RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **RMG-T08**

What (Actually, Specifically) Makes Security Programs EVEN MORE Successful?

Wade Baker
Partner and Co-Founder
Cyentia Institute
@wadebaker

Wendy Nather
Head of Advisory CISOs
Cisco
@wendynather

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

In our last episode …

2021 Security Outcomes Study

- Surveyed 4,800 IT & security pros
- 150+ responses from 25 countries
- All types and sizes of organizations
- 11 outcomes; 25 security practices

cisco.com/go/SecurityOutcomes

Security Outcomes: What does “success” look like?

Enabling the Business

- Keep up with business
- Gain trust from execs
- Obtain peer buy-in
- Create strong culture

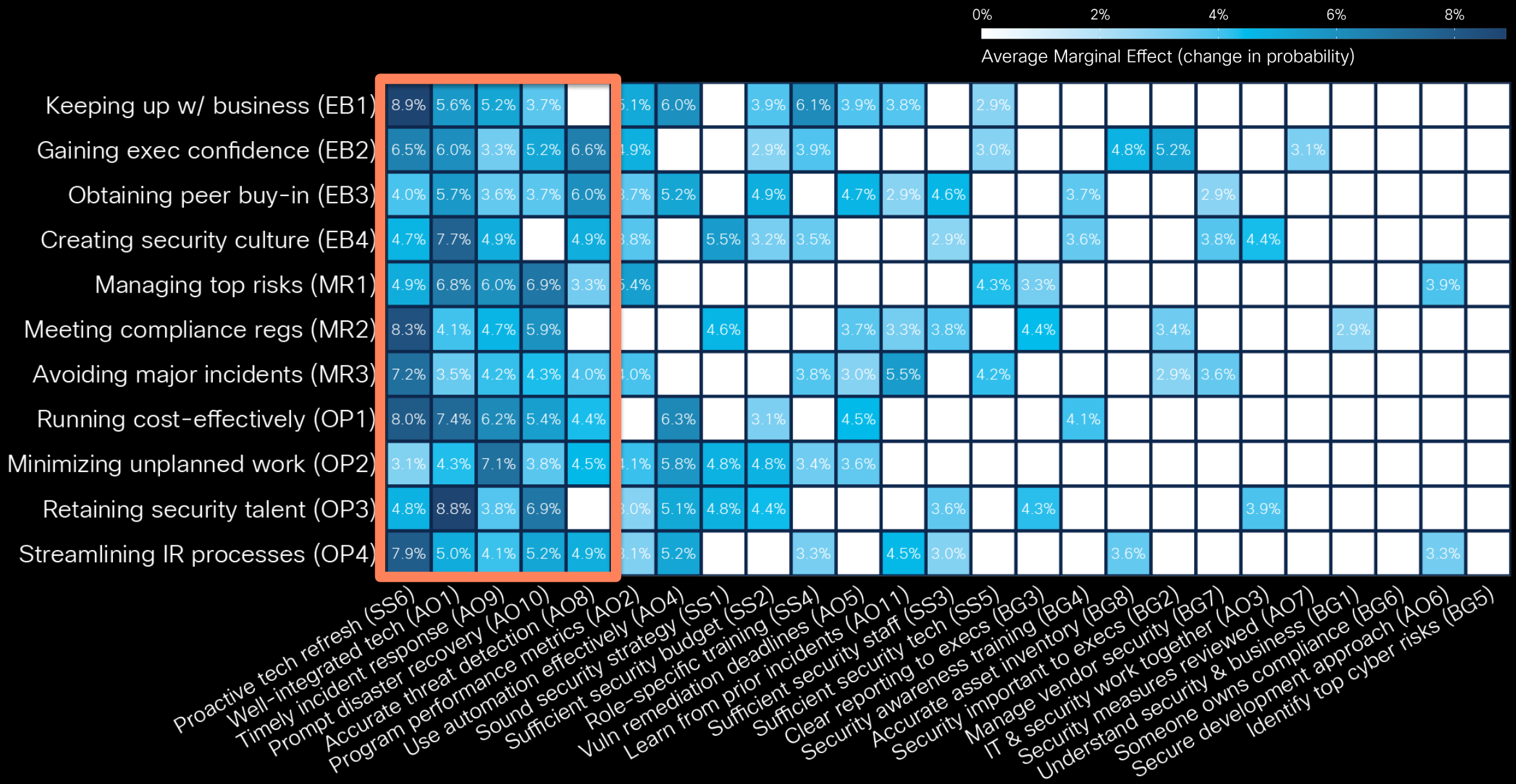
Managing Risk

- Manage top cyber risks
- Meet compliance reqs
- Avoid major incidents
- Maintain biz continuity

Operating Efficiently

- Run an effective program
- Reduce unplanned work
- Recruit & retain talent
- Streamline detection & response

Correlation matrix: 25 practices x 11 outcomes



The Fabulous Five: Most correlated with outcomes

Proactive tech refresh

Well-integrated tech

Timely incident response

Prompt disaster recovery

Accurate threat detection

NOTE

These top five practices had the greatest statistical likelihood of improving ALL the desired program outcomes across the board, from keeping up with the business to recruiting and retaining talent.

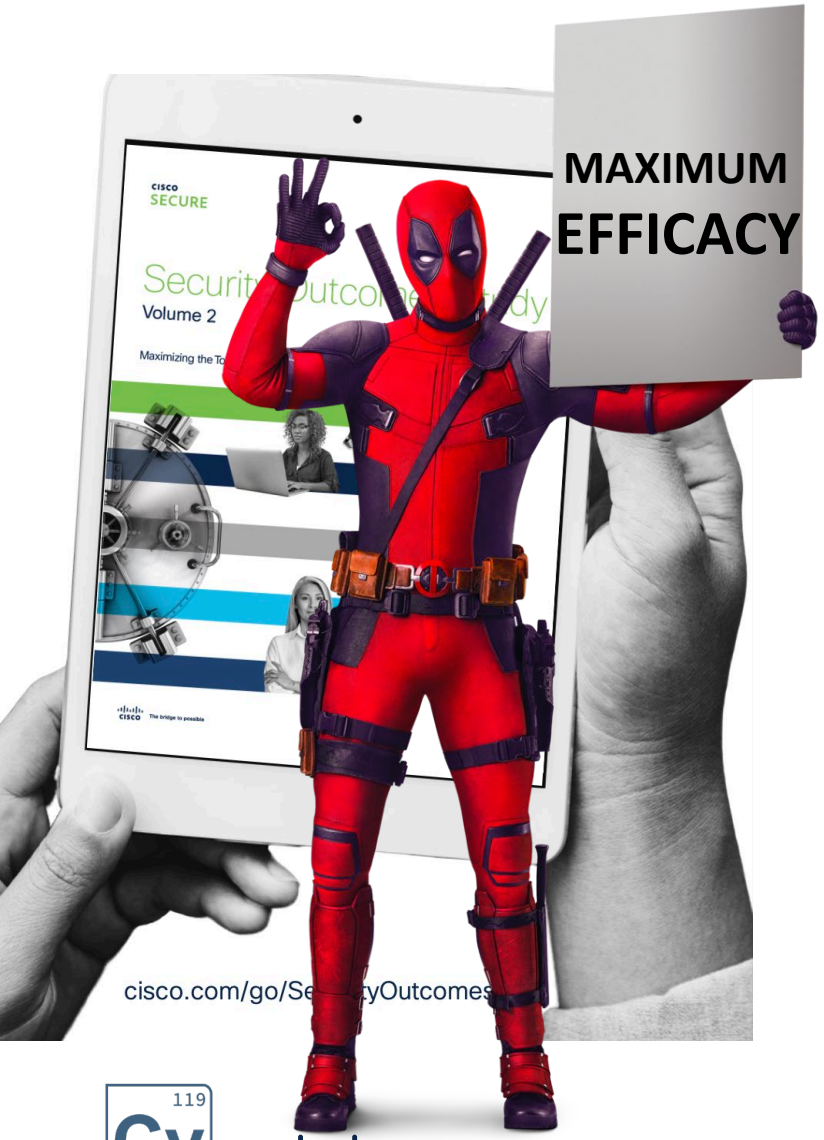
They helped everywhere.

RSAConference2022

Why these practices, and how do we apply them?

Volume 2: Double-clicking on the details

How can we maximize efficacy of the Fab 5?



