

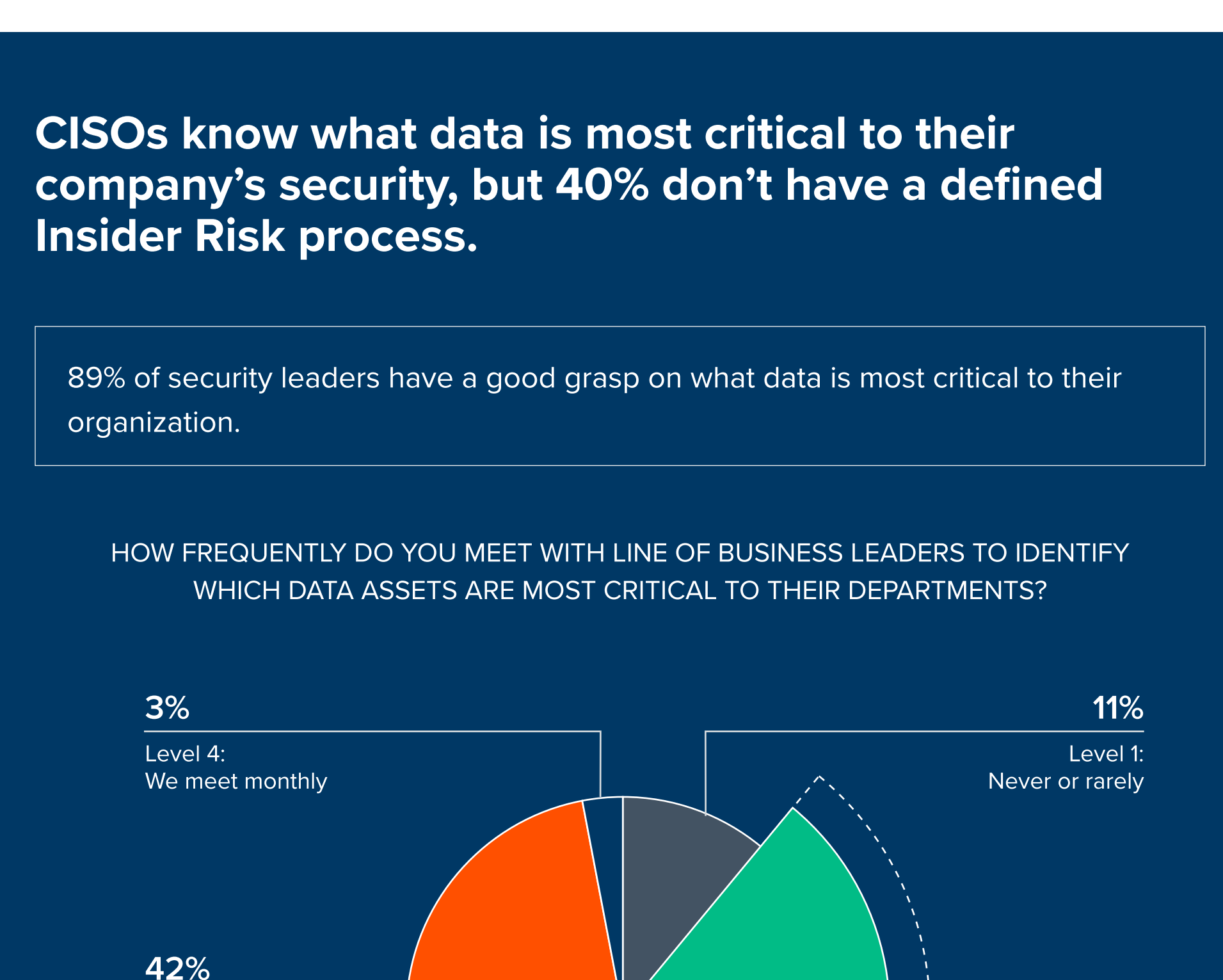
# The Average Enterprise Insider Risk Maturity is Level 2 out of 4

As remote work, cloud adoption and use of emerging technologies continue to expand, so, too, does data exposure surface.

While external threats certainly pose a threat to the security of data, so does Insider Risk. Insider Risk is the result of the way companies work today—the data exposure events (loss, leak, theft, sabotage, espionage) that result from accessing, creating and sharing files and data that jeopardize the well-being and reputation of a company and its employees, customers or partners. To effectively protect data in a modern enterprise it is critical to have technology, processes and procedures dedicated to mitigating Insider Risk, not just malicious threats.

