Why API Security Cannot Wait Until Production

Christopher M. Steffen, CISSP, CISA
VP Research – Information Security, EMA

Colin Domoney
Chief Technology Evangelist, 42Crunch

Introduction

Our Speakers

Christopher Steffen

VP Research – Information Security
Enterprise Management Associates

CISSP, CISA
@CloudSecChris

Colin Domoney

Chief Technology Evangelist
42Crunch

Editor of APISecurity.io
@colindomoney

Housekeeping Rules

- All attendees muted
- Questions via Q&A
- Recording will be shared after

Special offer - Copy of Research!

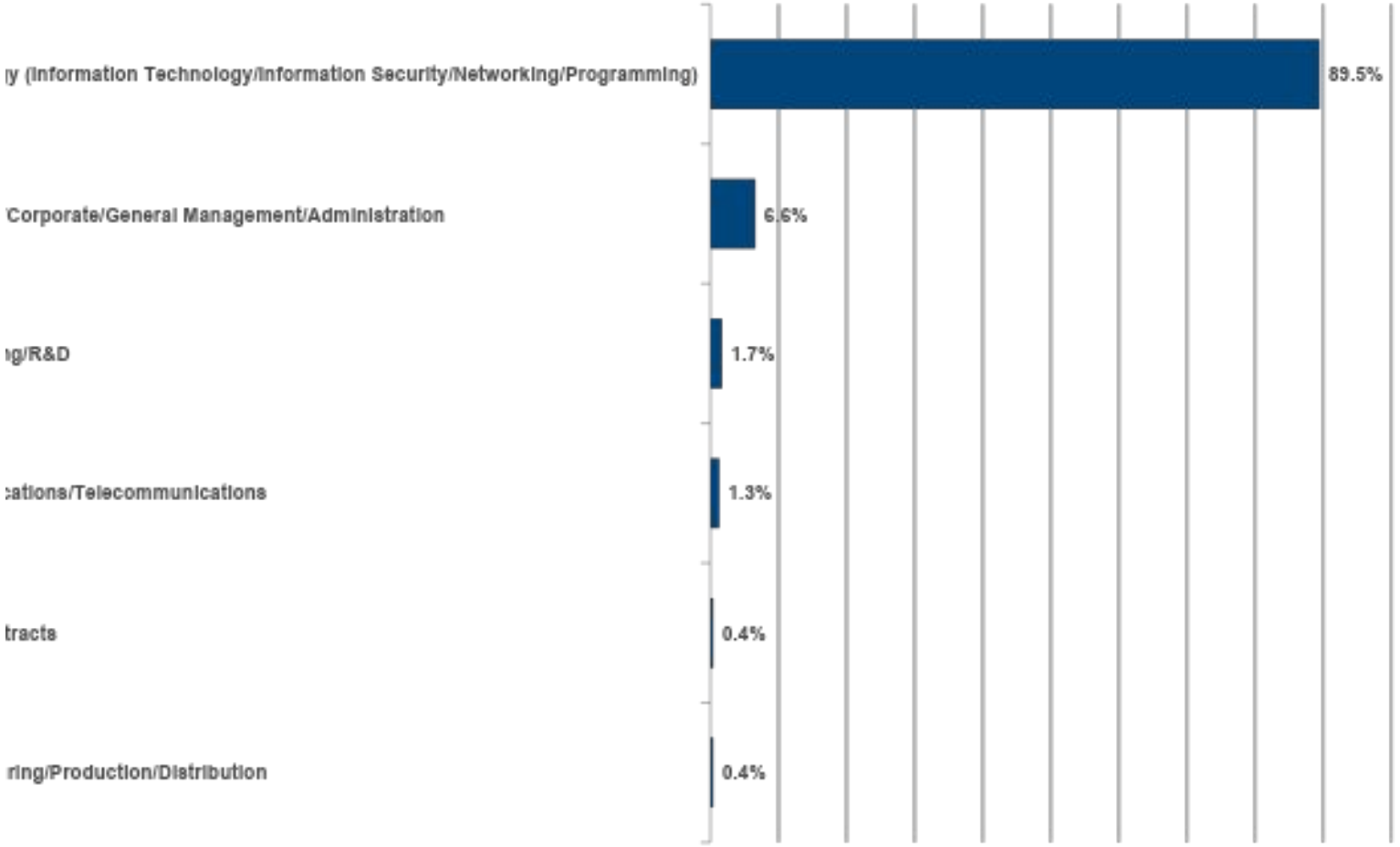
All attendees get a free copy of the Enterprise Management Associates Research report emailed to them after this webinar.