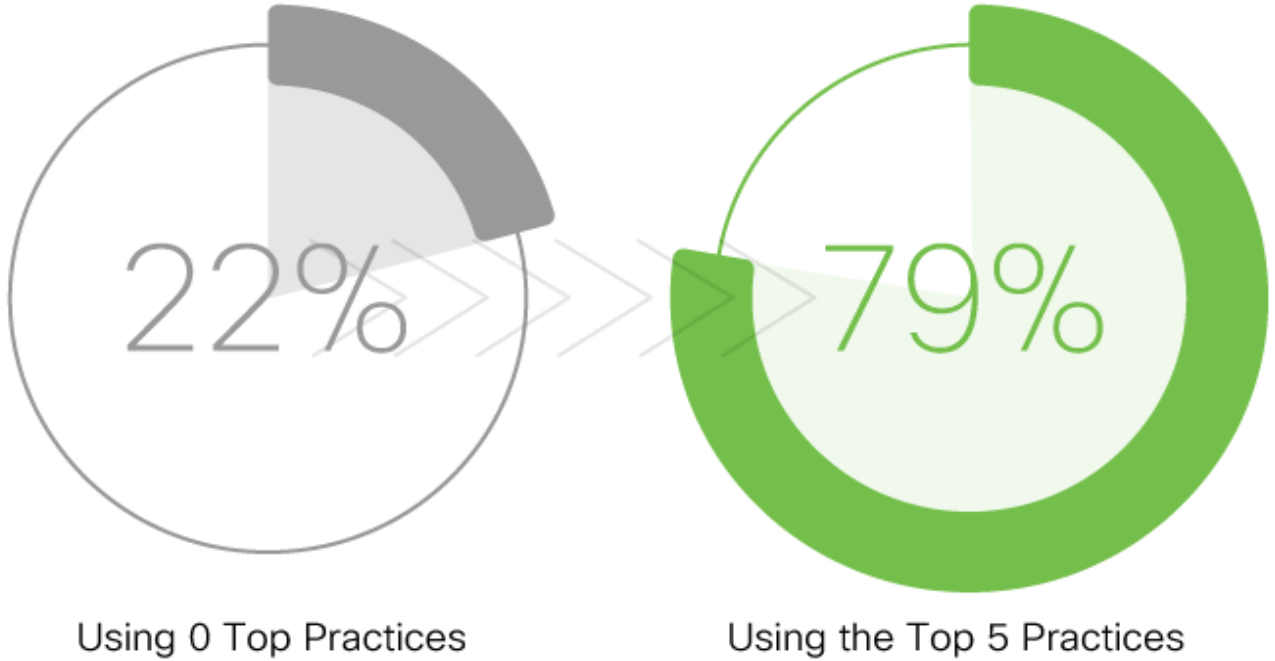
- Surveyed 5,100 IT & security pros
- 150+ responses from 27 countries
- All types and sizes of organizations
- 12 outcomes; 25 security practices

cyentia

cisco SECURE

A shortcut to security success

Go from the **BOTTOM 20%** of security programs to the **TOP 20%** with 5 practices!



Proactive tech refresh
&
Well-integrated tech

Modern IT: The gift that keeps on giving

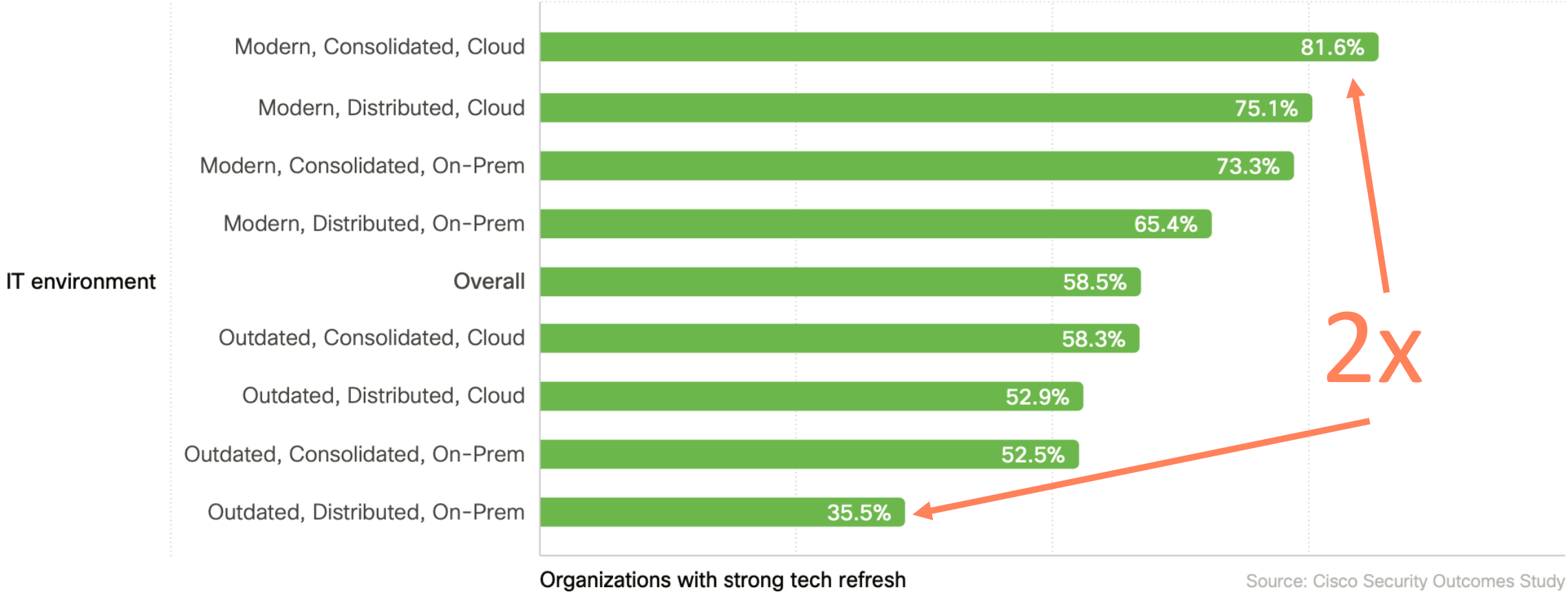
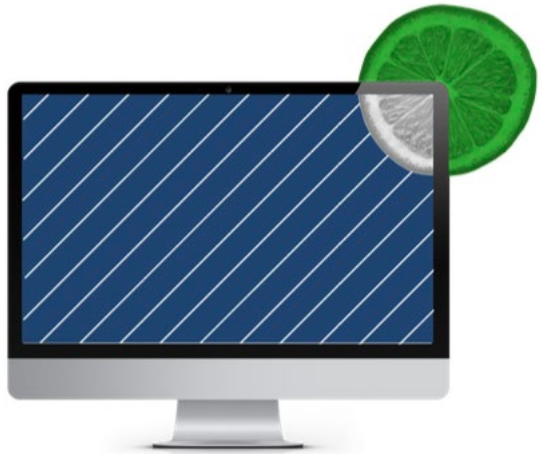
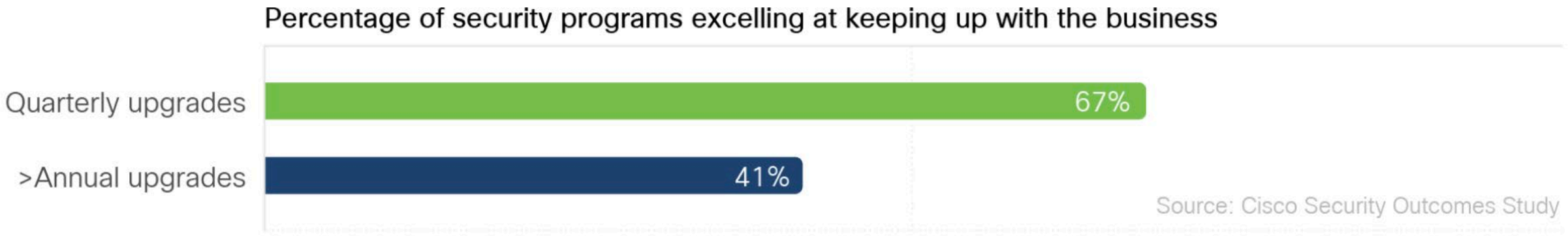


Figure 1: Effect of IT architecture traits on tech refresh performance

Upkeep your tech to keep up with the business



More frequent tech upgrades increase the likelihood of security programs keeping up with the business by 26%



Orgs would rather buy products with out-of-the-box integrations for their core platforms…

Figure 6: Common approaches to security tech integration among all organizations

… But it's actually better to stick with a preferred vendor for integrating security tech