But as this Code42 and Pulse survey of 100 enterprise security leaders finds, **less than 50% of organizations have the technology, structure and processes needed for mitigating Insider Risk—and the average Insider Risk maturity at these companies is at level 2 out of 4.**

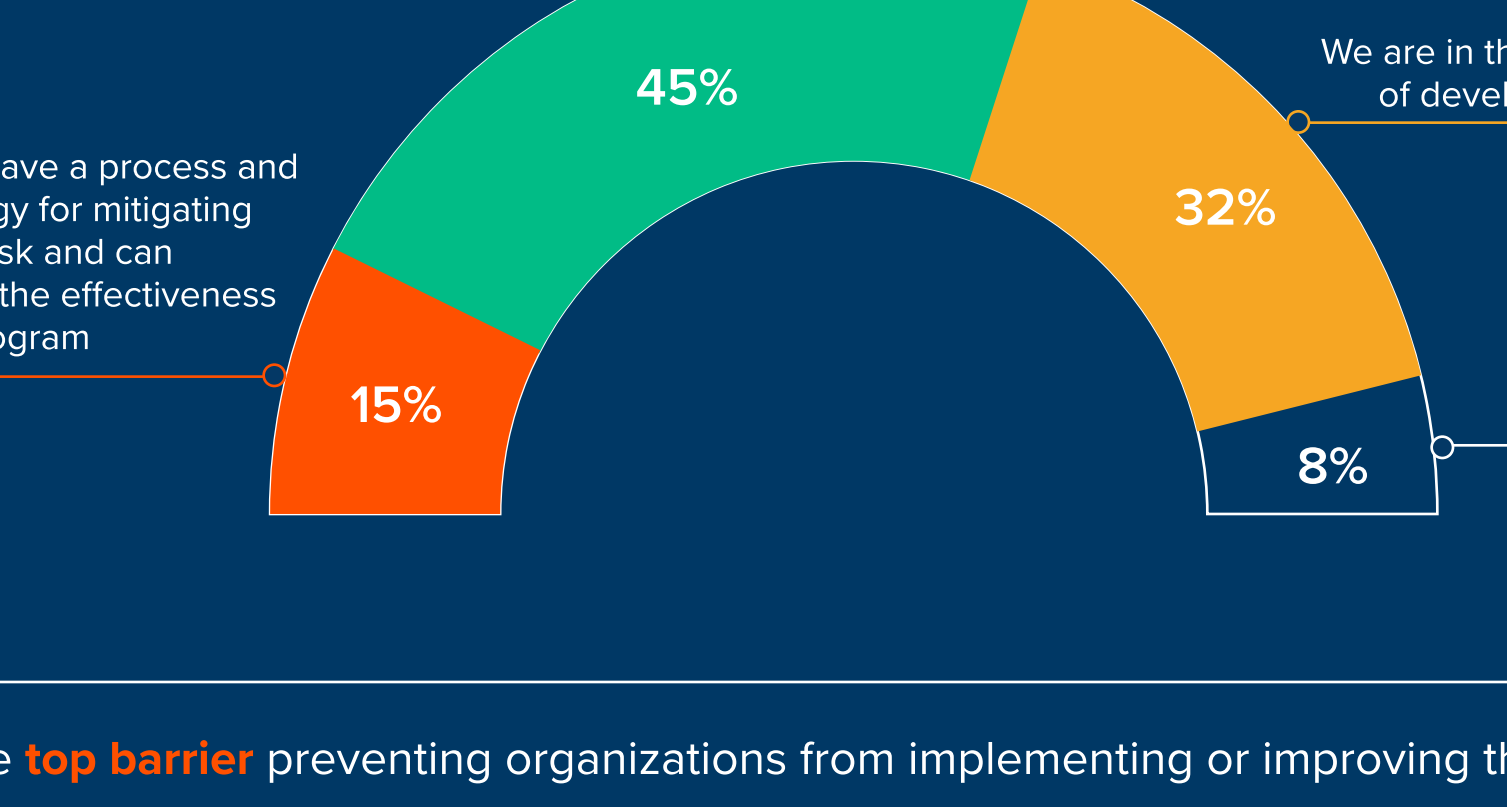
## HOW MATURE ARE GLOBAL ENTERPRISES IN MANAGING INSIDER RISK?