Agenda

- Introduction to the study: Methodologies & Demographics
- Research Results & Analysis
- Benefits
- Downloads

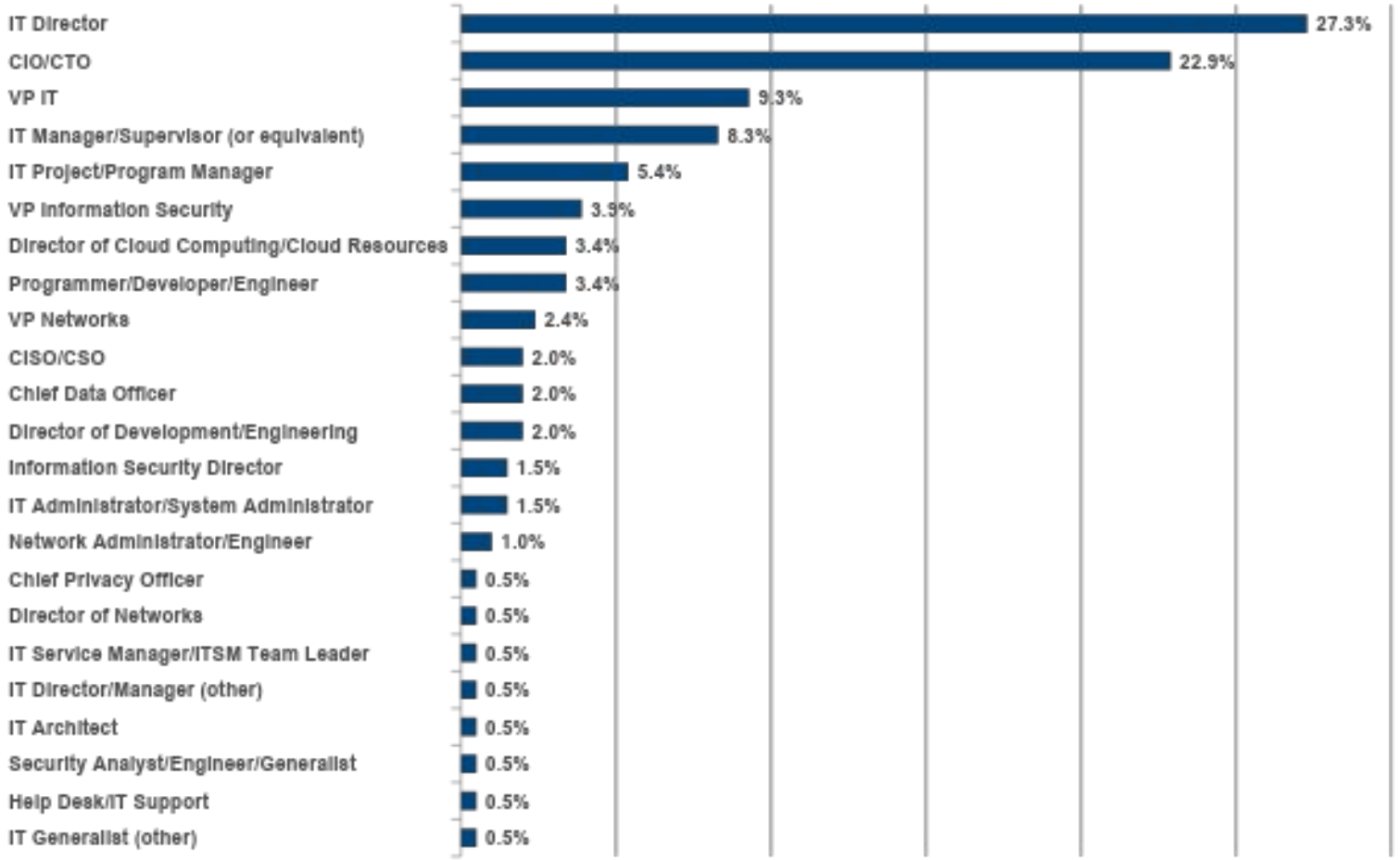
Research Methodologies and Demographics

Which of the following best describes the department or functional area in which you work?