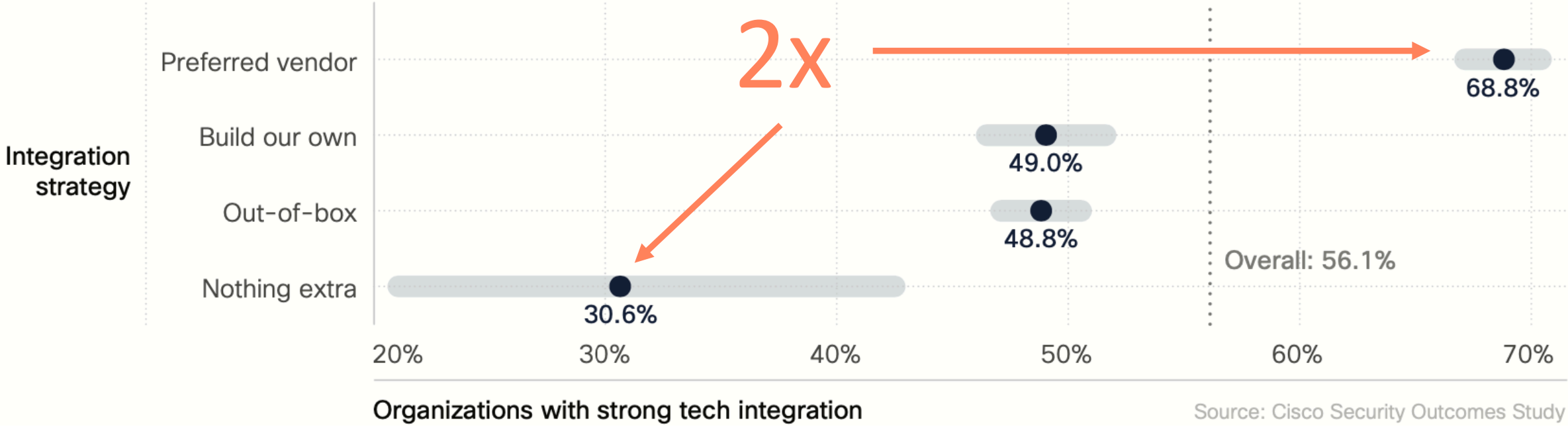
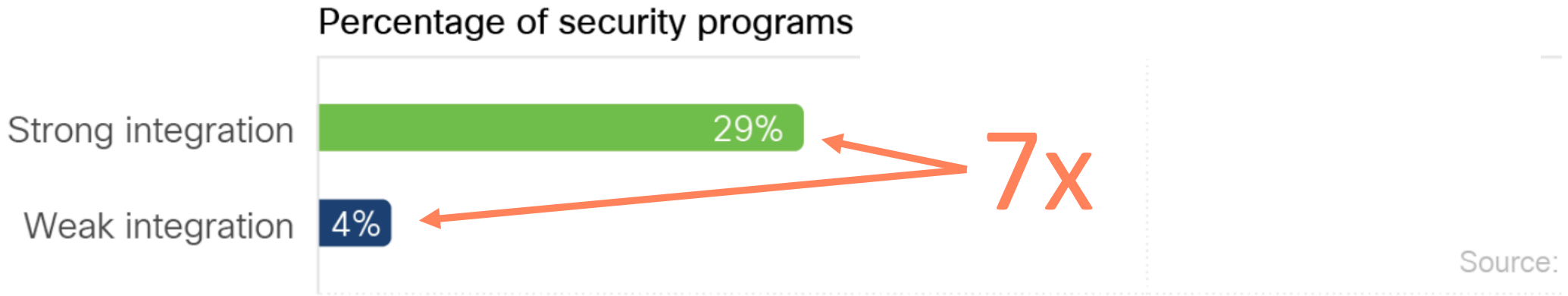


Figure 7: Effect of common integration approaches on level of security tech integration

Integrated tech drives automated processes

Integrated security technologies are 7x more likely to achieve high levels of process automation.



Which NIST CSF functions are best to integrate?

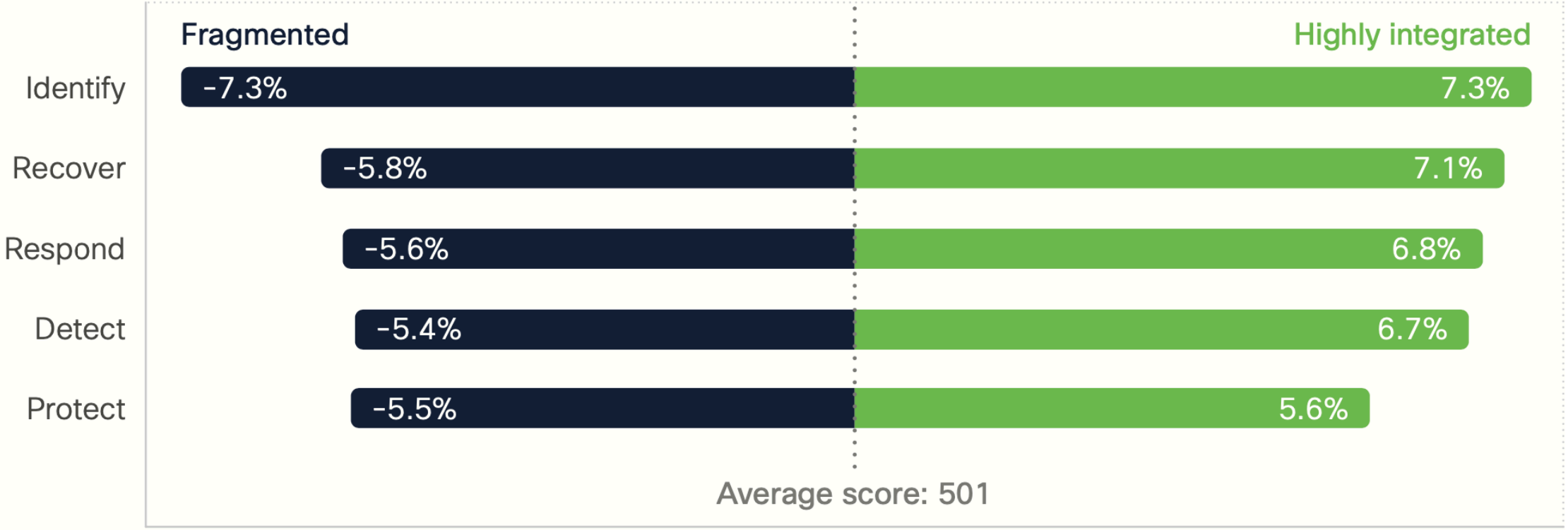
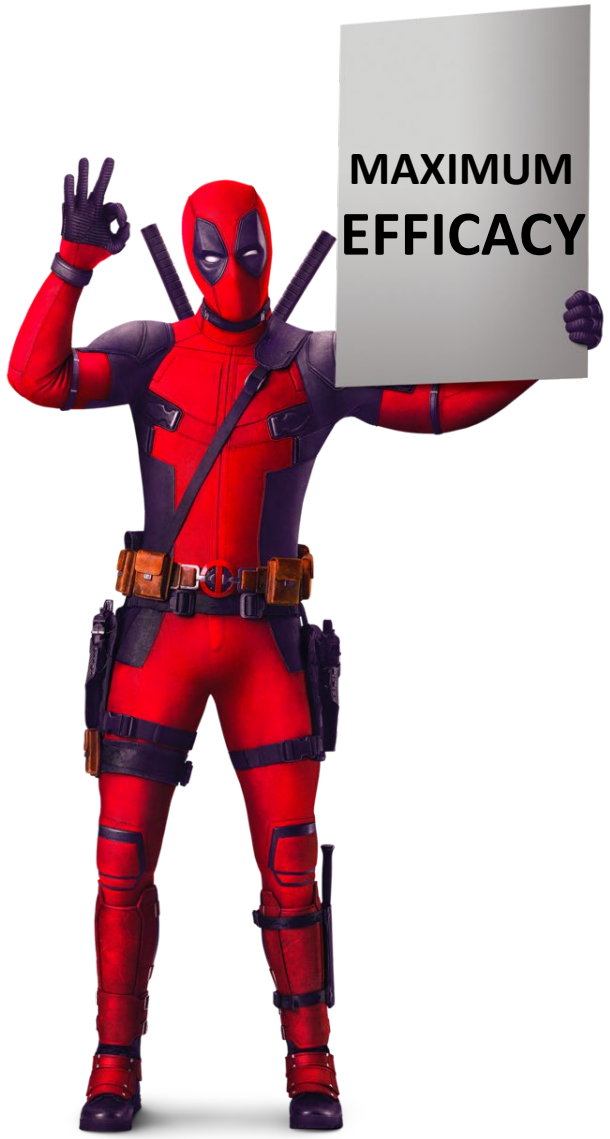


Figure 10: Effect of integrating NIST CSF functions on overall security outcomes score



Tips for MAXIMUM EFFICACY!

