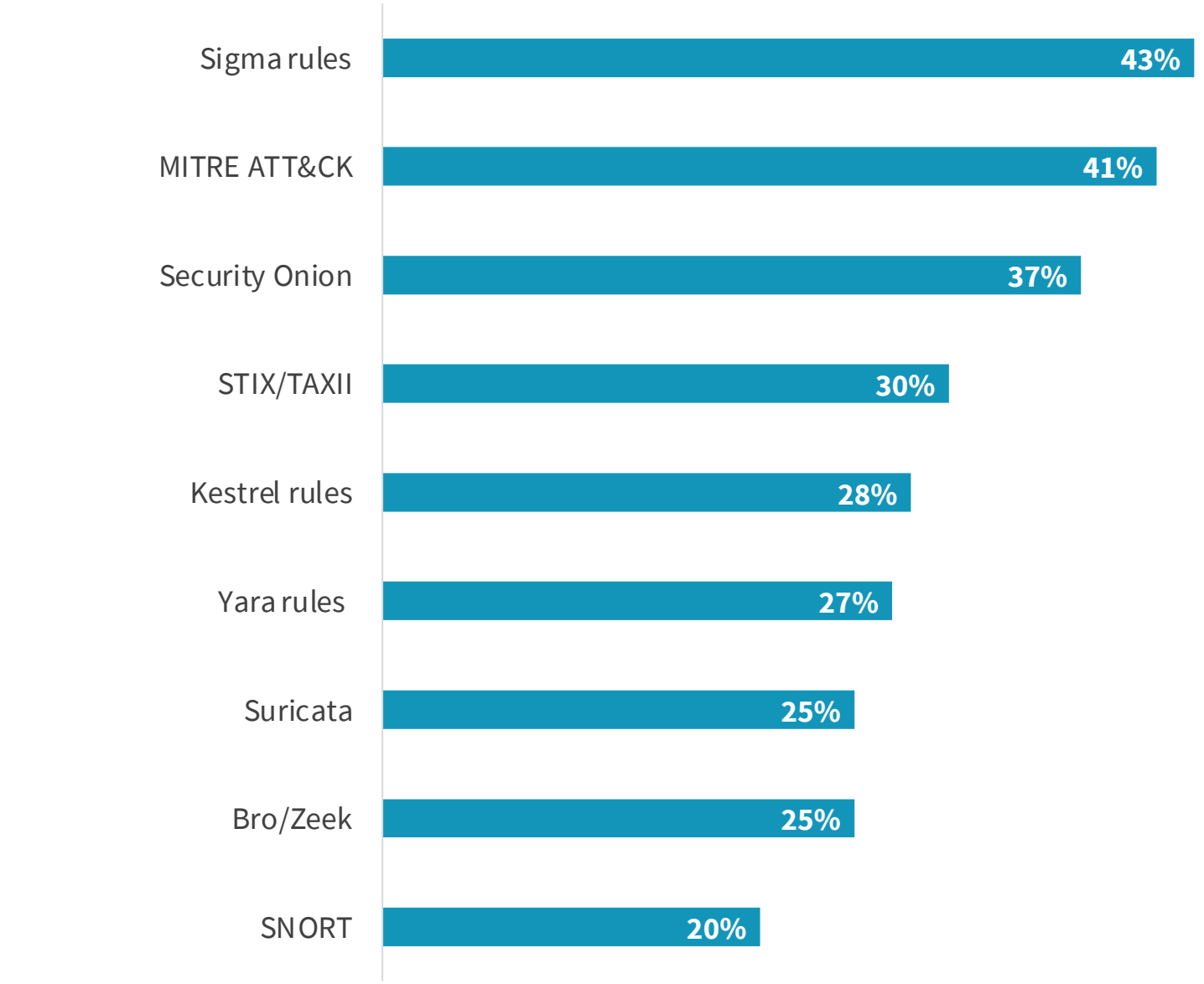
Question text: How important is it for your organization's threat detection technologies to support the ability to develop custom rules and/or custom machine learning models? (Percent of respondents, N=376)

Despite OOTB Detection Rules, Most Invest Further in Custom Detection Rules Engineering



Question text: When it comes to threat detection rules, which of the following best describes your organization's approach? (Percent of respondents, N=376)

Standards and Frameworks Are Having an Impact



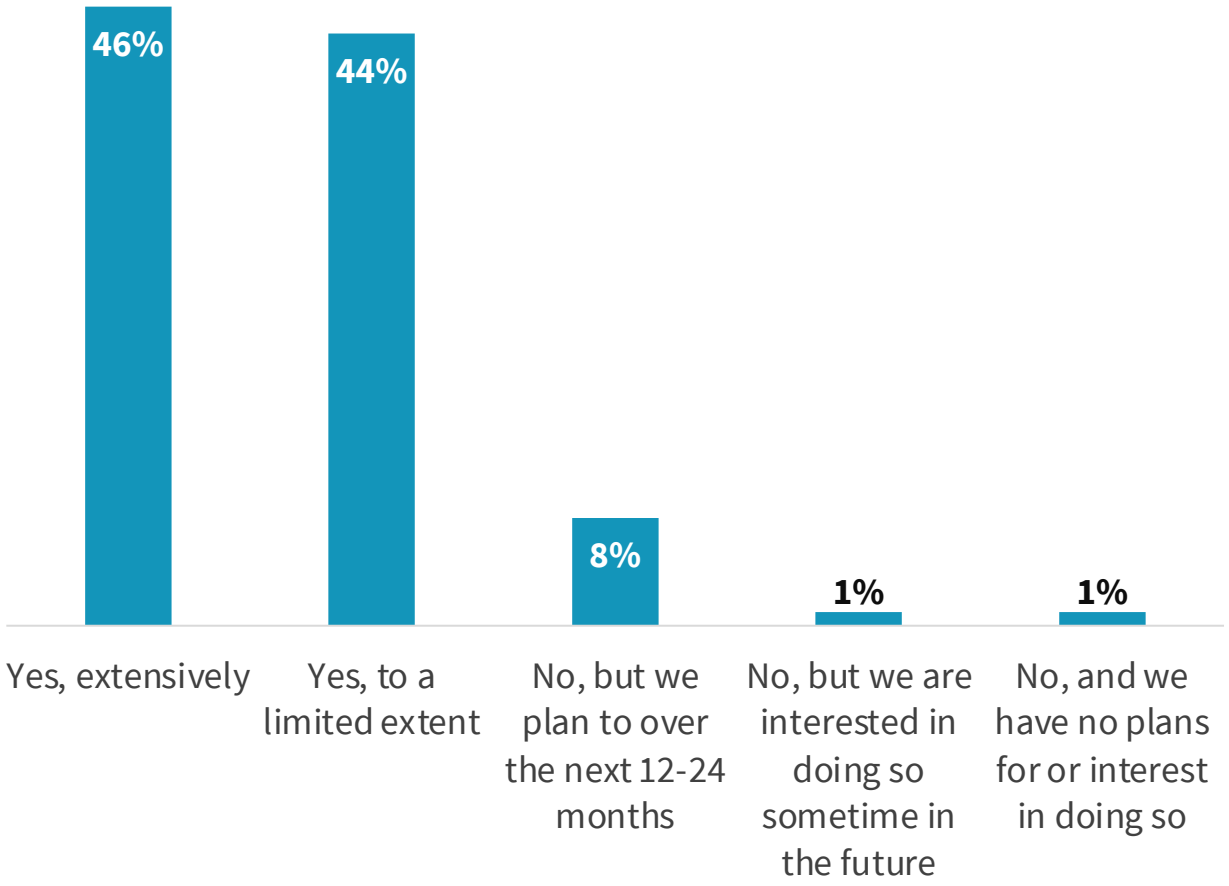
Question text:
Which of the following does your organization use as part of its threat detection program? (Percent of respondents, N=376, multiple responses accepted)

Modernizing Security Operations: *5 Key Trends*

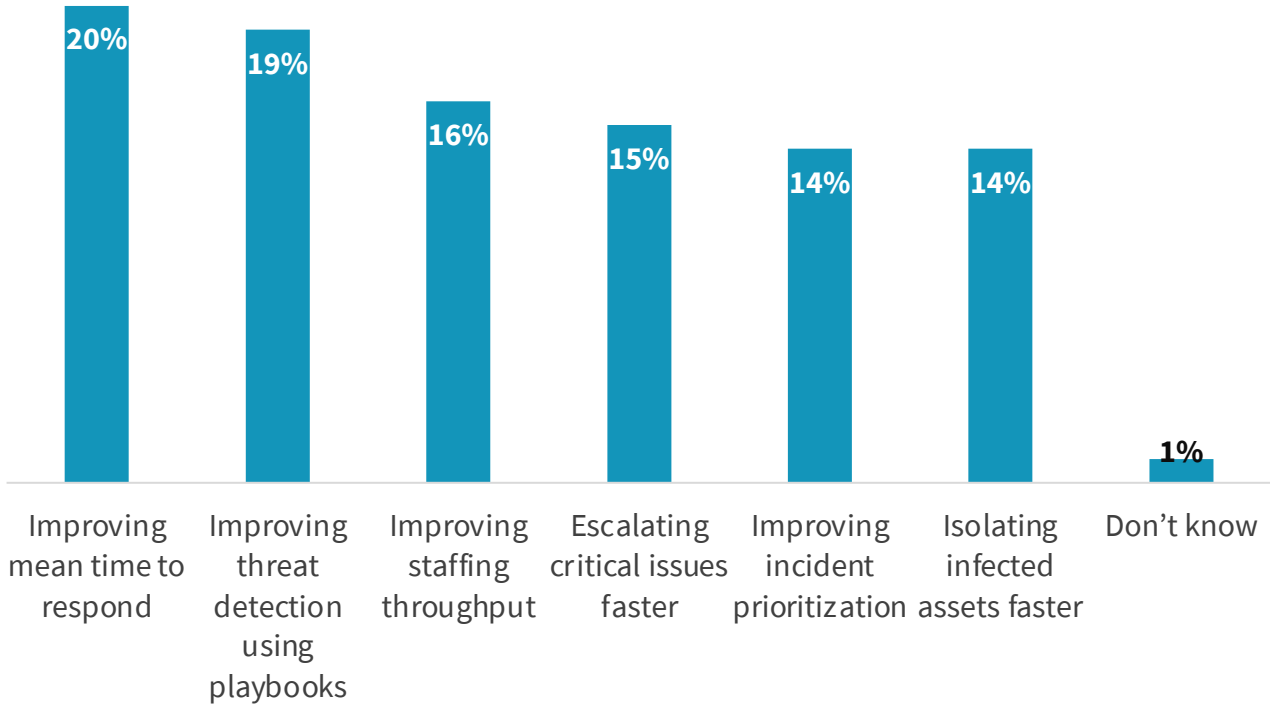
Trend 2: SecOps Process Automation Investments Are Proving Valuable

Most Have Already Invested in SOC Automation

While strategies vary, 90% are investing

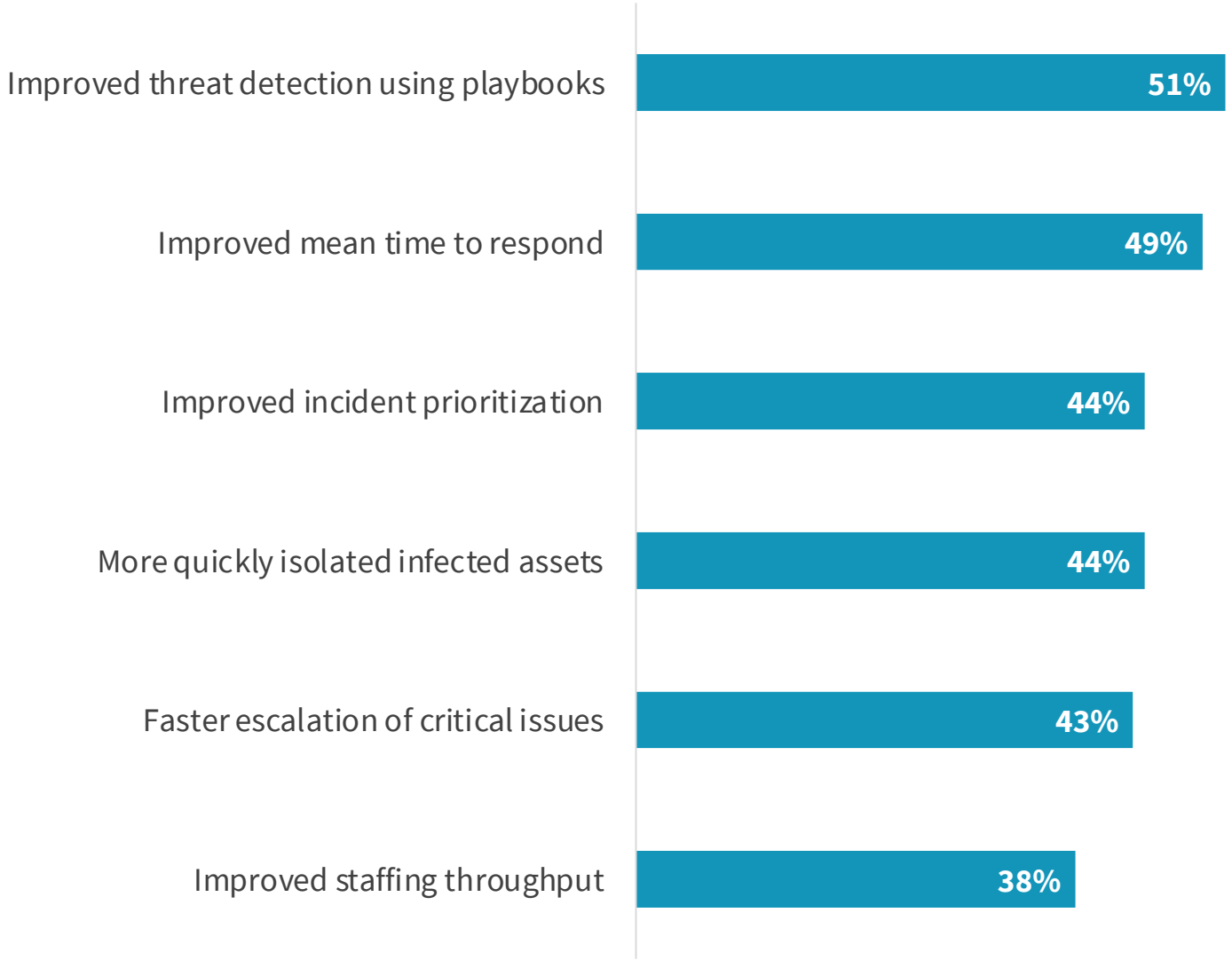


Question text: Is your organization actively automating security operations processes? (Percent of respondents, N=376)

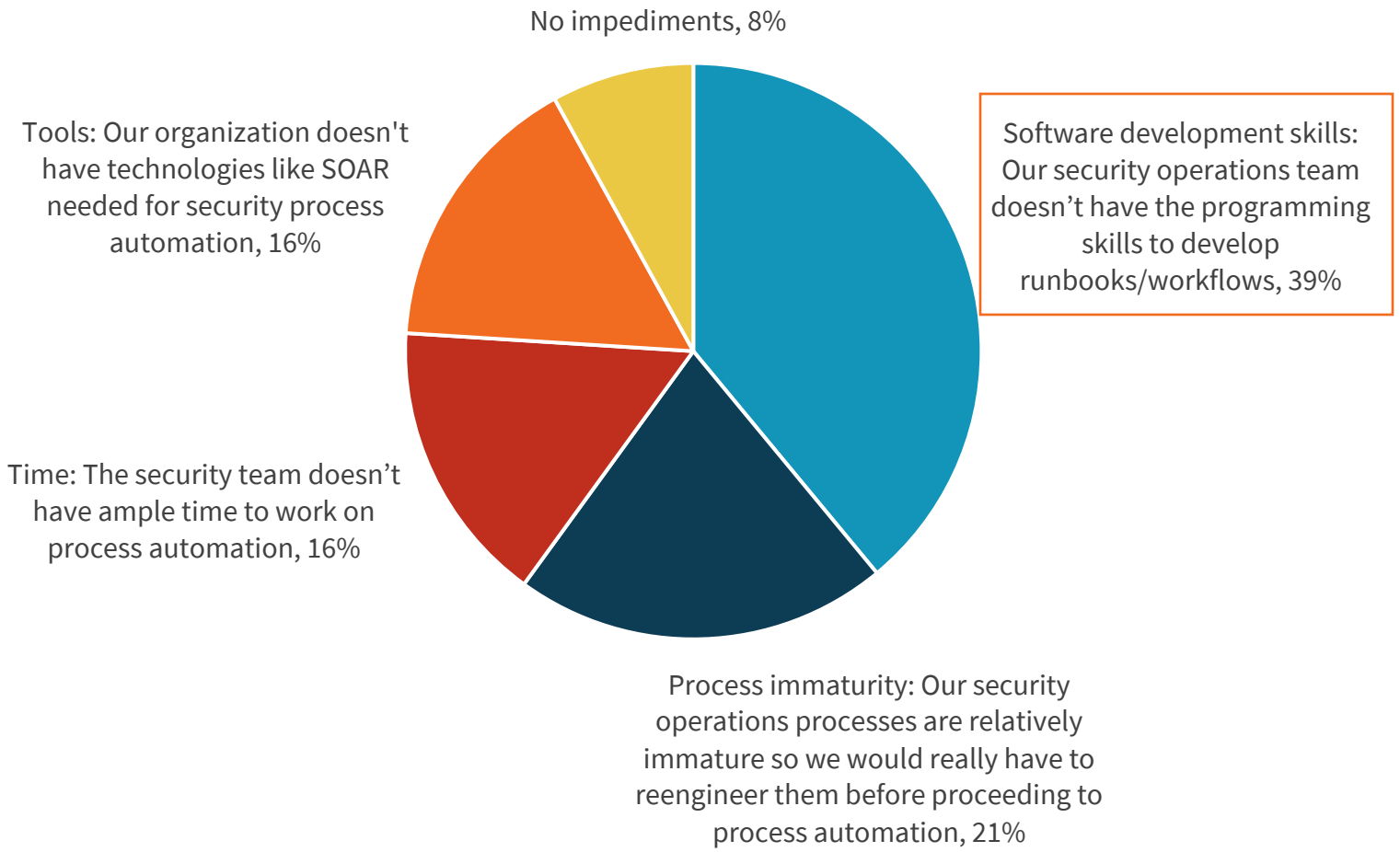


Question text: What was your organization's primary objective for automating its security operations processes? (Percent of respondents, N=338)

Automation Investments Are Proving Valuable



Question text:
How have your organization's security operations improved as a result of automating processes? (Percent of respondents, N=338, multiple responses accepted)



Question text: Which of the following factors represents the biggest impediment to security operations process automation? (Percent of respondents, N=338)

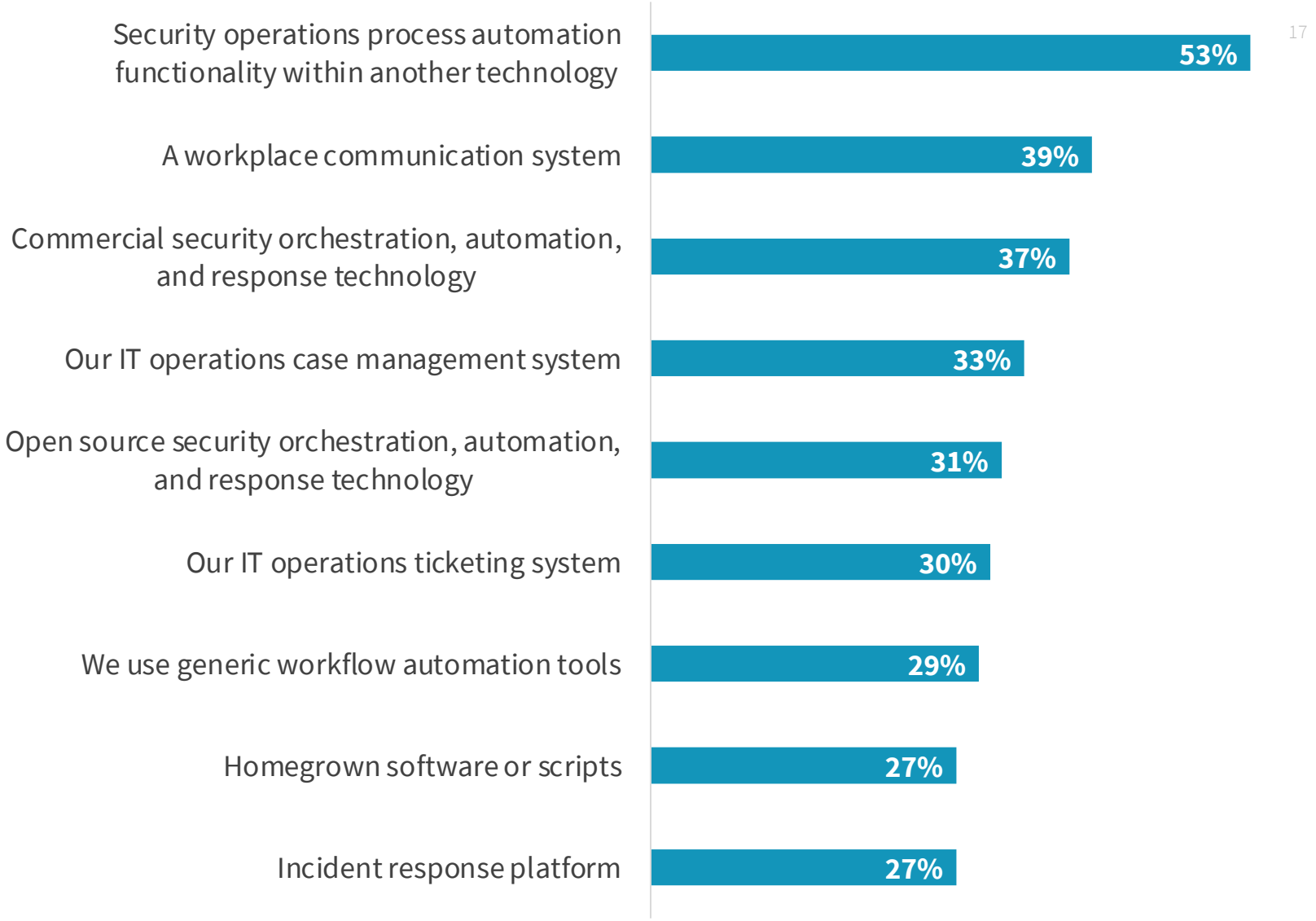
Challenges Still Exist for Many

Current automation required ongoing engineering skills to maintain, yet 1/3+ lack skills.

Half Leverage Process Automation within Existing Tools

1/3+ leverage commercial SOAR.

What's the glue between?