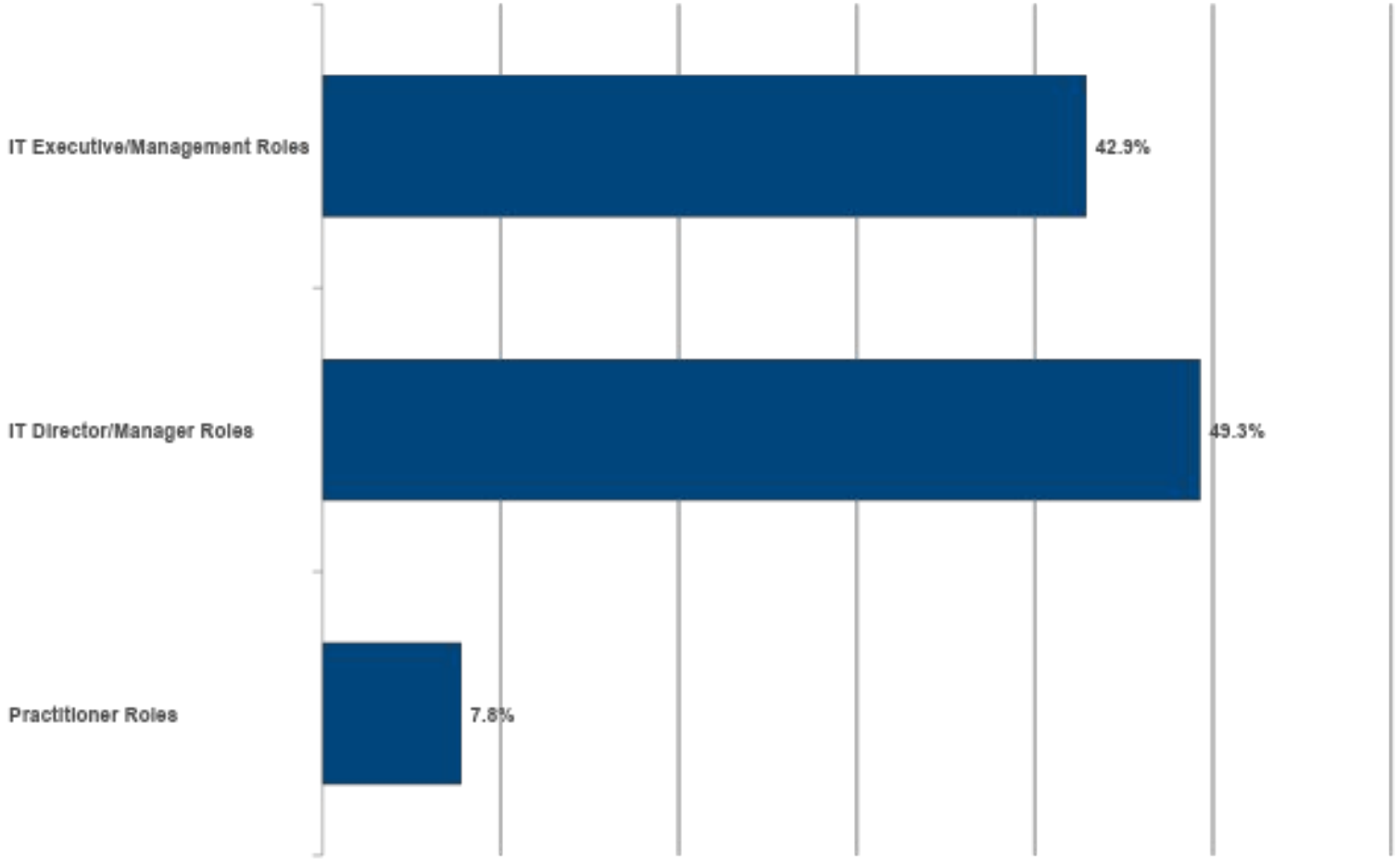
© 2023 Enterprise Management Associates, Inc.

You indicated that your department is IT-related. Which of the following BEST describes your specific role?



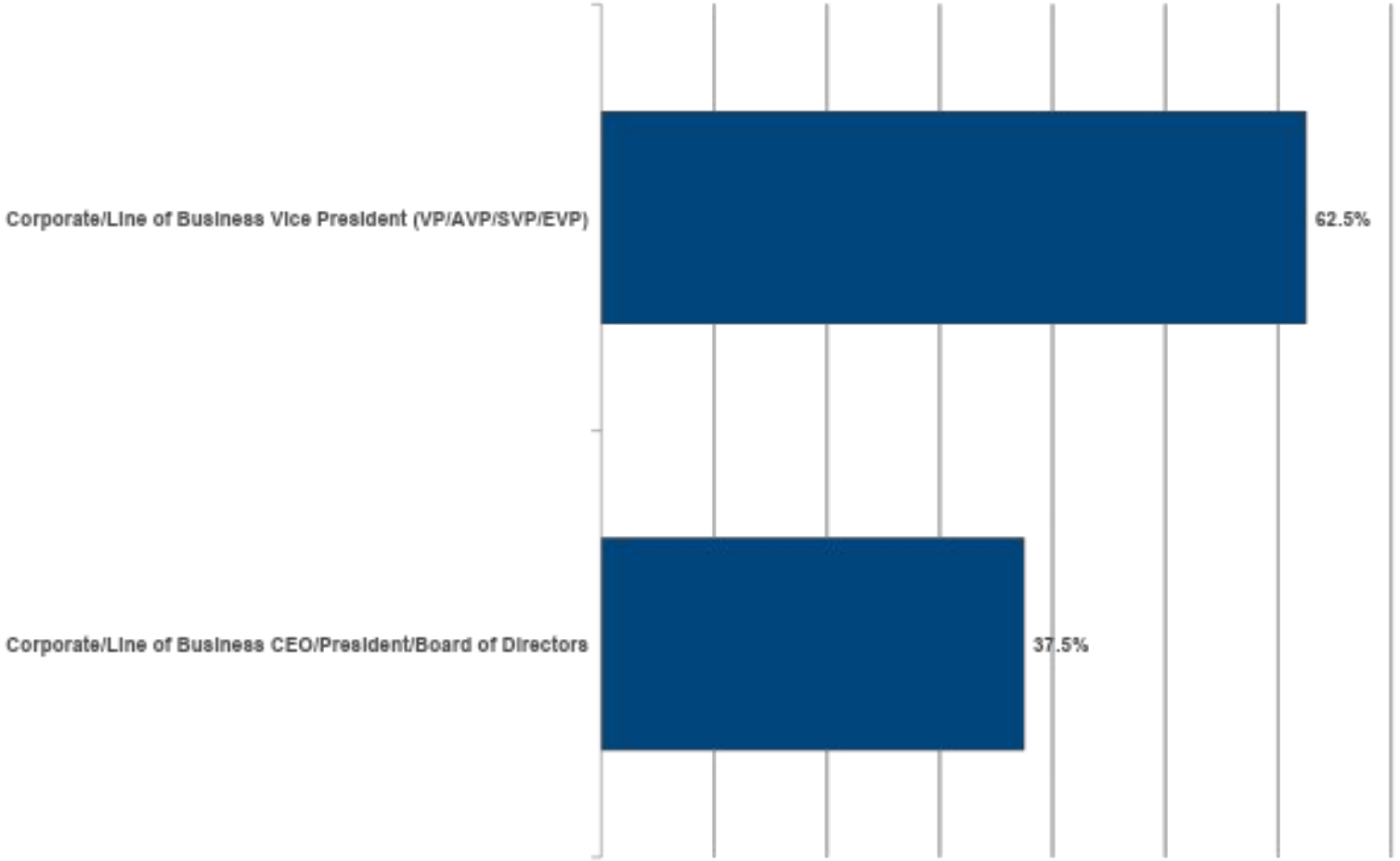
© 2023 Enterprise Management Associates, Inc.