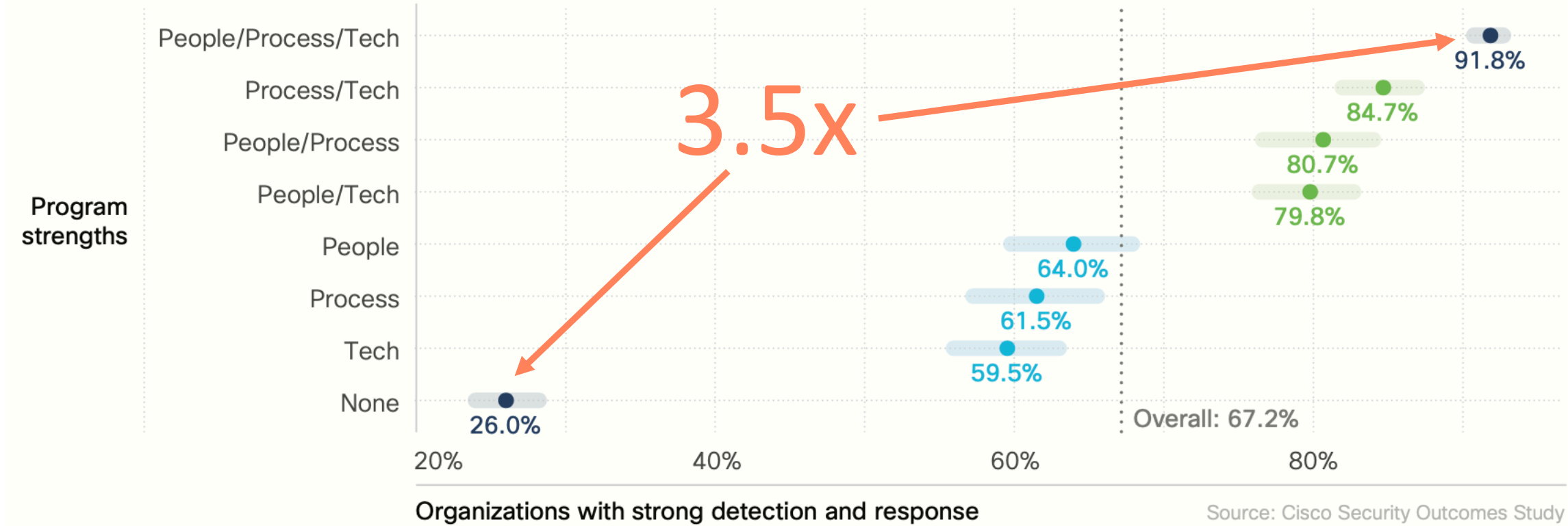
- On-prem is OK, so long as it's modernized and centralized
- A platform approach beats a piecemeal approach for integrated security tech
- Aim to integrate all functions, but start with what you can 'Identify'

Accurate threat detection
&
Timely incident response

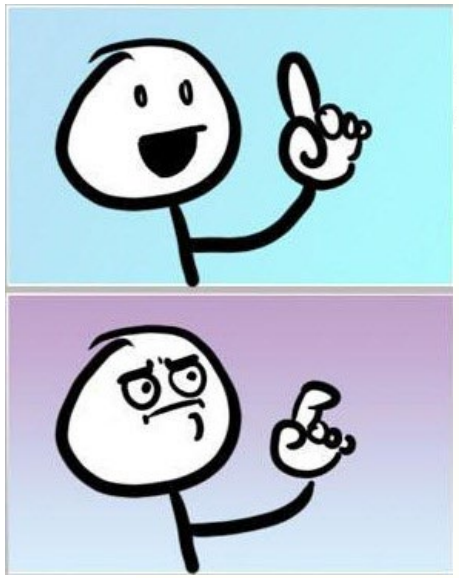
Priority for Strong SecOps: People, Process, Tech?

Higher Priority for SecOps: People, Process, Tech?

Answer: All of the above



Better to insource or outsource SecOps?



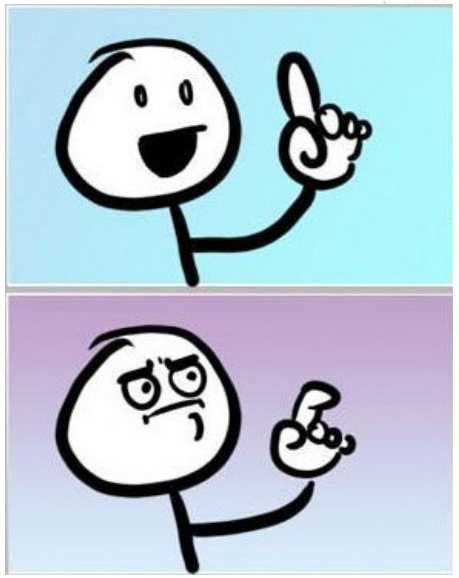
Threat detection and response staffing model

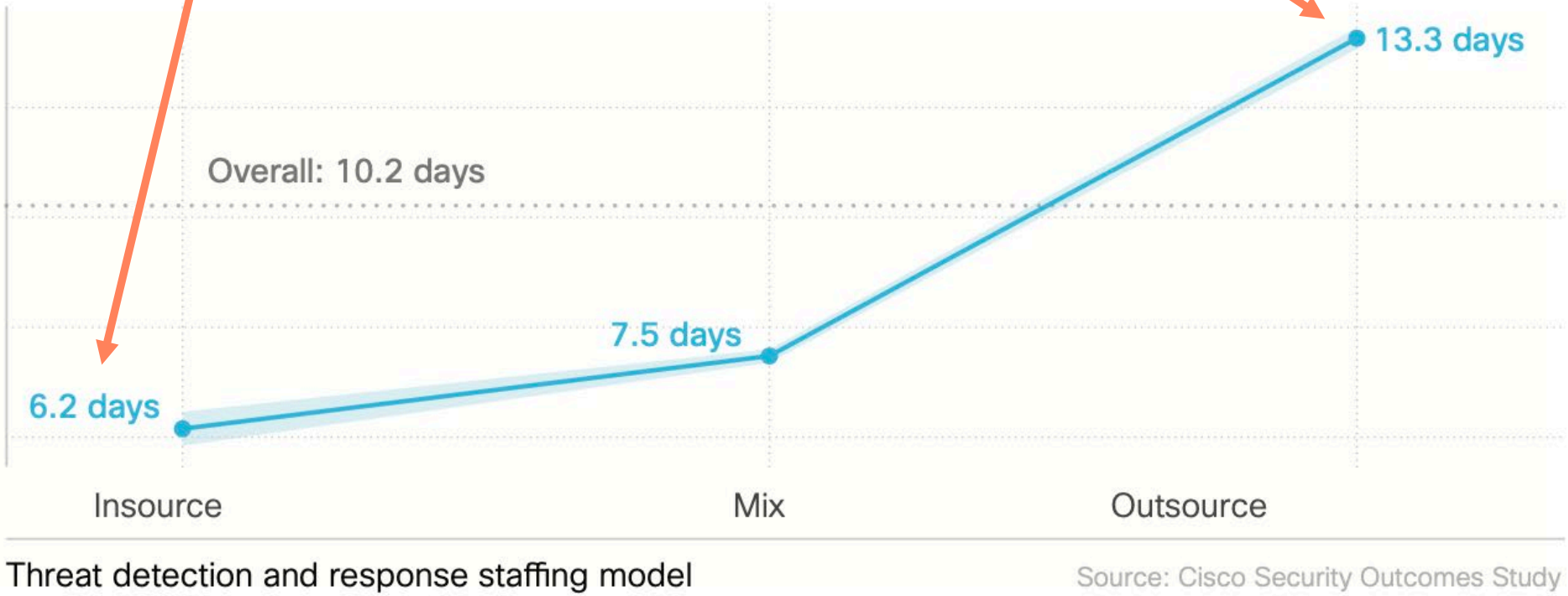
Source: Cisco Security Outcomes Study

cyentia SECURE

Better to insource or outsource SecOps?