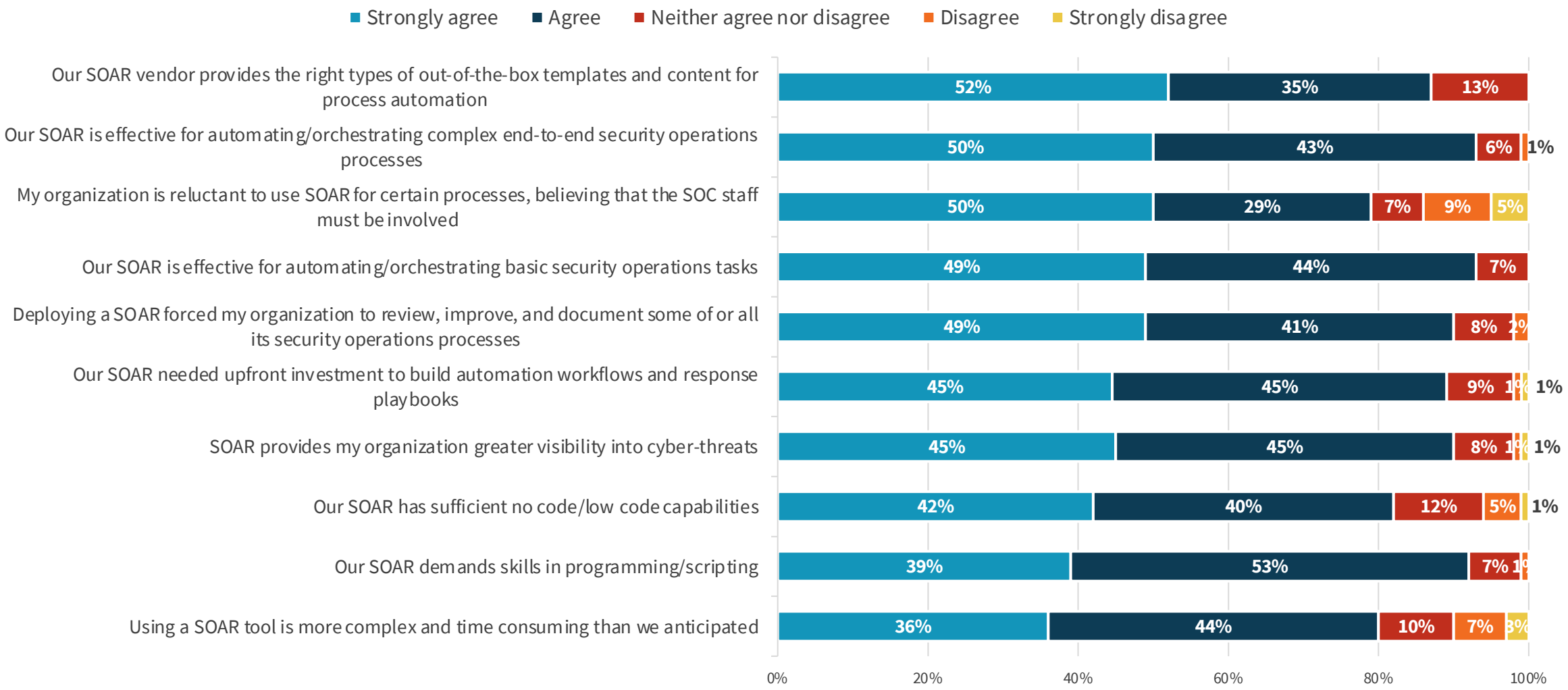


Question text:
Which of the following technologies does your organization currently use to automate security operations processes? (Percent of respondents, N=338, multiple responses accepted)

Many SOAR Use Cases Supported

Question text:
For which of the following activities does your organization use its SOAR? (Percent of respondents, N=187, multiple responses accepted)

Most Are Generally Positive, but SOAR Challenges Exist

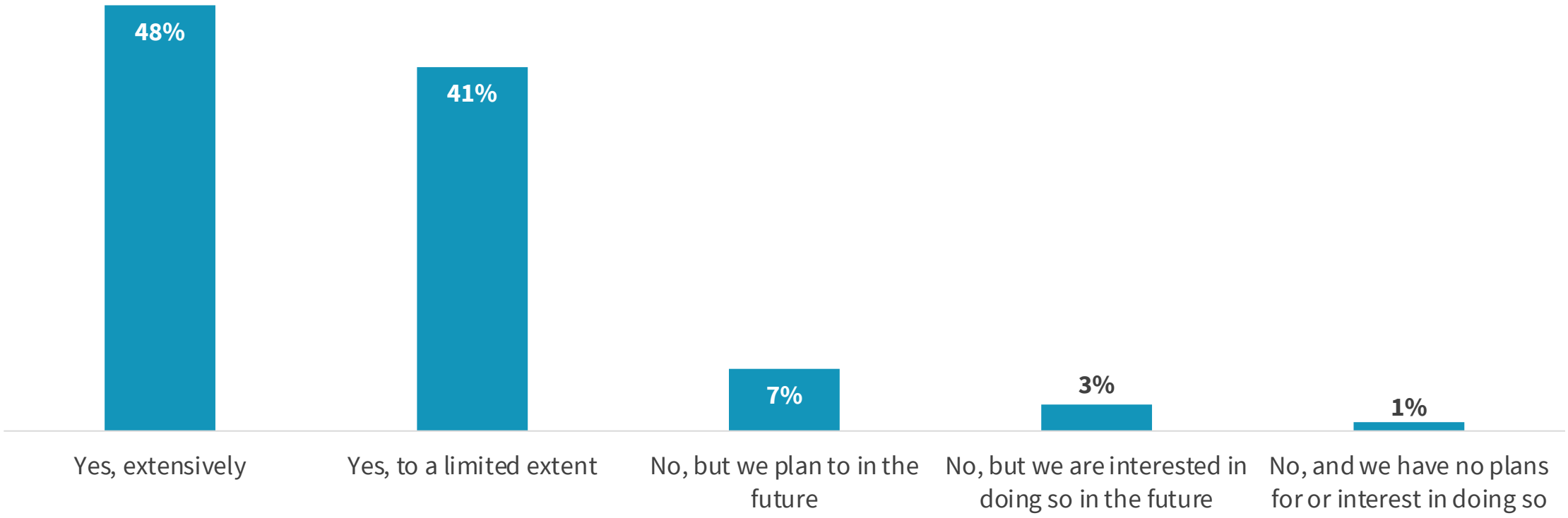


Question text: Please indicate your level agreement with each of the following statements regarding your organization's SOAR implementation. (Percent of respondents, N=187)

Modernizing Security Operations: *5 Key Trends*

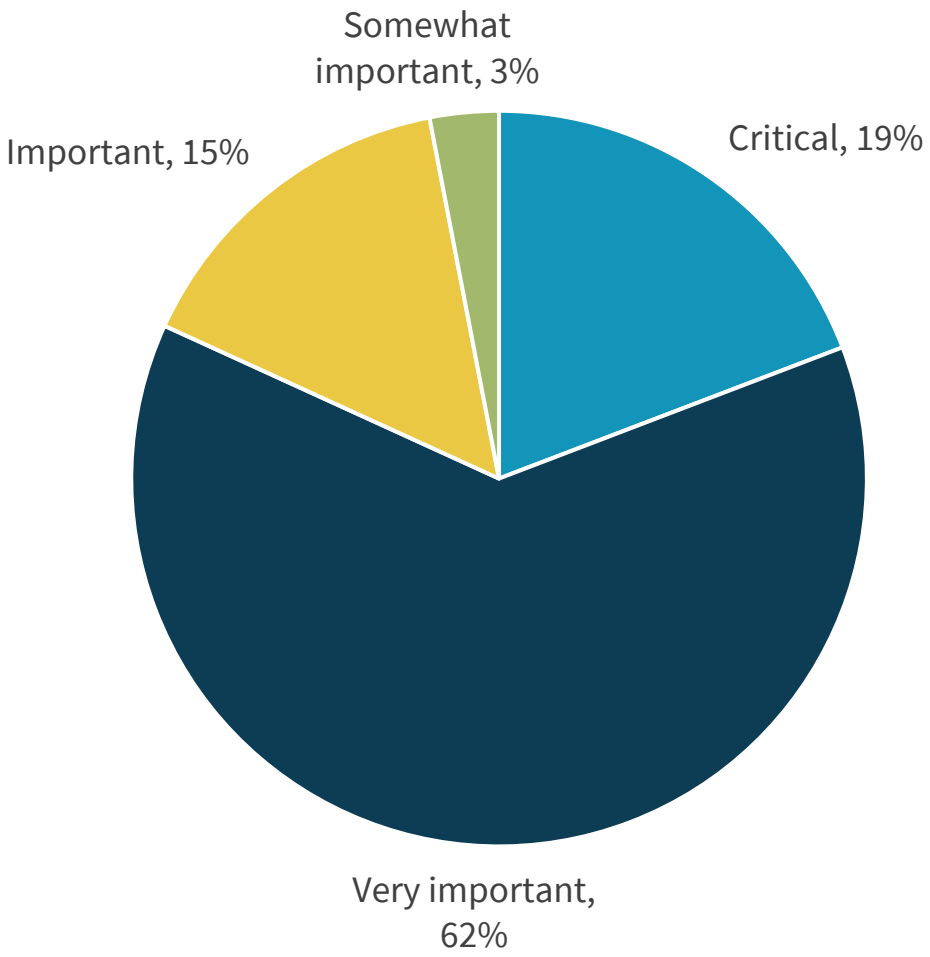
Trend 3: MITRE ATT&CK Framework Is Proving Valuable for Most

MITRE ATT&CK Becoming Mainstream, Yet Many Still Figuring it Out



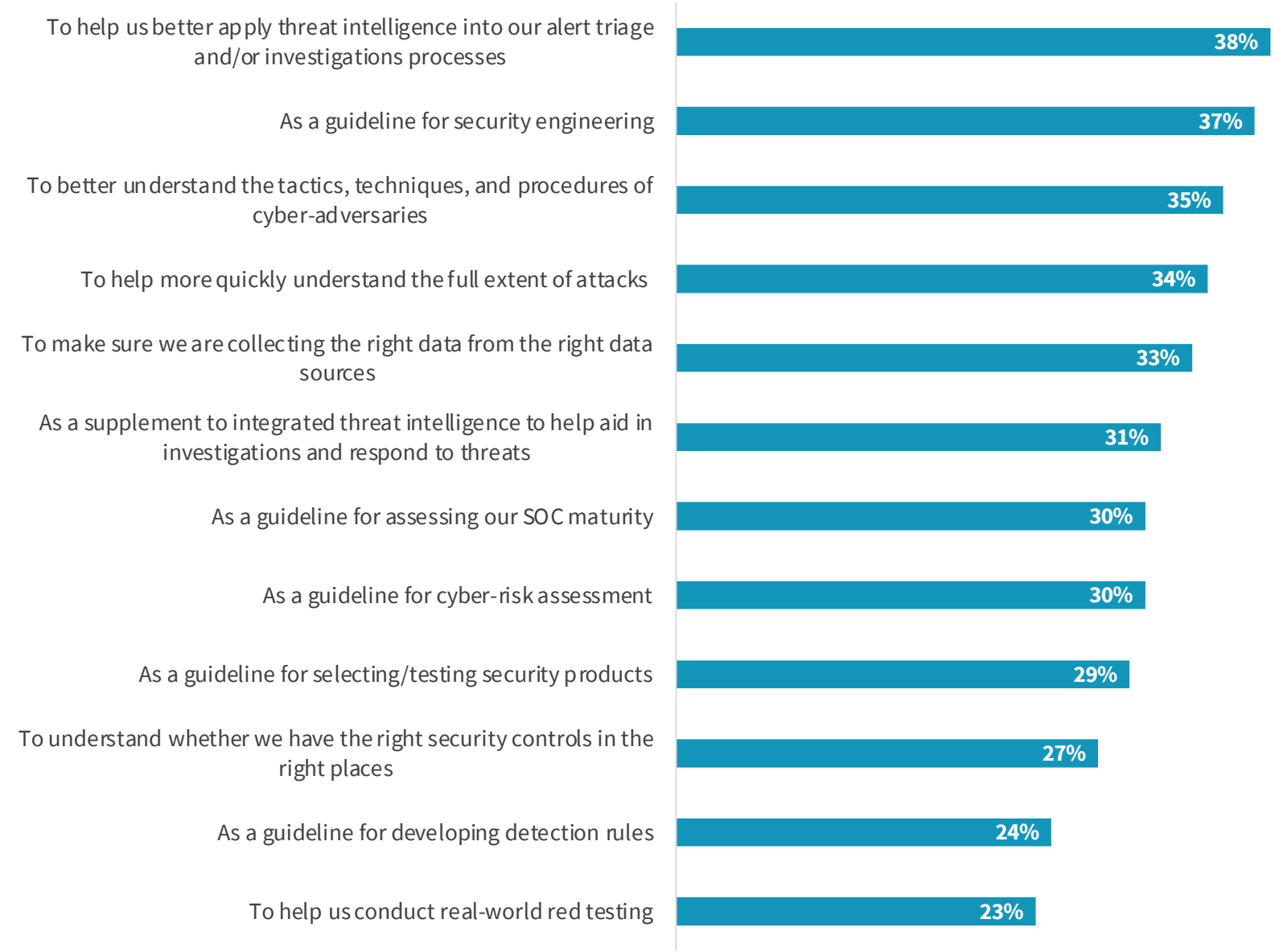
Question text: Does your organization utilize the MITRE ATT&CK framework for security operations? (Percent of respondents, N=376)

Most See Growing Value from Use of MITRE ATT&CK Framework



Question text: As you look forward, how important is the MITRE ATT&CK framework (and derivative MITRE projects like D3FEND) in your organization's overall security operations strategy? (Percent of respondents, N=374)

Many Use Cases are Evolving for MITRE ATT&CK

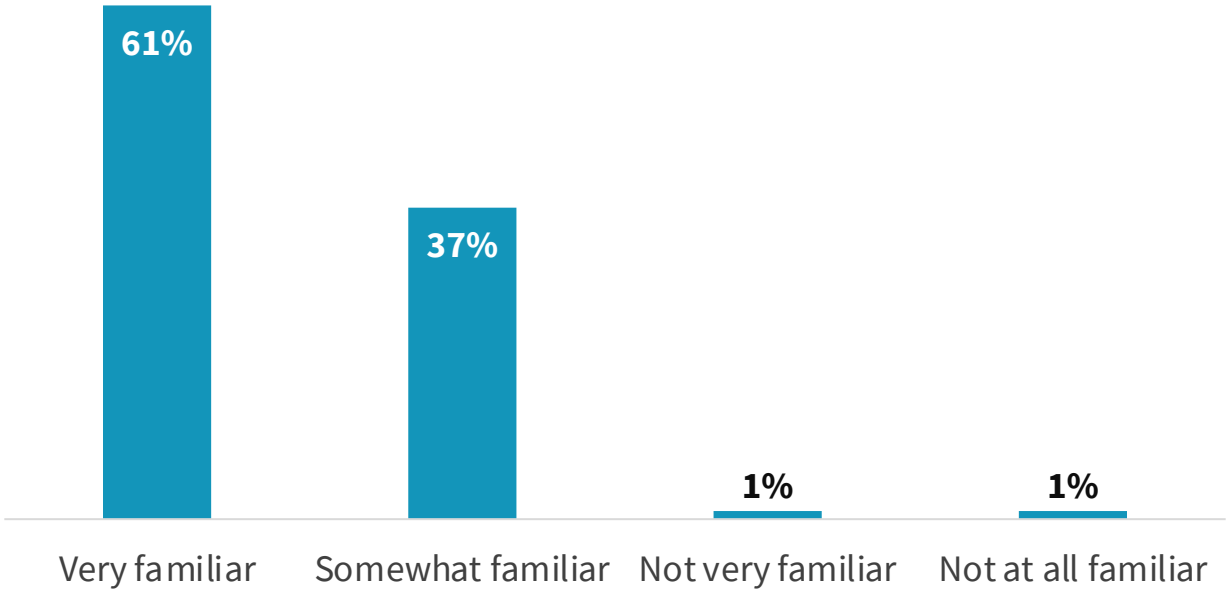


Question text:
You indicated that your organization utilizes the MITRE ATT&CK framework for security operations. Which of the following are ways your organization is utilizing MITRE ATT&CK? (Percent of respondents, N=335, multiple responses accepted)

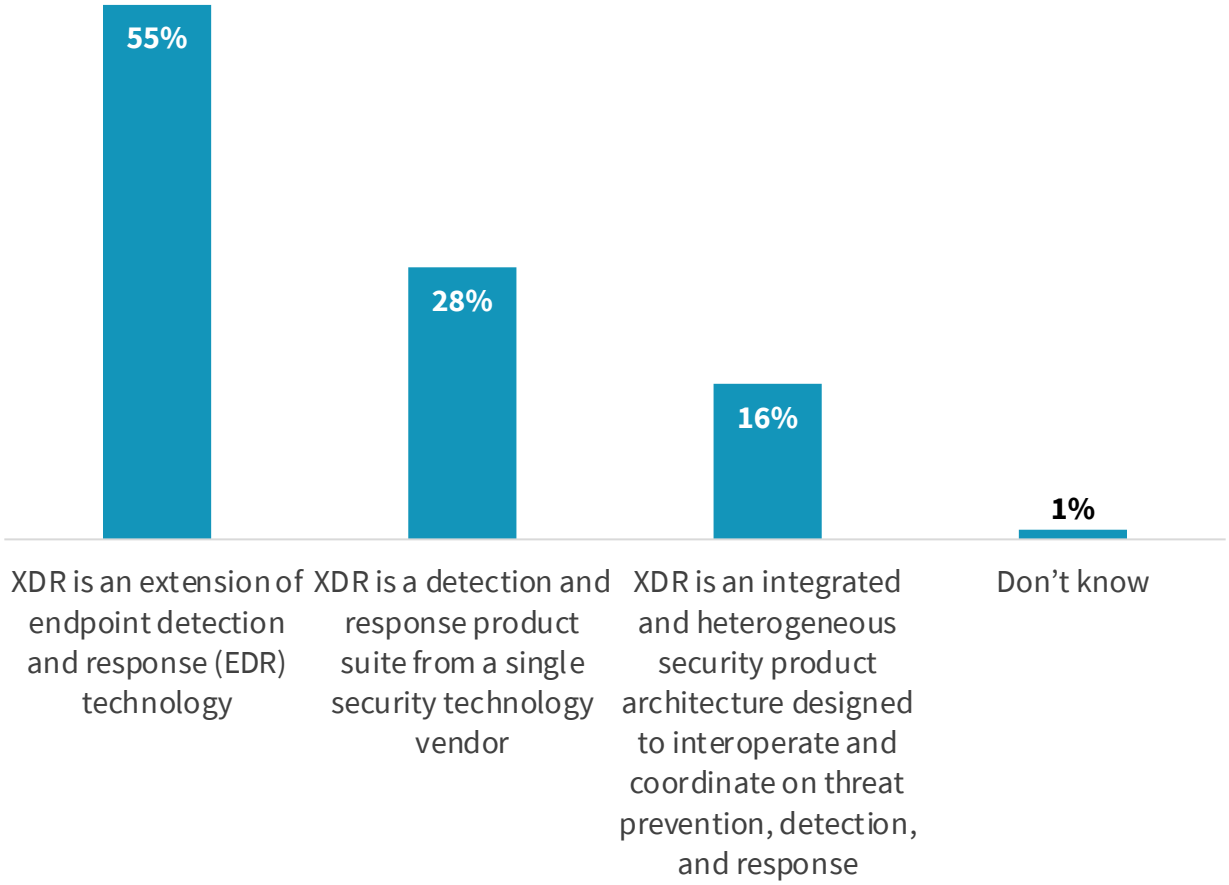
Modernizing Security Operations: *5 Key Trends*

Trend 4: XDR Momentum Continues to Build

XDR Awareness Continues to Grow Fast Despite Varying Definitions



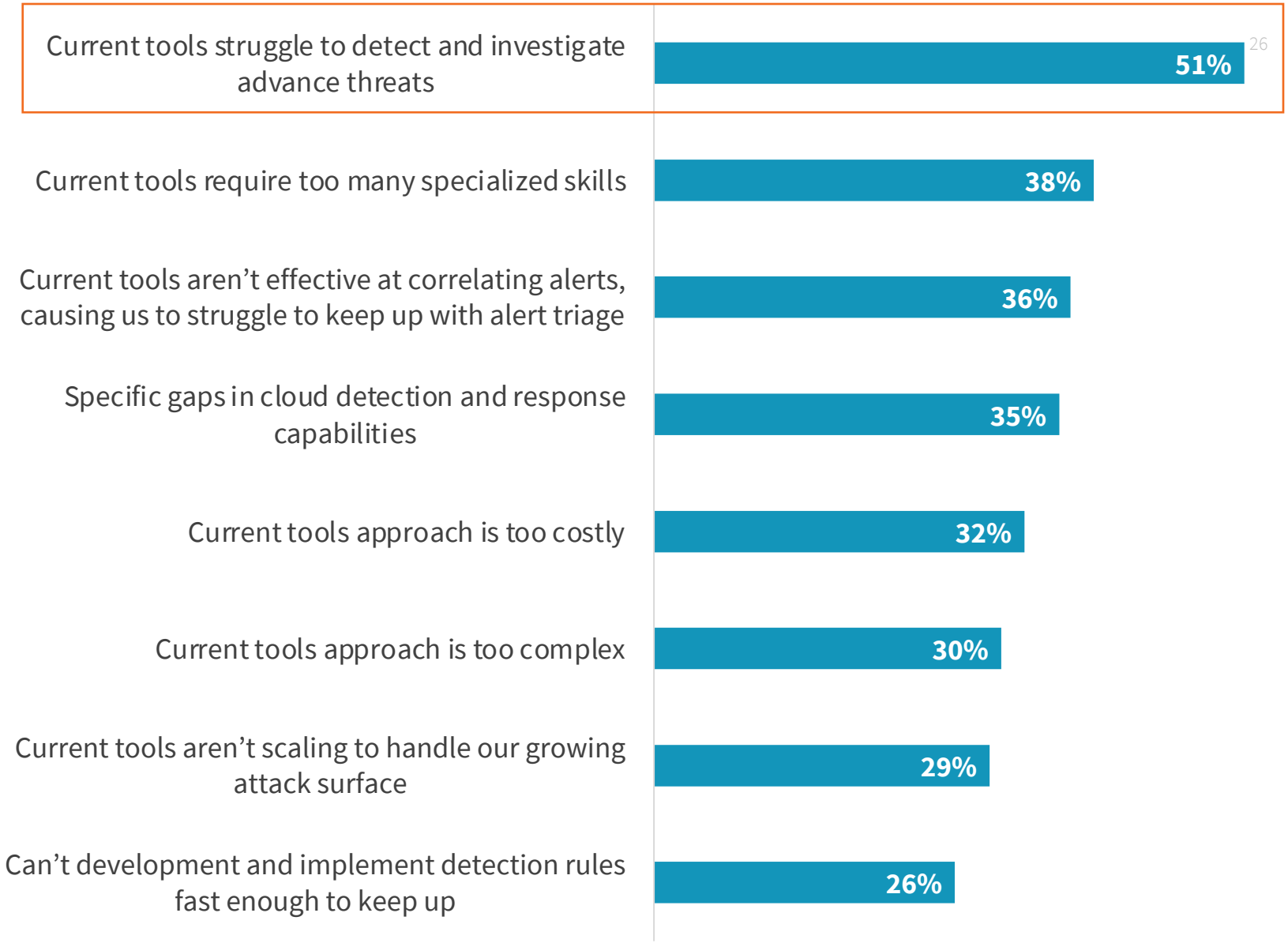
Question text: How familiar are you with extended detection and response (XDR) technology? (Percent of respondents, N=376)



Question text: In your opinion, which of the following most closely aligns with your organization's definition of XDR? (Percent of respondents, N=372)

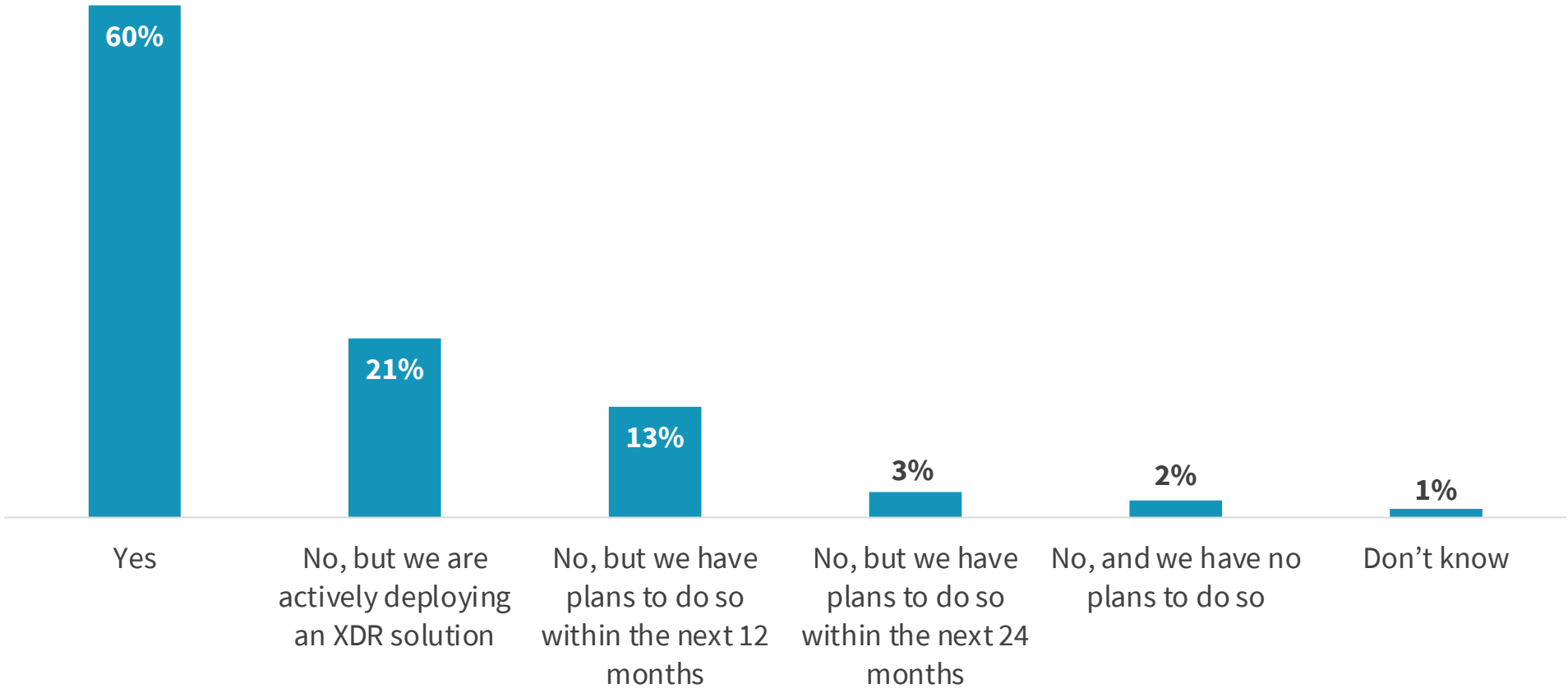
Advanced Threat Detection Still Leads the XDR Agenda

ESG 2020-2021 XDR study reported the same top priority.