You indicated that your department is IT-related. Which of the following BEST describes your specific role?



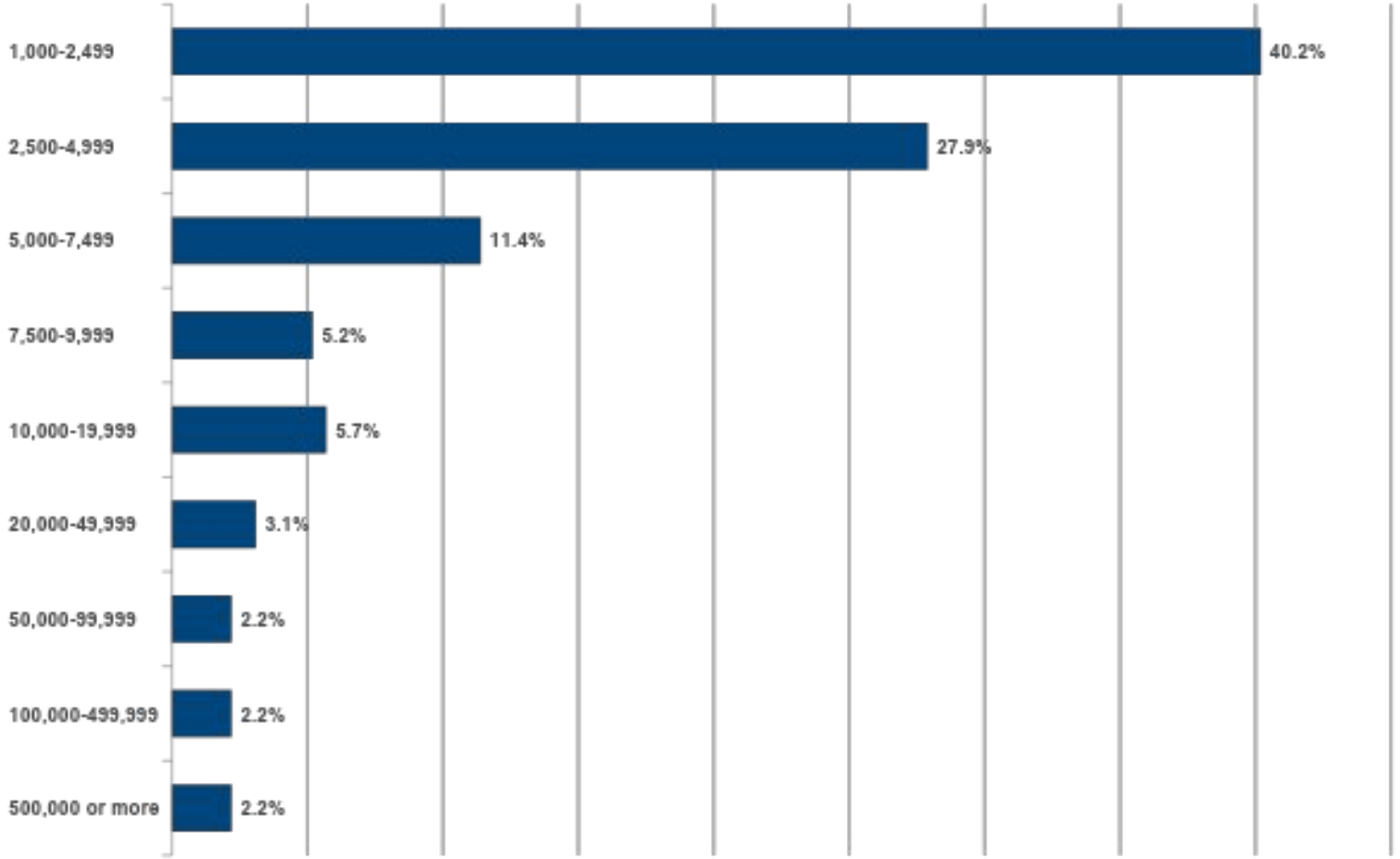
© 2023 Enterprise Management Associates, Inc.