BUT…internal teams work twice as fast



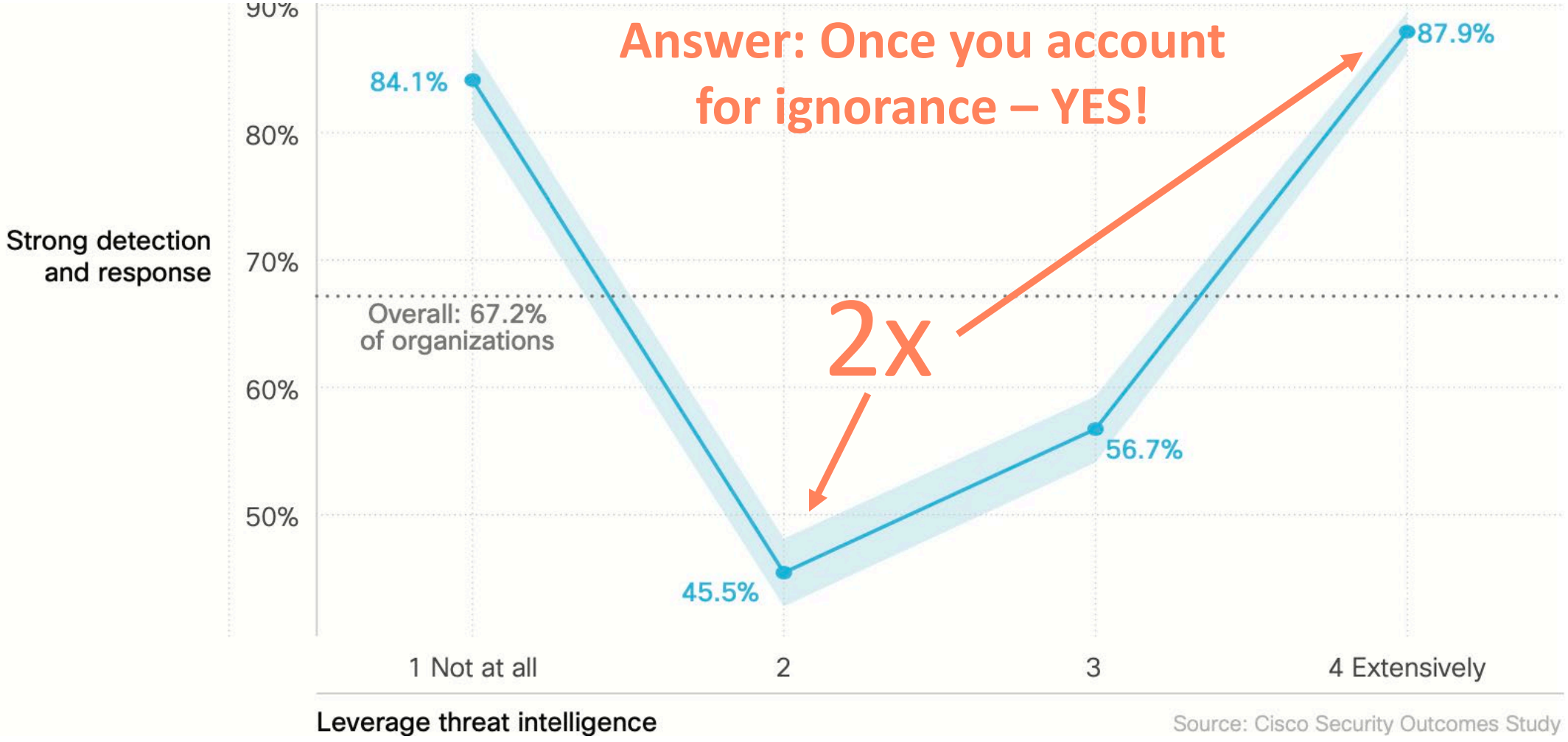


Threat detection and response staffing model

Source: Cisco Security Outcomes Study

Does cyber threat intel raise our intelligence?

Does cyber threat intel raise our intelligence?



Can automation compensate for lack of talent?

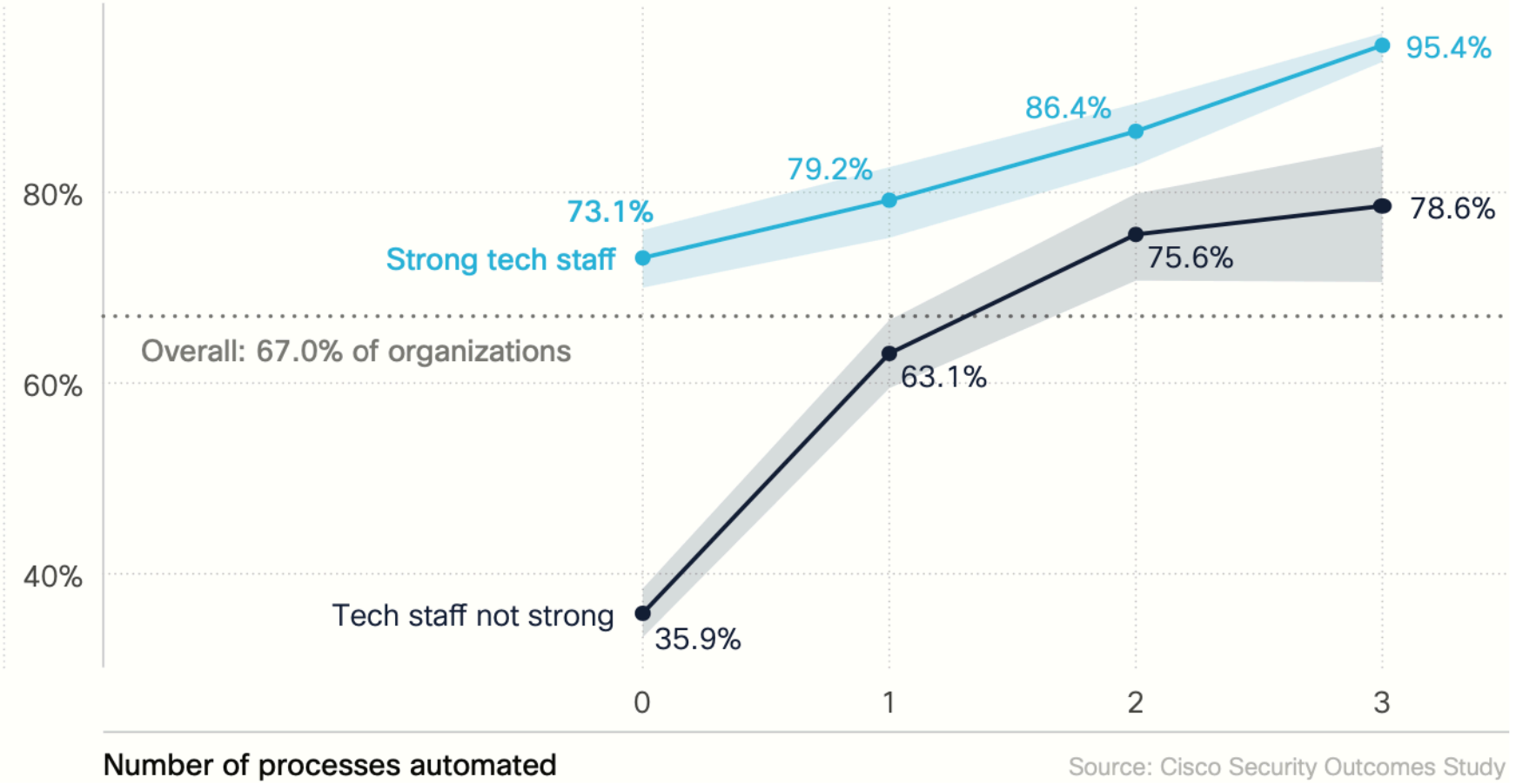


Figure 18: Effect of staffing and automation strength on threat detection and incident response capabilities

Can automation compensate for lack of talent?