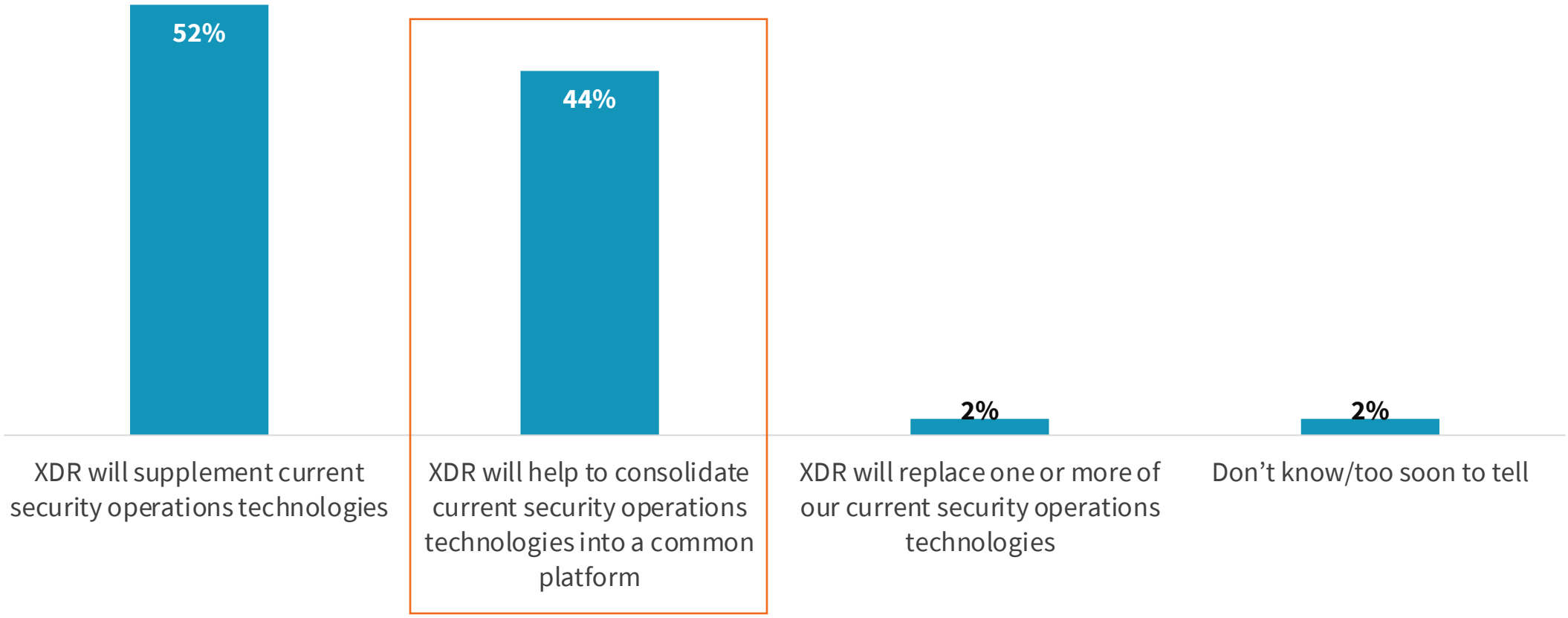
Question text:
What challenges are driving your organization's interest and investment in XDR solutions? (Percent of respondents, N=361, multiple responses accepted)

Despite Many Definitions, Nearly 2/3 Have Deployed XDR



Question text: Has your organization deployed an XDR solution? (Percent of respondents, N=372)

Nearly Half Can See XDR as Their New SOC platform

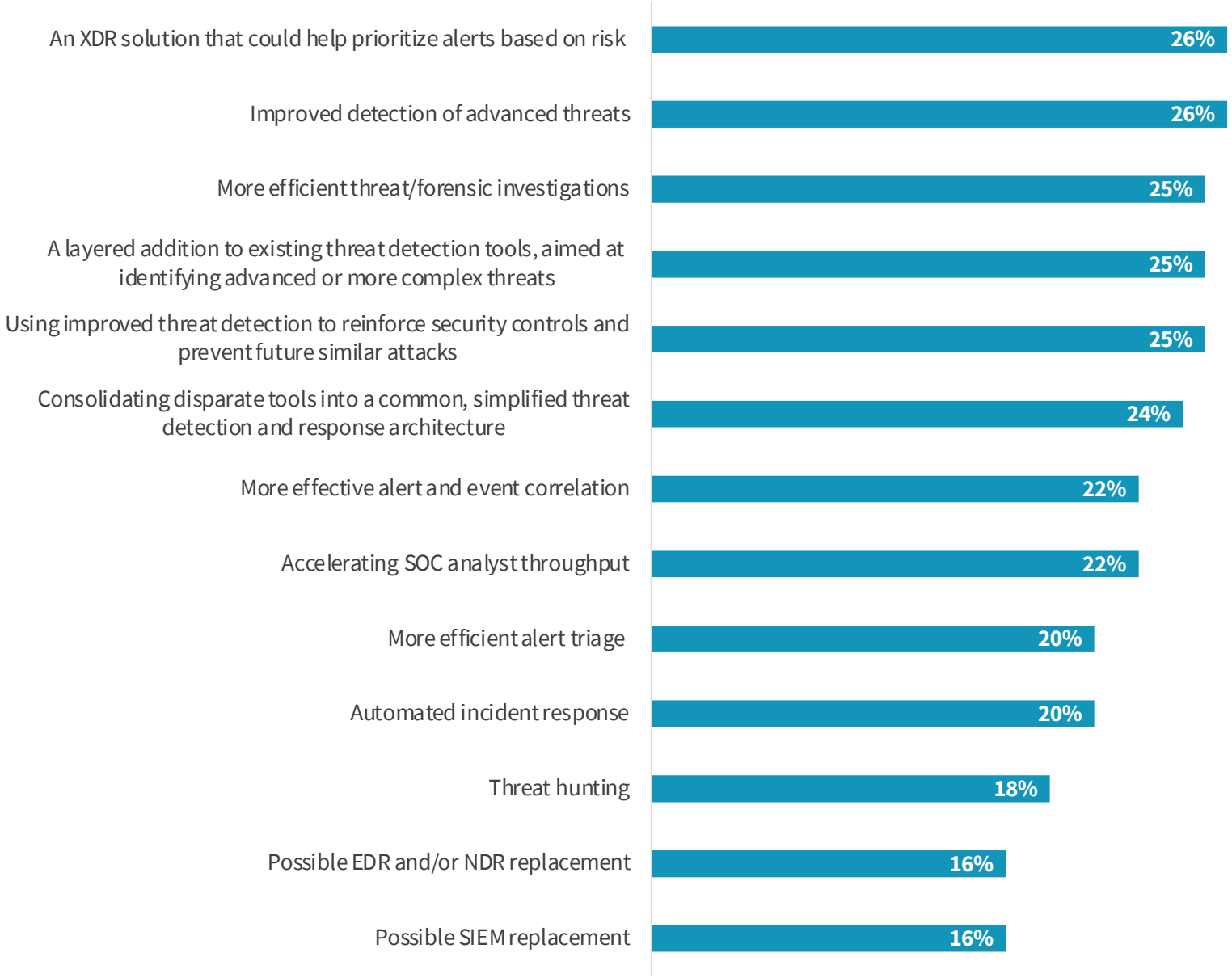


Question text: Which of the following most closely aligns with the impact that you expect XDR to have on your organization's security operations environment? (Percent of respondents, N=361)

But is XDR the Silver Bullet?

"I want it all!"

Highest priority considerations
(3 responses accepted)

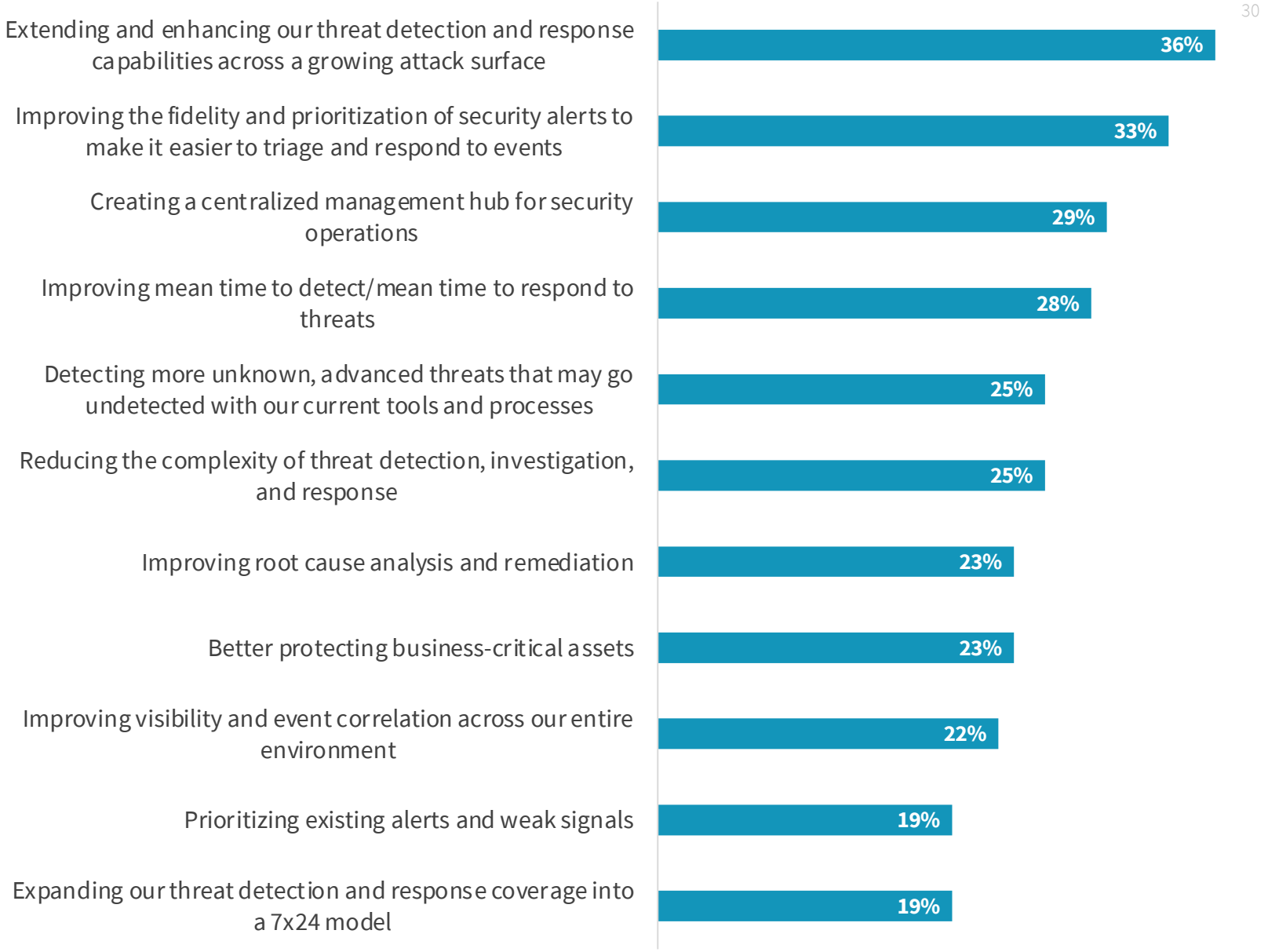


Question text:
Which of the following are, or likely would be, the highest priorities for your organization when considering use cases for XDR? (Percent of respondents, N=361, three responses accepted)

XDR Desired Outcomes:

Better attack surface coverage, triage support, centralized mgmt.

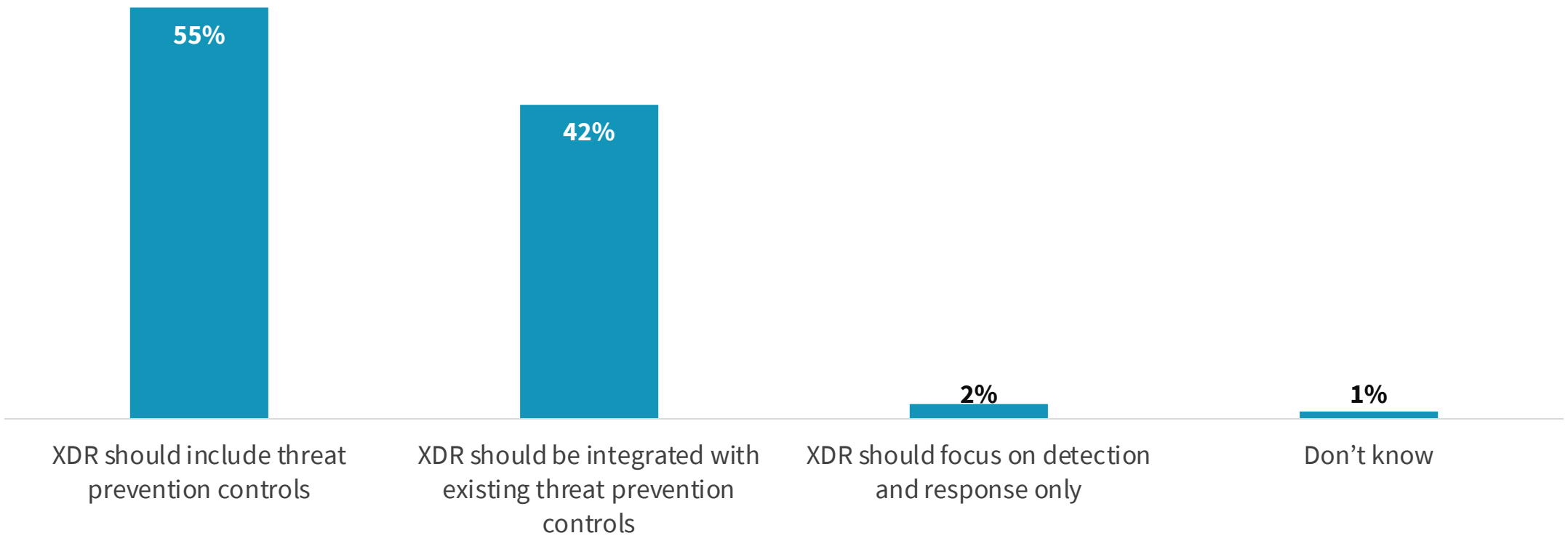
Desired outcomes
(3 responses accepted)



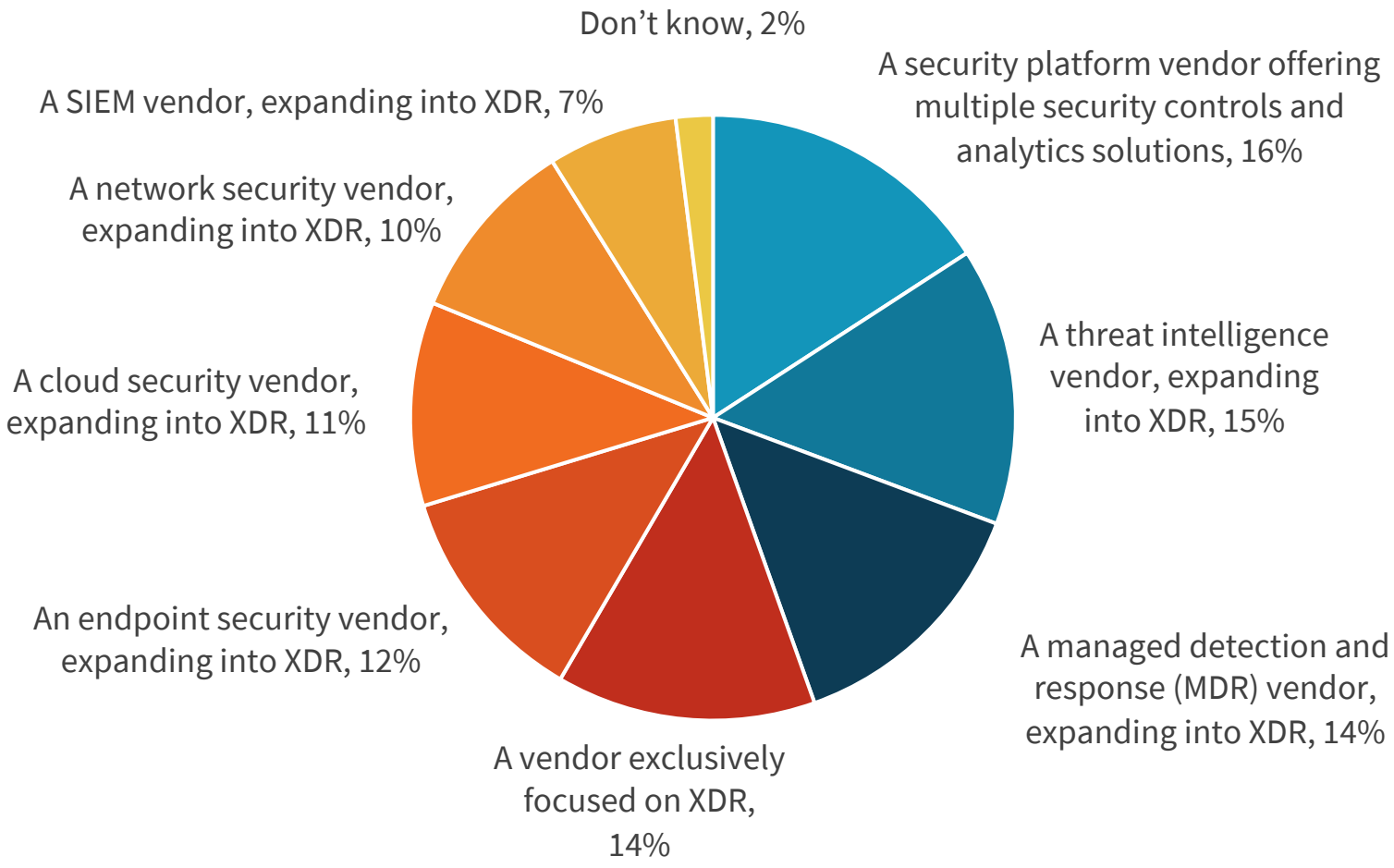
Question text:
What XDR outcomes would be most important for your organization in terms of security efficacy? (Percent of respondents, N=361, three responses accepted)

More than Half Want XDR to Offer Prevention

Again, is XDR a silver bullet?



Question text: What role should XDR play regarding threat prevention controls (i.e., security tools like antivirus software, firewalls, email gateways, web gateways, etc.) designed to block known malicious files, connections, emails, etc.? (Percent of respondents, N=361)



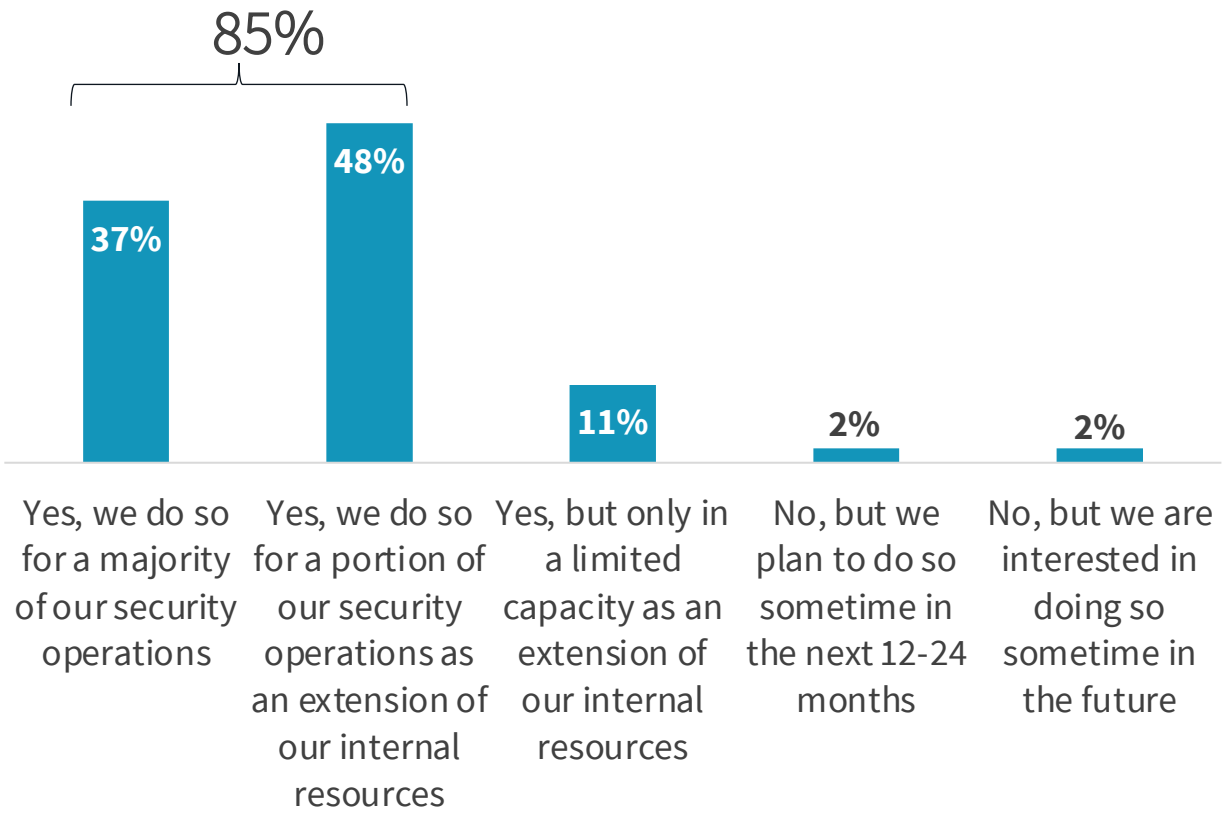
Question text: If your organization were to make an XDR technology purchase tomorrow, from which of the following would it be the likeliest to purchase? (Percent of respondents, N=361)