## CISOs know what data is most critical to their company's security, but 40% don't have a defined Insider Risk process.

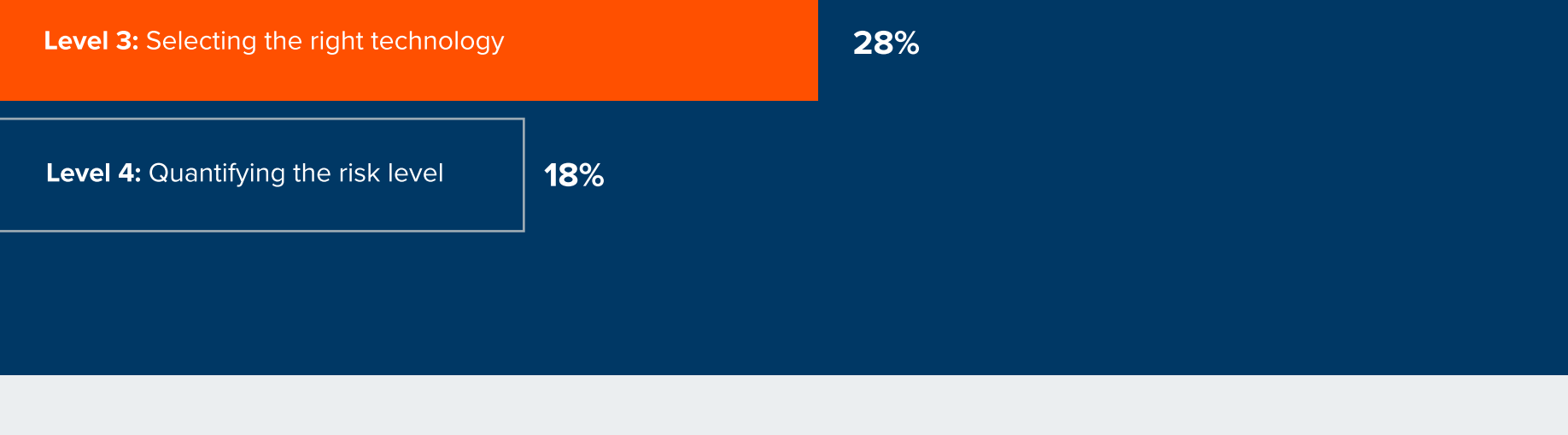
89% of security leaders have a good grasp on what data is most critical to their organization.

## HOW FREQUENTLY DO YOU MEET WITH LINE OF BUSINESS LEADERS TO IDENTIFY WHICH DATA ASSETS ARE MOST CRITICAL TO THEIR DEPARTMENTS?