Strong detection and response

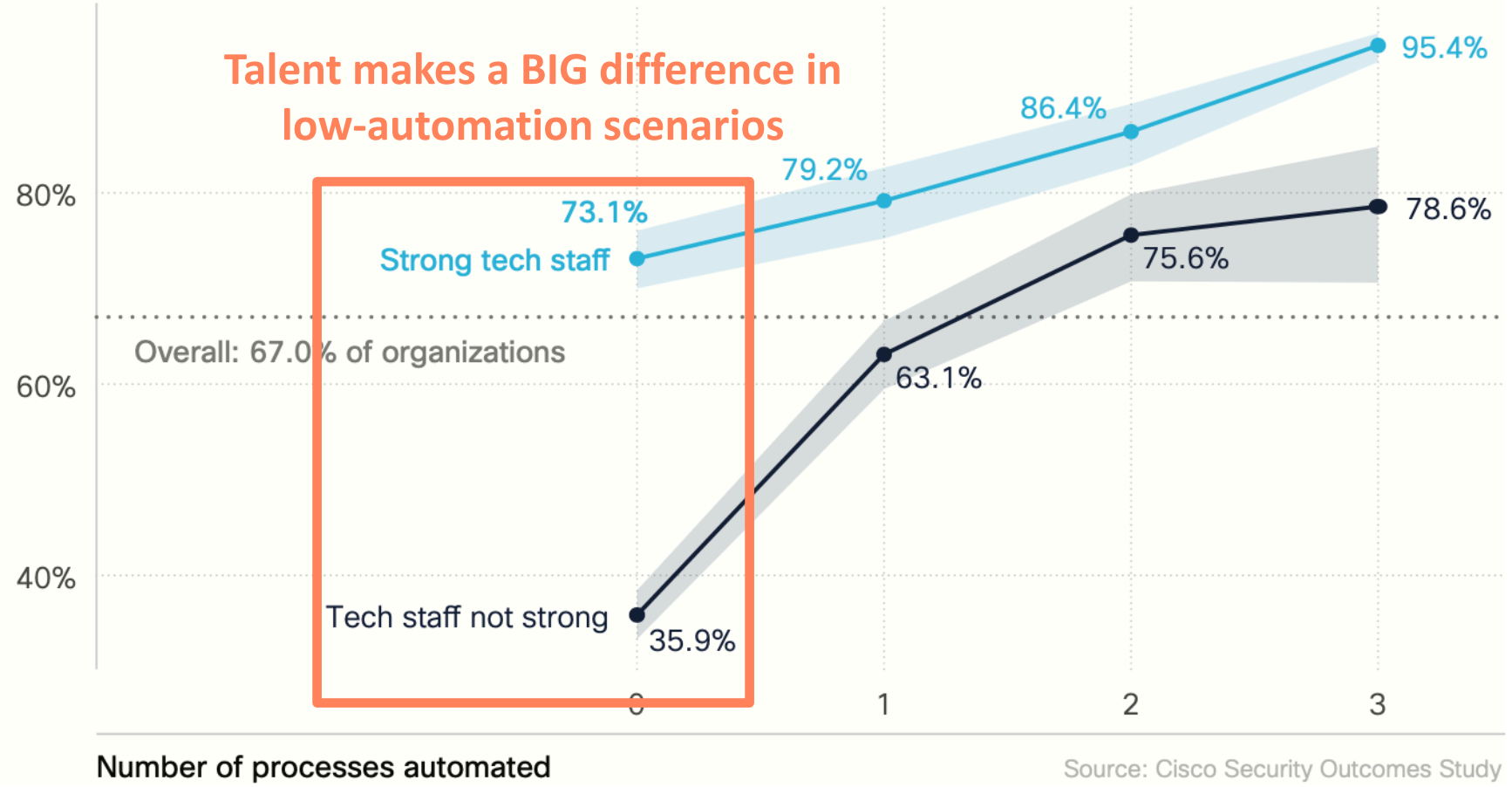


Figure 18: Effect of staffing and automation strength on threat detection and incident response capabilities

Can automation compensate for lack of talent?

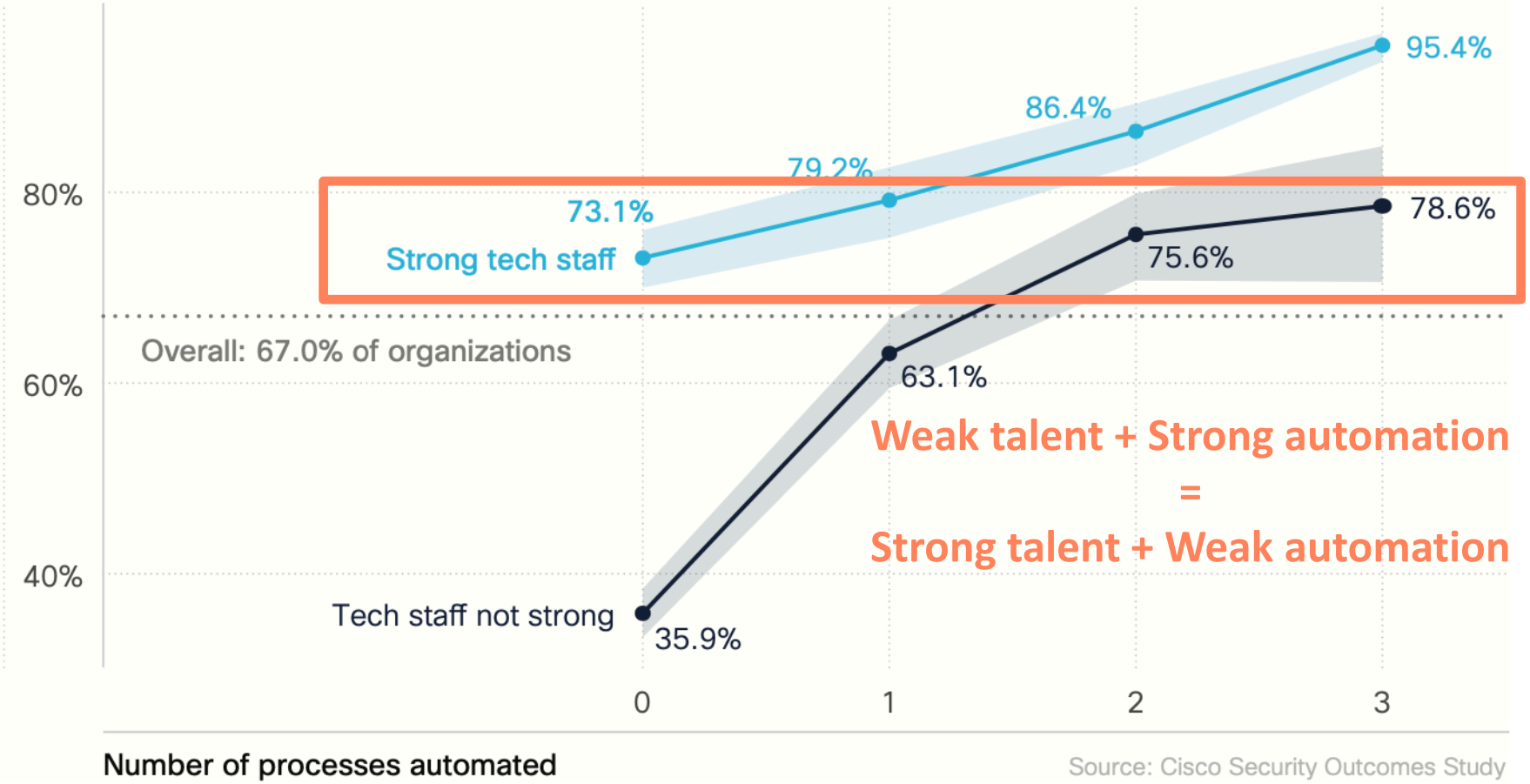


Figure 18: Effect of staffing and automation strength on threat detection and incident response capabilities

Can automation compensate for lack of talent?