Aligned with Previous ESG Research, Still No Preference for XDR Providers

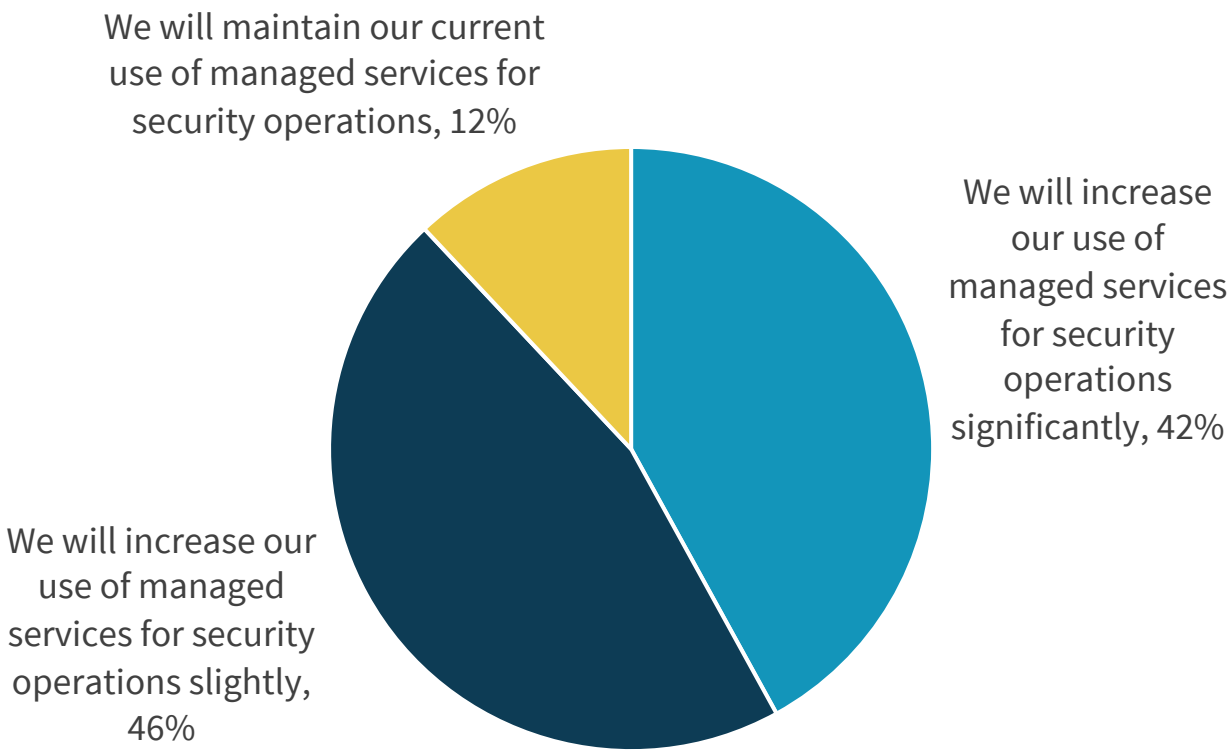
Modernizing Security Operations: *5 Key Trends*

Trend 5: The Use of MDR Is Mainstream and Expanding

The Use of MDR Is Mainstream… and Increasing



Question text: Does your organization currently or plan to use managed services for security operations? (Percent of respondents, N=376)



Question text: Which of the following best describes your organization's likely approach to using managed services over the next 12-24 months? (Percent of respondents, N=361)

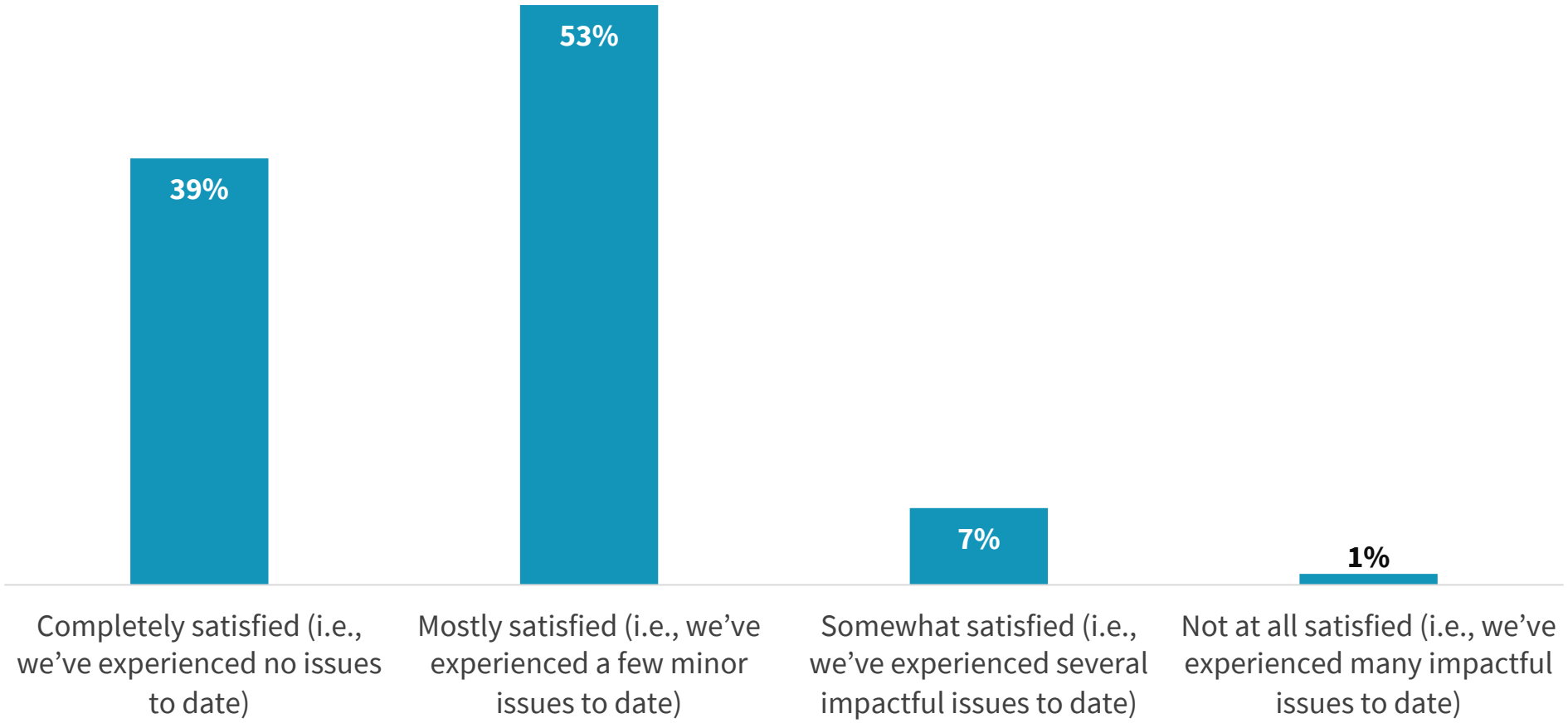
Why MDR?

Use cases vary, but more than half want employees focused on more strategic security initiatives.

Others lack skills or coverage.

Question text:
What are the primary reasons behind your organization's usage of or plans for managed services? (Percent of respondents, N=368, multiple responses accepted)

MDR Satisfaction Is High



Question text: How satisfied is your organization with its current managed security service provider(s)? (Percent of respondents, N=361)

Security Operations Investment Outcomes & Future Plans

Investment Outcomes and Future Plans

Most report that their security program is improving

1. 38% report significant progress; 45% good progress, but still have significant gaps.
2. Better efficiency, fewer breaches/compromises, better attack surface coverage, improved MTTD/MTTR

Biggest SecOps improvements

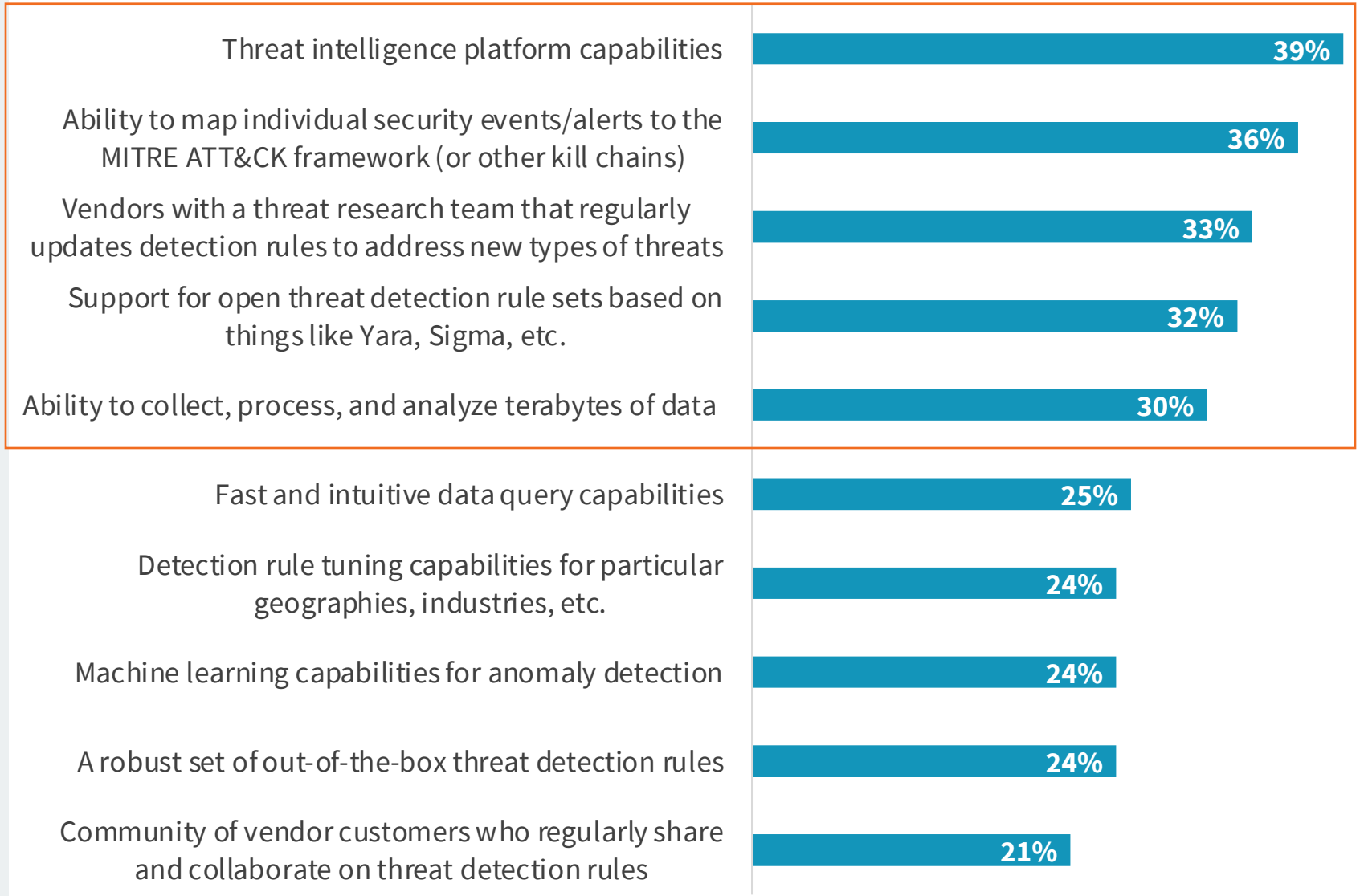
1. Tools consolidation (47%)
2. More scalable cloud analytics (44%)
3. Detection rules (43%)
4. Skills training (44%)

Improving SecOps is a Priority and is Funded

1. 88% will spend more this year
2. 66% report tools consolidation is a priority (cost is the key driver)
3. Modern applications development and deployment has increase velocity requiring new skills

What's most important when evaluating future TDR Solutions?

1. Threat intel
2. Support for MITRE ATT&CK mapping
3. More detection rules
4. Scalability needed to support more data



Question text:
When evaluating threat detection and response solutions, which of the following considerations are most important to your organization? (Percent of respondents, N=376, three responses accepted)

SOC Improvement Plans

This Year's Initiatives

1. Improve operationalization of threat intelligence
2. Improve integration of asset management data
3. Improve alert and risk prioritization

Planned Actions

1. Purchase SecOps tools to automate and orchestrate the process
2. Integrated architecture to converge siloed security tools
3. Improve alignment of SecOps and IT Ops to improve IR

Most beneficial for better efficacy and efficiency

1. Improve security hygiene and posture management to reduce attack surface
2. Deploy a common UI as a SecOps workbench
3. Deploy threat detection with advanced analytics

Thank You

Jon Oltsik
Senior Principal Analyst & ESG Fellow

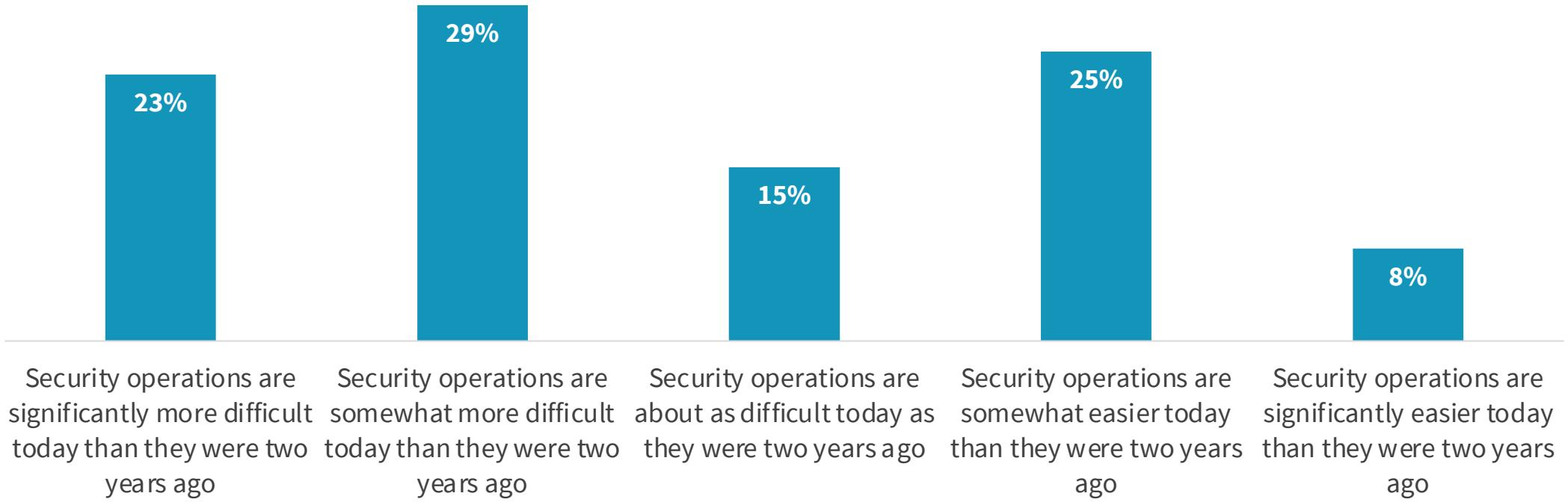
978-501-0862
jon.oltsik@esg-global.com I @esg_global

Dave Gruber
Principal Analyst

508-259-5056
dave.gruber@esg-global.com I @esg_global

Appendix

More Than Half Think SecOps is More Difficult



Question text: Which of the following responses best reflects your opinion about security operations at your organization? (Percent of respondents, N=376)

Why More Difficult?

1. Growing attack surface
2. Threat landscape
3. More cloud usage

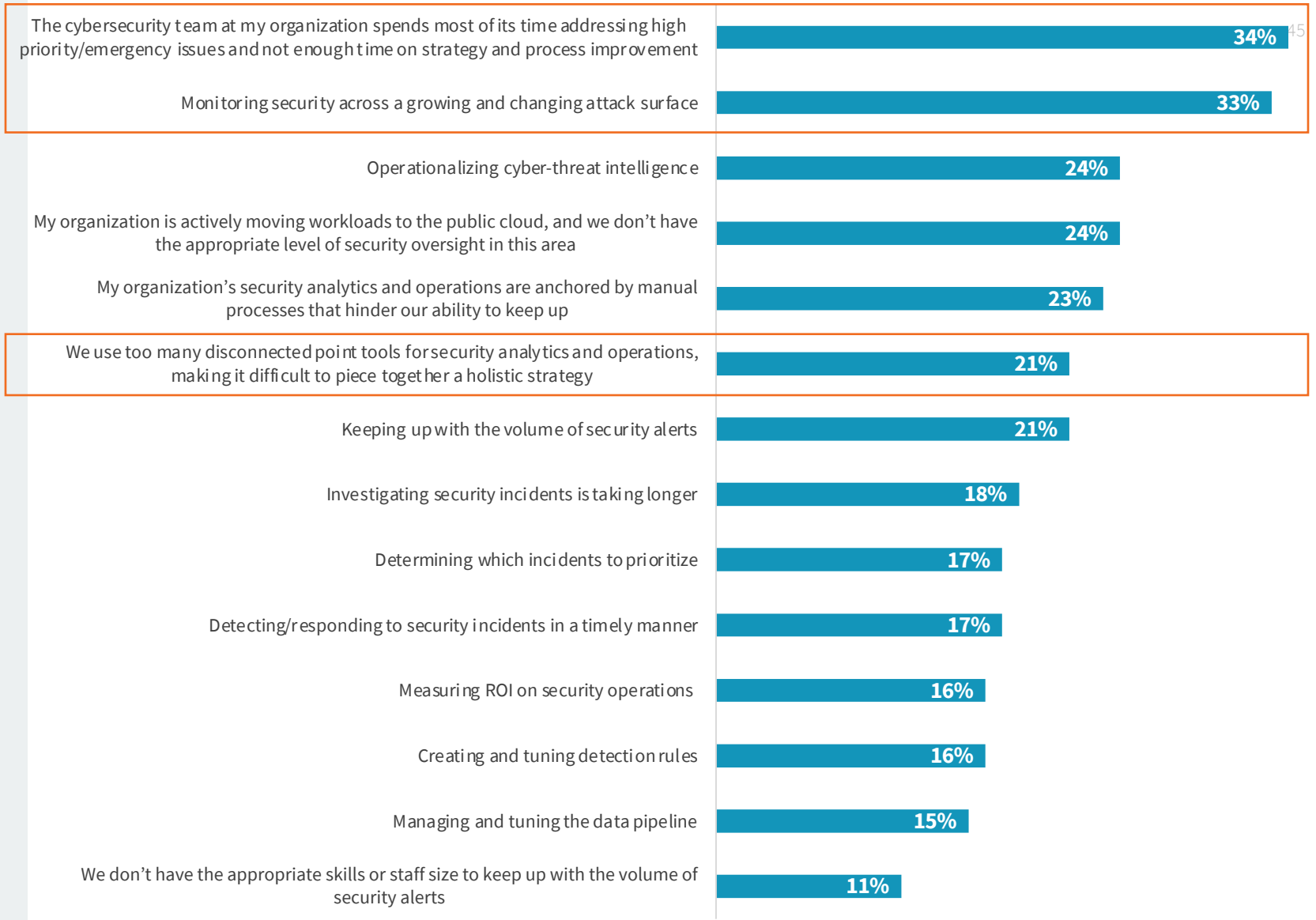
Question text:
You indicated that security operations are more difficult at your organization than they were two years ago. What are the primary reasons you believe this to be true? (Percent of respondents, N=194, multiple responses accepted)

SecOps Challenges:

1. Firefighting leaves no time to improve the program

2. Attack surface growth

Analysis



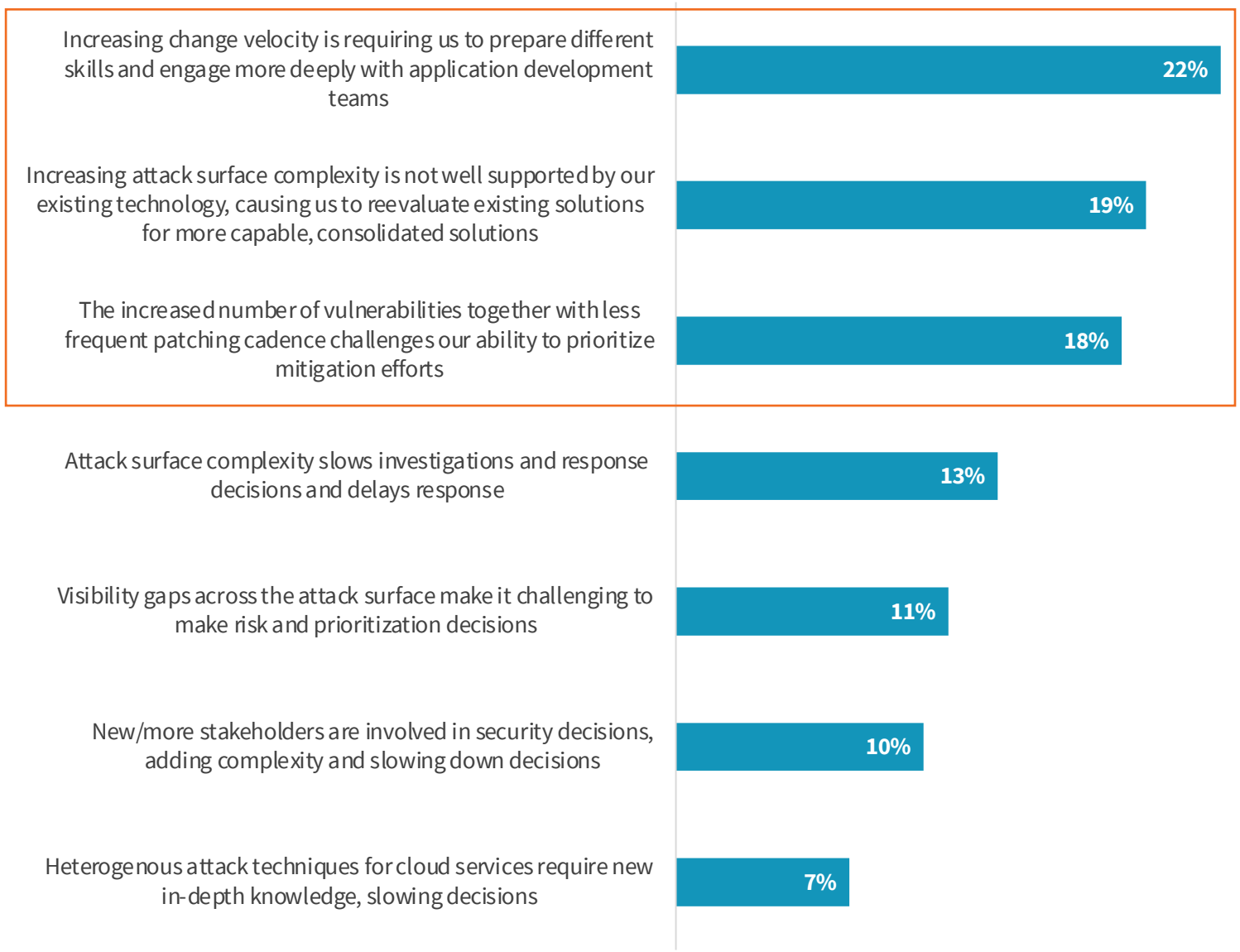
Question text:
Which of the following would you say are your organization's current, primary security operations challenges? (Percent of respondents, N=376, three responses accepted)