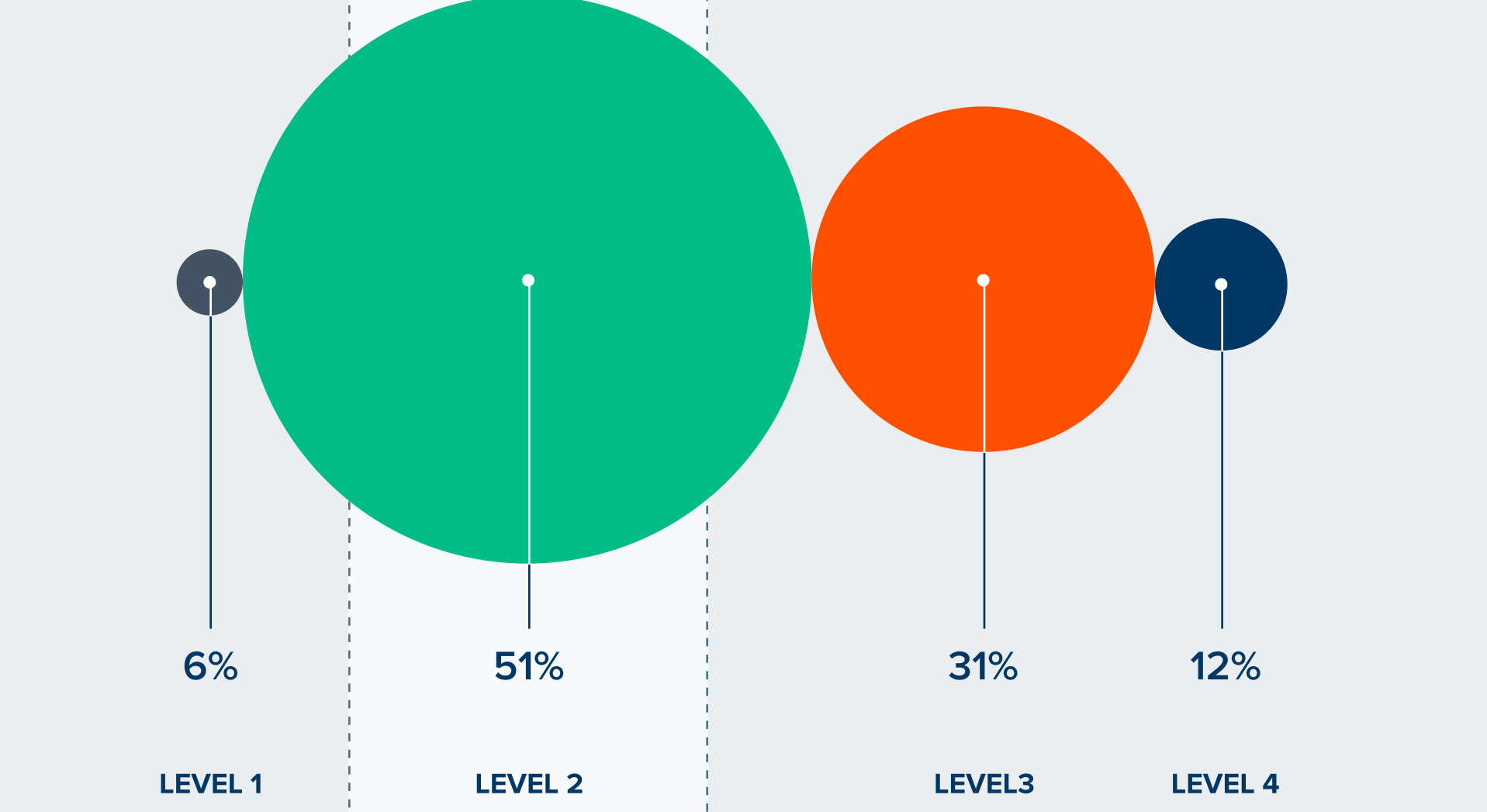
However, less than half (45%) of organizations have a defined and documented process for dealing with Insider Risk, and only 15% use a technology to measure the effectiveness of their Insider Risk program.

## AS PART OF YOUR ORGANIZATION'S BROADER DATA SECURITY STRATEGY, DO YOU HAVE A DEFINED PROCESS FOR MITIGATING INSIDER RISK TO CRITICAL AND PROPRIETARY DATA ASSETS?



The **top barrier** preventing organizations from implementing or improving their Insider Risk program is **defining processes and procedures (46%)—the challenge most closely associated with Level 2 of Insider Risk maturity.**