Strong detection and response

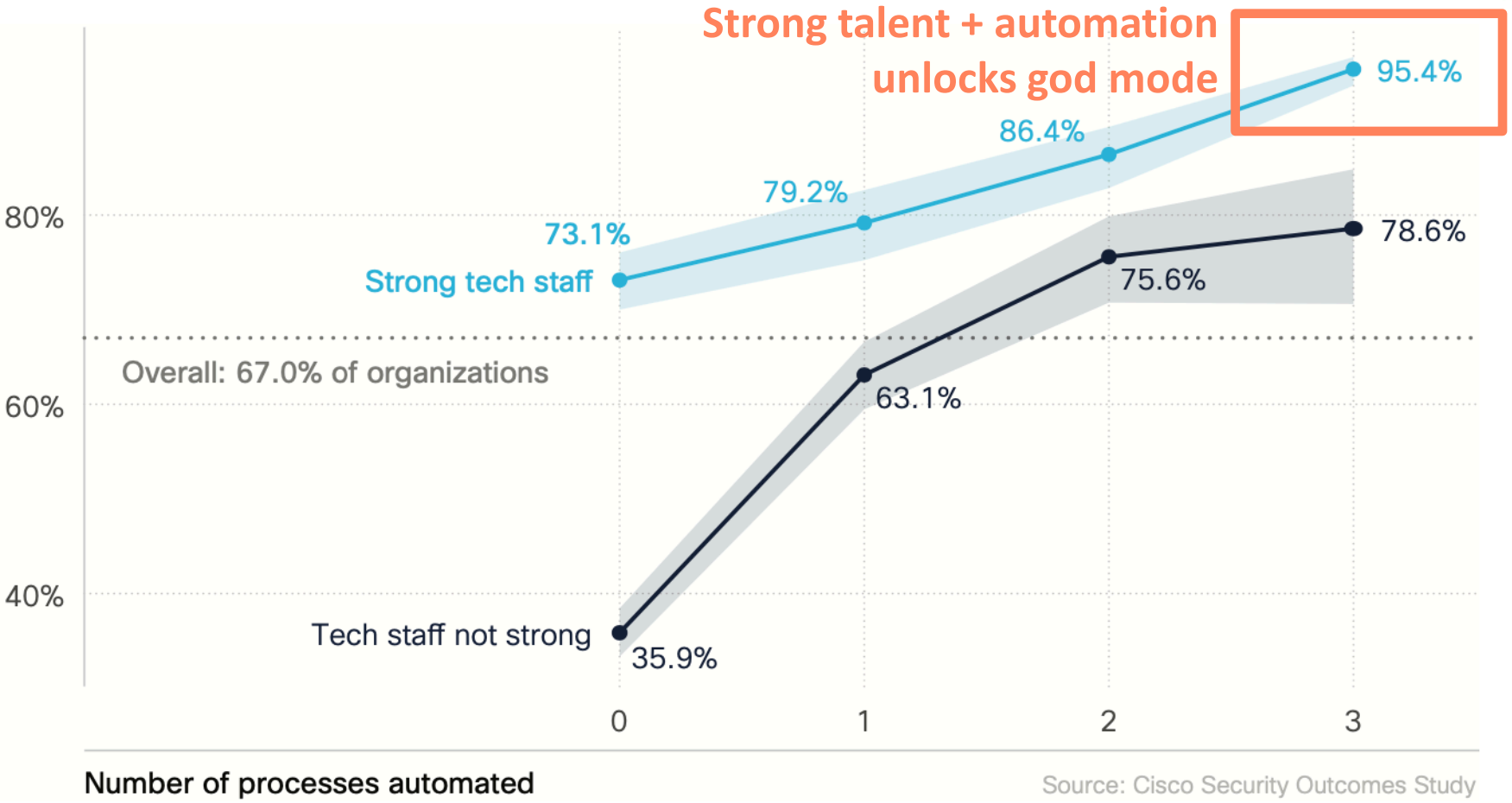
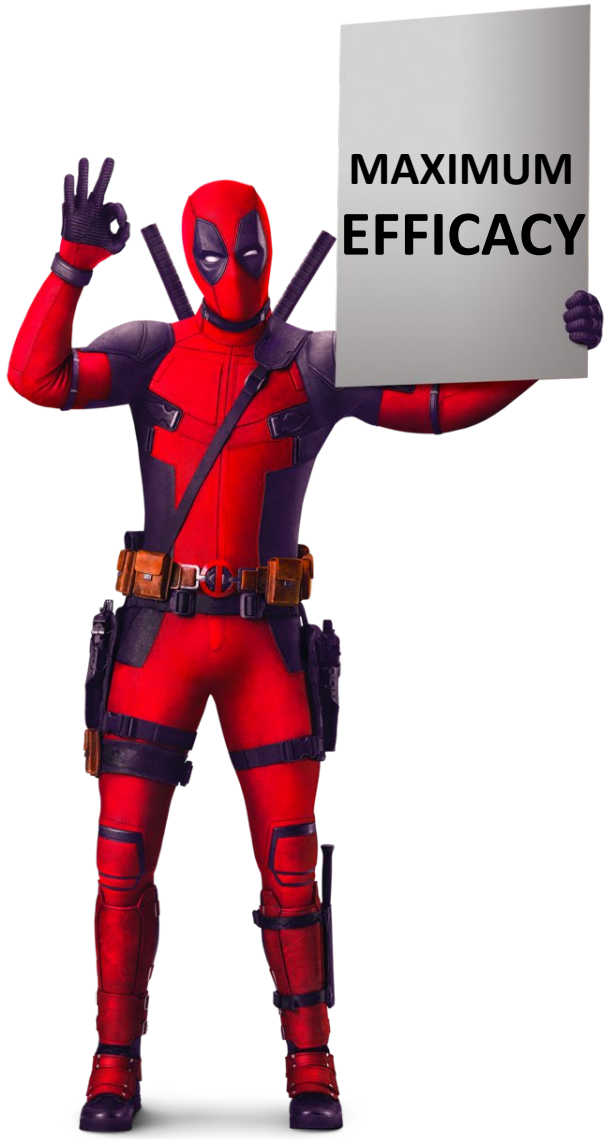


Figure 18: Effect of staffing and automation strength on threat detection and incident response capabilities

How often should we tweak, hack, & hunt?

Answer: More often is more better.

Source: Cisco Security Outcomes Study



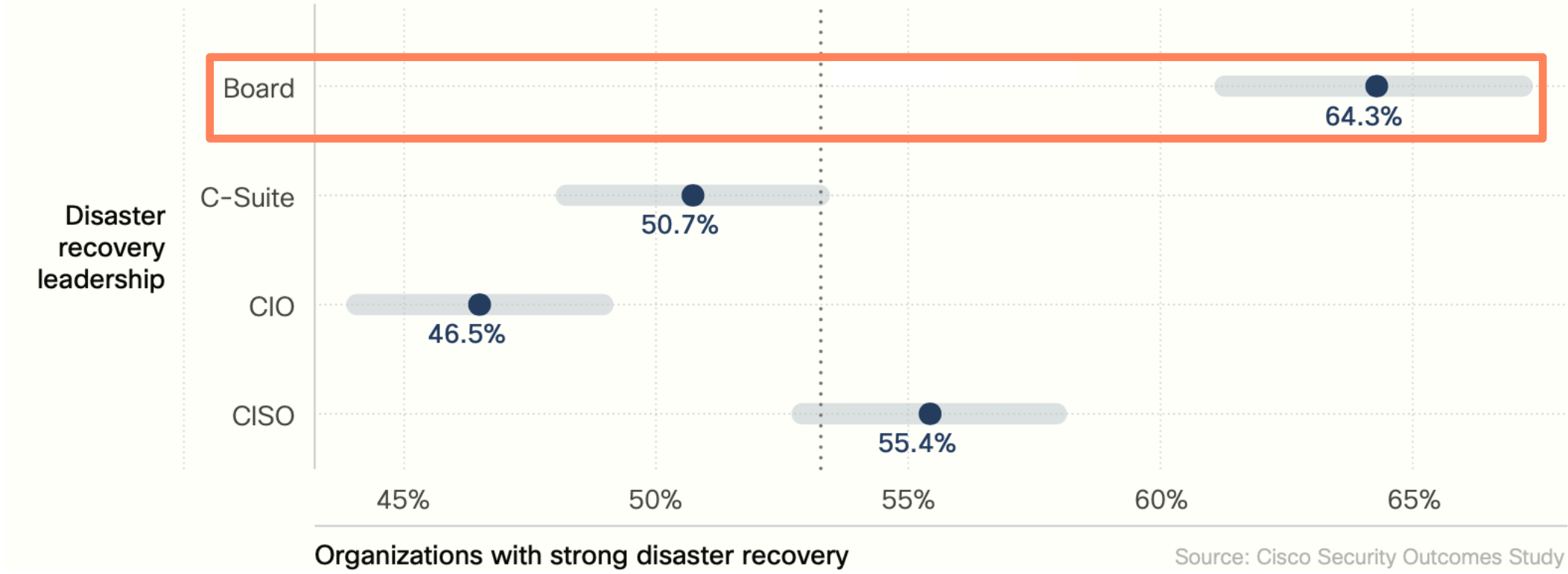
Tips for MAXIMUM EFFICACY!

- When investing in people, process, tech, start with your strength then build all 3.
- Outsourcing vs insourcing SecOps may be more subjective vs objective.
- You'll get more from using automation as a supplement than a substitute.
- Threat intelligence growing pains are better than the numbness of ignorance