The Impact of an Expanding Attack Surface

1. Modern AppDev requires new security skills

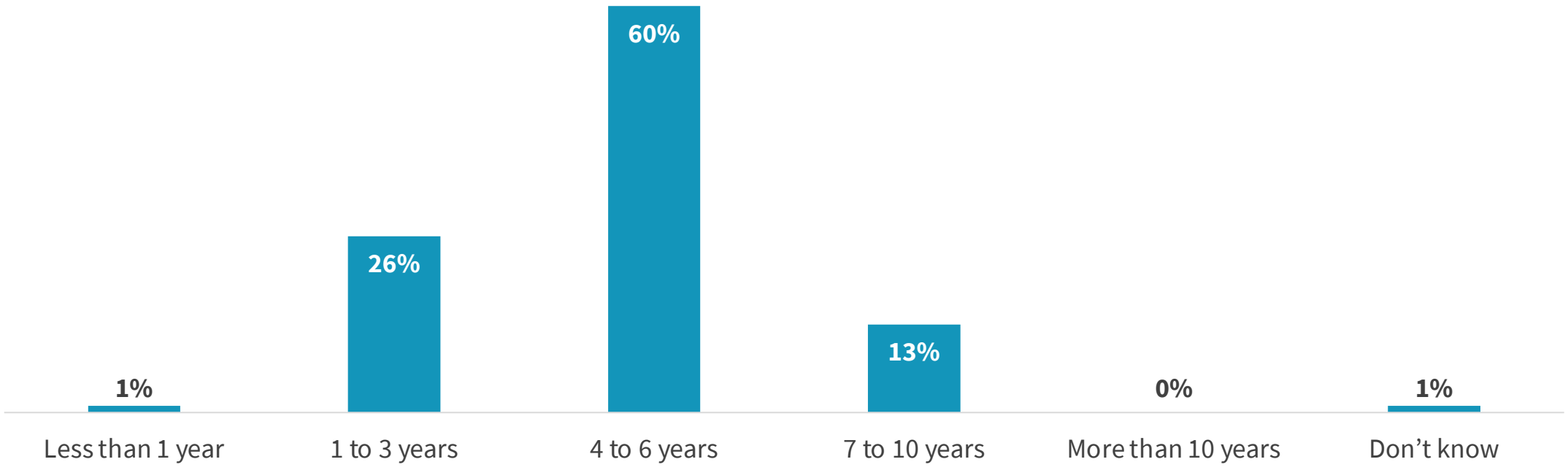
2. Current tools fail to support new attack surface requirements

3. More vulns



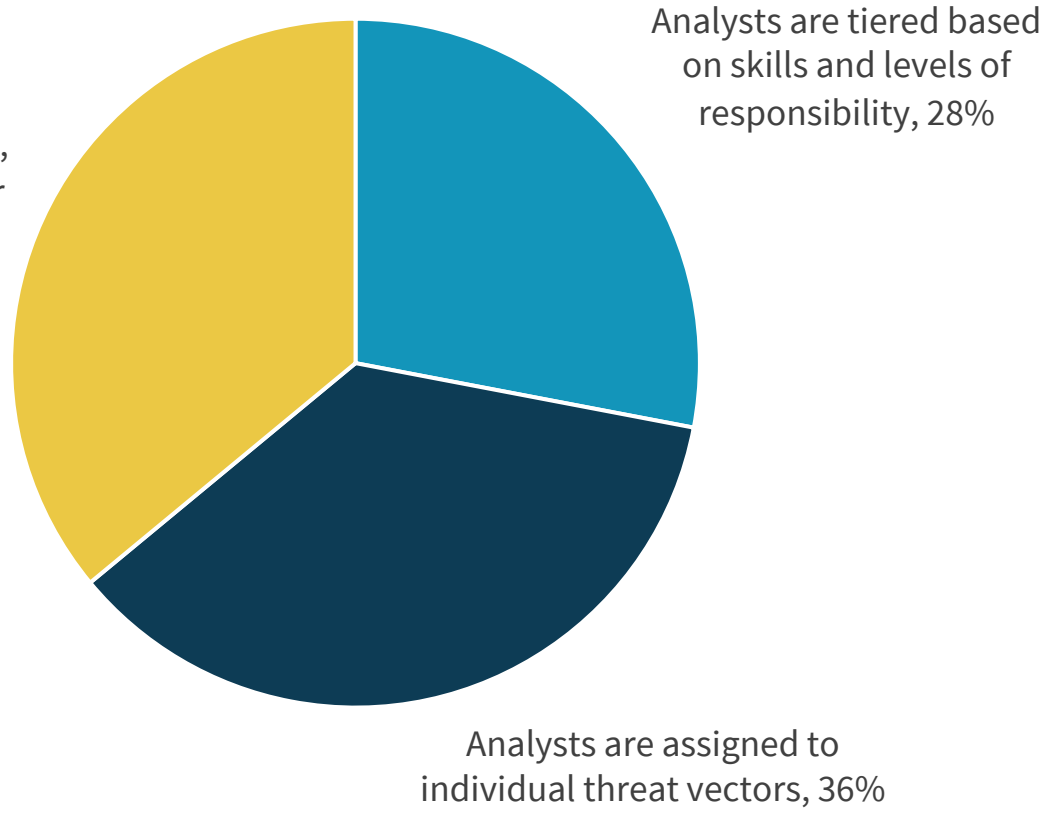
Question text:
What is the most significant impact the expanded attack surface (migration to cloud, work from anywhere, IoT, expanding supply chain, etc.) has had on your organization's security operations and technology decision processes? (Percent of respondents, N=181, one response accepted)

Over 70% have 4+ years of SOC Experience



Question text: Approximately how long has your organization's SOC been in place (i.e., fully established as a SOC, not a collection of tools and staff)? (Percent of respondents, N=376)

SOC Operating Models Vary

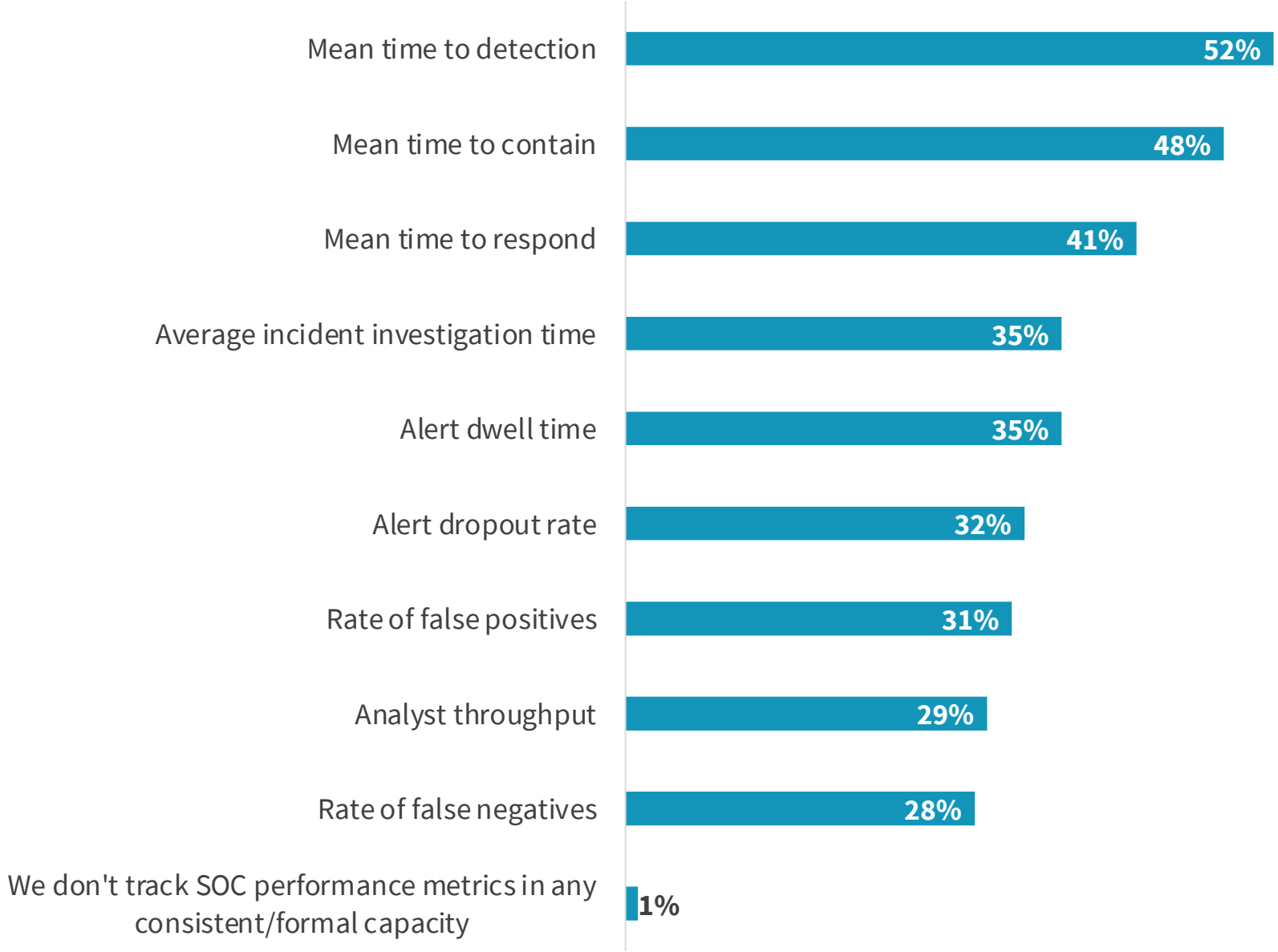


Question text: What is the division of labor within your organization's SOC? (Percent of respondents, N=376)

Regardless of Operating Model, traditional SOC metrics apply

Interesting focus on detection vs. response and dwell times.

Skill shortage. Alert fatigue. Yet rank lower??



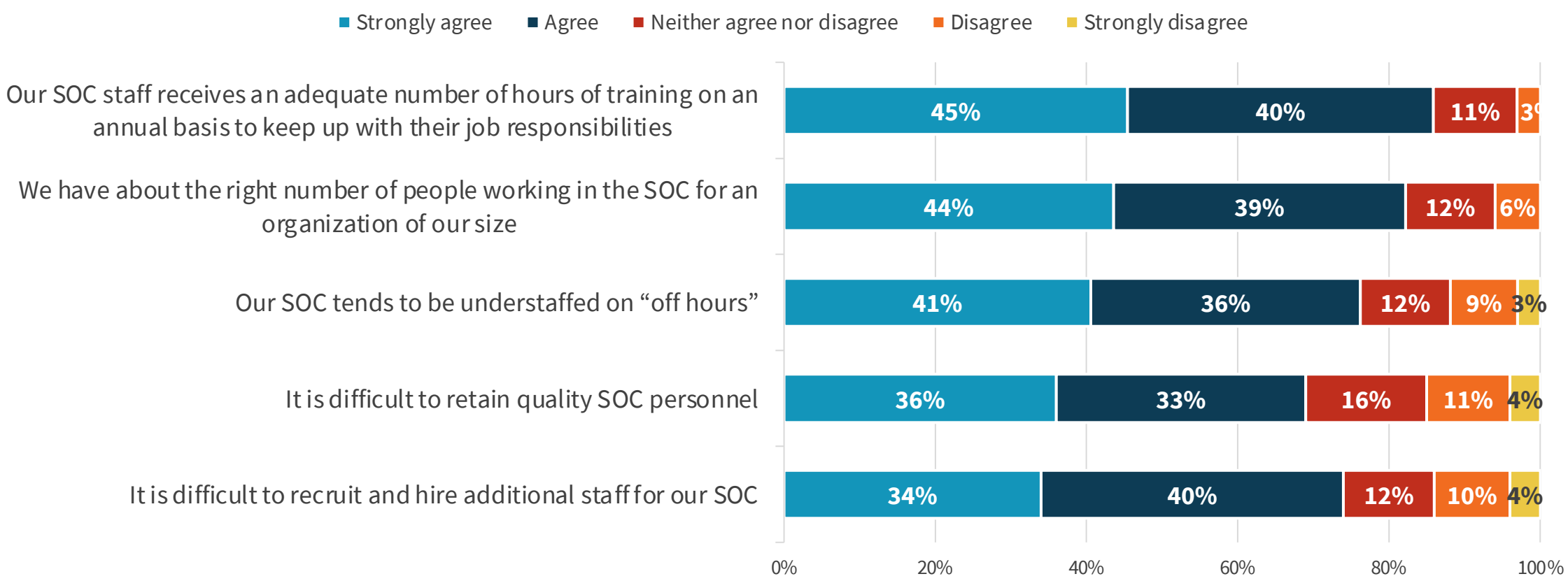
Question text:
Which of the following metrics does your organization's SOC use to measure its effectiveness? (Percent of respondents, N=376, multiple responses accepted)

Skills Gap Continues: Expert skills are in demand

Interesting focus on infrastructure

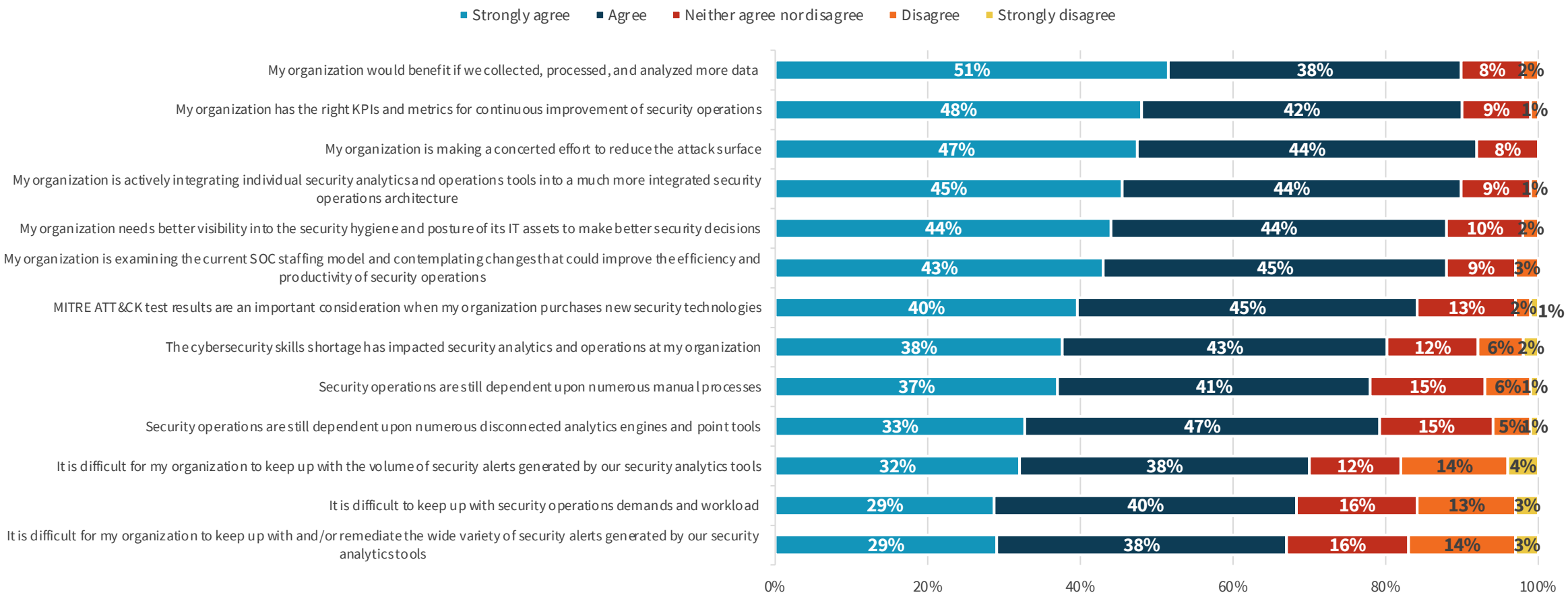
Question text:
Of the following jobs/roles, in which area is your organization most understaffed and/or lacking adequate skills? (Percent of respondents, N=376, multiple responses accepted)

Despite skills shortages, ¾ are happy with staffing, yet gaps after hours



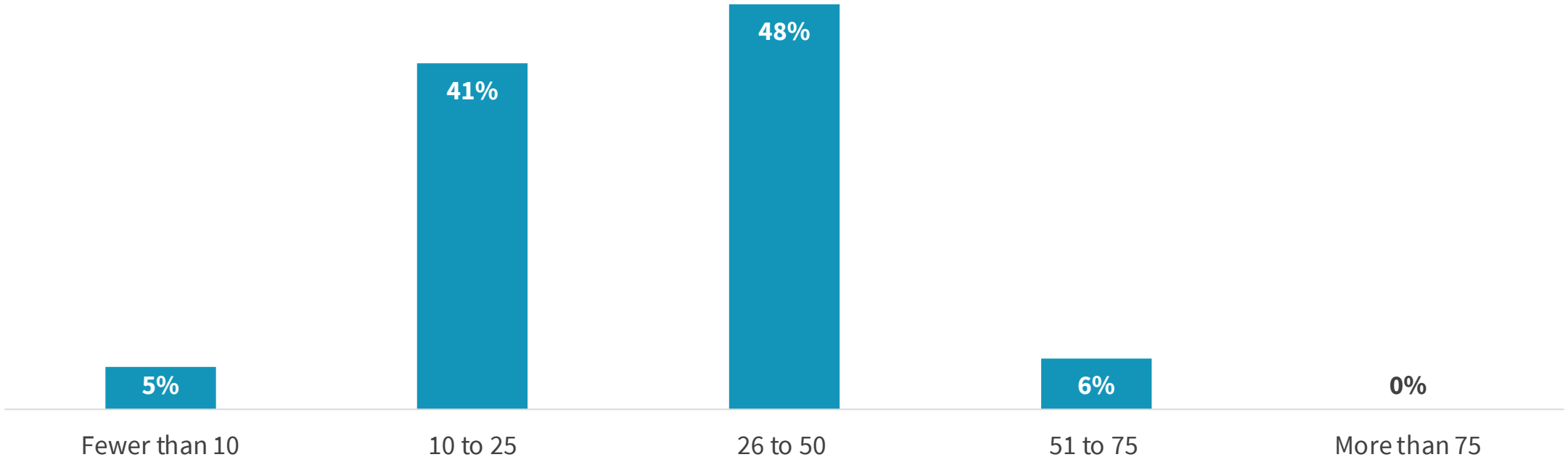
Question text: Please indicate your level of agreement with each of the following statements regarding your organization's SOC personnel. (Percent of respondents, N=376)

Trend 1: More data is desired, while…?



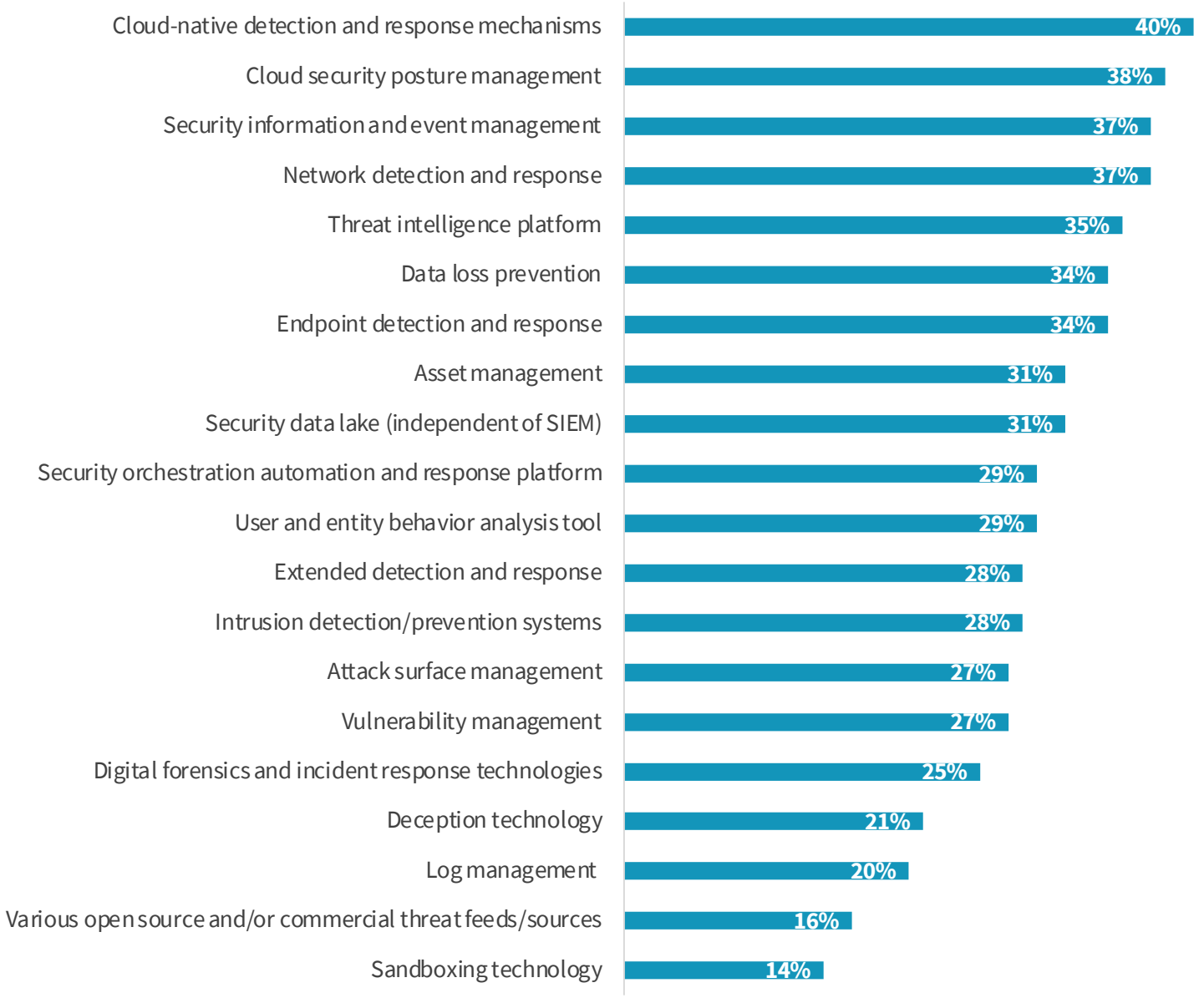
Question text: Please indicate your level of agreement with each of the following statements regarding your organization's security operations environment. (Percent of respondents, N=376)

Security Tools Usage Continues to Grow



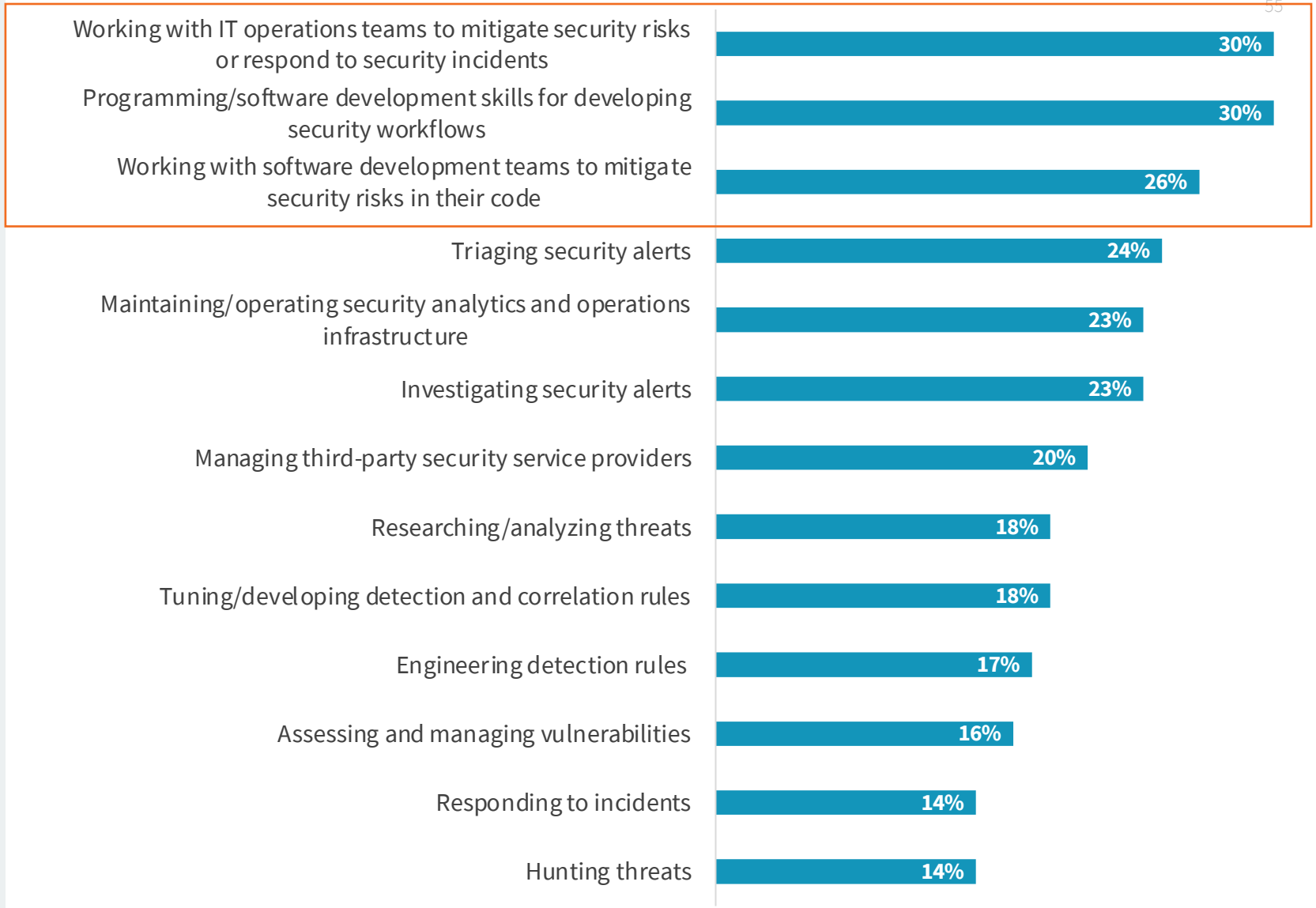
Question text: Approximately how many different tools and technologies (i.e., commercial, homegrown, open source, etc.) are used for security operations at your organization? (Percent of respondents, N=376)