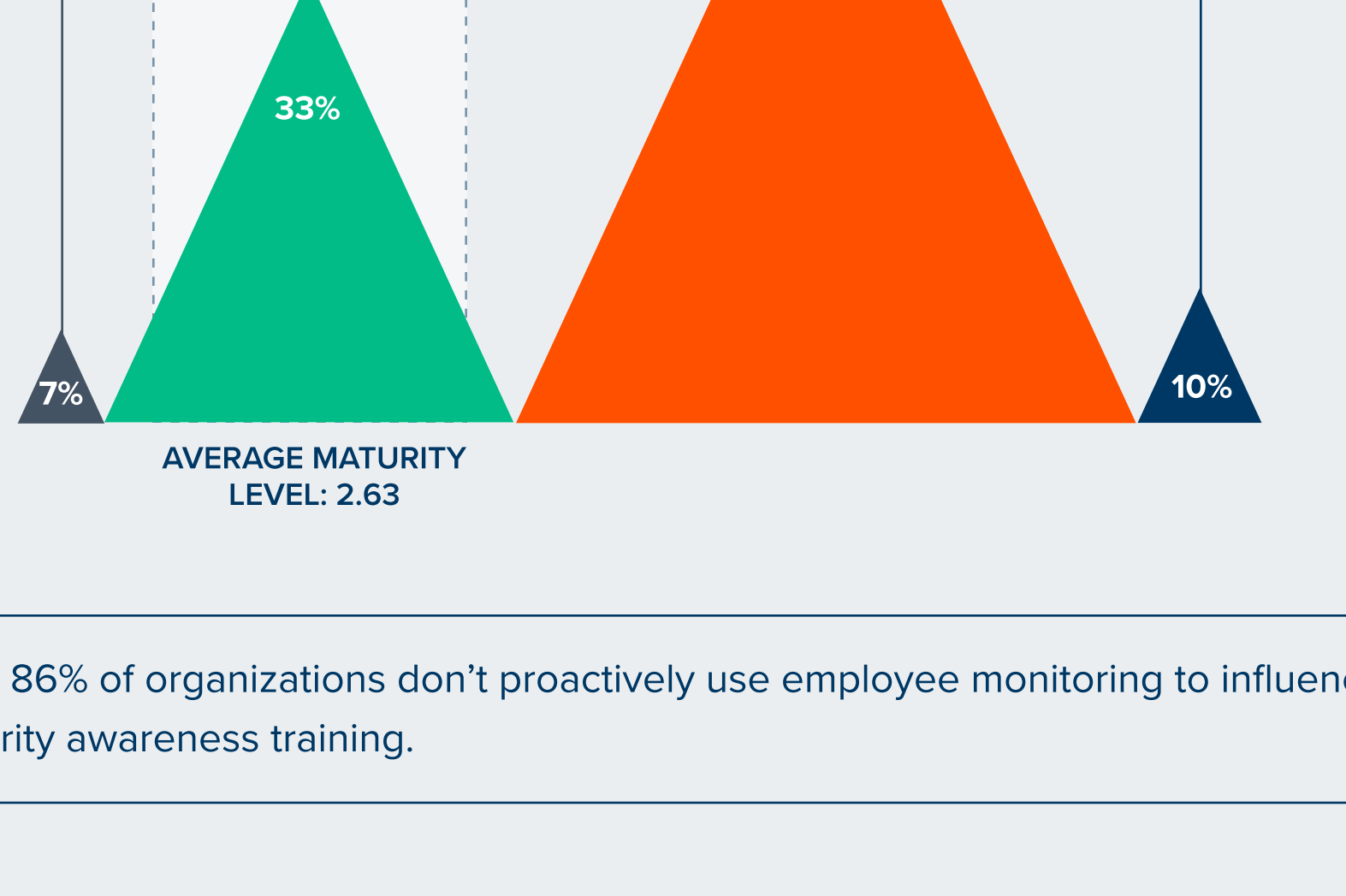
## WHAT IS YOUR ORGANIZATION'S BIGGEST BARRIER TO IMPLEMENTING OR IMPROVING YOUR INSIDER RISK PROGRAM?



## Most organizations have Acceptable Use policies, but few have proactive processes to monitor employees for policy adherence.

94% of organizations have implemented Acceptable Use policies for different data uses (i.e. cloud storage, endpoint use, cloud computing, removable storage).