Which of the following best describes your specific role in your organization?



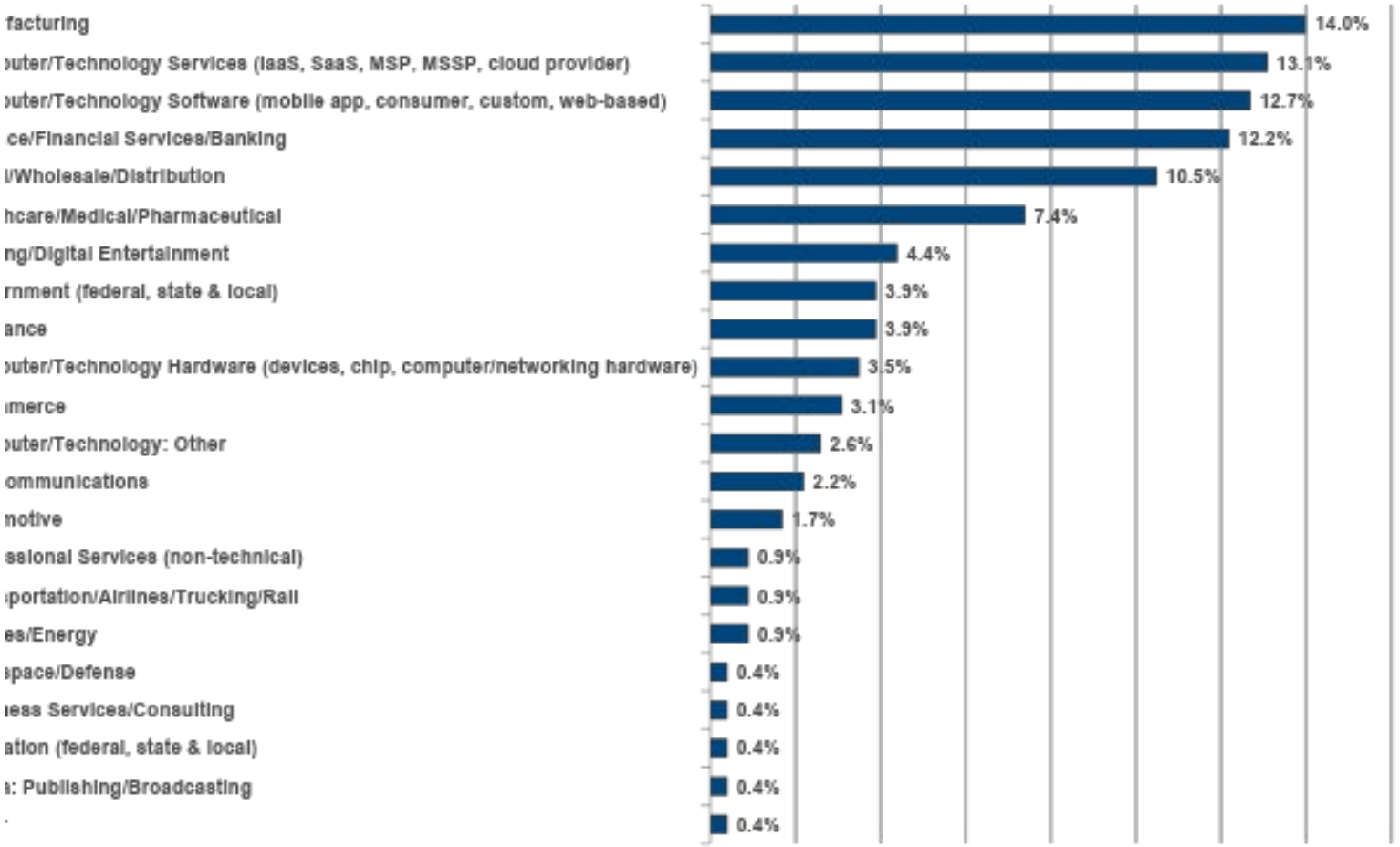
© 2023 Enterprise Management Associates, Inc.

In total, how many employees are currently working in your organization?



© 2023 Enterprise Management Associates, Inc.