Tools and Technologies Used for SecOps



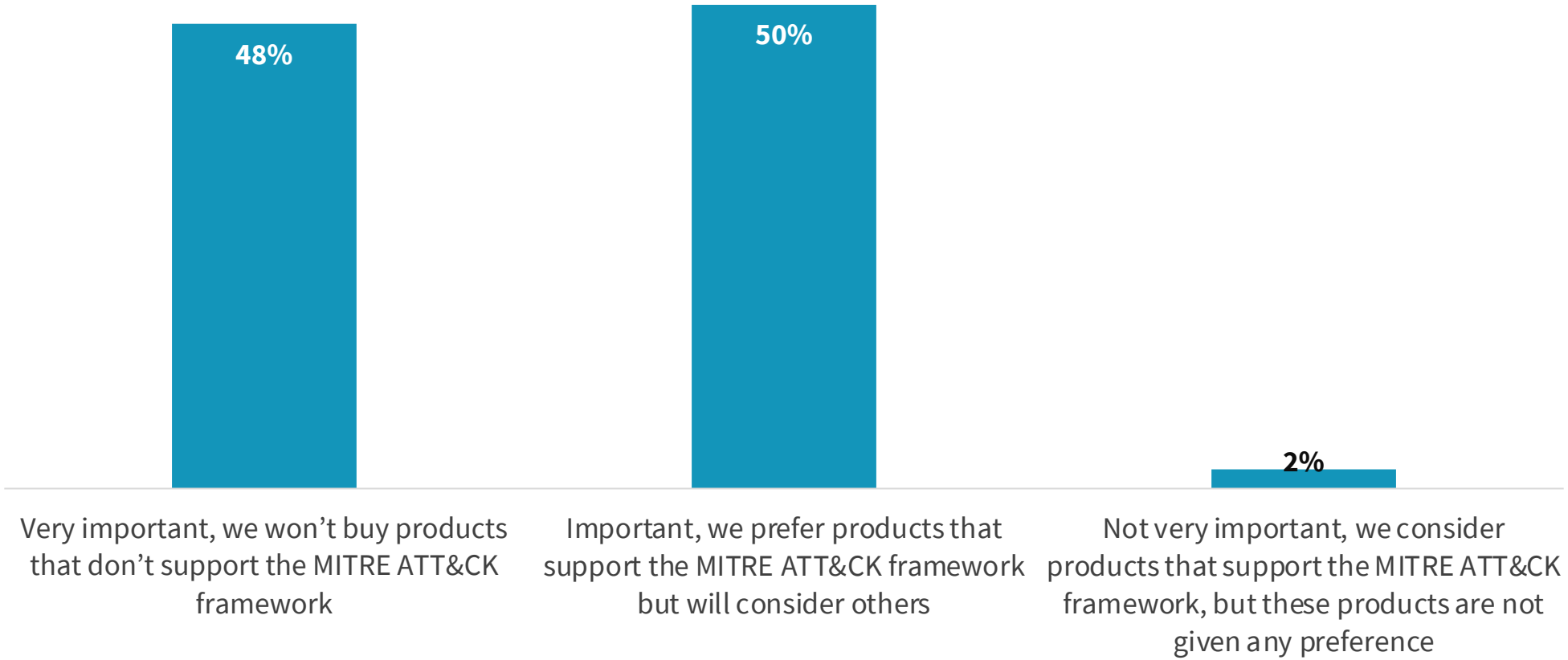
Question text:
Which of the following technologies does your organization currently use for security operations? (Percent of respondents, N=376, multiple responses accepted)

AppSec Skills Issues?



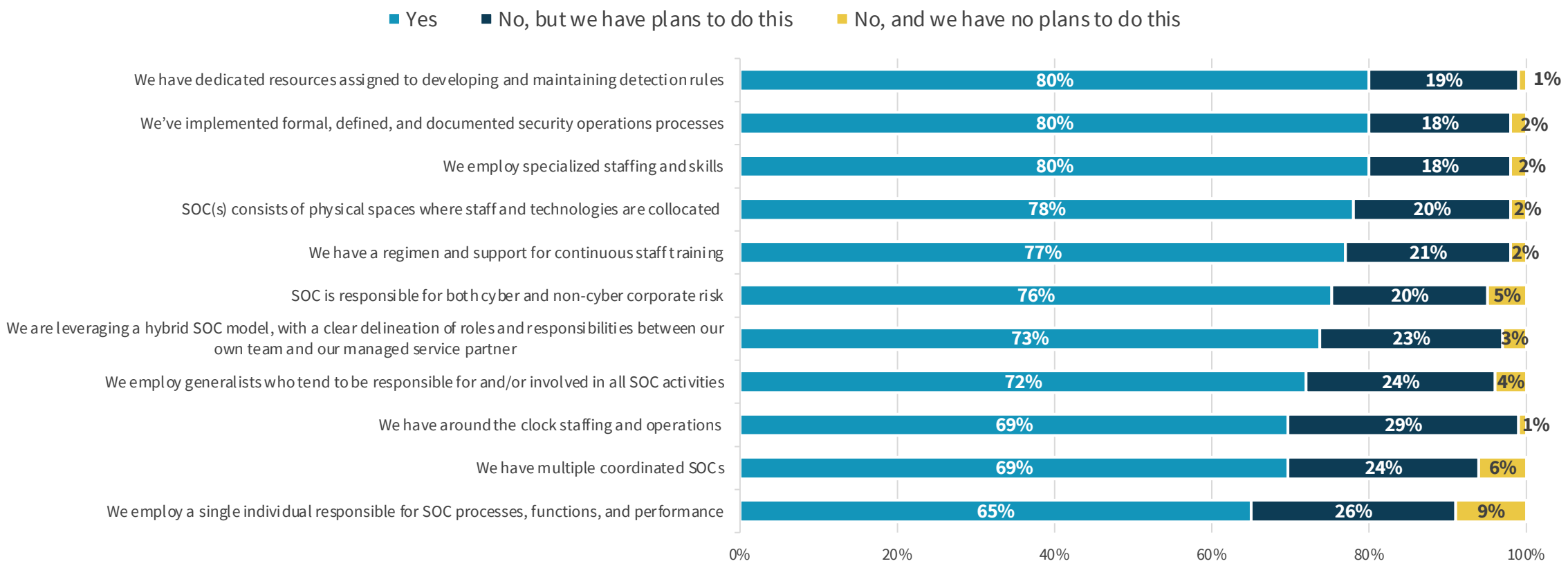
Question text:
In which of the following security analytics and operations skill sets is your organization's cybersecurity team least proficient? (Percent of respondents, N=376, three responses accepted)

MITRE ATT&CK Is Quickly Becoming an RFP Requirement



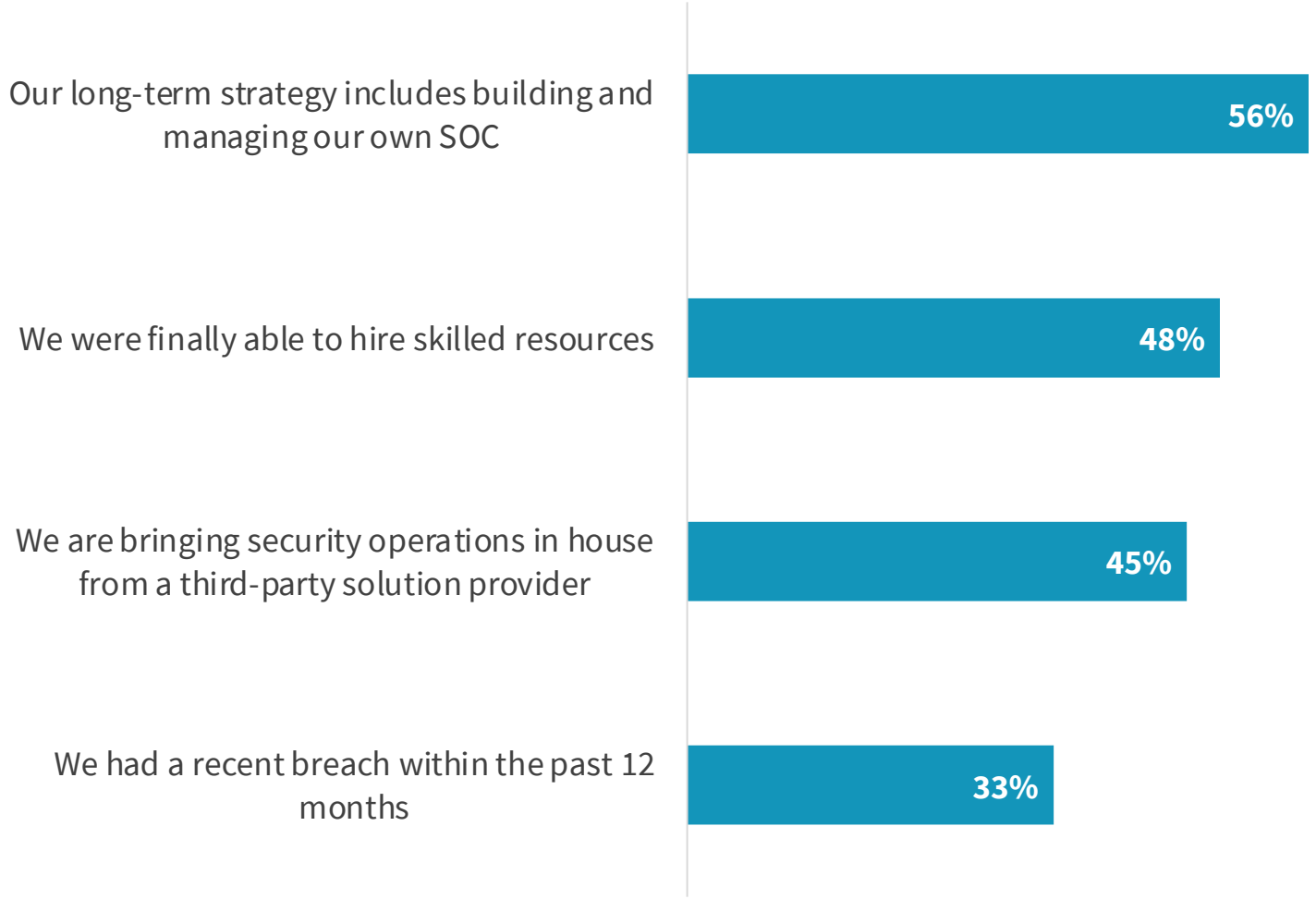
Question text: How important is it that your organization's security operations technologies and tools support the MITRE ATT&CK framework? (Percent of respondents, N=374)

Many Facets to SOC Strategies



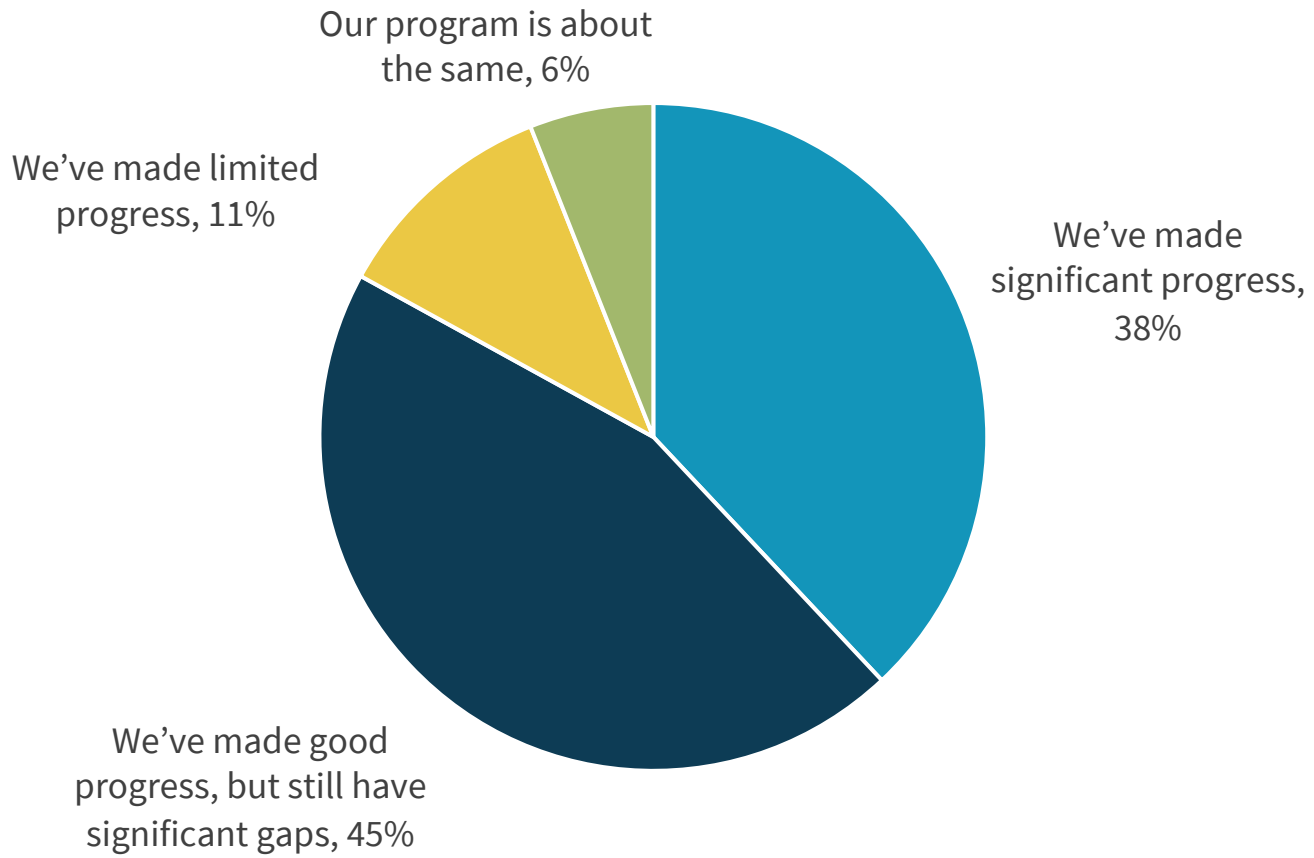
Question text: How do each of the following statements align with your organization's current SOC strategy? (Percent of respondents, N=376)

Key Drivers Underlying Future Investment



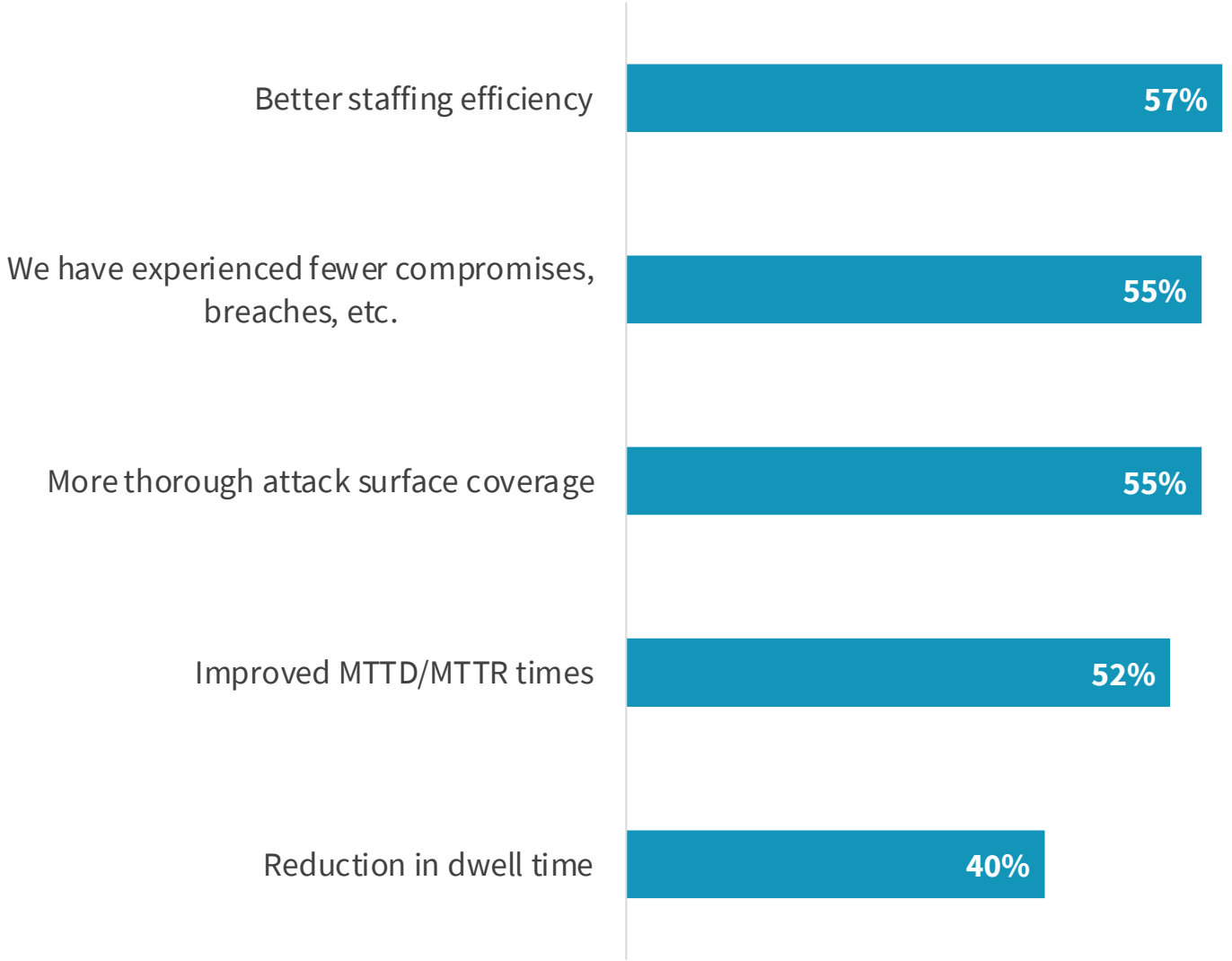
Question text:
Which of the following factors have influenced your organization's security operations investment decisions? (Percent of respondents, N=376, multiple responses accepted)

Most Think Their Security Program Is Improving



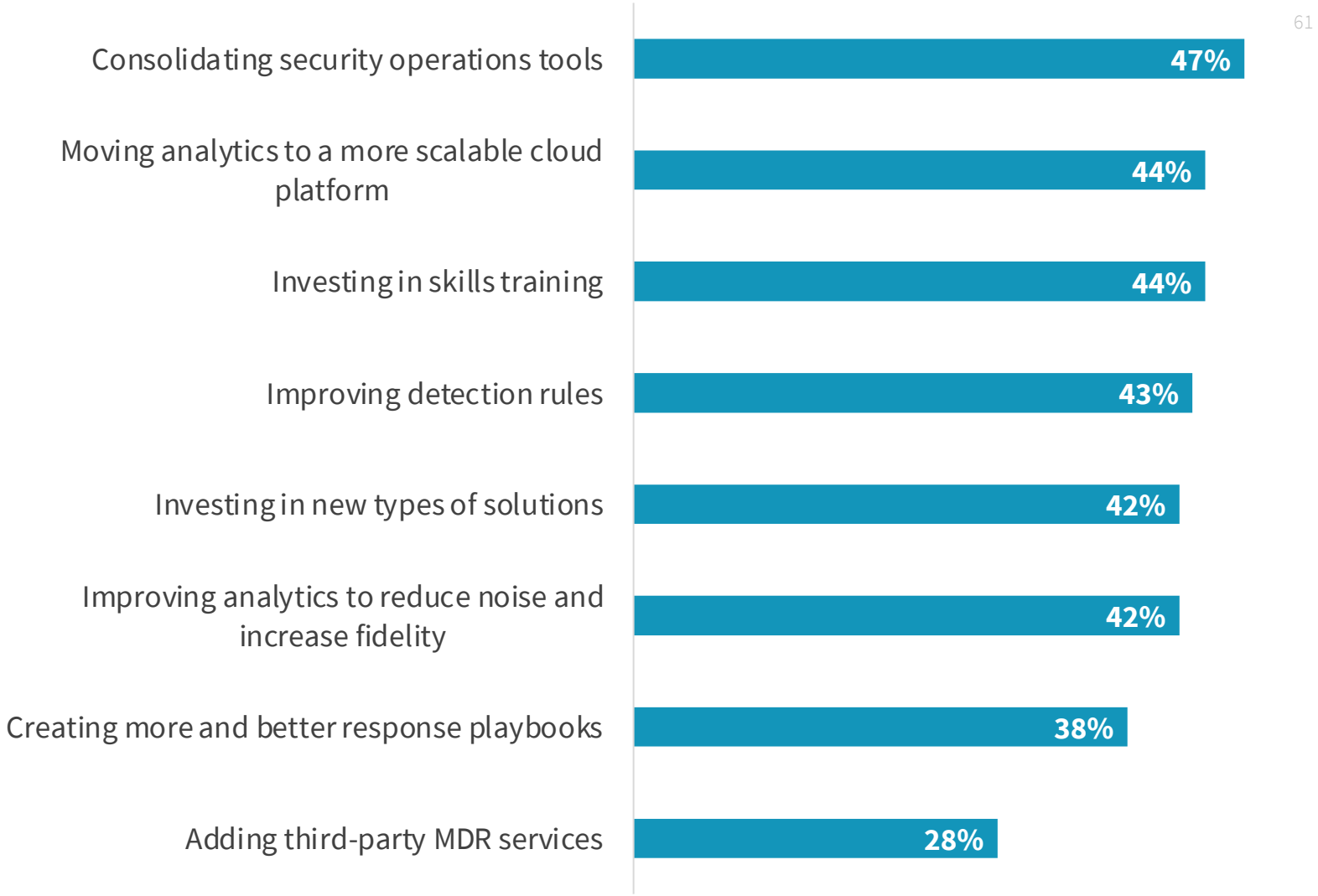
Question text: Which of the following best reflects your assessment of the effectiveness of your organization's security program in the past 12 months? (Percent of respondents, N=376)

Positive Outcomes: Efficiency, efficacy, and coverage.