## HAVE YOU CREATED AND ENFORCED ACCEPTABLE USE POLICIES FOR CLOUD COMPUTING, REMOVABLE MEDIA, AND CLOUD STORAGE?



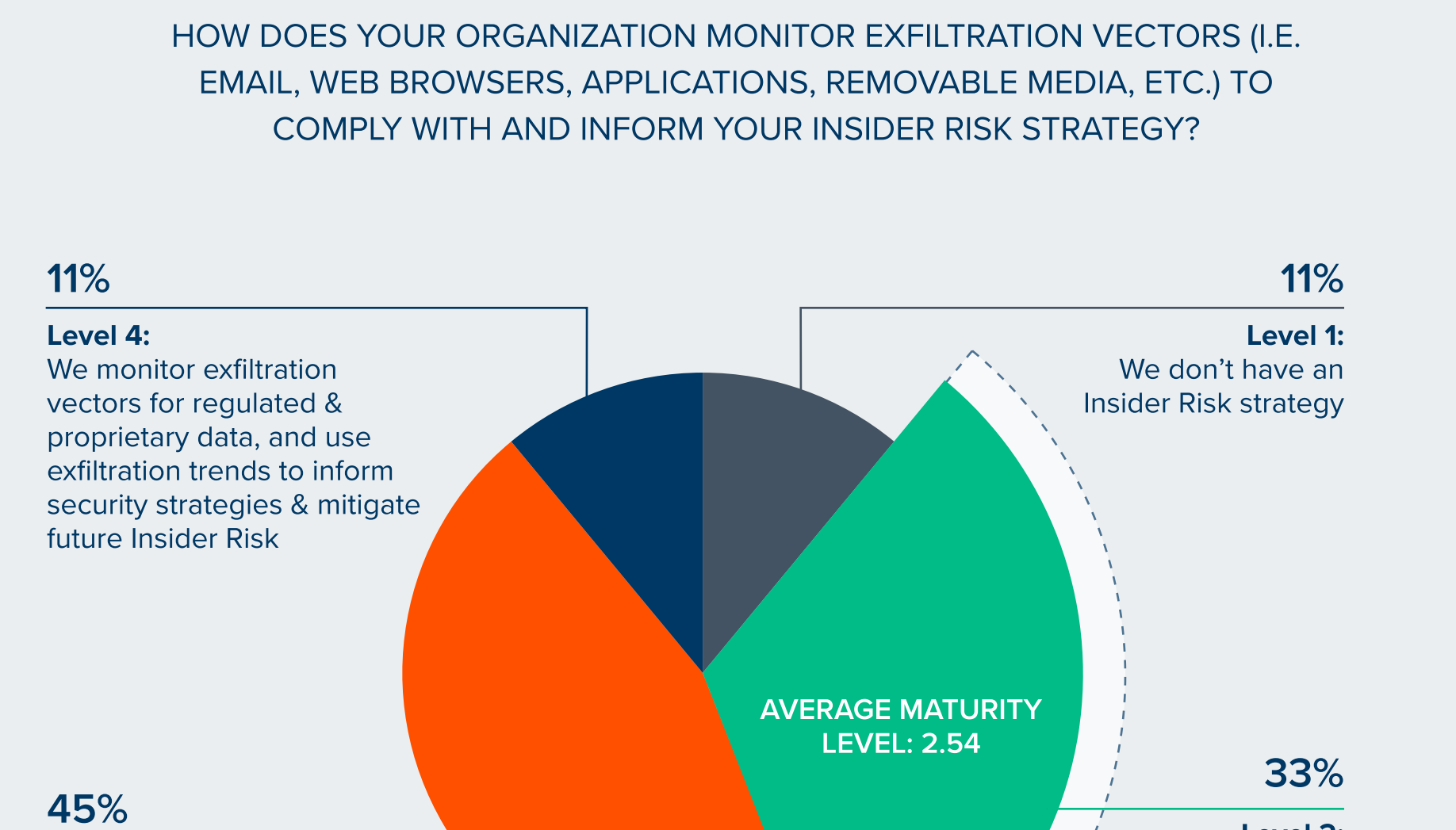
But, only 10% of organizations monitor whether new employees adhere to those policies.

## HOW DOES YOUR ORGANIZATION CURRENTLY DISCUSS AND MITIGATE INSIDER RISK DURING YOUR EMPLOYEE ONBOARDING PROCESS?



Plus, 86% of organizations don't proactively use employee monitoring to influence security awareness training.