Prompt disaster recovery
&
business continuity

The best BCDR programs have Board oversight

Bonus Fact: BCDR performs best when RUN by security



BCDR needs 80% coverage of assets for liftoff

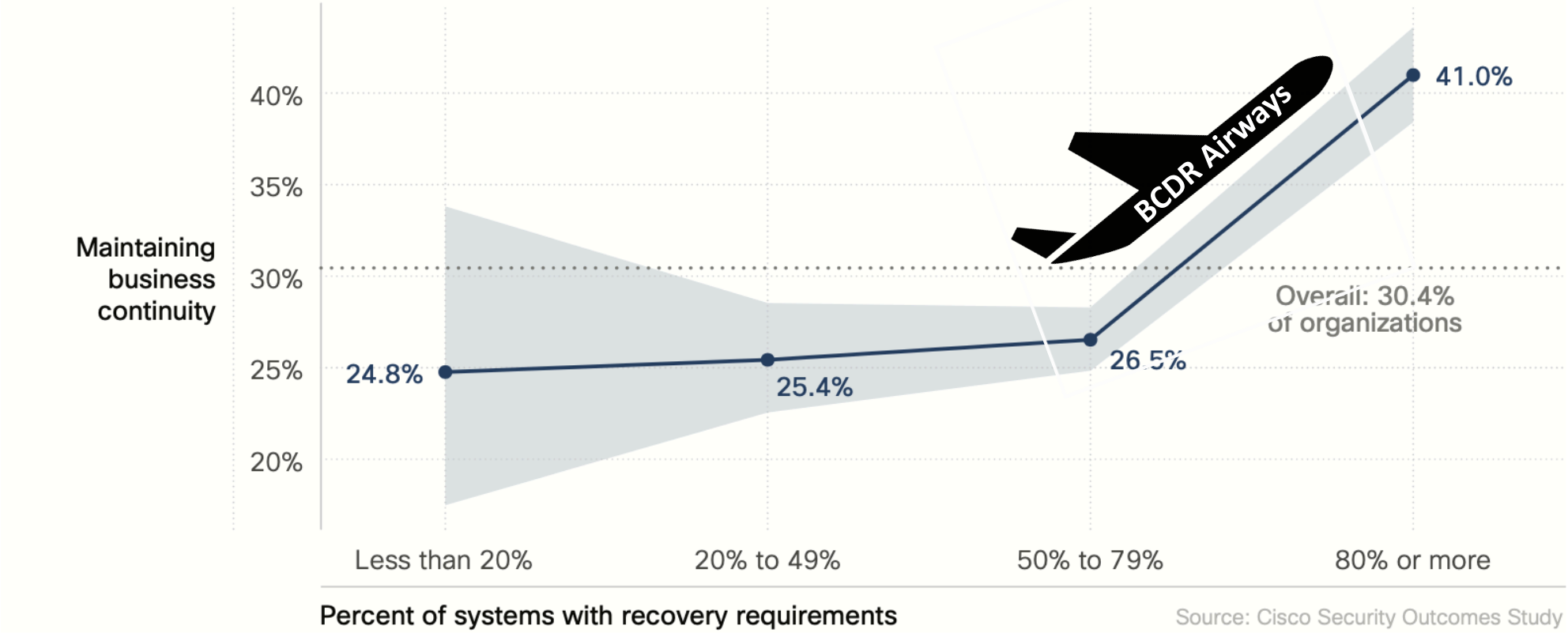
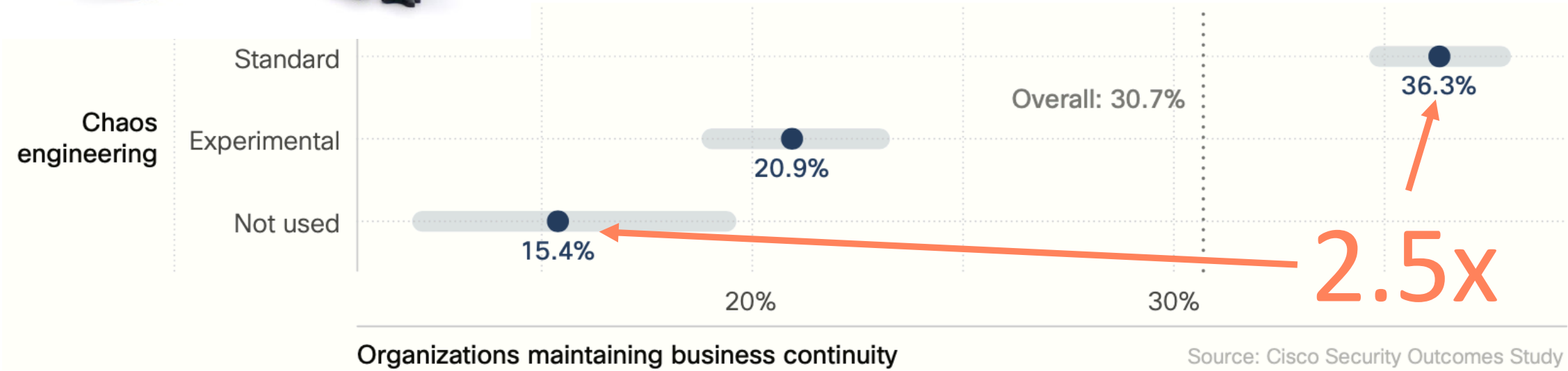


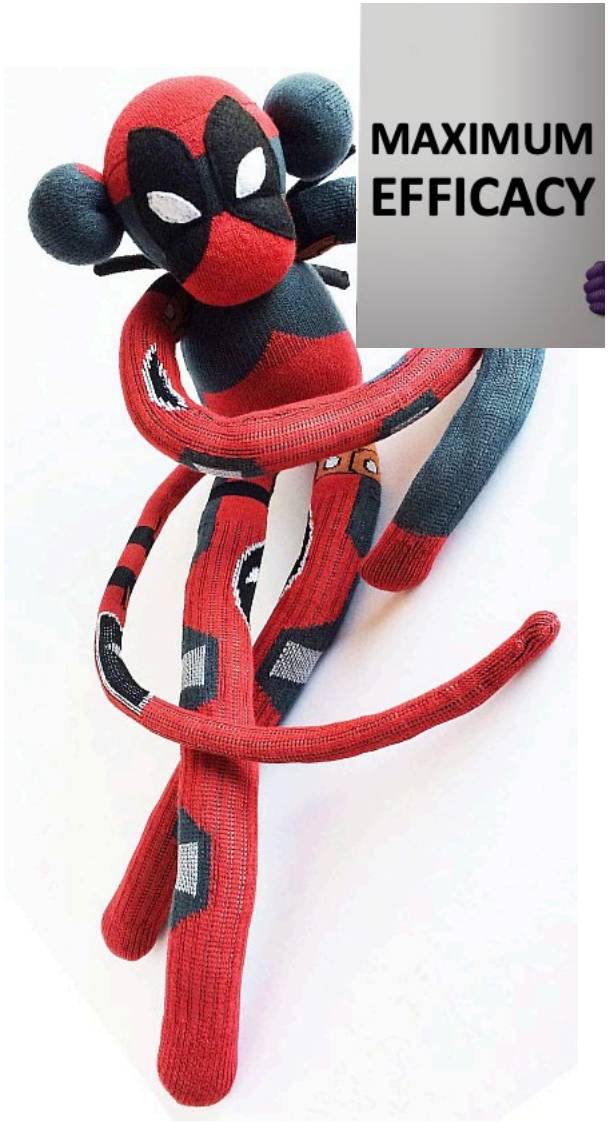
Figure 21: Effect of critical asset coverage on disaster recovery capabilities

Practice doesn't make perfect...
But it will make you a lot more resilient

Add a little chaos to your continuity planning

Organizations that make chaos engineering standard practice are twice as likely to achieve high resiliency





Tips for MAXIMUM EFFICACY!

- For best results, put BCDR under security but report up to Board.
- Cover ALL your assets to truly CYA when disaster strikes.
- Plan, test, test again, and break your way to better BCDR.

RSAConference2022

Summary and takeaways

First: open up a new spreadsheet ...

Apply what you have learned

- In the next six weeks:
  - Download the Security Outcomes Study Vol. 2 from this location: https://www.cisco.com/c/en/us/products/security/security-outcomes-study-vol-2.html
  - Or look at the interactive version of the full matrix here: https://cisco.com/go/securityoutcomes
  - Select outcomes that matter most to you and determine which practices might help you achieve them, and which environments apply most to your organization.
  - Send us feedback: what additional research would you like to see?

Apply what you have learned

- In the next three months:
  - Identify the practices that you can optimize to raise your chances of success:
    - **Proactive tech refresh:** develop a “Buy, Hold, Sell” strategy for your architecture and implement a review loop for future refresh cycles.
    - **Integration:** Look at introducing more automation for your best-integrated technologies, and make sure integration capabilities are part of your purchasing requirements.
    - **SecOps:** Evaluate your SecOps strengths – people, process, and technology – and build from there to maximize efficiency and mature detection and response.
    - **BCDR:** Don’t run your disaster recovery capabilities separately from your other security functions; make sure identification is part of BCDR, threat detection, and other security operations so that everyone is working from the same playbook.

Apply what you have learned

- In the next 6-9 months:
  - Choose metrics for your selected practices and outcomes and create a twice-annual report for at least some of them, so that you get used to evaluating your program and can deliver the results to management whenever needed.
  - Analyze your organization's overall tech architecture strategy against the success factors we listed in the report. Should you evaluate more cloud-based infrastructure? Is more consolidation indicated? Should you switch from performing your own tech integrations to a preferred-vendor strategy?
  - Consider overhauling your BCDR program to introduce more varied and frequent exercises, moving away from the standard playbooks and using more unexpected and unpredictable scenarios. Embrace the chaos!