Question text:
Which of the following outcomes has your organization realized due to its recent (past 12 months) security operations investments? (Percent of respondents, N=376, multiple responses accepted)

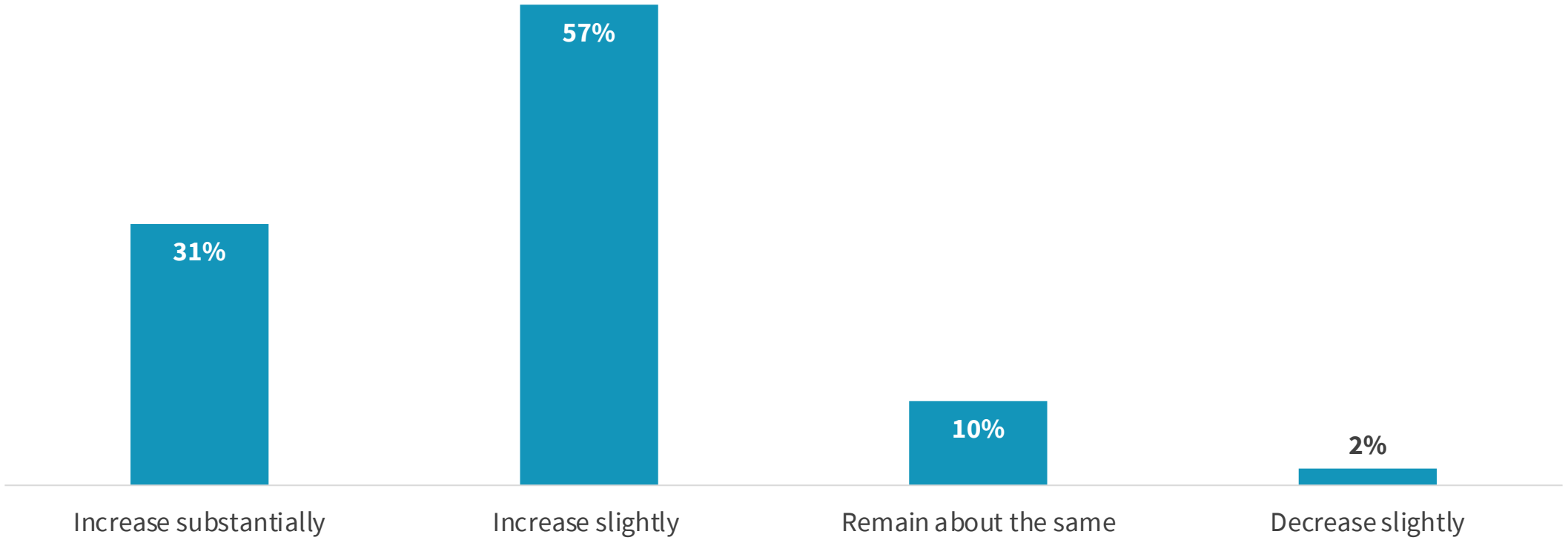
Investments are Paying Off



Question text:
Which of the following investments have produced the most significant, positive security operations improvements for your organization? (Percent of respondents, N=376, multiple responses accepted)

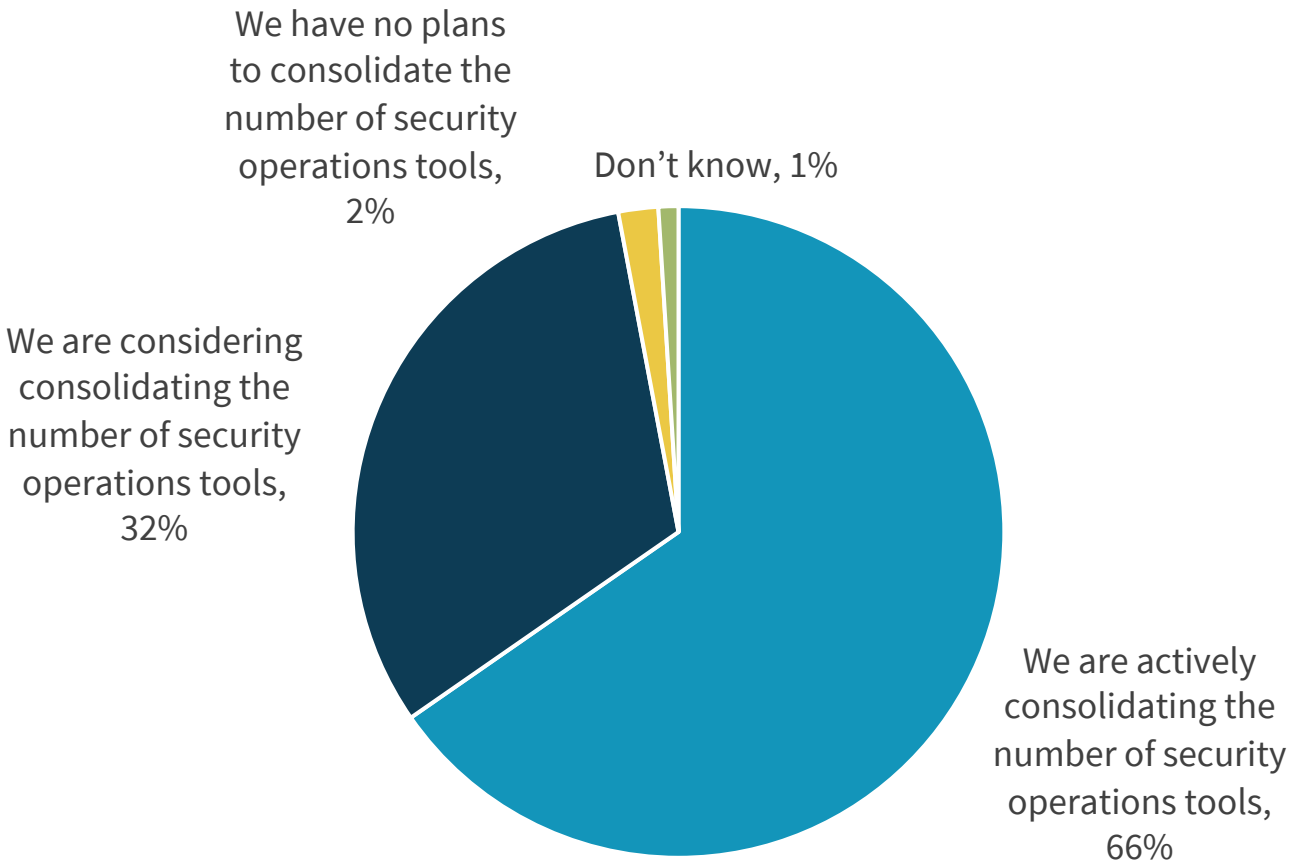
Improving Security Operations Is a Priority and Is Funded

88% will increase spending over the next 12-18 months



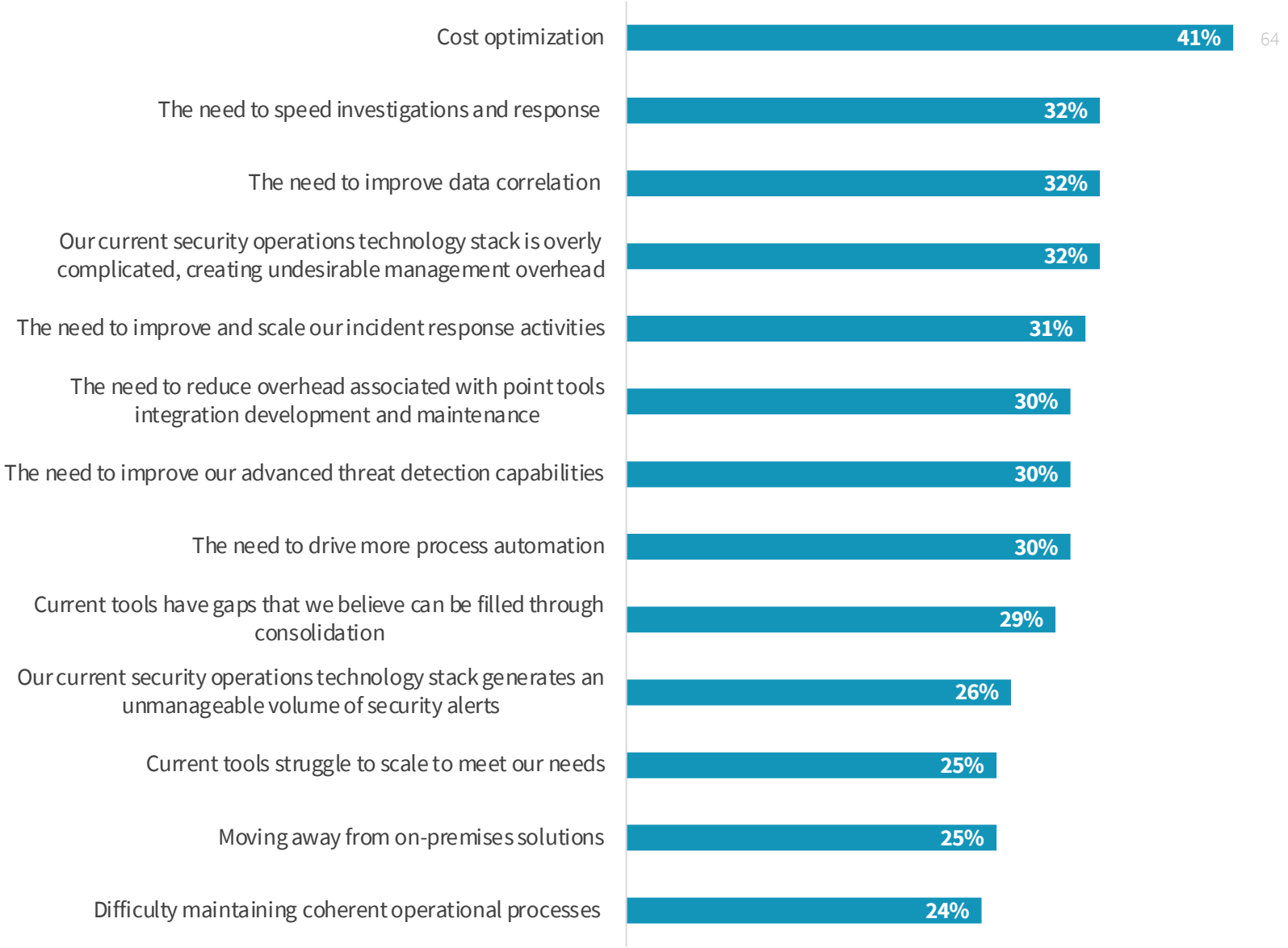
Question text: How do you expect your organization's spending on security operations technologies, services, and personnel to change over the next 12 to 18 months? (Percent of respondents, N=376)

Tools Consolidation Is a Continuing Priority for 2/3



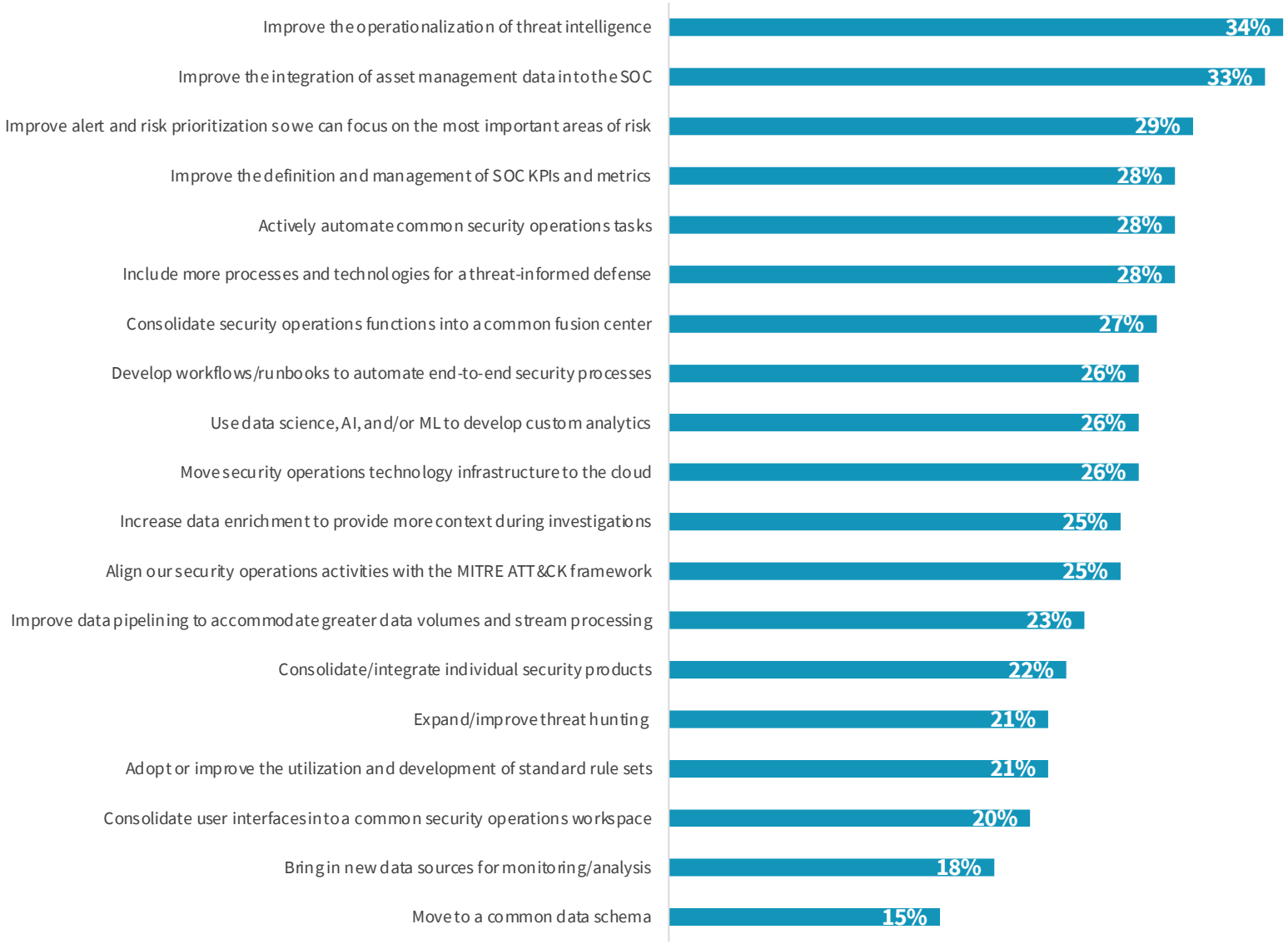
Question text: Which of the following statements regarding the consolidation of your organization’s security operations tools is most accurate? (Percent of respondents, N=376)

Cost Is #1 Driver for Consolidation Followed by Efficacy



Question text:
If your organization is actively or considering consolidating security operations tools, what is driving the need for consolidation? (Percent of respondents, N=368, multiple responses accepted)

This Year's SOC Improvement Initiatives



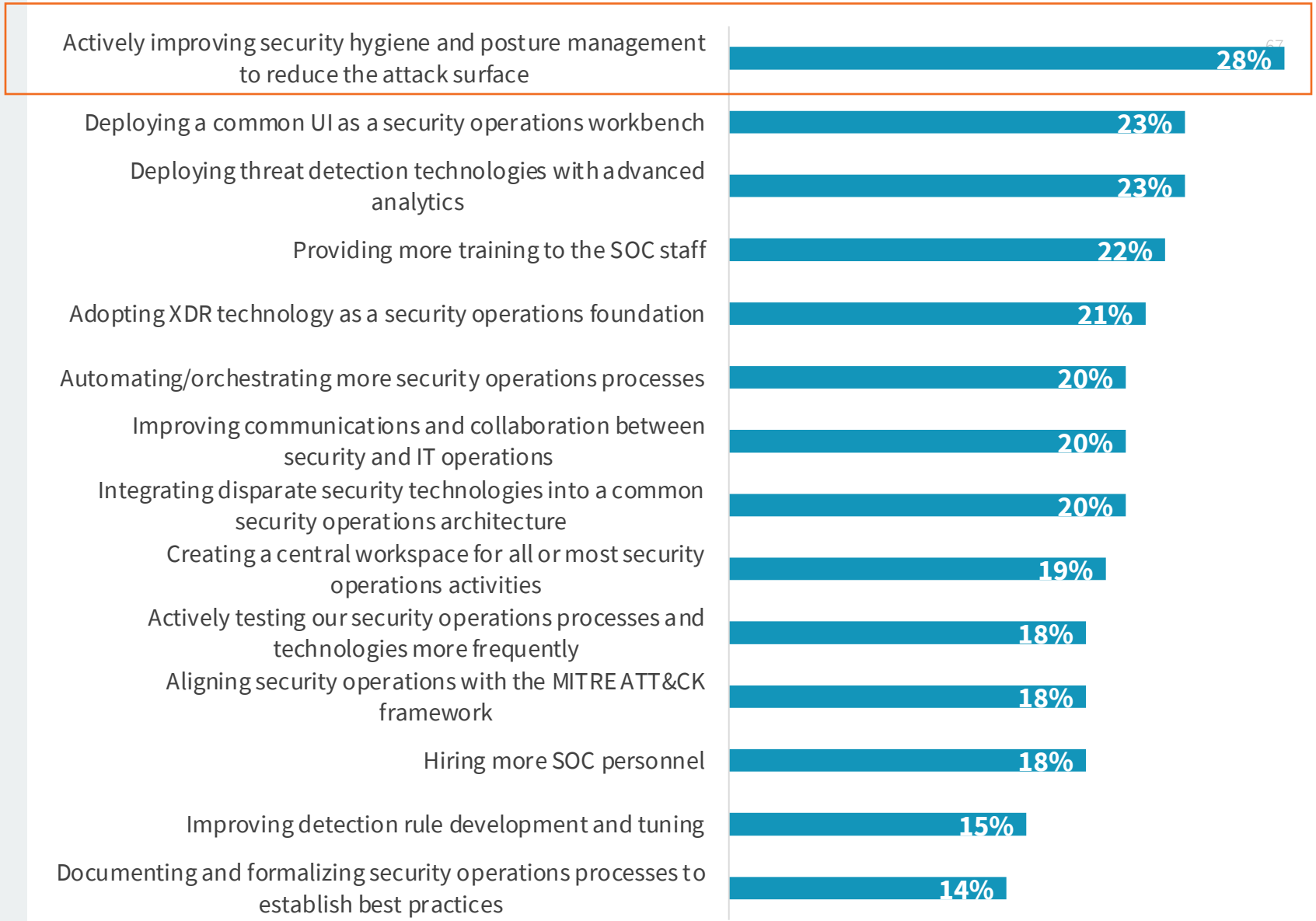
Question text:
Which of the following SOC-focused objectives, if any, will your organization pursue over the next 12 months? (Percent of respondents, N=376, multiple responses accepted)

Plenty of Areas to Focus on…

Process automation tops the list

Question text:
Which of the following actions will your organization take over the next 12 to 18 months to improve security operations? (Percent of respondents, N=376, multiple responses accepted)

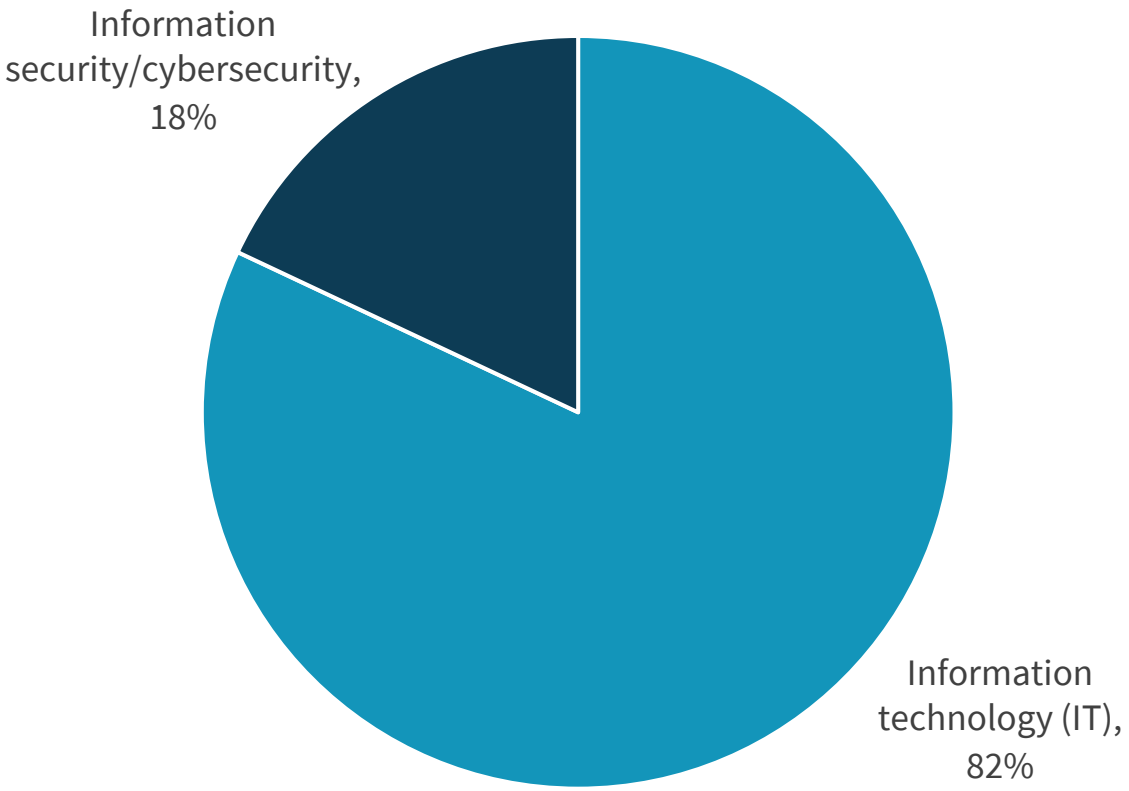
The Growing Attack Surface Underlies SOC Challenges



Question text:
Regardless of your organization's current security operations and plans, which of the following actions would be most beneficial for improving security efficacy and operational efficiency? (Percent of respondents, N=376, three responses accepted)