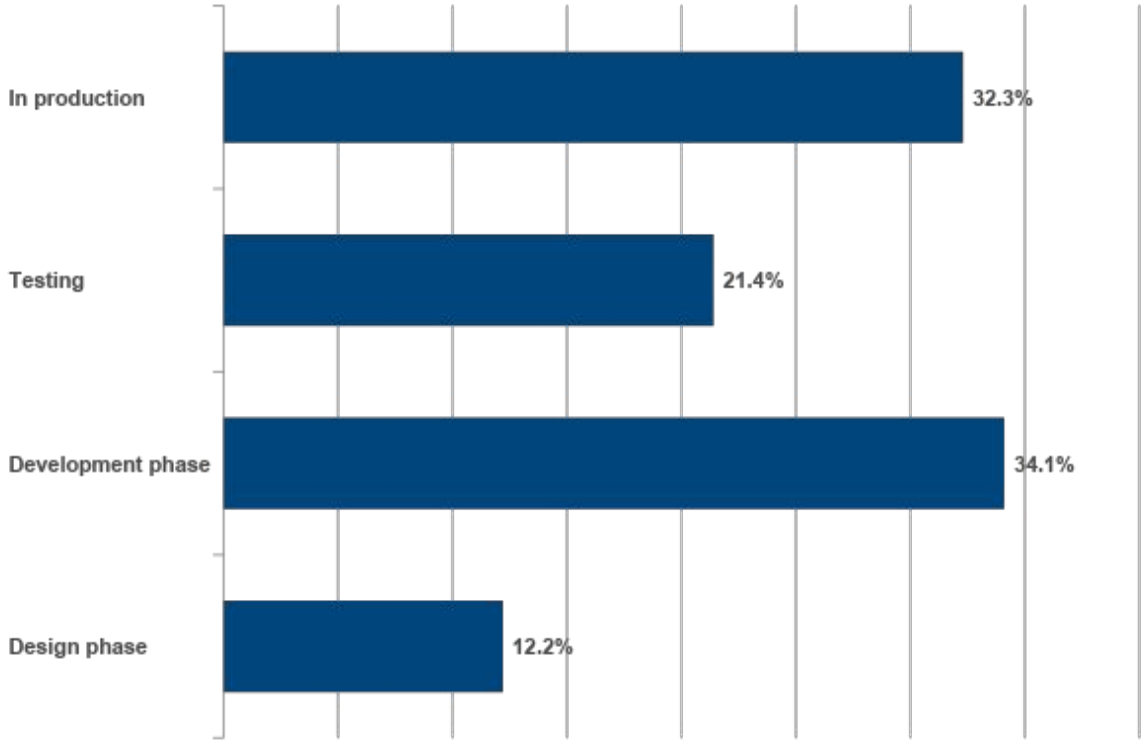
Which of the following best describes your organization's primary industry?



© 2023 Enterprise Management Associates, Inc.