## WHICH TYPE(S) OF INSIDER RISK INCIDENTS DO YOU ANALYZE AND INCORPORATE IN SECURITY AWARENESS TRAINING?



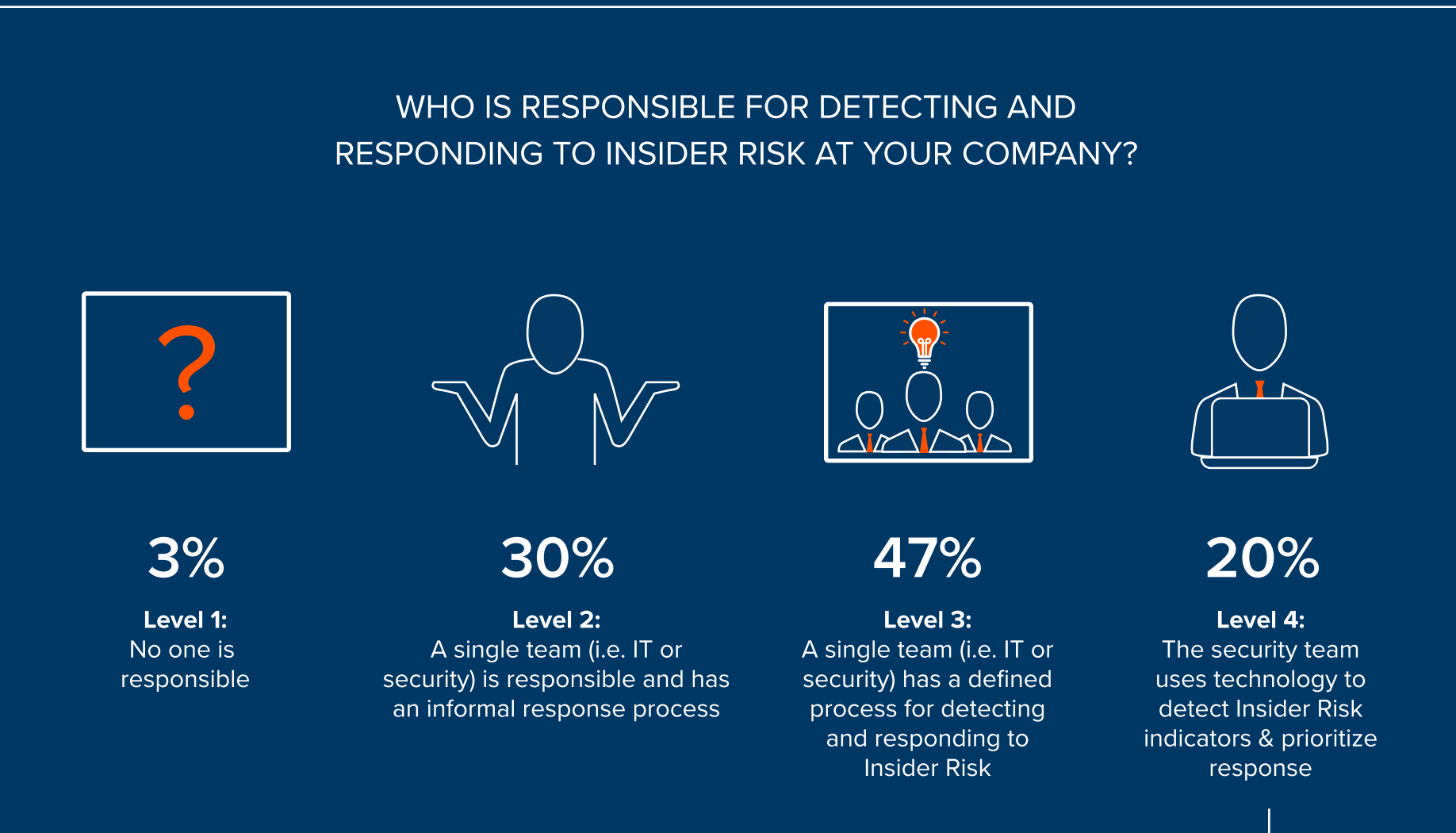
When employees leave the organization, only 8% of security leaders use Insider Risk technology to monitor the employee's behavior prior to departure.

## HOW WOULD YOU BEST DESCRIBE YOUR ORGANIZATION'S PROCESS FOR PROTECTING DATA FROM INSIDER RISK WHEN EMPLOYEES DEPART?



As well, only 11% of these teams are using data exfiltration trends analyzed through automated vector monitoring to inform their Insider Risk strategy.

## HOW DOES YOUR ORGANIZATION MONITOR EXFILTRATION VECTORS (I.E. EMAIL, WEB BROWSERS, APPLICATIONS, REMOVABLE MEDIA, ETC.) TO COMPLY WITH AND INFORM YOUR INSIDER RISK STRATEGY?