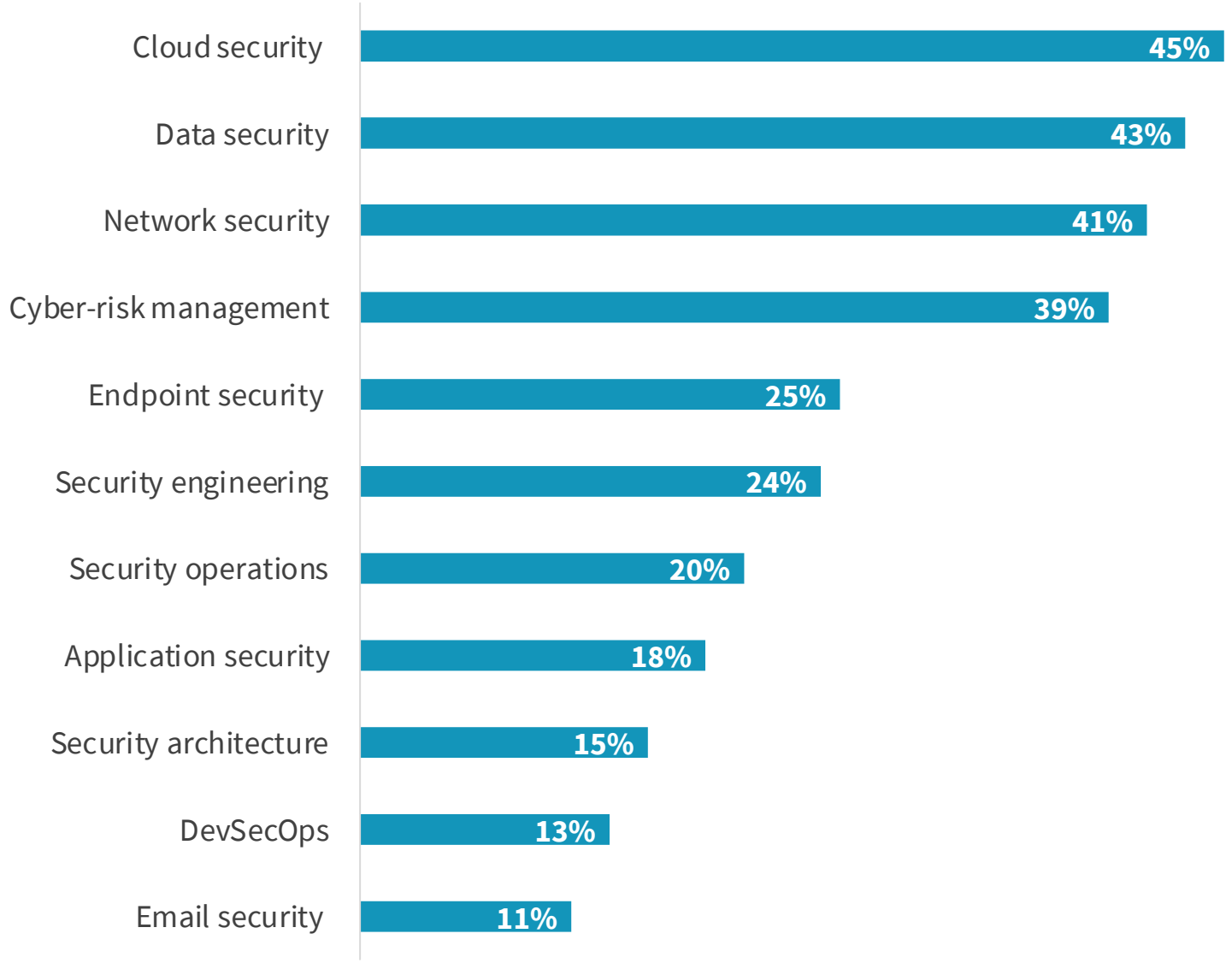
Demographics

Respondents by Job Function



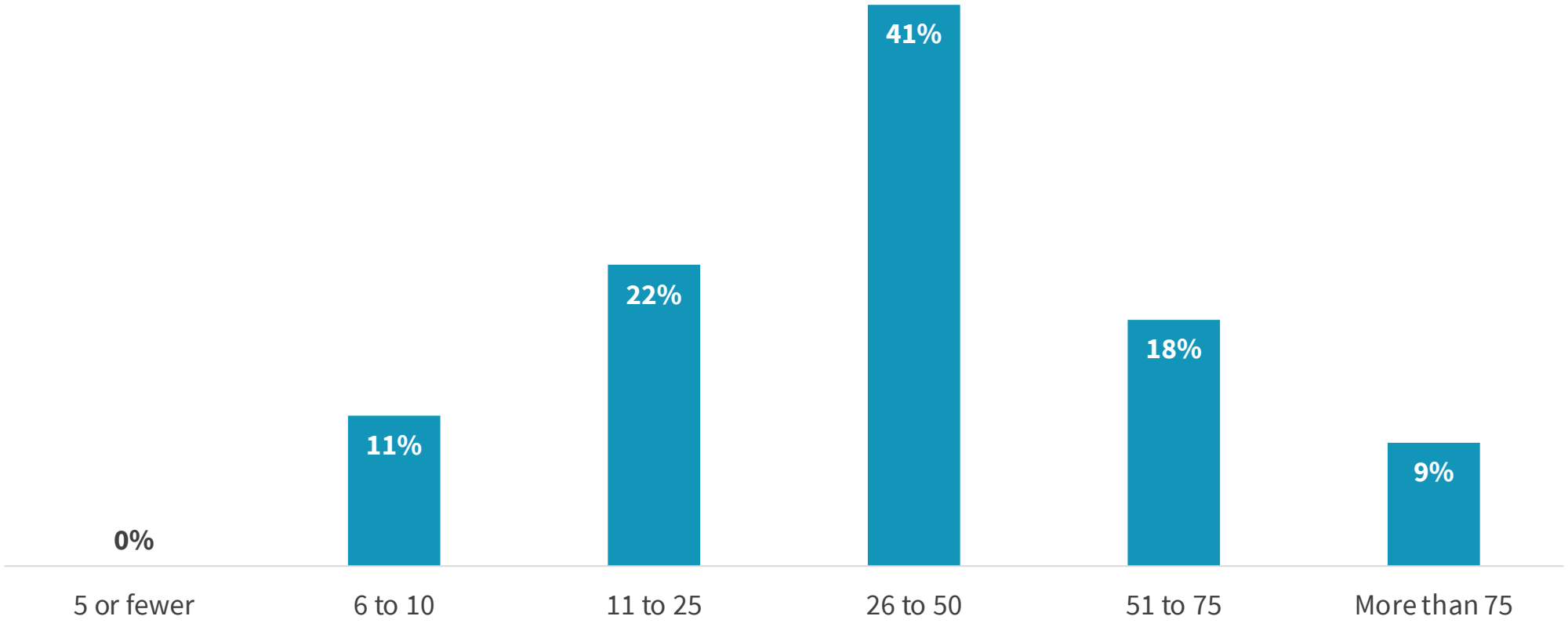
Question text: Which of the following best describes your current job function? (Percent of respondents, N=376)

Areas of Cybersecurity Involvement



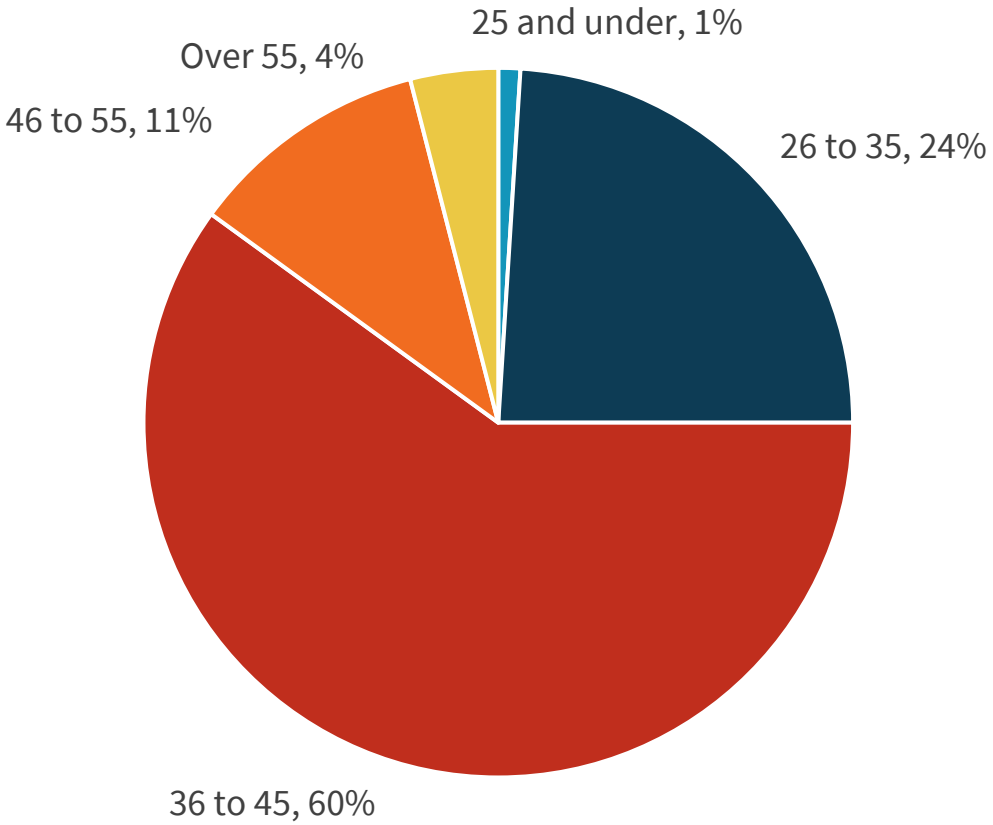
Question text:
With which of the following areas of cybersecurity are you most personally involved?
(Percent of respondents, N=376, three responses accepted)

Respondents by Number of SOC Employees



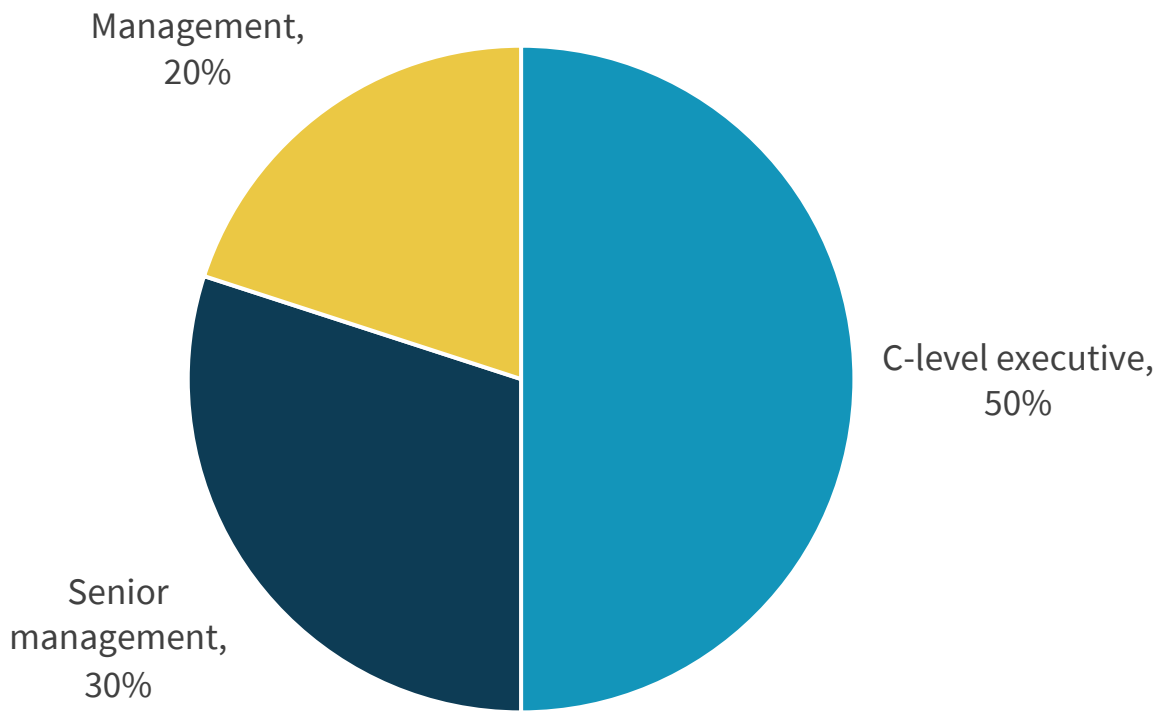
Question text: Approximately how many individuals work full- or part-time in your organization's SOC? (Percent of respondents, N=376)

Respondents by Age



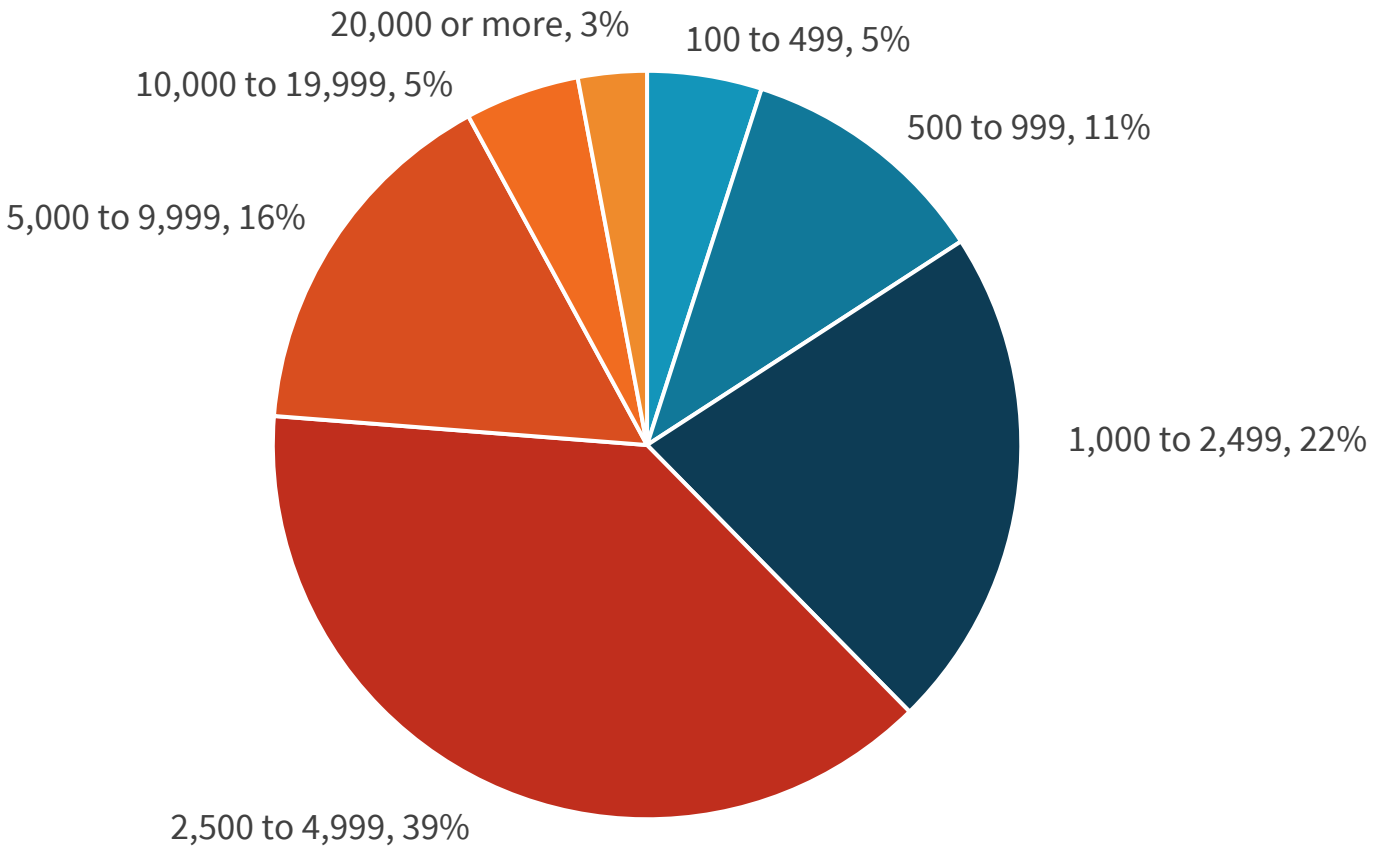
Question text: Please select your age group. (Percent of respondents, N=376)

Respondents by Role



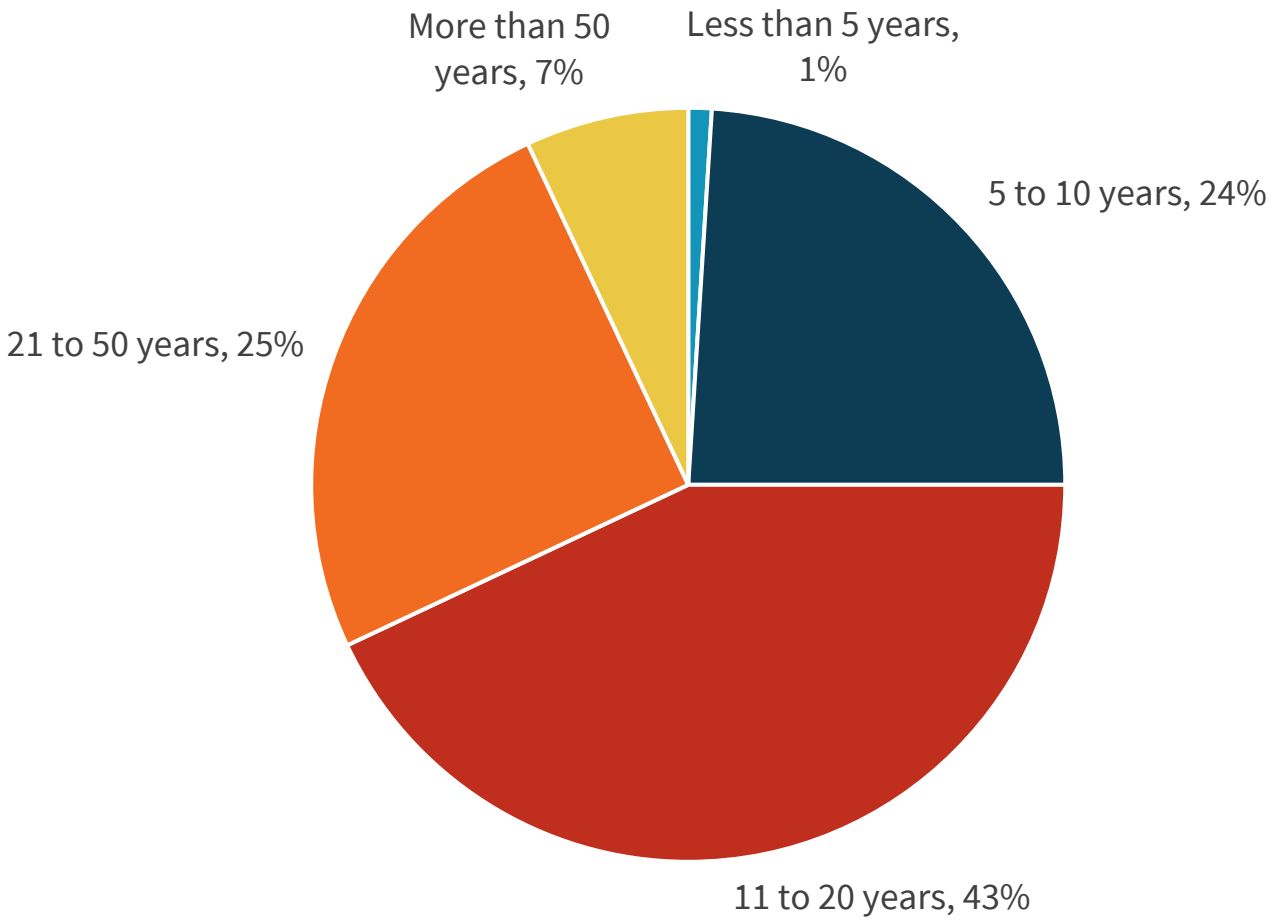
Question text: Which of the following best describes your current job title/level? (Percent of respondents, N=376)

Respondents by Number of Employees



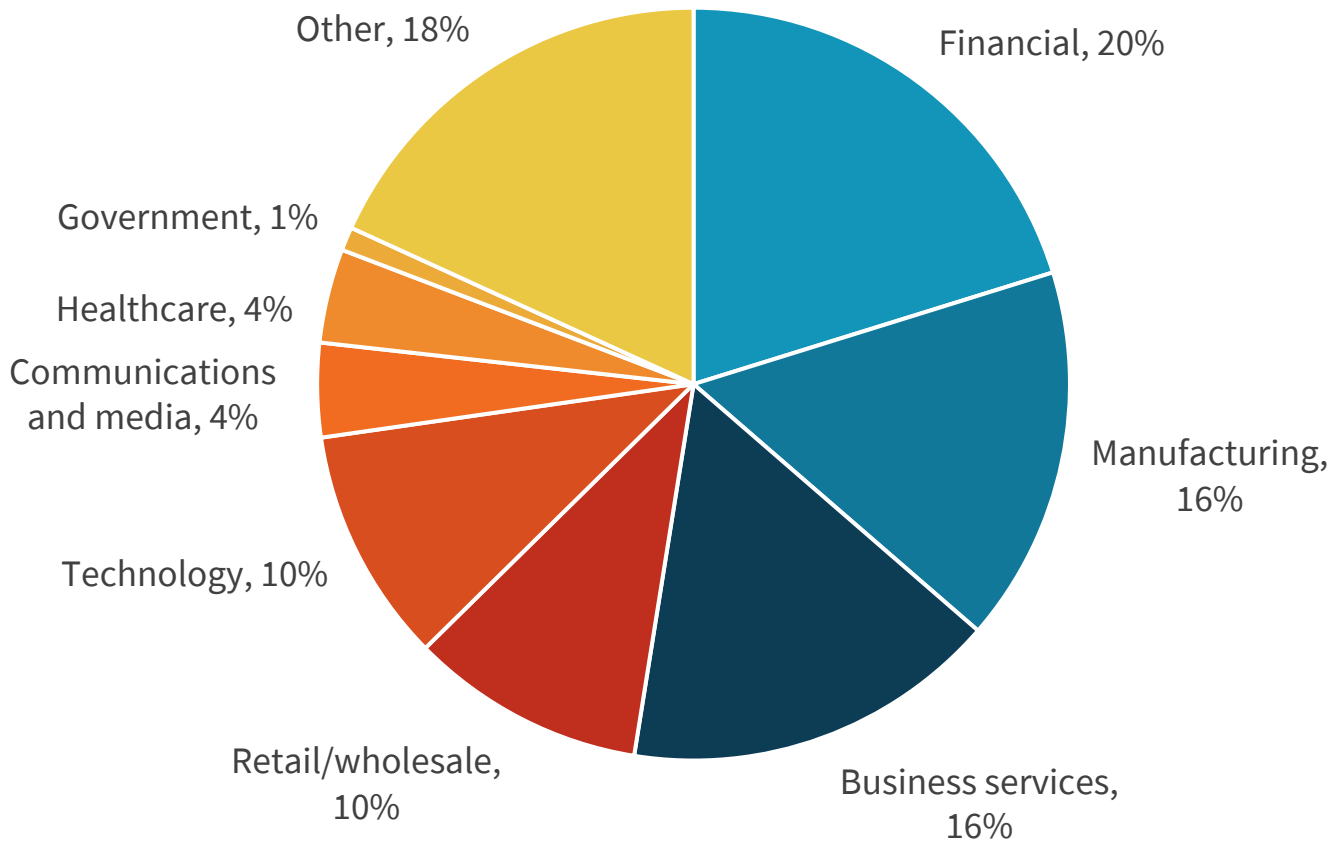
Question text: How many total employees does your organization have worldwide? (Percent of respondents, N=376)

Respondents by Age of Organization



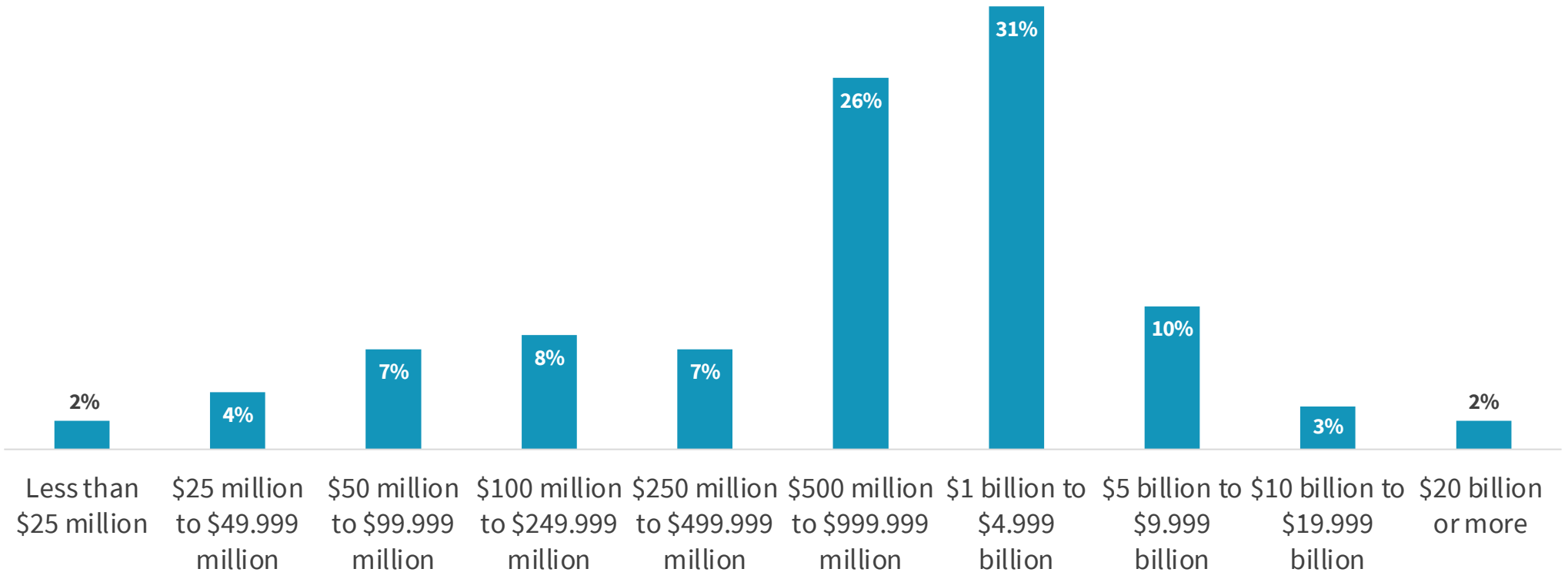
Question text: For approximately how long has your current employer been in existence? (Percent of respondents, N=376)

Respondents by Industry



Question text: What is your organization's primary industry? (Percent of respondents, N=376)

Respondents by Annual Revenue



Question text: What is your organization's total annual revenue ($US)? (Percent of respondents, N=376)