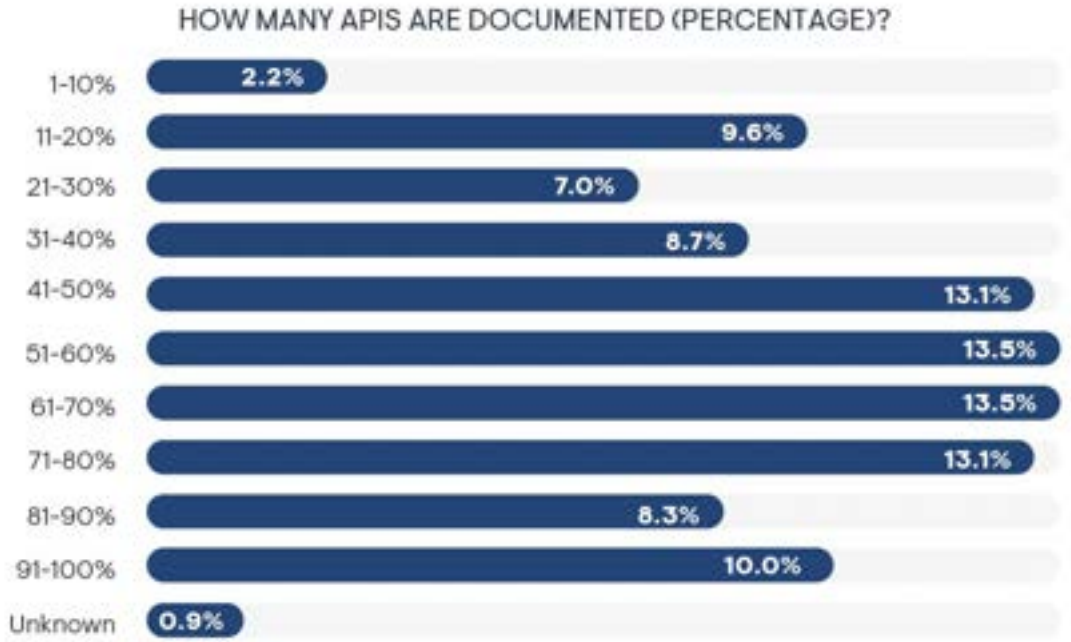
Research Results & Analysis

OBSERVATION #1



32% stated that API controls are first implemented in production

OBSERVATION #2

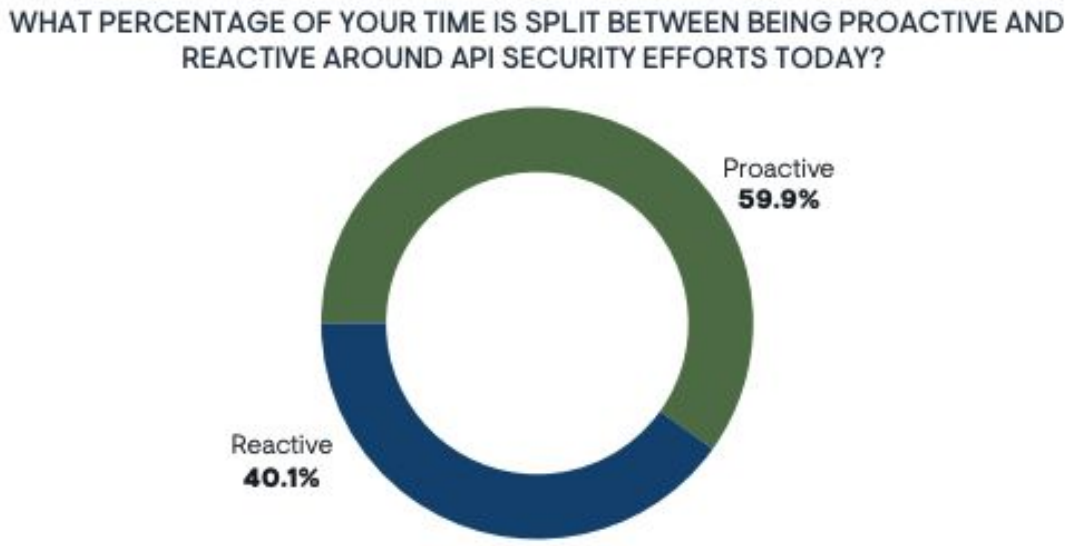


41% stated that fewer than 50% of their APIs were documented

OBSERVATION #3

31% stated their primary concern is a need for more collaboration between DevOps, SecOps, security teams & API experts

OBSERVATION #4



60-40 split between proactive and reactive API Security efforts

WHY THERE IS A SEISMIC GAP IN API SECURITY

Enterprise suffers from a false sense of security

- Current security tooling hides the issue

API attacks are specific and traditional solutions cannot prevent them

- AST/DAST Tooling
- Web Application Firewalls
- API Management Platforms

API Attacks focus on the Data NOT perimeter

New architectures and deployment patterns means 1 App = 10 APIs

- New microservices based architectures and deployment patterns results in an increased volume of APIs.
- Manual security is not an option

42Crunch

AUTOMATES & SCALES

enterprise API Security.

42Crunch platform

EMPOWERS

enterprises to adopt

a DevSecOps approach

to API Security.

LOVED BY DEVELOPERS, TRUSTED BY SECURITY

- A true DevSecOps' experience with integration of Dev, Ops and Security teams across the enterprise
- No false positives/negatives means no security reviews, manual testing, vulnerability assessment
- API Governance: All APIs comply with OpenAPI specification
- Single source of truth - Each API has its specific API Security contract
- Automation/Scalability to secure 1,000s of APIs

The only API Security Platform offering

API AUDIT, SCAN AND PROTECTION

FOR END-TO-END API SECURITY

THE DEVELOPER FIRST API SECURITY PLATFORM

SECURITY MANAGEMENT & GOVERNANCE

Visibility & control of security policy enforcement throughout API lifecycle for security teams.

API AUDIT

Lock down your API's definitions to reduce the attack surface and remove potential security gaps.

API SCAN

Dynamic runtime testing of your API to ensure compliance with API Contracts.

API PROTECT

Protect each API with an API micro-firewall to distinguish legitimate traffic from malicious API attacks.

INTEGRATED ACROSS API LIFECYCLE

Continuous security enforcement across IDE, CI/CD and at runtime.