## Security teams aren't using technology to simplify Insider Risk monitoring and remediation.

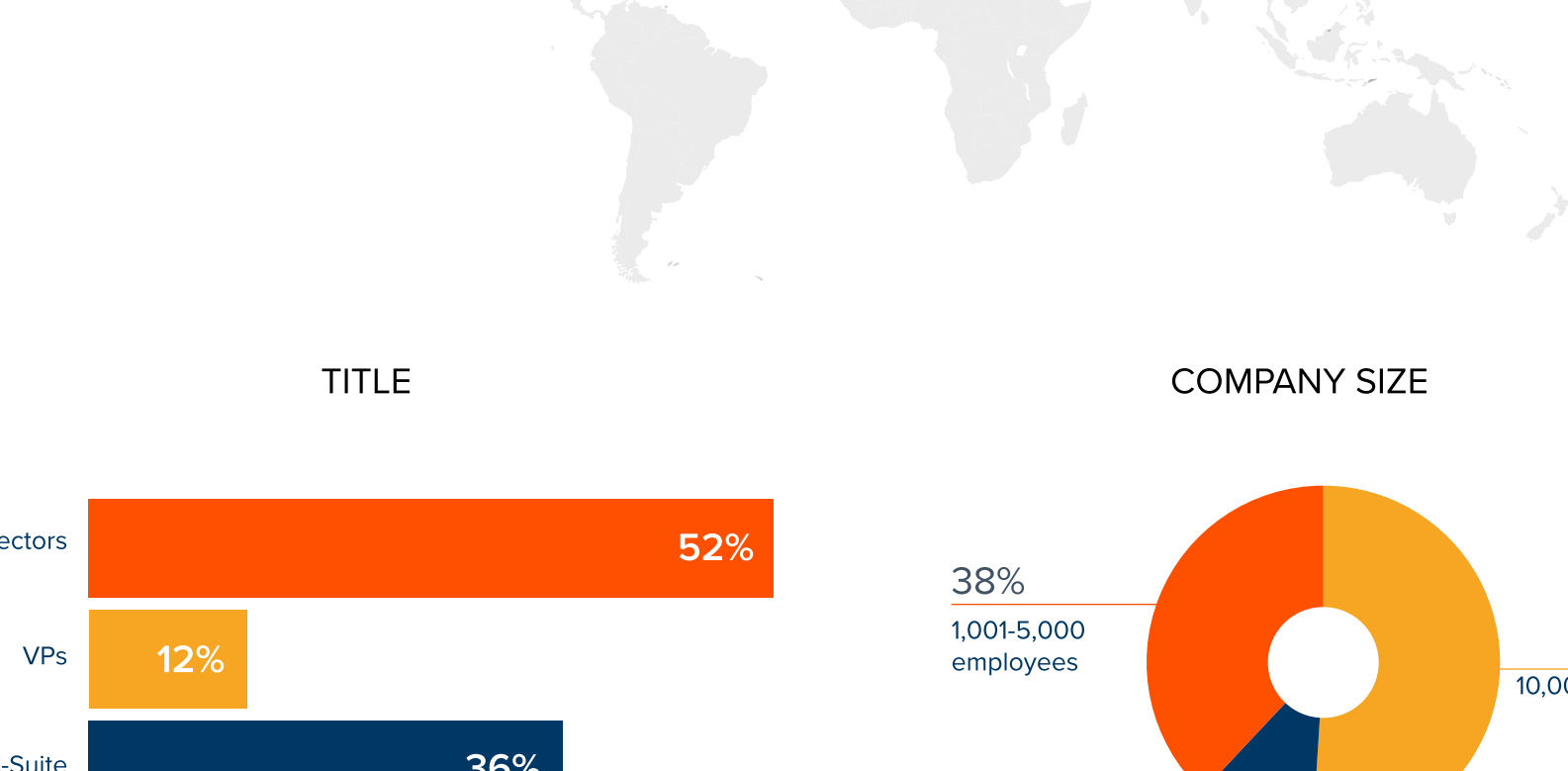
Further, during an Insider Risk investigation, **only 8% of these dedicated teams use technology to make evidence collection easy and centralized in a single location.** 42% are collecting evidence manually.

## WHICH OF THE FOLLOWING BEST DESCRIBES HOW YOUR COMPANY DOCUMENTS EVIDENCE DURING AN INSIDER RISK INVESTIGATION?



Most commonly, a single team—either IT or security—is responsible for detecting and responding to Insider Risk indicators (47%). **However, only 20% use a tool to automate monitoring and prioritize response.**

## WHO IS RESPONSIBLE FOR DETECTING AND RESPONDING TO INSIDER RISK AT YOUR COMPANY?



In the end, **94% of security teams use technology to monitor employees to reduce Insider Risk—but only 11% use the data they collect to improve their Insider Risk posture.**

## HOW WOULD YOU BEST DESCRIBE YOUR CORPORATE CULTURE WITH RESPECT TO THE MONITORING OF EMPLOYEE ACTIVITY TO MITIGATE FUTURE INSIDER RISKS?



Learn more about how Code42 Incydr™ can support security maturity through continual improvement of your Insider Risk posture, visit [Code42.com/Solutions/Insider-Risk/](https://code42.com/Solutions/Insider-Risk/)

## Respondent breakdown

### GEOGRAPHY



### TITLE



### COMPANY SIZE