IDE/DEV TOOLS

CI/CD

CUSTOM REPORTING

SCRIPTING

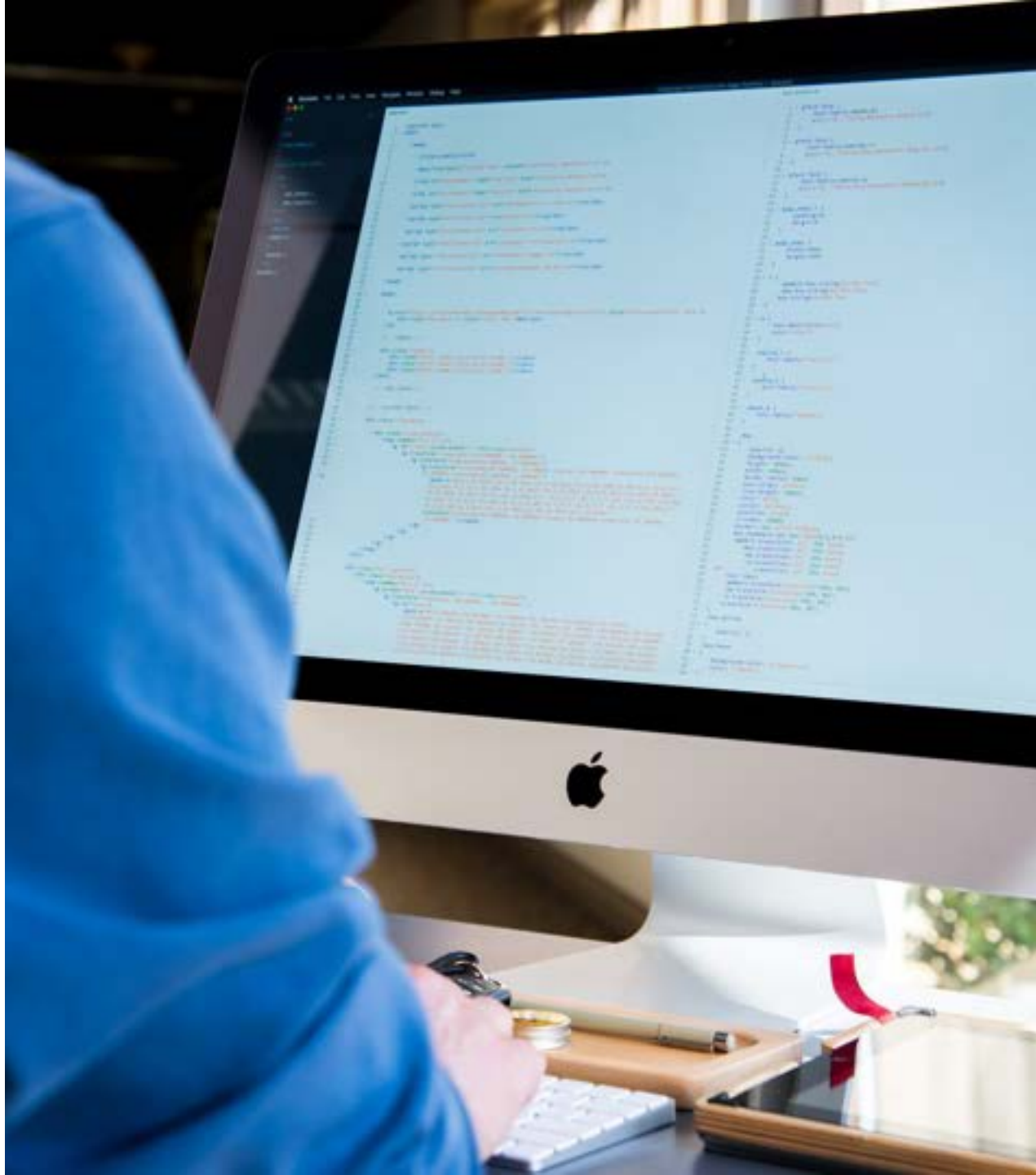
MONITORING

Empower Developers

- “No shame, no blame”: Establish a culture to reward
- Tools which can be used from developer flow
  - Limited false positives
  - Easy to use from IDEs
  - Educate/ Provide remediation guidelines
  - Interactive Security Testing

Benefits

- Increased productivity
- Meantime to fix issues is reduced significantly (> 50%)



Trust but Verify

- App Sec teams want to ensure corporate security standards are respected
- Allow them to enforce policies of what is acceptable or not, for example:
    - Basic Authentication is forbidden
    - JWTs must be signed with PS256
    - All inbound parameters must be constrained by patterns and limits
- Fast execution
- Results visible to dev teams as early as possible.

BUILDING A GLOBAL API SECURITY COMMUNITY

APISecurity.io is the API security industry's leading community newsletter

- A weekly newsletter for industry security and development professionals with insights to the latest API breaches, vulnerabilities and regulations.
- Curated and syndicated by 42Crunch it is subscribed to by over 10,000 cybersecurity & integration professionals, industry analysts, journalists and influencers globally.

Documentation

42Crunch Enhancing API Security of API Management Vendors

apigee axway Kong WSO2

API Gateway users can reduce manual tasks and automate security into the API DevSecOps workflow in order to get secure code quickly out the door and into production.

Download Technical Solution Briefs:

https://42crunch.com/api-gateways-integrations/

Free Copy of Research

All attendees receive a free copy of the Enterprise Management Associates Research report emailed to them after this webinar.

Questions?

Thank you

Christopher Steffen

Colin Domoney

WHY API SECURITY CANNOT WAIT UNTIL PRODUCTION